

openSUSE

11.0

www.novell.com

06. Juni 2008

Referenz



Referenz

Copyright © 2006-2007 Novell, Inc.

Es wird die Genehmigung erteilt, dieses Dokument unter den Bedingungen der GNU Free Documentation License, Version 1.2 oder einer späteren Version, veröffentlicht durch die Free Software Foundation, zu vervielfältigen, zu verbreiten und/oder zu verändern; dies gilt ausschließlich der unveränderlichen Abschnitte, der Texte auf dem vorderen Deckblatt und der Texte auf dem hinteren Deckblatt. Eine Kopie dieser Lizenz finden Sie im Abschnitt „GNU Free Documentation License“.

SUSE®, openSUSE®, das openSUSE®-Logo, Novell®, das Novell®-Logo, das N®-Logo sind eingetragene Marken von Novell, Inc. in den USA und anderen Ländern. Linux* ist eine eingetragene Marke von Linus Torvalds. Alle anderen Drittanbieter-Marken sind das Eigentum der jeweiligen Inhaber. Ein Markensymbol (®, ™, usw.) kennzeichnet eine Marke von Novell; ein Stern (*) kennzeichnet eine Drittanbieter-Marke.

Alle Informationen in diesem Buch wurden mit größter Sorgfalt zusammengestellt. Doch auch dadurch kann hundertprozentige Richtigkeit nicht gewährleistet werden. Weder Novell, Inc., noch die SUSE LINUX GmbH noch die Autoren noch die Übersetzer können für mögliche Fehler und deren Folgen haftbar gemacht werden.

Inhaltsverzeichnis

Allgemeines zu diesem Handbuch	xi
Teil I Fortgeschrittene Implementierungsszenarien	1
1 Installation mit entferntem Zugriff	3
1.1 Installationsszenarien für die Installation auf entfernten Systemen	4
1.2 Einrichten des Servers, auf dem sich die Installationsquellen befinden	14
1.3 Vorbereitung des Bootvorgangs für das Zielsystem	25
1.4 Booten des Zielsystems für die Installation	36
1.5 Überwachen des Installationsvorgangs	40
2 Fortgeschrittene Festplattenkonfiguration	45
2.1 Verwenden der YaST-Partitionierung	45
2.2 LVM-Konfiguration	55
2.3 Soft-RAID-Konfiguration	62
Teil II Verwaltung	69
3 Online-Update	71
3.1 Definition der Begriffe	72
3.2 YaST-Online-Update	73
3.3 Aktualisierung über die Kommandozeile mit zypper	76
4 YaST im Textmodus	79
4.1 Navigation in Modulen	80

4.2	Einschränkung der Tastenkombinationen	82
4.3	YaST-Kommandozeilenoptionen	82
5	Aktualisieren des Systems und Systemänderungen	85
5.1	Aktualisieren des Systems	85
5.2	Software-Änderungen von Version zu Version	88
6	Dienstprogramme zur Systemüberwachung	101
6.1	Fehlersuche	102
6.2	Dateien und Dateisysteme	104
6.3	Hardware-Informationen	106
6.4	Netzwerke	109
6.5	Das Dateisystem <code>/proc</code>	110
6.6	Vorgänge	113
6.7	Systemangaben	117
6.8	Benutzerinformationen	120
6.9	Zeit und Datum	121
Teil III	System	123
7	32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung	125
7.1	Laufzeitunterstützung	125
7.2	Software-Entwicklung	126
7.3	Software-Kompilierung auf Doppelarchitektur-Plattformen	127
7.4	Kernel-Spezifikationen	128
8	Booten und Konfigurieren eines Linux-Systems	129
8.1	Der Linux-Bootvorgang	129
8.2	Der <code>init</code> -Vorgang	133
8.3	Systemkonfiguration über <code>/etc/sysconfig</code>	143
9	Der Bootloader	147
9.1	Auswählen eines Bootloaders	148
9.2	Booten mit GRUB	148
9.3	Konfigurieren des Bootloaders mit YaST	158
9.4	Deinstallieren des Linux-Bootloaders	163
9.5	Erstellen von Boot-CDs	163
9.6	Der grafische SUSE-Bildschirm	164
9.7	Fehlersuche	165

9.8	Weiterführende Informationen	167
10	Spezielle Systemfunktionen	169
10.1	Informationen zu speziellen Softwarepaketen	169
10.2	Virtuelle Konsolen	177
10.3	Tastaturzuordnung	177
10.4	Sprach- und länderspezifische Einstellungen	178
11	Gerätemanagement über dynamischen Kernel mithilfe von udev	183
11.1	Das /dev-Verzeichnis	183
11.2	Kernel-uevents und udev	184
11.3	Treiber, Kernel-Module und Geräte	184
11.4	Booten und erstes Einrichten des Geräts	185
11.5	Überwachen des aktiven udev-Daemons	186
11.6	Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von udev-Regeln	187
11.7	Permanente Gerätebenennung	195
11.8	Von udev verwendete Dateien	196
11.9	Weiterführende Informationen	196
12	Zugriffssteuerungslisten unter Linux	199
12.1	Traditionelle Dateiberechtigungen	199
12.2	Vorteile von ACLs	201
12.3	Definitionen	202
12.4	Arbeiten mit ACLs	202
12.5	ACL-Unterstützung in Anwendungen	211
12.6	Weiterführende Informationen	212
13	Authentifizierung mit PAM	213
13.1	Struktur einer PAM-Konfigurationsdatei	214
13.2	PAM-Konfiguration von sshd	216
13.3	Konfigurieren von PAM mit pam-config	219
13.4	Weiterführende Informationen	220
Teil IV	Services	223
14	Grundlegendes zu Netzwerken	225
14.1	IP-Adressen und Routing	228
14.2	IPv6 – Das Internet der nächsten Generation	231

14.3	Namensauflösung	241
14.4	Konfigurieren von Netzwerkverbindungen mit YaST	243
14.5	NetworkManager	263
14.6	Manuelle Netzwerkkonfiguration	264
14.7	smpppd als Einwählhelfer	279
15	SLP-Dienste im Netzwerk	283
15.1	Installation	283
15.2	SLP aktivieren	284
15.3	SLP-Frontends in openSUSE	284
15.4	Installation über SLP	285
15.5	Bereitstellen von Diensten über SLP	285
15.6	Weiterführende Informationen	286
16	Domain Name System (DNS)	287
16.1	DNS-Terminologie	287
16.2	Installation	288
16.3	Konfiguration mit YaST	289
16.4	Starten des Namensservers BIND	297
16.5	Die Konfigurationsdatei /etc/dhcpd.conf	299
16.6	Zonendateien	304
16.7	Dynamische Aktualisierung von Zonendaten	309
16.8	Sichere Transaktionen	309
16.9	DNS-Sicherheit	311
16.10	Weiterführende Informationen	311
17	DHCP	313
17.1	Konfigurieren eines DHCP-Servers mit YaST	314
17.2	DHCP-Softwarepakete	325
17.3	Der DHCP-Server dhcpd	326
17.4	Weiterführende Informationen	330
18	Zeitsynchronisierung mit NTP	331
18.1	Konfigurieren eines NTP-Client mit YaST	331
18.2	Konfigurieren von xntp im Netzwerk	336
18.3	Einrichten einer lokalen Referenzuhr	337
19	Arbeiten mit NIS	339
19.1	Konfigurieren von NIS-Servern	339
19.2	Konfigurieren von NIS-Clients	346

20 LDAP – Ein Verzeichnisdienst	349
20.1 LDAP und NIS	350
20.2 Struktur eines LDAP-Verzeichnisbaums	351
20.3 Konfigurieren eines LDAP-Servers mit YaST	355
20.4 Konfigurieren eines LDAP-Client mit YaST	361
20.5 Konfigurieren von LDAP-Benutzern und -Gruppen in YaST	369
20.6 Navigieren in der LDAP-Verzeichnisstruktur	371
20.7 Manuelles Konfigurieren eines LDAP-Servers	373
20.8 Manuelles Verwalten von LDAP-Daten	379
20.9 Weiterführende Informationen	383
21 Verteilte Nutzung von Dateisystemen mit NFS	385
21.1 Installieren der erforderlichen Software	386
21.2 Importieren von Dateisystemen mit YaST	386
21.3 Manuelles Importieren von Dateisystemen	387
21.4 Exportieren von Dateisystemen mit YaST	390
21.5 Manuelles Exportieren von Dateisystemen	397
21.6 NFS mit Kerberos	400
21.7 Weiterführende Informationen	401
22 Der HTTP-Server Apache	403
22.1 Kurzanleitung	403
22.2 Konfigurieren von Apache	405
22.3 Starten und Beenden von Apache	421
22.4 Installieren, Aktivieren und Konfigurieren von Modulen	423
22.5 Aktivieren von CGI-Skripten	432
22.6 Einrichten eines sicheren Webservers mit SSL	435
22.7 Vermeiden von Sicherheitsproblemen	442
22.8 Fehlersuche	444
22.9 Weiterführende Informationen	445
23 Einrichten eines FTP-Servers mit YaST	449
23.1 Starten des FTP-Servers	450
23.2 Allgemeine FTP-Einstellungen	451
23.3 FTP-Leistungseinstellungen	452
23.4 Authentifizierung	453
23.5 Einstellungen für Experten	453
23.6 Weitere Informationen	454

Teil V	Mobilität	455
24	Energieverwaltung	457
24.1	Energiesparfunktionen	457
24.2	ACPI	459
24.3	Ruhezustand für Festplatte	467
24.4	Das Powersave-Paket	469
25	Drahtlose Kommunikation	477
25.1	Wireless LAN	477
26	Verwenden von Tablet PCs	485
26.1	Installieren der Tablet PC-Pakete	486
26.2	Konfigurieren des Tablet-Geräts	487
26.3	Verwenden der virtuellen Tastatur	487
26.4	Drehen der Ansicht	488
26.5	Verwenden der Bewegungserkennung	489
26.6	Aufzeichnen von Notizen und Skizzen mit dem Pen	490
26.7	Fehlersuche	492
26.8	Weiterführende Informationen	494
27	Verwendung des Fingerabdrucklesers	495
27.1	Unterstützte Anwendungen und Aktionen	496
27.2	Verwalten der Fingerabdrücke mit YaST	496
27.3	Verwalten von Fingerabdrücken mit <code>tf-tool</code>	498
27.4	Weiterführende Informationen	499
Teil VI	Sicherheit	501
28	Masquerading und Firewalls	503
28.1	Paketfilterung mit iptables	503
28.2	Grundlegendes zum Masquerading	507
28.3	Grundlegendes zu Firewalls	508
28.4	SuSEfirewall2	509
28.5	Weiterführende Informationen	515
29	SSH: Secure Network Operations	517
29.1	Das Paket OpenSSH	518

29.2	Das ssh-Programm	518
29.3	scp – Sichere Kopie	518
29.4	sftp – Sichere Dateiübertragung	519
29.5	Der SSH-Daemon (sshd) –Serverseite	519
29.6	SSH-Authentifizierungsmechanismen	521
29.7	X-, Authentifizierungs- und Weiterleitungsmechanismen	522
30	Verwalten der X.509-Zertifizierung	525
30.1	Prinzipien der digitalen Zertifizierung	525
30.2	YaST-Module für die Verwaltung von Zertifizierungsstellen	530
31	Verschlüsseln von Partitionen und Dateien	545
31.1	Einrichten von verschlüsselten Dateisystemen mit YaST	546
31.2	Verwenden von verschlüsselten Home-Verzeichnissen	550
31.3	Verschlüsselung einzelner ASCII-Textdateien mit vi	551
32	Einschränken von Berechtigungen mit AppArmor	553
32.1	Installieren von Novell AppArmor	554
32.2	Aktivieren und Deaktivieren von Novell AppArmor	555
32.3	Einführung in die Erstellung von Anwendungsprofilen	556
33	Sicherheit und Vertraulichkeit	565
33.1	Lokale Sicherheit und Netzwerksicherheit	566
33.2	Tipps und Tricks: Allgemeine Hinweise zur Sicherheit	575
33.3	Zentrale Adresse für die Meldung von neuen Sicherheitsproblemen	578
A	Ein Beispielnetzwerk	579
B	GNU Licenses	581
B.1	GNU General Public License	581
B.2	GNU Free Documentation License	584

Allgemeines zu diesem Handbuch

Dieses Handbuch vermittelt Ihnen Hintergrundinformationen zur Funktionsweise von openSUSE®. Es richtet sich in der Hauptsache an Systemadministratoren und andere Benutzer mit Grundkenntnissen der Systemadministration. In diesem Handbuch wird Ihnen eine Auswahl verschiedener Anwendungen vorgestellt, die Ihnen den Berufsalltag erleichtern. Außerdem erhalten Sie hier ausführliche Beschreibungen erweiterter Installations- und Konfigurationsszenarien.

Fortgeschrittene Implementierungsszenarien

Erfahren Sie, wie Sie openSUSE von einem entfernten Standort aus einsetzen können, und machen Sie sich mit komplexen Szenarien für Festplatten-Setups vertraut.

Verwaltung

Hier lernen Sie, wie Sie Ihr openSUSE aktualisieren und konfigurieren und Ihr System im Textmodus verwalten. Außerdem lernen Sie einige wichtige Dienstprogramme für Linux-Administratoren kennen.

System

Hier werden die Komponenten des Linux-Systems erläutert, sodass Sie deren Interaktion besser verstehen.

Services

In diesem Abschnitt erfahren Sie, wie Sie die unterschiedlichen Netzwerk- und Dateidienste konfigurieren, die zum Lieferumfang von openSUSE gehören.

Mobilität

Hier erhalten Sie eine Einführung in die mobile Computernutzung mit openSUSE und lernen die verschiedenen Optionen für die kabellose Computernutzung und Energiekontrolle kennen. Außerdem lernen Sie, wie man einen Tablet PC verwendet.

Sicherheit

Machen Sie sich vertraut mit openSUSE-Sicherheitsfunktionen und erfahren Sie, wie Sie Dienste einrichten und konfigurieren können, um für ein sicheres System zu sorgen.

1 Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Funktion "Benutzerkommentare" unten auf den einzelnen Seiten der Onlinedokumentation, um Ihre Kommentare einzugeben.

2 Zusätzliche Dokumentation

Wir stellen Ihnen unsere Handbücher in verschiedenen Sprachen in den Formaten HTML und PDF zur Verfügung. Für dieses Produkt sind folgende Handbücher verfügbar:

Start

Führt Sie durch die Installation und die grundlegende Konfiguration Ihres Systems. Für Neulinge behandelt das Handbuch auch grundlegende Linux-Konzepte, wie zum Beispiel das Dateisystem, das Benutzerkonzept und Zugriffsberechtigungen und bietet einen Überblick über die Features von openSUSE für die Unterstützung tragbarer Computer. Stellt Hilfe und Rat bei Problemlösungen bereit.

KDE Quick Start

Bietet eine kurze Einführung in den KDE-Desktop und einige wichtige Anwendungen, die darauf ausgeführt werden.

GNOME Quick Start

Bietet eine kurze Einführung in den GNOME-Desktop und einige wichtige Anwendungen, die darauf ausgeführt werden.

Referenz

Vermittelt Ihnen ein grundlegendes Verständnis von openSUSE und behandelt erweiterte Aufgaben der Systemadministration. Es richtet sich in der Hauptsache an Systemadministratoren und andere Benutzer mit Grundkenntnissen der Systemadministration. Es enthält ausführliche Informationen über erweiterte Einsatzmöglichkeiten, Administration Ihres Systems, Interaktion von Schlüsselsystemkomponenten sowie die Einrichtung verschiedener Netzwerk- und Dateidienste, die openSUSE bietet.

Novell AppArmor Quick Start

Unterstützt Sie beim Verstehen der Hauptkonzepte von Novell® AppArmor.

Novell AppArmor Administration Guide

Enthält ausführliche Informationen zur Verwendung von *AppArmor* in Ihrer Umgebung.

Lessons For Lizards

Ein Community-Buchprojekt für die openSUSE-Bereitstellung. Ein Snapshot des von der Open Source-Community verfassten Handbuchs wird zusammen mit den Novel/SUSE-Handbüchern veröffentlicht. Diese Lektionen wurden in Form eines Kochbuchs verfasst und behandelten besondere und exotischere Themen als die normalen Handbücher. Weitere Informationen finden Sie unter http://developer.novell.com/wiki/index.php/Lessons_for_Lizards.

HTML-Versionen der openSUSE-Handbücher finden Sie auf dem installierten System im Verzeichnis `/usr/share/doc/manual` bzw. in den Hilfezentren Ihres KDE- oder GNOME-Desktops. Die Dokumentation erhalten Sie auch auf unserer Website unter <http://www.novell.com/documentation/opensuse110/>. Von dort können Sie die Handbücher in den Formaten PDF oder HTML herunterladen. Die Speicherorte der Handbücher auf dem Installationsdatenträger entnehmen Sie bitte den Versionshinweisen zu diesem Produkt, die Sie auf dem installierten System im Verzeichnis `/usr/share/doc/release-notes/` vorfinden.

3 Konventionen in der Dokumentation

In diesem Handbuch werden folgende typografische Konventionen verwendet:

- `/etc/passwd`: Dateinamen und Verzeichnisnamen
- *Platzhalter*: Ersetzen Sie *Platzhalter* durch den tatsächlichen Wert.
- `PATH`: die Umgebungsvariable `PATH`
- `ls, --help`: Befehle, Optionen und Parameter
- `Benutzer`: Benutzer oder Gruppen
- `Alt, Alt + F1`: Eine Taste oder Tastenkombination. Tastennamen werden wie auf der Tastatur in Großbuchstaben dargestellt.

- *Datei, Datei > Speichern unter*: Menüoptionen, Schaltflächen
- *Tanzende Pinguine* (Kapitel *Pinguine*, ↑Anderes Handbuch): Dies ist ein Verweis auf ein Kapitel in einem anderen Handbuch.

4 Informationen über die Herstellung dieses Handbuchs

Dieses Handbuch wurde in Novdoc, einem Teilsatz von DocBook (siehe <http://www.docbook.org>), geschrieben. Die XML-Quelldateien wurden mit `xmllint` überprüft, von `xsltproc` verarbeitet und mit einer benutzerdefinierten Version der stylesheets von Norman Walsh in HTML konvertiert.

5 Quellcode

Der Quellcode von openSUSE ist öffentlich verfügbar. Um den Quellcode herunterzuladen, gehen Sie vor, wie unter http://www.novell.com/products/suselinux/source_code.html beschrieben. Auf Anforderung senden wir Ihnen den Quellcode auf DVD. Wir müssen eine Gebühr von 15 US-Dollar bzw. 15 Euro für Erstellung, Verpackung und Porto berechnen. Um eine DVD mit dem Quellcode anzufordern, senden Sie eine E-Mail an sourcedvd@suse.de [<mailto:sourcedvd@suse.de>] oder senden Sie Ihre Anforderung per Post an folgende Adresse:

```
SUSE Linux Products GmbH
Product Management openSUSE
Maxfeldstr. 5
D-90409 Nürnberg
Germany
```

6 Danksagung

Die Entwickler von Linux treiben in weltweiter Zusammenarbeit mit hohem freiwilligem Einsatz die Weiterentwicklung von Linux voran. Wir danken ihnen für ihr Engagement – ohne sie gäbe es diese Distribution nicht. Bedanken wollen wir uns außerdem auch bei Frank Zappa und Pawar. Unser besonderer Dank geht selbstverständlich an Linus Torvalds.

Viel Spaß!

Ihr SUSE-Team

Teil I. Fortgeschrittene Implementierungsszenarien

Installation mit entferntem Zugriff

1

Es gibt mehrere Möglichkeiten, openSUSE® zu installieren. Abgesehen von der normalen Medieninstallation, die in Kapitel 1, *Installation mit YaST* (↑Start) beschrieben wird, können Sie aus mehreren netzwerkbasierten Ansätzen auswählen oder eine voll-automatische Installation von openSUSE ausführen.

Die einzelnen Methoden werden über zwei kurze Checklisten eingeführt: in einer werden die Voraussetzungen für diese Methoden aufgeführt, in der anderen die grundlegenden Verfahren dargestellt. Anschließend werden alle in diesen Installationsszenarien verwendeten Techniken ausführlicher erläutert.

ANMERKUNG

In den folgenden Abschnitten wird das System, auf dem die neue openSUSE-Installation ausgeführt wird, als *Zielsystem* oder *Installationsziel* bezeichnet. Der Begriff *Installationsquelle* wird für alle Quellen der Installationsdaten verwendet. Dazu gehören physische Medien, z. B. CD und DVD, sowie Netzwerkserver, die die Installationsdaten im Netzwerk verteilen.

1.1 Installationsszenarien für die Installation auf entfernten Systemen

In diesem Abschnitt werden die gängigsten Installationsszenarien für Installationen auf entfernten Systemen beschrieben. Prüfen Sie für jedes Szenario die Liste der Voraussetzungen und befolgen Sie das für dieses Szenario beschriebene Verfahren. Falls Sie für einen bestimmten Schritt ausführliche Anweisungen benötigen, folgen Sie den entsprechenden Links.

WICHTIG

Die Konfiguration des X Window Systems ist nicht Teil des entfernten Installationsvorgangs. Melden Sie sich nach Abschluss der Installation beim Zielsystem als `root` an, geben Sie `telinit 3` ein und starten Sie `SaX2`, um die Grafikkarte wie in Abschnitt „Einrichten von Grafikkarte und Monitor“ (Kapitel 2, *Einrichten von Hardware-Komponenten mit YaST*, ↑Start) beschrieben zu konfigurieren.

1.1.1 Einfache Installation mit entferntem Zugriff über VNC – Statische Netzwerkkonfiguration

Diese Art der Installation erfordert physischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten. Die Installation selbst wird vollständig von einer entfernten Arbeitsstation gesteuert, die mit dem Installationsprogramm über VNC verbunden ist. Das Eingreifen des Benutzers ist wie bei der manuellen Installation erforderlich (siehe Kapitel 1, *Installation mit YaST* (↑Start)).

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Entfernte Installationsquelle: NFS, HTTP, FTP oder SMB mit einer funktionierenden Network-Verbindung

- Zielsystem mit funktionierender Netzwerkverbindung
- Steuersystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähiger Browser (Firefox, Konqueror, Internet Explorer oder Opera)
- Physisches Bootmedium (CD oder DVD) zum Booten des Zielsystems
- Gültige statische IP-Adressen, die der Installationsquelle und dem Steuersystem bereits zugewiesen sind
- Gültige statische IP-Adresse, die dem Zielsystem zugewiesen wird

Gehen Sie wie folgt vor, um diese Art der Installation durchzuführen:

- 1** Richten Sie die Installationsquelle ein wie in [Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 14) beschrieben. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zu SMB-Installationsquellen finden Sie in [Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 23).
- 2** Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des openSUSE-Medienkits.
- 3** Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie mithilfe der Eingabeaufforderung für die Boot-Optionen die entsprechenden VNC-Optionen und die Adresse der Installationsquelle fest. Dies wird ausführlich in [Abschnitt 1.4, „Booten des Zielsystems für die Installation“](#) (S. 36) beschrieben.

Das Zielsystem bootet in eine textbasierte Umgebung und gibt die Netzwerkadresse und Anzeigenummer an, unter der die grafische Installationsumgebung über eine VNC-Viewer-Anwendung oder einen Browser erreichbar ist. VNC-Installationen geben sich selbst über OpenSLP bekannt und können, sofern die Firewall-Einstellungen dies zulassen, mithilfe von Konqueror im Modus `service:/` oder `slp:/` ermittelt werden.

- 4** Öffnen Sie auf der steuernden Arbeitsstation eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in [Abschnitt 1.5.1, „VNC-Installation“](#) (S. 40) beschrieben eine Verbindung zum Zielsystem her.

- 5 Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑Start) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6 Schließen Sie die Installation ab.

1.1.2 Einfache Installation mit entferntem Zugriff über VNC – Dynamische Netzwerkkonfiguration

Diese Art der Installation erfordert physischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten. Die Netzwerkkonfiguration erfolgt über DHCP. Die Installation selbst wird vollständig über eine entfernte Arbeitsstation ausgeführt, die über VNC mit dem Installationsprogramm verbunden ist. Für die eigentliche Konfiguration ist jedoch das Eingreifen des Benutzers erforderlich.

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Entfernte Installationsquelle: NFS, HTTP, FTP oder SMB mit einer funktionierenden Network-Verbindung
- Zielsystem mit funktionierender Netzwerkverbindung
- Steuersystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähiger Browser (Firefox, Konqueror, Internet Explorer oder Opera)
- Physisches Bootmedium (CD, DVD oder benutzerdefinierte Bootdiskette) zum Booten des Zielsystems
- Laufender DHCP-Server, der IP-Adressen zur Verfügung stellt

Gehen Sie wie folgt vor, um diese Art der Installation durchzuführen:

- 1 Richten Sie die Installationsquelle ein wie in **Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“** (S. 14) beschrieben. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen

zu SMB-Installationsquellen finden Sie in [Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 23).

- 2 Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des openSUSE-Medienkits.
- 3 Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie mithilfe der Eingabeaufforderung für die Boot-Optionen die entsprechenden VNC-Optionen und die Adresse der Installationsquelle fest. Dies wird ausführlich in [Abschnitt 1.4, „Booten des Zielsystems für die Installation“](#) (S. 36) beschrieben.

Das Zielsystem bootet in eine textbasierte Umgebung und gibt die Netzwerkadresse und Anzeigenummer an, unter der die grafische Installationsumgebung über eine VNC-Viewer-Anwendung oder einen Browser erreichbar ist. VNC-Installationen geben sich selbst über OpenSLP bekannt und können, sofern die Firewall-Einstellungen dies zulassen, mithilfe von Konqueror im Modus `service:/` oder `slp:/` ermittelt werden.

- 4 Öffnen Sie auf der steuernden Arbeitsstation eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in [Abschnitt 1.5.1, „VNC-Installation“](#) (S. 40) beschrieben eine Verbindung zum Zielsystem her.
- 5 Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑Start) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6 Schließen Sie die Installation ab.

1.1.3 Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN

Diese Art der Installation wird vollständig automatisch durchgeführt. Der Zielcomputer wird über den entfernten Zugriff gestartet und gebootet. Das Eingreifen des Benutzers ist lediglich für die eigentliche Installation erforderlich. Dieser Ansatz ist für standortübergreifende Implementierungen geeignet.

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Entfernte Installationsquelle: NFS, HTTP, FTP oder SMB mit einer funktionierenden Network-Verbindung
- TFTP-Server
- Laufender DHCP-Server für Ihr Netzwerk
- Zielsystem, das PXE-Boot-, Netzwerk- und Wake-on-LAN-fähig, angeschlossen und mit dem Netzwerk verbunden ist
- Steuersystem mit funktionierender Netzwerkverbindung und VNC-Viewer-Software oder Java-fähiger Browser (Firefox, Konqueror, Internet Explorer oder Opera)

Gehen Sie wie folgt vor, um diese Art der Installation auszuführen:

- 1** Richten Sie die Installationsquelle ein wie in [Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 14) beschrieben. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver aus oder konfigurieren Sie eine SMB-Installationsquelle wie in [Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 23) beschrieben.
- 2** Richten Sie einen TFTP-Server ein, auf dem das Boot-Image gespeichert wird, das vom Zielsystem abgerufen werden kann. Die Konfiguration eines solchen Servers wird in [Abschnitt 1.3.2, „Einrichten eines TFTP-Servers“](#) (S. 27) beschrieben.
- 3** Richten Sie einen DHCP-Server ein, der IP-Adressen für alle Computer bereitstellt und dem Zielsystem den Speicherort des TFTP-Servers bekannt gibt. Die Konfiguration eines solchen Servers wird in [Abschnitt 1.3.1, „Einrichten eines DHCP-Servers“](#) (S. 25) beschrieben.
- 4** Bereiten Sie das Zielsystem für PXE-Boot vor. Dies wird ausführlich in [Abschnitt 1.3.5, „Vorbereiten des Zielsystems für PXE-Boot“](#) (S. 34) beschrieben.
- 5** Initiieren Sie den Bootvorgang des Zielsystems mithilfe von Wake-on-LAN. Die Konfiguration eines solchen Servers wird in [Abschnitt 1.3.7, „Wake-on-LAN“](#) (S. 35) beschrieben.

- 6 Öffnen Sie auf der steuernden Arbeitsstation eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in [Abschnitt 1.5.1, „VNC-Installation“](#) (S. 40) beschrieben eine Verbindung zum Zielsystem her.
- 7 Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑Start) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 8 Schließen Sie die Installation ab.

1.1.4 Einfache Installation mit entferntem Zugriff über SSH – Statische Netzwerkkonfiguration

Diese Art der Installation erfordert physischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten und um die IP-Adresse des Installationsziels zu ermitteln. Die Installation selbst wird vollständig von einer entfernten Arbeitsstation gesteuert, die mit dem Installationsprogramm über SSH verbunden ist. Das Eingreifen des Benutzers ist wie bei der regulären Installation erforderlich (siehe Kapitel 1, *Installation mit YaST* (↑Start)).

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Entfernte Installationsquelle: NFS, HTTP, FTP oder SMB mit einer funktionierenden Network-Verbindung
- Zielsystem mit funktionierender Netzwerkverbindung
- Steuersystem mit funktionierender Netzwerkverbindung und funktionierender SSH-Client-Software
- Physisches Bootmedium (CD, DVD oder benutzerdefinierte Bootdiskette) zum Booten des Zielsystems
- Gültige statische IP-Adressen, die der Installationsquelle und dem Steuersystem bereits zugewiesen sind

- Gültige statische IP-Adresse, die dem Zielsystem zugewiesen wird

Gehen Sie wie folgt vor, um diese Art der Installation durchzuführen:

- 1** Richten Sie die Installationsquelle ein wie in **Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“** (S. 14) beschrieben. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zu SMB-Installationsquellen finden Sie in **Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“** (S. 23).
- 2** Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des openSUSE-Medienkits.
- 3** Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie mithilfe der Eingabeaufforderung für die Boot-Optionen die entsprechenden Parameter für die Netzwerkverbindung, die Adresse der Installationsquelle und die SSH-Aktivierung fest. Dies wird ausführlich in **Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“** (S. 36) beschrieben.

Das Zielsystem bootet in eine textbasierte Umgebung und gibt die Netzwerkadresse an, unter der die grafische Installationsumgebung von einem beliebigen SSH-Client adressiert werden kann.

- 4** Öffnen Sie auf der steuernden Arbeitsstation ein Terminalfenster und stellen Sie wie in **„Herstellen der Verbindung mit dem Installationsprogramm“** (S. 42) beschrieben eine Verbindung zum Zielsystem her.
- 5** Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑Start) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6** Schließen Sie die Installation ab.

1.1.5 Einfache Installation mit entferntem Zugriff über SSH – Dynamische Netzwerkkonfiguration

Diese Art der Installation erfordert physischen Zugriff auf das Zielsystem, um dieses für die Installation zu booten und um die IP-Adresse des Installationsziels zu ermitteln. Die Installation selbst wird vollständig über eine entfernte Arbeitsstation ausgeführt, die über VNC mit dem Installationsprogramm verbunden ist. Für die eigentliche Konfiguration ist jedoch das Eingreifen des Benutzers erforderlich.

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Entfernte Installationsquelle: NFS, HTTP, FTP oder SMB mit einer funktionierenden Network-Verbindung
- Zielsystem mit funktionierender Netzwerkverbindung
- Steuersystem mit funktionierender Netzwerkverbindung und funktionierender SSH-Client-Software
- Physisches Bootmedium (CD oder DVD) zum Booten des Zielsystems
- Laufender DHCP-Server, der IP-Adressen zur Verfügung stellt

Gehen Sie wie folgt vor, um diese Art der Installation durchzuführen:

- 1** Richten Sie die Installationsquelle ein wie in [Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 14) beschrieben. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zu SMB-Installationsquellen finden Sie in [Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 23).
- 2** Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des openSUSE-Medienkits.
- 3** Wenn der Bootbildschirm des Zielsystems erscheint, legen Sie mithilfe der Eingabeaufforderung für die Boot-Optionen die entsprechenden Parameter für die Netzwerkverbindung, den Speicherort der Installationsquelle und die SSH-

Aktivierung fest. Weitere Informationen sowie ausführliche Anweisungen zur Verwendung dieser Parameter finden Sie in [Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“](#) (S. 36).

Das Zielsystem bootet in eine textbasierte Umgebung und gibt die Netzwerkadresse an, unter der die grafische Installationsumgebung über einen beliebigen SSH-Client erreichbar ist.

- 4 Öffnen Sie auf der steuernden Arbeitsstation ein Terminalfenster und stellen Sie wie in [„Herstellen der Verbindung mit dem Installationsprogramm“](#) (S. 42) beschrieben eine Verbindung zum Zielsystem her.
- 5 Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑Start) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6 Schließen Sie die Installation ab.

1.1.6 Installation auf entfernten Systemen über SSH – PXE-Boot und Wake-on-LAN

Diese Art der Installation wird vollständig automatisch durchgeführt. Der Zielcomputer wird über den entfernten Zugriff gestartet und gebootet.

Stellen Sie bei dieser Art der Installation sicher, dass die folgenden Anforderungen erfüllt sind:

- Entfernte Installationsquelle: NFS, HTTP, FTP oder SMB mit einer funktionierenden Network-Verbindung
- TFTP-Server
- Laufender DHCP-Server für Ihr Netzwerk, der dem zu installierenden Host eine statische IP-Adresse zuweist
- Zielsystem, das PXE-Boot-, Netzwerk- und Wake-on-LAN-fähig, angeschlossen und mit dem Netzwerk verbunden ist

- Steuersystem mit funktionierender Netzwerkverbindung und SSH-Client-Software

Gehen Sie wie folgt vor, um diese Art der Installation auszuführen:

- 1** Richten Sie die Installationsquelle ein wie in [Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 14) beschrieben. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zur Konfiguration einer SMB-Installationsquelle finden Sie in [Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 23).
- 2** Richten Sie einen TFTP-Server ein, auf dem das Boot-Image gespeichert wird, das vom Zielsystem abgerufen werden kann. Die Konfiguration eines solchen Servers wird in [Abschnitt 1.3.2, „Einrichten eines TFTP-Servers“](#) (S. 27) beschrieben.
- 3** Richten Sie einen DHCP-Server ein, der IP-Adressen für alle Computer bereitstellt und dem Zielsystem den Speicherort des TFTP-Servers bekannt gibt. Die Konfiguration eines solchen Servers wird in [Abschnitt 1.3.1, „Einrichten eines DHCP-Servers“](#) (S. 25) beschrieben.
- 4** Bereiten Sie das Zielsystem für PXE-Boot vor. Dies wird ausführlich in [Abschnitt 1.3.5, „Vorbereiten des Zielsystems für PXE-Boot“](#) (S. 34) beschrieben.
- 5** Initiieren Sie den Bootvorgang des Zielsystems mithilfe von Wake-on-LAN. Die Konfiguration eines solchen Servers wird in [Abschnitt 1.3.7, „Wake-on-LAN“](#) (S. 35) beschrieben.
- 6** Starten Sie auf der steuernden Arbeitsstation einen SSH-Client und stellen Sie wie in [Abschnitt 1.5.2, „SSH-Installation“](#) (S. 42) beschrieben eine Verbindung zum Zielsystem her.
- 7** Führen Sie die Installation wie in Kapitel 1, *Installation mit YaST* (↑Start) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 8** Schließen Sie die Installation ab.

1.2 Einrichten des Servers, auf dem sich die Installationsquellen befinden

Je nachdem, unter welchem Betriebssystem der Rechner ausgeführt wird, der als Netzwerkinstallationsquelle für openSUSE verwendet werden soll, stehen für die Serverkonfiguration mehrere Möglichkeiten zur Verfügung. Am einfachsten lässt sich ein Installationsserver mit YaST auf SUSE Linux 9.3 und höher einrichten. Bei anderen Versionen von openSUSE müssen Sie die Installationsquelle manuell einrichten.

TIPP

Für die Linux-Implementierung kann auch ein Microsoft Windows-Computer als Installationsserver verwendet werden. Weitere Informationen finden Sie in [Abschnitt 1.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 23).

1.2.1 Einrichten eines Installationsservers mithilfe von YaST

YaST bietet ein grafisches Werkzeug zum Erstellen von Netzwerkinstallationsquellen. Es unterstützt HTTP-, FTP- und NFS-Netzwerk-Installationsserver.

- 1 Melden Sie sich bei dem Computer, der als Installationsserver verwendet werden soll, als `root` an.
- 2 Installieren Sie das `yast2-instserver`-Paket.
- 3 Starten Sie *YaST* > *Verschiedenes* > *Installationsserver*.
- 4 Wählen Sie den gewünschten Servertyp (HTTP, FTP oder NFS). Der ausgewählte Serverdienst wird bei jedem Systemstart automatisch gestartet. Wenn ein Dienst des ausgewählten Typs auf dem System bereits ausgeführt wird und Sie diesen Dienst für den Server manuell konfigurieren möchten, deaktivieren Sie die automatische Konfiguration des Serverdiensts, indem Sie *Keine Netzwerkdienste*

konfigurieren wählen. Geben Sie in beiden Fällen das Verzeichnis an, in dem die Installationsdaten auf dem Server zur Verfügung gestellt werden sollen.

- 5 Konfigurieren Sie den erforderlichen Servertyp. Dieser Schritt bezieht sich auf die automatische Konfiguration der Serverdienste. Wenn die automatische Konfiguration deaktiviert ist, wird dieser Schritt übersprungen.

Legen Sie einen Aliasnamen für das root-Verzeichnis auf dem FTP- oder HTTP-Server fest, in dem die Installationsdaten gespeichert werden sollen. Die Installationsquelle befindet sich später unter `ftp://Server-IP/Alias/Name` (FTP) oder unter `http://Server-IP/Alias/Name` (HTTP). *Name* steht für den Namen der Installationsquelle, die im folgenden Schritt definiert wird. Wenn Sie im vorherigen Schritt NFS ausgewählt haben, legen Sie Platzhalter und Exportoptionen fest. Der Zugriff auf den NFS-Server erfolgt über `nfs://Server-IP/Name`. Informationen zu NFS und Exportvorgängen finden Sie in **Kapitel 21, *Verteilte Nutzung von Dateisystemen mit NFS*** (S. 385).

TIPP: Firewall-Einstellungen

Stellen Sie sicher, dass die Firewall-Einstellungen Ihres Server-Systems Datenverkehr an den entsprechenden Ports für HTTP, NFS und FTP erlauben. Sollte dies derzeit nicht der Fall sein, starten Sie das YaST-Firewall-Modul und öffnen Sie die entsprechenden Ports.

- 6 Konfigurieren Sie die Installationsquelle. Bevor die Installationsmedien in ihr Zielverzeichnis kopiert werden, müssen Sie den Namen der Installationsquelle angeben (dies sollte im Idealfall eine leicht zu merkende Abkürzung des Produkts und der Version sein). YaST ermöglicht das Bereitstellen von ISO-Images der Medien an Stelle von Kopien der Installations-CDs. Wenn Sie diese Funktion verwenden möchten, aktivieren Sie das entsprechende Kontrollkästchen und geben Sie den Verzeichnispfad an, in dem sich die ISO-Dateien lokal befinden. Je nachdem, welches Produkt mithilfe dieses Installationservers verteilt werden soll, können mehrere Add-on-CDs oder Service-Pack-CDs erforderlich sein. Sie müssen als zusätzliche Installationsquellen hinzugefügt werden. Um den Installationsserver über OpenSLP im Netzwerk bekannt zu geben, aktivieren Sie die entsprechende Option.

TIPP

Wenn Ihr Netzwerk diese Option unterstützt, sollten Sie Ihre Installationsquelle auf jeden Fall über OpenSLP bekannt machen. Dadurch ersparen Sie sich die Eingabe des Netzwerk-Installationspfads auf den einzelnen Zielcomputern. Die Zielsysteme werden einfach unter Verwendung der SLP-Boot-Option gebootet und finden die Netzwerkinstallationsquelle ohne weitere Konfigurationsschritte. Weitere Informationen zu dieser Option finden Sie in [Abschnitt 1.4, „Booten des Zielsystems für die Installation“](#) (S. 36).

- 7 Laden Sie die Installationsdaten hoch. Der die meiste Zeit in Anspruch nehmende Schritt bei der Konfiguration eines Installationsservers ist das Kopieren der eigentlichen Installations-CDs. Legen Sie die Medien in der von YaST angegebenen Reihenfolge ein und warten Sie, bis der Kopiervorgang abgeschlossen ist. Wenn alle Quellen erfolgreich kopiert wurden, kehren Sie zur Übersicht der vorhandenen Informationsquellen zurück und schließen Sie die Konfiguration, indem Sie *Verlassen* wählen.

Der Installationsserver ist jetzt vollständig konfiguriert und betriebsbereit. Er wird bei jedem Systemstart automatisch gestartet. Es sind keine weiteren Aktionen erforderlich. Sie müssen diesen Dienst lediglich ordnungsgemäß manuell konfigurieren und starten, wenn die automatische Konfiguration der ausgewählten Netzwerkdienste mit YaST anfänglich deaktiviert wurde.

Um eine Installationsquelle zu deaktivieren, wählen Sie die zu entfernende Installationsquelle aus und wählen Sie dann *Löschen*. Die Installationsdaten werden vom System entfernt. Um den Netzwerkdienst zu deaktivieren, verwenden Sie das entsprechende YaST-Modul.

Wenn der Installationsserver die Installationsdaten für mehrere Produkte einer Produktversion zur Verfügung stellen soll, starten Sie das YaST-Installationsservermodul und wählen Sie in der Übersicht der vorhandenen Installationsquellen die Option *Hinzufügen*, um die neue Installationsquelle zu konfigurieren.

1.2.2 Manuelles Einrichten einer NFS-Installationsquelle

Das Einrichten einer NFS-Quelle für die Installation erfolgt in zwei Schritten. Im ersten Schritt erstellen Sie die Verzeichnisstruktur für die Installationsdaten und kopieren diese in die Struktur. Im zweiten Schritt exportieren Sie das Verzeichnis mit den Installationsdaten in das Netzwerk.

Gehen Sie wie folgt vor, um ein Verzeichnis für die Installationsdaten zu erstellen:

- 1 Melden Sie sich als `root` an.
- 2 Erstellen Sie ein Verzeichnis, in dem die Installationsdaten gespeichert werden sollen, und wechseln Sie in dieses Verzeichnis. Beispiel:

```
mkdir install/product/productversion
cd install/product/productversion
```

Ersetzen Sie *Produkt* durch eine Abkürzung des Produktnamens und *Produktversion* durch eine Zeichenkette, die den Produktnamen und die Version enthält.

- 3 Führen Sie für die einzelnen im Medienkit enthaltenen CDs die folgenden Befehle aus:
 - 3a Kopieren Sie den gesamten Inhalt der Installations-CD in das Server-Installationsverzeichnis:

```
cp -a /media/path_to_your_CD-ROM_drive .
```

Ersetzen Sie *pfad_zu_ihrem_CD-ROM-Laufwerk* durch den tatsächlichen Pfad, in dem sich das CD- oder DVD-Laufwerk befindet. Dies kann je nach Laufwerktyp, der auf dem System verwendet wird, `cdrom`, `cdrecorder`, `dvd` oder `dvdrecorder` sein.

- 3b Benennen Sie das Verzeichnis in die CD-Nummer um:

```
mv path_to_your_CD-ROM_drive CDx
```

Ersetzen Sie *x* durch die Nummer der CD.

Bei openSUSE können Sie die Installationsquellen über NFS mit YaST exportieren. Führen Sie dazu die folgenden Schritte aus:

- 1 Melden Sie sich als `root` an.
- 2 Starten Sie *YaST > Netzwerkdienste > NFS-Server*.
- 3 Wählen Sie *Starten* und *Firewall-Port öffnen* und klicken Sie auf *Weiter*.
- 4 Wählen Sie *Verzeichnis hinzufügen* und navigieren Sie zum Verzeichnis mit den Installationsquellen, in diesem Fall *Produktversion*.
- 5 Wählen Sie *Host hinzufügen* und geben Sie die Hostnamen der Computer ein, auf die die Installationsdaten exportiert werden sollen. An Stelle der Hostnamen können Sie hier auch Platzhalter, Netzwerkadressbereiche oder einfach den Domänennamen Ihres Netzwerks eingeben. Geben Sie die gewünschten Exportoptionen an oder übernehmen Sie die Vorgabe, die für die meisten Konfigurationen ausreichend ist. Weitere Informationen dazu, welche Syntax beim Exportieren von NFS-Freigaben verwendet wird, finden Sie auf der Manualpage zu `exports`.
- 6 Klicken Sie auf *Verlassen*. Der NFS-Server, auf dem sich die openSUSE-Installationsquellen befinden, wird automatisch gestartet und in den Bootvorgang integriert.

Wenn Sie die Installationsquellen nicht mit dem YaST-NFS-Servermodul, sondern manuell exportieren möchten, gehen Sie wie folgt vor:

- 1 Melden Sie sich als `root` an.
- 2 Öffnen Sie die Datei `/etc/exports` und geben Sie die folgende Zeile ein:

```
/productversion *(ro,root_squash, sync)
```

Dadurch wird das Verzeichnis `//Produktversion` auf alle Hosts exportiert, die Teil dieses Netzwerks sind oder eine Verbindung zu diesem Server herstellen können. Um den Zugriff auf diesen Server zu beschränken, geben Sie an Stelle des allgemeinen Platzhalters `*` Netzmasken oder Domänennamen an. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `export`. Speichern und schließen Sie diese Konfigurationsdatei.

- 3 Um den NFS-Dienst zu der beim Booten des System generierten Liste der Server hinzuzufügen, führen Sie die folgenden Befehle aus:

```
insserv /etc/init.d/nfsserver
insserv /etc/init.d/portmap
```

- 4 Starten Sie den NFS-Server mit `rcnfsserver start`. Wenn Sie die Konfiguration des NFS-Servers zu einem späteren Zeitpunkt ändern müssen, ändern Sie die Konfigurationsdatei wie erforderlich und starten die den NFS-Daemon neu, indem Sie `rcnfsserver restart` eingeben.

Die Bekanntgabe des NFS-Servers über OpenSLP stellt dessen Adresse allen Clients im Netzwerk zur Verfügung.

- 1 Melden Sie sich als `root` an.
- 2 Wechseln Sie in das Verzeichnis `/etc/slp.reg.d/`.
- 3 Erstellen Sie eine Konfigurationsdatei namens `install.suse.nfs.reg`, die die folgenden Zeilen enthält:

```
# Register the NFS Installation Server
service:install.suse:nfs://$HOSTNAME/path_to_instsource/CD1,en,65535
description=NFS Installation Source
```

Ersetzen Sie `path_to_instsource` durch den eigentlichen Pfad der Installationsquelle auf dem Server.

- 4 Speichern Sie diese Konfigurationsdatei und starten Sie den OpenSLP-Daemon mit dem folgenden Befehl: `rcslpd start`.

