Red Hat Enterprise Linux 3

Handbuch zur System-Administration

Red Hat Enterprise Linux 3: Handbuch zur System-Administration


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

rhel-sag(DE)-3-Print-RHI (2003-07-25T17:10)

Der GPG-Code des security@redhat.com Schlüssels lautet:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

Inhaltsverzeichnis

Einführung

Willkommen im *Red Hat Enterprise Linux Handbuch zur System-Administration*.

Das *Red Hat Enterprise Linux Handbuch zur System-Administration* enthält Informationen darüber, wie Sie die Konfiguration Ihres Red Hat Enterprise Linux-Systems an Ihre individuellen Bedürfnisse anpassen können. Wenn Sie hierzu eine schrittweise und aufgabenspezifische Anleitung wünschen, dann ist dies das richtige Handbuch für Sie. Hier werden viele Themen behandelt, wie zum Beispiel folgende:

- Einrichten einer Netzwerk-Schnittstellenkarte (NIC)
- Ausführen einer Kickstart-Installation
- Konfigurieren von Samba-Shares
- Verwalten Ihrer Software mit RPM
- Ermitteln der Systeminformationen
- Aktualisieren Ihres Kernels

Das Handbuch ist in folgende Hauptkategorien unterteilt:

- Installation
- Netzwerk
- Systemkonfiguration
- Paketverwaltung

Dieses Handbuch setzt voraus, dass Sie über Grundkenntnisse Ihres Red Hat Enterprise Linux-Systems verfügen. Sollten Sie Hilfe bei der Installation benötigen, sehen Sie das *Red Hat Enterprise Linux Installationshandbuch*. Für allgemeine Informationen zur System-Administration, sehen Sie das *Red Hat Enterprise Linux Introduction to System Administration*. Für weiterführende Informationen, wie zum Beispiel einen Überblick über das Red Hat Enterprise Linux- Dateisystem, steht das *Red Hat Enterprise Linux Referenzhandbuch* zur Verfügung. Informationen zur Sicherheit, stehen im *Red Hat Enterprise Linux Sicherheitshandbuch* bereit.

HTML-, PDF- und RPM-Versionen der Handbücher sind auf der Red Hat Enterprise Linux Dokumentations-CD und Online unter http://www.redhat.com/docs/ erhältlich.

Anmerkung

Obwohl dieses Handbuch die neuesten Informationen enthält, lesen Sie die *Red Hat Enterprise Linux Release-Notes* für weitere Information, die zum Druck dieses Handbuchs noch nicht vorlagen. Diese können auf der Red Hat Enterprise Linux CD #1 und Online unter http://www.redhat.com/docs/ gefunden werden.

1. Änderungen in diesem Handbuch

Die vorhergehende Version dieses Handbuchs war das *Red Hat Linux Handbuch benutzerdefinierter Konfiguration*. Es wurde zu *Red Hat Enterprise Linux Handbuch zur System-Administration* umbenannt, um die angesprochenen Themen besser zu umschreiben, und seinen Stand in der Red Hat Dokumentation besser klar zu stellen.

Dieses Handbuch wurde erweitert, um die neuen Features von Red Hat Enterprise Linux 3, sowie die von unseren Lesern angeforderten Themen, aufzunehmen. In diesen grundlegenden Änderungen, sind Folgende enthalten:

Kapitel 7

Dieses neue Kapitel beschreibt die Verwendung von devlabel.

Kapitel 8

Dieses neue Kapitel beschreibt den Zugriff auf Kontrolllisten für Dateien und Verzeichnisse.

Kapitel 9

Dieses Kapitel wurde erweitert und umfasst nun auch kickstart-Anweisungen.

Kapitel 10

Dieses Kapitel wurde aktualisiert und umfasst nun neue Optionen von **Kickstart Configurator**.

Kapitel 14

Dieses neue Kapitel beschreibt eine PXE Installation.

Kapitel 15

Dieses neue Kapitel beschreibt die Erzeugung von plattenlosen Umgebungen.

Kapitel 24

Dieses Kapitel wurde für Samba 3.0 aktualisiert, und erklärt das Mounten von Samba-Shares.

Kapitel 32

Dieses neue Kapitel beschreibt das **Keyboard Configuration Tool**.

Kapitel 33

Dieses neue Kapitel beschreibt das **Mouse Configuration Tool**.

Kapitel 34

Dieses neue Kapitel beschreibt **X Configuration Tool**.

Kapitel 38

Dieses Kapitel wurde erweitert und umfasst nun die neuen Features von **Log Viewer**.

Kapitel 39

Dieses Kapitel wurde aktualisiert, um die neuen Kernel-Pakete und ein Upgrade des Kernels auf nicht-x86-Architekturen zu erklären.

Kapitel 43

Dieses neue Kapitel beschreibt die Verwendung des OProfile System-Profilers.

2. 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. Typen von Wörtern, die so dargestellt werden, schließen Folgende ein:

`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 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`

Text, der in diesem Stil dargestellt wird, ist Text, der in einem Shell-Prompt ausgegeben wird, wie Fehlermeldungen und Antworten auf bestimmte Befehle. Zum Beispiel:

Durch Eingabe von `ls` erscheint der Inhalt eines Verzeichnisses. Zum Beispiel:

```
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.

`replaceable`

Text, der vom Benutzer ersetzt werden soll, wird in diesem Stil dargestellt. Im folgenden Beispiel ist *<version-number>* in dieser Form dargestellt.

Das Verzeichnis für den Kernel-Source ist `/usr/src/`*<version-number>*`/`, wobei *<version-number>* die Version des installierten Kernel ist.

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

Seien Sie vorsichtig und entfernen Sie lediglich die notwendigen Red Hat Enterprise Linux Partitionen. Das Entfernen anderer Partitionen könnte zu Datenverlusten oder zur Korruption der Systemumgebung führen.

3. Das ist für die Zukunft geplant

Das *Red Hat Enterprise Linux Handbuch zur System-Administration* ist Bestandteil des ständig wachsenden Engagements von Red Hat, Red Hat Enterprise Linux-Benutzer zum richtigen Zeitpunkt durch nützliche Informationen zu unterstützen. Die künftigen Ausgaben werden die zugehörigen Informationen über neu entwickelte Tools und Anwendungen enthalten.

3.1. Wir brauchen Ihr Feedback!

Wenn Sie einen Fehler im *Red Hat Enterprise Linux Handbuch zur System-Administration* finden oder eine Idee haben, wie das Handbuch verbessert werden könnte, lassen Sie uns das bitte wissen! Schreiben Sie an Bugzilla (http://www.redhat.com/bugzilla/), und geben Sie die Komponente `Red Hat Enterprise Linux Handbuch zur System-Administration` an.

Geben Sie außerdem die Kennzeichnung des Handbuchs an:

```
rhel-sag(DE)-3-Print-RHI (2003-07-25T17:10)
```

Auf diese Weise wissen wir, auf welche Handbuchversion Sie sich beziehen.

Falls Sie uns einen Vorschlag zur Verbesserung der Dokumentation senden möchten, sollten Sie hierzu möglichst genaue Angaben machen. Wenn Sie einen Fehler gefunden haben, geben Sie bitte die Nummer des Abschnitts und einen Ausschnitt des Textes an, damit wir diesen leicht finden können.

4. Melden Sie sich für den Support an

Wenn Sie eine offizielle Version von Red Hat Enterprise Linux 3 erworben haben, können Sie die Vorteile als Kunde von Red Hat nutzen.

Sie können einige oder andere der folgenden Vorteile nutzen, je nachdem welches Produkt 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 Enterprise Linux Box.

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

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

Das Red Hat Dokumentationsteam

I. Dateisysteme

Dateisystem bezeichnet die Dateien und Verzeichnisse auf einem Computer. Ein Dateisystem kann verschiedene Formate haben, *Dateisystemtypen* genannt. Diese Formate bestimmen, wie die Information als Dateien und Verzeichnisse gespeichert wird. Einige Dateisystemtypen speichern redundante Kopien der Daten, während andere den Zugriff auf Festplatten beschleunigen. Dieser Abschnitt beschreibt die Dateisystemtypen ext3, swap, RAID und LVM. Auch wird `parted` behandelt, ein Utility zum Verwalten von Partitionen, sowie `devlabel`, ein Utility zum Erzeugen benutzerdefinierter Gerätenamen und Zugriffskontrolllisten (ACLs), die benutzerspezifische Zugriffsrechte auf Dateien erlauben.

Inhaltsverzeichnis

redhat

Kapitel 1.
Das ext3-Dateisystem

Das standardmäßige Dateisystem ist*ext3* des Typs Journaling.

1.1. Eigenschaften von ext3

Das ext3-Dateisystem ist im Wesentlichen eine erweiterte Version des ext2-Dateisystems. Diese Verbesserungen bringen folgende Vorteile mit sich:

Verfügbarkeit

Nach einem unerwarteten Stromausfall oder Systemabbruch (auch *Unsaubere Systemabschaltung*) genannt, muss jedes gemountete ext2-Dateisystem des Rechners durch das `e2fsck` Programm auf seine Konsistenz geprüt werden. Dies ist ein zeitaufwendiger Prozess, der die System-Bootzeit bedeutend hinauszögern kann, vor allem bei großen Volumen mit einer großen Anzahl an Dateien. Während dieser Zeit sind sämtliche Volumendaten unerreichbar.

Das vom ext3-Dateisystem angelegte Journal bewirkt, dass diese Art Kontrollen des Dateisystems nach einer unsauberen Systemabschaltung nicht mehr notwendig sind. Das einzige Mal, wenn eine Konsistenzkontrolle bei ext3 durchgeführt wird, ist bei selten auftretenden Hardware-Fehlern wie Festplattenlaufwerkfehlern. Die Zeit zum Wiederherstellen eines ext3-Dateisystems nach einer unsauberen Systemschließung hängt nicht von der Größe des Dateisystems oder der Anzahl der Dateien ab, sondern von der Größe des *Journals*, das zur Konsistenzpflege verwendet wird. Das Wiederherstellen eines Journals der Standardgröße dauert etwa eine Sekunde, je nachdem wie schnell die Hardware ist.

Datenintegrität

Das ext3-Dateisystem liefert eine bessere Datenintegrität im Falle einer unsauberen Systemabschaltung. Mit dem ext3-Dateisystem haben Sie die Möglichkeit, Art und Stufe des Schutzes Ihrer Daten zu wählen. Standardmäßig werden ext3-Volumen konfiguriert, um ein hohes Niveau an Datenkonsistenz im Hinblick auf den Dateisystemstatus beizubehalten.

Geschwindigkeit

Obwohl es einige Daten mehr als nur einmal schreibt, hat das ext3-Dateisystem in den meisten Fällen einen höheren Durchsatz als ext2, da das Journal des ext3 die Steuerbewegung des Festplattenlaufwerks optimiert. Sie können aus drei verschiedenen Journal-Arten wählen, um die Geschwindigkeit zu optimieren, dies hat jedoch Einschränkungen der Datenintegrität zur Folge.

Einfacher Umstieg

Es ist einfach, von ext2 zu ext3 zu wechseln und von den Vorteilen eines starken Journal-Dateisystems ohne Neuformatierung zu profitieren. Wie Sie diese Aufgabe ausführen können, wird in Abschnitt 1.3 beschrieben.

Bei einer Neuinstallation wird den Linux-Partitionen des Systems standardmäßig das ext3-Dateisystem zugeordnet. Aktualisieren Sieeine Version mit ext2-Partitionen, ermöglicht es Ihnen das Installationsprogramm, diese Partitionen in ext3-Partitionen umzuwandeln ohne Daten zu verlieren. Details hierzu finden Sie im Anhang mit dem Titel *Upgrade Ihres aktuellen Systems* im *Red Hat Enterprise Linux Installationshandbuch*.

Die nachfolgenden Abschnitte zeigen Ihnen schrittweise, wie Sie ext3-Partitionen erstellen und anpassen können. Wenn Sie ext2-Partitionen haben, können Sie die Abschnitte in Bezug auf das Partitionieren und Formatieren überspringen und direkt zu Abschnitt 1.3 übergehen.

1.2. Erstellen eines ext3-Dateisystems

Nach der Installation ist es manchmal notwendig, ein neues ext3-Dateisystem zu erstellen. Wenn Sie zum Beispiel einem System ein neues Festplattenlaufwerk hinzufügen, möchten Sie wahrscheinlich neue Partitionen für das Laufwerk erstellen und das ext3-Dateisystem verwenden.

Schritte zum Erstellen eines ext3-Dateisystems:

1. Partionen erstellen anhand von `parted` oder `fdisk`.
2. Formatieren der Partition mit dem ext3-Dateisystem anhand von `mkfs`.
3. Kennung der Partition anhand von `e2label`.
4. Erstellen des Mount-Points
5. Partition hinzufügen zu `/etc/fstab`.

Informationen zur Durchführung dieser Schritte erhalten Sie unter Kapitel 5.

1.3. Konvertierung in ein ext3-Dateisystem

Das Programm `tune2fs` kann dem bestehenden ext2-Dateisystem ein Journal hinzufügen, ohne die sich bereits auf der Partition befindlichen Daten zu ändern. Ist das Dateisystem während des Übergangs bereits gemountet, wird das Journal als Datei `.journal` im root-Verzeichnis des Dateisystems angezeigt. Ist das Dateisystem noch nicht gemountet, wird das Journal ausgeblendet und erscheint überhaupt nicht im Dateisystem.

Melden Sie sich zur Konvertierung eines ext2 in ein ext3-Dateisystem als root-Account an und geben Sie Folgendes ein:

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

Ersetzen Sie im obengenannten Befehl /dev/*hdb* mit dem Gerätenamen und *X* mit der Partitionsnummer.

Stellen Sie danach sicher, dass Sie den Partitionstyp in `/etc/fstab` von ext2 in ext3 ändern.

Konvertieren Sie Ihr root-Dateisystem, müssen Sie zum Booten ein `initrd` Image (oder RAM-Disk) verwenden. Starten Sie hierzu das `mkinitrd` Programm. Um Informationen zur Verwendung des `mkinitrd` Befehls zu erhalten, geben Sie `man mkinitrd` ein. Versichern Sie sich außerdem, dass Ihre GRUB oder LILO Konfiguration `initrd` lädt.

Versäumen Sie es, diese Änderung vorzunehmen, wird das System zwar gebootet, aber das Dateisystem wird als ext2 anstatt ext3 gemountet.

1.4. Rückkehr zu einem ext2-Dateisystem

Da ext3 relativ neu ist, wird es von einigen Laufwerk-Dienstprogrammen noch nicht unterstützt. Es kann zum Beispiel vorkommen, dass Sie eine Partition mit `resize2fs` verkleinern wollen, die ext3 noch nicht unterstützt. In einer solchen Situation empfiehlt es sich, vorübergehend zum ext2-Dateisystem zurückzukehren.

Um eine Partition zurückzuverwandeln, müssen Sie zunächst die Partition durch Anmeldung als root und mithilfe folgender Eingabe unmounten:

```
umount /dev/hdbX
```

Ersetzen Sie im obengenannten Befehl /dev/*hdb* mit dem Gerätenamen und *X* mit der Partitionsnummer. In den restlichen Abschnitten wird in den Beispielbefehlen use *hdb1* für diese Werte verwendet.

Ändern Sie den Dateisystemtyp in ext2 durch Eingabe des folgenden Befehls als root:

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

Kontrollieren Sie die Partition auf Fehler. Geben Sie hierzu als root den folgenden Befehl ein:

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

Mounten Sie dann die Partition erneut als ext2-Dateisystem durch Eingabe von:

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

Ersetzen Sie im obengenannten Befehl */mount/point* durch den Mount-Punkt der Partition.

Löschen Sie dann die Datei `.journal` im root-Verzeichnis dieser Partition, indem Sie zum Verzeichnis überwechseln, in dem sie gemountet ist, und Folgendes eingeben:

```
rm -f .journal
```

Sie verfügen jetzt über eine ext2-Partition.

Wenn Sie die Partition dauerhaft als ext2 belassen wollen, vergessen Sie nicht, die Datei `/etc/fstab` zu aktualisieren.

redhat

Kapitel 2.

Swap-Space

2.1. Was ist Swap-Space?

Swap-Space wird in Linux verwendet, wenn der physische Speicher (RAM) knapp ist. Benötigt das System weiteren Arbeitsspeicher und der physische Speicher ist voll, werden Speicherseiten, die nicht aktiv sind, in den Swap-Space verlagert. Während Swap-Space bei Rechnern mit kleinem RAM-Speicher nützlich sein kann, sollte es nicht als Ersatz für mehr RAM-Speicher angesehen werden. Swap-Space befindet sich auf Festplatten, die eine langsamere Zugriffszeit als physischer Speicher haben.

Swap-Space kann eine eigens erstellte Swap-Partition sein (empfehlenswert), eine Swap-Datei oder eine Kombination aus Swap-Partitionen und Swap-Dateien.

Die Größe des Swap-Space sollte doppelt so groß sein wie der RAM-Speicher Ihres Rechners bzw. 32 MB, je nachdem, welcher Wert größer ist. Jeder einzelne der Swap-Bereiche darf aber 2048 MB (oder 2 GB) nicht überschreiten.

2.2. Swap-Space hinzufügen

Manchmal ist es notwendig, weiteren Swap-Space nach der Installation hinzuzufügen. Zum Beispiel erweitern Sie den RAM-Speicher Ihres Systems von 64 MB auf 128 MB, aber es stehen nur 128 MB Swap-Space zur Verfügung. Es könnte von Vorteil sein, den Swap-Space auf 256 MB zu erhöhen, wenn Sie speicherintensive Vorgänge durchführen oder Anwendungen starten, die mehr Speicherplatz benötigen.

Sie haben zwei Möglichkeiten: entweder Sie fügen eine Swap-Partition oder aber eine Swap-Datei hinzu. Empfohlen wird eine Swap-Partition, aber dies ist nicht immer ganz einfach, wenn Sie keinen freien Festplattenplatz zur Verfügung haben.

Hinzufügen einer Swap-Partition (angenommen `/dev/hdb2` ist die Swap-Partition, die Sie hinzufügen möchten):

1. Die Festplatte darf nicht in Gebrauch sein (Partitionen dürfen nicht gemounted und kein Swap-Space darf aktiviert sein). Die Partitionstabelle sollte nicht geändert werden, solange sie in Gebrauch ist, da der Kernel die Änderungen eventuell nicht richtig erkennen kann. Daten können überschrieben werden, wenn auf die falsche Partition geschrieben wird, da die Partitionstabelle und gemounteten Partitionen nicht übereinstimmen. Dies erreichen Sie am einfachsten, wenn Sie Ihr System im Rescue-Modus booten. Hinweise zum Booten im Rescue-Modus finden Sie unter Kapitel 11 Werden Sie zum Mounten Ihres Dateisystems aufgefordert, wählen Sie **Überspringen**.

   Sind dagegen keine Partitionen auf der Festplatte in Gebrauch, können Sie diese unmounten und sämtlichen Swap-Space auf der Festplatte mit dem Befehl `swapoff` deaktivieren.

2. Erstellen Sie die Partition anhand von `parted`:

   - Geben Sie als root im Shell-Prompt folgenden Befehl ein `parted /dev/`*`hdb`*, wobei /dev/*`hdb`* er Gerätename für die Festplatte mit freiem Speicherplatz ist.
   - Geben Sie am Prompt `(parted)` **`print`** ein, um die bestehenden Partitionen und den vorhandenen Speicherplatz anzuzeigen. Die Anfangs- und Endwerte sind in Megabyte

angegeben. Bestimmen Sie, wie viel freier Platz sich auf der Festplatte befindet und wie viel Sie einer neuen Swap-Partition zuordnen möchten.

- Geben Sie am Prompt `(parted)` **`mkpartfs`** ***`Partitionstyp`*** **`linux-swap`** ***`Start Ende`*** ein, wobei *`Partitionstyp`* entweder primär, erweitert oder logisch ist, *`Start`* der Startpunkt der Partition und *`Ende`* der Endpunkt der Partition ist.

  
  Warnung

  Änderungen werden sofort wirksam; seien Sie daher vorsichtig bei der Eingabe.

- Verlassen Sie `parted` durch Eingabe von **`quit`**.

3. Jetzt, wo Sie über die Swap-Partition verfügen, verwenden Sie den Befehl `mkswap` zur Einrichtung der Swap-Partition. Geben Sie als root an einem Shell-Prompt Folgendes ein:
   ```
   mkswap /dev/hdb2
   ```
4. Geben Sie zur sofortigen Aktivierung der Swap-Partition folgenden Befehl ein:
   ```
   swapon /dev/hdb2
   ```
5. Bearbeiten Sie zur Aktivierung beim Booten die Datei `/etc/fstab` und fügen Sie folgende Zeile an:
   ```
   /dev/hdb2               swap                    swap    defaults        0 0
   ```
   Beim nächsten Booten des Systems wird die neue Swap-Partition aktiviert.
6. Nach Hinzufügen der neuen Swap-Partition und deren Aktivierung vergewissern Sie sich, dass diese wirklich aktiviert ist, indem Sie die Ausgabe des Befehls `cat /proc/swaps` oder `free` prüfen.

Hinzufügen einer Swap-Datei:

1. Bestimmen Sie die Größe der neuen Swap-Datei und multiplizieren Sie diese mit 1024, um die Größe der benötigten Blöcke festzulegen. Die Anzahl der benötigten Blöcke einer 64 MB-Swap-Datei ist zum Beispiel 65536.
2. Geben Sie an einem Shell-Prompt als root folgenden Befehl ein, wobei `count` dem Wert der benötigten Anzahl Blöcke entspricht:
   ```
   dd if=/dev/zero of=/swapfile bs=1024 count=65536
   ```
3. Richten Sie die Swap-Datei mit dem folgenden Befehl ein:
   ```
   mkswap /swapfile
   ```
4. Zur sofortigen Aktivierung der Swap-Datei (aber nicht automatisch beim Booten):
   ```
   swapon /swapfile
   ```
5. Bearbeiten Sie zur Aktivierung beim Booten die Datei `/etc/fstab` und fügen Sie folgende Zeile an:
   ```
   /swapfile               swap                    swap    defaults        0 0
   ```
   Beim nächsten Booten des Systems wird die neue Swap-Datei aktiviert.
6. Nach Hinzufügen der neuen Swap-Datei und ihrer Aktivierung vergewissern Sie sich, dass diese wirklich aktiv ist, indem Sie die Ausgabe des Befehls `cat /proc/swaps` oder `free` anzeigen.

2.3. Löschen von Swap-Space

Löschen einer Swap-Partition:

1. Die Festplatte darf nicht in Gebrauch sein (Partitionen dürfen nicht gemountet und kein Swap-Space aktiviert sein). Dies erreichen Sie am einfachsten durch Booten Ihres Systems im Rescue-Modus. Hinweise zum Booten im Rescue-Modus erhalten Sie unter Kapitel 11. Wenn Sie aufgefordert werden, das Dateisystem zu mounten, wählen Sie **Überspringen**.

   Sind dagegen keine Partitionen auf der Festplatte in Gebrauch, können Sie diese unmounten und sämtlichen Swap-Space auf der Festplatte mit dem Befehl `swapoff` deaktivieren.
2. Geben Sie als root an einem Shell-Prompt folgenden Befehl ein, um sicherzustellen, dass die Swap-Partition deaktiviert wurde (wobei `/dev/hdb2` die Swap-Partition ist):
   ```
   swapoff /dev/hdb2
   ```
3. Löschen Sie den Eintrag aus `/etc/fstab`.
4. Löschen Sie die Partition anhand von `parted`:
   - Geben Sie als root an einem Shell-Prompt den Befehl `parted /dev/`*`hdb`* ein, wobei /dev/*hdb* der Gerätename für die Festplatte der zu löschenden Swap-Partition ist.
   - Geben Sie am Prompt `(parted)` **`print`** ein, um die bestehenden Partitionen anzuzeigen und die Minor-Nummer der zu löschenden Swap-Partition zu bestimmen.
   - Geben Sie am Prompt `(parted)` **`rm`** ***`MINOR`*** ein, wobei *MINOR* die Minor-Nummer der zu löschenden Partition ist.

     Warnung

     Änderungen werden sofort wirksam. Sie müssen die korrekte Minor-Nummer eingeben.
   - Geben Sie **`quit`** ein, um `parted` zu verlassen.

Löschen einer Swap-Datei:

1. Geben Sie als root an einem Shell-Prompt den folgenden Befehl ein, um die Swap-Datei zu deaktivieren (wobei `/swapfile` die Swap-Datei ist):
   ```
   swapoff /swapfile
   ```
2. Löschen Sie den Eintrag aus `/etc/fstab`.
3. Löschen Sie die aktuelle Datei:
   ```
   rm /swapfile
   ```

2.4. Swap-Space verlagern

Um Swap-Space von einem Ort zu einem anderen zu verlagern, folgen Sie den Schritten zum Löschen von Swap-Space und dann den Anweisungen zum Hinzufügen von Swap-Space.

redhat

Kapitel 3.

Redundant Array of Independent Disks (RAID)

3.1. Was ist RAID?

Der Grundgedanke von RAID ist es, mehrere kleine, kostengünstige Laufwerke in einem Array zu kombinieren, um Leistungs- und Redundanzziele zu erfüllen, die mit einem einzelnen größeren und teureren Laufwerk nicht erreicht werden. Dieses Array an Laufwerken wird vom Computer als eine einzelne logische Speichereinheit oder ein Laufwerk angesehen.

Mit RAID werden Informationen über mehrere Platten verteilt. Hierfür werden Techniken wie *Disk Striping* (RAID-Level 0), *Disk Mirroring* (RAID-Level 1) und *Disk Striping mit Parität* (RAID-Level 5) verwendet, um Redundanz sowie geringere Wartezeiten zu erreichen und/oder die Bandbreite für Lesen/Schreiben auf Platten zu erhöhen bzw. mehr Möglichkeiten zur Verfügung zu stellen, Daten von Festplattenabstürzen wiederherzustellen.

RAID liegt die Vorstellung zu Grunde, dass Daten über alle Datenträger im Array konsistent verteilt werden können. Hierfür müssen die Daten zuerst in gleichgroße Speicherbereiche (Chunks) aufgeteilt werden (in der Regel 32K oder 64K, obwohl verschiedene Größen möglich sind). Jeder Speicherbereich wird dann je nach verwendetem RAID-Level auf eine Festplatte geschrieben. Sollen die Daten gelesen werden, wird der Prozess umgekehrt, wobei der Eindruck entsteht, dass mehrere Festplatten eine einzige Partition bilden.

3.2. Wer sollte RAID verwenden?

All diejenigen, die große Datenmengen jederzeit abrufbar aufbewahren müssen (zum Beispiel normale Systemadministratoren), profitieren von der RAID- Technologie. Die Hauptgründe, RAID zu verwenden, sind u.a. folgende:

- Höhere Geschwindigkeit
- Größere Speicherkapazität bei Verwendung eines einzigen virtuellen Datenträgers
- Begrenzung der Auswirkung von Plattenfehlern

3.3. Hardware-RAID kontra Software-RAID

Es gibt zwei RAID-Typen: Hardware-RAID und Software-RAID.

3.3.1. Hardware-RAID

Das auf Hardware basierende System verwaltet das RAID-Subsystem unabhängig vom Host und stellt dem Host nur eine einzige Platte pro RAID-Array zur Verfügung.

Ein Hardware-RAID-Gerät wäre zum Beispiel ein Gerät, das mit einem SCSI-Controller verbunden ist und die RAID-Arrays als ein einziges SCSI-Laufwerk darstellt. Ein externes RAID-System verschiebt das gesamte intelligente RAID- Handling in einen Controller im externen Platten-Subsystem. Das gesamte Subsystem wird über einen normalen SCSI-Controller mit dem Host verbunden und von ihm als eine einzige Platte aufgefasst.

RAID-Controller stehen auch als Karten zur Verfügung, die für das Betriebssystem wie SCSI-Controller *agieren*, aber jegliche Laufwerkskommunikation selbst bearbeiten. In solchen

Fällen schließen Sie die Laufwerke wie einen SCSI-Controller an den RAID-Controller an, fügen sie jedoch anschließend zur Konfiguration des RAID-Controllers hinzu. Das Betriebssystem stellt keinen Unterschied fest.

3.3.2. Software-RAID

Das Software-RAID implementiert die verschiedenen RAID-Levels im Laufwerkcode des Kernels (Blockgerät). Dies ist die günstigste Lösung, da keine teuren Controllerkarten für Datenträger oder Hot-Swap-Chassis[1] benötigt werden. Software-RAID funktioniert auch mit günstigeren IDE-Festplatten und SCSI-Platten. Mit den heutigen schnellen CPUs übertrifft die Leistung von Software-RAID die von Hardware-RAID.

Der MD-Treiber im Linux-Kernel ist ein Beispiel für eine RAID-Lösung, die komplett hardwareunabhängig ist. Die Leistung eines auf Software basierenden Arrays hängt von der Leistung und Auslastung der Server-CPU ab.

Weitere Informationen über das Konfigurieren des Software-RAID während der Installation finden Sie in Kapitel 12.

Sollten Sie an weiteren Informationen über die Möglichkeiten des Software-RAID interessiert sein, finden Sie im Folgenden eine kurze Liste mit den wichtigsten Eigenschaften:

- Wiederherstellungsprozess mit Thread
- Vollständig kernelbasierte Konfiguration
- Transportfähigkeit von Arrays zwischen Linux-Rechnern ohne Wiederherstellung
- Array-Wiederherstellung im Hintergrund mit Hilfe ungenutzter Systemressourcen
- Plattenunterstützung mit Hot-Swap
- Automatische CPU-Erkennung zur Nutzung bestimmter CPU-Verbesserungen

3.4. RAID Levels und Linearer Support

RAID unterstützt verschiedene Konfigurationen, einschließlich der Level 0, 1, 4, 5 sowie den Linear-Modus. Diese RAID-Typen werden folgendermaßen definiert:

- *Level 0* — RAID-Level 0, häufig auch "Striping" genannt, ist eine leistungsorientierte Zuordnungsmethode von Stripesetdaten. Dies bedeutet, dass die in das Array geschriebenen Daten in Stripesets aufgeteilt und über die Partitionen des Arrays geschrieben werden. Hierdurch wird die I/O-Leistung zu geringen inhärenten Kosten und ohne Redundanz erhöht. Die Speicherkapazität eines Arrays der Ebene 0 entspricht der Gesamtkapazität der Partitionen in einem Hardware-RAID bzw. der Gesamtkapazität der Partitionen in einem Software-RAID.
- *Level 1* — RAID-Level 1 oder Mirroring (Spiegelung) wurde länger als jede andere RAID-Form verwendet. Level 1 stellt Redundanz bereit, indem identische Daten auf jede Partition des Arrays geschrieben werden und dabei eine gespiegelte Kopie auf jeder Platte hinterlassen wird. Die Spiegelung ist nach wie vor beliebt, da sie einfach auszuführen ist und sehr viele Daten zur Verfügung stellt. Level 1 arbeitet mit zwei oder mehreren Platten, die für hohe Datenübertragungsraten beim Lesen parallelen Zugriff verwenden können, aber meist unabhängig funktionieren, um hohe

1. Mit einem Hot-Swap-Chassis können Sie eine Festplatte entfernen, ohne hierfür das System abschalten zu müssen.

I/O-Transaktionsraten bereitzustellen. Level 1 bietet eine äußerst gute Datenzuverlässigkeit und optimiert die Leistung für leseintensive Applikationen. Allerdings ist dies relativ kostenintensiv.[2] Die Speicherkapazität des Level 1 Arrays gleicht der Kapazität einer der gespiegelten Festplatten im Hardware-RAID oder einer der Mirror-Partitionen im Software-RAID.

- *Level 4* — Level 4 konzentriert Paritäten[3] auf einer einzelnen Platte, um Daten zu schützen. Er ist besser für I/O Transaktionen geeignet als der Transfer großer Dateien. Da die zugewiesene Parität einen inhärenten Engpass darstellt, wird Level 4 selten ohne begleitende Technologie wie zum Beispiel write-backcaching verwendet. Obwohl RAID-Level 4 eine Möglichkeit in einigen RAID-Partitionsschemata darstellt, ist dies nicht für RAID-Installationen in Red Hat Enterprise Linux RAID erlaubt.[4] Die Speicherkapazität von RAID-Level 4 gleicht der Kapazität von Partitionen abzüglich der Kapazität einer Partition. Die Speicherkapazität von Software-RAID-Level 4 entspricht der Kapazität der Partitionen abzüglich der Größe einer der Partitionen, wenn sie gleich groß sind.
- *Level 5* — Dies ist der häufigste RAID-Typ. Wird die Parität über einige oder alle Partitionslaufwerke eines Arrays verteilt, entfernt RAID-Level 5 den Level 4 inhärenten Schreibengpass. Der einzige Leistungsengpass ist der Prozess der Paritätsberechnung. Mit modernen CPUs und Software-RAID stellt dies in der Regel kein großes Problem dar. Ebenso wie bei Level 4 ist das Ergebnis eine asymmetrische Leistung mit Lesevorgängen, die die Leistung der Schreibvorgänge deutlich mindern. Level 5 wird häufig mit Schreiben nach Zwischenspeichern verwendet, um diese Asymmetrie zu reduzieren. Die Speicherkapazität von Hardware-RAID-Level 5 entspricht der Kapazität der Partitionen abzüglich der Kapazität einer Partition. Die Speicherkapazität von Software-RAID-Level 5 entspricht der Kapazität der Partitionen abzüglich der Größe einer der Partitionen, wenn sie gleich groß sind.
- *Linear RAID* —Linear RAID ist eine einfache Laufwerkgruppierung zum Erstellen eines größeren virtuellen Laufwerks. Im Modus Linear RAID werden die Speicherbereiche sequenziell von einer Partition zugeteilt. Das nächste Laufwerk wird erst dann verwendet, wenn das erste vollständig gefüllt ist. Diese Gruppierung bietet keine Leistungsverbesserung, da das Splitten von I/O-Vorgängen auf Partitionen unwahrscheinlich ist. Darüber hinaus bietet Linear RAID keine Redundanz und verringert in der Tat die Zuverlässigkeit — fällt eine Partition aus, kann das gesamte Array nicht verwendet werden. Die Kapazität ist die Summe aller Partitionen.

2. RAID-Level 1 ist teuer, da dieselben Informationen auf alle Platten im Array geschrieben werden, was sehr viel Platz auf dem Laufwerk in Anspruch nimmt. Haben Sie zum Beispiel RAID-Level 1 eingerichtet, so dass die Root-Partition(/) auf zwei 40G-Laufwerken vorhanden ist, verfügen Sie insgesamt über 80G, können jedoch nur auf 40G dieser 80G zugreifen. Die übrigen 40G fungieren als Spiegel der ersten 40G.
3. Paritätsinformationen werden im Array berechnet. Grundlage ist der Inhalt der restlichen Partitionen. Diese Informationen können dann zum Wiederherstellen der Daten verwendet werden, wenn eine Platte im Array ausfällt. Die wiederhergestellten Daten können dann für I/O-Anfragen an die fehlerhafte Platte verwendet werden, ehe sie ersetzt wird, sowie zum erneuten Auffüllen der fehlerhaften Platte nach dem Ersatz.
4. RAID-Level 4 nimmt denselben Platz wie RAID-Level 5 in Anspruch, aber Level 5 bietet im Vergleich zu Level 4 mehr Vorteile. Daher wird Level 4 nicht unterstützt.

Kapitel 4.

Logischer Volumenmanager (LVM)

4.1. Was ist LVM?

Mit dem LVM wird Festplattenplatz in logischen Volumen angeordnet, deren Größe im Gegensatz zu Partitionen einfach verändert werden kann.

Mit LVM werden eine oder mehrere Festplatten in ein oder mehrere *physische Volumen* angeordnet. Ein physisches Volumen muss sich dabei auf eine Festplatte beschränken.

Die physischen Volumen werden in *logische Volumengruppen* angeordnet, mit Ausnahme der `/boot/` Partition. Die `/boot/`-Partition kann sich nicht in einer logischen Volumengruppe befinden, da sie nicht vom Bootloader gelesen werden kann. Wenn Sie die root `/`-Partition in einem logischen Volumen anordnen möchten, müssen Sie eine separate `/boot/`-Partition anlegen, die nicht zu einer Volumengruppe gehört.

Da ein physisches Volumen auf eine Festplatte beschränkt sein muss, müssen Sie ein oder mehrere physische Volumen pro Festplatte anlegen, wenn eine logische Volumengruppe mehr als eine Festplatte umfassen soll.

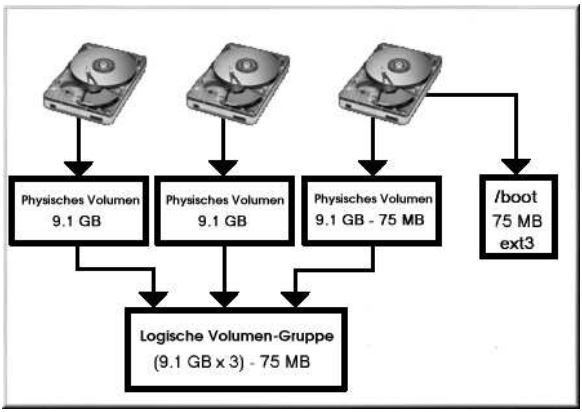

Abbildung 4-1. logische Volumengruppe

Eine logische Volumengruppe ist in *logische Volumen*, aufgeteilt, die Mount-Punkten wie `/home` und `/` und Dateisystemtypen wie ext3 zugewiesen werden. Wenn "Partitionen" ihre volle Kapazität erreichen, kann freier Platz von der logischen Volumengruppe zum logischen Volumen hinzugefügt werden, um die Partition zu vergrößern. Wird eine neue Festplatte in das System eingefügt, kann sie der logischen Volumengruppe hinzugefügt und die logischen Volumen, d.h. die Partitionen, können erweitert werden.

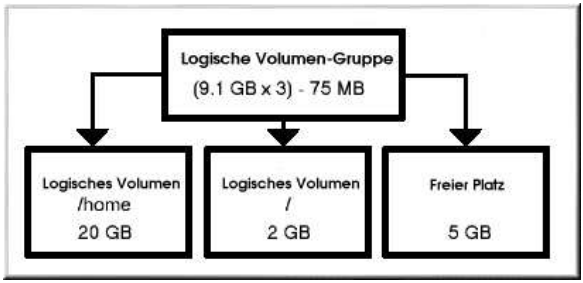

Abbildung 4-2. Logische Volumen

Wenn ein System mit dem ext3 Dateisystem partitioniert wurde, wird die Festplatte in Partitionen dagegen mit einer ganz bestimmten Größe aufgeteilt. Ist eine Partition voll, ist es nicht so einfach, die Größe der Partition zu erweitern. Wenn die Partition auf eine andere Festplatte verschoben wird, muss der ursprüngliche Festplattenplatz als andere Partition oder als nicht verwendet zugeordnet werden.

LVM-Support muss in den Kernel kompiliert werden. Der standardmäßige Red Hat Kernel wird mit LVM-Support kompiliert.

Informationen über die Konfiguration von LVM während des Installationsprozesses finden Sie im Kapitel 13.

4.2. Zusätzliche Ressourcen

Benutzen Sie diese Quellen, um mehr zu LVM zu lernen.

4.2.1. Installierte Dokumentation

- `rpm -qd lvm` — Dieser Befehl zeigt alle verfügbare Dokumentation des `lvm`-Pakets, einschließlich man-Seiten.

4.2.2. Nützliche Websites

- http://www.sistina.com/products_lvm.htm — LVM-Webseite, die einen Überblick, Links zu Mailing-Listen und mehr enthält.
- http://tldp.org/HOWTO/LVM-HOWTO/ — *LVM HOWTO* vom Linux Documentation Project.

redhat

Kapitel 5.

Verwalten des Festplattenspeichers

Viele Benutzer möchten eventuell existierende Partitionstabellen anzeigen, die Größe der Partitionen ändern, Partitionen löschen oder Partitionen aus freiem Speicherplatz oder zusätzliche Festplatten hinzufügen. Anhand des Dienstprogramms `parted` können Sie diese Aufgaben durchführen. In diesem Kapitel wird die Verwendung von `parted` behandelt, um Änderungen an Dateisystemen durchzuführen.

Möchten Sie die Speicherplatzverwendung des Systems anzeigen bzw. überwachen, erhalten Sie hierfür Hinweise unter Abschnitt 42.3.

Das Paket `parted` muss zur Verwendung des Dienstprogramms `parted` installiert sein. Starten Sie `parted` an einem Shell-Prompt als root, und geben Sie den Befehl `parted /dev/hdb` ein, wobei */dev/hdb* der Gerätename der zu konfigurierenden Festplatte ist. Ein `(parted)` Prompt wird angezeigt. Geben Sie `help` ein, um eine Liste der verfügbaren Befehle anzuzeigen.

Wenn Sie eine Partition erstellen, löschen bzw. deren Größe ändern möchten, darf das Gerät nicht in Gebrauch sein (Partitionen können nicht gemountet und Swap-Space kann nicht aktiviert werden). Die Partitionstabelle sollte nicht geändert werden, während diese benutzt wird, da der Kernel eventuell die Änderungen nicht erkennt. Daten können hierdurch überschrieben werden, da diese auf eine falsche Partition geschrieben werden, da Tabelle und gemountete Partition nicht übereinstimmen. Dies erreichen Sie am einfachsten dadurch, dass Sie Ihr System im Rescue Modus booten. Hinweise zum Booten im Rescue Modus erhalten Sie unter Kapitel 11. Wenn Sie vom System aufgefordert werden, das Dateisystem zu mounten, wählen Sie **Überspringen**.

Enthält die Festplatte dagegen keine Partitionen, die im Gebrauch sind, können Sie diese mit dem Befehl `umount` unmounten und den Swap-Space der Festplatte mit dem Befehl `swapoff` deaktivieren.

Tabelle 5-1 enthält eine Liste der am häufigsten verwendeten `parted` Befehle. Die nachfolgenden Abschnitte erklären einige davon näher.

Befehl	Beschreibung
`check` *minor-num*	Führt eine einfache Prüfung des Dateisystems durch
`cp` *von bis*	Kopiert das Dateisystem von einer Partition zur anderen; *von* und *bis* sind die Minor-Nummern der Partitionen
`help`	Zeigt Liste verfügbarer Befehle an
`mklabel` *Kennung*	Erstellt eine Laufwerkkennung für die Partitionstabelle
`mkfs` *minor-num Dateisystemtyp*	Erstellt Dateisystem des Typs *Dateisystemtyp*
`mkpart` *part-type fs-type start-mb end-mb*	Erstellt eine Partition, ohne ein neues Dateisystem anzulegen
`mkpartfs` *part-type fs-type start-mb end-mb*	Erstellt eine Partition und legt das angegebene Dateisystem an
`move` *minor-num start-mb end-mb*	Verschiebt die Partition
`name` *minor-num name*	Name nur für Mac und PC98 Kennungen

Befehl	Beschreibung
`print`	Zeigt die Partitionstabelle an
`quit`	Beendet `parted`
`rescue` *`start-mb end-mb`*	Retten einer verlorenen Partition von *`start-mb`* bis *`end-mb`*
`resize` *`minor-num start-mb end-mb`*	Ändert die Größe der Partition von *`start-mb`* bis *`end-mb`*
`rm` *`minor-num`*	Löscht die Partition
`select` *`device`*	Wählt ein neues zu konfigurierendes Gerät
`set` *`minor-num flag state`*	Setzt Flag auf eine Partition; *`state`* ist entweder aktiv oder inaktiv

Tabelle 5-1. `parted` Befehle

5.1. Anzeigen der Partitionstabelle

Geben Sie nach dem Start von `parted` folgenden Befehl ein, um die Partitionstabelle anzuzeigen:

```
print
```

Es erscheint eine Tabelle, die ähnlich wie folgende aussehen kann:

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

Die erste Zeile gibt die Größe des Laufwerks an, die zweite seinen Kennungstyp, und der Rest des Ausdrucks zeigt die Partitionstabelle. In der Partitionstabelle entspricht die **Minor** -Nummer der Partitionsnummer. Zum Beispiel entspricht die Partition mit der Minor-Nummer 1 `/dev/hda1`. Die Werte **Start** und **Ende** werden in Megabyte angegeben. Der **Typ** kann primär, erweitert oder logisch sein. **Dateisystem** gibt die Art des Dateisystems an, also entweder ext2, ext3, FAT, hfs, jfs, linux-swap, ntfs, reiserfs, hp-ufs, sun-ufs oder xfs. Die Spalte **Flags** listet die für die Partition gesetzten Flags auf. Verfügbare Flags sind boot, root, swap, hidden, raid, lvm oder lba.

Tipp

Möchten Sie ein anderes Gerät wählen, ohne `parted` neu starten zu müssen, verwenden Sie den Befehl `select` gefolgt vom Gerätenamen wie zum Beispiel `/dev/hdb`. Daraufhin können Sie die Partitionstabelle anzeigen oder sie konfigurieren.

5.2. Erstellen von Partitionen

Warnung

Versuchen Sie nicht, eine Partition auf einem Gerät zu erstellen, das in Gebrauch ist.

Bevor Sie eine Partition erstellen, booten Sie im Rescue Modus (oder unmounten Sie Partitionen und deaktivieren Sie jeglichen Swap-Space auf dem Gerät).

Starten Sie `parted`, wobei /dev/*hda* das Gerät ist, auf dem die Partition erstellt werden soll:

```
parted /dev/hda
```

Zeigen Sie die aktuelle Partitionstabelle an, um festzulegen, ob genug freier Platz vorhanden ist:

```
print
```

Ist nicht genug Speicherplatz vorhanden, können Sie die Größe einer bestehenden Partition ändern. Informationen dazu finden Sie unter Abschnitt 5.4.

5.2.1. Erstellen von Partitionen

Bestimmen Sie von der Partitionstabelle aus die Start-und Endpunkte der neuen Partition und um was für einen Partitionstyp es sich handeln soll. Es kann nur vier primäre Partitionen (ohne erweiterte Partitionen) auf einem Gerät geben. Benötigen Sie mehr als vier Partitionen, sind drei primäre Partitionen möglich, eine erweiterte Partition und mehrere logische Partitionen innerhalb der erweiterten Partition. Einen Überblick über die Festplattenpartitionen erhalten Sie im Anhang unter *Einführung in die Festplattenpartitionen* im *Red Hat Enterprise Linux Installationshandbuch*.

Um zum Beispiel eine primäre Partition mit einem ext3 Dateisystem von 1024 Megabyte bis 2048 Megabyte auf einem Festplattenlaufwerk zu erstellen, geben Sie folgenden Befehl ein:

```
mkpart primary ext3 1024 2048
```

Tipp

Verwenden Sie stattdessen den Befehl `mkpartfs`, wird zunächst die Partition erstellt und dann das Dateisystem. `parted` unterstützt jedoch nicht die Erstellung eines ext3 Dateisystems. Sie müssen also zum Erstellen eines ext3 Dateisystems `mkpart` verwenden und das Dateisystem mit dem Befehl `mkfs` erstellen, wie später beschrieben wird. `mkpartfs` funktioniert für den Dateisystemtyp Linux-Swap.

Die Änderungen werden wirksam, sobald Sie die [Enter-Taste] drücken, prüfen Sie also den Befehl, bevor Sie ihn ausführen.

Verwenden Sie nach Erstellen der Partition den Befehl `print` um zu bestätigen, dass sie sich mit dem richtigen Partitionstyp, Dateisystemtyp und der richtigen Größe in der Partitionstabelle befindet. Merken Sie sich auch die Minor-Nummer der neuen Partition, so dass Sie diese mit einer Kennung versehen können. Lassen Sie sichauch die Ausgabe von

```
cat /proc/partitions
```

anzeigen, um sicherzustellen, dass der Kernel die neue Partition erkennt.

5.2.2. Formatieren von Partitionen

Die Partition hat immer noch kein Dateisystem. Erstellen Sie das Dateisystem:

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

Warnung

Das Formatieren von Partitionen hat zur Folge, dass sämtliche Daten, die sich derzeit auf der Partition befinden, unwiderruflich gelöscht werden.

5.2.3. Partitionen mit Kennungen versehen

Geben Sie der Partition als nächstes eine Kennung. Heißt die neue Partition zum Beispiel `/dev/hda3` und Sie möchten sie mit folgender Kennung versehen: `/work`:

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

Standardmäßig verwendet das Installationsprogramm den Mount-Punkt der Partition als Kennung, um sicher zu gehen, dass die Kennung einmalig ist. Sie können jedoch jede beliebige Kennung verwenden.

5.2.4. Erstellen des Mount-Punktes

Erstellen Sie als root den Mount-Punkt:

```
mkdir /work
```

5.2.5. Hinzufügen zu `/etc/fstab`

Bearbeiten Sie als root die Datei `/etc/fstab`, um die neue Partition mit aufzunehmen. Die neue Zeile sollte etwa wie folgt aussehen:

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

Die erste Spalte sollte `LABEL=` enthalten, gefolgt von der Kennung, die Sie der Partition zugeordnet haben. Die zweite Spalte sollte den Mount-Punkt für die neue Partition enthalten, während die nächste Spalte den Dateityp angeben sollte (zum Beispiel ext3 oder swap). Weitere Informationen zum Format erhalten Sie auf der man-Seite mit dem Befehl `man fstab`.

Steht in der vierten Spalte das Wort `defaults`, wird die Partition beim Booten gemountet. Um die Partition ohne erneutes Booten zu mounten, geben Sie als root den folgenden Befehl ein:

```
mount /work
```

5.3. Löschen von Partitionen

Warnung

Versuchen Sie nicht, eine Partition auf einem Gerät zu löschen, das in Gebrauch ist.

Bevor Sie eine Partition löschen, booten Sie im Rescue Modus (oder unmounten Sie die Partitionen und deaktivieren Sie jeglichen Swap-Space auf dem Gerät).

Starten Sie `parted`, wobei /dev/*hda* das Gerät ist, auf dem die Partition erstellt werden soll:

```
parted /dev/hda
```

Zeigen Sie die aktuelle Partitionstabelle an, um die Minor-Nummer der zu löschenden Partition zu bestimmen:

```
print
```

Löschen Sie die Partition mit dem Befehl `rm`. Um zum Beispiel die Partition mit der Minor-Nummer 3 zu löschen:

```
rm 3
```

Die Änderungen werden wirksam, sobald Sie die [Enter-Taste] drücken, prüfen Sie also den Befehl, bevor Sie diesen ausführen.

Verwenden Sie nach dem Löschen der Partition den Befehl `print` um zu bestätigen, dass diese aus der Partitionstabelle gelöscht wurde. Sie sollten sich auch die Ausgabe von

```
cat /proc/partitions
```

anzeigen lassen, um sicherzustellen, dass der Kernel die gelöschte Partition anerkennt.

Zuletzt wird die Partition aus der Datei `/etc/fstab` gelöscht. Suchen Sie die Zeile, die die gelöschte Partition angibt, und löschen Sie diese aus der Datei.

5.4. Ändern der Partitionsgröße

Warnung

Versuchen Sie nicht, die Größe einer Partition auf einem Gerät zu ändern, das in Gebrauch ist.

Bevor Sie die Größe einer Partition ändern, booten Sie im Rescue Modus (oder unmounten Sie die Partitionen und deaktivieren Sie jeglichen Swap-Space auf dem Gerät).

Starten Sie `parted`, wobei /dev/*hda* das Gerät ist, auf dem die Partition erstellt werden soll:

```
parted /dev/hda
```

Zeigen Sie die aktuelle Partitionstabelle an, um die Minor-Nummer der zu löschenden Partition sowie die Start-und Endpunkte für die Partition zu bestimmen:

```
print
```

Warnung

Der zur Größenänderung der Partition verwendete Platz darf die neue Größe nicht überschreiten.

Verwenden Sie zur Änderung der Größe der Partition den Befehl `resize`, gefolgt von der Minor-Nummer der Partition, dem Ausgangsspeicherplatz in Megabyte und dem Endspeicherplatz in Megabyte. Zum Beispiel:

```
resize 3 1024 2048
```

Nachdem die Größe der Partition geändert wurde, bestätigen Sie mit dem Befehl `print`, dass die Größe der Partition korrekt geändert wurde und es sich um den richtigen Partitionstyp und den richtigen Dateisystemtyp handelt.

Nachdem Sie das System erneut in den normalen Modus gebootet haben, verwenden Sie den Befehl `df`, um sicherzustellen, dass die Partition gemountet wurde und mit der neuen Größe erkannt wird.

redhat

Kapitel 6.

Festplatten-Quoten implementieren

Zusätzlich zur Überwachung des Festplattenplatzes auf einem System kann der Festplattenplatz durch das Anlegen von Festplatten-Quoten eingeschränkt werden, so dass der Systemadministrator benachrichtigt wird, bevor ein Benutzer zuviel Festplattenplatz verwendet oder eine Partition voll wird.

Festplatten-Quoten können sowohl für Einzelbenutzer wie auch für Benutzergruppen konfiguriert werden. Diese Flexibilität ermöglicht es, jedem Benutzer für "persönliche" Dateien (wie z.B. E-Mails oder Berichte) eine kleine Quote neben einer größeren Quote für Projekte zuzuteilen (vorausgesetzt, dass die Projekte eigenen Gruppen zugewiesen wurden).

Zusätzlich dazu können Quoten nicht nur zur Kontrolle der Anzahl verwendeter Blöcke sondern auch zur Kontrolle der Anzahl von Inodes eingestellt werden. Da Inodes dateibezogene Informationen enthalten, gibt Ihnen dies Kontrolle über die Anzahl der Dateien, die erstellt werden können..

Die `quota`-RPMs müssen installiert sein, um Festplatten-Quoten implementieren zu können. Weitere Informationen zum Installieren von RPM-Paketen finden Sie unter Teil III.

6.1. Festplatten-Quoten konfigurieren

Um Festplatten-Quoten zu implementieren, folgen Sie den nachfolgenden Schritten:

1. Aktivieren Sie die Quoten pro Dateisystem, indem Sie die Datei `/etc/fstab` ändern
2. Mounten Sie das/die Dateisystem(e) neu
3. Erstellen Sie die Quoten-Dateien und erzeugen Sie eine Tabelle zur Festplattennutzung
4. Weisen Sie Quoten zu

Jeder dieser Schritte wird in den folgenden Abschnitten genauer erklärt.

6.1.1. Quoten aktivieren

Melden Sie sich als root an und fügen Sie in einem Texteditor Ihrer Wahl der Datei `/etc/fstab` den Befehl `usrquota` und/oder `grpquota` zum Dateisystem, das die Quoten benötigt, hinzu:

```
LABEL=/          /              ext3    defaults         1 1
LABEL=/boot      /boot          ext3    defaults         1 2
none             /dev/pts       devpts  gid=5,mode=620   0 0
LABEL=/home      /home          ext3    defaults,usrquota,grpquota 1 2
none             /proc          proc    defaults         0 0
none             /dev/shm       tmpfs   defaults         0 0
/dev/hda2        swap           swap    defaults         0 0
/dev/cdrom       /mnt/cdrom     udf,iso9660 noauto,owner,kudzu,ro 0 0
/dev/fd0         /mnt/floppy    auto    noauto,owner,kudzu 0 0
```

In diesem Beispiel hat das Dateisystem `/home` Benutzer- und Gruppen-Quoten aktiviert.

6.1.2. Erneutes Mounten des Dateisystems

Nachdem Sie die Optionen `userquota` und `grpquota` hinzugefügt haben, mounten Sie alle Dateisysteme, in denen der Eintrag `fstab` geändert wurde, neu. Wenn das Dateisystem von keinem anderen Prozess genutzt wird, können Sie den Befehl `umount`, gefolgt von `mount` zum erneuten Mounten des

Dateisystems verwenden. Wird das Dateisystem gerade verwendet, ist die einfachste Methode zum erneuten Mounten des Dateisystems ein Neustart des Systems.

6.1.3. Erstellen von Quoten-Dateien

Nachdem jedes für Quoten aktiviertes Dateisystem neu gemountet wurde, kann das System jetzt vom Festplatten-Quoten arbeiten. Das Dateisystem selbst ist jedoch noch nicht zur Unterstützung von Festplatten-Quoten bereit. Dazu müssen Sie im nächsten Schritt den Befehl `quotacheck` ausführen.

Der Befehl `quotacheck` untersucht quoten-aktivierte Dateisysteme und erstellt eine Tabelle der aktuellen Festplattenverwendung pro pro Dateisystem. Mit dieser Tabelle wird dann die Kopie der Festplattennutzung im Betriebssystem und außerdem die Quoten-Dateien des Dateisystems aktualisiert.

Zum Erstellen der Quoten-Dateien (`aquota.user` und `aquota.group`) im Dateisystem, geben Sie die Option `-c` des Befehls `quotacheck` ein. Wenn Sie zum Beispiel Benutzer- und Gruppen-Quoten für die Partition `/home` aktivieren möchten, erstellen Sie Dateien im Verzeichnis `/home`:

```
quotacheck -acug /home
```

Die Option `-a` bedeutet, dass alle gemounteten nicht-NFS Dateisysteme in `/etc/mtab` auf eine Aktivierung der Quoten überprüft werden. Die Option `-c` legt fest, dass die Quoten-Dateien für alle Quoten-aktivierten Dateisysteme erstellt werden sollen, die Option `-u` überprüft auf Benutzer-Quoten, und die Option `-g` überprüft auf Gruppen-Quoten.

Wenn weder `-u` noch `-g` angegeben werden, wird nur die Datei für die Benutzer-Quoten erstellt. Wenn nur `-g` angegeben wird, wird nur die Datei für Gruppen-Quoten erstellt.

Nachdem die Dateien erstellt wurden, führen Sie den folgenden Befehl aus, um die Tabelle für die aktuelle Festplattennutzung pro Dateisystem mit aktivierten Quoten zu erstellen:

```
quotacheck -avug
```

Die Optionen sind wie folgt:

- `a` — Überprüfen aller quoten-aktivierten, lokal gemounteten Dateisysteme
- `v` — Anzeigen detaillierter Statusinformationen während der Quoten-Überprüfung
- `u` — Überprüfen der Informationen zu Benutzer-Quoten
- `g` — Überprüfen der Informationen zu Gruppen-Quoten

Nachdem `quotacheck` beendet wurde, werden die Quoten-Dateien entsprechend der aktivierten Quoten (Benutzer und/oder Gruppen) mit Daten für jedes quoten-aktivierte Dateisystem, wie zum Beispiel `/home`, beschrieben.

6.1.4. Quoten pro Benutzer zuweisen

Der letzte Schritt ist das Zuweisen der Festplatten-Quoten mit Hilfe des Befehls `edquota`.

Um die Quoten für einen Benutzer zu konfigurieren, geben Sie als root im Shell-Prompt folgenden Befehl ein:

```
edquota username
```

Führen Sie diesen Schritt für jeden Benutzer aus, für den Sie eine Quote festlegen möchten. Wenn zum Beispiel eine Quote in der Datei `/etc/fstab` für die `/home`-Partition (`/dev/hda3`) aktiviert wurde und der Befehl `edquota testuser` ausgeführt wurde, wird Folgendes im Standardeditor des Systems angezeigt:

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

Anmerkung

Der Texteditor, der durch die Umgebungsvariable EDITOR festgelegt ist, wird auch vom Befehl `edquota` verwendet. Um den Editor zu ändern, müssen Sie die Umgebungsvariable EDITOR auf den vollständigen Pfad zum Editor Ihrer Wahl ändern.

In der ersten Spalte befindet sich der Name des Dateisystems, das für Quoten aktiviert wurde. In der zweiten Zeile wird angezeigt, wieviele Blöcke der Benutzer zur Zeit verwendet. Die nächsten beiden Spalten werden zum Einstellen weicher und harter Block-Grenzen für den jeweiligen Benutzer des Dateisystems verwendet. Die Spalte `inodes` zeigt an, wieviele Inodes der Benutzer zur Zeit verwendet. Die letzten beiden Spalten werden zum Einstellen weicher und harter Inode-Grenzen für den jeweiligen Benutzer dieses Dateisystems verwendet.

Eine harte Grenze ist der höchstzulässige Festplattenplatz, den ein Benutzer oder eine Gruppe verwenden kann. Sobald diese Grenze erreicht wird, kann kein weitere Platz in Anspruch genommen werden.

Die weiche Grenze definiert den höchstzulässigen Festplattenplatz, der verwendet werden kann. Im Gegensatz zur harten Grenze kann die weiche Grenze jedoch über einen bestimmten Zeitraum überschritten werden. Dieser Zeitraum wird als *Kulanzzeitraum* bezeichnet. Dieser Zeitraum kann in Sekunden, Minuten, Stunden, Tagen, Wochen oder Monaten ausgedrückt werden.

Wenn einer dieser Werte auf 0 gesetzt ist, bedeutet dies, dass keine Grenze angegeben wurde. Sie können im Texteditor die gewünschten Grenzen einstellen. Zum Beispiel:

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

Um zu prüfen, dass die Quote für den Benutzer gesetzt wurde, geben Sie folgenden Befehl ein:

```
quota testuser
```

6.1.5. Quoten pro Gruppe zuweisen

Quoten können auch auf Gruppen-Basis zugewiesen werden. Wenn Sie zum Beispiel eine Gruppen-Quote für die Gruppe `devel` festlegen möchten, verwenden Sie den folgenden Befehl (die Gruppe muss vor dem Einstellen der Gruppen-Quote bereits bestehen):

```
edquota -g devel
```

Dieser Befehl zeigt die bestehenden Quoten für die Gruppe im Texteditor an:

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

Ändern Sie nun die Grenzen, speichern Sie die Datei, und konfigurieren Sie dann die Quote.

Um zu prüfen, dass Sie Gruppen-Quote eingestellt wurde, geben Sie den folgenden Befehl ein:

```
quota -g devel
```

6.1.6. Quoten pro Dateisystem zuweisen

Um Quoten pro quoten-aktiviertes Dateisystem festzulegen, geben Sie den folgenden Befehl ein:

```
edquota -t
```

Wie bei den anderen `edquota`-Befehlen auch, werden im Texteditor die aktuellen Quoten pro Dateisystem angezeigt:

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

Ändern Sie hier den Kulanzzeitraum für Blöcke oder Inodes, speichern Sie die Änderungen, und beenden Sie den Texteditor.

6.2. Verwalten von Festplatten-Quoten

Nachdem die Quoten implementiert wurden, bedürfen diese einiger Wartung — vorwiegend durch Überprüfung auf Überschreitung und Richtigkeit bzw. Genauigkeit dieser Quoten. Wenn natürlich einige Benutzer wiederholt ihre Quoten überschreiten oder ständig die weichen Grenzen erreichen, muss ein Systemadministrator einige Entscheidungen in Bezug auf das Verhalten des Benutzer und wieviel Festplattenplatz dieser für seine Arbeit benötigt, treffen. Der Administrator kann dann zum Beispiel dem Benutzer zeigen, wie dieser weniger Festplattenplatz braucht oder die Quote dieses Benutzers erhöhen.

6.2.1. Berichte über Festplatten-Quoten erstellen

Um einen Bericht über die Festplattennutzung zu erstellen, müssen Sie das Dienstprogramm `repquota` ausführen. Der Befehl `repquota /home` gibt zum Beispiel folgendes aus:

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

Um einen Bericht über die Festplattennutzung aller quoten-aktivierten Dateisysteme anzeigen zu lassen, geben Sie den folgenden Befehl:

```
repquota -a
```

Auch wenn dieser Bericht relativ einfach zu verstehen ist, sollen doch einige Punkte erklärt werden. Durch `--` hinter jedem Benutzer können Sie schnell feststellen, ob die Block- oder Inodegrenzen überschritten wurden. Wenn die weichen Grenzen für Block- oder Inodegrenze überschritten würde, wird ein `+` anstelle von dem entsprechenden `-` angezeigt; das erste `-` steht für die Blockgrenze, und das zweite Zeichen steht für die Inodegrenze.

Die Spalten `grace` sind normalerweise leer. Wenn eine weiche Grenze überschritten wurde, enthält diese Spalte eine Zeitangabe, die dem Kulanzzeitraum, d.h. der Zeit, die innerhalb des Kulanzzeitraums verblieben ist, entspricht. Wenn der Kulanzzeitraum überschritten würde, erscheint `none` an dieser Stelle.

6.2.2. Genauigkeit der Quoten einhalten

Wenn ein Dateisystem nicht richtig gemounted wurde (zum Beispiel aufgrund eines Systemabsturzes), müssen Sie `quotacheck` ausführen. `quotacheck` kann jedoch auch regelmäßig ausgeführt werden, auch wenn das System nicht abgestürzt ist. Das Ausführen dieses Befehls hilft Ihnen, die Genauigkeit der Quoten besser einzuhalten (Optionen für diesen Befehl wurden unter Abschnitt 6.1.1) beschrieben:

```
quotacheck -avug
```

Der einfachste Weg zur regelmäßigen Ausführung ist mit `cron`. Sie können als root angemeldet entweder den Befehl `crontab -e` zum Planen eines regelmäßigen `quotacheck` verwenden, oder ein Skript, das `quotacheck` ausführt, in einem der folgenden Verzeichnisse ablegen (wählen Sie den Intervall, der Ihren Anforderungen am besten entspricht):

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

Die genaueste Quoten-Statistik wird dann erreicht, wenn die untersuchten Dateisysteme sich nicht in Benutzung befinden. Daher sollte cron zu einem Zeitpunkt ausgeführt werden, zu dem die Dateisysteme am wenigsten genutzt werden. Wenn auf verschiedenen Dateisysteme mit Quoten verschiedenen Zeiten zutreffen, können Sie `quotacheck` für jedes Dateisystem durch mehrere cron-Tasks zur jeweils besten Zeit ausführen.

Unter Kapitel 37 finden Sie weitere Informationen zur Konfiguration von `cron`.

6.2.3. Aktivieren und Deaktivieren

Sie können Quoten auch deaktivieren, ohne diese auf 0 setzen zu müssen. Um alle Benutzer- und Gruppen-Quoten zu deaktivieren, verwenden Sie den folgenden Befehl:

```
quotaoff -vaug
```

Wenn weder die Option `-u` noch die Option `-g` angegeben wird, werden nur die Benutzer-Quoten deaktiviert. Wenn nur `-g` angegeben wird, werden nur die Gruppen-Quoten deaktiviert.

Um die Quoten wieder zu aktivieren, verwenden Sie den Befehl `quotaon` mit den gleichen Optionen.

Wenn Sie zum Beispiel Benutzer- und Gruppen-Quoten für alle Dateisysteme aktivieren möchten:

```
quotaon -vaug
```

Um Quoten für ein bestimmtes Dateisystem wie zum Beispiel `/home` aktivieren möchten:

```
quotaon -vug /home
```

Wenn weder die Option `-u` noch die Option `-g` angegeben wird, werden nur die Benutzer-Quoten deaktiviert. Wenn nur `-g` angegeben wird, werden nur die Gruppen-Quoten deaktiviert.

6.3. Zusätzliche Ressourcen

In den folgenden Ressourcen finden Sie weitere Informationen zu Festplatten-Quoten.

6.3.1. Installierte Dokumentation

- Sie man-Seiten zu `quotacheck`, `edquota`, `repquota`, `quota`, `quotaon` und `quotaoff`

6.3.2. Bücher zum Thema

- *Red Hat Enterprise Linux Introduction to System Administration* Red Hat, Inc. — Erhältlich unter http://www.redhat.com/docs/ und auf der Dokumentations-CD. Dieses Handbuch enthält Hintergrundinformationen zu Speicherverwaltung (einschließlich Festplatten-Quoten) für neue Red Hat Enterprise Linux Systemadministratoren.

redhat

Kapitel 7.

Benutzerdefinierte Gerätenamen

Das Verzeichnis `/dev/` enthält virtuelle Dateien, die Geräte darstellen. Jede virtuelle Datei steht für ein Gerät im System, wie zum Beispiel Speichergeräte, USB-Geräte oder Drucker. Diese virtuellen Dateien nennen sich*Gerätenamen*.

Gerätenamen für IDE-Geräte beginnen mit `hd` und Gerätenamen für SCSI-Geräte beginnen mit `sd`. Diese beiden Buchstaben werden dann durch einen weiteren, beginnend mit a, ergänzt, was die Reihenfolge der Geräte festlegt. Zum Beispiel ist `/dev/hda` die erste IDE-Festplatte, `/dev/hdb` die zweite, `/dev/hdc` die dritte und so weiter.

Ist an den Gerätenamen eine Ziffer angehängt, steht diese für die Nummer der Partition. So steht zum Beispiel `/dev/hda1` für die erste Partition auf der ersten IDE-Festplatte.

Wird die Festplatte auf eine andere Stelle im Computer verlegt oder die Initialisierung dieser schlägt fehl, dann ändern sich einige der Gerätenamen, wodurch womöglich einige Referenzen zu Gerätenamen ungültig werden. Wie unter Abbildung 7-1 angezeigt, wird bei einem System mit drei SCSI-Festplatten, bei dem die zweite SCSI-Festplatte entfernt wird, `/dev/sdc` zu `/dev/sdb`, was Referenzen zu`/dev/sdc` und außerdem zu `/dev/sdb` ungültig werden lässt.

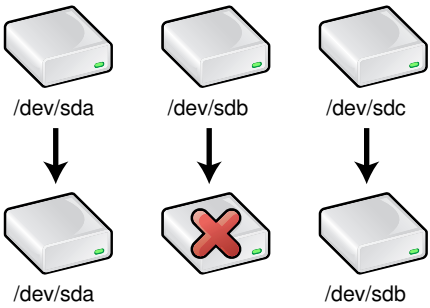

Abbildung 7-1. Entfernen einer Festplatte

Jede Festplatte hat eine eindeutige und einzigartige Identifikation, die mit *UUID* bezeichnet wird. Um das Problem wechselnder Gerätenamen zu lösen, ermöglicht `devlabel` benutzerdefinierte Gerätenamen, die mit diesem UUIDs in Verbindung stehen. Ein symbolischer Link wird vom benutzerdefinierten Gerätenamen zum tatsächlichen Gerätenamen hergestellt. Ändert sich der tatsächliche Gerätename, wird der symbolische Link aktualisiert, so dass dieser wieder auf die gleiche Festplatte mit der gleichen UUID weist. Es kann so auf IDE und SCSI Speichergeräte über die benutzerdefinierten Namen verwiesen werden.

`Devlabel` ermöglicht desweiteren das automatische Mounten von Hotplug-Geräten wie externe Festplatten und USB-Geräte wie die Speicherkarten für Digitalkameras. Wird das automatische Mounten konfiguriert, wird das Gerät nach dem Anschließen mit dem benutzerdefinierten Namen gemountet.

7.1. Konfiguration von `Devlabel`

Benutzerdefinierte Gerätenamen können basierend auf dem Gerätenamen, Partitionsnamen oder der UUID der Festplatte hinzugefügt werden.

Verwenden Sie die folgende Syntax, um einen benutzerdefinierten Gerätenamen für ein Speichergerät hinzuzufügen. Das angegebene Gerät kann entweder das gesamte Gerät sein, oder eine einzelne Partition auf einem Gerät.

```
devlabel add -d <device> -s <symlink>
```

Um zum Beispiel den symbolischen Link `/dev/work` alsDarstellung der `/dev/hdb1`-Partition zu verwenden, geben Sie folgenden Befehl ein:

```
devlabel add -d /dev/hdb1 -s /dev/work
```

War der Befehl erfolgreich, wird folgendes angezeigt:

```
Created symlink /dev/work -> /dev/hdb1
Added /dev/work to /etc/sysconfig/devlabel
```

Um einen Gerätenamen für ein Gerät basierend auf einer UUID zu vergeben, verwenden Sie folgende Syntax:

```
devlabel add -u <uuid> -s <symlink>
```

Um `devlabel` zum Herausfinden der UUID eines Geräts (oder um sicherzustellen, das dies Gerät eine besitzt), zu verwenden, geben Sie folgenden Befehl ein:

```
devlabel printid -d <device>
```

Der Name des symbolischen Links muss einzigartig sein. Wird versucht, einen Link hinzuzufügen. obwohl es diesen schon gibt, wird die Konfigurationsdateo nicht geändert, und das Folgende wird angezeigt:

```
The file /dev/work already exists.
Failure. Could not create a symlink.
```

Um einen symbolischen Link aus der `devlabel`-Liste zu entfernen, verwenden Sie den folgenden Befehl:

```
devlabel remove -s <symlink>
```

Der Eintrag wird aus der Konfigurationsdatei entfernt und der symbolische Link geläscht.

Um den Status der symbolischen Links unter `devlabel` festzustellen, verwenden Sie den folgenden Befehl:

```
devlabel status
```

Eine Ausgabe ähnlich wie folgende wird angezeigt:

```
lrwxrwxrwx    1 root             9 Apr 29 13:20 /dev/work -> /dev/hdb1
lrwxrwxrwx    1 root             9 Apr 29 13:41 /dev/tcf -> /dev/hda1
```

7.1.1. Hotplug-Geräte

Ein Programm mit dem Namen *Hotplug* führt Aktionen aus, wenn eine Systemvorgang, wie das Hinzufügen oder Entfernen von Hardware, stattfindet während das System läuft. Wenn zum Beispiel eine USB-Festplatte oder ein USB-Medienkartenleser ans das System angeschlossen wird, benachrichtigt `hotplug` Benutzer über eine Nachricht in der System-Log-Datei (`/var/log/messages`) und lädt das richtige Kernel-Modul, damit das Gerät funktioniert.

Wird ein PCI, USB oder IEEE 1394 (auch als FireWire bekannt) Gerät angeschlossen, starten die `hotplug` Skripte auch `devlabel` neu, so dass die Speichermedien einen benutzerdefinierten Gerätenamen (z.B. `/dev/usbcard`) erhalten und optional dazu das Speichergerät automatische gemountet wird.

Nachdem der USB-Kartenleser in den USB-Port des Computers eingesteckt wurde, geben Sie den folgenden Befehl als root ein (wobei `/dev/sda1` der Gerätename für die Medienkarte und `/dev/usbcard` der zu verwendene benutzerdefinierte Gerätename ist):

```
devlabel add -d /dev/sda1 -s /dev/usbcard --automount
```

Dieser Befehl fügt einen Eintrag für den Mount-Punkt zu `/etc/sysconfig/devlabel` hinzu und erstellt einen symbolischen Link von `/dev/usbcard` zu `/dev/sda1`. Die Option `--automount` für `devlabel` gibt an, dass das Gerät automatisch bei einem Neustart von `devlabel` gemountet werden soll, wenn ein Eintrag in `/etc/fstab` vorhanden ist und das Gerät existiert (ein Gerät mit der gleichen UUID gefunden wird).

`updfstab` ist ein Programm, das die IDE- und SCSI-Busse auf neue Geräte hin scannt und Einträge für diese in `/etc/fstab` hinzufügt, falls es noch keine Einträge gibt. Es fügt außerdem Einträge für USB-Geräte hinzu, da diese als SCSI-Geräte angezeigt werden. Weitere Informationen hierzu finden Sie auf den `updfstab` man-Seiten.

Wenn ein USB-Gerät angeschlossen wird, führt `hotplug` das Programm `updfstab` aus, welches wiederum einen Eintrag in die Datei `/etc/fstab` für das Speichergerät (z.B. eine Medienkarte) hinzufügt, wenn diese existiert. (Wird ein Kartenleser ohne Karte installiert, wird kein Eintrag hinzugefügt). Die hinzugefügte Zeile enthält den tatsächlichen Gerätenamen (z.B. `/dev/sda1`) und die Option `kudzu`. Die Option `kudzu` sagt **Kudzu**, [1] dass es die Zeile entfernen kann, wenn das Gerät nicht existiert. Da die Zeile von `devlabel` benötigt wird, muss die Option `kudzu` entfernt werden, damit die Zeile in der Datei bleibt. Ändern Sie auch den Gerätenamen in `devlabel`-Gerätenamen (z.B. `/dev/usbcard`) und erstellen Sie den Mountpunkt (z.B. `/mnt/usbcard`).

Nach den Änderungen sollten die Zeile wie folgt aussehen:

```
/dev/usbcard    /mnt/usbcard    auto    noauto,owner 0 0
```

Durch `--automount` wird, nachdem `devlabel` neu gestartet und das USB-Gerät an den Computer angeschlossen wurde, das Speichermedium im USB-Kartenleser unter `/mnt/usbcard` gemountet. Der Trick dabei ist, dass beim Anschließen des USB-Kartenlesers an den Computer sich die Karte bereits im Leser befinden muss. Sonst kann `devlabel` das Speichergerät nicht finden, und daher auch nicht automatisch mounten.

Ist der USB-Kartenleser bereits angeschlossen, aber ohne Karte, müssen Sie als root den Befehl `devlabel restart` eingeben, wenn die Karte eingelegt wurde, um diese zu mounten.

7.2. Funktionsweise

Der Befehl `devlabel restart` wird vom `/etc/rc.sysinit` Skript aufgerufen, wenn das System gebootet wird, sowie auch durch die jeweiligen Skripte im Verzeichnis `/etc/hotplug/`.

Die Option `restart` für `devlabel` liest die Geräteliste in der Konfigurationsdatei (`/etc/sysconfig/devlabel`) und folgt den symbolischen Links, um festzulegen, ob das Gerät am bisherigen Platz, z.B. `/dev/hdb1` existiert. Ist der symbolische Link ungültig, wird versucht, den neuen Ort der Festplatte basierend auf der UUID festzustellen. Wird eine Festplatte mit der selben UUID gefunden, wird der symbolische Link aktualisiert und weist auf den neuen Ort der Festplatte, die Konfigurationsdatei wird aktualisiert und eine Nachricht ähnlich wie folgende wird angezeigt:

1. **Kudzu** ist ein Hardware-Test-Tool, das zum System-Bootzeitpunkt ausgeführt wird, was festlegt, welche Hardware vom System entfernt oder zum System hinzugefügt wurde.

```
Device name incorrectly detected for symlink /dev/work!
The device /dev/hdb1 is now /dev/hdd1.
The symlink /dev/work will now point to the new device name.
```

Wird keine Festplatte mit der UUID gefunden (wenn die Festplatte entfernt wurde, zum Beispiel), wird folgendes angezeigt:

```
The device /dev/hdb1 no longer seems to exist. Because of this, the
symlink /dev/work -> /dev/hdb1 will not be available. The reference
to this symlink in /etc/sysconfig/devlabel will be ignored.
```

Der Eintrag für das Gerät wird nicht aus der Konfigurationsdatei gelöscht, sondern nur ignoriert.

7.3. Zusätzliche Ressourcen

Weitere Informationen zu `devlabel` finden Sie in den folgenden Ressourcen.

7.3.1. Installierte Dokumentation

- `man devlabel` — Die man-Seite für `devlabel` behandelt alle Optionen und enthält eine kurze Bescheibung zur Funktionsweise.
- `man updfstab` — Die man-Seite für das `updfstab`-Program, das von `hotplug` aufgerufen wird, wenn ein USB-Gerät angeschlossen wird.
- `man hotplug` — die man-Seite für `hotplug`.

7.3.2. Nützliche Webseiten

- http://www.dell.com/us/en/esg/topics/power_ps1q03-lerhaupt.htm — Unter *Resolving Device Renaming Issues in Linux*, beschreibt der Entwickler von `devlabel`, wie das Programm funktioniert.
- http://www.lerhaupt.com/devlabel/devlabel.html — Die Projektseite des Entwicklers.

redhat

Kapitel 8.

Zugriffskontroll-Listen (ACL)

Dateien und Verzeichnisse haben Berechtigungen für den Besitzer einer Datei, die Gruppe, zu der eine Datei gehört und alle anderen Benutzer des Systems. Diese Berechtigungen haben jedoch Grenzen. Es können z.B. verschiedene Berechtigungen nicht für verschiedene Benutzer konfiguriert werden. Aus diesem Grund wurden *Zugriffskontroll-Listen* (ACLs) eingeführt.

Der Red Hat Enterprise Linux 3 Kernel liefert ACL-Support für das ext3-Dateisystem und NFS-exportierte Dateisysteme. Die ACLs werden auch auf von Samba verwendeten ext3-Dateisystemen erkannt.

Zusammen mit dem Kernel wird das `acl`-Paket für die Implementierung von ACLs benötigt. Es enthält die Utilities zum Hinzufügen, Ändern, Entfernen und Abrufen von ACL-Informationen.

Die Befehle `cp` und `mv` kopieren oder verschieben alle ACLs, die in Zusammenhang mit Dateien und Verzeichnissen stehen.

8.1. Dateisysteme mounten

Bevor Sie ACLs für eine Datei oder ein Verzeichnis verwenden, muss die Partition hierfür mit AVL-Support gemountet werden. Ist dieses ein lokales ext3-Dateisystem, kann es mit dem folgenden Befehl gemountet werden:

```
mount -t ext3 -o acl <device-name> <partition>
```

Beispiel:

```
mount -t ext3 -o acl /dev/hdb3 /work
```

Ist die Partition in der Datei `/etc/fstab` aufgeführt, kann der Eintrag für die Partition die Option `acl` enthalten:

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

Wird auf ein ext3-Dateisystem über Samba zugegriffen und hierfür ACLs aktiviert, werden die ACLs erkannt, da Samba mit der Option `--with-acl-support` kompiliert wurde. Es werden keine besonderen Flags benötigt, wenn ein Samba-Share gemountet oder zugegriffen werden soll.

8.1.1. NFS

Als Vorgabe, wenn das von einem NFS-Server exportierte Dateisystem ACLs unterstützt, und der NFS-Client ACLs lesen kann, werden ACLs von dem Client-System verwendet.

Um ACLs auf NFS-Shares beim Konfigurieren des Servers zu deaktivieren, fügen Sie die `no_acl`-Option in der Datei `/etc/exports` hinzu. Um ACLs auf einer NFS-Share beim Mounten von einem Client zu deaktivieren, mounten Sie diese mit der `no_acl`-Option, entweder über die Befehlszeile, oder die Datei `/etc/fstab`.

8.2. Access ACLs einstellen

Es gibt zwei Arten von ACLs: *Access ACLs* und *Default ACLs*. Eine Access ACL ist die Zugriffskontroll-Liste für eine bestimmte Datei oder Verzeichnis. Eine Default ACL kann nur auf ein

Verzeichnis verweisen; wenn eine Datei innerhalb des Verzeichnisses keine Access ACL besitzt, werden die regeln der Default ACL für das Verzeichnis verwendet. Default ACLs sind optional.

ACLs können konfiguriert werden:

1. Pro Benutzer
2. Pro Gruppe
3. Über die effektive Rechte-Maske
4. Für Benutzer nicht in der Benutzergruppe für diese Datei

Das `setfacl` Utility setzt ACLs für Dateien und Verzeichnisse. Verwenden Sie `-m`, um die ACL für eine Datei oder ein Verzeichnis hinzuzufügen oder zu ändern:

```
setfacl -m <rules> <files>
```

Regeln (`<rules>`) müssen eines der folgenden Formate besitzen. Es können mehrere Regeln im gleichen Befehl festgelegt werden, wenn diese durch Kommata getrennt sind.

`u:<uid>:<perms>`

Setzt die Access-ACL für einen Benutzer. Der Benutzername oder UID kann angegeben werden. Der Benutzer kann ein beliebiger, gültiger Benutzer auf dem System sein.

`g:<gid>:<perms>`

Setzt die Access-ACL für eine Gruppe. Der Gruppenname oder GID kann angegeben werden. Die Gruppe kann eine beliebige, gültige Gruppe auf dem System sein.

`m:<perms>`

Setzt die effektive Rechte-Maske. Die Maske ist die Zusammenstellung aller Berechtigungen der Gruppe und aller Benutzer- und Gruppen-Einträge.

`o:<perms>`

Setzt die Access-ACL für Benutzer, die nicht in einer Gruppe für die Datei sind.

Leerzeichen werden ignoniert. Die Berechtigungen (`<perms>`) müssen eine Kombination der Zeichen `r`, `w` und `x` für Lesen, Schreiben und Ausführen sein.

Hat eine Datei oder ein Verzeichnis bereits ein ACL und es wird der `setfacl` Befehl verwendet, werden die zusätzlichen Regeln zu den bestehenden ACL hinzugefügt oder die bestehenden Regeln geändert.

Um der Benutzerin tfox Lese- und Schreibberechtigungen zu geben:

```
setfacl -m u:tfox:rw /project/somefile
```

Um alle Rechte für einen Benutzer, eine Gruppe oder Andere zu entfernen, benutzen Sie die Option `-x` ohne Angabe jeglicher Rechte:

```
setfacl -x <rules> <files>
```

Um alle Berechtigungen vom Benutzer mit der UID 500 zu entfernen:

```
setfacl -x u:500 /project/somefile
```

8.3. Einstellen von Default ACLs

Um eine Standard-ACL zu setzen, setzen Sie `d:` vor die Regel und geben Sie ein Verzeichnis anstelle eines Dateinamens an.

Um zum Beispiel die Default ACL für das `/share/`-Verzeichnis zu setzen, dass Benutzer, die nicht in der Benutzergruppe sind, diese Lesen und Schreiben können (eine Access ACL für eine individuelle Datei kann dies überschreiben):

```
setfacl -m d:o:rx /share
```

8.4. ACLs abrufen

Um die bestehenden ACLs für eine Datei oder ein Verzeichnis festzustellen, verwenden Sie den Befehl`getfacl`:

```
getfacl <filename>
```

Die Ausgabe sieht so ähnlich wie folgt aus:

```
# file: file
# owner: tfox
# group: tfox
user::rw-
user:smoore:r--
group::r--
mask::r--
other::r--
```

Wird ein Verzeichnis angegeben und besitzt eine Default ACl, wird diese auch angezeigt:

```
# file: file
# owner: tfox
# group: tfox
user::rw-
user:smoore:r--
group::r--
mask::r--
other::r--
default:user::rwx
default:user:tfox:rwx
default:group::r-x
default:mask::rwx
default:other::r-x
```

8.5. Dateisysteme mit ACLs archivieren

Achtung

Die Befehle `tar` und `dump` führen *keine* Backups von ACLs durch.

Das `star` Utility ähnelt der `tar` Utility idarin, das diese zum Erzeugen von Dateiarchiven verwendet werden kann; einige Optionen sind jedoch anders. Eine Liste häufig verwendeter Optionen finden Sie

unter Tabelle 8-1. Alle verfügbaren Optionen finden Sie auf der man-Seite zu `star`. Das `star`-Paket wird für die Verwendung dieser Utility benötigt.

Option	Beschreibung
`-c`	Erstellt eine Archivdatei.
`-n`	Extrahiert die Dateien nicht; Wird zusammen mit `-x` verwendet, um anzuzeigen, was ein Extrahieren der Dateien anrichtet.
`-r`	Ersetzt Dateien im Archiv. Die Dateien werden ans Ende der Archivdatei geschrieben und ersetzen alle Dateien mit dem gleichen Pfad- und Dateinamen.
`-t`	Zeigt den Inhalt einer Archivdatei an.
`-u`	Aktualisiert eine Archivdatei. Die Dateien werden ans Ende des Archivs geschrieben, wenn diese nicht im Archiv sein sollten oder wenn die Dateien neuer sind als solche mit dem gleichen Namen im Archiv. Diese Option funktioniert nur, wenn das Archiv eine Datei oder ein nicht-blockiertes Band ist, das die Fähigkeit zum Backspace hat.
`-x`	Extarhiert die Dateien aus dem Archiv. Wenn dies zusammen mit `-U` verwendet wird und eine Datei im Archiv älter ist als die entsprechende Datei auf dem Dateisystem, wird diese nicht extrahiert.
`-help`	Zeigt die wichtigsten Optionen an.
`-xhelp`	Zeigt die nicht so wichtigen Optionen an.
`-/`	Vorausgehende Schrägstriche vor Dateibnamen werden bei der Extraktion aus einem Archiv nicht entfernt. Standardmäßig werden die Schrägstriche beim Extrahieren entfernt.
`-acl`	Beim Erstellen oder Extrahieren, werden ACLs zu Dateien oder Verzeichnissen archiviert oder abgerufen.

Tabelle 8-1. Befehlszeilenoptionen für `star`

8.6. Kompatibilität mit älteren Systemen

Wurde auf einer Datei auf einem beliebigen Dateisystem eine ACL gesetzt, besitzt dieses Dateisystem das Attribut `ext_attr`. Dieses Attribut kann über den folgenden Befehl angezeigt werden:

```
tune2fs -l <filesystem-device>
```

Ein Dateisystem, das das Attribut `ext_attr` besitzt, kann mit älteren Kerneln gemountet werden, diese erzwingen jedoch keine gesetzten ACLs.

Versionen der `e2fsck` Utility, die ab Version 1.22 des `e2fsprogs`-Pakets enthalten sind (inklusive der Versionen in Red Hat Enterprise Linux 2.1 und 3) können eine Dateisystem mit dem `ext_attr`-Attribut prüfen. Ältere Versionen verweigern dieses.

8.7. Zusätzliche Ressourcen

In den folgenden Ressourcen finden Sie weitere Informationen.

8.7.1. Installierte Dokumentation

- `acl` man-Seite — Beschreibung von ACLs
- `getfacl` man-Seite — Beschreibt Datei-Zugriffskontroll-Listen
- `setfacl` man-Seite — Beschreibt das Setzen von Datei-Zugriffskontroll-Listen
- `star` man-Seite — Nähere Beschreibung der `star`-Utility und deren vieler Optionen

8.7.2. Nützliche Webseiten

- http://acl.bestbits.at/ — Webseite für ACLs
- http://www.fokus.gmd.de/research/cc/glone/employees/joerg.schilling/private/star.html — Webseite für die `star`-Utility

II. Installations-bezogene Informationen

Das *Red Hat Enterprise Linux Installationshandbuch* beschreibt den Installationsvorgang in Red Hat Enterprise Linux und einige grundlegende Punkte zum Troubleshooting. Erweiterte Installationsoptionen sind allerdings in diesem Handbuch beschrieben. Dieser Teil gibt Anleitungen zu*kickstart* (einer Methode zur automatischen Installation), System-Recovery Modi (wie Sie Ihr System booten können, wenn dies nicht in den normalen Runlevel startet), das Konfigurieren eines RAID und eines LVM während der Installation. Benutzen Sie diesen Teil in Verbindung mit dem *Red Hat Enterprise Linux Installationshandbuch*, um diese fortgeschrittenen Installations-Tasks durchzuführen.

Inhaltsverzeichnis

redhat

Kapitel 9.

Kickstart-Installation

9.1. Was ist eine Kickstart-Installation?

Viele Systemadministratoren würden Red Hat Enterprise Linux auf den Rechnern lieber mit automatisierten Methoden installieren. Als Antwort auf diese Nachfrage hat Red Hat die Installationsart Kickstart entwickelt. Der Systemadministrator kann dabei alle Informationen, die während einer typischen Installation abgefragt werden, in einer einzigen Datei zusammenstellen.

Die Kickstart-Dateien werden auf einem einzelnen Server-System bereitgestellt und können von dort während der Installation von den einzelnen Computern gelesen werden. Diese Methode ist so leistungsfähig, dass oft eine einzige Kickstart-Datei genügt, um Red Hat Enterprise Linux auf mehreren Maschinen zu installieren. Dadurch ist sie ideal für Netzwerk- und Systemadministratoren.

Kickstart ermöglicht die Automatisierung der Red Hat Enterprise Linux-Installation.

9.2. So führen Sie eine Kickstart-Installation durch

Kickstart-Installationen können mit Hilfe einer lokalen CD-ROM, einer lokalen Festplatte oder mit Hilfe von Installationsarten wie NFS, FTP oder HTTP durchgeführt werden.

Damit Sie Kickstart verwenden können, müssen Sie:

1. Eine Kickstart-Datei erstellen.
2. Eine Bootdisk mit der Kickstart-Datei erstellen oder die Kickstart- Datei auf dem Netzwerk zur Verfügung stellen.
3. Das Installationsverzeichnis zur Verfügung stellen.
4. Die Kickstart-Installation starten.

In diesem Kapitel werden diese Schritte detailliert vorgestellt.

9.3. Erstellen einer Kickstart-Datei

Bei der Kickstart-Datei handelt es sich um eine einfache Textdatei, die mehrere jeweils durch Schlüsselwörter gekennzeichnete Einträge enthält. Sie können diese Datei erstellen, indem Sie eine Kopie der Datei `sample.ks` aus dem `RH-DOCS` Verzeichnis der Red Hat Enterprise Linux Dokumentations-CD-ROM bearbeiten, die Applikation **Kickstart Configurator** benutzen oder die Datei ganz neu anlegen. Das Red Hat Enterprise Linux-Installationsprogramm erstellt auch auf Grundlage der während der Installation ausgewählten Optionen eine Beispiels-Kickstart-Datei. Sie wird in die Datei `/root/anaconda-ks.cfg` geschrieben. Sie sollten sie mit jedem Texteditor oder Textverarbeitungsprogramm bearbeiten können, die Dateien als ASCII-Text speichern können.

Zunächst ein paar grundsätzliche Regeln, die bei der Erstellung der Kickstart-Datei berücksichtigt werden müssen:

- Die *Reihenfolge* der Sektionen ist vorgeschrieben. Einträge in den Sektionen müssen nicht in einer bestimmten Reihenfolge angeordnet sein, sofern nicht anders angegeben. Die Sektionsreihenfolge lautet:

- Befehlssektion — Unter Abschnitt 9.4 finden Sie eine Liste mit Kickstart- Optionen. Sie müssen die erforderlichen Optionen aufnehmen.
- Die Sektion `%packages` — Unter Abschnitt 9.5 finden Sie weitere Informationen.
- Die Sektionen `%pre` und `%post` — — Diese beiden Sektionen können in jeder beliebigen Reihenfolge angeordnet werden und sind nicht erforderlich. Weitere Informationen finden Sie unter Abschnitt 9.6 und Abschnitt 9.7.

- Nicht erforderliche Einträge können weggelassen werden.
- Das Weglassen erforderlicher Einträge wirkt sich insofern aus, als das Installationsprogramm den Benutzer wie bei einer normalen Installation zur Eingabe der nötigen Angaben auffordert. Danach wird die Installation im automatischen Modus fortgesetzt (es sei denn, es fehlen noch weitere Einträge).
- Zeilen, die mit einem Hash-Zeichen ("#") beginnen, werden als Kommentar interpretiert und ignoriert.
- Für Kickstart-*Aktualisierungen* sind folgende Einträge erforderlich:
  - Sprache
  - Sprach-Support
  - Installationsart
  - Geräteangabe (wenn das Gerät zum Durchführen der Installation erforderlich ist)
  - Tastaturkonfiguration
  - Das Schlüsselwort `upgrade`
  - Bootloaderkonfiguration

  Andere eingetragene Informationen werden bei einer Aktualisierung ignoriert (dies gilt auch für ausgewählte Pakete).

9.4. Kickstart-Optionen

Die folgenden Optionen können in einer Kickstartdatei verwendet werden. Wenn Sie lieber ein grafisches Interface zum Erstellen der Kickstartdatei verwenden, können Sie die Applikation **Kickstart Configurator** verwenden. Weitere Details finden Sie im Kapitel 10.

Anmerkung

Folgt der Option ein Gleich-Zeichen (=), muss danach ein Wert angegeben werden. In den Beispielbefehlen sind die Optionen in Klammern ([]) optionale Argumente für den Befehl.

`autopart` (optional)

Erstellt automatisch Partitionen — eine 1 GB oder mehr root (`/`) Partition, eine Swap-Partition und eine angemessene Boot-Partition für die Architektur. Es können eine oder mehr Standard-Partitionsgrößen mit der `part`-Direktive definiert werden.

`autostep` (optional)

Ähnelt `interactive` mit dem Unterschied, dass es für Sie zum nächsten Bildschirm wechselt. Wird meistens zum Debuggen verwendet.

`auth` oder `authconfig` (obligatorisch)

Richtet die Authentifizierungsoptionen für das System ein. Dieser Befehl ähnelt dem Befehl `authconfig`, der nach der Installation ausgeführt werden kann. Standardmäßig wird statt Shadow-Passwörtern die normale Verschlüsselung verwendet.

`--enablemd5`

Verwendet die md5-Verschlüsselung für Benutzerpasswörter.

`--enablenis`

Aktiviert die NIS-Unterstützung. Standardmäßig verwendet `--enablenis` die nächste Domain, die im Netzwerk gefunden wird. Eine Domain sollte fast immer manuell eingestellt werden (über `--nisdomain`).

`--nisdomain`

NIS-Domainname für NIS-Dienste.

`--nisserver`

Server für NIS-Dienste (Standardvorgabe ist Broadcast).

`--useshadow` oder `--enableshadow`

Verwendet Shadow-Passwörter.

`--enableldap`

Aktiviert die LDAP-Unterstützung in `/etc/nsswitch.conf` und ermöglicht es dem System, Informationen über die Benutzer (UIDs, Home-Verzeichnisse, Shells, usw.) aus einem LDAP-Verzeichnis abzufragen. Um diese Option verwenden zu können, muss das Paket `nss_ldap` installiert sein. Außerdem müssen Sie einen Server und einen Basis-DN mit `--ldapserver=` und `--ldapbasedn=` angeben.

`--enableldapauth`

Verwendet LDAP als Methode zur Authentifizierung. Dadurch wird das Modul `pam_ldap` in die Lage versetzt, Authentifizierungen und Passwortänderungen unter Verwendung eines LDAP-Verzeichnisses vorzunehmen. Um diese Option verwenden zu können, muss das Paket `nss_ldap` installiert sein. Außerdem müssen Sie einen Server und einen Basis-DN mit `--ldapserver=` und `--ldapbasedn=` angeben.

`--ldapserver=`

Der Name des verwendeten LDAP-Servers, wenn Sie entweder `--enableldap` oder `--enableldapauth` angegeben haben. Diese Option wird in der Datei `/etc/ldap.conf` gespeichert.

`--ldapbasedn=`

Wenn Sie entweder `--enableldap` oder `--enableldapauth` angegeben haben, ist dies der eindeutige Name (Distinguished Name, DN) im LDAP-Verzeichnisbaum, unter dem die Benutzerinformationen gespeichert sind. Diese Option wird in der Datei `/etc/ldap.conf` gespeichert.

`--enableldaptls`

Verwendet TLS (Transport Layer Security)-Lookups. Mit dieser Option kann das LDAP vor der Authentifizierung verschlüsselte Benutzernamen und Passwörter an einen LDAP-Server senden.

`--enablekrb5`

Verwendet Kerberos 5 zur Authentifizierung von Benutzern. Kerberos selbst kann keine Home-Verzeichnisse, UIDs oder Shells abrufen. Wenn Sie Kerberos aktivieren, müssen Sie auch weiterhin LDAP, NIS oder Hesiod aktivieren bzw. den Befehl `/usr/sbin/useradd` verwenden, um der Workstation Informationen zu Accounts zu übergeben. Um diese Option verwenden zu können, muss das Paket `pam_krb5` installiert sein.

`--krb5realm`

Der Kerberos 5-Realm, zu dem Ihre Workstation gehört.

`--krb5kdc`

KDC (Key Distribution Center) oder KDCs, die Anfragen für den Realm bearbeiten. Falls sich mehrere KDCs im Realm befinden, müssen Sie die Namen durch Kommata (,) trennen.

`--krb5adminserver`

Das KDC in Ihrem Realm, das ebenfalls kadmind ausführt. Dieser Server bearbeitet Passwortänderungen und andere Verwaltungsanfragen. Dieser Server muss auf dem Master-KDC ausgeführt werden, wenn Sie über mehrere KDCs verfügen.

`--enablehesiod`

Aktiviert die Hesiod-Unterstützung, um Home-Verzeichnisse von Benutzern, UIDs und Shells anzuzeigen. Weitere Informationen dazu, wie Sie Hesiod in Ihrem Netzwerk einrichten und verwenden, finden Sie in der Datei `/usr/share/doc/glibc-2.x.x/README.hesiod`, die im Lieferumfang des Paketes `glibc` enthalten ist. Hesiod ist eine Erweiterung des DNS und verwendet DNS-Datensätze, um Informationen über Benutzer, Gruppen und andere Objekte zu speichern.

`--hesiodlhs`

Die Option Hesiod LHS ("left-hand side", linke Seite), die in `/etc/hesiod.conf` gespeichert wird. Diese Option wird von der Hesiod-Bibliothek verwendet, um den Namen zu bestimmen, nach dem im DNS bei der Abfrage von Informationen gesucht werden soll. Die Funktionsweise ähnelt der Art, wie LDAP einen Basis-DN verwendet.

`--hesiodrhs`

Die Option Hesiod RHS ("right-hand side", rechte Seite), die in `/etc/hesiod.conf` gespeichert wird. Diese Option wird von der Hesiod-Bibliothek verwendet, um den Namen zu bestimmen, nach dem im DNS bei der Abfrage von Informationen gesucht werden soll. Die Funktionsweise ähnelt der Art, wie LDAP einen Basis-DN verwendet.

Tipp

Um z.B. Benutzerinformationen zu "jim" anzuzeigen, sucht die Hesiod-Bibliothek nach *jim.passwd<LHS><RHS>*. Das Suchergebnis wäre dann ein TXT-Eintrag, der dem Passworteintrag des Benutzers "Jim" entspricht (`jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`). Dieselbe Vorgehensweise gilt auch für Gruppen, mit dem einzigen Unterschied, dass *jim.group<LHS><RHS>* verwendet wird.

Es kann auch anhand von Nummern nach Benutzern und Gruppen gesucht werden. Dazu muss "501.uid" als CNAME für "jim.passwd" und "501.gid" als CNAME für "jim.group" angegeben werden. Bitte beachten Sie, dass keine Punkte [.] vor LHS und RHS gesetzt werden, wenn die Bibliothek den zu suchenden Namen bestimmt, obwohl LHS und RHS meist mit Punkten beginnen.

`--enablesmbauth`

Aktiviert die Authentifizierung eines Benutzers über einen SMB-Server (üblicherweise ein Samba- oder Windows-Server). SMB-Authentifizierungssupport unterstützt keine Home-Verzeichnisse, UIDs oder Shells. Wenn Sie diese Option verwenden, muss der Benutzer-Account der Workstation bekannt sein. Aktivieren Sie hierzu LDAP, NIS oder Hesiod oder verwenden Sie den Befehl `/usr/sbin/useradd`, um der Workstation die Accounts bekannt zu geben. Wenn Sie diese Option verwenden, muss das Paket `pam_smb` installiert sein.

`--smbservers=`

Der Name der/des Server(s), der für die SMB-Authentifizierung verwendet wird. Wenn Sie mehr als einen Server angeben möchten, trennen Sie die Namen durch Kommata (,).

`--smbworkgroup=`

Der Name der Arbeitsgruppe der SMB-Server.

`--enablecache`

Aktiviert den Dienst `nscd`. Der `nscd`-Dienst speichert Informationen über Benutzer, Gruppen und Anderes. Caching ist besonders hilfreich, wenn Sie Informationen über Benutzer und Gruppen über Ihr Netzwerk mit Hilfe von NIS, LDAP oder Hesiod verteilen möchten.

`Bootloader` (obligatorisch)

Legt fest, wie und welcher Bootloader installiert werden soll: LILO oder GRUB. Diese Option ist sowohl für Installationen als auch für Aktualisierungen erforderlich. Sollte bei einer Aktualisierungen `--useLILO` nicht angegeben und LILO der aktuelle Bootloader sein, so wird der Bootloader in GRUB umgeändert. Soll LILO bei Aktualisierungen beibehalten werden, verwenden Sie den Befehl `bootloader--upgrade`.

`--append`

Legt Kernelparameter fest. Um mehrere Parameter gleichzeitig festzulegen, trennen Sie diese mit Leerzeichen. Beispiel:

```
bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
```

`--driveorder`

Geben Sie an, welche Festplatte die erste in der BIOS-Bootabfolge ist. Zum Beispiel:

```
bootloader --driveorder=sda,hda
```

`--location`

Legt fest, wo der Boot Record geschrieben wird. Gültige Werte sind: `mbr` (Standard), `partition` (installiert den Bootloader im ersten Sektor der Partition, die den Kernel enthält) oder **`none`** (der Bootloader wird nicht installiert).

`--password=`

Wenn GRUB verwendet wird, wird das GRUB Bootloader-Passwort auf das Angegebene gesetzt. Dieses sollte verwendet werden, um den Zugriff auf die GRUB-Shell einzuschränken, über die beliebig Kernel-Optionen eingegeben werden können.

`--md5pass=`

Sollte GRUB ähnlich wie `--password` verwenden, nur mit dem Unterschied, dass das Passwort bereits verschlüsselt sein sollte.

`--useLilo`

Verwendet LILO statt GRUB als Bootloader.

`--linear`

Wenn Sie LILO verwenden, benutzen Sie die LILO-Option `linear`. Nur für die Rückwärtskompatibilität (wird jetzt standardmäßig verwendet).

`--nolinear`

Wenn Sie LILO verwenden, benutzen Sie die LILO Option `nolinear` (standardmäßig wird linear verwendet).

`--lba32`

Bei Verwendung von LILO wird der lba32-Modus anstelle von auto-detecting erzwungen.

`--upgrade`

Aktualisiert die vorhandene Bootloader-Konfiguration und behält dabei die alten Eingaben bei. Diese Option ist nur bei Aktualisierungen verfügbar.

`clearpart` (optional)

Entfernt Partitionen aus dem System, bevor neue Partitionen erstellt werden. Standardmäßig werden keine Partitionen entfernt.

Anmerkung

Wenn der Befehl `clearpart` verwendet wird, kann der Befehl `--onpart` auf einer logischen Partition nicht verwendet werden.

`--all`

Löscht alle Partitionen vom System.

`--drives=`

Legt fest, von welchen Laufwerken Partitionen gelöscht werden. So löscht folgendes zum Beispiel die Partitionen auf den ersten beiden Festplatten des primären IDE-Controllers:

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

`--initlabel`

Initialisiert die Plattenkennung mit dem Standard für Ihre Architektur (z.B. `msdos` für x86 und `gpt` für Itanium). Sehr nützlich, da das Installationsprogramm nicht nachfragen muss, ob es die Plattenkennung für eine neue Festplatte initialisieren muss.

`--linux`

Entfernt alle Linux-Partitionen.

`--none` (default)

Entfernen Sie keine Partitionen.

`cmdline` (optional)

Führen Sie die Installation in einemBefehlszeilenmodus aus, der keinerlei interaktive Elemente enthält. Jegliche Prompts für Interaktion halten die Installation auf. Dieser Modus ist sinnvoll für S/390 Systeme mit der x3270 Konsole.

`device` (optional)

Auf den meisten PCI-Systemen erkennt das Installationsprogramm automatisch die meisten Ethernet- und SCSI-Karten ordnungsgemäß. Auf älteren Systemen und einigen PCI-Systemen muss Kickstart jedoch beim Suchen der richtigen Geräte unterstützt werden. Der Befehl `device`, der das Installationsprogramm anweist Zusatzmodule zu installieren, hat folgendes Format:

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

<type>

Ersetzt entweder mit `scsi` oder `eth`

<modulename>

Ersetzt mit dem Namen des Kernelmoduls, das installiert sein sollte.

`--opts`

Optionen, die an das Kernelmodul übergeben werden sollen. Beachten Sie, dass durch Verwenden von Anführungszeichen mehrere Optionen übergeben werden können. Beispiel:

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

`driverdisk` (optional)

Bei Kickstart können Treiberdisketten verwendet werden. Kopieren Sie dazu den Inhalt einer Treiberdiskette in das Root-Verzeichnis einer Partition auf der Festplatte des Systems und verwenden Sie dann den Befehl `driverdisk`, um das Installationsprogramm anzuweisen, wo es danach suchen soll.

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

Es kann alternativ dazu eine Netzwerkspeicherstelle für die Treiberdiskette angegeben werden:

```
driverdisk --source=ftp://path/to/dd.img
driverdisk --source=http://path/to/dd.img
driverdisk --source=nfs:host:/path/to/img
```

<partition>

Partition, auf der sich die Treiberdiskette befindet.

`--type=`

Dateisystemtyp (z.B. vfat oder ext2).

`firewall` (optional)

Diese Option entspricht dem Bildschirm **Firewall-Konfiguration** im Installationsprogramm.