Weitere Informationen zu OpenSLP finden Sie in der Paket-Dokumentation im Verzeichnis `/usr/share/doc/packages/openslp/` oder in **Kapitel 15, *SLP-Dienste im Netzwerk*** (S. 283). Weitere Informationen über NFS erhalten Sie unter **Kapitel 21, *Verteilte Nutzung von Dateisystemen mit NFS*** (S. 385).

1.2.3 Manuelles Einrichten einer FTP-Installationsquelle

Das Erstellen einer FTP-Installationsquelle erfolgt ähnlich wie das Erstellen einer NFS-Installationsquelle. FTP-Installationsquellen können ebenfalls mit OpenSLP im Netzwerk bekannt gegeben werden.

1 Erstellen Sie wie in [Abschnitt 1.2.2](#), „Manuelles Einrichten einer NFS-Installationsquelle“ (S. 17) beschrieben ein Verzeichnis für die Installationsquellen.

2 Konfigurieren Sie den FTP-Server für die Verteilung des Inhalts des Installationsverzeichnisses:

2a Melden Sie sich als `root` an und installieren Sie mithilfe des YaST-Paketmanagers das Paket `vsftpd`.

2b Wechseln Sie in das `root`-Verzeichnis des FTP-Servers:

```
cd /srv/ftp
```

2c Erstellen Sie im `root`-Verzeichnis des FTP-Servers ein Unterverzeichnis für die Installationsquellen:

```
mkdir instsource
```

Ersetzen Sie `instsource` durch den Produktnamen.

2d Hängen Sie den Inhalt des Installations-Repository in der `change-root`-Umgebung des FTP-Servers ein:

```
mount --bind path_to_instsource /srv/ftp/instsource
```

Ersetzen Sie `path_to_instsource` und `instsource` durch die entsprechenden Werte für Ihre Konfiguration. Wenn diese Einstellungen dauerhaft übernommen werden sollen, fügen Sie sie zu `/etc/fstab` hinzu.

2e Starten Sie `vsftpd` mit `vsftpd`.

3 Geben Sie die Installationsquelle über OpenSLP bekannt, sofern dies von Ihrer Netzwerkkonfiguration unterstützt wird:

- 3a** Erstellen Sie eine Konfigurationsdatei namens `install.suse.ftp.reg` unter `/etc/slp/reg.d/`, die die folgenden Zeilen enthält:

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/srv/ftp/instsource/CD1,en,65535
description=FTP Installation Source
```

Ersetzen Sie `instsource` durch den Namen des Verzeichnisses auf dem Server, in dem sich die Installationsquelle befindet. Die Zeile `Dienst :` sollte als eine fortlaufende Zeile eingegeben werden.

- 3b** Speichern Sie diese Konfigurationsdatei und starten Sie den OpenSLP-Daemon mit dem folgenden Befehl: `rcslpd start`.

TIPP: Konfigurieren eines FTP-Servers mit YaST

Wenn Sie lieber YaST verwenden, anstatt den FTP-Installationsserver manuell zu konfigurieren, finden Sie unter [Kapitel 23, Einrichten eines FTP-Servers mit YaST](#) (S. 449) weitere Informationen zum Verwenden des YaST-FTP-Servermoduls.

1.2.4 Manuelles Einrichten einer HTTP-Installationsquelle

Das Erstellen einer HTTP-Installationsquelle erfolgt ähnlich wie das Erstellen einer NFS-Installationsquelle. HTTP-Installationsquellen können ebenfalls mit OpenSLP im Netzwerk bekannt gegeben werden.

- 1** Erstellen Sie wie in [Abschnitt 1.2.2, „Manuelles Einrichten einer NFS-Installationsquelle“](#) (S. 17) beschrieben ein Verzeichnis für die Installationsquellen.
- 2** Konfigurieren Sie den HTTP-Server für die Verteilung des Inhalts des Installationsverzeichnisses:
 - 2a** Installieren Sie den Webserver Apache wie in [Abschnitt 22.1.2, „Installation“](#) (S. 404) beschrieben.

- 2b** Wechseln Sie in das root-Verzeichnis des HTTP-Servers (`/srv/www/htdocs`) und erstellen Sie ein Unterverzeichnis für die Installationsquellen:

```
mkdir instsource
```

Ersetzen Sie `instsource` durch den Produktnamen.

- 2c** Erstellen Sie einen symbolischen Link vom Speicherort der Installationsquellen zum root-Verzeichnis des Webservers (`/srv/www/htdocs`):

```
ln -s /path_instsource /srv/www/htdocs/instsource
```

- 2d** Ändern Sie die Konfigurationsdatei des HTTP-Servers (`/etc/apache2/default-server.conf`) so, dass sie symbolischen Links folgt. Ersetzen Sie die folgende Zeile:

```
Options None
```

mit

```
Options Indexes FollowSymLinks
```

- 2e** Laden Sie die HTTP-Server-Konfiguration mit `rcapache2 reload` neu.

- 3** Geben Sie die Installationsquelle über OpenSLP bekannt, sofern dies von Ihrer Netzwerkkonfiguration unterstützt wird:

- 3a** Erstellen Sie eine Konfigurationsdatei namens `install.suse.http.reg` unter `/etc/slp/reg.d/`, die die folgenden Zeilen enthält:

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/srv/www/htdocs/instsource/CD1/,en,65535
description=HTTP Installation Source
```

Ersetzen Sie `instsource` durch den eigentlichen Pfad der Installationsquelle auf dem Server. Die Zeile `Dienst:` sollte als eine fortlaufende Zeile eingegeben werden.

- 3b** Speichern Sie diese Konfigurationsdatei und starten Sie den OpenSLP-Daemon mit dem folgenden Befehl: `rcslpd restart`.

1.2.5 Verwalten einer SMB-Installationsquelle

Mithilfe von SMB können Sie die Installationsquellen von einem Microsoft Windows-Server importieren und die Linux-Implementierung starten, ohne dass ein Linux-Computer vorhanden sein muss.

Gehen Sie wie folgt vor, um eine exportierte Windows-Freigabe mit den openSUSE-Installationsquellen einzurichten:

- 1 Melden Sie sich auf dem Windows-Computer an.
- 2 Öffnen Sie den Explorer und erstellen Sie einen neuen Ordner, der die gesamte Baumstruktur der Installation aufnehmen soll, und nennen Sie ihn beispielsweise `INSTALL`.
- 3 Geben Sie diesen Ordner wie in der Windows-Dokumentation beschrieben im Netzwerk frei.
- 4 Wechseln Sie in den freigegebenen Ordner und erstellen Sie einen Unterordner namens *Produkt*. Ersetzen Sie *Produkt* durch den tatsächlichen Produktnamen.
- 5 Wechseln Sie in den Ordner `INSTALL/produkt` und kopieren Sie jede CD/DVD in einen separaten Ordner, z. B. `CD1` und `CD2`.

Um eine SMB-eingehängte Freigabe als Installationsquelle zu verwenden, gehen Sie wie folgt vor:

- 1 Booten Sie das Installationsziel.
- 2 Wählen Sie *Installation*.
- 3 Drücken Sie `F4`, um eine Auswahl der Installationsquellen anzuzeigen.
- 4 Wählen Sie `SMB` und geben Sie den Namen oder die IP-Adresse des Windows-Rechners, den Freigabennamen (`INSTALL/produkt/CD1` in diesem Beispiel), den Benutzernamen und das Passwort ein.

Wenn Sie die Eingabetaste drücken, wird YaST gestartet und Sie können die Installation ausführen.

1.2.6 Verwenden von ISO-Images der Installationsmedien auf dem Server

Statt physische Medien manuell in Ihr Serververzeichnis zu kopieren, können Sie auch die ISO-Images der Installationsmedien in Ihrem Installationsserver einhängen und als Installationsquelle verwenden. Gehen Sie wie folgt vor, um einen HTTP-, NFS- oder FTP-Server einzurichten, der ISO-Images anstelle von Medienkopien verwendet:

- 1 Laden Sie die ISO-Images herunter und speichern Sie sie auf dem Rechner, den Sie als Installationsserver verwenden möchten.
- 2 Melden Sie sich als `root` an.
- 3 Wählen und erstellen Sie einen geeigneten Speicherort für die Installationsdaten. Siehe dazu [Abschnitt 1.2.2, „Manuelles Einrichten einer NFS-Installationsquelle“](#) (S. 17), [Abschnitt 1.2.3, „Manuelles Einrichten einer FTP-Installationsquelle“](#) (S. 20) oder [Abschnitt 1.2.4, „Manuelles Einrichten einer HTTP-Installationsquelle“](#) (S. 21).

- 4 Erstellen Sie Unterverzeichnisse für jede CD oder DVD.

- 5 Erteilen Sie folgenden Befehl, um jedes ISO-Image an der endgültigen Position einzuhängen und zu entpacken:

```
mount -o loop path_to_iso path_to_instsource/product/mediumx
```

Ersetzen Sie *path_to_iso* durch den Pfad zu Ihrer lokalen Kopie des ISO-Images, *path_to_instsource* durch das Quellverzeichnis Ihres Servers, *product* durch den Produktnamen und *mediumx* durch Typ (CD oder DVD) und Anzahl der verwendeten Medien.

- 6 Wiederholen Sie die vorherigen Schritte, um alle erforderlichen ISO-Images für Ihr Produkt einzuhängen.
- 7 Starten Sie den Installationsserver wie gewohnt wie unter [Abschnitt 1.2.2, „Manuelles Einrichten einer NFS-Installationsquelle“](#) (S. 17), [Abschnitt 1.2.3,](#)

„Manuelles Einrichten einer FTP-Installationsquelle“ (S. 20) oder [Abschnitt 1.2.4](#), „Manuelles Einrichten einer HTTP-Installationsquelle“ (S. 21) beschrieben.

Um Iso-Images beim Systemstart automatisch einzuhängen, fügen Sie die entsprechenden Einträge in `/etc/fstab` hinzu. Ein Eintrag würde dann gemäß dem vorherigen Beispiel wie folgt aussehen:

```
path_to_iso path_to_instsource/productmediumx auto loop
```

1.3 Vorbereitung des Bootvorgangs für das Zielsystem

In diesem Abschnitt werden die für komplexe Boot-Szenarien erforderlichen Konfigurationsschritte beschrieben. Er enthält zudem Konfigurationsbeispiele für DHCP, PXE-Boot, TFTP und Wake-on-LAN.

1.3.1 Einrichten eines DHCP-Servers

Es gibt zwei Möglichkeiten zum Einrichten eines DHCP-Servers. Für openSUSE liefert YaST eine grafische Schnittstelle für den Vorgang. Benutzer können die Konfigurationsdateien auch manuell bearbeiten. Für weitere Informationen über DHCP-Server siehe auch [Kapitel 17, DHCP](#) (S. 313).

Einrichten eines DHCP-Servers mit YaST

Fügen Sie Ihrer DHCP-Serverkonfiguration zwei Deklarationen hinzu, um den Netzwerk-Clients den Standort des TFTP-Servers mitzuteilen und die Boot-Image-Datei für das Installationsziel anzugeben.

- 1 Melden Sie sich als `root` auf dem Computer an, der den DHCP-Server hostet.
- 2 Starten Sie `YaST > Netzwerkdienste > DHCP-Server`.
- 3 Schließen Sie den Installationsassistenten für die Einrichtung des grundlegenden DHCP-Server ab.

- 4 Wenn Sie eine Warnmeldung zum Verlassen des Start-Dialogfelds erhalten, wählen Sie *Einstellungen für Experten* und *Ja*.
- 5 Im Dialogfeld *Konfigurierte Deklarationen* wählen Sie das Subnetz aus, indem sich das neue System befinden soll und klicken Sie auf *Bearbeiten*.
- 6 Im Dialogfeld *Konfiguration des Subnetzes* wählen Sie *Hinzufügen*, um eine neue Option zur Subnetz-Konfiguration hinzuzufügen.
- 7 Wählen Sie `Dateiname` und geben Sie `pxelinux.0` als Wert ein.
- 8 Fügen Sie eine andere Option (`next-server`) hinzu und setzen Sie deren Wert auf die Adresse des TFTP-Servers.
- 9 Wählen Sie *OK* und *Verlassen*, um die DHCP-Serverkonfiguration abzuschließen.

Wenn Sie DHCP zum Angeben einer statischen IP-Adresse für einen bestimmten Host konfigurieren möchten, fügen Sie unter *Einstellungen für Experten* im DHCP-Serverkonfigurationsmodul (**Schritt 4** (S. 26)) eine neue Deklaration für den Hosttyp hinzu. Fügen Sie dieser Hostdeklaration die Optionen `hardware` und `fixed-address` hinzu und bieten Sie die entsprechenden Werte an.

Manuelles Einrichten eines DHCP-Servers

Die einzige Aufgabe des DHCP-Servers ist neben der Bereitstellung der automatischen Adresszuweisung für die Netzwerk-Clients die Bekanntgabe der IP-Adresse des TFTP-Servers und der Datei, die von den Installationsroutinen auf dem Zielcomputer abgerufen werden soll.

- 1 Melden Sie sich als `root` auf dem Computer an, der den DHCP-Server hostet.
- 2 Fügen Sie der Konfigurationsdatei des DHCP-Servers, die sich unter `/etc/dhcpd.conf` befindet, folgende Zeilen hinzu:

```
group {
    # PXE related stuff
    #
    # "next server" defines the tftp server that will be used
    next server ip_tftp_server:
    #
    # "filename" specifies the pxelinux image on the tftp server
    # the server runs in chroot under /srv/tftpbroot
```

```
    filename "pxelinux.0";  
}
```

Ersetzen Sie `ip_tftp_server` durch die IP-Adresse des TFTP-Servers. Weitere Informationen zu den in `dhcpd.conf` verfügbaren Optionen finden Sie auf der Manualpage `dhcpd.conf`.

3 Starten Sie den DHCP-Server neu, indem Sie `rcdhcpd restart` ausführen.

Wenn Sie SSH für die Fernsteuerung einer PXE- und Wake-on-LAN-Installation verwenden möchten, müssen Sie die IP-Adresse, die der DHCP-Server dem Installationsziel zur Verfügung stellen soll, explizit angeben. Ändern Sie hierzu die oben erwähnte DHCP-Konfiguration gemäß dem folgenden Beispiel:

```
group {  
    # PXE related stuff  
    #  
    # "next server" defines the tftp server that will be used  
    next server ip_tftp_server:  
    #  
    # "filename" specifies the pxelinux image on the tftp server  
    # the server runs in chroot under /srv/tftpboot  
    filename "pxelinux.0";  
    host test { hardware ethernet mac_address;  
                fixed-address some_ip_address; }  
}
```

Die Host-Anweisung gibt den Hostnamen des Installationsziels an. Um den Hostnamen und die IP-Adresse an einen bestimmten Host zu binden, müssen Sie die Hardware-Adresse (MAC) des Systems kennen und angeben. Ersetzen Sie alle in diesem Beispiel verwendeten Variablen durch die in Ihrer Umgebung verwendeten Werte.

Nach dem Neustart weist der DHCP-Server dem angegebenen Host eine statische IP-Adresse zu, damit Sie über SSH eine Verbindung zum System herstellen können.

1.3.2 Einrichten eines TFTP-Servers

Richten Sie einen TFTP-Server ein, entweder mit YaST oder manuell auf einem beliebigen Linux-Betriebssystem, das `xinetd` und `tftp` unterstützt. Der TFTP-Server übergibt das Boot-Image an das Zielsystem, sobald dieses gebootet ist und eine entsprechende Anforderung sendet.

Einrichten eines TFTP-Servers mit YaST

- 1 Melden Sie sich als `root` an.
- 2 Installieren Sie das `yast2-tftp-server`-Paket.
- 3 Starten Sie *YaST* > *Netzwerkdienste* > *TFTP-Server* und installieren Sie das erforderliche Paket.
- 4 Klicken Sie auf *Aktivieren*, um sicherzustellen, dass der Server gestartet und in die Boot-Routine aufgenommen wird. Ihrerseits sind hierbei keine weiteren Aktionen erforderlich. `tftpd` wird zur Boot-Zeit von `xinetd` gestartet.
- 5 Klicken Sie auf *Firewall-Port öffnen*, um den entsprechenden Port in der Firewall zu öffnen, die auf dem Computer aktiv ist. Diese Option ist nur verfügbar, wenn auf dem Server eine Firewall installiert ist.
- 6 Klicken Sie auf *Durchsuchen*, um nach dem Verzeichnis mit dem Boot-Image zu suchen. Das Standardverzeichnis `/tftpboot` wird erstellt und automatisch ausgewählt.
- 7 Klicken Sie auf *Verlassen*, um die Einstellungen zu übernehmen und den Server zu starten.

Manuelles Einrichten eines TFTP-Servers

- 1 Melden Sie sich als `root` an und installieren Sie die Pakete `tftp` und `xinetd`.
- 2 Erstellen Sie die Verzeichnisse `/srv/tftpboot` und `/srv/tftpboot/pxe/linux.cfg`, sofern sie noch nicht vorhanden sind.
- 3 Fügen Sie wie in [Abschnitt 1.3.3, „Verwenden von PXE Boot“](#) (S. 29) beschrieben die für das Boot-Image erforderlichen Dateien hinzu.
- 4 Ändern Sie die Konfiguration von `xinetd`, die sich unter `/etc/xinetd.d/` befindet, um sicherzustellen, dass der TFTP-Server beim Booten gestartet wird:
 - 4a Erstellen Sie, sofern noch nicht vorhanden, in diesem Verzeichnis eine Datei namens `tftp`, indem Sie `touch tftp` eingeben. Führen Sie anschließend folgenden Befehl aus: `chmod 755 tftp`.

4b Öffnen Sie die Datei `tftp` und fügen Sie die folgenden Zeilen hinzu:

```
service tftp
{
    socket_type          = dgram
    protocol             = udp
    wait                = yes
    user                 = root
    server               = /usr/sbin/in.tftpd
    server_args          = -s /srv/tftpboot
    disable              = no
}
```

4c Speichern Sie die Datei und starten Sie `xinetd` mit `rcxinetd restart` neu.

1.3.3 Verwenden von PXE Boot

Einige technische Hintergrundinformationen sowie die vollständigen PXE-Spezifikationen finden Sie in der PXE-(Preboot Execution Environment-)Spezifikation (<http://www.pix.net/software/pxeboot/archive/pxespec.pdf>).

1 Wechseln Sie in das Verzeichnis des Installations-Repositorys und kopieren Sie die Dateien `linux`, `initrd`, `message` und `memtest` in das Verzeichnis `/srv/tftpboot`, indem Sie folgenden Befehl eingeben:

```
cp -a boot/loader/linux boot/loader/initrd
    boot/loader/message boot/loader/memtest /srv/tftpboot
```

2 Installieren Sie mit YaST das Paket `syslinux` direkt von den Installations-CDs oder -DVDs.

3 Kopieren Sie die Datei `/usr/share/syslinux/pxelinux.0` in das Verzeichnis `/srv/tftpboot`, indem Sie folgenden Befehl eingeben:

```
cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot
```

4 Wechseln Sie in das Verzeichnis des Installations-Repositorys und kopieren Sie die Datei `isolinux.cfg` in das Verzeichnis `/srv/tftpboot/pxelinux.cfg/default`, indem Sie folgenden Befehl eingeben:

```
cp -a boot/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default
```

- 5 Bearbeiten Sie die Datei `/srv/tftpboot/pxelinux.cfg/default` und entfernen Sie die Zeilen, die mit `gfxboot`, `readinfo` und `framebuffer` beginnen.
- 6 Fügen Sie die folgenden Einträge in die `append`-Zeilen der standardmäßigen Kennungen `failsafe` und `apic` ein:

```
insmod=kernel module
```

Durch diesen Eintrag geben Sie das Netzwerk-Kernelmodul an, das zur Unterstützung der Netzwerkinstallation auf dem PXE-Client erforderlich ist. Ersetzen Sie *kernel module* durch den entsprechenden Modulnamen Ihres Netzwerkgeräts.

```
netdevice=interface
```

Dieser Eintrag definiert die Schnittstelle des Client-Netzwerks, die für die Netzwerkinstallation verwendet werden muss. Dieser Eintrag ist jedoch nur erforderlich und muss entsprechend angepasst werden, wenn der Client mit mehreren Netzwerkkarten ausgestattet ist. Falls nur eine Netzwerkkarte verwendet wird, kann dieser Eintrag ausgelassen werden.

```
install=nfs://IP_Instserver/Pfad_Instquelle/CD1
```

Dieser Eintrag gibt den NFS-Server und die Installationsquelle für die Client-Installation an. Ersetzen Sie *IP_Instserver* durch die IP-Adresse des Installationsservers. *Pfad_Instquelle* muss durch den Pfad der Installationsquellen ersetzt werden. HTTP-, FTP- oder SMB-Quellen werden auf ähnliche Weise adressiert. Eine Ausnahme ist das Protokollpräfix, das wie folgt lauten sollte: `http`, `ftp` oder `smb`.

WICHTIG

Wenn den Installationsroutinen weitere Boot-Optionen, z. B. SSH- oder VNC-Boot-Parameter, übergeben werden sollen, hängen Sie sie an den Eintrag `install` an. Einen Überblick über die Parameter sowie einige Beispiele finden Sie in [Abschnitt 1.4, „Booten des Ziel-systems für die Installation“](#) (S. 36).

Im Folgenden finden Sie die Beispieldatei

`/srv/tftpboot/pxelinux.cfg/default`. Passen Sie das Protokollpräfix für die Installationsquelle gemäß der Netzwerkkonfiguration an und geben Sie die bevorzugte Methode an, mit der die Verbindung zum Installationsprogramm hergestellt werden soll. Fügen Sie hierfür die Optionen `vnc` und `vncpassword` oder `usessh` und `sshpassword` zum Eintrag `install` hinzu. Die durch `\` getrennten Zeilen müssen als fortlaufende Zeile ohne Zeilenbruch und ohne den `\` eingegeben werden.

```
default linux

# default
label linux
  kernel linux
    append initrd=initrd ramdisk_size=65536 insmod=e100 \
    install=nfs://ip_instserver/path_instsource/product/CD1

# failsafe
label failsafe
  kernel linux
    append initrd=initrd ramdisk_size=65536 ide=nodma apm=off acpi=off \
    insmod=e100 install=nfs://ip_instserver/path_instsource/product/CD1

# apic
label apic
  kernel linux
    append initrd=initrd ramdisk_size=65536 apic insmod=e100 \
    install=nfs://ip_instserver/path_instsource/product/CD1

# manual
label manual
  kernel linux
    append initrd=initrd ramdisk_size=65536 manual=1

# rescue
label rescue
  kernel linux
    append initrd=initrd ramdisk_size=65536 rescue=1

# memory test
label memtest
  kernel memtest

# hard disk
label hddisk
  localboot 0

implicit      0
display       message
```

```
prompt      1
timeout     100
```

Ersetzen Sie *ip_instserver* und *path_instsource* durch die in Ihrer Konfiguration verwendeten Werte.

Der folgende Abschnitt dient als Kurzreferenz für die in dieser Konfiguration verwendeten PXELINUX-Optionen. Weitere Informationen zu den verfügbaren Optionen finden Sie in der Dokumentation des Pakets *syslinux*, die sich im Verzeichnis `/usr/share/doc/packages/syslinux/` befindet.

1.3.4 PXELINUX-Konfigurationsoptionen

Die hier aufgeführten Optionen sind eine Teilmenge der für die PXELINUX-Konfigurationsdatei verfügbaren Optionen.

DEFAULT Kernel Optionen...

Legt die standardmäßige Kernel-Kommandozeile fest. Wenn PXELINUX automatisch gebootet wird, agiert es, als wären die Einträge nach *DEFAULT* an der Boot-Eingabeaufforderung eingegeben worden, außer, dass die Option für das automatische Booten (*boot*) automatisch hinzugefügt wird.

Wenn keine Konfigurationsdatei vorhanden oder der *DEFAULT*-Eintrag in der Konfigurationsdatei nicht vorhanden ist, ist die Vorgabe der Kernel-Name „linux“ ohne Optionen.

APPEND Optionen...

Fügt der Kernel-Kommandozeile eine oder mehrere Optionen hinzu. Diese werden sowohl bei automatischen als auch bei manuellen Bootvorgängen hinzugefügt. Die Optionen werden an den Beginn der Kernel-Kommandozeile gesetzt und ermöglichen, dass explizit eingegebene Kernel-Optionen sie überschreiben können.

LABEL Kennung KERNEL Image APPEND Optionen...

Gibt an, dass, wenn *Kennung* als zu bootender Kernel eingegeben wird, PXELINUX stattdessen *Image* booten soll und die angegebenen *APPEND*-Optionen an Stelle der im globalen Abschnitt der Datei (vor dem ersten *LABEL*-Befehl) angegebenen Optionen verwendet werden sollen. Die Vorgabe für *Image* ist dieselbe wie für *Kennung* und wenn keine *APPEND*-Optionen angegeben sind, wird standardmäßig der globale Eintrag verwendet (sofern vorhanden). Es sind bis zu 128 *LABEL*-Einträge zulässig.

Beachten Sie, dass GRUB die folgende Syntax verwendet:

```
title mytitle
  kernel my_kernel my_kernel_options
  initrd myinitrd
```

PXELINUX verwendet die folgende Syntax:

```
label mylabel
  kernel mykernel
  append myoptions
```

Kennungen werden wie Dateinamen umgesetzt und müssen nach der Umsetzung (sogenanntes Mangling) eindeutig sein. Die beiden Kennungen „v2.1.30“ und „v2.1.31“ wären beispielsweise unter PXELINUX nicht unterscheidbar, da beide auf denselben DOS-Dateinamen umgesetzt würden.

Der Kernel muss kein Linux-Kernel, sondern kann ein Bootsektor oder eine COMBOOT-Datei sein.

APPEND –

Es wird nichts angehängt. APPEND mit einem Bindestrich als Argument in einem LABEL-Abschnitt kann zum Überschreiben einer globalen APPEND-Option verwendet werden.

LOCALBOOT *Typ*

Wenn Sie unter PXELINUX LOCALBOOT 0 an Stelle einer KERNEL-Option angeben, bedeutet dies, dass diese bestimmte Kennung aufgerufen und die lokale Festplatte an Stelle eines Kernels gebootet wird.

Argument	Beschreibung
0	Führt einen normalen Bootvorgang aus
4	Führt einen lokalen Bootvorgang mit dem noch im Arbeitsspeicher vorhandenen UNDI-Treiber (Universal Network Driver Interface) aus
5	Führt einen lokalen Bootvorgang mit dem gesamten PXE-Stack, einschließlich des UNDI-Treibers aus, der sich im Arbeitsspeicher befindet

Alle anderen Werte sind nicht definiert. Wenn Sie die Werte für die UNDI- oder PXE-Stacks nicht wissen, geben Sie 0 an.

`TIMEOUT` *Zeitlimit*

Gibt in Einheiten von 1/10 Sekunde an, wie lange die Boot-Eingabeaufforderung angezeigt werden soll, bevor der Bootvorgang automatisch gestartet wird. Das Zeitlimit wird aufgehoben, sobald der Benutzer eine Eingabe über die Tastatur vornimmt, da angenommen wird, dass der Benutzer die Befehlseingabe abschließt. Mit einem Zeitlimit von Null wird das Zeitüberschreitungsoption deaktiviert (dies ist die Vorgabe). Der größtmögliche Wert für das Zeitlimit ist 35996 (etwas weniger als eine Stunde).

`PROMPT` *flag_val*

Wenn `flag_val` 0 ist, wird die Boot-Eingabeaufforderung nur angezeigt, wenn die Taste Umschalttaste oder Alt gedrückt wird oder die Feststelltaste oder die Taste Rollen gesetzt ist (dies ist die Vorgabe). Wenn `flag_val` 1 ist, wird die Boot-Eingabeaufforderung immer angezeigt.

```
F2 filename
F1 filename
..etc...
F9 filename
F10 filename
```

Zeigt die angegebene Datei auf dem Bildschirm an, wenn an der Boot-Eingabeaufforderung eine Funktionstaste gedrückt wird. Mithilfe dieser Option kann auch die Preboot-Online-Hilfe implementiert werden (für die Kernel-Kommandozeilenoptionen). Aus Gründen der Kompatibilität mit früheren Versionen kann F10 auch als F0 verwendet werden. Beachten Sie, dass derzeit keine Möglichkeit besteht, Dateinamen an F11 und F12 zu binden.

1.3.5 Vorbereiten des Zielsystems für PXE-Boot

Bereiten Sie das System-BIOS für PXE-Boot vor, indem Sie die PXE-Option in die BIOS-Boot-Reihenfolge aufnehmen.

WARNUNG: BIOS-Bootreihenfolge

Die PXE-Option darf im BIOS nicht vor der Boot-Option für die Festplatte stehen. Andernfalls würde dieses System versuchen, sich selbst bei jedem Booten neu zu installieren.

1.3.6 Vorbereiten des Zielsystems für Wake-on-LAN

Wake-on-LAN (WOL) erfordert, dass die entsprechende BIOS-Option vor der Installation aktiviert wird. Außerdem müssen Sie sich die MAC-Adresse des Zielsystems notieren. Diese Daten sind für das Initiieren von Wake-on-LAN erforderlich.

1.3.7 Wake-on-LAN

Mit Wake-on-LAN kann ein Computer über ein spezielles Netzwerkpaket, das die MAC-Adresse des Computers enthält, gestartet werden. Da jeder Computer einen eindeutigen MAC-Bezeichner hat, ist es nicht möglich, dass versehentlich ein falscher Computer gestartet wird.

WICHTIG: Wake-on-LAN über verschiedene Netzwerksegmente

Wenn sich der Steuercomputer nicht im selben Netzwerksegment wie das zu startende Installationsziel befindet, konfigurieren Sie die WOL-Anforderungen entweder so, dass sie als Multicasts verteilt werden, oder steuern Sie einen Computer in diesem Netzwerksegment per entferntem Zugriff so, dass er als Absender dieser Anforderungen agiert.

1.3.8 Manuelles Wake-on-LAN

- 1 Melden Sie sich als `root` an.
- 2 Starten Sie `YaST > Softwareverwaltung` und installieren Sie das Paket `netdiag`.
- 3 Öffnen Sie ein Terminal und geben Sie als `root` den folgenden Befehl ein, um das Ziel zu starten:

`ether-wake mac_of_target`

Ersetzen Sie `mac_of_target` durch die MAC-Adresse des Ziels.

1.4 Booten des Zielsystems für die Installation

Abgesehen von der in [Abschnitt 1.3.7, „Wake-on-LAN“](#) (S. 35) und [Abschnitt 1.3.3, „Verwenden von PXE Boot“](#) (S. 29) beschriebenen Vorgehensweise gibt es im Wesentlichen zwei unterschiedliche Möglichkeiten, den Bootvorgang für die Installation anzupassen. Sie können entweder die standardmäßigen Boot-Optionen und Funktionstasten oder die Eingabeaufforderung für die Boot-Optionen im Bootbildschirm für die Installation verwenden, um die Boot-Optionen anzugeben, die der Installations-Kernel für die entsprechende Hardware benötigt.

1.4.1 Standardmäßige Boot-Optionen

Die Boot-Optionen werden unter Kapitel 1, *Installation mit YaST* (↑Start) genauer erläutert. In der Regel wird durch die Auswahl von *Installation* der Bootvorgang für die Installation gestartet.

Verwenden Sie bei Problemen *Installation—ACPI deaktiviert* oder *Installation—Sichere Einstellungen*.

Die Menüleiste unten im Bildschirm enthält einige erweiterte Funktionen, die bei einigen Setups erforderlich sind. Mithilfe der F-Tasten können Sie zusätzliche Optionen angeben, die an die Installationsroutinen weitergegeben werden, ohne dass Sie die detaillierte Syntax dieser Parameter kennen müssen (siehe [Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“](#) (S. 36)). Eine detaillierte Beschreibung der verfügbaren Funktionstasten erhalten Sie unter Abschnitt „Der Boot-Bildschirm“ (Kapitel 1, *Installation mit YaST*, ↑Start).

1.4.2 Benutzerdefinierte Boot-Optionen

Mithilfe geeigneter Boot-Optionen können Sie den Installationsvorgang vereinfachen. Viele Parameter können mit den `linuxrc`-Routinen auch zu einem späteren Zeitpunkt

konfiguriert werden, das Verwenden der Boot-Optionen ist jedoch viel einfacher. In einigen automatisierten Setups können die Boot-Optionen über die Datei `initrd` oder eine `info`-Datei bereit gestellt werden.

In der folgenden Tabelle sind alle in diesem Kapitel erwähnten Installationsszenarien mit den erforderlichen Parametern für das Booten sowie die entsprechenden Boot-Optionen aufgeführt. Um eine Boot-Zeichenkette zu erhalten, die an die Installationsroutinen übergeben wird, hängen Sie einfach alle Optionen in der Reihenfolge an, in der sie in dieser Tabelle angezeigt werden. Beispiel (alle in einer Zeile):

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

Ersetzen Sie alle Werte . . . in dieser Zeichenkette durch die für Ihre Konfiguration geeigneten Werte.

Tabelle 1.1 *In diesem Kapitel verwendete Installationsszenarien (Boot-Szenarien)*

Installationsszenario	Für den Bootvorgang erforderliche Parameter	Boot-Optionen
Kapitel 1, <i>Installation mit YaST</i> (↑Start)	Keine: Das System bootet automatisch.	Nicht erforderlich
Abschnitt 1.1.1, „Einfache Installation mit entferntem Zugriff über VNC – Statische Netzwerkkonfiguration“ (S. 4)	<ul style="list-style-type: none"> • Adresse des Installations-servers • Netzwerkgerät • IP-Adresse • Netzmaske • Gateway • VNC-Aktivierung • VNC-Passwort 	<ul style="list-style-type: none"> • <code>install=(nfs,http,?ftp,smb):// /Pfad_zu_Instmedium</code> • <code>netdevice=some_netdevice</code> (nur erforderlich, wenn mehrere Netzwerkgeräte verfügbar sind) • <code>hostip=some_ip</code> • <code>netmask=some_netmask</code> • <code>gateway=ip_gateway</code> • <code>vnc=1</code> • <code>vncpassword=some_password</code>

Installationsszenario	Für den Bootvorgang erforderliche Parameter	Boot-Optionen
<p>Abschnitt 1.1.2, „Einfache Installation mit entferntem Zugriff über VNC – Dynamische Netzwerkkonfiguration“ (S. 6)</p>	<ul style="list-style-type: none"> • Adresse des Installations-servers • VNC-Akti-vierung • VNC-Pass-wort 	<ul style="list-style-type: none"> • <code>install=(nfs,http,?ftp,smb):// /Pfad_zu_Instmedium</code> • <code>vnc=1</code> • <code>vncpassword=some_password</code>
<p>Abschnitt 1.1.3, „Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN“ (S. 7)</p>	<ul style="list-style-type: none"> • Adresse des Installations-servers • Adresse des TFTP-Ser-vers • VNC-Akti-vierung • VNC-Pass-wort 	<p>Nicht zutreffend; Prozess wird über PXE und DHCP verwaltet</p>
<p>Abschnitt 1.1.4, „Einfache Installation mit entferntem Zugriff über SSH – Statische Netzwerkkonfiguration“ (S. 9)</p>	<ul style="list-style-type: none"> • Adresse des Installations-servers • Netzwerkge-rät • IP-Adresse • Netzmaske • Gateway • SSH-Akti-vierung • SSH-Pass-wort 	<ul style="list-style-type: none"> • <code>install=(nfs,http,?ftp,smb):// /Pfad_zu_Instmedium</code> • <code>netdevice=some_netdevice</code> (nur erforderlich, wenn mehrere Netzwerkge-räte verfügbar sind) • <code>hostip=some_ip</code> • <code>netmask=some_netmask</code> • <code>gateway=ip_gateway</code> • <code>usessh=1</code> • <code>sshpassword=some_password</code>

Installationsszenario	Für den Bootvorgang erforderliche Parameter	Boot-Optionen
<p>Abschnitt 1.1.5, „Einfache Installation mit entferntem Zugriff über SSH – Dynamische Netzwerkkonfiguration“ (S. 11)</p>	<ul style="list-style-type: none"> • Adresse des Installations-servers • SSH-Aktivierung • SSH-Passwort 	<ul style="list-style-type: none"> • <code>install=(nfs,http,?ftp,smb):// /Pfad_zu_Instmedium</code> • <code>usessh=1</code> • <code>sshpassword=some_password</code>
<p>Abschnitt 1.1.6, „Installation auf entfernten Systemen über SSH – PXE-Boot und Wake-on-LAN“ (S. 12)</p>	<ul style="list-style-type: none"> • Adresse des Installations-servers • Adresse des TFTP-Servers • SSH-Aktivierung • SSH-Passwort 	<p>Nicht zutreffend; Prozess wird über PXE und DHCP verwaltet</p>

TIPP: Weitere Informationen zu den linuxrc-Boot-Optionen

Weitere Informationen zu den linuxrc-Boot-Optionen für das Booten eines Linux-Systems finden Sie in `/usr/share/doc/packages/linuxrc/linuxrc.html`.

1.5 Überwachen des Installationsvorgangs

Es gibt mehrere Möglichkeiten der entfernten Überwachung des Installationsvorgangs. Wenn beim Booten für die Installation die richtigen Boot-Optionen angegeben wurden, kann die Installation und Systemkonfiguration mit VNC oder SSH von einer entfernten Arbeitsstation aus überwacht werden.

1.5.1 VNC-Installation

Mithilfe einer beliebigen VNC-Viewer-Software können Sie die Installation von openSUSE von praktisch jedem Betriebssystem aus entfernt überwachen. In diesem Abschnitt wird das Setup mithilfe einer VNC-Viewer-Anwendung oder eines Webbrowsers beschrieben.

Vorbereiten der VNC-Installation

Um das Installationsziel für eine VNC-Installation vorzubereiten, müssen Sie lediglich die entsprechenden Boot-Optionen beim anfänglichen Bootvorgang für die Installation angeben (siehe [Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“](#) (S. 36)). Das Zielsystem bootet in eine textbasierte Umgebung und wartet darauf, dass ein VNC-Client eine Verbindung zum Installationsprogramm herstellt.

Das Installationsprogramm gibt die IP-Adresse bekannt und zeigt die für die Verbindung zum Installationsprogramm erforderliche Nummer an. Wenn Sie physischen Zugriff auf das Zielsystem haben, werden diese Informationen sofort nach dem Booten des Systems für die Installation zur Verfügung gestellt. Geben Sie diese Daten ein, wenn Sie von der VNC-Client-Software dazu aufgefordert werden, und geben Sie Ihr Passwort ein.

Da sich das Installationsziel über OpenSLP selbst bekannt gibt, können Sie die Adressinformationen des Installationsziels über einen SLP-Browser abrufen, ohne dass Sie physischen Zugriff auf die Installation selbst haben müssen, vorausgesetzt, OpenSLP wird von der Netzwerkkonfiguration und von allen Computern unterstützt:

- 1 Starten Sie KDE und den Webbrowser Konqueror.

- 2 Geben Sie `service://yast.installation.suse` in die Adressleiste ein. Daraufhin wird das Zielsystem als Symbol im Konqueror-Fenster angezeigt. Durch Klicken auf dieses Symbol wird der KDE-VNC-Viewer geöffnet, in dem Sie die Installation ausführen können. Alternativ können Sie die VNC-Viewer-Software auch mit der zur Verfügung gestellten IP-Adresse ausführen und am Ende der IP-Adresse für die Anzeige, in der die Installation ausgeführt wird, `:1` hinzufügen.

Herstellen der Verbindung mit dem Installationsprogramm

Im Wesentlichen gibt es zwei Möglichkeiten, eine Verbindung zu einem VNC-Server (in diesem Beispiel dem Installationsziel) herzustellen. Sie können entweder eine unabhängige VNC-Viewer-Anwendung unter einem beliebigen Betriebssystem starten oder die Verbindung über einen Java-fähigen Webbrowser herstellen.

Mit VNC können Sie die Installation eines Linux-Systems von jedem Betriebssystem, einschließlich anderer Linux-, Windows- oder Mac OS-Betriebssysteme, aus steuern.

Stellen Sie auf einem Linux-Computer sicher, dass das Paket `tightvnc` installiert ist. Installieren Sie auf einem Windows-Computer den Windows-Port dieser Anwendung, der über die Homepage von TightVNC (<http://www.tightvnc.com/download.html>) erhältlich ist.

Gehen Sie wie folgt vor, um eine Verbindung zu dem auf dem Zielcomputer ausgeführten Installationsprogramm herzustellen:

- 1 Starten Sie den VNC-Viewer.
- 2 Geben Sie die IP-Adresse und die Anzeigenummer des Installationsziels wie vom SLP-Browser oder dem Installationsprogramm selbst zur Verfügung gestellt ein:

ip_address:display_number

Auf dem Desktop wird ein Fenster geöffnet, in dem die YaST-Bildschirme wie bei einer normalen lokalen Installation angezeigt werden.

Wenn Sie die Verbindung zum Installationsprogramm mithilfe eines Webbrowsers herstellen, sind Sie von der VNC-Software bzw. dem zu Grunde liegenden Betriebssystem-

tem vollkommen unabhängig. Sie können die Installation des Linux-Systems in einem beliebigen Browser (Firefox, Internet Explorer, Konqueror, Opera usw.) ausführen, solange dieser Java unterstützt.

Gehen Sie wie folgt vor, um eine VNC-Installation auszuführen:

- 1 Starten Sie Ihren bevorzugten Webbrowser.
- 2 Geben Sie in der Adressleiste Folgendes ein:

```
http://ip_address_of_target:5801
```
- 3 Geben Sie Ihr VNC-Passwort ein, wenn Sie dazu aufgefordert werden. Die YaST-Bildschirme werden im Browserfenster wie bei einer normalen lokalen Installation angezeigt.

1.5.2 SSH-Installation

Mithilfe von SSH können Sie die Installation des Linux-Computers unter Verwendung einer beliebigen SSH-Client-Software von einem entfernten Standort aus überwachen.

Vorbereiten der SSH-Installation

Zusätzlich zum Installieren der entsprechenden Softwarepakete (OpenSSH für Linux und PuTTY für Windows) müssen Sie nur die entsprechenden Boot-Optionen übergeben, um SSH für die Installation zu aktivieren. Weitere Informationen finden Sie in [Abschnitt 1.4.2, „Benutzerdefinierte Boot-Optionen“](#) (S. 36). OpenSSH wird auf allen SUSE Linux-basierten Betriebssystemen standardmäßig installiert.

Herstellen der Verbindung mit dem Installationsprogramm

- 1 Rufen Sie die IP-Adresse des Installationsziels ab. Wenn Sie physischen Zugriff auf den Zielcomputer haben, verwenden Sie einfach die IP-Adresse, die von der Installationsroutine nach dem anfänglichen Bootvorgang auf der Konsole angezeigt wird. Verwenden Sie andernfalls die IP-Adresse, die diesem Host in der DHCP-Serverkonfiguration zugewiesen wurde.

2 Geben Sie an der Kommandozeile den folgenden Befehl ein:

```
ssh -X root@ip_address_of_target
```

Ersetzen Sie *ip_address_of_target* durch die IP-Adresse des Installationsziels.

- 3** Wenn Sie zur Eingabe eines Benutzernamens aufgefordert werden, geben Sie `root` ein.
- 4** Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie das Passwort ein, das mit der SSH-Boot-Option festgelegt wurde. Wenn Sie sich erfolgreich authentifiziert haben, wird eine Kommandozeilenaufforderung für das Installationsziel angezeigt.
- 5** Geben Sie `yast` ein, um das Installationsprogramm zu starten. Im aufgerufenen Fenster werden die gängigen YaST-Bildschirme wie in Kapitel 1, *Installation mit YaST* (↑Start) beschrieben angezeigt.

Fortgeschrittene Festplattenkonfiguration

2

Komplexe Systemkonfigurationen erfordern besondere Festplattenkonfigurationen. Alle Partitionierungsaufgaben können mit YaST erledigt werden. Um Gerätenamen mit Blockgeräten zu erhalten, verwenden Sie die Blockgeräte `/dev/disk/by-id` oder `/dev/disk/by-uuid`. Das Logical Volume Management (LVM) ist ein Schema für die Festplattenpartitionierung, das viel flexibler als die physische Partitionierung in Standardkonfigurationen ist. Mit der Snapshot-Funktion können Sie Datensicherungen einfach erstellen. Ein RAID (Redundant Array of Independent Disks) bietet verbesserte Datenintegrität, Leistung und Fehlertoleranz.

2.1 Verwenden der YaST-Partitionierung

Die in [Abbildung 2.1, „Die YaST-Partitionierung“](#) (S. 46) gezeigte Expertenpartitionierung ermöglicht die manuelle Änderung der Partitionierung einer oder mehrerer Festplatten. Partitionen können hinzugefügt, gelöscht, in ihrer Größe geändert und bearbeitet werden. Außerdem können Sie über dieses YaST-Modul auf die Soft RAID- und LVM-Konfiguration zugreifen.

WARNUNG: Neupartitionierung des laufenden Systems

Auch wenn es möglich ist, ein laufendes System neu zu partitionieren, ist das Risiko eines Fehlers mit daraus folgendem Datenverlust sehr hoch. Versuchen Sie daher eine Neupartitionierung des installierten Systems möglichst zu ver-

meiden. Sollte es sich wirklich nicht umgehen lassen, führen Sie zuvor unbedingt eine vollständige Datensicherung durch.

Abbildung 2.1 Die YaST-Partitionierung



Alle bestehenden oder vorgeschlagenen Partitionen auf allen angeschlossenen Festplatten werden in der Liste im YaST-Dialogfeld *Festplatte vorbereiten: Expertenmodus* angezeigt. Ganze Festplatten werden als Geräte ohne Nummern aufgeführt, beispielsweise als `/dev/sda`. Partitionen werden als Teile dieser Geräte aufgelistet, beispielsweise als `/dev/sda1`. Größe, Typ, Dateisystem und Einhängpunkt der Festplatten und ihrer Partitionen werden ebenfalls angezeigt. Der Einhängpunkt gibt an, wo sich die Partition im Linux-Dateisystembaum befindet.

Wenn Sie das Experten-Dialogfeld während der Installation ausführen, wird auch sämtlicher freier Speicherplatz aufgeführt und automatisch ausgewählt. Um weiteren Speicherplatz für openSUSE® zur Verfügung zu stellen, müssen Sie den benötigten Speicherplatz von unten nach oben in der Liste freigeben (Sie beginnen mit der letzten Partition der Festplatte und enden mit der ersten). Wenn Sie beispielsweise über drei

Partitionen verfügen, können Sie nicht die zweite ausschließlich für openSUSE und die dritte und erste für andere Betriebssysteme verwenden.

2.1.1 Partitionstypen

Jede Festplatte verfügt über eine Partitionierungstabelle mit Platz für vier Einträge. Ein Eintrag in der Partitionstabelle kann für eine primäre oder für eine erweiterte Partition stehen. Es ist jedoch nur ein Eintrag für eine erweiterte Partition zulässig.

Eine primäre Partition besteht aus einem kontinuierlichen Bereich von Zylindern (physikalischen Festplattenbereichen), die einem bestimmten Betriebssystem zugewiesen sind. Mit ausschließlich primären Partitionen wären Sie auf vier Partitionen pro Festplatte beschränkt, da die Partitionstabelle nicht mehr Platz bietet. Aus diesem Grund werden erweiterte Partitionen verwendet. Erweiterte Partitionen sind ebenfalls kontinuierliche Bereiche von Festplattenzylindern, können jedoch in mehrere *logische Partitionen* unterteilt werden. Für logische Partitionen sind keine Einträge in der Partitionstabelle erforderlich. Eine erweiterte Partition kann auch als Container für logische Partitionen bezeichnet werden.

Wenn Sie mehr als vier Partitionen benötigen, erstellen Sie als vierte Partition (oder früher) eine erweiterte Partition. Diese erweiterte Partition sollte den gesamten verbleibenden freien Zylinderbereich umfassen. Erstellen Sie dann mehrere logische Partitionen innerhalb der erweiterten Partition. Die maximale Anzahl der logischen Partitionen beträgt 15 auf SCSI-, SATA- und Firewire-Festplatten und 63 auf (E)IDE-Festplatten. Dabei spielt es keine Rolle, welche Arten von Partitionen für Linux verwendet werden. Sowohl primäre als auch logische Partitionen funktionieren problemlos.

2.1.2 Erstellen von Partitionen

Zum Erstellen einer neuen Partition von Grund auf gehen Sie wie folgt vor:

- 1 Wählen Sie *Erstellen*. Wenn mehrere Festplatten angeschlossen sind, wird ein Auswahldialogfeld angezeigt, in dem Sie eine Festplatte für die neue Partition auswählen können.
- 2 Geben Sie den Partitionstyp (primär oder erweitert) an. Sie können bis zu vier primäre Partitionen oder bis zu drei primäre Partitionen und eine erweiterte Par-

tion erstellen. Innerhalb der erweiterten Partition können Sie mehrere logische Partitionen erstellen (siehe [Abschnitt 2.1.1, „Partitionstypen“](#) (S. 47)).

- 3 Wählen Sie das zu verwendende Dateisystem und einen Einhängepunkt aus. YaST schlägt für jede erstellte Partition einen Einhängepunkt vor.
- 4 Geben Sie, falls erforderlich, zusätzliche Dateisystemoptionen an. Dies ist zum Beispiel für persistente Dateinamen erforderlich. Weitere Informationen zu den verfügbaren Optionen finden Sie in [Abschnitt 2.1.3, „Bearbeiten einer Partition“](#) (S. 48).
- 5 Klicken Sie auf *OK > Übernehmen*, um das Partitionierungs-Setup zu übernehmen und das Partitionierungsmodul zu verlassen.

Wenn Sie die Partition bei der Installation angelegt haben, wird wieder das Fenster mit der Installationsübersicht angezeigt.

2.1.3 Bearbeiten einer Partition

Wenn Sie eine neue Partition erstellen oder eine bestehende Partition bearbeiten, können verschiedene Parameter festgelegt werden. Bei neuen Partitionen werden von YaST geeignete Parameter festgelegt, für die normalerweise keine Bearbeitung erforderlich ist. Gehen Sie wie folgt vor, um Ihre Partitionseinstellungen manuell zu bearbeiten:

- 1 Wählen Sie die Partition aus.
- 2 Klicken Sie auf *Bearbeiten*, um die Partition zu bearbeiten und die Parameter festzulegen:

Dateisystem-ID

Auch wenn Sie die Partitionen zu diesem Zeitpunkt nicht formatieren möchten, weisen Sie eine Dateisystem-ID zu, um sicherzustellen, dass sie richtig registriert wird. Mögliche Werte sind *Linux*, *Linux Swap*, *Linux LVM* und *Linux RAID*. Einzelheiten zu LVM und RAID finden Sie unter [Abschnitt 2.2, „LVM-Konfiguration“](#) (S. 55) und [Abschnitt 2.3, „Soft-RAID-Konfiguration“](#) (S. 62).

Dateisystem

Ändern Sie hier das Dateisystem oder formatieren Sie die Partition. Wenn Sie das Dateisystem ändern oder Partitionen neu formatieren, werden alle Daten der Partition unwiederbringlich gelöscht.

Swap ist ein Sonderformat, das die Verwendung der Partition als virtuellen Arbeitsspeicher ermöglicht. Bei einer manuellen Partitionierung müssen Sie eine Swap-Partition mit mindestens 256 MB erstellen. Sollte der Swap-Speicher nicht ausreichen, empfiehlt es sich statt einer Erhöhung des Swap-Speichers, dem System mehr Arbeitsspeicher hinzuzufügen.

Ext3 ist das Standarddateisystem für die Linux-Partitionen. ReiserFS, JFS, and Ext3 sind Journaling-Dateisysteme. Mit diesen Dateisystemen kann das System nach einem Systemabsturz schnell wiederhergestellt werden, da die Schreibvorgänge während des Vorgangs protokolliert werden. Außerdem kann ReiserFS sehr schnell viele kleine Dateien verarbeiten. Ext2 ist kein Journaling-Dateisystem. Es ist jedoch extrem stabil und gut für kleinere Partitionen geeignet, da nicht viel Festplattenspeicher für die Verwaltung erforderlich ist.

Dateisystem verschlüsseln

Wenn Sie die Verschlüsselung aktivieren, werden alle Daten in verschlüsselter Form geschrieben. Dies erhöht die Sicherheit sensibler Daten, die Systemgeschwindigkeit wird jedoch leicht reduziert, da die Verschlüsselung einige Zeit erfordert. Weitere Informationen zur Verschlüsselung der Dateisysteme finden Sie in [Kapitel 31, *Verschlüsseln von Partitionen und Dateien*](#) (S. 545).

Fstab-Optionen

Legen verschiedene Parameter in der globalen Systemverwaltungsdatei (`/etc/fstab`) fest. In der Regel reichen die Standardeinstellungen für die meisten Konfigurationen aus. Sie können beispielsweise die Dateisystemkennung von einem Gerätenamen in eine Volume-Bezeichnung ändern. In Volume-Bezeichnungen können Sie alle Zeichen mit Ausnahme von `/` und dem Leerzeichen verwenden.

Für persistente Gerätenamen verwenden Sie die Einhängeloption *Geräte-ID*, *UUID* oder *LABEL*. In openSUSE sind persistente Gerätenamen standardmäßig aktiviert.

Wenn Sie die Einhängeloption *LABEL* zum Einhängen einer Partition verwenden, definieren Sie für die ausgewählte Partition ein passendes Label. Sie könnten beispielsweise das Partitions-Label *HOME* für eine Partition verwenden, die in */home* eingehängt werden soll.

Wenn Sie für das Dateisystem Quotas verwenden möchten, verwenden Sie die Einhängeloption *Enable Quota Support* (Quota-Unterstützung aktivieren). Diese Konfiguration ist erforderlich, bevor Sie in der *Benutzerverwaltung* von YaST Quotas für Benutzer festlegen. Weitere Informationen zur Konfiguration von Benutzerquotas finden Sie unter Abschnitt „Verwalten von Quoten“ (Kapitel 5, *Verwalten von Benutzern mit YaST*, ↑Start).

Einhängepunkt

Geben Sie das Verzeichnis an, in dem die Partition im Dateisystembaum eingehängt werden soll. Treffen Sie eine Auswahl aus verschiedenen YaST-Vorschlägen oder geben Sie einen beliebigen anderen Namen ein.

3 Wählen Sie *OK > Übernehmen*, um die Partition zu aktivieren.

ANMERKUNG: Anpassen der Größe von Dateisystemen

Verwenden Sie die Option *Größe ändern*, um die Größe eines vorhandenen Dateisystems anzupassen. Beachten Sie, dass die Größe von eingehängten Partitionen nicht verändert werden kann. Um die Größe von Partitionen zu ändern, hängen Sie die entsprechende Partition aus, bevor Sie den Partitionierer ausführen.

2.1.4 Optionen für Experten

Mit *Experten* wird ein Menü geöffnet, das folgende Befehle enthält:

Partitionstabelle neu einlesen

Liest die Partitionierung erneut von dem Datenträger ein. Dies ist beispielsweise nach der manuellen Partitionierung in der Textkonsole erforderlich.

Partitionstabelle und Festplattenkennung löschen

Mit dieser Option wird die alte Partitionstabelle vollständig überschrieben. Dies kann beispielsweise bei Problemen mit unkonventionellen Festplattenkennungen hilfreich sein. Bei dieser Methode gehen alle Daten auf der Festplatte verloren.

iSCSI-Konfiguration

Für den Zugriff auf SCSI über IP-Block-Geräte müssen Sie zunächst iSCSI konfigurieren. Dadurch erhalten Sie weitere verfügbare Geräte in der Hauptpartitionsliste.

2.1.5 Weitere Partitionierungstipps

Im folgenden Abschnitt finden Sie einige Hinweise und Tipps für die Partitionierung, die Ihnen bei der Einrichtung Ihres Systems helfen, die richtigen Entscheidungen zu treffen.

TIPP: Anzahl der Zylinder

Einige Partitionierungstools beginnen bei der Nummerierung der Zylinder mit 0 andere mit 1. Die Zylinderzahl berechnet sich immer aus der Differenz zwischen der letzten und der ersten Zylinder Nummer plus eins.

Fremde Partitionen und `fstab`

Wenn die Partitionierung von YaST durchgeführt wird und andere Partitionen im System erkannt werden, werden diese Partitionen ebenfalls in die Datei `/etc/fstab` aufgenommen, um den mühelosen Dateizugriff zu ermöglichen. Diese Datei enthält alle Partitionen im System sowie deren Eigenschaften, beispielsweise Dateisystem, Einhängepunkt und Benutzerberechtigungen.

Beispiel 2.1 `/etc/fstab`: Partitionsdaten

```
LABEL=DATA1    /data1    auto    noauto,user 0 0
LABEL=DATA2    /data2    auto    noauto,user 0 0
LABEL=DATA3    /data3    auto    noauto,user 0 0
```

Unabhängig davon, ob es sich um Linux- oder FAT-Partitionen handelt, werden diese Partitionen mit den Optionen `noauto` und `user` angegeben. Dadurch kann jeder Benutzer diese Partitionen nach Bedarf einhängen oder aushängen. Aus Sicherheitsgründen gibt YaST hier nicht automatisch die Option `exec` ein, die zur Ausführung von Programmen vom Speicherort aus erforderlich ist. Wenn Sie jedoch Programme von diesem Ort aus ausführen möchten, können Sie die Option manuell eingeben. Diese Maßnahme ist erforderlich, wenn Sie Systemmeldungen, wie beispielsweise Meldungen über einen „fehlerhaften Interpreter“ oder „verweigerte Berechtigungen“, erhalten.

Verwenden von Swap

Mittels Swap wird der physikalisch verfügbare Arbeitsspeicher erweitert. Ihnen steht dadurch über das physikalische RAM hinaus mehr Arbeitsspeicher zur Verfügung. Die Arbeitsspeicherverwaltungssysteme der Kernels vor Version 2.4.10 benötigten Swap als Sicherheitszugabe. Wenn Ihr Swap damals nicht zweimal so groß war wie Ihr RAM, kam es zu erheblichen Leistungseinbußen. Auf heutige Systeme treffen diese Einschränkungen allerdings nicht mehr zu.

Linux verwendet eine Seite namens „Kürzlich verwendet“ (LRU) zur Auswahl von Seiten, die eventuell vom Arbeitsspeicher auf die Festplatte verschoben werden. Den aktiven Anwendungen steht dadurch mehr Arbeitsspeicher zur Verfügung und selbst das Zwischenspeichern läuft reibungsloser ab.

Versucht eine Anwendung jedoch, sämtlichen Arbeitsspeicher für sich zu reklamieren, den sie nur irgendwie erhalten kann, kann es mit dem Swap-Speicher zu Problemen kommen. Wir sollten uns hierzu drei der wichtigsten Szenarien näher ansehen:

System ohne Swap

Die Anwendung erhält den gesamten Arbeitsspeicher, der, auf welche Weise auch immer, freigegeben werden kann. Der gesamte Cache-Speicher wird freigegeben. Dadurch verlangsamten sich alle anderen Anwendungen. Nach einigen Minuten tritt der "Out of Memory-Killermechanismus" des Kernels in Kraft und der Prozess wird abgebrochen.

System mit mittelgroßem Swap (128 MB – 512 MB)

Zunächst lässt die Leistung des Systems wie bei einem System ohne Swap nach. Sobald das gesamte physikalische RAM aufgebraucht ist, wird auch auf den Swap-Speicher zurückgegriffen. An diesem Punkt wird das System sehr langsam; die Fernausführung von Kommandos wird unmöglich. Je nach Geschwindigkeit der Festplatten, die den Swap-Speicher stellen, verbleibt das System etwa 10 bis 15 Minuten in diesem Zustand, bevor das Problem vom "Out of Memory-Killer" des Kernels endgültig "gelöst" wird. Beachten Sie, dass Sie eine bestimmte Swap-Größe benötigen, wenn der Computer einen „Suspend to Disk“ ausführen sollte. In diesem Fall sollte die Swap-Größe groß genug sein, um die benötigten Daten vom Arbeitsspeicher (512 MB–1GB) aufnehmen zu können.

System mit großem Swap (mehrere GB)

Auf einem solchen System sollte besser keine Anwendung ausgeführt werden, die völlig außer Rand und Band gerät und den Swap-Speicher grenzenlos nutzt. In

einem solchen Fall würde das System Stunden brauchen, um sich wieder zu regenerieren. Sehr wahrscheinlich treten in diesem Fall bei anderen Prozessen Timeouts und Fehler auf, wodurch das System in einem undefinierten Zustand zurückbleibt, selbst wenn der fehlerhafte Prozess abgebrochen wird. Am besten schalten Sie das System in einem solchen Fall aus und wieder ein und versuchen Sie, es wieder hochzufahren. Sehr viel Swap-Speicher ist nur dann sinnvoll, wenn Sie eine Anwendung verwenden, die diese Menge an Swap tatsächlich benötigt. Solche Anwendungen (wie Datenbanken oder Bildbearbeitungsprogramme) verfügen häufig über eine Option, mit der sie den benötigten Festplattenspeicher direkt abrufen können. Die Verwendung dieser Option ist auf jeden Fall einem übergroßen Swap-Speicher vorzuziehen.

Falls Ihre Anwendungen nicht außer Kontrolle geraten, aber dennoch nach einiger Zeit mehr Swap erforderlich ist, können Sie den Swap-Speicher auch online erweitern. Wenn Sie eine Partition als Swap-Speicher vorbereitet haben, fügen Sie diese Partition einfach mit Hilfe von YaST hinzu. Falls Sie auf keine Swap-Partition zurückgreifen können, können Sie den Swap-Speicher auch durch eine Swap-Datei erweitern. Swap-Dateien sind im Vergleich zu Partitionen in der Regel langsamer. Im Vergleich zu physikalischem RAM sind jedoch beide Swap-Methoden extrem langsam. Der tatsächliche Geschwindigkeitsunterschied ist allerdings nicht so bedeutend, wie es den Anschein hat.

Prozedur 2.1 *Manuelles Hinzufügen einer Swap-Datei*

So fügen Sie dem laufenden System eine Swap-Datei hinzu:

- 1** Erstellen Sie auf Ihrem System eine leere Datei. Um beispielsweise eine Swap-Datei für 128 MB Swap-Speicher unter `/var/lib/swap/swapfile` hinzuzufügen, geben Sie folgende Kommandos ein:

```
mkdir -p /var/lib/swap
dd if=/dev/zero of=/var/lib/swap/swapfile bs=1M count=128
```

- 2** Initialisieren Sie die Swap-Datei mit folgendem Kommando:

```
mkswap /var/lib/swap/swapfile
```

- 3** Aktivieren Sie den Swap-Speicher mit folgendem Kommando:

```
swapon /var/lib/swap/swapfile
```

Zum Deaktivieren der Swap-Datei verwenden Sie folgendes Kommando:

```
swapoff /var/lib/swap/swapfile
```

- 4 Zum Überprüfen des aktuell verfügbaren Swap-Speichers verwenden Sie folgendes Kommando:

```
cat /proc/swaps
```

Bislang handelt es sich hier lediglich um temporären Swap-Speicher. Nach dem nächsten Neustart wird dieser nicht mehr verwendet.

- 5 Wenn Sie die Swap-Datei permanent aktivieren möchten, fügen Sie `/etc/fstab` folgende Zeile hinzu:

```
/var/lib/swap/swapfile swap swap defaults 0 0
```

2.1.6 Partitionierung und LVM

Von der Expertenpartitionierung aus können Sie mit *LVM* die LVM-Konfiguration aufrufen (siehe [Abschnitt 2.2, „LVM-Konfiguration“](#) (S. 55)). Wenn jedoch bereits eine funktionierende LVM-Konfiguration auf Ihrem System vorhanden ist, wird diese automatisch aktiviert, sobald Sie die LVM-Konfiguration zum ersten Mal in einer Sitzung eingeben. In diesem Fall können alle Festplatten mit einer Partition, die zu einer aktivierten Volume-Gruppe gehören, nicht erneut partitioniert werden, da der Linux-Kernel die bearbeitete Partitionstabelle einer Festplatte nicht erneut lesen kann, wenn eine Partition auf diesem Datenträger verwendet wird. Wenn jedoch bereits eine funktionierende LVM-Konfiguration auf Ihrem System vorhanden ist, sollte eine physische Neupartitionierung nicht erforderlich sein. Ändern Sie stattdessen die Konfiguration des logischen Volumes.

Am Anfang der physischen Volumes (PVs) werden Informationen zum Volume auf die Partition geschrieben. Um eine solche Partition für andere Zwecke, die nichts mit LVM zu tun haben, wiederzuverwenden, sollten Sie den Anfang dieses Volumes löschen. Bei der VG `system` und dem PV `/dev/sda2` beispielsweise ist dies über den Befehl `ddif=/dev/zero of=/dev/sda2 bs=512 count=1` möglich.

WARNUNG: Dateisystem zum Booten

Das zum Booten verwendete Dateisystem (das Root-Dateisystem oder `/boot`) darf nicht auf einem logischen LVM-Volume gespeichert werden. Speichern Sie es stattdessen auf einer normalen physischen Partition.

2.2 LVM-Konfiguration

Dieser Abschnitt erläutert kurz die Prinzipien von LVM und seinen grundlegenden Funktionen, mit denen es in vielen Situationen nützlich ist. In [Abschnitt 2.2.2, „LVM-Konfiguration mit YaST“](#) (S. 57) wird erläutert, wie LVM mit YaST eingerichtet wird.

WARNUNG

Der Einsatz von LVM kann mit einem höheren Risiko (etwa des Datenverlusts) verbunden sein. Risiken umfassen auch Anwendungsausfälle, Stromausfälle und fehlerhafte Befehle. Speichern Sie Ihre Daten, bevor Sie LVM implementieren oder Volumes neu konfigurieren. Arbeiten Sie nie ohne Backup.

2.2.1 Der Logical Volume Manager

Der Logical Volume Manager (LVM) ermöglicht eine flexible Verteilung von Festplattenspeicher über mehrere Dateisysteme. Er wurde entwickelt, da gelegentlich die Segmentierung des Festplattenspeichers geändert werden muss, nachdem die erste Partitionierung bei der Installation abgeschlossen wurde. Da es schwierig ist, Partitionen in einem laufenden System zu ändern, bietet LVM einen virtuellen Pool (Volume-Gruppe, kurz: VG) an Speicherplatz, aus dem bei Bedarf logische Volumes (LVs) erzeugt werden können. Das Betriebssystem greift dann auf diese logischen Volumes statt auf physische Partitionen zu. Volume-Gruppen können sich über mehr als eine Festplatte erstrecken, wobei mehrere Festplatten oder Teile davon eine einzige VG bilden können. Auf diese Weise bietet LVM eine Art Abstraktion vom physischen Festplattenplatz, der eine viel einfachere und sicherere Möglichkeit zur Änderung der Aufteilung ermöglicht als die physische Umpartitionierung. Hintergrundinformationen zum physischen Partitionieren erhalten Sie in [Abschnitt 2.1.1, „Partitionstypen“](#) (S. 47) und [Abschnitt 2.1, „Verwenden der YaST-Partitionierung“](#) (S. 45).

Abbildung 2.2 *Physische Partitionierung versus LVM*

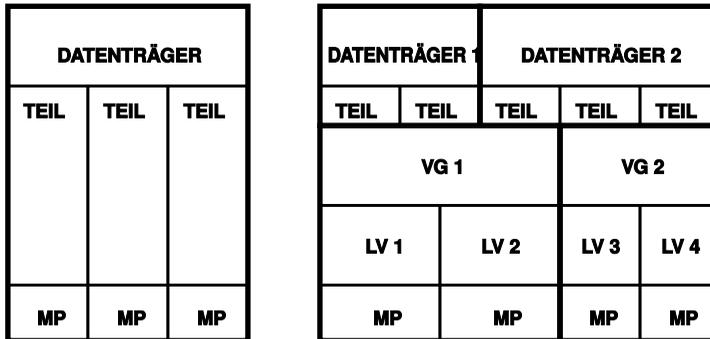


Abbildung 2.2, „Physische Partitionierung versus LVM“ (S. 56) stellt die physische Partitionierung (links) der LVM-Segmentierung (rechts) gegenüber. Auf der linken Seite wurde eine einzelne Festplatte in drei physische Partitionen (PART) aufgeteilt, von denen jede einen Einhängepunkt (MP) hat, auf den das Betriebssystem zugreifen kann. Auf der rechten Seite wurden zwei Festplatten in zwei bzw. drei physische Partitionen aufgeteilt. Es wurden zwei LVM-Volume-Gruppen (VG 1 und VG 2) angelegt. VG 1 enthält zwei Partitionen von DISK 1 und eine von DISK 2. VG 2 enthält die restlichen zwei Partitionen von DISK 2. In LVM werden die in einer Volume-Gruppe zusammengefassten physischen Festplattenpartitionen als physische Volumes (PVs) bezeichnet. In den Volume-Gruppen wurden vier logische Volumes (LV 1 bis LV 4) angelegt, die vom Betriebssystem über die zugewiesenen Einhängepunkte benutzt werden können. Die Grenzen zwischen verschiedenen logischen Volumes müssen sich nicht mit den Partitions Grenzen decken. Dies wird in diesem Beispiel durch die Grenze zwischen LV 1 und LV 2 veranschaulicht.

LVM-Funktionen:

- Mehrere Festplatten/Partitionen können zu einem großen logischen Volume zusammengefügt werden.
- Neigt sich bei einem LV (z. B. /usr) der freie Platz dem Ende zu, können Sie dieses bei geeigneter Konfiguration vergrößern.
- Mit dem LVM können Sie im laufenden System Festplatten oder LVs hinzufügen. Voraussetzung ist allerdings hotswap-fähige Hardware, die für solche Aktionen geeignet ist.

- Es ist möglich, einen "Striping-Modus" zu aktivieren, der den Datenstrom eines logischen Volumes über mehrere physische Volumes verteilt. Wenn sich diese physischen Volumes auf verschiedenen Festplatten befinden, kann dies die Lese- und Schreibgeschwindigkeit wie bei RAID 0 verbessern.
- Die Snapshot-Funktion ermöglicht vor allem bei Servern konsistente Backups im laufenden System.

Aufgrund dieser Eigenschaften lohnt sich der Einsatz von LVM bereits bei umfangreich genutzten Home-PCs oder kleinen Servern. Wenn Sie einen wachsenden Datenbestand haben wie bei Datenbanken, Musikarchiven oder Benutzerverzeichnissen, bietet sich der Logical Volume Manager an. Dann ist es möglich, Dateisysteme zu haben, die größer sind als eine physische Festplatte. Ein weiterer Vorteil des LVM ist die Möglichkeit, bis zu 256 LVs anlegen zu können. Beachten Sie jedoch, dass sich die Arbeit mit dem LVM sehr von der mit konventionellen Partitionen unterscheidet. Anleitungen und weiterführende Informationen zur Konfiguration des LVM finden Sie im offiziellen LVM-Howto unter <http://tldp.org/HOWTO/LVM-HOWTO/>.

Ab Kernel Version 2.6 steht Ihnen LVM in der Version 2 zur Verfügung. Er ist abwärtskompatibel zum bisherigen LVM und kann alte Volume-Gruppen weiter verwalten. Wenn Sie neue Volume-Gruppen anlegen, müssen Sie entscheiden, ob Sie das neue Format oder die abwärtskompatible Version verwenden möchten. LVM 2 benötigt keine Kernel-Patches mehr. Er verwendet die in Kernel 2.6 integrierte Gerätezuordnung. Dieser Kernel unterstützt nur LVM, Version 2. In diesem Abschnitt wird LVM gleichbedeutend mit LVM, Version 2 verwendet.

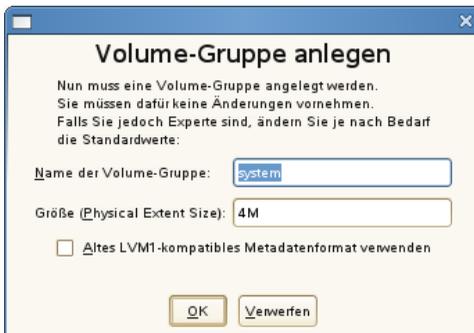
2.2.2 LVM-Konfiguration mit YaST

Zur LVM-Konfiguration mit YaST gelangen Sie über den YaST-Expertenmodus des Partitionierungsmoduls (siehe [Abschnitt 2.1](#), „**Verwenden der YaST-Partitionierung**“ (S. 45)). Mit diesem Partitionierungswerkzeug können Sie vorhandene Partitionen bearbeiten und löschen sowie neue Partitionen erstellen, die mit LVM verwendet werden sollen. Sie erstellen eine LVM-Partition, indem Sie zunächst auf *Anlegen > Nicht formatieren* klicken und anschließend *0x8E Linux LVM* als Partitions-ID wählen. Nachdem Sie alle mit LVM zu verwendenden Partitionen erstellt haben, klicken Sie auf *LVM*, um mit der Konfiguration von LVM zu beginnen.

Erstellen von Volume-Gruppen

Wenn auf Ihrem System noch keine Volume-Gruppe existiert, werden Sie aufgefordert, eine anzulegen (siehe [Abbildung 2.3](#), „Anlegen einer Volume-Gruppe“ (S. 58)). Zusätzliche Gruppen können mit *Gruppe hinzufügen* hinzugefügt werden. Gewöhnlich ist jedoch eine Volume-Gruppe ausreichend. Als Name für die Volume-Gruppe, auf der sich die Dateien des openSUSE®-Systems befinden, wird `system` vorgeschlagen. Die Physical Extent Size bestimmt die maximale Größe eines physischen Blocks in der Volume-Gruppe. Der gesamte Plattenplatz in einer Volume-Gruppe wird in Blöcken dieser Größe verwaltet. Dieser Wert wird normalerweise auf 4 MB festgelegt. Dies lässt eine Maximalgröße für ein physisches und logisches Volume von 256 GB zu. Sie sollten die Physical Extent Size also nur dann erhöhen (z. B. auf 8, 16 oder 32 GB), wenn Sie größere logische Volumes als 256 GB benötigen.

Abbildung 2.3 Anlegen einer Volume-Gruppe



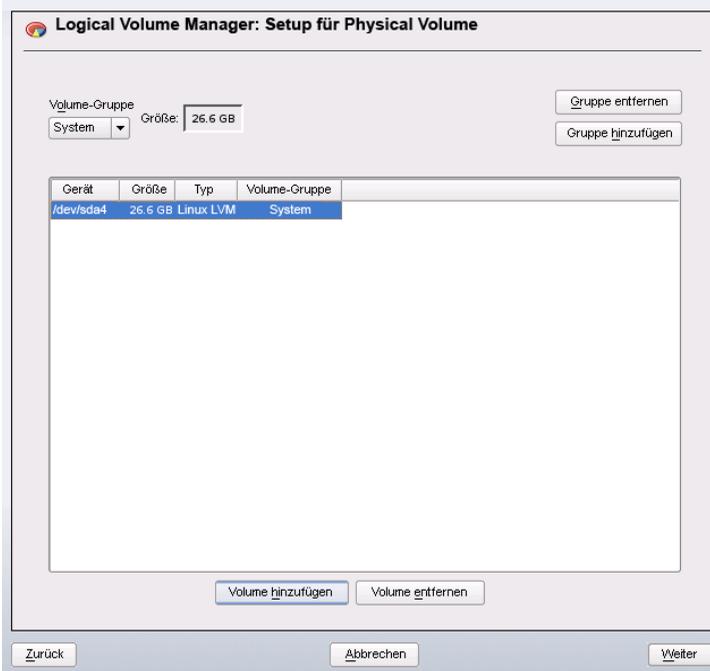
Konfigurieren von physischen Volumes

Sobald eine Volume-Gruppe angelegt wurde, listet das folgende Dialogfeld alle Partitionen auf, die entweder den Typ „Linux LVM“ oder „Linux native“ haben. Swap- oder DOS-Partitionen werden nicht angezeigt. Wenn eine Partition bereits einer Volume-Gruppe zugeordnet ist, wird der Name der Volume-Gruppe in der Liste angezeigt. Nicht zugewiesene Partitionen sind mit „-“ gekennzeichnet.

Falls es mehrere Volume-Gruppen gibt, stellen Sie die aktuelle Volume-Gruppe im Auswahlfeld links oben ein. Mit den Schaltflächen rechts oben ist es möglich, zusätzliche Volume-Gruppen anzulegen und bestehende Volume-Gruppen zu löschen. Es können allerdings nur solche Volume-Gruppen gelöscht werden, denen keine Partitionen mehr

zugeordnet sind. Partitionen, die einer Volume-Gruppe zugeordnet sind, werden auch physische Volumes (PV) genannt.

Abbildung 2.4 Setup für physische Volumes



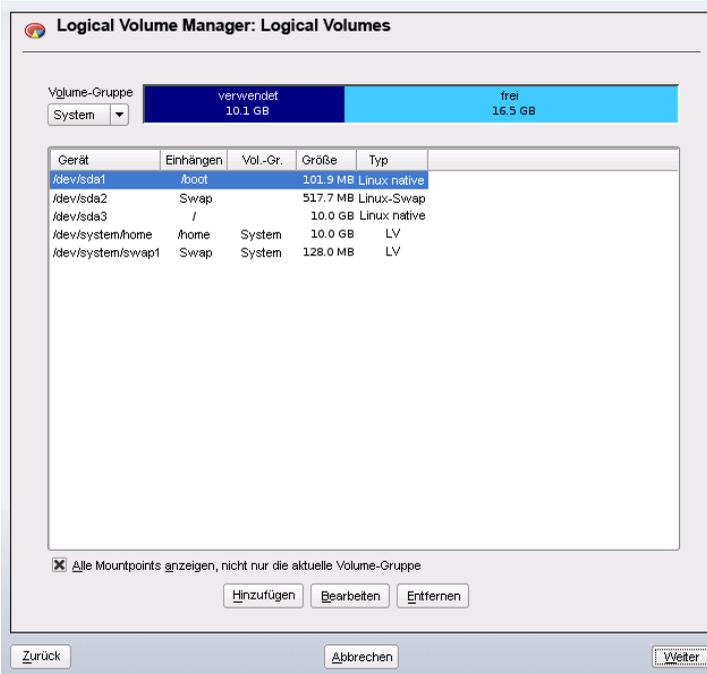
Um der ausgewählten Volume-Gruppe eine zuvor nicht zugewiesene Partition zuzuweisen, klicken Sie zuerst auf die Partition und anschließend auf *Volume hinzufügen*. Der Name der Volume-Gruppe wird dann bei der ausgewählten Partition eingetragen. Sie sollten alle Partitionen, die Sie für LVM vorgesehen haben, einer Volume-Gruppe zuordnen. Anderenfalls bleibt der Speicherplatz in den Partitionen unbenutzt. Bevor Sie das Dialogfeld schließen können, muss jeder Volume-Gruppe mindestens ein physisches Volume zugeordnet sein. Nachdem Sie alle physischen Volumes zugeordnet haben, klicken Sie auf *Weiter*, um zur Konfiguration der logischen Volumes zu gelangen.

Konfigurieren von logischen Volumes

Nachdem die Volume-Gruppe mit physischen Volumes gefüllt ist, bestimmen Sie im nächsten Dialogfeld die logischen Volumes, die das Betriebssystem benutzen soll.

Wählen Sie im Auswahlfeld oben links die aktuelle Volume-Gruppe. Der verfügbare Platz in der aktuellen Volume-Gruppe wird daneben angezeigt. Die Liste darunter enthält alle logischen Volumes in der Volume-Gruppe. Alle normalen Linux-Partitionen, denen ein Einhängepunkt zugewiesen wurde, alle Swap-Partitionen und alle existierenden logischen Volumes werden hier aufgeführt. Sie können nach Bedarf logische Volumes mithilfe der entsprechenden Schaltflächen *Hinzufügen*, *Bearbeiten* und *Entfernen*, bis der Platz in der Volume-Gruppe verbraucht ist. Weisen Sie jeder Volume-Gruppe mindestens ein logisches Volume zu.

Abbildung 2.5 Verwaltung der logischen Volumes



Um ein neues logisches Volume anzulegen, klicken Sie auf *Hinzufügen* und füllen das anschließende Pop-up-Fenster aus. Wie bei der Partitionierung kann die Größe, das Dateisystem und der Einhängepunkt eingegeben werden. Normalerweise wird in einem logischen Volume ein Dateisystem wie reiserfs oder ext2 erstellt und ein Einhängepunkt wird festgelegt. Die auf diesem logischen Volume gespeicherten Dateien sind dann im installierten System an diesem Einhängepunkt zu finden. Es ist auch möglich, den Datenfluss im logischen Volume über verschiedene physische Volumes zu verteilen (Striping). Wenn sich diese physischen Volumes auf verschiedenen Festplatten befinden,

verbessert dies in der Regel die Lese- und Schreibgeschwindigkeit (wie bei RAID 0). Ein Striping-LV mit n Stripes kann jedoch nur richtig angelegt werden, wenn der von dem LV benötigte Festplattenplatz gleichmäßig über n physische Volumes verteilt werden kann. Sind beispielsweise nur zwei physische Volumes verfügbar, ist ein logisches Volume mit drei Stripes nicht möglich.

WARNUNG: Striping

YaST hat zurzeit keine Möglichkeit, die Richtigkeit Ihrer Angaben zum Striping zu überprüfen. Fehler an dieser Stelle können erst festgestellt werden, wenn LVM auf der Festplatte in Betrieb genommen wird.

Abbildung 2.6 Erstellen logischer Volumes

The screenshot shows a dialog box titled "Logical Volume erstellen". It contains the following fields and options:

- Name des Logical Volume:** Home
- Größe:** +10G (with a "max" button and "max = 26.5 GB" text)
- Stripes:** 1
- Stripe-Größe:** 64
- Mountpoint:** /home
- Formatieren:** Radio buttons for "Nicht formatieren" and "Formatieren" (selected).
- Dateisystem:** Ext3 (dropdown menu)
- Dateisystem verschlüsseln:** Unchecked checkbox
- Buttons:** "OK" and "Abbrechen"

Falls Sie auf Ihrem System LVM bereits konfiguriert haben, können Sie jetzt die vorhandenen logischen Volumes eingeben. Bevor Sie fortfahren, weisen Sie diesen logischen Volumes passende Einhängepunkte zu. Klicken Sie auf *Weiter*, um in den YaST-Expertenmodus für Partitionierung zu gelangen und Ihre Arbeit abzuschließen.

Direkte Verwaltung von LVM

Falls Sie LVM bereits konfiguriert haben und lediglich etwas ändern möchten, gibt es eine alternative Methode. Wählen Sie im YaST-Kontrollzentrum *System > LVM*. Im Wesentlichen erlaubt dieses Dialogfeld dieselben Aktionen wie oben beschrieben, mit Ausnahme der physischen Partitionierung. Es zeigt die vorhandenen physischen Volumes und logischen Volumes in zwei Listen an. Sie können Ihr LVM-System mit den oben beschriebenen Methoden verwalten.

2.3 Soft-RAID-Konfiguration

Der Sinn eines RAID (Redundant Array of Independent Disks) ist es, mehrere Festplattenpartitionen in einer großen *virtuellen* Festplatte zusammenzufassen, um die Leistung und/oder die Datensicherheit zu optimieren. Die meisten RAID-Controller verwenden das SCSI-Protokoll, da es im Vergleich zum IDE-Protokoll eine größere Anzahl an Festplatten effektiver ansteuern kann und besser für eine parallele Verarbeitung der Befehle geeignet ist. Es gibt einige RAID-Controller, die IDE- oder SATA-Festplatten unterstützen. Soft RAID bietet die Vorteile von RAID-Systemen ohne die zusätzlichen Kosten für hardwareseitige RAID-Controller. Dies geht allerdings zu Lasten von Prozessorzeit und Arbeitsspeicher, weshalb Soft RAID für Hochleistungssysteme nicht wirklich geeignet ist.

openSUSE® ermöglicht die Zusammenfassung mehrerer Festplatten zu einem Soft-RAID-System. RAID bietet verschiedene Strategien für das Kombinieren mehrerer Festplatten in einem System, von der jede andere Ziele, Vorteile und Merkmale aufweist. Diese Variationen werden im Allgemeinen als *RAID-Level* bezeichnet.

Es gibt folgende gängige RAID-Level:

RAID 0

Dieser Level verbessert die Leistung des Datenzugriffs, indem er die einzelnen Dateiblöcke über mehrere Festplattenlaufwerke verteilt. Im Grunde ist dies gar kein RAID, da es keine Datensicherheit gibt, doch die Bezeichnung *RAID 0* hat sich für diese Art von System eingebürgert. Bei RAID 0 werden mindestens zwei Festplatten zusammengefasst. Die Leistung ist zwar sehr gut, aber wenn auch nur eine der Festplatten ausfällt, ist das RAID-System zerstört und Ihre Daten sind verloren.

RAID 1

Dieser Level bietet eine ausreichende Sicherheit für Ihre Daten, weil sie 1:1 auf eine andere Festplatte kopiert werden. Dies wird als *Festplattenspiegelung* bezeichnet. Ist eine Festplatte zerstört, steht eine Kopie des Inhalts auf einer anderen zur Verfügung. Solange noch eine Festplatte intakt ist, können alle anderen fehlerhaft sein, ohne dass Daten verloren gehen. Wird der Schaden jedoch nicht festgestellt, kann es passieren, dass die beschädigten Daten auf die intakte Festplatte gespiegelt werden. Erst dadurch geht die Integrität der Daten wirklich verloren. Die Schreibleistung leidet durch den Kopiervorgang im Vergleich zu einer normalen physischen Festplatte ein wenig (10 bis 20 % langsamer), dafür ist der Lesezugriff deutlich schneller, weil die Daten doppelt vorhanden sind und somit parallel ausgelesen werden können. Im Allgemeinen kann gesagt werden, dass RAID 1 fast eine doppelt so schnelle Transaktionsrate und nahezu dieselbe Schreibgeschwindigkeit wie einzelne Festplatten bieten.

RAID 2 und RAID 3

Dies sind keine typischen RAID-Implementierungen. Level 2 verteilt die Daten auf Bit- und nicht auf Blockebene. Level 3 bietet Byte-basiertes Verteilen mit einer dedizierten Paritätsfestplatte und kann nicht gleichzeitig mehrere Anforderungen verarbeiten. Diese beiden Level werden nur selten verwendet.

RAID 4

Level 4 verteilt die Daten auf Blockebene wie bei Level 0, wobei diese Vorgehensweise mit einer dedizierten Paritätsfestplatte kombiniert wird. Die Paritätsdaten werden im Fall eines Festplattenfehlers zum Erstellen einer Ersatzfestplatte verwendet. Die Paritätsfestplatte kann beim Schreibzugriff jedoch Engpässe verursachen. Dennoch wird Level 4 gelegentlich eingesetzt.

RAID 5

RAID 5 ist ein optimierter Kompromiss aus Level 0 und Level 1, was Leistung und Redundanz betrifft. Der nutzbare Festplattenplatz entspricht der Anzahl der eingesetzten Festplatten minus einer. Die Daten werden wie bei RAID 0 über die Festplatten verteilt. Für die Sicherheit sorgen die *Paritätsblöcke*, die bei RAID 5 auf einer der Partitionen angelegt werden. Diese werden mit XOR miteinander verknüpft, sodass sich beim Ausfall einer Partition durch den dazugehörigen Paritätsblock der Inhalt rekonstruieren lässt. Bei RAID 5 ist zu beachten, dass nicht mehrere Festplatten gleichzeitig ausfallen dürfen. Wenn eine Festplatte ausfällt, muss sie schnellstmöglich ausgetauscht werden, da sonst Datenverlust droht.

Weitere RAID-Level

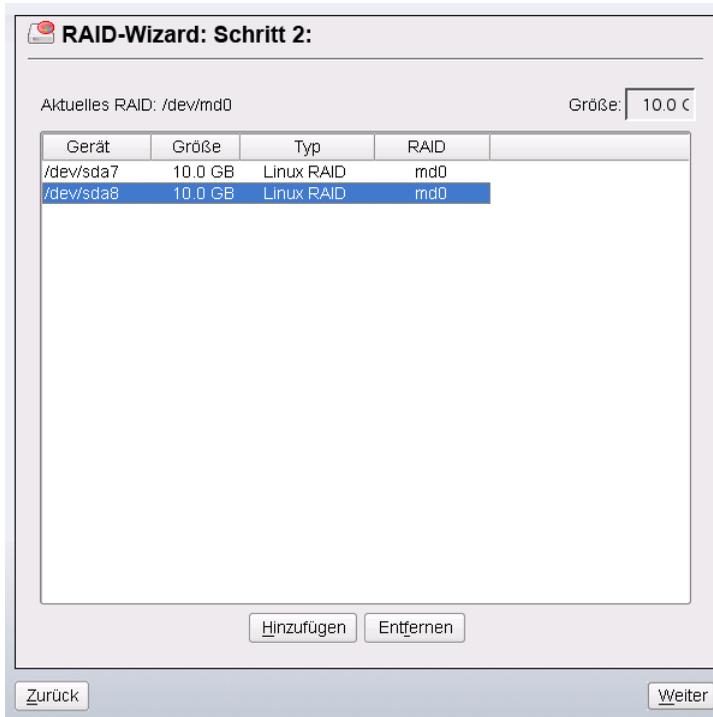
Es wurden noch weitere RAID-Level entwickelt (RAIDn, RAID 10, RAID 0+1, RAID 30, RAID 50 usw.), wobei einige von diesen proprietäre Implementierungen verschiedener Hardwarehersteller sind. Diese Level sind nicht sehr weit verbreitet und werden aus diesem Grund hier nicht näher beschrieben.

2.3.1 Soft-RAID-Konfiguration mit YaST

Zur Soft-RAID-Konfiguration gelangen Sie über den YaST-Expertenmodus des Partitionierungsmoduls, der in [Abschnitt 2.1, „Verwenden der YaST-Partitionierung“](#) (S. 45) beschrieben ist. Mit diesem Partitionierungswerkzeug können Sie vorhandene Partitionen bearbeiten und löschen sowie neue Partitionen erstellen, die mit Soft-RAID verwendet werden sollen. Sie erstellen die RAID-Partitionen, indem Sie zunächst auf *Erstellen > Nicht formatieren* klicken und anschließend *0xFD Linux RAID* als Partitions-ID wählen. Für RAID 0 und RAID 1 sind mindestens zwei Partitionen erforderlich, für RAID 1 in der Regel exakt zwei. Für RAID 5 sind mindestens drei Partitionen erforderlich. Es wird empfohlen, nur Partitionen gleicher Größe zu verwenden. Die einzelnen Partitionen eines RAIDs sollten auf verschiedenen Festplatten liegen, damit das Risiko eines Datenverlusts durch den Defekt einer Festplatte (RAID 1 und 5) verringert und die Leistung von RAID 0 optimiert wird. Wenn Sie alle gewünschten Partitionen erstellt haben, klicken Sie auf *RAID > RAID anlegen*, um die RAID-Konfiguration zu starten.

Wählen Sie im nächsten Dialogfeld zwischen RAID-Level 0, 1 oder 5. Wenn Sie auf *Weiter* klicken, werden im folgenden Dialogfeld alle Partitionen entweder mit dem Typ „Linux RAID“ oder „Linux native“ angezeigt (siehe [Abbildung 2.7, „RAID-Partitionen“](#) (S. 65)). Swap- oder DOS-Partitionen werden nicht angezeigt. Wenn eine Partition einem RAID-Volume bereits zugewiesen ist, wird in der Liste der Name des RAID-Geräts (zum Beispiel `/dev/md0`) angezeigt. Nicht zugewiesene Partitionen sind mit „--“ gekennzeichnet.

Abbildung 2.7 RAID-Partitionen



Um dem ausgewählten RAID-Volume eine zuvor nicht zugewiesene Partition zuzuweisen, klicken Sie zuerst auf die Partition und anschließend auf *Hinzufügen*. Der Name des RAID-Geräts wird dann zur ausgewählten Partition hinzugefügt. Weisen Sie alle für RAID reservierten Partitionen zu. Anderenfalls bleibt der Speicherplatz in den Partitionen unbenutzt. Klicken Sie nach dem Zuweisen aller Partitionen auf *Weiter*, um das Einstellungsdialogfeld aufzurufen, in dem Sie die Leistung optimieren können (siehe [Abbildung 2.8](#), „Dateisystemeinstellungen“ (S. 66)).

Abbildung 2.8 Dateisystemeinstellungen



Legen Sie wie bei der konventionellen Partitionierung das zu verwendende Dateisystem sowie die Verschlüsselung und den Einhängepunkt für das RAID-Volume fest. Durch Aktivieren der Option *Dauerhafter Superblock* wird gewährleistet, dass die RAID-Partitionen als solche beim Booten erkannt werden. Wenn Sie die Konfiguration mit *Verlassen* abgeschlossen haben, sind im Expertenmodus des Partitionierungsmoduls das Gerät `/dev/md0` und andere Geräte mit *RAID* gekennzeichnet.

2.3.2 Fehlersuche

Prüfen Sie die Datei `/proc/mdstats`, um festzustellen, ob eine RAID-Partition beschädigt ist. Grundsätzliche Vorgehensweise bei einem Systemfehler ist es, Ihr Linux-System herunterzufahren und die defekte Festplatte durch eine neue, gleichartig partitionierte Platte zu ersetzen. Starten Sie das System anschließend neu und geben Sie den Befehl `mdadm /dev/mdX --add /dev/sdX ein`. Ersetzen Sie "X" durch die

entsprechende Geräte-ID. Damit wird die neue Festplatte automatisch in das RAID-System integriert und vollautomatisch rekonstruiert.

Beachten Sie, dass Sie zwar bei einem Neuaufbau auf alle Daten zugreifen können, jedoch einige Probleme in der Leistung auftreten können, bis RAID voll neu aufgebaut ist.