```
firewall --enabled|--disabled [--trust=] <device> [--port=]
```

`--enabled`

Lehne eingehende Verbindungen, die keine Antwort zu ausgehenden Anfragen sind, wie DNS-Antworten und DHCP-Anfragen, ab. Sollte Zugriff auf bestimmte Services benötigt werden, können diese Services durch die Firewall gelassen werden.

`--disabled`

Konfiguriere keine iptables-Regeln.

`--trust=`

Wenn Sie das Gerät, zum Beispiel eth0, hier auflisten, werden alle Kommunikationen von diesem Gerät über die Firewall ermöglicht. Verwenden Sie `--trust eth0 --trust eth1`, um mehrere Geräte aufzulisten. Verwenden Sie KEIN Format, das Kommata enthält (beispielsweise `--trust eth0, eth1`).

<*incoming*>

Wählen Sie keine oder mehrere der folgenden Optionen, um die angegebenen Dienste über die Firewall zu ermöglichen.

- `--ssh`
- `--telnet`
- `--smtp`
- `--http`
- `--ftp`

`--port=`

Mit dem Format port:protocol können Sie angeben, dass die Ports über die Firewall zugelassen werden. Wenn Sie den IMAP-Zugriff über Ihre Firewall zulassen möchten, geben Sie `imap:tcp` an. Sie können auch numerische Ports ausdrücklich angeben. Um zum Beispiel UDP-Pakete über Port 1234 zuzulassen, geben Sie `1234:udp` an. Wenn Sie mehrere Ports angeben, trennen Sie diese durch Kommata.

`firstboot` (optional)

Legen Sie festm ob der **Setup Agent** beim Booten des Systems starten soll. Wenn aktiviert, muss das `firstboot`-Paket installiert sein. Wird nichts angegeben, ist diese Option standardmäßig deaktiviert.

`--enable`

Der **Setup Agent** wird beim ersten Booten des Systems gestartet.

`--disable`

Der **Setup Agent** wird nicht beim ersten Booten des Systems gestartet.

`--reconfig`

Aktivieren Sie den **Setup Agent**, so dass dieser beim Booten im Rekonfigurationsmodus startet. Dieser Modus aktiviert die Optionen Sprache, Maus, Tastatur, Root-Passwort, Sicherheitslevel, zeitzone und Netzwerkonfiguration zusätzlich zu den anderen Optionen.

`install` (optional)

Weist das System an, ein neues System zu installieren, statt ein vorhandenes System zu aktualisieren. Dies ist der Standardmodus. Zur Installation müssen Sie den Installationstyp aus einem der folgenden Befehle angeben `cdrom`, `harddrive`, `nfs` oder `url` (für ftp oder http Installationen). Der `install` Befehl und die Installationsmethode müssen sich in verschiedenen Zeilen befinden.

`cdrom`

Installation vom ersten CD-ROM-Laufwerks des Systems.

`harddrive`

Installation von einem Red Hat-Installationsverzeichnisbaum auf einem lokalen Laufwerk (VFAT oder ext2).

- `--partition=`

  Partition installieren von (wie z.B. sdb2).

- `--dir=`

  Verzeichnis, das das `RedHat`-Verzeichnis des Installationsverzeichnisbaums enthält.

Beispiel:

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

`nfs`

Installation vom angegebenen NFS-Server.

- `--server`

  Server, von dem aus die Installation vorgenommen werden soll (Rechnername oder IP).

- `--dir=`

  Verzeichnis, das das `RedHat`-Verzeichnis des Installationsverzeichnisbaums enthält.

Beispiel:

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

`url`

Installation von einem Red Hat-Installationsverzeichnisbaum auf einen Remote-Server über FTP oder HTTP.

Beispiel:

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

oder:

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

`interactive` (optional)

Verwendet die Informationen, die in der Kickstart-Datei während der Installation zur Prüfung und Modifizierung der Werte zur Verfügung stehen. In jedem Bildschirm des Installationsprogramms werden die Werte der Kickstart-Datei angezeigt. Sie können die Werte akzeptieren und auf **Weiter** klicken oder die Werte ändern und auf **Weiter** klicken, um fortzufahren. Siehe auch `autostep`.

`keyboard` (obligatorisch)

Zur Angabe des Typs der Systemtastatur. Hier die Liste der verfügbaren Tastaturen auf i386- und Alpha-Rechnern:

```
be-latin1, bg, br-abnt2, cf, cz-lat2, cz-us-qwertz, de,
de-latin1, de-latin1-nodeadkeys, dk, dk-latin1, dvorak, es, et,
fi, fi-latin1, fr, fr-latin0, fr-latin1, fr-pc, fr_CH, fr_CH-latin1,
gr, hu, hu101, is-latin1, it, it-ibm, it2, jp106, la-latin1, mk-utf,
no, no-latin1, pl, pt-latin1, ro_win, ru, ru-cp1251, ru-ms, ru1, ru2,
ru_win, se-latin1, sg, sg-latin1, sk-qwerty, slovene, speakup,
speakup-lt, sv-latin1, sg, sg-latin1, sk-querty, slovene, trq, ua,
uk, us, us-acentos
```

Die Datei `/usr/lib/python2.2/site-packages/rhpl/keyboard_models.py` enthält diese Liste auch und ist Teil des `rhpl` Pakets.

`lang` (obligatorisch)

Gibt die während der Installation zu verwendende Sprache an. Wenn Sie zum Beispiel Englisch als Sprache festlegen möchten, muss die Kickstart-Datei folgende Zeile enthalten:

```
lang en_US
```

Die Datei `/usr/share/redhat-config-language/locale-list` bietet eine Liste gültiger Sprachcodes in der ersten Spalte jeder Zeile und ist Teil des `redhat-config-languages` Pakets.

`langsupport` (obligatorisch)

Stellt die Sprache(n) ein, die auf dem System installiert wird. Dieselben Sprachcodes, die mit `lang` verwendet werden, können auch mit `langsupport` verwendet werden.

Wenn Sie nur eine Sprache installieren möchten, geben Sie diese an. Um zum Beispiel Französisch zu installieren, müssen Sie `fr_FR` verwenden:

```
langsupport fr_FR
```

`--default=`

Wenn Sie Sprachenunterstützung für mehrere Sprachen installieren möchten, müssen Sie eine Standardsprache angeben.

Beispiel für die Installation der Sprachen Englisch und Französisch und die Verwendung von Englisch als Standardsprache:

```
langsupport --default=en_US fr_FR
```

Wenn Sie `--default` mit nur einer Sprache verwenden, werden alle Sprachen installiert und die angegebene Sprache als Standardsprache eingestellt.

`logvol` (optional)

Erstellen eines logischen Laufwerkes für Logical Volume Management (LVM) mit folgender Syntax:

```
logvol <mntpoint> --vgname=<name> --size=<size> --name=<name> <options>
```

Es gibt folgende Optionen:

--noformat

Verwendet ein bestehende Volumen und formatiert dies nicht.

--useexisting

Verwendet ein bestehendes logisches Volumen und formatiert dies neu.

Erstellen Sie zuerst die Partition, dann die logische Datenträgergruppe und anschließend den logischen Datenträger. Beispiel:

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

`mouse` (obligatorisch)

Konfiguriert die Maus für das System, sowohl für den grafischen Modus als auch für den Textmodus. Optionen:

`--device=`

Das Gerät, an dem die Maus angeschlossen ist (z.B. `--device ttyS0`).

`--emulthree`

Wenn das X Window System installiert ist, erkennt es das gleichzeitige Klicken mit der linken und rechten Maustaste als dritte Maustaste. Verwenden Sie diese Option, wenn Sie über eine Maus mit zwei Maustasten verfügen.

Nach den Optionen kann einer der folgenden Maustypen angegeben werden:

`alpsps/2, ascii, asciips/2, atibm, generic, generic3, genericps/2, generic3ps/2, genericwheelps/2, genericusb, generic3usb, genericwheelusb, geniusnm, geniusnmps/2, geniusprops/2, geniusscrollps/2, geniusscrollps/2+, thinking, thinkingps/2, logitech, logitechcc, logibm, logimman, logimmanps/2, logimman+, logimman+ps/2, logimmusb, microsoft, msnew, msintelli, msintellips/2, msintelliusb, msbm, mousesystems, mmseries, mmhittab, sun, none`

Diese Liste kann auch in der Datei `/usr/lib/python2.2/site-packages/rhpl/mouse.py` gefunden werden, die Teil des `rhpl` Pakets ist.

Wenn der Befehl mouse ohne Argumente angegeben oder weggelassen wird, versucht das Installationsprogramm, die Maus automatisch zu erkennen (funktioniert bei den meisten neueren Mäusen).

`network` (optional)

Konfiguriert Netzwerkinformationen für das System. Wenn die Kickstart-Installation keine Netzwerkfunktion erfordert (also keine Installation über NFS, HTTP oder FTP), wird keine Netzwerkfunktionalität für das System konfiguriert. Wenn die Installation Netzwerkfunktionalität erfordert, aber keine Netzwerkinformationen in der Kickstart-Datei zur Verfügung gestellt werden, geht das Red Hat Linux-Installationsprogramm davon aus, dass die Installation über eth0 und eine dynamische IP-Adresse (BOOTP/DHCP) erfolgen soll und konfiguriert das fertig installierte System so, dass die IP-Adresse dynamisch bestimmt wird. Der Befehl `network` konfiguriert die Netzwerkinformationen für Kickstart-Installationen über ein Netzwerk sowie für das installierte System.

`--bootproto`

Eine der folgenden Angaben: `dhcp`, `bootp` oder `static`.

Standard ist `dhcp`. `bootp` und `dhcp` werden gleich behandelt.

Die DHCP-Methode verwendet ein DHCP-Serversystem zur Netzwerkkonfiguration. Wie Sie bereits vermuten, ist die BOOTP-Methode ähnlich, wobei ein BOOTP-Server zur Netz-

werkkonfiguration nötig ist. Mit der folgenden Zeile weisen Sie das System an, die Netzwerkkonfiguration über DHCP zu beziehen:

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

Mit der folgenden Zeile in der Kickstart-Datei weisen Sie den Rechner an, die Netzwerkkonfiguration über BOOTP zu beziehen:

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

Bei der statischen Methode müssen Sie selbst alle erforderlichen Informationen zum Netzwerk in die Kickstart-Datei eintragen. Diese Informationen sind statisch, d.h. sie werden während der Installation und auch nach der Installation verwendet. Die Zeile für das statische Netzwerk ist etwas komplexer, da Sie alle Konfigurationsinformationen in einer Zeile angeben müssen. Sie müssen die IP-Adresse, die Netzmaske, das Gateway und den Name-Server angeben. Beispiel (\ gibt an, dass es sich um eine einzige Zeile handelt):

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

Beachten Sie bitte die folgenden zwei Einschränkungen, die für die statische Methode gelten:

- Alle statischen Informationen zur Netzwerkkonfiguration müssen in *einer* Zeile angegeben werden. Es ist nicht möglich, Zeilen z.B. mit Hilfe eines umgekehrten Schrägstrichs umzubrechen.
- Sie können hier nur einen Name-Server angeben. Im Abschnitt `%post` der Kickstart-Datei (beschrieben in Abschnitt 9.7) können Sie jedoch bei Bedarf weitere Name-Server hinzufügen.

`--device=`

Wird verwendet, um ein spezifisches Ethernet-Gerät für die Installation auszuwählen. Bitte beachten Sie: Der Befehl `--device` wird erst dann wirksam, wenn es sich bei der Kickstart-Datei um eine lokale Datei handelt (z.B. `ks=floppy`), da das Installationsprogramm das Netzwerk für das Auffinden der Kickstart-Datei konfiguriert. Beispiel:

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

`--ip=`

IP-Adresse des zu installierenden Rechners.

`--gateway=`

Standard-Gateway als IP-Adresse.

`--nameserver=`

Primärer Name-Server als IP-Adresse.

`--nodns`

Konfiguriert keine DNS-Server.

`--netmask=`

Netzmaske für das installierte System.

`--hostname=`

Rechnername für das installierte System.

`part` oder `partition` (obligatorisch für Installationen, bei Aktualisierungen ignoriert)

Erstellt auf dem System eine Partition.

Wenn auf dem System auf verschiedenen Partitionen mehrere Red Hat Enterprise Linux-Installationen vorhanden sind, fordert das Installationsprogramm den Benutzer zur Eingabe der Installation auf, die aktualisiert werden soll.

Warnung

Alle erstellten Partitionen werden als Teil des Installationsprozesses formatiert, es sei denn, die Befehle `--noformat` und `--onpart` werden verwendet.

<Mount-Punkt>

Der *<Mount-Punkt>* gibt an, wo die Partition gemountet wird. Die Partitionsvorgaben müssen folgende Form haben:

- `/`*<Pfad>*

  Zum Beispiel `/`, `/usr`, `/home`

- `swap`

  Die Partition wird als Swap-Bereich verwendet.

  Verwenden Sie die Option `--recommended`, um die Größe der Swap-Partition automatisch zu ermitteln:

  ```
  swap --recommended
  ```

  Die Swap-Partition ist mindestens genauso groß wie das System-RAM, und nicht größer als das zweifache System-RAM.

- `raid.`*<id>*

  Die Partition wird für Software-RAID verwendet (siehe `raid`).

- `pv.`*<id>*

  Die Partition wird für LVM verwendet (siehe `logvol`).

`--size=`

Die Mindestgröße der Partition in Megabytes. Geben Sie einen ganzen Wert an, beispielsweise 500, und lassen Sie dabei die Angabe in MB weg.

`--grow`

Weist die Partition an, sich an den verfügbaren Platz (falls vorhanden) anzupassen oder die maximale Größe anzunehmen.

`--maxsize=`

Richtet die maximale Partitionsgröße in MB ein, wenn die Partition angewiesen wurde, ihre Größe anzupassen. Geben Sie einen ganzen Wert an und lassen Sie dabei die Angabe in MB weg.

`--noformat`

Weist das Installationsprogramm an, die Partition nicht zu formatieren, damit sie für die Verwendung mit dem Befehl `--onpart` zur Verfügung steht.

`--onpart=` oder `--usepart=`

Weist das Installationsprogramm an, die Partition auf dem *bereits vorhandenen* Gerät anzulegen. Beispiel:

```
partition /home --onpart=hda1
```

legt `/home` auf Gerät `/dev/hda1` an, das bereits vorhanden sein muss.

`--ondisk=` oder `--ondrive=`

Erzwingt die Erstellung der Partition auf einem bestimmten Laufwerk. `--ondisk=sdb` legt die Partition zum Beispiel auf die zweite SCSI-Platte des Systems.

`--asprimary`

Erzwingt die automatische Zuweisung der Partition als primäre Partition oder die Partitionierung schlägt fehl.

`--type=` (durch `fstype` ersetzt)

Diese Option steht nicht länger zur Verfügung. Verwenden Sie `fstype`.

`--fstype=`

Stellt den Dateisystem-Typ für die Partition ein. Gültige Werte sind `ext2`, `ext3`, `swap` und `vfat`.

`--start=`

Gibt den Start-Zylinder für die Partition an. Setzt voraus, dass ein Laufwerk mit `--ondisk=` oder `ondrive=` festgelegt wurde, die End-Zylinder mit `--end=` oder die Partitionsgröße mit `--size=` festgelegt wurde.

`--end=`

Legt den End-Zylinder für die Partition fest. Setzt voraus, dass der Start-Zylinder mit `--start=` festgelegt wurden.

Anmerkung

Falls die Partitionierung aus irgendeinem Grund nicht vorgenommen werden kann, werden auf der 3. virtuellen Konsole Diagnosemeldungen angezeigt.

`raid` (optional)

Erstellt ein Software-RAID-Gerät. Dieser Befehl sieht folgendermaßen aus:

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

<Mount-Punkt>

Speicherstelle, an der das RAID-Dateisystem gemountet wird. Bei `/`muss RAID Level 1 verwendet werden, es sei denn, es ist eine Boot-Partition vorhanden (`/boot`). In diesem Fall muss die `/boot`-Partition vom Typ Level 1 sein. Für den Typ der Root-Partition (`/`kann dann jeder der verfügbaren Typen verwendet werden. *<Partitionen*>* (* deutet an, dass mehrere Partitionen aufgeführt werden können) gibt die RAID-Bezeichnungen an, die zum RAID-Array hinzugefügt werden sollen.

`--level=`

Zu verwendender RAID-Level (0, 1 oder 5).

`--device=`

Bezeichnung des zu verwendenden RAID-Gerätes (z.B. md0 oder md1). Für RAID-Geräte können die Bezeichnungen md0 bis md7 (und jede nur einmal) verwendet werden.

`--spares=`

Legt fest, wie viele Spare-Laufwerke für das RAID-Array verwendet werden sollen. Spare-Laufwerke werden verwendet, um das Array neu zu erstellen, falls ein Laufwerk ausfällt.

`--fstype=`

Legt den Dateisystemtyp für das RAID-Array fest. Gültige Werte sind ext2, ext3, swap und vfat.

`--noformat`

Verwendet ein bestehendes RAID-Array und formatiert dieses nicht.

`--useexisting`

Verwendet ein bestehendes RAID Array und formatiert dieses.

Im Folgenden sehen Sie ein Beispiel dafür, wie eine Partition vom Typ RAID Level 1 für `/` und eine Partition vom Typ RAID Level 5 für `/usr` erstellt wird. In diesem Beispiel wird davon ausgegangen, dass im System drei SCSI-Platten vorhanden sind. Es werden außerdem drei Swap-Partitionen erstellt, auf jedem Laufwerk eine.

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

`reboot` (optional)

Neustart nach abgeschlossener Installation (keine Argumente). Normalerweise zeigt Kickstart eine Meldung an und wartet darauf, dass der Benutzer zum Neustart eine Taste betätigt.

`rootpw` (obligatorisch)

Stellt das Root-Passwort des Systems als <*Passwort*>-Argument ein.

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

`--iscrypted`

Wenn diese Angabe vorhanden ist, wird davon ausgegangen, dass das Passwort-Argument bereits verschlüsselt ist.

`skipx` (optional)

Wenn diese Angabe vorhanden ist, wird auf dem installierten System X nicht konfiguriert.

`text` (optional)

Führt die Kickstart-Installation im Text-Modus aus. Standardmäßig wird der Grafikmodus ausgeführt.

`timezone` (obligatorisch)

Die System-Zeitzone wird auf <*Zeitzone*> eingestellt. Es kann jede der in `timeconfig` aufgeführten Zeitzonen angegeben werden.

`timezone [--utc] <timezone>`

`--utc`

Wenn diese Angabe vorhanden ist, geht das System davon aus, dass die Hardware-Uhr auf UTC (Greenwich Mean)-Zeit eingestellt ist.

`upgrade` (optional)

Weist das System an, ein vorhandenes System zu aktualisieren, statt ein neues System zu installieren. Sie müssen ein Element von CD-ROM, Laufwerk, nfs oder url (für ftp und http) als Speicherstelle für den Installationsbaum angeben.

`xconfig` (optional)

Konfiguriert das X Window System. Wenn diese Option nicht angegeben wird, muss X während der Installation vom Benutzer manuell konfiguriert werden, falls X zuvor installiert wurde. Diese Option sollte nur verwendet werden, wenn X auf dem Endsystem installiert ist.

`--noprobe`

Keine Monitor-Erkennung.

`--card=`

Verwendet die angegebene Karte. Der Kartenname muss in der Kartenliste in `/usr/share/hwdata/Cards` im Paket `hwdata` enthalten sein. Die Liste der Karten finden Sie auch im **X Configuration** Bildschirm **Kickstart Configurator**. Wenn dieses Argument nicht angegeben wird, sucht das Installationsprogramm den PCI-Bus nach der Karte ab. Da AGP ein Teil des PCI-Busses ist, werden AGP- Karten erkannt, wenn sie unterstützt werden. Die Suchreihenfolge ist durch die PCI-Scanreihenfolge des Motherboards festgelegt.

`--videoram=`

Bestimmt die Größe des Grafik-RAM der Grafikkarte.

`--monitor=`

Verwendet den angegebenen Monitor. Der Monitorname muss in der Monitorliste in `/usr/share/hwdata/MonitorsDB` im Paket `hwdata` enthalten sein. Die Liste der Monitore finden Sie auch im **X Configuration** Bildschirm des **Kickstart Configurator**. Diese Angabe wird ignoriert, wenn `--hsync` oder `--vsync` angegeben ist. Wenn keine Monitorinformationen angegeben sind, wird die Monitorerkennung automatisch durchgeführt.

`--hsync=`

Gibt die horizontale Bildwiederholrate des Monitors an.

`--vsync=`

Gibt die vertikale Bildwiederholrate des Monitors an.

`--defaultdesktop=`

Stellt als Standard-Desktop entweder GNOME oder KDE ein (und geht davon aus, dass GNOME und/oder KDE Desktopumgebungen durch `%packages` installiert wurden).

`--startxonboot`

Verwendung eines grafischen Dialogfelds für die Anmeldung an das installierte System.

`--resolution=`

Legt die standardmäßige Auflösung für das X Window System fest. Gültige Werte sind 640x480, 800x600, 1024x768, 1152x864, 1280x1024, 1400x1050, 1600x1200. Stellen Sie sicher, dass die Auflösung mit Ihrer Grafikkarte und Ihrem Bildschirm kompatibel ist.

`--depth=`

Legt die Farbtiefe für das X Window System auf dem installierten System fest. Gültige Werte sind 8, 16, 24 und 32. Stellen Sie sicher, dass die Farbtiefe mit Ihrer Grafikkarte und Ihrem Bildschirm kompatibel ist.

`volgroup` (optional)

Zum Erstellen einer LVM-Gruppe (Logical Volume Management) mit folgender Syntax:
`volgroup <name> <partition> <options>`

Es gibt folgende Optionen:

--noformat

Verwendet eine bestehende Volumengruppe und formatiert diese nicht.

--useexisting

Verwendet eine bestehende Volumengruppe und formatiert diese.

Erstellen Sie zuerst die Partition, dann die logische Datenträgergruppe und anschließend den logischen Datenträger. Beispiel:

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

`zerombr` (optional)

Wenn `zerombr` angegeben wird und `yes` das einzige Argument ist, werden alle auf den Festplatten gefundenen ungültigen Partitionstabellen initialisiert. Dadurch wird der gesamte Inhalt der Festplatten mit ungültigen Partitionstabellen gelöscht. Dieser Befehl sollte in folgendem Format vorliegen:

```
zerombr yes
```

Es ist kein anderes Format möglich.

`%include`

Verwenden Sie den Befehl `%include /path/to/file`, um den Inhalt einer anderen Datei in die Kickstart-Datei mit aufzunehmen, als wenn sich der Inhalt an der Speicherstelle des Befehls `%include` in der Kickstart-Datei befände.

9.5. Paketauswahl

Der Befehl `%packages` steht am Beginn eines Kickstart-Dateiabschnitts, in dem die zu installierenden Pakete aufgeführt sind (nur für Installationen, die Paketauswahl bei Aktualisierungen wird nicht unterstützt).

Pakete können per Gruppe oder per Paketnamen bestimmt werden. Das Installationsprogramm definiert verschiedene Gruppen, die verwandte Pakete enthalten. Siehe die `RedHat/base/comps.xml` Datei auf der ersten Red Hat Enterprise Linux CD-ROM für eine Liste dieser Gruppen. Jede Gruppe besitzt eine ID, einen für den Benutzer sichtbaren Wert, einen Namen, eine Beschreibung und eine Paketliste. In der Paketliste werden die als obligatorisch gekennzeichneten Pakete immer installiert, wenn die Gruppe gewählt wird. Die als Standard gekennzeichneten Pakete werden standardmäßig gewählt, wenn die Gruppe gewählt wird. Die als optional gekennzeichneten Pakete müssen separat ausgewählt werden, selbst wenn die Gruppe zur Installation gewählt ist.

Normalerweise reicht es aus, wenn Sie nur die gewünschten Gruppen und nicht die einzelnen Pakete angeben. Bitte beachten Sie, dass standardmäßig immer die `Core` und `Base`-Gruppen ausgewählt werden. Es ist daher nicht notwendig, sie im Abschnitt `%packages` anzugeben.

Hier ein Beispiel für eine `%packages`- -Auswahl:

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

Wie das Beispiel zeigt, werden die Gruppen zeilenweise angegeben, angefangen mit dem Symbol `@` gefolgt von einem Leerzeichen und dem vollständigen Namen der Gruppe, wie in der Datei `comps.xml`angegeben. Gruppen können auch mit durch die Gruppen-ID wie z.B. `gnome-desktop` angegeben werden. Geben Sie einzelne Pakete ohne zusätzliche Zeichen an (im obigen Beispiel steht die Zeile `dhcp` für ein einzelnes Paket).

In der Standardpaketliste können Sie auch angeben, welche Pakete nicht installiert werden sollen:

```
-autofs
```

Es gibt folgende Optionen für die `%packages` Option:

`--resolvedeps`

Installieren der aufgeführten Pakete und automatisches Lösen von Paketabhängigkeiten. Wird diese Option nicht angegeben und es liegen Paketabhängigkeiten vor, hält die automatische Installation an und fordert en Benutzer zur Eingabe auf. Beispiel:

```
%packages --resolvedeps
```

`--ignoredeps`

Ignoriert ungelöste Abhängigkeiten und installiert die aufgelisteten Pakete ohne die Abhängigkeiten. Beispiel:

```
%packages --ignoredeps
```

`--ignoremissing`

Ignoriert die fehlenden Pakete und Gruppen anstelle die Installation anzuhalten und nachzufragen, ob die Installation abgebrochen oder weitergeführt werden soll. Beispiel:

```
%packages --ignoremissing
```

9.6. Pre-Installations-Skript

Sie können Befehle hinzufügen, die direkt nach der Analyse von `ks.cfg` im System ausgeführt werden. Dieser Abschnitt muss sich am Ende der Kickstart-Datei befinden (nach den Befehlen) und mit dem Befehl `%pre` beginnen. Im Abschnitt `%pre` können Sie auf das Netzwerk zugreifen. Allerdings wurde *Name-Service* bisher noch nicht konfiguriert, so dass nur IP-Adressen funktionieren.

Anmerkung

Das Pre-Installations-Skript wird nicht in der chroot-Umgebung ausgeführt.

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

Ermöglicht es Ihnen, eine andere Skript-Sprache anzugeben wie z.B. Python. Ersetzen Sie *`/usr/bin/python`* durch die Skript-Sprache Ihrer Wahl.

9.6.1. Beispiel

Hier ein Beispiel für ein `%pre`:

```
%pre

#!/bin/sh

hds=""
mymedia=""

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

set $hds
numhd=`echo $#`

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

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

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

```
  echo "part / --fstype ext3 --size 2048" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 2048 --grow" >> /tmp/part-include
fi
```

Dieses Skript bestimmt die Anzahl der Laufwerke im System und schreibt eine Textdatei mit einem unterschiedlichen Partitionsschema je nachdem, ob es ein oder zwei Laufwerke besitzt. Statt eine Reihe von Partitionsbefehlen in der Kickstart-Datei zu haben, nehmen Sie folgende Zeile mit auf:

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

Die im Skript gewählten Partitionsbefehle werden verwendet.

9.7. Post-Installations-Skript

Sie können Befehle hinzufügen, die nach der abgeschlossenen Installation auf dem System ausgeführt werden. Dieser Abschnitt muss sich am Ende der Kickstart-Datei befinden und mit dem Befehl `%post` beginnen. Der Abschnitt ist für Funktionen wie das Installieren zusätzlicher Software oder das Konfigurieren eines weiteren Name-Servers hilfreich.

Anmerkung

Wenn Sie das Netzwerk einschließlich eines Name-Servers mit statischen IP-Informationen konfigurieren, können Sie auf das Netzwerk zugreifen und IP-Adressen in der `%post`-Sektion auflösen. Wenn Sie das Netzwerk für DHCP konfigurieren, ist die Datei `/etc/resolv.conf` nicht komplett, wenn die Installation die `%post`-Sektion ausführt. Sie haben Zugriff auf das Netzwerk, können aber keine IP-Adressen auflösen. Deshalb müssen Sie IP-Adressen in der `%post`-Sektion benutzen, wenn Sie DHCP verwenden.

Anmerkung

Das nach der Installation ausgeführte Skript wird in einer chroot-Umgebung ausgeführt. Daher ist zum Beispiel das Kopieren von Skripten oder RPMs vom Installationsmedium nicht möglich.

`--nochroot`

Damit können Befehle angegeben werden, die außerhalb der chroot-Umgebung ausgeführt werden sollen.

Im folgenden Beispiel wird die Datei `/etc/resolv.conf` in das gerade erstellte Dateisystem kopiert.

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

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

Ermöglicht es Ihnen, eine andere Skript-Sprache anzugeben wie z.B. Python. Ersetzen Sie *`/usr/bin/python`* durch die Skript-Sprache Ihrer Wahl.

9.7.1. Beispiele

Aktivieren und Deaktivieren von Diensten:

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

Das Skript `runme` von einem NFS-Share ausführen:

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

Dem System einen neuen Benutzer hinzufügen:

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

9.8. Kickstart-Datei zur Verfügung stellen

Eine Kickstart-Datei muss an einem der beiden Speicherstellen abgelegt werden:

- Auf einer Bootdiskette
- Auf einer bootfähigen CD-ROM
- Auf einem Netzwerk

In der Regel werden die Kickstart-Dateien auf die Bootdiskette kopiert oder im Netzwerk zur Verfügung gestellt. Der netzwerkbasierte Ansatz wird in der Regel verwendet, da die meisten Kickstart-Installationen auf Netzwerkcomputern durchgeführt werden.

Im Folgenden wird die Frage der Speicherstelle der Kickstart-Dateien etwas genauer betrachtet.

9.8.1. Erstellen einer Kickstart-Bootdiskette

Um eine diskettenbasierte Kickstart-Installation durchführen zu können, muss die Kickstart-Datei als `ks.cfg` benannt und zu Beginn des Verzeichnisses der Bootdiskette gespeichert sein. Informationen zum Erstellen von Bootdisketten finden Sie unter *Erstellen einer Installations-Bootdiskette* im *Red Hat Enterprise Linux Installationshandbuch*. Da die Bootdisketten im MS-DOS-Format vorliegen, ist das Kopieren der Kickstart-Datei unter Linux mithilfe des Befehls `mcopy` sehr einfach:

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

Alternativ hierzu können Sie die Datei mit Hilfe von Windows kopieren. Sie können auch die MS-DOS-Bootdiskette in Red Hat Enterprise Linux mit dem Dateisystem vfat mounten und mit dem Befehl `cp` die Datei auf Diskette kopieren.

9.8.2. Erstellen einer Kickstart Boot-CD-ROM

Um eine CD-ROM-basierte Kickstartinstallation durchzuführen, muss die Kickstartdatei `ks.cfg` benannt sein, und sich im obersten Verzeichnis der Boot-CD-ROM befinden. Da die CD-ROM nur lesbar ist, muss die Datei zu dem Verzeichnis hinzugefügt werden, das zum Erstellen des Images auf der CD verwendet wurde. Siehe Abschnitt *Erstellen einer Installations-Boot-CD-ROM* im *Red Hat Enterprise Linux Installationshandbuch* für weitere Informationen zum Erstellen einer bootfähigen CD-ROM. Bevor Sie jedoch die `file.iso` Imagedatei erstellen, kopieren Sie die Datei `ks.cfg` in das `isolinux/` Verzeichnis.

9.8.3. Verfügbarmachen der Kickstart-Datei im Netzwerk

Netzwerkinstallationen mit Hilfe von Kickstart sind recht häufig, da Systemadministratoren die Installation auf vielen, über das Netzwerk verbundenen Computern schnell und problemlos automatisieren können. In der Regel sollten die Administratoren sowohl einen BOOTP/DHCP-Server als auch einen NFS-Server im lokalen Netzwerk zur Verfügung haben. Der BOOTP/DHCP-Server wird verwendet, um dem Client Netzwerkinformationen zu senden, während die während der Installation verwendeten Dateien vom NFS-Server bereitgestellt werden. Diese beiden Server werden häufig auf demselben Rechner ausgeführt. Dies ist allerdings keine Bedingung.

Zum Durchführen einer netzwerkbasierten Kickstart-Installation müssen Sie in Ihrem Netzwerk über einen BOOTP/DHCP-Server verfügen, der Konfigurationsinformationen für den Rechner enthalten muss, auf dem Sie Red Hat Enterprise Linux installieren möchten. Der BOOTP/DCHP-Server stellt dem Client nicht nur Netzwerkinformationen zur Verfügung, sondern auch die Speicherstelle der Kickstart-Datei.

Wenn eine Kickstart-Datei vom BOOTP/DHCP-Server angegeben wird, versucht der Client, den Dateipfad mit NFS zu mounten und kopiert die angegebene Datei auf den Client, wobei er diese als Kickstart-Datei verwendet. Die exakten erforderlichen Einstellungen variieren je nach dem BOOTP/DHCP-Server, den Sie verwenden.

Es folgt ein Beispiel für eine Zeile aus der Datei `dhcpd.conf` für den DHCP-Server:

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

Beachten Sie, dass Sie den Wert nach `filename` durch den Namen der Kickstart-Datei ersetzen müssen (oder dem Verzeichnis, in dem die Kickstart- Datei abgelegt ist) sowie den Wert nach `next-server` durch den NFS-Servernamen.

Wenn der vom BOOTP/DHCP-Server zurückgegebene Dateiname mit einem Schrägstrich ("/") endet, wird er nur als Pfad interpretiert. In diesem Fall mountet der Client diesen Pfad mit NFS und sucht nach einer bestimmten Datei. Der Client sucht nach folgendem Dateinamen:

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

Die Sektion *<IP-Adresse>* des Dateinamens sollte mit der IP-Adresse des Clients in Dezimalangaben mit Punkten ersetzt werden. Beispiel: Der Dateiname für einen Computer mit der IP-Adresse 10.10.0.1 lautete `10.10.0.1-kickstart`.

Beachten Sie, dass der Client bei fehlendem Servernamen versuchen wird, den Server als NFS-Server zu verwenden, der auf die BOOTP/DHCP-Anfrage geantwortet hat. Wenn Sie keinen Pfad oder Dateinamen angeben, versucht der Client, `/kickstart` vom BOOTP/DHCP-Server zu mounten und die Kickstart-Datei mit Hilfe desselben Dateinamens *<IP-Adresse>*`-kickstart` wie oben beschrieben zu finden.

9.9. Den Installationsbaum zur Verfügung stellen

Die Kickstart-Installation muss auf einen *Installationsbaum* zugreifen können. Ein Installationsbaum ist eine Kopie der binären Red Hat Enterprise Linux-CD-ROMs mit derselben Verzeichnisstruktur.

Wenn Sie eine CD-basierte Installation durchführen, legen Sie die Red Hat Enterprise Linux-CD-ROM Nr. 1 vor dem Starten der Kickstart-Installation in den Computer.

Wenn Sie eine Festplatteninstallation durchführen, müssen Sie sicherstellen, dass die ISO-Images der binären Red Hat Enterprise Linux-CD-ROMs auf einer Festplatte vorhanden sind.

Wenn Sie eine netzwerkbasierte Installation (NFS, FTP oder HTTP) durchführen, müssen Sie den Installationsbaum über das Netzwerk zur Verfügung stellen. Weitere Informationen finden Sie im Abschnitt *Netzwerkinstallation vorbereiten* im *Red Hat Enterprise Linux Installationshandbuch*.

9.10. Starten einer Kickstart-Installation

Um eine Kickstart-Installation zu beginnen, müssen Sie das System von einer Red Hat Enterprise Linux-Bootdiskette oder der Red Hat Enterprise Linux CD-ROM oder der Red Hat Enterprise Linux CD-ROM 1 booten und einen speziellen Bootbefehl am Bootprompt eingeben. Das Installationsprogramm sucht nach einer Kickstartdatei, wenn das `ks` Befehlszeilenargument an den Kernel weitergegeben wird.

Boot Diskette

Wenn sich die Kickstartdatei auf einer Bootdiskette wie unter Abschnitt 9.8.1 beschrieben befindet, booten Sie das System mit der Diskette und geben Sie folgenden Befehl am `boot:`-Prompt ein:

```
linux ks=floppy
```

CD-ROM #1 und Diskette

Der Befehl **`linux ks=floppy`** funktioniert auch, wenn die `ks.cfg` Datei sich auf einem vfat oder ext2 Dateisystem auf einer Diskette befindet, und Sie von der Red Hat Enterprise Linux CD-ROM #1 booten.

Alternativ dazu können Sie von der Red Hat Enterprise Linux CD-ROM #1 booten und die Kickstartdatei auf einem vfat oder ext2 Dateisystem gespeichert haben. Geben Sie hierzu folgendes am `boot:` Prompt ein:

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

Mit Treiberdiskette

Wenn Sie für Kickstart eine Treiberdiskette benötigen, geben Sie die Option **`dd`** an. Um zum Beispiel von einer Bootdiskette zu booten und eine Treiberdiskette zu verwenden, geben Sie den folgenden Befehl am `boot:` Prompt ein:

```
linux ks=floppy dd
```

Boot CD-ROM

Befindet sich die Kickstartdatei auf einer bootfähigen CD-ROM, wie unter Abschnitt 9.8.2 beschrieben, legen Sie die CD-ROM ein, booten Sie das System und geben Sie den folgenden Befehl am `boot:`-Prompt ein (wobei `ks.cfg` der Name der Kickstartdatei ist):

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

Weitere Optionen zum Starten einer Kickstartinstallation:

`ks=nfs:<Server>/<Pfad>`

Das Installationsprogramm sucht nach der Kickstart-Datei auf dem NFS- Server *<Server>* als Datei *<Pfad>*. Das Installationsprogramm verwendet DHCP, um die Ethernetkarte zu konfigurieren. Beispiel: Wenn der NFS-Server server.expample.com heißt und sich die Kickstart-Datei im NFS-Share `/mydir/ks.cfg` befindet, lautet der richtige Bootbefehl `ks=nfs:server.example.com:/mydir/ks.cfg`.

`ks=http:<Server>/<Pfad>`

Das Installationsprogramm sucht nach der Kickstart-Datei auf dem HTTP- Server *<Server>* als Datei *<Pfad>*. Das Installationsprogramm verwendet DHCP, um die Ethernetkarte zu konfigurieren. Beispiel: Wenn der HTTP-Server server.expample.com heißt und sich die Kickstart-Datei im HTTP-Verzeichnis `/mydir/ks.cfg` befindet, lautet der richtige Bootbefehl `ks=http:server.example.com:/mydir/ks.cfg`.

`ks=floppy`

Das Installationsprogramm sucht nach der Datei `ks.cfg` auf einem vfat oder ext2 Dateisystem auf der Diskette im Verzeichnis `/dev/fd0`.

`ks=floppy:/<Pfad>`

Das Installationsprogramm sucht nach der Kickstartdatei auf der Diskette im Verzeichnis `/dev/fd0` als Datei *<Pfad>*.

`ks=hd:<Gerät>:/<Datei>`

Das Installationsprogramm mountet das Dateisystem auf *<Gerät>* (das vfat oder ext2 sein muss) und sucht nach der Kickstart-Konfigurationsdatei als *<Datei>* im Dateisystem (zum Beispiel `ks=hd:sda3:/mydir/ks.cfg`).

`ks=file:/<Datei>`

Das Installationsprogramm versucht, die Datei *<Datei>* vom Dateisystem zu lesen und mountet nichts. Dies wird in der Regel verwendet, wenn sich die Kickstart-Datei bereits im `initrd`-Image befindet.

`ks=cdrom:/<Pfad>`

Das Installationsprogramm sucht nach der Kickstart-Datei auf der CD-ROM als Datei *<Pfad>*.

`ks`

Wenn nur `ks` verwendet wird, konfiguriert das Installationsprogramm die Ethernetkarte im System mit Hilfe von DHCP. Das System verwendet den "bootServer" aus der DHCP-Antwort als NFS-Server, um die Kickstart-Datei zu lesen. Standardmäßig stimmt er mit dem DHCP-Server überein. Der Name der Kickstart-Datei lautet unter anderem folgendermaßen:

- Wenn DHCP angegeben wurde und die Bootdatei mit einem `/` beginnt, wird die von DHCP bereitgestellte Bootdatei auf dem NFS-Server gesucht.
- Wenn DHCP angegeben wurde und die Bootdatei nicht mit einem `/` beginnt, wird nach der von DHCP bereitgestellten Bootdatei im Verzeichnis `/kickstart` auf dem NFS-Server gesucht.
- Wenn DHCP keine Bootdatei angegeben hat, versucht das Installationsprogramm, die Datei `/kickstart/1.2.3.4-kickstart` zu lesen, wobei *1.2.3.4* die numerische IP-Adresse des Rechners ist, auf dem die Installation ausgeführt werden soll.

`ksdevice=<Gerät>`

Das Installationsprogramm verwendet dieses Netzwerkgerät, um eine Verbindung mit dem Netzwerk herzustellen. Um zum Beispiel eine Kickstart-Installation mit der Kickstart-Datei auf einem NFS-Server zu starten, der mit dem System über das eth1-Gerät verbunden ist, müssen Sie den Befehl `ks=nfs:<Server:>/<Pfad> ksdevice=eth1` am `boot:`-Prompt verwenden.

Kapitel 10.

Kickstart Configurator

Mit **Kickstart Configurator** können Sie unter Verwendung einer grafischen Benutzeroberfläche eine Kickstart-Datei erstellen, so dass Sie sich nicht an die korrekte Syntax der Datei erinnern müssen.

Um **Kickstart Configurator** zu verwenden, müssen Sie das X Window System ausführen. Starten Sie den **Kickstart Configurator** durch Auswahl von **Hauptmenü** (im Panel) => **Systemtools** => **Kickstart** oder geben Sie den Befehl `/usr/sbin/redhat-config-kickstart` ein.

Beim Erstellen einer Kickstart-Datei können Sie jederzeit **Datei** => **Vorschau** wählen, um Ihre aktuelle Auswahl vorab anzusehen.

Um eine bestehende Kickstart-Datei zu verwenden, klicken Sie auf**Datei** => **Öffnen**, und wählen Sie die bestehende Datei aus.

10.1. Basiskonfiguration

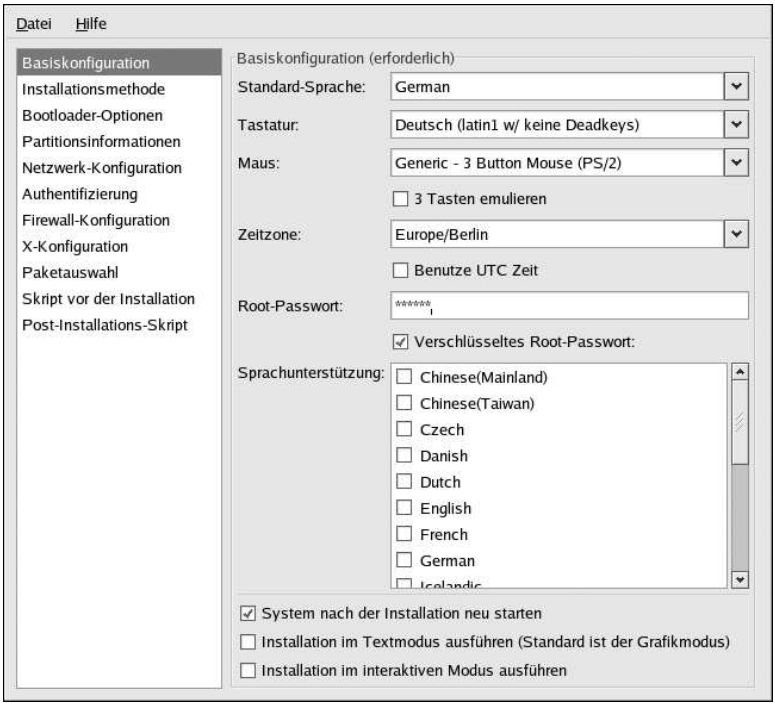

Abbildung 10-1. Basiskonfiguration

Wählen Sie aus dem Menü **Sprache** die Sprache aus, die während der Installation und als Standardsprache nach der Installation verwendet werden soll.

Wählen Sie im Menü **Tastatur** den Tastaturtyp des Systems aus.

Wählen Sie im Menü **Maus** die Maus für Ihr System aus. Wenn Sie **Keine Maus** auswählen, wird keine Maus konfiguriert. Wenn Sie **Maus erkennen** auswählen, versucht das Installationsprogramm, die Maus automatisch zu erkennen. Dies funktioniert für die meisten neueren Mäuse.

Wenn Sie eine Zwei-Tasten-Maus haben, können Sie eine Drei-Tasten-Maus emulieren, indem Sie **3 Tasten emulieren** auswählen. Wenn diese Option ausgewählt ist, können Sie durch gleichzeitiges Drücken beider Maustasten die mittlere Maustaste ersetzen.

Im Menü **Zeitzone** wählen Sie die Zeitzone für Ihr System aus. Um das System auf UTC zu konfigurieren, wählen Sie **UTC-Zeit verwenden**.

Geben Sie ein Root-Passwort für das System in das Textfeld **Root Passwort** ein. Geben Sie das gleiche Passwort in das Textfeld **Passwort bestätigen** ein. Dieses Textfeld dient dazu, sicherzustellen, dass Sie keine Schreibfehler beim Passwort gemacht haben und dann das richtige Passwort nach Beendigung der Installation nicht mehr eingeben können. Wenn Sie das Passwort verschlüsselt in der Datei speichern möchten, aktivieren Sie das Kontrollkästchen **Root-Passwort verschlüsseln**. Beim Speichern der Datei wird das im Klartext eingegebene Passwort verschlüsselt und in die Kickstart-Datei geschrieben. Verwenden Sie kein bereits verschlüsseltes Passwort, um es zu verschlüsseln. Da eine Kickstart-Datei im Nur-Text erstellt wird, die leicht gelesen werden kann, wird empfohlen, ein verschlüsseltes Passwort zu verwenden.

Um zusätzlich zu der aus dem Pull-Down-Menü **Sprache** ausgewählten Sprache weitere zu installieren, markieren Sie diese in der Liste **Sprachsupport**. Die aus dem Pull-Down-Menü **Sprache** ausgewählte Sprache wird nach der Installation als Standard verwendet. Diese kann jedoch mit dem **Language Configuration Tool** (`redhat-config-language`) nach der Installation geändert werden.

Wenn Sie **System nach der Installation neu starten** auswählen, wird Ihr System automatisch neu gebootet, nachdem die Installation abgeschlossen ist.

Kickstart-Installationen werden standardmäßig im grafischen Modus durchgeführt. Wenn Sie diese Standardeinstellung ändern und stattdessen den Textmodus verwenden möchten, markieren Sie das Kontrollkästchen **Installation im Textmodus ausführen**.

Sie können die Kickstart-Installation im interaktiven Modus ausführen. Das bedeutet, dass das Installationsprogramm alle in der Kickstart-Datei vorkonfigurierten Optionen verwendet. Allerdings können Sie die Optionen jedes Bildschirms als Vorschau anzeigen, bevor Sie zum nächsten Bildschirm gelangen. Um zum nächsten Bildschirm zu gelangen, klicken Sie auf den Button **Weiter**, nachdem Sie die Einstellungen angenommen haben. Wenn Sie die vorkonfigurierten Optionen nicht übernehmen möchten, können Sie diese ändern, ehe Sie mit der Installation fortfahren. Wenn Sie diesen Installationstyp verwenden möchten, markieren Sie das Kontrollkästchen **Installation im interaktiven Modus ausführen**.

10.2. Installationsmethode

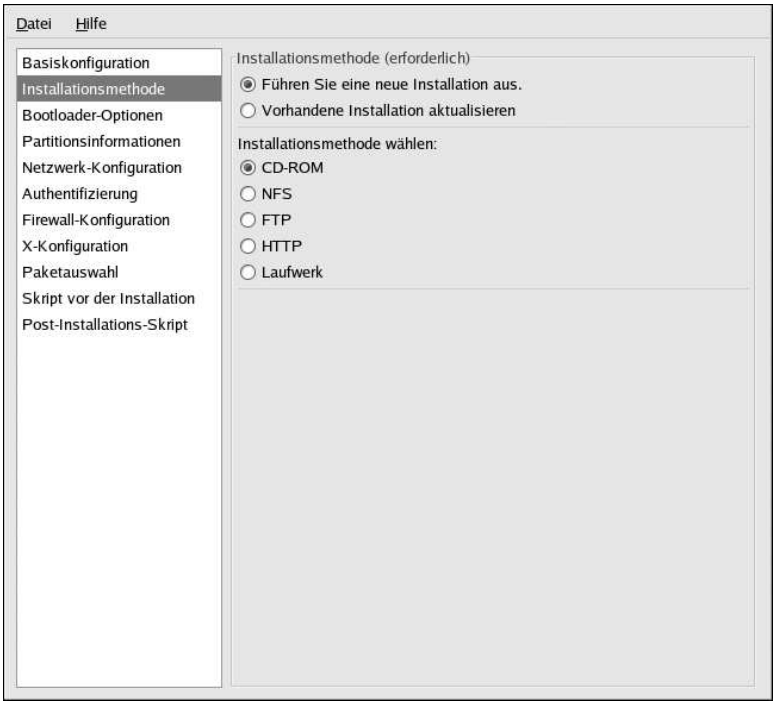

Abbildung 10-2. Installationsmethode

In **Installationsmethode** können Sie wählen, ob Sie eine vollständige Installation oder eine Aktualisierung durchführen möchten. Wenn Sie sich für eine Aktualisierung entscheiden, werden die Optionen **Partitionsinformationen** und **Paketauswahl** deaktiviert. Diese werden für Kickstart-Aktualisierungen nicht unterstützt.

Wählen Sie auf diesem Schirm auch den Typ der Kickstart-Installation oder das Upgrade, dasSie durchführen möchten. Sie können aus folgenden Optionen wählen:

- **CD-ROM** — Wählen Sie diese Option, wenn Sie von den Red Hat Enterprise Linux CD-ROMs installieren möchten.
- **NFS** — Wählen Sie diese Option, wenn Sie von einem NFS-Share-Verzeichnis installieren oder aktualisieren möchten. Geben Sie in das Textfeld für den NFS Server einen vollständigen Domain-Namen oder eine IP-Adresse ein. Geben Sie für das NFS-Verzeichnis den Namen des NFS-Verzeichnisses an, das das `RedHat`-Verzeichnis des Installaitonsbaums enthält. Wenn z.B. der NFS Server das Verzeichnis `/mirrors/redhat/i386/RedHat/` enthält, geben Sie `/mirrors/redhat/i386/` für das NFS-Verzeichnis an.
- **FTP** — Wählen Sie diese Option, wenn Sie von einem FTP-Server installieren oder aktualisieren möchten. Geben Sie im Textfeld für den FTP Server einen Domain-Namen oder IP-Adresse an. Geben Sie für das FTP-Verzeichnis den Namen des FTP-Verzeichnisses ein, das das `RedHat`-Verzeichnis enthält. Wenn Ihr FTP-Server zum Beispiel das Verzeichnis

`/mirrors/redhat/i386/RedHat/` enthält, geben Sie `/mirrors/redhat/i386/` für das FTP-Verzeichnis ein. Wenn der FTP-Server einen Benutzernamen und ein Passwort benötigt, geben Sie diese ebenfalls ein.

- **HTTP** — Wählen Sie diese Option, wenn Sie von einem HTTP-Server installieren oder aktualisieren möchten. Im Textfeld für den HTTP-Server geben Sie einen Domain-Namen oder eine IP-Adresse an. Geben Sie für das HTTP-Verzeichnis den Namen des HTTP-Verzeichnisses ein, das das `RedHat` -Verzeichnis enthält. Wenn Ihr HTTP-Server zum Beispiel das Verzeichnis `/mirrors/redhat/i386/RedHat/` enthält, geben Sie `/mirrors/redhat/i386/` für das HTTP-Verzeichnis ein.
- **Laufwerk** — Wählen Sie diese Option, wenn Sie von einer Festplatte installieren oder aktualisieren möchten. Eine Installation von einer Festplatte erfordert die Verwendung von ISO-(oder CD-ROM-) Images. Stellen Sie sicher, dass die ISO-Images intakt sind, bevor Sie die Installation starten. Verwenden Sie dazu ein `md5sum` Programm sowie die `linux mediacheck` Bootoption wie im *Red Hat Enterprise Linux Installationshandbuch* beschrieben. Geben Sie die Festplatten-Partition, die die ISO-Images enthält (zum Beispiel `/dev/hda1`) in das Textfeld **Festplattenpartition** ein. Geben Sie das Verzeichnis, das die ISO-Images enthält, in das Textfeld **Festplattenverzeichnis** ein.

10.3. Bootloaderoptionen

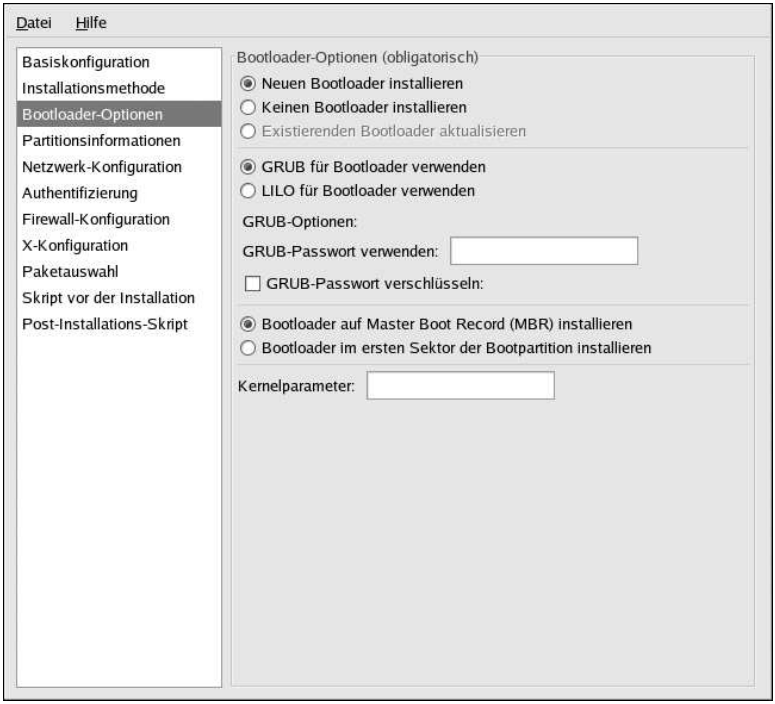

Abbildung 10-3. Bootloaderoptionen

Sie können entweder GRUB oder LILO als Bootloader installieren. Wenn Sie keinen Bootloader installieren möchten, wählen Sie **Keinen Bootloader installieren**. Wenn Sie keinen Bootloader installieren, stellen Sie sicher, dass Sie eine Bootdiskette erstellen oder Ihr System auf eine andere Weise booten können (z.B. mit einem fremden Bootloader).

Wenn Sie einen Bootloader installieren möchten, müssen Sie sich für einen der beiden (GRUB oder LILO) entscheiden und festlegen, wo dieser Bootloader installiert werden soll (im Master Boot Record oder im ersten Sektor der `/boot`-Partition). Installieren Sie den Bootloader im MBR, wenn Sie ihn als Bootloader verwenden möchten. Wenn Sie einen anderen Bootloader verwenden, installieren Sie LILO oder GRUB im ersten Sektor der `/boot`-Partition und konfigurieren Sie den anderen Bootloader, um Red Hat Enterprise Linux zu booten.

Wenn Sie einige spezielle Parameter an den Kernel übergeben müssen, die verwendet werden, wenn das System bootet, geben Sie diese in das Textfeld **Kernelparameter** ein. Wenn Sie zum Beispiel einen IDE-CD-ROM-Brenner haben, können Sie den Kernel anweisen, den SCSI-Emulationstreiber zu verwenden, der geladen sein muss, bevor `cdrecord` verwendet wird. Geben Sie dazu **`hdd=ide-scsi`** als Kernelparameter ein (wobei **`hdd`** das CD-ROM-Gerät ist).

Wenn Sie GRUB als Bootloader verwenden, können Sie diesen mit einem Passwort schützen, indem Sie ein GRUB-Passwort konfigurieren. Wählen Sie **GRUB-Passwort verwenden** und geben Sie das Passwort in das **Password**-Feld ein. Geben Sie das gleiche Passwort nochmal im Feld **Passwort bestätigen** ein. Wenn Sie das Passwort verschlüsselt in der Datei speichern möchten, aktivieren Sie die Option **GRUB-Passwort verschlüsseln**. Beim Speichern der Datei wird das im Nur-Text eingegebene Passwort verschlüsselt und in die Kickstart-Datei geschrieben. Verwenden Sie kein bereits verschlüsseltes Passwort, um es zu verschlüsseln.

Wenn Sie LILO als Bootloader verwenden, wählen Sie, ob Sie den linearen Modus verwenden und ob Sie die Verwendung des lba32-Modus erzwingen möchten.

Wenn Sie **Vorhandene Installation aktualisieren** auf der Seite **Installationsmethode** ausgewählt haben, wählen Sie **Existierenden Bootloader aktualisieren** um die vorhandene Bootloaderkonfiguration zu aktualisieren und dabei die alten Einträge zu erhalten.

10.4. Partitionsinformationen

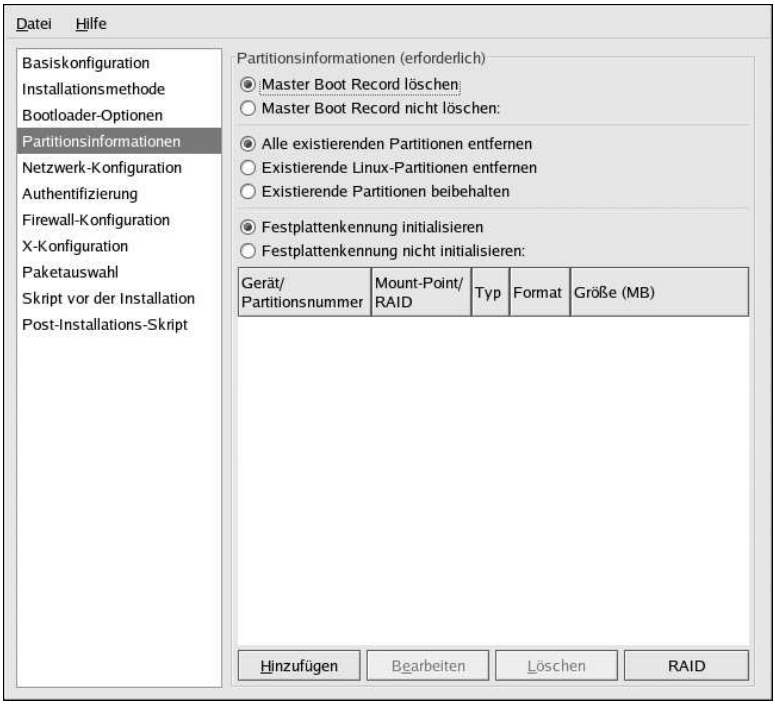

Abbildung 10-4. Partitionsinformationen

Wählen Sie, ob Sie den Master Boot Record (MBR) löschen möchten oder nicht. Sie können auch alle vorhandenen Partitionen löschen, alle vorhandenen Linux-Partitionen löschen oder alle vorhandenen Partitionen behalten.

Sie können die Plattenkennung mit dem Standard für die Architektur des Systems initialisieren (z.B. `msdos` für x86 und `gpt` für Itanium). Wählen Sie **Festplattenkennung initialisieren**, wenn Sie auf einer völlig neuen Festplatte installieren.

10.4.1. Erstellen von Partitionen

Um eine Partition zu erstellen, klicken Sie auf den Button **Hinzufügen**. Das Fenster **Partitionsoptionen** wie in Abbildung 10-5 abgebildet, erscheint. Wählen Sie den Mount-Punkt, den Dateisystemtyp und die Partitionsgröße für die neue Partition. Sie haben außerdem folgende Optionen:

- Wählen Sie in **Zusätzliche Größenoptionen**, ob die Größe der Partition auf eine feste Größe oder bis zur gewählten Größe eingestellt bzw. der verbleibende Platz auf der Festplatte ausgefüllt werden soll. Haben Sie Swap als Dateisystemtyp ausgewählt, können Sie entscheiden, ob das Installationsprogramm die Swap-Partition mit der empfohlenen Größe erstellen soll statt eine Größe anzugeben.
- Erzwingt, dass die Partition als primäre Partition erstellt wird.

- Erstellt die Partition auf einer bestimmten Festplatte. Beispiel: Geben Sie zum Erstellen der Partition auf der ersten IDE-Festplatte (`/dev/hda`) **`hda`** als Laufwerk an. Nehmen Sie `/dev` nicht in den Laufwerknamen auf.
- Verwendet eine vorhandene Partition. Beispiel: Geben Sie zum Erstellen der Partition auf der ersten IDE-Festplatte (`/dev/hda1`) **`hda1`** als Partition an. Nehmen Sie `/dev` nicht in den Partitionsnamen auf.
- Formatiert die Partition als den gewählten Dateisystemtyp.

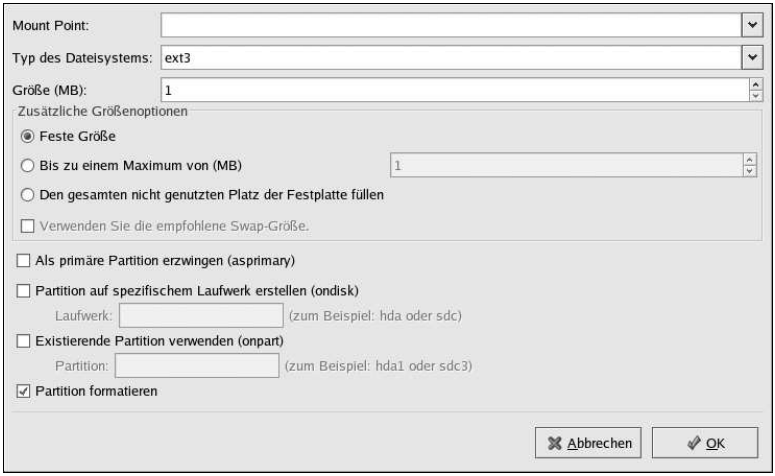

Abbildung 10-5. Erstellen von Partitionen

Um eine vorhandene Partition zu bearbeiten, wählen Sie eine Partition aus der Liste und klicken Sie auf den Button **Bearbeiten**. Es wird dasselbe Fenster **Partitionsoptionen** wie beim Hinzufügen einer Partition angezeigt, siehe Abbildung 10-5, mit dem Unterschied, dass es die Werte für die ausgewählte Partition enthält. Modifizieren Sie die Partitionsoptionen und klicken Sie auf **OK**.

Um eine vorhandene Partition zu löschen, wählen Sie die Partition aus der Liste, und klicken Sie auf den Button **Löschen**.

10.4.1.1. Erstellen von Software-RAID-Partitionen

Lesen Sie Kapitel 3, um mehr über RAID und die unterschiedlichen RAID-Levels zu erfahren. RAID 0, 1 und 5 können konfiguriert werden.

Gehen Sie beim Erstellen einer Software-RAID-Partition wie folgt vor:

1. Klicken Sie auf den Button **RAID**.
2. Wählen Sie **Erstellen einer Software-RAID-Partition**.
3. Konfigurieren Sie die Partitionen wie zuvor beschrieben, wählen Sie jedoch **Software RAID** als Dateisystemtyp. Sie müssen außerdem ein Laufwerk angeben, auf dem die Partition angelegt bzw. welche vorhandene Partition verwendet werden soll.

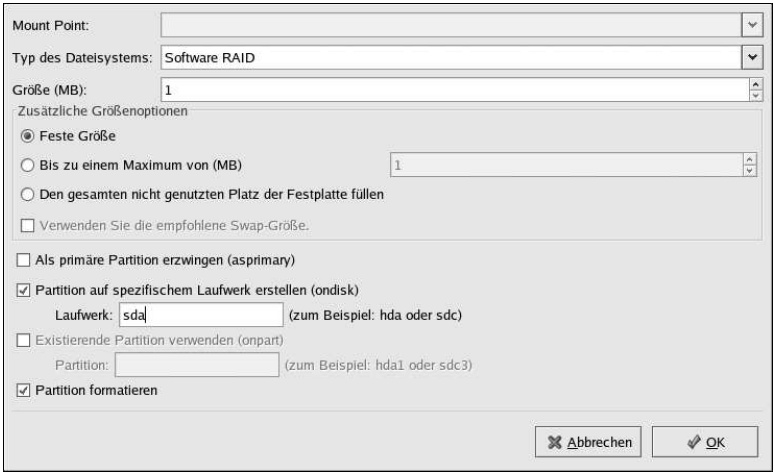

Abbildung 10-6. Erstellen einer Software-RAID-Partition

Wiederholen Sie diese Schritte, um so viele Partitionen zu erstellen, wie Sie für Ihr RAID-Setup benötigen. Nicht alle Ihre Partitionen müssen RAID-Partitionen sein.

Nachdem Sie alle Partitionen erstellt haben, die zur Erstellung eines RAID-Gerätes nötig waren, gehen Sie wie folgt vor:

1. Klicken Sie auf den Button **RAID**.
2. Wählen Sie **Erstellen eines RAID-Gerätes**.
3. Wählen Sie einen Mount-Punkt, ein Dateisystemtyp, einen RAID-Gerätenamen eine RAID-Level, RAID-Member, die Anzahl der Spares für das Software-RAID-Gerät und ob die Partition formatiert werden soll.

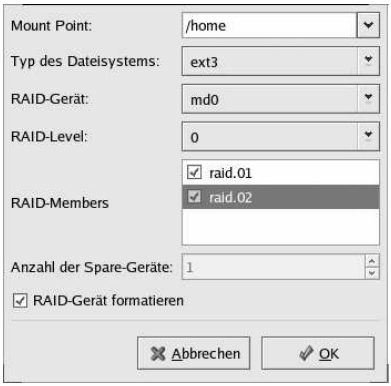

Abbildung 10-7. Erstellen eines Software-RAID-Gerätes

4. Klicken Sie auf **OK**, um das Gerät zur Liste hinzuzufügen.

10.5. Netzwerkkonfiguration

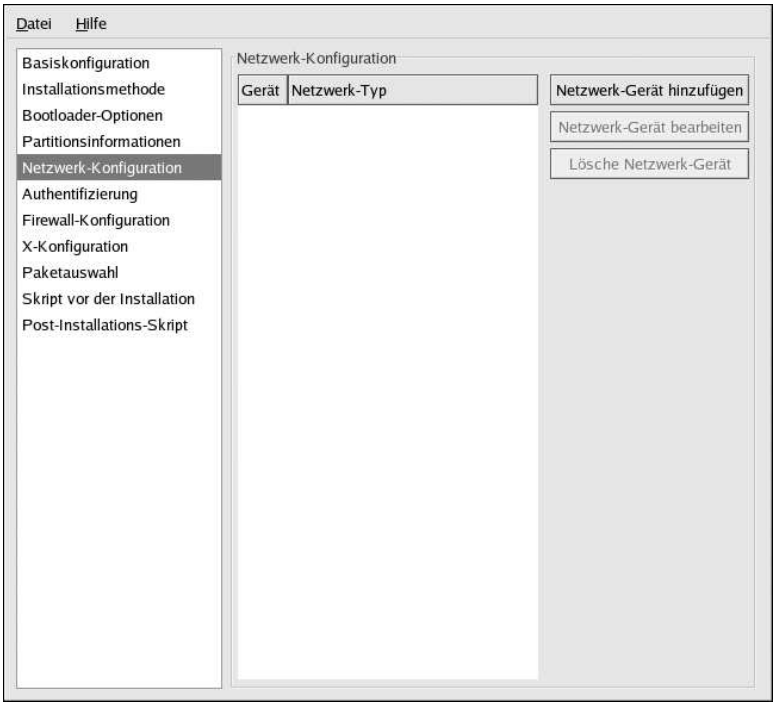

Abbildung 10-8. Netzwerkkonfiguration

Wenn das über Kickstart zu installierende System über keine Ethernetkarte verfügt, konfigurieren Sie keine auf der Seite **Netzwerkkonfiguration**.

Die Vernetzung ist nur erforderlich, wenn Sie eine Installationsmethode für den Netzwerk-Typ wählen (NFS, FTP oder HTTP). Das Netzwerk kann auch nach der Installation mit dem **Network Administration Tool** (`redhat-config-network`) konfiguriert werden. Weitere Informationen finden Sie unter Kapitel 19.

Klicken Sie für jede Ethernetkarte im System auf **Netzwerkgerät hinzufügen** und wählen Sie das Netzwerkgerät und den Netzwerktyp dieses Gerätes. Wählen Sie **eth0** als Netzwerkgerät für die erste Ethernetkarte, wählen Sie **eth1** für die zweite Ethernetkarte usw.

10.6. Authentifizierung

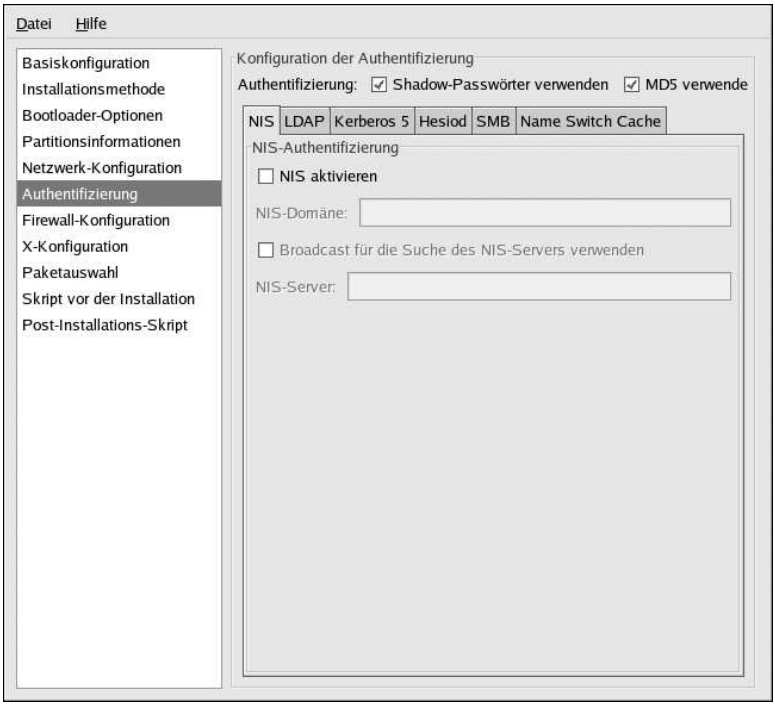

Abbildung 10-9. Authentifizierung

Im Abschnitt **Authentifizierung** wählen Sie, ob Sie Shadow-Passwörter und die md5-Verschlüsselung für Benutzer-Passwörter verwenden. Diese Optionen werden standardmäßig gewählt und sind sehr zu empfehlen.

Mit den Optionen des Bereichs **Konfiguration der Authentifizierung** können Sie folgende Authentifizierungsmethoden konfigurieren:

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- Name Switch Cache

Diese Methoden sind standardmäßig nicht aktiviert. Um eine oder mehrere dieser Methoden zu aktivieren, klicken Sie auf das entsprechende Tab, markieren das Kontrollkästchen neben **Aktivieren** und geben je nach Authentifizierungsmethode die entsprechenden Informationen ein. Weitere Informationen finden Sie unter Kapitel 29.

10.7. Firewall-Konfiguration

Der Bildschirm **Firewall-Konfiguration** ähnelt dem Bildschirm im Installationsprogramm und dem im **Security Level Configuration Tool**.

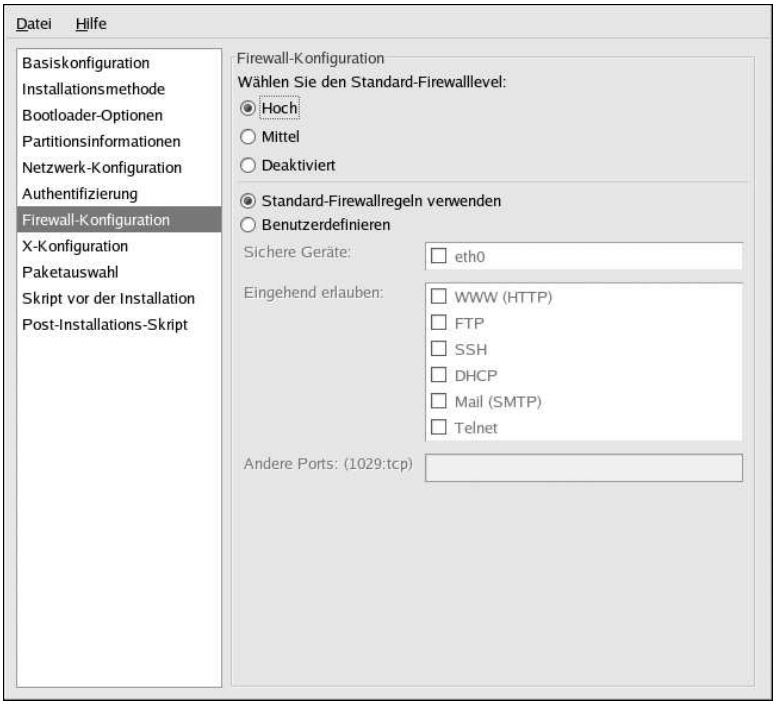

Abbildung 10-10. Firewall-Konfiguration

Wenn **Firewall deaktivieren** ausgewählt ist, erlaubt das System vollständigen Zugriff auf alle Services und Ports. Keine Verbindungen zum System werden abgelehnt.

Die Auswahl **Firewall aktivieren** konfiguriert das System zum Ablehnen eigehender Verbindungen, sofern diese keine Antwort auf ausgehende Anfragen sind, wie DNS-Antworten und DHCP-Anforderungen. Sollte Zugriff auf einen bestimmten Service benötigt werden, kann dieser durch die Firewall gelassen werden.

Lediglich Geräte, die im Abschnitt **Netzwerk-Konfiguration** konfiguriert sind, werden als **Sichere Geräte** aufgeführt. Verbindungen von jedem dieser Geräte werden angenommen. Wenn, zum Beispiel, **eth1** nur Verbindungen vom internen System erhält, möchten Sie eventuell Verbindungen von diesem Gerät zulassen.

Wenn ein Service in der Liste **Sichere Services** ausgewählt wird, werden Verbindungen für diesen Service vom System angenommen und bearbeitet.

Im Textfeld **Andere Ports** können Sie zusätzliche Ports angeben, die für Remote-Zugriff geöffnet werden sollen. Benutzen Sie das Format `port:protocol`. Um, zum Beispiel, IMAP-Zugriff durch die Firewall zu ermöglichen, geben Sie `imap:tcp` ein. Numerische Ports können auch angegeben

werden. Um UDP-Pakete auf Port 1234 durch die Firewall zu lassen, geben Sie **`1234:udp`** ein. Trennen Sie mehrere Ports hierbei durch Kommas.

10.8. X-Konfiguration

Wenn Sie das X Window System installieren, können Sie es während der Kickstart-Installation konfigurieren, indem Sie das Kontrollkästchen **X Window System konfigurieren** im Fenster **X Konfiguration** wie in Abbildung 10-11. Iabgebildet markieren. Wird diese Option nicht aktiviert, werden die Optionen der X Konfiguration deaktiviert und die Option `skipx` wird in die Kickstart-Datei geschrieben.

10.8.1. Allgemein

Der erste Schritt bei der Konfigurierung von X ist die Auswahl der standardmäßigen Farbtiefe und Auflösung. Wählen Sie diese im entsprechenden Pull-Down-Menü aus. Stellen Sie sicher, dass Sie eine Farbtiefe und Auflösung angeben, die mit der Grafikkarte und dem Monitor des Systems kompatibel sind.

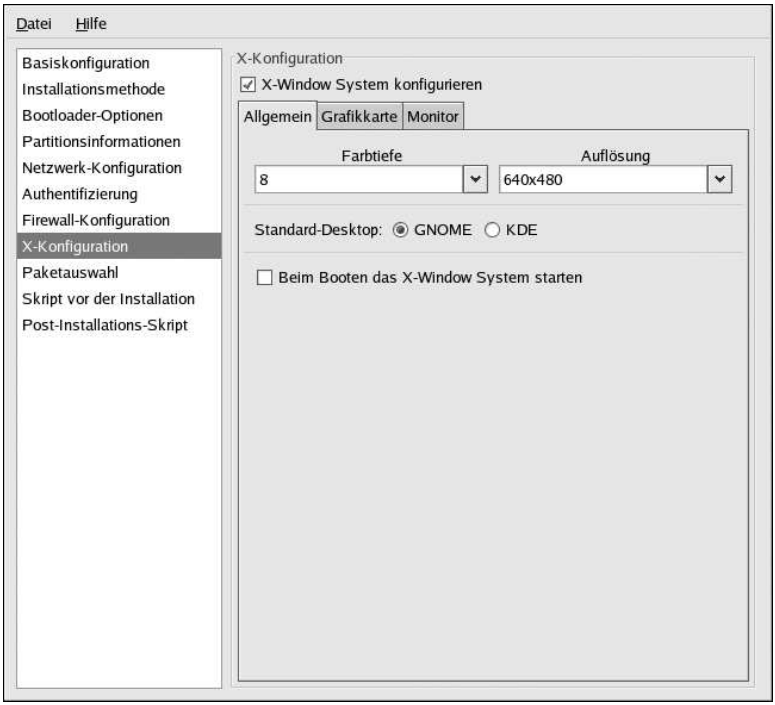

Abbildung 10-11. X-Konfiguration - Allgemein

Wenn Sie sowohl den GNOME- als auch den KDE-Desktop installieren, müssen Sie festlegen, welchen Desktop Sie standardmäßig verwenden möchten. Wenn Sie nur einen Desktop installieren, stel-

len Sie sicher, dass Sie diesen auch auswählen. Nachdem das System installiert ist, können die Benutzer wählen, welchen Desktop sie standardmäßig verwenden möchten.

Wählen Sie anschließend, ob das X Window System beim Systemstart gestartet werden soll. Diese Option startet das System mit einem grafischen Anmeldebildschirm im Runlevel 5. Nachdem das System installiert ist, kann dies geändert werden, indem die Konfigurationsdatei `/etc/inittab` modifiziert wird.

Sie können auch wählen, ob Sie den **Setup Agent** beim Booten des Systems starten möchten. Diese Funktion ist standardmäßig deaktiviert, kann aber aktiviert oder im Rekonfigurationsmodus aktiviert werden. Der rekonfigurationsmodus aktiviert die Sprache, Maus, Tastatur, Root-Passwort, Sicherheitslevel, Zeitzone und Netzwerkkonfigurationsoptionen zusätzlich zu den Standardoptionen.

10.8.2. Grafikkarte

Erkennung der Grafikkarte ist standardmäßig aktiviert. Übernehmen Sie diese Standardeinstellung, wenn das Installationsprogramm während der Installation die Grafikkarte erkennen soll. Diese Erkennung funktioniert bei den meisten neueren Grafikkarten. Wenn Sie diese Option markieren, aber das Installationsprogramm die Grafikkarte nicht erfolgreich erkennt, hält das Programm im Bildschirm für die Grafikkartenkonfiguration an. Sie müssen die Grafikkarte aus der Liste auswählen und auf **Weiter** klicken, um die Installation fortzusetzen.

Alternativ hierzu können Sie die Grafikkarte aus der Liste des **Grafikkarte** Tabs auswählen, wie in Abbildung 10-12 abgebildet. Wählen Sie das Grafik-RAM der ausgewählten Grafikkarte aus dem Pull-Down-Menü **RAM Grafikkarte**. Diese Werte werden vom Installationsprogramm zum Konfigurieren von X Window System verwendet.

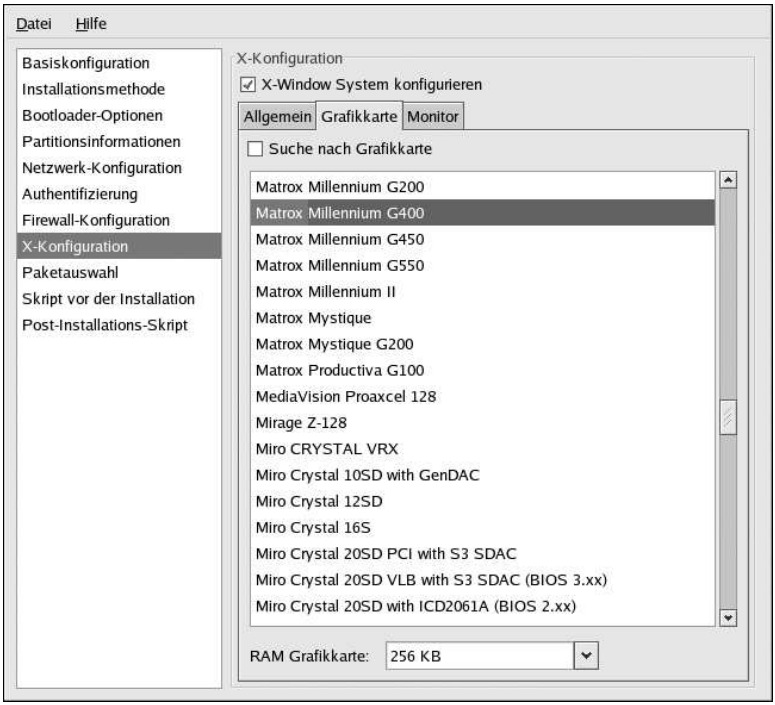

Abbildung 10-12. X-Konfiguration - Grafikkarte

10.8.3. Monitor

Nach der Konfiguration der Grafikkarte klicken Sie auf das Tab **Monitor** wie in Abbildung 10-13 abgebildet.

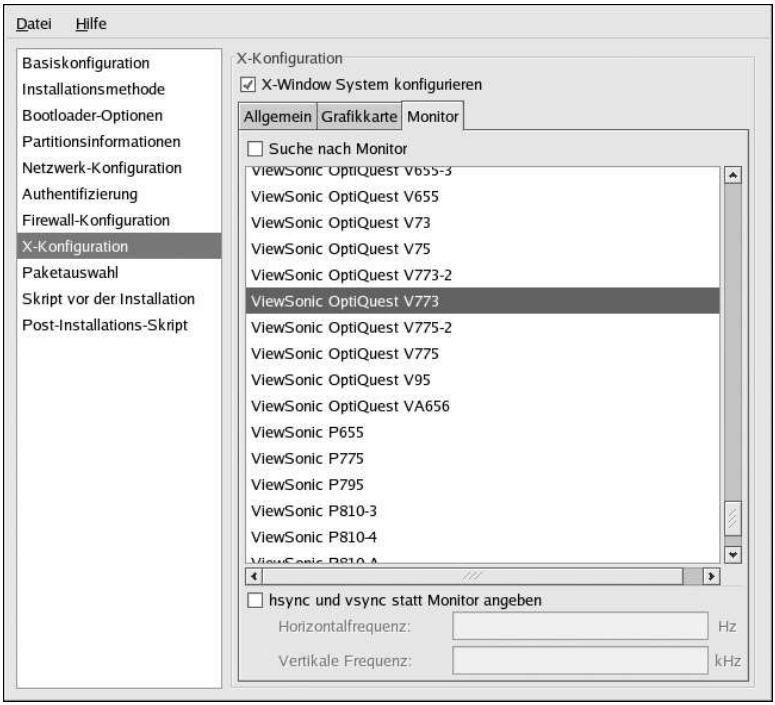

Abbildung 10-13. X-Konfiguration - Monitor

Monitor-Erkennung ist standardmäßig aktiviert. Übernehmen Sie diese Standardeinstellung, wenn das Installationsprogramm während der Installation den Monitor erkennen soll. Diese Erkennung funktioniert bei den meisten neueren Monitoren. Wenn Sie diese Option markieren, aber das Installationsprogramm den Monitor nicht erfolgreich erkennt, hält das Programm im Bildschirm für die Monitorkonfiguration an. Sie müssen den Monitor aus der Liste auswählen und auf **Weiter** klicken, um die Installation fortzusetzen.

Alternativ hierzu können Sie den Monitor aus der Liste auswählen. Sie können auch die horizontale und vertikale Bildwiederholrate statt eines Monitors angeben. Markieren Sie hierfür die Option **hsync und vsync statt Monitor angeben**. Diese Option ist nützlich, wenn der Monitor für das System nicht aufgelistet ist. Beachten Sie, dass die Monitorliste deaktiviert ist wenn diese Option aktiv ist.

10.9. Paketauswahl

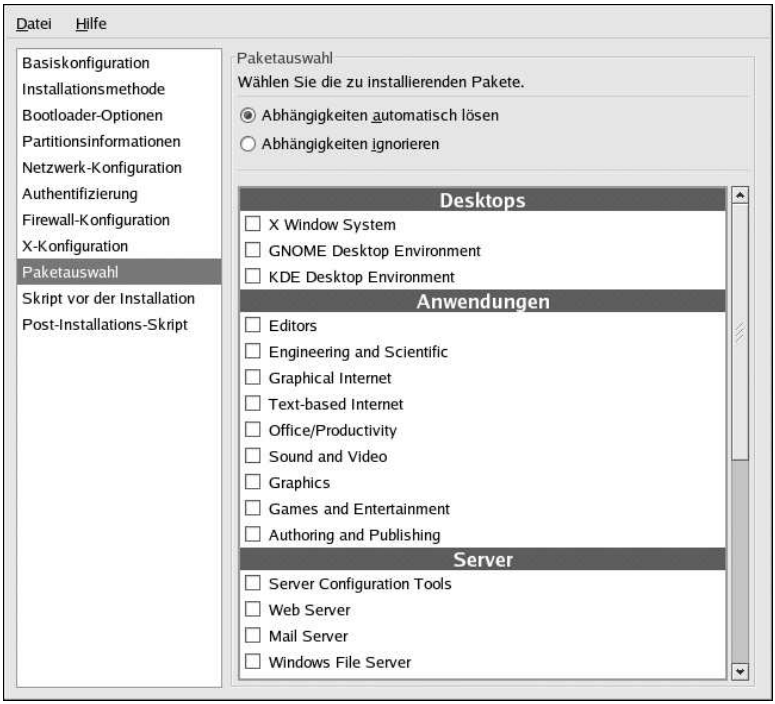

Abbildung 10-14. Paketauswahl

Im Fenster **Paketauswahl** können Sie wählen, welche Kategorie von Paketen Sie installieren möchten.

Es gibt auch Optionen, die Paketabhängigkeiten automatisch auflösen bzw. diese ignorieren.

Zur Zeit erlaubt **Kickstart Configurator** Ihnen nicht, einzelne Pakete auszuwählen. Um einzelne Pakete zu installieren, modifizieren Sie die `%packages` -Sektion der Kickstart-Datei, nachdem Sie diese gespeichert haben. Weitere Informationen finden Sie unter Abschnitt 9.5.

10.10. Pre-Installations-Skript

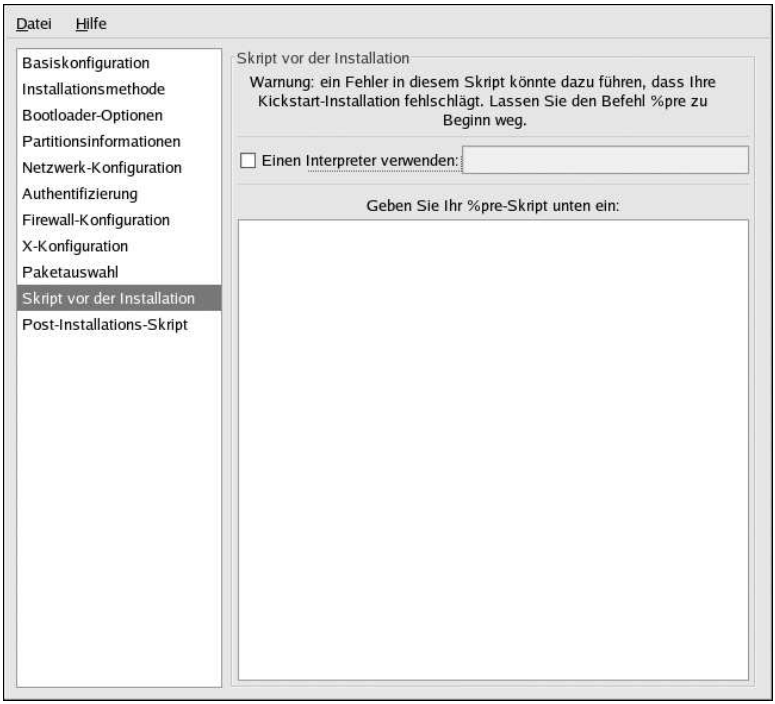

Abbildung 10-15. Pre-Installations-Skript

Sie können Befehle hinzufügen, die auf dem System ausgeführt werden, sofort nachdem die Kickstart-Datei analysiert wurde und bevor die Installation startet. Wenn Sie das Netzwerk in der Kickstart-Datei konfiguriert haben, wird das Netzwerk aktiviert, bevor diese Sektion ausgeführt wird. Wenn ein Pre-Installations-Skript enthalten sein soll, geben Sie es in den Textbereich ein.

Wenn Sie eine Skript-Sprache bestimmen möchten, die Sie zum Ausführen des Skripts verwenden, klicken Sie auf den Button **Interpreter verwenden**, und geben Sie den Interpreter in das Feld neben dem Kästchen ein. Beispiel: **`/usr/bin/python2.2`** kann für ein Python-Skript angegeben werden. Diese Option ist gleichbedeutend mit `%pre --interpreter` *`/usr/bin/python2.2`* in der Kickstart- Datei.

Achtung

Fügen Sie den Befehl `%pre` nicht ein. Er wird automatisch hinzugefügt.

10.11. Post-Installations-Skript

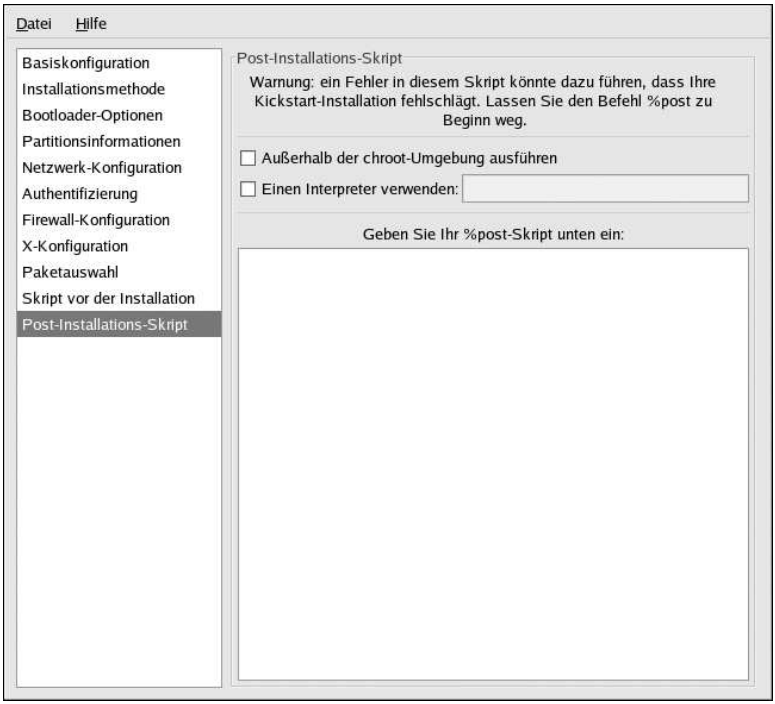

Abbildung 10-16. Post-Installations-Skript

Sie können auch Befehle hinzufügen, die auf dem System ausgeführt werden, nachdem die Installation abgeschlossen ist. Wenn Sie das Netzwerk in der Kickstart-Datei richtig konfiguriert haben, ist das Netzwerk aktiviert. Wenn ein Post-Installations-Skript enthalten sein soll, geben Sie es in den Textbereich ein.

Achtung

Fügen Sie den Befehl `%post` nicht ein. Er wird automatisch hinzugefügt.

Wenn Sie zum Beispiel die Mitteilung des Tages für das neu installierte System ändern möchten, fügen Sie den folgenden Befehl zu der `%post`-Sektion hinzu:

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

Tipp

Weitere Beispiele finden Sie in Abschnitt 9.7.1.

10.11.1. Chroot-Umgebung

Wenn Sie möchten, dass Ihr Nach-Installations-Skript außerhalb der Chroot-Umgebung ausgeführt wird, markieren Sie das Kontrollkästchen neben dieser Option im oberen Teil des Fensters **Post-Installation**. Dies ist gleichbedeutend mit der Verwendung der Option `--nochroot` in der Sektion `%post`.

Wenn Sie Änderungen am neu installierten Dateisystem der Post-Installations-Sektion außerhalb der Chroot-Umgebung vornehmen möchten, müssen Sie den Verzeichnisnamen mit `/mnt/sysimage/` anfügen.

Wenn Sie das Kontrollkästchen **Außerhalb der chroot-Umgebung ausführen** markieren, muss das Beispiel wie folgt geändert werden:

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

10.11.2. Verwenden eines Interpreters

Wenn Sie eine Skript-Sprache bestimmen möchten, die Sie zum Ausführen des Skripts verwenden, aktivieren Sie das Kontrollkästchen **Interpreter verwenden** und geben Sie den Interpreter in das Feld neben dem Kästchen ein. Beispiel: **`/usr/bin/python2.2`** kann für ein Python-Skript angegeben werden. Diese Option ist gleichbedeutend mit `%post --interpreter` *`/usr/bin/python2.2`* in der Kickstart-Datei.

10.12. Speichern von Dateien

Wenn Sie, nachdem Sie Ihre Kickstart-Optionen gewählt haben, sich den Inhalt Ihrer Kickstart-Datei ansehen möchten, wählen Sie **Datei => Vorschau** aus dem Pull-Down-Menü.

Abbildung 10-17. Vorschau

Wählen Sie zum Speichern der Kickstart-Datei **In Datei speichern** im Vorschau-Fenster. Zum Speichern der Datei ohne Vorschau wählen Sie **Datei => Datei speichern** oder drücken Sie [Strg]-[S]. Ein Dateidialogfeld wird angezeigt, aus dem Sie wählen können, wo die Datei gespeichert werden soll.

Im Abschnitt 9.10 finden Sie Informationen über das Starten der Kickstart-Installation.

redhat

Kapitel 11.

Systemwiederherstellung

Wenn Probleme auftreten, gibt es auch immer Möglichkeiten, sie zu lösen. Es ist hierzu jedoch erforderlich, dass Sie das System gut kennen. In diesem Kapitel wird beschrieben, wie Sie Rettungsmodi und Einzelplatzmodi starten können und wo Sie Ihr eigenes Wissen einsetzen können, um Schäden am System zu beheben.

11.1. Häufige Probleme

Üblicherweise ist der Rettungsmodus aus den folgenden Gründen erforderlich:

- Es ist Ihnen nicht möglich, Red Hat Enterprise Linux zu booten (Runlevel 3 oder 5).
- Es sind Probleme mit der Hardware oder der Software aufgetreten, und Sie möchten wichtige Dateien von der Festplatte Ihres Systems entfernen.
- Sie haben das root-Passwort vergessen.

11.1.1. Booten von Red Hat Enterprise Linux nicht möglich

Dieses Problem lässt sich häufig darauf zurückführen, dass ein anderes Betriebssystem installiert wurde, nachdem Sie Red Hat Enterprise Linux installiert haben. Es gibt Betriebssysteme, die davon ausgehen, dass kein anderes Betriebssystem auf Ihrem Computer vorhanden ist, und überschreiben daher den Master Boot Record (MBR), der jedoch den GRUB- oder den LILO- Bootloader enthält. Wird der Bootloader überschrieben, kann Red Hat Enterprise Linux nicht gebootet werden. Die einzige Abhilfe ist hier der Rettungsmodus und das Rekonfigurieren des Bootloaders.

Weiterhin tritt häufig folgendes Problem auf: Sie benutzen ein Partitions-Tool, um eine Partition in der Größe anzupassen oder erstellen nach der Installation eine neue Partition aus dem freien Speicherplatz, wodurch sich die Reihenfolge Ihrer Partitionen verändert. Wenn sich jedoch die Partitionszahl der Partition `/` ändert, findet der Boot-Loader sie nicht mehr, wenn er die Partition mounten will. Dieses Problem können Sie lösen, indem Sie in den Rettungsmodus booten und, falls Sie GRUB benutzen, die Datei `/boot/grub/grub.conf` abändern oder, falls Sie LILO benutzen, die Datei `/etc/lilo.conf` abändern. Sie *müssen* außerdem den Befehl `/sbin/lilo` jedesmal wenn Sie die LILO-Konfigurationsdatei ändern, ausführen.

11.1.2. Probleme mit Hardware/Software

In diese Kategorie fallen eine Vielzahl verschiedener Situationen. Zwei Beispiele sind Fehler der Festplatten oder das Angeben eines ungültigen root-Geräte oder Kernels in der Bootloader-Konfigurationsdatei. Tritt einer dieser beiden Fehler auf, können Sie Red Hat Enterprise Linux unter Umständen nicht booten. Wenn Sie den Rettungsmodus aktivieren können, können Sie das Problem lösen oder zumindest Kopien der wichtigsten Dateien erstellen.

11.1.3. Root-Passwort

Was können Sie machen, wenn Sie das root-Passwort vergessen haben? Ein anderes Passwort einstellen, im Rettungsmodus oder Einzelbenutzermodus hochfahren und mit dem Befehl `passwd` das root-Passwort neu setzen.

11.2. In den Rettungsmodus booten

Der Rettungsmodus bedeutet, eine kleine Red Hat Enterprise Linux-Umgebung vollständig von einer Diskette oder einer CD-ROM zu booten oder eine andere Methode anstelle der Festplatte zu verwenden.

Wie der Name schon sagt, dient der Rettungsmodus dazu, etwas zu retten. Während des normalen Betriebs verwendet Ihr Red Hat Enterprise Linux System Dateien, die auf der Festplatte Ihres Systems gespeichert sind — um Programme auszuführen, Dateien zu speichern u.v.m.

Es kann jedoch vorkommen, dass Sie, dadurch dass Red Hat Enterprise Linux nicht vollständig funktionsfähig ist, keinen Zugriff auf die Dateien Ihrer Festplatte erhalten. Der Rettungsmodus ermöglicht es Ihnen, auch dann auf diese Dateien zuzugreifen, wenn Red Hat Enterprise Linux nicht von der entsprechenden Festplatte ausgeführt werden kann.

Wenn Sie Ihr System im Rettungsmodus starten wollen, müssen Sie Ihr System mit einer der folgenden Methoden booten können:

- Booten Sie Ihr System von der Installationsboot-CD-ROM.[1]
- In dem Sie das System von einer Installations-CD-ROM booten.[1]
- Indem Sie Ihr System von der Red Hat Enterprise Linux CD-ROM #1 booten.

Sobald Sie mit einer dieser Methoden gebootet haben, geben Sie das Schlüsselwort **rescue** als Kernelparameter an. Für beispielsweise ein x86-System, geben Sie den folgenden Befehl am Installationsboot-Prompt ein:

```
linux rescue
```

Sie müssen hier ein paar grundlegende Fragen, wie zum Beispiel nach der zu verwendenden Sprache, beantworten. Sie werden außerdem danach gefragt, wo sich ein gültiges Rescue-Image befindet. Wählen Sie **Lokale CD-ROM**, **Festplatte**, **NFS-Image**, **FTP** oder **HTTP**. Der ausgewählte Ort muss einen gültigen Installationsbaum enthalten, und diese muss für die gleiche Version von Red Hat Enterprise Linux sein wie der von der Red Hat Enterprise Linux CD-ROM #1. Wenn Sie eine Boot-CD-ROM oder -Diskette zum Starten des Rettungsmodus verwendet haben, muss der Installationsbaum vom gleichem Baum wie das davon erstellte Medium sein. Weitere Informationen zum Erstellen eines Installationsbaums auf einer Festplatte, NFS-Server, FTP-Server oder HTTP-Server finden Sie im *Red Hat Enterprise Linux Installationshandbuch*.

Wenn Sie ein Rescue-Image ausgewählt haben, das keine Netzwerkverbindung erfordert, werden Sie gefragt, ob Sie eine Netzwerkverbindung herstellen wollen oder nicht. Eine Netzwerkverbindung ist dann sinnvoll, wenn Sie z.B. Dateien auf einem anderen Computer sichern wollen oder RPM-Pakete von einem gemeinsamen Netzwerk installieren möchten.

Außerdem wird folgende Nachricht angezeigt:

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

1. Um eine Installationsboot-CD-ROM zu erstellen, lesen Sie bitte die Anweisungen im *Red Hat Enterprise Linux Installationshandbuch*.

1. Um eine Installationsboot-CD-ROM zu erstellen, lesen Sie bitte die Anweisungen im *Red Hat Enterprise Linux Installationshandbuch*.

Wenn Sie **Fortfahren** wählen, wird es versuchen, Ihr Dateisystem unter dem Verzeichnis `/mnt/sysimage` zu mounten. Falls es eine Partition nicht mounten sollte, wird dies Ihnen angezeigt. Wenn Sie **Schreibgeschützt** auswählen, wird es versuchen, das Dateisystem unter dem Verzeichnis `/mnt/sysimage`im schreibgeschützten Modus zu mounten. Wenn Sie **Überspringen** wählen, wird Ihr Dateisystem nicht gemountet. Wählen Sie **Überspringen**, wenn Sie denken, dass Ihr Dateisystem defekt ist.

Wenn sich Ihr System dann im Rettungsmodus befindet, erscheint ein Prompt auf der VC (virtuelle Konsole) 1 und der VC 2 (verwenden Sie die Tastenkombination [Strg]-[Alt]-[F1], um auf VC 1 Zugriff zu erhalten, und die Tastenkombination [Strg]-[Alt]-[F2], um auf VC 2 Zugriff zu erhalten):

```
sh-2.05b#
```

Wenn Sie **Fortfahren** gewählt haben, um Ihre Partitionen automatisch zu mounten, und diese mit Erfolg gemountet wurden, befinden Sie sich im Einzelbenutzermodus.

Wenn Ihr Dateisystem gemountet ist, und Sie die Root-Partition zur Root-Partition des System machen wollen, anstelle der temporären Rettungs-Umgebung, geben Sie den folgenden Befehl ein:

```
chroot /mnt/sysimage
```

ein. Dies kann Ihnen von Nutzen sein, wenn Sie Befehle wie `rpm` eingeben, da hierbei Ihre root-Partition als `/` gemountet sein muss. Wenn Sie die Chroot-Umgebung verlassen wollen, geben Sie den Befehl `exit` ein und springen damit zum Prompt zurück.

Wenn Sie **Überspringen** gewählt haben, können Sie trotzdem versuchen, eine Partition von Hand im Rettungsmodus zu mounten, in dem Sie ein Verzeichnis wie */foo* erstellen und den folgenden Befehl eingeben:

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

Im obenstehenden Befehl handelt es sich bei */foo* um ein Verzeichnis, das Sie erstellt haben, und bei */dev/hda5* um die Partition, die Sie mounten wollen. Wenn die Partition vom Typ `ext2` ist, ersetzen Sie `ext3` durch `ext2`.

Wenn Sie die Namen Ihrer Partitionen nicht kennen, geben Sie den folgenden Befehl ein, und Sie erhalten eine Liste der Namen:

```
fdisk -l
```

Vom Prompt können zahlreiche nützliche Befehle aufgerufen werden, darunter:

- `list-harddrives` um alle Festplatten im System aufzulisten
- `ssh`, `scp` und `ping`, wenn das Netzwerk gestartet wurde
- `dump` und `restore` für Benutzer mit Bandgeräten
- `parted` und `fdisk` für die Verwaltung von Partitionen
- `rpm` für das Installieren oder Aktualisieren von Software
- `joe` für das Bearbeiten von Konfigurationsdateien (Wenn Sie `joe`, `emacs`, `pico` oder `vi` eingeben, wird der `joe`-Editor gestartet.)

11.3. Booten im Einzelbenutzermodus

Einer der Vorteile des Einzelbenutzermodus ist es, dass Sie keine Boot-Diskette oder -CD-ROM benötigen. Die Option, Dateisysteme schreibgeschützt oder gar nicht zu mounten besteht hier jedoch nicht.

Wenn Ihr System zwar bootet, die Anmeldung im System jedoch nicht möglich ist, versuchen Sie den Einzelbenutzermodus.

Im Einzelbenutzermodus bootet Ihr Computer auf Runlevel 1. Ihre lokalen Dateisysteme werden gemountet, Ihr Netzwerk wird jedoch nicht aktiviert. Sie benötigen eine Shell zur Systemwartung. Im Gegensatz zum Rettungsmodus versucht der Einzelbenutzermodus, automatisch die Dateisysteme zu mounten; Benutzen Sie den Einzelbenutzermodus *nicht*, wenn Ihr Dateisystem nicht erfolgreich gemountet werden kann. Sie können den Einzelbenutzermodus nicht verwenden, wenn die Runlevel 1 Konfiguration Ihres Systems korrupt ist.

Falls Sie auf einem x86-System GRUB verwenden, gehen Sie folgendermaßen vor, um in den Einzelbenutzermodus zu booten:

1. Falls Sie ein GRUB-Passwort konfiguriert haben, geben Sie `p` und dann das Passwort ein.
2. Wählen Sie **Red Hat Enterprise Linux** mit der Kernelversion, die Sie booten möchten, und geben Sie `a` für Anfügen einer Zeile ein.
3. Gehen Sie auf das Zeilenende und geben Sie **`single`** als ein getrenntes Wort ein (drücken Sie auf [Leertaste]; geben Sie dann **`single`** ein). Beenden Sie den Modus mit [Enter].
4. Jetzt sind Sie wieder auf dem GRUB-Bildschirm: geben Sie `b` ein, um in den Einzelbenutzermodus zu booten:

Wenn Sie auf einem x86-System LILO benutzen, geben Sie eine dieser Optionen im LILO-Boot-Prompt ein (wenn Sie den grafischen LILO verwenden, drücken Sie [Strg]-[x], um den Grafikbildschirm zu verlassen, und rufen Sie den `boot:` Prompt auf):

```
linux single
```

Geben Sie bei allen anderen Plattformen **`single`** als Kernelparamter am Boot-Prompt ein.

11.4. Booten in den Rettungsmodus

Im Rettungsmodus booten Sie in eine kleinstmögliche Umgebung. Das root-Dateisystem wird schreibgeschützt gemountet, und es wird so gut wie gar nichts eingerichtet. Der Hauptvorteil dieses Modus im Vergleich zum Einzelbenutzermodus ist, dass die `init` -Dateien nicht geladen werden. Wenn `init` beschädigt ist oder nicht funktioniert, können Sie immer noch Dateisysteme mounten, um Daten wiederherzustellen, die während einer erneuten Installation verloren gehen könnten.

Um in den Rettungsmodus zu booten gehen Sie wie für das Booten in den Einzelbenutzermodus, wie unter Abschnitt 11.3 beschrieben, vor. Sie müssen jedoch das Wort **`single`** durch **`emergency`** ersetzen.

Kapitel 12.

Software-RAID Konfiguration

Lesen Sie zuerst Kapitel 3, um einen Einblick über RAID, die Unterschiede zwischen Hardware-RAID und Software-RAID sowie die Unterschiede zwischen RAID 0, 1 und 5 zu bekommen.

Software-RAID kann sowohl während der grafischen Installation von Red Hat Enterprise Linux als auch während der Kickstart-Installation konfiguriert werden. In diesem Kapitel wird die Konfiguration des Software-RAIDs während des Installation mit Hilfe von **Disk Druid** beschrieben.

Bevor Sie ein RAID-Laufwerk erstellen können, müssen zuerst RAID-Partitionen erstellt werden. Gehen Sie dabei nach der folgenden Schritt-für-Schritt-Anweisung vor:

1. Wählen Sie auf dem Bildschirm **Festplattenpartitionierung einstellen** die Schaltfläche **Manuelles Partitionieren mit Disk Druid**.
2. Wählen Sie in **Disk Druid** die Schaltfläche **Neu**, um eine neue Partition anzulegen.
3. Wählen Sie **Software-RAID** aus dem Pull-Down-Menü **Dateisystemtyp** wie in Abbildung 12-1 gezeigt.

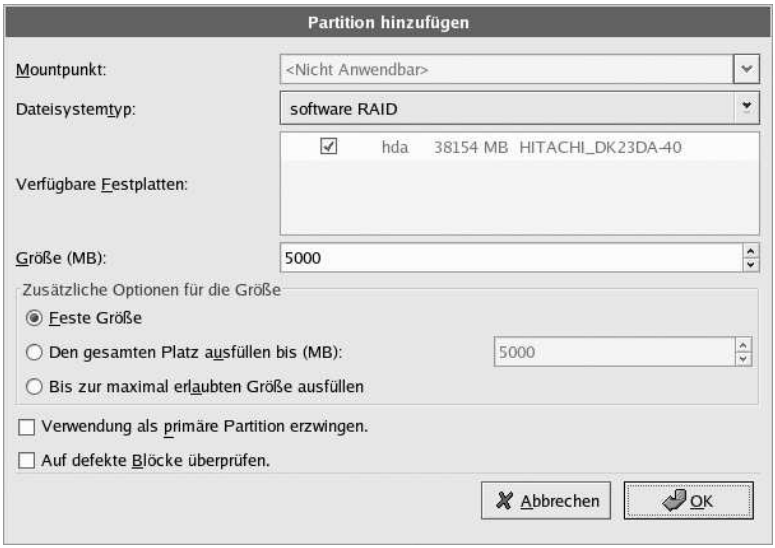

Abbildung 12-1. Erstellen einer neuen RAID Partition

4. Sie können keinen Mount-Punkt eingeben (dies ist erst nach der Anlage des RAID-Geräts möglich).
5. Ein Software RAID muss sich auf eine Festplatte beschränken. Wählen Sie unter **Verfügbare Festplatten** die Festplatte, auf der Sie das RAID erstellen wollen. Falls Sie mehrere Laufwerke haben, werden hier alle Platten ausgewählt. Machen Sie die Auswahl aller Platten, auf denen sich kein RAID befinden soll rückgängig.

6. Geben Sie die gewünschte Größe für die Partition ein.
7. Wählen Sie **Bis zur maximal erlaubten Größe ausfüllen**, wenn die erweiterungsfähige Partition den gesamten Platz auf der Festplatte ausfüllen soll. Wählen Sie **Feste Größe**, um der Partition die angegebene Größe zu geben. Wählen Sie **Gesamten Platz bis zu (MB) füllen** und geben Sie eine Größe in MB ein, um einen Bereich für die mögliche Partitionsgröße anzugeben, oder wählen Sie **Bis zur maximal erlaubten Größe füllen**, wenn die Partition den gesamten Platz auf der Festplatte ausfüllen soll. Wenn Sie mehrere erweiterungsfähige Partitionen haben, teilen sich die Partitionen den zur Verfügung stehenden Platz auf der Platte.
8. Wählen Sie **Als primäre Partition forcieren**, wenn die Partition eine Primärpartition sein soll.
9. Klicken Sie auf **OK**, um zum Hauptfenster zurückzukehren.

Wiederholen Sie diese Schritte und erstellen Sie so viele Partitionen, wie für die RAID-Einrichtung benötigt werden. Beachten Sie, dass nicht alle Partitionen RAID Partitionen sein müssen. So können Sie zum Beispiel nur die Partition `/home` als ein Software-RAID Gerät konfigurieren.

Wenn Sie alle Partitionen als Partitionen **Software-RAID** erstellt haben, folgen Sie diesen Schritten:

1. Wählen Sie die Schaltfläche **RAID** im Hauptbildschirm der Partitionierung **Disk Druid** (siehe Abbildung 12-4).
2. Es erscheint Abbildung 12-3. Wählen Sie **RAID Gerät erstellen**.

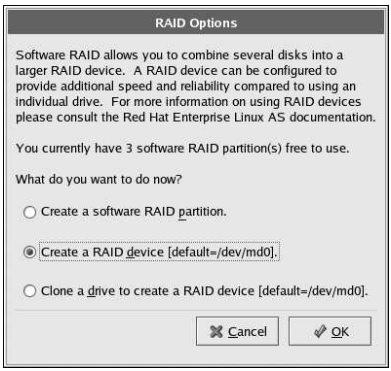

Abbildung 12-2. RAID Optionen

3. Es erscheint Abbildung 12-3: hier können Sie ein RAID-Gerät erstellen.

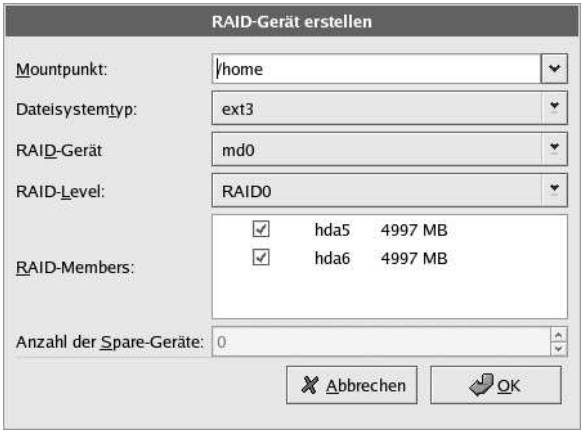

Abbildung 12-3. RAID-Gerät anlegen

4. Geben Sie einen Mount-Punkt an.
5. Wählen Sie den Dateisystemtyp für die Partition.
6. Wählen Sie einen Gerätenamen wie z.B. **md0** für das RAID-Gerät.
7. Wählen Sie den RAID-Level aus. Sie können zwischen **RAID 0**, **RAID 1** und **RAID 5** wählen.

Anmerkung

Wenn Sie eine RAID-Partition von `/boot` erstellen, müssen Sie RAID Level 1 auswählen. Zudem muss eines der ersten beiden Laufwerke (IDE als erstes, SCSI als zweites) verwendet werden. Wenn Sie keine RAID-Partition von `/boot`, sondern von `/` erstellen, müssen Sie ebenfalls RAID Level 1 auswählen. Auch in diesem Fall muss eines der beiden ersten Laufwerke (IDE als erstes, SCSI als zweites) verwendet werden.

8. Die von Ihnen erstellten RAID Partitionen erscheinen in der **RAID Partitionen** Liste. Wählen Sie hier, welche dieser Partitionen zum Erstellen des RAID-Geräts verwendet werden soll.
9. Für RAID 1 und RAID 5 kann eine Reserve-Partition bestimmt werden. Falls eine RAID-Software-Partition ausfällt, wird sie automatisch durch die Reserve-Partition ersetzt. Für jede Reservepartition, die Sie bestimmen wollen, müssen Sie eine zusätzliche RAID-Software-Partition erstellen (zusätzlich zu den Partitionen für das RAID-Gerät). Wählen Sie im vorausgehenden Schritt die Partitionen für das RAID-Gerät und die Reserve-Partition(en) aus. Bestimmen Sie die Zahl der Reserve-Partitionen.
10. Nach dem Sie auf **OK** geklickt haben, erscheint das RAID-Gerät in der Liste **Festplattenzusammenfassung** wie in Abbildung 12-4 gezeigt. Ab hier können Sie mit dem Installationsprozess fortfahren. Weitere Informationen finden Sie im *Red Hat Enterprise Linux Installationshandbuch*.

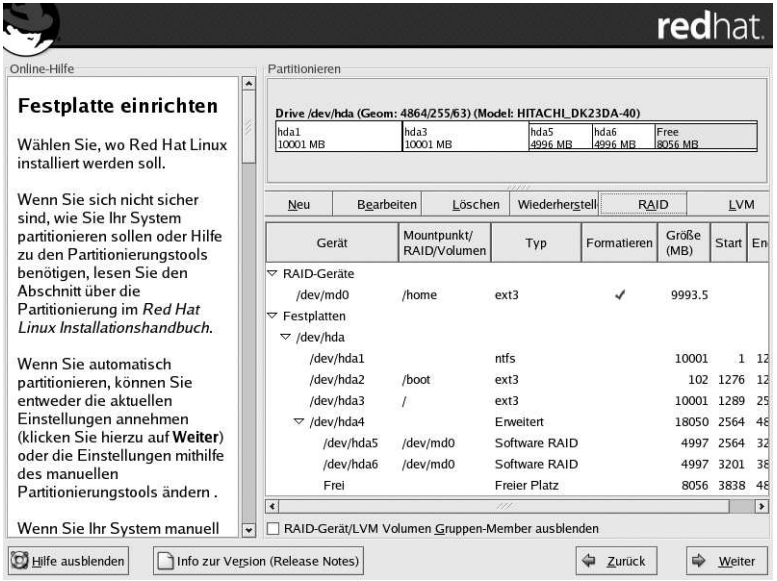

Abbildung 12-4. Erstellen eines RAID-Arrays

Kapitel 13.

LVM-Konfiguration

LVM kann während der grafischen Installation oder der Kickstart-Installation konfiguriert werden. Sie können `lvm` verwenden, um Ihre LVM-Konfiguration zu erstellen. Diese Anweisungen konzentrieren sich allerdings hauptsächlich auf die Verwendung von **Disk Druid**.

Lesen Sie eine Einführung über LVM in Kapitel 4. Ein Überblick über die für die Konfiguration von LVM erforderlichen Schritte:

- Legen Sie *physische Volumen* auf den Festplatten an.
- Legen Sie *Volumengruppen* der physischen Volumen an.
- Legen Sie *logische Volumen* der Volumengruppen an und weisen Sie den logischen Volumen Mount-Punkte zu.

Anmerkung

Sie können LVM Volumengruppen nur im GUI Installationsmodus anlegen. Im Text-Installationsmodus können existierenden logischen Volumen Mount-Punkte zugewiesen werden.

Wenn Sie eine logisches Volumengruppe mit logischen Volumen erstellen möchten:

1. Wählen Sie im Bildschirm **Festplattenpartitionierung einstellen** den Button **Manuell mit Disk Druid einstellen**.
2. Wählen Sie anschließend **Neu**.
3. Wählen Sie **Physisches Volumen (LVM)** aus dem Pull-Down-Menü **Dateisystemtyp** wie in Abbildung 13-1 beschrieben aus.

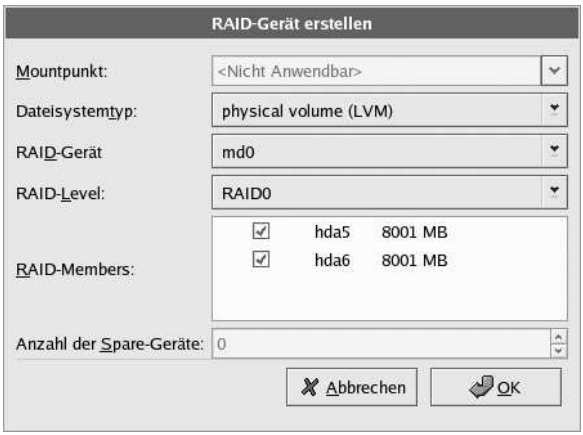

Abbildung 13-1. Anlage eines physischen Volumens

4. Sie können keinen Mount-Punkt eingeben (dies ist erst nach Anlage der Volumengruppe möglich).
5. Ein physisches Volumen muss auf eine Festplatte beschränkt sein. Rufen Sie die **Zulässigen Festplatten** ab und wählen Sie die Festplatte, auf der das physische Volumen angelegt werden soll. Wenn Sie mehrere Festplatten besitzen, werden hier alle Festplatten ausgewählt, entfernen Sie die Auswahl all dieser Festplatten und lassen Sie nur die gewünschte Festplatte ausgewählt.
6. Geben Sie die Größe für das physischen Volumens ein.
7. Wählen Sie **Feste Größe** und anschließend **Platz ausfüllen bis (MB)** und geben Sie eine Größe in MB ein, um einen Bereich zu spezifizieren, oder wählen Sie **Bis zur maximal zulässigen Größe füllen**, um den gesamten verfügbaren Platz in Anspruch zu nehmen.
8. Wählen Sie **Als primäre Partition forcieren**, wenn Sie die Partition als primäre Partition einstellen möchten.
9. Klicken Sie auf **OK**, um zum Hauptbildschirm zurückzukehren.

Wiederholen Sie diese Schritte, um so viele physische Volumen zu erstellen, wie für das Einstellen von LVM erforderlich sind. Wenn eine Volumengruppe mehr als eine Festplatte umfassen soll, legen Sie auf jeder Festplatte ein physisches Volumen an.

Warnung

Die `/boot`-Partition kann keine Volumengruppe sein, da sie der Bootloader nicht lesen kann. Wenn sich die root-Partition auf einem logischen Volumen befinden soll, müssen Sie eine separate `/boot`-Partition anlegen, die zu keiner Volumengruppe gehört.

Führen Sie die folgenden Schritte aus, nachdem alle physischen Volumen angelegt wurden:

1. Klicken Sie auf **LVM**, um die physischen Volumen in Volumengruppen zusammenzufassen. Eine Volumengruppe stellt damit prinzipiell eine Gruppe physischer Volumen dar. Es können mehrere Volumengruppen bestehen, ein physisches Volumen kann sich jedoch nur in einer Volumengruppe befinden.

Anmerkung

In der logischen Volumengruppe steht allgemeiner Platz zur Verfügung. Die Summe der physischen Volumen entspricht nicht unbedingt der Größe der Volumengruppe. Die Größe der angezeigten logischen Volumen ist jedoch korrekt.

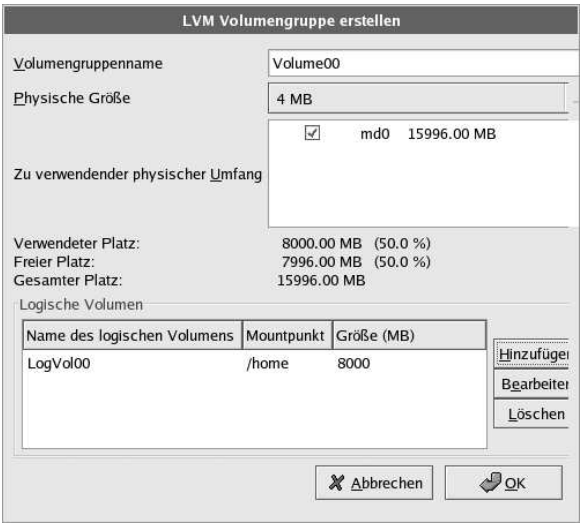

Abbildung 13-2. Anlage eines LVM-Geräts

2. Ändern Sie, wenn erforderlich, den **Volumengruppennamen**.
3. Alle logischen Volumen in der Volumengruppe müssen in Einheiten einer *physischen Größe* angeordnet sein. Standardmäßig beträgt diese Größe 4 MB. Die Größe der logischen Volumen muss sich daher durch 4 MB teilen lassen. Wenn Sie eine andere Größe eingeben, wählt das Installationsprogramm automatisch die am ehesten entsprechende Größe in 4 MB. Sie sollten diese Einstellung nicht ändern.
4. Wählen Sie die physischen Volumen, die für die Volumengruppe verwendet werden sollen.
5. Legen Sie logische Volumen mit Mount-Punkten wie `/home` an. Denken Sie dabei daran, dass `/boot` kein logisches Volumen sein kann. Um ein logisches Volumen hinzuzufügen, klicken Sie auf den Button **Hinzufügen** im Abschnitt **Logische Volumen**. Es erscheint ein Dialogfenster wie in Abbildung 13-3 gezeigt.

Abbildung 13-3. Anlage eines logischen Volumens

Wiederholen Sie diese Schritte für jede Volumengruppe, die Sie anlegen möchten.

Tipp

Sie sollten eventuell freien Platz in der logischen Volumengruppe lassen, damit Sie die logischen Volumen zu einem späteren Zeitpunkt erweitern können.

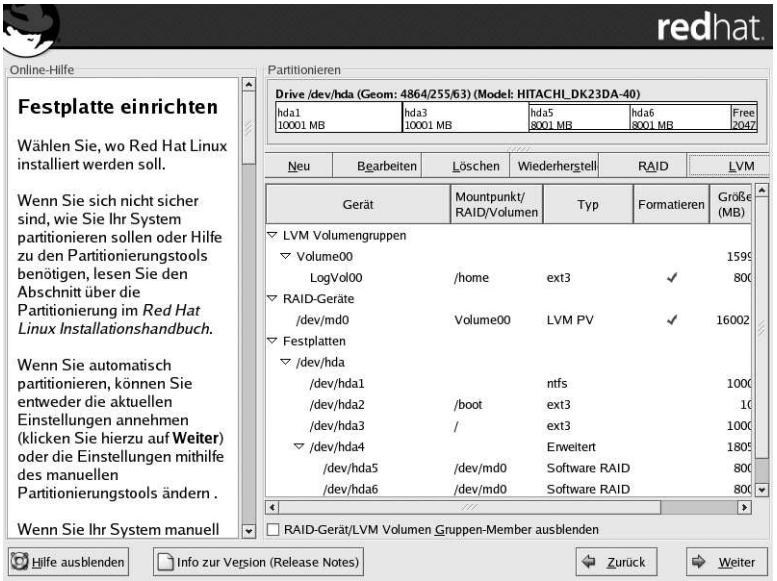

Abbildung 13-4. Angelegte logische Volumen

redhat

Kapitel 14.

PXE-Netzwerk-Installationen

Red Hat Enterprise Linux ermöglicht die Installierung über ein Netzwerk unter Verwendung des NFS-, FTP- oder HTTP-Protokolls. Eine Netzwerk-Installation kann von einer Netzwerk-Boot-Diskette, einer Boot-CD-ROM oder mit der `askmethod` Boot-Option von Red Hat Enterprise Linux CD #1 gestartet werden. Unter der Voraussetzung, dass das zu installierende System eine Netzwerk-Schnittstellenkarte (NIC) mit PXE hat, kann es auch so konfiguriert werden, dass es von Dateien auf einem anderen System im Netzwerk hochfährt anstelle von einer Diskette oder CD-Rom.

Bei einer PXE-Netzwerk-Installation sendet die PXE-unterstützte NIC des Clients eine Sendeanfrage für DHCP-Information aus. Der DHCP-Server stellt dem Client eine IP-Adresse zur Verfügung und auch andere Netzwerk-Informationen, wie den Namen des Servers, die IP-Adresse oder den Hostnamen des `tftp` Servers (der die für den Start des Installationsprogrammes nötigen Dateien bereitstellt) und den Ort der Dateien auf dem `tftp` Server. Ermöglicht wird dies durch PXELINUX, das Teil des `syslinux` Paketes ist.

Zur Vorbereitung auf die PXE-Installation müssen folgende Schritte ausgeführt werden:

1. Konfigurieren Sie den Netzwerk-Server (NFS, FTP, HTTP), damit er den Installationsbaum exportiert.
2. Konfigurieren Sie die Dateien auf dem `tftp` Server, die für das Hochfahren mit PXE nötig sind.
3. Konfigurieren Sie, welche Hosts von der PXE-Konfiguration aus hochfahren dürfen.
4. Starten Sie den `tftp` Dienst.
5. Konfigurieren Sie DHCP
6. Fahren Sie den Client hoch und starten Sie die Installation.

14.1. Einrichtung des Netzwerk-Servers

Richten Sie zuerst einen NFS-, FTP- oder HTTP-Server so ein, dass er den gesamten Installationsbaum für die Version und Variante von Red Hat Enterprise Linux, die installiert werden soll, exportiert.. Siehe Abschnitt *Vorbereitung für die Netzwerk-Installation* im *Red Hat Enterprise Linux Installationshandbuch* for genauere Informationen.

14.2. PXE-Konfiguration zum Hochfahren

Der nächste Schritt ist, die für den Installationsstart notwendigen Dateien auf den `tftp` Server zu kopieren, damit sie gefunden werden, wenn sie der Client braucht. Der `tftp` Server ist normalerweise der gleiche Server wie der Netzwerk-Server, der den Installationsbaum exportiert.

Um diese Dateien zu kopieren, starten Sie **Network Booting Tool** auf dem NFS-, FTP- oder HTTP-Server. Ein eigener PXE-Server ist nicht notwendig.

Für die Befehlszeilen-Version dieser Anweisungen siehe Abschnitt 14.2.1.

Um die grafische Version von **Network Booting Tool** zu verwenden, müssen Sie das X Window System und Root-Privilegien haben, außerdem muss das `redhat-config-netboot` RPM-Paket installiert sein. Um **Network Booting Tool** vom Desktop aus zu starten, gehen Sie zum **Main Menu Button** (auf der Leiste) => **System Settings** => **Server Settings** => **Network Booting Service**. Oder Sie geben den Befehl `redhat-config-netboot` an einem Shell Prompt ein (z.B. bei **XTerm** oder **GNOME terminal**).

Wenn Sie **Network Booting Tool** zum ersten Mal starten, wählen Sie **Network Install** vom **First Time Druid**. Oder Sie wählen **Configure => Network Installation** vom Pulldown-Menü und klicken dann **Add**. Das Dialogfenster in Abbildung 14-1 wird angezeigt.

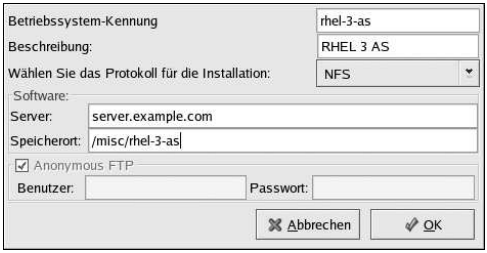

Abbildung 14-1. Einrichtung der Netzwerk-Installation

Geben Sie folgende Informationen an:

- **Operating system identifier** — Geben Sie einen einmaligen Namen an, der aus einem Wort besteht, um die Red Hat Enterprise Linux Version und Variante zu identifizieren. Der Name wird als der Verzeichnisname im `/tftpboot/linux-install/` Verzeichnis verwendet.
- **Description** — Geben Sie eine kurze Beschreibung des Red Hat Enterprise Linux Version und Variante.
- **Select protocol for installation** — Wählen Sie NFS, FTP oder HTTP als Netzwerk-Installationstyp, je nachdem, welcher Typ davor konfiguriert wurde. Wenn FTP gewählt wird, anonymes FTP aber nicht verwendet wird, entfernen Sie die Kennzeichnung bei **Anonymous FTP** und geben Sie eine gültige Benutzernamen/Passwort-Kombination an.
- **Server** — Geben Sie die IP-Adresse oder den Domain-Namen des NFS-, FTP- or HTTP-Servers an.
- **Location** — Geben Sie das gemeinsam verwendete Verzeichnis des Netzwerk-Servers an. Wenn FTP oder HTTP gewählt wurde, muss sich das Verzeichnis auf das standardmäßige Verzeichnis des FTP-Servers oder auf den Dokumenten-Root des HTTP-Servers beziehen. Für alle Netzwerk-Installationen muss das angegebene Verzeichnis das `RedHat/` Verzeichnis des Installationsbaumes enthalten.

Nachdem Sie **OK** geklickt haben, werden die `initrd.img` und `vmlinuz` Dateien, die für das Hochfahren des Installationsprogrammes notwendig sind, von `images/pxeboot/` in den angegebenen Installationsbaum nach `/tftpboot/linux-install/<os-identifier>/` auf den `tftp` Server transferiert.(der, auf dem **Network Booting Tool** ausgeführt ist).

14.2.1. Konfiguration der Befehlszeile

Wenn am Netzwerk-Server X nicht ausgeführt ist, kann die `pxeos` Befehlszeilen-Utility, die Teil des `redhat-config-netboot` Paketes ist, verwendet werden, um die `tftp` Server Dateien wie in Abschnitt 14.4 beschrieben zu konfigurieren:

```
pxeos -a -i "<description>" -p <NFS|HTTP|FTP> -D 0 -s client.example.com \
-L <net-location> <os-identifer>
```

Die folgende Liste erklärt die Optionen:

- `-a` — Legt fest, dass ein OS-Vorgang zur PXE-Konfiguration hinzugefügt wird.

- `-i "<description>"` — Ersetzen Sie "`<description>`" mit einer Beschreibung des OS-Vorganges. Dies korrespondiert mit dem **Description** Feld in Abbildung 14-1.
- `-p <NFS|HTTP|FTP>` — Legen Sie fest, welche der NFS-, FTP- oder HTTP-Protokolle für die Installation verwendet werden sollen Es kann nur eines festgelegt werden. Dies korrespondiert mit dem **Select protocol for installation** Menü in Abbildung 14-1.
- `-D 0` — Zeigt an, dass keine plattenlose Konfiguration vorliegt, weil `pxeos` auch zur Konfiguration einer plattenlosen Umgebung verwendet werden kann.
- `-s client.example.com` — Geben Sie den Namen des NFS, FTP oder HTTP-Servers nach der `-s` Option an. Dies korrespondiert mit dem **Server** Feld in Abbildung 14-1.
- `-L <net-location>` — Geben Sie den Ort des Installationsbaumes an diesem Server nach der`-L` Option an. Dies korrespondiert mit dem **Location** Feld in Abbildung 14-1.
- `<os-identifer>` — Legen Sie den OS- Identifizierer fest, der als Verzeichnisname im`/tftpboot/linux-install/` Verzeichnis verwendet wird. Dies korrespondiert mit dem **Operating system identifier** Feld Abbildung 14-1.

Wenn FTP als das Installationsprotokoll gewählt wird und die anonyme Einlog-Funktion nicht verfügbar ist, legen Sie einen Benutzernamen und ein Passwort zum Einloggen fest, mit den folgenden Optionen vor `<os-identifer>`im vorhergehenden Befehl:

```
-A 0 -u <username> -p <password>
```

14.3. Hinzufügung von PXE-Hosts

Nach der Konfiguration des Netzwerk-Servers wird die in Abbildung 14-2 gezeigte Schnittstelle angezeigt.

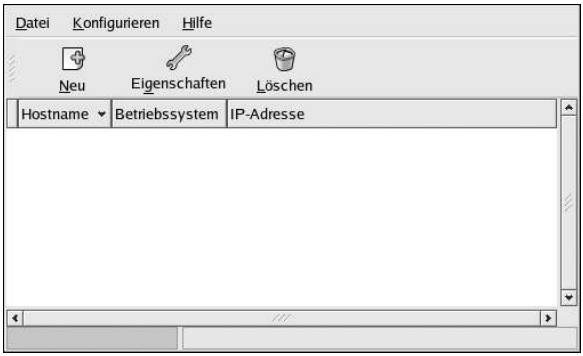

Abbildung 14-2. Hosts hinzufügen

Als nächster Schritt muss konfiguriert werden, welche Hosts sich mit dem PXE- Boot-Server verbinden dürfen. Für die Befehlszeilen-Version dieses Schrittes siehe Abschnitt 14.3.1.

Um Hosts hinzuzufügen, klicken Sie den **New** Button.

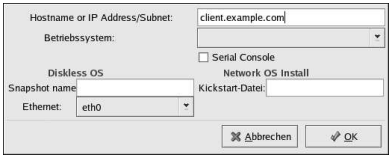

Abbildung 14-3. Einen Host hinzufügen

Geben Sie die folgende Information ein:

- **Hostname or IP Address/Subnet** — Geben Sie die IP- Adresse, den voll qualifizierten Hostnamen oder ein Subnetz der Systeme ein, die sich zur Installation mit dem PXE-Server verbinden dürfen.
- **Operating System** — Wählen sie den Operationssystem- Identifizierer zur Installation auf diesem Client aus. Die Liste setzt sich aus den Netzwerk- Installiervorgängen zusammen, die von dem **Network Installation Dialog** erzeugt werden.
- **Serial Console** — Wählen Sie diese Möglichkeit aus, um eine serielle Konsole zu verwenden.
- **Kickstart File** — Legen Sie den Ort einer Kickstart- Datei fest, z.B. **`http://server.example.com/kickstart/ks.cfg`**. Diese Datei kann mit **Kickstart Configurator** erzeugt werden. Für weitere Details siehe Kapitel 10.

Ignorieren Sie die **Snapshot name** und **Ethernet** Optionen. Sie werden nur bei plattenlosen Umgebungen verwendet.

14.3.1. Konfiguration der Befehlszeile

Wenn der Netzwer-Server X nicht ausführt, kann die `pxeboot` Utility, ein Teil des `redhat-config-netboot` Paketes, dafür verwendet werden, Hosts hinzuzufügen, die sich mit dem PXE-Server verbinden dürfen.

```
pxeboot -a -O <os-identifier> -r <value> <host>
```

Die folgende Liste beschreibt die Optionen:

- `-a` — Legt fest, dass ein Host hinzugefügt werden muss.
- `-O` *<os-identifier>* — Ersetzen Sie *<os-identifier>* mit dem Operationssystem-Identifizierer, wie in Abschnitt 14.2 angegeben.
- `-r` *<value>* — Ersetzen Sie *<value>* mit der RAM-Plattengröße.
- *<host>* — Ersetzen Sie *<host>* mit der IP-Adresse oder dem Hostnamen des Host, der hinzugefügt werden soll.

14.4. Starten des `tftp` Servers

Überprüfen Sie auf dem DHCP-Server, ob das Paket `tftp-server` installiert ist. Verwenden Sie hierzu den Befehl `rpm -q tftp-server`. Sollte dies nicht der Fall sein, installieren Sie es über Red Hat Network oder von den Red Hat Enterprise Linux CD-ROMs. Weitere Informationen zum Installieren von RPM-Paketen finden Sie unter Teil III.

`tftp` ist ein xinetd-basierter Service; Starten Sie diesen mit den folgenden Befehlen:

```
/sbin/chkconfig --level 345 xinetd on
/sbin/chkconfig --level 345 tftp on
```

Dieser Befehl konfiguriert die `tftp` und `xinetd` Services zum augenblicklichen Start und auch zum Starten zur Bootzeit in den Runlevels 3, 4 und 5.

14.5. Konfigurierung des DHCP-Servers

Sollte noch kein DHCP-Server auf dem Netzwerk bestehen, konfigurieren Sie einen. Sehen Sie Kapitel 25 für genauere Informationen. Stellen Sie sicher, dass die Konfigurationsdatei Folgendes enthält, so dass PXE-Booting für Systeme, die dies unterstützen, aktiviert ist:

```
allow booting;
allow bootp;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server <server-ip>;
   filename "linux-install/pxelinux.0";
}
```

Die IP-Adresse hinter der Option `next-server` sollte die des `tftp`-Servers sein.

14.6. Hinzufügung einer angepassten Boot-Nachricht

Sie können `/tftpboot/linux-install/msgs/boot.msg` verändern, um eine angepasste Boot-Nachricht zu verwenden.

14.7. Ausführung der PXE-Installation

Anweisungen über die Konfiguration der Netzwerk-Schnittstelle mit PXE-Unterstützung zum Hochfahren vom Netzwerk aus erhalten Sie in der Betriebsanleitung der NIC. Zwischen den verschiedenen Karten können leichte Unterschiede auftreten.

Wenn das System das Installationsprogramm hochgefahren hat, siehe *Red Hat Enterprise Linux Installationshandbuch*.

Kapitel 15.
Plattenlose Umgebungen

Einige Netzwerke brauchen mehrere Systeme mit der gleichen Konfiguration. Diese Systeme sollten außerdem einfach neu zu starten, einfach aufzuwerten und einfach zu leiten sein. Eine Lösung ist die Verwendung einer *plattenlosen Umgebung*, in der der Großteil des Operationssystems, dies kann ein nicht-beschreibbares System (Read Only) sein, von einem zentralen Server aus von den den Clients gemeinsam verwendet wird. Für den Rest des Operationssystems, er muss beschreibbar (Read/Write) sein, haben die individuellen Clients ihre eigenen Verzeichnisse auf dem zentralen Server. Jedes Mal, wenn die Clients hochfahren, wird die meiste OS von dem NFS-Server als Read-Only gemountet, zusätzlich ein anderes Verzeichnis als beschreibbar. Jeder Client hat sein eigenes beschreibbares Verzeichnis, sodass sich die Clients gegenseitig nicht in die Quere kommen können.

Die folgenden Schritte sind zur Konfiguration von Red Hat Enterprise Linux auf einem plattenlosen Client notwendig:

1. Installieren Sie Red Hat Enterprise Linux auf einem System, sodass die Dateien auf den NFS-Server kopiert werden können. (Siehe *Red Hat Enterprise Linux Installationshandbuch* für Details.) Jede Software, die von den Clients verwendet werden soll, muss auf diesem System installiert werden. Außerdem muss das `busybox-anaconda` Paket installiert sein.
2. Erstellen Sie ein Verzeichnis auf dem NFS-Server, der die plattenlose Umgebung beinhaltet, z.B. `/diskless/i386/RHEL3-AS/`:
   ```
   mkdir -p /diskless/i386/RHEL3-AS/
   ```
   Dieses Verzeichnis wird als `diskless directory` bezeichnet.
3. Erstellen Sie für dieses Verzeichnis ein Unterverzeichnis mit dem Namen `root/`:
   ```
   mkdir -p /diskless/i386/RHEL3-AS/root/
   ```
4. Kopieren Sie Red Hat Enterprise Linux vom Client-System auf den Server, indem Sie `rsync` verwenden. Zum Beispiel:
   ```
   rsync -a -e ssh installed-system.example.com:/ /diskless/i386/RHEL3-AS/root/
   ```
   Die Länge dieser Operation hängt von der Verbindungsgeschwindigkeit des Netzwerkes und von der Größe des Dateisystems auf dem installierten System ab. Es kann eine Weile dauern.
5. Start Sie den `tftp` Server wie besprochen in Abschnitt 15.1.
6. Konfigurieren Sie den DHCP-Server wie besprochen in Abschnitt 15.2.
7. Beenden Sie die Erstellung der plattenlosen Umgebung wie besprochen in Abschnitt 15.4.
8. Konfigurieren Sie die plattenlosen Clients wie besprochen in Abschnitt 15.5.
9. Konfigurieren Sie jeden plattenlosen Client auf Hochfahren mit PXE, und fahren Sie sie hoch.

15.1. Starten Sie den `tftp` Server

Überprüfen Sie auf dem DHCP-Server, ob das Paket `tftp-server` installiert ist. Verwenden Sie hierzu den Befehl `rpm -q tftp-server`. Sollte dies nicht der Fall sein, installieren Sie es über Red Hat Network oder von den Red Hat Enterprise Linux CD-ROMs. Weitere Informationen zum Installieren von RPM-Paketen finden Sie unter Teil III.

`tftp` ist ein xinetd-basierter Service; Starten Sie diesen mit den folgenden Befehlen:

```
/sbin/chkconfig --level 345 xinetd on
/sbin/chkconfig --level 345 tftp on
```

Dieser Befehl konfiguriert die `tftp` und `xinetd` Services zum augenblicklichen Start und auch zum Starten zur Bootzeit in den Runlevels 3, 4 und 5.

15.2. Konfiguration des DHPC-Servers

Sollte noch kein DHCP-Server auf dem Netzwerk bestehen, konfigurieren Sie einen. Sehen Sie Kapitel 25 für genauere Informationen. Stellen Sie sicher, dass die Konfigurationsdatei Folgendes enthält, so dass PXE-Booting für Systeme, die dies unterstützen, aktiviert ist:

```
allow booting;
allow bootp;
class "pxeclients" {
   match if substring(option vendor-class-identifier, 0, 9) = "PXEClient";
   next-server <server-ip>;
   filename "linux-install/pxelinux.0";
}
```

Die IP-Adresse hinter der Option `next-server` sollte die des `tftp`-Servers sein.

15.3. Konfiguration des NFS-Servers

Der gemeinsam benützte nicht-beschreibbare Teil des Operationssystemes wird über NFS gemeinsam benützt.

Konfigurieren Sie NFS so, dass die `root/` und `snapshot/` Verzeichnisse exportiert werden, indem, sie zu `/etc/exports` dazugegeben werden. Zum Beispiel:

```
/diskless/i386/RHEL3-AS/root/     *(ro,sync,no_root_squash)
/diskless/i386/RHEL3-AS/snapshot/ *(rw,sync,no_root_squash)
```

Ersetzen Sie `*` mit einem der Hostnamen-Formate, wie in Abschnitt 23.3.2 besprochen. Machen Sie die Erklärung der Hostnamen so spezifisch wie möglich, damit ungewollte Systeme keinen Zugang zum NFS-Mount haben.

Wenn der NFS-Dienst nicht läuft, starten Sie ihn:

```
service nfs start
```

Wenn der NFS-Dienst bereits läuft, laden Sie die Konfigurationsdatei neu:

```
service nfs reload
```

15.4. Beenden Sie die Konfiguration der plattenlosen Umgebung

Um die grafische Version von **Network Booting Tool** verwenden zu können, müssen Sie das X Window System, sowie Root-Privilegien haben und das `redhat-config-netboot` RPM-Paket installiert haben. Um **Network Booting Tool** vom Desktop aus zu starten, verwenden Sie den **Main Menu Button** (auf der Leiste) **=> System Settings => Server Settings => Network Booting Service**. Oder geben Sie den Befehl `redhat-config-netboot` bei einem Shell-Prompt (zum Beispiel bei einem **XTerm** oder einem **GNOME terminal**) ein.

Wenn Sie **Network Booting Tool** zum ersten Mal starten, wählen Sie **Diskless** vom **First Time Druid**. Oder Sie wählen **Configure => Diskless** aus dem Pulldown-Menü und klicken dann **Add**.

Ein Hilfsprogramm (Wizard) startet, das Sie Schritt für Schritt durch den Installationsprozess führt.

1. Klicken Sie **Forward** auf der erste Seite.
2. Geben Sie einen Namen **Name** und eine Beschreibung **Description**auf der **Diskless Identifier** Seite ein. Klicken Sie **Forward**.
3. Geben Sie die IP-Adresse oder den Domain-Namen des NFS-Servers ein, der in Abschnitt 15.3 konfiguriert ist, sowie das Verzeichnis, das als plattenlose Umgebung exportiert wurde. Klicken Sie **Forward**.
4. Die in der plattenlosen Umgebung installierten Kernel-Versionen werden aufgelistet. Wählen Sie die Kernelversion aus, die Sie am plattenlosen System hochfahren wollen.
5. Klicken Sie **Apply**, um die Konfiguration abzuschließen.

Nachdem Sie **Apply** geklickt haben, werden der plattenlose Kernel und die Image-Datei auf Grundlage des gewählten Kernels erstellt. Sie werden in das PXE-Boot-Verzeichnis `/tftpboot/linux-install/ <os-identifier>/` kopiert. Das Verzeichnis `snapshot/` wird in dem gleichen Verzeichnis erstellt wie das `root/` Verzeichnis (z.B. `/diskless/i386/RHEL3-AS/snapshot/`), mit einer Datei namens `files` darin. Diese Datei enthält eine Liste von Dateien und Verzeichnissen, die für jedes plattenloses System beschreibbar (Read/Write) sein müssen. Ändern Sie diese Datei nicht. Wenn bei der Liste zusätzliche Eintragungen gemacht werden müssen, erstellen Sie eine`files.custom` Datei in dem gleichen Verzeichnis wie die `files` Datei, und fügen Sie jede zusätzliche Datei bzw. jedes zusätzliche Verzeichnis auf einer eigenen Linie hinzu.

15.5. Hinzufügung von Hosts

Jeder plattenlose Client muss sein eigenes *snapshot* Verzeichnis auf dem NFS-Server haben, das als sein beschreibbares Dateisystem verwendet wird. **Network Booting Tool** kann dazu verwendet werden, diese Snapshot-Verzeichnisse zu erstellen.

Nachdem die Schritte in Abschnitt 15.4 fertig gestellt sind, erscheint ein Fenster, mit dem Hosts zu der plattenlosen Umgebung hinzugefügt werden können. Klicken Sie auf den **New** button. Geben Sie die folgende Information in dem Dialogfenster Abbildung 15-1 ein:

- **Hostname or IP Address/Subnet** — Legen Sie den Hostnamen oder die IP-Adresse für ein Systems fest, das als Host in der plattenlosen Umgebung aufgenommen werden soll. Geben Sie ein Subnetz ein, um eine Gruppe von Systemen festzulegen.
- **Operating System** — Wählen Sie die plattenlose Umgebung für den Host oder das Subnetz der Hosts aus.
- **Serial Console** — Kennzeichnen Sie dieses Kästchen, um eine serielle Installation auszuführen.
- **Snapshot name** — Geben Sie einen Namen für ein Unterverzeichnis an, das verwendet wird, um sämtliche beschreibbaren Inhalte für den Host zu speichern.
- **Ethernet** — Wählen Sie das Ethernet-Gerät beim Host aus, um die plattenlose Umgebung zu mounten. Wenn der Host nur eine Ethernetkarte hat, wählen Sie **eth0**.

Ignorieren Sie die **Kickstart File** Option. Sie wird nur für PXE Installationen verwendet.

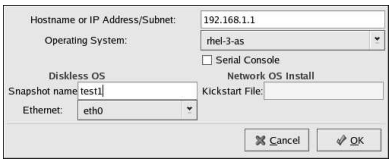

Abbildung 15-1. Hinzufügung von plattenlosen Hosts

Im existierenden `snapshot/` Verzeichnis im plattenlosen Verzeichnis wird ein Unterverzeichnis mit dem **Snapshot name** als festgelegtem Dateinamen erstellt. Dann werden alle Dateien, die in `snapshot/files` und `snapshot/files.custom` aufgelistet sind, vom `root/` Verzeichnis in dieses neue Verzeichnis kopiert.

15.6. Hochfahren der Hosts

Ziehen Sie die Beschreibung Ihrer PXE-Karte zu Rate, wie man den Host zum Hochfahren mit PXE konfiguriert.

Wenn der plattenlose Client hochfährt, mountet er das Remote `root/` Verzeichnis im plattenlosen Verzeichnis als nicht-beschreibbar. Er mountet auch sein individuelles Schnappschuss-Verzeichnis als beschreibbar. Dann mountet er alle Dateien und Verzeichnisse in den `files` und `files.custom` Dateien, indem er `mount -o bind` über dem nicht-beschreibbaren plattenlosen Verzeichnis verwendet, damit die Anwendungen in das Root-Verzeichnis der plattenlosen Umgebung schreiben können, wenn sie müssen.

III. Paket-Management

Jegliche Software auf einem Red Hat Enterprise Linux-System ist in RPM-Pakete unterteilt, die installiert, aktualisiert oder gelöscht werden können. Dieser Teil beschreibt das Management von RPM-Paketen auf einem Red Hat Enterprise Linux-System, unter Verwendung von grafischen und Befehlszeilentools.

Inhaltsverzeichnis

redhat

Kapitel 16.

Paketverwaltung mit RPM

Der RPM Paket-Manager (RPM) ist ein offenes Paketsystem, das für alle Benutzer von Red Hat Enterprise Linux und anderen Linux- und UNIX- Systemen zur Verfügung steht. Red Hat, Inc. ermutigt auch die anderen Distributoren, RPM für ihre Produkte zu verwenden. RPM wird gemäß GPL vertrieben.

RPM erleichtert dem Endanwender das Aktualisieren des Systems. Die Installation, die Deinstallation und das Aktualisieren der RPM-Pakete erfolgt über einfache Befehle. RPM erstellt eine Datenbank der installierten Pakete und ihrer Dateien, so dass Sie effiziente Such- und Prüfvorgänge in Ihrem System vornehmen können. Wenn Sie die grafische Schnittstelle bevorzugen, steht Ihnen **Package Management Tool** mit zahlreichen RPM-Befehlen zur Verfügung.

Während den Aktualisierungsvorgängen behandelt RPM die Konfigurationsdateien mit großer Umsicht, so dass Sie nicht Gefahr laufen, Ihre individuellen Einstellungen zu verlieren — die üblichen `.tar.gz` Dateien gewährleisten dies dagegen nicht.

RPM ermöglicht es dem Entwickler, den Software-Quellcode in die Quell- und Binärpakete für Endanwender zu übernehmen. Hierbei handelt es sich um einen sehr einfachen Prozess, der von einer einzigen Datei und optionalen Korrekturen, die Sie erstellen, ausgeführt wird. Diese klare Darstellung von *ursprünglichen* Quellen und Ihren Korrekturen und Erstellungsanleitungen erleichtert die Wartung des Pakets, wenn neue Software-Versionen herausgegeben werden.

Anmerkung

Da Sie mit RPM Änderungen an Ihrem System vornehmen, müssen Sie als root-Benutzer angemeldet sein, um ein RPM-Paket zu installieren, zu entfernen oder zu aktualisieren.

16.1. Ziele von RPM

Um den Gebrauch von RPM zu verstehen, kann es von Nutzen sein, die konzeptuellen Ziele dieser Anwendung zu betrachten.

Aktualisierbarkeit

Mit RPM können Sie einzelne Komponenten Ihres Systems aktualisieren, ohne Ihr System komplett neu installieren zu müssen. Wenn Sie eine neue Version eines RPM-Betriebssystems (beispielsweise Red Hat Enterprise Linux) besitzen, ist es ebenfalls nicht notwendig, dass Sie Ihr System neu installieren (wie bei Betriebssystemen mit anderen Paketsystemen). RPM ermöglicht intelligente und voll automatische Upgrades Ihres Systems. Die Konfigurationsdateien der Pakete werden dabei beibehalten, so dass Sie Ihre individuellen Einstellungen nicht verlieren. Für die Aktualisierung eines Pakets sind keine speziellen Upgrade-Dateien erforderlich, da dies ebenfalls durch die RPM-Datei erfolgt.

Anfragen von Paketen

RPM bietet leistungsstarke Anfrageoptionen. Sie können dabei in Ihrer gesamten Datenbank nach Paketen oder auch nach bestimmten Dateien suchen. Weiterhin können Sie ganz einfach herausfinden, zu welchem Paket eine Datei gehört und wo der Ursprung des Pakets liegt. Die Dateien, die ein RPM-Paket enthalten, befinden sich in einem komprimierten Archiv. Dieses Archiv beinhaltet einen benutzerdefinierten binären Header, der nützliche Informationen über

das Paket und seinen Inhalt enthält. Mit Hilfe dieses Headers bekommen Sie schnell und einfach Informationen zu den einzelnen Paketen.

System-Prüfung

Ein weiteres leistungsfähiges Feature ist das Prüfen von Paketen. Wenn Sie zum Beispiel nicht sicher sind, ob Sie eine wichtige Datei in einem Paket gelöscht haben, können Sie das Paket überprüfen. Ihnen werden dann jegliche Unstimmigkeiten mitgeteilt. An diesem Punkt können Sie die Pakete wenn nötig neu installieren. Alle Konfigurationsdateien, die Sie geändert haben, werden während einer Neuinstallation erhalten.

Ursprüngliche Quellen

Ein wichtiges konzeptuelles Ziel dieser Anwendung ist es, den Gebrauch von "ursprünglichen" Quellen, wie sie von den Entwicklern der Software herausgegeben wurden, möglich zu machen. Ein RPM-Paket beinhaltet bietet solche ursprünglichen Quellen zusammen mit den verwendeten Korrekturen und den kompletten Erstellungsanleitungen. Dies bedeutet aus mehreren Gründen einen enormen Vorteil. Wenn zum Beispiel eine neue Version eines Programms erscheint, so müssen Sie sie nicht unbedingt unbedingt bei "Null" beginnen, um kompilieren zu können. Sie können die Korrekturen überprüfen, um zu sehen, was Sie *eventuell* tun sollten. Alle einkompilierten Standards und alle Änderungen an der Software können auf diese Weise ganz einfach getrennt voneinander angezeigt werden.

Das Ziel der Beibehaltung der ursprünglichen Quellen mag auf den ersten Blick nur für Entwickler von Bedeutung zu sein, bietet aber auch den Endanwendern eine bessere Softwarequalität. An dieser Stelle möchten wir daher den Mitarbeitern der BOGUS Distribution für die Entwicklung des Konzepts der ursprünglichen Quellen danken.

16.2. Verwenden von RPM

RPM bietet fünf grundlegende Funktionen (wobei die Erstellung von Paketen nicht inbegriffen ist): Installieren, Deinstallieren, Aktualisieren, Anfragen und Prüfen. In diesem Kapitel werden die einzelnen Funktionen näher beschrieben. Detailliertere Informationen und Optionen finden Sie unter `rpm --help` oder Abschnitt 16.5.

16.2.1. Suche nach RPM-Paketen

Bevor Sie ein RPM verwenden, müssen Sie wissen, wo diese zu finden sind. Eine Suche im Internet liefert viele RPM-Repositories. Wenn Sie allerdings RPM-Pakete suchen, die von Red Hat erstellt wurden, können Sie diese an folgenden Orten finden:

- Red Hat Enterprise Linux CD-ROMs
- Red Hat Errata-Seite unter http://www.redhat.com/apps/support/errata/
- Red Hat FTP Mirror-Site unter http://www.redhat.com/download/mirror.html
- Red Hat Network — Siehe Kapitel 18 für Weiteres zu Red Hat Network

16.2.2. Installieren

RPM-Pakete besitzen üblicherweise Dateinamen wie `foo-1.0-1.i386.rpm`, die den Paketnamen (`foo`), die Version (`1.0`), die Release-Nummer (`1`) und die Systemarchitektur (`i386`) enthalten. Zum Installieren eines Pakets müssen Sie sich lediglich als root anmelden und den folgenden Befehl am Shell-Prompt eingeben:

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

Ist die Installation erfolgreich, wird Folgendes ausgegeben:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [100%]
```

RPM gibt den Paketnamen und eine Reihe von Hash-Zeichen auf dem Bildschirm aus, um den Installationsfortschritt anzuzeigen.

Beginnend mit Version 4.1 von RPM wird die Signatur eines Paketes bei der Installation oder Aktualisierung eines Paketes geprüft. Schlägt die Prüfung der Signatur fehl, erscheint eine Fehlermeldung, die wie folgt aussehen kann:

```
error: V3 DSA signature: BAD, key ID 0352860f
```

Handelt es sich um eine neue Signatur, die nur im Header-Bereich vorkommt, erscheint eine Fehlermeldung, die wie folgt aussehen kann:

```
error: Header V3 DSA signature: BAD, key ID 0352860f
```

Haben Sie nicht den richtigen Schlüssel zur Prüfung der Signatur installiert, erscheint in der Nachricht `NOKEY` wie z.B.:

```
warning: V3 DSA signature: NOKEY, key ID 0352860f
```

Unter Abschnitt 16.3 finden Sie weitere Informationen zur Prüfung einer Paketsignatur.

Anmerkung

Zur Installation eines Kernel-Pakets sollten Sie dagegen `rpm -ivh` verwenden. Weitere Details finden Sie unter Kapitel 39.

Die Installation von Paketen ist zwar ein sehr einfacher Vorgang, es können jedoch trotzdem Fehler auftreten:

16.2.2.1. Paket bereits installiert

Falls das Paket derselben Version bereits installiert wurde, erscheint folgende Anzeige:

```
Preparing...                ########################################### [100%]
package foo-1.0-1 is already installed
```

Wenn Sie das Paket dennoch installieren möchten und die gleiche Version, die Sie installieren möchten, bereits installiert ist, können Sie die Option `--replacepkgs` verwenden, mit der RPM angewiesen wird, den Fehler zu ignorieren:

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

Diese Option ist vor allem dann sehr nützlich, wenn die von RPM installierten Dateien gelöscht wurden oder wenn die ursprünglichen Konfigurationsdateien von RPM installiert werden sollen.

16.2.2.2. Dateikonflikte

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

```
Preparing...                ########################################### [100%]
file /usr/bin/foo from install of foo-1.0-1 conflicts with file from package bar-2.0.20
```

Wenn RPM diesen Fehler ignorieren soll, hängen Sie die Option `--replacefiles` an den Befehl an:

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

16.2.2.3. Ungelöste Abhängigkeiten

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

```
Preparing...                ########################################### [100%]
error: Failed dependencies:
        bar.so.2 is needed by foo-1.0-1
    Suggested resolutions:
        bar-2.0.20-3.i386.rpm
```

Installieren Sie ein Paket von den Red Hat Enterprise Linux CD-ROMs, wird normalerweise vorgeschlagen, dass das Paket die Abhängigkeit auflösen. Suchen Sie dieses Paket in den Red Hat Enterprise Linux CD-ROMs oder aus der Red Hat FTP-Site (oder Mirror) und fügen Sie es dem Befehl hinzu:

```
rpm -ivh foo-1.0-1.i386.rpm bar-2.0.20-3.i386.rpm
```

Ist die Installation beider Pakete erfolgreich, erscheint ein Meldung ähnlich Folgender:

```
Preparing...                ########################################### [100%]
   1:foo                    ########################################### [ 50%]
   2:bar                    ########################################### [100%]
```

Wird kein Paket zur Lösung der Abhängigkeit vorgeschlagen, können Sie es mit der Option `--redhatprovides` versuchen, um zu bestimmen in welchem Paket die gewünschte Datei enthalten ist. Damit Sie diese Optionen verwenden können, muss das Paket `rpmdb-redhat` installiert sein.

```
rpm -q --redhatprovides bar.so.2
```

Befindet sich das Paket mit `bar.so.2` in der installierten Datenbank des Pakets `rpmdb-redhat`, wird der Name des Pakets angezeigt:

```
bar-2.0.20-3.i386.rpm
```

Falls Sie jedoch mit der Installation fortfahren möchten (was nicht zu empfehlen ist, da das Paket vermutlich nicht korrekt ausgeführt werden kann), geben Sie an der Befehlszeile `--nodeps` ein.

16.2.3. Deinstallieren

Das Deinstallieren von Paketen ist ebenso einfach wie das Installieren. Geben Sie am Shell-Prompt Folgendes ein:

```
rpm -e foo
```

Anmerkung

Hier wurde der *Paketname* `foo` und nicht der Name der ursprünglichen Paketdatei `foo-1.0-1.i386.rpm` verwendet. Um ein Paket zu deinstallieren, müssen Sie `foo` mit dem tatsächlichen Namen des ursprünglichen Pakets ersetzen.

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

```
Preparing...                ########################################### [100%]
error: removing these packages would break dependencies:
        foo is needed by  bar-2.0.20-3.i386.rpm
```

Wenn Sie möchten, dass RPM diesen Fehler ignoriert und das Paket dennoch deinstalliert (was ebenfalls keine gute Idee ist, da das hiervon abhängige Paket vermutlich nicht korrekt funktionieren wird), hängen Sie die Option `--nodeps` an den Befehl an.

16.2.4. Aktualisieren

Das Aktualisieren von Paketen erfolgt ähnlich wie das Installieren. Geben Sie den folgenden Befehl am Shell-Prompt ein:

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

Was Sie hier nicht sehen, ist, dass RPM automatisch alte Versionen des `foo` Pakets deinstalliert. Sie können jedoch auch die Funktion `-U` zum Installieren von Paketen verwenden, da sie auch funktioniert, wenn keine älteren Versionen des zu installierenden Pakets vorhanden sind.

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

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

Diese Meldung bedeutet, dass Ihre Änderungen an der Konfigurationsdatei mit der neuen Konfigurationsdatei des Pakets nicht "vorwärtskompatibel" sind, und RPM Ihre ursprüngliche Datei gespeichert und eine neue installiert hat. Sie sollten die Differenzen zwischen den beiden Konfigurationsdateien überprüfen und diese so bald wie möglich beheben. Andernfalls besteht das Risiko, dass Ihr System nicht korrekt funktioniert.

Das Aktualisieren ist im Prinzip eine Kombination der Vorgänge Deinstallieren und Installieren. Bei einer RPM-Aktualisierung können daher auch Deinstallations- und Installationsfehler auftreten. Wenn RPM vermutet, dass Sie versuchen, ein Paket mit einer *älteren* Version zu aktualisieren, erscheint folgende Meldung:

```
package foo-2.0-1 (which is newer than foo-1.0-1) is already installed
```

Um mit RPM dennoch eine "Aktualisierung" durchzuführen, hängen Sie die Option `--oldpackage` an den Befehl an:

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

16.2.5. Auffrischen

Das Auffrischen eines Pakets ist dem Aktualisieren sehr ähnlich. Geben Sie den folgenden Befehl am Shell-Prompt ein:

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

Die Option Auffrischen von RPM überprüft die Versionen der in der Befehlszeile angegebenen Pakete und vergleicht sie mit den Versionen der bereits in Ihrem System installierten Pakete. Wenn eine neuere Version eines bereits installierten Pakets von der Option Auffrischen bearbeitet wird, aktualisiert RPM dieses auf die neuere Version. Mit der Option Auffrischen von RPM kann jedoch kein Paket installiert werden, wenn nicht ein bereits zuvor installiertes Paket des gleichen Namens vorhanden ist. Dies ist ein wesentlicher Unterschied zur Funktion Aktualisieren von RPM, da bei einer Aktualisierung *in jedem Fall* Pakete installiert werden, gleichgültig, ob eine ältere Version des Pakets bereits installiert wurde.

Die Option Auffrischen von RPM funktioniert bei einzelnen Paketen oder bei Paketgruppen. Wenn Sie eine große Anzahl verschiedener Pakete heruntergeladen haben und nur die Pakete aktualisieren möchten, die bereits in Ihrem System installiert sind, dann sollten Sie die Funktion des Auffrischens verwenden. Hierbei ist es nicht notwendig, dass Sie unerwünschte Pakete aus der Gruppe entfernen, die Sie zuvor mit dem RPM heruntergeladen haben.

In diesem Fall können Sie den folgenden Befehl eingeben:

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

RPM wird nun automatisch nur die Pakete aktualisieren, die bereits installiert sind.

16.2.6. Anfragen

Anfragen an die Datenbank der installierten Pakete werden mit `rpm -q` durchgeführt. Der Befehl `rpm -q foo` gibt den Namen sowie Versions- und Release-Nummern des installierten Pakets foo aus:

```
foo-2.0-1
```

Anmerkung

Hier wurde der *Paketname* `foo` verwendet. Um ein Paket anzufragen, müssen Sie `foo` mit dem tatsächlichen Namen des Pakets ersetzen.

Statt einen Paketnamen festzulegen, können Sie auch folgende Optionen mit `-q` verwenden, um anzugeben, welche Pakete Sie abfragen möchten. Diese Optionen heißen *Paketspezifizierungsoptionen*.

- `-a` Anfrage zu allen derzeit installierten Paketen.
- `-f <Datei>` Anfrage zu welchem Paket `<Datei>` gehört. Bei der Angabe einer Datei müssen Sie den vollständigen Pfad angeben (zum Beispiel `/usr/bin/ls`).
- `-p <packagefile>` Anfrage an die nicht installierte Paketdatei `<packagefile>`.

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

- `-i` zeigt Paketinformationen, zum Beispiel Name, Beschreibung, Release-Nummer, Größe, Erstellungsdatum, Installationsdatum, Händler und verschiedene andere Informationen.
- `-l` zeigt eine Liste der Dateien an, die im Paket enthalten sind.
- `-s` zeigt den Status aller Dateien des Pakets an.
- `-d` zeigt eine Liste der als Dokumentationen gekennzeichneten Dateien an (man-Seiten, info-Seiten, README- Dateien usw.).
- `-c` zeigt eine Liste der als Konfigurationsdateien gekennzeichneten Dateien an. Dies sind die Dateien, die Sie nach der Installation bearbeiten, um das Paket an Ihr System anzupassen (zum Beispiel `sendmail.cf`, `passwd`, `inittab` etc.).

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

16.2.7. Prüfen

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

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

- So prüfen Sie ein Paket, das eine bestimmte Datei enthält:
  ```
  rpm -Vf /bin/vi
  ```
- So prüfen Sie ALLE installierten Pakete:
  ```
  rpm -Va
  ```
- So prüfen Sie ein installiertes Paket gegenüber einer RPM-Paketdatei:
  ```
  rpm -Vp foo-1.0-1.i386.rpm
  ```
  Dieser Befehl kann nützlich sein, wenn Sie vermuten, dass Ihre RPM-Datenbank beschädigt ist.

Wenn alles überprüft und für korrekt befunden wurde, erfolgt keine weitere Ausgabe. Falls Abweichungen festgestellt wurden, werden diese angezeigt. Das Ausgabeformat besteht aus einer Zeichenkette mit acht Zeichen (`c` kennzeichnet eine Konfigurationsdatei). Jedes der acht Zeichen steht für das Vergleichsergebnis eines Attributs der Datei mit dem aufgezeichneten Wert für dieses Attribut in RPM-Datenbank. Ein einzelner Punkt `.` bedeutet, dass der Test bestanden wurde. Die folgenden Zeichen kennzeichnen Fehler bei bestimmten Tests:

- `5` — MD5 Prüfsumme
- `S` — Dateigröße
- `L` — symbolischer Link
- `T` — Dateibearbeitungszeit
- `D` — Gerät
- `U` — Benutzer
- `G` — Gruppe
- `M` — Modus (einschließlich Berechtigungen und Dateityp)
- `?` — nicht lesbare Datei

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

16.3. Überprüfen der Signatur eines Pakets

Wenn Sie überprüfen möchten, dass ein Paket unbeschädigt ist, prüfen Sie lediglich die MD5-Summe. Geben Sie hierzu den folgenden Befehl am Shell-Prompt ein (<*rpm-file*> mit dem Dateinamen Ihres RPM-Pakets):

```
rpm -K --nogpg <rpm-file>
```

Es erscheint die Meldung <*rpm-file*>: `md5 OK`. Diese kurze Meldung gibt an, dass die Datei beim Herunterladen nicht beschädigt wurde. Soll die Meldung ausführlicher erscheinen, ersetzen Sie im Befehl `-K` mit `-Kvv`.

Aber wie vertrauenswürdig ist der Entwickler des Pakets? Nur wenn das Paket mit dem GnuPG *Schlüssel* des Entwicklers *signiert* wurde, wissen Sie, dass das Paket wirklich vom angegebenen Entwickler stammt.

Ein RPM-Paket kann mithilfe des Gnu Privacy Guard(oder GnuPG) signiert werden, was sicherstellt, dass das heruntergeladene Paket "vertrauenswürdig" ist.

GnuPG ist ein Tool für sichere Kommunikation und stellt einen umfassenden und freien Ersatz für die Verschlüsselungstechnologie von PGP, einem elektronischem Privacy-Programm dar. Mit GnuPG können Sie die Echtheit von Dokumenten überprüfen und Daten für den Austausch mit anderen Benutzern verschlüsseln und entschlüsseln. Das Tool ist auch in der Lage, PGP5.*x* Dateien zu entschlüsseln und zu überprüfen.

Bei der Installation wird GnuPG standardmäßig installiert. Sie können somit GnuPG sofort verwenden, um alle Pakete zu überprüfen, die Sie von Red Hat erhalten haben. Zunächst müssen Sie den öffentlichen Schlüssel von Red Hat importieren.

16.3.1. Importieren von Schlüsseln

Zur Überprüfung offizieller Red Hat Pakete müssen Sie den Red Hat GPG-Schlüssel importieren. Führen Sie dazu folgenden Befehl an einem Shell-Prompt aus:

```
rpm --import /usr/share/rhn/RPM-GPG-KEY
```

Um eine Liste aller zur RPM-Prüfung installierten Schlüssel anzuzeigen, führen Sie folgenden Befehl aus:

```
rpm -qa gpg-pubkey*
```

Für den Red Hat Schlüssel schließt die Ausgabe Folgendes mit ein:

```
gpg-pubkey-db42a60e-37ea5438
```

Verwenden Sie `rpm -qi` um Details zu einem bestimmten Schlüssel anzuzeigen, gefolgt von der Ausgabe des vorhergehenden Befehls:

```
rpm -qi gpg-pubkey-db42a60e-37ea5438
```

16.3.2. Prüfen von Paketen

Um die GnuPG-Signatur einer RPM-Datei zu prüfen, nachdem der GnuPG-Schlüssel des Herstellers importiert wurde, geben Sie den folgenden Befehl ein (ersetzen Sie *<rpm-file>* mit dem Dateinamen des RPM-Paketes):

```
rpm -K <rpm-file>
```

Verläuft der Vorgang problemlos, erscheint die folgende Meldung: `md5 gpg OK`. Dies bedeutet, dass die Signatur des Paketes geprüft wurde und es unbeschädigt ist.

16.4. Weitere Features der RPM

RPM ist ein nützliches Tool für die Verwaltung Ihres Systems und die Ermittlung und Behebung von Problemen. Um diese Anwendung und ihre Optionen besser zu erläutern, sind im Folgenden einige Beispiele aufgeführt.

- Möglicherweise haben Sie unbeabsichtigt einige Dateien gelöscht. Sie sind sich aber nicht sicher, welche. Wenn Sie Ihr gesamtes System prüfen und herausfinden möchten, was genau fehlt, können Sie auch den folgenden Befehl verwenden:
  ```
  rpm -Va
  ```
  Wenn einige Dateien fehlen oder beschädigt sind, sollten Sie das Paket entweder einfach neu installieren oder zunächst deinstallieren und anschließend neu installieren.
- Es könnte vorkommen, dass Sie eine Datei sehen, die Ihnen nicht bekannt ist. Wenn Sie herausfinden möchten, zu welchem Paket sie gehört, geben Sie Folgendes am Shell-Prompt ein:
  ```
  rpm -qf /usr/X11R6/bin/ghostview
  ```
  Es erscheint eine Ausgabe, die etwa wie folgt aussieht:
  ```
  gv-3.5.8-22
  ```
- Diese beiden Beispiele können wie im Folgenden beschrieben kombiniert werden. Angenommen, Sie haben Probleme mit `/usr/bin/paste`. Sie möchten das Paket prüfen, zu dem die Datei gehört, wissen aber nicht, zu welchem Paket `paste` gehört. Geben Sie hierzu den folgenden Befehl ein:
  ```
  rpm -Vf /usr/bin/paste
  ```
  Auf diese Weise wird das entsprechende Paket geprüft.
- Möchten Sie mehr Informationen über ein bestimmtes Programm? Verwenden Sie den folgenden Befehl, um die Dokumentation zu suchen, die mit dem Paket geliefert wurde, das das Programm enthält:
  ```
  rpm -qdf /usr/bin/free
  ```
  Es erscheint eine Ausgabe, die etwa wie folgt aussieht:
  ```
  /usr/share/doc/procps-2.0.11/BUGS
  /usr/share/doc/procps-2.0.11/NEWS
  /usr/share/doc/procps-2.0.11/TODO
  /usr/share/man/man1/free.1.gz
  /usr/share/man/man1/oldps.1.gz
  /usr/share/man/man1/pgrep.1.gz
  /usr/share/man/man1/pkill.1.gz
  /usr/share/man/man1/ps.1.gz
  /usr/share/man/man1/skill.1.gz
  /usr/share/man/man1/snice.1.gz
  /usr/share/man/man1/tload.1.gz
  /usr/share/man/man1/top.1.gz
  /usr/share/man/man1/uptime.1.gz
  /usr/share/man/man1/w.1.gz
  /usr/share/man/man1/watch.1.gz
  ```

```
/usr/share/man/man5/sysctl.conf.5.gz
/usr/share/man/man8/sysctl.8.gz
/usr/share/man/man8/vmstat.8.gz
```

- Sie finden eine neue RPM-Datei, wissen aber nicht, was das Tool genau bietet. Geben Sie den folgenden Befehl ein, um mehr Informationen hierüber zu erhalten:

  ```
  rpm -qip crontabs-1.10-5.noarch.rpm
  ```

  Es erscheint eine Ausgabe, die etwa wie folgt aussieht:

  ```
  Name        : crontabs                     Relocations: (not relocateable)
  Version     : 1.10                              Vendor: Red Hat, Inc.
  Release     : 5                             Build Date: Fri 07 Feb 2003 04:07:32 PM EST
  Install date: (not installed)               Build Host: porky.devel.redhat.com
  Group       : System Environment/Base       Source RPM: crontabs-1.10-5.src.rpm
  Size        : 1004                             License: Public Domain
  Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
  Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
  Summary     : Root crontab files used to schedule the execution of programs.
  Description :
  The crontabs package contains root crontab files. Crontab is the
  program used to install, uninstall, or list the tables used to drive the
  cron daemon. The cron daemon checks the crontab files to see when
  particular commands are scheduled to be executed. If commands are
  scheduled, then it executes them.
  ```

- Jetzt möchten Sie vielleicht sehen, welche Dateien das `crontabs` RPM installiert. Sie würden dann folgendes eingeben:

  ```
  rpm -qlp crontabs-1.10-5.noarch.rpm
  ```

  Es erscheint eine Ausgabe, die etwa wie Folgt aussieht:

  ```
  Name        : crontabs                     Relocations: (not relocateable)
  Version     : 1.10                              Vendor: Red Hat, Inc.
  Release     : 5                             Build Date: Fri 07 Feb 2003 04:07:32 PM EST
  Install date: (not installed)               Build Host: porky.devel.redhat.com
  Group       : System Environment/Base       Source RPM: crontabs-1.10-5.src.rpm
  Size        : 1004                             License: Public Domain
  Signature   : DSA/SHA1, Tue 11 Feb 2003 01:46:46 PM EST, Key ID fd372689897da07a
  Packager    : Red Hat, Inc. <http://bugzilla.redhat.com/bugzilla>
  Summary     : Root crontab files used to schedule the execution of programs.
  Description :
  The crontabs package contains root crontab files. Crontab is the
  program used to install, uninstall, or list the tables used to drive the
  cron daemon. The cron daemon checks the crontab files to see when
  particular commands are scheduled to be executed. If commands are
  scheduled, then it executes them.
  ```

Dies sind nur ein paar Beispiele. Mit dem Gebrauch von RPM werden Sie noch mehr Optionen dieses Tools kennenlernen.

16.5. Zusätzliche Ressourcen

RPM ist ein sehr komplexes Dienstprogramm mit zahlreichen Optionen und Methoden zum Anfragen, Installieren, Aktualisieren und Entfernen von Paketen. Die folgenden Ressourcen bieten Ihnen detailliertere Informationen zu diesem Tool.

16.5.1. Installierte Dokumentation

- `rpm --help` — Dieser Befehl liefert kurze Angaben über die RPM-Parameter.
- `man rpm` — Die man-Seite von RPM liefert Ihnen mehr Details über die RPM-Parameter als der Befehl `rpm --help`.

16.5.2. Hilfreiche Websites

- http://www.rpm.org/ — Die RPM Website.
- http://www.redhat.com/mailing-lists/rpm-list/ — Die RPM Mailing-Liste ist hier gespeichert. Wenn Sie sich registrieren möchten, senden Sie eine E-Mail an <`rpm-list-request@redhat.com`> und geben Sie als Betreff `subscribe` an.

16.5.3. Zusätzliche Literatur

- *Red Hat RPM Guide* von Eric Foster-Johnson; Wiley, John & Sons, Inc. — Dieses Buch ist ein umfassendes Werk zu RPM, vom Installieren von Paketen, zum Erstellen von RPMs.

Kapitel 17.

Package Management Tool

Während der Installation wird eine Vorgabe von Software-Paketen installiert. Da Personen ihren Computer unterschiedlich nutzen, möchten die Benutzer nach der Installation möglicherweise weitere Pakete installieren oder Pakete entfernen. Mit dem **Package Management Tool** sind Benutzer in der Lage, diese Aktionen durchzuführen.

Das X Window System ist für das **Package Management Tool** erforderlich. Um die Applikation zu starten, klicken Sie auf **Hauptmenü** (im Panel) => **Systemeinstellungen** => **Pakete** oder geben Sie den Befehl `redhat-config-packages` an einem Shell-Prompt ein.

Die gleiche Oberfläche erscheint, wenn Sie die Red Hat Enterprise Linux CD-ROM #1 in Ihren Computer einlegen.

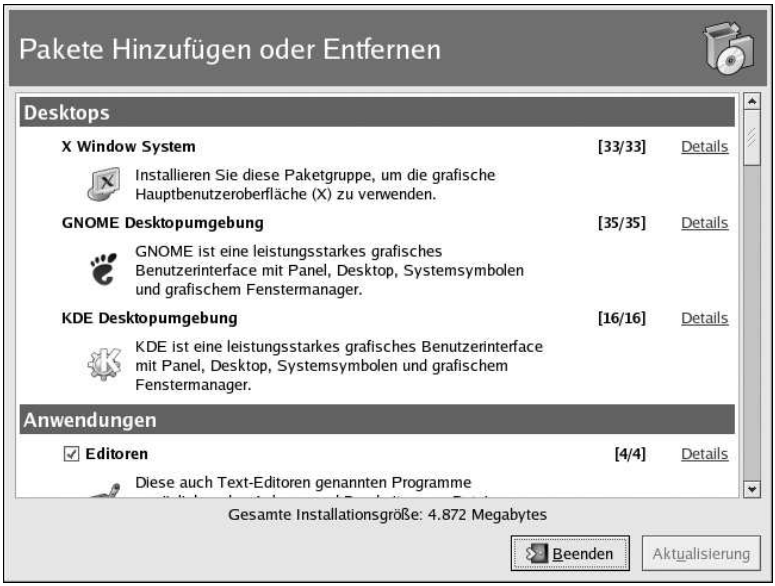

Abbildung 17-1. Package Management Tool

Die Oberfläche für diese Applikation ähnelt der bei der Installation verwendeten Oberfläche. Pakete werden in Paketgruppen eingeteilt. Die Gruppen enthalten eine Liste mit *Standardpaketen* und *Zusatzpaketen*, deren Funktionen ähnlich sind. Die Gruppe **Grafisches Internet** enthält zum Beispiel einen Web-Browser, einen E-Mail-Client und weitere Grafikprogramme, die zur Verbindungsherstellung mit Internet verwendet werden. Diese Standardpakete können nur entfernt werden, wenn die gesamte Paketgruppe entfernt wird. Die Extrapakete sind optionale Pakete, die zur Installation oder Deinstallation ausgewählt werden können. Voraussetzung hierfür ist, dass die Paketgruppe ausgewählt ist.

Das Hauptfenster zeigt eine Liste mit Paketgruppen an. Wenn das Kontrollkästchen neben der Paketgruppe ein Häkchen aufweist, sind Pakete aus dieser Gruppe aktuell installiert. Klicken Sie auf die

Schaltfläche **Details** neben der Paketgruppe, um die Liste mit den einzelnen Paketen für eine Gruppe anzuzeigen. Die einzelnen Pakete, die mit einem Häkchen versehen sind, sind aktuell installiert.

17.1. Installation von Paketen

Markieren Sie das Kontrollkästchen neben einer aktuell nicht installierten Paketgruppe, deren Standardpakete Sie installieren möchten. Klicken Sie auf die Schaltfläche **Details** neben der Paketgruppe, um die Pakete in der Gruppe festzulegen, die installiert werden sollen. Die Liste mit den Standard- und Extrapaketen wird angezeigt (siehe Abbildung 17-2. Wenn Sie auf den Paketnamen klicken, wird der für die Installation des Pakets erforderliche Plattenplatz unten im Fenster angezeigt. Wenn Sie das Kontrollkästchen neben dem Paketnamen markieren, wird das Paket für die Installation vorgesehen.

Sie können einzelne Pakete aus bereits installierten Paketgruppen auswählen, indem Sie auf die Schaltfläche **Details** klicken und ein beliebiges, noch nicht installiertes Extrapaket markieren.

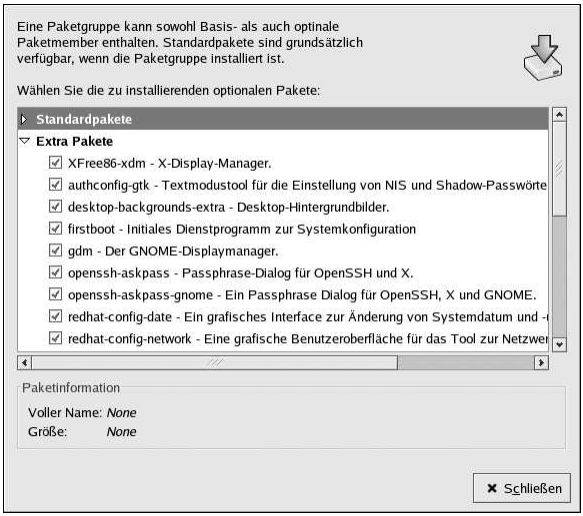

Abbildung 17-2. Auswahl einzelner Pakete

Wenn Sie die zu installierenden Paketgruppen und einzelnen Pakete ausgewählt haben, klicken Sie im Hauptfenster auf die Schaltfläche **Aktualisieren**. Die Anwendung berechnet daraufhin den für die zu installierenden Pakete erforderlichen Plattenplatz wie auch alle Paketabhängigkeiten und zeigt ein Übersichtsfenster an. Wenn Paketabhängigkeiten bestehen, werden sie automatisch zu der Liste mit den zu installierenden Paketen hinzugefügt. Klicken Sie auf die Schaltfläche **Details zeigen**, um die vollständige Liste der Pakete anzuzeigen, die installiert werden sollen.

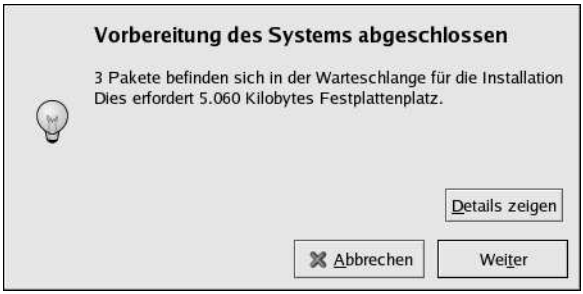

Abbildung 17-3. Übersicht über die Paketinstallation

Klicken Sie auf **Weiter**, um die Installation zu starten. Nach Installationsabschluss wird die Nachricht **Vorbereitung des Systems abgeschlossen** angezeigt.

Tipp

Wenn Sie auf Ihrem Computer zur Datei- und Verzeichnissuche **Nautilus** verwenden, können Sie das Programm auch zum Installieren von Paketen einsetzen. Wechseln Sie in **Nautilus** zu dem Verzeichnis mit einem RPM- Paket (in der Regel weisen die Pakete die Endung `.rpm` auf) und doppelklicken Sie auf das RPM-Symbol.

17.2. Entfernen von Paketen

Deaktivieren Sie das Kontrollkästchen neben der Paketgruppe, deren Pakete Sie entfernen möchten. Wenn Sie einzelne Pakete entfernen möchten, klicken Sie auf die Schaltfläche **Details** neben der Paketgruppe und heben Sie die Markierung der einzelnen Pakete auf.

Wenn Sie die Pakete markiert haben, die deinstalliert werden sollen, klicken Sie im Hauptfenster auf die Schaltfläche **Aktualisieren** Die Anwendung berechnet neben den Softwareabhängigkeiten den Plattenplatz, der freigesetzt wird. Hängen andere Pakete von den Paketen ab, die zur Deinstallation ausgewählt sind, werden die Pakete automatisch zur Liste der zu entfernenden Pakete hinzugefügt. Klicken Sie auf die Schaltfläche **Details zeigen**, um die Liste der Pakete anzuzeigen, die deinstalliert werden sollen.

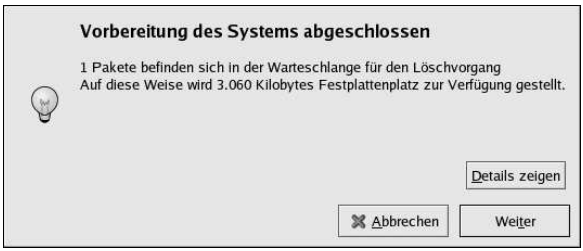

Abbildung 17-4. Übersicht über das Deinstallieren von Paketen

Klicken Sie auf **Weiter**, um die Deinstallation zu starten. Nach Installationsabschluss wird die Nachricht **Vorbereitung des Systems abgeschlossen** angezeigt.

Tipp

Sie können die Installation und Deinstallation von Paketen kombinieren, indem Sie Paketgruppen/Pakete auswählen, die installiert bzw. deinstalliert werden sollen, und anschließend auf die Schaltfläche **Aktualisieren** klicken. Das Fenster **Systemvorbereitung abgeschlossen** zeigt die Anzahl der Pakete an, die installiert bzw. entfernt werden sollen.

Kapitel 18.

Red Hat Network

Red Hat Network ist eine Internet-Lösung für die Verwaltung einer oder mehrerer Red Hat Enterprise Linux-Systeme. Alle Sicherheitswarnungen, Bug-Fixes und Erweiterungen (umfassend unter Errata bekannt) können direkt von Red Hat mittels der Applikation **Red Hat Update Agent** oder über die RHN Webseite unter http://rhn.redhat.com/ heruntergeladen werden.

Abbildung 18-1. Ihr RHN

Red Hat Network spart Zeit, da Benutzer per E-Mail Informationen bei der Herausgabe von aktualisierten Paketen erhalten. Benutzer müssen nicht stundenlang im Internet nach aktualisierten Paketen oder Sicherheitswarnungen suchen. Standardmäßig installiert Red Hat Network diese Pakete auch. Benutzer müssen nicht erst alles über RPMs wissen oder sich um das Lösen von Softwarepaket-Abhängigkeiten kümmern; all dies wird automatisch von RHN übernommen.

Red Hat Network Features enthalten:

- Errata-Warnungen — Seien Sie über die Herausgabe von Sicherheitswarnungen, Bug-Fixes und Erweiterungen für alle Systeme in Ihrem Netzwerk informiert.

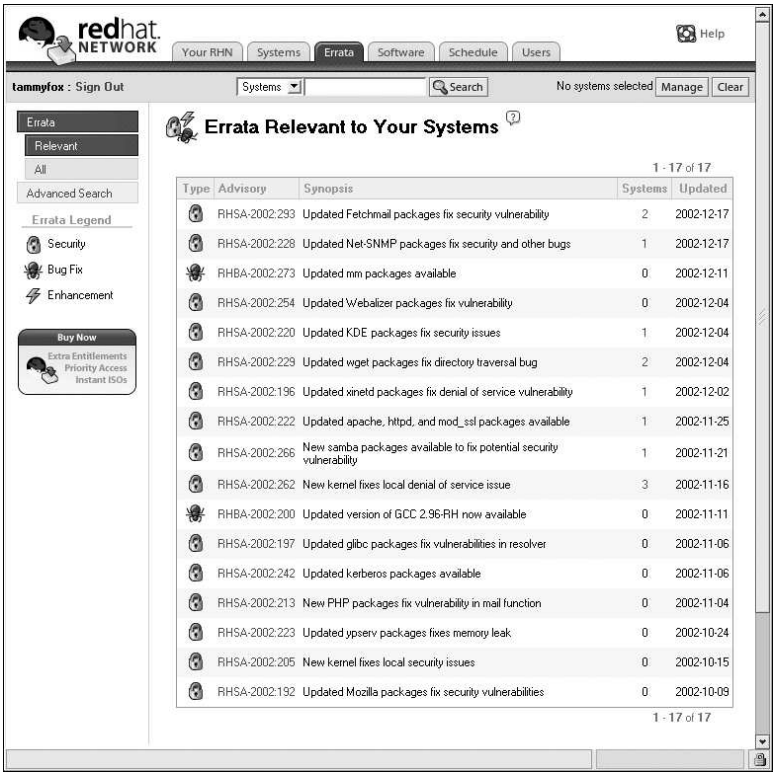

Abbildung 18-2. Wichtige Errata

- Automatische E-Mail Benachrichtigung — Sie erhalten eine E-Mail, sobald eine Errata-Warnung für Ihr System herausgegeben wird
- Geplante Errata Aktualisierungen — Planen Sie das Erhalten von Errata Aktualisierungen
- Paket-Installation — Planen Sie das Installieren von Paketen für ein oder mehrerer Systeme mit einem Klick
- **Red Hat Update Agent** — Verwenden Sie die Applikation **Red Hat Update Agent** zum Herunterladen der neuesten Softwarepakete für Ihr System (Paket-Installation optional)
- Red Hat Network Webseite — Verwalten Sie mehrere Systeme, heruntergeladene Einzelpakete und planen Sie Aktionen wie Errata Aktualisierungen über eine sichere Webbrowser-Verbindung von jedem Computer aus

Achtung

Sie müssen Ihr Red Hat Enterprise Linux Produkt aktivieren, bevor Sie sich beimRed Hat Network registrieren, damit Ihnen die richtigen Services zugewiesen werden können. Um Ihr Produkt zu aktivieren, gehen Sie zu:

```
http://www.redhat.com/apps/activate/
```

Nach der Aktivierung Ihres Produkts, registrieren Sie dies mit Red Hat Network, um Errata Updates zu erhalten. Der Registrierungsprozess sammelt Informationen über das System, das Sie über Updates auf dem laufenden halten wird. Wenn, zum Beispiel, eine Liste von Paketen kompiliert wird, die auf Ihrem System installiert sind, werden Sie nur über Updates dieser Pakete informiert.

Beim Ersten Booten Ihres Systems, wird der **Setup Agent** Sie zur Registrierung auffordern. Sollten Sie sich zu diesem Zeitpunkt nicht registriert haben, wählen Sie **Hauptmenü => Systemtools => Red Hat Network** auf Ihrem Desktop, um die Registrierung durchzuführen. Alternativ, können Sie auch den Befehl `up2date` in einem Shell-Prompt ausführen.

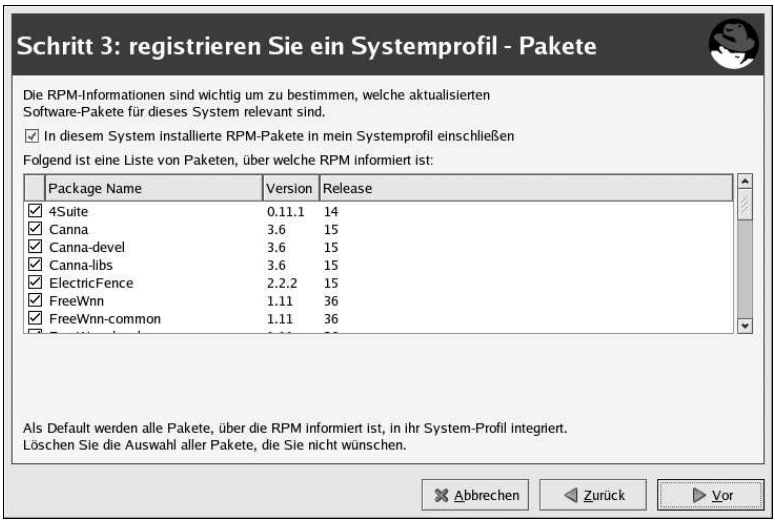

Abbildung 18-3. Beim RHN registrieren

Nach dem Registrieren, benutzen Sie eine der folgenden Methoden, um Updates zu erhalten:

- Wählen Sie **Hauptmenü => Systemtools => Red Hat Network** auf Ihrem Desktop.
- Führen Sie den Befehl `up2date` in einem Shell-Prompt aus.
- Die RHN Website unter https://rhn.redhat.com/.

Für genauere Anleitungen, sehen Sie die Dokumentation unter:

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

Tipp

Red Hat Enterprise Linux enthält das **Red Hat Network Alert Notification Tool**, ein Symbol im Panel, das Ihnen deutlich anzeigt, wenn Aktualisierungen für Ihr Red Hat Enterprise Linux System erhältlich sind.

IV. Netzwerk-bezogene Konfiguration

Nachdem erklärt wird, wie ein Netzwerk konfiguriert wird, beschreibt dieser Abschnitt Netzwerk-bezogene Themen. Darunter fallen Remote-Logins, gemeinsam über ein Netzwerk verwendete (Shared) Dateien und Verzeichnisse und das Einrichten eines Web-Servers.

Inhaltsverzeichnis

Kapitel 19.

Netzwerkkonfiguration

Computer benötigen eine Netzwerkverbindung, um mit anderen Computern kommunizieren zu können. Dies wird dadurch erreicht, dass das Betriebssystem eine Schnittstellenkarte (wie Ethernet, ISDN-Modem oder Token Ring) erkennt und die Schnittstelle für die Verbindung mit dem Netzwerk konfiguriert.

Das **Network Administration Tool** kann für das Konfigurieren folgender Typen von Netzwerkschnittstellen verwendet werden.

- Ethernet
- ISDN
- Modem
- xDSL
- Token Ring
- CIPE
- Wireless-Geräte

Es kann auch dazu verwendet werden, IPsec-Verbindungen zu konfigurieren, DNS-Einstellungen zu verwalten und die Datei `/etc/hosts`, in der zusätzliche Paare von Hostnamen und IP-Adressen gespeichert sind, zu warten.

Um das **Network Administration Tool** verwenden zu können, müssen Sie über Root-Rechte verfügen. Um die Applikation zu starten, klicken Sie auf **Hauptmenü** (im Panel) **=> Systemeinstellungen => Netzwerk** oder geben Sie den Befehl `redhat-config-network` an einem Shell-Prompt ein (zum Beispiel in einem **XTerm** oder einem **GNOME Terminal**). Wenn Sie den Befehl eingeben, wird die grafische Version angezeigt, wenn X ausgeführt wird, ansonsten wird die textbasierte Version ausgeführt. Um das Ausführen der textbasierten Version zu zwingen, geben Sie den folgenden Befehl ein: `redhat-config-network-tui`.

Um die Befehlszeilen-Version zu verwenden, führen Sie den Befehl `redhat-config-network-cmd --help` als root aus, um alle Optionen anzuzeigen.

Abbildung 19-1. Network Administration Tool

Wenn Sie die Konfigurationsdateien lieber direkt modifizieren möchten, finden Sie im *Red Hat Enterprise Linux Referenzhandbuch* weitere Informationen zu Speicherstelle und Inhalten.

Tipp

Rufen Sie die Red Hat Hardware Kompatibilitätsliste (http://hardware.redhat.com/hcl/) ab, um zu ermitteln, ob Red Hat Enterprise Linux Ihr Hardware-Gerät unterstützt.

19.1. Überblick

Führen Sie folgende Schritte aus, um eine Netzwerkverbindung mit dem **Network Administration Tool** durchzuführen:

1. Fügen Sie ein dem physischen Hardware-Gerät zugeordnetes Netzwerkgerät hinzu.
2. Fügen Sie das physische Hardware-Gerät zur Hardwareliste hinzu, sofern noch nicht vorhanden.
3. Konfigurieren Sie den Hostnamen und die DNS-Einstellungen.
4. Konfigurieren Sie die Hosts, die nicht über DNS gesucht werden können.

In diesem Kapitel werden diese Schritte für alle Netzwerkverbindungstypen erläutert.

19.2. Herstellen einer Ethernet-Verbindung

Für das Herstellen einer Internetverbindung benötigen Sie eine Netzwerkschnittstellenkarte (Network Interface Card, NIC), ein Netzwerkkabel (in der Regel ein CAT5-Kabel) und ein Netzwerk. Netzwerke weisen verschiedene Geschwindigkeiten auf; stellen Sie sicher, dass die NIC mit dem Netzwerk kompatibel ist, mit dem Sie eine Verbindung herstellen möchten.

Führen Sie diese Schritte aus, um eine Ethernet-Verbindung hinzuzufügen:

1. Klicken Sie auf das Tab **Geräte**.
2. Klicken Sie auf den Button **Neu**.
3. Wählen Sie **Ethernet-Verbindung** aus der Liste **Gerätetyp** aus und klicken Sie auf **Vor**.
4. Ist die Netzwerkschnittstellenkarte bereits zur Hardwareliste hinzugefügt, wählen Sie sie aus der Liste **Ethernet-Karte** aus. Wählen Sie andernfalls **Andere Ethernet-Karte**, um das Hardware-Gerät hinzuzufügen.

Anmerkung

Das Installationsprogramm erkennt in der Regel die unterstützten Ethernet-Geräte und fordert Sie auf, diese zu konfigurieren. Haben Sie während der Installation Ethernet-Geräte konfiguriert, werden diese in der Hardwareliste auf dem Tab **Hardware** angezeigt.

5. Wenn Sie **Andere Ethernet-Karte** ausgewählt haben, wird das Fenster**Ethernet-Adapter wählen** angezeigt. Wählen Sie den Hersteller und das Modell der Ethernet-Karte aus. Wählen Sie den Gerätenamen aus. Ist dies die erste Ethernet-Karte des Systems, wählen Sie **eth0** als Gerätenamen aus, ist es die zweite Ethernet-Karte, wählen Sie **eth1** aus, usw. Das **Network Administration Tool** ermöglicht Ihnen auch das Konfigurieren der Ressourcen für die NIC. Klicken Sie auf **Vor**, um fortzufahren.
6. Im Fenster **Netzwerkeinstellungen konfigurieren**, wie in Abbildung 19-2 abgebildet, können Sie zwischen DHCP und statischer IP-Adresse wählen. Wenn das Gerät bei jedem Netzwerkstart eine andere IP-Adresse erhält, geben Sie keinen Hostnamen an. Klicken Sie auf **Vor**, um fortzufahren.
7. Klicken Sie auf **Anwenden** auf der Seite **Ethernet-Gerät erstellen**.

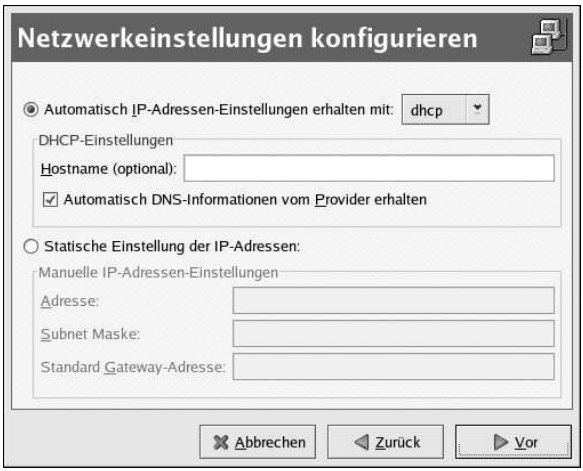

Abbildung 19-2. Etherneteinstellungen

Nach der Konfiguration wird das Ethernet-Gerät in der Geräteliste wie in Abbildung 19-3 angezeigt.

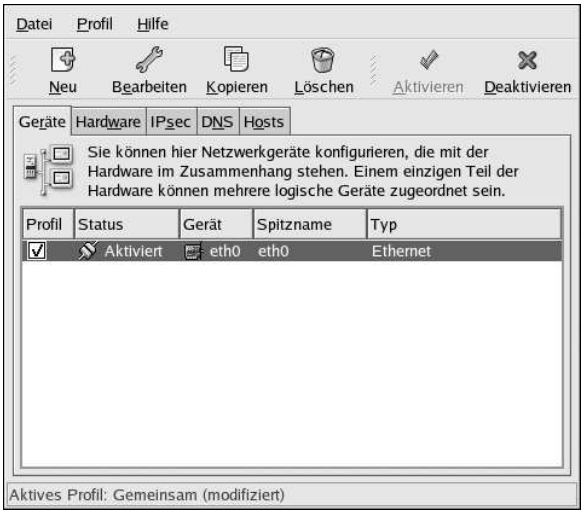

Abbildung 19-3. Ethernet-Gerät

Stellen Sie sicher, dass Sie **Datei => Speichern** gewählt haben, um Änderungen zu speichern.

Nach dem Hinzufügen des Ethernet-Geräts können Sie die Konfiguration bearbeiten, indem Sie das Gerät aus der Geräteliste auswählen und auf **Bearbeiten** klicken. Beispiel: Das hinzugefügte Gerät ist so konfiguriert, dass es zur Bootzeit standardmäßig startet. Sie können den Wert **Gerät beim Starten des Computers aktivieren** bearbeiten, und die Änderungen speichern.

Wenn das Gerät hinzugefügt wurde, wird es nicht sofort aktiviert, wie Sie am **Inaktiv**-Status erkennen können. Um das Gerät zu aktivieren, wählen Sie dieses aus der Liste aus und klicken Sie auf den Button **Aktivieren**. Wenn das System zum Aktivieren des Gerätes beim Starten des Computers konfiguriert wurde (Standard), muss dieser Schritt nicht nocheinmal ausgeführt werden.

Wenn Sie einer Ethernet-Karte mehr als ein Gerät zuordnen, sind die nachfolgenden Geräte *Geräte Aliase*. Ein Geräte Alias ermöglicht Ihnen das Einrichten mehrerer virtueller Geräte für ein physisches Gerät, und gibt damit diesem physischen Gerät mehr als eine IP-Adresse. Sie können z.B. ein eth1 und ein eth1:1 Gerät konfigurieren. Informationen hierzu finden Sie unter Abschnitt 19.13.

19.3. Herstellen einer ISDN-Verbindung

Eine ISDN-Verbindung ist eine Internetverbindung, die mit einer ISDN- Modemkarte über eine spezielle Telefonleitung hergestellt wird, die von einer Telefongesellschaft installiert wurde. In Europa sind ISDN-Verbindungen weit verbreitet.

Führen Sie diese Schritte aus, um eine ISDN-Verbindung hinzuzufügen:

1. Klicken Sie auf das Tab **Geräte**.
2. Klicken Sie auf den Button **Neu**.
3. Wählen Sie **ISDN-Verbindung** aus der Liste **Gerätetyp** aus und klicken Sie auf **Vor**.
4. Wählen Sie den ISDN-Adapter aus dem Pull-Down-Menü aus. Konfigurieren Sie dann die Ressourcen und das D-Channel-Protokoll für den Adapter. Klicken Sie auf **Vor**, um fortzufahren.

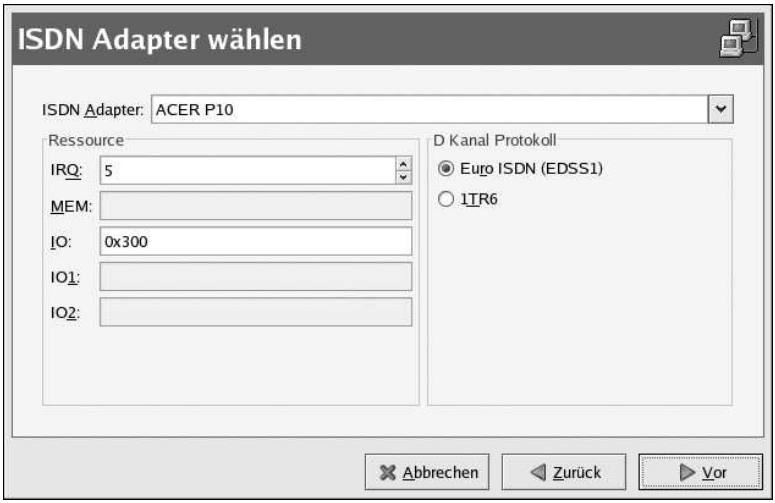

Abbildung 19-4. ISDN-Einstellungen

5. Wenn Ihr Internet Service Provider (ISP) in der vorkonfigurierten Liste genannt wird, wählen Sie diesen aus. Geben Sie andernfalls die erforderlichen Informationen über Ihren ISP-Account ein. Wenn Sie die Werte nicht kennen, wenden Sie sich bitte an Ihren ISP. Klicken Sie auf **Vor**.
6. Wählen Sie im Fenster **IP-Einstellungen** den **Kapselungsmodus**, und ob Sie eine IP-Adresse über DHCP erhalten oder eine statisch einstellen wollen. Klicken Sie wenn Sie fertig sind auf **Vor**.
7. Klicken Sie auf der Seite **Dialup-Verbindung erstellen** auf **Anwenden**.

Nachdem Sie das ISDN-Gerät konfiguriert haben, erscheint es in der Geräteliste als Gerätetyp **ISDN** wie in Abbildung 19-5 abgebildet.

Stellen Sie sicher, dass Sie **Datei => Speichern** gewählt haben, um Änderungen zu speichern.

Nachdem Sie das ISDN-Gerät hinzugefügt haben, können Sie dessen Konfiguration ändern, in dem Sie das Gerät aus der Geräteliste auswählen und auf **Bearbeiten** klicken. Wenn zum Beispiel das Gerät hinzugefügt wurde, ist es automatisch so konfiguriert, dass es standardmäßig nicht beim Booten startet. Bearbeiten Sie die Konfiguration, um diese Einstellungen zu ändern. Sie können z.B. die Kompression, PPP-Optionen, Login-Namen, Passwörter und vieles mehr ändern.

Wenn das Gerät hinzugefügt wurde, wird es nicht sofort aktiviert, wie Sie am **Inaktiv**-Status erkennen können. Um das Gerät zu aktivieren, wählen Sie dieses aus der Liste aus und klicken Sie auf den Button **Aktivieren**. Wenn das System zum Aktivieren des Gerätes beim Starten des Computers konfiguriert wurde (Standard), muss dieser Schritt nicht nocheinmal ausgeführt werden.

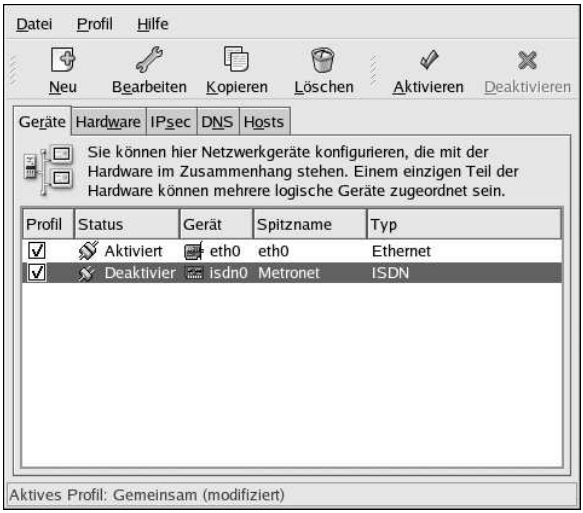

Abbildung 19-5. ISDN-Gerät

19.4. Herstellen einer Modem-Verbindung

Ein Modem kann zum Konfigurieren einer Internetverbindung über eine aktive Telefonleitung verwendet werden. Ein ISP-Account (auch Einwählkonto) ist erforderlich.

Führen Sie diese Schritte aus, um eine Modem-Verbindung hinzuzufügen:

1. Klicken Sie auf das Tab **Geräte**.
2. Klicken Sie auf den Button **Neu**.
3. Wählen Sie **Modemverbindung** aus der Liste **Gerätetyp** aus und klicken Sie auf **Vor**.
4. Ist bereits ein Modem in der Hardwareliste konfiguriert, (auf dem **Hardware** Tab), nimmt das **Network Administration Tool** an, dass Sie dieses zum Erstellen einer Internetverbindung verwenden wollen. Ist noch kein Modem konfiguriert, wird versucht, etwaige Modems im System zu erkennen. Dies kann eine Weile dauern. Wird kein Modem gefunden, wird eine Mitteilung angezeigt, dass die angezeigten Einstellungen nicht auf durch den Test herausgefunden wurden.
5. Nach der Prüfung wird das Fenster in Abbildung 19-6 angezeigt.

Abbildung 19-6. Modem-Einstellungen

6. Konfigurieren Sie die Baudrate, Datenflusssteuerung und Modemlautstärke. Wenn Sie die Werte nicht kennen, übernehmen Sie die Standardwerte. Wenn Sie keine Tonwahlverwendung haben, heben Sie die Markierung des entsprechenden Kontrollkästchens auf. Klicken Sie auf **Vor**.
7. Wenn Ihr ISP in der vorkonfigurierten Liste genannt wird, wählen Sie diesen aus. Geben Sie andernfalls die erforderlichen Informationen über Ihren ISP-Account ein. Wenn Sie die Werte nicht kennen, wenden Sie sich bitte an Ihren ISP. Klicken Sie auf **Vor**.
8. Wählen Sie auf der Seite **IP-Einstellungen** ob Sie eine IP-Adresse automatisch erhalten oder statisch setzen möchten. Klicken Sie dann auf **Vor**.
9. Klicken Sie auf der Seite **Dialup-Verbindung erstellen** auf **Anwenden**.

Nach der Konfiguration wird das Modem in der Gerätelistemit dem Gerätetyp `Modem` wie in Abbildung 19-7 abgebildet angezeigt.

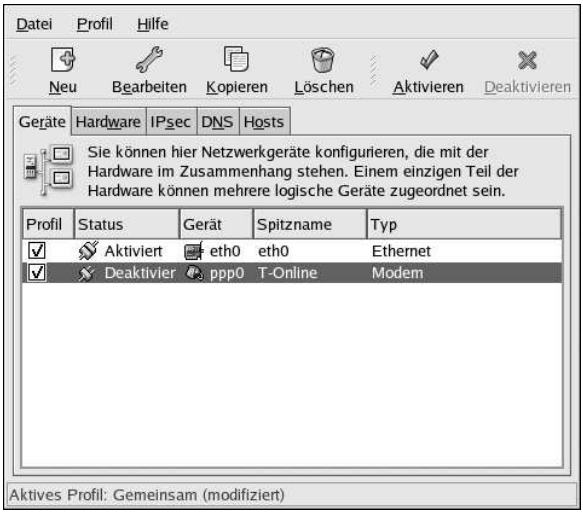

Abbildung 19-7. Modem

Stellen Sie sicher, dass Sie **Datei => Speichern** gewählt haben, um Änderungen zu speichern.

Nach dem Hinzufügen des Modems können Sie die Konfiguration bearbeiten, indem Sie das Gerät aus der Geräteliste auswählen und auf **Bearbeiten** klicken. Beispiel: Das hinzugefügte Gerät ist so konfiguriert, dass es zur Bootzeit standardmäßig nicht startet. Bearbeiten Sie die Konfiguration, um diese Einstellung zu modifizieren. Sie können auch Komprimierung, PPP-Optionen, Anmeldenamen, Passwort und vieles mehr ändern.

Wenn das Gerät hinzugefügt wurde, wird es nicht sofort aktiviert, wie Sie am **Inaktiv**-Status erkennen können. Um das Gerät zu aktivieren, wählen Sie dieses aus der Liste aus und klicken Sie auf den Button **Aktivieren**. Wenn das System zum Aktivieren des Gerätes beim Starten des Computers konfiguriert wurde (Standard), muss dieser Schritt nicht nocheinmal ausgeführt werden.

19.5. Herstellen einer xDSL-Verbindung

DSL steht für Digital Subscriber Lines. Es gibt verschiedene Arten von DSL wie zum Beispiel ADSL, IDSL und SDSL. Das **Network Administration Tool** verwendet den Begriff xDSL, um alle Arten von DSL-Verbindungen zu bezeichnen.

Manche DSL-Anbieter fordern Sie auf, Ihr System zu konfigurieren, um über DHCP eine IP-Adresse mit einer Ethernet-Karte zu erhalten. Manche DSL-Anbieter fordern Sie auf, eine PPPoE-Verbindung (Point-to-Point Protocol over Ethernet) mit einer Ethernet-Karte zu konfigurieren. Fragen Sie Ihre DSL-Anbieter, welche Methode Sie verwenden sollten.

Wenn Sie zum Verwenden von DHCP aufgefordert werden, lesen Sie Abschnitt 19.2, um die Ethernet-Karte zu konfigurieren.

Wenn Sie PPPoE verwenden sollen, befolgen Sie diese Schritte:

1. Klicken Sie auf das Tab **Geräte**.
2. Klicken Sie auf den Button **Hinzufügen**.
3. Wählen Sie **xDSL-Verbindung** aus der Liste **Gerätetyp** aus und klicken Sie auf **Vor**.

4. Wenn sich die Ethernet-Karte bereits auf der Hardwareliste befindet, wählen Sie **Ethernet-Gerät** aus dem Pull-Down-Menü auf der in Abbildung 19-8 abgebildeten Seite aus. Andernfalls wird das Fenster **Ethernet-Adapter wählen** angezeigt.

Anmerkung

Das Installationsprogramm erkennt in der Regel die unterstützten Ethernet-Geräte und fordert Sie auf, diese zu konfigurieren. Haben Sie während der Installation Ethernet-Geräte konfiguriert, werden diese in der Hardwareliste auf dem Tab **Hardware** angezeigt.

Abbildung 19-8. xDSL-Einstellungen

5. Wird das Fenster **Ethernet-Adapter wählen** angezeigt, wählen Sie den Hersteller und das Modell der Ethernet-Karte aus. Wählen Sie den Gerätenamen aus. Ist dies die erste Ethernet-Karte des Systems, wählen Sie **eth0** als Gerätenamen aus, ist es die zweite Ethernet-Karte, wählen Sie **eth1** (usw.). Das **Network Administration Tool** ermöglicht Ihnen auch das Konfigurieren der Ressourcen für die NIC. Klicken Sie auf **Vor**, um fortzufahren.
6. Geben Sie den **Providername**, **Anmeldename** und **Passwort** ein. Wenn Sie einen T-Online Account haben, klicken Sie anstelle von **Anmeldename** und **Passwort** im Standardfenster auf **T-Online Zugangsdatenformular** und geben Sie die benötigten Informationen ein. Klicken Sie auf **Vor**.
7. Klicken Sie auf der Seite **DSL Verbindung erstellen** auf **Anwenden**.

Nach der Konfiguration der DSL-Verbindung wird diese in der Geräteliste wie in Abbildung 19-7 angezeigt.

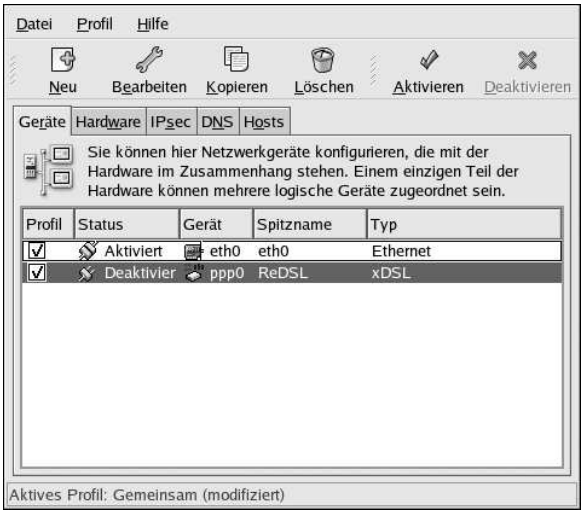

Abbildung 19-9. xDSL-Gerät

Stellen Sie sicher, dass Sie **Datei => Speichern** gewählt haben, um Änderungen zu speichern.

Nach dem Hinzufügen der xDSL-Verbindung können Sie die Konfiguration bearbeiten, indem Sie das Gerät aus der Geräteliste auswählen und auf **Bearbeiten** klicken. Beispiel: Das hinzugefügte Gerät ist so konfiguriert, dass es zur Bootzeit standardmäßig nicht startet. Bearbeiten Sie die Konfiguration, um diese Einstellung zu modifizieren.

Wenn das Gerät hinzugefügt wurde, wird es nicht sofort aktiviert, wie Sie am **Inaktiv**-Status erkennen können. Um das Gerät zu aktivieren, wählen Sie dieses aus der Liste aus und klicken Sie auf den Button **Aktivieren**. Wenn das System zum Aktivieren des Gerätes beim Starten des Computers konfiguriert wurde (Standard), muss dieser Schritt nicht nocheinmal ausgeführt werden.

19.6. Herstellen einer Token Ring-Verbindung

Ein Token Ring-Netzwerk ist ein Netzwerk, in dem alle Computer kreisförmig miteinander verbunden sind. Ein *Token*, oder ein spezielles Netzwerkpaket, bewegt sich durch den Token Ring und ermöglicht den Computern das Senden von Informationen untereinander.

Tipp

Weitere Informationen zur Verwendung eines Token Ring unter Linux finden Sie auf der *Linux Token Ring Project*-Web-Site unter http://www.linuxtr.net/.

Führen Sie diese Schritte aus, um eine Token Ring-Verbindung hinzuzufügen:

1. Klicken Sie auf das Tab **Geräte**.
2. Klicken Sie auf den Button **Neu**.
3. Wählen Sie **Token Ring-Verbindung** aus der Liste **Gerätetyp** aus und klicken Sie auf **Vor**.

4. Ist die Token Ring-Karte bereits zur Hardwareliste hinzugefügt, wählen Sie diese aus der Liste **Ethernet-Karte** aus. Wählen Sie andernfalls **Andere Token Ring-Karte**, um das Hardware-Gerät hinzuzufügen.

5. Wenn Sie **Andere Token Ring-Karte** ausgewählt haben, wird das **Token Ring-Adapter wählen** wie in Abbildung 19-10 angezeigt. Wählen Sie Hersteller und Modell des Adapters aus. Wählen Sie den Gerätenamen aus. Ist dies die erste Token Ring-Karte des Systems, wählen Sie **tr0**; aus, wenn es die zweite ist, wählen Sie **tr1** (usw.). Das **Network Administration Tool** ermöglicht dem Benutzer auch das Konfigurieren der Ressourcen für den Adapter. Klicken Sie auf **Vor**, um fortzufahren.

Abbildung 19-10. Token Ring-Einstellungen

6. Wählen Sie auf der Seite **Netzwerkeinstellungen konfigurieren** zwischen DHCP und einer statischen IP-Adresse aus. Sie können einen Hostnamen für das Gerät angeben. Wenn das Gerät bei jedem Netzwerkstart eine dynamische IP-Adresse erhält, geben Sie keinen Hostnamen an. Klicken Sie auf **Vor**, um fortzufahren.

7. Klicken Sie auf **Anwenden** auf der **Neues Token Ring-Gerät erstellen** Seite.

Nach der Konfiguration wird das Token Ring-Gerät in der Geräteliste wie in Abbildung 19-11 angezeigt.

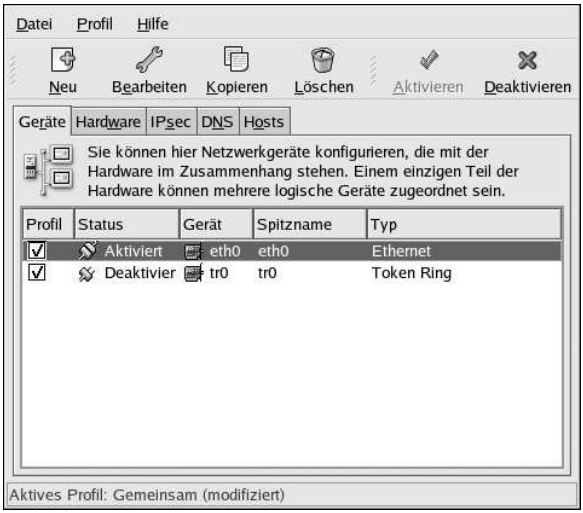

Abbildung 19-11. Token Ring-Gerät

Stellen Sie sicher, dass Sie **Datei => Speichern** gewählt haben, um Änderungen zu speichern.

Nach dem Hinzufügen des Geräts können Sie die Konfiguration bearbeiten, indem Sie das Gerät aus der Geräteliste auswählen und auf **Bearbeiten** klicken. So können Sie zum Beispiel konfigurieren, ob das Gerät zur Bootzeit gestartet wird.

Wenn das Gerät hinzugefügt wurde, wird es nicht sofort aktiviert, wie Sie am **Inaktiv**-Status erkennen können. Um das Gerät zu aktivieren, wählen Sie dieses aus der Liste aus und klicken Sie auf den Button **Aktivieren**. Wenn das System zum Aktivieren des Gerätes beim Starten des Computers konfiguriert wurde (Standard), muss dieser Schritt nicht nocheinmal ausgeführt werden.

19.7. Herstellen einer CIPE-Verbindung

CIPE steht für Crypto IP Encapsulation (IP-Verschlüsselung). Es wird zum Konfigurieren eines IP-Tunneling-Geräts verwendet. CIPE kann zum Beispiel zum Gewähren von externem Zugriff auf ein VPN (Virtual Private Network, virtuelles privates Netzwerk) verwendet werden. Wenn Sie ein CIPE-Gerät einrichten müssen, wenden Sie sich wegen der korrekten Werte bitte an Ihren Systemadministrator.

Führen Sie diese Schritte aus, um eine CIPE-Verbindung zu konfigurieren:

1. Klicken Sie auf das Tab **Geräte**.
2. Klicken Sie auf den Button **Neu**.
3. Wählen Sie **CIPE-Verbindung** aus der Liste **Gerätetyp** aus und klicken Sie auf **Vor**.

   Fragen Sie Ihren Systemadministrator nach den zu verwendenden Werten.

Abbildung 19-12. CIPE-Einstellungen

4. Klicken Sie auf **Anwenden** auf der Seite **CIPE-Verbindung erstellen**.

Nach der Konfiguration wird das CIPE-Gerät in der Geräteliste wie in Abbildung 19-13 angezeigt.

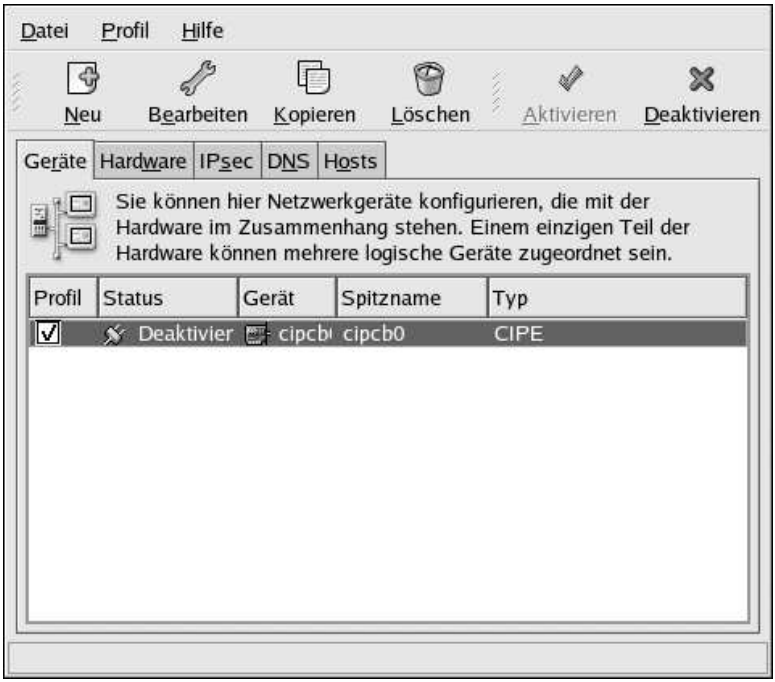

Abbildung 19-13. CIPE-Gerät

Stellen Sie sicher, dass Sie **Datei => Speichern** gewählt haben, um Änderungen zu speichern.

Nach dem Hinzufügen des Geräts können Sie die Konfiguration bearbeiten, indem Sie das Gerät aus der Geräteliste auswählen und auf **Bearbeiten** klicken. So können Sie zum Beispiel konfigurieren, ob das Gerät zur Bootzeit gestartet wird und die zu verwendenden Routen, während das Gerät aktiv ist.

Wenn das Gerät hinzugefügt wurde, wird es nicht sofort aktiviert, wie Sie am **Inaktiv**-Status erkennen können. Um das Gerät zu aktivieren, wählen Sie dieses aus der Liste aus und klicken Sie auf den Button **Aktivieren**. Wenn das System zum Aktivieren des Gerätes beim Starten des Computers konfiguriert wurde (Standard), muss dieser Schritt nicht nocheinmal ausgeführt werden.

Tipp

Weitere Informationen zu CIPE und das Einstellen von CIPE finden Sie im *Red Hat Enterprise Linux Sicherheitshandbuch*.

19.8. Herstellen einer Wireless-Verbindung

Kabellose Ethernet-Geräte werden immer beliebter. Die Konfiguration ähnelt der Ethernetkonfiguration. Allerdings können Sie zum Beispiel SSID oder den Schlüssel für das Wireless-Gerät konfigurieren.

Führen Sie diese Schritte aus, um eine Wireless-Ethernet-Verbindung hinzuzufügen:

1. Klicken Sie auf das Tab **Geräte**.
2. Klicken Sie auf den Button **Neu**.
3. Wählen Sie **Wireless-Verbindung** aus der Liste **Gerätetyp** aus und klicken Sie auf **Vor**.
4. Ist die Wireless-Netzwerkschnittstellenkarte bereits zur Hardwareliste hinzugefügt, wählen Sie diese aus der Liste **Ethernet-Karte** aus. Wählen Sie andernfalls **Andere Wireless-Karte**, um das Hardware-Gerät hinzuzufügen.

Anmerkung

Das Installationsprogramm erkennt in der Regel die unterstützten Wireless-Ethernet- Geräte und fordert Sie auf, diese zu konfigurieren. Wurden diese während der Installation konfiguriert, werden sie bereits auf dem **Hardware** Tab angezeigt.

5. Wenn Sie **Andere Wireless-Karte** ausgewählt haben, erscheint das **Ethernet-Adapter wählen** Fenster. Wählen Sie den Hersteller und das Modell der Ethernet-Karte und des Gerätes aus. Wenn dies die erste Ethernet-Karte des Systems ist, wählen Sie **eth0** aus, wenn es die zweite ist, **eth1** (usw.). Das **Network Administration Tool** ermöglicht Ihnen auch das Konfigurieren der Ressourcen für die Wireless-Netzwerkschnittstellenkarte. Klicken Sie auf **Vor**, um fortzufahren.
6. Auf der Seite **Wireless-Verbindungen konfigurieren** wie in Abbildung 19-14 abgebildet, konfigurieren Sie die Einstellungen für das Wireless-Gerät.

Abbildung 19-14. Wireless-Einstellungen

7. Wählen Sie auf der Seite **Netzwerkeinstellungen konfigurieren** zwischen DHCP und einer statischen IP-Adresse aus. Sie können einen Hostnamen für das Gerät angeben. Wenn das Gerät bei jedem Netzwerkstart eine dynamische IP-Adresse erhält, geben Sie keinen Hostnamen an. Klicken Sie auf **Vor**, um fortzufahren.
8. Klicken Sie auf **Anwenden** auf der Seite **Wireless-Geräte erstellen**.

Nach der Konfiguration wird das Wireless-Gerät in der Geräteliste wie in Abbildung 19-15 angezeigt.

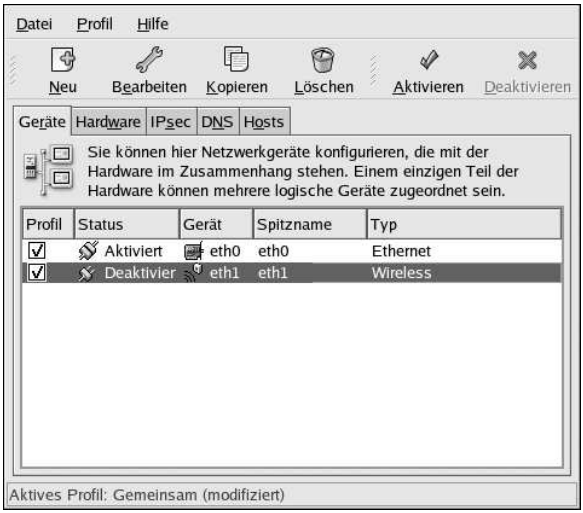

Abbildung 19-15. Wireless-Geräte

Stellen Sie sicher, dass Sie **Datei => Speichern** gewählt haben, um Änderungen zu speichern.

Nach dem Hinzufügen des Wireless-Geräts können Sie die Konfiguration bearbeiten, indem Sie das Gerät aus der Geräteliste auswählen und auf **Bearbeiten** klicken. So können Sie das Gerät zum Beispiel so konfigurieren, dass es zur Bootzeit aktiviert wird.

Wenn das Gerät hinzugefügt wurde, wird es nicht sofort aktiviert, wie Sie am **Inaktiv**-Status erkennen können. Um das Gerät zu aktivieren, wählen Sie dieses aus der Liste aus und klicken Sie auf den Button **Aktivieren**. Wenn das System zum Aktivieren des Gerätes beim Starten des Computers konfiguriert wurde (Standard), muss dieser Schritt nicht nocheinmal ausgeführt werden.

19.9. Verwalten von DNS-Einstellungen

Mit dem Tab **DNS** können Sie den Hostnamen, Domäne, Namenserver und Suchdomänen des Systems konfigurieren. Nameserver werden zum Suchen anderer Hosts auf dem Netzwerk verwendet.

Wenn die DNS-Servernamen von DHCP oder PPPoE abgerufen (oder von einem ISP), dürfen Sie keine primären, sekundären oder tertiären DNS-Server hinzufügen.

Wurde der Hostname dynamisch von DHCP oder PPPoE (oder vom ISP) abgerufen, ändern Sie diesen nicht.

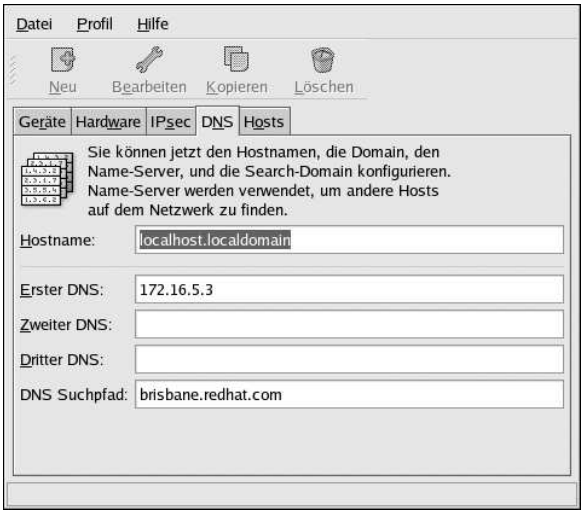

Abbildung 19-16. DNS-Konfiguration

Anmerkung

Der Abschnitt Nameserver konfiguriert nicht das das gesamte System als Nameserver. Es wird stattdessen konfiguriert, welche Nameserver zum Lösen von IP-Adressen zu Hostnamen und umgekehrt verwendet werden sollen.

19.10. Verwalten von Hosts

Mit dem Tab **Hosts** können Sie Hosts zur Datei `/etc/hosts` hinzufügen, bearbeiten oder entfernen. Diese Datei enthält IP-Adressen und die jeweiligen Hostnamen.

Versucht Ihr System, einen Hostnamen bei einer IP-Adresse aufzulösen oder den Hostnamen für eine IP-Adresse festzulegen, greift es auf die Datei `/etc/hosts` zu, ehe es die Nameserver verwendet (wenn Sie die Standardkonfiguration von Red Hat Enterprise Linux verwenden). Wird die IP-Adresse in der Datei `/etc/hosts` genannt, werden die Nameserver nicht verwendet. Befinden sich in Ihrem Netzwerk Computer, deren IP-Adressen nicht in DNS genannt werden, ist es empfehlenswert, sie zu `/etc/hosts` hinzuzufügen.

Um einem Eintrag zur Datei `/etc/hosts` hinzuzufügen, gehen Sie zum **Hosts** Tab, klicken Sie auf **Neu** geben Sie benötigten Informationen ein und klicken auf **OK**. Wählen Sie **Datei => Speichern** oder drücken Sie [Strg]-[S], um die Änderungen in der Datei `/etc/hosts` zu speichern. Das Netzwerk oder die Netzwerkservices müssen nicht neu gestartet werden, da jedes Mal, wenn eine Adresse gelöst wird, auf die aktuelle Version der Datei verwiesen wird.

Warnung

Entfernen Sie nicht den Eintrag `localhost`. Auch wenn das System keine Netzwerkverbindung oder keine Dauerverbindung ins Netzwerk hat, müssen sich einige Programme über die localhost Loopback-Schnittstelle mit dem System verbinden.

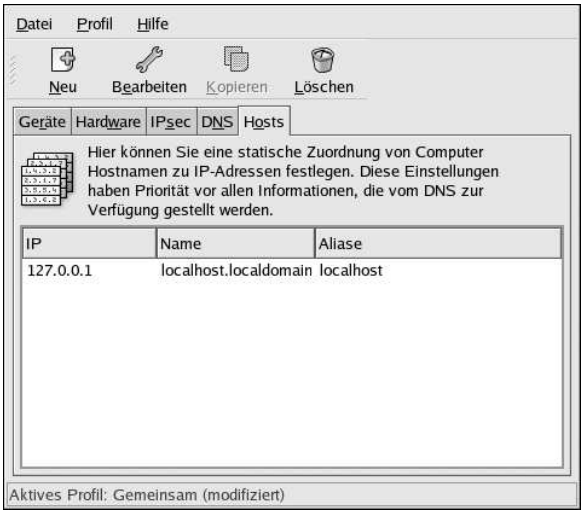

Abbildung 19-17. Hostkonfiguration

Tipp

Um die Suchreihenfolge zu ändern, bearbeiten Sie die Datei `/etc/host.conf`. Die Zeile `order hosts, bind` gibt an, dass `/etc/hosts` Vorrang vor dem Nameserver hat. Wenn Sie die Zeile in `order bind, hosts` ändern, konfiguriert dies das System zum Lösen der Hostnamen und IP-Adressen mittels des Nameservers. Kann die IP-Adresse nicht über den Nameserver gelöst werden, sucht das System nach der IP-Adresse in der Datei `/etc/hosts`.

19.11. Geräte aktivieren

Netzwerkgeräte können entweder so konfiguriert werden, dass sie beim Booten aktiviert werden oder nicht beim Booten starten. Zum Beispiel ein Netzwerkgerät für eine Modemverbindung wird normalerweise nicht so konfiguriert, dass sie beim Booten startet, während eine Ethernet-Verbindung so konfiguriert wird, dass sie beim Booten startet. Ist ihr Netzwerkgerät so konfiguriert, dass es nicht beim Booten startet, können Sie das **Red Hat Control Network** Programm verwenden, um es nach dem Booten zu aktivieren. Wählen Sie zum Starten **Hauptmenü** (im Panel) => **Systemtools** => **Netzwerkgeräte-Kontrolle** oder geben Sie den Befehl `redhat-control-network` ein.

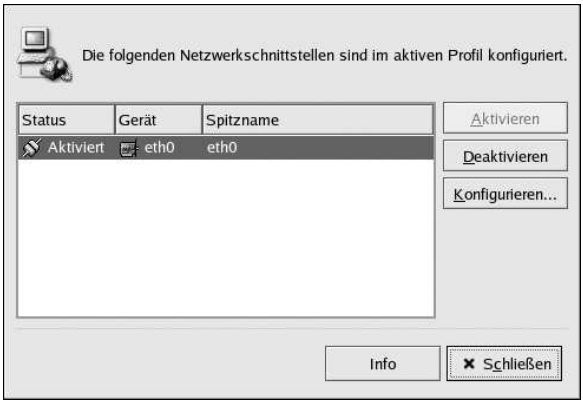

Abbildung 19-18. Geräte aktivieren

Aktivieren Sie ein Gerät, indem Sie es aus der Liste auswählen und auf den Button **Aktivieren** klicken. Stoppen Sie das Gerät, indem Sie es aus der Liste auswählen und auf **Deaktivieren** klicken.

Ist mehr als ein Netzwerk-Profil konfiguriert, werden diese in der Schnittstelle aufgelistet und können aktiviert werden. Weitere Informationen finden Sie unter Abschnitt 19.12.

19.12. Arbeiten mit Profilen

Für jedes physische Hardware-Gerät können mehrere logische Netzwerkgeräte erstellt werden. Besitzt Ihr System zum Beispiel eine Ethernet-Karte (eth0), können Sie logische Netzwerkgeräte mit unterschiedlichen Beinamen und Konfigurationsoptionen erstellen, die alle mit eth0 zusammenhängen.

Logische Netzwerkgeräte unterscheiden sich von Geräte-Aliasen. Logische Netzwerkgeräte, die mit dem gleichen physischen Gerät verbunden sind, müssen in unterschiedlichen Profilen vorhanden sein und können nicht gleichzeitig aktiviert werden. Geräte-Aliase sind auch mit dem gleichen physischen Hardware-Gerät verbunden, können jedoch zur gleichen Zeit aktiviert werden. Weitere Einzelheiten zur Erstellung von Geräte-Aliasen finden Sie unter Abschnitt 19.13.

Profile können dazu benutzt werden, mehrere Konfigurationssets für unterschiedliche Netzwerke zu erstellen. Ein Konfigurationsset kann logische Geräte beinhalten sowie Hosts und DNS-Einstellungen. Nachdem Sie die Profile konfiguriert habe, können Sie das **Network Administration Tool** verwenden, um zwischen diesen hin und her zu schalten.

Standardmäßig gibt es ein Profil mit dem Namen **Allgemein**. Legen Sie ein neues Profil an, indem Sie **Profil => Neu** aus dem Pull-Down-Menü auswählen und einen einmaligen Namen für dieses Profil eingeben.

Sie ändern nun das neue Profil wie in der Statuszeile unten im Hauptfenster angegeben.

Klicken Sie auf ein bestehendes Gerät in der Liste, und klicken Sie dann auf **Kopieren**, um das bestehende Gerät in ein logisches Netzwerkgerät zu kopieren. Wenn Sie den Button **Neu** verwenden, wird ein Netzwerk-Alias erstellt, der nicht korrekt ist. Um die Eigenschaften des logischen Geräts zu ändern, wählen Sie dieses aus der Liste aus, und klicken Sie auf **Bearbeiten**. Es kann zum Beispiel der Nickname in einen eindeutigeren Namen wie zum Beispiel **`eth0_office`** geändert werden, damit dieser einfacher erkannt werden kann.

In der Geräteliste befindet sich eine Spalte mit Kontrollkästchen mit der Kennung **Profil**. Sie können für jedes Profil Geräte ankreuzen bzw. die Auswahl entfernen. Nur die angekreuzten Geräte werden für die derzeit ausgewählten Profile mit eingeschlossen. Wenn Sie zum Beispiel ein logisches Gerät

mit dem Namen **eth0_office** in einem Profil **Office** erstellt haben, und das logische Gerät aktiviert werden soll, wenn das Profil ausgewählt wird, heben Sie die Auswahl von `eth0` auf und markieren Sie stattdessen `eth0_office`.

Abbildung 19-19 zeigt zum Beispiel ein Profil mit dem Namen **Office** mit dem logischen Gerät **eth0_office**. Es ist so konfiguriert, dass es die erste Ethernet-Karte anhand von DHCP aktiviert.

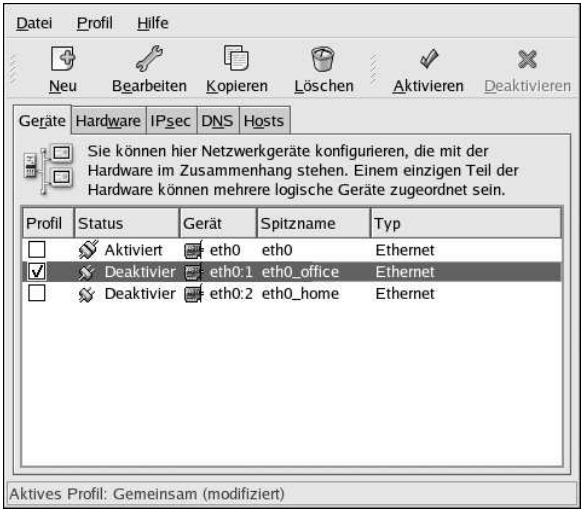

Abbildung 19-19. Office-Profil

Beachten Sie, dass das Profil **Home** wie in Abbildung 19-20 gezeigt das logische Gerät **eth0_home** aktiviert, das mit `eth0` verbunden ist.

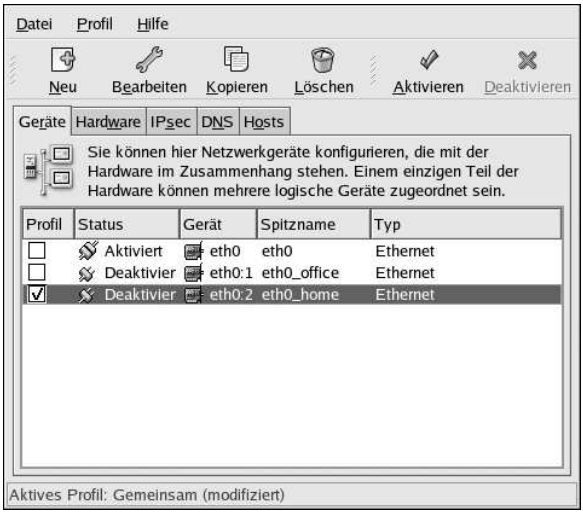

Abbildung 19-20. Home-Profil

Sie können `eth0` auch so konfigurieren, dass es nur im **Office**-Profil aktiviert wird und ein PPP (Modem) Gerät nur im **Home**-Profil. Eine andere Möglichkeit wäre, dass das **Allgemein**-Profil `eth0` aktiviert, und ein **Away**-Profil auf Reisen ein PPP-Gerät aktiviert.

Um ein Profile zur Bootzeit zu aktivieren, ändern Sie die Konfigurationsdatei des Bootloaders, um die Option `netprofile=<`*`profilename`*`>` zu enthalten. Wenn das System, zum Beispiel, GRUB als Bootloader verwendet und `/boot/grub/grub.conf` Folgendes enthält:

```
title Red Hat Enterprise Linux (2.4.21-1.1931.2.399.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-1.1931.2.399.ent ro root=LABEL=/
        initrd /initrd-2.4.21-1.1931.2.399.ent.img
```

ändern Sie dies wie Folgt (ersetzen Sie <*profilname*> mit dem Namen des Profils, dass zur Bootzeit aktiviert werden soll):

```
title Red Hat Enterprise Linux (2.4.21-1.1931.2.399.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-1.1931.2.399.ent ro root=LABEL=/ netprofile=<profilename>
        initrd /initrd-2.4.21-1.1931.2.399.ent.img
```

Um Profile nach dem Booten zu wechseln, gehen Sie zu **Hauptmenü** (im Panel) => **Systemtools** => **Netzwerkgerät-Kontrolle** (oder geben Sie den Befehl `redhat-control-network` ein), um ein Profil auszuwählen und zu aktivieren. Der Abschnitt für das aktivierte Profil erscheint nur in der **Network Device Control** Schnittstelle wenn mehr als die standardmäßige **Allgemein**-Schnittstelle bestehen.

Alternativ dazu können Sie den folgenden Befehl ausführen, um ein Profil zu aktivieren (ersetzen Sie <*Profilname*> mit dem Namen des Profils):

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

19.13. Geräte-Aliase

Geräte-Aliase sind virtuelle Geräte, die mit der gleichen physischen Hardware verbunden sind, jedoch gleichzeitig aktiviert werden können, um unterschiedliche IP-Adressen zu haben. Sie werden normalerweise mit dem Gerätennahmen gefolgt von einem Doppelpunkt und einer Zahl dargestellt (zum Beispiel eth0:1). Sie sind dann von Nutzen, wenn Sie mehr als eine IP-Adresse für ein System möchten, das System jedoch nur eine Netzwerkkarte besitzt.

Nachdem Sie ein Ethernet-Gerät wie `eth0` zur Verwendung einer statischen IP-Adresse konfiguriert haben (DHCP funktioniert nicht mit Aliasen), gehen Sie zum Tab **Geräte** und klicken Sie auf **Neu**. Wählen Sie die Ethernet-Karte, die mit einem Alias konfiguriert werden soll, geben Sie eine statische IP-Adresse für den Alias an und klicken Sie auf **Anwenden**, um diese zu erstellen. Da das Gerät bereits für diese Ethernet-Karte besteht, ist das eben erstellte der Alias, wie z.B. `eth0:1`.

Warnung

Wenn Sie ein Ethernet-Gerät konfigurieren, um einen Alias zu erhalten, können weder das Gerät noch der Alias zur Verwendung von DHCP konfiguriert werden. Sie müssen Sie IP-Adressen manuell konfigurieren.

Abbildung 19-21 zeigt ein Beispiel eines Alias für ein `eth0`-Gerät. Beachten Sie das Gerät `eth0:1` — der erste Alias für `eth0`. Der zweite Alias für `eth0` hätte den Gerätenamen `eth0:2`, usw. Zur Änderung der Einstellungen für den Geräte-Alias wie das Aktivieren beim Booten oder die Alias-Zahl, wählen Sie diesen aus der Liste und klicken Sie auf den Button **Bearbeiten**.

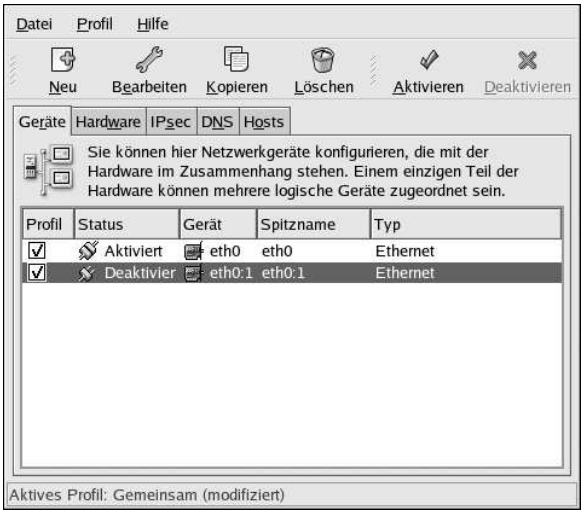

Abbildung 19-21. Beispiel eines Netzwerkgerätalias

Wählen Sie den Alias und klicken Sie auf den Button **Aktivieren**, um den Alias zu aktivieren. Haben Sie mehrere Profile konfiguriert, wählen Sie in welchen Profilen dieser enthalten sein soll.

Prüfen Sie anhand des Befehls `/sbin/ifconfig`, dass der Alias tatsächlich aktiviert wurde. Der Ausdruck sollte das Gerät und den Geräte-Alias mit unterschiedlichen IP-Adressen enthalten:

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

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

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

19.14. Herstellen einer IP-Verbindung

IPsec steht für *Internet Protocol Security*. Es ist eine VPN-Lösung (Virtual Private Network), in der eine verschlüsselte Verbindung zwischen zwei Systemen aufgebaut wird (*host-to-host*) oder zwischen zwei Netzwerken (*network-to-network*).

Tipp

Gehen Sie zu http://www.ipsec-howto.org/ für weitere Informationen zu IPsec.

19.14.1. Host-zu-Host-Verbindung

Eine Host-zu-Host IPsec-Verbindung ist eine verschlüsselte Verbindung zwischen zwei Systemen, die beide IPsec mit dem selben Authentifizierungs-Schlüssel laufen lassen. Mit der IPsec-Verbindung aktiv, ist jeglicher Netzwerkverkehr zwischen zwei Hosts verschlüsselt.

Um eine Host-zu-Host IPsec-Verbindung zu konfigurieren, benutzen Sie die folgenden Schritte auf jedem Host:

1. Starten Sie **Network Administration Tool**.
2. In der **IPsec**-Tab, wählen Sie **Neu**.
3. Klicken Sie **Vor**, um mit der Konfiguration einer Host-zu-Host IPsec-Verbindung zu beginnen.
4. Geben Sie einen aus einem einzelnen Wort bestehenden Namen, wie **`ipsec0`**, für die Verbindung an, und wählen Sie, ob die Verbindung beim Starten des Computers automatisch aktiviert werden soll. Klicken Sie **Vor**.
5. Wählen Sie **Host zu Host Verschlüsselung** als Verbindungstyp und klicken Sie auf **Vor**.
6. Wählen Sie den Verschlüsselungstyp: Manuell oder Automatisch.

Wenn manuell gewählt ist, muss später ein Verschlüsselungsschlüssel angegeben werden. Wenn automatisch gewählt ist, wird der `racoon`-Daemon diesen Schlüssel verwalten. Sollte `racoon` verwendet werden, muss das Paket `ipsec-tools` installiert werden.

Klicken Sie auf **Vor** um fortzufahren.

7. Geben Sie die IP-Adresse des anderen Host an.

   Wenn Ihnen die IP-Adresse des anderen Systems nicht bekannt ist, führen Sie den Befehl `/sbin/ifconfig <device>` auf dem anderen System aus, wobei `<device>` das Ethernet-Gerät ist, mit dem Sie zum anderen Host verbinden. Wenn lediglich eine Ethernet-Karte auf dem System ist, ist der Gerätename eth0. Die IP-Adresse ist die Nummer hinter der Bezeichnung `inet addr:`.

   Klicken Sie auf **Vor** um fortzufahren.

8. Wenn manuelle Verschlüsselung in Schritt 6 gewählt wurde, geben Sie den Verschlüsselungsschlüssel an, oder **Erstellen** Sie einen neuen.

   Geben Sie den Authentifizierungsschlüssel an, oder **Erstellen** Sie einen neuen. Dieser kann jegliche Kombination von Zahlen und Buchstaben sein.

   Klicken Sie auf **Vor** um fortzufahren.

9. Prüfen Sie die Informationen auf der Seite **IPsec — Zusammenfassung** und klicken Sie **Anwenden**.

10. Wählen Sie **Datei => Speichern**, um die Konfiguration zu sichern.

11. Wählen Sie die IPsec-Verbindung aus der Liste und klicken Sie auf **Aktivieren**.

12. Wiederholen Sie dies für die anderen Hosts. Es ist sehr wichtig, dass der selbe Schlüssel wie in Schritt 8 verwendet wird, ansonsten wird IPsec nicht funktionieren.

Nach der Konfiguration der IPsec-Verbindung wird diese in der IPsec-Liste erscheinen, wie in Abbildung 19-7 gezeigt.

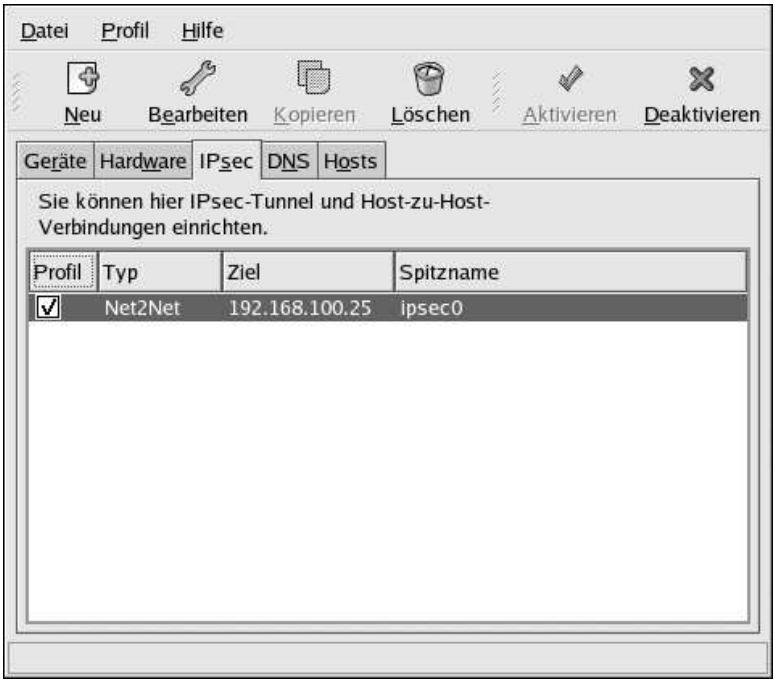

Abbildung 19-22. IPsec-Verbindung

Zwei Dateien werden in `/etc/sysconfig/network-scripts/` erzeugt — `ifcfg-<`*`nickname`*`>` und `keys-<`*`nickname`*`>`. Ist automatische Verschlüsselung gewählt, wird zusätzlich `/etc/racoon/racoon.conf` erzeugt.

Wenn das Interface aktiviert wird, werden `<`*`remote-ip`*`>.conf` und `psk.txt` in `/etc/racoon/` erzeugt und `racoon.conf` wird modifiziert, um `<`*`remote-ip`*`>.conf` zu enthalten.

Sehen Sie Abschnitt 19.14.3, um zu bestimmen, ob die IPsec-Verbindung erfolgreich aufgebaut wurde.

19.14.2. Netzwerk-zu-Netzwerk (VPN) verbindung

Eine Netzwerk-zu-Netzwerk IPsec-Verbindung verwendet zwei IPsec Router, einen pro Netzwerk, durch welche der Netzwerkverkehr für private Subnetze geleitet wird.

Wie in Abbildung 19-23 gezeigt, wenn, zum Beispiel, das 192.168.0/24 private Netzwerk Pakete zum 192.168.2.0/24 privaten Netzwerk senden will, gehen diese Pakete über gateway0, zum ipsec0, über das Internet, zum ipsec1, über gateway1 und dann zum 192.168.2.0/24 Subnetz.

Die IPsec-Router müssen öffentliche IP-Adressen haben, wie auch mit deren privaten Netzwerken verbunden Ethernet-Geräte. Netzwerkverkehr gelangt lediglich durch, wenn dieser für den anderen IPsec Router bestimmt ist, mit dem eine verschlüsselte Verbindung besteht.

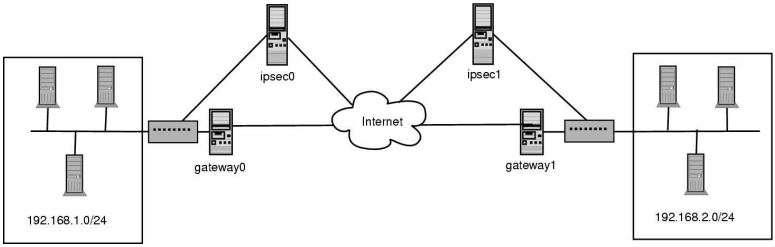

Abbildung 19-23. Netzwerk-zu-Netzwerk IPsec

Alternative Netzwerk-Konfigurationsoptionen schließen eine Firewall zwischen den IPsec-Routern und dem Internet ein und eine Intranet-Firewall zwischen den IPsec-Routern und den Subnetz-Gateways. Der IPsec-Router und der Gateway für das Subnetz kann ein System mit zwei Ethernet-Geräten sein, wobei das eine eine öffentliche IP-Adresse hat, die als IPsec-Router agiert und das andere eine private IP-Adresse, die als Gateway zum privaten Subnetz agiert. Jeder IPsec-Router kann den Gateway für sein privates Netzwerk verwenden oder einen öffentlichen Gateway, um Pakete zum anderen IPsec-Router zu senden.

Führen Sie folgende Schritte aus, um eine Netzwerk-zu-Netzwerk IPsec-Verbindung zu konfigurieren:

1. Starten Sie **Network Administration Tool**.
2. In der **IPsec**-Tab, wählen Sie **Neu**.
3. Klicken Sie **Vor**, um mit der Konfiguration einer Netzwerk-zu-Netzwerk IPsec-Verbindung zu beginnen.
4. Geben Sie einen aus einem einzelnen Wort bestehenden Namen, wie **`ipsec0`**, für die Verbindung an, und wählen Sie, ob die Verbindung beim Starten des Computers automatisch aktiviert werden soll. Klicken Sie **Vor**.
5. Wählen Sie **Netzwerk zu Netzwerk Verschlüsselung (VPN)** und klicken Sie **Vor**.
6. Wählen Sie den Verschlüsselungstyp: Manuell oder Automatisch.

   Wenn manuell gewählt ist, muss später ein Verschlüsselungsschlüssel angegeben werden. Wenn automatisch gewählt ist, wird der `racoon`-Daemon diesen Schlüssel verwalten. Sollte `racoon` verwendet werden, muss das Paket `ipsec-tools` installiert werden. Klicken Sie **Vor** um fortzufahren.
7. Auf der Seite **Lokales Netzwerk**, geben Sie folgende Informationen ein:
   - **Lokale Netzwerk-Adresse** — Die IP-Adresse des Geräts auf dem IPsec-Router, das mit dem private Netzwerk verbunden ist.
   - **Lokale Subnet-Maske** — Die Subnetz-Maske der IP-Adresse des lokalen Netzwerks.
   - **Lokaler Netzwerk-Gateway** — Der Gateway für das private Subnetz.

   Klicken Sie auf **Vor** um fortzufahren.

Abbildung 19-24. Informationen zum lokalen Netzwerk

8. Auf der Seite **Remote-Netzwerk**, geben Sie folgende Informationen ein:

   - **Remote IP-Adresse** — Die öffentliche IP-Adresse des IPsec-Router für das *andere* private Netzwerk. In unserem Beispiel, geben Sie die öffentliche IP-Adresse von ipsec1 für ipsec0 ein, und umgekehrt.
   - **Remote Netzwerk-Adresse** — Die Netzwerk-Adresse des privaten Subnetz hinter dem *anderen* IPsec-Router. In unserem Beispiel, geben Sie `192.168.1.0` bei ipsec1 ein und `192.168.2.0` bei ipsec0.
   - **Remote Subnet-Maske** — Die Subnetz-Maske der Remote IP-Adresse.
   - **Remote Netzwerk-Gateway** — Die IP-Adresse des Gateway für die Remote Netzwerk-Adresse.
   - Wenn manuelle Verschlüsselung in Schritt 6 gewählt wurde, geben Sie den Verschlüsselungsschlüssel an, oder **Erstellen** Sie einen neuen.

     Geben Sie den Authentifizierungsschlüssel an, oder **Erstellen** Sie einen neuen. Dieser kann jegliche Kombination von Zahlen und Buchstaben sein.

   Klicken Sie auf **Vor** um fortzufahren.

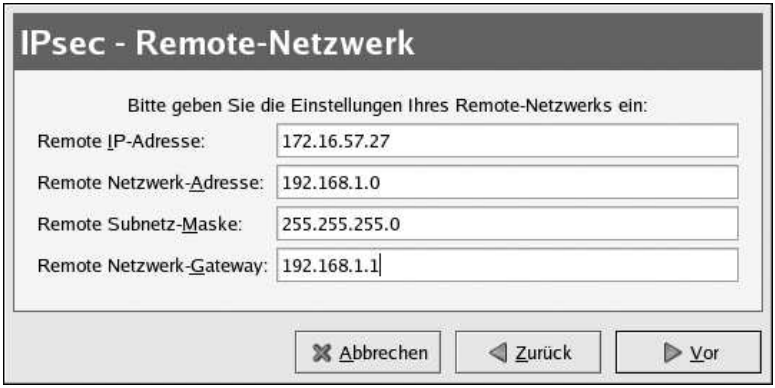

Abbildung 19-25. Informationen zum Remote-Netzwerk

9. Prüfen Sie die Informationen auf der Seite **IPsec — Zusammenfassung** und klicken Sie **Anwenden**.
10. Wählen Sie **Datei => Speichern**, um die Konfiguration zu sichern.
11. Wählen Sie die IPsec-Verbindung aus der Liste und klicken Sie auf **Aktivieren**.
12. Aktivieren Sie IP-Forwarding als root am Shell-Prompt:
    a. Bearbeiten Sie `/etc/sysctl.conf` und setzen `net.ipv4.ip_forward` auf **`1`**.
    b. Geben Sie den folgenden Befehl ein, damit die Änderung in Kraft tritt:
    ```
    sysctl -p /etc/sysctl.conf
    ```

Das Netzwerk-Skript zur Aktivierung der IPsec-Verbindung erzeugt die Routen über das Netzwerk automatisch, falls erforderlich, um Pakete über den IPsec-Router zu senden.

Sehen Sie Abschnitt 19.14.3, um zu bestimmen, ob die IPsec-Verbindung erfolgreich aufgebaut wurde.

19.14.3. Testen der IPsec-Verbindung

Verwenden Sie das `tcpdump`-Utility, um die zwischen den Hosts (oder Netzwerken) übertragenen Netzwerkpakete anzusehen und zu prüfen, ob diese über IPsec verschlüsselt wurden. Die Pakete sollten einen AH-Header enthalten und als ESP-Pakete angezeigt sein. ESP heisst, diese sind verschlüsselt. Zum Beispiel:

```
17:13:20.617872 pinky.example.com > ijin.example.com: \
     AH(spi=0x0aaa749f,seq=0x335): ESP(spi=0x0ec0441e,seq=0x335) (DF)
```

19.14.4. Starten und Beenden einer Verbindung

Sollte die IPsec-Verbindung nicht dazu konfiguriert gewesen sein, zu Bootzeit zu aktivieren, starten und beenden Sie diese als root über die Befehlszeile.

Um die Verbindung aufzubauen, geben Sie den folgenden Befehl auf jedem Host (für Host-zu-Host IPsec) oder jedem IPsec-Router (für Netzwerk-zu-Netzwerk IPsec) ein (<*ipsec-nick*> ist hierbei mit dem vorher konfigurierten Namen, wie `ipsec0`, zu ersetzen):

```
/sbin/ifup <ipsec-nick>
```

Um die Verbindung abzubauen, geben Sie den folgenden Befehl auf jedem Host (für Host-zu-Host IPsec) oder jedem IPsec-Router (für Netzwerk-zu-Netzwerk IPsec) ein (<*ipsec-nick*> ist hierbei mit dem vorher konfigurierten Namen, wie `ipsec0`, zu ersetzen):

```
/sbin/ifdown <ipsec-nick>
```

19.15. Sichern und Wiederherstellen der Netzwerkkonfiguration

Die Befehlszeilen-Version von **Network Administration Tool** kann verwendet werden, um die Netzwerkkonfiguration des Systems in einer Datei zu sichern. Diese Datei kann später verwendet werden, um die Netzwerk-Einstellungen eines Red Hat Enterprise Linux Systems wiederherzustellen.

Dieses Feature kann als Teil eines automatisierten Backup-Skripts verwendet werden, um die Konfiguration vor einem Upgrade oder einer Neuinstallation zu sichern, oder die Konfiguration zu einem anderen Red Hat Enterprise Linux System zu kopieren.

Um die Netzwerkkonfiguration des Systems zur Datei `/tmp/network-config` zu speichern, oder zu *exportieren*, führen Sie folgenden Befehl als root aus:

```
redhat-config-network-cmd -e > /tmp/network-config
```

Um die Netzwerkkonfiguration des Systems aus der im vorhergehenden Schritt erzeugten Datei wiederherzustellen, oder zu *importieren*, führen Sie folgenden Befehl als root aus:

```
redhat-config-network-cmd -i -c -f /tmp/network-config
```

Die Option `-i` ist für das Importieren von Daten, die Option `-c` ist für das Löschen der bestehenden Konfiguration vor dem Importieren und die Option `-f` gibt die zu importierende Datei an.

Kapitel 20.

Basiskonfiguration der Firewall

Ebenso wie eine Feuerwand in einem Gebäude die Ausbreitung eines Feuers verhindert, dient die Firewall in einem Computer als Schutz vor der Verbreitung von Viren und vor unbefugtem Zugriff auf Ihren Computer. Die Firewall befindet sich zwischen Ihrem Computer und dem Netzwerk. Sie bestimmt, auf welche Dienste auf Ihrem Computer Remote-Benutzer vom Netzwerk aus zugreifen können. Eine korrekt konfigurierte Firewall kann die Sicherheit Ihres Systems erheblich verbessern. Wir empfehlen Ihnen, für jedes Red Hat Enterprise Linux System mit Internet-Verbindung eine Firewall zu konfigurieren.

20.1. Security Level Configuration Tool

Im Bildschirm **Firewall-Konfiguration** können Sie während der Installation von Red Hat Enterprise Linux die Firewall aktivieren und bestimmte Geräte, Services und Ports von den Firewall-Regeln ausschließen.

Nach der Installation können Sie diese Einstellungen mithilfe von **Security Level Configuration Tool** ändern.

Um die Anwendung zu starten, wählen Sie **Hauptmenü** (im Panel) => **Systemeinstellungen** => **Sicherheitslevel** oder geben Sie den Befehl `redhat-config-securitylevel` von einem Shell-Prompt aus ein (zum Beispiel in einem Xterm- oder einem GNOME-Terminal).

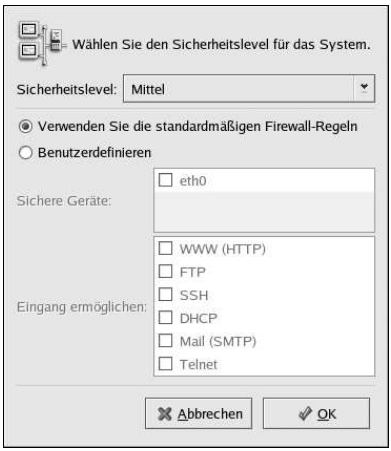

Abbildung 20-1. Security Level Configuration Tool

Anmerkung

Das **Security Level Configuration Tool** konfiguriert nur eine einfache Firewall. Muss das System Zugang zu bestimmten Ports erlauben oder verweigern können, oder benötigt es komplexere Regeln,

lesen Sie bitte das *Red Hat Enterprise Linux Referenzhandbuch* für weitere Informationen zu Konfiguration spezifischer `iptables`-Regeln.

Wählen Sie eine der folgenden Optionen:

- **Firewall deaktivieren** — Wenn Sie keine Firewall einrichten, erlauben Sie den ungehinderten Zugriff auf Ihr System ohne Sicherheitskontrollen. Sicherheitskontrollen verfolgen das Ziel, den Zugriff auf bestimmte Dienste zu verweigern. Sie sollten diese Option nur dann wählen, wenn Sie sich in einem sicheren Netzwerk (nicht im Internet) befinden oder beabsichtigen, die Konfiguration Ihrer Firewall auf einen späteren Zeitpunkt zu verschieben.

  
  Warnung

  Wenn Sie eine Firewall konfiguriert haben oder eine Firewall-Regel in der Datei `/etc/sysconfig/iptables`, wird diese Datei gelöscht, wenn Sie **Firewall deaktivieren** wählen und **Ok** klicken, um die Änderungen zu speichern.

- **Firewall aktivieren** — Diese Option konfiguriert das System dazu eingehende Verbindungen abzulehnen, die keine Antwort auf ausgehende Anfragen sind, wie DNS-Antworten oder DHCP-Anforderungen. Sollte Zugriff auf bestimmte Services benötigt werden, können Sie diese bestimmten Services durch die Firewall lassen.

  Dies empfiehlt sich, wenn Sie Ihr System an das Internet anschließen und dabei keinen Server ausführen lassen wollen.

  Indem Sie eines der **Sicheren Geräte** wählen, bestimmen Sie den ungehinderten Datenaustausch Ihres Systems mit diesem Gerät; dieses Gerät wird somit von der Firewall nicht beachtet. Wenn Sie sich also z.B. in einem lokalen Netzwerk befinden, aber gleichzeitig über einen PPP-Onlinedienst an das Internet angeschlossen sind, können Sie **eth0** markieren und somit den ungehinderten Datenverkehr mit Ihrem lokalen Netzwerk aktivieren. Wenn Sie **eth0** als sicher bestimmen, aktivieren Sie den ungehinderten Datenverkehr mit dem Ethernet, wobei das ppp0-Interface jedoch weiterhin der Kontrolle durch die Firewall unterliegt. Markieren Sie keine Schnittstellen, deren Datenverkehr Sie weiterhin kontrollieren wollen.

  Geräte, die an öffentliche Netzwerke wie z.B. das Internet angeschlossen sind, sollten niemals zu **Sicheren Geräten** bestimmt werden.

  Das Auswählen von Optionen in der Liste der **Sicheren Services**, erlaubt diesen Services den Durchgang durch die Firewall.

  WWW (HTTP)

  Das HTTP-Protokoll wird von Apache (und anderen Web-Servern) zur Handhabung von Webseiten verwendet. Sie sollten diese Option aktivieren, wenn Sie öffentlichen Zugriff auf Ihren Webserver gewähren wollen. Wenn Sie Webseiten lokal betrachten oder erstellen wollen, benötigen Sie diese Option nicht. Zur Handhabung von Webseiten müssen Sie das `httpd`-Paket installieren.

  Durch das Aktivieren von **WWW (HTTP)** wird nicht automatisch auch ein Port für HTTPS geöffnet, der SSL-Version von HTTP.

  FTP

  Das FTP-Protokoll ist für die Dateiübertragung zwischen Rechnern in einem Netzwerk zuständig. Sie sollten diese Option aktivieren, wenn Sie öffentlichen Zugriff auf Ihren FTP-Server gewähren wollen.

SSH

Bei der Secure Shell (SSH) handelt es sich um eine Gruppe von Tools, mit der man sich in einen Remote-Computer einloggen und dort Befehle ausführen kann. Aktivieren Sie diese Option, wenn Sie mithilfe von SSH-Tools durch die Firewall Zugriff auf Ihren Computer erlangen wollen. Sie können auf Ihren Rechner nur dann Fernzugriff mithilfe von SSH-Tools bekommen, wenn das `openssh-server`-Paket auf Ihrem Rechner installiert ist.

Telnet

Bei Telnet handelt es sich um ein Protokoll, mit dem man sich in Remote-Computer einloggen kann. Telnet-Datenübertragungen sind unverschlüsselt und bieten keinerlei Sicherheit vor Netzwerkspionage. Es ist also nicht empfehlenswert, eingehenden Telnet Zugriff zu gewähren. Wenn Sie dies dennoch wünschen, müssen Sie das `telnet-server`-Paket installieren.

Mail (SMTP)

Aktivieren Sie diese Option, wenn Sie den Posteingang ungehindert durch die Firewall ermöglichen wollen, so dass sich Remote-Rechner zum Senden von Post direkt mit Ihrem Computer verbinden können. Diese Option wird nicht benötigt, wenn Sie Ihre Post von Ihrem ISP-Server unter Verwendung von POP3 oder IMAP abrufen oder Tools wie z.B. `fetchmail`verwenden. Beachten Sie, dass Sie im Falle eines nicht fachgerecht konfigurierten SMTP-Servers Remote-Computern die Möglichkeit geben, Ihnen ungewollte Post (Spam) zu senden.

Klicken Sie auf **OK**, um die Firewall zu aktivieren. Nachdem Sie auf **OK** geklickt haben, werden die ausgewählten Optionen in `iptables` Befehle umgewandelt und in die Datei `/etc/sysconfig/iptables` geschrieben. Der `iptables`-Service wird gestartet, so dass die Firewall sofort nach dem Speichern der gewählten Optionen aktiv ist. Wurde **Firewall deaktivieren** gewählt, wird die Datei `/etc/sysconfig/iptables` gelöscht und der `iptables`-Service augenblicklich angehalten.

Die ausgewählten Optionen werden außerdem in die Datei `/etc/sysconfig/redhat-config-securitylevel` geschrieben, so dass die Einstellungen beim nächsten Starten der Applikation wiederhergestellt werden. Bearbeiten Sie diese Datei nicht manuell.

Auch wenn die Firewall sofort aktv wird, ist der `iptables` Service nicht zum automatischen Starten beim Booten konfiguriert. Informationen hierzu finden Sie unter Abschnitt 20.2.

20.2. Aktivieren des Befehls `iptables`

Die Firewallregeln werden nur aktiviert, wenn der Befehl `iptables` ausgeführt wird. Verwenden Sie folgenden Befehl, um den Dienst manuell zu starten:

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

Führen Sie den folgenden Befehl aus, um sicherzustellen, dass der Dienst beim Booten des Systems gestartet wird:

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

Der `ipchains`-Service ist nicht in Red Hat Enterprise Linux enthalten. Wenn `ipchains` jedoch installiert ist (wenn, zum Beispiel, ein Upgrade ausgeführt wurde, und `ipchains` war vorher auf dem System installiert, sollten Sie den `ipchains`-Service nicht gleichzeitig mit dem `iptables`-Service ausführen. Um sicherzustellen, dass der `ipchains`-Service deaktiviert ist, führen Sie folgende zwei Befehle aus:

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

Das **Services Configuration Tool** kann zum Konfigurieren der Dienste `iptables` und `ipchains` verwendet werden.

redhat.

Kapitel 21.

Zugriffskontrolle für Dienste

Die Sicherheit in Ihrem System ist sehr wichtig. Eine Möglichkeit, die Sicherheit in Ihrem System zu verwalten, ist das umsichtige Zugriffsmanagement Ihrer Systemdienste. Auch wenn Ihr System für bestimmte Dienste (z.B. `httpd` für einen Webserver) freien Zugriff ermöglichen muss, sollten Sie Dienste, die Sie nicht benötigen, abschalten. Hierdurch verringern Sie das Risiko eines unbefugten Zugriffs.

Es gibt verschiedene Möglichkeiten, den Zugriff zu Systemdiensten zu verwalten. Je nach Dienst, Systemkonfiguration und eigener Erfahrung mit Linux sollten Sie die Option wählen, die für Sie die geeignetste ist.

Der einfachste Weg, den Zugriff über eine bestimmten Dienst zu sperren, besteht darin, den Dienst einfach abzuschalten. Die (De)Aktivierung der Dienste, die mit `xinetd` verwaltet werden (diese werden an anderer Stelle in diesem Kapitel noch genauer erklärt), als auch der Dienste in der `/etc/rc.d/init.d` Hierarchie (auch als SysV-Services bekannt) kann mit drei verschiedenen Applikationen durchgeführt werden:

- **Services Configuration Tool** — eine grafische Applikation, die jeden Dienst beschreibt und anzeigt, welche Dienste beim Booten gestartet werden (für die Runlevel 3, 4, und 5), und es Ihnen ermöglicht jeden der Dienste zu starten, abzubrechen oder neu zu starten
- **ntsysv** — Eine textbasierte Applikation, mit der Sie konfigurieren können, welche Dienste zum jeweiligen Runlevel beim Booten gestartet werden sollen. Änderungen werden nicht sofort für Nicht-`xinetd` Dienste wirksam. Nicht-`xinetd`-Dienste können mit diesem Programm nicht gestartet, abgebrochen oder neu gestartet werden.
- `chkconfig` — ein Befehlszeilen-Programm, mit dem Sie in den verschiedenen Runlevel Dienste ein- und ausschalten können. Änderungen werden nicht sofort für Nicht-`xinetd`-Dienste wirksam. Nicht-`xinetd`-Dienste können mit diesem Programm nicht gestartet, abgebrochen oder neu gestartet werden.

Diese Tools erscheinen Ihnen vielleicht einfacher als die Alternativen — das manuelle Bearbeiten der vielen symbolischen Links, die sich in Verzeichnissen unter `/etc/rc.d` befinden oder das Bearbeiten der `xinetd`-Konfigurationsdateien unter `/etc/xinetd.d`.

Eine andere Möglichkeit der Zugriffsverwaltung Ihrer Systemdienste steht Ihnen mit `iptables` zur Verfügung, mit dem Sie eine IP- Firewall konfigurieren können. Falls Sie erst seit kurzem Linux-Benutzer sind, sollten Sie wissen, dass `iptables` wahrscheinlich nicht die optimale Lösung für Sie ist. Das Einrichten von `iptables` ist sehr kompliziert und eignet sich am ehesten für erfahrene LINUX-Systemadministratoren.

Auf der anderen Seite ist `iptables` extrem flexibel. Wenn Sie z.B. eine individuell gestaltete Lösung suchen, mit der bestimmte Hosts Zugriff auf bestimmte Dienste erhalten, kann Ihnen `iptables` dabei helfen. Im *Red Hat Enterprise Linux Referenzhandbuch* und *Red Hat Enterprise Linux Sicherheitshandbuch* finden Sie weitere Informationen zu `iptables`.

Wenn Sie hingegen ein Utility suchen, mit dem Sie allgemeine Zugriffsregeln für Ihren Rechner aufstellen können und/oder wenn Sie erst seit kurzem zu den Linux-Benutzern gehören, empfiehlt sich **Security Level Configuration Tool** (`redhat-config-securitylevel`), mit dem Sie die Sicherheitsstufe für Ihr System wählen können, ähnlich wie im Bildschirm **Firewall Konfiguration** im Installationsprogramm.

Weitere Informationen zu diesen Tools finden Sie im Kapitel 20. Benötigen Sie spezifischere Firewallregeln, sehen Sie das Kapitel `iptables` im *Red Hat Enterprise Linux Referenzhandbuch*.

21.1. Runlevel

Um den Zugriff zu den Diensten konfigurieren zu können, müssen Sie zunächst die Linux-Runlevel genau kennen. Bei einem Runlevel handelt es sich um einen Zustand oder auch einen *Modus*, der über die im Verzeichnis `/etc/rc.d/rc<x>.d`, aufgeführten Dienste definiert wird, und in dem `<x>` für die Nummer des Runlevels steht.

Es gibt die folgende Runlevel:

- 0 — Halt
- 1 — Einzelbenutzer-Modus
- 2 — Nicht belegt (vom Benutzer zu definieren)
- 3 — Vollständiger Mehrbenutzer-Modus
- 4 — Nicht belegt (vom Benutzer zu definieren)
- 5 — Vollständiger Mehrbenutzer-Modus (mit einem X-basierten Login-Bildschirm)
- 6 — Neustart

Wenn Sie einen Text-Login-Bildschirm wählen, arbeiten Sie im Runlevel 3. Wenn Sie hingegen einen grafischen Login- Bildschirm wählen, arbeiten Sie im Runlevel 5.

Um den standardmäßigen Runlevel zu wechseln, ändern Sie die `/etc/inittab` Datei. Relativ weit am Anfang enthält sie eine Zeile, welche in etwa folgendermaßen aussieht:

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

Geben Sie in dieser Zeile die Ziffer des gewünschten Runlevels ein. Ihre Änderungen werden erst nach einem Neustart des Systems aktiviert.

Um den Runlevel augenblicklich zu ändern, verwenden Sie den Befehl `telinit`, gefolgt von der Nummer des Runlevels. Sie können diesen Befehl nur als root verwenden. Der Befehl `telinit` ändert die Datei `/etc/inittab` nicht, sondern lediglich den zur Zeit ausgeführten Runlevel. Wenn das System neu startet, wird sich dies wieder in dem Runlevel befinden, der in `/etc/inittab` angegeben ist.

21.2. TCP-Wrapper

Viele UNIX-System-Administratoren greifen auf TCP-Wrapper zurück, um den Zugriff auf bestimmte Netzdienste zu verwalten. Bei allen Netzwerkdiensten, die von `xinetd` verwaltet werden (auch bei allen Programmen mit integriertem Support für die Bibliothek `libwrap`), können Sie den Zugriff mit TCP-Wrappern verwalten. `xinetd` verwendet die Dateien `/etc/hosts.allow` und `/etc/hosts.deny` zur Konfiguration des Zugriffs auf Systemdienste. Die Datei `hosts.allow` enthält eine Liste von Regeln, die bestimmt, welche Clients Zugriff auf die Netzwerkdienste, die von `xinetd` verwaltet werden, haben, während die Datei `hosts.deny` Regeln enthält, die den Zugriff verweigern kann. Die Datei `hosts.allow` hat Vorrang vor der Datei `hosts.deny`. Die Zugriffsberechtigungen basieren entweder auf individuellen IP-Adressen (oder Hostnamen) oder auf bestimmten Client-Kriterien. Weitere Informationen finden Sie im *Red Hat Enterprise Linux Referenzhandbuch* und auf der `hosts_access` man-Seite in Abschnitt 5 der man-Seiten (`man 5 hosts_access`).

21.2.1. `xinetd`

Zur Kontrolle des Zugriffs auf Ihre Internet-Dienste steht Ihnen `xinetd` zur Verfügung, der den unsichereren Dienst `inetd` ersetzt. Der `xinetd`-Daemon schont Systemressourcen, bietet eine Zugriffskontrolle und Protokollfunktionen und kann außerdem dazu verwendet werden, Server für spezielle

Zwecke zu starten. `xinetd` können Sie einsetzen, um unter anderem den Zugriff nur auf bestimmte Hosts zu gewähren, den Zugriff auf bestimmte Hosts zu verweigern, den Zugriff auf bestimmte Dienste nur zu bestimmten Zeiten zu gewähren oder die Zahl der eingehenden Verbindungen und/oder die durch die eingehenden Verbindungen entstehende Systembelastung beschränken.

`xinetd` läuft kontinuierlich und überwacht alle Ports für die von ihm verwalteten Dienste. Wenn eine Verbindungsanfrage für eine der von ihm verwalteten Dienste eingeht, startet `xinetd` den für diesen Dienst vorgesehenen Server.

Die Konfigurationsdatei für `xinetd` ist `/etc/xinetd.conf`, diese Datei enthält jedoch nur Datei einige Standards und Anweisungen zur Einbettung des `/etc/xinetd.d` Verzeichnisses. Um einen `xinetd`-Dienst zu aktivieren oder zu deaktivieren, müssen Sie müssen Sie seine Konfigurationsdatei im Verzeichnis `/etc/xinetd.d` bearbeiten. Wenn das `disable`-Attribut als **`yes`** eingestellt ist, wurde der Dienst deaktiviert. Wenn als `disable`-Attribut **`no`** eingestellt ist, ist der Dienst aktiviert. Sie können jede der `xinetd` Konfigurationsdateien bearbeiten oder den Status der Aktivierung/Deaktivierung mit Hilfe von **Services Configuration Tool**, **ntsysv** oder `chkconfig` ändern. Um eine Liste der Netzwerkdienste, die von `xinetd` verwaltet werden, zu erhalten, rufen Sie den Inhalt des `/etc/xinetd.d` Verzeichnisses mit dem Befehl `ls /etc/xinetd.d` auf.

21.3. Services Configuration Tool

Services Configuration Tool ist eine von Red Hat entwickelte grafische Applikation, mit der Sie konfigurieren können, welche SysV-Dienste unter `/etc/rc.d/init.d` beim Booten (für die Runlevel 3, 4 und 5) gestartet werden sollen, und welche `xinetd`-Dienste aktiviert werden. Mit dieser Applikation können Sie außerdem Sysv starten, abbrechen oder neu starten, sowie `xinetd` neu starten.

Um **Services Configuration Tool** vom Desktop zu starten, gehen Sie zum **Hauptmenü- Button** (auf dem Panel) => **Servereinstellungen** => **Dienstekonfiguration** oder geben Sie den Befehl `redhat-config-services` am Shell-Prompt ein (z.B. in einem **XTerm**- oder einem **GNOME- Terminal**).

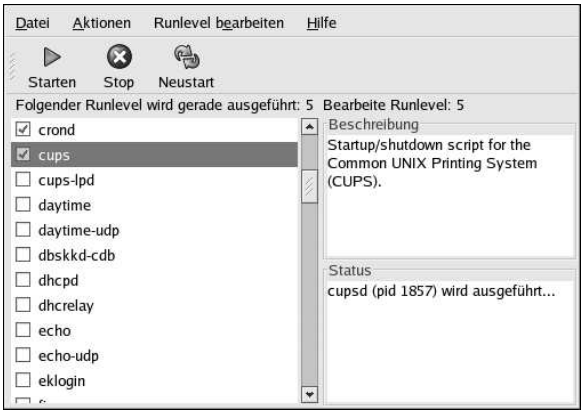

Abbildung 21-1. Services Configuration Tool

Die Applikation **Services Configuration Tool** zeigt Ihnen den Runlevel, auf dem Sie sich gerade befinden und den, den Sie gerade bearbeiten, an. Um einen anderen Runlevel zu bearbeiten, klicken Sie auf **Runlevel bearbeiten** im Pulldown-Menü und wählen dann Runlevel 3, 4 oder 5 . Nähere Erläuterungen der Runlevel finden Sie unter Abschnitt 21.1.

Die Applikation **Services Configuration Tool** listet alle Dienste aus `/etc/rc.d/init.d` und die von `xinetd` verwalteten Dienste auf. Klicken Sie auf den Namen des Dienstes in der Liste auf der linken Seite der Applikation, um eine kurze Beschreibung des Dienstes und den jeweiligen Status anzuzeigen. Wenn der Dienst kein `xinetd`-Dienst ist, zeigt das Statusfenster ob der Dienst gerade ausgeführt wird oder nicht. Wenn der Dienst von `xinetd` verwaltet wird, zeigt das Statusfenster **xinetd service** an.

Um einen Dienst zu starten, abzubrechen oder neu zu starten, wählen Sie den Dienst aus der Liste aus und klicken Sie auf den entsprechenden Button in der Toolleiste (oder wählen Sie die Aktion aus dem Pulldown-Menü **Aktionen**). Wenn der Dienst ein `xinetd`-Dienst ist, sind die Aktions-Buttons deaktiviert, da diese nicht einzeln gestartet oder angehalten werden können.

Wenn Sie einen `xinetd`-Dienst aktivieren/deaktivieren in dem Sie das Kontrollkästchen neben dem Namen des Dienstes markieren bzw. die Markierung aufheben, müssen Sie **Datei => Änderungen speichern** aus dem Pulldown-Menü wählen, um `xinetd` neu zu starten, und dann sofort den `xinetd`-Dienst, den Sie geändert haben, aktivieren/deaktivieren. `xinetd` ist so konfiguriert, dass die Einstellungen gespeichert werden. Sie können mehrere `xinetd`-Dienste gleichzeitig aktivieren/deaktivieren, und alles speichern, sobald Sie fertig sind.

Nehmen wir beispielsweise an, dass Sie `rsync` markieren, um dieses im Runlevel 3 zu aktivieren, und dann die Änderungen speichern. Der `rsync`-Dienst wird sofort aktiviert. Wenn Sie dann das nächste Mal `xinetd` starten, ist `rsync` weiterhin aktiviert.

Warnung

Wenn Sie Änderungen an `xinetd`-Diensten speichern, wird `xinetd` neu gestartet und die Änderungen werden sofort wirksam. Wenn Sie Änderungen an anderen Diensten speichern, wird der Runlevel neu konfiguriert, die Änderungen werden jedoch nicht sofort wirksam.

Um einen Nicht-`xinetd`-Dienst so zu konfigurieren, dass dieser beim Booten des derzeitig ausgewählten Runlevels startet, markieren Sie das Kontrollkästchen neben dem Namen des Dienstes in der Liste. Nachdem Sie den Runlevel konfiguriert haben, aktivieren Sie die Änderungen, in dem Sie **Datei => Änderungen speichern** im Pull-Down-Menü auswählen. Die Konfiguration des Runlevels wird geändert, der Runlevel selbst jedoch nicht neu gestartet. Die Änderungen werden daher nicht sofort wirksam.

Nehmen wir beispielsweise an, dass Sie gerade Runlevel 3 konfigurieren. Wenn Sie den Status für den `httpd`-Dienst von markiert zu nicht markiert ändern und dann **Änderungen speichern** auswählen, ändert sich die Konfiguration für Runlevel 3, so dass `httpd` beim Booten nicht gestartet wird. Runlevel 3 wird jedoch nicht neu initialisiert, so dass `httpd` weiterhin ausgeführt wird. Wählen Sie jetzt eine der folgenden Optionen:

1. Stoppen Sie den `httpd`-Dienst — Sie stoppen den Dienst, indem Sie ihn aus der Liste auswählen und dann den Button **Stop** anklicken. Es erscheint eine Nachricht, die Sie darüber informiert, dass der Dienst erfolgreich gestoppt wurde.
2. Starten Sie den Runlevel neu — Sie können den Runlevel neu starten, in dem Sie an einem Shell-Prompt den Befehl `telinit 3` (3 ist hier die Ziffer des Runlevel). Wir empfehlen diese Option für den Fall, dass Sie die **Beim Booten starten**-Einstellung von einem oder mehreren Diensten geändert haben und möchten, dass die Änderungen sofort übernommen werden.
3. Keine weitere Aktion durchführen — Sie müssen den `httpd`-Dienst nicht stoppen. Es reicht, wenn Sie den Dienst dann stoppen, wenn das System neu gebootet wird. Wenn das System das darauffolgende Mal gebootet wird, wird auch der Runlevel gestartet, ohne dass der `httpd`-Dienst gleichzeitig aktiviert wird.

Um einen Service zu einem Runlevel hinzuzufügen, wählen Sie den Runlevel im **Runlevel bearbeiten** Pulldown-Menü und wählen dann **Aktionen => Service hinzufügen**. Um einen Service aus einem

Runlevel zu löschen, wählen Sie den Runlevel aus dem **Runlevel bearbeiten** Pulldown-Menü, dann den zu löschenden Service in der Liste auf der linken Seite und zuletzt **Aktionen => Service löschen**.

21.4. ntsysv

Mit dem Dienstprogramm **ntsysv** steht Ihnen eine einfache Schnittstelle für die Aktivierung und Deaktivierung von Diensten zur Verfügung. Mit **ntsysv** können Sie einen von `xinetd` verwalteten Dienst starten oder stoppen. Außerdem können Sie mit **ntsysv** Runlevel konfigurieren. Standardmäßig wird nur der derzeitig laufende Runlevel konfiguriert. Um einen anderen Runlevel zu konfigurieren können Sie mit der Option `--level` einen oder mehrere Runlevel auswählen. So konfiguriert zum Beispiel der Befehl `ntsysv --level 345` die Runlevel 3, 4 und 5.

Die **ntsysv**-Schnittstelle funktioniert wie das Installationsprogramm für den Textmodus. Sie können mit den Pfeiltasten in der Liste hinauf- und hinunterscrollen. Mit der Leertaste markieren Sie Dienste oder nehmen Sie aus der Liste heraus und können mit ihr auch die **Ok** und **Abbrechen** Buttons drücken. Um zwischen den Dienst-Listen und den Buttons **Ok** und **Abbrechen** hin- und her zu springen verwenden Sie die [Tab]-Taste. * bedeutet, dass ein Dienst aktiviert ist. Wenn Sie [F1] drücken, erhalten Sie eine kurze Beschreibung zum jeweiligen Dienst.

Warnung

Dienste, die von `xinetd` verwaltet werden, werden sofort von **ntsysv** betroffen. Bei allen anderen Diensten werden die Änderungen nicht sofort wirksam. Sie müssen den jeweiligen Dienst mit dem Befehl `service` *`daemon`* `stop` stoppen. Ersetzen Sie im vorigen Beispiel den Namen des Dienstes, z.B. *`daemon`*, mit dem Namen des Dienstes den Sie stoppen möchten, zum Beispiel `httpd`. Ersetzen Sie `stop` durch `start` oder `restart`, um den Dienst zu starten oder neu zu starten.

21.5. `chkconfig`

Der Befehl `chkconfig` kann ebenfalls verwendet werden, um einen Dienst zu aktivieren oder zu deaktivieren. Wenn Sie den Befehl `chkconfig --list` verwenden, wird Ihnen eine Liste von Systemdiensten angezeigt und Sie werden informiert, ob diese Dienste in den Runlevel 0-6 aktiviert (`on`) oder deaktiviert (`off`) wurden. Am Ende der Liste erscheint ein Abschnitt über die von `xinetd` verwalteten Dienste).

Wenn Sie mit `chkconfig --list` einen von `xinetd` verwalteten Dienst anfragen, können Sie sehen, ob der `xinetd`-Dienst aktiviert (`on`) oder deaktiviert (`off`) wurde. Mit dem folgenden Befehl wird z.B. angezeigt, dass `chkconfig --list finger` als xinetd-Dienst aktiviert wurde:

```
finger          on
```

`finger` ist also als `xinetd`-Dienst aktiviert. Wenn `xinetd` ausgeführt wird, ist `finger` aktiviert.

Wenn Sie mit `chkconfig --list` einen Dienst aus `/etc/rc.d`, anfragen, werden die Einstellungen des Dienstes für jeden Runlevel angezeigt. So wird zum Beispiel mit dem Befehl `chkconfig --list httpd` folgendes angezeigt:

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

Darüber hinaus können Sie mit `chkconfig` einen bestimmten Dienst auch so einstellen, dass er in einem bestimmten Runlevel gestartet oder nicht gestartet wird. Um beispielsweise `nscd` in den Runlevels 3, 4, und 5 abzuschalten, verwenden Sie folgenden Befehl:

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

Warnung

Dienste, die von `xinetd` verwaltet werden, werden sofort durch `chkconfig` beeinflusst. Wenn z.B. `xinetd` läuft, `finger` deaktiviert ist und der Befehl `chkconfig finger on` ausgeführt wird, wird `finger` sofort aktiviert, ohne `xinetd` manuell neu starten zu müssen. Änderungen für andere Dienste werden nicht sofort wirksam, wenn Sie `chkconfig` verwendet haben. Diese Dienste müssen Sie jeweils mit dem Befehl `service` *`daemon`* `stop` stoppen. Wie im vorangegangenen Beispiel ersetzen Sie *`daemon`* durch den Namen des Dienstes, den Sie stoppen wollen, z.B. `httpd`. Ersetzen Sie `stop` with `start` oder `restart`, um den Dienst zu starten oder neu zu starten.

21.6. Zusätzliche Ressourcen

Weitere Informationen finden Sie in den folgenden Quellen.

21.6.1. Installierte Dokumentation

- Die man-Seiten für `ntsysv`, `chkconfig`, `xinetd` und `xinetd.conf`
- `man 5 hosts_access` — Die man-Seite für das Format der Kontrolldateien für den Hostzugriff (im Abschnitt 5 der man-Seiten).

21.6.2. Hilfreiche Websites

- http://www.xinetd.org — Die `xinetd` Webseite. Hier finden Sie eine detaillierte Liste der Funktionen und Musterkonfigurationsdateien.

21.6.3. Verwandte Bücher

- *Red Hat Enterprise Linux Referenzhandbuch*, Red Hat, Inc. — Dieses mitgelieferte Handbuch enthält detaillierte Informationen darüber, wie TCP-Wrappers und `xinetd` Zugriff erlauben oder ablehnen, und wie unter Verwendung dieser Netzwerkzugriff konfiguriert werden kann. Es gibt auch Anleitungen zum Erzeugen von `iptables` Firewallregeln.
- *Red Hat Enterprise Linux Sicherheitshandbuch* Red Hat, Inc. — Dieses Handbuch beschreibt die Sicherung von Services mit TCP-Wrappers und `xinetd`, wie das Loggen von abgelehnten Verbindungsversuchen.

Kapitel 22.

OpenSSH

OpenSSH ist eine frei verfügbare Open Source-Implementierung des SSH (*S*ecure *SH*ell)-Protokolls. Es ersetzt `telnet`, `ftp`, `rlogin`, `rsh` und `rcp` durch Tools mit sicherer und verschlüsselter Netzwerkverbindung. OpenSSh unterstützt die Versionen 1.3, 1.5 und 2 des SSH-Protokolls. Ab der Version 2.9 von OpenSSH ist die Version 2 das Standard-Protokoll, das standardmäßig RSA Schlüssel verwendet.

22.1. Warum sollte OpenSSH verwendet werden?

Durch die Verwendung des OpenSSH-Tools erhöhen Sie die Sicherheit Ihres Computers. Alle Verbindungen, die die OpenSSH-Tools verwenden (einschließlich Passwörter) sind verschlüsselt. `Telnet` und `ftp` verwenden Passwörter im einfachen Textformat und versenden alle Informationen unverschlüsselt. Somit können Informationen abgefangen und Passwörter abgerufen werden, wodurch sich unbefugte Personen mit diesen abgefangenen Passwörtern sich in Ihrem System anmelden können. OpenSSH sollte wann immer möglich verwendet werden, um diese Sicherheitsprobleme zu vermeiden.

Ein anderer Grund für die Verwendung von OpenSSH ist, dass die `DISPLAY`-Variable automatisch zum Client-Rechner weitervermittelt wird. Anders ausgedrückt, wenn Sie das X Window System auf Ihrem lokalen Rechner ausführen und mit dem Befehl `ssh` in einem Remote-Rechner angemeldet sind, auf dem Sie ein Programm ausführen wollen, welches X verlangt, wird dies auf Ihrem lokalen Rechner angezeigt. Das ist sehr praktisch, wenn Sie grafische Systemadministrations-Tools bevorzugen, jedoch nicht immer tatsächlich physikalischen Zugriff zu Ihrem Server haben.

22.2. Konfigurieren eines OpenSSH-Servers

Um einen OpenSSH-Server auszuführen, müssen Sie zuerst sicherstellen, dass Sie die richtigen RPM-Pakete installiert haben. Das Paket `openssh-server` ist notwendig und vom Paket `openssh` abhängig.

Der OpenSSH-Daemon verwendet die Konfigurationsdatei `/etc/ssh/sshd_config`. Die standardmäßige Konfigurationsdatei ist in der Regel ausreichend. Wenn Sie den Daemon in anderer Weise konfigurieren möchten als in der Standarddatei `sshd_config` angegeben, lesen Sie die `sshd` man-Seite, in der Sie eine Liste von Schlüsselwörtern finden, die in der Konfigurationsdatei verwendet werden können.

Um den OpenSSH-Service zu starten, verwenden Sie den Befehl `/sbin/service sshd start`. Um ihn anzuhalten, benutzen Sie den Befehl `/sbin/service sshd stop`. Wenn Sie den Daemon automatisch beim Booten starten möchten, finden Sie unter Kapitel 21 die entsprechenden Informationen.

Wenn Sie ein System neu installieren und sich vorher Clients mit diesem über ein OpenSSH Tool verbunden hatte, so wird den Client-Benutzern nach der Reinstallation folgende Meldung angezeigt:

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

Das neu installierte System legt ein neues Set Identifikationsschlüssel für das System an, daher die Warnung über die Änderung des RSA Host-Schlüssels. Wenn Sie die für das System

generierten Host-Schlüssel beibehalten möchten, stellen Sie eine Sicherungskopie der Dateien `/etc/ssh/ssh_host*key*` her, um diese nach der Neuinstallation zu verwenden. Durch diesen Prozess wird die Identität des Systems beibehalten, und wenn sich Clients nach der Neuinstallation hiermit verbinden, wird keine Warnmeldung ausgegeben.

22.3. Konfigurieren eines OpenSSH-Clients

Um sich einem Client-Rechner mit einem OpenSSH-Server zu verbinden, müssen Sie die Pakete `openssh-clients` und `openssh` auf dem Client-Rechner installiert haben.

22.3.1. Verwenden des Befehls `ssh`

Der Befehl `ssh` ist ein sicherer Ersatz für die Befehle `rlogin`, `rsh` und `telnet`. Mit diesem Befehl können Sie sich sowohl auf einem Remote-Rechner anmelden als auch auf diesem Rechner Befehle ausführen.

Die Verwendung des Befehls `ssh` für die Anmeldung auf einem Rechner ist vergleichbar mit dem Befehl `telnet`. Wenn Sie sich auf einem Remote-Rechner mit dem Namen penguin.example.net anmelden möchten, geben Sie am Shell-Prompt den folgenden Befehl ein:

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

Wenn Sie sich das erste Mal mit dem Befehl `ssh` auf einem Remote-Rechner anmelden, erscheint folgende (oder eine ähnliche) Meldung:

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

Geben Sie **`yes`** ein, um fortzufahren. Der Server wird Ihrer Liste von bekannten Hosts wie im Folgenden angegeben hinzugefügt:

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

Anschließend werden Sie aufgefordert, Ihr Passwort für den Remote-Rechner einzugeben. Nach der Eingabe des Passworts befinden Sie sich im Shell-Prompt des Remote-Rechners. Wenn Sie keinen Benutzernamen angeben, so wird der Benutzername, mit dem Sie auf dem lokalen Rechner angemeldet sind, an den Remote-Rechner weitergegeben. Mit dem folgenden Befehl können Sie einen anderen Benutzernamen festlegen:

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

Sie können auch die Syntax `ssh -l username penguin.example.net` verwenden.

Mit dem Befehl `ssh` können Sie Befehle auf einem Remote-Rechner ausführen, ohne am Shell-Prompt angemeldet sein zu müssen. Die entsprechende Syntax ist `ssh hostname command`. Wenn Sie zum Beispiel den Befehl `ls /usr/share/doc` auf dem Remote-Rechner penguin.example.net ausführen möchten, geben Sie am Shell-Prompt den folgenden Befehl ein:

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

Nachdem Sie das korrekte Passwort eingegeben haben, wird der Inhalt des Verzeichnisses `/usr/share/doc` angezeigt, und Sie kehren zum Shell-Prompt zurück.

22.3.2. Verwenden des Befehls `scp`

Der Befehl `scp` kann für die Übertragung von Dateien zwischen Computern über eine sichere, verschlüsselte Verbindung verwendet werden und ist vergleichbar mit dem Befehl `rcp`.

Die allgemeine Syntax für die Übertragung einer lokalen Datei zu einem Remote-System lautet wie folgt:

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

Die Datei *`localfile`* legt die Quelle fest und *`username@tohostname:/newfilename`* den Bestimmungsort.

Um die lokale Datei `shadowman` an penguin. example.net zu übermitteln, geben Sie Folgendes am Shell-Prompt ein (ersetzen Sie dabei *`username`* durch Ihren Benutzernamen):

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

Die Datei `shadowman` wird somit an die Datei `/home/`*`username`*`/shadowman` des Rechners penguin.example.net übermittelt.

Die allgemeine Syntax für die Übermittlung von Remote-Dateien zu einem lokalen System lautet:

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

Die Datei *`remotefile`* legt die Quelle fest und *`newlocalfile`* den Bestimmungsort.

Viele Dateien können als Quelldateien festgelegt sein. Um zum Beispiel den Inhalt des Verzeichnisses `/downloads` an das Verzeichnis `uploads` des Remote-Rechners penguin.example.net zu übertragen, geben Sie Folgendes am Shell-Prompt ein:

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

22.3.3. Verwenden des Befehls `sftp`

Das Dienstprogramm `sftp` kann zum Öffnen einer sicheren, interaktiven FTP-Sitzung verwendet werden. Es gleicht `ftp`, mit dem Unterschied, dass es eine sichere, verschlüsselte Verbindung verwendet. Die allgemeine Syntax ist *`sftp username@hostname.com`*. Nach der Authentifizierung können Sie einen Satz von Befehlen verwenden (ähnlich wie die Verwendung von FTP). In der man-Seite `sftp` finden Sie eine Liste dieser Befehle. Um die man-Seite lesen zu können, müssen Sie am Shell-Prompt den Befehl`man sftp` ausführen. Das Dienstprogramm `sftp` ist nur in den OpenSSH Versionen 2.5.0p1 und höher verfügbar.

22.3.4. Erstellen eines Schlüsselpaares

Wenn Sie nicht jedesmal Ihr Passwort eingeben möchten, wenn Sie die Befehle `ssh`, `scp` oder `sftp` verwenden, um sich mit einem Remote-Rechner zu verbinden, können Sie ein Authorisierungsschlüsselpaar erstellen.

Für jeden Benutzer müssen Schlüssel erstellt werden. Wenn Sie als Benutzer mit einem Remote-Rechner verbunden werden möchten, müssen Sie die Schlüssel gemäß den folgenden Schritten erstellen. Wenn Sie diese Schritte als root ausführen, können diese Schlüssel auch nur von root verwendet werden.

Das Starten mit OpenSSH Version 3.0, `~/.ssh/authorized_keys2`, `~/.ssh/known_hosts2` und `/etc/ssh_known_hosts2` ist veraltet. SSH Protokoll 1 und 2 verwenden die Dateien `~/.ssh/authorized_keys`, `~/.ssh/known_hosts` und `/etc/ssh/ssh_known_hosts`.

Red Hat Enterprise Linux 3 verwendet SSH Protokoll 2 und RSA-Schlüssel standardmäßig.

Tipp

Wenn Sie Ihr System neu installieren, das erstellte Schlüsselpaar jedoch beibehalten möchten, erstellen Sie eine Sicherungskopie des Verzeichnisses `.ssh` in Ihrem Home-Verzeichnis. Kopieren Sie dieses Verzeichnis nach der Installation erneut in Ihr Home-Verzeichnis. Dies ist für alle Benutzer Ihres Systems, einschließlich dem root-Benutzer, möglich.

22.3.4.1. Erstellen eines RSA-Schlüsselpaares für die Version 2

Befolgen Sie die nachstehenden Schritte für die Erstellung eines RSA-Schlüsselpaares für die Version 2 des SSH-Protokolls. Dieses ist der Standard seit OpenSSH 2.9.

1. Um ein RSA-Schlüsselpaar für das Arbeiten mit der Version 2 des Protokolls zu erstellen, geben Sie am Shell-Prompt den folgenden Befehl ein:
   ```
   ssh-keygen -t rsa
   ```
   Übernehmen Sie die standardmäßige Dateispeicherstelle `~/.ssh/id_rsa`. Geben Sie ein Passwort ein, das sich von Ihrem Accountpasswort unterscheidet. Bestätigen Sie diesen, indem Sie ihn erneut eingeben.

   Der öffentliche Schlüssel wird in die Datei `~/.ssh/id_rsa.pub` und der private Schlüssel in die Datei `~/.ssh/id_rsa` geschrieben. Geben Sie Ihren privaten Schlüssel niemals an andere weiter.
2. Ändern Sie die Berechtigungen Ihres Verzeichnisses `.ssh` mit folgendem Befehl:
   ```
   chmod 755 ~/.ssh
   ```
3. Kopieren Sie den Inhalt von `~/.ssh/id_rsa.pub` in die Datei `~/.ssh/authorized_keys` des Rechners, mit dem Sie verbunden werden möchten. Wenn die Datei `~/.ssh/authorized_keys` existiert, können Sie die Datei `~/.ssh/id_rsa.pub` in die Datei `~/.ssh/authorized_keys` des anderen Computers kopieren.
4. Ändern Sie die Berechtigungen des Verzeichnisses `authorized_keys` mit folgendem Befehl:
   ```
   chmod 644 ~/.ssh/authorized_keys
   ```
5. Wenn Sie GNOME ausführen, gehen Sie über zu Abschnitt 22.3.4.4. Wenn Sie das X Window System nicht ausführen, rufen Sie Abschnitt 22.3.4.5 auf.

22.3.4.2. Erstellen eines DSA-Schlüsselpaares für die Version 2

Folgen Sie den folgenden Schritten, um ein DSA-Schlüsselpaar für Version 2 des SSH Protokolls zu erstellen.

1. Um ein DSA Schlüsselpaar für Version 2 des Protokolls zu erstellen, geben Sie am Shell Prompt den folgenden Befehl ein:
   ```
   ssh-keygen -t dsa
   ```
   Übernehmen Sie standardmäßige Dateispeicherstelle `~/.ssh/id_dsa`. Geben Sie ein Passwort ein, das sich von Ihrem Accountpasswort unterscheidet. Bestätigen Sie diesen, indem Sie es erneut eingeben.

   

   Tipp

   Passwort hier meint eine Folge von Wörtern und Zeichen um einen Benutzer zu authentifizieren. Es unterscheidet sich hier von herkömmlichen Passwörtern in der Form, das Sie Leerzeichen oder Tabs verwenden können. Passwörter hier sind für gewöhnlich länger als herkömmliche Passwörter, da sie üblicherweise ganze Sätze statt nur ein einzelnes Wort sind.

Der öffentliche Schlüssel wird in die Datei `~/.ssh/id_dsa.pub` und der private Schlüssel in die Datei `~/.ssh/id_dsa` geschrieben. Geben Sie Ihren privaten Schlüssel niemals an andere weiter.

2. Ändern Sie die Berechtigungen des Verzeichnisses `.ssh` mit folgendem Befehl:
   `chmod 755 ~/.ssh`
3. Kopieren Sie den Inhalt von `~/.ssh/id_dsa.pub` in die Datei `~/.ssh/authorized_keys` des Rechners, mit dem Sie verbunden werden möchten. Wenn die Datei `~/.ssh/authorized_keys` existiert, können Sie die Datei `~/.ssh/id_dsa.pub` in die Datei `~/.ssh/authorized_keys` des anderen Computers kopieren.
4. Ändern Sie die Berechtigungen des Verzeichnisses `authorized_keys` mit folgendem Befehl:
   `chmod 644 ~/.ssh/authorized_keys`
5. Wenn Sie GNOME ausführen, gehen Sie über zu Abschnitt 22.3.4.4. Wenn Sie das X Window System nicht ausführen, rufen Sie Abschnitt 22.3.4.5 auf.

22.3.4.3. Erstellen eines Schlüsselpaares für Version 1.3 und 1.5

Befolgen Sie die nachstehenden Schritte für die Erstellung eines RSA-Schlüsselpaares für die Version 1 des SSH- Protokolls. Wenn Sie nur mit DSA-Systemen verbinden, benötigen Sie die RSA Schlüsselpaare der Version 1.3 oder 1.5 nicht.

1. Um ein RSA-Schlüsselpaar für das Arbeiten mit den Versionen 1.3 und 1.5 des Protokolls zu erstellen, geben Sie am Shell-Prompt folgenden Befehl ein:
   `ssh-keygen -t rsa1`

   Übernehmen Sie standardmäßige Dateispeicherstelle (`~/.ssh/identity`). Geben Sie ein Passwort ein, das sich von Ihrem Accountpasswort unterscheidet. Bestätigen Sie diesen, indem Sie ihn erneut eingeben.

   Der öffentliche Schlüssel wird in die Datei `~/.ssh/identity.pub`. und der private Schlüssel in die Datei `~/.ssh/identity` geschrieben. Geben Sie Ihren privaten Schlüssel niemals an andere weiter.
2. Ändern Sie die Berechtigungen Ihres Verzeichnisses `.ssh` und Ihrer Schlüssel mit dem Befehlen `chmod 755 ~/.ssh` und `chmod 644 ~/.ssh/identity.pub`.
3. Kopieren Sie den Inhalt von `~/.ssh/identity.pub` in die Datei `~/.ssh/authorized_keys` des Rechners, mit dem Sie verbunden werden möchten. Wenn die Datei `~/.ssh/authorized_keys` nicht existiert, können Sie die Datei `~/.ssh/identity.pub` in die Datei `~/.ssh/authorized_keys` des anderen Computers kopieren.
4. Wenn Sie GNOME ausführen, gehen Sie zu Abschnitt 22.3.4.4. Wenn Sie GNOME nicht ausführen, gehen Sie zu Abschnitt 22.3.4.5.

22.3.4.4. Konfigurieren von ssh-agent mit GNOME

Das Dienstprogramm `ssh-agent` kann zum Speichern Ihres Passwortes verwendet werden. Somit müssen Sie das Passwort nicht jedesmal eingeben, wenn Sie eine `ssh` oder `scp`-Verbindung starten. Wenn Sie GNOME verwenden, können Sie das `openssh-askpass-gnome` Dienstprogramm verwenden. Es fordert Sie auf, Ihr Passwort einzugeben, wenn Sie sich in GNOME anmelden, und sichert das Passwort, wenn Sie sich aus GNOME abmelden. Sie müssen Ihr Passwort während einer GNOME-Sitzung nicht jedesmal eingeben, wenn Sie eine `ssh` oder `scp`-Verbindung während einer GNOME-Sitzung ausführen. Wenn Sie GNOME nicht verwenden, gehen Sie zu Abschnitt 22.3.4.5.

Um Ihr Passwort während Ihrer GNOME-Sitzung zu sichern, führen Sie folgende Schritte aus:

1. Das Paket `openssh-askpass-gnome` muss installiert sein. Um dies festzustellen, verwenden Sie den Befehl `rpm -q openssh-askpass-gnome`. Installieren Sie das Paket von Ihrem Red Hat Enterprise Linux CD-ROM-Set, von einer Red Hat FTP Mirror-Site oder vom Red Hat Network für den Fall, dass es nicht vorhanden ist.
2. Wählen Sie den **Hauptmenü-Button** (auf dem Panel) => **Extras** => **Präferenzen** => **Sitzungen**, und klicken Sie auf **Startup Programme**. Klicken Sie auf **Hinzufügen** und geben Sie **`/usr/bin/ssh-add`** in den Textbereich **Start-Befehl** ein. Die Prioritätzahl für diesen Befehls muss höher sein als für alle anderen Befehle, damit sichergestellt wird, dass dieser Befehl zuletzt ausgeführt wird. Eine gute Prioritätszahl für `ssh-add` ist 70 oder höher. Je höher diese Zahl ist, umso niedriger ist die Priorität. Sollten noch andere Programme aufgelistet sein, sollte dies die niedrigste Priorität haben. Klicken Sie auf **Schließen** um das Programm zu beenden.
3. Melden Sie sich aus GNOME ab und wieder an. Mit anderen Worten, starten Sie X erneut. Nachdem GNOME wieder gestartet wurde, erscheint ein Dialogfeld und Sie werden aufgefordert, Ihr Passwort einzugeben. Wenn Sie DSA und RSA- Schlüsselpaare konfiguriert haben, müssen Sie für beide Schlüsselpaare das Passwort eingeben. Ab diesem Zeitpunkt sollten Sie von `ssh`, `scp`, or `sftp` nicht mehr aufgefordert werden, ein Passwort einzugeben.

22.3.4.5. Konfigurieren von `ssh-agent`

Der `ssh-agent` kann zum Speichern Ihres Passwortes verwendet werden. Somit müssen Sie das Passwort nicht jedesmal eingeben, wenn Sie eine `ssh` oder `scp`-Verbindung starten. Wenn Sie das X Window System nicht ausführen, führen Sie die folgenden Schritte vom Shell-Prompt aus durch. Wenn Sie GNOME ausführen, aber nicht so konfigurieren möchten, das Sie beim Anmelden aufgefordert werden, das Passwort einzugeben, (siehe Abschnitt 22.3.4.4) wird die Prozedur in einem Terminalfenster wie zum Beispiel einem XTerm ausgeführt. Wenn Sie X, jedoch nicht GNOME ausführen, wird dieses Verfahren in einem Terminalfenster ausgeführt. Ihr Passwort wird dann jedoch nur für dieses Terminalfenster wiedererkannt. Es handelt sich also nicht um eine globale Einstellung.

1. Geben Sie am Shell-Prompt folgenden Befehl ein:
   ```
   exec /usr/bin/ssh-agent $SHELL
   ```
2. Und anschließend den Befehl:
   ```
   ssh-add
   ```
   Geben Sie nun Ihr Passwort/Passwörter ein. Wenn Sie mehr als ein Schlüsselpaar konfiguriert haben, müssen Sie die Passwörter entsprechend für jedes Paar eingeben.
3. Wenn Sie sich abmelden, geht Ihr Passwort verloren. Sie müssen diese beiden Befehle immer wieder ausführen, wenn Sie sich in einer virtuellen Konsole anmelden oder ein Terminalfenster öffnen.

22.4. Zusätzliche Ressourcen

Die Projekte OpenSSh und OpenSSL werden ständig weiterentwickelt. Sie finden daher die aktuellsten Informationen in den entsprechenden Websites. Eine weitere Quelle für detaillierte Informationen sind die man-Seiten von OpenSSH und OpenSSL.

22.4.1. Installierte Dokumentation

- Die man-Seiten `ssh`, `scp`, `sftp`, `sshd` und `ssh-keygen` — Diese man-Seiten enthalten Informationen über die Verwendung dieser Befehle sowie alle Parameter, die für diese Befehle verwendet werden können.

22.4.2. Hilfreiche Websites

- http://www.openssh.com/ — Die OpenSSH FAQ-Seite, Bug-Berichte, Mailinglisten, Projektziele und eine eher technische Beschreibung der Sicherheitsmerkmale.
- http://www.openssl.org/ — Die OpenSSL FAQ-Seite, Mailing-Lists und Beschreibungen der Projektziele.
- http://www.freessh.org/ — SSH-Client-Software für andere Plattformen.

22.4.3. Bücher zum Thema

- *Red Hat Enterprise Linux Referenzhandbuch* — Erfahren Sie mehr über den Event-Ablauf einer SSH-Verbindung, sehen Sie eine Liste der Konfigurationsdateien und entdecken Sie, wie SSH für das X-Forwarding eingesetzt werden kann.

Kapitel 23.

Network File System (NFS)

Das Network File System (NFS) bietet die Möglichkeit, Dateien zwischen den Rechnern eines Netzwerks gemeinsam zu benutzen, als ob sie auf Ihrer lokalen Festplatte gespeichert wären. Red Hat Enterprise Linux kann dabei sowohl ein NFS-Server als auch ein NFS-Client sein, d.h. kann Dateisysteme in andere Systeme exportieren und aus anderen Rechnern importierte Dateisysteme mounten.

23.1. Warum sollte man NFS verwenden?

NFS dient der gemeinsamen Nutzung von Dateiverzeichnissen unter mehreren Benutzern desselben Netzwerks. Zum Beispiel kann eine Gruppe Benutzer, die am gleichen Projekt arbeiten, Zugriff auf einen gemeinsamen Teil des NFS-Systems im Verzeichnis `/myproject` haben. Um auf die gemeinsam genutzten Dateien zuzugreifen, ruft der Benutzer das Verzeichnis `/myproject` auf seinem Rechner auf. In diesem Fall müssen keine Passwörter oder spezielle Programme eingegeben werden. Der Benutzer arbeitet in diesem Verzeichnis, als ob es sich tatsächlich in seinem lokalen System befinden würde.

23.2. Mounten eines NFS-Dateisystems

Verwenden Sie den Befehl `mount`, um ein NFS-Dateisystem eines anderen Rechners zu mounten:

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

Warnung

Das Mount-Punkt Verzeichnis auf dem lokalen Rechner (`/misc/local` im obigen Beispiel) muss existieren.

In diesem Befehl ist `shadowman.example.com` der Rechnername des NFS Dateiservers, `/misc/export` ist das Dateisystem, das `shadowman` exportiert, und `/misc/local` ist das Verzeichnis des lokalen Rechners, wo das Dateisystem gemountet werden soll. Nachdem der Befehl `mount` aktiviert wurde (und wenn `shadowman.example.com` die notwendigen Berechtigungen erteilt hat), können Sie `ls/misc/local` eingeben, um eine Liste der Dateien in `/misc/export` auf `shadowman.example.com` abzurufen.

23.2.1. Mounten des NFS-Dateisystems mit `/etc/fstab`

Eine andere Möglichkeit, ein NFS-Dateisystem eines anderen Rechners zu mounten, besteht darin, in Ihrer Datei `/etc/fstab` eine Zeile hinzuzufügen. In dieser Zeile muss der Rechnername des NFS-Servers, das zu exportierende Verzeichnis auf dem Server und das Verzeichnis auf dem lokalen Rechner angegeben werden, in das das Dateisystem gemountet werden soll. Beachten Sie, dass Sie als root-Benutzer angemeldet sein müssen, um die Datei `/etc/fstab` bearbeiten zu können.

Die allgemeine Syntax für die Zeile in `/etc/fstab` lautet:

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

Der Mount-Punkt `/pub` muss auf Ihrem Rechner vorhanden sein. Nachdem Sie die Zeile in `/etc/fstab` hinzugefügt haben, können Sie den Befehl `mount /pub` an der Shell-Prompt eingeben. Der Mount-Punkt `/pub` wird nun vom Server gemountet.

23.2.2. Mounten des NFS-Dateisystems mit autofs

Weiterhin besteht die Möglichkeit, ein NFS-Dateisystem mithilfe von autofs zu mounten. Autofs verwendet zur Verwaltung Ihrer Mount-Punkte den automount-Daemon, indem er diese dynamisch mountet, wenn auf sie zugegriffen wird.

Autofs bestimmt anhand der Master Map Konfigurationsdatei `/etc/auto.master`, welche Mount-Punkte definiert werden. Anschließend wird automount mit den für jeden Mount-Punkt entsprechenden Parametern gestartet. Jede Zeile im Master Map kennzeichnet einen Mount-Punkt und eine separate Map-Datei, die bestimmt, welche Dateisysteme unter diesem Mount-Punkt gemountet werden sollen. Die Datei `/etc/auto.misc` zum Beispiel kann Mount-Punkte im Verzeichnis `/misc` definieren. Diese Beziehung wird entsprechend in der Datei `/etc/auto.master` bestimmt.

Jeder Eintrag in `auto.master` besitzt drei Felder. Das erste Feld entspricht dem Mount-Punkt, das zweite der Speicherstelle der Map-Datei, und das dritte Feld ist optional und kann Informationen wie zum Beispiel einen Wert der Zeitüberschreitung enthalten.

Um beispielsweise das Verzeichnis `/proj52` des Remote-Rechners penguin.example.net am Mount-Punkt `/misc/myproject` in Ihrem System zu mounten, fügen Sie die folgende Zeile in `auto.master` hinzu:

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

Fügen Sie in `/etc/auto.misc` die folgende Zeile hinzu:

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

Das erste Feld in `/etc/auto.misc` ist der Name des `/misc` Unterverzeichnisses. Dieses Verzeichnis wird dynamisch durch das automount erstellt und sollte im Client-Rechner nicht existieren. Das zweite Feld enthält Optionen zum Mounten wie `rw` für den Lese- und Schreibzugriff. Das dritte Feld ist die Speicherstelle des NFS-Exports einschließlich des Rechnernamens und des Verzeichnisses.

Anmerkung

Das Verzeichnis `/misc` muss im lokalen Dateisystem vorhanden sein. Hier sollten jedoch keine Unterverzeichnisse im `/misc` bestehen.

Autofs ist ein Dienst. Um diesen Dienst zu starten, geben Sie die folgenden Befehle am Shell-Prompt ein:

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

Um die aktivierten Mount-Punkte zu sehen, geben Sie am Shell-Prompt folgenden Befehl ein:

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

Wenn Sie die `/etc/auto.master` Konfigurationsdatei ändern, während autofs ausgeführt wird, müssen Sie den automount-Daemon zum Neuladen anweisen. Geben Sie hierzu den folgenden Befehl am Shell-Prompt ein:

```
/sbin/service autofs reload
```

Informationen darüber, wie Sie autofs konfigurieren müssen, um diesen beim Booten zu starten, finden Sie in Kapitel 21.

23.2.3. TCP verwenden

The default transport protocol for NFS is UDP; however, the Red Hat Enterprise Linux 3 kernel includes support for NFS over TCP. To use NFS over TCP, include the `-o tcp` option to `mount` when mounting the NFS-exported file system on the client system. For example:

```
mount -o tcp shadowman.example.com:/misc/export /misc/local
```

Wenn der NFS-Mount in `/etc/fstab` angegeben ist:

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

Wenn es in einer autofs-Konfigurationsdatei angegeben:

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

Da der Standard UDP ist, wird, wenn die Option `-o tcp` nicht angegeben ist, auf das aus NFS-exportierte Dateisystem über UDP zugegriffen.

Die Vorteile von TCP sind unter anderem folgende:

- Verbesserte Verbindungsdauer und dadurch weniger `NFS stale file handles`-Nachrichten.
- Leistungsanstieg für schwerbelastete Netzwerke, da TCP jedes Paket erkennt, im Gegensatz zu UDP, das nur die Vervollständigung anerkennt.
- TCP hat bessere Optionen für Engpässe als UDP (UDP hat keine). Auf einem verstopften Netzwerk werden die UDP-Pakete als erstes fallen gelassen. Was bedeutet, dass falls NFS Daten schreibt (in 8K Blöcken), die gesamten 8K neu übertragen werden müssen. Durch die Verlässlichkeit von TCP wird nur ein Teil dieser 8K auf einmal übertragen.
- Fehlererkennung. Bricht eine tcp-Verbindung (durch einen Serverausfall), stoppt der Client die Datenübertragung und startet den Verbindungsaufbau. Mit dem verbindungslosen UDP fährt der Client mit dem Senden von Daten fort, bis der Server wieder aufgebaut ist.

Der Hauptnachteil ist, dass es winzige Leistungseinbußen aufgrund des Überhangs durch das TCP-Protokoll gibt.

23.2.4. ACLs erhalten

Der Red Hat Enterprise Linux 3 Kernel bietet ACL-Support für das ext3-Dateisystem und ext3-Dateisysteme, die mit NFS oder Samba-Protokollen gemountet sind. Aus diesem Grund können, wenn ein ext3-Dateisystem über NFS von einem Server, der ACLs unterstützt, exportiert und von einem Client der NFS Share gemountet werden, diese ACLS vom NFS-Client aus zugegriffen werden.

Weitere Informationen über das Mounten von NFS-Dateisystemen mit ACLs finden Sie unter Kapitel 8.

23.3. Exportieren des NFS-Dateisystems

Die gemeinsame Nutzung von Verzeichnissen eines NFS-Servers ist als Exportieren der Verzeichnisse bekannt. Das **NFS Server Configuration Tool** kann dazu verwendet werden, ein System als NFS-Server zu konfigurieren.

Um **NFS Server Configuration Tool** verwenden zu können, müssen Sie das X Window System laufen haben, über root-Berechtigungen verfügen und das RPM-Paket `redhat-config-nfs` muss installiert sein. Um die Applikation zu starten, wählen Sie **Hauptmenü** (im Panel) **=> Systemeinstellungen => Servereinstellungen => NFS** oder geben Sie den Befehl `redhat-config-nfs` ein.

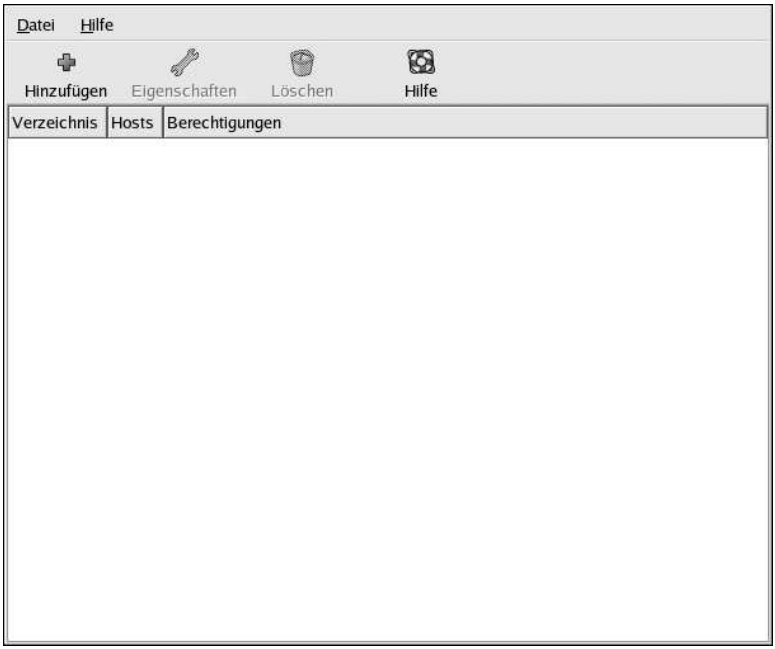

Abbildung 23-1. NFS Server Configuration Tool

Um NFS ein gemeinsam zu nutzendes Verzeichnis (Share) hinzuzufügen, klicken Sie auf den Button **Hinzufügen**. Das in Abbildung 23-2 abgebildete Dialogfeld erscheint.

Das Tab **Basis** verlangt folgende Information:

- **Verzeichnis** — Geben Sie das Share an sowie `/tmp`.
- **Host(s)** — Geben Sie den/die Host(s) an, mit denen das Verzeichnis gemeinsam genutzt werden soll. Erklärungen zu möglichen Formaten finden Sie unter Abschnitt 23.3.2.
- **Basisgenehmigungen** — geben Sie an, ob das Verzeichnis nur schreibgeschützt sein soll oder Schreib-und Lesezugriffe erlaubt sind.

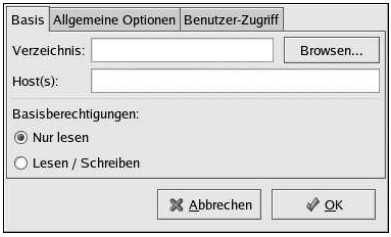

Abbildung 23-2. Share hinzufügen

Das Tab **Allgemeine Optionen** erlaubt die Konfigurationen folgender Optionen:

- **Verbindungen von Port 1024 und höher zulassen** — Dienste, die von Port-Nummern starten, die niedriger sind als 1024 müssen als root gestartet werden. Wählen Sie diese Option um dem NFS-Dienst zu erlauben, von einem Benutzer gestartet zu werden, der kein root ist. Diese Option entspricht `insecure`.
- **Sperren nicht gesicherter Dateien zulassen** — Verlangen Sie keine Sperranfrage. Diese Option entspricht `insecure_locks`.
- **Subtree-Prüfung deaktivieren** — wird das Unterverzeichnis eines Dateisystems exportiert, jedoch nicht das gesamte Dateisystem, prüft der Server, ob sich die verlangte Datei im exportierten Unterverzeichnis befindet. Diese Prüfung wird als *Subtree-Prüfung* bezeichnet. Wählen Sie diese Option, um die Subtree-Prüfung zu deaktivieren. Wird das gesamte Dateisystem exportiert, kann das Deaktivieren der Subtree-Prüfung die Übertragungsrate erhöhen. Diese Option entspricht dem Befehl `no_subtree_check`.
- **Sync-Schreibvorgänge auf Anfrage** — Standardmäßig aktiviert, erlaubt es diese Option dem Server nicht, auf Anfragen zu antworten, bevor die durch die Anfrage verursachten Änderungen auf die Platte geschrieben wurden. Diese Option entspricht `sync`. Wird sie nicht gewählt, wird die Option `async` verwendet.
  - **Sync der Schreibvorgänge sofort erzwingen** — Das Schreiben auf die Platte soll nicht verschoben werden. Diese Option entspricht `no_wdelay`.

Das Tab **Benutzerzugriff** erlaubt die Konfiguration folgender Optionen:

- **Remote root-Benutzer wie lokalen root behandeln** — standardmäßig sind der Benutzer und die Gruppen-IDs des root-Benutzers beide 0. Das Zusammenlegen von roots bewirkt, dass die Benutzer-ID 0 und die Gruppen ID 0 den anonymen Benutzer- und Gruppen-IDs zugeordnet werden, so dass ein root bei einem Kunden keine root-Vorrechte an einem NFS-Server bedeutet. Wird diese Option gewährt, wird der root nicht als anonym eingestuft, und ein root bei einem Kunden bedeutet root-Vorrechte beim Exportieren von Verzeichnissen. Die Auswahl dieser Option kann die Sicherheit des Systems erheblich mindern. Wählen Sie diese nur, wenn unbedingt notwendig. Diese Option entspricht `no_root_squash`.
- **Alle Client-Benutzer wie Anonymous-Benutzer behandeln** — wird diese Option gewählt, werden alle Benutzer- und Gruppen IDs den anonymen Benutzern zugeordnet. Diese Option entspricht `all_squash`.
  - **Lokale Benutzer-ID für Anonymous-Benutzer angeben** — wurde **Alle Client-Benutzer wie Anonymous-Benutzer behandeln** gewählt, können Sie anhand dieser Option eine Benutzer-ID für den anonymen Benutzer angeben. Diese Option entspricht `anonuid`.

- **Lokale Gruppen-ID für Anonymous-Benutzer angeben** — wurde **Alle Client-Benutzer wie Anonymous-Benutzer behandeln** gewählt, können Sie anhand dieser Option eine Gruppen-ID für den anonymen Benutzer angeben. Dieser Option entspricht `anongid`.

Wählen Sie zur Bearbeitung einer vorhandenen NFS-Share diese Share aus der Liste und klicken Sie auf den Button **Eigenschaften**. Um eine bestehende NFS-Share zu löschen, wählen Sie diese aus der Liste und klicken Sie den Button **Löschen** .

Nach dem Sie nach dem Hinzufügen, Bearbeiten oder Löschen eines NFS-Shares auf **OK** geklickt haben, werden die Änderungen sofort wirksam — der Server-Daemon wird neu gestartet und die alte Konfigurationsdatei unter `/etc/exports.bak` gespeichert. Die neue Konfigurationsdatei wird in die Datei `/etc/exports` geschrieben.

Das **NFS Server Configuration Tool** liest und schreibt direkt auf die `/etc/exports` Konfigurationsdatei. Das heißt die Datei kann nach Verwendung des Tools manuell geändert werden und das Tool kann verwendet werden, nachdem die Datei manuell modifiziert wurde (vorausgesetzt die Datei wurde mit korrekter Syntax modifiziert).

23.3.1. Befehlszeilenkonfiguration

Wenn Sie es vorziehen, Konfigurationsdateien mit einem Text-Editor zu bearbeiten oder wenn Sie das X Window System nicht installiert haben, können Sie die Konfigurationsdatei direkt ändern.

Die Datei `/etc/exports` prüft, welche Verzeichnisse der NFS-Server exportiert. Das Format ist folgendes:

```
directory hostname(options)
```

Die einzige Option, die angegeben werden muss, ist entweder `sync` oder `async` (`sync` wird empfohlen). Wenn `sync` angegeben wird, antwortet der Server nicht auf Anfragen, bis die Änderungen der Anfrage auf die Festplatte geschrieben wurde.

Beispiel:

```
/misc/export      speedy.example.com(sync)
```

würde den Benutzern von `speedy.example.com` erlauben, `/misc/export` mit den standardmäßigen schreibgeschützten Genehmigungen zu mounten, aber

```
/misc/export      speedy.example.com(rw,sync)
```

würde die Benutzer von `speedy.example.com` dazu veranlassen, `/misc/export` im Lese- und Schreib-Modus zu mounten.

Erklärungen zu möglichen Hostnamen-Formaten finden Sie unter Abschnitt 23.3.2.

Im *Red Hat Enterprise Linux Referenzhandbuch* finden Sie eine Liste der Optionen, dieangegeben werden können.

Achtung

Seien Sie mit den Leerzeichen in der Datei `/etc/exports` vorsichtig. Wenn sich zwischen dem Hostnamen und den in Klammern stehenden Optionen keine Leerzeichen befinden, dann betreffen die Optionen nur den Hostname. Wenn sich hingegen zwischen dem Hostname und den Optionen Leerzeichen befinden, gelten die Optionen für alles. Schauen Sie sich z.B. die folgenden Zeilen an:

```
/misc/export speedy.example.com(rw,sync)
/misc/export speedy.example.com (rw,sync)
```

Mit der ersten Zeile erhalten die Benutzer von `speedy.example.com` Lese-/Schreibzugriff, während allen anderen Benutzern der Zugriff verwehrt ist. Mit der zweiten Zeile erhalten die Benutzer von `speedy.example.com` schreibgeschützten Zugriff (der Standard) und alle anderen Lese-/Schreibzugriff.

Jedes Mal, wenn Sie `/etc/exports` ändern, müssen Sie den NFS-Daemon über die Änderung informieren oder die Konfigurationsdatei mit folgendem Befehl neu laden:

```
/sbin/service nfs reload
```

23.3.2. Hostnamen-Formate

Der/die Host(s) können folgende Formen annehmen:

- Einzelrechner — ein vollberechtigter Domain-Name (der vom Server entschieden werden kann), Hostname (der vom Server entschieden werden kann) oder eine IP-Adresse
- Reihen von Maschinen, die über Wildcards angegeben werden — Verwenden Sie * oder ?, um eine Zeichenkette anzugeben. Wildcards dürfen nicht mit IP-Adressen verwender werden; diese können jedoch funktionieren, wenn ein Reverse DNS Lookup fehlschlägt. Wenn Sie Wildcards in Domainnamen angeben, werden Punkte (.) nicht mit angegeben. Beipsiel: `*.example.com` enthält one.example.com jedoch nicht one.two.example.com.
- IP-Netzwerke — Verwenden Sie *`a.b.c.d/z`*, wobei *`a.b.c.d`* das Netzwerk ist und *`z`* die Anzahl von Bits in der Netmask (zum Beispiel 192.168.0.0/24). Ein weiteres akzeptables Format ist *`a.b.c.d/netmask`*, wobei *`a.b.c.d`* das Netzwerk ist und *`netmask`* die Netmask (zum Beispiel 192.168.100.8/255.255.255.0).
- Netzgruppen — Im Format *`@Gruppen-Name`*, wobei *`Gruppen-Name`* der NIS-Netzgruppenname ist.

23.3.3. Den Server starten und stoppen

Auf dem Server, der die NFS-Dateiensysteme exportiert, muss der Dienst `nfs` ausgeführt werden.

Zeigen Sie den Status des NFS-Daemons mit folgendem Befehl an:

```
/sbin/service nfs status
```

Starten Sie den NFS-Daemon mit folgendem Befehl:

```
/sbin/service nfs start
```

Stoppen Sie den NFS-Daemon mit folgendem Befehl:

```
/sbin/service nfs stop
```

Um den Dienst `nfs` zum Boot-Zeitpunkt zu starten, erteilen Sie folgenden Befehl:

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

Sie können auch `chkconfig`, **ntsysv** oder das **Services Configuration Tool** verwenden, um zu konfigurieren, welche Dienste zum Boot-Zeitpunkt starten sollen. Details können Sie dem Kapitel 21 entnehmen.

23.4. Zusätzliche Ressourcen

Dieses Kapitel liefert Basisinformationen für die Verwendung von NFS. Detailliertere Informationen finden Sie in den folgenden Quellen.

23.4.1. Installierte Dokumentation

- Die man-Seiten für `nfsd`, `mountd`, `exports`, `auto.master` und `autofs` (in den Kapiteln 5 und 8 des Handbuchs) — Auf diesen man-Seiten wird die korrekte Syntax für die Konfigurationsdateien NFS und autofs angegeben.

23.4.2. Nützliche Websites

- http://nfs.sourceforge.net/ — Die NFS Webseite, enthaält Links zu Mailinglisten und FAQs.
- http://www.tldp.org/HOWTO/NFS-HOWTO/index.html — der *Linux NFS-HOWTO* aus dem Linux-Dokumentationsprojekt.

23.4.3. Zusätzliche Literatur

- *Managing NFS and NIS Services* von Hal Stern; O'Reilly & Associates, Inc.

Kapitel 24.

Samba

Samba verwendet das SMB-Protokoll zur gemeinsamen Nutzung von Dateien und Druckern über eine Netzwerkverbindung. Betriebssysteme, die dieses Protokoll unterstützen, sind Microsoft Windows, OS/2 und Linux.

Der Red Hat Enterprise Linux 3 Kernel enthält *Zugriffskontrolllisten* (ACL) Support für ext3-Dateisysteme. Wenn der Samba-Server eine ext3-Dateisystem bereitstellt, das ACLs aktiviert hat, und der Kernel auf dem Client-System enthält Support zum Lesen der ACLs von ext3-Dateisystemen, wird der Client diese ACLs automatisch erkennen und verwenden. Siehe Kapitel 8 für weitere Informationen zu ACLs.

24.1. Warum sollte man Samba verwenden?

Samba ist nützlich, wenn Sie über ein Netzwerk mit Windows- und Linux-Rechnern verfügen. Samba ermöglicht allen Systemen in Ihrem Netzwerk die gemeinsame Nutzung von Dateien und Druckern. Wenn Sie Dateien ausschließlich auf Linux-Rechnern gemeinsam nutzen möchten, verwenden Sie NFS wie unter Kapitel 23 beschrieben. Wenn Sie Drucker ausschließlich auf Linux-Rechnern gemeinsam nutzen möchten, müssen Sie Samba nicht verwenden; Informationen hierzu finden Sie unter Kapitel 36.

24.2. Konfiguration eines Samba-Servers

Samba verwendet standardmäßig die Konfigurationsdatei (`/etc/samba/smb.conf`), die Benutzern ermöglicht, ihre Home-Verzeichnisse aus Samba-Share anzuzeigen. Konfigurierte Drucker können unter Samba als gemeinsame Drucker verwendet werden. Anders ausgedrückt: Sie können einen Drucker an Ihr System anschließen und von einem Windows-Rechner aus über Ihr Netzwerk mit ihm drucken.

24.2.1. Grafische Konfiguration

Um Samba mit einer grafischen Benutzeroberfläche zu konfigurieren, verwenden Sie das **Samba Server Configuration Tool**. Für die Befehslzeilenkonfiguration gehen Sie zu Abschnitt 24.2.2.

Das **Samba Server Configuration Tool** ist eine grafische Benutzeroberfläche zum Verwalten von Samba Shares, Benutzern und allgemeinen Servereinstelllungen. Es ändert die Konfigurationsdateien im Verzeichnis `/etc/samba/`. Jegliche Änderungen, die ohne die Applikation durchgeführt wurden, werden erhalten.

Um diese Applikation verwenden zu können, müssen Sie das X Window System ausführen, über root-Berechtigungen verfügen und das `redhat-config-samba` RPM-Paket installiert haben. Um das **Samba Server Configuration Tool** vom Desktop aus zu starten, gehen Sie zum **Hauptmenü** (im Panel) => **Extras** => **Servereinstellungen** => **Samba Server** oder geben Sie den Befehl `redhat-config-samba` an einem Shell-Prompt (z.B. XTerm oder GNOME Terminal) ein.

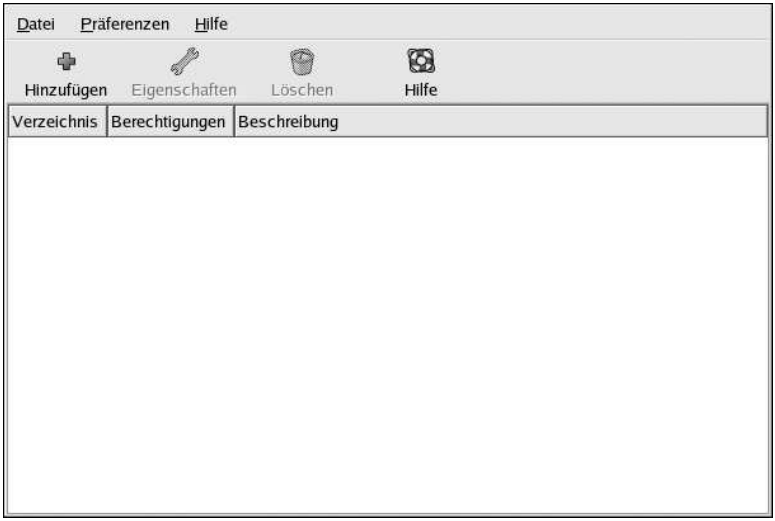

Abbildung 24-1. Samba Server Configuration Tool

Anmerkung

Das **Samba Server Configuration Tool** zeigt keine gemeinsamen Drucker oder Default Stanza, mit der Benutzer ihr Home-Verzeichnis auf dem Samba-Server ansehen können.

24.2.1.1. Servereinstellungen konfigurieren

Der erste Schritt bei der Konfiguration eines Samba-Servers ist das Konfigurieren der Grundeinstellungen für den Server und einige Sicherheitsoptionen. Nachdem Sie die Applikation gestartet haben, wählen Sie aus dem Pull-Down-Menü **Präferenzen** => **Servereinstellungen**. Der Tab **Basis** wird wie in Abbildung 24-2 abgebildet angezeigt.

Abbildung 24-2. Servereinstellungen konfigurieren

Geben Sie auf dem Tab **Basis** ein, welcher Arbeitsgruppe der Computer zugehören soll, sowie eine Kurzbeschreibung des Computers. Dies entspricht den Optionen in `workgroup` und `server string` in der Datei `smb.conf`.

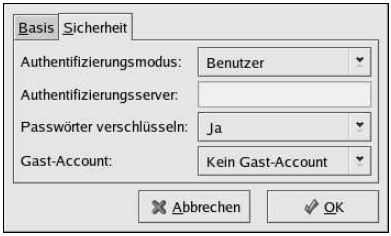

Abbildung 24-3. Sicherheitseinstellungen des Servers konfigurieren

Der Tab **Sicherheit** enthält die folgenden Optionen:

- **Authentifizierungsmodus** — Dies entspricht der `security`-Option. Wählen Sie einen der folgenden Authentifizierungstypen.
  - **ADS** — Der Samba-Server agiert als Domain-Member im Realm einer Active Directory Domain (ADS). Für diese Option, muss Kerberos auf dem Server installiert und konfiguriert sein, und Samba muss ein Member des ADS Realm werden, unter Verwendung des `net`-Utility, das Teil des Pakets `samba-client` ist. Sehen Sie die `net` man-Seiten für Weiteres. Diese Option konfiguriert Samba nicht als ADS-Controller.
  - **Domain** — Der Samba-Server verlässt sich auf einen Windows NT Primary oder Backup Domain Controller, um den Benutzer zu authentifizieren. Der Server gibt den Benutzernamen und das Passwort an den Controller weiter und wartet auf die Rückgabe. Geben Sie den NetBIOS Namen des Primary oder Backup Domain Controller im Feld **Authentifizierungsserver** an.

    Die Option **Verschlüsselte Passwörter** muss auf **Ja** gesetzt sein, wenn dies ausgewählt ist.
  - **Server** — Der Samba-Server versucht den Benutzernamen und das Passwort durch Weitergabe an einen anderen Samba-Server zu authentifizieren. Wird dies nicht erkannt, versucht der Server die Authentifikation durch den Benutzer-Authentifizierungsmodus. Geben Sie den NetBIOS Namen des anderen Samba-Server im Feld **Authentifizierungsserver** ein.
  - **Share** — Samba-Benutzer müssen ihren Benutzernamen und ihr Passwort nicht für jeden Server eingeben. Sie werden nicht zur Eingabe eines Benutzernamens und eines Passworts aufgefordert, bis Sie versuchen, auf ein bestimmtes, gemeinsames Verzeichnis auf einem Samba-Server zuzugreifen.
  - **Benutzer** — (Standard) Samba-Benutzer müssen einen gültigen Benutzernamen und ein Passwort pro Samba-Server eingeben. Wählen Sie diese Option, wenn Sie die Option **Windows Benutzername** verwenden möchten. Informationen hierzu finden Sie unter Abschnitt 24.2.1.2.

- **Passwörter verschlüsseln** — Diese Option muss aktiviert sein, wenn die Clients Windows 98, Windows NT 4.0 mit Service Pack 3 oder andere, neuere Versionen von Microsoft Windows verwenden. Die Passwörter werden zwischen dem Server und dem Client verschlüsselt anstelle von Klartext übertragen, was die Sicherheit erhöht. Dies entspricht der Option `encrypted passwords`. Weitere Informationen zu verschlüsselten Samba-Passwörtern finden Sie unter Abschnitt 24.2.3.
- **Gast-Account** — Wenn sich Benutzer oder Gastbenutzer an einem Samba-Server anmelden, müssen diese zu einem gültigen Benutzer auf dem Server "gemappt" werden. Wählen Sie einen

der bestehenden Benutzernamen im System, der dann den Gastaccount für Samba bietet. Wenn sich Gäste im Samba-Server anmelden, haben diese die gleichen Rechte wie dieser Benutzer. Dies entspricht der Option `guest account`.

Nachdem Sie auf **OK** geklickt haben, werden die Änderungen in die Konfigurationsdatei geschrieben und der Daemon wird neu gestartet. Die Änderungen werden sofort wirksam.

24.2.1.2. Verwaltung von Samba-Benutzern

Das **Samba Server Configuration Tool** benötigt einen bestehenden Benutzeraccount, der im System aktiv ist und sich als Samba-Server verhält, bevor ein Samba-Benutzer hinzugefügt werden kann. Der Samba-Benutzer wird dann mit dem bestehenden Benutzeraccount assoziiert.

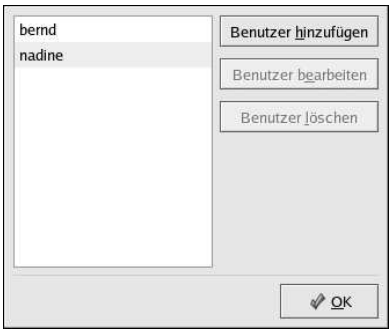

Abbildung 24-4. Verwaltung von Samba-Benutzern

Um einen Samba-Benutzer hinzuzufügen, wählen Sie **Präferenzen** => **Samba-Benutzer** aus dem Pull-Down-Menü und klicken Sie auf **Benutzer hinzufügen**. Im Fenster **Neuen Samba-Benutzer anlegen** wählen Sie einen **Unix Benutzernamen** aus der Liste der bestehenden Benutzer im lokalen System.

Wenn der Benutzer einen anderen Benutzernamen auf einem Windowsrechner hat, und sich in den Samba-Server von diesem Windowsrechern aus anmelden, geben Sie diesen Windows-Benutzernamen im Feld **Windows-Benutzername** an. Der **Authentifizierungsmodus** im **Sicherheit** Tab der **Servereinstellungen** muss auf **Benutzer** gesetzt sein.

Konfigurieren Sie auch ein **Samba Passwort** für diesen Samba-Benutzer und bestätigen Sie das Passwort, indem Sie es noch einmal eingeben. Auch wenn Sie verschlüsselte Passwörter für Samba verwenden, sollten die Passwörter für alle Samba-Benutzer sich von denen für das System unterscheiden.

Um einen bestehenden Benutzer zu bearbeiten, wählen Sie diesen Benutzer aus der Liste aus und klicken Sie auf **Benutzer bearbeiten**. Um einen bestehenden Samba-Benutzer zu löschen, wählen Sie den Benutzer aus und klicken Sie auf **Benutzer löschen**. Das Löschen eines Samba-Benutzers löscht nicht den Benutzeraccount dieses Benutzers.

Sie Benutzereinstellungen werden geändert, sobald Sie auf **OK** klicken.

24.2.1.3. Share hinzufügen

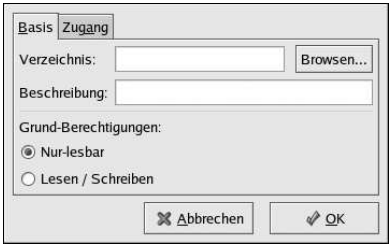

Abbildung 24-5. Share hinzufügen

Um einen Share hinzuzufügen, klicken Sie auf **Hinzufügen**. Der **Basis** Tab konfiguriert folgende Optionen:

- **Verzeichnis** — Das gemeinsam über Samba zu verwendende Verzeichnis. Das Verzeichnis muss vorhanden sein.
- **Beschreibung** — Eine kurze Beschreibung des Shares.
- **Grund-Berechtigungen** — Legt Nur-Lese oder Schreib- und Leseberechtigungen für Benutzer auf den gemeinsam verwendeten Verzeichnissen fest.

Auf dem Tab **Zugang** können Sie wählen, ob nur bestimmte Benutzer Zugriff auf den Share haben sollen oder ob alle Samba-Benutzer hierauf zugreifen dürfen. Wenn Sie nur bestimmten Benutzern Zugang erlauben wollen, wählen Sie deren Namen aus der Liste der verfügbaren Samba-Benutzer.

Der Share wird sofort nach dem Klicken auf **OK** hinzugefügt.

24.2.2. Befehlszeilenkonfiguration

Samba verwendet `/etc/samba/smb.conf` als Konfigurationsdatei. Wenn Sie diese Konfigurationsdatei ändern, werden diese Änderungen erst dann wirksam, wenn Sie den Samba-Daemon mit dem Befehl `service smb restart` neu starten.

Um die Windows-Arbeitsgruppe und deren Beschreibung für Samba festzulegen, bearbeiten Sie die folgenden Zeilen in der Datei `smb.conf`:

```
workgroup = WORKGROUPNAME
server string = BRIEF COMMENT ABOUT SERVER
```

Ersetzen Sie *WORKGROUPNAME* mit dem Namen der Windows-Arbeitsgruppe, zu der der Rechner gehören soll. *BRIEF COMMENT ABOUT SERVER* ist optional und stellt den Windows-Kommentar zum Samba-System dar.

Um ein gemeinsam genutztes Verzeichnis für Samba auf Ihrem Linux- System zu erstellen, fügen Sie den folgenden Bereich zu Ihrer `smb.conf`-Datei hinzu (nachdem Sie diese Datei an Ihre Bedürfnisse und Ihr System angepasst haben):

```
[sharename]
comment = Insert a comment here
path = /home/share/
valid users = tfox carole
public = no
```

```
writable = yes
printable = no
create mask = 0765
```

Dieses Beispiel erlaubt den Benutzern tfox und carole von einem Samba-Client aus, das Verzeichnis `/home/share` im Samba- Server zu lesen und darin zu schreiben.

24.2.3. Verschlüsselte Passwörter

Verschlüsselte Passwörter sind standardmäßig aktiviert, da dies sicherer ist. Werden keine verschlüsselten Passwörter verwendet, werden Passwörter im Klartext verwendet, die von anderen mithilfe von Netzwerk Packet Sniffern abgefangen werden können. Die Verwendung von verschlüsselten Passwörter wird empfohlen.

Das Microsoft SMB-Protokoll verwendete ursprünglich Klartext-Passwörter. Windows 2000 und Windows NT 4.0 mit Service Pack 3 oder höher, Windows ME und Windows XP erfordern jedoch verschlüsselte Samba-Passwörter. Um Samba zwischen einem Linux-System und einem dieser Windows-Systeme zu verwenden, können Sie entweder die Windows-Registrierung bearbeiten, so dass Klartext-Passwörter verwendet werden, oder Samba auf Ihrem Linux- System konfigurieren, so dass verschlüsselte Passwörter verwendet werden. Wenn Sie die Registrierung ändern, müssen Sie dies für alle unter Windows laufenden Rechner tun — dies ist risikoreich und kann Konflikte hervorrufen. Aufgrund höherer Sicherheit sind verschlüsselte Passwörter zu empfehlen.

Um Samba zur Verwendung verschlüsselter Passwörter zu konfigurieren, führen Sie folgende Schritte aus:

1. Erstellen Sie eine separate Passwortdatei für Samba. Um eine auf der vorhandenen Datei `/etc/passwd` basierende Datei zu erstellen, geben Sie am Shell-Prompt folgenden Befehl ein:
   ```
   cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   Wenn das System NIS verwendet, geben Sie folgenden Befehl ein:
   ```
   ypcat passwd | mksmbpasswd.sh > /etc/samba/smbpasswd
   ```
   Das Skript `mksmbpasswd.sh` ist im Verzeichnis `/usr/bin` mit dem `samba`-Paket installiert.
2. Ändern Sie die Berechtigungen in der Samba-Passwortdatei, so dass nur der unter einem root-Account angemeldete Benutzer über Lese- und Schreibzugriff verfügt:
   ```
   chmod 600 /etc/samba/smbpasswd
   ```
3. Das Skript kopiert die Benutzerpasswörter nicht in die neue Datei, und der Samba-Benutzeraccount wird erst aktiv, wenn ein Samba-Passwort für ihn festgelegt ist. Aus Gründen der Sicherheit sollte das Samba-Passwort sich von dem Passwort für das System unterscheiden. Um für jeden Samba-Benutzer das Passwort festzulegen, verwenden Sie folgenden Befehl (ersetzen Sie *`username`* mit dem jeweiligen Benutzernamen).
   ```
   smbpasswd username
   ```
4. Verschlüsselte Passwörter müssen aktiviert sein. Da diese als Standard aktiviert sein müssen, ist es nicht nötig diese in der Konfigurationsdatei zu aktivieren. Diese können allerdings auch nicht in der Konfigurationsdatei deaktiviert werden. Prüfen Sie in der Datei `/etc/samba/smb.conf`, dass die folgenden Zeilen nicht enthalten sind:
   ```
   encrypt passwords = no
   ```
   Wenn diese enthalten ist, aber mit einem Semikolon (`;`) am Anfang der Zeile auskommentiert ist, wird diese Zeile ignoriert und verschlüsselte Passwörter sind aktiviert. Ist die Zeile enthalten, aber nicht auskommentiert, tun Sie dies, oder löschen Sie diese.

   Um verschlüsselte Passwörter in der Konfigurationsdatei zu aktivieren, fügen Sie folgende Zeilen zu `etc/samba/smb.conf` hinzu:
   ```
   encrypt passwords = yes
   smb passwd file = /etc/samba/smbpasswd
   ```

5. Stellen Sie sicher, dass der Dienst `smb` gestartet ist; geben Sie hierfür den Befehl `service smb restart` am Shell-Prompt ein.
6. Soll der `smb` Service automatisch gestartet werden, verwenden Sie `ntsysv`, `chkconfig` oder **Services Configuration Tool**, um ihn zur Laufzeit zu aktivieren. Weitere Information finden Sie unter Kapitel 21.

Das PAM-Modul `pam_smbpass` kann zum Synchronisieren der Samba-Benutzerpasswörter mit den Systempasswörtern verwendet werden, wenn der Befehl `passwd` verwendet wird. Ruft ein Benutzer den Befehl `passwd` auf, wird sowohl das bei der Anmeldung am Red Hat Enterprise Linux-System verwendete Passwort als auch das zur Verbindung mit einem Samba-Share verwendete Passwort geändert.

Fügen Sie folgende Zeile zu `/etc/pam.d/system- auth` unter dem Aufruf `pam_cracklib.so` hinzu, um diese Funktion zu aktivieren:

```
password required /lib/security/pam_smbpass.so nullok use_authtok try_first_pass
```

24.2.4. Starten und Anhalten des Servers

Auf dem Server, auf dem Verzeichnisse über Samba gemeinsam verwendet werden, muss `smb` ausgeführt werden.

Sie können den Status des Samba-Daemon mit dem folgenden Befehl anzeigen:

```
/sbin/service smb status
```

Starten Sie den Daemon mit dem folgenden Befehl:

```
/sbin/service smb start
```

Stoppen Sie den Server mit dem folgenden Befehl:

```
/sbin/service smb stop
```

Um den `smb` Dienst beim Booten zu starten, geben Sie folgenden Befehl ein:

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

Sie können auch `chkconfig`, **ntsysv** oder das **Services Configuration Tool** zum Konfigurieren der Dienste beim Booten verwenden. Weitere Informationen finden Sie unter Kapitel 21.

Tipp

Um aktive Verbindungen zum System anzuzeigen, führen Sie den Befehl `smbstatus` aus.

24.3. Herstellen einer Verbindung mit einem Samba-Share

Um die Samba-Shares in Ihrem Netzwerk anzuzeigen, können Sie auch **Nautilus** verwenden. Wählen Sie **Hauptmenü** (im Panel) => **Netzwerkserver** um eine Liste der Samba-Arbeitsgruppen in Ihrem Netzwerk anzuzeigen. Sie können auch den Befehl **`smb:`** im Feld **Position:** von Nautilus eingeben.

Wie in Abbildung 24-6 gezeigt, wird für jede verfügbare SMB-Arbeitsgruppe in Ihrem Netzwerk ein Symbol angezeigt.

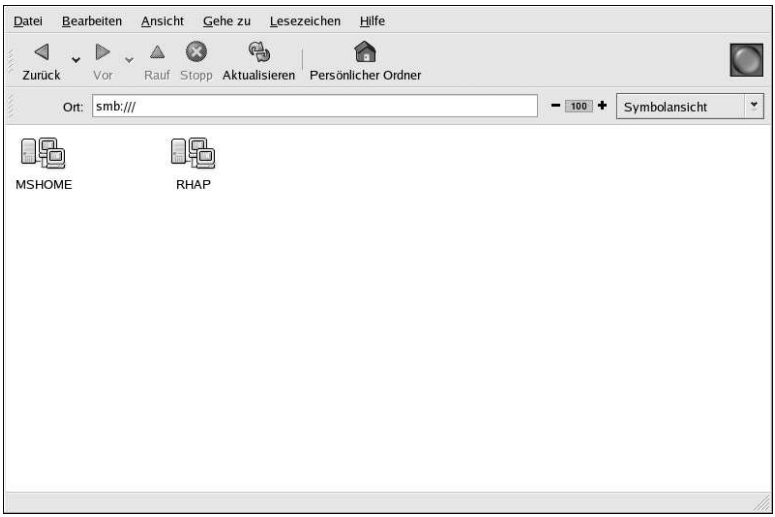

Abbildung 24-6. SMB Arbeitsgruppen in Nautilus

Doppelklicken Sie auf ein Arbeitsgruppen Symbol, um eine Liste der Computer innerhalb dieser Arbeitsgruppe anzuzeigen.

Abbildung 24-7. SMB Computer in Nautilus

Wie in Abbildung 24-7 gezeigt, gibt es ein Symbol für jeden Computer innerhalb der Arbeitsgruppe. Doppelklicken Sie auf ein Symbol um die Samba-Shares dieses Computers anzuzeigen. Wenn ein Benutzername und ein Passwort erforderlich ist, werden Sie zur Eingabe dessen aufgefordert.

Sie können alternativ dazu auch den Samba-Server und Sharenamen im Feld **Position:** mit Hilfe der folgenden Syntax eingeben (ersetzen Sie *<servername>* and *<sharename>* mit den entsprechenden Werten):

```
smb://<servername>/<sharename>/
```

24.3.1. Befehlszeile

Um das Netzwerk nach Samba-Servern abzufragen, benutzen Sie den Befehl `findsmb`. Für jeden gefundenen Server, wird IP-Adresse, NetBIOS-Name, Name der Workgroup, Betriebssystem und SMB-Server-Version angezeigt.

Geben Sie folgenden Befehl an einem Shell-Prompt ein, um eine Verbindung mit einer Samba-Share herzustellen:

```
smbclient //<hostname>/<sharename> -U <username>
```

Sie müssen *<hostname>* durch den Namen oder die IP-Adresse des Samba-Servers, mit dem Sie verbunden werden möchten, *<sharename>* durch den Namen des gemeinsam verwendeten Verzeichnisses, in dem Sie suchen möchten, und *<username>* durch den Samba-Benutzernamen für das System ersetzen. Geben Sie dann das richtige Passwort ein, oder drücken Sie die [Enter-Taste], falls kein Passwort für den Benutzer erforderlich ist.

Wenn Sie nun den Prompt `smb:\>` sehen, haben Sie sich erfolgreich angemeldet. Geben Sie nun **`Hilfe`** ein, um eine Liste von Befehlen zu erhalten. Wenn Sie die Inhalte Ihres Home-Verzeichnisses durchsuchen möchten, ersetzen Sie *sharename* durch Ihren Benutzernamen. Wenn der Schalter `-U` nicht verwendet wird, wird der Benutzername des aktuellen Benutzers an den Samba-Server weitergeleitet.

Um `smbclient` zu beenden, geben Sie **`Beenden`** am `smb: \>`-Prompt ein.

24.3.2. Share mounten

Manchmal ist es nützlich eine Samba-Share auf ein Verzeichnis zu mounten, so dass die Dateien als Teil des lokalen Dateisystems behandelt werden können.

Um eine Samba-Share auf ein Verzeichnis zu mounten, erzeugen Sie dies, falls nicht bereits vorhanden und führen Sie den folgenden Befehl als root aus:

```
mount -t  smbfs -o username=<username> //<servername>/<sharename> /mnt/point/
```

Dieser Befehl mountet *<sharename>* von *<servername>* auf das lokale Verzeichnis */mnt/point/*.

24.4. Zusätzliche Ressourcen

Weitere Informationen zu Konfigurationsoptionen, die hier nicht besprochen wurden, finden Sie in folgenden Ressourcen.

24.4.1. Installierte Dokumentation

- `smb.conf`-man-Seite — Erklärt, wie die Konfigurationsdatei von Samba zu konfigurieren ist.
- `smbd`-man-Seite — Beschreibt, wie der Samba-Daemon arbeitet.
- `smbclient` und `findsmb` man-Seiten — Lernen sie mehr zu diesen Client-Tools
- `/usr/share/doc/samba-<version-number>/docs/` — Hilfedateien im `samba`-Paket enthalten

24.4.2. Hilfreiche Websites

- http://www.samba.org/ — Die Samba-Webseite enthält nützliche Dokumentationen und Informationen über Adressenlisten sowie eine Liste mit GUI-Interfaces.
- http://www.samba.org/samba/docs/using_samba/toc.html — Eine Online-Version des *Using Samba, 2nd Edition* von Jay Ts, Robert Eckstein und David Collier-Brown; O'Reilly & Associates

redhat.

Kapitel 25.

Dynamic Host Configuration Protocol (DHCP)

Das Dynamic Host Configuration Protocol (DHCP) ist ein Netzwerkprotokoll für die automatische Zuordnung von TCP/IP-Daten auf Client-Rechnern. Jeder DHCP-Client steht mit dem zentralen DHCP-Server in Verbindung, der die Netzwerk-Konfiguration des Client zurücksendet, u.a. IP-Adresse, Gateway und DNS-Server.

25.1. Warum sollte man DHCP verwenden?

DHCP eignet sich zur schnellen Übertragung der Netzwerkkonfiguration eines Client-Rechners. Bei der Konfiguration des Client-Systems kann der Administrator einfach DHCP wählen und muss weder die IP-Adresse, Netzmaske, Gateway, noch DNS-Server eingeben. Der Client ruft diese Daten vom DHCP-Server ab. DHCP ist auch nützlich, wenn ein Administrator die IP-Adressen einer großen Zahl von Systemen ändern möchte. Anstatt alle Systeme neu zu konfigurieren, braucht er für die Neueinstellung der IP-Adressen nur eine DHCP-Konfigurationsdatei auf dem Server zu bearbeiten. Wenn sich der DNS-Server einer Organisation ändert, werden diese Änderungen auf dem DHCP-Server und nicht auf den DHCP-Clients vorgenommen. Sobald das Netzwerk für die Clients erneut gestartet wird oder (wenn die Clients neu gebootet werden), werden die Änderungen wirksam.

Auch für Laptops oder mobile Computer jeder Art bringt DHCP Vorteile: wenn sie auf DHCP konfiguriert sind, kann man sie an jedem beliebigen Arbeitsplatz benutzen, ohne sie jeweils neu konfigurieren zu müssen - vorausgesetzt natürlich, der betreffende Arbeitsplatz hat einen DHCP-Server, mit dem das Laptop oder der mobile Computer an das Netzwerk angeschlossen werden kann.

25.2. Konfigurieren eines DHCP Servers

Um einen DHCP-Server zu konfigurieren, bearbeiten Sie die Datei `/etc/dhcpd.conf`.

DHCP verwendet auch die Datei `/var/lib/dhcp/dhcpd.leases`, um die Lease-Datenbank des Clients zu speichern. Nähere Informationen finden Sie im Abschnitt 25.2.2.

25.2.1. Konfigurationsdatei

Der erste Schritt zur Konfiguration eines DHCP-Servers ist die Erstellung einer Konfigurationsdatei, die die Netzwerk-Daten für die Clients speichert. Man kann globale Optionen für alle Clients einstellen oder für jedes Client-System individuelle Optionen wählen.

Die Konfigurationsdatei kann beliebige Leerzeichen oder Tabs sowie leere Zeilen für eine einfachere Formatierung enthalten. Die Schlüsselwörter beachten keine Groß- und Kleinschreibung und Zeilen, die mit einer Raute beginnen (#), gelten als Kommentare.

Derzeit sind zwei Modi der DNS-Aktualisierungen implementiert — der Ad-Hoc DNS und Interim DHCP-DNS Interaktionsentwurf. Wenn diese beiden Schemata als Teil des IETF Standardprozess angenommen werden, erscheint ein dritter Modus — die standardmäßige DNS-Aktualisierungsmethode. Der DHCP-Server muss für den Gebrauch einer der beiden aktuellen Methoden konfiguriert werden. Version 3.0b2pl11 und ältere Versionen verwendeten den Ad-Hoc Modus, der inzwischen jedoch an Bedeutung verloren hat. Wenn Sie das gleiche Verhalten beibehalten möchten, fügen Sie am Anfang der Konfigurationsdatei die folgende Zeile hinzu:

```
ddns-update-style ad-hoc;
```

Um den empfohlenen Modus zu verwenden, fügen Sie am Anfang der Konfigurationsdatei die folgende Zeile hinzu:

```
ddns-update-style interim;
```

Auf der man-Seite `dhcpd.conf` finden Sie Details über die verschiedenen Methoden.

In der Konfigurationsdatei gibt es zwei Kategorien von Angaben:

- Parameter — geben an, wie eine Funktion ausgeführt wird, ob eine Funktion ausgeführt wird oder welche Optionen der Netzwerkkonfiguration an den Client gesendet werden sollen.
- Deklarationen — beschreiben die Topologie des Netzwerks, die Clients, bietet den Clients Adressen an oder wendet eine Reihe von Parametern auf eine Gruppe von Deklarationen an.

Einige Parameter müssen mit dem Schlüsselwort `Option` gestartet werden und werden als Optionen bezeichnet. Mit Optionen konfiguriert man DHCP-Optionen; während man mit Parametern nicht-optionale Werte konfiguriert oder das Verhalten des DHCP-Servers steuert.

Parameter (einschließlich Optionen), die vor einem Segment in geschweiften Klammern angegeben werden ({ }), gelten als globale Parameter. Die allgemeinen Parameter werden auf alle Segmente darunter angewandt.

Wichtig

Wenn Sie die Konfigurationsdatei verändern, kommen die Änderungen erst zum Tragen, wenn Sie den DHCP-Daemon neu starten, und zwar mit dem Befehl `service dhcpd restart`.

Im Beispiel 25-1 werden die Optionen `routers`, `subnet-mask`, `domain-name`, `domain-name-servers` und `time-offset` für alle darauffolgenden `host` Statement Deklarationen verwendet.

Wie Sie im Beispiel 25-1 sehen können, können Sie ein `subnet` angeben. Sie müssen eine `subnet` Angabe für jedes Subnet Ihres Netzwerks machen. Tun Sie dies nicht, kann der DHCP-Server nicht starten.

In unserem Beispiel gibt es für jeden DHCP-Client im Subnet allgemeine Optionen und einen `Range`. Die Zuweisung der IP-Adresse an die Clients erfolgt innerhalb des `Range`.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
        option routers                  192.168.1.254;
        option subnet-mask              255.255.255.0;

        option domain-name              "example.com";
        option domain-name-servers       192.168.1.1;

        option time-offset              -18000;     # Eastern Standard Time

 range 192.168.1.10 192.168.1.100;
}
```

Beispiel 25-1. Subnet-Deklaration

Alle Subnets, die ein gemeinsames physisches Netzwerk verwenden, sollten in der Datei `shared-network`, wie in Beispiel 25-2 gezeigt, angegeben werden. Parameter, die in `shared-network` angegeben sind, aber nicht in der `subnet` Deklaration enthalten sind, werden als allgemeine Parameter betrachtet. Die Bezeichnung des `shared-network` sollte ein aussagekräftiger Titel für das

Netzwerk sein, z.B. Test-Labor, wenn alle Subnets innerhalb eines Test-Labors beschrieben werden sollen.

```
shared-network name {
    option domain-name              "test.redhat.com";
    option domain-name-servers      ns1.redhat.com, ns2.redhat.com;
    option routers                  192.168.1.254;
    more parameters for EXAMPLE shared-network
    subnet 192.168.1.0 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.1 192.168.1.31;
    }
    subnet 192.168.1.32 netmask 255.255.255.0 {
        parameters for subnet
        range 192.168.1.33 192.168.1.63;
    }
}
```

Beispiel 25-2. Gemeinsam genutzte Netzwerk-Deklaration

Wie in Beispiel 25-3 gezeigt, kann die `Gruppen`-Vereinbarung verwendet werden, um allgemeine Parameter für eine Gruppe von Vereinbarungen anzuwenden. Sie können gemeinsam genutzte Netzwerke, Subnets, Hosts oder andere Gruppen als Gruppe zusammenfassen.

```
group {
   option routers                  192.168.1.254;
   option subnet-mask              255.255.255.0;

   option domain-name              "example.com";
   option domain-name-servers       192.168.1.1;

   option time-offset              -18000;     # Eastern Standard Time

   host apex {
      option host-name "apex.example.com";
      hardware ethernet 00:A0:78:8E:9E:AA;
      fixed-address 192.168.1.4;
   }

   host raleigh {
      option host-name "raleigh.example.com";
      hardware ethernet 00:A1:DD:74:C3:F2;
      fixed-address 192.168.1.6;
   }
}
```

Beispiel 25-3. Gruppen-Vereinbarung

Um einen DHCP-Server zu konfigurieren, der dynamische IP-Adressen in einem Subnet an ein System vergibt, ändern Sie Beispiel 25-4 entsprechend Ihren Werten. Es bezeichnet die Standard-Vergabe-Dauer, die maximale Vergabe-Dauer und Netzwerk-Konfigurationswerte für die Clients. In diesem Beispiel wird die IP-Adresse in der `range` 192.168.1.10 und 192.168.1.100 Client-Systemen zugeordnet.

```
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "example.com";

subnet 192.168.1.0 netmask 255.255.255.0 {
   range 192.168.1.10 192.168.1.100;
}
```

Beispiel 25-4. Range-Parameter

Um einem Client anhand der MAC-Adresse der Netzwerkkarte eine IP-Adresse zuzuordnen, verwenden Sie den Parameter `hardware ethernet`, der in der `host` Deklaration enthalten ist. Wie in Beispiel 25-5 gezeigt, legt die `host apex` Deklaration fest, dass die Netzwerkkarte mit der MAC-Adresse 00:A0:78:8E:9E:AA immer die IP-Adresse 192.168.1.4 zugewiesen bekommt.

Beachten Sie, dass Sie auch den optionalen Parameter `host-name` benutzen können, um einem Client einen Hostnamen zuzuordnen.

```
host apex {
   option host-name "apex.example.com";
   hardware ethernet 00:A0:78:8E:9E:AA;
   fixed-address 192.168.1.4;
}
```

Beispiel 25-5. Statische IP-Adresse, die DHCP verwendet

Tipp

Sie können zunächst die Musterkonfigurationsdatei benutzen und dann Ihre eigenen Anpassungen für die Konfiguration hinzufügen. Kopieren Sie diese an die richtige Stelle mit dem Befehl

```
cp /usr/share/doc/dhcp-<version-number>/dhcpd.conf.sample /etc/dhcpd.conf
```

(wobei <*version-number*> die DHCP-Version ist, die Sie verwenden).

Eine vollständige Liste der Optionen und deren Anwendung finden Sie auf der `dhcp-options` man-Seite.

25.2.2. Vergabe-Datenbank

`/var/lib/dhcp/dhcpd.leases` die Vergabe-Datenbank des DHCP-Client. Diese Datei sollte nicht manuell geändert werden. In der Vergabe-Datenbank werden automatisch alle DHCP-Vergabedaten aller zuletzt zugeordneten IP-Adressen gespeichert. Die Daten enthalten die Vergabedauer, wem die IP-Adresse zugeordnet wurde sowie Anfangs- und Enddaten für die Vergabe und die MAC-Adresse der Netzwerkkarte, von der die Vergabe abgerufen wurde.

Alle Zeitangaben in der Vergabe-Datenbank sind Greenwich Mean Time (GMT) und nicht Ortszeit.

Datei wird umbenannt in `dhcpd.leases~` und die temporäre Vergabe-Datei wird gespeichert unter `dhcpd.leases`.

Der DHCP-Daemon könnte beendet werden oder das System abstürzen, nachdem die Vergabe-Datenbank in Backup-Datei umbenannt, die neue Datei jedoch noch nicht gespeichert wurde. In diesem Fall gibt es keine `dhcpd.leases`-Datei, die zum Starten erforderlich ist. Erstellen Sie keine neue Vergabe-Datei, wenn dies passiert. Wenn Sie dies tun, gehen alle alten Vergaben verloren, was zu Problemen führt. Sie sollten stattdessen die `dhcpd. leases~` Backup-Datei in `dhcpd.leases` umbenennen und dann den Daemon starten.

25.2.3. Starten und Stoppen des Servers

Wichtig

Bevor Sie den DHCP-Server zum ersten Mal starten, muss die `dhcpd.leases` Datei existieren, ansonsten wird es nicht funktionieren. Sollte die Datei nicht existieren, können Sie diese mit dem Befehl `touch /var/lib/dhcp/dhcpd.leases` erstellen.

Um DHCP zu starten, geben Sie den Befehl`/sbin/service dhcpd start` ein. Um den DHCP-Server anzuhalten, geben Sie den Befehl `/sbin/service dhcpd stop` ein. Wenn Sie wünschen, dass der Daemon automatisch beim Booten startet, finden Sie unter Kapitel 21 nähere Informationen über den Umgang mit den Diensten.

Wenn mehrere Netzwerkschnittstellen in Ihrem System vorhanden sind, Sie aber möchten, dass der DHCP-Server nur auf einer Schnittstelle startet, können Sie den DHCP-Server entsprechend konfigurieren. Fügen Sie in der Datei `/etc/sysconfig/dhcpd` den Namen dieser Schnittstelle zu der Liste von `DHCPDARGS` hinzu:

```
# Command line options here
DHCPDARGS=eth0
```

Dies ist sinnvoll, wenn Sie einen Rechner mit Firewall und zwei Netzwerk-Karten haben. Eine der Netzwerk-Karten kann als DHCP-Client konfiguriert werden, um eine IP-Adresse aus dem Internet abzurufen. Die andere Netzwerkkarte kann als DHCP-Server für das interne Netzwerk hinter der Firewall benutzt werden, wodurch das System sicherer wird, da Benutzer über das Internet keine Verbindung zu dem Daemon aufnehmen können.

In `/etc/sysconfig/dhcpd` können noch andere Befehlszeilenoptionen festgelegt werden, wie zum Beispiel:

- `-p <portnum>` — Legt die udp Port-Nummer fest, auf die dhcpd warten soll. Der Standard-Port ist 67. Der DHCP-Server überträgt Antworten an DHCP-Clients mit einer Port-Nummer, die um eins größer ist als der festgelegte udp-Port. Wenn Sie z.B. den Standard-Port 67 annehmen, wartet der Server am Port 67 auf Anfragen und Antworten für den Client auf Port 68. Wenn Sie hier einen Port festlegen und den DHCP Relay Agent verwenden, müssen Sie den gleichen Port festlegen, an dem der DHCP Relay Agent wartet. Weitere Informationen finden Sie im Abschnitt 25.2.4.
- `-f` — Führt den Daemon als Vordergrundprozess aus und wird meistens für das Debuggen verwendet.
- `-d` — Protokolliert den DCHP Server Daemon im Standard-Fehlerdeskriptor und wird meistens für das Debuggen verwendet. Ist dies nicht festgelegt, wird das Protokoll in der Datei `/var/log/messages` geschrieben.
- `-cf <filename>` — Legt den Speicherplatz für die Konfigurationsdatei fest. Die standardmäßige Speicherstelle ist `/etc/dhcpd.conf`.
- `-lf <filename>` — Legt die Speicherstelle für die Vergabe Datenbank-Datei fest. Ist die Vergabe Datenbank-Datei bereits vorhanden, ist es sehr wichtig, dass bei jedem Start

des DHCP-Servers dieselbe Datei verwendet wird. Es wird empfohlen, diese Option nur für Debugging-Aufgaben in nicht- produktiven Computern zu verwenden. Die Standard-Speicherstelle ist `/var/lib/dhcp/dhcpd.leases`.

- `-q` — Druckt beim Starten des Daemons nicht die gesamte Copyright Info.

25.2.4. DHCP Relay Agent

Mit dem DHCP Relay Agent (`dhcrelay`) können Sie DHCP- oder BOOTP-Anfragen des Subnets, die keinen DHCP-Server haben, auf einen oder mehrere DHCP-Server anderer Subnets übertragen.

Wenn ein DHCP-Client Daten anfragt, gibt der DHCP Relay Agent die Anfrage an die Liste der DHCP-Server weiter, die angegeben wurden, als der DHCP Relay Agent gestartet wurde. Wenn ein DHCP- Server antwortet, wird die Antwort als Broadcast oder Unicast auf das Netzwerk übertragen, das die ursprüngliche Anfrage gesendet hat.

Der DHCP Relay Agent wartet auf DHCP-Anfragen an allen Schnittstellen, es sei denn, die Schnittstellen werden in `/etc/sysconfig/dhcrelay` mit der Anweisung `INTERFACES` angegeben.

Um den DHCP Relay Agent zu starten, geben Sie den Befehl `service dhcrelay start` ein.

25.3. Konfigurieren eines DHCP-Clients

Der erste Schritt zum Konfigurieren eines DHCP-Clients besteht darin sicherzustellen, dass der Kernel die Netzwerkkarte erkennt. Die meisten Karten werden während des Installations-Vorgangs erkannt und dabei wird das System so konfiguriert, dass es für die Karte das richtige Kernel-Modul benutzt. Wenn Sie erst nach der Installation eine Karte installieren, müsste **Kudzu** [1] diese erkennen und Sie auffordern, das entsprechende Kernel-Modul für diese zu konfigurieren. Überprüfen Sie auf jeden Fall die Red Hat Linux Hardware-Kompatibilitätsliste unter http://hardware.redhat.com/hcl/. Wenn die Netzwerkkarte nicht vom Installationsprogramm oder **Kudzu** konfiguriert wird, und Sie das zu ladende Kernel-Modul wissen finden Sie unter Kapitel 40 weitere Informationen zum Laden von Kernel-Modulen.

Um einen DHCP-Client manuell zu konfigurieren, müssen Sie die `/etc/sysconfig/network` Datei ändern, um die Verbindung mit dem Netzwerk und die Konfigurationsdatei für jedes Netzwerk-Gerät im `/etc/sysconfig/network-scripts` Verzeichnis zu aktivieren. In diesem Verzeichnis sollte jedes Gerät immer dann eine Konfigurationsdatei mit der Bezeichnung `ifcfg-eth0` haben, wenn `eth0` die Bezeichnung für das Netzwerk-Gerät ist.

Die Datei `/etc/sysconfig/network` sollte folgende Zeile enthalten:

```
NETWORKING=yes
```

Sie müssen sicherstellen, dass die `NETWORKING` Variable auf `yes` eingestellt ist, wenn Sie beim Booten gleichzeitig das Netzwerk starten wollen.

Die Datei `/etc/sysconfig/network-scripts/ifcfg-eth0` sollte folgende Zeilen enthalten:

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

Sie benötigen eine Konfigurationsdatei für jedes Gerät, das DHCP benutzen soll.

Andere Optionen für das Netzwerk-Skript umfassen:

1. **Kudzu** ist ein Tool zur Erkennung der Hardware zum Zeitpunkt des Bootens des Systems, um festzustellen, welche Hardware zum System hinzugefügt oder aus dem System entfernt wurde.

- `DHCP_HOSTNAME` — Verwenden Sie diese Optione nur, wenn der DHCP-Server eine Angabe des Hostnamens vom Client erfordertm bevor eine IP-Adresse erhalten wird. (Der DHCP-Server-Daemon in Red Hat Enterprise Linux unterstützt dieses Feature nicht.)
- `PEERDNS=<answer>`, wobei `<answer>` eines der folgenden sein kann:
  - `yes` — Ändern Sie `/etc/resolv.conf` mit den Informaitonen vom Server. Wird DHCP verwendet, ist `yes` der Standardwert.
  - `no` — Ändern Sie `/etc/resolv.conf` nicht.

- `SRCADDR=<address>`, wobei `<address>` die spezifische Source-IP-Adresse für ausgehende Pakete ist.
- `USERCTL=<answer>`, wobei `<answer>` eines der folgenden sein kann:
  - `yes` — Nicht-root-Benutzer können dieses Gerät steuern.
  - `no` — Nicht-root-Benutzer können dieses Gerät nicht steuern.

Wenn Sie für das Konfigurieren eines DHCP-Clients eine grafische Benutzeroberfläche vorziehen, finden Sie unter Kapitel 19 nähere Informationen für die Verwendung von **Network Administration Tool** zur Konfiguration einer Netzwerkschnittstelle für DHCP.

25.4. Zusätzliche Ressourcen

Informationen über Konfigurationsoptionen, die hier nicht beschrieben werden, finden Sie in den nachstehend aufgeführten Ressourcen.

25.4.1. Installierte Dokumentation

- `dhcpd` man Seite — beschreibt, wie der DHCP-Daemon arbeitet.
- Die `dhcpd.conf` man Seite — erklärt, wie die DHCP-Konfigurationsdatei konfiguriert wird und zeigt einige Beispiele.
- Die `dhcpd.leases` man Seite — erklärt, wie man die DHCP-Lease-Datei konfiguriert und zeigt einige Beispiele.
- Die `dhcp-options` man Seite — erklärt die Syntax zur Bezeichnung von DHCP-Optionen unter `dhcpd.conf` und gibt hierzu einige Beispiele.
- `dhcrelay` man Seite — erklärt den DHCP Relay Agent und dessen Konfigurationsoptionen.

Kapitel 26.

Apache HTTP Server-Konfiguration

Red Hat Enterprise Linux bietet Apache HTTP Server Version 2.0. Wenn Sie eine vorhandene Konfigurationsdatei manuell migrieren möchten, finden Sie weitere Informationen im Migrationshandbuch unter `/usr/share/doc/httpd-<ver>/migration.html` oder im *Red Hat Enterprise Linux Referenzhandbuch*.

Wenn Sie Apache HTTP Server in früheren Versionen von Red Hat Enterprise Linux mit dem **HTTP Configuration Tool** konfiguriert und dann eine Aktualisierung durchgeführt haben, können Sie die Anwendung zum Migrieren der Konfigurationsdatei in das neue Format für Version 2.0 verwenden. Starten Sie das **HTTP Configuration Tool**, ändern Sie die Konfiguration und speichern Sie diese. Die gespeicherte Konfigurationsdatei ist mit Version 2.0 kompatibel

Mit dem **HTTP Configuration Tool** können Sie die Konfigurationsdatei `/etc/httpd/conf/httpd.conf` für Apache HTTP Server konfigurieren. Das Programm verwendet die alten Konfigurationsdateien `srm.conf` oder `access.conf` nicht; lassen Sie sie leer. Über das grafische Interface können Sie Direktiven wie virtuelle Hosts, Protokollierungsattribute und die Höchstanzahl von Verbindungen konfigurieren.

Nur Module, die mit Red Hat Enterprise Linux geliefert werden, können mit dem **HTTP Configuration Tool** konfiguriert werden. Sind zusätzliche Module installiert, können diese nicht mithilfe dieses Tools konfiguriert werden.

Die `httpd` und `redhat-config-httpd` RPM-Pakete müssen installiert sein, um **HTTP Configuration Tool** verwenden zu können. Es benötigt außerdem das X Window System und root-Berechtigung. Um die Applikation zu starten, wählen Sie **Hauptmenü => Systemeinstellungen => Servereinstellungen => HTTP** oder geben Sie den Befehl `redhat-config-httpd` an einem Shell-Prompt ein (z.B. ein XTerm oder GNOME-Terminal).

Achtung

Bearbeiten Sie die Konfigurationsdatei `/etc/httpd/conf/httpd.conf` nicht manuell, wenn Sie dieses Tool verwenden möchten. Das **HTTP Configuration Tool** generiert diese Datei, nachdem Sie die Änderungen gespeichert und das Programm beendet haben. Wenn Sie zusätzliche Module oder Konfigurationsoptionen hinzufügen möchten, die im **HTTP Configuration Tool** nicht zur Verfügung stehen, können Sie dieses Tool nicht verwenden.

Die allgemeinen Schritte zum Konfigurieren von Apache HTTP Server mithilfe von **HTTP Configuration Tool** sind folgende:

1. Konfigurieren Sie die Grundeinstellungen auf dem Tab **Hauptfenster**.
2. Klicken Sie auf das Tab **Virtuelle Hosts** und konfigurieren Sie die Standardeinstellungen.
3. Konfigurieren Sie auf dem Tab **Virtuelle Hosts** die standardmäßigen virtuellen Hosts.
4. Wenn Sie mehrere URLs oder virtuelle Hosts bereitstellen möchten, fügen Sie die virtuellen Hosts hinzu.
5. Konfigurieren Sie die Servereinstellungen auf dem Tab **Server**.
6. Konfigurieren Sie die Verbindungseinstellungen auf dem Tab **Leistungsoptimierung**.
7. Kopieren Sie alle notwendigen Dateien in die Verzeichnisse `DocumentRoot` und `cgi-bin`.
8. Beenden Sie die Applikation und speichern Sie die Einstellungen.

26.1. Grundeinstellungen

Verwenden Sie das Tab **Hauptfenster**, um die grundlegenden Servereinstellungen zu konfigurieren.

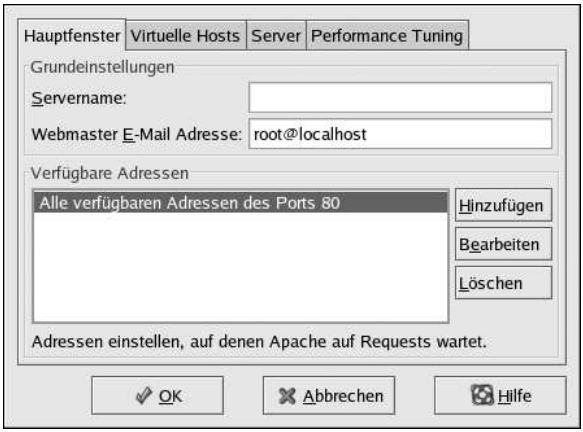

Abbildung 26-1. Grundeinstellungen

Geben Sie einen gültigen Domainnamen, den Sie verwenden dürfen, in das Textfeld **Servername** ein. Diese Option entspricht der `ServerName` Richtlinie in `httpd.conf`. Die `ServerName` Direktive legt den Hostnamen des Web-Servers fest. Er wird beim Erstellen von Umleitungs-URLs verwendet. Wenn Sie keinen Servernamen definieren, versucht der Web-Server, dies über IP-Adresse des Systems zu erfahren. Der Servername muss nicht dem über die IP-Adresse des Servers aufgelöste Domainname übereinstimmen. Möglicherweise möchten Sie den Servernamen auf www.Beispiel.com festlegen, obwohl der tatsächliche DNS-Name Ihres Servers foo.beispiel.com.

Geben Sie im Textbereich **E-Mail-Adresse Webmaster** die E-Mail-Adresse der Person ein, die den Web-Server pflegt. Diese Option entspricht der Direktive `ServerAdmin` in `httpd.conf`. Wenn Sie die Fehlerseiten des Servers so konfigurieren, dass sie eine E-Mail-Adresse enthalten, verwenden Benutzer diese E-Mail-Adresse, um sich im Falle von Problemen per Mail an den Administrator des Servers zu wenden. Der Standardwert ist root@localhost.

Verwenden Sie den Bereich **Verfügbare Adressen** um die Ports zu definieren, an denen der Server eingehende Anfragen akzeptiert. Diese Option entspricht der `Listen` Richtlinie in `httpd.conf`. Standardmäßig konfiguriert Red Hat das Apache HTTP Server Port 80 nach nicht sicheren Webkommunikationen abzuhören.

Klicken Sie auf die Schaltfläche **Hinzufügen** um zusätzliche Ports zu definieren, an denen Anfragen akzeptiert werden sollen. Ein Fenster wird wie in Abbildung 26-2 wird angezeigt. Wählen Sie entweder die Option **Alle Adressen abhören** , um alle IP-Adressen an den definierten Ports abzuhören, oder geben Sie im Feld **Adresse** eine bestimmte IP-Adresse an, über die der Server Verbindungen akzeptiert. Geben Sie pro Portnummer nur eine IP-Adresse an. Erstellen Sie einen Eintrag pro IP-Adresse, wenn Sie mehrere IP-Adressen mit derselben Portnummer angeben möchten. Wenn möglich sollte Sie eine IP-Adresse anstelle eines Domainnamens verwenden, um DNS-Suchfehler zu vermeiden. Weitere Informationen finden Sie unter http://httpd.apache.org/docs-2.0/dns-caveats.html zu *Themen in Bezug auf DNS und Apache*.

Die Eingabe eines Sternchens (*) in das Feld **Adresse** entspricht dem Klicken auf **Alle Adressen abhören**. Wenn Sie auf die Schaltfläche **Bearbeiten** im **Verfügbare Adressen**-Frame klicken, wird dasselbe Fenster wie für die Schaltfläche **Hinzufügen** angezeigt, allerdings mit dem Unterschied, dass

die Felder für den ausgewählten Eintrag aufgefüllt sind. Wenn Sie einen Eintrag löschen möchten, markieren Sie ihn und klicken Sie auf die Schaltfläche **Löschen**.

Tipp

Wenn Sie festgelegt haben, dass der Server einen Port unter 1024 abhört, müssen Sie unter einem root-Account angemeldet sein, um ihn starten zu können. Für Port 1024 und höher können Sie `httpd` als normaler Benutzer starten.

Abbildung 26-2. Verfügbare Adressen

26.2. Standardeinstellungen

Nachdem Sie den **Servernamen**, die **E-Mail- Adresse Webmaster** und **Verfügbare Adressen** definiert haben, klicken Sie auf das Tab **Virtuelle Hosts** und auf die Schaltfläche **Standardeinstellungen bearbeiten**. Das in Abbildung 26-3 abgebildete Fenster wird angezeigt. Konfigurieren Sie die Standardeinstellungen für Ihren Web-Server in diesem Fenster. Wenn Sie einen virtuellen Host hinzufügen, haben die für den virtuellen Host konfigurierten Einstellungen Vorrang für diesen virtuellen Host. Für eine in den Einstellungen des virtuellen Hosts nicht definierte Direktive wird der Standardwert verwendet.

26.2.1. Site-Konfiguration

Die Standardwerte für **Suchliste Verzeichnisseite** und **Fehlerseiten** funktionieren für die meisten Server. Wenn Sie sich wegen dieser Einstellungen nicht sicher sind, ändern Sie sie nicht.

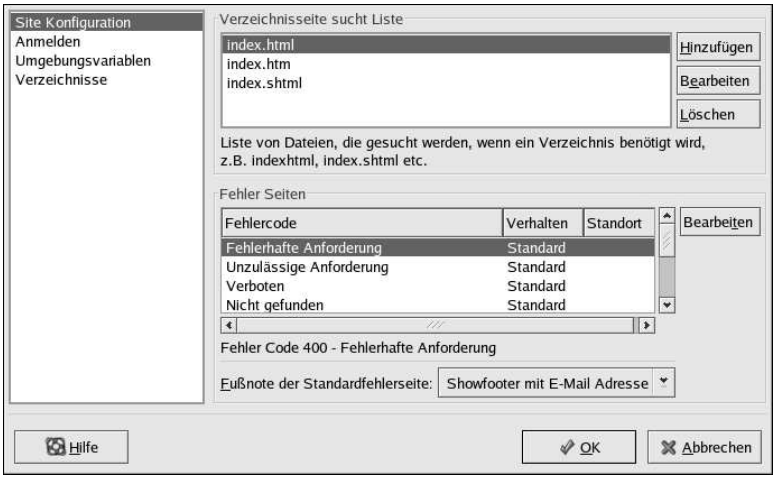

Abbildung 26-3. Site-Konfiguration

Die in **Suchliste Verzeichnisseite** aufgelisteten Einträge definieren die `DirectoryIndex`-Direktive. `DirectoryIndex` ist die vom Server bereitgestellte Standardseite, wenn ein Benutzer einen Verzeichnisindex anfordert, indem er einen Schrägstrich (/) am Ende des Verzeichnisnamen eingibt.

Wenn ein Benutzer zum Beispiel die Seite http://*`www.Beispiel.com`*/*`Dieses_Verzeichnis`*/ anfordert, wird entweder sofort die Seite `DirectoryIndex` angezeigt, falls sie vorhanden ist, oder eine vom Server generierte Verzeichnisliste. Der Server versucht, eine der in der `DirectoryIndex`-Direktive aufgelisteten Dateien zu finden, und gibt die erste zurück, die er findet. Wenn er keine Datei findet und `Options Indexes` für dieses Verzeichnis festgelegt ist, generiert der Server eine Liste im HTML-Format. Die Liste umfasst die Unterverzeichnisse und Dateien des Verzeichnisses.

Verwenden Sie den Bereich **Fehlercode**, um Apache HTTP Server im Falle eines Problems oder Fehlers zum Umleiten des Clients an einen lokalen oder externen URL zu konfigurieren. Diese Option entspricht der `ErrorDocument`-Direktive. Tritt ein Problem oder Fehler auf, wenn ein Client versucht, eine Verbindung mit Apache HTTP Server herzustellen, besteht die Standardaktion darin, die kurze, in der Spalte **Fehlercode** gezeigte Fehlermeldung anzuzeigen. Wählen Sie zum Überschreiben der Standardkonfiguration den Fehlercode aus und klicken Sie auf die Schaltfläche **Bearbeiten**. Wählen Sie **Standard**, um die kurze Standardfehlermeldung anzuzeigen. Wählen Sie **URL** aus, um den Client an einen externen URL umzuleiten, und geben Sie einen vollständigen URL einschließlich http:// in das Feld **Speicherplatz** ein. Wählen Sie **Datei** aus, um den Client an einen internen URL umzuleiten, und geben Sie einen Dateispeicherplatz unter dem Dokumentroot für den Web-Server ein. Der Speicherplatz muss mit einem Schrägstrich (/) beginnen und ist relativ zum Document Root.

Um zum Beispiel einen 404 Not Found-Fehlercode an eine Webseite umzuleiten, die Sie in der Datei `404.html` erstellt haben, kopieren Sie `404.html` nach *`DocumentRoot`*`/../error/404.html`. In diesem Fall ist *`DocumentRoot`* das von Ihnen definierte Dokument-Root-Verzeichnis (das Standardverzeichnis ist `/var/www/html/`). Wird das Dokument-Root-Verzeichnis an seiner Standard-Stelle belassem, sollte die Datei nach `/var/www/error/404.html` kopiert werden. Wählen Sie dann **Datei** als Verhalten für den **404 - Not Found**-Fehlercode und geben Sie `/error/404.html` als **Speicherplatz** an.

Im Menü **Fußzeile Standardfehlerseite** können Sie eine der folgenden Optionen auswählen:

- **Fußzeile mit E-Mail-Adresse anzeigen** — Zeigt auf allen Fehlerseiten unten die Standardfußzeile zusammen mit der E-Mail-Adresse des Website-Administrators an, die in

der `ServerAdmin`-Direktive angegeben ist. Unter Abschnitt 26.3.1.1 finden Sie weitere Informationen zum Konfigurieren der `ServerAdmin`-Direktive.

- **Fußzeile anzeigen** — Zeigt nur die Standardfußzeile unten auf den Fehlerseiten an.
- **Keine Fußzeile** — Zeigt unten auf den Fehlerseiten keine Fußzeile an.

26.2.2. Protokollierung

Der Server schreibt das Übertragungsprotokoll standardmäßig in die Datei `/var/log/httpd/access_log` und das Fehlerprotokoll in die Datei `/var/log/httpd/error_log`.

Das Übertragungsprotokoll enthält eine Liste mit allen Versuchen, auf den Web-Server zuzugreifen. Es wird die IP- Adresse des Clients, Datum und Uhrzeit der Verbindung, sowie die Datei, die auf dem Web-Server abgerufen wird aufgezeichnet. Geben Sie den Namen des Pfads sowie der Datei ein, in der diese Informationen gespeichert werden sollen. Wenn der Pfad- und Dateiname nicht mit einem Schrägstrich (/) beginnen, so ist er relativ zum konfigurierten ServerRoot-Verzeichnis. Diese Option entspricht der `TransferLog`- Direktive.

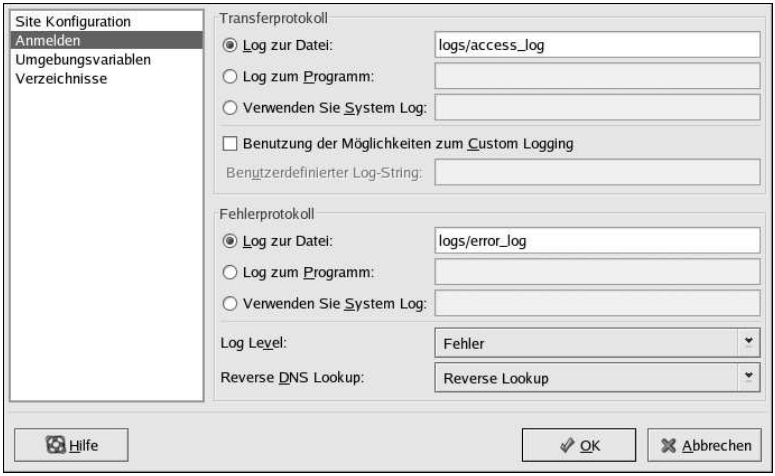

Abbildung 26-4. Protokollierung

Sie können das Protokollformat individuell gestalten, indem Sie **Benutzung der Möglichkeiten zum Custom Logging** aktivieren und eine individuell gestaltete Protokollzeichenfolge in das Feld **Benutzerdefinierter Log-String** eingeben. Hierdurch wird die `LogFormat`-Direktive konfiguriert. Weitere Informationen zum Format dieser Direktive finden Sie unter http://httpd.apache.org/docs-2.0/mod/mod_log_config.html#formats.

Das Fehlerprotokoll enthält alle aufgetretenen Serverfehler. Geben Sie den Namen des Pfads sowie der Datei ein, in der diese Informationen gespeichert werden sollen. Wenn der Pfad- und Dateiname nicht mit einem Schrägstrich (/) beginnen, so ist er relativ zum konfigurierten ServerRoot-Verzeichnis. Diese Option entspricht der `ErrorLog`-Direktive.

Verwenden Sie das Menü **Log Level** zum Festlegen der Ausführlichkeit der Fehlermeldungen in den Fehlerprotokollen. Sie kann (von geringer bis maximaler Ausführlichkeit) auf Notfall, Alert, Kritisch,

Fehler, Warnung, Benachrichtigung, Info oder Debugging festgelegt werden. Diese Option entspricht der `LogLevel`-Direktive.

Der über das Menü **Reverse DNS-Lookup** ausgewählte Wert definiert die `HostnameLookups` -Direktive. Durch Auswahl von **Kein Reverse Lookup** wird der Wert deaktiviert. Durch Auswahl von **Reverse Lookup** wird der Wert aktiviert. Mit **Doppelter Reverse Lookup** wird der Wert verdoppelt.

Wenn Sie **Reverse Lookup** auswählen, löst der Server automatisch die IP-Adresse für jede Verbindung auf, die ein Dokument vom Web-Server abruft. Das Auflösen der IP-Adresse bedeutet, dass der Server eine oder mehrere Verbindungen mit dem DNS herstellt, um den Hostnamen herauszufinden, der einer bestimmten IP-Adresse entspricht.

Wenn Sie **Doppelter Reverse Lookup** auswählen, führt der Server einen doppelten Reverse-DNS-Vorgang durch. Mit anderen Worten: nach einem Reverse Lookup wird das Ergebnis nochmals vorwärts durchsucht. Mindestens eine der IP-Adressen muss hierbei mit der Adresse des ersten Reverse Lookups übereinstimmen.

Sie sollten diese Option auf **Kein Reverse Lookup** belassen, da DNS-Abfragen den Server zusätzlich belasten und die Leistung beeinträchtigen. Wenn Ihr Server ausgelastet ist, sind die Auswirkungen des Versuchs, diese Reverse Lookups oder doppelten Reverse Lookup durchzuführen, deutlich spürbar.

Reverse Lookups und doppelte Reverse Lookups sind auch für Internet insgesamt ein Problem. Alle einzelnen, zum Suchen der Hostnamen hergestellten Verbindungen, summieren sich zur Last. Daher sollten Sie zu Gunsten Ihres eigenen Web-Servers wie auch zu Gunsten des Internet diese Option auf **Kein Reverse Lookup** belassen.

26.2.3. Umgebungsvariablen

Unter Umständen ist es notwendig, Umgebungsvariablen für CGI Skripts oder Server Side Include (SSI) Seiten zu ändern. Das Apache HTTP Server kann das Modul `mod_env` zum Konfigurieren der Umgebungsvariablen verwenden, die an CGI-Skripte und SSI-Seiten weitergeleitet werden. Verwenden Sie die Seite **Umgebungsvariablen**, um die Richtlinien für dieses Modul zu konfigurieren.

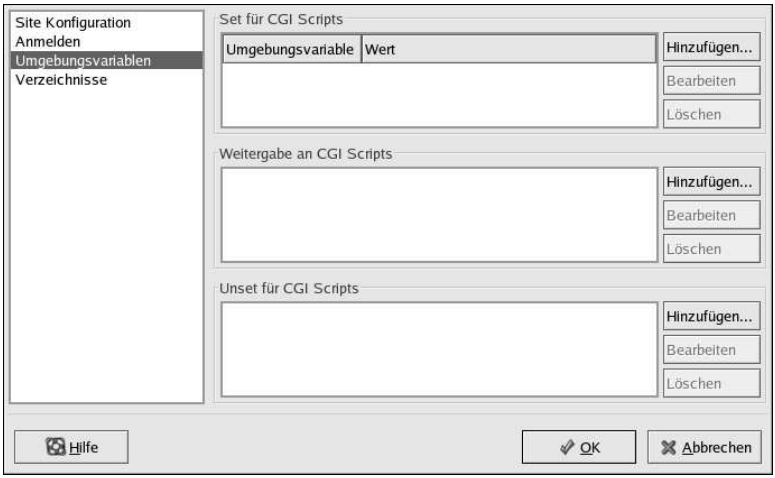

Abbildung 26-5. Umgebungsvariablen

Verwenden Sie den Bereich **Weitergabe an CGI-Skripte** zum Festlegen einer Umgebungsvariable, die an CGI- Skripte und SSI-Seiten weitergeleitet wird. Beispiel: zum Festlegen der Umgebungsvariable `MAXNUM` auf `50`, klicken Sie auf **Hinzufügen** im Bereich **Für CGI-Skripte festlegen** wie in Abbildung 26-5 gezeigt, und geben Sie **`MAXNUM`** in das Textfeld **Umgebungsvariable** sowie **`50`** in das Textfeld **Festzulegender Wert** ein. Klicken Sie auf **OK**, um diesen zur Liste hinzuzufügen. Der Abschnitt **Für CGI-Skripte festlegen** konfiguriert die `SetEnv` Direktive.

Verwenden Sie den Bereich **An CGI-Skripte weiterleiten**, um den Wert einer Umgebungsvariablen den sie beim Start des Servers hatte an CGI-Skripte weiterzuleiten. Geben Sie den Befehl `env` an einem Shell-Prompt ein, um diese Umgebungsvariable anzuzeigen. Klicken Sie auf **Hinzufügen** im Bereich **An CGI-Skripte weiterleiten** und geben Sie den Namen der Umgebungsvariable in das folgende Dialogfeld ein. Klicken Sie auf **OK** um diese zur Liste hinzuzufügen. Der Bereich **An CGI-Skripte weiterleiten** konfiguriert die `PassEnv` Direktive.

Wenn Sie eine Umgebungsvariable entfernen möchten, damit der Wert nicht an CGI-Skripte und SSI-Seiten weitergeleitet wird, müssen Sie den Bereich **Einstellung für CGI-Skripte aufheben** verwenden. Klicken Sie auf **Hinzufügen** im Bereich **Einstellung für CGI-Skripte aufheben** und geben Sie den Namen der Umgebungsvariablen ein, um die Einstellung aufzuheben. Klicken Sie auf **OK**, um diese zur Liste hinzuzufügen. Dies entspricht `UnsetEnv`.

Um diese Umgebungswerte zu ändern, wählen Sie diese aus der Liste aus und klicken Sie auf den entsprechenden **Bearbeiten**-Button. Um einen Eintrag aus der Liste zu löschen, wählen Sie diesen aus und klicken Sie auf den entsprechenden **Löschen**-Button.

Weitere Informationen zu den Umgebungsvariablen in Apache HTTP Server finden Sie unter:

`http://httpd.apache.org/docs-2.0/env.html`

26.2.4. Verzeichnisse

Verwenden Sie die Seite **Verzeichnisse**, um die Optionen für bestimmte Verzeichnisse zu konfigurieren. Dies entspricht der `<Directory>`-Direktive.

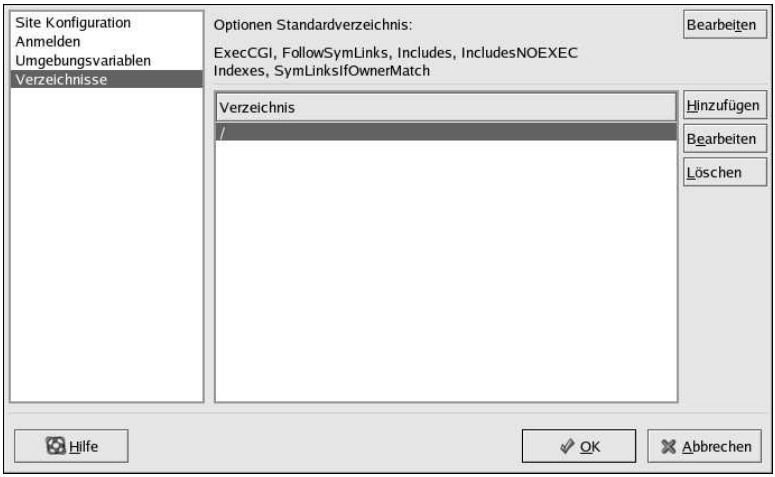

Abbildung 26-6. Verzeichnisse

Klicken Sie oben rechts auf die Schaltfläche **Bearbeiten**, um **Standardverzeichnis-Optionen** für alle Verzeichnisse zu konfigurieren, die nicht in der darunter aufgeführten **Verzeichnis**-Liste nicht genannt sind. Die von Ihnen gewählten Optionen werden als Optionen in der `<Directory>`-Direktive genannt. Sie können folgende Optionen konfigurieren:

- **ExecCGI** — Ermöglicht die Ausführung von CGI-Skripten. CGI-Skripte werden nicht ausgeführt, wenn diese Option nicht ausgewählt ist.
- **FollowSymLinks** — Ermöglicht die Verwendung symbolischer Verknüpfungen.
- **Includes** — Ermöglicht serverseitige Includes.
- **IncludesNOEXEC** — Ermöglicht serverseitige Includes, deaktiviert jedoch die Befehle `#exec` und `#include` in CGI- Skripten.
- **Indizes** — Zeigt eine formatierte Liste mit dem Inhalt der Verzeichnisse an, wenn kein `DirectoryIndex` (wie zum Beispiel `index.html`) im angeforderten Verzeichnis vorhanden ist.
- **Multiview** — Unterstützt Multiansichten mit ausgehandeltem Inhalt; diese Option ist standardmäßig deaktiviert.
- **SymLinksIfOwnerMatch** — Folgt symbolischen Verknüpfungen nur dann, wenn die Zieldatei oder das Zielverzeichnis demselben Besitzer wie der Verknüpfung gehört.

Klicken Sie zur Angabe von Optionen für bestimmte Verzeichnisse auf die Schaltfläche **Hinzufügen** neben dem Listenfeld **Verzeichnis**. Das in Abbildung 26-7 abgebildete Fenster wird angezeigt. Geben Sie das zu konfigurierende Verzeichnis in das Textfeld **Verzeichnis** unten im Fenster ein. Wählen Sie die Optionen in der Liste rechts und konfigurieren Sie die `Order`- Direktive mit den Optionen auf der linken Seite. Die `Order`-Direktive steuert die Reihenfolge, in der Erlaubnis- bzw. Ablehnungsdirektiven bewertet werden. In den Textfeldern **Zulassen der Hosts von** und **Verweigern der Hosts von** können Sie Folgendes festlegen:

- Alle Hosts zulassen — Geben Sie **`Alle`** ein, um den Zugriff auf alle Hosts zu erlauben.
- Teil des Domainnamens — Lässt alle Hosts zu, deren Name mit der angegebenen Zeichenfolge übereinstimmt bzw. auf sie endet.
- Volle IP-Adresse — Ermöglicht den Zugriff auf eine bestimmte IP-Adresse.
- Ein Sub-Netz — Zum Beispiel **`192.168.1.0/255.255.255.0`**
- Eine Netzwerk-CIDR-Spezifikation — Zum Beispiel **`10.3.0.0/16`**

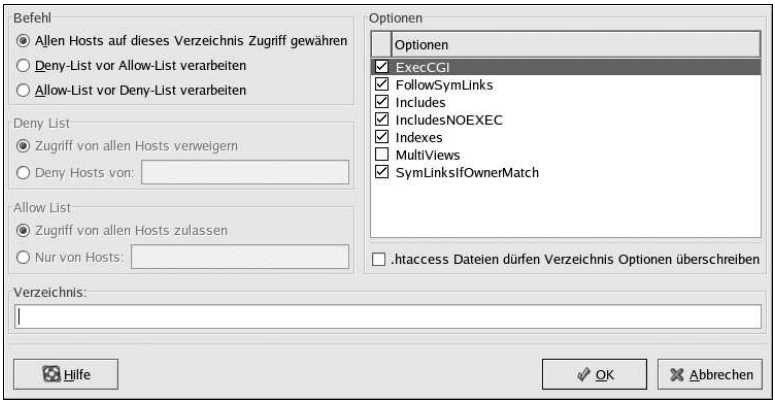

Abbildung 26-7. Verzeichniseinstellungen

Wenn Sie **Let .htaccess files override directory options** aktivieren, haben die Konfigurationsdirektiven in der Datei `.htaccess` Vorrang.

26.3. Einstellungen virtueller Hosts

Mit dem **HTTP Configuration Tool** können Sie virtuelle Hosts konfigurieren. Mit virtuellen Hosts können Sie verschiedene Server für verschiedene IP-Adressen, Hostnamen oder Ports auf demselben Rechner ausführen. Mithilfe virtueller Hosts können Sie zum Beispiel die Website für http://www.beispiel.com and http://www.nocheinbeispiel.com auf demselben Web-Server ausführen. Diese Option entspricht der <VirtualHost> für den virtuellen Standardhost und IP-basierte virtuelle Hosts. Dies entspricht `<NameVirtualHost>` für einen namenbasierten virtuellen Host.

Die für einen virtuellen Host festgelegten Einstellungen gelten nur für diesen bestimmten virtuellen Host. Wenn eine Direktive mit der Schaltfläche **Standardeinstellungen bearbeiten** serverweit und nicht in den virtuellen Hosteinstellungen festgelegt wird, wird die Standardeinstellung verwendet. Sie können beispielsweise eine **E-Mail-Adresse Webmaster** auf dem Tab **Haupt** definieren, ohne einzelne E-Mail-Adressen für jeden virtuellen Host definieren zu müssen.

Das **HTTP Configuration Tool** enthält einen virtuellen Standardhost, wie in Abbildung 26-8 zu sehen ist.

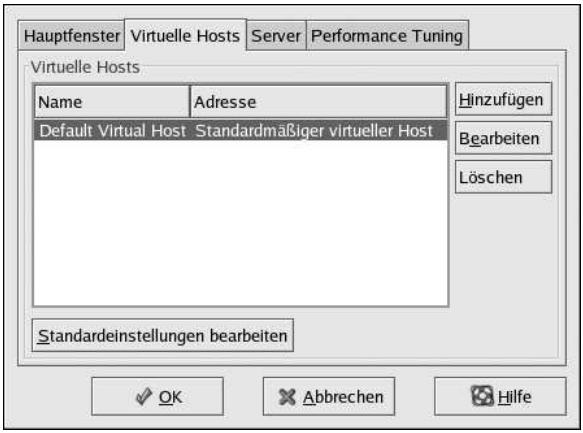

Abbildung 26-8. Virtuelle Hosts

http://www.apache.org/docs- 2.0/vhosts/ und die Apache HTTP Server-Dokumentation auf Ihrem Rechner bieten weitere Informationen über virtuelle Hosts.

26.3.1. Hinzufügen und Bearbeiten eines virtuellen Hosts

Klicken Sie zum Hinzufügen eines virtuellen Hosts auf den Tb **Virtuelle Hosts** und dann auf die Schaltfläche **Hinzufügen**. Sie können einen virtuellen Host auch bearbeiten, indem Sie ihn in der Liste auswählen und auf die Schaltfläche **Bearbeiten** klicken.

26.3.1.1. Allgemeine Optionen

Die Einstellungen **Allgemeine Optionen** gelten nur für den virtuellen Host, den Sie gerade konfigurieren. Legen Sie im Textbereich **Virtueller Hostname** den Namen des virtuellen Hosts fest. Dieser Name wird vom **HTTP Configuration Tool** verwendet, um die virtuellen Hosts zu unterscheiden.

Legen Sie den Wert für **Dokument-Root-Verzeichnis** auf das Verzeichnis fest, das das root-Dokument (wie zum Beispiel index.html) für den virtuellen Host enthält. Diese Option entspricht der`DocumentRoot`-Direktive in der `<VirtualHost>`-Direktive. Der standardmäßige`DocumentRoot` jedoch `/var/www/html`.

Die **E-Mail-Adresse Webmaster** entspricht der `ServerAdmin`- Direktive in der `VirtualHost` - Direktive. Diese E-Mail-Adresse wird in der Fußzeile von Fehlerseiten verwendet, wenn Sie sich für die Anzeige einer Fußzeile in einer E-Mail-Adresse auf Fehlerseiten entschieden haben.

Wählen Sie im Bereich **Hostinformation** die Option **Virtueller Standardhost**, **IP- basierter virtueller Host** oder **namenbasierter virtueller Host**.

Virtueller Standardhost

Sie sollten nur einen virtuellen Standardhost konfigurieren. Die Einstellungen des virtuellen Standardhosts werden verwendet, wenn die angeforderte IP-Adresse mit keinem anderen virtuellen Host übereinstimmt. Ist kein virtueller Standardhost definiert, werden die Einstellungen des Hauptservers verwendet.

IP-basierter virtueller Host

Wenn Sie **IP-basierter virtueller Host** wählen, wird ein Fenster zum Konfigurieren der <VirtualHost> -Direktive angezeigt, die auf der IP-Adresse des Servers basiert.

Geben Sie diese IP-Adresse in das Feld **IP-Adresse** ein. Trennen Sie jede IP-Adresse mithilfe von Leerzeichen, um mehrere IP-Adressen anzugeben. Verwenden Sie die Syntax *IP-Address:Port*, um einen Port anzugeben. Verwenden Sie :* um alle Ports für die IP-Adresse zu konfigurieren. Geben Sie den Hostnamen für den virtuellen Host in das Feld **Server-Hostname** ein.

Namenbasierter virtueller Host

Wenn Sie **Namenbasierter virtueller Host** wählen, wird ein Fenster zum Konfigurieren der `NameVirtualHost` -Direktive angezeigt, die auf dem Hostnamen des Servers basiert. Geben Sie die IP-Adresse in das Feld **IP- Adresse** ein. Trennen Sie jede IP-Adresse mithilfe von Leerzeichen, um mehrere IP-Adressen anzugeben. Verwenden Sie die Syntax *IP-Adresse:Port*, um einen Port anzugeben. Verwenden Sie :*, um alle Ports für die IP-Adresse zu konfigurieren. Geben Sie den Hostnamen für den virtuellen Host in das Feld **Server-Hostname** ein. Klicken Sie im Bereich **Aliases** auf **Hinzufügen**, um einen Hostnamen-Alias hinzuzufügen. Durch das Hinzufügen eines Alias wird eine `ServerAlias`-Direktive in der `NameVirtualHost`-Direktive hinzugefügt.

26.3.1.2. SSL

Anmerkung

Sie können namenbasierte virtuelle Hosts nicht mit SSL verwenden, da der SSL-Handshake (wenn der Browser das sichere Zertifikat des Web-Servers akzeptiert) vor der HTTP-Anforderung stattfindet, die den geeigneten namenbasierten virtuellen Host identifiziert. Sie können namenbasierte virtuelle Hosts nur mit nicht sicheren Web-Servern verwenden.

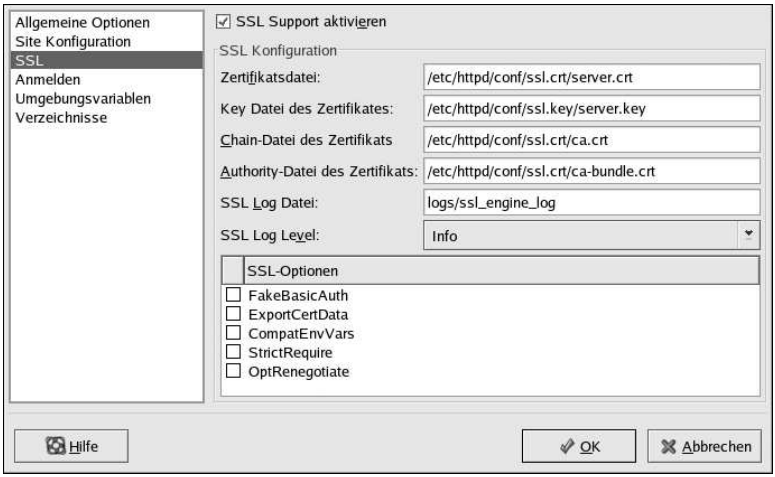

Abbildung 26-9. SSL-Unterstützung

Wenn Apache HTTP Server nicht mit SSL-Unterstützung konfiguriert ist, werden die Kommunikationen zwischen Apache HTTP Server und den Clients nicht verschlüsselt. Dies eignet sich für Websites ohne persönliche oder vertrauliche Informationen. Eine Open Source- Website, die Open Source-Software und Dokumentation verteilt, benötigt zum Beispiel keine sicheren Kommunikationen. Für eine E-Commerce-Website mit Kreditkarteninformationen sollten Sie jedoch die Apache SSL-Unterstützung verwenden, um die Kommunikationen zu verschlüsseln. Durch das Aktivieren der Apache SSL-Unterstützung wird die Verwendung des Sicherheitsmoduls `mod_ssl` aktiviert. Wenn Sie sie über das **HTTP Configuration Tool** aktivieren möchten, müssen Sie den Zugriff über Port 443 erlauben. Klicken Sie hierfür auf das Tab **Hauptfenster => Verfügbare Adressen**. Weitere Informationen finden Sie unter Abschnitt 26.1. Wählen Sie dann auf dem Tab **Virtuelle Hosts** den Namen des virtuellen Hosts aus, klicken Sie auf die Schaltfläche **Bearbeiten**, wählen Sie im Menü links **SSL** aus und aktivieren Sie die Option **SSL-Unterstützung aktivieren** wie in Abbildung 26-9 zu sehen ist. Der Bereich **SSL-Konfiguration** ist mit dem digitalen Dummy- Zertifikat vorkonfiguriert. Das digitale Zertifikat stellt Authentifizierung für den sicheren Web-Server zur Verfügung und identifiziert den sicheren Server für Web-Browser der Clients. Sie müssen Ihr eigenes digitales Zertifikat erwerben. Verwenden Sie für Ihre Website nicht das Dummy-Zertifikat. Weitere Informationen zum Erwerb eines von einer Zertifizierungsstelle genehmigten digitalen Zertifikats finden Sie unter Kapitel 27.

26.3.1.3. Zusätzliche Optionen virtueller Hosts

Die Optionen **Site-Konfiguration**, **Umgebungsvariablen** und **Verzeichnisse** für virtuelle Hosts sind dieselben Direktiven, die Sie festlegen, wenn Sie auf die Schaltfläche **Standardeinstellungen bearbeiten** klicken. Der einzige Unterschied besteht darin, dass die hier festgelegten Optionen für einzelne virtuelle Hosts gelten, die Sie konfigurieren. Weitere Einzelheiten zu diesen Optionen finden Sie unter Abschnitt 26.2.

26.4. Servereinstellungen

Mit dem Tab **Server** können Sie die grundlegenden Servereinstellungen konfigurieren. Die Standardeinstellungen für diese Optionen eignen sich für die meisten Situationen.

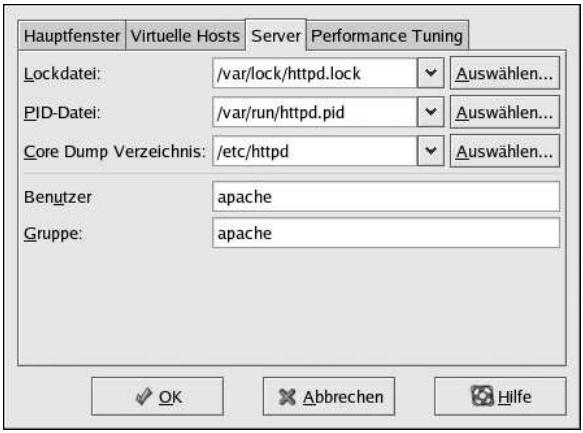

Abbildung 26-10. Serverkonfiguration

Der Wert **Lockdatei** entspricht der `LockFile`-Direktive. Diese Direktive legt den Pfad zur Sperrdatei fest, die verwendet wird, wenn der Server entweder mit USE_FCNTL_SERIALIZED_ACCEPT oder USE_FLOCK_SERIALIZED_ACCEPT kompiliert wird. Sie muss auf der lokalen Festplatte gespeichert werden. Die Standardwerte sollten beibehalten werden, es sei denn, dass sich das `logs`-Verzeichnis auf einem NFS-Share befindet. In diesem Fall muss der Standardwert auf einen Speicherplatz auf der lokalen Festplatte und ein Verzeichnis eingestellt werden, das nur vom root gelesen werden kann.

Der Wert **PID-Datei** entspricht der `PidFile`-Direktive. Diese Direktive legt die Datei fest, in der der Server die Prozess-ID (PID) speichert. Nur der root sollte diese Datei lesen können. In den meisten Fällen sollte der Standardwert beibehalten werden.

Der Wert **Core Dump Verzeichnis** entspricht der `CoreDumpDirectory`-Direktive. Apache HTTP Server versucht vor dem Kopieren der core Datei in dieses Verzeichnis zu wechseln. Der Standardwert ist `ServerRoot`. Wenn der Benutzer, unter dem der Server ausgeführt wird, jedoch nicht über Schreibzugriff auf dieses Verzeichnis verfügt, kann die core Datei nicht kopiert werden. Ändern Sie diesen Wert in ein Verzeichnis, auf das Benutzer, unter dem der Server ausgeführt wird, Schreibzugriff hat, wenn Sie die core Dateien zu Debuggingzwecken auf die Festplatte schreiben möchten.

Der Wert **Benutzer** entspricht der `User`-Direktive. Hierdurch wird die vom Server beim Antworten auf Anforderungen verwendete Benutzer-ID festgelegt. Die Benutzereinstellungen bestimmen den Serverzugriff. Die Besucher Ihrer Website haben keinen Zugriff auf die Daten, auf die dieser Benutzer nicht zugreifen kann. Der Standard für `User` ist apache.

Der Benutzer sollte nur Privilegien haben, so dass er auf Dateien zugreifen kann, die für externen Zugriff bestimmt sind. Der Benutzer ist auch der Besitzer aller vom Server erzeugten CGI-Prozesse. Der Benutzer sollte Code nur als Antwort auf HTTP-Anforderungen ausführen dürfen.

Warnung

Legen Sie die `User`-Direktive nur dann auf den root-Account fest, wenn Sie sich der Auswirkungen Ihres Handelns bewusst sind. Wenn Sie das root-Account als `User` verwenden, entstehen große Sicherheitslöcher auf Ihrem Web-Server.

Der übergeordnete `httpd`-Prozess wird zuerst während normaler Vorgänge als root-Account ausgeführt, wird dann aber sofort an den Apache-Benutzer übergeben. Der Server muss als root-Account

starten, da er eine Bindung mit einem Port unter 1024 errichten muss. Ports unter 1024 sind für Systemverwendung reserviert, sodass sie nur vom unter dem root-Account angemeldeten Benutzer verwendet werden können. Sobald der Server eine Verbindung mit seinem Port hergestellt hat, übergibt er den Prozess an den Apache-Benutzer, bevor er Verbindungsanforderungen akzeptiert.

Der Wert **Gruppe** entspricht der `Group`-Direktive. Die `Group`-Direktive ähnelt der `User`-Direktive. `Group` legt die Gruppe fest, unter der der Server auf Anfragen antwortet. Die Standardgruppe ist auch Apache.

26.5. Leistungsoptimierung

Klicken Sie auf das Tab **Performance Tuning**, um die gewünschte maximale Anzahl untergeordneter Serverprozesse sowie die Apache HTTP Server-Optionen für die Client-Verbindungen zu konfigurieren. Die Standardeinstellungen für diese Optionen sind ausreichend für die meisten Situationen. Werden diese Einstellungen geändert, kann dies Auswirkungen auf die Gesamtleistung des Web-Servers haben.

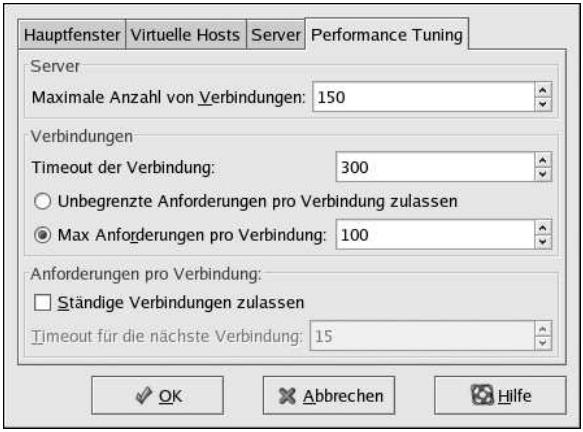

Abbildung 26-11. Leistungsoptimierung

Legen Sie **Maximale Anzahl von Verbindungen** auf die maximale Anzahl an gleichzeitigen Client-Anfragen fest, die der Server bearbeiten kann. Für jede Verbindung wird ein untergeordneter `httpd`-Prozess erstellt. Wenn die maximale Prozessanzahl erreicht wird, können solange keine Verbindungen mehr mit dem Web- Server hergestellt werden, bis ein untergeordneter Serverprozess freigesetzt wird. Überschreitet dieser Wert 256, müssen Sie neu kompilieren. Diese Option entspricht der `MaxClients`- Direktive.

Timeout der Verbindungen definiert in Sekunden die Zeit, die der Server auf Bestätigungen und Übertragungen während der Kommunikationen wartet. Insbesondere **Timeout der Verbindungen** definiert, wie lange der Server auf den Empfang einer GET-Anfrage wartet, wie lange er auf den Empfang von TCP-Paketen auf eine POST- oder PUT-Anfrage wartet und wie lange er zwischen ACK-Antworten auf TCP-Pakete wartet. Standardmäßig ist **Timeout der Verbindungen** auf 300 Sekunden festgelegt, was für die meisten Situationen geeignet ist. Diese Option entspricht der `TimeOut`-Direktive.

Legen Sie **Max. Anforderungen pro Verbindung** auf die maximale Anfragenanzahl fest, die pro dauerhafter Verbindung erlaubt ist. Der Standardwert ist 100, was für die meisten Situationen geeignet ist. Diese Option entspricht der `MaxRequestsPerChild`-Direktive.

Wenn Sie die Option **Unbegrenzte Anfragenanzahl pro Verbindung zulassen** aktivieren, wird die `MaxKeepAliveRequests` -Direktive auf 0 gesetzt, und die Anzahl der Anfragen wird nicht eingeschränkt.

Wenn Sie die Option **Ständige Verbindungen zulassen** deaktivieren, wird die `KeepAlive`-Direktive auf falsch (false) gesetzt. Wenn Sie sie aktivieren, wird die `KeepAlive`-Direktive auf wahr (true) und die `KeepAliveTimeout`- Direktive auf die Anzahl gesetzt, die als der Wert **Timeout für nächste Verbindung** ausgewählt ist. Diese Direktive legt die Anzahl der Sekunden fest, die der Server nach dem Senden einer Anfrage auf eine nachfolgende Anfrage wartet, ehe er die Verbindung beendet. Wenn er eine Anfrage erhält, gilt stattdessen der Wert **Timeout der Verbindung**.

Wenn Sie **Ständige Verbindungen** auf einen hohen Wert einstellen, kann die Serverleistung beeinträchtigt werden, je nachdem, wie viele Benutzer versuchen, eine Verbindung herzustellen. Je höher die Anzahl ist, desto mehr Serverprozesse warten auf eine andere Verbindung vom letzten Client, der eine Verbindung herstellte.

26.6. Speichern der Einstellungen

Wenn Sie die Apache HTTP Server-Konfigurationseinstellungen nicht speichern möchten, klicken Sie im Fenster **HTTP Configuration Tool** rechts unten auf die Schaltfläche **Abbrechen**. Sie werden aufgefordert, diese Entscheidung zu bestätigen. Wenn Sie zum Bestätigen auf **Ja** klicken, werden die Einstellungen nicht gespeichert.

Wenn Sie die Apache HTTP Server-Konfigurationseinstellungen speichern möchten, klicken Sie im Fenster **HTTP Configuration Tool** links unten auf die Schaltfläche **OK**. Ein Dialogfenster wird angezeigt. Wenn Sie mit **Ja** antworten, werden die Einstellungen in `/etc/httpd/conf/httpd.conf` gespeichert. Beachten Sie bitte, dass Ihre ursprüngliche Konfigurationsdatei überschrieben wird.

Wenn Sie das **HTTP Configuration Tool** zum ersten Mal verwenden, wird ein Dialogfenster mit dem Hinweis angezeigt, dass die Konfigurationsdatei manuell geändert wurde. Wenn das **HTTP Configuration Tool** erkennt, dass die Konfigurationsdatei `httpd.conf` manuell geändert wurde, speichert es die manuell geänderte Datei als `/etc/httpd/conf/httpd.conf.bak`.

Wichtig

Nach dem Speichern der Einstellungen müssen Sie den `httpd`-Daemon mit dem Befehl `service httpd restart` neu starten. Sie müssen unter einem root-Account angemeldet sein, um diesen Befehl ausführen zu können.

26.7. Zusätzliche Ressourcen

Weitere Informationen über Apache HTTP Server finden Sie in folgenden Ressourcen.

26.7.1. Installierte Dokumentation

- `/usr/share/docs/httpd-`<*version*> — Das Dokument *Apache Migration HOWTO* enthält eine Liste mit den Änderungen, die bei der Aktualisierung von Version 1.3 auf Version 2.0 erfolgten, sowie Informationen über das manuelle Migrieren der Konfigurationsdatei.

26.7.2. Hilfreiche Websites

- http://www.apache.org/ — *The Apache Software Foundation*.
- http://httpd.apache.org/docs-2.0/ — The Apache Software Foundation's Dokumentation für Apache HTTP Server Version 2.0, einschließlich *Apache HTTP Server Version 2.0 User's Guide*.
- http://www.redhat.com/support/resources/web_ftp/apache.html — Red Hat-Support pflegt eine Liste mit hilfreichen Apache HTTP Server-Links.
- http://www.redhat.com/support/docs/faqs/RH-apache-FAQ/book1.html — Die von Red Hat kompilierte Apache Centralized Knowledgebase.

26.7.3. Bücher zum Thema

- *Apache: The Definitive Guide* von Ben Laurie und Peter Laurie; O'Reilly & Associates, Inc.
- *Red Hat Enterprise Linux Referenzhandbuch*; Red Hat, Inc. — Dieses Begleithandbuch enthält Anweisungen für die manuelle Migration von Apache HTTP Server Version 1.3 zu Apache HTTP Server Version 2.0, weitere Details über die Apache HTTP Server-Direktiven und Anweisungen zum Hinzufügen von Modulen zu Apache HTTP Server.

redhat

Kapitel 27.

Konfiguration von Apache HTTP Secure Server

27.1. Einführung

Dieses Kapitel enthält grundlegende Informationen über Apache HTTP Server mit dem `mod_ssl` -Sicherheitsmodul, mit dessen Hilfe die OpenSSL-Bibliothek und das Toolkit verwendet werden können. Die Kombination dieser drei Komponenten wird in diesem Kapitel nachfolgend als Secure Web-Server oder Secure Server bezeichnet.

Das `mod_ssl`-Modul ist ein Sicherheitsmodul für Apache HTTP Server. Das `mod_ssl`-Modul verwendet die vom OpenSSL-Projekt zur Verfügung gestellten Tools, um Apache HTTP Server mit einer sehr wichtigen Funktion zusätzlich auszustatten — der Möglichkeit, Nachrichten zu verschlüsseln. Dagegen werden die zwischen Browser und Web-Server ausgetauschten Daten bei normaler HTTP-Übertragung unverschlüsselt übertragen und können theoretisch zwischen Browser und Server abgefangen und gelesen werden.

Dieses Kapitel ist nicht als vollständige und ausschließliche Dokumentation für irgendeines dieser Programme zu verstehen. Wenn möglich, wird in diesem Handbuch auf geeignete Quellen verwiesen, in denen Sie detailliertere Informationen zu speziellen Themenbereichen finden können.

In diesem Kapitel wird die Installation dieser Programme beschrieben. Außerdem werden die Schritte erklärt, die notwendig sind, um einen privaten Schlüssel und eine Zertifikatsanforderung sowie Ihr eigensigniertes Zertifikat zu erstellen wie auch die Installation eines Zertifikats, das Sie für Ihren Secure Server verwenden können.

Die Konfigurationsdatei von `mod_ssl` befindet sich im `/etc/httpd/conf.d/ssl.conf`. Damit diese Datei geladen werden kann, und somit `mod_ssl` funktioniert, muss die Anweisung `Include conf.d/*.conf` im `/etc/httpd/conf/httpd.conf` vorhanden sein. Dieses Statement ist standardmäßig in der Apache HTTP Server Konfigurationsdatei enthalten.

27.2. Überblick über die Sicherheitspakete

Für den Secure Server müssen mindestens folgende Pakete installiert sein:

`httpd`

> Das `httpd`-Paket enthält den `httpd`-Daemon und zugehörige Dienstprogramme, Konfigurationsdateien, Symbole, Apache HTTP Server-Module, man-Seiten sowie andere, von Apache HTTP Server verwendete Dateien.

`mod_ssl`

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

`openssl`

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

Daneben stehen weitere Softwarepakete mit bestimmten Sicherheitsfunktionen zur Verfügung (die allerdings nicht für das ordnungsgemäße Funktionieren von Secure Server erforderlich sind):

`httpd-devel`

Das `httpd-devel`-Paket enthält die in Include- und Header-Dateien sowie das APXS-Dienstprogramm von Apache HTTP Server. Sie benötigen alle, wenn Sie zusätzlich zu den in diesem Produkt enthaltenen Modulen noch weitere Module laden möchten. Weitere Informationen über das Laden von Modulen in Ihrem Secure Server unter Verwendung der Apache HTTP Server DSO-Funktion finden Sie im *Red Hat Enterprise Linux Referenzhandbuch*.

Wenn Sie keine weiteren Module auf Ihren Apache HTTP Server-Server laden möchten, brauchen Sie dieses Paket nicht zu installieren.

OpenSSH-Pakete

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

Das `openssh`-Paket enthält Hauptdateien, die sowohl für die OpenSSH-Clientprogramme als auch für den OpenSSH-Server benötigt werden. Das `openssh`-Paket enthält außerdem `scp`, ein sicherer Ersatz für `rcp` (zum Übertragen von Dateien zwischen Rechnern).

Das `openssh-askpass`-Paket unterstützt die Anzeige eines Dialogfensters, das während der Verwendung des OpenSSH-Agenten zur Eingabe des Passworts auffordert.

Das `openssh-askpass-gnome`-Paket enthält ein Dialogfenster für die GNOME GUI-Desktopumgebung, das angezeigt wird, wenn OpenSSH-Programme zur Eingabe des Passwortes auffordern. Wenn Sie GNOME ausführen und OpenSSH-Dienstprogramme verwenden, sollten Sie dieses Paket installieren.

Das `openssh-server`-Paket enthält den `sshd` Secure-Shell-Daemon und die entsprechenden Dateien. Beim Secure-Shell-Daemon handelt es sich um den serverseitigen Teil der OpenSSH-Programmsuite, der auf Ihrem Rechner installiert sein muss, wenn Sie SSH-Clients die Verbindung mit Ihrem Rechner ermöglichen möchten.

Das `openssh-clients`-Paket enthält die Client-Programme, die für die Erstellung von verschlüsselten Verbindungen zu SSH-Servern benötigt werden, einschließlich: `ssh`, ein sicherer Ersatz für `rsh`; `sftp`, ein sicherer Ersatz für `ftp` (für die Dateiübertragung zwischen Rechnern); und `slogin`, ein sicherer Ersatz für `rlogin` (für eine Remote-Anmeldung) und `telnet` (für die Kommunikation mit einem anderen Rechner mit Hilfe des Telnet-Protokolls).

Weitere Informationen zu OpenSSH finden Sie unter Kapitel 22, im *Red Hat Enterprise Linux Referenzhandbuch* und auf der OpenSSH-Website unter http://www.openssh.com.

`openssl-devel`

Das `openssl-devel`-Paket enthält die statischen Bibliotheken und die Include-Datei, die benötigt werden, um Applikationen mit Support für verschiedene Verschlüsselungsalgorithmen und Protokolle zu kompilieren. Sie müssen dieses Paket nur installieren, wenn Sie Applikationen entwickeln, die SSL-Support enthalten — Sie brauchen dieses Paket nicht, um SSL verwenden zu können.

`stunnel`

Das `stunnel`-Paket stellt Ihnen den Stunnel-SSL-Wrapper zur Verfügung. Stunnel unterstützt die SSL-Verschlüsselung von TCP-Verbindungen. Damit können Daemonen und Protokolle, die nicht SSL benutzen (z.B. POP, IMAP und LDAP), verschlüsselt werden, ohne dass der Code des Daemon geändert werden muss.

Tabelle 27-1 zeigt eine Zusammenfassung der Secure Server-Pakete und ob das jeweilige Paket für die Installation des Secure Server optional ist.

Paketname	Erforderlich
`httpd`	ja
`mod_ssl`	ja
`openssl`	ja
`httpd-devel`	nein
`openssh`	nein
`openssh-askpass`	nein
`openssh-askpass-gnome`	nein
`openssh-clients`	nein
`openssh-server`	nein
`openssl-devel`	nein
`stunnel`	nein

Tabelle 27-1. Sicherheitspakete

27.3. Ein Überblick über Zertifikate und Sicherheit

Ihr Secure Server gewährt Ihnen Sicherheit aufgrund einer Kombination aus einem Secure Sockets Layer (SSL)-Protokoll und (in den meisten Fällen) einem digitalen Zertifikat von einer Zertifizierungsstelle (ZS). SSL verwaltet die verschlüsselte Kommunikation und die gegenseitige Authentifizierung zwischen Browsern und Ihrem Secure Server. Die von der ZS genehmigten digitalen Zertifikate stellen die Authentifizierung für Ihren Secure Server bereit (Die ZS setzt Ihren Namen unter die Zertifizierung der Identität Ihres Unternehmens). Wenn Ihr Browser unter Verwendung der SSL- Verschlüsselung kommuniziert, wird in der Navigationsleiste vor dem Uniform Resource Locator (URL) das `https://` angezeigt.

Die Verschlüsselung hängt von der Verwendung der Schüssel ab (stellen Sie sie sich als eine Art Sicherheitsring zur Ver- und Entschlüsselung im Datenformat vor). Im Falle der konventionellen und symmetrischen Kryptografie haben beide Transaktionen am Ende den gleichen Schlüssel, mit dem sie ihre jeweiligen Übertragungen gegenseitig entschlüsseln können. In der öffentlichen oder asymmetrischen Kryptografie bestehen zwei Schlüssel gleichzeitig nebeneinander: ein öffentlicher und ein privater Schlüssel. Eine Privatperson oder ein Unternehmen gibt seinen privaten Schlüssel nicht heraus und hält ihn geheim und veröffentlicht nur den öffentlichen Schlüssel. Daten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur mit dem privaten Schlüssel entschlüsselt werden; Und Daten, die mit dem privaten Schlüssel verschlüsselt wurden, können nur mit dem öffentlichen Schlüssel entschlüsselt werden.

Für das Einrichten Ihres Secure Server verwenden Sie zur Erstellung eines öffentlichen und privaten Schlüsselpaares die öffentliche Kryptografie. In den meisten Fällen senden Sie Ihren Zertifikatsantrag (einschließlich des öffentlichen Schlüssels), den Nachweis der Identität Ihres Unternehmens und die Zahlung an die ZS. Die ZS wird Ihren Antrag und Ihre Identität überprüfen und Ihnen sodann ein Zertifikat für Ihren Secure Server ausstellen.

Ein Secure Server verwendet ein Zertifikat, um von Web-Browsern identifiziert werden zu können. Sie können entweder Ihr eigenes Zertifikat erstellen (eigensigniertes Zertifikat genannt) oder sich ein Zertifikat von einer Zertifizierungsstelle (ZS) erstellen lassen. Das Zertifikat einer namhaften ZS gewährleistet, dass eine Website mit einem bestimmten Unternehmen oder einer Organisation in Verbindung steht.

Alternativ hierzu können Sie Ihr eigensigniertes Zertifikat erstellen. Beachten Sie aber, dass eigensignierte Zertifikate in den meisten Produktionszusammenhängen vermieden werden sollten. Eigensi-

gnierte Zertifikate werden nicht automatisch vom Browser eines Benutzers akzeptiert — Der Benutzer wird vom Browser gefragt, ob er das Zertifikat akzeptieren und eine sichere Verbindung herstellen möchte. Unter Abschnitt 27.5 finden Sie weitere Informationen zum Unterschied zwischen eigensignierten und ZS-signierten Zertifikaten.

Nachdem Sie ein eigensigniertes Zertifikat erstellt oder eines von einer ZS Ihrer Wahl erhalten haben, müssen Sie es auf dem Secure Server installieren.

27.4. Verwendung bereits vorhandener Schlüssel und Zertifikate

Wenn Sie bereits einen Schlüssel oder ein Zertifikat haben (z.B. wenn Sie den Secure Server installieren, um einen Secure Server eines anderen Unternehmens damit zu ersetzen), werden Sie wahrscheinlich den bereits bestehenden Schlüssel und das Zertifikat für den Secure Server verwenden können. Nachfolgend werden zwei Fälle beschrieben, in denen Sie Ihren bereits bestehenden Schlüssel und das Zertifikat nicht verwenden können:

- *Wenn Sie Ihre IP-Adresse oder Ihren Domainnamen ändern* — Zertifikate werden für ein bestimmtes Paar aus IP-Adresse und Domainnamen erstellt. Bei Änderung Ihrer IP-Adresse oder Ihres Domainnamens benötigen Sie daher ein neues Zertifikat.
- *Wenn Sie ein Zertifikat von VeriSign haben und Ihre Server-Software ändern* — Sehr viele Zertifikate werden von der ZS VeriSign erstellt. Wenn Sie bereits ein VeriSign- Zertifikat zu einem anderen Zweck haben, mögen Sie daran gedacht haben, dieses bereits bestehende VeriSign-Zertifikat auch für Ihren neuen Secure Server zu verwenden. Dies ist allerdings nicht erlaubt, denn VeriSign erteilt seine Zertifikate nur für eine ganz bestimmte Serversoftware und Kombination aus IP-Adresse und Domainnamen.

  Wenn Sie einen dieser beiden Parameter ändern (z.B. wenn Sie vorher ein anderes Secure Server-Produkt verwendet haben), können Sie das VeriSign-Zertifikat, das Sie für die vorherige Konfiguration erhalten haben, nicht mehr mit der neuen Konfiguration verwenden. Sie müssen ein neues Zertifikat beantragen.

Wenn Sie bereits einen Schlüssel und ein Zertifikat haben, müssen Sie keinen neuen Schlüssel erstellen oder ein neues Zertifikat beantragen. Es kann allerdings erforderlich sein, dass Sie die Dateien, die Schlüssel und Zertifikat enthalten, verschieben und umbenennen müssen.

Verschieben Sie Ihre vorhandene Schlüsseldatei nach:

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

Verschieben Sie Ihre vorhandene Zertifikatdatei nach:

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

Nachdem Sie Ihren Schlüssel und Ihr Zertifikat verschoben haben, gehen Sie zu Abschnitt 27.9.

Wenn Sie ein Upgrade von Red Hat Secure Web Server durchführen, wird Ihr alter Schlüssel (`httpsd.key`) und das Zertifikat (`httpsd.crt`) im Verzeichnis `/etc/httpd/conf/` abgelegt. Sie müssen Ihren Schlüssel und Ihr Zertifikat verschieben und umbenennen, damit der Secure Server sie verwenden kann. Verwenden Sie zum Verschieben und Umbenennen Ihrer Schlüssel- und Zertifikatsdateien die beiden folgenden Befehle:

```
mv /etc/httpd/conf/httpsd.key /etc/httpd/conf/ssl.key/server.key
mv /etc/httpd/conf/httpsd.crt /etc/httpd/conf/ssl.crt/server.crt
```

Starten Sie anschließend Ihren Secure Server mit folgendem Befehl:

```
/sbin/service httpd start
```

Um die Sicherheit des Secure Server zu gewährleisten, werden Sie aufgefordert, Ihr Passwort einzugeben. Nach der Eingabe Ihres Passworts drücken Sie die [Enter-Taste], und der Server wird gestartet.

27.5. Zertifikatstypen

Wenn Sie den Secure Server mit dem von Red Hat bereitgestellten RPM-Paket installiert haben, wird ein zufällig-generierter Schlüssel und ein Testzertifikat erstellt und in die hierfür geeigneten Verzeichnisse abgelegt. Vor der Verwendung des Secure Server müssen Sie jedoch Ihren eigenen Schlüssel erstellen und benötigen ein Zertifikat, das Ihren Server korrekt identifiziert.

Um mit dem Secure Server benötigen Sie einen Schlüssel und ein Zertifikat — das heißt, Sie müssen entweder ein eigensigniertes Zertifikat erstellen oder ein ZS-signiertes Zertifikat bei einer ZS bestellen. Worin unterscheiden sich diese zwei Zertifikatstypen?

Mit einem ZS-signierten Zertifikat verfügt Ihr Server über zwei wichtige Funktionen:

- Browser erkennen das Zertifikat (in der Regel) automatisch und erlauben sodann ohne zusätzliche Nachfrage beim Benutzer die Herstellung einer sicheren Verbindung.
- Mit einem ZS-signierten Zertifikat wird die Identität des Unternehmens garantiert, das dem Browser die Webseiten zur Verfügung stellt.

Wenn eine breitere Öffentlichkeit Zugriff auf den Secure Server hat, benötigt der Secure Server ein ZS-signiertes Zertifikat, damit die Personen, die sich Ihre Webseite anschauen, auch darauf vertrauen können, dass diese Webseite tatsächlich Eigentum des Unternehmens ist, die dies behauptet.

Die meisten Web-Browser, die SSL unterstützen, haben eine Liste von ZS, deren Zertifikate sie automatisch akzeptieren. Wenn der Browser auf ein Zertifikat stößt, das nicht in der Liste der autorisierenden ZS enthalten ist, wird der Benutzer vom Browser aufgefordert, die Verbindung anzunehmen oder abzulehnen.

Sie können ein eigensigniertes Zertifikat für Ihren Secure Server erstellen, aber Sie sollten dabei bedenken, dass ein eigensigniertes Zertifikat nicht die gleiche Funktionalität wie ein ZS-signiertes Zertifikat bietet. Ein eigensigniertes Zertifikat wird nicht automatisch vom Browser des Benutzers anerkannt und kann auch keine Garantie für die Identität des Unternehmens geben, das die Website zur Verfügung stellt. Ein ZS-signiertes Zertifikat hingegen liefert die beiden vorgenannten Vorteile eines sicheren Servers. Und wenn Ihr Secure Server in einer Produktionsumgebung eingesetzt wird, benötigen Sie wahrscheinlich ein ZS-signiertes Zertifikat.

Die Beantragung eines Zertifikats bei einer ZS ist denkbar einfach, wie der nachfolgende kurze Überblick zeigt:

1. Erstellen eines privaten und eines öffentlichen Schlüssels
2. Erstellen eines Zertifikatsantrags, der auf dem öffentlichen Schlüssel basiert. Der Zertifikatsantrag enthält Informationen zu Ihrem Server und dem dazugehörigen Unternehmen.
3. Senden Sie den Antrag zusammen mit den Dokumenten, mit denen Sie Ihre Identität nachweisen, zu einer ZS. Da Ihre Wahl der ZS vermutlich auf eigenen Erfahrungen oder denen von Freunden und Kollegen beruht oder auf rein finanziellen Überlegungen basiert, möchten wir Ihnen keinen Vorschlag machen, für welche Zertifizierungsstelle Sie sich entscheiden sollten.

   Nachdem Sie sich für eine ZS entschieden haben, folgen Sie den Anweisungen dieser Stelle, wie Sie ein Zertifikat erhalten.
4. Nach Überprüfung der Identität Ihres Unternehmens wird Ihnen die Zertifizierungsstelle ein digitales Zertifikat übersenden.
5. Nach der Installation dieses Zertifikats auf Ihrem Secure Server sind Ihre Transaktionen nun gegen unerlaubten Zugriff geschützt.

Unabhängig davon, ob Sie ein ZS-signiertes oder ein selbstsigniertes Zertifikat haben, müssen Sie zuallererst einen Schlüssel erstellen. Unter Abschnitt 27.6 finden Sie die Anweisungen zur Erstellung eines Schlüssels.

27.6. Erstellen eines Schlüssels

Sie müssen als unter einem root-Account angemeldet sein, um einen Schlüssel erstellen zu können.

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

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

Als nächstes müssen Sie Ihren eigenen zufälligen Schlüssel erstellen. Wechseln Sie ins Verzeichnis `/usr/share/ssl/certs/` und geben Sie folgenden Befehl ein:

```
make genkey
```

Ihr System zeigt eine Meldung ähnlich der Folgenden an:

```
umask 77 ; \
/usr/bin/openssl genrsa -des3 1024 > /etc/httpd/conf/ssl.key/server.key
Generating RSA private key, 1024 bit long modulus
.......++++++
.....................................................................++++++
e is 65537 (0x10001)
Enter pass phrase:
```

Geben Sie jetzt Ihr Passwort ein. Um größtmögliche Sicherheit zu gewähren, sollte Ihr Passwort aus mindestens acht Zeichen bestehen, Zahlen und/oder Punkte enthalten und ein Wort sein, das man in keinem Wörterbuch findet. Bedenken Sie außerdem, dass Ihr Passwort Groß- und Kleinschreibung beachtet.

Anmerkung

Sie müssen Ihr Passwort bei jedem Start Ihres Secure Server eingeben, prägen Sie es sich also gut ein.

Sie werden aufgefordert, Ihr Passwort ein zweites Mal einzugeben, um zu überprüfen, dass es korrekt ist. Nach der korrekten Eingabe wird die Datei `/etc/httpd/conf/ssl.key/server.key` erstellt, die Ihren Schlüssel enthält.

Wenn Sie nicht bei jedem Start Ihres Secure Server Ihr Passwort eingeben möchten, müssen Sie die beiden folgenden Befehle statt `make genkey` verwenden, um einen Schlüssel zu erstellen.

Verwenden Sie folgenden Befehl zum Erstellen des Schlüssels:

```
/usr/bin/openssl genrsa 1024 > /etc/httpd/conf/ssl.key/server.key
```

Verwenden Sie dann folgenden Befehl zum Sicherstellen, dass die Berechtigungen für den Schlüssel korrekt festgelegt sind:

```
chmod go-rwx /etc/httpd/conf/ssl.key/server.key
```

Nach Verwendung der o.g. Befehle zur Erstellung Ihres Schlüssels brauchen Sie nicht mehr Ihr Passwort einzugeben, um den Secure Server zu starten.

Achtung

Die Deaktivierung der Passwort-Funktion für Ihren Secure Server is a stellt ein Sicherheitsrisiko dar. Aus diesem Grund empfehlen wir Ihnen, die Passwort-Funktion für Ihren Secure Server NICHT zu deaktivieren.

Die Probleme, die auftreten, wenn kein Passwort benutzt wird, haben direkten Einfluss auf die Sicherheit des Rechners. Wenn z.B. jemand die reguläre UNIX-Sicherheit eines Rechners überwindet, kann diese Person Ihren privaten Schlüssel (die Inhalte Ihrer `server.key` Datei) abrufen. Der Schlüssel kann dann benutzt werden, um Webseiten zu erstellen, die scheinbar von Ihrem Secure Server stammen.

Wenn die UNIX-Sicherheitsregeln auf dem Rechner strikt eingehalten werden (d.h. alle Betriebssystem-Patches und -Aktualisierungen werden bei Verfügbarkeit sofort installiert, es werden keine unnötigen oder riskanten Dienste in Anspruch genommen o.ä.), mag Ihnen die Verwendung Ihres Passworts für den Secure Server überflüssig und unnötig erscheinen. Da Ihr Secure Server aber ohnehin nicht allzuoft neu gebootet werden sollte, lohnt es sich dennoch in den meisten Fällen, Ihr Passwort zu verwenden, das Ihnen extrem hohe Sicherheit gewährleistet.

Die `server.key`-Datei sollte Eigentum des root-Accounts Ihres Systems und für andere Benutzer nicht zugänglich sein. Erstellen Sie eine Sicherungskopie dieser Datei und bewahren Sie die Sicherungskopie an einem sicheren und geheimen Ort auf. Die Sicherungskopie ist wichtig für den Fall, dass die `server.key`-Datei nach der Erstellung des Zertifikatsantrags verloren gehen sollte. In diesem Fall wird Ihr Zertifikat ungültig, und die ZS wird Ihnen in diesem Fall nicht weiterhelfen können. Die einzige Lösung wäre dann ein neuer Antrag eines Zertifikats (und dessen Bezahlung).

Wenn Sie ein Zertifikat von einer ZS erwerben, fahren Sie unter Abschnitt 27.7 fort. Wenn Sie Ihr eigensigniertes Zertifikat erstellen möchten, fahren Sie unter Abschnitt 27.8 fort.

27.7. Erstellen eines Zertifikatsantrags für eine ZS

Sobald Sie einen Schlüssel erstellt haben, ist der nächste Schritt für Sie die Erstellung eines Zertifikatsantrags, den Sie an die ZS Ihrer Wahl schicken. Stellen Sie sicher, dass Sie sich im `/usr/share/ssl/certs`-Verzeichnis befinden, und geben Sie folgenden Befehl ein:

```
make certreq
```

Ihr System zeigt folgende Ausgabe an und fordert Sie auf, Ihr Passwort einzugeben (es sei denn, Sie haben die Passwort-Option deaktiviert):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-out /etc/httpd/conf/ssl.csr/server.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter pass phrase:
```

Geben Sie das Passwort ein, mit dem Sie den Schlüssel erstellt haben. Ihr System wird einige Anweisungen anzeigen und Sie dann auffordern, eine Reihe von Fragen zu beantworten. Ihre Eingaben werden in den Zertifikatsantrag integriert. Die anschließende Anzeige mit Beispielantworten sieht folgendermaßen aus:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:Test Company
Organizational Unit Name (eg, section) []:Testing
Common Name (your name or server's hostname) []:test.example.com
Email Address []:admin@example.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Die Standardantworten werden unmittelbar nach den jeweiligen Eingabeaufforderungen in Klammern angezeigt `[]`. Die erste Angabe, zu der Sie aufgefordert werden, ist das Land, in dem das Zertifikat benutzt werden soll. Dies sieht dann wie folgt aus:

```
Country Name (2 letter code) [GB]:
```

Die vordefinierte Eingabe in eckigen Klammern ist **GB**. Wenn Sie den Standardwert akzeptieren möchten, drücken Sie einfach die [Enter-Taste] oder geben den zweistelligen Code Ihres Landes an.

Geben Sie dann die restlichen Angaben ein. Dies sollte selbsterklärend sein, halten Sie sich jedoch an folgende Richtlinien:

- Kürzen Sie den Namen der Stadt oder des Landes nicht ab, sondern schreiben ihn jeweils aus (St. Augustin wird also beispielsweise als Sankt Augustin eingegeben).
- Wenn Sie diesen Zertifikatsantrag an eine ZS schicken, achten Sie bitte darauf, dass Ihre Angaben in allen Feldern vollständig und korrekt sind, insbesondere in den Feldern `Organization Name` und `Common Name`. Eine ZS überprüft die Angaben im Zertifikatsantrag, um sicherzustellen, dass Ihr Unternehmen wie unter `Common Name` angegeben haftbar ist. Die ZS wird solche Anträge, in denen aus Ihrer Sicht ungültige Angaben enthalten sind, zurückschicken.
- Stellen Sie bei der Eingabe des `Common Name` sicher, dass Sie den *wirklichen* Namen Ihres Secure Server (ein gültiger DNS-Name) und keinen Alias-Namen eingeben.
- Die `Email Address` sollte mit der E-Mail-Adresse Ihres Webmasters oder Systemadministratoren übereinstimmen.
- Vermeiden Sie alle Sonderzeichen wie z.B. @, #, &, ! o.ä. Einige ZS weisen Zertifikatsanträge, die Sonderzeichen enthalten, zurück. Wenn also Ihr Unternehmens-Name ein "&" enthält, schreiben Sie ihn aus und geben statt "&" das Wort "und" ein.
- Füllen Sie unter den zusätzlichen Attributen weder (`A challenge password` noch `An optional company name`) aus. Um mit der Eingabe fortzufahren, ohne diese Felder auszufüllen, drücken Sie einfach die [Enter-Taste], um die leeren Felder der Voreinstellung bei beiden Felder zu übernehmen.

Nach der Eingabe Ihrer Daten wird eine Datei mit dem Namen `/etc/httpd/conf/ssl.csr/server.csr` erstellt. Diese Datei ist Ihre Zertifikatsanfrage, die Sie nun an die ZS schicken können.

Nachdem Sie sich für eine ZS entschieden haben, folgen Sie deren Anweisungen auf der Website. Diesen Anweisungen entnehmen Sie, wie Sie Ihren Zertifikatsantrag verschicken sollen, welche Dokumente außerdem noch für die ZS erforderlich sind. Desweiteren werden Sie hier über die Zahlungsmodalitäten informiert.

Sobald Sie die Anforderungen der ZS erfüllt haben, wird Ihnen diese das Zertifikat (in der Regel per E-Mail) zusenden. Speichern Sie (auch durch Ausschneiden/Einfügen möglich) das Ihnen von der ZS zugesandte Zertifikat unter dem Namen `/etc/httpd/conf/ssl.crt/server.crt`. Stellen Sie sicher, dass Sie ein Backup dieser Datei erstellen.

27.8. Erstellen eines eigensignierten Zertifikats

Sie können Ihr eigensigniertes Zertifikat erstellen. Beachten Sie dabei aber bitte, dass eigensignierte Zertifikate nicht die gleiche Sicherheit wie ein ZS-signiertes Zertifikat gewährleisten. Weitere Einzelheiten zu Zertifikaten finden Sie unter Abschnitt 27.5.

Wenn Sie ein eigensigniertes Zertifikat erstellen wollen, müssen Sie zunächst einen willkürlichen Schlüssel erstellen, und zwar nach den Anweisungen unter Abschnitt 27.6. Sobald Sie diesen Schlüssel erstellt haben, stellen Sie sicher, dass Sie sich im Verzeichnis `/usr/share/ssl/certs/` befinden, und geben Sie folgenden Befehl ein:

```
make testcert
```

Sie erhalten sodann folgende Mitteilung und werden aufgefordert, Ihr Passwort einzugeben (es sei denn, Sie haben einen Schlüssel ohne Passwort erstellt):

```
umask 77 ; \
/usr/bin/openssl req -new -key /etc/httpd/conf/ssl.key/server.key
-x509 -days 365 -out /etc/httpd/conf/ssl.crt/server.crt
Using configuration from /usr/share/ssl/openssl.cnf
Enter pass phrase:
```

Nachdem Sie Ihr Passwort eingegeben haben (oder wenn Sie einen Schlüssel ohne Passwort erstellt haben), werden Sie aufgefordert weitere Angaben zu machen. Die Computerausgaben und eine Reihe von Eingaben sehen wie folgt aus (Sie müssen korrekte Angaben zu Ihrem Unternehmen und Ihrem Rechner machen):

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:North Carolina
Locality Name (eg, city) [Newbury]:Raleigh
Organization Name (eg, company) [My Company Ltd]:My Company, Inc.
Organizational Unit Name (eg, section) []:Documentation
Common Name (your name or server's hostname) []:myhost.example.com
Email Address []:myemail@example.com
```

Nach der vollständigen Eingabe aller korrekten Angaben wird das Zertifikat erstellt und in der Datei `/etc/httpd/conf/ssl.crt/server.crt` abgelegt. Nach der Erstellung des Zertifikats starten Sie Ihren Secure Server mit dem folgenden Befehl neu:

```
/sbin/service httpd restart
```

27.9. Testen Ihres Zertifikats

Um das standardmäßig installierte Test-Zertifikat, ein ZS-signiertes oder ein selbstsigniertes Zertifikat zu testen, gehen Sie durch Ihren Web-Browser auf die folgende Homepage (ersetzen Sie *server.example.com* durch Ihren Domainnamen):

`https://server.example.com`

Anmerkung

Beachten Sie das `s` hinter `http`. `https:` wird für sichere HTTP-Transaktionen verwendet.

Wenn Sie ein ZS-signiertes Zertifikat einer anerkannten ZS verwenden, wird Ihr Browser das Zertifikat höchstwahrscheinlich automatisch akzeptieren (ohne jedwede Eingaben zu verlangen), und die Verbindung herstellen. Ihr Browser erkennt nicht automatisch ein Test - oder eigensigniertes Zertifikat, da dieses nicht von einer ZS signiert wurde. Wenn Sie kein ZS-signiertes Zertifikat verwenden, folgen Sie den Anweisungen in Ihrem Browser, um diese Zertifikate anzunehmen.

Wenn Ihr Browser das Zertifikat anerkannt hat, zeigt Ihnen der Secure Server eine Standard-Homepage.

27.10. Zugriff auf Ihren Server

Um auf Ihren Secure Server zugreifen zu können, verwenden Sie die folgende URL:

`https://server.example.com`

Auf Ihren ungesicherten Server kann mit folgendem URL zugegriffen werden:

`http://server.example.com`

Der Standardport für gesicherte Web-Übertragungen ist Port 443. Der Standardport für ungesicherte Web-Übertragungen ist Port 80. Der Secure Server ist standardmäßig so konfiguriert, dass beide Standardports abgehört werden, weswegen Sie die Portnummer in der URL- Zeile nicht näher angegeben müssen (sie wird automatisch angenommen).

Wenn Sie Ihren Server allerdings so konfigurieren, dass er einen nicht voreingestellten Port abhört (d.h. alle Ports außer 80 oder 443), müssen Sie diese Portnummer in allen URLs angeben, mit der die Verbindung zum Server auf dem nichtvoreingestellten Port hergestellt werden soll.

Beispiel: Sie haben Ihren Server so konfiguriert, dass ein virtueller Rechner über den nicht gesicherten Port 12331 läuft. Alle URLs, die mit diesem virtuellen Rechner eine Verbindung herstellen sollen, müssen dessen Portnummer im URL enthalten. Mit dem folgenden URL-Beispiel soll die Verbindung mit einem nicht gesicherten Web-Server hergestellt werden, der Port 12331 abhört:

`http://server.example.com:12331`

27.11. Zusätzliche Ressourcen

Unter Abschnitt 26.7 finden Sie zusätzliches Referenzmaterial zu Apache HTTP Server.

27.11.1. Hilfreiche Websites

- http://www.redhat.com/mailman/listinfo/redhat-secure-server — Die `redhat-secure-server` Mailing-Liste.

  Desweiteren können Sie die `redhat-secure-server`-Mailingliste abonnieren, indem Sie ein E-Mail an <`redhat-secure-server-request@redhat.com`> und das Wort *subscribe* in der Betreffzeile angeben.
- http://www.modssl.org/ — Die `mod_ssl`-Website ist die optimale Quelle für Informationen zu `mod_ssl`. Die Website enthält zahlreiche Dokumentationen, einschließlich eines *Benutzerhandbuchs* unter http://www.modssl.org/docs/.

27.11.2. Literatur zu diesem Thema

- *Apache: The Definitive Guide*, zweite Ausgabe, Laurie and Peter Laurie, O'Reilly & Associates, Inc.

Kapitel 28.

BIND-Konfiguration

In diesem Kapitel wird vorausgesetzt, dass Sie bereits über Grundwissen in BIND und DNS verfügen, da hier die Basiskonzepte nicht erläutert werden, sondern erklärt wird, wie das **Domain Name Service Configuration Tool** (`redhat-config- bind`) verwendet wird, um die grundlegenden BIND-Serverzonen zu konfigurieren. Das **Domain Name Service Configuration Tool** erstellt die Konfigurationsdatei `/etc/named.conf` und die Zonen-Konfigurationsdateien im Verzeichnis `/var/named/`, sobald Ihre Änderungen wirksam werden.

Wichtig

Bearbeiten Sie die Konfigurationsdatei `/etc/named.conf` nicht. Das **Domain Name Service Configuration Tool** generiert diese Datei, nachdem Ihre Änderungen angewendet wurden. Wenn Sie Einstellungen konfigurieren möchten, die nicht mit dem **Domain Name Service Configuration Tool** konfigurierbar sind, fügen Sie sie zu `/etc/named.custom` hinzu.

Das **Domain Name Service Configuration Tool** erfordert das X Window System und die Anmeldung unter einem root-Account. Starten Sie das **Domain Name Service Configuration Tool**, indem Sie auf **Hauptmenü** (im Panel) => **Systemeinstellungen** => **Servereinstellungen** => **Domain Name Service** klicken, oder an einem Shell-Prompt den Befehl `redhat-config-bind` eingeben (zum Beispiel an einem XTerm- oder GNOME-Terminal).

Abbildung 28-1. Domain Name Service Configuration Tool

Das **Domain Name Service Configuration Tool** konfiguriert als standardmäßiges Zonenverzeichnis `/var/named/`. Alle angegebenen Zonendateien beziehen sich auf dieses Verzeichnis. Das **Domain Name Service Configuration Tool** sieht bei der Eingabe von Werten auch die Prüfung der Syntax vor. Wenn ein gültiger Eintrag beispielsweise eine IP-Adresse ist, können Sie ausschließlich Zahlen und Punkte (.) in das Textfeld eingeben.

Mit dem **Domain Name Service Configuration Tool** können Sie eine Forward-Masterzone, eine Reverse-Masterzone und eine Slave-Zone hinzuzufügen. Nachdem Sie diese Zonen hinzugefügt haben, können Sie sie im Hauptfenster bearbeiten oder löschen (siehe Abbildung 28-1.

Nachdem eine Zone hinzugefügt, bearbeitet oder gelöscht wurde, klicken Sie auf **Speichern** oder **Datei => Speichern**, um die Konfigurationsdatei `/etc/named.conf` und alle Zonendateien in das Verzeichnis `/var/named/` zu schreiben. Durch die Übernahme Ihrer Änderungen wird weiterhin der `named` -Dienst veranlasst, die Konfigurationsdateien neu zu laden. Sie können auch auf **Datei => Beenden** klicken, um die Änderungen zu speichern und das Programm zu beenden.

28.1. Hinzufügen einer Forward-Masterzone

Um eine Forward-Masterzone (auch bekannt als primärer Master) hinzuzufügen, klicken Sie auf die Schaltfläche **Neu** Wählen Sie **Forward-Masterzone**, und geben Sie den Domainnamen für die Masterzone in das Textfeld **Domainname** ein.

Ein neues Fenster (siehe Abbildung 28-2) mit folgenden Optionen wird angezeigt:

- **Name** — Der Domainname, der im vorigen Fenster eingegeben wurde.
- **Dateiname** — Der Dateiname der DNS-Datenbankdatei in Bezug auf `/var/named`. Mit `.zone` wird der Dateiname auf den Domainnamen gesetzt.
- **Kontakt** — Die E-Mail-Adresse des Hauptkontakts für die Masterzone.
- **Primärer Nameserver (SOA)** — Datensatz des Berechtigungsstatus (State of Authority, SOA). Hiermit wird der Name des Servers angegeben, der die beste Informationsressource für diese Domain darstellt.
- **Seriennummer** — Die Seriennummer der DNS-Datenbankdatei. Diese Zahl muss jedes Mal erhöht werden, wenn die Datei geändert wird, so dass die Slave-Name- Server für die Zone die jüngsten Daten abrufen. Das **Domain Name Service Configuration Tool** erhöht diese Zahl, sobald die Konfiguration verändert wird. Die Zahl kann auch manuell geändert werden. Klicken Sie hierzu auf **Einstellen** neben dem Wert **Seriennummer**.
- **Zeiteinstellung** — Die Werte **Refresh**, **Retry**, **Expire** und **Minimum**-TTL (Time to Live), die in der DNS-Datenbankdatei gespeichert sind. Alle Werte sind in Sekunden angegeben.
- **Datensätze** — Datensatzressourcen des Typs **Host**, **Alias** und **Nameserver** hinzufügen, bearbeiten und löschen.

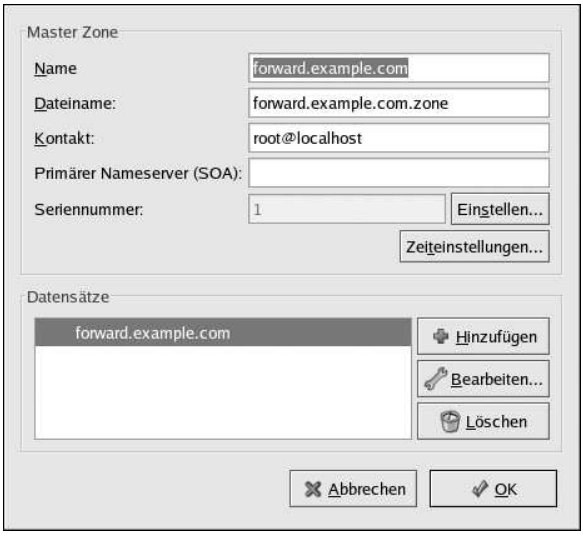

Abbildung 28-2. Hinzufügen einer Forward-Masterzone

Ein **Primärer Nameserver (SOA)** muss angegeben werden, und es muss mindestens ein Nameserver-Datensatz angegeben werden, in dem Sie auf **Hinzufügen** im Abschnitt **Datensätze** klicken.

Klicken Sie nach der Konfiguration der Forward-Masterzone auf **OK**, um in das in Abbildung 28-1 gezeigte Hauptfenster zurückzukehren. Klicken Sie auf **Speichern**, um die Konfigurationsdatei `/etc/named.conf` zu schreiben, um alle Zonendateien in das Verzeichnis `/var/named` zu schreiben und den Daemon zu veranlassen, die Konfigurationsdateien neu zu laden.

Die Konfiguration erstellt dann einen Eintrag ähnlich dem folgenden in `/etc/named.conf`:

```
zone  "forward.example.com" {
 type master;
 file  "forward.example.com.zone";
};
```

Sie erstellt weiterhin die Datei `/var/named/forward.example.com.zone` mit folgenden Informationen:

```
$TTL 86400
@       IN      SOA     ns.example.com.  root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )


        IN      NS      192.168.1.1.
```

28.2. Hinzufügen einer Reverse-Masterzone

Um eine Reverse-Masterzone hinzuzufügen, klicken Sie auf **Neu** und wählen Sie **Reverse Master Zone**. Geben Sie die ersten drei Achtergruppen des IP-Adressenbereichs ein, den Sie konfigurieren möchten. Wenn Sie beispielsweise den Bereich 192.168.10.0/255.255.255.0 konfigurieren möchten, geben Sie 192.168.10 in das Textfeld **IP-Adresse (ersten 3 Achtergruppen)** ein.

Ein neues Fenster (siehe Abbildung 28-3) mit den folgenden Optionen wird angezeigt:

1. **IP-Adresse** — Die ersten drei Achtergruppen, die Sie im vorigen Fenster eingegeben haben.
2. **Reverse IP-Adresse** — Nicht bearbeitbar und bereits auf der Grundlage der eingegebenen IP-Adresse aufgefüllt.
3. **Kontakt** — E-Mail-Adresse des Hauptkontaktes für die Masterzone.
4. **Dateiname** — Dateiname der DNS- Datenbankdatei im Verzeichnis `/var/named`.
5. **Primärer Nameserver (SOA)** — Datensatz des Berechtigungsstatus (State of Authority, SOA). Hiermit wird der Name des Servers angegeben, der die beste Informationsressource für diese Domain darstellt.
6. **Seriennummer** — Die Seriennummer der DNS-Datenbankdatei. Diese Zahl muss jedes Mal erhöht werden, wenn die Datei geändert wird, so dass die Slave-Name- Server für die Zone die jüngsten Daten abrufen. Das **Domain Name Service Configuration Tool** erhöht diese Zahl, sobald die Konfiguration verändert wird. Die Zahl kann auch manuell geändert werden. Klicken Sie hierzu auf **Einstellen** neben dem Wert **Seriennummer**.
7. **Zeiteinstellung** — Die Werte **Refresh**, **Retry**, **Expire** und **Minimum**-TTL (Time to Live), die in der DNS-Datenbankdatei gespeichert sind.
8. **Nameserver** — Nameserver für die Reverse-Masterzone hinzufügen, bearbeiten und löschen. Mindestens ein Nameserver ist erforderlich.
9. **Reverse-Adressen-Tabelle** — Liste mit IP- Adressen innerhalb der Reverse-Masterzone und den entsprechenden Hostnamen. Für die Reverse-Masterzone 192.168.10 zum Beispiel können Sie 192.168.10.1 in **Reverse-Adressen-Tabelle** mit dem Rechnernamen one.example.com. hinzufügen. Der Rechnername muss mit einem Punkt (.) enden, um anzugeben, dass es sich um einen vollständigen Rechnernamen handelt.

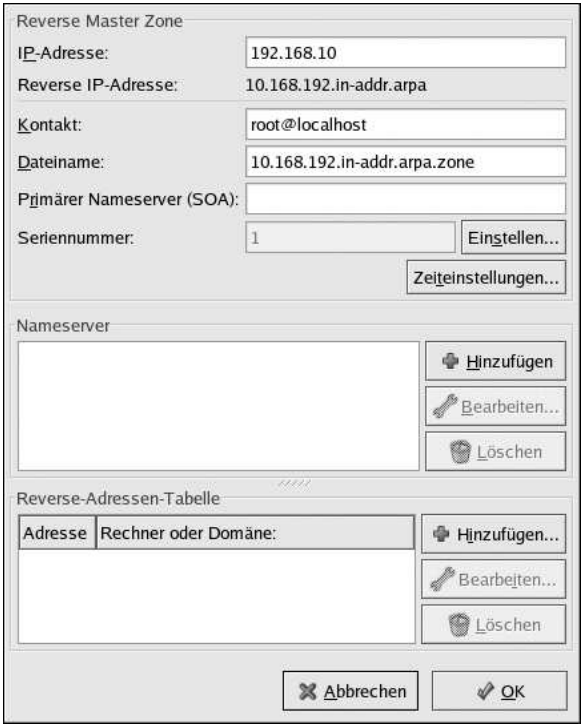

Abbildung 28-3. Hinzufügen einer Reverse-Masterzone

Ein **Primärer Nameserver (SOA)** muss angegeben werden, und es muss mindestens ein Nameserver-Datensatz angegeben werden, in dem Sie auf **Hinzufügen** im Abschnitt **Nameserver** klicken.

Klicken Sie nach der Konfiguration der Reverse-Masterzone auf **OK**, um in das in Abbildung 28-1 gezeigte Hauptfenster zurückzukehren. Klicken Sie auf **Speichern** um die Konfigurationsdatei `/etc/named.conf` zu schreiben, um alle Zonendateien in das Verzeichnis `/var/named` zu schreiben und den Daemon zu veranlassen, die Konfigurationsdateien neu zu laden.

Die Konfiguration erstellt dann einen Eintrag ähnlich dem folgenden in `/etc/named.conf`:

```
zone  "10.168.192.in-addr.arpa" {
        type master;
        file  "10.168.192.in-addr.arpa.zone";
};
```

Sie erstellt weiterhin die Datei `/var/named/10.168.192.in-addr.arpa.zone` mit folgenden Informationen:

```
$TTL 86400
@       IN      SOA     ns.example.com. root.localhost (
                        2 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttk
```

```
                        )

@       IN      NS      ns2.example.com.

1       IN      PTR     one.example.com.
2       IN      PTR     two.example.com.
```

28.3. Hinzufügen einer Slave-Zone

Um eine Slave-Zone hinzuzufügen (auch bekannt als sekundärer Master), klicken Sie auf **Neu** und wählen Sie **Slave Zone**. Geben Sie den Domainnamen für die Slave-Zone in das Textfeld **Domainname** ein.

Ein neues Fenster (siehe Abbildung 28-4) mit folgenden Optionen wird angezeigt:

- **Name** — Der Domainname, der im vorigen Fenster eingegeben wurde.
- **Master-Liste** — Der Nameserver, von dem die Slave-Zone die Daten erhält. Dieser Wert muss eine gültige IP-Adresse sein. In diesem Textfeld können nur Zahlen und Punkte (.) eingegeben werden.
- **Dateiname** — Dateiname der DNS- Datenbankdatei in `/var/named`.

Abbildung 28-4. Hinzufügen einer Slave-Zone

Klicken Sie nach der Konfiguration der Slave-Zone auf **OK**, um zu dem in Abbildung 28-1 gezeigten Hauptfenster zurückzukehren. Klicken Sie auf **Speichern** um die Konfigurationsdatei `/etc/named.conf` zu schreiben und den Daemon zu veranlassen, die Konfigurationsdateien neu zu laden.

Die Konfiguration erstellt dann einen Eintrag ähnlich dem folgenden in `/etc/named.conf`:

```
zone "slave.example.com" {
        type slave;
        file "slave.example.com.zone";
        masters {
                 1.2.3.4;
                };
```

```
};
```

Die Konfigurationsdatei `/var/named/slave.example.com.zone` wird vom `named`-Dienst erstellt, wenn dieser die Zonendaten vom Master-Server herunterlädt.

Kapitel 29.
Konfiguration der Authentifizierung

Wenn sich Benutzer in einem Red Hat Enterprise Linux-System anmelden, müssen der Benutzername und das Passwort und somit der Benutzer als gültig und aktiv überprüft oder *authentifiziert* werden. In manchen Fällen befindet sich die Informationen für den Benutzer auf dem lokalen System, in anderen Fällen verweist das System die Authentifizierung an eine Benutzer-Datenbank auf einem Remote-System.

Das **Authentication Configuration Tool** bietet eine grafische Oberfläche für die Konfiguration von NIS, LDAP und Hesiod für das abrufen von Benutzerinformationen sowie das Konfigurieren von LDAP, Kerberos und SMB als Authentifizierungsprotokolle.

Anmerkung

Wenn Sie mit dem **Security Level Configuration Tool** einen mittleren oder hohen Sicherheitslevel konfiguriert haben, sind Netzwerkauthentifizierungs-Methoden inklusive NIS und LDAP durch die Firewall nicht gestattet.

In diesem Kapitel werden die verschiedenen Authentifizierungstypen nicht im Detail erklärt. Stattdessen wird beschrieben, wie Sie das **Authentication Configuration Tool** für die Konfiguration dieser einsetzen können.

Um die grafische Version des **Authentication Configuration Tool** vom Desktop aus zu starten, wählen Sie **Hauptmenü** (im Panel) => **Systemeinstellungen** => **Authentifizierung** oder geben Sie den Befehl `authconfig-gtk` an einem Shell-Prompt (z.B. in **XTerm** oder **GNOME terminal**) ein. Um die textbasierte Version zu starten, geben Sie den Befehl `authconfig` an einem Shell-Prompt ein..

Wichtig

Die Änderungen werden sofort nach dem Beenden des Authentifizierungsprogramms wirksam.

29.1. Benutzer-Informationen

Der Tab **Benutzer-Informationen** hat mehrere Optionen. Um eine Option zu aktivieren, klicken Sie auf das Kontrollkästchen neben der Option. Um eine Option zu deaktivieren, klicken Sie auf das Kästchen, um die Markierung aufzuheben. Klicken Sie auf **OK**, um das Programm zu beenden und die Änderungen anzuwenden.

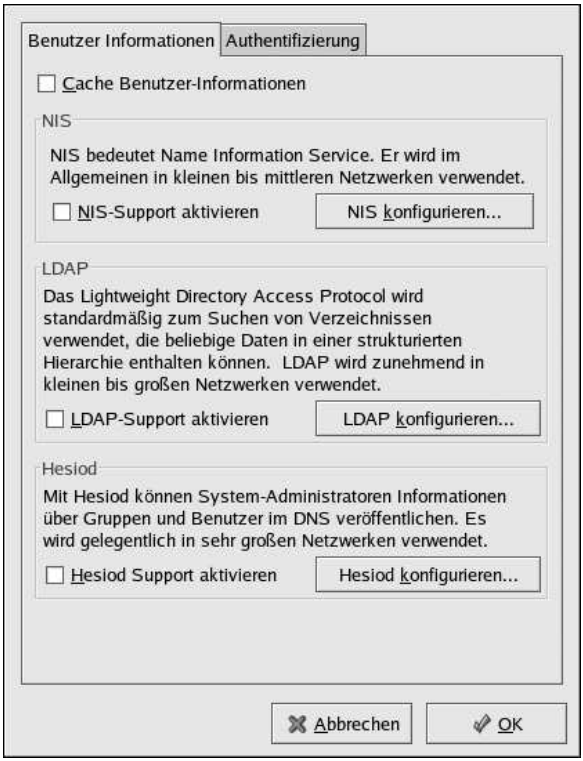

Abbildung 29-1. Benutzer-Informationen

In der folgenden Liste wird erklärt, was welche Option konfiguriert:

- **Cache Benutzer-Informationen** — Wählen Sie diese Option, um den Name Service Cache Daemon zu aktivieren (`nscd`) und diesen zum Starten beim Booten zu konfigurieren.

  Das `nscd`-Paket muss für diese Option installiert sein.

- **NIS-Support aktivieren** — Wählen Sie diese Option zum Konfigurieren des Systems als NIS Client, der sich mit einem NIS Server für Benutzer- und Passwort-Authentifizierung verbindet. Klicken Sie auf den Button **NIS konfigurieren**, um die NIS Domain und den NIS Server anzugeben. Wird kein NIS Server angegeben, versucht der Daemon, diesen über Broadcast zu finden.

  Das `ypbind`-Paket muss für diese Option installiert sein. Ist der NIS-Support aktiviert, werden die Services `portmap` und `ypbind` gestartet und werden außerdem beim Booten gestartet.

- **LDAP Support aktivieren** — Wählen Sie diese Option, um das System für das Abrufen von Benutzer-Informationen über LDAP zu konfigurieren. Klicken Sie auf **LDAP konfigurieren**, um **LDAP Search Base DN** und **LDAP Server** einzustellen. Wenn **Verbindungen mit TLS verschlüsseln** ausgewählt wird, werden Passwörter, die an den LDAP Server gesendet wurden, mittels Transport Layer Security verschlüsselt.

  Das `openldap-clients`-Paket muss für diese Option installiert sein.

  Weitere Informationen zu LDAP finden Sie im *Red Hat Enterprise Linux Referenzhandbuch*.

- **Hesiod-Support aktivieren** — Wählen Sie diese Option, um das System für das Abrufen von Informationen, einschließlich Benutzer-Informationen von einer Remote-Hesiod-Datenbank zu konfigurieren.

  Das `hesiod`-Paket muss installiert sein.

29.2. Authentifizierung

Der Tab **Authentifizierung** ermöglicht die Konfiguration von Netzwerk-Authentifizierungsmethoden. Um eine Option zu aktivieren, klicken Sie auf das leere Kästchen daneben. Um eine Option zu deaktivieren, klicken Sie auf das Kästchen um die Markierung aufzuheben.

Abbildung 29-2. Authentifizierung

Im folgenden wird erklärt, was durch welche Option konfiguriert wird:

- **Shadow-Passwörter verwenden** — Wählen Sie diese Option, um Passwörter im Shadow-Passwortformat in der Datei `/etc/shadow` anstelle von `/etc/passwd` zu speichern. Shadow-Passwörter werden standardmäßig während der Installation aktiviert, und werden dringend empfohlen, um die Sicherheit des Systems zu erhöhen.

Das Paket `shadow-utils` muss für diese Option installiert sein. Weitere Informationen über Shadow-Passwörter finden Sie im Kapitel *Benutzer und Gruppen* im *Red Hat Enterprise Linux Referenzhandbuch*.

- **MD5-Passwörter verwenden** — Wählen Sie diese Option, um MD5-Passwörter zu aktivieren, wodurch Passwörter bis zu 256 Zeichen anstelle von 8 oder weniger Zeichen lang sein können. Dies wird standardmäßig bei der Installation ausgewählt und ist für erhöhte Sicherheit empfohlen.
- **LDAP-Support aktivieren** — Wählen Sie diese Option, wenn Standard-PAM-fähige Applikationen LDAP für die Authentifizierung verwenden sollen. Klicken Sie auf **LDAP konfigurieren**, um folgendes anzugeben:
  - **Verbindungen mit TLS verschlüsseln** — Verwendet Transport Layer Security um an den LDAP-Server gesendete Passwörter zu verschlüsseln.
  - **LDAP Search Base DN** — Ruft Benutzer-Information durch ihren Distinguished Name (DN) ab.
  - **LDAP-Server** — Gibt die IP-Adresse des LDAP-Servers an.

  Das `openldap-clients`-Paket muss für diese Option installiert sein. Weitere Informationen zu LDAP finden Sie im *Red Hat Enterprise Linux Referenzhandbuch*.
- **Kerberos-Support aktivieren** — Wählen Sie diese Option, um die Kerberos-Authentifizierung zu aktivieren. Klicken Sie auf den Button **Kerberos konfigurieren** um folgendes zu konfigurieren:
  - **Realm** — Konfiguriert den Realm für den Kerberos-Server. Realm ist das Netzwerk, das Kerberos verwendet, und besteht aus einem oder mehreren KDCs und einer großen Anzahl Clients.
  - **KDC** — Definiert den Key Distribution Center (KDC), den Server, der Kerberos Tickets ausgibt.
  - **Admin-Server** — Gibt die Administrations-Server an, die `kadmind` ausführen.

  Die Pakete `krb5-libs` und `krb5-workstation` müssen für diese Option installiert sein. Weitere Informationen zu Kerberos finden Sie im *Red Hat Enterprise Linux Referenzhandbuch*.
- **SMB-Support aktivieren** — Diese Option konfiguriert PAM zur Verwendung eines SMB-Servers, um Benutzer zu authentifizieren. Klicken Sie auf **SMB konfigurieren** um folgendes anzugeben:
  - **Arbeitsgruppe** — Gibt die SMB-Arbeitsgruppe an.
  - **Domain Controller** — Gibt die SMB-Domain Controller an.

29.3. Befehlszeilen-Version

Das **Authentication Configuration Tool** kann auch als Befehlszeilentool ohne grafische Schnittstelle ausgeführt werden. Die Befehlszeilen-Version kann in einem Konfigurationsskript oder in einem Kickstartskript verwendet werden. Die Optionen zur Authentifizierung werden unter Tabelle 29-1 beschrieben.

Option	Beschreibung
`--enableshadow`	Shadow-Passwörter aktivieren
`--disableshadow`	Shadow-Passwörter deaktivieren
`--enablemd5`	MD5-Passwörter aktivieren
`--disablemd5`	MD5-Passwörter deaktivieren
`--enablenis`	NIS aktivieren

Option	Beschreibung
`--disablenis`	NIS deaktivieren
`--nisdomain=<`*`domain`*`>`	NIS-Domain angeben
`--nisserver=<`*`server`*`>`	NIS-Server angeben
`--enableldap`	LDAP für Benutzer-Informationen aktivieren
`--disableldap`	LDAP für Benutzer-Informationen deaktivieren
`--enableldaptls`	TLS mit LDAP aktivieren
`--disableldaptls`	TLS mit LDAP deaktivieren
`--enableldapauth`	LDAP für Authentifizierung aktivieren
`--disableldapauth`	LDAP für Authentifizierung deaktivieren
`--ldapserver=<`*`server`*`>`	LDAP-Server angeben
`--ldapbasedn=<`*`dn`*`>`	LDAP base DN angeben
`--enablekrb5`	Kerberos aktivieren
`--disablekrb5`	Kerberos deaktivieren
`--krb5kdc=<`*`kdc`*`>`	Kerberos KDC angeben
`--krb5adminserver=<`*`server`*`>`	Kerberos Administrations-Server angeben
`--krb5realm=<`*`realm`*`>`	Kerberos Realm angeben
`--enablesmbauth`	SMB aktivieren
`--disablesmbauth`	SMB deaktivieren
`--smbworkgroup=<`*`workgroup`*`>`	SMB Arbeitsgrupp angeben
`--smbservers=<`*`server`*`>`	SMB Server angeben
`--enablehesiod`	Hesiod aktivieren
`--disablehesiod`	Hesiod deaktivieren
`--hesiodlhs=<`*`lhs`*`>`	Hesiod LHS angeben
`--hesiodrhs=<`*`rhs`*`>`	Hesiod RHS angeben
`--enablecache`	`nscd` aktivieren
`--disablecache`	`nscd` deaktivieren
`--nostart`	Die Services `portmap`, `ypbind` oder `nscd` nicht starten oder stoppen, auch wenn sie konfiguriert sind
`--kickstart`	Benutzerschnittstelle nicht anzeigen
`--probe`	Netzwerk-Standards testen und anzeigen

Tabelle 29-1. Befehlszeilen-Optionen

Tipp

Diese Optionen finden Sie auch auf der `authconfig` man-Seite, oder indem Sie `authconfig --help` an einem Shell-Prompt eingeben.

V. System-Konfiguration

Teil der Aufgaben eines System-Administrators ist die Konfiguration des Systems für verschiedene Aufgaben, Typen von Benutzern und Hardware-Konfigurationen. Dieser Abschnitt beschreibt die Konfiguration eines Red Hat Enterprise Linux Systems.

Inhaltsverzeichnis

redhat.

Kapitel 30.

Konsolenzugriff

Wenn sich normale Benutzer (keine root-Accounts) an einem Computer lokal anmelden, verfügen sie über zwei Arten von Sonderberechtigungen:

1. Sie können bestimmte Programme ausführen, die sie andernfalls nicht ausführen könnten.
2. Sie können auf bestimmte Dateien zugreifen (in der Regel besondere Gerätedateien, die zum Zugreifen auf Disketten, CD-ROMs, usw. verwendet werden), auf die sie andernfalls nicht zugreifen könnten.

Da auf einem einzelnen Computer mehrere Konsolen vorhanden sind und sich mehrere Benutzer gleichzeitig lokal am Computer anmelden können, muss einer der Benutzer das Rennen um den Dateuzugang "gewinnen". Der Benutzer, der sich zuerst an der Konsole anmeldet, besitzt diese Dateien. Meldet sich der erste Benutzer ab, wird der nächste Benutzer, der sich anmeldet, zum Besitzer der Dateien.

Allerdings kann *jeder* an der Konsole angemeldete Benutzer Programme ausführen, die in der Regel nur von unter einem root-Account angemeldeten Benutzern ausgeführt werden dürfen. Wird X ausgeführt, können diese Aktionen als Menüelemente in eine grafische Benutzerschnittstelle aufgenommen werden. Bei Lieferung enthalten die Programme mit Konsolenzugriff `halt`, `poweroff` und `reboot`.

30.1. Shutdown deaktivieren über [Strg]-[Alt]-[Ent]

Standardmäßig gibt `/etc/inittab` an, dass das System als Antwort auf die Tastenkombination [Strg]-[Alt]-[Ent] an der Konsole heruntergefahren und erneut gestartet wird. Wenn Sie diese Funktion vollständig deaktivieren möchten, müssen Sie in `/etc/inittab` folgende Zeile auskommentieren, indem Sie ein Nummernzeichen (`#`) vor die Zeile setzen:

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

Möglicherweise möchten Sie zulassen, dass bestimmte Benutzer, die nicht unter einem root-Account angemeldet sind, das System von der Konsole mit Hilfe von [Strg]-[Alt]-[Ent] herunterfahren können. Mithilfe folgender Schritte können Sie dieses Recht auf bestimmte Benutzer einschränken:

1. Fügen Sie die Option `-a` zur oben genannten Zeile `/etc/inittab` hinzu, so dass Folgendes gelesen wird:
   ```
   ca::ctrlaltdel:/sbin/shutdown -a -t3 -r now
   ```
   Das Flag `-a` weist `shutdown` an, die Datei `/etc/shutdown.allow` zu suchen, die Sie im nächsten Schritt erstellen.
2. Erstellen Sie in `/etc` eine Datei `shutdown.allow`. Die Datei `shutdown.allow` führt die Benutzernamen aller Benutzer auf, die zum Herunterfahren des Systems mit Hilfe von [Strg]-[Alt]-[Ent] berechtigt sind. Das Format der Datei `/etc/shutdown.allow` ist eine Liste mit Benutzernamen, wobei ein Name pro Zeile genannt wird. Es folgt ein Beispiel:
   ```
   stephen
   jack
   sophie
   ```

In dieser Beispieldatei `shutdown.allow` sind Stephen, Jack und Sophie dazu berechtigt, das System von der Konsole mit Hilfe von [Strg]-[Alt]-[Ent] herunterzufahren. Wird diese Tastenkombination verwendet, überprüft `shutdown -a` in `/etc/inittab`, ob ein in `/etc/shutdown.allow` genannter Benutzer (oder root-Account) an einer virtuellen Konsole angemeldet ist. Ist einer dieser Benutzer

angemeldet, wird das System heruntergefahren. Ist keiner angemeldet, wird stattdessen eine Fehlermeldung in die Systemkonsole geschrieben.

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

30.2. Deaktivieren des Zugriffs auf das Konsolenprogramm

Um den Benutzerzugriff auf Konsolenprogramme zu deaktivieren, müssen Sie diesen Befehl als root-Benutzer ausführen:

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

In Umgebungen mit auf andere Art und Weise gesicherten Konsolen (festgelegte BIOS- und Bootloader-Passwörter, [Strg]-[Alt]-[Ent], Power- und Resetschalter, usw. sind deaktiviert) möchten Sie möglicherweise allen Benutzern das Ausführen der Befehle `poweroff`, `halt` und `reboot` verweigern, auf die von der Konsole standardmäßig zugegriffen werden kann.

Melden Sie sich unter einem root-Account an und führen Sie folgende Befehle aus, um diese Funktionen zu entfernen:

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

30.3. Deaktivieren aller Konsolenzugriffe

Mit Hilfe des PAM-Moduls `pam_console.so` werden die Dateiberechtigungen und Authentifizierung der Konsole verwaltet. (Weitere Informationen zum Konfigurieren von PAM finden Sie im *Red Hat Enterprise Linux Referenzhandbuch*). Möchten Sie den Konsolenzugriff generell einschließlich Programm- und Dateizugriff verweigern, müssen Sie alle Zeilen auskommentieren, die im Verzeichnis `/etc/pam.d` auf `pam_console.so` verweisen. Melden Sie sich hierfür unter einem root-Account an und führen Sie folgendes Skript aus:

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

30.4. Definieren des Konsolenzugriffs

Das Modul `pam_console.so` verwendet die Datei `/etc/security/console.perms` zum Festlegen der Benutzerberechtigungen für die Systemkonsole. Die Dateisyntax ist sehr flexibel. Sie können die Datei so bearbeiten, dass diese Anweisungen nicht mehr angewendet werden. Die Standarddatei verfügt über folgende Zeile:

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

Wenn sich ein Benutzer anmeldet, wird er zu einem Terminal hinzugefügt. Dabei handelt es sich entweder um einen X-Server mit einem Namen wie `:0` oder `mymachine.example.com:1.0` oder um ein Gerät wie `/dev/ttyS0` oder `/dev/pts/2`. Standardmäßig sollten die lokalen virtuellen Konsolen und lokalen X-Server als lokal definiert werden. Wenn Sie allerdings das serielle Terminal an Port `/dev/ttyS1` ebenfalls als lokal festlegen möchten, können Sie die Zeile folgendermaßen ändern:

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

30.5. Dateizugriff von der Konsole

In `/etc/security/console.perms` ist ein Abschnitt vorhanden, der zum Beispiel folgende Zeilen enthält:

```
<floppy>=/dev/fd[0-1]* \
         /dev/floppy/* /mnt/floppy*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
        /dev/mixer* /dev/sequencer \
        /dev/sound/* /dev/beep
<cdrom>=/dev/cdrom* /dev/cdroms/* /dev/cdwriter* /mnt/cdrom*
```

Bei Bedarf können Sie eigene Zeilen zu diesem Abschnitt hinzufügen. Stellen Sie sicher, dass alle hinzugefügten Zeilen auf das entsprechende Gerät verweisen. Sie können zum Beispiel folgende Zeile hinzufügen:

```
<scanner>=/dev/scanner /dev/usb/scanner*
```

(Stellen Sie auf jeden Fall sicher, dass `/dev/sga` tatsächlich Ihrem Scanner und nicht zum Beispiel der Festplatte entspricht.)

Dies ist der erste Schritt. Im zweiten Schritt müssen Sie nun definieren, was mit diesen Dateien geschehen soll. Suchen Sie im letzten Abschnitt von `/etc/security/console.perms` nach folgenden oder so ähnlichen Zeilen:

```
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound>  0640 root
<console> 0600 <cdrom>  0600 root.disk
```

Fügen Sie zum Beispiel folgende Zeile hinzu:

```
<console> 0600 <scanner> 0600 root
```

Wenn Sie sich dann an der Konsole anmelden, sind Sie der Besitzer des Geräts `/dev/scanner`. Die Berechtigung lautet 0600 (exklusiver Lese-/Schreibzugriff). Wenn Sie sich abmelden, geht das Gerät in das Eigentum des root-Accounts über. Die Berechtigung lautet auch weiterhin 0600 (nun: exklusiver Lese-/Schreibzugriff für den root-Account).

30.6. Aktivieren des Konsolenzugriffs für andere Anwendungen

Wenn Sie Konsolenbenutzern den Zugriff auf weitere Applikationen gewähren möchten, müssen Sie mehrere Schritte ausführen.

Der Konsolenzugriff funktioniert *nur* bei Applikationen, die sich in `/sbin/` oder `/usr/sbin/` befinden. Das heißt, die auszuführende Applikation muss dort gespeichert sein. Führen Sie folgende Schritte aus, nachdem Sie dies überprüft haben:

1. Erstellen Sie eine Verknüpfung von dem Applikationsnamen wie zum Beispiel dem Beispielprogramm *foo* mit der Applikation `/usr/bin/consolehelper`:
   ```
   cd /usr/bin
   ln -s consolehelper foo
   ```
2. Erstellen Sie die Datei `/etc/security/console.apps/`*foo*:
   ```
   touch /etc/security/console.apps/foo
   ```
3. Erstellen Sie eine PAM-Konfigurationsdatei in `/etc/pam.d/` für den Dienst *foo*. Am besten erstellen Sie hierfür eine Kopie der PAM-Konfigurationsdatei des halt-Dienstes und ändern dann die Datei, deren Verhalten Sie ändern möchten:

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

Wenn Sie nun den Befehl `/usr/bin/`*`foo`* ausführen, wird `consolehelper` aufgerufen, der den Benutzer mithilfe von `/usr/sbin/userhelper` authentifiziert. Ist `/etc/pam.d/`*`foo`* eine Kopie von `/etc/pam.d/halt`, fordert `consolehelper` zum Authentifizieren des Benutzers das Passwort des Benutzers an (andernfalls wird genau das ausgeführt, was in `/etc/pam.d/`*`foo`* angegeben ist). Anschließend wird `/usr/sbin/`*`foo`* mit root-Account-Berechtigungen ausgeführt.

In der PAM-Konfigurationsdatei können Sie festlegen, dass eine Anwendung das *pam_timestamp*-Modul zum Zwischenspeichern einer erfolgreichen Authentifizierung verwendet. Wenn eine Anwendung gestartet und die richtige Authentifizierung zur Verfügung gestellt wird (das root-Passwort), wird eine Timestampdatei erstellt. Eine erfolgreiche Authentifizierung wird standardmäßig fünf Minuten lang zwischengespeichert. Während dieser Zeit wird jede weitere Anwendung, die `pam_timestamp` verwendet und von derselben Sitzung ausgeführt wird, für den Benutzer automatisch authentifiziert — Der Benutzer muss das root-Passwort nicht erneut eingeben.

Dieses Modul ist im `pam`-Paket enthalten. Die PAM- Konfigurationsdatei in `etc/pam.d/` muss zum Aktivieren dieser Funktion folgende Zeilen enthalten:

```
auth sufficient /lib/security/pam_timestamp.so
session optional /lib/security/pam_timestamp.so
```

Die erste Zeile, die mit `auth` beginnt, sollte hinter allen anderen Zeilen mit `auth sufficient` stehen. Die Zeile, die mit `session` beginnt, sollte allen anderen `session optional`-Zeilen folgen.

Wenn eine Anwendung, die für die Verwendung von `pam_timestamp` konfiguriert wurde, erfolgreich im **Hauptmenü** (im Panel) authentifiziert, wird das Symbol  im Benachrichtigungsbereich des Panels angezeigt, wenn Sie sich in der GNOME- oder KDE-Desktopumgebung befinden. Nach Ablauf der Authentifizierung (der Standard sind fünf Minuten) wird das Symbol ausgeblendet.

Der Benutzer kann auswählen, dass die zwischengespeicherte Authentifizierung gelöscht wird, indem er auf das Symbol klickt und die Option zum Löschen der Authentifizierungsinformationen auswählt.

30.7. Die `floppy`-Gruppe

Wenn Sie aus einem bestimmten Grund Benutzern, die nicht unter root-Accounts angemeldet sind, Zugriff auf das Diskettenlaufwerk gewähren müssen, können Sie dies mithilfe der `floppy`-Gruppe ausführen. Fügen Sie einfach den oder die Benutzer mit Hilfe eines Tools Ihrer Wahl zur `floppy`-Gruppe hinzu. Im Folgenden wird ein Beispiel gegeben, wie der Benutzer Fred zur `floppy`-Gruppe mithilfe von `gpasswd` hinzugefügt wird:

```
gpasswd -a fred floppy
```

Nun kann der Benutzer Fred auf das Diskettenlaufwerk des Systems von der Konsole aus zugreifen.

Kapitel 31.
Datums- und Zeitkonfiguration

Mit dem **Time and Date Properties Tool** können Benutzer die Systemzeit und das -datum ändern, die vom System verwendete Zeitzone konfigurieren und den Network Time Protocol (NTP) Daemon für die Synchronisierung der Systemuhr mit dem Time Server einstellen.

Das X Window System muss laufen, und Sie müssen über Root-Berechtigungen verfügen. Um die Applikation vom Desktop aus zu starten, wählen Sie **Hauptmenü => Systemeinstellungen => Datum & Uhrzeit** oder geben Sie den Befehl `redhat-config-date` an einem Shell-Prompt (zum Beispiel an einem XTerm oder GNOME Terminal) ein.

31.1. Zeit- und Datumseigenschaften

Wie in Abbildung 31-1 gezeigt, ist das erste Fenster das zum Konfigurieren des Systemdatums, der -zeit und des NTP Daemons (`ntpd`).

Abbildung 31-1. Zeit- und Datumseigenschaften

Um das Datum zu ändern, verwenden Sie die Pfeile links und rechts neben dem Monat, um den Monat zu ändern. Mit den Pfeilen links und rechts neben dem Jahr, um das Jahr zu ändern. Klicken Sie auf den Wochentag, um diesen zu ändern. Änderungen werden erst wirksam, wenn Sie auf **OK** klicken.

Um die Zeit zu ändern, verwenden Sie die Pfeile neben der **Stunde**, **Minute** und **Sekunde** im Abschnitt **Zeit** Änderungen werden erst wirksam, wenn Sie auf **OK** klicken.

Der Network Time Protocol (NTP) Daemon synchronisiert die Systemuhr über einen Remote Time Server oder eine Zeitquelle (wie zum Beispiel ein Satellit). Mit dieser Applikation können Sie einen NTP-Server konfigurieren, so dass dieser die Systemuhr über einen Remote Server synchronisiert. Um dieses Feature zu aktivieren, klicken Sie auf **Netzwerk-Zeitprotokoll aktivieren**. Dies aktiviert das Pull-Down-Menü **Server**. Sie können einen der vordefinierten Server auswählen oder einen Servernamen eingeben. Das System synchronisiert erst mit dem NTP-Server, wenn Sie **OK** klicken. Nachdem Sie auf **OK** geklickt haben, wird die Konfiguration gespeichert und der NTP-Daemon gestartet (oder neu gestartet, wenn dieser bereits läuft).

Das Klicken auf **OK** wendet jegliche Änderungen, die Sie an der Uhrzeit, dem Datum, den NTP-Einstellungen und den Zeitzoneneinstellungen vorgenommen haben, an und beendet das Programm.

31.2. Konfiguration der Zeitzone

Um die System-Zeitzone zu konfigurieren, klicken Sie auf den Tab **Zeitzone**. Die Zeitzone kann entweder durch die interaktive Landkarte oder durch Auswahl der gewünschten Zeitzone aus der Liste unterhalb der Karte geändert werden. Um die Landkarte zu verwenden, klicken Sie auf die Stadt, die die gewünschte Zeitzone repräsentiert. Es erscheint ein rotes **X**, und die Zeitzonen-Auswahl ändert sich in der Liste unterhalb der Landkarte. Klicken Sie auf **OK**, um die Änderungen anzunehmen und das Programm zu beenden.

Abbildung 31-2. Zeitzonen-Eigenschaften

Ist Ihre Systemuhr auf UTC eingestellt, wählen Sie die Option **Systemuhr verwendet UTC**. UTC steht für Universelle Zeitzone, auch als Greenwich Mean Time (GMT) bekannt. Andere Zeitzonen werden durch Addieren oder Subtrahieren von der UTC-Zeit bestimmt.

Kapitel 32.

Konfiguration der Tastatur

Das Installationsprogramm erlaubt es Benutzern das Tastaturlayout für Ihr System einzustellen. Um das Tastaturlayout nach der Installation zu ändern, benutzen Sie **Keyboard Configuration Tool**.

Um **Keyboard Configuration Tool** zu starten, wählen Sie den **Hauptmenü**-Button (auf dem Panel) => **Systemeinstellungen** => **Tastatur**, oder geben Sie `redhat-config-keyboard` an einem Shell-Prompt ein.

Abbildung 32-1. Keyboard Configuration Tool

Wählen Sie ein Tastaturlayout aus der Liste (zum Beispiel, **U.S. English**) und klicken **OK**. Damit die Änderungen in Kraft treten, sollten Sie sich aus der grafischen Oberfläche aus- und wieder einloggen.

Kapitel 33.

Konfigurieren der Maus

Das Installationsprogramm ermöglicht Benutzern, den Typ der mit dem System verbundenen Maus auszuwählen. Um einen anderen Maustyp für das System zu konfigurieren, verwenden Sie das **Mouse Configuration Tool**.

Um das **Mouse Configuration Tool** zu starten, wählen Sie **Hauptmenü** (im Panel) => **Systemeinstellungen** => **Maus** oder geben Sie den Befehl `redhat-config-mouse` an einem Shell-Prompt ein (z.B. in einem XTerm oder GNOME Terminal). Wird das X Window System inicht ausgeführt, wird die text-basierte Version des Tools gestartet.

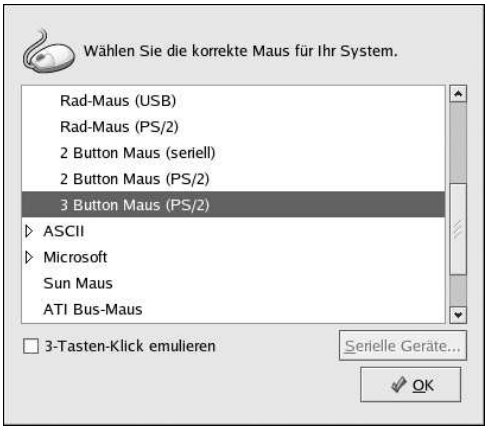

Abbildung 33-1. Maus auswählen

Wählen Sie jetzt den Maustyp für Ihr System aus. Wenn Sie keine genaue Übereinstimmung finden, wählen Sie einen Maustyp aus, bei dem Sie sicher sind, dass er mit Ihrem System kompatibel ist.

Ein eingebautes Zeigegerät, wie zum Beispiel ein Touchpad bei einem Laptop, ist meistens PS/2-kompatibel.

Alle Maustypen werden durch entweder **PS/2**, **seriell** oder **USB** in Klammern ergänzt. Dies gibt den Mausport an.

Ein PS/2 Maus-Port sieht wie folgt aus  .

Ein serieller Maus-Port sieht wie folgt aus  .

Ein USB Maus-Port sieht wie folgt aus  .

Wenn Ihr Mausmodell nicht aufgeführt ist, wählen Sie einen der **generischen** Einträge. Stützen Sie Ihre Auswahl hierbei auf die Anzahl der Maustasten und die Mausschnittstelle.

Tipp

Wenn Sie eine Scroll-Maus haben, wählen Sie den Eintrag **Generisch - Rad-Maus** (mit dem entsprechenden Maus-Port).

Die Scroll-Taste auf einer Rad-Maus kann als mittlere Maustaste für das Einfügen und Ausschneiden von text und andere Funktionen dieser Taste verwendet werden. Hat Ihre Maus nur zwei Tasten, wählen Sie **3-Tasten emulieren**, um diese als 3-Tasten Maus einzurichten. Wird diese Option aktiviert, wird durch das Drücken beider Maustasten gleichzeitig eine dritte Maustaste emuliert.

Wird eine serielle Maus ausgewählt, klicken Sie auf **Serielle Geräte**, um die richtige Nummer des seriellen Geräts, wie z.B. `/dev/ttyS0` für die Maus zu konfigurieren.

Klicken Sie auf **OK**, um den neuen Maustyp zu speichern. Die Auswahl wird in die Datei `/etc/sysconfig/mouse` geschrieben, und der Konsolen-Mausservice `gpm` neu gestartet. Die Änderungen werden auch in die X Window System Konfigurationsdatei `/etc/X11/XF86Config` geschrieben; die Änderung des Maustyps wird jedoch nicht automatisch auf die aktuelle X Sitzung angewendet. Um den neuen Maustyp zu aktivieren, melden Sie sich am grafischen Desktop ab und wieder an.

Tipp

Um die Anordnung der Tasten für Linkshänder anzupassen, klicken Sie auf **Hauptmenü** (im Panel) => **Präferenzen** => **Maus**, und wählen Sie **Mit links bediente Maus**.

Kapitel 34.

X Window System Konfiguration

Während der Installation werden der Monitor, die Garfikkarte und die Anzeige-Einstellungen des Systems konfigurier. Um diese Einstellungen zu ändern, verwenden Sie das **X Configuration Tool**.

Um das **X Configuration Tool** zu starten, wählen Sie **Hauptmenü** (im Panel) => **Systemeinstellungen** => **Anzeige** oder geben Sie den Befehl `redhat-config-xfree86` an einem Shell-Prompt (z.B. ein XTerm oder GNOME Terminal) ein. Läuft das X Window System nicht, wird eine kleine Version von X gestartet, die das Programm ausführt.

Nachdem Sie die Einstellungen geändert haben, melden Sie sich am grafischen Desktop ab und wieder an, damit die Änderungen wirksam werden.

34.1. Anzeige-Einstellungen

Das Tab **Anzeige** ermöglicht es Benutzern, die *Auflösung* und *Farbtiefe* zu ändern. Die Bildschirmanzeige besteht aus kleinen Punkten, die *Pixel* genannt werden. Die Anzahl der Pixel, die zur gleichen Zeit angezeigt werden können, wird als Auflösung bezeichnet. So bedeutet eine Auflösung von 1024x768, dass 1024 horizontale Pixel und 768 vertikale Pixel verwendet werden. Je höher die Auflösung, desto mehr Bilder kann der Monitor anzeigen. Je höher z.B. die Auflösung, desto kleiner erscheinen die Desktopsymbole und je mehr Symbole werden benötigt, um den Bildschirm zu füllen.

Die Farbtiefe gibt an, wieviele mögliche Farben angezeigt werden können. Je höher die Farbtiefe, desto besser der Kontrast zwischen den Farben.

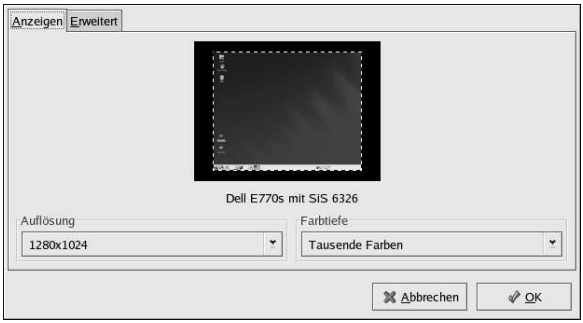

Abbildung 34-1. Anzeige-Einstellungen

34.2. Erweiterte Einstellungen

Wenn die Applikation gestartet wird, testet diese den Monitor und die Grafikkarte. Wird die Hardware ordnungsgemäß getestet, werden die Informationen hierzu im Tab **Erweitert** wie unter Abbildung 34-2 gezeigt abgebildet.

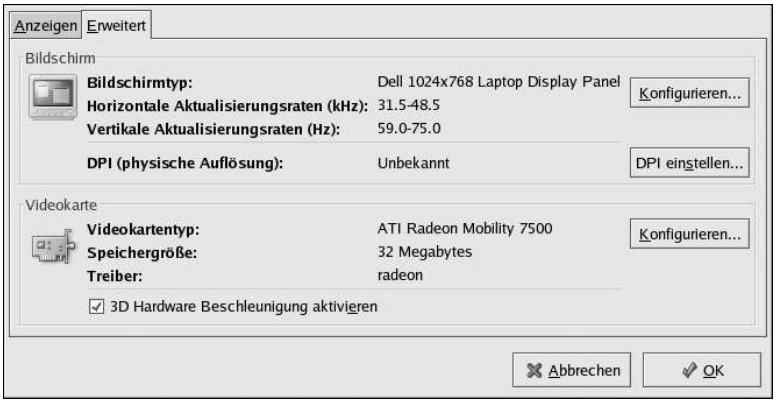

Abbildung 34-2. Erweiterte Einstellungen

Um den Monitortyp oder dessen Einstellungen zu ändern, klicken Sie auf dieSchaltfläche **Konfigurieren**. Um den Grafikkartentyp oder dessen Einstellungen zu ändern, klicken Sie auf dieSchaltfläche **Konfigurieren** neben den Einstellungen.

Kapitel 35.

Benutzer- und Gruppenkonfiguration

Mit dem **User Manager** können Sie lokale Benutzer und Gruppen anzeigen, ändern, hinzufügen und löschen.

Um den **User Manager** verwenden zu können, müssen Sie sich im X Window System befinden, das RPM-Paket `redhat-config-users` installiert haben und über root-Berechtigungen verfügen. Um den **User Manager** vom Desktop aus zu starten, gehen Sie zu **Hauptmenü** (im Panel) **=> Systemeinstellungen => Benutzer & Gruppen**. Oder geben Sie den Befehl `redhat-config-users` an einem Shell-Prompt ein (z.B. in einem XTerm oder einem GNOME Terminal).

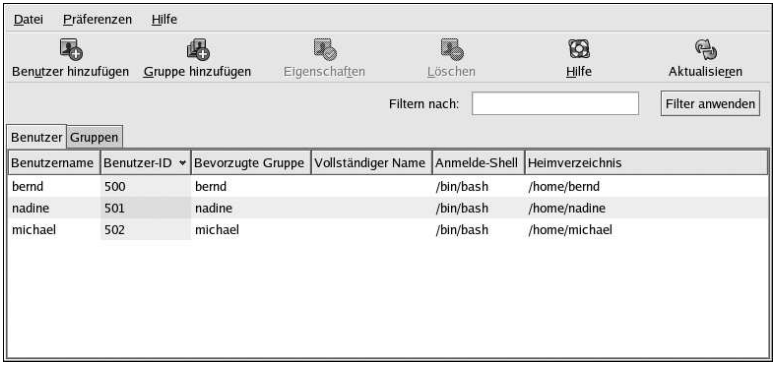

Abbildung 35-1. User Manager

Um eine Liste aller lokalen Benutzer anzuzeigen, klicken Sie auf **Benutzer**. Um eine Liste aller lokaler Gruppen auf dem System anzuzeigen, klicken Sie auf **Gruppen**.

Wenn Sie einen bestimmten Benutzer oder eine bestimmte Gruppe suchen, geben Sie die ersten Buchstaben des Namens in das Feld **Filtern nach** ein und drücken Sie die [Enter-Taste] oder klicken Sie auf den Button **Filter anwenden**. Daraufhin wird die gefilterte Liste angezeigt.

Zum Sortieren der Benutzer oder Gruppen klicken Sie auf den Namen der Spalte. Die Benutzer oder Gruppen werden auf diese Weise nach dem Wert der Spalte sortiert.

Red Hat Enterprise Linux reserviert die ersten 500 IDs für Systembenutzer. Standardmäßig zeigt das **User Manager** keine Systembenutzer an. Um alle Benutzer einschließlich der Systembenutzer anzuzeigen, wählen Sie im Menü **Präferenzen => Filter Systembenutzer und Gruppen** ab.

35.1. Hinzufügen eines neuen Benutzers

Um einen neuen Benutzer hinzuzufügen, klicken Sie auf den Button **Benutzer hinzufügen**. Es erscheint ein Fenster, wie in Abbildung 35-2 gezeigt wird. Geben Sie den Benutzernamen sowie den vollständigen Namen des neuen Benutzers in das entsprechende Feld und das Benutzerpasswort in das Feld **Passwort** ein und bestätigen Sie es im Feld **Passwort bestätigen**. Das Passwort muss aus mindestens sechs Zeichen bestehen.

Tipp

Je länger das Benutzerpasswort ist, desto schwieriger ist es von anderen zu erraten und sich unerlaubt in einen Benutzeraccount anzumelden. Das Passwort sollte kein Wort sein, sondern aus einer Kombination von Buchstaben, Zahlen und Sonderzeichen bestehen.

Wählen Sie eine Login-Shell. Wenn Sie sich nicht sicher sind, welche Shell Sie wählen sollen, übernehmen Sie den Standardwert `/bin/bash`. Das Standard Home-Verzeichnis ist `/home/`*`Benutzername`*. Sie können das Home-Verzeichnis, das für den Benutzer erstellt wurde, ändern. Sie können sich auch dafür entscheiden, kein Home-Verzeichnis zu erstellen, indem Sie **Hauptverzeichnis erstellen** deaktivieren.

Wenn Sie das Home-Verzeichnis erstellen möchten, werden Standard-Konfigurationsdateien vom Verzeichnis `/etc/skel` in das neue Home-Verzeichnis kopiert.

Red Hat Enterprise Linux verwendet ein *user private group* (UPG) (de: Private Benutzergruppen) Schema. Dieses Schema ändert nichts an der Art, wie UNIX mit Gruppen umgeht, sondern bietet einfach nur neue Konventionen. Sobald Sie einen neuen Benutzer erstellen, wird standardmäßig auch eine Gruppe mit dem gleichen Namen erstellt, den der Benutzer verwendet. Wenn Sie diese Gruppe nicht erstellen möchten, deaktivieren Sie **Eine private Gruppe für diesen Benutzer erstellen**.

Um für einen Benutzer eine Benutzer ID festzulegen, wählen Sie **Benutzer-ID manuell festlegen**. Falls diese Option nicht gewählt wird, wird die nächstmögliche Nummer, bei 500 beginnend, an den neuen Benutzer vergeben. Red Hat Enterprise Linux reserviert die ersten 500 Benutzer IDs für Systembenutzer.

Klicken Sie auf **OK**, um den Benutzer zu erstellen.

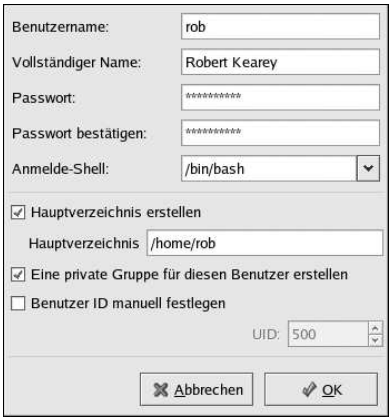

Abbildung 35-2. Neuer Benutzer

Um erweiterte Benutzereigenschaften zu konfigurieren, wie z.B. die Gültigkeitsdauer des Passworts, bearbeiten Sie die Benutzereigenschaften, nachdem Sie den Benutzer hinzugefügt haben. Weitere Informationen finden Sie unter Abschnitt 35.2.

Um einen Benutzer in weitere Benutzergruppen hinzuzufügen, klicken Sie auf **Benutzer**, wählen den Benutzer und klicken anschließend auf **Eigenschaften**. Im Fenster **Benutzereigenschaften** wählen Sie den Button **Gruppen**. Wählen Sie die Gruppe, zu der Sie den Benutzer hinzufügen möchten, und die primäre Gruppe für den Benutzer, und klicken Sie auf **OK**.

35.2. Ändern der Benutzereigenschaften

Wenn Sie die Eigenschaften eines Benutzers anzeigen möchten, klicken Sie auf das Tab **Benutzer**, wählen Sie den Benutzer aus der Liste aus und klicken Sie auf **Eigenschaften** aus dem Button-Menü (oder wählen Sie im Pull-Down Menü **Datei => Eigenschaften**). Es erscheint ein Fenster wie in Abbildung 35-3 gezeigt.

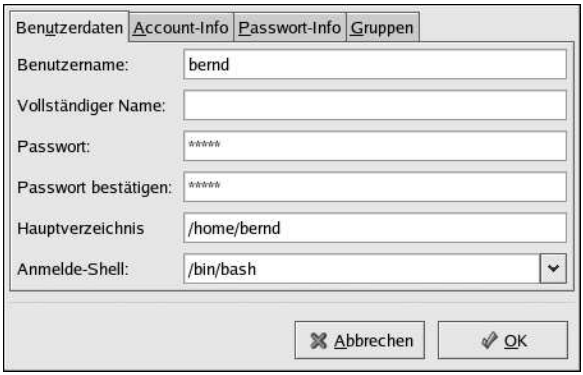

Abbildung 35-3. Benutzereigenschaften

Das Fenster **Benutzereigenschaften** ist in verschiedene Tabs unterteilt:

- **Benutzerdaten** — Allgemeine Informationen über den Benutzer, die beim Hinzufügen des Benutzers festgelegt wurden. Hier können Sie den kompletten Namen, das Passwort, das Home-Verzeichnis oder die Anmeldeshell des Benutzers ändern.
- **Account-Info** — Wählen Sie **Ablauf des Accounts aktivieren** wenn Sie möchten, dass der Account nach einer festgelegten Zeit abläuft. Geben Sie das entsprechende Datum in das Feld ein. Wählen Sie **Benutzer-Account ist gesperrt**, um den Benutzeraccount zu sperren und damit dem Benutzer das Anmelden im System nicht zu ermöglichen.
- **Passwort-Info** — Dieses Tab zeigt das Datum, an dem das Passwort vom Benutzer zuletzt geändert wurde. Um zu erzwingen, dass der Benutzer das Passwort nach einer bestimmten Anzahl von Tagen ändert, wählen Sie **Passwort-Ablauf aktivieren**. Sie können auch die Anzahl der Tage einstellen, nach denen der Benutzer sein Passwort ändern kann, oder die Anzahl der Tage, nach denen der Benutzer gewarnt wird, dass das Passwort abläuft, sowie die Anzahl der Tage, nach denen der Account nicht mehr aktiv ist.
- **Gruppen** — Wählen Sie die Gruppe, zu der der Benutzer hinzugefügt werden soll, sowie die primäre Gruppe des Benutzers.

35.3. Hinzufügen einer neuen Gruppe

Um eine neue Benutzergruppe hinzuzufügen, klicken Sie auf den Button **Gruppe hinzufügen**. Es erscheint ein Fenster, wie in Abbildung 35-4 abgebildet. Geben Sie den Namen der neu zu erstellenden Gruppe ein. Wählen Sie **Gruppen-ID manuell festlegen**, um für die neue Gruppe eine Gruppen-ID festzulegen und wählen Sie die GID. Red Hat Enterprise Linux reserviert die ersten 500 Gruppen- IDs für System-Gruppen.

Klicken Sie auf **OK**, um die Gruppe zu erstellen. Die neue Gruppe erscheint in der Liste der Gruppen.

Abbildung 35-4. Neue Gruppe

Informationen darüber, wie Benutzer zu Gruppen hinzugefügt werden, finden Sie im Abschnitt 35.4.

35.4. Ändern der Gruppeneigenschaften

Um die Eigenschaften einer Gruppe anzuzeigen, wählen Sie die Gruppe aus der Liste aus und klicken Sie auf **Eigenschaften** aus dem Button-Menü (oder wählen Sie im Pull-Down Menü **Datei => Eigenschaften**). Es erscheint ein Fenster, wie in Abbildung 35-5 abgebildet.

Abbildung 35-5. Gruppeneigenschaften

Das Tab **Gruppenbenutzer** zeigt die Benutzer an, die einer Gruppe angehören. Wählen Sie zusätzliche Benutzer, die Sie zu der Gruppe hinzufügen, oder deselektieren Sie die Benutzer, die Sie aus der Gruppe entfernen möchten. Klicken Sie auf **OK**, um die Benutzer in der Gruppe zu bearbeiten.

35.5. Befehlszeilen-Konfiguration

Wenn Sie lieber Befehlszeilen verwenden oder das X Window System nicht installiert haben, finden Sie in diesem Kapitel Informationen zum Konfigurierenvon Benutzern und Gruppen.

35.5.1. Benutzer hinzufügen

Um einen Benutzer zum System hinzuzufügen:

1. Mit dem Befehl `useradd` erstellen Sie einen gesperrten Benutzeraccount:

```
useradd <username>
```

2. Entsperren Sie den Account mit dem Befehl `passwd` und vergeben Sie ein Passwort sowie Passwortablauf-Richtlinien:
```
passwd <username>
```

Die Befehlszeilen-Optionen für `useradd` finden Sie unter Tabelle 35-1.

Option	Beschreibung
`-c Befehl`	Kommentar für den Benutzer
`-d home-dir`	Home-Verzeichnis, das anstelle des Standardverzeichnisses `/home/username` verwendet wird
`-e Datum`	Datum, wann der Account abläuft, das Format ist JJJJ-MM-TT
`-f Tage`	Anzahl der Tage, nach denen das Passwort und damit der Account ungültig wird. (Wenn **`0`** angegeben wird, wird der Account sofort deaktiviert, wenn das Passwort ungültig wird. Wenn **`-1`** angegeben wird, wird der Account nicht deaktiviert, auch wenn das Passwort ungültig wird.)
`-g Gruppen-Name`	Gruppenname oder Gruppennummer für die Standardgruppe des Benutzers (Die Gruppe muss bereits bestehen, bevor Sie diese hier angeben können.)
`-G Gruppenliste`	Liste aller weiteren Gruppennamen oder Gruppennummern zu denen der Benutzer gehört, durch Kommata getrennt aufgeführt. (Die Gruppe muss bereits bestehen, bevor Sie diese hier angeben können).
`-m`	Erstellt das Home-Verzeichnis, falls dies noch nicht erstellt wurde
`-M`	Kein Home-Verzeichnis erstellen
`-n`	Keine User Private Group für den Benutzer erstellen
`-r`	Erstellt einen Systemaccount mit einer Benutzer ID unter 500 und ohne Home-Verzeichnis
`-p Passwort`	Das mit `crypt` verschlüsselte Passwort
`-s`	Anmelde-Shell des Benutzers, weist standardmäßig auf `/bin/bash`
`-u uid`	Benutzer-ID für den Benutzer. Muss einmalig und größer als 499 sein

Tabelle 35-1. `useradd` Befehlszeilen-Optionen

35.5.2. Gruppe hinzufügen

Um eine Gruppe dem System hinzuzufügen, verwenden Sie den Befehl `groupadd`:

```
groupadd <group-name>
```

Die Befehlszeilen-Optionen für `groupadd` finden Sie unter Tabelle 35-2.

Option	Beschreibung
`-g gid`	Gruppen-ID für die Gruppe. Muss einmalig und größer als 499 sein

Option	Beschreibung
`-r`	Erstellt eine Systemgruppe mit einer ID unter 500
`-f`	Beendet mit einem Fehler, wenn die Gruppe bereits besteht. (Die Gruppe wird nicht verändert.) Wenn `-g` und `-f` angegeben werden, die Gruppe jedoch schon existiert, wird die Option `-g` ignoriert

Tabelle 35-2. `groupadd` Befehlszeilen-Optionen

35.5.3. Ablauf des Passworts

Aus Gründen der Sicherheit sollten Benutzer angewiesen werden, ihre Passwörter in regelmäßigen Abständen zu ändern. Dies kann während des Hinzufügens oder Bearbeitens eines Benutzers im Tab **Passwort-Info** des **User Manager** durchgeführt werden.

Um den Ablauf des Passworts für einen Benutzer vom Shell-Prompt aus zu konfigurieren, verwenden Sie den Befehl `chage`, gefolgt von einer Option aus Tabelle 35-3, gefolgt vom Benutzernamen des Benutzers.

Wichtig

Shadow-Passwörter müssen aktiviert werden, wenn Sie den Befehl `chage` verwenden möchten.

Option	Beschreibung
`-m` *`Tage`*	Gibt die Mindestanzahl der Tage an, in denen der Benutzer sein Passwort ändern muss. Ist der Wert auf 0 gesetzt, läuft das Passwort nicht ab.
`-M` *`Tage`*	Gibt die Höchstzahl der Tage an, für die das Passwort gültig ist. Wenn die Anzahl der Tage für die das Passwort gültig ist plus die Anzahl der Tage, die durch die Option `-d` festgelegt wurde, einen früheren Zeitpunkt als den aktuellen Tag beschreibt, muss der Benutzer das Passwort ändern, bevor er den Account verwenden kann.
`-d` *`Tage`*	Gibt die Anzahl der Tage seit dem 1. Januar 1970 an, an denen das Passwort geändert wurde.
`-I` *`Tage`*	Gibt die Anzahl der Tage an, bevor der Account gesperrt wird, wenn das Passwort nicht geändert wird. Wenn der Wert 0 ist, wird der Account nicht gesperrt wenn das Passwort abläuft.
`-E` *`Datum`*	Gibt das Datum an, an dem der Account gesperrt wird. Das Format ist JJJJ-MM-TT. Anstelle des Datums kann auch die Anzahl von Tagen seit dem 1. Januar 1970 verwendet werden.
`-W` *`Tage`*	Gibt die Anzahl der Tage vor Ablauf des Passworts an, um den Benutzer zu warnen.

Tabelle 35-3. `chage` Befehlszeilen-Optionen

Tipp

Wenn der Befehl `chage` direkt von einem Benutzernamen (ohne Optionen) gefolgt wird, werden die aktuellen Werte zum Ablauf des Passworts angezeigt. Diese können geändert werden.

Wenn ein Systemadministrator möchte, dass ein Benutzer sein Passwort beim ersten Anmelden ändert, kann das Benutzerpasswort so gesetzt werden, dass es sofort abläuft und damit den Benutzer zwingt, dieses sofort nach dem ersten Einloggen zu ändern.

Um einen Benutzer zu zwingen, das Passwort beim ersten Anmelden an der Konsole zu ändern, folgen Sie den nachfolgenden Anweisungen. Bitte beachten Sie, dass dieser Vorgang nicht funktioniert, wenn der Benutzer sich über das SSH-Protokoll anmeldet.

1. *Sperren Sie das Benutzerpasswort* — Wenn der Benutzer nicht existiert, verwenden Sie den Befehl `useradd`, um einen Benutzer-Account zu erstellen, weisen Sie diesem aber kein Passwort zu, so dass der Account gesperrt bleibt.

   Wenn bereits ein Passwort aktiviert wurde, sperren Sie dieses mit dem Befehl:
   `usermod -L username`

2. *Erzwingen sofortigen Ablaufs des Passworts* — geben Sie dazu Folgendes ein:
   `chage -d 0 username`

   Dieser Befehl setzt den Wert für wann das Passwort zuletzt geändert wurde auf Epoche (1. Januar, 1970). Dieser Wert erzwingt den sofortigen Ablauf des Passworts, jegliche Einstellungen für den Ablauf von Passwörtern werden ignoriert.

3. *Entsperren Sie den Account* — Hier gibt es zwei Möglichkeiten. Der Administrator kann ein anfängliches Passwort oder ein Null-Passwort zuweisen.

   

   Warnung

   Verwenden Sie nicht den Befehl `passwd`, um das Passwort zu erstellen, da dieser Befehl den sofortigen Ablauf des Passworts, den Sie im vorigen Schritt eingestellt haben, deaktiviert.

   Folgen Sie den Anweisungen, um ein anfängliches Passwort zu erstellen:

   - Starten Sie den Befehlszeilen-Python-Interpreter mit dem Befehl `python`. Folgendes wird angezeigt:
     ```
     Python 2.2.2 (#1, Dec 10 2002, 09:57:09)
     [GCC 3.2.1 20021207 (Red Hat Enterprise Linux 3 3.2.1-2)] on linux2
     Type "help", "copyright", "credits" or "license" for more information.
     >>>
     ```
   - Geben Sie am Prompt das Folgende ein (ersetzen Sie *`Passwort`* mit dem zu verschlüsselnden Passwort und *`salt`* mit einer Kombination aus genau 2 Groß- oder Kleinbuchstaben, Zahlen, dem Punkt (.) oder Schrägstrich (/), wie zum Beispiel `ab` oder `12`:
     `import crypt; print crypt.crypt("password","salt")`

     Die Ausgabe ist das verschlüsselte Passwort, zum Beispiel `12CsGd8FRcMSM`.
   - Drücken Sie [Strg]-[D] um den Python-Interpreter zu beenden.
   - Kopieren Sie das verschlüsselte Passwort ohne Leerzeichen vorne und hinten, und fügen Sie dieses in den folgenden Befehl ein:
     `usermod -p "encrypted-password" username`

   Anstelle eines anfänglichen Passworts kann ein Null-Passwort mit Hilfe des folgenden Befehls zugewiesen werden:
   `usermod -p "" username`

Achtung

Auch wenn das Verwenden eines Null-Passworts für Benutzer und Administrator sehr bequem ist, existiert ein geringes Risiko, dass ein Unbefugter sich als erstes anmeldet und damit auf das System zugreift. Um diese Gefahr zu verringern empfiehlt es sich, dass der Administrator sicher geht, dass der Benutzer zum Anmelden bereit ist bevor der Account entsperrt wird.

In beiden Fällen wird der Benutzer bei der ersten Anmeldung aufgefordert, ein neues Passwort einzugeben.

35.6. Beschreibung des Vorgangs

Die folgenden Schritte verdeutlichen was passiert, wenn der Befehl `useradd juan` auf ein System mit Shadow-Passwörtern angewendet wird:

1. Eine neue Zeile für `juan` wird in der Datei `/etc/passwd` angelegt. Diese Zeile hat die folgenden Merkmale:
   - Sie beginnt mit dem Benutzernamen `juan`.
   - Im Passwort-Feld steht ein `x`, was anzeigt, dass das System Shadow-Passwörter verwendet.
   - Eine UID überhalb von 500 wird erstellt. (In Red Hat Enterprise Linux werden UIDs und GIDs unterhalb von 500 für die Systembenutzung reserviert.)
   - Eine GID überhalb von 500 wird erstellt.
   - Die optionale GECOS-Information wird frei gelassen.
   - Das Home-Verzeichnis für `juan` wird auf `/home/juan/` gesetzt.
   - Die Standard-Shell wird auf `/bin/bash` gesetzt.

2. Eine neue Zeile für `juan` wird in `/etc/shadow` erstellt. Diese Zeile hat die folgenden Merkmale:
   - Sie beginnt mit dem Benutzernamen `juan`.
   - Zwei Ausrufezeichen (`!!`) erscheinen im Passwort-Feld der Datei `/etc/shadow`, die den Account sperrt.

     

     Anmerkung

     Wenn ein verschlüsseltes Passwort mit der `-p` Flag verwendet wird, wird dies in der Datei `/etc/shadow` auf der neuen Zeile für den Benutzer angelegt.

   - Das Passwort ist so eingestellt, dass es nicht abläuft.

3. Eine neue Zeile für eine Gruppe mit dem Namen `juan` wird in `/etc/group` erstellt. Eine Gruppe mit dem gleichen Namen wie der Benutzer wird auch *User Private Group* genannt. Weitere Informationen zu diesen privaten Benutzergruppen finden Sie unter Abschnitt 35.1.

   Die Zeile, die in `/etc/group` erstellt wurde, hat die folgenden Merkmale:
   - Sie beginnt mit dem Gruppennamen `juan`.
   - Ein `x` erscheint im Passwort-Feld, und zeigt damit an, dass das System Shadow-Passwörter verwendet.

- Die GID stimmt mit der für den Benutzer `juan` in `/etc/passwd` aufgelisteten ID überein.

4. Eine neue Zeile für den Gruppennamen `juan` wird in `/etc/gshadow` erstellt. Diese Zeile hat die folgenden Merkmale:
   - Sie beginnt mit dem Gruppennamen `juan`.
   - Ein Ausrufezeichen (`!`) erscheint im Passwort-Feld in der Datei `/etc/gshadow`, die die Gruppe sperrt.
   - Alle anderen Felder sind leer.
5. Ein Verzeichnis für den Benutzer `juan` wird im Verzeichnis `/home/` erstellt. Dieses Verzeichnis gehört dem Benutzer `juan` und der Gruppe `juan`. Es hat jedoch Lese-, Schreib- und Ausführberechtigungen *ausschließlich* für den Benutzer `juan`. Alle anderen Berechtigungen werden zurückgewiesen.
6. Die Dateien innerhalb des `/etc/skel/`-Verzeichnisses (das die Standard-Benutzereinstellungen enthält) werden in das neue Verzeichnis `/home/juan/` kopiert.

An dieser Stelle wird ein gesperrter Account mit dem Namen `juan` im System angelegt. Um diesen zu aktivieren, muss der Administrator als nächstes ein Passwort für den Account mit Hilfe des Befehls `passwd` festlegen, und optional Richtlinien für den Passwort-Ablauf einrichten.

35.7. Zusätzliche Informationen

In diesem Ressourcen finden Sie weitere Informationen über das Verwalten von Benutzern und Gruppen.

35.7.1. Installierte Dokumentation

- Die man-Seiten für `useradd`, `passwd`, `groupadd` und `chage`.

35.7.2. Bücher zum Thema

- *Red Hat Enterprise Linux Referenzhandbuch* — In diesem Handbuch werden standarmäßige Benutzer und Gruppen beschrieben, User Private Groups behandelt und ein Überblick über Shadow-Passwörter gegeben.
- *Red Hat Enterprise Linux Introduction to System Administration* — Dieses Begleithandbuch enthält weitere Informationen zur Verwaltung von Benutzern und Gruppen und zur Verwaltung von Benutzerressourcen.

Kapitel 36.

Druckerkonfiguration

Mit der Anwendung **Printer Configuration Tool** können Benutzer einen Drucker konfigurieren. Mit diesem Tool können Sie die Drucker-Konfigurationsdatei, DruckerSpool-Verzeichnisse und Druckfilter warten.

Red Hat Enterprise Linux 3 verwendet das CUPS Drucksystem. Wenn ein System von einer vorherigen Version von Red Hat Enterprise Linux das CUPS verwendet, aktualisiert wurde, erhält die Aktualisierung die Konfiguration der Warteschlangen.

Um das **Printer Configuration Tool** verwenden zu können, müssen Sie über root-Berechtigungen verfügen. Wählen Sie zum Starten der Anwendung **Hauptmenü** (auf dem Panel) => **Systemeinstellungen** => **Printing** oder geben Sie den Befehl `redhat-config-printer` ein. Dieser Befehl legt automatisch fest, ob die Grafikversion oder die text-basierte Version gestartet werden soll, abhängig davon, ob der Befehl in der grafischen X Window Systemumgebung oder von einer text-basierten Konsole aus eingegeben wird.

Sie können das **Printer Configuration Tool** auch als text-basierte Version ausführen, indem Sie den Befehl `redhat-config-printer-tui` von einem Shell-Prompt aus ausführen.

Wichtig

Ändern Sie nicht die Datei `/etc/printcap` oder die Dateien im `/etc/cups/` Verzeichnis. Jedes Mal, wenn der Drucker-Daemon (`cups`) gestartet oder neu gestartet wird, werden neue Konfigurationsdateien dynamisch erstellt. Diese Dateien werden auch dynamisch erstellt, wenn Änderungen über das **Printer Configuration Tool** durchgeführt werden.

Abbildung 36-1. Printer Configuration Tool

Die folgenden Druckerwarteschlangen-Typen können konfiguriert werden:

- **Lokal-verbunden** — ein Drucker, der direkt durch einen parallelen oder USB-Port an den Computer angeschlossen ist.
- **CUPS im Netzwerk (IPP)** — ein Drucker, der an ein anderes CUPS-System angeschlossen ist, auf den über ein TCP/IP Netzwerk zugegriffen werden kann (zum Beispiel ein Drucker, der an ein

anderes Red Hat Enterprise Linux System angeschlossen ist, und bei dem CUPS übers Netzwerk läuft).

- **UNIX im Netzwerk (LPD)** — ein Drucker, der an ein anderes UNIX-System angeschlossen ist, auf den über ein TCP/IP Netzwerk zugegriffen werden kann (zum Beispiel ein Drucker, der an ein anderes Red Hat Enterprise Linux System angeschlossen ist, und bei dem LPD übers Netzwerk läuft).
- **Windows im Netzwerk(SMB)** — Ein Drucker, der an ein anderes System angeschlossen ist, das einen Drucker über ein SMB Netzwerk gemeinsam verwendet (zum Beispiel ein Drucker, der an einen Microsoft Windows™ Computer angeschlossen ist).
- **Novell im Netzwerk(NCP)** — Ein Drucker, der an ein anderes System angeschlossen ist, das die Netzwerktechnologie von Novell Netware verwendet.
- **JetDirect im Netzwerk** — ein Drucker, der direkt über HP JetDirect anstelle eines Computers an das Netzwerk angeschlossen ist.

Wichtig

Wenn Sie eine neue Druckwarteschlange hinzufügen oder eine vorhandene Warteschlange modifizieren, müssen Sie die Änderungen übernehmen, damit diese wirksam werden.

Wenn Sie auf den Button **Anwenden** klicken, werden alle Änderungen gespeichert und der Drucker-Daemon neu gestartet. Die Änderungen werden nicht in die Konfigurationsdatei geschrieben, bis der Drucker-Daemon neu gestartet wird. Alternativ hierzu können Sie erst auf **Datei => Änderungen speichern** und dann **Aktion => Übernehmen** klicken.

36.1. Hinzufügen eines lokalen Druckers

Um einen lokalen Drucker wie zum Beispiel einen an den parallelen Port oder USB-Port des Computers angeschlossenen Drucker hinzuzufügen, klicken Sie auf den Button **Neu** im Hauptfenster vom **Printer Configuration Tool**. Das unter Abbildung 36-2 abgebildete Fenster wird angezeigt. Klicken Sie zum Fortfahren auf **Vor**.

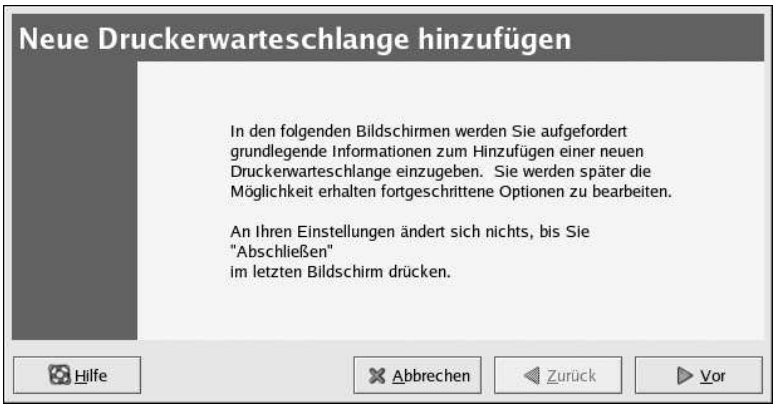

Abbildung 36-2. Drucker hinzufügen

Im unter Abbildung 36-3 angezeigten Fenster geben Sie nun einen einmaligen Namen für den Drucker im Feld **Name** ein. Der Name des Druckers darf keine Leerstellen enthalten und muss mit einem Buchstaben beginnen. Der Name darf Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Sie können außerdem eine kurze Beschreibung des Druckers hinzufügen (diese darf Leerstellen enthalten).

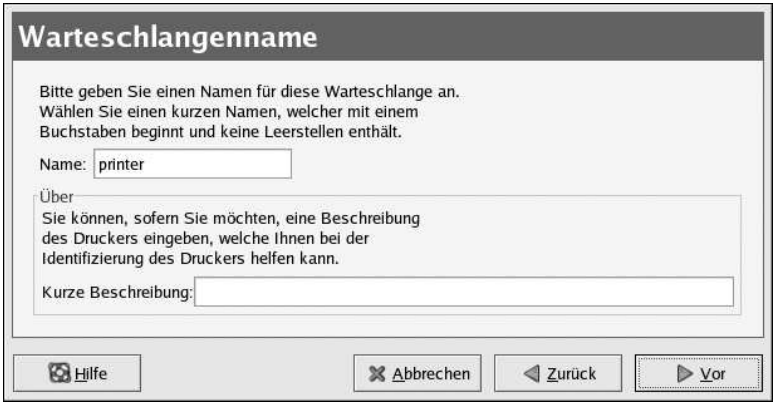

Abbildung 36-3. Warteschlangenname auswählen

Nachdem Sie auf **Vor** geklickt haben, erscheint das Fenster Abbildung 36-4. Wählen Sie **Lokal-verbunden** aus dem Menü **Warteschlangentyp auswählen** und das Gerät aus. Das Gerät ist in der Regel `/dev/lp0` für einen Paralleldrucker oder `/dev/usb/lp0` für einen USB-Drucker. Werden in der Liste keine Geräte angezeigt, klicken Sie auf **Geräte erneut prüfen**, um erneut zu suchen, oder klicken Sie auf **Kundenspezifisches Gerät**, um dieses manuell einzugeben. Klicken Sie dann auf **Vor**.

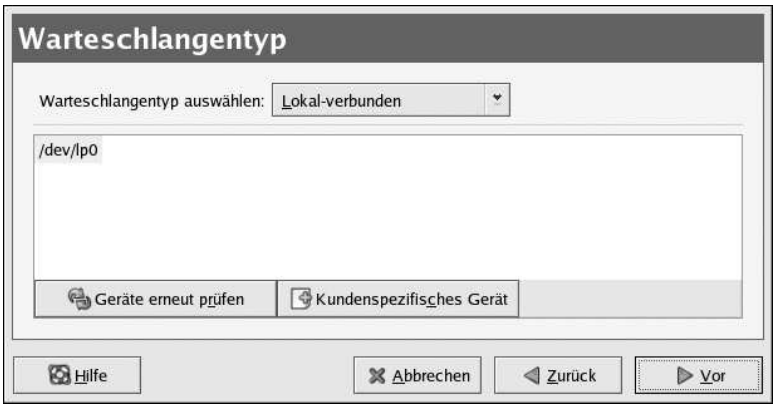

Abbildung 36-4. Hinzufügen eines lokalen Druckers

Im nächsten Schritt wählen Sie den Druckertyp aus. Gehen Sie zum Fortfahren zu Abschnitt 36.7.

36.2. Hinzufügen eines CUPS (IPP) Netzwerkdruckers

Ein IPP-Drucker ist ein Drucker, der an ein anderes Linux-System auf dem selben Netzwerk mit CUPS angeschlossen ist. Standardmäßig durchsucht **Printer Configuration Tool** das Netzwerk auf gemeinsam verwendete IPP-Drucker. (Diese Einstellung kann geändert werden: Wählen Sie **Allgemein** nach **Aktion => Sharing** aus dem Pull-Down-Menü). Jegliche IPP-Drucker erscheinen im Hauptfenster als **Durchgesehene Warteschlangen**.

Wenn Sie eine Firewall auf dem Druckserver konfiguriert haben, muss über diese der Empfang und das Senden von Verbindungen auf dem Eingangsport UDP 631 möglich sein. Wenn Sie eine Firewall auf dem Clienten haben (der Computer, der die Druckanfragen sendet), muss dieser Verbinden auf Port 631 senden und empfangen können.

Wenn Sie die automatische Suchfunktion deaktivieren, können Sie trotzdem weiterhin CUPS Netzwerkdrucker hinzufügen, in dem Sie auf **Neu** im Hauptfenster des **Printer Configuration Tool** klicken, um das Fenster in Abbildung 36-2 anzuzeigen. Klicken Sie zum Fortfahren auf **Vor**.

Im unter Abbildung 36-3 angezeigten Fenster geben Sie nun einen einmaligen Namen für den Drucker im Feld **Name** ein. Der Name des Druckers darf keine Leerstellen enthalten und muss mit einem Buchstaben beginnen. Der Name darf Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Sie können außerdem eine kurze Beschreibung des Druckers hinzufügen (diese darf Leerstellen enthalten).

Nachdem Sie auf **Vor** geklickt haben, erscheint Abbildung 36-5. Wählen Sie **Networked CUPS (IPP)** aus dem Menü **Warteschlangentyp auswählen**.

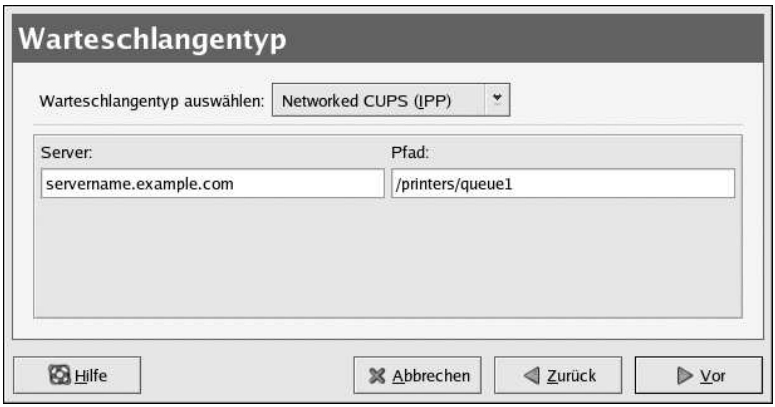

Abbildung 36-5. Hinzufügen eines CUPS (IPP) Netzwerkdruckers

Die Textfelder für die folgenden Optionen sind:

- **Server** — Der Hostname oder die IP-Adresse des Rechners, an den der Drucker angeschlossen ist.
- **Pfad** — Der Pfad zu der Drucker-Warteschlange auf dem Remote-Computer.

Klicken Sie zum Fortfahren auf **Weiter**.

Im nächsten Schritt wählen Sie den Druckertyp aus. Gehen Sie zum Fortfahren zu Abschnitt 36.7.

Wichtig

Der Druckserver für den CUPS Netzwerkdrucker muss Verbindungen vom lokalen System zusallen. Weitere Informationen finden Sie unter Abschnitt 36.13.

36.3. Hinzufügen eines Remote-UNIX (LPD) Druckers

Um einen Remote-UNIX-Drucker hinzuzufügen, wie zum Beispiel einen Drucker, der im gleichen Netzwerk an ein anderes Linux-System angeschlossen ist, klicken Sie auf den Button **Neu** im Hauptfenster vom **Printer Configuration Tool**. Das in Abbildung 36-2 abgebildete Fenster wird angezeigt. Klicken Sie zum Fortfahren auf **Vor**.

Im unter Abbildung 36-3 angezeigten Fenster geben Sie nun einen einmaligen Namen für den Drucker im Feld **Name** ein. Der Name des Druckers darf keine Leerstellen enthalten und muss mit einem Buchstaben beginnen. Der Name darf Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Sie können außerdem eine kurze Beschreibung des Druckers hinzufügen (diese darf Leerstellen enthalten).

Wählen Sie **Networked UNIX (LPD)** aus dem Menü **Warteschlangentyp auswählen** und klicken Sie auf **Weiter**.

Abbildung 36-6. Hinzufügen eines Remote-LPD-Druckers

Es werden Textfelder für folgende Optionen angezeigt:

- **Server** — Der Hostname oder die IP-Adresse des Remote-Rechners, an den der Drucker angeschlossen ist.
- **Warteschlange** — Die Warteschlange des Remote-Druckers. Die Standard-Druckerwarteschlange ist in der Regel `lp`.

Klicken Sie zum Fortfahren auf **Vor**.

Im nächsten Schritt wählen Sie den Druckertyp aus. Gehen Sie zum Fortfahren zu Abschnitt 36.7.


Wichtig

Der Remote-Drucker muss Druckaufträge vom lokalen System annehmen können.

36.4. Samba-Drucker (SMB) hinzufügen

Wenn Sie einen Drucker hinzufügen möchten, auf den Sie mit Hilfe des SMB-Protokolls zugreifen können (wie zum Beispiel ein Drucker, der an ein Microsoft Windows System angeschlossen ist), klicken Sie auf den Button **Neu** im Hauptfenster vom **Printer Configuration Tool**. Das unter Abbildung 36-2 abgebildete Fenster wird angezeigt. Klicken Sie zum Fortfahren auf **Vor**.

Im unter Abbildung 36-3 angezeigten Fenster geben Sie nun einen einmaligen Namen für den Drucker im Feld **Name** ein. Der Name des Druckers darf keine Leerstellen enthalten und muss mit einem Buchstaben beginnen. Der Name darf Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Sie können außerdem eine kurze Beschreibung des Druckers hinzufügen (diese darf Leerstellen enthalten).

Wählen Sie **Windows (SMB) im Netzwerk** im Menü **Warteschlangentyp auswählen** und klicken Sie auf **Vor**. Wenn der Drucker an ein Microsoft Windows System angeschlossen ist, wählen Sie diesen Warteschlangentyp.

Abbildung 36-7. SMB-Drucker hinzufügen

Wie in Abbildung 36-7 abgebildet, werden SMB-Shares automatisch erkannt und aufgelistet. Klicken Sie auf den Pfeil neben jedem Namen, um die Liste erweitert anzuzeigen. Wählen Sie aus dieser Liste den Drucker aus.

Wenn der gewünschte Drucker nicht in dieser Liste aufgeführt wird, klicken Sie auf **Festlegen** auf der rechten Seite. Es werden Textfelder für folgende Optionen angezeigt:

- **Arbeitsgruppe** — Der Name der Samba-Arbeitsgruppe für den Drucker.
- **Server** — Der Name des Server, der den geteilten Drucker verwendet.
- **Share** — Der Name des freigegebenen Druckers, auf dem Sie drucken möchten. Dieser Name muss mit dem Namen übereinstimmen, unter dem der Samba-Drucker auf dem Remote-Windows-Rechner definiert ist.

- **Benutzername** — Der Name des Benutzers, unter dem Sie sich anmelden müssen, um auf den Drucker zugreifen zu können. Dieser Benutzer muss auf dem Windows-Rechner vorhanden sein, und der Benutzer muss Zugriffsberechtigung für den Drucker haben. Der Benutzername lautet in der Regel **guest** für Windows-Server oder **nobody** für Samba-Server.
- **Passwort** — Das Passwort (falls erforderlich) für den im Feld **Benutzer** angegebenen Benutzer.

Klicken Sie zum Fortfahren auf **Weiter**. **Printer Configuration Tool** versucht dann, eine Verbindung zum geteilten Drucker herzustellen. Wenn für diesen Drucker ein Benutzername und ein Passwort verlangt wird, erscheint ein Fenster, in dem Sie zur Eingabe eines gültigen Benutzernamens und eines Passworts aufgefordert werden. Wenn Sie einen inkorrekten Share-Namen angegeben haben, können Sie diesen hier ändern. Wird ein Arbeitsgruppen-Name verlangt, kann dieser hier festgelegt werden. Dieser Dialog ist der gleiche wie unter **Festlegen**.

Im nächsten Schritt wählen Sie den Druckertyp aus. Gehen Sie zum Fortfahren zu Abschnitt 36.7.

Warnung

Wenn Sie you einen Benutzernamen und ein Passwort benötigen, werden diese unverschlüsselt in Dateien gespeichert, die nur vom root und lpd gelesen werden können. Es ist daher für andere möglich, den Benutzernamen und das Passwort als root herauszufinden. Um dies zu verhindern, sollten Benutzername und Passwort für den Drucker sich von Benutzername und Passwort des Accounts auf dem lokalen Red Hat Enterprise Linux-System unterscheiden. Unterscheiden sich diese, ist die einzige Sicherheitsverletzung das unberechtigte Nutzen des Druckers. Sind Datei-Shares vom Server vorhanden, sollten diese auch ein anderes Passwort als das für die Druckerwarteschlange haben.

36.5. Novell NetWare-Drucker (NCP) hinzufügen

Klicken Sie zum Hinzufügen eines Novell NetWare-Druckers (NCP-Druckers) auf den Button **Neu** im Hauptfenster vom **Printer Configuration Tool** Das in Abbildung 36-1 abgebildete Fenster wird angezeigt. Klicken Sie zum Fortfahren auf **Vor**.

Im unter Abbildung 36-3 angezeigten Fenster geben Sie nun einen einmaligen Namen für den Drucker im Feld **Name** ein. Der Name des Druckers darf keine Leerstellen enthalten und muss mit einem Buchstaben beginnen. Der Name darf Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Sie können außerdem eine kurze Beschreibung des Druckers hinzufügen (diese darf Leerstellen enthalten).

Wählen Sie **Novell (NCP) im Netzwerk** im Menü **Warteschlangentyp auswählen** aus.

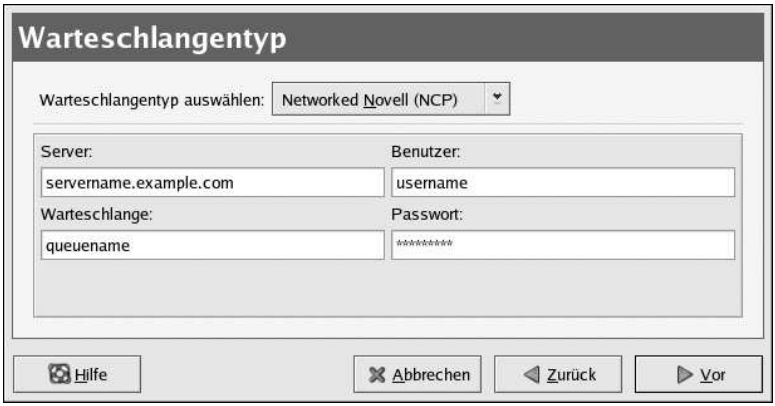

Abbildung 36-8. NCP-Drucker hinzufügen

Die Textfelder für die Optionen sind wie folgt:

- **Server** — Der Hostname oder die IP-Adresse des NCP-Rechners, an den der Drucker angeschlossen ist.
- **Warteschlange** — Die Remote-Warteschlange für den Drucker auf dem NCP-System.
- **Benutzer** — Der Name des Benutzers, unter dem Sie sich anmelden müssen, um auf den Drucker zugreifen zu können.
- **Passwort** — Das Passwort für den im Feld **Benutzer** angegebenen Benutzer.

Im nächsten Schritt wählen Sie den Druckertyp aus. Gehen Sie zum Fortfahren zu Abschnitt 36.7.

Warnung

Wenn Sie you einen Benutzernamen und ein Passwort benötigen, werden diese unverschlüsselt in Dateien gespeichert, die nur vom root und lpd gelesen werden können. Es ist daher für andere möglich, den Benutzernamen und das Passwort als root herauszufinden. Um dies zu verhindern, sollten Benutzername und Passwort für den Drucker sich von Benutzername und Passwort des Accounts auf dem lokalen Red Hat Enterprise Linux-System unterscheiden. Unterscheiden sich diese, ist die einzige Sicherheitsverletzung das unberechtigte Nutzen des Druckers. Sind Datei-Shares vom Server vorhanden, sollten diese auch ein anderes Passwort als das für die Druckerwarteschlange haben.

36.6. Hinzufügen eines JetDirect-Druckers

Klicken Sie zum Hinzufügen eines JetDirect-Druckers auf den Button **Neu** im Hauptfenster vom **Printer Configuration Tool**. Das in Abbildung 36-1 abgebildete Fenster wird angezeigt. Klicken Sie zum Fortfahren auf **Vor**.

Im unter Abbildung 36-3 angezeigten Fenster geben Sie nun einen einmaligen Namen für den Drucker im Feld **Name** ein. Der Name des Druckers darf keine Leerstellen enthalten und muss mit einem Buchstaben beginnen. Der Name darf Buchstaben, Zahlen, Bindestriche (-) und Unterstriche (_) enthalten. Sie können außerdem eine kurze Beschreibung des Druckers hinzufügen (diese darf Leerstellen enthalten).

Wählen Sie **Networked JetDirect** aus dem Menü **Warteschlangentyp auswählen** und klicken Sie dann auf **Vor**.

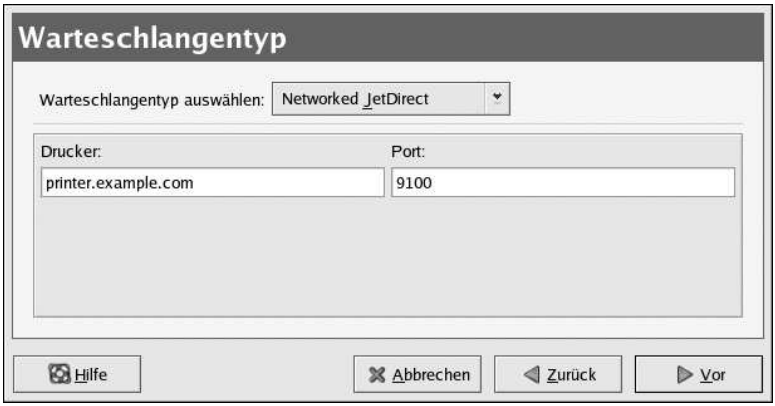

Abbildung 36-9. Hinzufügen eines JetDirect-Druckers

Die Textfelder für die folgenden Optionen werden angezeigt:

- **Drucker** — Der Hostname oder die IP-Adresse des JetDirect-Druckers.
- **Port** — Der Port auf dem JetDirect- Drucker, der auf Druckerjobs achtet. Der Standardport ist 9100.

Im nächsten Schritt wählen Sie den Druckertyp aus. Gehen Sie zum Fortfahren zu Abschnitt 36.7.

36.7. Auswahl des Druckermodells und Fertigstellung

Nachdem Sie den Warteschlangentyp des Druckers ausgewählt haben, müssen Sie nun das Druckermodell auswählen.

Ein Fenster wie Abbildung 36-10 wird angezeigt. Wurde Ihr Drucker nicht automatisch erkannt, wählen Sie das Modell aus der Liste aus. Die Drucker werden nach Hersteller unterteilt. Wählen Sie den Namen des Druckerherstellers aus dem Pull-Down-Menü. Die Druckermodelle werden immer dann aktualisiert, wenn ein andere Hersteller ausgewählt wird. Wählen Sie das Druckermodell aus der Liste aus.

Abbildung 36-10. Auswahl des Druckermodells

Der empfohlene Druckertreiber wird je nach ausgewähltem Drucker ausgewählt. Der Druckertreiber verarbeitet die Daten, die Sie drucken möchten in ein Format, dass der Drucker versteht. Da ein lokaler Drucker direkt an Ihren Computer angeschlossen ist, benötigen Sie einen Druckertreiber zum Verarbeiten der Daten, die an den Drucker gesendet werden.

Wenn Sie einen Remote-Drucker (IPP, LPD, SMB oder NCP) konfigurieren, hat der Remote-Druckerserver meist einen eigenen Druckertreiber. Wenn Sie einen zusätzlichen Druckertreiber auf Ihrem lokalen Computer auswählen, werden die Daten mehrfach gefiltert, und in ein Format umgewandelt, dass der Drucker nicht versteht.

Um sicher zu stellen, dass Daten nicht mehr als einmal gefiltert werden, versuchen Sie als erstes, **Generisch** als Hersteller und **Raw Drucker-Warteschlange** oder **Postscript Drucker** als Druckermodell auszuwählen. Nachdem Sie die Änderungen übernommen haben, drucken Sie eine Test-Seite, um die neue Konfiguration zu prüfen. Schlägt der Test fehl, wurde unter Umständen kein Druckertreiber für den Remote-Drucker konfiguriert. Versuchen Sie dann, einen Druckertreiber für den Hersteller und das Modell des Remote-Druckers auszuwählen, die Änderungen anzunehmen und dann eine Test-Seite zu drucken.

Tipp

Sie können einen anderen Druckertreiber nach dem Hinzufügen eines Druckers auswählen, indem Sie das **Printer Configuration Tool** starten, den Drucker aus der Liste auswählen, auf **Bearbeiten** klicken, dann auf den Reiter **Treiber** klicken, hier einen anderen Druckertreiber auswählen und die Änderungen übernehmen.

36.7.1. Druckerkonfiguration bestätigen

Der letzte Schritt besteht im Bestätigen der Druckerkonfiguration. Klicken Sie auf **Übernehmen**, um die Druckerwarteschlange hinzuzufügen, wenn die Einstellungen richtig sind. Klicken Sie auf **Zurück**, um die Druckerkonfiguration zu ändern.

Klicken Sie im Hauptfenster auf den Button **Übernehmen**, um die Änderungen zu speichern und den Drucker-Daemon neu zu starten. Nach dem Übernehmen der Änderungen sollten Sie eine Test-Seite drucken, um sicherzustellen, dass die Konfiguration richtig ist. Weitere Informationen finden Sie unter Abschnitt 36.8.

Wenn Sie mehr Zeichen als den Basis-ASCII-Satz drucken müssen (einschließlich derjenigen, die für Sprachen wie Japanisch verwendet werden), müssen Sie die Treiberoptionen abrufen und **Prerender Postscript** auswählen. Weitere Informationen finden Sie unter Abschnitt 36.9. Sie können auch Optionen wie zum Beispiel Papiergröße konfigurieren, wenn Sie die Druckerwarteschlange nach dem Hinzufügen bearbeiten.

36.8. Eine Testseite drucken

Nach dem Konfigurieren des Druckers sollten Sie eine Testseite drucken, um sicherzustellen, dass der Drucker korrekt funktioniert. Um eine Testseite zu drucken, müssen Sie den Drucker, den Sie testen möchten, in der Druckerliste auswählen und die geeignete Testseite aus dem Pull-Down-Menü **Test** auswählen.

Wenn Sie den Druckertreiber oder die Treiberoptionen ändern, sollten Sie eine Testseite drucken, um die geänderte Konfiguration zu testen.

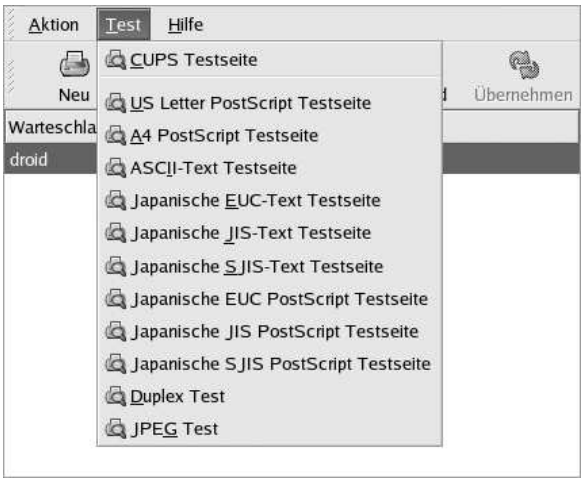

Abbildung 36-11. Testseiten-Optionen

36.9. Vorhandene Drucker ändern

Wählen Sie zum Löschen eines vorhandenen Druckers den jeweiligen Drucker aus und klicken Sie auf der Symbolleiste auf den Button **Löschen**. Der Drucker wird aus der Druckerliste entfernt. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern und den Drucker-Daemon neu zu starten.

Um den Standard-Drucker zu setzen, wählen Sie den Drucker aus der Liste und klicken Sie auf die Schaltfläche **Standard** auf der Werkzeugleiste. Das Symbol für den Standard-Drucker ✔ erscheint in der Spalte **Standard** des Standard-Druckers. Ein IPP-Drucker mit durchgesehener Warteschlange kann nicht als Standard-Drucker in **Printer Configuration Tool** verwendet werden. Um einen IPP-Drucker zum Standard zu machen, fügen Sie diesen entweder wie in Abschnitt 36.2 beschrieben hinzu und markieren diesen als Standard, oder benutzen Sie den **GNOME Print Manager**, um diesen als Standard zu setzen. Um **GNOME Printer Manager** zu starten, wählen Sie **Hauptmenü => Systemtools => Druck-Manager**. Klicken Sie mit der rechten Maustaste auf den Warteschlangennamen,

und wählen Sie **Als Default setzen**. Das Setzen des Standard-Druckers im **GNOME Print Manager** ändert lediglich den Standard-Drucker für den Benutzer, der diesen konfiguriert; dies ist keine System-weite Einstellung.

Nachdem Sie die Drucker hinzugefügt haben, können Sie die Einstellungen bearbeiten, indem Sie den Drucker aus der Druckerliste auswählen und auf den Button **Bearbeiten** klicken. Das unter Abbildung 36-12 abgebildete Fenster wird angezeigt. Das Fenster enthält die aktuellen Werte für den ausgewählten Drucker. Nehmen Sie die Änderungen vor und klicken Sie auf **OK**. Klicken Sie auf **Übernehmen** im Hauptfenster vom **Printer Configuration Tool**, um die Änderungen zu speichern und den Drucker-Daemon neu zu starten.

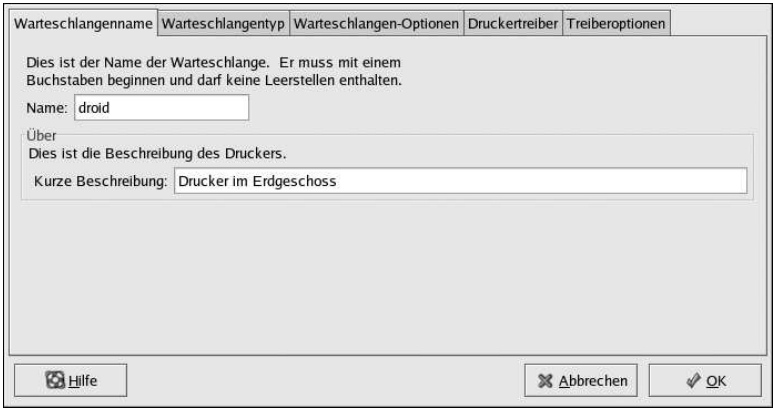

Abbildung 36-12. Bearbeiten eines Druckers

36.9.1. Warteschlangenname

Wenn Sie einen Drucker umbenennen oder dessen Kurzbeschreibung ändern möchten, ändern Sie einfach den Wert unter **Warteschlangenname**. Klicken Sie auf **OK**, um zum Hauptfenster zurückzukehren. Der Name des Druckers sollte sich in der Druckerliste ändern. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern und den Drucker-Daemon neu zu starten.

36.9.2. Warteschlangentyp

Warteschlangentyp zeigt den Warteschlangentyp, der beim Hinzufügen des Druckers ausgewählt wurde, und dessen Einstellungen. Sie können den Warteschlangentyp des Druckers oder nur die Einstellungen ändern. Nachdem Sie die Änderungen vorgenommen haben, klicken Sie auf **OK**, um zum Hauptfenster zurückzukehren. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern und den Drucker-Daemon neu zu starten.

Je nach ausgewähltem Warteschlangentyp werden verschiedene Optionen angezeigt. Im entsprechenden Abschnitt zum Hinzufügen eines Druckers finden Sie eine Beschreibung der Optionen.

36.9.3. Druckertreiber

Druckertreiber zeigt an, welcher Druckertreiber gerade verwendet wird. Wird dieser geändert, klicken Sie auf **OK**, um zum Hauptfenster zurückzukehren. Klicken Sie auf **Übernehmen**, um die Änderung zu speichern und den Drucker-Daemon zu neu zu starten.

36.9.4. Treiberoptionen

Treiberoptionen zeigt erweiterte Druckeroptionen an. Die Optionen variieren je nach Druckertreiber. Die am häufigsten verwendeten Optionen sind folgende:

- **Prerender Postscript** sollte ausgewählt werden, wenn Sie andere als im Basis-ASCII-Satz vorhandene Zeichen drucken, diese aber nicht korrekt gedruckt werden (wie zum Beispiel japanische Zeichen). Diese Option passt die nicht standardmäßigen PostScript-Fonts an, so dass diese richtig gedruckt werden.

  Wenn Ihr Drucker die zu druckenden Fonts nicht unterstützt, versuchen Sie es mit dieser Option. Sie sollten zum Beispiel diese Option auswählen, wenn Sie japanische Fonts mit einem nicht-japanischen Drucker drucken möchten.

  Das Durchführen dieser Aktion erfordert etwas Zeit. Führen Sie dies nur aus, wenn Sie beim Drucken der Schriften auf Probleme stoßen.

  Sie sollten diese Option auch dann auswählen, wenn Ihr Drucker mit dem PostScript Stufe 3, nicht arbeiten kann. Diese Option wandelt es in PostScript Stufe 1 um.
- **GhostScript pre-filtering** — Sie können **No pre-filtering** (Nicht vorfiltern), **Convert to PS level 1** (Zu PS Stufe 1 umwandeln) oder **Convert to PS level 2** (Zu PS Stufe 2 umwandeln) wählen, wenn der Drucker bestimmte PostScript Stufen nicht bearbeiten kann. Diese Option ist nur verfügbar, wenn der PostScript-Treiber verwendet wird.
- Mit **Seitengröße** können Sie das Seitenformat für Ihren Drucker wie US Letter, US Legal, A3 und A4 auswählen.
- **Effective Filter Locale** schlägt standardmäßig **C** vor. Wenn Sie japanische Zeichen drucken, sollten Sie **ja_JP** auswählen. Übernehmen Sie andernfalls den Standardwert **C**.
- **Media Source** (Medien-Quelle) ist standardmäßig der **Druckerstandard**. Ändern Sie diese Option, um die Papierzufuhr auf einen anderen Schacht umzustellen.

Nachdem Sie die Treiberoptionen geändert haben, klicken Sie auf **OK**, um zum Hauptfenster zurückzukehren. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern und den Drucker-Daemon neu zu starten.

36.10. Konfigurationsdatei speichern

Wenn Sie Ihre Druckerkonfiguration mit Hilfe vom **Printer Configuration Tool** speichern, erstellt die Anwendung ihre eigene Konfigurationsdatei, die zum Erstellen der Dateien im `/etc/cups` Verzeichnis verwendet wird. Sie können die Befehlszeilenoptionen zum Speichern oder Wiederherstellen der **Printer Configuration Tool** Datei verwenden. Wenn Sie das Verzeichnis `/etc/cups` oder die Datei `/etc/printcap` speichern und damit diese im gleichen Speicherort wiederherstellen, kann die Druckerkonfiguration nicht wiederhergestellt werden, da jedes Mal, wenn der Drucker-Daemon neu gestartet wird, eine neue `/etc/printcap` Datei aus der **Printer Configuration Tool** Konfigurationsdatei erstellt wird. Wenn Sie ein Backup der Konfigurationsdateien des System erstellt haben, sollten Sie mit der folgenden Methode die Konfigurationsdateien des Druckers speichern.

Um die Druckerkonfiguration zu speichern, geben Sie folgenden Befehl als root ein:

```
/usr/sbin/redhat-config-printer-tui --Xexport > settings.xml
```

Ihre Konfiguration wird in der Datei `settings.xml` gespeichert.

Wenn Sie diese Datei speichern, können Sie Ihre Druckereinstellungen wiederherstellen. Dies ist hilfreich, wenn Ihre Druckerkonfiguration gelöscht wird, Sie Red Hat Enterprise Linux neu installieren oder dieselbe Druckerkonfiguration auf mehreren System verwenden möchten. Die Datei sollte vor

dem Neuinstallieren auf einem anderen System gespeichert werden. Um die Konfiguration wiederherzustellen, geben Sie folgenden Befehl als root ein:

```
/usr/sbin/redhat-config-printer-tui --Ximport < settings.xml
```

Wenn Sie bereits über eine Konfigurationsdatei verfügen (Sie haben bereits einen oder mehrere Drucker auf dem System konfiguriert) und eine andere Konfigurationsdatei importieren möchten, wird die vorhandene Konfigurationsdatei überschrieben. Wenn Sie die vorhandene Konfiguration beibehalten und die Konfiguration zur gespeicherten Datei hinzufügen möchten, können Sie die Dateien mit dem folgendem Befehl (als root) zusammenführen:

```
/usr/sbin/redhat-config-printer-tui --Ximport --merge < settings.xml
```

Ihre Druckerliste enthält dann die Drucker, die Sie auf dem System konfiguriert haben, und die Drucker, die aus der gespeicherten Konfigurationsdatei importiert wurden. Wenn die importierte Konfigurationsdatei über eine Druckerwarteschlange mit demselben Namen wie eine auf dem System vorhandene Druckerwarteschlange verfügt, überschreibt die Warteschlange der importierten Datei den vorhandenen Drucker.

Nach dem Import der Konfigurationsdatei (mit oder ohne den Befehl `merge`) müssen Sie den Drucker-Daemon neu starten. Wenn Sie CUPS verwenden, geben Sie den folgenden Befehl ein:

```
/sbin/service cups restart
```

36.11. Befehlszeilen-Konfiguration

Wen X nicht installiert ist und Sie die textbasierte Version nicht verwenden möchten, können Sie anhand der Befehlszeile einen Drucker hinzufügen. Diese Methode ist nützlich, wenn Sie einen Drucker von einem Skript aus oder über die %post Sektion einer Kickstart-Installation hinzufügen möchten.

36.11.1. Hinzufügen eines lokalen Druckers

Um einen Drucker hinzuzufügen:

```
redhat-config-printer-tui --Xadd-local options
```

Optionen:

--device=*Knoten*

(Erforderlich) Der zu verwendende Geräteknoten, z.B. `/dev/lp0`.

--make=*Erstellen*

(Erforderlich) Der IEEE 1284 HERSTELLER-String oder der Name des Druckerherstellers wie in der Foomatic-Datenbank angegeben, wenn der String des Herstellers nicht verfügbar ist.

--model=*Modell*

(Erforderlich) Der IEEE 1284 MODELL-String oder das Druckermodell aus der Foomatic-Datenbank, wenn der Modell-String nicht verfügbar ist.

--name=*Name*

(Optional) Name, der der neuen Schlange gegeben werden soll. Wird keiner vergeben, wird ein auf dem Geräteknoten basierender Name verwendet (wie z.B. „lp0“).

--as-default

(Optional) Dies als Standardschlange einrichten.

Geben Sie nach dem Hinzufügen des Druckers den folgenden Befehl zum Starten/Neustarten des Drucker-Daemons ein:

```
service cups restart
```

36.11.2. Löschen eines lokalen Druckers

Eine Druckerschlange kann auch über eine Befehlszeile gelöscht werden.

Geben Sie als root angemeldet folgendes zum Löschen einer Druckerschlange ein:

```
redhat-config-printer-tui --Xremove-local options
```

Optionen:

--device=*Knoten*

(Erforderlich) Der verwendete Geräteknoten (zum Beispiel `/dev/lp0`).

--make=*Erstellen*

(Erforderlich) Der IEEE 1284 HERSTELLER-String oder (wenn nicht vorhanden) der Name des Druckerherstellers, wie in der Foomatic-Datenbank angegeben.

--model=*Modell*

(Erforderlich) Der IEEE 1284 MODELL-String oder (wenn nicht vorhanden) das Druckermodell, wie in der Foomatic-Datenbank angegeben.

Starten Sie nach dem Löschen des Druckers aus der **Printer Configuration Tool** Konfiguration den Drucker-Daemon neu, damit die Änderungen wirksam werden:

```
service cups restart
```

Wenn Sie alle Drucker gelöscht haben, und den Drucker-Daemon nicht weiter verwenden möchten, geben Sie den folgenden Befehl ein:

```
service cups stop
```

36.11.3. Setzen des Standard-Druckers

Um den Standard-Drucker zu setzen, benutzen Sie den folgenden Befehl und geben Sie den *queuename* an:

```
redhat-config-printer-tui --Xdefault --queue=queuename
```

36.12. Druckaufträge verwalten

Wenn Sie einen Druckerjob an den Druckerdaemon senden, wie zum Beispiel zum Drucken einer Textdatei aus **Emacs** oder zum Drucken eines Bildes aus **The GIMP**, wird der Druckauftrag zur Warteschlange des Druckerspooler hinzugefügt. Die Warteschlange des Druckerspooler ist eine Liste mit

Druckaufträgen, die an den Drucker gesendet wurden, sowie Informationen über jeden Druckauftrag wie zum Beispiel den Auftragsstatus, den Benutzernamen der Person, die den Auftrag sendete, den Hostnamen des Systems, das den Auftrag sendete, die Jobnummer u.v.m.

Wenn Sie mit der grafischen Desktopumgebung arbeiten, klicken Sie auf **Printer Manager** auf dem Panel, um den **GNOME Print Manager** wie in Abbildung 36-13 gezeigt zu öffnen.

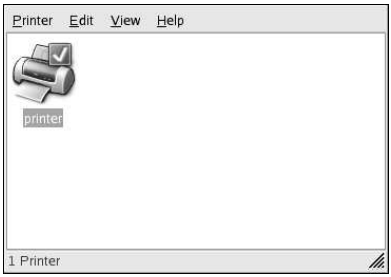

Abbildung 36-13. GNOME Print Manager

Diese Applikation kann auch durch **Hauptmenü** (im Panel) => **Systemeinstellungen** => **Print Manager** geöffnet werden.

Um die Druckeinstellungen zu ändern, klicken Sie mit der rechten Maustaste auf das Symbol für den Drucker und wählen Sie dann **Eigenschaften**. Das **Printer Configuration Tool** wird daraufhin gestartet.

Doppelklicken Sie auf den konfigurierten Drucker, um sich die Druckerspooler-Warteschlange anzeigen zu lassen, wie in Abbildung 36-14 abgebildet.

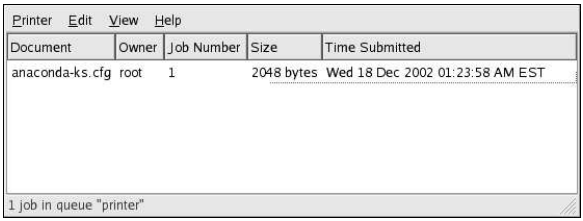

Abbildung 36-14. Liste der Druckaufträge

Wenn Sie einen Druckauftrag in **GNOME Print Manager** abbrechen möchten, wählen Sie diesen aus der Liste aus und wählen Sie aus dem Pull-Down-Menü **Edit** => **Cancel**.

Wenn sich aktive Druckaufträge im Druckspooler befinden, erscheint ein Druckbenachrichtigungs-Symbol in der **Panel Notification Area** des Desktop-Panels, wie in Abbildung 36-15 abgebildet. Da dieser alle 5 Sekunden nach aktiven Druckaufträgen sucht, wird dieses Symbol unter Umständen nicht für kurze Druckaufträge angezeigt.

Abbildung 36-15. Printer Notification Icon

Wenn Sie auf das Printer Notification Icon klicken, wird der **GNOME Print Manager** gestartet, und zeigt eine Liste der aktuellen Aufträge an.

Auf dem Panel befindet sich außerdem ein Symbol für den **Print Manager**. Um eine Datei aus **Nautilus** zu drucken, gehen Sie zum Speicherort der Datei und ziehen Sie diese auf das **Print Manager** Symbol im Panel (drag und drop). Das Fenster wie in Abbildung 36-16 gezeigt erscheint. Klicken Sie auf **OK**, um diese Datei zu drucken.

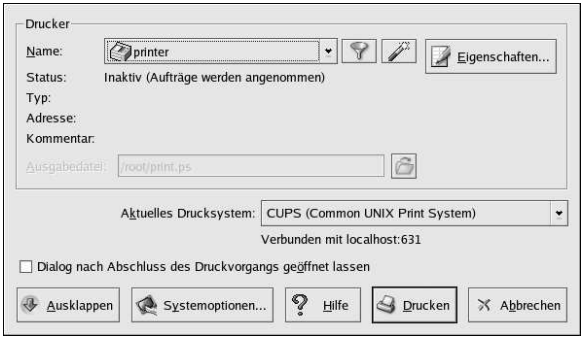

Abbildung 36-16. Print Verification Fenster

Um die Liste der Druckaufträge im Druckerspooler vom Shell-Prompt aus anzuzeigen, geben Sie den Befehl `lpq` ein. Die letzten Zeilen sehen dann wie folgt oder ähnlich aus:

```
Rank    Owner/ID            Class  Job Files       Size Time
active user@localhost+902     A    902 sample.txt  2050 01:20:46
```

Beispiel 36-1. Beispiel der Ausgabe mit `lpq`

Wenn Sie einen Druckerjob abbrechen möchten, müssen Sie die Jobnummer des Auftrags mit dem Befehl `lpq` suchen und dann den Befehl `lprm` *`job number`* verwenden. Zum Beispiel: Mit `lprm 902` wird der Druckauftrag in Beispiel 36-1 abgebrochen. Sie müssen über Berechtigungen zum Abbrechen eines Druckauftrags verfügen. Sie können Druckaufträge, die von einem anderen Benutzer gestartet wurden, nicht abbrechen, es sei denn, Sie sind als root an dem Rechner angemeldet, an den der Drucker angeschlossen ist.

Sie können eine Datei auch direkt von einem Shell-Prompt aus drucken. So druckt zum Beispiel der Befehl `lpr sample.txt` die Textdatei `sample.txt`. Der Druckerfilter legt den Dateityp fest und konvertiert die Datei in ein für den Drucker lesbares Format.

36.13. Drucker gemeinsam verwenden

Die Fähigkeit des **Printer Configuration Tool** für das gemeinsame Verwenden von Konfigurationsoptionen kann nur unter CUPS Drucksystem verwendet werden.

Wenn Sie anderen Benutzern an einem anderen Rechner im Netzwerk erlauben, auf einem Drucker, der für Ihr System konfiguriert ist, zu drucken, wird dies als *Sharing* (gemeinsames Verwenden) des Druckers bezeichnet. Standardmäßig können mit **Printer Configuration Tool** konfigurierte Drucker nicht geteilt werden.

Um einen konfigurierten Drucker gemeinsam nutzen zu können, starten Sie **Printer Configuration Tool** und wählen Sie einen Drucker aus der Liste aus. Wählen Sie dann **Aktion => Sharing** aus dem Pull-Down-Menü.

Anmerkung

Wird kein Drucker ausgewählt, zeigt **Aktion => Sharing** nur die systemweiten Sharing-Optionen, die normalerweise unter **Allgemein** angezeigt werden.

Wählen Sie unter **Warteschlange** die Option, die die Schlange anderen Benutzern zur Verfügung stellt.

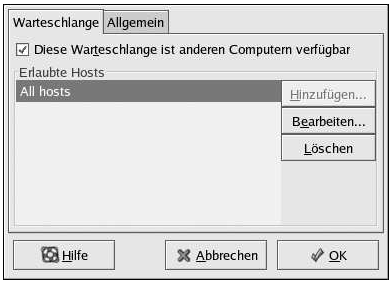

Abbildung 36-17. Warteschlangenoptionen

Nachdem Sie das Teilen der Warteschlange ausgewählt haben, werden standardmäßig *alle* Hosts zum Drucken über den gemeinsamen Drucker zugelassen. Allen Systemen im Netzwerk das Drucken auf dieser Warteschlange zu erlauben kann ein Sicherheitsrisiko darstellen, insbesondere, wenn das System direkt mit dem Internet verbunden ist. Es wird empfohlen, diese Option zu ändern, indem Sie den Eintrag **Alle Hosts** markieren und dann auf **Bearbeiten** klicken, um das in Abbildung 36-18 gezeigte Fenster zu öffnen.

Wenn Sie auf Ihrem Druckserver eine Firewall haben, muss diese in der Lage sein, Verbindungen auf dem Eingangsport 631 senden und empfangen zu können. Wenn Sie eine Firewall auf dem Client haben (der Computer, der die Druckanfrage sendet), muss diese Verbindungen auf dem Port 631 akzeptieren und senden können.

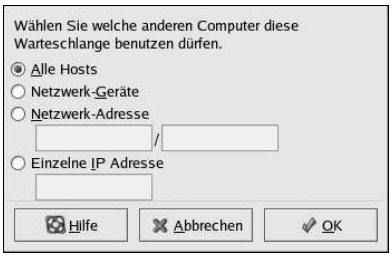

Abbildung 36-18. Zugelassene Hosts

Der Reiter **Allgemein** konfiguriert Einstellungen für alle Drucker, inklusive derer, die nicht über **Printer Configuration Tool** angezeigt werden. Es gibt zwei Möglichkeiten:

- **Gemeinsame Remote-Warteschlangen automatisch finden** — Als Standard eingestellt aktiviert diese Option das IPP-Browsing, d.h. wenn andere Computer im Netzwerk deren Warteschlangen bekanntgeben, werden diese automatisch zu der Druckerliste im System hinzugefügt. Es ist keine zusätzliche Konfiguration für einen durch IPP-Browsing gefundenen Drucker notwendig. Diese Option teilt jedoch nicht automatisch Drucker im lokalen System.
- **LPD Protokoll aktivieren** — Mit dieser Option kann der Drucker Druckaufträge von Clients, die für die Verwendung des LPD-Protokolls mittels `cups-lpd` (ein `xinetd` Service) konfiguriert wurden, empfangen.

Warnung

Wenn diese Option aktiviert ist, werden alle Druckaufträge aller Hosts angenommen, wenn diese durch einen LPD-Client empfangen wurden.

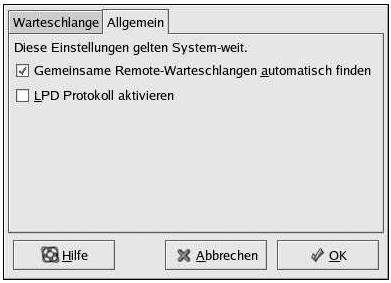

Abbildung 36-19. System-weite Sharing Optionen

36.14. Zusätzliche Ressourcen

Weitere Informationen über das Drucken unter Red Hat Enterprise Linux finden Sie in den folgenden Ressourcen.

36.14.1. Installierte Dokumentation

- `map lpr` — Die man-Seite für den Befehl `lpr`, mit dem Sie Dateien von der Befehlszeile aus drucken können.
- `man lprm` — Die man-Seite über das Befehlszeilen-Dienstprogramm zum Entfernen von Druckaufträgen aus der Druck-Warteschlange.
- `man mpage` — Die man-Seite über das Befehlszeilen-Dienstprogramm zum Drucken mehrerer Seiten auf einem Blatt Papier.
- `man cupsd` — Die man-Seite für den CUPS-Druckerdaemon.
- `man cupsd.conf` — Die man-Seite für die Konfigurationsdatei des CUPS-Drucker-Daemons.
- `man classes.conf` — Die man-Seite für die Klassenkonfigurationsdatei für CUPS.

36.14.2. Hilfreiche Websites

- http://www.linuxprinting.org — *GNU/Linux Printing* enthält sehr viele Informationen zum Drucken in Linux.
- http://www.cups.org/ — Dokumentation, häufig gestellte Fragen (FAQs) und Newsgroups zu CUPS.

Kapitel 37.

Automatisierte Tasks

In Linux können Tasks automatisch innerhalb eines bestimmten Zeitraums, zu einem bestimmten Zeitpunkt oder wenn die Systemlast unterhalb eines bestimmten Wertes liegt, ausgeführt werden. Red Hat Enterprise Linux ist so vorkonfiguriert, dass wichtige Systemtasks ausgeführt werden, um Ihr System stets auf dem neuesten Stand zu halten. So wird zum Beispiel die slocate-Datenbank, die von dem Befehl `locate` verwendet wird, täglich aktualisiert. Ein Systemadministrator kann automatisierte Tasks zum Durchführen von regelmäßigen Backups, zur Systemüberwachung, zum Ausführen von benutzerdefinierten Skripten und vielem mehr verwenden.

Red Hat Enterprise Linux bietet vier automatische Tasks: `cron`, `anacron`, `at` und `batch`.

37.1. Cron

Cron ist ein Daemon zum Ausführen wiederkehrender Tasks nach einer festgelegten Kombination aus Zeit, Kalendertag, Monat, Wochentag und Woche.

Cron geht davon aus, dass das System kontinuierlich läuft. Ist das System zum Zeitpunkt der Ausführung eines Tasks heruntergefahren, wird dieser Task nicht ausgeführt. Informationen zum Ausführen einmaliger Tasks finden Sie unter Abschnitt 37.2.

Für die Verwendung von Cron muss das RPM-Paket `vixie-cron` installiert sein und der `crond` Service laufen. Mit dem Befehl `rpm -q vixie-cron` können Sie feststellen, ob das Paket installiert ist. Um festzustellen, ob der Dienst ausgeführt wird, verwenden Sie den Befehl `/sbin/service crond status`.

37.1.1. Konfigurieren von Cron-Tasks

Die Hauptkonfigurationsdatei für Cron `/etc/crontab` enthält die folgenden Zeilen:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

Die ersten vier Zeilen sind Variablen, die zum Konfigurieren der Umgebung verwendet werden, in der die Cron-Tasks ausgeführt werden. Der Wert der Variable `SHELL` teilt dem System mit, welche Shell-Umgebung zu verwenden ist (hier zum Beispiel Bash-Shell) und die Variable `PATH` definiert den zum Ausführen der Befehle verwendeten Pfad. Die Ausgabe der Cron-Tasks werden per E-Mail an den Benutzernamen gesendet, der mit Hilfe der Variable `MAILTO` definiert wurde. Wurde die Variable `MAILTO` als leere Zeichenfolge (`MAILTO=""`) definiert, wird keine E-Mail gesendet. Die Variable `HOME` kann zum Festlegen des home-Verzeichnisses zum Ausführen von Befehlen oder Skripten verwendet werden.

Jede Zeile der Datei `/etc/crontab` steht für einen Task und hat folgendes Format:

```
minute   hour   day   month   dayofweek   command
```

- `minute` — jede beliebige ganze Zahl von 0 bis 59
- `hour` — jede beliebige ganze Zahl von 0 bis 23
- `day` — jede beliebige ganze Zahl von 1 bis 31 (wurde ein Monat angegeben, muss der Tag gültig sein)
- `month` — jede beliebige ganze Zahl von 1 bis 12 (oder die englische Abkürzung des Monatsnamens, z.B. Jan, Feb, etc.)
- `dayofweek` — jede beliebige ganze Zahl von 0 bis 7. 0 oder 7 stehen für Sonntag (oder die englische Abkürzung der Wochentage, z.B. Sun, Mon, etc.)
- `command` — der auszuführende Befehl (der Befehl kann entweder ein Befehl wie z.B. `ls /proc >> /tmp/proc` oder ein Befehl zum Ausführen eines benutzerdefinierten Skriptes sein.)

Für alle oben angegebenen Werte kann der Stern (*) verwendet werden, um alle gültigen Werte anzugeben. Wenn Sie zum Beispiel den Stern für den Monatswert eingeben wird der Befehl jeden Monat innerhalb der Einschränkungen der anderen Werte ausgeführt.

Ein Bindestrich (-) zwischen den ganzen Zahlen gibt den Bereich von ganzen Zahlen an. **`1-4`** steht zum Beispiel für die ganzen Zahlen 1, 2, 3 und 4.

Durch Kommata getrennte Werte (,) geben eine Liste an. **`3, 4, 6, 8`** gibt zum Beispiel diese vier ganzen Zahlen an.

Der Schrägstrich (/) kann zum Angeben von Schrittwerten verwendet werden. Der Wert einer ganzen Zahl kann in einem Bereich durch **`/`***`<Ganze Zahl>`* übersprungen werden. **`0-59/2`** kann zum Beispiel zum Definieren bzw. Überspringen jeder weiteren (zweiten) Minute im Feld minute (Minute) verwendet werden. Schrittwerte können auch mit dem Stern verwendet werden. Der Wert **`*/3`** kann zum Beispiel im Feld month (Monat) verwendet werden, um den Task in jedem dritten Monat auszuführen.

Alle Zeilen, die mit einem Nummernzeichen (Hash) (#) beginnen, sind Kommentare und werden nicht verarbeitet.

Wie an der Datei `/etc/crontab` zu erkennen ist, verwendet sie das Skript `run-parts`, um die Skripte in den Verzeichnissen `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly` stündlich, täglich, wöchentlich oder monatlich auszuführen. Die Dateien in diesem Verzeichnis sollten Shell-Skripte sein.

Wenn ein Cron-Task nicht stündlich, täglich, wöchentlich oder monatlich ausgeführt werden soll, kann er dem Verzeichnis `/etc/cron.d` hinzugefügt werden. Alle Dateien in diesem Verzeichnis verwenden die gleiche Syntax wie `/etc/crontab`. Weitere Beispiele finden Sie unter Beispiel 37-1.

```
# record the memory usage of the system every monday
# at 3:30AM in the file /tmp/meminfo
30 3 * * mon cat /proc/meminfo >> /tmp/meminfo
# run custom script the first day of every month at 4:10AM
10 4 1 * * /root/scripts/backup.sh
```

Beispiel 37-1. Beispiele für crontabs

Wenn Sie nicht als Root angemeldet sind, können Sie Cron-Tasks mit dem Dienstprogramm `crontab` konfigurieren. Alle benutzerdefinierten Crontabs werden im Verzeichnis `/var/spool/cron` gespeichert und mit Hilfe der Benutzernamen der Benutzers ausgeführt, die die jeweiligen Crontabs erstellt haben. Um einen Crontab als Benutzer zu erstellen, melden Sie sich als Benutzer an und geben Sie den Befehl `crontab -e` ein, um diesen Crontab mit Hilfe des von der Umgebungsvariable `VISUAL` oder `EDITOR` definierten Editors zu bearbeiten. Die Datei verwendet das gleiche Format wie `/etc/crontab`. Wenn die an Crontab vorgenommenen Änderungen gespeichert werden, wird der Crontab entsprechend dem Benutzernamen gespeichert und in die Datei `/var/spool/cron/`*`Benutzername`* geschrieben.

Der Cron-Daemon überprüft minütlich die Datei `/etc/crontab`, das Verzeichnis `/etc/cron.d/` und das Verzeichnis `/var/spool/cron` auf Änderungen. Werden Änderungen erkannt, werden diese in den Speicher geladen. Wenn also eine Crontab-Datei geändert wird, muss der Daemon nicht erneut gestartet werden.

37.1.2. Zugriffskontrolle auf Cron

Die Dateien `/etc/cron.allow` und `/etc/cron.deny` schränken den Zugriff auf Cron ein. In jeder Zeile der beiden Zugriffskontroll-Dateien steht ein Benutzername. Es dürfen keine Leerstellen in diesen beiden Dateien verwendet werden. Der Cron-Daemon (`crond`) muss nicht erneut gestartet werden, wenn die Zugriffskontroll-Dateien geändert wurden. Die Zugriffskontroll-Dateien werden immer dann gelesen, wenn der Benutzer einen Cron-Task hinzuzufügen oder zu löschen versucht.

Der root-Benutzer kann Cron immer verwenden, unabhängig von den in den Zugriffskontroll-Dateien aufgelisteten Benutzernamen.

Wenn die Datei `cron.allow` vorhanden ist, können nur die in dieser Datei aufgelisteten Benutzer Cron verwenden, und die Datei `cron.deny` wird ignoriert.

Wenn die Datei `cron.allow` nicht vorhanden ist, kann keiner der in `cron.deny` aufgelisteten Benutzer Cron verwenden.

37.1.3. Starten und Beenden des Dienstes

Verwenden Sie zum Starten des Cron-Dienstes den Befehl `/sbin/service crond start` und zum Beenden den Befehl `/sbin/service crond stop`. Es wird empfohlen, den Dienst beim Booten zu starten. Weitere Informationen zum automatischen Starten des Cron-Dienstes beim Booten finden Sie unter Kapitel 21.

37.2. At und Batch

Während mit Cron und Anacron wiederkehrende Tasks geplant werden, wird mit dem Befehl `at` eine einmalige Aufgabe zu einer bestimmten Zeit geplant. Der Befehl `batch` wird zur Planung eines einmaligen Tasks verwendet, der ausgeführt wird, wenn die durchschnittliche Belastung des Systems unter 0.8 liegt.

Um `at` oder `batch` verwenden zu können, muss das `at` RPM Paket installiert und der `atd` Dienst ausgeführt werden. Mit dem Befehl `rpm -q at` können Sie feststellen, ob das Paket installiert wurde, und mit dem Befehl `/sbin/service atd status` stellen Sie fest, ob der Dienst ausgeführt wird.

37.2.1. Konfigurieren von At-Jobs

Um einen einmaligen Job zu einem bestimmten Zeitpunkt zu planen, geben Sie den Befehl `at` *`time`* ein, wobei *`time`* der Zeitpunkt ist, an dem der Befehl ausgeführt werden soll.

Das Argument *`time`* kann wie folgt aussehen:

- HH:MM format — z.B. 04:00 bedeutet 4:00 morgens. Ist dieser Zeitpunkt bereits verstrichen, wird der Job am nächsten Tag zur angegebenen Zeit ausgeführt.
- midnight — bedeutet 24:00 Uhr (Mitternacht).
- noon — bedeutet 12:00 Uhr (Mittag).
- teatime — bedeutet 16:00 Uhr.

- month-name day year format — zum Beispiel January 15 2002 bedeutet der 15. Tag im Januar des Jahres 2002. Das Jahr kann, muss aber nicht angegeben werden.
- MMDDYY, MM/DD/YY, or MM.DD.YY formats — z.B. 011502 für den 15. Tag im Januar des Jahres 2002 (Amerikanisches Datumsformat).
- now + time — Zeit in Minuten, Stunden, Tagen oder Wochen. Z.B. bedeutet now (jetzt) + 5 Tage, dass der Befehl in fünf Tagen zur gleichen Zeit ausgeführt wird.

Es muss zuerst die Zeit und anschließend das fakultative Datum festgelegt werden. Weitere Informationen über das Zeitformat finden Sie in der `/usr/share/doc/at-<version>/timespec` Textdatei.

Nach der Eingabe des Befehls `at` und des Zeit- arguments erscheint der `at>` Prompt. Geben Sie den Befehl ein, drücken Sie die [Enter-Taste], und geben Sie anschließend Strg-D ein. Es können mehrere Befehle festgelegt werden, indem Sie nach jedem eingegebenen Befehl die [Enter-Taste] drücken. Nachdem Sie alle Befehle eingegeben haben und die [Enter-Taste] gedrückt haben, geben Sie in einer leeren Zeile Strg-D ein. Alternativ kann ein Shell-Skript am Prompt eingegeben werden, indem nach jeder Zeile im Skript die [Enter-Taste] gedrückt und zum Beenden Strg-D in eine leere Zeile eingegeben wird. Ist ein Skript eingegeben, ist die verwendete Shell die Shell, die in der SHELL Umgebung des Benutzers eingestellt ist, die Anmeldeshell des Benutzers oder `/bin/sh` (je nachdem, was zuerst gefunden wird).

Ausgaben der Befehle oder Skripten werden an den Benutzer gemailt.

Mit dem Befehl `atq` können Sie anstehende Jobs anzeigen. Im Abschnitt 37.2.3 finden Sie weitere Informationen.

Die Verwendung des Befehls `at` kann eingeschränkt werden. Im Abschnitt 37.2.5 finden Sie weitere Einzelheiten.

37.2.2. Konfigurieren von Batch Jobs

Um einmalige Tasks auszuführen, wenn die durchschnittliche Belastung des Systems unter 0.8 liegt, verwenden Sie den Befehl `batch` command.

Nach der Eingabe des Befehls `batch` erscheint der `at>` Prompt. Geben Sie den Befehl zum Ausführen ein, drücken Sie die [Enter-Taste] und geben Sie Strg-D ein. Es können mehrere Befehle festgelegt werden, indem Sie nach jedem eingegebenen Befehl die [Enter-Taste] drücken. Nachdem Sie alle Befehle eingegeben haben und die [Enter-Taste] gedrückt haben, geben Sie in einer leeren Zeile Strg-D ein. Alternativ kann ein Shell-Skript am Prompt eingegeben werden, indem nach jeder Zeile im Skript die [Enter-Taste] gedrückt und zum Beenden Strg-D in eine leere Zeile eingegeben wird. Ist ein Skript eingegeben, ist die verwendete Shell die Shell, die in der SHELL Umgebung des Benutzers eingestellt ist, die Anmeldeshell des Benutzers oder `/bin/sh` (je nachdem, was zuerst gefunden wird). Sobald die durchschnittliche Belastung des Systems unter 0.8 liegt, wird der Satz von Befehlen und Skripten ausgeführt.

Ausgaben der Befehle oder Skripten werden an den Benutzer gemailt.

Mit dem Befehl `atq` können Sie anstehende Jobs anzeigen. Im Abschnitt 37.2.3 finden Sie weitere Informationen.

Die Verwendung des Befehls `batch` kann eingeschränkt werden. Im Abschnitt 37.2.5 finden Sie weitere Einzelheiten.

37.2.3. Anzeigen von anstehenden Jobs

Um anstehende`at` und `batch` Jobs zu sehen, verwenden Sie den Befehl `atq`. Er zeigt eine Liste der anstehenden Jobs, wobei jeder einzelne Job in einer Zeile erscheint. Jede Zeile wird wie folgt

dargestellt: Jobnummer, Datum, Stunde, Jobklasse und Benutzername. Die Benutzer können nur ihre eigenen Jobs sehen. Führt ein root den Befehl `atq` aus, werden alle Jobs aller Benutzer angezeigt.

37.2.4. Zusätzliche Optionen der Befehlszeile

Zusätzliche Befehlszeilen-Optionen für `at` und `batch` enthalten:

Option	Beschreibung
`-f`	Liest die Befehle oder Shell-Skripten von einer Datei anstatt sie am Prompt festzulegen.
`-m`	Verschickt eine Mail an den Benutzer, wenn der Job abgeschlossen ist.
`-v`	Zeigt die Zeit an, wann der Job ausgeführt wird.

Tabelle 37-1. `at` und `batch` Befehlszeilen-Optionen

37.2.5. Zugriffskontrolle für At und Batch

Mit den Dateien `/etc/at.allow` und `/etc/at.deny` kann der Zugriff auf die Befehle `at` und `batch` eingeschränkt werden. In jeder Zeile dieser beiden Zugriffskontroll-Dateien steht ein Benutzername. Es dürfen in keiner der beiden Dateien Leerstellen eingegeben werden. Der `at` Daemon (`atd`) muss nicht erneut gestartet werden wenn die Zugriffskontroll-Dateien geändert wurden. Die Zugriffskontroll-Dateien werden immer dann gelesen, wenn der Benutzer versucht, den Befehl `at` oder `batch` auszuführen.

Die Befehle `at` und `batch` können jederzeit, unabhängig von den Zugriffskontroll-Dateien von einem root-Benutzer ausgeführt werden.

Wenn die Datei `at.allow` vorhanden ist, können nur die in dieser Datei aufgelisteten Benutzer die Befehle `at` oder `batch` ausführen, und die Datei `at.deny` wird ignoriert.

Ist die Datei `at.allow` nicht vorhanden, kann keiner der in der Datei `at.deny` aufgelisteten Benutzer die Befehle `at` oder `batch` verwenden.

37.2.6. Starten und Beenden des Dienstes

Um den `at` Dienst zu starten, verwenden Sie den Befehl `/sbin/service atd start`, um ihn zu beenden den Befehl `/sbin/service atd stop`. Es empfiehlt sich, den Dienst während des Bootens zu starten. Im Kapitel 21 finden Sie weitere Details über das automatische Starten des Cron-Dienstes während des Bootens.

37.3. Zusätzliche Ressourcen

Weitere Informationen über das Konfigurieren automatisierter Tasks finden Sie in folgenden Ressourcen.

37.3.1. Installierte Dokumentation

- `cron` man-Seite — Übersicht über Cron.

- `crontab` man-Seiten in Abschnitten 1 und 5 — Die man-Seite enthält in Abschnitt 1 eine Übersicht über die Datei `crontab`. Die man-Seite enthält in Abschnitt 5 das Format für die Datei und einige Beispieleinträge.
- `/usr/share/doc/at-`*`<version>`*`/timespec` enthält detaillierte Informationen über die festzulegenden Zeiten zur Ausführung von Cron-Jobs.
- `at` man-Seite — Beschreibung von `at` und `batch` sowie deren Befehlszeilen-Optionen.

redhat

Kapitel 38.
Log-Dateien

Log-Dateien sind Dateien, die Systemnachrichten enthalten, einschließlich Kernel, Dienste und Anwendungen. Unterschiedliche Informationen haben unterschiedliche Log-Dateien. Es gibt zum Beispiel eine Standard-Systemlogdatei, eine Log-Datei nur für Sicherheitsnachrichten und eine Log-Datei für Cron-Tasks.

Log-Dateien sind sehr nützlich, wenn Sie Probleme mit dem System lösen möchten, wie das Laden eines Kernel-Treibers oder wenn Sie nach nicht authorisierten Anmeldeversuchen im System suchen. Dieses Kapitel beschreibt, wie man Log-Dateien findet, wie diese angezeigt werden und nach was in Log-Dateien zu suchen ist.

Einige Log-Dateien werden von einem Daemon mit dem Namen `syslogd` kontrolliert. Eine Liste der Log-Nachrichten, die von `syslogd` gepflegt werden, finden Sie in der `/etc/syslog.conf` Konfigurationsdatei.

38.1. Lokalisieren von Log-Dateien

Die meisten Log-Dateien befinden sich im Verzeichnis `/var/log/`. Einige Anwendungen wie `httpd` und `samba` verfügen über ein Verzeichnis in `/var/log/` für ihre Log-Dateien.

Hinter vielen Dateien im Log-Dateien-Verzeichnis stehen Nummern. Diese entstehen bei der Rotation der Log-Dateien. Log-Dateien rotieren, damit sie nicht zu groß werden. Das Paket `logrotate` enthält einen Cron-Task, der Log-Dateien automatisch je nach `/etc/logrotate.conf` Konfigurationsdatei und den Konfigurationsdateien im Verzeichnis `/etc/logrotate.d/` rotiert. Standardmäßig bewirkt die Konfiguration, dass die Rotation jede Woche erfolgt und alte Log-Dateien vier Wochen lang aufbewahrt werden.

38.2. Log-Dateien anzeigen

Die meisten Log-Dateien sind in reinem Textformat. Sie können sie mit einem Text-Editor wie zum Beispiel **Vi** oder **Emacs** ansehen. Einige Log-Dateien können von allen Benutzern des Systems gelesen werden, für die meisten Dateien müssen Sie jedoch als root angemeldet sein.

Verwenden Sie **Log Viewer**, um System-Log-Dateien in einer interaktiven Echtzeit-Anwendung anzuzeigen. Starten Sie die Anwendung über den **Hauptmenü-Button** (auf dem Panel) => **System-Tools => System-Logs** oder geben Sie am Shell-Prompt den Befehl `redhat-logviewer` ein.

Die Anwendung zeigt nur vorhandene Log-Dateien an, d.h. Ihre Liste könnte sich von der in Abbildung 38-1 unterscheiden.

Um den Inhalt der Log-Datei nach Schlüsselwörtern zu filtern, geben Sie im Textfeld **Filtern nach** das Wort bzw. die Wörter ein nach denen Sie suchen und klicken Sie auf **Filtern**. Klicken Sie auf **Reset**, um den Inhalt zurückzusetzen.

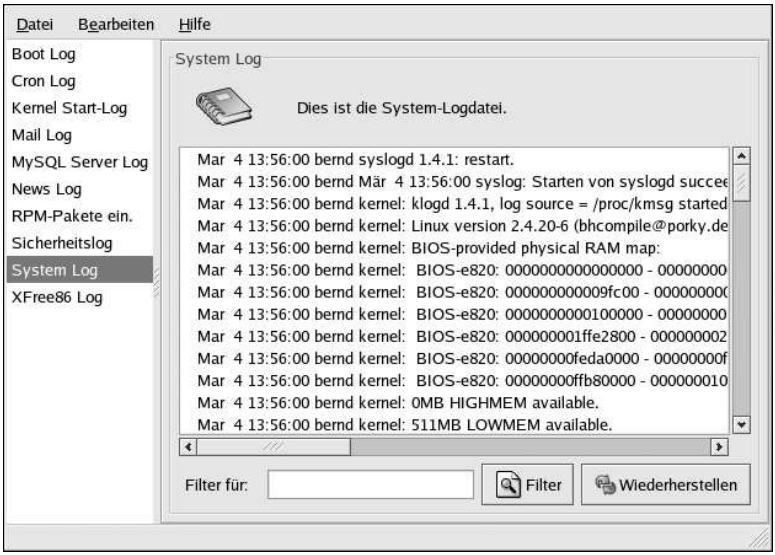

Abbildung 38-1. Log Viewer

Standardmäßig wird die derzeit angezeigte Log-Datei alle 30 Sekunden aufgefrischt. Um die Auffrischrate zu ändern, wählen Sie **Bearbeiten** => **Präferenzen** aus dem Pull-Down-Menü. Das in Abbildung 38-2 abgebildete Fenster erscheint. Klicken Sie im Tab **Log-Dateien** auf die Bildlaufpfeile neben der Auffrischungsrate, um diese zu ändern. Klicken Sie auf **Schließen**, um zum Hauptfenster zurückzukehren. Die Auffrischungsrate wird sofort geändert. Um die derzeit angezeigte Datei manuell aufzufrischen, wählen Sie **Datei** => **Jetzt auffrischen** oder drücken Sie [Strg]-[R].

Vom Tab **Log-Dateien** aus können Sie die Speicherstelle der Log-Datei ändern. Wählen Sie die Log-Datei aus der Liste und klicken Sie auf den Button **Speicherstelle ändern**. Geben Sie die neue Speicherstelle der Log-Datei ein oder klicken Sie auf den Button **Blättern** um die Datei-Speicherstelle anhand eines Dateiauswahldialogs ausfindig zu machen. Klicken Sie auf **OK** um zu den Präferenzen zurückzukehren und klicken Sie auf **Schließen** um zum Hauptfenster zurückzukehren.

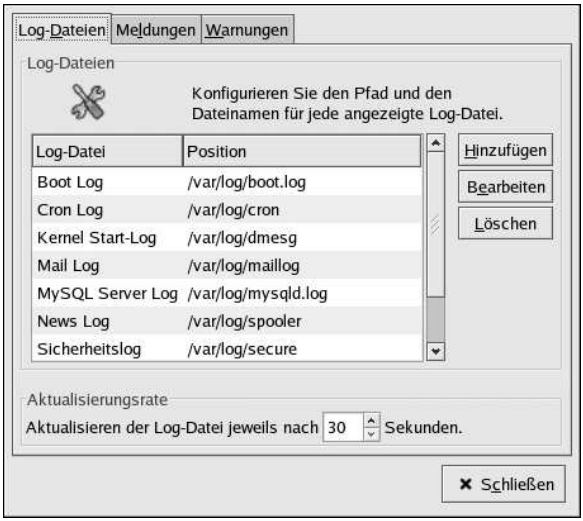

Abbildung 38-2. Log-Datei Speicherstelle

38.3. Log-Dateien hinzufügen

Um eine Log-Datei hinzuzufügen, wählen Sie **Beareiten** => **Präferenzen** und klicken Sie dann auf **Hinzufügen** im Tab **Log-Dateien**.

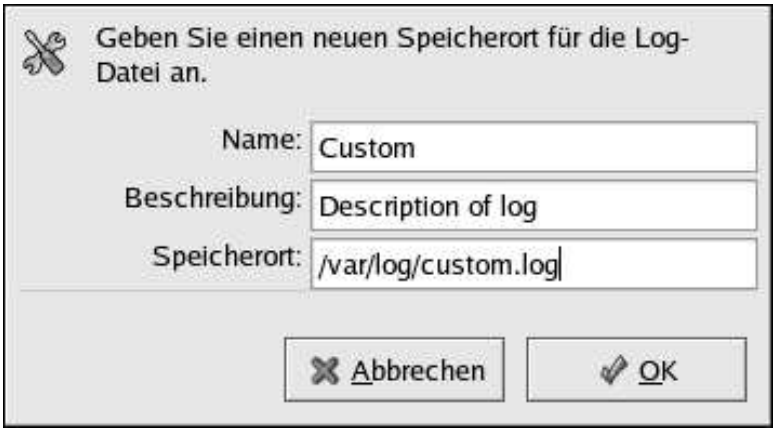

Abbildung 38-3. Log-Dateien hinzufügen

Geben Sie einen Namen, Beschreibung und Speicherort der hinzuzufügenden Log-Datei an. Nach dem Sie auf**OK** geklickt haben, wird die Datei sofort hinzugefügt.

38.4. Log-Dateien untersuchen

Log Viewer kann so konfiguriert werden, dass ein Alert-Symbol neben den Zeilen mit Alerts und ein Warnsymbol neben den Zeilen mit Warnungen angezeigt wird.

Um Alert-Begriffe hinzuzufügen, wählen Sie **Bearbeiten => Präferenzen** aus dem Pull-Down-Menü und klicken Sie auf den Tab **Alerts**. Klicken Sie auf den Button **Hinzufügen**, um einen Alert-Begriff hinzuzufügen. Um einen Alert-Begriff zu löschen, wählen Sie den entsprechenden Begriff aus der Liste und klicken Sie auf **Löschen**.

Das Alert-Symbol wird links neben den Zeilen, die einen Alert-Begriff enthalten, angezeigt.

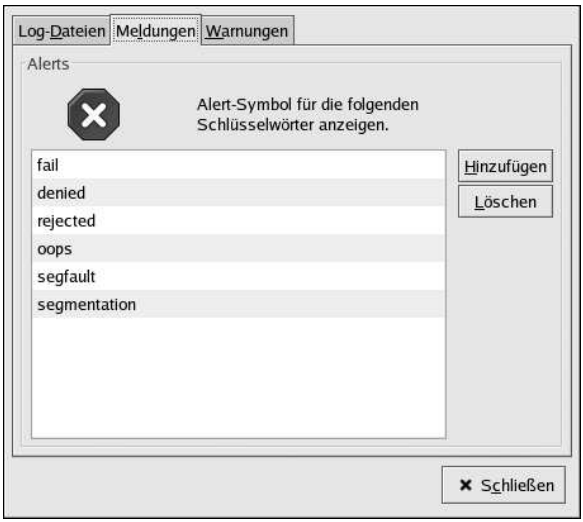

Abbildung 38-4. Alerts

Um Warn-Begriffe hinzuzufügen, wählen Sie **Bearbeiten => Präferenzen** aus dem Pull-Down-Menü und klicken Sie auf das Tab **Warnungen**. Klicken Sie auf den Button **Hinzufügen** um einen Warn-Begriff hinzuzufügen. Um einen WarnBegriff zu löschen, wählen Sie den entsprechenden Begriff aus der Liste und klicken Sie auf **Löschen**.

Das Warn-Symbol wird links neben den Zeilen angezeigt, die den Warn-Begriff enthalten.

Abbildung 38-5. Warnen

redhat

Kapitel 39.

Aktualisieren des Kernels

Der Red Hat Enterprise Linux-Kernel wurde vom Red Hat Kernel-Team benutzerdefiniert entwickelt, um Integrität und Kompatibilität mit der unterstützten Hardware sicherzustellen. Bevor eine neue Version eines Kernels von Red Hat freigegeben wird, muss dieser erst umfangreichen Tests zur Qualitätssicherung unterzogen werden.

Red Hat Enterprise Linux-Kernel sind im RPM-Format verpackt und damit einfach zu aktualisieren und zu verifizieren. Wenn zum Beispiel das RPM-Paket `kernel`, das über Red Hat, Inc. vertrieben wird, installiert wird, wird ein `initrd`-Image erstellt. Es ist daher nicht notwendig, den Befehl `mkinitrd` nach dem Installieren eines anderen Kernels auszuführen. Die Bootloader-Konfigurationsdatei wird außerdem geändert, um den neuen Kernel einzuschließen.

Warnung

Das Red Hat-Installations-Support-Team unterstützt die Erstellung eines eigenen benutzerdefinierten Kernels nicht. Weitere Informationen über das Erstellen eines benutzerdefinierten Kernels vom Sourcecode finden Sie unterAnhang A.

39.1. Überblick über Kernel-Pakete

Red Hat Enterprise Linux enthält die folgenden Kernel-Pakete (abhängig von der Architektur):

- `kernel` — enthält Kernel und die folgenden Schlüsseleigenschaften:
  - Uniprozessor-Support für x86- und Athlon-Systeme (kann auf einem Multi-Prozessor System ausgeführt werden, aber nur ein Prozessor wird verwendet)
  - Multi-Prozessor Support für alle anderen Architekturen
  - Für x86-Systeme werden lediglich die ersten 4 GB RAM verwendet; benutzen Sie das Paket `kernel-hugemem` für x86-Systeme mit mehr als 4 GB RAM

- `kernel-hugemem` — (nur für i686-Systeme) Zusätzlich zu den für das `kernel`-Paket aktivierten Optionen. Die Schlüssel-Konfigurationsoptionen sind wie Folgt:
  - Support für mehr als 4 GB RAM (bis zu 16 GB für x86)
  - PAE (Physical Address Extension), oder 3-Stufen-Paging auf x86-Prozessoren die PAE unterstützen
  - Support für mehrere Prozessoren
  - 4GB/4GB Split — 4GB virtueller Adressraum für den Kernel und nahezu 4GB für jeden Benutzerprozess auf x86 Systemen

- `kernel-BOOT` — nur während der Installation verwendet.
- `kernel-pcmcia-cs` — enthält Support für PCMCIA-Karten.
- `kernel-smp` — enthält den Kernel für Multi-Prozessor Systeme. Die Folgenden sind Schlüsselfeatures:
  - Multiprozessor-Support

- Support für mehr als 4 GB RAM (bis zu 64 GB für x86)
- PAE (Physical Address Extension), oder 3-Stufen-Paging auf x86-Prozessoren die PAE unterstützen

- `kernel-source` — Enthält die Quellcodedateien für den Linux-Kernel
- `kernel-utils` — Enthält Utilities, die zum Steuern des Kernels bzw. der Systemhardware verwendet werden.
- `kernel-unsupported` — Besteht für einige Architekturen

  Da es Red Hat Enterprise Linux nicht möglich ist jede Hardware zu unterstützen, enthält dieses Paket Module, die nicht von Red Hat, Inc. unterstützt sind. Dieses Paket wird nicht während dem Installationsprozess installiert, sondern dies muss später stattfinden. Treiber in dem nicht-unterstützten Paket werden auf einer so-gut-wie-möglich-Basis bereitgestellt — Updates und Fixes werden oder werden nicht mit der Zeit eingearbeitet.

39.2. Vorbereiten einer Aktualisierung

Bevor Sie Ihren Kernel aktualisieren, müssen Sie im Vorfeld einige Schritte zur Vorbereitung durchführen. Zuerst müssen Sie sicherstellen, dass Sie über eine funktionsfähige Bootdiskette für Ihr System verfügen, falls Probleme auftreten sollten. Wenn der Bootloader zum Booten des neuen Kernels nicht richtig konfiguriert ist, können Sie Ihr Red Hat Enterprise Linux-System nicht booten, es sei denn, Sie verfügen über eine Bootdiskette.

Um eine Bootdiskette zu erstellen, melden Sie sich als root an einem Shell-Prompt an und geben Sie den folgenden Befehl ein:

```
/sbin/mkbootdisk `uname -r`
```

Tipp

Weitere Optionen finden Sie auf der man-Seite von `mkbootdisk`.

Booten Sie Ihren Computer mit der Boot-Diskette neu und stellen Sie sicher, dass sie funktioniert, bevor Sie fortfahren.

Sie sollten die Diskette an einem sicheren Ort verwahren, für den Fall, dass Sie diese benötigen.

Um festzustellen, welche Kernel-Pakete installiert sind, geben Sie den folgenden Befehl an einem Shell-Prompt ein:

```
rpm -qa | grep kernel
```

Die Ausgabe enthält einige oder alle der folgenden Pakete, abhängig von der jeweiligen Architektur (Versionsnummern und Pakete können verschieden sein):

```
kernel-2.4.21-1.1931.2.399.ent
kernel-source-2.4.21-1.1931.2.399.ent
kernel-utils-2.4.21-1.1931.2.399.ent
kernel-pcmcia-cs-3.1.31-13
kernel-smp-2.4.21-1.1931.2.399.ent
```

Durch diese Angaben können Sie feststellen, welche Pakete Sie für die Aktualisierung des Kernels herunterladen müssen. Für ein aus einem einzelnen Prozessor bestehendes System wird nur das `kernel`-Paket benötigt. Sehen Sie Abschnitt 39.1 für Beschreibungen der anderen Pakete.

Die Architektur, für den das Kernel-Paket erstellt wurde, ist Teil des Dateinamens. Das Format ist kernel-<*variant*>-<*version*>.<*arch*>.rpm, wobei <*variant*> `smp`, `utils`, usw. ist. <*arch*> ist eine der Folgenden:

1. `x86_64` für die AMD64-Architektur.
2. `ia64` für die Intel® Itanium™ Architektur.
3. `ppc64pseries` für die IBM® eServer™ pSeries™ Architektur.
4. `ppc64iseries` für die IBM® eServer™ iSeries™ Architektur.
5. `s390` für die IBM® S/390® Architektur.
6. `s390x` für die IBM® eServer™ zSeries® Architektur.
7. x86 variant: Die x86-Kernel sind für die verschiedenen x86-Versionen optimiert. Diese sind die Folgenden:
   - `athlon` für AMD Athlon® und AMD Duron® Systeme
   - `i686` für Intel® Pentium® II, Intel® Pentium® III und Intel® Pentium® 4 Systeme

39.3. Herunterladen des aktualisierten Kernels

Es gibt verschiedene Möglichkeiten, um festzustellen, ob für Ihr System ein aktualisierter Kernel zur Verfügung steht.

- Sicherheits-Errata; gehen Sie zum folgenden Ort für Informationen zu Sicherheits-Errata, einschließlich Kernel-Upgrades, die Sicherheitsprobleme beseitigen:
  `http://www.redhat.com/apps/support/errata/`
- Über vierteljährliche Updates; sehen Sie den folgenden Ort für genaueres:
  `http://www.redhat.com/apps/support/errata/rhlas_errata_policy.html`
- Sie können das Red Hat Network zum Herunterladen und anschließendem Installieren der Kernel-RPM-Pakete verwenden. Über Red Hat Network können Sie den neuesten Kernel herunterladen, den Kernel auf dem System aktualisieren, wenn nötig ein RAMdisk-Image erstellen und den Bootloader zum Laden des neuen Kernels konfigurieren. Weitere Informationen finden Sie unter http://www.redhat.com/docs/manuals/RHNetwork/.

Wenn Red Hat Network zum Herunterladen und Installieren des aktuellen Kernels verwendet wurde, folgen Sie den Anweisungen unter Abschnitt 39.5 und Abschnitt 39.6, ändern Sie jedoch nicht den Kernel zum standardmäßigen Booten, da Red Hat Network automatisch den Kernel auf die neueste Version ändert. Um den Kernel manuell zu installieren, gehen Sie zu Abschnitt 39.4 über.

39.4. Durchführen einer Aktualisierung

Nachdem Sie alle nötigen Pakete erhalten haben, können Sie nun den Kernel aktualisieren. Wechseln Sie am Shell-Prompt als root zu dem Verzeichnis, das den Kernel enthält, und folgen Sie den Anweisungen.


Wichtig

Bewahren Sie den alten Kernel unbedingt für den Fall auf, dass mit dem neuen Kernel Probleme auftreten.

Um den alten Kernel zu erhalten, verwenden Sie das Argument `-i` mit dem Befehl `rpm`. Wenn Sie die Option `-U` zum Aktualisieren des `kernel`-Pakets verwenden, überschreibt es den aktuell installierten Kernel (die Kernelversionen können variieren):

```
rpm -ivh kernel-2.4.21-1.1931.2.399.ent.<arch>.rpm
```

Wenn es sich um ein Multiprozessorsystem handelt, müssen Sie auch die `kernel-smp`-Pakete installieren (die Kernel-Versionen können variieren):

```
rpm -ivh kernel-smp-2.4.21-1.1931.2.399.ent.<arch>.rpm
```

Wenn das System auf `i686` basiert und mehr als 4 GB RAM enthält, sollten Sie außerdem das `kernel-hugemem`-Paket, für die `i686` Architektur entwickelt, installieren (die Kernelversion kann abweichen):

```
rpm -ivh kernel-hugemem-2.4.21-1.1931.2.399.ent.i686.rpm
```

Sollen die Pakete `kernel-source` oder `kernel-utils` aktualisiert werden, werden die alten Versionen höchstwahrscheinlich nicht mehr benötigt. Verwenden Sie folgende Befehle, um die Pakete zu aktualisieren (die Versionen können abweichen):

```
rpm -Uvh kernel-source-2.4.21-1.1931.2.399.ent.<arch>.rpm
rpm -Uvh kernel-utils-2.4.21-1.1931.2.399.ent.<arch>.rpm
```

Im nächsten Schritt müssen Sie prüfen, ob ein RAMDisk-Image erstellt wurde. Weitere Informationen hierzu finden Sie unter Abschnitt 39.5.

39.5. Bestätigen des Initial RAM Disk Image

Wenn das System das ext3-Dateisystem, einen SCSI-Controller oder Bezeichner, die Partitionen in `/etc/fstab` referenzieren, verwendet, benötigen Sie eine initiale RAM-Disk. Der Zweck einer solchen Disk ist, einem modularen Kernel Zugriff zu den Modulen zu gewähren, die zum Booten benötigt werden, bevor der Kernel Zugriff auf das Gerät erhält, in dem die Module normalerweise abgelegt sind.

Auf Red Hat Enterprise Linux Architekturen, die nicht der IBM eServer iSeries zugehören, kann die initiale RAM-Disk mit dem Befehl `mkinitrd` erstellt werden. Dieser Schritt muss jedoch nicht manuell ausgeführt werden, da er automatisch ausgeführt wird, wenn die jeweiligen Pakete von den von Red Hat, Inc. herausgegebenen RPM-Paketen aktualisiert oder installiert wurden. Um die Erstellung der RAMDisk zu überprüfen, verwenden Sie den Befehl `ls -l /boot` um sicherzugehen, dass die Datei `initrd-<version>.img` erstellt wurde (diese Version sollte mit der des eben installierten Kernels übereinstimmen).

Auf iSeries-Systemen, sind die initiale RAM-Disk und vmlinux in einer Datei zusammengefasst, die mit dem Befehl `addRamDisk` erstellt werden kann. Dieser Schritt muss jedoch nicht manuell ausgeführt werden, da er automatisch ausgeführt wird, wenn die jeweiligen Pakete von den von Red Hat, Inc. herausgegebenen RPM-Paketen aktualisiert oder installiert wurden. Um die Erstellung der RAMDisk zu überprüfen, verwenden Sie den Befehl `ls -l /boot` um sicherzugehen, dass die Datei `/boot/vmlinitrd-<kernel-version>` erstellt wurde (diese Version sollte mit der des eben installierten Kernels übereinstimmen).

Im nächsten Schritt müssen Sie überprüfen, dass der Bootloader zum Booten des neuen Kernels konfiguriert wurde. Informationen hierzu finden Sie unter Abschnitt 39.6.

39.6. Überprüfen des Bootloader

Das `kernel`-RPM-Paket konfiguriert den Bootloader, damit dieser den neu installierten Kernel bootet (dies gilt nicht für IBM eServer iSeries Systeme). Es konfiguriert diesen jedoch nicht zum Booten des neuen Kernels als Vorgabe.

Sie sollten grundsätzlich überprüfen, ob der Bootloader richtig konfiguriert wurde. Dies ist ein entscheidender Schritt. Wurde der Bootloader nämlich nicht richtig konfiguriert, kann das System nicht ordnungsgemäß in Red Hat Enterprise Linux booten. Tritt dies auf, booten Sie ihr System mit der zuvor erstellten Bootdiskette und versuchen Sie erneut, den Bootloader zu konfigurieren.

39.6.1. x86-Systeme

x86-Systeme können entweder GRUB oder LILO als Bootloader verwenden. Die einzige Ausnahme stellen AMD64-Systeme dar, die nicht über LILO verfügen. Für alle x86-Systeme ist GRUB die Vorgabe.

39.6.1.1. GRUB

Wenn Sie GRUB als Bootloader verwenden, müssen Sie bestätigen, dass die Datei `/boot/grub/grub.conf` einen `title`-Abschnitt mit der gleichen Version wie das eben installierte `kernel`-Paket enthält (wenn `kernel-smp` oder `kernel-hugemem` Pakete installiert wurden, ist entsprechend für diese auch ein Abschnitt vorhanden):

```
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=1
timeout=10
splashimage=(hd0,0)/grub/splash.xpm.gz
title Red Hat Enterprise Linux (2.4.21-1.1931.2.399.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-1.1931.2.399.ent ro root=LABEL=/
        initrd /initrd-2.4.21-1.1931.2.399.ent.img
title Red Hat Enterprise Linux (2.4.20-2.30.ent)
        root (hd0,0)
        kernel /vmlinuz-2.4.20-2.30.ent ro root=LABEL=/
        initrd /initrd-2.4.20-2.30.ent.img
```

Wenn Sie eine separate `/boot/`-Partition erstellt haben, sind die Pfade zum Kernel und initrd-Image relativ zur `/boot/`-Partition.

Bitte beachten Sie, dass der Standard noch nicht auf den neuen Kernel gesetzt wurde. Um GRUB zum standardmäßigen Booten des neuen Kernels zu konfigurieren, müssen Sie den Wert der `default`-Variable für den Titelabschnitt in die Nummer des Abschnitts, der den neuen Kernel enthält, ändern. Der Zähler beginnt bei 0. Wenn sich der neue Kernel z.B. im ersten Titelabschnitt befindet, setzen Sie `default` auf **0**.

Testen Sie den neuen Kernel, indem Sie den Computer neu booten, und die Systemmitteilungen überprüfen, um sicherzustellen, dass die Hardware richtig erkannt wurde.

39.6.1.2. LILO

Wenn Sie LILO als Bootloader verwenden, müssen Sie bestätigen, dass die Datei `/etc/lilo.conf` einen `image`-Abschnitt mit der gleichen Version wie das eben installierte `kernel`-Paket enthält. (wenn die Pakete `kernel-smp` oder `kernel-hugemem` installiert wurden, ist für diese auch ein Abschnitt vorhanden):

Bitte beachten Sie, dass der Standard noch nicht auf den neuen Kernel gesetzt wurde. Um LILO zum standardmäßigen Booten des neuen Kernels zu konfigurieren, müssen Sie den Wert der `default`-Variable auf den Wert `label` im Abschnitt `image` für den neuen Kernel ändern. Führen Sie den Befehl `/sbin/lilo` als root aus, damit die Änderungen wirksam werden. Nach dem Ausführen wird eine Ausgabe angezeigt, die der folgenden ähnelt:

```
Added 2.4.21-1.1931.2.399.ent *
Added linux
```

`*` nach `2.4.21-1.1931.2.399.ent` bedeutet, dass der Kernel in diesem Abschnitt der Kernel ist, der standardmäßig von LILO gebootet wird.

Testen Sie den Kernel, in dem Sie Ihrem Computer neu booten, und die Mitteilungen überprüfen, um sicherzustellen, dass die Hardware richtig erkannt wurde.

39.6.2. Itanium-Systeme

Itanium-Systeme verwenden ELILO als Bootloader, welcher `/boot/efi/EFI/redhat/elilo.conf` als Konfigurationsdatei verwendet. Prüfen Sie, dass diese Datei einen `image`-Abschnitt mit der gleichen Version wie das eben installierte `kernel`-Paket enthält:

```
prompt
timeout=50
default=old

image=vmlinuz-2.4.21-1.1931.2.399.ent
        label=linux
        initrd=initrd-2.4.21-1.1931.2.399.ent.img
        read-only
        append="root=LABEL=/"
image=vmlinuz-2.4.20-2.30.ent
        label=old
        initrd=initrd-2.4.20-2.30.ent.img
        read-only
        append="root=LABEL=/"
```

Bitte beachten Sie, dass der Standard noch nicht auf den neuen Kernel gesetzt wurde. Um ELILO zum standardmäßigen Booten des neuen Kernels zu konfigurieren, müssen Sie den Wert der `default`-Variable auf den Wert `label` im Abschnitt `image` für den neuen Kernel ändern.

Testen Sie den neuen Kernel, indem Sie den Computer neu booten, und die Systemmitteilungen überprüfen, um sicherzustellen, dass die Hardware richtig erkannt wurde.

39.6.3. IBM S/390 und IBM eServer zSeries-Systeme

Systeme der IBM S/390 und IBM eServer zSeries benutzen z/IPL als Bootloader, welcher `/etc/zipl.conf` als Konfigurationsdatei verwendet. Prüfen Sie, dass die Datei einen Abschnitt mit der gleichen Version wie der eben installierte Kernel enthält:

```
[defaultboot]
default=old
target=/boot/
[linux]
        image=/boot/vmlinuz-2.4.21-1.1931.2.399.ent
        ramdisk=/boot/initrd-2.4.21-1.1931.2.399.ent.img
        parameters="root=LABEL=/"
[old]
        image=/boot/vmlinuz-2.4.20-2.30.ent
        ramdisk=/boot/initrd-2.4.20-2.30.ent.img
        parameters="root=LABEL=/"
```

Bitte beachten Sie, dass der Standard noch nicht auf den neuen Kernel gesetzt wurde. Um Z/IPL zum standardmäßigen Booten des neuen Kernels zu konfigurieren, müssen Sie den Wert der `default`-Variable auf den Namen des Abschnitts setzen, der den neuen Kernel enthält. Die erste Zeile jeden Abschnitts enthält den Namen in Klammern.

Nach Ändern der Konfigurationsdatei, führen Sie folgenden Befehl als root aus, damit die Änderungen wirksam werden:

```
/sbin/zipl
```

Testen Sie den neuen Kernel, indem Sie den Computer neu booten, und die Systemmitteilungen überprüfen, um sicherzustellen, dass die Hardware richtig erkannt wurde.

39.6.4. IBM eServer iSeries Systeme

Die Datei `/boot/vmlinitrd-<kernel-version>` wird mit einem Upgrade des Kernels installiert. Sie müssen jedoch den Befehl `dd` verwenden, um das System zum Booten des neuen Kernels zu konfigurieren:

1. Führen Sie den Befehl `cat /proc/iSeries/mf/side` als root aus, um die Standard-Seite zu bestimmen (entweder A, B oder C).
2. Führen Sie den folgenden Befehl als root aus, wobei *<kernel-version>* die Version des neuen Kernel ist und *<side>* die im vorigen Beispiel erhaltene Seite:
   `dd if=/boot/vmlinitrd-<kernel-version> of=/proc/iSeries/mf/<side>/vmlinux bs=8k`

Testen Sie den neuen Kernel, indem Sie den Computer neu booten, und die Systemmitteilungen überprüfen, um sicherzustellen, dass die Hardware richtig erkannt wurde.

39.6.5. IBM eServer pSeries Systeme

Systeme der IBM eServer pSeries verwenden YABOOT als Bootloader, der `/etc/aboot.conf` als Konfigurationsdatei benutzt. Prüfen Sie, dass diese Datei einen `image`-Abschnitt mit der gleichen Version wie das eben installierte `kernel`-Paket enthält:

```
boot=/dev/sda1
init-message=Welcome to Red Hat Enterprise Linux!
Hit <TAB> for boot options

partition=2
timeout=30
install=/usr/lib/yaboot/yaboot
delay=10
nonvram

image=/vmlinux--2.4.20-2.30.ent
```

```
        label=old
        read-only
        initrd=/initrd--2.4.20-2.30.ent.img
        append="root=LABEL=/"

image=/vmlinux-2.4.21-1.1931.2.399.ent
        label=linux
        read-only
        initrd=/initrd-2.4.21-1.1931.2.399.ent.img
        append="root=LABEL=/"
```

Beachten Sie, dass die Vorgabe nicht der neue Kernel ist. Der Kernel im ersten Image wird standardmäßig gebootet. Um die Vorgabe für den zu bootenden Kernel zu ändern, verschieben Sie die Image-Stanza, so dass der zu bootende Kernel der Erste in der Liste ist, oder fügen Sie die `default`-Anweisung hinzu und setzen Sie diese auf das `label` der Image-Stanza, die den neuen Kernel enthält.

Testen Sie den neuen Kernel, indem Sie den Computer neu booten, und die Systemmitteilungen überprüfen, um sicherzustellen, dass die Hardware richtig erkannt wurde.

redhat

Kapitel 40.

Kernelmodule

Der Linux-Kernel ist modular aufgebaut. Beim Booten wird nur ein minimaler residenter Kernel in den Speicher geladen. Wenn ein Benutzer ein Feature anfordert, das nicht im residenten Kernel vorhanden ist, wird ein *Kernelmodul*, manchmal auch als *Treiber* bezeichnet, dynamisch in den Speicher geladen.

Während der Installation wird die Hardware auf dem System geprüft. Basierend auf dieser Prüfung und vom Benutzer bereitgestellten Informationen entscheidet das Installationsprogramm, welche Module beim Booten geladen werden. Das Installationsprogramm stellt den dynamischen Lademechanismus auf transparentes Arbeiten ein.

Wenn neue Hardware nach der Installation hinzugefügt werden soll und diese ein Kernelmodul benötigt, muss das System so konfiguriert werden, dass des richtige Kernelmodul für die neue Hardware geladen wird. Wird das System mit der neuen Hardware gebootet, läuft das Programm **Kudzu**, erkennt die neue Hardware wenn diese unterstützt wird, und konfiguriert das Modul dafür. Das Modul kann auch manuell eingestellt werden, indem Sie die Konfigurationsdatei `/etc/modules.conf` des Moduls bearbeiten.

Anmerkung

Grafikkartenmodule, die zum Anzeigen des X Window Systems-Schnittstelle verwendet werden, sind Teil des `XFree86`-Pakets, nicht des Kernels. Dieses Kapitel kann daher nicht auf diese angewendet werden.

Enthält Ihr System zum Beispiel bei der Installation einen SMC EtherPower 10 PCI-Netzwerkadapter, enthält die Konfigurationsdatei des Moduls folgende Zeile:

```
alias eth0 tulip
```

Wenn Sie eine zweite, zur ersten identische, Netzwerkkarte zu Ihrem System hinzufügen, müssen Sie folgende Zeile zu `/etc/modules.conf` hinzufügen:

```
alias eth1 tulip
```

Die alphabetische Liste der Kernelmodule und die von den Modulen unterstützte Hardware finden Sie im *Red Hat Enterprise Linux Referenzhandbuch*.

40.1. Dienstprogramme der Kernelmodule

Eine Reihe von Befehlen für die Verwaltung von Kernelmodulen ist erhältlich, wenn das `modutils`-Paket installiert ist. Sie können mit diesen Befehlen feststellen, ob ein Modul erfolgreich geladen wurde oder wenn Sie verschiedene Module für neue Hardware ausprobieren.

Mithilfe des Befehls `/sbin/lsmod` wird eine Liste der aktuell geladenen Module angezeigt. Zum Beispiel:

```
Module                  Size  Used by    Not tainted
iptable_filter          2412   0 (autoclean) (unused)
ip_tables              15864   1 [iptable_filter]
nfs                    84632   1 (autoclean)
lockd                  59536   1 (autoclean) [nfs]
```

```
sunrpc                  87452   1 (autoclean) [nfs lockd]
soundcore                7044   0 (autoclean)
ide-cd                  35836   0 (autoclean)
cdrom                   34144   0 (autoclean) [ide-cd]
parport_pc              19204   1 (autoclean)
lp                       9188   0 (autoclean)
parport                 39072   1 (autoclean) [parport_pc lp]
autofs                  13692   0 (autoclean) (unused)
e100                    62148   1
microcode                5184   0 (autoclean)
keybdev                  2976   0 (unused)
mousedev                 5656   1
hid                     22308   0 (unused)
input                    6208   0 [keybdev mousedev hid]
usb-uhci                27468   0 (unused)
usbcore                 82752   1 [hid usb-uhci]
ext3                    91464   2
jbd                     56336   2 [ext3]
```

In jeder Zeile gibt die erste Spalte den Namen des Moduls, die zweite Spalte die Größe des Moduls und die dritte Spalte die Verwendungshäufigkeit des Moduls an.

Die Informationen hinter der Verwendungshäufigkeit variieren leicht von Modul zu Modul. Wenn `(unused)` in der Modul-Zeile aufgelistet wird, wird das jeweilige Modul zur Zeit nicht verwendet. Wird `(autoclean)` in einer Zeile angezeigt, kann dieses Modul mit dem Befehl `rmmod -a` automatisch bereinigt werden. Wenn dieser Befehl ausgeführt wird, werden alle Module, die als autoclean markiert sind und seit dem letzten autoclean nicht verwendet wurden, entfernt. Red Hat Enterprise Linux führt diesen autoclean-Vorgang nicht standardmäßig aus.

Wird ein Modulname am Ende der Zeile in Klammern angegeben, ist das Modul in Klammern anhängig vom in der ersten Spalte der Zeile angegebenen Modul. Zum Beispiel in der Zeile

```
usbcore                 82752   1 [hid usb-uhci]
```

die `hid` und `usb-uhci` Kernelmodule hängen vom usbcore Modul ab.

Die `/sbin/lsmod` Ausgabe ist die gleiche wie `/proc/modules`.

Um ein Kernelmodul zu laden, verwenden Sie de Befehl `/sbin/modprobe` gefolgt vom Namen des Kernelmoduls. Standardmäßig versucht `modprobe` das Modul aus den Unterverzeichnissen `/lib/modules/<kernel-version>/kernel/drivers/` zu laden. Es gibt ein Unterverzeichnis für jeden Modultyp, zum Beispiel ist das Unterverzeichnis `net/` für Netzwerk-Schnittstellen-Treiber. Manche Kernelmodule verfügen über Modulabhängigkeiten, d.h. andere Module müssen zuerst geladen werden, um das Laden dieser Module zu ermöglichen. Der Befehl `/sbin/modprobe` prüft diese Abhängigkeiten und lädt die abhängigen Module, bevor die angegebenen Module geladen werden.

So entfernt zum Beispiel der Befehl

```
/sbin/modprobe hid
```

alle abhängigen Module und dann das Modul `hid`.

Um alle Befehle so auf dem Bildschirm anzuzeigen, wie diese von `/sbin/modprobe` ausgeführt werden, verwenden Sie die Option `-v`. Beispiel:

```
/sbin/modprobe -v hid
```

Es wird folgendes oder ähnliches angezeigt:

```
/sbin/insmod /lib/modules/2.4.21-1.1931.2.399.ent/kernel/drivers/usb/hid.o
Using /lib/modules/2.4.21-1.1931.2.399.ent/kernel/drivers/usb/hid.o
Symbol version prefix 'smp_'
```

Mit dem Befehl `/sbin/insmod` können Sie auch Kernelmodule laden, er löst jedoch keine Abhängigkeiten. Aus diesem Grund wird die Verwendung des `/sbin/modprobe` Befehls empfohlen.

Um Kernelmodule zu entfernen, verwenden Sie den Befehl `/sbin/rmmod`, gefolgt vom Modulnamen. Das `rmmod` Utility entfernt nur Module, die nicht verwendet werden, und die keine Abhängigkeiten zu anderen verwendeten Modulen aufweisen.

So entfernt zum Beispiel der Befehl

```
/sbin/rmmod hid
```

das Kernelmodul `hid`.

Eine weitere, nützliche Utility ist `modinfo`. Mit dem Befehl `/sbin/modinfo` können Sie Informationen über ein Kernelmodul anzeigen. Die allgemeine Syntax ist folgende:

```
/sbin/modinfo [options] <module>
```

Optionen sind unter anderem `-d` zur Anzeige einer Kurzbeschreibung des Moduls sowie `-p` zur Auflistung der vom Modul unterstützten Parameter. Die vollständige Liste der Optionen finden Sie auf der `modinfo` man-Seite (`man modinfo`).

40.2. Zusätzliche Ressourcen

Weitere Informationen über Kernelmodule und die Utilities finden Sie in folgenden Ressourcen.

40.2.1. Installierte Dokumentation

- `lsmod`-man-Seite — Beschreibung und Erklärung der Ausgabe.
- `insmod`-man-Seite — Beschreibung und Liste der Befehlszeilenoptionen.
- `modprobe`-man-Seite — Beschreibung und Liste der Befehlszeilenoptionen.
- `rmmod`-man-Seite — Beschreibung und Liste von Befehlszeilenoptionen.
- `modinfo`-man-Seite — Beschreibung und Liste von Befehlszeilenoptionen.
- `/usr/src/linux-2.4/Documentation/modules.txt` — Informationen zum Kompilieren und Verwenden der Kernelmodule. Diese Datei ist Teil des `kernel-source` Pakets.

40.2.2. Hilfreiche Webseiten

- http://www.redhat.com/mirrors/LDP/HOWTO/Module-HOWTO/index.html — *Linux Loadable Kernel Module HOWTO* vom Linux-Dokumentation-Projekt.

Kapitel 41.

Konfiguration von Mail Transport Agent (MTA)

Ein *Mail Transport Agent* (MTA) ist notwendig für das Versenden von E-Mail. Ein *Mail User Agent* (MUA) wie zum Beispiel **Evolution**, **Mozilla Mail** und **Mutt** wird zum Lesen und Verfassen von E-Mails verwendet. Verschickt ein Benutzer eine E-Mail von einem MUA, wird diese Mitteilung an den MTA weitergeleitet, der sie wiederum an eine Reihe von MTAs verschickt, bis sie ihren Bestimmungsort erreicht.

Auch wenn ein Benutzer keine E-Mail verschicken will, könnten einige automatische Tasks oder Systemprogramme mit dem Befehl `/bin/mail` E-Mails mit Protokollen an das root-Account des lokalen Systems verschicken.

Red Hat Enterprise Linux 3 bietet zwei MTAs: Sendmail und Postfix. Sind beide installiert, ist `sendmail` der standardmäßige MTA. Mit dem **Mail Transport Agent Switcher** können Sie entweder `sendmail` oder `postfix` als Standard-MTA für das System wählen.

Das RPM-Paket `redhat-switch-mail` muss zum Verwenden der textbasierten Version von **Mail Transport Agent Switcher** installiert werden. Wenn Sie die grafische Version verwenden möchten, muss außerdem das Paket `redhat-switch-mail-gnome` installiert werden. Weitere Informationen zum Installieren von RPM-Paketen finden Sie unter Teil III.

Wählen Sie zum Starten von **Mail Transport Agent Switcher Hauptmenü** (im Panel) => **Extras** => **Systemeinstellungen** => **Mail Transport Agent Switcher**, oder geben Sie den Befehl `redhat-switch-mail` in einem Shell-Prompt ein (z.B. in XTerm oder GNOME).

Das Programm erkennt automatisch, ob das X Window System ausgeführt wird. Wird es ausgeführt, startet das Programm im Grafikmodus, wie in Abbildung 41-1 gezeigt. Wird X nicht erkannt, wird der Textmodus gestartet. Um **Mail Transport Agent Switcher** im Textmodus auszuführen, geben Sie den Befehl `redhat-switch-mail-nox` ein.

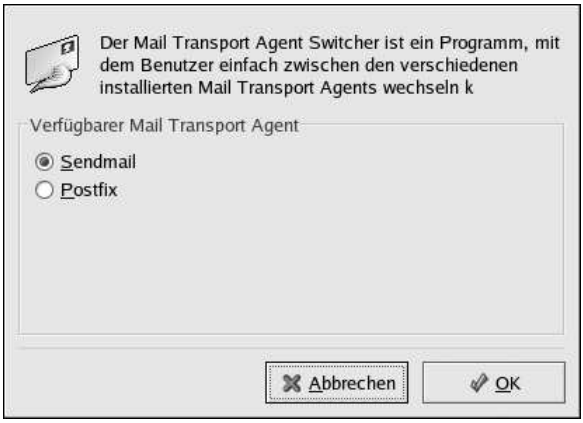

Abbildung 41-1. Mail Transport Agent Switcher

Wenn Sie zum Wechseln des MTA **OK** gedrückt haben, wird der ausgewählte Mail-Daemon aktiviert und wird beim Booten gestartet, und der andere Mail-Daemon wird deaktiviert, so dass dieser beim Booten nicht geladen wird. Der ausgewählte Daemon wird gestartet, der andere gestoppt - die Änderungen werden somit sofort wirksam.

Weitere Informationen über E-Mail-Protokolle und MTAs finden Sie im *Red Hat Enterprise Linux Referenzhandbuch*.

VI. Systemüberwachung

System-Administratoren überwachen auch die Systemleistung. Red Hat Enterprise Linux enthält Tools, die Administratoren bei diesen Aufgaben helfen.

Inhaltsverzeichnis

redhat.

Kapitel 42.

Informationen über das System

Bevor Sie in Erfahrung bringen, wie Sie Ihr System konfigurieren, sollten Sie sich zunächst darüber informieren, wie Sie wichtige Systeminformationen abrufen können. Sie sollten z.B. wissen, wie Sie herausfinden, wie viel freien Speicherplatz Sie haben, wie viel Speicherplatz auf Ihrer Festplatte zur Verfügung steht und wie sie partitioniert ist als auch, welche Prozesse gerade ausgeführt werden. In diesem Kapitel wird beschrieben, wie Sie diese Angaben mithilfe von kurzen Befehlen und einigen einfachen Programmen von Ihrem Red Hat Enterprise Linux-Systems abrufen können.

42.1. Systemprozesse

Der Befehl `ps ax` zeigt eine Liste der laufenden Systemprozesse, einschließlich der Prozesse anderer Benutzer, an. Um den Eigentümer eines Prozesses und die jeweiligen Prozesse selbst anzuzeigen, verwenden Sie den Befehl `ps aux`. Bei der erscheinenden Liste handelt es sich um eine statische Liste, d.h. sie stellt Ihnen einen kurzen Überblick über die bei Ihrer Befehlseingabe laufenden Prozesse zur Verfügung. Wenn Sie eine ständig aktualisierte Liste der laufenden Prozesse wünschen, können Sie diese mit Hilfe vom weiter unten beschriebenen Befehl `top` abrufen.

Die Ausgabe des Befehls `ps` kann lang sein. Um zu verhindern, dass diese über den aktuellen Bildschirm hinaus reicht, können Sie die Anweisung less angeben:

```
ps aux | less
```

Sie können den Befehl `ps` in Kombination mit `grep` verwenden, um zu überprüfen, ob ein bestimmter Prozess gerade ausgeführt wird. Wenn Sie z.B. wissen möchten, ob **Emacs** läuft, finden Sie dies mithilfe des folgenden Befehls heraus:

```
ps ax | grep emacs
```

Der Befehl `top` zeigt derzeit laufende Prozesse und die dazuhörigen wichtigen Informationen einschließlich Speicher und CPU- Nutzung an. Es handelt sich hierbei sowohl um eine Echtzeit- als auch interaktive Liste. Nachfolgend sehen Sie ein Beispiel für die Ausgabe von `top`:

```
 19:11:04  up  7:25,  9 users,  load average: 0.00, 0.05, 0.12
89 processes: 88 sleeping, 1 running, 0 zombie, 0 stopped
CPU states:  cpu    user    nice  system    irq  softirq  iowait    idle
           total    6.6%    0.0%    0.1%   0.1%     0.0%    0.0%  192.8%
           cpu00    6.7%    0.0%    0.1%   0.1%     0.0%    0.0%   92.8%
           cpu01    0.0%    0.0%    0.0%   0.0%     0.0%    0.0%  100.0%
Mem:  1028556k av,  241972k used,  786584k free,       0k shrd,   37712k buff
       162316k active,              18076k inactive
Swap: 1020116k av,       0k used, 1020116k free                   99340k cached

  PID USER     PRI  NI  SIZE  RSS SHARE STAT %CPU %MEM   TIME CPU COMMAND
 1899 root      15   0 17728  12M  4172 S     6.5  1.2 111:20   0 X
 6380 root      15   0  1144 1144   884 R     0.3  0.1   0:00   0 top
    1 root      15   0   488  488   432 S     0.0  0.0   0:05   1 init
    2 root      RT   0     0    0     0 SW    0.0  0.0   0:00   0 migration/0
    3 root      RT   0     0    0     0 SW    0.0  0.0   0:00   1 migration/1
    4 root      15   0     0    0     0 SW    0.0  0.0   0:00   0 keventd
    5 root      34  19     0    0     0 SWN   0.0  0.0   0:00   0 ksoftirqd/0
    6 root      34  19     0    0     0 SWN   0.0  0.0   0:00   1 ksoftirqd/1
    9 root      25   0     0    0     0 SW    0.0  0.0   0:00   0 bdflush
    7 root      15   0     0    0     0 SW    0.0  0.0   0:00   1 kswapd
    8 root      15   0     0    0     0 SW    0.0  0.0   0:00   1 kscand
```

```
  10 root      15   0     0    0     0 SW    0.0  0.0   0:01   1 kupdated
  11 root      25   0     0    0     0 SW    0.0  0.0   0:00   0 mdrecoveryd
```

Um `top` zu beenden, drücken Sie die Taste [q].

Zu den nützlichen interaktiven Befehlen, die Ihnen mit `top` zur Verfügung stehen, gehören die folgenden:

Befehl	Beschreibung
[Leertaste]	Bildschirm sofort auffrischen
[h]	Hilfebildschirm anzeigen
[k]	Prozess beenden. Sie werden aufgefordert, die Prozess-ID und das zu sendende Signal anzugeben.
[n]	Anzahl der angezeigten Prozesse ändern. Sie werden aufgefordert, die gewünschte Anzahl einzugeben.
[u]	Nach Benutzer anordnen.
[M]	Nach Speichernutzung anordnen.
[P]	Nach CPU-Nutzung anordnen.

Tabelle 42-1. Interaktive `top` Befehle

Tipp

Anwendungen wie **Mozilla** und **Nautilus** sind *Thread-aware* — Mehrfach-Ketten dienen der Bearbeitung von mehreren Benutzern oder mehreren Anfragen. Dabei wird jedem Thread eine Prozess-ID zugewiesen. Standardmäßig wenden `ps` und `top` nur den Hauptthread (initial thread) an. Wenn Sie alle Threads anzeigen möchten, verwenden Sie den Befehl `ps -m` oder geben Sie [Strg]-[H] in `top` ein.

Wenn Sie eine grafische Schnittstelle für `top` vorziehen, steht Ihnen der **GNOME System-Monitor** zur Verfügung. Für einen Start vom GNOME-Desktop aus gehen Sie zum **Hauptmenü-Button** (auf der Menüleiste) => **Systemtools** => **System-Monitor** => oder geben Sie an einem Shell-Prompt `gnome-system-monitor` aus jedem beliebigen Bildschirm vom X Window- System-Desktop heraus ein. Wählen Sie anschließend das Tab **Prozesse anzeigen**.

Der **GNOME System-Monitor** ermöglicht Ihnen die Suche nach Prozessen in der Liste der laufenden Prozesse sowie die Anzeige aller Prozesse, Ihrer Prozesse oder der aktiven Prozesse.

Wenn Sie mehr Informationen über einen Prozess benötigen, klicken Sie die Schaltfläche **Weitere Infos** an. Die entsprechenden Details werden anschließend im unteren Teil des Fensters angezeigt.

Wenn Sie einen Prozess unterbrechen möchten, klicken Sie ihn an und klicken Sie auf die Schaltfläche **Prozess beenden**. Diese Funktion ist insbesondere bei den Prozessen nützlich, die nicht mehr auf die Eingaben des Benutzers antworten.

Um nach den Informationen einer bestimmten Spalte zu sortieren, klicken Sie auf den Namen der Spalte. Die entsprechende Spalte wird in einem dunkleren Grauton angezeigt.

Standardmäßig zeigt der **GNOME System-Monitor** keine Threads an. Wenn Sie diese Einstellung ändern möchten, wählen Sie **Bearbeiten** => **Präferenzen**, klicken Sie auf das Tab **Prozesse anzeigen**

und wählen Sie **Ketten anzeigen**. In den Präferenzen können Sie auch das Aktualisierungsintervall, die Art der über jeden Prozess angezeigten Informationen und die Farben des Systemmonitors konfigurieren.

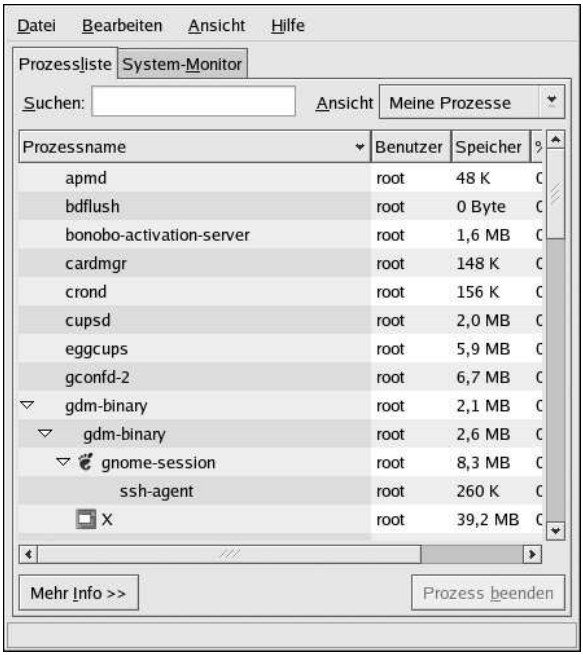

Abbildung 42-1. GNOME System-Monitor

42.2. Speichernutzung

Der Befehl `free` zeigt den gesamten physischen Speicher und die Größe des Swap-Bereichs an. Weiterhin zeigt `free` die Aufteilung in genutzten und freien Speicher, sowie wie viel davon für den gemeinsam benutzten Speicher, den Kernel-Buffer und Cache genutzt wird.

```
             total       used       free     shared    buffers     cached
Mem:        256812     240668      16144     105176      50520      81848
-/+ buffers/cache:     108300     148512
Swap:       265032        780     264252
```

Der Befehl `free -m` zeigt die gleichen Informationen in Megabytes an, die leichter zu lesen sind.

```
             total       used       free     shared    buffers     cached
Mem:           250        235         15        102         49         79
-/+ buffers/cache:        105        145
Swap:          258          0        258
```

Wenn Sie eine grafische Schnittstelle für `free` bevorzugen, steht Ihnen hierfür der **GNOME System-Monitor** zur Verfügung. Für einen Start vom GNOME- Desktop aus gehen Sie zum **Hauptmenü-Button** (in der Menüleiste) => **Systemtools** => **System-Monitor** oder geben Sie nach einem Shell Prompt `gnome-system-monitor` aus jedem beliebigem Bildschirm vom X Window-System-Desktop heraus ein. Wählen Sie anschließend das Tab **System-Monitor**.

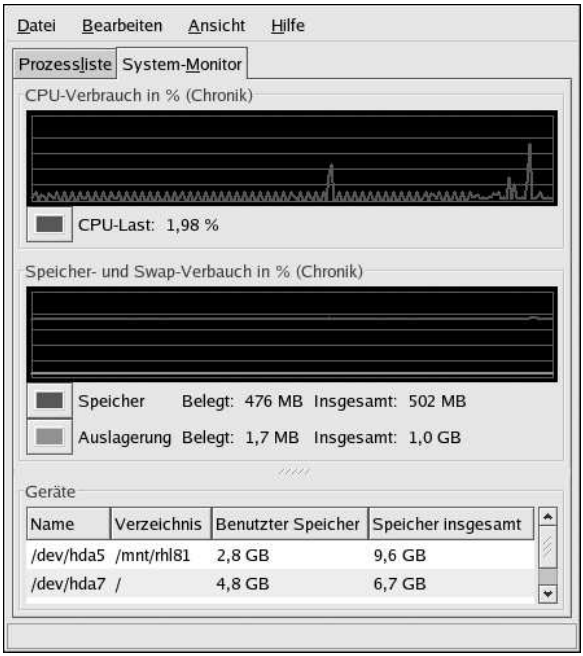

Abbildung 42-2. GNOME System-Monitor

42.3. Dateisysteme

Der Befehl `df` liefert Informationen zur Speicherbelegung auf der Festplatte. Wenn Sie an einem Shell-Prompt `df` eingeben, erscheint in etwa das folgende Output:

```
Filesystem           1k-blocks      Used Available Use% Mounted on
/dev/hda2             10325716   2902060   6899140  30% /
/dev/hda1                15554      8656      6095  59% /boot
/dev/hda3             20722644   2664256  17005732  14% /home
none                    256796         0    256796   0% /dev/shm
```

Die Partitionsgröße wird hier standardmäßig in Kilobyte-Blöcken und der genutzte und verfügbare Speicherplatz der Laufwerke in Kilobytes angegeben. Um diese Angaben in Megabytes und Gigabytes abzurufen, verwenden Sie den Befehl `df -h`. Der Hinweis `-h` steht für lesbares Format. Die Ausgabe sieht ungefähr folgendermaßen aus:

```
Filesystem            Size  Used Avail Use% Mounted on
```

```
/dev/hda2             9.8G  2.8G  6.5G  30% /
/dev/hda1              15M  8.5M  5.9M  59% /boot
/dev/hda3              20G  2.6G   16G  14% /home
none                  251M     0  250M   0% /dev/shm
```

In der Liste der Partitionen gibt es einen Eintrag für `/dev/shm`. Dieser Eintrag stellt das Dateisystem des virtuellen Speichers des Systems dar.

Mit dem Befehl `du` wird die geschätzte Speicherbelegung durch Dateien eines Verzeichnisses angezeigt. Wenn Sie nach einem Shell-Prompt `du` eingeben, wird die Laufwerkbelegung für jedes einzelne Unterverzeichnis in einer Liste angezeigt. In der untersten Zeile dieser Liste wird auch die Gesamtspeicherbelegung für das aktuelle Verzeichnis und die Unterverzeichnisse angezeigt. Wenn Sie nicht möchten, dass alle Unterverzeichnisse angezeigt werden, wählen Sie den Befehl `du -hs`, um nur noch die Gesamtbelegung des Verzeichnisses in lesbarem Format zu sehen. Mit dem Befehl `du -- help` stehen Ihnen weitere Optionen zur Verfügung.

Um die Partitionen und die Speichernutzung des Systems in einem grafischen Format anzuzeigen, verwenden Sie das Tab **Systemmonitor** wie im unteren Teil von Abbildung 42-2 angegeben.

42.4. Hardware

Wenn bei der Konfiguration Ihrer Hardware Probleme auftreten oder Sie einfach nur wissen möchten, mit welcher Hardware Ihr System ausgestattet ist, können Sie mithilfe der Anwendung **Hardware Browser** die Hardware anzeigen lassen, die Sie dann testen können. Starten Sie das System vom Desktop, indem Sie **Hauptmenü- Button => Systemtools => Hardware Browser** wählen oder indem Sie an einem Shell-Prompt `hwbrowser` eingeben. Wie unter Abbildung 42-3 erklärt, zeigt es Ihre CD-ROM-Laufwerke, Floppy-Laufwerke, Festplatten und deren Partitionen, Netzwerkgeräte, Mäuse, Systemgeräte und Grafikkarten an. Wenn Sie auf den Kategorienamen im linken Menü klicken, erscheinen die erwünschten Informationen.

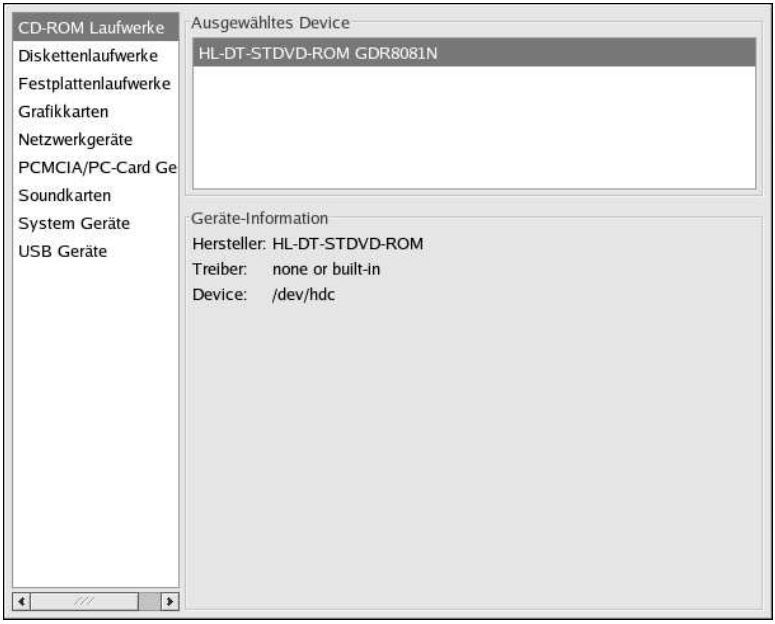

Abbildung 42-3. Hardware Browser

Sie können auch mit dem Befehl `lspci` alle PCI-Geräte auflisten. Mit dem Befehl `lspci -v` erhalten Sie nähere Informationen und mit `lspci -vv` eine sehr detaillierte Ausgabe.

Mit `lspci` können Sie z.B. den Hersteller, Modell und Speicherkapazität der Grafikkarte eines Systems in Erfahrung bringen:

```
01:00.0 VGA compatible controller: Matrox Graphics, Inc. MGA G400 AGP (rev 04) \
(prog-if 00 [VGA])
Subsystem: Matrox Graphics, Inc. Millennium G400 Dual Head Max
Flags: medium devsel, IRQ 16
Memory at f4000000 (32-bit, prefetchable) [size=32M]
Memory at fcffc000 (32-bit, non-prefetchable) [size=16K]
Memory at fc000000 (32-bit, non-prefetchable) [size=8M]
Expansion ROM at 80000000 [disabled] [size=64K]
Capabilities: [dc] Power Management version 2
Capabilities: [f0] AGP version 2.0
```

Mit `lspci` kann auch die Netzwerkkarte Ihres Systems ermittelt werden, wenn Sie den Hersteller oder das Modell nicht kennen.

42.5. Zusätzliche Ressourcen

Um noch mehr darüber zu erfahren, wie Sie Systeminformationen sammeln können, stehen Ihnen die folgenden Ressourcen zur Verfügung.

42.5.1. Installierte Dokumentation

- `ps --help` — Mit dem Befehl `ps --help` wird eine Liste mit Optionen angezeigt, die mit `ps` verwendet werden können.
- `top` man-Seite — Geben Sie `man top` ein, um weitere Informationen zu `top` und den vielen dazugehörigen Optionen zu erhalten.
- `free` man-Seite — Geben Sie `man free` ein, um weitere Informationen zu `free` und den vielen dazugehörigen Optionen zu erhalten.
- `df` man-Seite — Geben Sie `man df` ein, um mehr Informationen zu `df` und den vielen dazugehörigen Optionen zu erhalten.
- `du` man-Seite — Geben Sie `man du` ein, um weitere Informationen zu `du` und den vielen dazugehörigen Optionen zu erhalten.
- `lspci` man-Seite — Geben Sie `man lspci` ein, um weitere Informationen zu `lspci` und den vielen dazugehörigen Optionen zu erhalten.
- `/proc/` — Der Inhalt des `/proc/` Verzeichnisses kann auch dazu dienen, detailliertere Systeminformationen zu sammeln. Im *Red Hat Enterprise Linux Referenzhandbuch* finden Sie zusätzliche Informationen zum `/proc/` Verzeichnis.

42.5.2. Bücher zum Thema

- *Red Hat Enterprise Linux Introduction to System Administration*; Red Hat, Inc. — Enthält ein Kapitel zur Überwachung von Ressourcen.

Kapitel 43.

OProfile

OProfile ist ein Tool mit geringem Overhead zur systemweiten Leistungsüberwachung. Es verwendet die Leistungsüberwachungs-Hardware auf dem System, um Information über den Kernel und die Befehle des Systems herauszufinden, wie z.B. wann Speicherkapazität zugewiesen wird, die Anzahl der Anfragen bezüglich L2-Cache und die Anzahl der erhaltenen Hardware-Unterbrechungen. Auf einem Red Hat Enterprise Linux System muss das `oprofile` RPM-Paket installiert sein, damit dieses Tool verwendet werden kann.

Bei vielen Prozessoren ist eine spezielle Leistungsüberwachungs-Hardware dabei. Diese Hardware ermöglicht es, herauszufinden, wann gewisse Ereignisse stattfinden (z.B. wenn gesuchte Daten nicht in Cache sind). Die Hardware nimmt normalerweise die Form von einem oder mehreren *counters* (Zähler) an, die bei jedem Ereignis erhöht werden. Wenn der Wert der Zähler "hinaufklettert," wird eine Unterbrechung verursacht, wodurch möglich wird, die Menge der Details (und des Overhead) zu kontrollieren, die bei der Leistungsüberwachung entsteht.

OProfile verwendet diese Hardware (oder einen auf einer Zeituhr basierenden Ersatz, wenn keine Leistungsüberwachungs-Hardware vorhanden ist), um *samples* (Proben) von leistungsbezogenen Daten einzuholen, und zwar jedes Mal, wenn ein Zähler eine Unterbrechung verursacht. Diese Proben werden in regelmäßigen Abständen auf Diskette geschrieben. Später können die in den Proben enthaltenen Daten dazu verwendet werden, Berichte über die Leistung auf System-Level und auf Anwendungs-Level zu erstellen.

Wichtig

Die Unterstützung für OProfile in Red Hat Enterprise Linux 3 basiert auf dem rückgeführten Code von der 2.5 Kernel-Entwicklung. Wenn auf die OProfile Dokumentation verwiesen wird, dann gelten 2.5 spezifische Eigenschaften für OProfile in Red Hat Enterprise Linux 3, obwohl die Kernel-Version 2.4 ist. Gleichfalls gelten Oprofile-Eigenschaften, die Kernel 2.4 spezifisch sind, *nicht* für Red Hat Enterprise Linux 3.

OProfile ist ein nützliches Tool, aber bitte beachten Sie bei der Verwendung folgende Einschränkungen:

- *Verwendung von gemeinsamen Bibliotheken* — Proben für Codes in gemeinsamen Bibliotheken sind nicht mit der gegenständlichen Anwendung verbunden, außer es wird die `--separate=library` Option verwendet.
- *Leistungsüberwachungs-Proben sind ungenau* — Wenn ein Leistungsüberwachungs-Register eine Probe auslöst, ist die Handhabung der Unterbrechungen nicht so präzise wie eine Ausnahme mit Nullunterteilung. Wegen der außer-Betrieb-Ausführung von Anordnungen durch den Prozessor ist es möglich, dass die Probe auf einer nahegelegenen Anordnung aufgezeichnet wird.
- *`oprofpp` teilt Proben für Inline-Funktionen nicht richtig zu* — `oprofpp` verwendet einen einfachen Adressbereich-Mechanismus, um zu bestimmen, in welcher Funktion eine Adresse sich befindet. Proben für Inline-Funktion sind nicht mit der Inline-Funktion verbunden, sondern eher mit der Funktion, in die die Inline-Funktion eingesetzt wurde.
- *OProfile sammelt Daten von mehreren Durchläufen an* — OProfile ist eine systemweite Profileinrichtung und erwartet, dass Prozessoren mehrfach hoch- und heruntergefahren werden. Deswegen sammeln sich Daten von mehreren Durchläufen an. Verwenden Sie den Befehl `opcontrol --reset`, um die Proben von vorherigen Durchläufen zu löschen.

- *Leistungsprobleme, die nicht CPU-limitiert sind* — OProfile ist darauf ausgerichtet, Probleme bei CPU-limitierten Prozessen zu finden. OProfile kann keine schlafenden Prozesse identifizieren, weil diese an Sperrungen in Warteposition sind oder auf andere Ereignisse warten (z.B. dass ein I/O-Gerät einen Vorgang beendet).

In Red Hat Enterprise Linux haben nur die Multi-Prozessor-(SMP)-Kernels OProfile-Unterstützung. Um festzustellen, welcher Kernel gerade läuft, geben Sie folgenden Befehl ein:

```
uname -r
```

Wenn die angezeigte Kernel-Version mit `.entsmp` endet, dann läuft der Multi-Prozessor-Kernel. Wenn nicht, installieren Sie ihn über Red Hat Network oder von den mitgelieferten CDs, auch wenn das System kein Multi-Prozessor-System ist. Der Multi- Prozessor Kernel kann auf einem Single-Prozessor-System laufen.

43.1. Übersicht der Tools

Tabelle 43-1 bietet eine kurze Übersicht über die Tools, die mit dem `oprofile`-Paket geliefert werden.

Befehl	Beschreibung
`opcontrol`	Konfiguriert, welche Daten gesammelt werden. Für Details siehe Abschnitt 43.2.
`op_help`	Zeigt verfügbare Ereignisse für den System-Prozessor an, zusätzlich eine kurze Beschreibung jedes Ereignisses.
`op_merge`	Verbindet mehrere Proben derselben ausführbaren Datei. Für Details siehe Abschnitt 43.5.4
`op_time`	Gibt einen Überblick über alle erfassten ausführbaren Dateien.
`op_to_source`	Kreiert eine annotierte Quelle für eine ausführbare Datei, wenn die Anwendung mit Debbugging-Symbolen zusammengestellt wurde. Für Details siehe Abschnitt 43.5.3.
`oprofiled`	Führt einen Daemon aus, um Probedaten in regelmäßigen Abständen auf Diskette zu schreiben
`oprofpp`	Holt Profildaten ein. Für Details siehe Abschnitt 43.5.2.
`op_import`	Wandelt Dateien von Probe-Datenbanken von einer fremden Binärdatei in das Heimformat des Systems um. Verwenden Sie diese Option nur, wenn Sie eine Probe-Datenbank von einer anderen Architektur analysieren.

Tabelle 43-1. OProfile-Befehle

43.2. Konfiguration von OProfile

Bevor OProfile ausgeführt werden kann, muss es konfiguriert werden. Es muss zumindest gewählt werden, ob der Kernel beobachtet werden soll (oder ob er nicht beobachtet werden soll). Die folgenden Abschnitte beschreiben, wie die `opcontrol` Utility verwendet wird, um OProfile zu konfigurieren. Beim Ausführen der `opcontrol`Befehle werden die Setup-Optionen in der `/root/.oprofile/daemonrc` Datei gespeichert.

43.2.1. Bestimmung des Kernels

Stellen Sie zuerst ein, ob OProfile den Kernel beobachten soll. Das ist die einzige Konfigurationsoption, die nötig ist, um OProfile zu starten. Alle anderen Einstellungen sind fakultativ.

Um den Kernel zu beobachten, führen Sie folgenden Befehl als Root aus:

```
opcontrol --vmlinux=/boot/vmlinux-`uname -r`
```

Um einzustellen, dass OProfile den Kernel nicht beobachten soll, führen Sie den folgenden Befehl als Root aus:

```
opcontrol --no-vmlinux
```

Dieser Befehl lädt auch das `oprofile` Kernel-Module (wenn es noch nicht geladen wurde) and erstellt das `/dev/oprofile/` Verzeichnis, wenn es noch nicht existiert. Für Details über dieses Verezichnis siehe Abschnitt 43.6 .

Anmerkung

Auch wenn OProfile nicht so konfiguriert ist, dass es ein Profil des Kernels erstellt, muss der SMP-Kernel trotzdem ausgeführt sein, damit das `oprofile` Modul geladen werden kann.

Die Einstellung, ob Proben innerhalb des Kernels gesammelt werden sollen, bezieht sich darauf, welche Daten gesammelt werden, nicht wie oder wo die gesammelten Daten gespeichert werden. Um unterschiedliche Probedateien für den Kernel und die Anwendungsbibliotheken zu erstellen, siehe Abschnitt 43.2.3.

43.2.2. Einstellung der zu beobachtenden Ereignisse

Die meisten Prozessoren enthalten *counters* (Zähler), die von OProfile verwendet werden, um bestimmte Ereignisse zu beobachten. Wie in Tabelle 43-2 gezeigt wird, hängt die Anzahl der verfügbaren Zähler vom Prozessor ab

Prozessor	`cpu_type`	Anzahl der Zähler
Pentium Pro	i386/ppro	2
Pentium II	i386/pii	2
Pentium III	i386/piii	2
Pentium 4 (Non-Hyper-Threaded)	i386/p4	8
Pentium 4 (Hyper-Threaded)	i386/p4-ht	4
Athlon	i386/athlon	4
AMD64	x86-64/hammer	4
Itanium	ia64/itanium	4
Itanium 2	ia64/itanium2	4
TIMER_INT	Timer	1
IBM eServer iSeries	Timer	1

Prozessor	cpu_type	Anzahl der Zähler
IBM eServer pSeries	Timer	1
IBM eServer S/390	Timer	1
IBM eServer zSeries	Timer	1

Tabelle 43-2. OProfile Prozessoren und Zähler

Verwenden Sie Tabelle 43-2 um sicherzustellen, dass der richtige Prozessor-Typ gefunden wurde, und um herauszufinden, wieviele Ereignisse gleichzeitig beobachtet werden können. `timer` wird verwendet, wenn der Prozessor-Typ keine unterstützte Leistungsbeobachtungs-Hardware hat.

Wenn `timer` verwendet wird, können für keinen Prozessor Ereignisse eingestellt werden, weil die Hardware keine Unterstützung für Hardware-Leistungszähler hat. Stattdessen wird die Zeituhr (Timer)-Unterbrechung für die Erstellung des Profils verwendet.

Wenn `timer` nicht als Prozessor-Typ verwendet wird, können die beobachteten Ereignisse verändert werden. Für den Prozessor wird standardmäßig Zähler 0 als ein auf Zeit basierendes Ereignis eingestellt. Wenn mehr als ein Zähler am Prozessor vorhanden ist, werden außer Zähler 0 keine anderen Zähler standardmäßig auf ein Ereignis eingestellt. Die standardmäßig beobachteten Ereignisse werden in Tabelle 43-3 angezeigt.

Prozessor	Standard-Ereignis für Zähler 0	Beschreibung
Pentium Pro, Pentium II, Pentium III, Athlon, AMD64	CPU_CLK_UNHALTED	Die Uhr des Prozessors wird nicht angehalten
Pentium 4 (HT und nicht-HT)	GLOBAL_POWER_EVENTS	Die Zeit, in der der Prozessor nicht gestoppt wird.
Itanium 2	CPU_CYCLES	CPU Cycles
TIMER_INT	(keine)	Probe für jede Zeituhr-Unterbrechung

Tabelle 43-3. Standard-Ereignisse

Die Anzahl der Ereignisse, die zugleich beobachtet werden können, wird durch die Anzahl der Zähler für den Prozessor bestimmt. Allerdings ist dies keine direkte Beziehung. Bei manchen Prozessoren müssen gewisse Ereignisse zu bestimmten Zählern vorgezeichnet werden.

```
cat /dev/oprofile/cpu_type
```

Die verfügbaren Ereignisse variieren je nach Typ des Prozessors. Um zu bestimmen, welche Ereignisse zur Profilerstellung verfügbar sind, führen Sie den folgenden Befehl als Root aus (die Liste bezieht sich auf den Prozessor-Typ des Sytems):

```
op_help
```

Die Ereignisse für jeden Zähler können über die Befehlszeile oder mit einer grafischen Schnittstelle konfiguriert werden. Wenn der Zähler nicht auf ein bestimmtes Ereignis eingestellt werden kann, wird eine Fehlermeldung angezeigt.

Verwenden Sie `opcontrol`, um das Ereignis für jeden konfigurierbaren Zähler über die Befehlszeile einzustellen:

```
opcontrol --ctrlN-event=<event-name>
```

Ersetzen Sie *N* mit der Zählernummer (beginnend mit 0), und ersetzen Sie <*event-name*> mit dem exakten Namen des Ereignisses von `op_help`.

43.2.2.1. Proberate

Standardmäßig ist eine auf Zeit basierende Ereignisgruppe ausgewählt. Sie erzeugt etwa 2000 Proben pro Sekunde pro Prozessor. Wenn die Zeituhr-Unterbrechung verwendet wird, ist die Zeituhr auf die augenblickliche Rate eingestellt und kann nicht vom Benutzer eingestellt werden. Wenn der `cpu_type` nicht `timer` ist, kann jedes Eregnis eine*sampling rate* Einstellung haben. Die Sampling Rate (Proberate) ist Anzahl der Ereignisse zwischen jedem Probe-Schnappschuss.

Wenn das Ereignis für den Zähler eingestellt wird, können Sie auch eine Proberate bestimmen:

```
opcontrol --ctrN-event=<event-name> --ctrN-count=<sample-rate>
```

Ersetzen Sie <*sample-rate*> mit der Anzahl der Ereignisse, die abgewartet werden sollen, bevor eine neue Probe gezogen wird. Je kleiner die Anzahl, umso öfter die Proben. Für Ereignisse, die nicht oft passieren, muss eine niedrigere Anzahl eingestellt werden, damit die Ereignismomente erfasst werden.

Achtung

Seien Sie extrem vorsichtig, wenn Sie die Proberate einstellen. Zu häufige Proben können das System überladen. Das System reagiert dann wie eingefroren oder es friert tatsächlich ein.

43.2.2.2. Unit-Masken

Wenn der `cpu_type` nicht `timer` ist, können *unit masks* notwendig sein, um das Ereignis näher zu bestimmen.

Unit Masken für jedes Ereignis können mit dem `op_help` Befehl angezeigt werden. Die Werte für jede Unit-Maske werden in einem hexadezimalen Format angezeigt. Um mehr als eine Unit-Maske zu bestimmen, müssen die hexadezimalen Werte kombiniert werden, indem eine bitmäßige *or* Operation angewendet wird.

```
opcontrol --ctrN-event=<event-name> --ctrN-count=<sample-rate> --ctrN-unit-mask=<value>
```

43.2.3. Trennung von Kernel- und Benutzerspeicher-Profilen

Standardmäßig wird für jedes Ereignis Information im Kernel- und im Benutzer-Modus eingeholt. Damit OProfile keine Ereignisse für einen bestimmten Zähler im Kernel-Modus zählt, führen Sie eine Konfiguration mit folgendem Befehl aus (wobei *N* die Zählernummer ist):

```
opcontrol --ctrN-kernel=0
```

Führen Sie den folgenden Befehl aus, um für den Zähler wieder Proben im Kernel-Modus zu starten:

```
opcontrol --ctrN-kernel=1
```

Damit OProfile keine Ereignisse für einen bestimmten Zähler im Benutzer-Modus zählt, führen Sie den folgenden Befehl aus (wobei *N* die Zählernummer ist):

```
opcontrol --ctrN-user=0
```

Führen Sie den folgenden Befehl aus, um für den Zähler wieder Proben im Benutzer-Modus zu starten:

```
opcontrol --ctrN-user=1
```

Wenn der OProfile-Daemon die Profildaten in Probedateien schreibt, kann er die Kernel- und Bibliotheks-Profildaten in jeweils unterschiedliche Probedateien schreiben. Konfigurieren Sie, wie der Daemon die Probedateien schreibt, mit dem folgenden Root- Befehl:

```
opcontrol --separate=<choice>
```

<choice> kann eines der folgenden sein:

- `none` — die Profile nicht voneinander trennen (Standard)
- `library` — Profile per Anwendung für Bibliotheken erzeugen
- `kernel` — Profile per Anwendung für den Kernel und die Kernel-Module erzeugen
- `all` — Profile per Anwendung für Bibliotheken und für den Kernel und die Kernel-Module erzeugen

Wenn `--separate=library` verwendet wird, enthält der Probedateiname den Namen der ausführbaren Datei und den Namen der Bibliothek.

43.3. Starten und Anhalten von OProfile

Um das Beobachten des Systems mit OProfile zu starten, führen Sie folgenden Befehl als Root aus:

```
opcontrol --start
```

Eine Anzeige ähnlich der folgenden wird angezeigt:

```
Using log file /var/lib/oprofile/oprofiled.log
Daemon started.
Profiler running.
```

Die Einstellungen in `/root/.oprofile/daemonrc` werden verwendet.

Der OProfile Daemon, `oprofiled`, wird gestartet;er schreibt die Probedaten in regelmäßigen Abständen in das `/var/lib/oprofile/samples/` Verzeichnis. Die Logdatei für den Daemon findet sich unter `/var/lib/oprofile/oprofiled.log`.

Wenn OProfile mit anderen Konfigurationsoptionen neu gestartet wird, werden die Probedateien der vorherigen Abläufe im Verzeichnis`/var/lib/oprofile/samples/session-`*N* gesichert, wobei *N* die Nummer der zuvor gesicherten Abläufe plus 1 ist.

```
Backing up samples file to directory /var/lib/oprofile/samples//session-1
Using log file /var/lib/oprofile/oprofiled.log
Daemon started.
Profiler running.
```

Um den Profilersteller anzuhalten, führen Sie folgenden Befehl als Root aus:

```
opcontrol --shutdown
```

43.4. Speicherung von Daten

Manchmal ist es nützlich, Proben zu einer bestimmten Zeit zu speichern. Wenn z.B. das Profil für eine ausführbare Datei erstellt wird, kann es nützlich sein, verschiedene Proben, die auf verschiedenen Eingabedatenreihen beruhen, einzuholen. Wenn die Anzahl der Ereignisse, die beobachtet werden soll, die Anzahl der für den Prozessor verfügbaren Zähler übersteigt, können mehrere Durchläufe von OProfile zur Datensammlung verwendet werden. Die Probedateien werden dabei jedes Mal in eine andere Datei gespeichert.

Um die aktuelle Gruppe von Probedateien zu speichern, führen Sie folgenden Befehl aus, indem Sie <*name*> mit einem einmaligen beschreibenden Namen für den aktuellen Ablauf ersetzen.

```
opcontrol --save=<name>
```

Das Verzeichnis `/var/lib/oprofile/samples/`*name*`/` wird erstellt und die aktuellen Probedateien werdenhineinkopiert.

43.5. Datenanalyse

In regelmäßigen Abständen holt der OProfile Daemon, `oprofiled` die Proben ein und shreibt sie in das `/var/lib/oprofile/samples/` Verzeichnis. Bevor Sie die Daten lesen, stellen Sie sicher, dass alle Daten in dieses Verzeichnis geschrieben worden sind. Führen Sie dazu folgenden Befehl als Root aus:

```
opcontrol --dump
```

Der Name jeder Probedateien basiert auf dem Namen der ausführbaren Datei, wobei ein geschwungenes Klammer-zu-Zeichen (`}`) alle Schrägstriche (`/`) ersetzt. Der Dateiname endet mit einem Rautezeichen (`#`), gefolgt von der Nummer des Zählers, der für diese Probedatei verwendet wurde. Die folgende Datei enthält z.B. die Probedaten für die ausführbare `/sbin/syslogd` Datei, die mit Zähler 0 gesammelt wurden.

```
}sbin}syslogd#0
```

Zur Profilerstellung der bereits eingeholten Daten stehen folgende Tools zur Verfügung:

- `op_time`
- `oprofpp`
- `op_to_source`
- `op_merge`

Verwenden Sie diese Tools gemeinsam mit den Binärdateien, für die Profile erstellt wurden, um Berichte zu erstellen, die noch weiter analysiert werden können.

Warnung

Die ausführbare Datei, für die ein Profil erstellt wird, muss mit diesen Tools zur Datenanalyse verwendet werden. Wenn die Datei sich verändern muss, nachdem die Daten eingeholt wurden, sichern Sie die verwendete ausführbare Datei und auch die Probedateien.

Proben für jede ausführbare Datei werden in eine einzige Probedatei geschrieben. Proben von jeder dynamisch verbundenen Bibliothek werden auch in eine einzige Probedatei geschrieben. Wenn die

ausführbare Datei, die beobachtet wird, sich verändert, während OProfile läuft, und wenn eine Probedatei für diese ausführbare Datei existiert, dann wird diese existierende Probedatei automatisch gelöscht. Deswegen muss die existierende Probedatei gesichert werden, wenn sie gebraucht wird, gemeinsam mit der verwendeten ausführbaren Datei, mit der die Probedatei erstellt wurde, bevor die ausführbare Datei mit einer neuen Version ersetzt wird. Details über das Sichern von Probedateien finden Sie unterAbschnitt 43.4.

43.5.1. Die Verwendung von `op_time`

Das `op_time` Tool bietet eine Übersicht über alle ausführbaren Dateien, für die gerade ein Profil erstellt wird.

Dies ist Teil einer Beispiels-Ausgabe:

```
581         0.2949  0.0000 /usr/bin/oprofiled
966         0.4904  0.0000 /usr/sbin/cupsd
1028        0.5218  0.0000 /usr/sbin/irqbalance
1187        0.6026  0.0000 /bin/bash
1480        0.7513  0.0000 /usr/bin/slocate
2039        1.0351  0.0000 /usr/lib/rpm/rpmq
6249        3.1722  0.0000 /usr/X11R6/bin/XFree86
8842        4.4885  0.0000 /bin/sed
31342      15.9103  0.0000 /usr/bin/gdmgreeter
58283      29.5865  0.0000 /no-vmlinux
82853      42.0591  0.0000 /usr/bin/perl
```

Jede ausführbare Datei ist auf einer eigenen Zeile aufgelistet.Die erste Spalte zeigt die Anzahl der Proben, die für die ausführbare Datei aufgezeichnet wurden. Die zweite Spalte zeigt den Prozentsatz der Proben in Relation zu der Gesamtanzahl der Proben. Die dritte Spalte ist ungenützt und die vierte Spalte zeigt den Name der ausführbaren Datei.

Siehe `op_time` man Seite für eine Liste der verfügbaren Optionen für die Befehlszeile, z.B. die `-r` Option, die verwendet wird,um die Ausgabe von der ausführbaren Datei mit der größten Anzahl von Proben bis zu jener mit der kleinsten Anzahl von Proben zu sortieren. Die `-c` Option ist auch nützlich, um eine Zählernummer zu bestimmen.

43.5.2. Die Verwendung von `oprofpp`

Um mehr detaillierte Information über eine bestimmte ausführbare Datei zu erhalten, verwenden Sie `oprofpp`:

```
oprofpp <mode> <executable>
```

<*executable*> muss den vollen Pfad zu der ausführbaren Datei erhalten, die analysiert werden soll. <*mode*> muss eines der folgenden sein:

`-l`

Probedaten anhand von Symbolen auflisten. Dies ist z.B. Teil der Ausgabe,wenn der Befehl `oprofpp -l /usr/X11R6/bin/XFree86` ausgeführt wird:

```
vma      samples  %           symbol name
...
08195d10 4        3.0303      miComputeCompositeClip
080b9180 5        3.78788     Dispatch
080cdce0 5        3.78788     FreeResource
080ce4a0 5        3.78788     LegalNewID
080ce640 5        3.78788     SecurityLookupIDByClass
080dd470 9        6.81818     WaitForSomething
```

```
080e1360 12       9.09091     StandardReadRequestFromClient
...
```

Die erste Spalte zeigt die virtuelle Speicheradresse (vma) zu Beginn. Die zweite Spalte zeigt die Anzahl der Proben für das Symbol. Die dritte Spalte zeigt den Prozentsatz der Proben für dieses Symbol in Relation zu den gesamten Proben für die ausführbare Datei, und die vierte Spalte ist der Name des Symbols.

Um die Ausgabe von der größten Anzahl der Proben zu der kleinsten zu sortieren (verkehrte Reihenfolge), verwenden Sie `-r` in Verbindung mit der `-l` Option.

`-s <symbol-name>`

Probedaten spezifisch zu einem Symbolnamen auflisten. Diese Ausgabe ist zum Beispiel von dem Befehl `oprofpp -s StandardReadRequestFromClient /usr/X11R6/bin/XFree86`:

```
vma      samples  %           symbol name
080e1360 12       100         StandardReadRequestFromClient
080e1360 1        8.33333
080e137f 1        8.33333
080e13bb 1        8.33333
080e13f4 1        8.33333
080e13fb 1        8.33333
080e144a 1        8.33333
080e15aa 1        8.33333
080e1668 1        8.33333
080e1803 1        8.33333
080e1873 1        8.33333
080e190a 2        16.6667
```

Die erste Line ist eine Zusammenfassung für die Kombination Symbol/ausführbare Datei.

Die erste Spalte besteht aus den virtuellen Speicheradressen, für die Proben erstellt wurden. Die zweite Spalte zeigt die Anzahl von Proben für die Speicheradresse. Die dritte Spalte ist der Prozentsatz von Proben für die Speicheradresse in Relation zu der Gesamtanzahl der Proben für das Symbol.

`-L`

Auflisten von Probedaten nach Symbolen mit mehr Details als `-l`. Zum Beispiel:

```
vma      samples  %           symbol name
08083630 2        1.51515     xf86Wakeup
 08083641 1        50
 080836a1 1        50
080b8150 1        0.757576    Ones
 080b8179 1        100
080b8fb0 2        1.51515     FlushClientCaches
 080b8fb9 1        50
 080b8fba 1        50
...
```

Die Daten sind die gleichen wie bei der `-l` Option, außer dass für jedes Symbol jede verwendete virtuelle Speicheradresse gezeigt wird. Für jede virtuelle Speicheradresse wird die Nummer der Proben sowie der Prozentsatz der Proben in Relation zu der Anzahl der Proben für das Symbol gezeigt.

`-g <file-name>`

Eine Ausgabe in eine Datei in `gprof` Format erzeugen. Wenn die erzeugte Datei `gmon.out`genannt wird, kann `gprof` verwendet werden,um die Daten weiter zu analysieren. Siehe `gprof` man Seite für weitere Details.

Andere Optionen, um die Daten weiter zu beschränken, sind wie folgt

`-f <file-name>`

Verwenden Sie die spezifizierte Probedatei *<file-name>*. Standardmäßig wird die Probedatei in `/var/lib/oprofile/samples/` verwendet. Verwenden Sie diese Option, um eine Probedatei von einem früheren Durchlauf festzulegen.

`-i <file-name>`

Verwenden Sie *<file-name>* als Namen für die ausführbare Datei, für die Daten eingeholt werden sollen.

`-d`

"Demangle" C++ Symbol-Namen.

`-D`

"Demangle" C++ Symbol-Namen und Vereinfachung der "demangled" Namen der STL-Bibliotheken.

`--counter <number>`

Informationen von einem festgelegten Zähler einholen. Der standardmäßige Zähler ist 0 wenn nicht anders festgelegt.

`-o`

Die Zeilennummer im Quellcode für jede Probe anzeigen. Beim Erstellen der ausführbaren Datei hätte die GCC's `-g` Option verwendet werden sollen. Andernfalls kann diese Option die Zeilennummern nicht anzeigen. Keine der Red Hat Enterprise Linux ausführbaren Dateien können standardmäßig mit dieser Option erstellt werden.

```
vma      samples  %      symbol name         linear info
0806cbb0 0        0      _start              ../sysdeps/i386/elf/start.S:47
```

`-e <symbol-name>`

Schließen Sie die Liste der Komma-getrennten Symbole von der Ausgabe aus.

`-k`

Eine zusätzliche Spalte anzeigen, die die gemeinsame Bibliothek enthält. Diese Option bringt nur Resultate, wenn der `--separate=library` option to `opcontrol` Befehl beim Konfigurieren von OProfile festgelegt wird und wenn die `--dump-gprof-file` Option nicht in Verbindung mit dieser Option verwendet wird.

`-t <format>`

Die Ausgabe in einer festgelegten Spaltenfolge anzeigen. Diese Option kann nicht mit `-g` verwendet werden.

Verwenden Sie die folgenden Buchstaben, um die Spalten darzustellen:

Buchstabe	Beschreibung
v	Virtuelle Speicheradresse
s	Anzahl der Proben
S	Anwachsende Anzahl der Proben
p	Prozentsatz der Proben in Relation zu der Gesamtanzahl von Proben für die ausführbare Datei

Buchstabe	Beschreibung
P	Anwachsender Prozentsatz der Proben in Relation zu der Gesamtanzahl der Proben für die ausführbare Datei
q	Prozentsatz der Proben in Relation zu allen ausführbaren Dateien, für die Proben erstellt wurden.
Q	Anwachsender Prozentsatz der Proben in Relation zu allen ausführbaren Dateien, für die Proben erstellt wurden
n	Symbolname
l	Dateiname oder Quelldatei und Zeilennummer samt vollem Pfad
L	Basisname des Quellcode-Dateinamens und Zeilennummer
i	Name der ausführbaren Datei samt vollem Pfad
I	Basisname der ausführbaren Datei
d	Details der Probe
h	Kopfzeilen der Spalten anzeigen

Tabelle 43-4. Buchstaben für Spaltenfolge

`--session` <*name*>

Den vollen Pfad zum Ablauf festlegen oder ein Verzeichnis bezüglich des `/var/lib/oprofile/samples/` Verzeichnisses festlegen

`-p` <*path-list*>

Eine Liste von Komma-getrennten Pfaden festlegen, in der sich die ausführbaren Dateien befinden, die analysiert werden sollen.

43.5.3. Using `op_to_source`

Das `op_to_source` Tool versucht, die Proben für bestimmte Instruktionen mit den dazugehörigen Zeilen im Quellcode zu vergleichen. Die sich ergebenden Dateien sollten die Proben in den Zeilen auf der linken Seite haben. Dies setzt auch einen Kommentar an den Beginn jeder Funktion, indem die Gesamtproben für die Funktion aufgelistet werden.

Damit diese Utility funktioniert, müssen die ausführbaren Dateien mit der GCC's `-g` Option erstellt werden. Standardmäßig werden Red Hat Enterprise Linux Pakete nicht mit dieser Option erstellt.

Die Generalsyntax für `op_to_source` lautet:

```
op_to_source --source-dir <src-dir> <executable>
```

Das Verzeichnis, in dem sich der Quellcode und die ausführbare Datei befinden, die analysiert werden sollen, muss festgelegt werden. Siehe `op_to_source` man-Seite für eine Liste zusätzlicher Optionen für die Befehlszeile.

43.5.4. Verwendung von `op_merge`

Wenn für die exakt gleiche ausführbare Datei oder Bibliothek mehrere Probedateien existieren, können die Probedateien für eine leichtere Analyse zusammengeführt werden.

Um z.B. Dateien für die Bibliothek `/usr/lib/library-1.2.3.so` zusammenzuführen, führen Sie den folgenden Befehl als Root aus:

```
op_merge /usr/lib/library-1.2.3.so
```

Die resultierende Datei ist `/var/lib/oprofile/samples/}usr}lib}library-1.2.3.so`.

Um die Proben, die zu einem bestimmten Zähler zusammengeführt werden, zu begrenzen, verwenden Sie die `-c` Option, gefolgt von der Zählernummer.

43.6. Verstehen von `/dev/profile/`

Das `/dev/oprofile/` Verzeichnis enthält das Dateiverzeichnis für OProfile. Verwenden Sie den `cat` Befehl, um die Werte der virtuellen Dateien in diesem Dateisystem anzuzeigen. Der folgende Befehl zeigt z.B. den Prozessor-Typ an, den OProfile ausfindig gemacht hat.

```
cat /dev/oprofile/cpu_type
```

In `/dev/oprofile/` existiert ein Verzeichnis für jeden Zähler. Wenn es z.B. 2 Zähler gibt, existieren die Verzeichnisse `/dev/oprofile/0/` und `dev/oprofile/1/`.

Jedes Zählerverzeichnis beinhaltet die folgenden Dateien:

- `count` — Intervall zwischen den Proben
- `enabled` — Wenn auf 0, ist der Zähler abgeschaltet und keine Proben werden für ihn gesammelt; wenn auf 1,ist der Zähler an und es werden Proben für ihn gesammelt.
- `event` — Ereignis, das beobachtet werden soll
- `kernel` — Wenn auf 0, werden für dieses Zählereignis keine Proben gesammelt, wenn der Prozessor im Kernel-Bereich ist; wenn auf 1, werden Proben gesammelt, sogar wenn der Prozessor im Kernel-Bereich ist
- `unit_mask` — Zeigt an, welche Unit-Masken für den Zähler aktiviert sind
- `user` — Wenn auf 0, werden für den Zähler keine Proben gesammelt, wenn der Prozessor im Benutzer-Bereich ist; wenn auf 1, werden Proben gesammelt, sogar wenn der Prozessor im Benutzer-Bereich ist.

Die Werte dieser Dateien können mit dem `cat` Befehl abgerufen werden.

```
cat /dev/oprofile/0/count
```

43.7. Beispielsverwendung

OProfile kann von Entwicklern verwendet werden, um die Leistung von Anwendungen zu überprüfen, aber auch von Systemadministratoren, um eine Systemanalyse durchzuführen. Zum Beispiel:

- *Stellen Sie fest, welche Anwendungen und Dienste in einem System am meisten verwendet werden* — `op_time` kann verwendet werden, um festzustellen, wieviel Prozessorzeit eine Anwendung oder ein Dienst verbraucht. Wenn das System für mehrere Dienste verwendet wird, dabei aber unter seiner Leistung bleibt, kann der Dienst, der die meiste Prozessorzeit konsumiert, auf bestimmte Systeme verlegt werden.
- *Stellen Sie die Prozessorlast fest* — Das `CPU_CLK_UNHALTED` Ereignis kann beobachtet werden, um die Prozessorlast über eine bestimmte Zeitspanne zu festzustellen. Diese Daten können dann

dazu verwendet werden, zu bestimmen, ob zusätzliche Prozessoren oder ein schnellerer Prozessor die Leistung des Systems verbessern würden.

43.8. Grafische Schnittstelle

Manche OProfile-Einstellungen können mit einer grafischen Schnittstelle festgelegt werden. Um sie zu starten, führen Sie den `oprof_start` Befehl als Root bei einem Shell Prompt aus.

Nachdem die Optionen geändert wurden, können sie durch Klicken des **Save and quit**Buttons gespeichert werden. Die Einstellungen werden in `/root/.oprofile/daemonrc`, geschrieben und die Anwendung wird beendet. Das Beenden der Anwendung beendet aber nicht das Erstellen von Proben durch OProfile.

Wenn Sie Ereignisse für die Prozessor-Zähler auf dem **Setup** Tabulator wie in Abschnitt 43.2.2besprochen einstellen wollen, wählen Sie den Zähler vom Pulldown-Menü und wählen Sie das Ereignis von der Liste. Es werden nur Ereignisse angezeigt, die für den spezifischen Zähler und die spezifische Architektur verfügbar sind. Die Schnittstelle zeigt auch an, ob die Profilerstellung läuft, außerdem werden ein paar kurze Statistiken angezeigt.

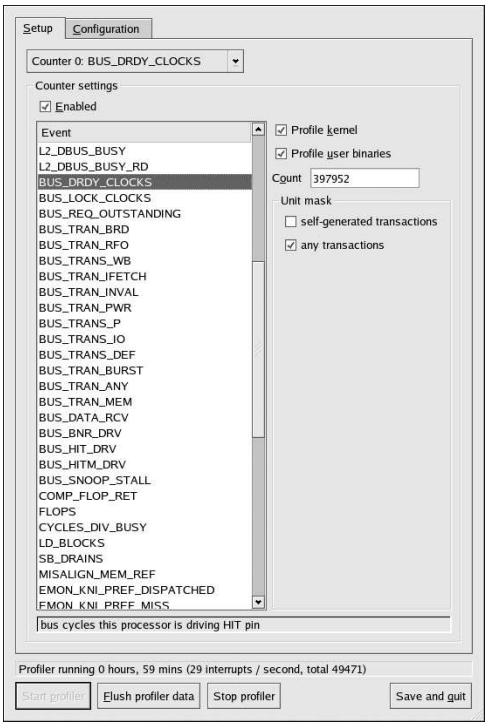

Abbildung 43-1. Einstellung von OProfile

Wählen Sie auf der rechten Seite des Tabulators die **Profile kernel** Option, um Ereignisse im Kernel-Modus für das gerade gewählte Ereignis zu zählen, wie in Abschnitt 43.2.3 besprochen. Dies en-

sprichtdem `opcontrol --ctrN-kernel=1` Befehl, wobei *N* die Zählernummer ist. Wenn diese Option nicht gewählt ist, entspricht es dem `opcontrol --ctrN-kernel=0` Befehl.

Wählen Sie die **Profil- Benutzer-Binärdateien** Option, um Ereignisse im Benutzer-Modus für das gerade gewählte Ereignis anzuzeigen, wie in Abschnitt 43.2.3 besprochen. Dies entspricht dem `opcontrol --ctrN-user=1` Befehl, wobei *N* die Zählernummer ist. Wenn diese Option nicht gewählt wird, enspricht es dem `opcontrol --ctrN-user=0` Befehl.

Verwenden Sie das **Count** Textfeld, um die Proberate für das gerade gewählte Ereignis einzustellen, wie in Abschnitt 43.2.2.1 besprochen.

Sollten für das gerade gewählte Ereignis Unit-Masken verfügbar sein, wie in Abschnitt 43.2.2.2 besprochen, werden sie im **Unit Masks** Bereich auf der rechten Seite des **Setup** Tabulators angezeigt. Kennzeichnen Sie das Kästchen neben der Unit-Maske, um sie für das Ereignis zu aktivieren.

Um ein Profil für den Kernel zu erstellen, geben Sie bei dem **Configuration** Tabulator im **Kernel image file** Textfeld den Namen und den Ort der `vmlinux` Datei des Kernels sein, der beobachtet werden soll. Damit OProfile den Kernel nicht beobachtet wählen Sie die Konfiguration **No kernel image**.

Abbildung 43-2. Konfiguration von OProfile

Wenn die **Verbose** Option gewählt wird, beinhaltet das `oprofiled` Daemon-Log mehr Information.

Wenn **Per-application kernel samples files** gewählt wird, erzeugt OProfile Profile per Anwendung für den Kernel und die Kernel-Module, wie in Abschnitt 43.2.3 besprochen. Dies entspricht dem `opcontrol --separate=kernel` Befehl. Wenn **Per-application shared libs samples files** gewählt wird, erzeugt OProfile Profile per Anwendung für Bibliotheken. Dies entspricht dem `opcontrol --separate=library` Befehl.

Um zu erzwingen, dass Daten in Probedateien geschrieben werden, wie in Abschnitt 43.5 besprochen, klicken Sie auf den **Flush profiler data** Button. Dies entspricht dem `opcontrol --dump` Befehl.

Um OProfile von der grafischen Schnittstelle aus zu starten, klicken Sie auf **Start profiler**. Um den Profilersteller anzuhalten, klicken Sie auf **Stop profiler**. Das Anhalten der Anwendung beendet nicht die weitere Erstellung von Proben durch OProfile

43.9. Zusätzliche Informationsquellen

Dieses Kapitel bezieht sich nur auf OProfile, seine Konfiguration und Verwendung. Um mehr zu erfahren, siehe folgende Informationsquellen.

43.9.1. Installierte Dokumente

- `/usr/share/doc/oprofile-0.5.4/oprofile.html` — *OProfile Manual*
- `oprofile` man-Seite — Bespricht `opcontrol`, `oprofpp`, `op_to_source`, `op_time`, `op_merge`, und `op_help`

43.9.2. Hilfreiche Websites

- http://oprofile.sourceforge.net/ — enthält die neuesten Dokumentationen, Mailing-Listen, IRC-Kanäle und mehr.

VII. Anhänge

Dieser Abschnitt enthält Anleitungen zum Kompilieren eines benutzerdefinierten Kernel, aus den von Red Hat, Inc. zur Verfügung gestellten Quelldateien.

Inhaltsverzeichnis

Anhang A.

Erstellen eines benutzerdefinierten Kernels

Viele Linux-Einsteiger fragen sich oft, weshalb sie ihren eigenen Kernel erstellen sollten. Aufgrund der Fortschritte, die beim Einsatz der Kernel-Module gemacht wurden, ist die passende Antwort auf diese Frage: Wenn Sie noch nicht wissen, weshalb Sie Ihren eigenen Kernel erstellen sollten, brauchen Sie es nicht zu tun.

Der mit Red Hat Enterprise Linux und über das Red Hat Enterprise Linux Errata System zur Verfügung gestellteKernel bietet Support für die meiste moderne Hardware und Kernelfeatures. Für die meisten Benutzer muss dieser auch nicht neu kompiliert werden. Dieser Anhang bietet einen Leitfaden für Benutzer, die Ihren Kernel neu kompilieren möchten, um mehr über diesen zu erfahren, für Benutzer, die experimentelle Feature in den Kernel kompilieren möchten, etc.

Um den Kernel mittels der über Red Hat, Inc. erhältlichen Kernelpakete zu aktualisieren, lesen Sie bitte Kapitel 39.

Warnung

Das Erstellen eines benutzerdefinierten Kernels wird nicht vom Installations-Support Team unterstützt. Weitere Informationen zum Aktualisieren des Kernels mithilfe von RPM-Paketen erhältlich über Red Hat, Inc. finden Sie unter Kapitel 39.

A.1. Vorbereitung

Bevor Sie einen benutzerdefinierten Kernel erstellen, ist es wichtig, dass eine funktionierende Notfall-Bootdiskette für den Fall, dass ein Fehler auftritt, vorhanden ist. Um eine Bootdiskette, die den aktuellen Kernel bootet, zu erstellen, führen Sie den folgenden Befehl aus:

```
/sbin/mkbootdisk `uname -r`
```

Nachdem Sie die Diskette erstellt haben, testen Sie diese, um sicherzustellen, dass das System gebootet wird.

Um den Kernel neu zu kompilieren, muss das Paket `kernel-source` installiert sein. Geben Sie folgenden Befehl ein,

```
rpm -q kernel-source
```

um zu bestimmen, ob es installiert ist. Sollte es nicht installiert sein, installieren Sie es von den Red Hat Enterprise Linux CD-ROMs oder Red Hat Network. Weitere Informationen zum Installieren von RPM-Paketen finden Sie unter Teil III.

A.2. Erstellen des Kernels

Um einen benutzerdefinierten Kernel zu erstellen (führen Sie alle Schritte als root aus):

Anmerkung

In diesem Beispiel wird 2.4.21-1.1931.2.399.ent als Kernel-Version verwendet (Ihre Kernel-Version könnte anders sein). Um Ihre Kernel-Version zu bestimmen, geben Sie den Befehl `uname -r` ein und ersetzen Sie 2.4.21-1.1931.2.399.ent mit Ihrer Kernel-Version.

1. Öffnen Sie einen Shell-Prompt, und wechseln Sie zum Verzeichnis `/usr/src/linux-2.4/`. Ab diesem Zeitpunkt müssen alle Befehle von diesem Verzeichnis ausgeführt werden.
2. Es ist wichtig, dass Sie vor dem Erstellen eines Kernels sicherstellen, dass sich der Quellcodebaum in einem vordefinierten Zustand befindet. Daher ist es empfehlenswert, dass Sie mit dem Befehl `make mrproper` beginnen. Auf diese Weise werden alle Konfigurationsdateien zusammen mit allen noch im Quellcodebaum verstreuten Überresten von vorangegangenen Kernelkompilationen entfernt. Wenn Sie bereits eine funktionierende Konfigurationsdatei `/usr/src/linux-2.4/.config` besitzen, die Sie verwenden möchten, erstellen Sie in einem anderen Verzeichnis eine Sicherungskopie, bevor Sie diesen Befehl ausführen, und kopieren Sie sie wieder zurück, nachdem Sie den Befehl durchgeführt haben.
3. Es wird empfohlen, die Konfiguration des Red Hat Enterprise Linux Standard-Kernels als Ausgangspunkt zu verwenden. Hierfür kopieren Sie die Konfigurationsdatei für die Systemarchitektur vom `/usr/src/linux-2.4/configs/` Verzeichnis nach `/usr/src/linux-2.4/.config`. Sollte das System mehr als einen Prozessor haben, kopieren Sie die Datei, die das Schlüsselwort `smp` enthält. Hat das System jedoch mehr als vier Gigabytes Speicher, kopieren Sie die Datei mit dem Schlüsselwort `hugemem`.
4. Als nächstes können Sie die Einstellungen benutzerdefinieren. Die empfohlene Methode ist das Ausführen des Befehls `make menuconfig`, um **Linux Kernel Configuration**zu starten. Das X Window System ist nicht benötigt.

   Nach Abschluss der Konfiguration, klicken Sie auf **Beenden** und wählen Sie **Beenden**, um die neueKonfigurationsdatei des Kernel zu erstellen (`/usr/src/linux-2.4/.config`).

   Auch wenn keine Änderungen an den Einstellungen vorgenommen wurden, ist das Ausführen des Befehls `make menuconfig` (oder einer der anderen Methoden für die Kernelkonfiguration) vor dem Fortfahren erforderlich.

   Andere Methoden der Kernelkonfiguration sind u.a.:

   - `make config` — Ein interaktives Textprogramm. Komponenten werden im linearen Format dargestellt und nacheinander beantwortet. Diese Methode erfordert nicht das X Window System und Antworten auf vorhergehende Fragen können nicht geändert werden.
   - `make xconfig` — Diese Methode erfordert das X Window System und das Paket `tk`. Diese Methode wird nicht empfohlen, da das Einlesen der Konfigurationsdatei unverlässlich ist.
   - `make oldconfig` — Dies ist ein nicht-interaktives Skript, dass die bestehende Konfigurationsdatei (`.config`) einliest und lediglich die Fragen stellt, die hinzugekommen sind.

Anmerkung

Um `kmod` und Kernelmodule zu verwenden, müssen Sie mit **`Yes`** zu `kmod support` und `module version (CONFIG_MODVERSIONS) support` während der Konfiguration antworten.

5. Nachdem Sie eine `/usr/src/linux-2.4/.config`-Datei erstellt haben, wählen Sie den Befehl `make dep`, um alle Abhängigkeiten korrekt einzustellen.

6. Wählen Sie den Befehl `make clean`, um den Quellcodebaum für das Bauen des Kernels vorzubereiten.
7. Es wird empfohlen, dem benutzerdefinierten Kernel, den Sie erstellen, eine geänderte Versionsnummer zu geben, damit Sie den vorhandenen Kernel nicht überschreiben. Die hier beschriebene Methode ist die einfachste im Falle eines Ausrutschers. Wenn Sie an anderen Möglichkeiten interessiert sind, finden Sie Details unter http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html oder in der Datei `Makefile` in `/usr/src/linux-2.4/`.

   Standardmäßig enthält `/usr/src/linux-2.4/Makefile` das Wort `custom` (benutzerdefiniert) am Ende der Zeile, die mit `EXTRAVERSION` anfängt. Durch das Anfügen der Zeichenfolge können Sie gleichzeitig den alten und den neuen Kernel, Version 2.4.21-1.1931.2.399.entcustom) auf Ihrem System behalten.

   Sie können auch das Datum an das Ende der Zeichenfolge anhängen, um dem Kernel einen "eindeutigen" Namen zu verleihen.
8. Für x86- und AMD64-Architekturen, kompilieren und linken Sie den Kernel mit `make bzImage`. Für die Itanium-Architektur, kompilieren und linken Sie den Kernel mit `make compressed`. Für S/390- und zSeries-Architekturen, kompilieren und linken Sie den Kernel mit `make image`. Für iSeries- und pSeries-Architekturen, kompilieren und linken Sie den Kernel mit `make boot`.
9. Erstellen Sie alle konfigurierten Module mit `make modules`.
10. Verwenden Sie den Befehl `make modules_install`, um die Kernel-Module zu installieren (auch wenn Sie keine erstellt haben). Beachten Sie den Unterstrich (_) im Befehl. Auf diese Weise werden die Kernel-Module in den Verzeichnispfad `/lib/modules/<`*`KERNELVERSION`*`>/kernel/drivers` installiert (wobei *`KERNELVERSION`* für die in `Makefile` angegebene Version steht). In diesem Beispiel wäre dies `/lib/modules/2.4.21-1.1931.2.399.entcustom/kernel/drivers/`.
11. Kopieren Sie mit `make install` den neuen Kernel und die verknüpften Dateien in die entsprechenden Verzeichnisse.

    Mit diesem Befehl installieren Sie nicht nur die Kerneldateien in das `/boot`-Verzeichnis, sondern führen auch das Skript `/sbin/new-kernel-pkg` aus, das ein neues `initrd`-Image erstellt und neue Einträge zur Bootloader-Konfigurationsdatei hinzufügt.

    Wenn das System einen SCSI-Adapter hat und den SCSI-Treiber als Modul kompiliert bzw. wenn Sie den Kernel mit ext3-Unterstützung als Modul erstellt haben (Standard in Red Hat Enterprise Linux), ist das `initrd`-Image erforderlich.
12. Sie sollten die Änderungen am `initrd`-Image und dem Bootloader überprüfen, und sicherstellen, dass die Custom-Version des Kernels anstelle von 2.4.21-1.1931.2.399.ent verwendet wird, auch wenn diese automatisch für Sie erstellt wurden. Einzelheiten finden Sie unter Abschnitt 39.5 und Abschnitt 39.6.

A.3. Zusätzliche Ressourcen

Weitere Informationen zum Linux-Kernel finden Sie in folgenden Ressourcen.

A.3.1. Installierte Dokumentationen

- `/usr/src/linux-2.4/Documentation` — Weiterführende Dokumentation zum Linux-Kernel und seinen Module. Diese Unterlagen sind für diejenigen Personen geschrieben, die sich für den Kernel-Quellcode interessieren und die Funktionsweise des Kernels verstehen möchten.

A.3.2. Hilfreiche Websites

- http://www.redhat.com/mirrors/LDP/HOWTO/Kernel-HOWTO.html — *The Linux Kernel HOWTO* vom Linux Documentation Project.
- http://www.kernel.org/pub/linux/docs/lkml/ — Die Mailingliste zum Linux-Kernel.

Stichwortverzeichnis

Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

Colophon

Die 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-Produktdokumentation besteht aus:

Sandra A. Moore — Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™ und AMD64 Architekturen* Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Installationshandbuch für IBM® eServer™ iSeries™ und IBM® eServer™ pSeries™ Architekturen* Co-Autorin des *Red Hat Enterprise Linux Schrittweise Einführung*

Tammy Fox — Verantwortliche Autorin/Bearbeiterin des *Red Hat Enterprise Linux Handbuch zur System-Administration*; Co-Autorin des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™ und AMD64 Architekturen*; Co-Autorin des *Red Hat Enterprise Linux Sicherheitshandbuch*; Co-Autorin des *Red Hat Enterprise Linux Schrittweise Einführung*; Autorin/Bearbeiterin der benutzerdefinierten DocBook Stylesheets und Skripte

Edward C. Bailey — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Introduction to System Administration*; Verantwortlicher Autor/Bearbeiter der *Release Notes*; Co-Autor des *Red Hat Enterprise Linux Installationshandbuch für x86, Itanium™ und AMD64 Architekturen*

Johnray Fuller — Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Referenzhandbuch*; Co-Autor/Co-Bearbeiter des *Red Hat Enterprise Linux Sicherheitshandbuch*; Co-Autor des *Red Hat Enterprise Linux Introduction to System Administration*

John Ha — Verantwortlicher Autor/Bearbeiter des *Red Hat Cluster Suite Configuring and Managing a Cluster*; Verantwortlicher Autor/Bearbeiter des *Red Hat Glossary*; Verantwortlicher Autor/Bearbeiter des *Red Hat Enterprise Linux Installationshandbuch für IBM® S/390® und IBM® eServer™ zSeries® Architekturen*; Co-Autor/Co-Bearbeiter des *Red Hat Enterprise Linux Sicherheitshandbuch*; Co-Autor des *Red Hat Enterprise Linux Introduction to System Administration*; Co-Autor des *Red Hat Enterprise Linux Schrittweise Einführung*

Das Red Hat-Team verantwortlich für Übersetzungen besteht aus:

Jean-Paul Aubry — Französisch

David Barzilay — Portugisisch (Brasilien)

Bernd Groh — Deutsch

James Hashida — Japanisch

Michelle Ji-yeen Kim — Koreanisch

Yelitza Louze — Spanisch

Noriko Mizumoto — Japanisch

Nadine Richter — Deutsch

Audrey Simons — Französisch

Francesco Valente — Italienisch

Sarah Saiying Wang — Einfaches Chinesisch

Ben Hung-Pin Wu — Traditionelles Chinesisch