2.3.3 Weiterführende Informationen

Weitere Informationen sowie eine Anleitung zur Konfiguration von Soft-RAID finden Sie in den angegebenen HOWTO-Dokumenten unter:

- <http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html>.
- `/usr/share/doc/packages/mdadm/Software-RAID.HOWTO.html`
- <http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html>

Linux-RAID-Mailinglisten sind beispielsweise unter folgender URL verfügbar:
<http://marc.theaimsgroup.com/?l=linux-raid>.

Teil II. Verwaltung

Online-Update

openSUSE bietet fortlaufend Software-Sicherheitsupdates für Ihr Produkt. Standardmäßig wird openSUSE Updater verwendet, um Ihr System auf dem neuesten Stand zu halten. Weitere Informationen zu openSUSE Updater erhalten Sie unter Abschnitt „Halten Sie Ihr System auf dem neuesten Stand“ (Kapitel 3, *Installieren bzw. Entfernen von Software*, ↑Start). Dieses Kapitel behandelt zwei alternative Grafikwerkzeuge und Kommandozeilen-Dienstprogramme zur Aktualisierung von Softwarepaketen.

Die aktuellen Patches für openSUSE® finden Sie in einem Repository mit Aktualisierungssoftware. Wenn Sie Ihr Produkt während der Installation registriert haben, ist das Aktualisierungs-Repository bereits konfiguriert. Wenn Sie openSUSE nicht registriert haben, können Sie dies in YaST durch Ausführen von *Software > Online-Update-Konfiguration* tun. Alternativ können Sie ein Aktualisierungs-Repository manuell mithilfe jedes Aktualisierungswerkzeugs von einer verbürgten Quelle hinzufügen. Anleitungen finden Sie bei der nachfolgenden Beschreibung für die jeweilige Anwendung.

openSUSE bietet Aktualisierungen mit verschiedenen Relevanzstufen. Updates vom Typ *Sicherheit* beseitigen ernsthafte Sicherheitsgefahren und sollten auf jeden Fall installiert werden. Updates vom Typ *Empfohlen* beheben Probleme, die zu Schäden an Ihrem Computer führen können, während Updates vom Typ *Optional* Probleme ohne Sicherheitsrelevanz beheben oder Verbesserungen bieten.

3.1 Definition der Begriffe

Repository

Ein lokales oder entferntes Verzeichnis mit Paketen und zusätzlichen Informationen zu diesen Paketen (Metadaten des Pakets).

(Repository) Alias

Ein Kurzname für ein Repository, das von verschiedenen Zypper-Kommandos verwendet wird. Ein Alias kann vom Benutzer beim Hinzufügen eines Repository ausgewählt werden und muss eindeutig sein.

Produkt

Steht für ein gesamtes Produkt, wie zum Beispiel openSUSE.

Muster

Ein Schema ist eine installierbare Liste von Paketen, die für einen bestimmten Zweck benötigt werden. Beispiele: `Basissystem` mit dem openSUSE-Basissystem oder `GNOME-Basissystem` mit allen Paketen, die zur Ausführung der GNOME Desktop-Umgebung erforderlich sind.

Paket

Ein Paket ist eine komprimierte Datei im RPM-Format, die die Dateien für ein bestimmtes Programm enthält.

Patch

Ein Patch besteht aus einem oder mehreren Paketen – entweder vollständige Pakete oder `patchrpm`- bzw. `deltarpm`-Pakete; es kann auch Abhängigkeiten zu Paketen einführen, die noch nicht installiert sind.

Auflösbares Objekt

Ein generischer Begriff für Produkt, Schema, Paket oder Patch. Der am häufigsten verwendete Typ auflösbarer Objekte ist ein Paket oder ein Patch.

patchrpm

Ein `patchrpm` besteht nur aus Dateien, die seit ihrer ersten Version für openSUSE-11.0 aktualisiert wurden. Die heruntergeladene Größe ist in der Regel erheblich kleiner als die Größe eines Pakets.

deltarpm

Ein deltarpm besteht nur aus der binären diff zwischen zwei definierten Versionen eines Pakets und hat daher die kleinste Downloadgröße. Vor der Installation muss das rpm-Paket auf dem lokalen Rechner neu aufgebaut werden.

3.2 YaST-Online-Update

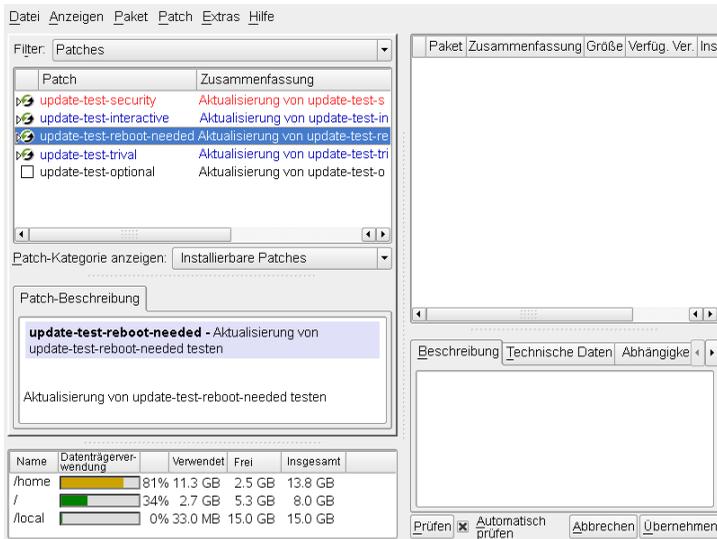
Wichtige Aktualisierungen und Verbesserungen können Sie mit YaST Online Update installieren. Die aktuellen Updates für Ihr openSUSE finden Sie in den spezifischen Aktualisierungs-Repositories, die die Patches enthalten. Zum Hinzufügen oder Entfernen von Repositories starten Sie den Repository Manager, indem Sie entweder *Repositories* > *Repository Manager* in der Menüleiste auswählen oder **Strg + M** drücken. Weitere Informationen zum Repository Manager finden Sie in Abschnitt „Hinzufügen von Software-Repositorys“ (Kapitel 3, *Installieren bzw. Entfernen von Software*, ↑Start)

Um Aktualisierungen und Verbesserungen mit YaST zu installieren, führen Sie *Software* > *Online-Update* aus. Alle neuen Patches (außer den optionalen), die derzeit für Ihr System verfügbar sind, sind bereits zur Installation markiert. Klicken Sie auf *Übernehmen*, um die Patches automatisch zu installieren. Bestätigen Sie den Abschluss der Installation mit *Beenden*. Ihr System ist nun auf dem neuesten Stand.

3.2.1 Manuelles Installieren von Patches

Das Fenster *Online-Update* ist in fünf Abschnitte unterteilt. Die Liste aller verfügbaren Patches wird links angezeigt. Unter der Liste der Patches sehen Sie die Beschreibung des ausgewählten Patches. Die Festplattenauslastung wird unten in der linken Spalte angezeigt (diese Anzeige ist standardmäßig ausgeblendet - verwenden Sie zum Einblenden den gepunkteten Schieber). Die rechte Spalte listet die Pakete auf, die im ausgewählten Patch inbegriffen sind. (Ein Patch kann mehrere Pakete umfassen.) Darunter wird eine ausführliche Beschreibung des ausgewählten Pakets angezeigt.

Abbildung 3.1 YaST-Online-Update



Die Patch-Anzeige listet die für openSUSE verfügbaren Patches auf. Die Patches werden nach Sicherheitsrelevanz sortiert. `security`, `recommended` und `optional`. Patches können in drei verschiedenen Ansichten angezeigt werden. Mit *Patch-Kategorie anzeigen* können Sie die Ansicht wechseln:

Erforderliche Patches (Standardansicht)

Zurzeit nicht installierte Patches für Pakete, die auf Ihrem System installiert sind.

Nicht erforderliche Patches

Patches, die entweder auf Pakete anzuwenden sind, die nicht auf Ihrem System installiert sind, oder Patches, deren Voraussetzungen bereits erfüllt sind.

Alle Patches

Alle für openSUSE verfügbaren Patches.

Ein Listeneintrag besteht aus einem Symbol und dem Patchnamen. Eine Liste der möglichen Symbole erhalten Sie, indem Sie Umschalttaste + F1 drücken. Die erforderlichen Aktionen für Patches der Kategorie `Sicherheit` und `Empfohlen` sind automatisch voreingestellt. Möglich sind die Aktionen *Automatisch installieren*, *Automatisch aktualisieren* oder *Automatisch löschen*. Die Aktionen für `optionale` Patches

sind nicht voreingestellt – zur Auswahl einer Aktion klicken Sie mit der rechten Maustaste auf das Patch und wählen Sie die gewünschte Aktion aus.

Wenn Sie ein aktuelles Paket aus einem anderen als dem Aktualisierungs-Repository installieren, können die Anforderungen eines Patches für dieses Paket mit dieser Installation erfüllt sein. In diesem Fall wird ein Häkchen vor der Patchzusammenfassung angezeigt. Das Patch wird in der Liste angezeigt, bis Sie es für die Installation kennzeichnen. Dadurch wird nicht das Patch installiert (da das Paket bereits aktuell ist), sondern das Patch als installiert gekennzeichnet.

Die meisten Patches umfassen Aktualisierungen für mehrere Pakete. Wenn Sie Aktionen für einzelne Pakete ändern möchten, klicken Sie mit der rechten Maustaste auf ein Paket im Paketfenster und wählen Sie eine Aktion. Sobald Sie alle Patches und Pakete wie gewünscht markiert haben, fahren Sie mit *Übernehmen* fort.

TIPP: Deaktivieren von deltarpm

Da der Neuaufbau von rpm-Paketen aus deltarpm eine Speicher- und CPU-aufwändige Aufgabe ist, können bestimmte Setups oder Hardwarekonfigurationen das Deaktivieren der deltarpm-Verwendung aus Performancegründen erfordern. Um die Verwendung von deltarpm zu deaktivieren, bearbeiten Sie die Datei `/etc/zypp/zypp.conf` und legen `download.use_deltarpm` auf `false` fest.

3.2.2 Automatische Online-Updates

YaST bietet auch die Möglichkeit, eine automatische Aktualisierung einzurichten. Öffnen Sie *Software > Automatisches Online-Update* für das Konfigurationsfenster. Sie können für eine Aktualisierung *Täglich* oder *Wöchentlich* einstellen. Einige Patches, z. B. Kernel-Updates, erfordern Benutzerinteraktion, wodurch der automatische Aktualisierungsprozess angehalten würde. Daher sollten Sie *Interaktive Patches überspringen* aktivieren, wenn der Aktualisierungsvorgang vollautomatisch erfolgen soll. In diesem Fall sollten Sie hin und wieder ein manuelles *Online-Update* ausführen, um Patches zu installieren, bei denen eine Interaktion erforderlich ist.

3.3 Aktualisierung über die Kommandozeile mit zypper

openSUSE wird mit dem Kommandozeilenwerkzeug zypper für die Installation und Aktualisierung von Paketen ausgeliefert. Damit können Sie Software per Fernzugriff oder mit Hilfe von Shell-Skripten verwalten.

3.3.1 Installieren und Entfernen von Software mit zypper

Um ein Paket aus registrierten Repositories zu installieren, verwenden Sie

```
zypper install package_name
```

Um ein installiertes Paket zu entfernen, verwenden Sie

```
zypper remove package_name
```

zypper fordert vor der Installation oder Deinstallation eines Pakets standardmäßig eine Bestätigung an. Mit der Option `--non-interactive` können Sie diese Bestätigungsabfrage deaktivieren. Die Option muss jedoch vor der tatsächlich auszuführenden Aktion (Installieren, Entfernen oder Aktualisieren) angegeben werden, wie in

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

Mit dieser Option kann zypper auch in Skripten und Cron-Aufträgen verwendet werden.

3.3.2 Aktualisieren von Software mit zypper

zypper bietet zwei Methoden der Softwareaktualisierung. Wenn Sie alle offiziell verfügbaren Patches in Ihr System integrieren möchten, führen Sie einfach das Kommando

```
zypper update
```

aus. In diesem Fall werden alle in Ihren Repositories vorhandenen Patches auf Relevanz überprüft und bei Bedarf installiert.

Wenn ein Repository neue Pakete enthält, aber keine Patches zur Verfügung stellt, zeigt `zypper update` keinerlei Wirkung. Um all diese Pakete zu aktualisieren, müssen Sie angeben, dass Aktualisierungen vom Typ `Paket` installiert werden sollen:

```
zypper update -t package
```

Um einzelne Pakete zu aktualisieren, verwenden Sie einfach das Installationskommando:

```
zypper install package_name
```

Mit dem Kommando kann eine Liste mit allen neu verfügbaren Paketen abgerufen werden.

```
zypper list-updates -t package
```

3.3.3 Verwalten von Repositories

Sämtliche Installations- und Update-Kommandos von `zypper` sind von der Liste der Repositories abhängig, die `zypper` bekannt sind. Um alle dem System bekannten Repositories aufzulisten, verwenden Sie das Kommando

```
zypper repos
```

Das Ergebnis ist der folgenden Ausgabe ähnlich.

#	Enabled	Refresh	Type	Alias	Name
1	Yes	Yes	yast2	openSUSE-DVD 11.0	openSUSE-DVD 11.0
2	Yes	No	yast2	Main (OSS)	Main (OSS)
3	Yes	No	yast2	Main (Non-OSS)	Main (Non-OSS)

Wenn ein Repository von der Liste entfernt werden soll, verwenden Sie das Kommando `zypper renamerepo` zusammen mit dem Alias des zu löschenden Repository. Zum Entfernen des Haupt-Repository (nicht-OSS) aus dem Beispiel, verwenden Sie das folgende Kommando:

```
zypper renamerepo Main Repository (Non-OSS)
```

Zum Hinzufügen eines Repository, führen Sie folgendes aus:

```
zypper addrepo URI Alias
```

`URI` kann entweder ein Internet-Repository (eine Liste der verfügbaren Repositories finden Sie unter http://en.opensuse.org/Additional_YaST_Package_Repositories), ein Verzeichnis oder eine CD/DVD sein. Der `Alias` ist ein

Kürzel und eine eindeutige Kennung für das Repository. Sie können ihn frei wählen, vorausgesetzt, er ist eindeutig. `zypper` gibt eine Warnung aus, wenn Sie einen Alias angeben, der bereits verwendet wird.

3.3.4 Verwenden der `zypper`-Shell

Eventuell möchten Sie mehrere `zypper`-Kommandos nacheinander ausführen. Um zu verhindern, dass `zypper` für jedes `zypper`-Kommando alle Datenbanken neu einliest, kann `zypper` auch im Shell-Modus: `zypper shell` ausgeführt werden.

In der Shell brauchen Sie die `zypper`-Kommandos nur mit ihren jeweiligen Parametern einzugeben:

```
zypper shell
zypper> in zsh
...
zypper> exit
```

Die Kommandosausführung in der `zypper`-Shell ist in der Regel schneller, da alle relevanten Daten im Arbeitsspeicher verbleiben.

`zypper` unterstützt die `readline`-Bibliothek. Sie können daher in der `zypper`-Shell sämtliche Kommandozeilenfunktionen verwenden, die auch in der `Bash`-Shell zur Verfügung stehen. `zypper` führt seine Kommando-History in der Datei `~/.zypper_history`.

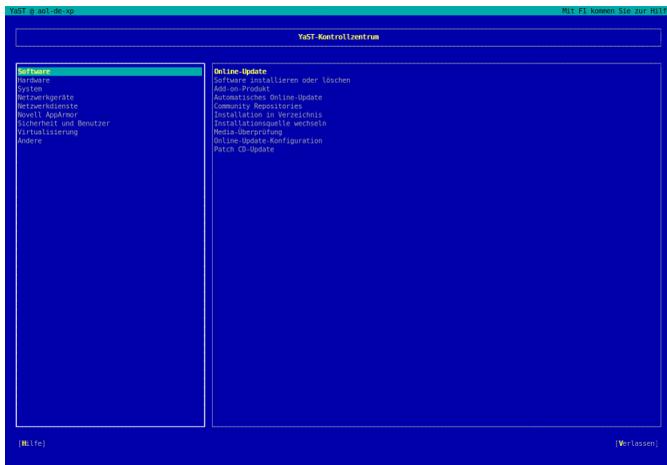
3.3.5 Weiterführende Informationen

Weitere Informationen zur Aktualisierung über die Kommandozeile erhalten Sie, wenn Sie `zypper --help` eingeben oder die man-Seite `zypper(8)` aufrufen. Beispiele und ausführliche Informationen finden Sie unter <http://en.opensuse.org/Zypper/Usage>.

YaST im Textmodus

Dieser Abschnitt richtet sich an Systemadministratoren und Experten, die keinen X-Server auf Ihren Systemen ausführen und daher auf das textbasierte Installationswerkzeug angewiesen sind. Der Abschnitt enthält grundlegende Informationen zum Start und Betrieb von YaST im Textmodus.

Abbildung 4.1 *Hauptfenster von YaST im Textmodus*



Beim Start von YaST im Textmodus wird zuerst das YaST-Kontrollzentrum angezeigt. Weitere Informationen hierzu finden Sie unter [Abbildung 4.1](#). Das Hauptfenster besteht aus drei Bereichen. Der linke Bereich, der von einem dicken weißen Rahmen umgeben ist, enthält die Kategorien, zu denen die verschiedenen Module gehören. Die aktive Kategorie wird durch einen farbigen Hintergrund angezeigt. Im rechten Bereich, der

von einem dünnen weißen Rahmen umgeben ist, finden Sie eine Übersicht über die in der aktiven Kategorie verfügbaren Module. Der untere Bereich enthält die Schaltflächen für *Hilfe* und *Verlassen*.

Beim Starten des YaST-Kontrollzentrums wird die Kategorie *Software* automatisch ausgewählt. Mit ↓ und ↑ können Sie die Kategorie ändern. Um ein Modul aus der ausgewählten Kategorie zu starten, drücken Sie → Die Modulauswahl ist nun mit einem dicken Rahmen umgeben. Mit ↓ und ↑ können Sie das gewünschte Modul auswählen. Halten Sie die Pfeiltasten gedrückt, um durch die Liste der verfügbaren Module zu blättern. Wenn ein Modul ausgewählt wird, erscheint der Modultitel auf farbigem Hintergrund.

Drücken Sie die Eingabetaste, um das gewünschte Modul zu starten. Mehrere Schaltflächen bzw. Auswahlfelder im Modul enthalten einen Buchstaben in einer anderen Farbe (standardmäßig gelb). Mit Alt + gelber_Buchstabe können Sie eine Schaltfläche direkt auswählen und müssen nicht mit Tabulator zu der Schaltfläche wechseln. Verlassen Sie das YaST-Kontrollzentrum durch Drücken von Alt + Q oder durch Auswählen von *Verlassen* und Drücken von Eingabetaste.

4.1 Navigation in Modulen

Bei der folgenden Beschreibung der Steuerelemente in den YaST-Modulen wird davon ausgegangen, dass alle Kombinationen aus Funktionstasten und Alt -Taste funktionieren und nicht anderen globalen Funktionen zugewiesen sind. In [Abschnitt 4.2, „Einschränkung der Tastenkombinationen“](#) (S. 82) finden Sie Informationen zu möglichen Ausnahmen.

Navigation zwischen Schaltflächen und Auswahllisten

Verwenden Sie Tab, um zwischen den Schaltflächen und Einzelbildern mit den Auswahllisten zu navigieren. Zum Navigieren in umgekehrter Reihenfolge verwenden Sie die Tastenkombinationen Alt + Tab oder Shift + Tab.

Navigation in Auswahllisten

Mit den Pfeiltasten (↑ and ↓) können Sie zwischen den einzelnen Elementen in einem aktiven Rahmen, der eine Auswahlliste enthält, navigieren. Wenn einzelne Einträge innerhalb eines Rahmens dessen Breite überschreiten, können Sie mit Umschalt + → oder Umschalt + ← horizontal nach links und rechts blättern. Alternativ können Sie Strg + E oder Strg + A verwenden. Diese Kombination kann auch verwendet werden, wenn → oder ← zu einem Wechsel des aktiven Rahmens

oder der aktuellen Auswahlliste führen würde, wie dies im Kontrollzentrum der Fall ist.

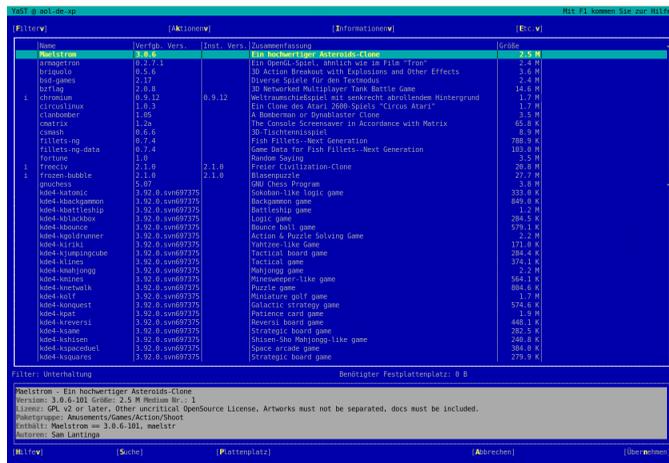
Schaltflächen, Optionsschaltfläche und Kontrollkästchen

Um Schaltflächen mit leeren eckigen Klammern (Kontrollkästchen) oder leeren runden Klammern (Optionsschaltflächen) auszuwählen, drücken Sie die Leertaste oder die Eingabetaste. Alternativ können Optionsschaltflächen und Kontrollkästchen unmittelbar mit Alt + gelber_Buchstabe ausgewählt werden. In diesem Fall brauchen Sie die Auswahl nicht mit der Eingabetaste zu bestätigen. Wenn Sie mit Tabulator zu einem Element wechseln, können Sie durch Drücken der Eingabetaste die ausgewählte Aktion ausführen bzw. das betreffende Menüelement aktivieren.

Funktionstasten

Die F-Tasten (F1 bis F12) bieten schnellen Zugriff auf die verschiedenen Schaltflächen. Verfügbare F-Tastenkürzel werden in der untersten Zeile des YaST-Bildschirms angezeigt. Welche Funktionstasten welchen Schaltflächen zugeordnet sind, hängt vom aktiven YaST-Modul ab, da die verschiedenen Module unterschiedliche Schaltflächen aufweisen ("Details", "Info", "Hinzufügen", "Löschen" usw.). F10 wird für *ÜbernehmenOK*, *Weiter* und *Beenden* verwendet. Drücken Sie F1, um Zugriff auf die YaST-Hilfe zu erhalten.

Abbildung 4.2 Das Software-Installationsmodul



4.2 Einschränkung der Tastenkombinationen

Wenn der Fenster-Manager globale Alt-Kombinationen verwendet, funktionieren die Alt-Kombinationen in YaST möglicherweise nicht. Tasten wie Alt oder Umschalt können auch durch die Einstellungen des Terminals belegt sein.

Ersetzen von Alt durch Esc

Tastenkombinationen mit Alt können auch mit Esc, anstatt mit Alt, ausgeführt werden. Esc – H beispielsweise ersetzt Alt + H. (Drücken Sie zunächst Esc, *und drücken Sie dann* H.)

Navigation vor und zurück mit Strg + Fund Strg + B

Wenn die Kombinationen mit Alt und Umschalt vom Fenster-Manager oder dem Terminal belegt sind, verwenden Sie stattdessen die Kombinationen Strg + F (vor) und Strg + B (zurück).

Einschränkung der Funktionstasten

Die F-Tasten werden auch für Funktionen verwendet. Bestimmte Funktionstasten können vom Terminal belegt sein und stehen eventuell für YaST nicht zur Verfügung. Auf einer reinen Textkonsole sollten die Tastenkombinationen mit Alt und die Funktionstasten jedoch stets vollständig zur Verfügung stehen.

4.3 YaST-Kommandozeilenoptionen

Neben der Schnittstelle im Textmodus bietet YaST auch eine reine Kommandozeilenschnittstelle. Eine Liste der YaST-Kommandozeilenoptionen erhalten Sie, wenn Sie Folgendes eingeben:

```
yast -h
```

4.3.1 Starten der einzelnen Module

Um Zeit zu sparen, können die einzelnen YaST-Module direkt gestartet werden. Um ein Modul zu starten, geben Sie Folgendes ein:

```
yast <module_name>
```

Eine Liste aller auf Ihrem System verfügbaren Modulnamen können Sie mit `yast -l` oder `yast --list` anzeigen. Das Netzwerkmodul beispielsweise wird mit `yast lan` gestartet.

4.3.2 Installation von Paketen über die Kommandozeile

Wenn Sie den Namen eines Pakets kennen und das Paket von einer Ihrer aktiven Installations-Repositories bereitgestellt wird, können Sie das Paket mithilfe der Kommandozeilenoption `-i` installieren.

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

oder

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

package_name kann ein einzelner kurzer Paketname sein, beispielsweise `gvim` (solche Pakete werden mit Abhängigkeitsüberprüfung installiert), oder der vollständige Pfad zu einem RPM-Paket, das ohne Abhängigkeitsüberprüfung installiert wird.

Wenn Sie ein kommandozeilenbasiertes Softwareverwaltungs-Dienstprogramm mit Funktionen benötigen, die über die von YaST hinausgehen, sollten Sie möglicherweise `zypper` verwenden. Dieses neue Dienstprogramm verwendet die Softwareverwaltungsbibliothek, die auch die Grundlage des YaST-Paket-Managers bildet. Die grundlegende Verwendung von `zypper` wird unter [Abschnitt 3.3, „Aktualisierung über die Kommandozeile mit zypper“](#) (S. 76) erläutert.

4.3.3 Kommandozeilenparameter der YaST-Module

Um die Verwendung von YaST-Funktionen in Skripten zu ermöglichen, bietet YaST Kommandozeilenunterstützung für einzelne Module. Die Kommandozeilenunterstützung steht jedoch nicht für alle Module zur Verfügung. Um die verfügbaren Optionen eines Moduls anzuzeigen, geben Sie Folgendes ein:

```
yast <module_name> help
```

Wenn ein Modul keine Kommandozeilenunterstützung bietet, wird es im Textmodus gestartet und es wird folgende Meldung angezeigt.

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

Aktualisieren des Systems und Systemänderungen

5

Sie können ein bestehendes System aktualisieren, ohne es vollständig neu zu installieren. Es gibt zwei Arten von Updates: die *Updates für einzelne Software-Pakete* und die *Update für das gesamte System*.

5.1 Aktualisieren des Systems

Software weist normalerweise von Version zu Version mehr „Umfang“ auf. Folglich sollten Sie vor dem Aktualisieren mit `df` den verfügbaren Partitionsspeicher überprüfen. Wenn Sie befürchten, dass demnächst kein Speicherplatz mehr zur Verfügung steht, sichern Sie die Daten, bevor Sie Ihr System aktualisieren und neu partitionieren. Es gibt keine Faustregel hinsichtlich des Speicherplatzes einzelner Partitionen. Die Speicherplatzanforderungen werden durch Ihr jeweiliges Partitionierungsprofil, die ausgewählte Software sowie die Versionsnummer des Systems bestimmt.

5.1.1 Vorbereitung

Kopieren Sie vor der Aktualisierung die alten Konfigurationsdateien auf ein separates Medium, beispielsweise ein Bandlaufwerk, eine Wechselfestplatte oder einen USB-Stick, um die Daten zu sichern. Dies gilt hauptsächlich für die in `/etc` gespeicherten Dateien sowie einige der Verzeichnisse und Dateien in `/var`. Zudem empfiehlt es sich, die Benutzerdaten in `/home` (den `HOME`-Verzeichnissen) auf ein Sicherungsmedium zu schreiben. Melden Sie sich zur Sicherung dieser Daten als `root` an. Nur Benutzer `root` verfügt über die Leseberechtigung für alle lokalen Dateien.

Notieren Sie sich vor der Aktualisierung die Root-Partition. Mit dem Befehl `df /` können Sie den Gerätenamen der Root-Partition anzeigen. In **Beispiel 5.1**, „Über `df -h` angezeigte Liste“ (S. 86) ist `/dev/sda3` die Root-Partition, die Sie sich notieren sollten (eingehängt als `/`).

Beispiel 5.1 Über `df -h` angezeigte Liste

Filesystem	Size	Used	Avail	Use%	Mounted on
<code>/dev/sda3</code>	74G	22G	53G	29%	<code>/</code>
<code>udev</code>	252M	124K	252M	1%	<code>/dev</code>
<code>/dev/sda5</code>	116G	5.8G	111G	5%	<code>/home</code>
<code>/dev/sda1</code>	39G	1.6G	37G	4%	<code>/windows/C</code>
<code>/dev/sda2</code>	4.6G	2.6G	2.1G	57%	<code>/windows/D</code>

5.1.2 Potenzielle Probleme

Wenn Sie ein standardmäßiges System von der Vorgängerversion auf diese Version aktualisieren, ermittelt YaST die erforderlichen Änderungen und nimmt sie vor. Abhängig von den individuellen Anpassungen, die Sie vorgenommen haben, kommt es bei einigen Schritten der vollständigen Aktualisierung zu Problemen und Ihnen bleibt nur die Möglichkeit, Ihre Sicherungsdaten zurückzukopieren. Nachfolgend sind weitere Punkte aufgeführt, die vor dem Beginn der Systemaktualisierung überprüft werden müssen.

Überprüfen von "passwd" und "group" in "/etc"

Stellen Sie vor dem Aktualisieren des Systems sicher, dass `/etc/passwd` und `/etc/group` keine Syntaxfehler enthalten. Rufen Sie hierzu die Überprüfungs-Dienstprogramme `pwck` und `grpck` als `root` auf und beseitigen Sie sämtliche gemeldeten Fehler.

PostgreSQL

Führen Sie vor der Aktualisierung von PostgreSQL (`postgres`) den `dump`-Vorgang für die Datenbanken durch. Ziehen Sie die Manualpage zu `pg_dump` zurate. Dies ist nur erforderlich, wenn Sie PostgreSQL bereits vor der Aktualisierung verwendet haben.

5.1.3 Aktualisieren mit YaST

Im Anschluss an die in [Abschnitt 5.1.1, „Vorbereitung“](#) (S. 85) erläuterte Vorbereitung kann Ihr System nun aktualisiert werden:

- 1 Booten Sie das System wie zu Installationszwecken (siehe Beschreibung in Abschnitt „Systemstart für die Installation“ (Kapitel 1, *Installation mit YaST*, ↑Start)). Wählen Sie in YaST eine Sprache aus und klicken Sie im Dialogfeld *Installationsmodus* auf *Aktualisieren*. Wählen Sie nicht die Option *Neuinstallation*. Fügen Sie außerdem Repositorys hinzu, um sicherzustellen, dass die gesamte verfügbare Software aktualisiert wird, sobald Updates zur Verfügung stehen. Informationen zur Installation von Repositorys finden Sie unter Abschnitt „Add-On-Produkte“ (Kapitel 1, *Installation mit YaST*, ↑Start).
- 2 YaST ermittelt, ob mehrere Stammpartitionen vorhanden sind. Wenn nur eine vorhanden ist, fahren Sie mit dem nächsten Schritt fort. Wenn mehrere vorhanden sind, wählen Sie die richtige Partition aus und bestätigen Sie mit *Weiter* (im Beispiel in [Abschnitt 5.1.1, „Vorbereitung“](#) (S. 85) wurde `/dev/sda3` ausgewählt). YaST liest die alte `fstab` auf dieser Partition, um die hier aufgeführten Dateisysteme zu analysieren und einzuhängen.
- 3 Überprüfen Sie die früheren Repositorys, sofern welche eingerichtet waren. Aktivieren Sie alle Repositorys, die Sie noch zur Aktualisierung der Software von Drittanbietern verwenden möchten. Klicken Sie für jedes Element der Liste, dessen Status Sie wechseln möchten, auf *Status wechseln*.
- 4 Falls Sie während der Aktualisierung, wie oben empfohlen, Repositorys hinzugefügt haben, können Sie nun diejenigen aktivieren, an denen Sie tatsächlich Interesse haben.
- 5 Passen Sie im Dialogfeld *Installationseinstellungen* die Einstellungen gemäß Ihren Anforderungen an. Normalerweise können die Standardeinstellungen unverändert übernommen werden, wenn Sie Ihr System jedoch erweitern möchten, überprüfen Sie die in den Untermenüs von *Software-Auswahl* aufgeführten Pakete (und aktivieren Sie sie gegebenenfalls) oder fügen Sie die Unterstützung für zusätzliche Sprachen hinzu.

Sie haben zudem die Möglichkeit, verschiedene Systemkomponenten zu sichern. Durch Sicherungen wird der Aktualisierungsvorgang verlangsamt. Verwenden Sie diese Option, wenn Sie über keine aktuelle Systemsicherung verfügen.

6 Klicken Sie zur Bestätigung auf *Update starten*.

Führen Sie nach der grundlegenden Installation des Updates den von YaST angebotenen Test der Internetverbindung aus. Nach der Aktualisierung der verbleibenden Software bietet YaST die Konfiguration für das Novell Customer Center an und blendet die Versionshinweise ein. Klicken Sie auf *Fertig stellen*, um die YaST-Konfiguration zu speichern.

5.1.4 Aktualisieren einzelner Pakete

Ungeachtet der insgesamt aktualisierten Umgebung ist die Aktualisierung einzelner Pakete stets möglich. Ab diesem Punkt liegt es jedoch bei Ihnen, sicherzustellen, dass die Konsistenz Ihres Systems stets gewährleistet ist. Ratschläge zur Aktualisierung finden Sie unter <http://www.novell.com/linux/download/updates/>.

Wählen Sie gemäß Ihren Anforderungen Komponenten in der YaST-Paketauswahl aus. Wenn Sie ein Paket auswählen, das für den Gesamtbetrieb des Systems unerlässlich ist, gibt YaST eine Warnung aus. Pakete dieser Art sollten nur im Aktualisierungsmodus aktualisiert werden. Zahlreiche Pakete enthalten beispielsweise *freigegebene Bibliotheken*. Wenn diese Programme und Anwendungen im aktiven System aktualisiert werden, kann es zu Fehlfunktionen kommen.

5.2 Software-Änderungen von Version zu Version

Welche Aspekte sich zwischen den Versionen genau geändert haben, geht aus den nachfolgenden Erläuterungen hervor. Diese Zusammenfassung gibt beispielsweise Aufschluss darüber, ob grundlegende Einstellungen vollkommen neu konfiguriert wurden, ob Konfigurationsdateien an andere Speicherorte verschoben wurden oder ob es bedeutende Änderungen gängiger Anwendungen gegeben hat. Signifikante Änderungen, die sich auf den täglichen Betrieb des Systems auswirken – entweder auf Benutzer- oder Administratorebene – werden hier genannt.

Probleme und spezielle Aspekte der jeweiligen Version werden bei Bekanntwerdung online zur Verfügung gestellt. Nutzen Sie die unten aufgeführten Links. Wichtige Aktualisierungen einzelner Pakete stehen mit YaST Online Update unter <http://>

www.novell.com/products/linuxprofessional/downloads/ zur Verfügung. Weitere Informationen finden Sie unter **Kapitel 3, *Online-Update*** (S. 71).

5.2.1 Von 10.0 auf 10.1

Ziehen Sie den Artikel „Bekannte Probleme und Besonderheiten in SUSE Linux 10“ in der SUSE-Support-Datenbank unter <http://www.novell.com/suselinuxportal> zu Rate (Schlüsselwort: *Besonderheiten*).

Apache 2.2

Für Apache Version 2.2 wurde **Kapitel 22, *Der HTTP-Server Apache*** (S. 403) komplett überarbeitet. Allgemeine Informationen zur Aktualisierung erhalten Sie unter <http://httpd.apache.org/docs/2.2/upgrading.html> und unter http://httpd.apache.org/docs/2.2/new_features_2_2.html finden Sie eine Beschreibung der neuen Funktionen.

Starten von FTP-Servern (vsftpd)

Der vsftpd-FTP-Server wird standardmäßig nicht mehr über xinetd gestartet. Er ist jetzt ein eigenständiger Daemon, der mit dem runtime-Editor von YaST konfiguriert werden muss.

Firefox 1.5: Befehl zum Öffnen von URLs

In Firefox 1.5 wurde die Methode geändert, mit der Anwendungen eine Firefox-Instanz oder ein Firefox-Fenster öffnen. Die neue Methode stand teilweise bereits in älteren Versionen zur Verfügung, in denen das Verhalten im Packer-Skript implementiert war.

Wenn in Ihrer Anwendung weder `mozilla-xremote-client` noch `firefox-remote` verwendet wird, müssen Sie keine Änderungen vornehmen. Andernfalls lautet der neue Befehl zum Öffnen von URLs `firefox url`. Dabei spielt es keine Rolle, ob Firefox bereits ausgeführt wird oder nicht. Wenn Firefox bereits ausgeführt wird, wird die Einstellung unter *Open links from other applications in* (Links aus anderen Anwendungen öffnen in) verwendet.

Über die Kommandozeile können Sie das Verhalten mit den Befehlen `firefox-new-window url` oder `firefox-new-tab url` beeinflussen.

Firefox mit Pango-Unterstützung

Auf einigen Computern ist Firefox mit aktivierter Pango-Unterstützung sehr langsam. Die Leistung scheint vom X-Server abzuhängen. Setzen Sie `MOZ_DISABLE_PANGO=0`, wenn Sie ohnehin für Ihre Umgebung das Rendering von Schriften aktivieren möchten:

```
export MOZ_DISABLE_PANGO=0
firefox
```

Aktualisieren auf MySQL 5.0

Wie bei jeder größeren Release-Aktualisierung wird dringend die vorherige Sicherung der MySQL-Tabellendateien sowie das Erstellen eines SQL-Speicherauszugs empfohlen. Nach der Aktualisierung führt `/etc/init.d/mysql` automatisch `mysql_fix_privilege_tables` aus. Weitere Informationen hierzu sowie detaillierte Anleitungen finden Sie unter <http://dev.mysql.com/doc/refman/5.0/en/upgrade.html>.

Lokaler und E/A-APIC

Der lokale und E/A-APIC für die 32-Bit-x86-Architektur hat sich geändert. Ein lokaler und E/A-APIC (Advanced Programmable Interrupt Controller) ist ein SMP-fähiger Ersatz für Interrupt-Controller im Stil von PCs. SMP-Systeme und alle neueren Einprozessorsysteme besitzen einen solchen Controller.

Bisher war der lokale und E/A-APIC auf Einprozessorsystemen standardmäßig deaktiviert und musste manuell mit dem Kernel-Parameter "apic" aktiviert werden. Nun läuft er standardmäßig und kann manuell deaktiviert werden. Für 64-Bit-Systeme ist APIC immer standardmäßig aktiviert.

- Für jedes System mit einer BIOS-Version nach 2001 ist der lokale und E/A-APIC standardmäßig aktiviert, es sei denn, dass lokaler und E/A-APIC im BIOS oder durch den Benutzer deaktiviert wurde.
- Für jedes BIOS von Intel nach 1998 ist der lokale und E/A-APIC standardmäßig aktiviert.

- Für jedes System mit mehreren CPUs wird der lokale und E/A-APIC standardmäßig aktiviert.

Wenn Probleme mit nicht korrekt arbeitenden Geräten auftreten, können Sie die folgenden Konfigurationsoptionen manuell anwenden:

- Verwenden Sie zum Deaktivieren des lokalen APIC `nolapic` (impliziert das Deaktivieren von E/A-APICs).
- Verwenden Sie zum Deaktivieren von E/A-APIC `noapic`.
- Verwenden Sie `nolapic`, um denselben Standard wie in früheren Versionen zu erhalten.

ulimit-Einstellungen

Die `ulimit`-Einstellungen können in `/etc/sysconfig/ulimit` konfiguriert werden. Standardmäßig werden nur zwei Grenzwerte von den Kernel-Standards geändert:

- `SOFTVIRTUALLIMIT=80` begrenzt einen einzelnen Prozess so, dass er nicht mehr als 80 % des verfügbaren virtuellen Speichers (RAM und Swap) belegen kann.
- `SOFTRESIDENTLIMIT=85` begrenzt einen einzelnen Prozess so, dass er nicht mehr als 85 % des verfügbaren physischen Speichers (RAM) belegen kann.

Diese Soft-Grenzwerte kann der Benutzer mit dem Befehl "`ulimit`" überschreiben. Festgrenzwerte können nur von "`root`" überschrieben werden.

Die Werte wurden konservativ gewählt, um die Störung von umfangreichen Prozessen zu verhindern, die in der Vergangenheit funktioniert haben. Wenn keine ausgewiesenen Prozesse mit hohem Speicherbedarf vorhanden sind, setzen Sie die Grenzwerte niedriger, um wirksameren Schutz vor unkontrollierbaren Prozessen zu haben. Die Grenzwerte gelten pro Prozess und sind daher kein wirksamer Schutz vor bösartigen Benutzern. Die Grenzwerte sollen vor versehentlicher exzessiver Speicherbelastung schützen.

Verwenden Sie für benutzerbezogene Grenzwerte die Funktion `pam_limits` und konfigurieren Sie `/etc/security/limits.conf`. Dafür ist das `ulimit`-Paket nicht erforderlich, aber beide Mechanismen können parallel benutzt werden. Die in `limits`

`.conf` konfigurierten Grenzwerte überschreiben die globalen Standards aus dem `ulimit`-Paket.

Enriegeln von CD- und DVD-Laufwerken und Auswerfen der Medien

Ein neuer Einhängemechanismus ersetzt das früher verwendete `submount`-System. Dieser neue Mechanismus hängt Medien nicht automatisch aus, sondern auf Hardwareanforderung. Einige Geräte, vor allem ältere CD-Laufwerke, aber auch einige neue Laufwerke mit beschädigter Firmware, senden dieses Signal nicht. Um die Medien an solchen Geräten auszuwerfen, wählen Sie "Auswerfen" aus dem Kontextmenü des Geräts in "Arbeitsplatz" (geöffnet durch Klicken der rechten Maustaste) oder "Auswerfen" aus dem Kontextmenü des Gerätesymbols auf dem Desktop.

5.2.2 Von 10.1 auf 10.2

Lesen Sie hierzu den Artikel „Bugs“ in der openSUSE-Wiki unter <http://en.opensuse.org/Bugs>.

Der Standard-Kernel

Das Paket `kernel-default` enthält den Standard-Kernel für Einprozessor- und Multiprozessorsysteme. Der Kernel wird mit SMP-Unterstützung geliefert und läuft mit minimalem Overhead auf Multiprozessorsystemen. Das Paket `kernel-smp` gibt es nicht mehr.

Add-On-Medium mit zusätzlichen Sprachen

Nehmen Sie das Add-On-Medium für Sprachen in die Liste Ihrer Installationsquellen auf, wenn Sie für eine unserer Sprachen der Stufe 2 bessere Unterstützung wünschen. Sprachen der Stufe 2 sind alle Sprachen außer den Sprachen der Stufe 1 (Englisch, Französisch, Deutsch, Italienisch, Spanisch, Brasilianisch Portugiesisch, vereinfachtes und traditionelles Chinesisch, Japanisch und Tschechisch). Unterstützung für Sprachen der Stufe 1 befindet sich auf dem Standard-Mediensatz.

5.2.3 Von 10.2 auf 10.3

Lesen Sie hierzu den Artikel „Bugs“ in der openSUSE-Wiki unter <http://en.opensuse.org/Bugs>.

Text-Installationsschema

Der Umfang des Text-Installationsschemas ist sehr begrenzt. Es ist nicht empfehlenswert, dieses Schema ohne zusätzliche Software zu installieren. Fügen Sie Pakete aus anderen Schemata hinzu. Dieses Schema hat zum Zweck, ein minimal bootfähiges System auf einer realen Hardware auszuführen. Es stellt ein Mehrbenutzersystem mit lokaler Anmeldung, Netzwerkeinrichtung und Standard-Dateisystemen zur Verfügung. Standardmäßig wird kein Dienst aktiviert und die einzigen YaST-Module, die installiert werden, sind die Module, die bei der Installation erforderlich sind.

Hinzufügen zusätzlicher Software-Repositories bei der Installation

Nach Einrichten der Aktualisierungskonfiguration am Ende der Installation bietet YaST an, die folgenden drei Software-Repositories als zusätzliche Installationsquellen hinzuzufügen:

- Das „oss“-Repository enthält die vollständige FTP-Distribution einschließlich anderer Pakete, die nicht auf den CDs verfügbar sind.
- Das „non-oss“-Repository enthält Software unter einer proprietären oder Nicht-Open-Source-Lizenz.
- Das „debug“-Repository enthält Pakete mit Informationen zur Fehlersuche, die zur Fehlersuche bei Programmen und Bibliotheken und zum Abrufen von Rückverfolgungsdaten verwendet werden. Bei Auftreten eines Fehlers können Sie mit diesen zusätzlichen Informationen einen guten Fehlerbericht schreiben.

Die Quell-RPMs für „oss“ sind unter <http://download.opensuse.org/distribution/10.3/src-oss> verfügbar, die Quell-RPMs für „non-oss“ unter <http://download.opensuse.org/distribution/10.3/src-non-oss>.

Lokalisierungsunterstützung

Die Installationsmedien auf einer CD (GNOME oder KDE) bieten nur Sprachunterstützung für US-Englisch.

Unterstützung für alle anderen Sprachen steht separat zur Verfügung. Wenn Sie an weiteren Sprachen interessiert sind, fügen Sie bei der Installation ein zusätzliches Online-Repository hinzu, das diese Übersetzungen bietet. Das „oss“-Repository, das oben im Abschnitt "Hinzufügen zusätzlicher Software-Repositories bei der Installation" genannt wird, ist ein solches Repository.

GTK- und QT-Frontends für YaST Software-Management

Standardmäßig wird das neue YaST-GTK-Frontend auf dem GNOME-Desktop ausgeführt, das YaST-Qt-Frontend dagegen auf allen anderen Desktops. Das GTK-Frontend ist, was die Funktionen betrifft, dem in den Handbüchern beschriebenen Qt-Frontend sehr ähnlich.

Eine Ausnahme stellt das GTK-Softwareverwaltungsmodul dar (siehe die Inbetriebnahmeanleitungen in Kapitel 3), das sich erheblich vom Qt-Port unterscheidet. Gehen Sie wie folgt vor, um die Qt-Version auf dem GNOME-Desktop zu starten:

- Öffnen Sie die Datei `/etc/sysconfig/yast2` als Root.
- Ändern Sie `WANTED_GUI="auto"` zu `WANTED_GUI="qt"` und speichern und beenden Sie die Datei.
- Um die GTK-Version von YaST auf jedem beliebigen Desktop zu starten, gehen Sie genauso vor, ändern Sie jedoch `WANTED_GUI="auto"` zu `WANTED_GUI="gtk"`.

AppArmor 2.1

Weitere detaillierte Informationen über neue Funktionen finden Sie unter http://en.opensuse.org/AppArmor/Changes_AppArmor_2_1.

Die Syntax unterscheidet nun Verzeichnisse und Dateien. Es gibt einige zusätzliche geringfügige Syntax-Bug-Fixes.

Die Berichterstellung für Ereignisse und Informationen in Bezug auf `change_hat` wurde geändert. Die Protokollmeldungen und der Profilstatus (verfügbar unter `/proc/<pid>/attr/current`) werden als `/profile//hat` gemeldet.

Eine neue Richtlinienpezifikation `change_profile` wurde hinzugefügt. `Change_profile` ähnelt `change_hat`, ermöglicht jedoch den Wechsel zu beliebigen Profilen (einschließlich Hats), nicht nur zu Hats. Die Einschränkung besteht darin, dass die Profile, zu denen gewechselt wird, angegeben werden müssen. Um über `change_profile` anstatt über `change_hat` zu einem Hat zu wechseln, wird der Hat-Name angegeben, indem das Profil und der `hat_name` durch `//` getrennt werden.

GAIM umbenannt zu Pidgin

Der Instant Messenger "GAIM" wurde umbenannt zu "Pidgin".

Neuer Speicherort für KDE und GNOME.

GNOME 2 wird seit openSUSE 10.3 unter der Dateisystemhierarchie `/usr` installiert; KDE 4 folgt nach. KDE 3 bleibt aus Gründen der Kompatibilität in `/opt`.

Bevor Sie mit der Aktualisierung beginnen, vergewissern Sie sich, dass unter `/usr` genügend Speicherplatz (ca. 2,5GB für beide Desktops) vorhanden ist. Wenn der Speicherplatz unter `/usr` nicht ausreicht, ändern Sie die Größe der Partitionen oder ordnen Sie sie neu an.

Berkeley DB-Änderung beeinträchtigt OpenLDAP Server

Bei den Berkeley DBs wurde das Format der Protokolldateien auf Festplatte zwischen Berkeley DB 4.3 und 4.4 geändert. Diese Änderung verhindert, dass ein installierter OpenLDAP-Server nach der Systemaktualisierung gestartet wird.

Um dieses Problem zu vermeiden, exportieren Sie die vorhandenen LDAP-Datenbanken mithilfe des `slapcat`-Dienstprogramms, *bevor* Sie mit der Systemaktualisierung beginnen. Importieren Sie diese Daten wieder nach der Aktualisierung mithilfe von `slapadd`. Starten Sie den LDAP-Server auf einem bereits aktualisierten Computer wie folgt:

1. Stoppen Sie den LDAP-Server.
2. Entfernen Sie alle Dateien, die mit `_db.` beginnen, aus dem Datenbankverzeichnis.
3. Starten Sie den LDAP-Server erneut.

libata für IDE-Geräte

libata verwendet `/dev/sda` für die erste Festplatte anstelle von `/dev/hda`. Festplatten mit mehr als 15 Partitionen werden derzeit nicht automatisch verarbeitet. Sie können die Unterstützung für libata deaktivieren, indem Sie das System mit den folgenden Kernel-Parametern starten:

```
hwprobe=-modules.pata
```

Daraufhin erscheinen wieder alle Partitionen > 15 und Sie können auf diese zur Installation zugreifen.

Änderungen bei der Einrichtung verschlüsselter Partitionen

Die Backend-Technologie von `boot.crypt` wurde geändert von `cryptoloop` zu `dm-crypt`.

Alte `/etc/cryptotab` funktionieren unverändert auf openSUSE 10.3 (Probleme bei Modulo `hdX->sdX` aufgrund von libata-Änderungen - siehe oben). Außerdem wird `/etc/crypttab` (beachten Sie das weggelassene 'o') nun unterstützt, was auch die Unterstützung für LUKS-Volumes einschließt. Im Gegensatz zu früheren Versionen wird `boot.crypt` nicht länger standardmäßig aktiviert. YaST aktiviert es, wenn Sie ein verschlüsseltes Volume mit YaST erstellen. Sie können es auch mit dem folgenden Kommando manuell aktivieren:

```
chkconfig boot.crypt on
```

Es ist immer noch möglich, `cryptoloop` über `losetup` und `mount` zu verwenden. Da wir den nicht ausgereiften `loop-AES-Patch` vom `util-linux`-Paket entfernt haben, sind einige Parameter für `losetup` (wie zum Beispiel `itercountk` und `pseed`) nicht mehr verfügbar. Wenn einige dieser Einstellungen in `/etc/fstab` verwendet werden, kann das Gerät nicht mehr direkt eingehängt werden. Migrieren Sie diese Einstellungen

nach `/etc/crypttab`, wo `boot.crypto` den erforderlichen Kompatibilitätscode enthält.

Aktivieren der Quota-Unterstützung

Quota für Benutzerkonten können nun in YaST konfiguriert werden. Zum Aktivieren der Quota-Unterstützung aktivieren Sie in den `fstab`-Optionen das Kontrollkästchen neben „Quota-Unterstützung aktivieren“, wenn Sie eine Partitionierung in der ersten Installationsstufe durchführen. Stellen Sie damit sicher, dass das Skript `/etc/init.d/boot.quota` beim Starten ausgeführt wird. In der zweiten Stufe befindet sich das Quota-Modul dann in den erweiterten Optionen für Benutzerkonten, in dem Sie Quota-Regeln festlegen können.

Wenn Sie die Quota-Unterstützung im Partitionierer bei laufendem Betrieb des Systems nach der Installation aktivieren, starten Sie das System entweder neu oder hängen Sie die entsprechenden Partitionen manuell erneut ein und führen Sie das folgende Kommando als `root` aus:

```
/etc/init.d/boot.quota restart
```

Zeroconf

Zeroconf-Service (auch Bonjour, Multicast DNS, mDNS oder DNS-SD genannt) wird nun durch den Avahi-Stack statt durch mDNSResponder zur Verfügung gestellt. Der mDNSResponder und die Howl-Kompatibilitätsbibliotheken sind immer noch verfügbar.

Zur Aktivierung von mDNS für alle Netzwerkschnittstellen verwenden Sie die SuSE-firewall Regel „Zeroconf/Bonjour Multicast DNS“.

Ältere Intel Grafik-Chips

Ältere Intel Grafik-Chips werden von zwei Treibern unterstützt („i810“ und „intel“). Bei openSUSE 10.3 ist der Intel-Treiber aufgrund der hohen Anforderungen für Funktionen wie die Einstellung des Native-Modus (nicht mehr VESA BIOS-basiert) und die Unterstützung von RANDR 1.2 als Standard festgelegt.

Bei der Aktualisierung zu openSUSE 10.3 wird der i810-Treiber nicht durch den Intel-Treiber ausgetauscht. Verwenden Sie `sax2 -r`, um zum Intel-Treiber zu wechseln.

Der Intel-Treiber läuft noch nicht so stabil wie der i810; verwenden Sie "`sax2 -r -m 0=i810`", um zum i810 zurückzukehren, falls Probleme auftauchen, die beim i810-Treiber nicht vorgekommen sind. Denken Sie in diesem Fall daran, einen Fehlerbericht über den Intel-Treiber zu erstellen.

Intel-WiFi-Treiber für Drahtlosverbindungen

Es sind nun zwei Treiber verfügbar: Der herkömmliche `ipw3945`-Treiber ist standardmäßig installiert und der neue `iwlwifi`-Treiber wird als Alternative angeboten. Folgende Vorbehalte sind zu beachten:

- `ipw3945` funktioniert bei verborgenen Netzwerken. Er übersteht keine unterbrochenen Zyklen.
- `iwlwifi` funktioniert nicht bei verborgenen Netzwerken. Er unterstützt unterbrochene Zyklen.

Die Standardeinstellung kann mit YaST geändert werden. Klicken Sie auf "Software" -> "Software-Management" und entfernen Sie das Paket `ipw3945d`. Der alternative `iwlwifi`-Treiber wird damit automatisch zur Installation ausgewählt.

Tools zum Schreiben auf optische Medien (CD-ROM und DVD)

Das `cdrecord`-Paket wurde aus der Distribution entfernt. Die neuen Pakete `wodim`, `genisoimage` und `icedax` aus dem `cdrkit`-Projekt können zur Aufzeichnung von Daten oder Audio-CDs auf einem CD-Rekorder, der der Orange Book-Norm entspricht, verwendet werden. Binärdateien wurden wie folgt umbenannt:

```
cdrecord -> wodim
readcd   -> readom
mkisofs  -> genisoimage
cdda2wav -> icedax
```

Wenn Ihre Anwendung auf die alten Namen angewiesen ist, installieren Sie das Paket `cdrkit-cdrtools-compat`. Auf lange Sicht wäre es jedoch gut, wenn alle Frontend-Anwendungen native Unterstützung für `wodim` bieten würden, da es darin einige Verbesserungen gibt:

- Die bevorzugte Form zur Angabe eines Geräts ist `dev=/dev/cdrecorder`, `dev=/dev/hdc`, `dev=/dev/sr0`, etc.
- Verfügbare Geräte können mit `wodim -devices` aufgelistet werden
- SUID-Root ist nicht erforderlich

Wenn Sie ein derartiges Frontend oder Skript beibehalten, sollten Sie native Unterstützung für `wodim` vorsehen.

Verwenden Sie `growisofs` zum Schreiben von DVDs. Die Bearbeitung mit grafischen Frontends ist transparent.

Pfad für KDE 4-Anwendungen

Wenn Sie bei der Erstinstallation von openSUSE 10.3 den KDE-Desktop nicht installiert haben und das KDE-Basissystems sowie die Schemata des KDE 4-Basissystems später installieren, steht der Pfad der KDE 4-Anwendung vor dem Pfad der KDE 3-Anwendung. Wenn Sie also eine KDE-Anwendung wie Konqueror starten, wird die KDE 4-Version von Konqueror statt dessen KDE 3-Version geladen.

Abspielen von MP3-Dateien in Kaffeine

Beim Öffnen einer MP3-Datei in Kaffeine erhalten Sie eine Fehlermeldung, die Ihnen mitteilt, dass die Software zum Abspielen dieser Datei nicht installiert ist. openSUSE bietet Ihnen daraufhin an, nach einem geeigneten Codec zu suchen, den Sie mit YaST installieren können. Sie können die Engine auch von Xine auf Gstreamer umstellen, indem Sie auf *Einstellungen > Player Engine* klicken, um MP3-Unterstützung zu erhalten.

Dienstprogramme zur Systemüberwachung

In diesem Kapitel werden verschiedene Programme und Mechanismen vorgestellt, mit denen Sie den Zustand Ihres Systems untersuchen können. Weiterhin werden einige, für die tägliche Arbeit nützliche Dienstprogramme sowie deren wichtigste Optionen beschrieben.

Für die vorgestellten Befehle werden jeweils beispielhafte Ausgaben dargestellt. Darin ist die erste Zeile der Befehl selbst (nach einem `>`- oder `#`-Zeichen als Eingabeaufforderung). Auslassungen sind durch eckige Klammern (`[. . .]`) gekennzeichnet und lange Zeilen werden, falls erforderlich, umgebrochen. Umbrüche langer Zeilen sind durch einen umgekehrten Schrägstrich (`\`) gekennzeichnet.

```
# command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
```

Damit möglichst viele Dienstprogramme erwähnt werden können, sind die Beschreibungen kurz gehalten. Weitere Informationen zu allen Befehlen finden Sie auf den entsprechenden Manualpages. Die meisten Befehle verstehen auch die Option `--help`, mit der Sie eine kurze Liste der verfügbaren Parameter anzeigen können.

6.1 Fehlersuche

6.1.1 Angeben der benötigten Bibliothek: `ldd`

Mit dem Befehl `ldd` können Sie ermitteln, welche Bibliotheken die als Argument angegebene dynamische Programmdatei laden würde.

```
tux@mercury:~> ldd /bin/ls
linux-vdso.so.1 => (0x00007ffffbe7fe000)
librt.so.1 => /lib64/librt.so.1 (0x00007f55b639d000)
libacl.so.1 => /lib64/libacl.so.1 (0x00007f55b6195000)
libc.so.6 => /lib64/libc.so.6 (0x00007f55b5e3d000)
libpthread.so.0 => /lib64/libpthread.so.0 (0x00007f55b5c21000)
/lib64/ld-linux-x86-64.so.2 (0x00007f55b65a6000)
libattr.so.1 => /lib64/libattr.so.1 (0x00007f55b5a1c000)
```

Statische Binärdateien benötigen keine dynamischen Bibliotheken.

```
tux@mercury:~> ldd /bin/sash
not a dynamic executable
tux@mercury:~> file /bin/sash
/bin/sash: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), for GNU/Linux
2.6.4, statically linked, stripped
```

6.1.2 Bibliotheksaufrufe eines aktiven Programms: `ltrace`

Mit dem Befehl `ltrace` können Sie die Bibliotheksaufrufe eines Prozesses verfolgen. Dieser Befehl wird auf ähnliche Weise verwendet wie `strace`. Der Parameter `-c` gibt die Anzahl und die Dauer der erfolgten Bibliotheksaufrufe aus:

```
tux@mercury:~> ltrace -c find ~
% time      seconds  usecs/call   calls      function
-----
 34.37      6.758937      245         27554     __errno_location
 33.53      6.593562      788         8358     __fprintf_chk
 12.67      2.490392      144         17212    strlen
 11.97      2.353302      239         9845     readdir64
  2.37      0.466754      27          16716    __ctype_get_mb_cur_max
  1.17      0.230765      27          8358     memcpy
[...]
```

% time	seconds	usecs/call	calls	function
34.37	6.758937	245	27554	__errno_location
33.53	6.593562	788	8358	__fprintf_chk
12.67	2.490392	144	17212	strlen
11.97	2.353302	239	9845	readdir64
2.37	0.466754	27	16716	__ctype_get_mb_cur_max
1.17	0.230765	27	8358	memcpy
[...]				
0.00	0.000036	36	1	textdomain

100.00 19.662715 105717 total

6.1.3 Systemaufrufe eines aktiven Programms: `strace`

Mit dem Dienstprogramm `strace` können Sie alle Systemaufrufe eines aktuell ausgeführten Prozesses verfolgen. Geben Sie den Befehl wie üblich ein und fügen Sie am Zeilenanfang `strace` hinzu:

```
tux@mercury:~> strace ls
execve("/bin/ls", ["ls"], [/* 61 vars */]) = 0
uname({sys="Linux", node="mercury", ...}) = 0
brk(0) = 0x805c000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or \
    directory)
open("/etc/ld.so.cache", O_RDONLY) = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=89696, ...}) = 0
mmap2(NULL, 89696, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb7ef2000
close(3) = 0
open("/lib/librt.so.1", O_RDONLY) = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\000\36\0"... , 512) \
    = 512
fstat64(3, {st_mode=S_IFREG|0755, st_size=36659, ...}) = 0
[...]
stat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
    = 0xb7ca7000
write(1, "bin Desktop Documents music\tM"... , 55bin Desktop Documents \
    \ music      Music public_html tmp
) = 55
close(1) = 0
munmap(0xb7ca7000, 4096) = 0
exit_group(0) = ?
```

Um beispielsweise alle Versuche, eine bestimmte Datei zu öffnen, zu verfolgen, geben Sie Folgendes ein:

```
tux@mercury:~> strace -e open ls .bashrc
open("/etc/ld.so.cache", O_RDONLY) = 3
open("/lib/librt.so.1", O_RDONLY) = 3
open("/lib/libacl.so.1", O_RDONLY) = 3
open("/lib/libc.so.6", O_RDONLY) = 3
open("/lib/libpthread.so.0", O_RDONLY) = 3
open("/lib/libattr.so.1", O_RDONLY) = 3
[...]
```

Um alle untergeordneten Prozesse zu verfolgen, verwenden Sie den Parameter `-f`. Das Verhalten und das Ausgabeformat von `strace` können weitgehend gesteuert werden. Weitere Informationen erhalten Sie durch die Eingabe von `man strace`.

6.2 Dateien und Dateisysteme

6.2.1 Bestimmen Sie den Dateityp: `file`

Mit dem Befehl `file` wird der Typ einer Datei oder einer Dateiliste durch Überprüfung der Datei `/etc/magic` ermittelt.

```
tux@mercury:~> file /usr/bin/file
/usr/bin/file: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), \
    for GNU/Linux 2.6.4, dynamically linked (uses shared libs), stripped
```

Mit dem Parameter `-f list` wird eine zu prüfende Datei mit einer Dateinamensliste angegeben. Mit `-z` kann `file` komprimierte Dateien überprüfen:

```
tux@mercury:~> file /usr/share/man/man1/file.1.gz
usr/share/man/man1/file.1.gz: gzip compressed data, from Unix, max compression
tux@mercury:~> file -z /usr/share/man/man1/file.1.gz
/usr/share/man/man1/file.1.gz: ASCII troff or preprocessor input text \
    (gzip compressed data, from Unix, max compression)
```

6.2.2 Dateisysteme und ihre Verwendung: `mount`, `df` und `du`

Mit dem Befehl `df` können Sie anzeigen, welches Dateisystem (Gerät und Typ) an welchem Einhängepunkt eingehängt ist:

```
tux@mercury:~> mount
/dev/sda3 on / type reiserfs (rw,acl,user_xattr)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/sda1 on /boot type ext2 (rw,acl,user_xattr)
/dev/sda4 on /local type reiserfs (rw,acl,user_xattr)
/dev/fd0 on /media/floppy type subfs (rw,nosuid,nodev,noatime,fs=floppyfss,p
```

Die Gesamtnutzung der Dateisysteme kann mit dem Befehl `df` ermittelt werden. Der Parameter `-h` (oder `--human-readable`) übersetzt die Ausgabe in ein für normale Benutzer verständliches Format.

```
tux@mercury:~> df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        11G  3.2G  6.9G  32% /
udev            252M  104K  252M   1% /dev
/dev/sda1        16M   6.6M   7.8M  46% /boot
/dev/sda4        27G   34M   27G   1% /local
```

Die Gesamtgröße aller Dateien in einem bestimmten Verzeichnis und dessen Unterverzeichnissen lässt sich mit dem Befehl `du` ermitteln. Der Parameter `-s` unterdrückt die Ausgabe der detaillierten Informationen. `-h` wandelt die Daten wieder in normal lesbare Form um:

```
tux@mercury:~> du -sh /local
1.7M    /local
```

6.2.3 Zusätzliche Informationen zu ELF-Binärdateien

Der Inhalt von Binärdateien wird mit dem Dienstprogramm `readelf` gelesen. Dies funktioniert auch für ELF-Dateien, die für andere Hardware-Architekturen entwickelt wurden:

```
tux@mercury:~> readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00
  Class:                               ELF64
  Data:                                  2's complement, little endian
  Version:                               1 (current)
  OS/ABI:                                UNIX - System V
  ABI Version:                           0
  Type:                                  EXEC (Executable file)
  Machine:                               Advanced Micro Devices X86-64
  Version:                               0x1
  Entry point address:                   0x402430
  Start of program headers:              64 (bytes into file)
  Start of section headers:              98616 (bytes into file)
  Flags:                                  0x0
  Size of this header:                    64 (bytes)
  Size of program headers:                56 (bytes)
  Number of program headers:              9
  Size of section headers:                64 (bytes)
  Number of section headers:              31
  Section header string table index:      30
```

6.2.4 Dateieigenschaften: stat

Mit dem Befehl `stat` zeigen Sie die Eigenschaften einer Datei an:

```
tux@mercury:~> stat /etc/profile
  File: `/etc/profile'
  Size: 8080          Blocks: 16          IO Block: 4096   regular file
Device: 806h/2054d   Inode: 64942       Links: 1
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2007-07-16 23:28:18.000000000 +0200
Modify: 2006-09-19 14:45:01.000000000 +0200
Change: 2006-12-05 14:54:55.000000000 +0100
```

Mit dem Parameter `--filesystem` werden Eigenschaften des Dateisystems angezeigt, in dem sich die angegebene Datei befindet:

```
tux@mercury:~> stat /etc/profile --filesystem
  File: "/etc/profile"
   ID: 0          Namelen: 255       Type: reiserfs
Block size: 4096      Fundamental block size: 4096
Blocks: Total: 2622526   Free: 1809771     Available: 1809771
Inodes: Total: 0        Free: 0
```

6.3 Hardware-Informationen

6.3.1 PCI-Ressourcen: lspci

Der Befehl `lspci` listet die PCI-Ressourcen auf:

```
mercury:~ # lspci
00:00.0 Host bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
  DRAM Controller/Host-Hub Interface (rev 01)
00:01.0 PCI bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
  Host-to-AGP Bridge (rev 01)
00:1d.0 USB Controller: Intel Corporation 82801DB/DBL/DBM \
  (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #1 (rev 01)
00:1d.1 USB Controller: Intel Corporation 82801DB/DBL/DBM \
  (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #2 (rev 01)
00:1d.2 USB Controller: Intel Corporation 82801DB/DBL/DBM \
  (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #3 (rev 01)
00:1d.7 USB Controller: Intel Corporation 82801DB/DBM \
  (ICH4/ICH4-M) USB2 EHCI Controller (rev 01)
00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev 81)
00:1f.0 ISA bridge: Intel Corporation 82801DB/DBL (ICH4/ICH4-L) \
  LPC Interface Bridge (rev 01)
00:1f.1 IDE interface: Intel Corporation 82801DB (ICH4) IDE \
```

```

    Controller (rev 01)
00:1f.3 SMBus: Intel Corporation 82801DB/DBL/DBM (ICH4/ICH4-L/ICH4-M) \
    SMBus Controller (rev 01)
00:1f.5 Multimedia audio controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) AC'97 Audio Controller (rev 01)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. G400/G450 (rev 85)
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM) \
    Ethernet Controller (rev 81)

```

Mit der Option `-v` werden ausführlichere Informationen angezeigt:

```

mercury:~ # lspci
[...]
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM)\
    Ethernet Controller (rev 81)
    Subsystem: Fujitsu Siemens Computer GmbH: Unknown device 1001
    Flags: bus master, medium devsel, latency 66, IRQ 11
    Memory at d1000000 (32-bit, non-prefetchable) [size=4K]
    I/O ports at 3000 [size=64]
    Capabilities: [dc] Power Management version 2

```

Die Informationen zur Auflösung der Gerätenamen stammen aus der Datei `/usr/share/pci.ids`. PCI-IDs, die in dieser Datei fehlen, werden als „Unknown device“ (Unbekanntes Gerät) markiert.

Der Parameter `-vv` generiert alle Informationen, die vom Programm abgefragt werden können. Die reinen numerischen Werte werden mit dem Parameter `-n` angezeigt.

6.3.2 USB-Geräte: `lsusb`

Mit dem Befehl `lsusb` werden alle USB-Geräte aufgelistet. Mit der Option `-v` wird eine detailliertere Liste ausgegeben. Die detaillierten Informationen werden aus dem Verzeichnis `/proc/bus/usb/` gelesen. Das Folgende ist die Ausgabe von `lsusb` mit den angeschlossenen USB-Geräten Hub, Memorystick, Festplatte und Maus.

```

mercury:/ # lsusb
Bus 004 Device 007: ID 0ea0:2168 Ours Technology, Inc. Transcend JetFlash \
    2.0 / Astone USB Drive
Bus 004 Device 006: ID 04b4:6830 Cypress Semiconductor Corp. USB-2.0 IDE \
    Adapter
Bus 004 Device 005: ID 05e3:0605 Genesys Logic, Inc.
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 005: ID 046d:c012 Logitech, Inc. Optical Mouse
Bus 001 Device 001: ID 0000:0000

```

6.3.3 Informationen zu einem SCSI-Gerät: `scsiinfo`

Mit dem Befehl `scsiinfo` können Sie Informationen zu einem SCSI-Gerät anzeigen. Mit der Option `-l` werden alle dem System bekannten SCSI-Geräte aufgelistet (ähnliche Informationen erhalten Sie über den Befehl `lsscsi`). Im Folgenden sehen Sie die Ausgabe von `scsiinfo -i /dev/sda`, die Informationen zu einer Festplatte enthält. Mit der Option `-a` erhalten Sie noch ausführlichere Informationen.

```
mercury:/ # scsiinfo -i /dev/sda
Inquiry command
-----
Relative Address                0
Wide bus 32                     0
Wide bus 16                     1
Synchronous neg.               1
Linked Commands                 1
Command Queueing                1
SftRe                           0
Device Type                     0
Peripheral Qualifier            0
Removable?                      0
Device Type Modifier            0
ISO Version                     0
ECMA Version                    0
ANSI Version                    3
AENC                            0
TrmIOP                          0
Response Data Format            2
Vendor:                         FUJITSU
Product:                        MAS3367NP
Revision level:                 0104A0K7P43002BE
```

Mit der Option `-d` wird eine Liste der Fehler in Form von zwei Tabellen mit fehlerhaften Blöcken der Festplatte ausgegeben: eine vom Händler bereitgestellte Tabelle (Herstellertabelle) und eine Liste der beim Betrieb aufgetretenen fehlerhaften Blöcke (gewachsene Tabelle). Wenn die Anzahl der Einträge in der während des Betriebs generierten Tabelle (grown table) zunimmt, empfiehlt es sich, die Festplatte zu ersetzen.

6.4 Netzwerke

6.4.1 Netzwerkstatus anzeigen: netstat

netstat zeigt Netzwerkverbindungen, Routing-Tabellen (-r), Schnittstellen (-i), Masquerade-Verbindungen (-M), Multicast-Mitgliedschaften (-g) und Statistiken (-s) an.

```
tux@mercury:~> netstat -r
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
192.168.2.0      *                255.255.254.0  U       0  0        0 eth0
link-local       *                255.255.0.0    U       0  0        0 eth0
loopback         *                255.0.0.0      U       0  0        0 lo
default          192.168.2.254  0.0.0.0        UG      0  0        0 eth0
```

```
tux@mercury:~> netstat -i
Kernel Interface table
Iface  MTU Met  RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0   1500  0  1624507 129056  0      0  7055  0      0      0 BMNRU
lo     16436  0   23728  0      0      0  23728  0      0      0 LRU
```

Wenn Sie Netzwerkverbindungen oder Statistiken anzeigen, können Sie den anzuzeigenden Socket-Typ angeben: TCP (-t), UDP (-u) oder Raw (-r). Mit der Option -p werden die PID und der Name des Programms angezeigt, zu dem das einzelne Socket gehört.

Im folgenden Beispiel werden alle TCP-Verbindungen und die Programme aufgelistet, die diese Verbindungen verwenden.

```
mercury:~ # netstat -t -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Pro
tcp 0 0 mercury:33513 www.novell.com:www-http ESTABLISHED 6862/fi
tcp 0 352 mercury:ssh mercury2.:trc-netpoll ESTABLISHED
19422/s
tcp 0 0 localhost:ssh localhost:17828 ESTABLISHED -
```

Nachfolgend werden die Statistiken für das TCP-Protokoll angezeigt:

```
tux@mercury:~> netstat -s -t
Tcp:
 2427 active connections openings
 2374 passive connection openings
 0 failed connection attempts
```

```

0 connection resets received
1 connections established
27476 segments received
26786 segments send out
54 segments retransmitted
0 bad segments received.
6 resets sent
[...]
TCPAbortOnLinger: 0
TCPAbortFailed: 0
TCPMemoryPressures: 0

```

6.5 Das Dateisystem /proc

Das Dateisystem `/proc` ist ein Pseudo-Dateisystem, in dem der Kernel wichtige Daten in Form von virtuellen Dateien speichert. Der CPU-Typ kann beispielsweise mit dem folgenden Befehl abgerufen werden:

```

tux@mercury:~> cat /proc/cpuinfo
processor       : 0
vendor_id     : GenuineIntel
cpu family    : 15
model         : 4
model name    : Intel(R) Pentium(R) 4 CPU 3.40GHz
stepping     : 3
cpu MHz      : 2800.000
cache size   : 2048 KB
physical id  : 0
[...]

```

Mit folgendem Befehl wird die Zuordnung und Verwendung von Interrupts abgefragt:

```

tux@mercury:~> cat /proc/interrupts
CPU0
 0:   3577519      XT-PIC  timer
 1:     130      XT-PIC  i8042
 2:         0      XT-PIC  cascade
 5:   564535      XT-PIC  Intel 82801DB-ICH4
 7:         1      XT-PIC  parport0
 8:         2      XT-PIC  rtc
 9:         1      XT-PIC  acpi, uhci_hcd:usb1, ehci_hcd:usb4
10:         0      XT-PIC  uhci_hcd:usb3
11:    71772      XT-PIC  uhci_hcd:usb2, eth0
12:   101150      XT-PIC  i8042
14:   33146      XT-PIC  ide0
15:   149202      XT-PIC  ide1
NMI:         0
LOC:         0

```

```
ERR:      0
MIS:      0
```

Einige wichtige Dateien und die enthaltenen Informationen sind:

```
/proc/devices
  Verfügbare Geräte
```

```
/proc/modules
  Geladene Kernel-Module
```

```
/proc/cmdline
  Kernel-Kommandozeile
```

```
/proc/meminfo
  Detaillierte Informationen zur Arbeitsspeichernutzung
```

```
/proc/config.gz
  gzip-komprimierte Konfigurationsdatei des aktuell aktivierten Kernels
```

Weitere Informationen finden Sie in der Textdatei `/usr/src/linux/Documentation/filesystems/proc.txt`. Informationen zu aktuell laufenden Prozessen finden Sie in den `/proc/NNN`-Verzeichnissen, wobei *NNN* für die Prozess-ID (PID) des jeweiligen Prozesses steht. Mit `/proc/self/` können die zum aktiven Prozess gehörenden Eigenschaften abgerufen werden:

```
tux@mercury:~> ls -l /proc/self
lrwxrwxrwx 1 root root 64 2007-07-16 13:03 /proc/self -> 5356
tux@mercury:~> ls -l /proc/self/
total 0
dr-xr-xr-x 2 tux users 0 2007-07-16 17:04 attr
-r----- 1 tux users 0 2007-07-16 17:04 auxv
-r--r--r-- 1 tux users 0 2007-07-16 17:04 cmdline
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 cwd -> /home/tux
-r----- 1 tux users 0 2007-07-16 17:04 environ
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 exe -> /bin/ls
dr-x----- 2 tux users 0 2007-07-16 17:04 fd
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 loginuid
-r--r--r-- 1 tux users 0 2007-07-16 17:04 maps
-rw----- 1 tux users 0 2007-07-16 17:04 mem
-r--r--r-- 1 tux users 0 2007-07-16 17:04 mounts
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 oom_adj
-r--r--r-- 1 tux users 0 2007-07-16 17:04 oom_score
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 root -> /
-rw----- 1 tux users 0 2007-07-16 17:04 seccomp
-r--r--r-- 1 tux users 0 2007-07-16 17:04 smaps
-r--r--r-- 1 tux users 0 2007-07-16 17:04 stat
```

```
[...]
dr-xr-xr-x 3 tux users 0 2007-07-16 17:04 task
-r--r--r-- 1 tux users 0 2007-07-16 17:04 wchan
```

Die Adresszuordnung der Programmdateien und Bibliotheken befindet sich in der Datei maps:

```
tux@mercury:~> cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:03 17753      /bin/cat
0804c000-0804d000 rw-p 00004000 03:03 17753      /bin/cat
0804d000-0806e000 rw-p 0804d000 00:00 0          [heap]
b7d27000-b7d5a000 r--p 00000000 03:03 11867      /usr/lib/locale/en_GB.utf8/
b7d5a000-b7e32000 r--p 00000000 03:03 11868      /usr/lib/locale/en_GB.utf8/
b7e32000-b7e33000 rw-p b7e32000 00:00 0
b7e33000-b7f45000 r-xp 00000000 03:03 8837       /lib/libc-2.3.6.so
b7f45000-b7f46000 r--p 00112000 03:03 8837       /lib/libc-2.3.6.so
b7f46000-b7f48000 rw-p 00113000 03:03 8837       /lib/libc-2.3.6.so
b7f48000-b7f4c000 rw-p b7f48000 00:00 0
b7f52000-b7f53000 r--p 00000000 03:03 11842      /usr/lib/locale/en_GB.utf8/
[...]
b7f5b000-b7f61000 r--s 00000000 03:03 9109       /usr/lib/gconv/gconv-module
b7f61000-b7f62000 r--p 00000000 03:03 9720       /usr/lib/locale/en_GB.utf8/
b7f62000-b7f76000 r-xp 00000000 03:03 8828       /lib/ld-2.3.6.so
b7f76000-b7f78000 rw-p 00013000 03:03 8828       /lib/ld-2.3.6.so
bfd61000-bfd76000 rw-p bfd61000 00:00 0          [stack]
ffffe000-fffff000 ---p 00000000 00:00 0          [vdso]
```

6.5.1 procinfo

Wichtige Informationen zum Dateisystem `/proc` werden mit dem Befehl `procinfo` zusammengefasst:

```
tux@mercury:~> procinfo
Linux 2.6.18.8-0.5-default (geeko@buildhost) (gcc 4.1.2 20061115) #1 2CPU

Memory:      Total      Used      Free      Shared      Buffers
Mem:         2060604    2011264    49340     0           200664
Swap:        2104472     112       2104360

Bootup: Tue Jul 10 10:29:15 2007      Load average: 0.86 1.10 1.11 3/118 21547

user   :      2:43:13.78   0.8%  page in  :      71099181  disk 1:  2827023r 968
nice   :      1d 22:21:27.87 14.7%  page out:   690734737
system:      13:39:57.57   4.3%  page act:  138388345
IOwait:      18:02:18.59   5.7%  page dea:   29639529
hw irq:      0:03:39.44   0.0%  page flt:  9539791626
sw irq:      1:15:35.25   0.4%  swap in  :           69
idle   :      9d 16:07:56.79 73.8%  swap out:           209
uptime:      6d 13:07:11.14      context :   542720687
```

```

irq 0: 141399308 timer          irq 14: 5074312 ide0
irq 1: 73784 i8042             irq 50: 1938076 uhci_hcd:usb1, ehci_
irq 4: 2                       irq 58: 0 uhci_hcd:usb2
irq 6: 5 floppy [2]          irq 66: 872711 uhci_hcd:usb3, HDA I
irq 7: 2                       irq 74: 15 uhci_hcd:usb4
irq 8: 0 rtc                  irq 82: 178717720 0 PCI-MSI e
irq 9: 0 acpi                 irq169: 44352794 nvidia
irq 12: 3                     irq233: 8209068 0 PCI-MSI 1

```

Verwenden Sie den Parameter `-a`, wenn Sie alle Informationen anzeigen möchten. Der Parameter `-nN` aktualisiert die Informationen alle N Sekunden. Beenden Sie in diesem Fall das Programm mit der Taste `Q`.

Standardmäßig werden die kumulativen Werte angezeigt. Mit dem Parameter `-d` werden die Einzelwerte generiert. `procinfo -dn5` zeigt die Werte an, die sich in den letzten fünf Sekunden geändert haben:

6.6 Vorgänge

6.6.1 Prozessübergreifende Kommunikation: `ipcs`

Der Befehl `ipcs` generiert eine Liste der aktuell verwendeten IPC-Ressourcen:

```

----- Shared Memory Segments -----
key          shmid      owner      perms      bytes      nattch     status
0x00000000  58261504   tux       600        393216     2          dest
0x00000000  58294273   tux       600        196608     2          dest
0x00000000  83886083   tux       666        43264     2
0x00000000  83951622   tux       666        192000     2
0x00000000  83984391   tux       666        282464     2
0x00000000  84738056   root      644        151552     2          dest

----- Semaphore Arrays -----
key          semid      owner      perms      nsems
0x4d038abf  0          tux       600        8

----- Message Queues -----
key          msqid      owner      perms      used-bytes  messages

```

6.6.2 Prozessliste: ps

Mit dem Befehl `ps` wird eine Liste von Prozessen generiert. Die meisten Parameter müssen ohne Minuszeichen angegeben werden. Über `ps --help` erhalten Sie eine kurze und auf der entsprechenden Manualpage eine ausführliche Hilfe.

Um alle Prozesse mit Benutzer- und Kommandozeileninformation aufzulisten, verwenden Sie `ps axu`:

```
tux@mercury:~> ps axu
USER      PID  %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0   696   272 ?        S    12:59   0:01 init [5]
root         2  0.0  0.0     0     0 ?        SN   12:59   0:00 [ksoftirqd
root         3  0.0  0.0     0     0 ?        S<   12:59   0:00 [events
[...]
tux      4047  0.0  6.0 158548 31400 ?        Ssl  13:02   0:06 mono-best
tux      4057  0.0  0.7   9036  3684 ?        S1   13:02   0:00 /opt/gnome
tux      4067  0.0  0.1   2204   636 ?        S    13:02   0:00 /opt/gnome
tux      4072  0.0  1.0  15996  5160 ?        Ss   13:02   0:00 gnome-scre
tux      4114  0.0  3.7 130988 19172 ?        SLl  13:06   0:04 sound-juic
tux      4818  0.0  0.3   4192  1812 pts/0    Ss   15:59   0:00 -bash
tux      4959  0.0  0.1   2324   816 pts/0    R+   16:17   0:00 ps axu
```

Um zu prüfen, wie viele `sshd`-Prozesse laufen, verwenden Sie die Option `-p` zusammen mit dem Befehl `pidof`, der die Prozess-IDs der gegebenen Prozesse auflistet.

```
tux@mercury:~> ps -p `pidof sshd`
  PID TTY          STAT TIME  COMMAND
 3524 ?           Ss     0:00 /usr/sbin/sshd -o PidFile=/var/run/sshd.init.pid
 4813 ?           Ss     0:00 sshd: tux [priv]
 4817 ?           R      0:00 sshd: tux@pts/0
```

Sie können die Prozessliste entsprechend Ihren Anforderungen formatieren. Mit der Option `-L` wird eine Liste aller Schlüsselwörter zurückgegeben. Geben Sie den folgenden Befehl ein, um eine nach Speichernutzung aller Prozesse sortierte Liste zu erhalten:

```
tux@mercury:~> ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2     0 [ksoftirqd/0]
    3     0 [events/0]
    4     0 [khelper]
    5     0 [kthread]
   11     0 [kblockd/0]
   12     0 [kacpid]
  472     0 [pdflush]
  473     0 [pdflush]
[...]
 4028 17556 nautilus --no-default-window --sm-client-id default2
 4118 17800 ksnapshot
```

```

4114 19172 sound-juicer
4023 25144 gnome-panel --sm-client-id default1
4047 31400 mono-best --debug /usr/lib/beagle/Best.exe --autostarted
3973 31520 mono-beagled --debug /usr/lib/beagle/BeagleDaemon.exe --bg --aut

```

6.6.3 Prozessbaum: pstree

Mit dem Befehl `ps tree` wird eine Liste der Prozesse in Form einer Baumstruktur generiert:

```

tux@mercury:~> pstree
init--NetworkManagerD
  |-acpid
  |-3*[automount]
  |-cron
  |-cupsd
  |-2*[dbus-daemon]
  |-dbus-launch
  |-dcopserver
  |-dhcpcd
  |-events/0
  |-gpg-agent
  |-hald--hald-addon-acpi
  |   `--hald-addon-stor
  |-kded
  |-kdeinit--kdesu---su---kdesu_stub---yast2---y2controlcenter
  |   |   |-kio_file
  |   |   |-klauncher
  |   |   |-konqueror
  |   |   |-konsole--bash---su---bash
  |   |   |   `--bash
  |   `--kwin
  |-kdesktop---kdesktop_lock---xmatrix
  |-kdesud
  |-kdm--X
  |   `--kdm---startkde---kwrapper
[...]
```

Mit dem Parameter `-p` werden die Namen durch die jeweiligen Prozess-IDs ergänzt. Damit auch die Kommandozeilen angezeigt werden, verwenden Sie den Parameter `-a`:

6.6.4 Prozesse: top

Mit dem Befehl `top`, der für "Table of Processes" (Tabelle der Prozesse) steht, wird eine Liste der Prozesse angezeigt, die alle zwei Sekunden aktualisiert wird. Um das Programm zu beenden, drücken Sie die Taste `Q`. Mit der Option `-n 1` wird das Pro-

gramm nach einmaliger Anzeige der Prozessliste beendet. Im Folgenden finden Sie ein Beispiel für die Ausgabe des Befehls `top -n 1`:

```
tux@mercury:~> top -n 1
top - 17:06:28 up 2:10, 5 users, load average: 0.00, 0.00, 0.00
Tasks: 85 total, 1 running, 83 sleeping, 1 stopped, 0 zombie
Cpu(s): 5.5% us, 0.8% sy, 0.8% ni, 91.9% id, 1.0% wa, 0.0% hi, 0.0% si
Mem: 515584k total, 506468k used, 9116k free, 66324k buffers
Swap: 658656k total, 0k used, 658656k free, 353328k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1	root	16	0	700	272	236	S	0.0	0.1	0:01.33	init
2	root	34	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
3	root	10	-5	0	0	0	S	0.0	0.0	0:00.27	events/0
4	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	khelper
5	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	kthread
11	root	10	-5	0	0	0	S	0.0	0.0	0:00.05	kblockd/0
12	root	20	-5	0	0	0	S	0.0	0.0	0:00.00	kacpid
472	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pdflush
473	root	15	0	0	0	0	S	0.0	0.0	0:00.06	pdflush
475	root	11	-5	0	0	0	S	0.0	0.0	0:00.00	aio/0
474	root	15	0	0	0	0	S	0.0	0.0	0:00.07	kswapd0
681	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	kseriod
839	root	10	-5	0	0	0	S	0.0	0.0	0:00.02	reiserfs/0
923	root	13	-4	1712	552	344	S	0.0	0.1	0:00.67	udev
1343	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	khubb
1587	root	20	0	0	0	0	S	0.0	0.0	0:00.00	shpchpd_event
1746	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_control
1752	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_bus_master1
2151	root	16	0	1464	496	416	S	0.0	0.1	0:00.00	acpid
2165	messageb	16	0	3340	1048	792	S	0.0	0.2	0:00.64	dbus-daemon
2166	root	15	0	1840	752	556	S	0.0	0.1	0:00.01	syslog-ng
2171	root	16	0	1600	516	320	S	0.0	0.1	0:00.00	klogd
2235	root	15	0	1736	800	652	S	0.0	0.2	0:00.10	resmgrd
2289	root	16	0	4192	2852	1444	S	0.0	0.6	0:02.05	hald
2403	root	23	0	1756	600	524	S	0.0	0.1	0:00.00	hald-addon-acpi
2709	root	19	0	2668	1076	944	S	0.0	0.2	0:00.00	NetworkManagerD
2714	root	16	0	1756	648	564	S	0.0	0.1	0:00.56	hald-addon-stor

Wenn Sie die Taste `F` drücken, während `top` aktiv ist, wird ein Menü geöffnet, in dem das Format der Ausgabe umfassend bearbeitet werden kann.

Um nur die Prozesse eines bestimmten Benutzers zu überwachen, kann der Parameter `-U UID` verwendet werden. Ersetzen Sie `UID` durch die Benutzer-ID des Benutzers. Der Befehl `top -U `id -u`` gibt die UID des Benutzers auf Basis des Benutzernamens zurück und zeigt dessen Prozesse an.

6.7 Systemangaben

6.7.1 Auslastung des Arbeitsspeichers: `free`

Die Nutzung des Arbeitsspeichers (RAM) wird mit dem Dienstprogramm `free` überprüft. Es werden Details zum freien und zum verwendeten Speicher sowie zu den Auslagerungsbereichen angezeigt:

```
tux@mercury:~> free
              total        used         free       shared    buffers     cached
Mem:          2062844      2047444         15400           0        129580       921936
-/+ buffers/cache:  995928      1066916
Swap:          2104472           0         2104472
```

Die Optionen `-b,-k,-m,-g` zeigen die Ausgabe in Byte, KB, MB bzw. GB. Der Parameter `-d N` gewährleistet, dass die Anzeige alle N Sekunden aktualisiert wird. So wird die Anzeige mit `free -d 1.5` beispielsweise alle 1,5 Sekunden aktualisiert.

6.7.2 Benutzerzugriffsdateien: `fuser`

Es kann hilfreich sein, zu ermitteln, welche Prozesse oder Benutzer aktuell auf bestimmte Dateien zugreifen. Sie möchten beispielsweise ein Dateisystem aushängen, das unter `/mnt` eingehängt ist. `umount` gibt "device is busy" zurück. Mit dem Befehl `fuser` können Sie anschließend ermitteln, welche Prozesse auf das Gerät zugreifen:

```
tux@mercury:~> fuser -v /mnt/*

/mnt/notes.txt          USER          PID ACCESS COMMAND
                        tux           26597 f.... less
```

Nach dem Beenden des Prozesses `less`, der auf einem anderen Terminal ausgeführt wurde, kann das Aushängen des Dateisystems erfolgreich ausgeführt werden.

6.7.3 Kernel-Ring-Puffer: `dmesg`

Der Linux-Kernel hält bestimmte Meldungen in einem Ringpuffer zurück. Um diese Meldungen anzuzeigen, geben Sie den Befehl `dmesg` ein:

```
$ dmesg
[...]
```

```

end_request: I/O error, dev fd0, sector 0
subfs: unsuccessful attempt to mount media (256)
e100: eth0: e100_watchdog: link up, 100Mbps, half-duplex
NET: Registered protocol family 17
IA-32 Microcode Update Driver: v1.14 <tigran@veritas.com>
microcode: CPU0 updated from revision 0xe to 0x2e, date = 08112004
IA-32 Microcode Update Driver v1.14 unregistered
boot splash: status on console 0 changed to on
NET: Registered protocol family 10
Disabled Privacy Extensions on device c0326ea0(lo)
IPv6 over IPv4 tunneling driver
powernow: This module only works with AMD K7 CPUs
boot splash: status on console 0 changed to on

```

Ältere Ereignisse werden in den Dateien `/var/log/messages` und `/var/log/warn` protokolliert.

6.7.4 Liste der geöffneten Dateien: `lsdf`

Um eine Liste aller Dateien anzuzeigen, die für den Prozess mit der Prozess-ID `PID` geöffnet sind, verwenden Sie `-p`. Um beispielsweise alle von der aktuellen Shell verwendeten Dateien anzuzeigen, geben Sie Folgendes ein:

```

tux@mercury:~> lsdf -p $$
COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME
bash 5552 tux cwd DIR 3,3 1512 117619 /home/tux
bash 5552 tux rtd DIR 3,3 584 2 /
bash 5552 tux txt REG 3,3 498816 13047 /bin/bash
bash 5552 tux mem REG 0,0 0 [heap] (stat: No such
bash 5552 tux mem REG 3,3 217016 115687 /var/run/nsd/passwd
bash 5552 tux mem REG 3,3 208464 11867 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 882134 11868 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 1386997 8837 /lib/libc-2.3.6.so
bash 5552 tux mem REG 3,3 13836 8843 /lib/libdl-2.3.6.so
bash 5552 tux mem REG 3,3 290856 12204 /lib/libncurses.so.5.5
bash 5552 tux mem REG 3,3 26936 13004 /lib/libhistory.so.5.1
bash 5552 tux mem REG 3,3 190200 13006 /lib/libreadline.so.5.
bash 5552 tux mem REG 3,3 54 11842 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 2375 11663 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 290 11736 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 52 11831 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 34 11862 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 62 11839 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 127 11664 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 56 11735 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 23 11866 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 21544 9109 /usr/lib/gconv/gconv-m
bash 5552 tux mem REG 3,3 366 9720 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 97165 8828 /lib/ld-2.3.6.so

```

```

bash    5552 tux    0u    CHR  136,5          7 /dev/pts/5
bash    5552 tux    1u    CHR  136,5          7 /dev/pts/5
bash    5552 tux    2u    CHR  136,5          7 /dev/pts/5
bash    5552 tux   255u  CHR  136,5          7 /dev/pts/5

```

Es wurde die spezielle Shell-Variable \$\$ verwendet, deren Wert die Prozess-ID der Shell ist.

Wird der Befehl `lsdf` ohne Parameter eingegeben, werden alle aktuell geöffneten Dateien angezeigt. Da dies in der Regel recht viele sind, wird dieser Befehl selten verwendet. Die Liste der Dateien kann jedoch mit Suchfunktionen kombiniert werden, um sinnvolle Listen zu generieren. Beispiel: Liste aller verwendeten zeichenorientierten Geräte:

```

tux@mercury:~> lsdf | grep CHR
bash    3838    tux    0u    CHR  136,0          2 /dev/pts/0
bash    3838    tux    1u    CHR  136,0          2 /dev/pts/0
bash    3838    tux    2u    CHR  136,0          2 /dev/pts/0
bash    3838    tux   255u  CHR  136,0          2 /dev/pts/0
bash    5552    tux    0u    CHR  136,5          7 /dev/pts/5
bash    5552    tux    1u    CHR  136,5          7 /dev/pts/5
bash    5552    tux    2u    CHR  136,5          7 /dev/pts/5
bash    5552    tux   255u  CHR  136,5          7 /dev/pts/5
X       5646    root  mem    CHR    1,1          1006 /dev/mem
lsdf    5673    tux    0u    CHR  136,5          7 /dev/pts/5
lsdf    5673    tux    2u    CHR  136,5          7 /dev/pts/5
grep    5674    tux    1u    CHR  136,5          7 /dev/pts/5
grep    5674    tux    2u    CHR  136,5          7 /dev/pts/5

```

6.7.5 Kernel- und udev-Ereignissequenzanzeige: `udevadm monitor`

`udevadm monitor` überwacht die Kernel-uevents und die Ereignisse, die über eine udev-Regel gesendet werden, und sendet den Gerätepfad (DEVPATH) des Ereignisses an die Konsole. Hierbei handelt es sich um eine Ereignissequenz beim Anschließen eines USB-Memorysticks:

```

UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806687] add@/class/scsi_host/host4
UEVENT[1138806687] add@/class/usb_device/usbdev4.10
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806687] add@/class/scsi_host/host4
UDEV [1138806687] add@/class/usb_device/usbdev4.10
UEVENT[1138806692] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806692] add@/block/sdb
UEVENT[1138806692] add@/class/scsi_generic/sg1
UEVENT[1138806692] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806693] add@/class/scsi_generic/sg1
UDEV [1138806693] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/block/sdb
UEVENT[1138806694] add@/block/sdb/sdb1
UDEV [1138806694] add@/block/sdb/sdb1
UEVENT[1138806694] mount@/block/sdb/sdb1
UEVENT[1138806697] umount@/block/sdb/sdb1

```

6.8 Benutzerinformationen

6.8.1 Wer macht was: w

Mit dem Befehl `w` ermitteln Sie, wer beim System angemeldet ist und was die einzelnen Benutzer gerade machen. Beispiel:

```

tux@mercury:~> w
 14:58:43 up 1 day,  1:21,  2 users,  load average: 0.00, 0.00, 0.00
USER  TTY          LOGIN@  IDLE   JCPU   PCPU WHAT
tux   :0          12:25  ?xdm?  1:23   0.12s /bin/sh /usr/bin/startkde
root  pts/4      14:13   0.00s  0.06s  0.00s w

```

Wenn sich Benutzer von entfernten Systemen angemeldet haben, können Sie mit dem Parameter `-f` anzeigen lassen, von welchen Computern aus diese Verbindungen aufgebaut wurden.

6.9 Zeit und Datum

6.9.1 Zeitmessung mit `time`

Der Zeitaufwand von Befehlen lässt sich mit dem Dienstprogramm `time` ermitteln. Dieses Dienstprogramm ist in zwei Versionen verfügbar: in Shell integriert und als Programm (`/usr/bin/time`).

```
tux@mercury:~> time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```


Teil III. System

32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung

7

openSUSE® ist für 64-Bit-Plattformen verfügbar. Das bedeutet jedoch nicht unbedingt, dass alle enthaltenen Anwendungen bereits auf 64-Bit-Plattformen portiert wurden. openSUSE unterstützt die Verwendung von 32-Bit-Anwendungen in einer 64-Bit-Systemumgebung. Dieses Kapitel bietet einen kurzen Überblick über die Implementierung dieser Unterstützung auf openSUSE-64-Bit-Plattformen. Es wird erläutert, wie 32-Bit-Anwendungen ausgeführt werden (Laufzeitunterstützung) und wie 32-Bit-Anwendungen kompiliert werden sollten, damit sie sowohl in 32-Bit- als auch in 64-Bit-Systemanwendungen ausgeführt werden können. Außerdem finden Sie Informationen zur Kernel-API und es wird erläutert, wie 32-Bit-Anwendungen unter einem 64-Bit-Kernel ausgeführt werden können.

openSUSE für die 64-Bit-Plattformen amd64 und Intel 64 ist so konzipiert, dass bestehende 32-Bit-Anwendungen sofort in der 64-Bit-Umgebung ausgeführt werden können.,“ Diese Unterstützung bedeutet, dass Sie weiterhin Ihre bevorzugten 32-Bit-Anwendungen verwenden können und nicht warten müssen, bis ein entsprechender 64-Bit-Port verfügbar ist.

7.1 Laufzeitunterstützung

WICHTIG: Konflikte zwischen Anwendungsversionen

Wenn eine Anwendung sowohl für 32-Bit- als auch für 64-Bit-Umgebungen verfügbar ist, führt die parallele Installation beider Versionen zwangsläufig zu

Problemen. Entscheiden Sie sich in diesen Fällen für eine der beiden Versionen und installieren und verwenden Sie nur diese.

Für eine korrekte Ausführung benötigt jede Anwendung eine Reihe von Bibliotheken. Leider sind die Namen für die 32-Bit- und 64-Bit-Versionen dieser Bibliotheken identisch. Sie müssen auf andere Weise voneinander unterschieden werden.

Um die Kompatibilität mit der 32-Bit-Version aufrechtzuerhalten, werden die Bibliotheken am selben Ort im System gespeichert wie in der 32-Bit-Umgebung. Die 32-Bit-Version von `libc.so.6` befindet sich sowohl in der 32-Bit- als auch in der 64-Bit-Umgebung unter `/lib/libc.so.6`.

Alle 64-Bit-Bibliotheken und Objektdateien befinden sich in Verzeichnissen mit dem Namen `lib64`. Die 32-Bit-Objektdateien, die sich normalerweise unter `/lib` und `/usr/lib` befinden, werden nun unter `/lib64` und `/usr/lib64` gespeichert. Unter `/lib` und `/usr/lib` ist also Platz für die 32-Bit-Bibliotheken, sodass der Dateiname für beide Versionen unverändert bleiben kann.

Unterverzeichnisse von 32-Bit-Verzeichnissen namens `/lib`, deren Dateninhalt nicht von der Wortgröße abhängt, werden nicht verschoben. Das Schema entspricht LSB (Linux Standards Base) und FHS (File System Hierarchy Standard).

7.2 Software-Entwicklung

Eine Doppelarchitektur-Entwicklungswerkzeugkette (Biarch Development Toolchain) ermöglicht die Erstellung von 32-Bit- und 64-Bit-Objekten. Standardmäßig werden 64-Bit-Objekte kompiliert. 32-Bit-Objekte können durch Verwendung spezieller Flaggen erstellt werden. Bei GCC lautet diese Flagge `-m32`.

Alle Header-Dateien müssen in architekturunabhängiger Form geschrieben werden. Die installierten 32-Bit- und 64-Bit-Bibliotheken müssen eine API (Anwendungsschnittstelle) aufweisen, die zu den installierten Header-Dateien passt. Die normale openSUSE-Umgebung wurde nach diesem Prinzip gestaltet. Bei manuell aktualisierten Bibliotheken müssen Sie diese Probleme selbst lösen.

7.3 Software-Kompilierung auf Doppelarchitektur-Plattformen

Um bei einer Doppelarchitektur Binärdateien für die jeweils andere Architektur zu entwickeln, müssen die entsprechenden Bibliotheken für die zweite Architektur zusätzlich installiert werden. Diese Pakete heißen `rpmname-32bit`. Außerdem benötigen Sie die entsprechenden Header und Bibliotheken aus den `rpmname-devel`-Paketen und die Entwicklungsbibliotheken für die zweite Architektur aus `rpmname-devel-32bit`.

Die meisten Open Source-Programme verwenden eine `autoconf`-basierte Programm-konfiguration. Um mit `autoconf` ein Programm für die zweite Architektur zu konfigurieren, überschreiben Sie die normalen Compiler- und Linker-Einstellungen von `autoconf`, indem Sie das Skript `configure` mit zusätzlichen Umgebungsvariablen ausführen.

Das folgende Beispiel bezieht sich auf ein `x86_64`-System mit `x86` als zweiter Architektur.

- 1 Verwenden Sie den 32-Bit-Compiler:

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

- 2 Weisen Sie den Linker an, 32-Bit-Objekte zu verarbeiten (verwenden Sie stets `gcc` als Linker-Frontend):

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

- 3 Legen Sie den Assembler für die Erstellung von 32-Bit-Objekten fest:

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

- 4 Legen Sie fest, dass die Bibliotheken für `libtool` usw. aus `/usr/lib` stammen sollen:

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

- 5 Legen Sie fest, dass die Bibliotheken im Unterverzeichnis `lib` gespeichert werden sollen:

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

6 Legen Sie fest, dass die 32-Bit-X-Bibliotheken verwendet werden sollen:

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

Nicht alle diese Variablen werden für jedes Programm benötigt. Passen Sie sie an das entsprechende Programm an.

```
CC="gcc -m32" \
LD_FLAGS="-L/usr/lib;" \
    .configure \
        --prefix=/usr \
        --libdir=/usr/lib
make
make install
```

7.4 Kernel-Spezifikationen

Die 64-Bit-Kernels für x86_64 bieten sowohl eine 64-Bit- als auch eine 32-Bit-Kernel-ABI (binäre Anwendungsschnittstelle). Letztere ist mit der ABI für den entsprechenden 32-Bit-Kernel identisch. Das bedeutet, dass die 32-Bit-Anwendung mit dem 64-Bit-Kernel auf die gleiche Weise kommunizieren kann wie mit dem 32-Bit-Kernel.

Die 32-Bit-Emulation der Systemaufrufe für einen 64-Bit-Kernel unterstützt nicht alle APIs, die von Systemprogrammen verwendet werden. Dies hängt von der Plattform ab. Aus diesem Grund muss eine kleine Zahl von Anwendungen, wie beispielsweise `lspci`, kompiliert werden.

Ein 64-Bit-Kernel kann nur 64-Bit-Kernel-Module laden, die speziell für diesen Kernel kompiliert wurden. 32-Bit-Kernel-Module können nicht verwendet werden.

TIPP

Für einige Anwendungen sind separate, Kernel-ladbare Module erforderlich. Wenn Sie vorhaben, eine solche 32-Bit-Anwendung in einer 64-Bit-Systemumgebung zu verwenden, wenden Sie sich an den Anbieter dieser Anwendung und an Novell, um sicherzustellen, dass die 64-Bit-Version des Kernel-ladbaren Moduls und die kompilierte 32-Bit-Version der Kernel-API für dieses Modul verfügbar sind.

Booten und Konfigurieren eines Linux-Systems

8

Das Booten eines Linux-Systems umfasst mehrere unterschiedliche Komponenten. Die Hardware selbst wird vom BIOS initialisiert, das den Kernel mithilfe eines Bootloaders startet. Jetzt wird der Bootvorgang mit `init` und den Runlevels vollständig vom Betriebssystem gesteuert. Mithilfe des Runlevel-Konzepts können Sie Setups für die tägliche Verwendung einrichten und Wartungsaufgaben am System ausführen.

8.1 Der Linux-Bootvorgang

Der Linux-Bootvorgang besteht aus mehreren Phasen, von denen jede einer anderen Komponente entspricht. In der folgenden Liste werden der Bootvorgang und die daran beteiligten Komponenten kurz zusammengefasst.

1. **BIOS** Nach dem Einschalten des Computers initialisiert das BIOS den Bildschirm und die Tastatur und testet den Arbeitsspeicher. Bis zu dieser Phase greift der Computer nicht auf Massenspeichergeräte zu. Anschließend werden Informationen zum aktuellen Datum, zur aktuellen Uhrzeit und zu den wichtigsten Peripheriegeräten aus den CMOS-Werten geladen. Wenn die erste Festplatte und deren Geometrie erkannt wurden, geht die Systemkontrolle vom BIOS an den Bootloader über.
2. **Bootloader** Der erste physische 512 Byte große Datensektor der ersten Festplatte wird in den Arbeitsspeicher geladen und der *Bootloader*, der sich am Anfang dieses Sektors befindet, übernimmt die Steuerung. Die vom Bootloader ausgegebenen Befehle bestimmen den verbleibenden Teil des Bootvorgangs. Aus diesem Grund werden die ersten 512 Byte auf der ersten Festplatte als *Master Boot Record* (MBR)

bezeichnet. Der Bootloader übergibt die Steuerung anschließend an das eigentliche Betriebssystem, in diesem Fall an den Linux-Kernel. Weitere Informationen zu GRUB, dem Linux-Bootloader, finden Sie unter [Kapitel 9, *Der Bootloader*](#) (S. 147).

3. **Kernel und "initramfs"** Um die Systemkontrolle zu übergeben, lädt das Startladeprogramm sowohl den Kernel als auch ein initiales RAM-basiertes Dateisystem (initramfs) in den Arbeitsspeicher. Der Inhalt des initramfs kann vom Kernel direkt verwendet werden. Das initramfs enthält eine kleine Programmdatei namens "init", die das Einhängen des eigentlichen Root-Dateisystems ausführt. Spezielle Hardware-Treiber für den Zugriff auf den Massenspeicher müssen in initramfs vorhanden sein. Weitere Informationen zu initramfs finden Sie unter [Abschnitt 8.1.1, „initramfs“](#) (S. 130).
4. **init on initramfs** Dieses Programm führt alle für das Einhängen des entsprechenden Root-Dateisystems erforderlichen Aktionen aus, z. B. das Bereitstellen der Kernel-Funktionalität für die erforderlichen Dateisystem- und Gerätetreiber der Massenspeicher-Controller mit udev. Nachdem das Root-Dateisystem gefunden wurde, wird es auf Fehler geprüft und eingehängt. Wenn dieser Vorgang erfolgreich abgeschlossen wurde, wird das initramfs bereinigt und das init-Programm wird für das Root-Dateisystem ausgeführt. Weitere Informationen zum init-Programm finden Sie in [Abschnitt 8.1.2, „init on initramfs“](#) (S. 132). Weitere Informationen zu udev finden Sie in [Kapitel 11, *Gerätemanagement über dynamischen Kernel mithilfe von udev*](#) (S. 183).
5. **init** Das init-Programm führt den eigentlichen Boot-Vorgang des Systems über mehrere unterschiedliche Ebenen aus und stellt dabei die unterschiedlichen Funktionalitäten zur Verfügung. Eine Beschreibung des init-Programms finden Sie in [Abschnitt 8.2, „Der init-Vorgang“](#) (S. 133).

8.1.1 initramfs

initramfs ist ein kleines cpio-Archiv, das der Kernel auf einen RAM-Datenträger laden kann. Es stellt eine minimale Linux-Umgebung bereit, die das Ausführen von Programmen ermöglicht, bevor das eigentliche Root-Dateisystem eingehängt wird. Diese minimale Linux-Umgebung wird von BIOS-Routinen in den Arbeitsspeicher geladen und hat, abgesehen von ausreichend Arbeitsspeicher, keine spezifischen Hardware-Anforderungen. initramfs muss immer eine Programmdatei namens "init" zur Verfügung stellen, die das eigentliche init-Programm für das Root-Dateisystem ausführt, damit der Boot-Vorgang fortgesetzt werden kann.

Bevor das Root-Dateisystem eingehängt und das Betriebssystem gestartet werden kann, ist es für den Kernel erforderlich, dass die entsprechenden Treiber auf das Gerät zugreifen, auf dem sich das Root-Dateisystem befindet. Diese Treiber können spezielle Treiber für bestimmte Arten von Festplatten oder sogar Netzwerktreiber für den Zugriff auf ein Netzwerk-Dateisystem umfassen. Die erforderlichen Module für das Root-Dateisystem können mithilfe von `init` oder `initramfs` geladen werden. Nachdem die Module geladen wurden, stellt `udev` das `initramfs` mit den erforderlichen Geräten bereit. Später im Boot-Vorgang, nach dem Ändern des Root-Dateisystems, müssen die Geräte regeneriert werden. Dies erfolgt durch `boot . udev` mit dem Kommando `udevtrigger`.

Wenn in einem installierten System Hardwarekomponenten (z. B. Festplatten) ausgetauscht werden müssen und diese Hardware zur Boot-Zeit andere Treiber im Kernel erfordert, müssen Sie das `initramfs` aktualisieren. Sie gehen hierbei genauso vor, wie bei der Aktualisierung des Vorgängers `initrd`. Rufen Sie `mkinitrd` auf. Durch das Aufrufen von `mkinitrd` ohne Argumente wird ein `initramfs` erstellt. Durch das Aufrufen von `mkinitrd -R` wird ein `initrd` erstellt. In openSUSE® werden die zu ladenden Module durch die Variable `INITRD_MODULES` in `/etc/sysconfig/kernel` angegeben. Nach der Installation wird diese Variable automatisch auf den korrekten Wert eingestellt. Die Module werden genau in der Reihenfolge geladen, in der sie in `INITRD_MODULES` angezeigt werden. Dies ist nur wichtig, wenn Sie sich auf die korrekte Einstellung der Gerätedateien `/dev/sd?` verlassen. In bestehenden Systemen können Sie jedoch auch die Gerätedateien unter `/dev/disk/` verwenden, die in mehreren Unterverzeichnissen angeordnet sind (`by-id`, `by-path` und `by-uuid`) und stets dieselbe Festplatte darstellen. Dies ist auch während der Installation durch Angabe der entsprechenden Einhängeoption möglich.

WICHTIG: Aktualisieren von `initramfs` oder `initrd`

Der Bootloader lädt `initramfs` oder `initrd` auf dieselbe Weise wie den Kernel. Es ist nicht erforderlich, GRUB nach der Aktualisierung von `initramfs` oder `initrd` neu zu installieren, da GRUB beim Booten das Verzeichnis nach der richtigen Datei durchsucht.

8.1.2 init on initramfs

Der Hauptzweck von init unter initramfs ist es, das Einhängen des eigentlichen Root-Dateisystems sowie den Zugriff darauf vorzubereiten. Je nach aktueller Systemkonfiguration ist init für die folgenden Tasks verantwortlich.

Laden der Kernelmodule

Je nach Hardwarekonfiguration sind für den Zugriff auf die Hardwarekomponenten des Computers (vor allem auf die Festplatte) spezielle Treiber erforderlich. Für den Zugriff auf das eigentliche Root-Dateisystem muss der Kernel die entsprechenden Dateisystemtreiber laden.

Bereitstellen von speziellen Blockdateien

Der Kernel generiert Geräteereignisse für alle geladenen Module. udev verarbeitet diese Ereignisse und generiert die erforderlichen blockspezifischen Dateien auf einem RAM-Dateisystem im Verzeichnis `/dev`. Ohne diese speziellen Dateien wäre ein Zugriff auf das Dateisystem und andere Geräte nicht möglich.

Verwalten von RAID- und LVM-Setups

Wenn Ihr System so konfiguriert ist, dass das Root-Dateisystem sich unter RAID oder LVM befindet, richtet init LVM oder RAID so ein, dass der Zugriff auf das Root-Dateisystem zu einem späteren Zeitpunkt erfolgt. Informationen zu RAID finden Sie in [Abschnitt 2.3, „Soft-RAID-Konfiguration“](#) (S. 62). Informationen zu LVM finden Sie in [Abschnitt 2.2, „LVM-Konfiguration“](#) (S. 55).

Verwalten von Netzwerkkonfigurationen

Wenn Ihr System für die Verwendung eines Netzwerk-eingehängten Root-Dateisystems (über NFS eingehängt) konfiguriert ist, muss init sicherstellen, dass die entsprechenden Netzwerktreiber geladen und für den Zugriff auf das Root-Dateisystem eingerichtet werden.

Wenn init im Rahmen des Installationsvorgangs während des anfänglichen Boot-Vorgangs aufgerufen wird, unterscheiden sich seine Tasks von den zuvor beschriebenen:

Suchen des Installationsmediums

Wenn Sie den Installationsvorgang starten, lädt Ihr Computer vom Installationsmedium einen Installationskernel und ein spezielles initrd mit dem YaST-Installationsprogramm. Das YaST-Installationsprogramm, das in einem RAM-Dateisystem ausgeführt wird, benötigt Daten über den Speicherort des Installationsmediums, um auf dieses zugreifen und das Betriebssystem installieren zu können.

Initiieren der Hardware-Erkennung und Laden der entsprechenden Kernelmodule

Wie unter [Abschnitt 8.1.1](#), „*initramfs*“ (S. 130) beschrieben, startet der Boot-Vorgang mit einem Mindestsatz an Treibern, die für die meisten Hardwarekonfigurationen verwendet werden können. *init* startet einen anfänglichen Hardware-Scan-Vorgang, bei dem die für die Hardwarekonfiguration geeigneten Treiber ermittelt werden. Die für den Boot-Vorgang benötigten Namen der Module werden in `INITRD_MODULES` in das Verzeichnis `/etc/sysconfig/kernel` geschrieben. Diese Namen werden verwendet, um ein benutzerdefiniertes *initramfs* zu erstellen, das zum Booten des Systems benötigt wird. Wenn die Module nicht zum Booten, sondern für *coldplug* benötigt werden, werden die Module in `/etc/sysconfig/hardware/hwconfig-*` geschrieben. Alle Geräte, die durch Konfigurationsdateien in diesem Verzeichnis beschrieben werden, werden beim Boot-Vorgang initialisiert.

Laden des Installations- oder Rettungssystems

Sobald die Hardware erfolgreich erkannt und die entsprechenden Treiber geladen wurden und *udev* die speziellen Gerätedateien erstellt hat, startet *init* das Installationssystem, das das eigentliche YaST-Installationsprogramm bzw. das Rettungssystem enthält.

Starten von YaST

init startet schließlich YaST, das wiederum die Paketinstallation und die Systemkonfiguration startet.

8.2 Der *init*-Vorgang

Das Programm *init* ist der Prozess mit der Prozess-ID 1. Es ist für die ordnungsgemäße Initialisierung des Systems verantwortlich. *init* wird direkt vom Kernel gestartet und widersteht dem Signal 9, das in der Regel Prozesse beendet. Alle anderen Programme werden entweder direkt von *init* oder von einem seiner untergeordneten Prozesse gestartet.

init wird zentral in der Datei `/etc/inittab` konfiguriert, in der auch die *Runlevel* definiert werden (siehe [Abschnitt 8.2.1](#), „*Runlevel*“ (S. 134)). Diese Datei legt auch fest, welche Dienste und Dämons in den einzelnen Runlevels verfügbar sind. Je nach den Einträgen in `/etc/inittab` werden von *init* mehrere Skripten ausgeführt. Standardmäßig wird nach dem Booten als erstes Skript `/etc/init.d/boot` gestartet. Nach Abschluss der Systeminitialisierung ändert das System den Runlevel mithilfe des Skripts

`/etc/init.d/rc` auf seinen Standard-Runlevel. Diese Skripten, die der Deutlichkeit halber als *init-Skripten* bezeichnet werden, befinden sich im Verzeichnis `/etc/init.d` (siehe [Abschnitt 8.2.2](#), „Init-Skripten“ (S. 137)).

Der gesamte Vorgang des Startens und Herunterfahrens des Systems wird von `init` verwaltet. Von diesem Gesichtspunkt aus kann der Kernel als Hintergrundprozess betrachtet werden, dessen Aufgabe es ist, alle anderen Prozesse zu verwalten und die CPU-Zeit sowie den Hardwarezugriff entsprechend den Anforderungen anderer Programme anzupassen.

8.2.1 Runlevel

Unter Linux definieren *Runlevel*, wie das System gestartet wird und welche Dienste im laufenden System verfügbar sind. Nach dem Booten startet das System wie in `/etc/inittab` in der Zeile `initdefault` definiert. Dies ist in der Regel die Einstellung 3 oder 5. Weitere Informationen hierzu finden Sie unter [Tabelle 8.1](#), „Verfügbare Runlevel“ (S. 134). Alternativ kann der Runlevel auch zur Boot-Zeit (beispielsweise durch Einfügen der Runlevel-Nummer an der Eingabeaufforderung) angegeben werden. Alle Parameter, die nicht direkt vom Kernel ausgewertet werden können, werden an `init` übergeben. Zum Booten in Runlevel 3 fügen Sie der Boot-Eingabeaufforderung einfach die Ziffer 3 hinzu.

Tabelle 8.1 *Verfügbare Runlevel*

Runlevel	Beschreibung
0	Systemstopp
S or 1	Einzelbenutzer-Modus
2	Lokaler Mehrbenutzer-Modus mit entferntem Netzwerk (NFS usw.)
3	Mehrbenutzer-Vollmodus mit Netzwerk
4	Nicht verwendet

Runlevel	Beschreibung
5	Mehrbenutzer-Vollmodus mit Netzwerk und X-Display-Manager – KDM, GDM oder XDM
6	Systemneustart

WICHTIG: Runlevel 2 mit einer über NFS eingehängten Partition ist zu vermeiden

Sie sollten Runlevel 2 nicht verwenden, wenn Ihr System eine Partition, wie `/usr`, über NFS einhängt. Das System zeigt möglicherweise unerwartetes Verhalten, wenn Programmdateien oder Bibliotheken fehlen, da der NFS-Dienst in Runlevel 2 nicht zur Verfügung steht (lokaler Mehrbenutzer-Modus ohne entferntes Netzwerk).

Um die Runlevel während des laufenden Systembetriebs zu ändern, geben Sie `telinit` und die entsprechende Zahl als Argument ein. Dies darf nur von Systemadministratoren ausgeführt werden. In der folgenden Liste sind die wichtigsten Befehle im Runlevel-Bereich aufgeführt.

`telinit 1` oder `shutdown now`

Das System wechselt in den *Einzelbenutzer-Modus*. Dieser Modus wird für die Systemwartung und administrative Aufgaben verwendet.

`telinit 3`

Alle wichtigen Programme und Dienste (einschließlich Netzwerkprogramme und -dienste) werden gestartet und reguläre Benutzer können sich anmelden und mit dem System ohne grafische Umgebung arbeiten.

`telinit 5`

Die grafische Umgebung wird aktiviert. Normalerweise wird ein Display-Manager, wie XDM, GDM oder KDM, gestartet. Wenn Autologin aktiviert ist, wird der lokale Benutzer beim vorausgewählten Fenster-Manager (GNOME, KDE oder einem anderem Fenster-Manager) angemeldet.

`telinit 0` oder `shutdown -h now`

Das System wird gestoppt.

```
telinit 6 oder shutdown -r now
```

Das System wird gestoppt und anschließend neu gestartet.

Runlevel 5 ist Standard bei allen openSUSE-Standardinstallationen. Die Benutzer werden aufgefordert, sich mit einer grafischen Oberfläche anzumelden, oder der Standardbenutzer wird automatisch angemeldet. Wenn 3 das standardmäßige Runlevel ist, muss das X Window System vorschriftsmäßig konfiguriert werden, bevor der Runlevel auf 5 geändert werden kann. Prüfen Sie anschließend, ob das System wie gewünscht funktioniert, indem Sie `telinit 5` eingeben. Wenn alles ordnungsgemäß funktioniert, können Sie mithilfe von YaST das Standard-Runlevel auf 5 setzen.

WARNUNG: Fehler in /etc/inittab können zu einem fehlerhaften Systemstart führen

Wenn `/etc/inittab` beschädigt ist, kann das System möglicherweise nicht ordnungsgemäß gebootet werden. Daher müssen Sie bei der Bearbeitung von `/etc/inittab` extrem vorsichtig sein. Lassen Sie `init stets /etc/inittab` mit dem Befehl `telinit q` neu lesen, bevor Sie den Rechner neu starten.

Beim Ändern der Runlevel geschehen in der Regel zwei Dinge. Zunächst werden Stopp-Skripten des aktuellen Runlevel gestartet, die einige der für den aktuellen Runlevel wichtigen Programme schließen. Anschließend werden die Start-Skripten des neuen Runlevel gestartet. Dabei werden in den meisten Fällen mehrere Programme gestartet. Beim Wechsel von Runlevel 3 zu 5 wird beispielsweise Folgendes ausgeführt:

1. Der Administrator (`root`) fordert `init` durch die Eingabe des Befehls `telinit 5` auf, zu einem anderen Runlevel zu wechseln.
2. `init` prüft den aktuellen Runlevel (`Runlevel`) und stellt fest, dass `/etc/init.d/rc` mit dem neuen Runlevel als Parameter gestartet werden soll.
3. Jetzt ruft `rc` die Stopp-Skripten des aktuellen Runlevel auf, für die es im neuen Runlevel keine Start-Skripten gibt. In diesem Beispiel sind dies alle Skripten, die sich in `/etc/init.d/rc3.d` (alter Runlevel war 3) befinden und mit einem `K` beginnen. Die Zahl nach `K` gibt die Reihenfolge an, in der die Skripten mit dem Parameter `stop` ausgeführt werden sollen, da einige Abhängigkeiten berücksichtigt werden müssen.
4. Die Start-Skripten des neuen Runlevel werden zuletzt gestartet. In diesem Beispiel befinden sie sich im Verzeichnis `/etc/init.d/rc5.d` und beginnen mit einem

S. Auch hier legt die nach dem S angegebene Zahl die Reihenfolge fest, in der die Skripten gestartet werden sollen.

Bei dem Wechsel in denselben Runlevel wie der aktuelle Runlevel prüft `init` nur `/etc/inittab` auf Änderungen und startet die entsprechenden Schritte, z. B. für das Starten von `getty` auf einer anderen Schnittstelle. Dieselbe Funktion kann durch den Befehl `telinit q` erreicht werden.

8.2.2 Init-Skripten

Im Verzeichnis `/etc/init.d` gibt es zwei Skripttypen:

Skripten, die direkt von `init` ausgeführt werden

Dies ist nur während des Boot-Vorgangs der Fall oder wenn das sofortige Herunterfahren des Systems initiiert wird (Stromausfall oder Drücken der Tastenkombination `Strg + Alt + Entf`). Die Ausführung dieser Skripten ist in `/etc/inittab` definiert.

Skripten, die indirekt von `init` ausgeführt werden

Diese werden beim Wechsel des Runlevels ausgeführt und rufen immer das Master-Skript `/etc/init.d/rc` auf, das die richtige Reihenfolge der relevanten Skripten gewährleistet.

Sämtliche Skripten befinden sich im Verzeichnis `/etc/init.d`. Skripten, die während des Bootens ausgeführt werden, werden über symbolische Links aus `/etc/init.d/boot.d` aufgerufen. Skripten zum Ändern des Runlevels werden jedoch über symbolische Links aus einem der Unterverzeichnisse (`/etc/init.d/rc0.d` bis `/etc/init.d/rc6.d`) aufgerufen. Dies dient lediglich der Übersichtlichkeit und der Vermeidung doppelter Skripten, wenn diese in unterschiedlichen Runleveln verwendet werden. Da jedes Skript sowohl als Start- als auch als Stopp-Skript ausgeführt werden kann, müssen sie die Parameter `start` und `stop` erkennen. Die Skripten erkennen außerdem die Optionen `restart`, `reload`, `force-reload` und `status`. Diese verschiedenen Optionen werden in **Tabelle 8.2, „Mögliche init-Skript-Optionen“** (S. 138) erläutert. Die von `init` direkt ausgeführten Skripten verfügen nicht über diese Links. Sie werden unabhängig vom Runlevel bei Bedarf ausgeführt.

Tabelle 8.2 *Mögliche init-Skript-Optionen*

Option	Beschreibung
<code>start</code>	Startet den Dienst.
<code>stop</code>	Stoppt den Dienst.
<code>restart</code>	Wenn der Dienst läuft, wird er gestoppt und anschließend neu gestartet. Wenn der Dienst nicht läuft, wird er gestartet.
<code>reload</code>	Die Konfiguration wird ohne Stoppen und Neustarten des Dienstes neu geladen.
<code>force-reload</code>	Die Konfiguration wird neu geladen, sofern der Dienst dies unterstützt. Anderenfalls erfolgt dieselbe Aktion wie bei dem Befehl <code>restart</code> .
<code>status</code>	Zeigt den aktuellen Status des Dienstes an.

Mithilfe von Links in den einzelnen Runlevel-spezifischen Unterverzeichnissen können Skripten mit unterschiedlichen Runleveln verknüpft werden. Bei der Installation oder Deinstallation von Paketen werden diese Links mithilfe des Programms "insserv" hinzugefügt oder entfernt (oder mithilfe von `/usr/lib/lsb/install_initd`, ein Skript, das dieses Programm aufruft). Weitere Informationen hierzu finden Sie auf der Manualpage "insserv(8)".

All diese Einstellungen können auch mithilfe des YaST-Moduls geändert werden. Wenn Sie den Status über die Kommandozeile prüfen, verwenden Sie das Werkzeug `chkconfig`, das auf der Manualpage "chkconfig(8)" beschrieben ist.

Im Folgenden finden Sie eine kurze Einführung in die zuerst bzw. zuletzt gestarteten Boot- und Stopp-Skripten sowie eine Erläuterung des Steuerskripten.

`boot`

Werden ausgeführt, wenn das System direkt mit `init` gestartet wird. Es wird unabhängig vom gewählten Runlevel und nur einmalig ausgeführt. Dabei werden die Dateisysteme `/proc` und `/dev/pts` eingehängt und `blogd` (Boot Logging Daemon) wird aktiviert. Wenn das System nach einer Aktualisierung oder einer

Installation das erste Mal gebootet wird, wird die anfängliche Systemkonfiguration gestartet.

Der `blogd`-Daemon ist ein Dienst, der von `boot` und `rc` vor allen anderen Diensten gestartet wird. Er wird beendet, sobald die von diesen Skripten (die eine Reihe von Unterskripten ausführen, beispielsweise um spezielle Blockdateien verfügbar zu machen) ausgelösten Aktionen abgeschlossen sind. `blogd` schreibt alle Bildschirm- ausgaben in die Protokolldatei `/var/log/boot.msg`, jedoch nur wenn `/var` mit Schreib-/Lesezugriff eingehängt ist. Anderenfalls puffert `blogd` alle Bildschirm- daten, bis `/var` zur Verfügung steht. Weitere Informationen zu `blogd` erhalten Sie auf der Manualpage "`blogd(8)`".

Das Skript `boot` ist zudem für das Starten aller Skripten in `/etc/init.d/boot.d` verantwortlich, deren Name mit `S` beginnt. Dort werden die Dateisysteme überprüft und bei Bedarf Loop-Devices konfiguriert. Außerdem wird die Systemzeit festgelegt. Wenn bei der automatischen Prüfung und Reparatur des Dateisystems ein Fehler auftritt, kann der Systemadministrator nach Eingabe des Root-Passworts eingreifen. Zuletzt wird das Skript `boot.local` ausgeführt.

`boot.local`

Hier können Sie zusätzliche Befehle eingeben, die beim Booten ausgeführt werden sollen, bevor Sie zu einem Runlevel wechseln. Dieses Skript ist mit der `AUTOEXEC.BAT` in DOS-Systemen vergleichbar.

`halt`

Dieses Skript wird nur beim Wechsel zu Runlevel 0 oder 6 ausgeführt. Es wird entweder als `halt` oder als `reboot` ausgeführt. Ob das System heruntergefahren oder neu gebootet wird, hängt davon ab, wie `halt` aufgerufen wird. Falls beim Herunterfahren Sonderkommandos benötigt werden, fügen Sie diese dem Skript `halt.local` hinzu.

`rc`

Dieses Skript ruft die entsprechenden Stopp-Skripten des aktuellen Runlevels und die Start-Skripten des neu gewählten Runlevels auf. Wie das Skript `/etc/init.d/boot` wird auch dieses Skript über `/etc/inittab` mit dem gewünschten Runlevel als Parameter aufgerufen.

Sie können Ihre eigenen Skripten erstellen und diese problemlos in das oben beschriebene Schema integrieren. Anweisungen zum Formatieren, Benennen und Organisieren benutzerdefinierter Skripten finden Sie in den Spezifikationen von LSB und auf den

man-Seiten von `init`, `init.d`, `chkconfig` und `insserv`. Weitere Informationen finden Sie zudem auf den man-Seiten zu `startproc` und `killproc`.

WARNUNG: Fehlerhafte init-Skripte können das System stoppen

Bei fehlerhaften `init`-Skripten kann es dazu kommen, dass der Computer hängt. Diese Skripte sollten mit großer Vorsicht bearbeitet werden und, wenn möglich, gründlich in der Mehrbenutzer-Umgebung getestet werden. Einige hilfreiche Informationen zu `init`-Skripten finden Sie in [Abschnitt 8.2.1, „Runlevel“](#) (S. 134).

Sie erstellen ein benutzerdefiniertes `init`-Skript für ein bestimmtes Programm oder einen Dienst, indem Sie die Datei `/etc/init.d/skeleton` als Schablone verwenden. Speichern Sie eine Kopie dieser Datei unter dem neuen Namen und bearbeiten Sie die relevanten Programm- und Dateinamen, Pfade und ggf. weitere Details. Sie können das Skript auch mit eigenen Ergänzungen erweitern, sodass die richtigen Aktionen vom `init`-Prozess ausgelöst werden.

Der Block `INIT INFO` oben ist ein erforderlicher Teil des Skripts und muss bearbeitet werden. Weitere Informationen hierzu finden Sie unter [Beispiel 8.1, „Ein minimaler INIT INFO-Block“](#) (S. 140).

Beispiel 8.1 *Ein minimaler INIT INFO-Block*

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

Geben Sie in der ersten Zeile des `INFO`-Blocks nach `Provides:` den Namen des Programms oder des Dienstes an, das bzw. der mit diesem Skript gesteuert werden soll. Geben Sie in den Zeilen `Required-Start:` und `Required-Stop:` alle Dienste an, die gestartet oder gestoppt werden müssen, bevor der Dienst selbst gestartet oder gestoppt wird. Diese Informationen werden später zum Generieren der Nummerierung der Skriptnamen verwendet, die in den Runlevel-Verzeichnissen enthalten sind. Geben Sie nach `Default-Start:` und `Default-Stop:` die Runlevel an, in denen der Dienst automatisch gestartet oder gestoppt werden soll. Geben Sie für `Description:` schließlich eine kurze Beschreibung des betreffenden Dienstes ein.

Um in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) die Links auf die entsprechenden Skripten in `/etc/init.d/` zu erstellen, geben Sie den Befehl `insserv neuer skriptname` ein. Das Programm "insserv" wertet den `INIT INFO`-Header aus, um die erforderlichen Links für die Start- und Stopp-Skripten in den Runlevel-Verzeichnissen (`/etc/init.d/rc?.d/`) zu erstellen. Das Programm sorgt zudem für die richtige Start- und Stopp-Reihenfolge für die einzelnen Runlevel, indem es die erforderlichen Nummern in die Namen dieser Links aufnimmt. Wenn Sie ein grafisches Werkzeug bevorzugen, um solche Links zu erstellen, verwenden Sie den von YaST zur Verfügung gestellten Runlevel-Editor wie in [Abschnitt 8.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 141) beschrieben.

Wenn ein in `/etc/init.d/` bereits vorhandenes Skript in das vorhandene Runlevel-Schema integriert werden soll, erstellen Sie die Links in den Runlevel-Verzeichnissen direkt mit `insserv` oder indem Sie den entsprechenden Dienst im Runlevel-Editor von YaST aktivieren. Ihre Änderungen werden beim nächsten Neustart wirksam und der neue Dienst wird automatisch gestartet.

Diese Links dürfen nicht manuell festgelegt werden. Wenn der `INFO`-Block Fehler enthält, treten Probleme auf, wenn `insserv` zu einem späteren Zeitpunkt für einen anderen Dienst ausgeführt wird. Der manuell hinzugefügte Dienst wird bei der nächsten Ausführung von `insserv` für dieses Skript entfernt.

8.2.3 Konfigurieren von Systemdiensten (Runlevel) mit YaST

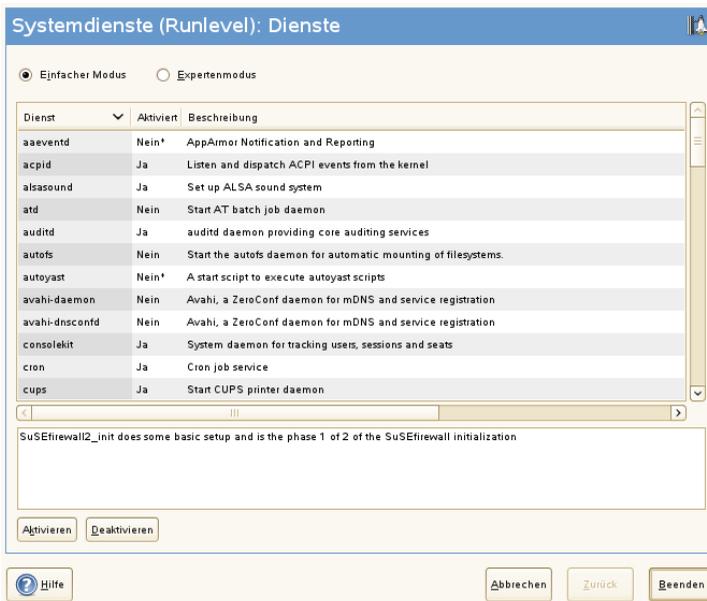
Nach dem Start dieses YaST-Moduls mit `YaST > System > Systemdienste (Runlevel)` werden ein Überblick über alle verfügbaren Dienste sowie der aktuelle Status der einzelnen Dienste (deaktiviert oder aktiviert) angezeigt. Legen Sie fest, ob das Modul im *einfachen Modus* oder im *Expertenmodus* ausgeführt werden soll. Der vorgegebene *einfache Modus* sollte für die meisten Zwecke ausreichend sein. In der linken Spalte wird der Name des Dienstes, in der mittleren Spalte sein aktueller Status und in der rechten Spalte eine kurze Beschreibung angezeigt. Der untere Teil des Fensters enthält eine ausführlichere Beschreibung des ausgewählten Dienstes. Um einen Dienst zu aktivieren, wählen Sie ihn in der Tabelle aus und klicken Sie anschließend auf *Aktivieren*. Führen Sie die gleichen Schritte aus, um einen Dienst zu deaktivieren.

Die detaillierte Steuerung der Runlevel, in denen ein Dienst gestartet oder gestoppt bzw. die Änderung des vorgegebenen Runlevel erfolgt im *Expertenmodus*. Der aktuell

vorgegebene Runlevel oder „initdefault“ (der Runlevel, in den das System standardmäßig bootet) wird oben angezeigt. Das standardmäßige Runlevel eines openSUSE-Systems ist in der Regel Runlevel 5 (Mehrbenutzer-Vollmodus mit Netzwerk und X). Eine geeignete Alternative kann Runlevel 3 sein (Mehrbenutzer-Vollmodus mit Netzwerk).

In diesem YaST-Dialogfeld können Sie ein Runlevel (wie unter **Tabelle 8.1, „Verfügbare Runlevel“** (S. 134) aufgeführt) als neuen Standard wählen. Zudem können Sie mithilfe der Tabelle in diesem Fenster einzelne Dienste und Daemons aktivieren oder deaktivieren. In dieser Tabelle sind die verfügbaren Dienste und Daemons aufgelistet und es wird angezeigt, ob sie aktuell auf dem System aktiviert sind und wenn ja, für welche Runlevel. Nachdem Sie mit der Maus eine der Zeilen ausgewählt haben, klicken Sie auf die Kontrollkästchen, die die Runlevel (*B, 0, 1, 2, 3, 5, 6* und *S*) darstellen, um die Runlevel festzulegen, in denen der ausgewählte Dienst oder Daemon ausgeführt werden sollte. Runlevel 4 ist nicht definiert, um das Erstellen eines benutzerdefinierten Runlevel zu ermöglichen. Unterhalb der Tabelle wird eine kurze Beschreibung des aktuell ausgewählten Dienstes oder Daemons angezeigt.

Abbildung 8.1 Systemdienste (Runlevel)



Legen Sie mit den Optionen "Start", "Anhalten" oder "Aktualisieren" fest, ob ein Dienst aktiviert werden soll. *Status aktualisieren* prüft den aktuellen Status. Mit "Übernehmen"

oder "Zurücksetzen" können Sie wählen, ob die Änderungen für das System angewendet werden sollen, oder ob die ursprünglichen Einstellungen wiederhergestellt werden sollen, die vor dem Starten des Runlevel-Editors wirksam waren. Mit *Verlassen* speichern Sie die geänderten Einstellungen.

WARNUNG: Fehlerhafte Runlevel-Einstellungen können das System beschädigen

Fehlerhafte Runlevel-Einstellungen können ein System unbrauchbar machen. Stellen Sie vor dem Anwenden der Änderungen sicher, dass Sie deren Auswirkungen kennen.

8.3 Systemkonfiguration über `/etc/sysconfig`

Die Hauptkonfiguration von openSUSE wird über die Konfigurationsdateien in `/etc/sysconfig` gesteuert. Die einzelnen Dateien in `/etc/sysconfig` werden nur von den Skripten gelesen, für die sie relevant sind. Dadurch wird gewährleistet, dass Netzwerkeinstellungen beispielsweise nur von netzwerkbezogenen Skripten analysiert werden.

Sie haben zwei Möglichkeiten, die Systemkonfiguration zu bearbeiten. Entweder verwenden Sie den YaST-Editor "sysconfig" oder Sie bearbeiten die Konfigurationsdateien manuell.

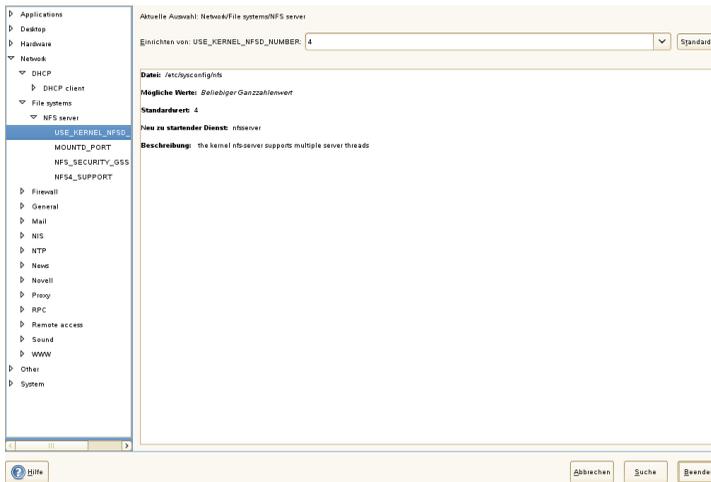
8.3.1 Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"

Der YaST-Editor "sysconfig" bietet ein benutzerfreundliches Frontend für die Systemkonfiguration. Ohne den eigentlichen Speicherort der zu ändernden Konfigurationsvariablen zu kennen, können Sie mithilfe der integrierten Suchfunktion dieses Moduls den Wert der Konfigurationsvariable wie erforderlich ändern. YaST wendet diese Änderungen an, aktualisiert die Konfigurationen, die von den Werten in `sysconfig` abhängig sind, und startet die Dienste neu.

WARNUNG: Das Ändern von `/etc/sysconfig/*`-Dateien kann die Installation beschädigen

Sie sollten die Dateien `/etc/sysconfig`-Dateien nur bearbeiten, wenn Sie über ausreichende Sachkenntnisse verfügen. Das unsachgemäße Bearbeiten dieser Dateien kann zu schwerwiegenden Fehlern des Systems führen. Die Dateien in `/etc/sysconfig` enthalten einen kurzen Kommentar zu den einzelnen Variablen, der erklärt, welche Auswirkungen diese tatsächlich haben.

Abbildung 8.2 Systemkonfiguration mithilfe des `sysconfig`-Editors



Das YaST-Dialogfeld "sysconfig" besteht aus drei Teilen. Auf der linken Seite des Dialogfelds wird eine Baumstruktur aller konfigurierbaren Variablen angezeigt. Wenn Sie eine Variable auswählen, werden auf der rechten Seite sowohl die aktuelle Auswahl als auch die aktuelle Einstellung dieser Variable angezeigt. Unten werden in einem dritten Fenster eine kurze Beschreibung des Zwecks der Variable, mögliche Werte, der Standardwert und die Konfigurationsdatei angezeigt, aus der diese Variable stammt. In diesem Dialogfeld werden zudem Informationen dazu zur Verfügung gestellt, welche Konfigurationsskripte nach dem Ändern der Variable ausgeführt und welche neuen Dienste als Folge dieser Änderung gestartet werden. YaST fordert Sie auf, die Änderungen zu bestätigen und zeigt an, welche Skripte ausgeführt werden, wenn Sie *Verlassen* wählen. Außerdem können Sie die Dienste und Skripte auswählen, die jetzt übersprungen und zu einem späteren Zeitpunkt gestartet werden sollen. YaST wendet

alle Änderungen automatisch an und startet alle von den Änderungen betroffenen Dienste neu, damit die Änderungen wirksam werden.

8.3.2 Manuelles Ändern der Systemkonfiguration

Gehen Sie wie folgt vor, um die Systemkonfiguration manuell zu ändern:

- 1 Melden Sie sich als `root` an.
- 2 Wechseln Sie mit `telinit 1` in den Einzelbenutzer-Modus (Runlevel 1).
- 3 Nehmen Sie die erforderlichen Änderungen an den Konfigurationsdateien in einem Editor Ihrer Wahl vor.

Wenn Sie die Konfigurationsdateien in `/etc/sysconfig` nicht mit YaST ändern, müssen Sie sicherstellen, dass leere Variablenwerte durch zwei Anführungszeichen (`KEYTABLE=""`) gekennzeichnet sind, und Werte, die Leerzeichen enthalten, in Anführungszeichen gesetzt werden. Werte, die nur aus einem Wort bestehen, müssen nicht in Anführungszeichen gesetzt werden.

- 4 Führen Sie `SuSEconfig` aus, um sicherzustellen, dass die Änderungen wirksam werden.
- 5 Mit einem Kommando wie `telinit default_runlevel` stellen Sie den vorherigen Runlevel des Systems wieder her. Ersetzen Sie `default_runlevel` durch den vorgegebenen Runlevel des Systems. Wählen Sie 5, wenn Sie in den Mehrbenutzer-Vollmodus mit Netzwerk und X zurückkehren möchten, oder wählen Sie 3, wenn Sie lieber im Mehrbenutzer-Vollmodus mit Netzwerk arbeiten möchten.

Dieses Verfahren ist hauptsächlich beim Ändern von systemweiten Einstellungen, z. B. der Netzwerkkonfiguration, relevant. Für kleinere Änderungen ist der Wechsel in den Einzelbenutzer-Modus nicht erforderlich. In diesem Modus können Sie jedoch sicherstellen, dass alle von den Änderungen betroffenen Programme ordnungsgemäß neu gestartet werden.

TIPP: Konfigurieren der automatisierten Systemkonfiguration

Um die automatisierte Systemkonfiguration von SuSEconfig zu deaktivieren, setzen Sie die Variable `ENABLE_SUSECONFIG` in `/etc/sysconfig/suseconfig` auf `no`. Wenn Sie den SUSE-Support für die Installation nutzen möchten, darf SuSEconfig nicht deaktiviert werden. Es ist auch möglich, die automatisierte Konfiguration teilweise zu deaktivieren.

Der Bootloader

In diesem Kapitel wird die Konfiguration von GRUB, dem in openSUSE® verwendeten Bootloader, beschrieben. Zum Vornehmen der Einstellungen steht ein spezielles YaST-Modul zur Verfügung. Wenn Sie mit dem Bootvorgang unter Linux nicht vertraut sind, lesen Sie die folgenden Abschnitte, um einige Hintergrundinformationen zu erhalten. In diesem Kapitel werden zudem einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen beschrieben.

Dieses Kapitel konzentriert sich auf das Bootmanagement und die Konfiguration des Bootloaders GRUB. Eine Übersicht über den Bootvorgang finden Sie in [Kapitel 8, *Booten und Konfigurieren eines Linux-Systems*](#) (S. 129). Der Bootloader ist eine Schnittstelle zwischen Computer (BIOS) und Betriebssystem (openSUSE). Die Konfiguration des Bootloaders wirkt sich direkt auf das Starten des Betriebssystems aus.

In diesem Kapitel werden folgende Begriffe regelmäßig verwendet und daher ausführlicher beschrieben:

Master Boot Record

Die Struktur des MBR ist durch eine vom Betriebssystem unabhängige Konvention definiert. Die ersten 446 Byte sind für Programmcode reserviert. Sie enthalten typischerweise einen Teil eines Bootloader-Programms oder eine Betriebssystemauswahl. Die nächsten 64 Byte bieten Platz für eine Partitionstabelle mit bis zu vier Einträgen (siehe [Abschnitt 2.1.1, „Partitionstypen“](#) (S. 47)). Die Partitionstabelle enthält Informationen zur Partitionierung der Festplatte und zu Dateisystemtypen. Das Betriebssystem benötigt diese Tabelle für die Verwaltung der Festplatte. Beim konventionellen generischen Code im MBR muss genau eine Partition als *aktiv* markiert sein. Die letzten beiden Byte müssen eine statische „magische Zahl“

(AA55) enthalten. Ein MBR, der dort einen anderen Wert enthält, wird von einigen BIOS als ungültig und daher nicht zum Booten geeignet angesehen.

Bootsektoren

Bootsektoren sind die jeweils ersten Sektoren der Festplattenpartitionen, außer bei der erweiterten Partition, die nur ein „Container“ für andere Partitionen ist. Diese Bootsektoren reservieren 512 Byte Speicherplatz für Code, der ein auf dieser Partition befindliches Betriebssystem starten kann. Dies gilt für Bootsektoren formatierter DOS-, Windows- oder OS/2-Partitionen, die zusätzlich noch wichtige Basisdaten des Dateisystems enthalten. Im Gegensatz dazu sind Bootsektoren von Linux-Partitionen nach der Einrichtung eines anderen Dateisystems als XFS zunächst leer. Eine Linux-Partition ist daher nicht durch sich selbst bootfähig, auch wenn sie einen Kernel und ein gültiges root-Dateisystem enthält. Ein Bootsektor mit gültigem Code für den Systemstart trägt in den letzten 2 Byte dieselbe "magische" Zahl wie der MBR (AA55).

9.1 Auswählen eines Bootloaders

In openSUSE wird standardmäßig der Bootloader GRUB verwendet. In einigen Fällen und für bestimmte Hardware- und Softwarekonstellationen ist jedoch möglicherweise LILO erforderlich. Wenn Sie ein Update einer älteren openSUSE-Version durchführen, die LILO benutzt, wird auch wieder LILO installiert.

Informationen zur Installation und Konfiguration von LILO finden Sie in der Supportdatenbank unter dem Schlüsselwort LILO und in `/usr/share/doc/packages/lilo`.

9.2 Booten mit GRUB

GRUB (Grand Unified Bootloader) besteht aus zwei Stufen. Die Stufe 1 (stage1) mit 512 Byte erfüllt lediglich die Aufgabe, die zweite Stufe des Bootloaders zu laden. Anschließend wird Stufe 2 (stage2) geladen. Diese Stufe enthält den Hauptteil des Bootloaders.

In einigen Konfigurationen gibt es eine zusätzliche Zwischenstufe 1.5, die Stufe 2 von einem geeigneten Dateisystem lokalisiert und lädt. Wenn diese Methode zur Verfügung

steht, wird sie bei der Installation oder bei der anfänglichen Einrichtung von GRUB mit YaST standardmäßig gewählt.

stage2 kann auf zahlreiche Dateisysteme zugreifen. Derzeit werden Ext2, Ext3, ReiserFS, Minix und das von Windows verwendete DOS FAT-Dateisystem unterstützt. Bis zu einem gewissen Grad werden auch die von BSD-Systemen verwendeten , XFS, UFS und FFS unterstützt. Seit Version 0.95 kann GRUB auch von einer CD oder DVD booten, die das ISO 9660-Standarddateisystem nach der „El Torito“-Spezifikation enthält. GRUB kann noch vor dem Booten auf Dateisysteme unterstützter BIOS-Datenträgerlaufwerke (vom BIOS erkannte Disketten-, Festplatten-, CD- oder DVD-Laufwerke) zugreifen. Daher ist keine Neuinstallation des Bootmanagers nötig, wenn die Konfigurationsdatei von GRUB (`menu.lst`) geändert wird. Beim Booten des Systems liest GRUB die Menüdatei sowie die aktuellen Pfade und Partitionsdaten zum Kernel oder zur Initial RAM-Disk (`initrd`) neu ein und findet diese Dateien selbstständig.

Die eigentliche Konfiguration von GRUB basiert auf den im Folgenden beschriebenen drei Dateien:

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

Diese Datei enthält alle Informationen zu Partitionen oder Betriebssystemen, die mit GRUB gebootet werden können. Wenn diese Angaben nicht zur Verfügung stehen, muss der Benutzer in der GRUB-Kommandozeile das weitere Vorgehen angeben (siehe „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 154)).

```
/boot/grub/device.map
```

Diese Datei übersetzt Gerätenamen aus der GRUB- und BIOS-Notation in Linux-Gerätenamen.

```
/etc/grub.conf
```

Diese Datei enthält die Befehle, Parameter und Optionen, die die GRUB-Shell für das ordnungsgemäße Installieren des Bootloaders benötigt.

GRUB kann auf mehrere Weisen gesteuert werden. Booteinträge aus einer vorhandenen Konfiguration können im grafischen Menü (Eröffnungsbildschirm) ausgewählt werden. Die Konfiguration wird aus der Datei `menu.lst` geladen.

In GRUB können alle Bootparameter vor dem Booten geändert werden. Auf diese Weise können beispielsweise Fehler behoben werden, die beim Bearbeiten der Menüdatei aufgetreten sind. Außerdem können Bootbefehle über eine Art Eingabeaufforderung (siehe „Ändern von Menü-Einträgen während des Bootvorgangs“ (S. 154)) interaktiv

eingegeben werden. GRUB bietet die Möglichkeit, noch vor dem Booten die Position des Kernels und die Position von `initrd` zu ermitteln. Auf diese Weise können Sie auch ein installiertes Betriebssystem booten, für das in der Konfiguration des Bootloaders noch kein Eintrag vorhanden ist.

GRUB ist in zwei Versionen vorhanden: als Bootloader und als normales Linux-Programm in `/usr/sbin/grub`. Dieses Programm wird als *GRUB-Shell* bezeichnet. Es stellt auf dem installierten System eine Emulation von GRUB bereit, die zum Installieren von GRUB oder zum Testen neuer Einstellungen verwendet werden kann. Die Funktionalität, GRUB als Bootloader auf einer Festplatte oder Diskette zu installieren, ist in Form der Befehle `install` und `setup` in GRUB integriert. Diese Befehle sind in der GRUB-Shell verfügbar, wenn Linux geladen ist.

9.2.1 Das GRUB-Bootmenü

Der grafische Eröffnungsbildschirm mit dem Bootmenü basiert auf der GRUB-Konfigurationsdatei `/boot/grub/menu.lst`, die alle Informationen zu allen Partitionen oder Betriebssystemen enthält, die über das Menü gebootet werden können.

Bei jedem Systemstart liest GRUB die Menüdatei vom Dateisystem neu ein. Es besteht also kein Bedarf, GRUB nach jeder Änderung an der Datei neu zu installieren. Mit dem YaST-Bootloader können Sie die GRUB-Konfiguration wie in [Abschnitt 9.3, „Konfigurieren des Bootloaders mit YaST“](#) (S. 158) beschrieben ändern.

Die Menüdatei enthält Befehle. Die Syntax ist sehr einfach. Jede Zeile enthält einen Befehl, gefolgt von optionalen Parametern, die wie bei der Shell durch Leerzeichen getrennt werden. Einige Befehle erlauben aus historischen Gründen ein Gleichheitszeichen (=) vor dem ersten Parameter. Kommentare werden durch ein Rautezeichen (#) eingeleitet.

Zur Erkennung der Menüeinträge in der Menü-Übersicht, müssen Sie für jeden Eintrag einen Namen oder einen `title` vergeben. Der nach dem Schlüsselwort `title` stehende Text wird inklusive Leerzeichen im Menü als auswählbare Option angezeigt. Alle Befehle bis zum nächsten `title` werden nach Auswahl dieses Menüeintrags ausgeführt.

Der einfachste Fall ist die Umleitung zu Bootloadern anderer Betriebssysteme. Der Befehl lautet `chainloader` und das Argument ist normalerweise der Bootblock einer anderen Partition in der Blocknotation von GRUB. Beispiel:

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

Die Gerätenamen in GRUB werden in „**Namenskonventionen für Festplatten und Partitionen**“ (S. 151) beschrieben. Dieses Beispiel spezifiziert den ersten Block der vierten Partition auf der ersten Festplatte.

Mit dem Befehl `kernel` wird ein Kernel-Image angegeben. Das erste Argument ist der Pfad zum Kernel-Image auf einer Partition. Die restlichen Argumente werden dem Kernel in seiner Kommandozeile übergeben.

Wenn der Kernel nicht über die erforderlichen Treiber für den Zugriff auf die root-Partition verfügt oder ein aktuelles Linux-System mit erweiterten Hotplug-Funktionen verwendet wird, muss `initrd` mit einem separaten GRUB-Befehl angegeben werden, dessen einziges Argument der Pfad zur Datei `initrd` ist. Da die Ladeadresse von `initrd` in das geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` auf den Befehl `kernel` folgen.

Der Befehl `root` vereinfacht die Angabe der Kernel- und `initrd`-Dateien. Das einzige Argument von `root` ist ein Gerät oder eine Partition. Allen Kernel-, `initrd`- oder anderen Dateipfaden, für die nicht explizit ein Gerät angegeben ist, wird bis zum nächsten `root`-Befehl das Gerät vorangestellt.

Am Ende jeden Menüeintrags steht implizit der `boot`-Befehl, sodass dieser nicht in die Menüdatei geschrieben werden muss. Wenn Sie GRUB jedoch interaktiv zum Booten verwenden, müssen Sie den `boot`-Befehl am Ende eingeben. Der Befehl selbst hat keine Argumente. Er führt lediglich das geladene Kernel-Image oder den angegebenen Chainloader aus.

Wenn Sie alle Menüeinträge geschrieben haben, müssen Sie einen Eintrag als `default` festlegen. Anderenfalls wird der erste Eintrag (Eintrag 0) verwendet. Sie haben auch die Möglichkeit, ein Zeitlimit in Sekunden anzugeben, nach dem der `default`-Eintrag gebootet wird. `timeout` und `default` werden den Menüeinträgen in der Regel vorangestellt. Eine Beispieldatei finden Sie in „**Beispiel einer Menüdatei**“ (S. 152).

Namenskonventionen für Festplatten und Partitionen

Die von GRUB für Festplatten und Partitionen verwendeten Namenskonventionen unterscheiden sich von denen, die für normale Linux-Geräte verwendet werden. Sie sind der einfachen Plattenummerierung, die das BIOS durchführt, sehr ähnlich und die Syntax gleicht derjenigen, die in manchen BSD-Derivaten verwendet wird. In GRUB beginnt die Nummerierung der Partitionen mit null. Daher ist `(hd0, 0)` die erste Partition auf der ersten Festplatte. Auf einem gewöhnlichen Desktop-Computer, bei dem

eine Festplatte als Primary Master angeschlossen ist, lautet der entsprechende Linux-Gerätename `/dev/sda1`.

Die vier möglichen primären Partitionen haben die Partitionsnummern 0 bis 3. Ab 4 werden die logischen Partitionen hochgezählt:

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

In seiner Abhängigkeit von BIOS-Geräten unterscheidet GRUB nicht zwischen IDE-, SATA-, SCSI- und Hardware RAID-Geräten. Alle Festplatten, die vom BIOS oder anderen Controllern erkannt werden, werden der im BIOS voreingestellten Bootreihenfolge entsprechend nummeriert.

Leider ist eine eindeutige Zuordnung zwischen Linux-Gerätenamen und BIOS-Gerätenamen häufig nicht möglich. Es generiert die Zuordnung mithilfe eines Algorithmus und speichert sie in der Datei `device.map`, in der sie bei Bedarf bearbeitet werden kann. Informationen zur Datei `device.map` finden Sie in [Abschnitt 9.2.2, „Die Datei `device.map`“](#) (S. 155).

Ein vollständiger GRUB-Pfad besteht aus einem Gerätenamen, der in Klammern geschrieben wird, und dem Pfad der Datei im Dateisystem auf der angegebenen Partition. Der Pfad beginnt mit einem Schrägstrich. Auf einem System mit einer einzelnen IDE-Festplatte und Linux auf der ersten Partition könnte der bootbare Kernel beispielsweise wie folgt spezifiziert werden:

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

Beispiel einer Menüdatei

Das folgende Beispiel zeigt die Struktur einer GRUB-Menüdatei. Diese Beispiel-Installation beinhaltet eine Linux-Bootpartition unter `/dev/sda5`, eine Root-Partition unter `/dev/sda7` und eine Windows-Installation unter `/dev/sda1`.

```
gfxmenu (hd0,4)/boot/message
color white/blue black/light-gray
default 0
timeout 8

title linux
    root (hd0,4)
```

```

kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
initrd /boot/initrd

title windows
rootnoverify (hd0,4)
chainloader(hd0,0)+1

title floppy
rootnoverify (hd0,4)
chainloader(fd0)+1

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

```

Der erste Block definiert die Konfiguration des Eröffnungsbildschirms:

`gfxmenu (hd0,4)/message`

Das Hintergrundbild `message` befindet sich im Verzeichnis der obersten Ebene der Partition `/dev/sda5`.

`color white/blue black/light-gray`

Farbschema: `white` (Vordergrund), `blue` (Hintergrund), `black` (Auswahl) und `light gray` (Hintergrund der Markierung). Das Farbschema wirkt sich nicht auf den Eröffnungsbildschirm, sondern nur auf das anpassbare GRUB-Menü aus, auf das Sie zugreifen können, wenn Sie den Eröffnungsbildschirm mit `Esc` beenden.

`default 0`

Der erste Menüeintrag `title linux` soll standardmäßig gebootet werden.

`timeout 8`

Nach acht Sekunden ohne Benutzereingabe bootet GRUB den Standardeintrag automatisch. Um das automatische Booten zu deaktivieren, löschen Sie die Zeile `timeout`. Wenn Sie `timeout 0` einstellen, bootet GRUB den Standardeintrag sofort.

Im zweiten und größten Block sind die verschiedenen bootbaren Betriebssysteme aufgelistet. Die Abschnitte für die einzelnen Betriebssysteme werden durch `title` eingeleitet.

- Der erste Eintrag (`title linux`) ist für das Booten von openSUSE verantwortlich. Der Kernel (`vmlinuz`) befindet sich in der ersten logischen Partition (die

Bootpartition) der ersten Festplatte. Hier werden Kernel-Parameter, z. B. die Root-Partition und der VGA-Modus, angehängt. Die Angabe der root-Partition erfolgt nach der Linux-Namenskonvention (`/dev/sda7/`), da diese Information für den Kernel bestimmt ist und nichts mit GRUB zu tun hat. Die `initrd` befindet sich ebenfalls in der ersten logischen Partition der ersten Festplatte.

- Der zweite Eintrag ist für das Laden von Windows verantwortlich. Windows wird von der ersten Partition der ersten Festplatte aus gebootet (`hd0, 0`). Mit `chainloader +1` wird das Auslesen und Ausführen des ersten Sektors der angegebenen Partition gesteuert.
- Der nächste Eintrag dient dazu, das Booten von Diskette zu ermöglichen, ohne dass dazu die BIOS-Einstellungen geändert werden müssten.
- Die Bootoption `failsafe` dient dazu, Linux mit einer bestimmten Auswahl an Kernel-Parametern zu starten, die selbst auf problematischen Systemen ein Hochfahren von Linux ermöglichen.

Die Menüdatei kann jederzeit geändert werden. GRUB verwendet die geänderten Einstellungen anschließend für den nächsten Bootvorgang. Sie können diese Datei mit dem Editor Ihrer Wahl oder mit YaST editieren und dauerhaft speichern. Alternativ können Sie temporäre Änderungen interaktiv über die Bearbeitungsfunktion von GRUB vornehmen. Weitere Informationen hierzu finden Sie unter „**Ändern von Menü-Einträgen während des Bootvorgangs**“ (S. 154).

Ändern von Menü-Einträgen während des Bootvorgangs

Wählen Sie im grafischen Bootmenü das zu bootende Betriebssystem mit den Pfeiltasten aus. Wenn Sie ein Linux-System wählen, können Sie an der Booteingabeaufforderung zusätzliche Bootparameter eingeben. Um einzelne Menüeinträge direkt zu bearbeiten, drücken Sie die Esc-Taste. Der Eröffnungsbildschirm wird geschlossen und das textbasierte GRUB-Menü aufgerufen. Drücken Sie anschließend die Taste E. Auf diese Weise vorgenommene Änderungen gelten nur für den aktuellen Bootvorgang und können nicht dauerhaft übernommen werden.

WICHTIG: Tastaturbelegung während des Bootvorgangs

Beim Bootvorgang ist nur die amerikanische Tastaturbelegung verfügbar.

Durch die Möglichkeit, die Menüeinträge zu bearbeiten, kann ein defektes System, das nicht mehr gebootet werden kann, repariert werden, da die fehlerhafte Konfigurationsdatei des Bootloaders mittels der manuellen Eingabe von Parametern umgangen werden kann. Die manuelle Eingabe vom Parametern während des Bootvorgangs ist zudem hilfreich zum Testen neuer Einstellungen, ohne dass diese sich auf das native System auswirken.

Aktivieren Sie den Bearbeitungsmodus und wählen Sie mithilfe der Pfeiltasten den Menüeintrag aus, dessen Konfiguration sie ändern möchten. Um die Konfiguration zu bearbeiten, drücken Sie die Taste E erneut. Auf diese Weise korrigieren Sie falsche Partitions- oder Pfadangaben, bevor sich diese negativ auf den Bootvorgang auswirken. Drücken Sie die Eingabetaste, um den Bearbeitungsmodus zu verlassen und zum Menü zurückzukehren. Drücken Sie anschließend die Taste B, um diesen Eintrag zu booten. Im Hilfetext am unteren Rand werden weitere mögliche Aktionen angezeigt.

Um die geänderten Bootoptionen dauerhaft zu übernehmen und an den Kernel zu übergeben, öffnen Sie die Datei `menu.lst` als Benutzer `root` und hängen Sie die entsprechenden Kernel-Parameter an folgende vorhandene Zeile getrennt durch Leerzeichen an:

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

GRUB übernimmt den neuen Parameter beim nächsten Booten automatisch. Alternativ können Sie diese Änderung auch mit dem YaST-Bootloader-Modul vornehmen. Hängen Sie die neuen Parameter getrennt durch Leerzeichen an die vorhandene Zeile an.

9.2.2 Die Datei "device.map"

Die Datei `device.map` enthält Zuordnungen zwischen den GRUB- und BIOS-Gerätenamen und den Linux-Gerätenamen. In einem Mischsystem aus IDE- und SCSI-Festplatten muss GRUB anhand eines bestimmten Verfahrens versuchen, die Bootreihenfolge zu ermitteln, da die BIOS-Informationen zur Bootreihenfolge für GRUB unter Umständen nicht zugänglich sind. GRUB speichert das Ergebnis dieser Analyse in der Datei `/boot/grub/device.map`. Auf einem System, für das IDE vor SCSI gebootet werden soll, kann die Datei `device.map` beispielsweise wie folgt aussehen:

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

Da die Reihenfolge von IDE, SCSI und anderen Festplatten abhängig von verschiedenen Faktoren ist und Linux die Zuordnung nicht erkennen kann, besteht die Möglichkeit, die Reihenfolge in der Datei `device.map` manuell festzulegen. Wenn beim Booten Probleme auftreten sollten, prüfen Sie, ob die Reihenfolge in dieser Datei der BIOS-Reihenfolge entspricht, und ändern Sie sie notfalls temporär mithilfe der GRUB-Eingabeaufforderung. Sobald das Linux-System gebootet ist, können Sie die Datei `device.map` mithilfe des YaST-Bootloader-Moduls oder eines Editors Ihrer Wahl dauerhaft bearbeiten.

Installieren Sie nach der manuellen Bearbeitung von `device.map` GRUB über den folgenden Befehl erneut. Dieser Befehl führt dazu, dass die Datei `device.map` neu geladen wird und die in `grub.conf` aufgelisteten Befehle ausgeführt werden:

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

9.2.3 Die Datei `"/etc/grub.conf"`

Nach `menu.lst` und `device.map` ist `/etc/grub.conf` die drittwichtigste Konfigurationsdatei von GRUB. Diese Datei enthält die Befehle, Parameter und Optionen, die die GRUB-Shell für das ordnungsgemäße Installieren des Bootloaders benötigt.

```
root (hd0,4)
    install /grub/stage1 (hd0,3) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
quit
```

Bedeutung der einzelnen Einträge:

`root (hd0,4)`

Mit diesem Befehl wird GRUB angewiesen, folgende Befehle auf die erste logische Partition der ersten Festplatte anzuwenden. Dort befinden sich die Bootdateien.

`install` Parameter

Führen Sie den Befehl `grub` mit dem Parameter `install` aus. Installieren Sie `stage1` des Bootloaders im erweiterten Partitionscontainer (`/grub/stage1 (hd0,3)`). Dies ist eine etwas "alternative" Konfiguration, die jedoch meist funktioniert. `stage2` muss in die Speicheradresse `0x8000` (`/grub/stage2 0x8000`) geladen werden. Der letzte Eintrag (`(hd0,4)/grub/menu.lst`) zeigt GRUB, wo sich die Menüdatei befindet.

9.2.4 Festlegen eines Bootpassworts

Schon vor dem Booten des Betriebssystems ermöglicht GRUB den Zugriff auf Dateisysteme. Dies bedeutet, dass Benutzer ohne root-Berechtigungen auf Dateien des Linux-Systems zugreifen können, auf die sie nach dem Booten keinen Zugriff haben. Um diese Zugriffe oder das Booten bestimmter Betriebssysteme zu verhindern, können Sie ein Bootpasswort festlegen.

WICHTIG: Bootpasswort und Eröffnungsbildschirm

Wenn Sie für GRUB ein Bootpasswort verwenden, wird der übliche Eröffnungsbildschirm nicht angezeigt.

Legen Sie als Benutzer `root` das Bootpasswort wie folgt fest:

- 1 Verschlüsseln Sie an der `root`-Eingabeaufforderung das Passwort mit Hilfe von `grub-md5-crypt`:

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

- 2 Fügen Sie die verschlüsselte Zeichenkette in den globalen Abschnitt der Datei `menu.lst` ein:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

Jetzt können GRUB-Befehle in der Booteingabeaufforderung nur ausgeführt werden, wenn die Taste `P` gedrückt und das Passwort eingegeben wurde. Benutzer können jedoch über das Bootmenü weiterhin alle Betriebssysteme booten.

- 3 Um zu verhindern, dass ein oder mehrere Betriebssysteme über das Bootmenü gebootet werden, fügen Sie den Eintrag `lock` zu allen Abschnitten in `menu.lst` hinzu, die ohne Eingabe eines Passworts nicht gebootet werden sollen.
Beispiel:

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

```
initrd (hd0,4)/initrd
lock
```

Nach dem Neubooten des Systems und der Auswahl des Linux-Eintrags im Bootmenü erscheint zunächst folgende Fehlermeldung:

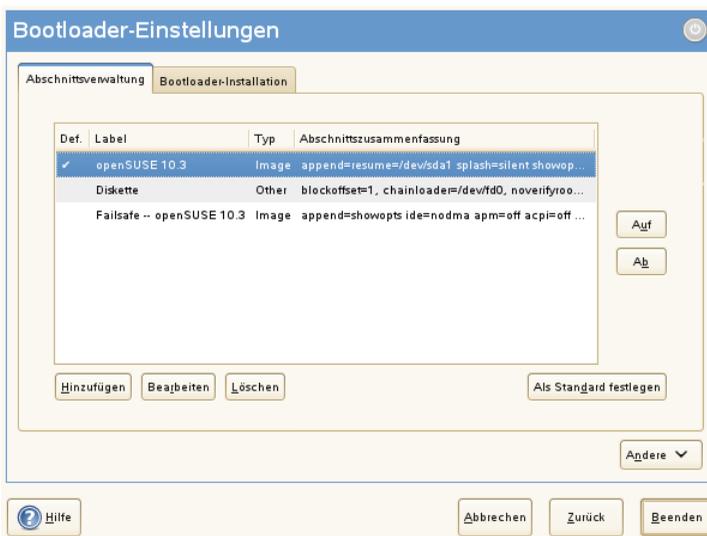
```
Error 32: Must be authenticated
```

Drücken Sie die Eingabetaste, um das Menü zu öffnen. Drücken Sie anschließend die Taste P, um die Eingabeaufforderung für das Passwort zu öffnen. Wenn Sie das Passwort eingegeben und die Eingabetaste gedrückt haben, sollte das ausgewählte Betriebssystem (in diesem Fall Linux) gebootet werden.

9.3 Konfigurieren des Bootloaders mit YaST

Mit dem YaST-Modul ist die Konfiguration des Bootloaders auf Ihrem openSUSE-System am einfachsten. Wählen Sie im YaST-Kontrollzentrum *System > Bootloader*. Wie in [Abbildung 9.1](#), „**Bootloader-Einstellungen**“ (S. 158) zeigt dies die aktuelle Bootloader-Konfiguration des Systems und ermöglicht Ihnen, Änderungen vorzunehmen.

Abbildung 9.1 Bootloader-Einstellungen



Auf dem Karteireiter *Abschnittsverwaltung* können Sie die Bootloader-Abschnitte für die einzelnen Betriebssysteme bearbeiten, ändern und löschen. Klicken Sie auf *Hinzufügen*, um eine Option hinzuzufügen. Wenn Sie den Wert einer bestehenden Option ändern möchten, wählen Sie ihn mit der Maus aus und klicken Sie auf *Bearbeiten*. Um ein vorhandenes Schema zu löschen, wählen Sie das Schema aus und klicken Sie auf *Löschen*. Wenn Sie nicht mit den Bootloader-Optionen vertraut sind, lesen Sie zunächst [Abschnitt 9.2, „Booten mit GRUB“](#) (S. 148).

Verwenden Sie die Karteireiter *Bootloader-Installation*, um die Einstellungen in Bezug auf Typ, Speicherort und erweiterte Bootloader-Einstellungen anzuzeigen und zu ändern.

Erweiterte Konfigurationsoptionen erhalten Sie im Dropdown-Menü der Option *Andere*. Über den integrierten Editor können Sie die GRUB-Konfigurationsdateien ändern (Einzelheiten finden Sie unter [Abschnitt 9.2, „Booten mit GRUB“](#) (S. 148)). Sie können die vorhandene Konfiguration auch löschen und eine *neue Konfiguration ohne Vorschlag erstellen* oder sich von YaST *eine neue Konfiguration vorschlagen lassen*. Sie können die Konfiguration auch auf die Festplatte schreiben und sie von der Festplatte wieder einlesen. Zur Wiederherstellung des ursprünglichen, während der Installation gespeicherten MBR (Master Boot Record) wählen Sie *MBR von Festplatte wiederherstellen* aus.

9.3.1 Bootloader-Typ

Legen Sie den Bootloader-Typ unter *Bootloader-Installation* fest. In openSUSE wird standardmäßig der Bootloader GRUB verwendet. Gehen Sie wie folgt vor, wenn Sie LILO verwenden möchten:

Prozedur 9.1 *Ändern des Bootloader-Typs*

- 1 Wählen Sie die Karteireiter *Bootloader-Installation*.
- 2 Wählen Sie unter *Bootloader* die Option *LILO*.
- 3 Wählen Sie in dem sich öffnenden Dialogfeld folgende Aktionen aus:

- Neue Konfiguration vorschlagen
- Lässt YaST eine neue Konfiguration erstellen.

Aktuelle Konfiguration konvertieren

Lässt YaST die aktuelle Konfiguration konvertieren. Es ist möglich, dass beim Konvertieren der Konfiguration einige Einstellungen verloren gehen.

Neue Konfiguration ohne Vorschlag erstellen

Erstellt eine benutzerdefinierte Konfiguration. Diese Aktion ist während der Installation von openSUSE nicht verfügbar.

Auf Festplatte gespeicherte Konfiguration einlesen

Lädt Ihre eigene Datei `/etc/lilo.conf`. Diese Aktion ist während der Installation von openSUSE nicht verfügbar.

4 Klicken Sie zum Speichern der Änderungen auf *OK*

5 Klicken Sie im Hauptdialogfeld auf *Verlassen*, um die Änderungen zu übernehmen.

Während der Konvertierung wird die alte GRUB-Konfiguration gespeichert. Wenn Sie sie verwenden möchten, ändern Sie einfach den Bootloader-Typ zurück in GRUB und wählen Sie *Vor der Konvertierung gespeicherte Konfiguration wiederherstellen*. Diese Aktion ist nur auf einem installierten System verfügbar.

ANMERKUNG: Benutzerdefinierter Bootloader

Wenn Sie einen anderen Bootloader als GRUB oder LILO verwenden möchten, wählen Sie *Keinen Bootloader installieren*. Lesen Sie die Dokumentation Ihres Bootloaders sorgfältig durch, bevor Sie diese Option auswählen.

9.3.2 Speicherort des Bootloaders

Um den Speicherort des Bootloaders zu ändern, gehen Sie wie folgt vor:

Prozedur 9.2 *Speicherort des Bootloaders ändern*

1 Wählen Sie die Karteireiter *Bootloader-Installation* und anschließend eine der folgenden Optionen für *Speicherort des Bootloaders*:

Booten von der Bootpartition

Der Bootsektor der Partition `/boot`.

Booten von der erweiterten Partition

Der Bootloader wird in den Container der erweiterten Partition installiert.

Booten vom Master Boot Record

Der Bootloader wird in den MBR des ersten Laufwerks installiert (entsprechend der im BIOS voreingestellten Bootreihenfolge).

Booten von der root-Partition

Der Bootloader wird in den Bootsektor der Partition // installiert.

Benutzerdefinierte Bootpartition

Mit dieser Option können Sie den Speicherort des Bootloaders manuell angeben.

2 Klicken Sie zum Anwenden der Einstellungen auf *Verlassen*.

9.3.3 Standardsystem

Um das System zu ändern, das standardmäßig gebootet wird, gehen Sie wie folgt vor:

Prozedur 9.3 *Standardsystem einrichten*

- 1 Öffnen Sie die Karteireiter *Abschnittsverwaltung*.
- 2 Wählen Sie den gewünschten Eintrag in der Liste aus.
- 3 Klicken Sie auf *Als Standard festlegen*.
- 4 Klicken Sie auf *Verlassen*, um die Änderungen zu aktivieren.

9.3.4 Zeitlimit des Bootloaders

Der Bootloader bootet das Standardsystem nicht sofort. Während des Zeitlimits können Sie das zu bootende System auswählen oder einige Kernel-Parameter schreiben. Gehen Sie wie folgt vor, um das Zeitlimit des Bootloaders festzulegen:

Prozedur 9.4 *Ändern des Bootloader-Zeitlimits*

- 1 Öffnen Sie die Karteireiter *Bootloader-Installation*.
- 2 Klicken Sie auf *Bootloader-Optionen*.
- 3 Ändern Sie den Wert für *Zeitüberschreitung in Sekunden*, indem Sie einen neuen Wert eingeben, mit der Maus auf den entsprechenden Pfeil klicken oder die Pfeiltasten der Tastatur verwenden.
- 4 Klicken Sie auf *OK*.
- 5 Klicken Sie auf *Verlassen*, um die Änderungen zu speichern.

9.3.5 Sicherheitseinstellungen

Mit diesem YaST-Modul können Sie zum Schutz des Bootvorgangs auch ein Passwort einrichten. Damit wird ein zusätzlicher Grad an Sicherheit geboten.

Prozedur 9.5 *Festlegen eines Bootloader-Passworts*

- 1 Öffnen Sie die Karteireiter *Bootloader-Installation*.
- 2 Klicken Sie auf *Bootloader-Optionen*.
- 3 Geben Sie in *Passwort für die Menüschnittstelle* Ihr Passwort an.
- 4 Klicken Sie auf *OK*.
- 5 Klicken Sie auf *Verlassen*, um die Änderungen zu speichern.

9.4 Deinstallieren des Linux-Bootloaders

Mit YaST können Sie den Linux-Bootloader deinstallieren und den Zustand des MBR vor der Installation wiederherstellen. YaST erstellt während der Installation automatisch ein Backup der ursprünglichen MBR-Version und stellt sie bei Bedarf wieder her.

Um GRUB zu deinstallieren, starten Sie das YaST-Bootloader-Modul (*System > Bootloader*). Wählen Sie *Andere > MBR von Festplatte wiederherstellen* aus und bestätigen Sie mit *Yes, Rewrite*.

9.5 Erstellen von Boot-CDs

Wenn beim Booten Ihres Systems unter Verwendung eines Bootmanagers Probleme auftreten oder wenn der Bootmanager auf dem MBR Ihrer Festplatte oder einer Diskette nicht installiert werden kann, ist es auch möglich, eine bootfähige CD mit all den für Linux erforderlichen Startdateien zu erstellen. Hierfür muss ein CD-Brenner in Ihrem System installiert sein.

Für die Erstellung einer bootfähigen CD-ROM mit GRUB ist lediglich eine spezielle Form von *stage2* mit Namen *stage2_eltorito* erforderlich sowie optional eine benutzerdefinierte Datei *menu.lst*. Die klassischen Dateien *stage1* und *stage2* sind nicht erforderlich.

Prozedur 9.6 Erstellen von Boot-CDs

1 Wechseln Sie in ein Verzeichnis, in dem das ISO-Image erstellt werden soll, beispielsweise: `cd /tmp`

2 Erstellen Sie ein Unterverzeichnis für GRUB:

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

3 Kopieren Sie den Kernel, die Dateien *stage2_eltorito*, *initrd*, *menu.lst* und */message* nach *iso/boot/*:

```
cp /boot/vmlinuz iso/boot/  
cp /boot/initrd iso/boot/  
cp /boot/message iso/boot/
```

```
cp /usr/lib/grub/stage2_eltorito iso/boot/grub
cp /boot/grub/menu.lst iso/boot/grub
```

- 4 Passen Sie die Pfadeinträge in `iso/boot/grub/menu.lst` so an, dass sie auf ein CD-ROM-Laufwerk verweisen. Ersetzen Sie hierfür in den Pfadnamen den Gerätenamen der Festplatten, die im Format `(hdx, y)` aufgeführt sind, mit dem Gerätenamen des CD-ROM-Laufwerks, das mit `(cd)` angegeben wird. Sie müssen unter Umständen auch den Pfad zum Kernel und zur `initrd`-Datei anpassen, sodass sie auf `/boot/vmlinuz` und `boot/initrd` verweisen. Nachdem Sie die Anpassungen durchgeführt haben, sollte `menu.lst` wie im folgenden Beispiel aussehen:

```
timeout 8
default 0
gfxmenu (cd)/boot/message

title Linux
    root (cd)
    kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
    splash=verbose showopts
    initrd /boot/initrd
```

Verwenden Sie `splash=silent` anstelle von `splash=verbose`, um zu vermeiden, dass beim Bootvorgang Bootmeldungen angezeigt werden.

- 5 Erstellen Sie das ISO-Image mit dem folgenden Befehl:

```
mkisofs -R -b iso/boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso /tmp/iso
```

- 6 Schreiben Sie die so erstellte Datei namens `grub.iso` unter Verwendung Ihres bevorzugten Dienstprogramms auf eine CD. Brennen Sie das ISO-Image nicht als Datendatei, sondern verwenden Sie die Option zum Brennen eines CD-Images, die in Ihrem Dienstprogramm angeboten wird.

9.6 Der grafische SUSE-Bildschirm

Der grafische SUSE-Bildschirm wird auf der ersten Konsole angezeigt, wenn die Option `vga=<Wert>` als Kernel-Parameter verwendet wird. Bei der Installation mit YaST wird diese Option automatisch in Abhängigkeit von der gewählten Auflösung und der verwendeten Grafikkarte aktiviert. Sie haben bei Bedarf drei Möglichkeiten, den SUSE-Bildschirm zu deaktivieren:

Den SUSE-Bildschirm bei Bedarf deaktivieren

Geben Sie den Befehl `echo 0 >/proc/splash` in der Kommandozeile ein, um den grafischen Bildschirm zu deaktivieren. Um ihn wieder zu aktivieren, geben Sie den Befehl `echo 1 >/proc/splash` ein.

Den SUSE-Bildschirm standardmäßig deaktivieren

Fügen Sie der Bootloader-Konfiguration den Kernel-Parameter `splash=0` hinzu. Weitere Informationen hierzu finden Sie in [Kapitel 9, *Der Bootloader*](#) (S. 147). Wenn Sie jedoch den Textmodus wie in früheren Versionen bevorzugen, legen Sie Folgendes fest: `vga=normal`.

Den SUSE-Bildschirm vollständig deaktivieren

Kompilieren Sie einen neuen Kernel und deaktivieren Sie die Option zum *Verwenden des Eröffnungsbildschirms anstelle des Bootlogos im Menü Framebuffer-Unterstützung*.

TIPP

Wenn Sie im Kernel die Framebuffer-Unterstützung deaktiviert haben, ist der Eröffnungsbildschirm automatisch auch deaktiviert. Wenn Sie einen eigenen Kernel kompilieren, kann SUSE dafür keinen Support garantieren.

9.7 Fehlersuche

In diesem Abschnitt werden einige der Probleme, die beim Booten mit GRUB auftreten können, sowie deren Lösungen behandelt. Einige der Probleme werden in den Artikeln in der Support-Datenbank unter <http://en.opensuse.org/SDB:SDB> beschrieben. Verwenden Sie das Dialogfeld "Suche", um nach Schlüsselwörtern wie *GRUB*, *boot* und *Bootloader* zu suchen.

GRUB und XFS

XFS lässt im Partitions-Bootblock keinen Platz für `stage1`. Sie dürfen also als Speicherort des Bootloaders keinesfalls eine XFS-Partition angeben. Um dieses Problem zu beheben, erstellen Sie eine separate Bootpartition, die nicht mit XFS formatiert ist.

GRUB meldet GRUB Geom Error

GRUB überprüft die Geometrie der angeschlossenen Festplatten beim Booten des Systems. In seltenen Fällen macht das BIOS hier inkonsistente Angaben, sodass GRUB einen "GRUB Geom Error" meldet. Verwenden Sie in solchen Fällen LILO oder aktualisieren Sie ggf. das BIOS. Detaillierte Informationen zur Installation, Konfiguration und Wartung von LILO finden Sie in der Support-Datenbank unter dem Stichwort LILO.

GRUB gibt diese Fehlermeldung auch aus, wenn Linux auf einer zusätzlichen Festplatte im System installiert wurde, diese aber nicht im BIOS registriert ist. Der erste Teil des Bootloaders *stage1* wird korrekt gefunden und geladen, die zweite Stufe *stage2* wird jedoch nicht gefunden. Dieses Problem können Sie umgehen, indem Sie die neue Festplatte unverzüglich im BIOS registrieren.

System, das IDE- und SCSI-Festplatten enthält, bootet nicht

Möglicherweise wurde die Bootsequenz der Festplatten während der Installation von YaST falsch ermittelt. So erkennt GRUB die IDE-Festplatte unter Umständen als `hd0` und die SCSI-Festplatte als `hd1`, obwohl im BIOS die umgekehrte Reihenfolge (SCSI *vor* IDE) angegeben ist.

Korrigieren Sie in solchen Fällen mithilfe der GRUB-Kommandozeile beim Booten die verwendeten Festplatten. Bearbeiten Sie im gebooteten System die Datei `device.map`, um die neue Zuordnung dauerhaft festzulegen. Überprüfen Sie anschließend die GRUB-Gerätenamen in den Dateien `/boot/grub/menu.lst` und `/boot/grub/device.map` und installieren Sie den Bootloader mit dem folgenden Befehl neu:

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

Windows von der zweiten Festplatte booten

Einige Betriebssysteme, z. B. Windows, können nur von der ersten Festplatte gebootet werden. Wenn ein solches Betriebssystem auf einer anderen als der ersten Festplatte installiert ist, können Sie für den entsprechenden Menüeintrag einen logischen Tausch veranlassen.

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

In diesem Beispiel soll Windows von der zweiten Festplatte gestartet werden. Zu diesem Zweck wird die logische Reihenfolge der Festplatten mit `map` getauscht. Die Logik innerhalb der GRUB-Menüdatei ändert sich dadurch jedoch nicht. Daher müssen Sie bei `chainloader` nach wie vor die zweite Festplatte angeben.

9.8 Weiterführende Informationen

Umfassende Informationen zu GRUB finden Sie auf der Webseite unter <http://www.gnu.org/software/grub/>. Ausführliche Informationen finden Sie auch auf der Infoseite für den Befehl `grub`. Um weitere Informationen zu bestimmten Themen zu erhalten, können Sie auch „SDB: GRUB“ als Suchwort in der Supportdatenbank unter <http://www.opensuse.org/> eingeben.

Spezielle Systemfunktionen

In diesem Kapitel erhalten Sie zunächst Informationen zu den verschiedenen Softwarepaketen, zu den Virtuellen Konsolen und zur Tastaturbelegung. Hier finden Sie Hinweise zu Software-Komponenten, wie `bash`, `cron` und `logrotate`, da diese im Laufe der letzten Veröffentlichungszyklen geändert oder verbessert wurden. Selbst wenn sie nur klein sind oder als nicht besonders wichtig eingestuft werden, können die Benutzer ihr Standardverhalten ändern, da diese Komponenten häufig eng mit dem System verbunden sind. Das Kapitel endet mit einem Abschnitt mit sprach- und landesspezifischen Einstellungen (`I18N` und `L10N`).

10.1 Informationen zu speziellen Softwarepaketen

Die Programme `bash`, `cron`, `logrotate`, `locate`, `ulimit` und `free` sowie die Datei `resolv.conf` spielen für Systemadministratoren und viele Benutzer eine wichtige Rolle. `man`-Seiten und `info`-Seiten sind hilfreiche Informationsquellen zu Befehlen, sind jedoch nicht immer verfügbar. GNU Emacs ist ein beliebter konfigurierbarer Texteditor.

10.1.1 Das Paket `bash` und `/etc/profile`

`Bash` ist die Standard-System-Shell. Wenn sie als Anmelde-Shell verwendet wird, werden mehrere Initialisierungsdateien gelesen. `Bash` verarbeitet die entsprechenden Informationen in der Reihenfolge dieser Liste:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Nehmen Sie benutzerdefinierte Einstellungen in `~/.profile` oder `~/.bashrc` vor. Um die richtige Verarbeitung der Dateien zu gewährleisten, müssen die Grundeinstellungen aus `/etc/skel/.profile` oder `/etc/skel/.bashrc` in das Home-Verzeichnis des Benutzers kopiert werden. Es empfiehlt sich, die Einstellungen aus `/etc/skel` nach einer Aktualisierung zu kopieren. Führen Sie die folgenden Shell-Befehle aus, um den Verlust persönlicher Einstellungen zu vermeiden:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Kopieren Sie anschließend die persönlichen Einstellungen erneut aus den `*.old`-Dateien.

10.1.2 Das cron-Paket

Wenn Sie Kommandos regelmäßig und automatisch zu bestimmten Zeiten im Hintergrund ausführen möchten, verwenden Sie dazu am besten das Tool `cron`. `cron` wird durch speziell formatierte Zeittabellen gesteuert. Einige sind bereits im Lieferumfang des Systems enthalten, bei Bedarf können Benutzer jedoch auch eigene Tabellen erstellen.

Die `cron`-Tabellen befinden sich im Verzeichnis `/var/spool/cron/tabs`. `/etc/crontab` dient als systemübergreifende `cron`-Tabelle. Geben Sie den Benutzernamen zur Ausführung des Befehls unmittelbar nach der Zeittabelle und noch vor dem Befehl ein. In **Beispiel 10.1**, „Eintrag in `/etc/crontab`“ (S. 171), wird `root` eingegeben. Die paketspezifischen Tabellen in `/etc/cron.d` weisen alle dasselbe Format auf. Informationen hierzu finden Sie auf der Manualpage zu `cron` (`man cron`).

Beispiel 10.1 Eintrag in /etc/crontab

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Sie können `/etc/crontab` nicht bearbeiten, indem Sie den Befehl `crontab -e` bearbeiten. Die Datei muss direkt in einem Editor geladen, geändert und dann gespeichert werden.

Einige Pakete installieren Shell-Skripte in die Verzeichnisse `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly`, deren Ausführung durch `/usr/lib/cron/run-crons` gesteuert wird. `/usr/lib/cron/run-crons` wird alle 15 Minuten von der Haupttabelle (`/etc/crontab`) ausgeführt. Hiermit wird gewährleistet, dass vernachlässigte Prozesse zum richtigen Zeitpunkt ausgeführt werden können.

Um die Skripte `hourly`, `daily` oder andere Skripte für regelmäßige Wartungsarbeiten zu benutzerdefinierten Zeiten auszuführen, entfernen Sie regelmäßig die Zeitstempeldateien mit `/etc/crontab`-Einträgen (siehe **Beispiel 10.2, „/etc/crontab: Entfernen der Zeitstempeldateien“** (S. 171) - u. a. wird `hourly` vor jeder vollen Stunde und `daily` einmal täglich um 2:14 Uhr entfernt).

Beispiel 10.2 /etc/crontab: Entfernen der Zeitstempeldateien

```
59 * * * * root rm -f /var/spool/cron/lastrun/cron.hourly
14 2 * * * root rm -f /var/spool/cron/lastrun/cron.daily
29 2 * * 6 root rm -f /var/spool/cron/lastrun/cron.weekly
44 2 1 * * root rm -f /var/spool/cron/lastrun/cron.monthly
```

Stellen Sie `DAILY_TIME` in `/etc/sysconfig/cron` alternativ auf die Zeit ein, zu der `cron.daily` gestartet werden soll. Mit `MAX_NOT_RUN` stellen Sie sicher, dass die täglichen Aufträge auch dann ausgeführt werden, wenn der Computer zur angegebenen `DAILY_TIME` und auch eine längere Zeit danach nicht eingeschaltet ist. Die maximale Einstellung von `MAX_NOT_RUN` sind 14 Tage.

Die täglichen Systemwartungsaufträge werden zum Zwecke der Übersichtlichkeit auf mehrere Skripts verteilt. Sie sind im Paket `aaa_base` enthalten. `/etc/cron.daily` enthält beispielsweise die Komponenten `suse.de-backup-rpmdb`, `suse.de-clean-tmp` oder `suse.de-cron-local`.

10.1.3 Protokolldateien: Paket logrotate

Mehrere Systemdienste (*Daemons*) zeichnen zusammen mit dem Kernel selbst regelmäßig den Systemstatus und spezielle Ereignisse in Protokolldateien auf. Auf diese Weise kann der Administrator den Status des Systems zu einem bestimmten Zeitpunkt regelmäßig überprüfen, Fehler oder Fehlfunktionen erkennen und die Fehler mit Präzision beheben. Die Protokolldateien werden in der Regel, wie von FHS angegeben, unter `/var/log` gespeichert und werden täglich umfangreicher. Mit dem Paket `logrotate` kann der Umfang der Dateien gesteuert werden.

Konfigurieren Sie Logrotate mit der Datei `/etc/logrotate.conf`. Die Dateien, die zusätzlich gelesen werden sollen, werden insbesondere durch die `include`-Spezifikation konfiguriert. Programme, die Protokolldateien erstellen, installieren einzelne Konfigurationsdateien in `/etc/logrotate.d`. Solche Dateien sind beispielsweise im Lieferumfang der Pakete `apache2` (`/etc/logrotate.d/apache2`) und `syslogd` (`/etc/logrotate.d/syslog`) enthalten.

Beispiel 10.3 *Beispiel für `/etc/logrotate.conf`*

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#   monthly
#   create 0664 root utmp
#   rotate 1
#}

# system-specific logs may be also be configured here.
```

`logrotate` wird über `cron` gesteuert und täglich durch `/etc/cron.daily/logrotate` aufgerufen.

WICHTIG

Mit der Option `create` werden alle vom Administrator in `/etc/permissions*` vorgenommenen Einstellungen gelesen. Stellen Sie sicher, dass durch persönliche Änderungen keine Konflikte auftreten.

10.1.4 Der Befehl "locate"

`locate`, ein Befehl zum schnellen Suchen von Dateien ist nicht im Standardumfang der installierten Software enthalten. Wenn Sie möchten, installieren Sie das Paket `findutils-locate`. Der Prozess `updatedb` wird jeden Abend etwa 15 Minuten nach dem Booten des Systems gestartet.

10.1.5 Der Befehl "ulimit"

Mit dem Befehl `ulimit` (*user limits*) können Grenzwerte für die Verwendung der Systemressourcen festgelegt und angezeigt werden. `ulimit` ist insbesondere für die Begrenzung des für Anwendungen verfügbaren Speichers hilfreich. Hiermit kann verhindert werden, dass eine Anwendung zu viel Speicher belegt, wodurch es zu einem Stillstand des Systems kommen kann.

`ulimit` kann mit verschiedenen Optionen verwendet werden. Verwenden Sie zum Begrenzen der Speicherauslastung die in [Tabelle 10.1, „ulimit: Einstellen von Ressourcen für Benutzer“](#) (S. 173) aufgeführten Optionen.

Tabelle 10.1 *ulimit: Einstellen von Ressourcen für Benutzer*

<code>-m</code>	Die maximale nicht auslagerbare festgelegte Größe
<code>-v</code>	Die maximale Größe des virtuellen Arbeitsspeichers, der der Shell zur Verfügung steht
<code>-s</code>	Die maximale Größe des Stapels
<code>-c</code>	Die maximale Größe der erstellten Kerndateien
<code>-a</code>	Alle aktuellen Grenzwerte werden gemeldet

In `/etc/profile` können Sie systemweite Einträge vornehmen. Aktivieren Sie hier die Erstellung der Core-Dateien, die Programmierer für die *Fehlersuche* benötigen. Ein normaler Benutzer kann die in `/etc/profile` vom Systemadministrator festgelegten Werte nicht erhöhen, er kann jedoch spezielle Einträge in `~/.bashrc` vornehmen.

Beispiel 10.4 *ulimit: Einstellungen in ~/.bashrc*

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

Die Speicherangaben müssen in KB erfolgen. Weitere Informationen erhalten Sie mit `man bash`.

WICHTIG

`ulimit`-Direktiven werden nicht von allen Shells unterstützt. PAM (beispielsweise `pam_limits`) bietet umfassende Anpassungsmöglichkeiten, wenn Sie Einstellungen für diese Beschränkungen vornehmen müssen.

10.1.6 Der Befehl "free"

Der Befehl `free` ist leicht irreführend, wenn Sie herausfinden möchten, wie viel Arbeitsspeicher zurzeit verwendet wird. Die entsprechenden Informationen finden Sie in `/proc/meminfo`. Heute müssen sich Benutzer, die ein modernes Betriebssystem wie Linux verwenden, in der Regel kaum Gedanken über den Arbeitsspeicher machen. Das Konzept des *verfügbaren Arbeitsspeichers* geht auf Zeiten vor der einheitlichen Speicherverwaltung zurück. Bei Linux gilt der Grundsatz *freier Arbeitsspeicher ist schlechter Arbeitsspeicher*. Daher wurde bei Linux immer darauf geachtet, die Caches auszugleichen, ohne freien oder nicht verwendeten Arbeitsspeicher zuzulassen.

Der Kernel verfügt nicht direkt über Anwendungs- oder Benutzerdaten. Stattdessen verwaltet er Anwendungen und Benutzerdaten in einem *Seiten-Cache*. Falls nicht mehr genügend Arbeitsspeicher vorhanden ist, werden Teile auf der Swap-Partition oder in Dateien gespeichert, von wo aus sie mithilfe des Befehls `mmap` abgerufen werden können. (siehe `man mmap`).

Der Kernel enthält zusätzlich andere Caches, wie beispielsweise den *slab-Cache*, in dem die für den Netzwerkzugriff verwendeten Caches gespeichert werden. Dies erklärt die Unterschiede zwischen den Zählern in `/proc/meminfo`. Die meisten, jedoch nicht alle dieser Zähler können über `/proc/slabinfo` aufgerufen werden.

10.1.7 Die Datei `/etc/resolv.conf`

Die Auflösung von Domännennamen erfolgt über die Datei `/etc/resolv.conf`. Weitere Informationen finden Sie im Abschnitt **Kapitel 16, Domain Name System (DNS)** (S. 287).

Diese Datei wird ausschließlich mit dem Skript `/sbin/modify_resolvconf` aktualisiert. Kein anderes Programm verfügt über direkte Änderungsberechtigungen für `/etc/resolv.conf`. Das Erzwingen dieser Regel ist die einzige Möglichkeit, um die Konsistenz der Netzwerkkonfiguration und der relevanten Dateien des Systems zu gewährleisten.

10.1.8 man-Seiten und Info-Seiten

Für einige GNU-Anwendungen (wie beispielsweise `tar`) sind keine man-Seiten mehr vorhanden. Verwenden Sie für diese Befehle die Option `--help`, um eine kurze Übersicht über die info-Seiten zu erhalten, in der Sie detailliertere Anweisungen erhalten. `info` befindet sich im Hypertextsystem von GNU. Eine Einführung in dieses System erhalten Sie, wenn Sie `infoinfo` eingeben. Info-Seiten können mit Emacs angezeigt werden, wenn Sie `emacs -f info` eingeben oder mit `info` direkt in einer Konsole angezeigt werden. Sie können auch `tinfo`, `xinfo` oder das Hilfesystem von `man` zum Anzeigen von info-Seiten verwenden.

10.1.9 Einstellungen für GNU Emacs

GNU Emacs ist eine komplexe Arbeitsumgebung. In den folgenden Abschnitten werden die beim Starten von GNU Emacs verarbeiteten Dateien beschrieben. Weitere Informationen hierzu erhalten Sie online unter <http://www.gnu.org/software/emacs/>.

Beim Starten liest Emacs mehrere Dateien, in denen die Einstellungen für den Benutzer, den Systemadministrator und den Distributor zur Anpassung oder Vorkonfiguration

enthalten sind. Die Initialisierungsdatei `~/ .emacs` ist in den Home-Verzeichnissen der einzelnen Benutzer von `/etc/skel` installiert. `.emacs` wiederum liest die Datei `/etc/skel/.gnu-emacs`. Zum Anpassen des Programms kopieren Sie `.gnu-emacs` in das Home-Verzeichnis (mit `cp /etc/skel/.gnu-emacs ~/ .gnu-emacs`) und nehmen Sie dort die gewünschten Einstellungen vor.

`.gnu-emacs` definiert die Datei `~/ .gnu-emacs-custom` als `custom-file`. Wenn Benutzer in Emacs Einstellungen mit den `customize`-Optionen vornehmen, werden die Einstellungen in `~/ .gnu-emacs-custom` gespeichert.

Bei openSUSE wird mit dem `emacs`-Paket die Datei `site-start.el` im Verzeichnis `/usr/share/emacs/site-lisp` installiert. Die Datei `site-start.el` wird vor der Initialisierungsdatei `~/ .emacs` geladen. Mit `site-start.el` wird unter anderem sichergestellt, dass spezielle Konfigurationsdateien mit Emacs-Zusatzpaketen, wie `psgml`, automatisch geladen werden. Konfigurationsdateien dieses Typs sind ebenfalls unter `/usr/share/emacs/site-lisp` gespeichert und beginnen immer mit `suse-start-`. Der lokale Systemadministrator kann systemweite Einstellungen in `default.el` festlegen.

Weitere Informationen zu diesen Dateien finden Sie in der Info-Datei zu Emacs unter *Init File*: <info:/emacs/InitFile>. Informationen zum Deaktivieren des Ladens dieser Dateien (sofern erforderlich) stehen dort ebenfalls zur Verfügung.

Die Komponenten von Emacs sind in mehrere Pakete unterteilt:

- Das Basispaket `emacs`.
- `emacs-x11` (in der Regel installiert): das Programm *mit* X11-Support.
- `emacs-nox`: das Programm *ohne* X11-Support.
- `emacs-info`: Online-Dokumentation im `info`-Format.
- `emacs-el`: die nicht kompilierten Bibliotheksdateien in Emacs Lisp. Sie sind während der Laufzeit nicht erforderlich.
- Verschiedene Add-On-Pakete können bei Bedarf installiert werden: `emacs-auctex` (für LaTeX), `psgml` (für SGML und XML), `gnuserv` (für Client- und Server-Vorgänge) und andere.

10.2 Virtuelle Konsolen

Linux ist ein Multitasking-System für den Mehrbenutzerbetrieb. Die Vorteile dieser Funktionen können auch auf einem eigenständigen PC-System genutzt werden. Im Textmodus stehen sechs virtuelle Konsolen zur Verfügung. Mit den Tastenkombinationen Alt + F1 bis Alt + F6 können Sie zwischen den Konsolen umschalten. Die siebte Konsole ist für X und reserviert und in der zehnten Konsole werden Kernel-Meldungen angezeigt. Durch Ändern der Datei `/etc/inittab` können mehrere oder weniger Konsolen zugewiesen werden.

Wenn Sie von X ohne Herunterfahren zu einer anderen Konsole wechseln möchten, verwenden Sie die Tastenkombinationen Strg + Alt + F1 bis Strg + Alt + F6. Mit Alt + F7 kehren Sie zu X zurück.

10.3 Tastaturzuordnung

Um die Tastaturzuordnung der Programme zu standardisieren, wurden Änderungen an folgenden Dateien vorgenommen:

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Diese Änderungen betreffen nur Anwendungen, die `terminfo`-Einträge verwenden oder deren Konfigurationsdateien direkt geändert werden (`vi`, `less` usw.). Anwendungen, die nicht im Lieferumfang des Systems enthalten sind, sollten an diese Standards angepasst werden.

Unter X kann mit der Tastenkombination Strg + Umschalttaste (rechts) auf die Compose-Taste (Multi-Key) zugegriffen werden. Siehe auch den entsprechenden Eintrag in `/etc/X11/Xmodmap`.

Weitere Einstellungen sind mit der X-Tastaturerweiterung (XKB) möglich. Diese Erweiterung wird auch von den Desktop-Umgebungen GNOME (gswitchit) und KDE (kxkb) verwendet.

TIPP: Weiterführende Informationen

Informationen zu XKB finden Sie in `/etc/X11/xkb/README` und den dort aufgeführten Dokumenten.

Detaillierte Informationen zur Eingabe von Chinesisch, Japanisch und Koreanisch (CJK) finden Sie auf der Seite von Mike Fabian: <http://www.suse.de/~mfabian/suse-cjk/input.html>.

10.4 Sprach- und länderspezifische Einstellungen

Das System wurde zu einem großen Teil internationalisiert und kann flexibel an lokale Gegebenheiten angepasst werden. Anders ausgedrückt: Die Internationalisierung (*I18N*) ermöglicht spezielle Lokalisierungen (*L10N*). Die Abkürzungen I18N und L10N wurden von den ersten und letzten Buchstaben der englischsprachigen Begriffe und der Anzahl der dazwischen stehenden ausgelassenen Wörter abgeleitet.

Die Einstellungen werden mit `LC_`-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dies bezieht sich nicht nur auf die *native Sprachunterstützung*, sondern auch auf die Kategorien *Meldungen* (Sprache) *Zeichensatz*, *Sortierreihenfolge*, *Uhrzeit und Datum*, *Zahlen* und *Währung*. Diese Kategorien können direkt über eine eigene Variable oder indirekt mit einer Master-Variable in der Datei `language` festgelegt werden (weitere Informationen erhalten Sie auf der Manualpage zu `locale`).

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`,
`RC_LC_NUMERIC`, `RC_LC_MONETARY`

Diese Variablen werden ohne das Präfix `RC_` an die Shell weitergegeben und stehen für die aufgelisteten Kategorien. Die betreffenden Shell-Profile werden unten aufgeführt. Die aktuelle Einstellung lässt sich mit dem Befehl `locale` anzeigen.

RC_LC_ALL

Sofern diese Variable festgelegt ist, setzt Sie die Werte der bereits erwähnten Variablen außer Kraft.

RC_LANG

Falls keine der zuvor genannten Variablen festgelegt ist, ist dies das Fallback. Standardmäßig wird nur `RC_LANG` festgelegt. Dadurch wird es für die Benutzer einfacher, eigene Werte einzugeben.

ROOT_USES_LANG

Eine Variable, die entweder den Wert `yes` oder den Wert `no` aufweist. Wenn die Variable auf `no` gesetzt ist, funktioniert `root` immer in der POSIX-Umgebung.

Die Variablen können über den `sysconfig`-Editor von YaST (siehe [Abschnitt 8.3.1](#), „Ändern der Systemkonfiguration mithilfe des YaST-Editors `sysconfig`“ (S. 143)) festgelegt werden. Der Wert einer solchen Variable enthält den Sprachcode, den Ländercode, die Codierung und einen Modifier. Die einzelnen Komponenten werden durch Sonderzeichen verbunden:

```
LANG=<language>[_<COUNTRY>].<Encoding>[@<Modifier>]
```

10.4.1 Beispiele

Sprach- und Ländercode sollten immer gleichzeitig eingestellt werden. Die Spracheinstellungen entsprechen der Norm ISO 639, die unter <http://www.evertype.com/standards/iso639/iso639-en.html> und <http://www.loc.gov/standards/iso639-2/> verfügbar ist. Die in ISO 3166 aufgeführten Ländercodes sind unter http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html verfügbar.

Es ist nur sinnvoll, Werte festzulegen, für die verwendbare Beschreibungsdateien unter `/usr/lib/locale` zu finden sind. Anhand der Dateien in `/usr/share/i18n` können mit dem Befehl `localedef` zusätzliche Beschreibungsdateien erstellt werden. Die Beschreibungsdateien sind Bestandteil des Pakets `glibc-i18ndata`. Eine Beschreibungsdatei für `en_US.UTF-8` (für Englisch und USA) kann beispielsweise wie folgt erstellt werden:

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

```
LANG=en_US.UTF-8
```

Dies ist die Standardeinstellung, wenn während der Installation US-Englisch ausgewählt wurde. Wenn Sie eine andere Sprache ausgewählt haben, wird diese Sprache ebenfalls mit der Zeichencodierung UTF-8 aktiviert.

```
LANG=en_US.ISO-8859-1
```

Hiermit wird als Sprache Englisch, als Land die USA und als Zeichensatz ISO-8859-1 festgelegt. In diesem Zeichensatz wird das Eurozeichen nicht unterstützt, es kann jedoch gelegentlich in Programmen nützlich sein, die nicht für die UTF-8-Unterstützung aktualisiert wurden. Die Zeichenkette, mit der der Zeichensatz definiert wird (in diesem Fall ISO-8859-1), wird anschließend von Programmen, wie Emacs, ausgewertet.

```
LANG=en_IE@euro
```

Im oben genannten Beispiel wird das Eurozeichen explizit in die Spracheinstellung aufgenommen. Streng genommen ist diese Einstellung mittlerweile veraltet, da das Eurozeichen jetzt ebenfalls in UTF-8 enthalten ist. Diese Einstellung ist nur sinnvoll, wenn eine Anwendung UTF-8 nicht unterstützt, ISO-8859-15 jedoch unterstützt.

SuSEconfig liest die Variablen in `/etc/sysconfig/language` und speichert die erforderlichen Änderungen in `/etc/SuSEconfig/profile` und `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` von `/etc/profile` gelesen oder als *Quelle verwendet*. `/etc/SuSEconfig/csh.cshrc` wird von `/etc/csh.cshrc` als *Quelle verwendet*. Auf diese Weise werden die Einstellungen systemweit verfügbar.

Die Benutzer können die Standardeinstellungen des Systems außer Kraft setzen, indem Sie die Datei `~/ .bashrc` entsprechend bearbeiten. Wenn Sie die systemübergreifende Einstellung `en_US` für Programm Meldungen beispielsweise nicht verwenden möchten, nehmen Sie beispielsweise `LC_MESSAGES=es_ES` auf, damit die Meldungen stattdessen auf Spanisch angezeigt werden.

10.4.2 Locale-Einstellungen in `~/ .i18n`

Wenn Sie mit den Locale-Systemstandardwerten nicht zufrieden sind, können Sie die Einstellungen in `~/ .i18n` ändern. Achten Sie dabei jedoch auf die Einhaltung der

Bash-Scripting-Syntax. Die Einträge in `~/ .i18n` setzen die Systemstandardwerte aus `/etc/sysconfig/language` außer Kraft. Verwenden Sie dieselben Variablennamen, jedoch ohne die `RC_`-Präfixe für den Namespace, also beispielsweise `LANG` anstatt `RC_LANG`:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

10.4.3 Einstellungen für die Sprachunterstützung

Die Dateien in der Kategorie *Meldungen* werden generell im entsprechenden Sprachverzeichnis (wie beispielsweise `en`) gespeichert, damit ein Fallback vorhanden ist.

Wenn Sie für `LANG` den Wert `en_US` festlegen und in `/usr/share/locale/en_US/LC_MESSAGES` keine Meldungsdatei vorhanden ist, wird ein Fallback auf `/usr/share/locale/en/LC_MESSAGES` ausgeführt.

Darüber hinaus kann eine Fallback-Kette definiert werden, beispielsweise für Bretonisch zu Französisch oder für Galizisch zu Spanisch oder Portugiesisch:

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Wenn Sie möchten, können Sie die norwegischen Varianten Nynorsk und Bokmål (mit zusätzlichem Fallback auf `no`) verwenden:

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

oder

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

Beachten Sie, das bei Norwegisch auch `LC_TIME` anders behandelt wird.

Ein mögliches Problem ist, dass ein Trennzeichen, das zum Trennen von Zifferngruppen verwendet wird, nicht richtig erkannt wird. Dies passiert, wenn LANG auf einen aus zwei Buchstaben bestehenden Sprachcode wie de eingestellt ist, die Definitionsdatei, die glibc verwendet, jedoch in /usr/share/lib/de_DE/LC_NUMERIC gespeichert ist. Daher muss LC_NUMERIC auf de_DE gesetzt sein, damit das System die Trennzeichendefinition erkennen kann.

10.4.4 Weiterführende Informationen

- *The GNU C Library Reference Manual*, Kapitel „Locales and Internationalization“. Dieses Handbuch ist in `glibc-info` enthalten.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, momentan verfügbar unter <http://www.cl.cam.ac.uk/~mgk25/unicode.html>.
- *Unicode-Howto*, von Bruno Haible: /usr/share/doc/howto/en/html/Unicode-HOWTO.html.

Gerätemanagement über dynamischen Kernel mithilfe von udev

11

Der Kernel kann fast jedes Gerät am laufenden System hinzufügen oder entfernen. Änderungen des Gerätestatus (ob ein Gerät angeschlossen oder entfernt wird) müssen an den userspace weitergegeben werden. Geräte müssen konfiguriert werden, sobald sie angeschlossen und erkannt wurden. Benutzer eines bestimmten Geräts müssen über sämtliche Statusänderungen für das entsprechende Gerät informiert werden. udev bietet die erforderliche Infrastruktur, um die Geräteknottendateien und symbolische Links im `/dev`-Verzeichnis dynamisch zu warten. Mithilfe von udev-Regeln können externe Werkzeuge in die Ereignisverarbeitung des Kernel-Geräts eingebunden werden. Auf diese Weise können Sie die udev-Gerätebehandlung anpassen. Beispielsweise, indem Sie bestimmte Skripten hinzufügen, die als Teil der Kernel-Gerätebehandlung ausgeführt werden, oder indem Sie zusätzliche Daten zur Auswertung bei der Gerätebehandlung anfordern und importieren.

11.1 Das `/dev`-Verzeichnis

Die Geräteknotten im `/dev`-Verzeichnis ermöglichen den Zugriff auf die entsprechenden Kernel-Geräte. Mithilfe von udev spiegelt das `/dev`-Verzeichnis den aktuellen Status des Kernel wieder. Jedes Kernel-Gerät verfügt über eine entsprechende Gerätedatei. Falls ein Gerät vom System getrennt wird, wird der Geräteknotten entfernt.

Der Inhalt des `/dev`-Verzeichnisses wird auf einem temporären Dateisystem gespeichert und alle Dateien werden bei jedem Systemstart neu erstellt. Manuell erstellte oder geänderte Dateien überdauern ein erneutes Booten planmäßig nicht. Statische Dateien

und Verzeichnisse, die unabhängig vom Status des entsprechenden Kernel-Geräts immer im `/dev`-Verzeichnis vorhanden sein sollten, können im Verzeichnis `/lib/udev/devices` platziert werden. Beim Systemstart wird der Inhalt des entsprechenden Verzeichnisses in das `/dev`-Verzeichnis kopiert und erhält dieselbe Eigentümerschaft und dieselben Berechtigungen wie die Dateien in `/lib/udev/devices`.

11.2 Kernel-uevents und udev

Die erforderlichen Geräteinformationen werden vom `sysfs`-Dateisystem exportiert. Für jedes Gerät, das der Kernel erkennt und initialisiert hat, wird ein Verzeichnis mit dem Gerätenamen erstellt. Es enthält Attributdateien mit gerätespezifischen Eigenschaften.

Jedes Mal, wenn ein Gerät hinzugefügt oder entfernt wird, sendet der Kernel ein `uevent`, um `udev` über die Änderung zu informieren. Der `udev`-Daemon liest und analysiert alle angegebenen Regeln aus den `/etc/udev/rules.d/*.rules`-Dateien einmalig beim Start und speichert diese. Falls Regeldateien verändert, hinzugefügt oder entfernt werden, empfängt der Daemon ein Ereignis und aktualisiert die gespeicherten Regeldarstellungen. Weitere Informationen zu den `udev`-Regeln und deren Syntax finden Sie unter [Abschnitt 11.6, „Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von `udev`-Regeln“](#) (S. 187).

Jedes empfangene Ereignis wird mit dem Satz der angegebenen Regeln abgeglichen. Die Regeln können Ereignisergebnisschlüssel hinzufügen oder ändern, einen bestimmten Namen für den zu erstellenden Geräteknoten anfordern, auf den Knoten verweisende Symlinks hinzufügen oder Programme hinzufügen, die ausgeführt werden sollen, nachdem der Geräteknoten erstellt wurde. Die Treiber-Core-uevents werden von einem Kernel-Netlink-Socket empfangen.

11.3 Treiber, Kernel-Module und Geräte

Die Kernel-Bus-Treiber prüfen, ob Geräte vorhanden sind. Für jedes erkannte Gerät erstellt der Kernel eine interne Gerätestruktur und der Treiber-Core sendet ein `uevent` an den `udev`-Daemon. Bus-Geräte identifizieren sich mithilfe einer speziell formatierten ID, die Auskunft über die Art des Geräts gibt. Normalerweise bestehen diese IDs aus einer Hersteller- und einer Produkt-ID und anderen das Subsystem betreffenden Werten.

Jeder Bus weist ein eigenes Schema für diese IDs auf, das so genannte `MODALIAS`-Schema. Der Kernel bedient sich der Geräteinformationen, verfasst daraus eine `MODALIAS`-ID-Zeichenkette und sendet diese Zeichenkette zusammen mit dem Ereignis. Beispiel für eine USB-Maus:

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

Jeder Gerätetreiber verfügt über eine Liste bekannter Aliase für Geräte, die er behandeln kann. Die Liste ist in der Kernel-Moduldatei selbst enthalten. Das Programm `depmod` liest die ID-Listen und erstellt die Datei `modules.alias` im Verzeichnis `/lib/modules` des Kernel für alle zurzeit verfügbaren Module. Bei dieser Infrastruktur ist das Laden des Moduls ein ebenso müheloser Vorgang, wie das Aufrufen von `modprobe` für jedes Ereignis, das über einen `MODALIAS`-Schlüssel verfügt. Falls `modprobe $MODALIAS` aufgerufen wird, gleicht es den für das Gerät verfassten Geräte-Alias mit den Aliassen von den Modulen ab. Falls ein übereinstimmender Eintrag gefunden wird, wird das entsprechende Modul geladen. Alle diese Vorgänge werden von `udev` ausgelöst und erfolgen automatisch.

11.4 Booten und erstes Einrichten des Geräts

Alle Geräteereignisse, die während des Bootvorgangs stattfinden, bevor der `udev`-Daemon ausgeführt wird, gehen verloren. Dies liegt daran, dass die Infrastruktur für die Behandlung dieser Ereignisse sich auf dem Root-Dateisystem befindet und zu diesem Zeitpunkt nicht verfügbar ist. Diesen Verlust fängt der Kernel mit der Datei `uevent` ab, die sich im Geräteverzeichnis jedes Geräts im `sysfs`-Dateisystem befindet. Durch das Schreiben von `add` in die entsprechende Datei sendet der Kernel dasselbe Ereignis, das während des Bootvorgangs verloren gegangen ist, neu. Eine einfache Schleife über alle `uevent`-Dateien in `/sys` löst alle Ereignisse erneut aus, um die Geräteknotten zu erstellen und die Geräteeinrichtung durchzuführen.

Beispielsweise kann eine USB-Maus, die während des Bootvorgangs vorhanden ist, nicht durch die frühe Bootlogik initialisiert werden, da der Treiber zum entsprechenden Zeitpunkt nicht verfügbar ist. Das Ereignis für die Geräteerkennung ist verloren gegangen und konnte kein Kernel-Modul für das Gerät finden. Anstatt manuell nach möglicherweise angeschlossenen Geräten zu suchen, fordert `udev` lediglich alle Geräteereignisse aus dem Kernel an, wenn das Root-Dateisystem verfügbar ist. Das Ereignis für die USB-Maus wird also lediglich erneut ausgeführt. Jetzt wird das Kernel-Modul

auf dem eingehängten Root-Dateisystem gefunden und die USB-Maus kann initialisiert werden.

Von userspace aus gibt es keinen erkennbaren Unterschied zwischen einer coldplug-Gerätesequenz und einer Geräteerkennung während der Laufzeit. In beiden Fällen werden dieselben Regeln für den Abgleich verwendet und dieselben konfigurierten Programme ausgeführt.

11.5 Überwachen des aktiven udev-Daemons

Das Programm `udevadm monitor` kann verwendet werden, um die Treiber-Core-Ereignisse und das Timing der udev-Ereignisprozesse zu visualisieren.

```
UEVENT[1185238505.276660] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV [1185238505.279198] add /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

Die UEVENT-Zeilen zeigen die Ereignisse an, die der Kernel an Netlink gesendet hat. Die UDEV-Zeilen zeigen die fertig gestellten udev-Ereignisbehandlungsroutinen an. Das Timing wird in Mikrosekunden angegeben. Die Zeit zwischen UEVENT und UDEV ist die Zeit, die udev benötigt hat, um dieses Ereignis zu verarbeiten oder der udev-Daemon hat eine Verzögerung bei der Ausführung der Synchronisierung dieses Ereignisses mit zugehörigen und bereits ausgeführten Ereignissen erfahren. Beispielsweise warten Ereignisse für Festplattenpartitionen immer, bis das Ereignis für den primären Datenträger fertig gestellt ist, da die Partitionereignisse möglicherweise auf die Daten

angewiesen sind, die das Ereignis für den primären Datenträger von der Hardware angefordert hat.

`udevadm monitor --env` zeigt die vollständige Ereignisumgebung an:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

udev sendet auch Meldungen an syslog. Die Standard-syslog-Priorität, die steuert, welche Meldungen an syslog gesendet werden, wird in der udev-Konfigurationsdatei `/etc/udev/udev.conf` angegeben. Die Protokollpriorität des ausgeführten Daemons kann mit `udev control log_priority=level/number` geändert werden.

11.6 Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von udev-Regeln

Eine udev-Regel kann mit einer beliebigen Eigenschaft abgeglichen werden, die der Kernel der Ereignisliste hinzufügt oder mit beliebigen Informationen, die der Kernel in `sysfs` exportiert. Die Regel kann auch zusätzliche Informationen aus externen Programmen anfordern. Jedes Ereignis wird gegen alle angegebenen Regeln abgeglichen. Alle Regeln befinden sich im Verzeichnis `/etc/udev/rules.d/`.

Jede Zeile in der Regeldatei enthält mindestens ein Schlüsselwertepaar. Es gibt zwei Arten von Schlüsseln: die Übereinstimmungsschlüssel und Zuweisungsschlüssel. Wenn alle Übereinstimmungsschlüssel mit ihren Werten übereinstimmen, wird diese Regel angewendet und der angegebene Wert wird den Zuweisungsschlüsseln zugewiesen. Eine übereinstimmende Regel kann den Namen des Geräteknotens angeben, auf den

Knoten verweisende Symlinks hinzufügen oder ein bestimmtes Programm als Teil der Ereignisbehandlung ausführen. Falls keine übereinstimmende Regel gefunden wird, wird der standardmäßige Geräteknotenname verwendet, um den Geräteknoten zu erstellen. Ausführliche Informationen zur Regelsyntax und den bereitgestellten Schlüsseln zum Abgleichen oder Importieren von Daten werden auf der man-Seite von udev beschrieben. Nachfolgend finden Sie einige Beispielregeln, die Sie in die grundlegende Regelsyntax von udev einführen. Sämtliche Beispielregeln stammen aus dem udev-Standardregelsatz, der sich in `/etc/udev/rules.d/50-udev-default.rules` befindet.

Beispiel 11.1 *udev-Beispielregeln*

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

Die Regel `console` besteht aus drei Schlüsseln: einem Übereinstimmungsschlüssel (`KERNEL`) und zwei Zuweisungsschlüsseln (`MODE` und `OPTIONS`). Der Übereinstimmungsschlüssel `KERNEL` durchsucht die Geräteliste nach Elementen des Typs `console`. Nur exakte Übereinstimmungen sind gültig und lösen die Ausführung dieser Regel aus. Der Zuweisungsschlüssel `MODE` weist dem Geräteknoten spezielle Berechtigungen zu, in diesem Fall Lese- und Schreibberechtigung nur für den Eigentümer des Geräts. Der Schlüssel `OPTIONS` bewirkt, dass diese Regel auf Geräte dieses Typs als letzte Regel angewendet wird. Alle nachfolgenden Regeln, die mit diesem Gerätetyp übereinstimmen, werden nicht mehr angewendet.

Die Regel `serial devices` steht in `50-udev-default.rules` nicht mehr zur Verfügung; es lohnt sich jedoch, sie sich dennoch anzusehen. Sie besteht aus zwei Übereinstimmungsschlüsseln (`KERNEL` und `ATTRS`) und einem Zuweisungsschlüssel (`SYMLINK`). Der Übereinstimmungsschlüssel `KERNEL` sucht nach allen Geräten des Typs `ttyUSB`. Durch den Platzhalter `*` trifft dieser Schlüssel auf mehrere dieser Geräte zu. Der zweite Übereinstimmungsschlüssel (`ATTRS`) überprüft, ob die Attributdatei `product` in `sysfs` der jeweiligen `ttyUSB`-Geräte eine bestimmte Zeichenkette enthält. Der Zuweisungsschlüssel `SYMLINK` bewirkt, dass dem Gerät unter `/dev/pilot` ein symbolischer Link hinzugefügt wird. Der Operator dieses Schlüssels (`+=`) weist udev

an, diese Aktion auch dann auszuführen, wenn dem Gerät bereits durch frühere (oder auch erst durch spätere) Regeln andere symbolische Links hinzugefügt wurden. Die Regel wird nur angewendet, wenn die Bedingungen beider Übereinstimmungsschlüssel erfüllt sind.

Die Regel `printer` gilt nur für USB-Drucker. Sie enthält zwei Übereinstimmungsschlüssel (`SUBSYSTEM` und `KERNEL`), die beide zutreffen müssen, damit die Regel angewendet wird. Die drei Zuweisungsschlüssel legen den Namen dieses Gerätetyps fest (`NAME`), die Erstellung symbolischer Gerätelinks (`SYMLINK`) sowie die Gruppenmitgliedschaft dieses Gerätetyps (`GROUP`). Durch den Platzhalter `*` im Schlüssel `KERNEL` trifft diese Regel auf mehrere `lp`-Druckergeräte zu. Sowohl der Schlüssel `NAME` als auch der Schlüssel `SYMLINK` verwenden Ersetzungen, durch die der Zeichenkette der interne Gerätenamen hinzugefügt wird. Der symbolische Link für den ersten `lp`-USB-Drucker würde zum Beispiel `/dev/usb/lp0` lauten.

Die Regel `kernel firmware loader` weist `udev` an, während der Laufzeit weitere Firmware mittels eines externen Hilfsskripts zu laden. Der Übereinstimmungsschlüssel `SUBSYSTEM` sucht nach dem Subsystem `firmware`. Der Schlüssel `ACTION` überprüft, ob bereits Geräte des Subsystems `firmware` hinzugefügt wurden. Der Schlüssel `RUN+=` löst die Ausführung des Skripts `firmware.sh` aus, das die noch zu ladende Firmware lokalisiert.

Die folgenden allgemeinen Eigenschaften treffen auf alle Regeln zu:

- Jede Regel besteht aus einem oder mehreren, durch Kommas getrennten Schlüssel-/Wertepaaren.
- Die Aktion eines Schlüssels wird durch seinen Operator festgelegt. `udev`-Regeln unterstützen verschiedene Operatoren.
- Jeder angegebene Wert muss in Anführungszeichen eingeschlossen sein.
- Jede Zeile der Regeldatei stellt eine Regel dar. Falls eine Regel länger als eine Zeile ist, verbinden Sie die Zeilen wie bei jeder anderen Shell-Syntax mit `\`.
- `udev`-Regeln unterstützen shell-typische Übereinstimmungsregeln für die Schemata `*`, `?` und `[]`.
- `udev`-Regeln unterstützen Ersetzungen.

11.6.1 Verwenden von Operatoren in udev-Regeln

Bei der Erstellung von Schlüsseln stehen Ihnen je nach gewünschtem Schlüsseltyp verschiedene Operatoren zur Auswahl. Übereinstimmungsschlüssel werden in der Regel nur zum Auffinden eines Wertes verwendet, der entweder mit dem Suchwert übereinstimmt oder explizit nicht mit dem gesuchten Wert übereinstimmt. Übereinstimmungsschlüssel enthalten einen der folgenden Operatoren:

==

Suche nach übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

!=

Suche nach nicht übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

Folgende Operatoren können für Zuweisungsschlüssel verwendet werden:

=

Weist einem Schlüssel einen Wert zu. Wenn der Schlüssel zuvor aus einer Liste mit mehreren Werten bestand, wird der Schlüssel durch diesen Operator auf diesen Einzelwert zurückgesetzt.

+=

Fügt einem Schlüssel, der eine Liste mehrerer Einträge enthält, einen Wert hinzu.

:=

Weist einen endgültigen Wert zu. Eine spätere Änderung (durch nachfolgende Regeln) ist nicht möglich.

11.6.2 Verwenden von Ersetzungen in udev-Regeln

udev-Regeln unterstützen sowohl Platzhalter als auch Ersetzungen. Diese setzen Sie genauso ein wie in anderen Skripten. Folgende Ersetzungen können in udev-Regeln verwendet werden:

`%r, $root`
Standardmäßig das Geräteverzeichnis `/dev`

`%p, $devpath`
Der Wert von `DEVPATH`

`%k, $kernel`
Der Wert von `KERNEL` oder der interne Gerätename

`%n, $number`
Die Gerätenummer

`%N, $tempnode`
Der temporäre Name der Gerätedatei

`%M, $major`
Die höchste Nummer des Geräts

`%m, $minor`
Die niedrigste Nummer des Geräts

`%s{attribute}, $attr{attribute}`
Der Wert eines `sysfs`-Attributs (das durch `attribute` festgelegt ist)

`%E{variable}, $attr{variable}`
Der Wert einer Umgebungsvariablen (die durch `variable` festgelegt ist)

`%c, $result`
Die Ausgabe von `PROGRAM`

`%%`
Das `%`-Zeichen

`$$`
Das `$`-Zeichen

11.6.3 Verwenden von udev-Übereinstimmungsschlüsseln

Übereinstimmungsschlüssel legen Bedingungen fest, die erfüllt sein müssen, damit eine udev-Regel angewendet werden kann. Folgende Übereinstimmungsschlüssel sind verfügbar:

ACTION

Der Name der Ereignisaktion, zum Beispiel `add` oder `remove` zum Hinzufügen oder Entfernen eines Geräts.

DEVPATH

Der Gerätepfad des Ereignisgeräts, zum Beispiel

`DEVPATH=/bus/pci/drivers/ipw3945` für die Suche nach allen Ereignissen in Zusammenhang mit dem Treiber `ipw3945`.

KERNEL

Der interne Name (Kernel-Name) des Ereignisgeräts.

SUBSYSTEM

Das Subsystem des Ereignisgeräts, zum Beispiel `SUBSYSTEM=usb` für alle Ereignisse in Zusammenhang mit USB-Geräten.

ATTR{*Dateiname*}

sysfs-Attribute des Ereignisgeräts. Für die Suche nach einer Zeichenkette im Attributdateinamen `vendor` können Sie beispielsweise

`ATTR{vendor}=="On[SS]tream"` verwenden.

KERNELS

Weist udev an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätenamen zu durchsuchen.

SUBSYSTEMS

Weist udev an, den Gerätepfad aufwärts nach einem übereinstimmenden Geräte-Subsystemnamen zu durchsuchen.

DRIVERS

Weist udev an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätetreibernamen zu durchsuchen.

`ATTRS{Dateiname}`

Weist udev an, den Gerätepfad aufwärts nach einem Gerät mit übereinstimmenden sysfs-Attributwerten zu durchsuchen.

`ENV{Schlüssel}`

Der Wert einer Umgebungsvariablen, zum Beispiel `ENV{ID_BUS}="ieee1394` für die Suche nach allen Ereignissen in Zusammenhang mit der FireWire-Bus-ID.

`PROGRAM`

Weist udev an, ein externes Programm auszuführen. Damit der Schlüssel zutrifft, darf das Programm nicht den Endcode Null zurückgeben. Die Programmausgabe wird in stdout geschrieben und steht dem Schlüssel `RESULT` zur Verfügung.

`RESULT`

Überprüft den Rückgabewert bzw. die Rückgabezeichenkette des letzten `PROGRAM`-Aufrufs. Diesen Schlüssel können Sie entweder sofort der Regel mit dem `PROGRAM`-Schlüssel hinzufügen oder erst einer nachfolgenden Regel.

11.6.4 Verwenden von udev-Zuweisungsschlüsseln

Im Gegensatz zu den zuvor beschriebenen Übereinstimmungsschlüsseln definieren Zuweisungsschlüssel keine Bedingungen, die erfüllt sein müssen, sondern sie weisen den von udev verwalteten Geräteknotten Werte, Namen und Aktionen zu.

`NAME`

Der Name des zu erstellenden Geräteknottens. Nachdem der Knotenname durch eine Regel festgelegt wurde, werden alle anderen Regeln mit dem Schlüssel `NAME`, die auf diesen Knoten zutreffen, ignoriert.

`SYMLINK`

Der Name eines symbolischen Links, der dem zu erstellenden Knoten hinzugefügt werden soll. Einem Geräteknotten können mittels mehrerer Zuweisungsregeln mehrere symbolische Links hinzugefügt werden. Ebenso können Sie aber mehrere symbolische Links für einen Knoten auch in einer Regel angeben. Die Namen der einzelnen Symlinks müssen in diesem Fall jeweils durch ein Leerzeichen getrennt sein.

OWNER, GROUP, MODE

Die Berechtigungen für den neuen Geräteknoten. Die hier angegebenen Werte überschreiben sämtliche kompilierten Werte.

ATTR{*Schlüssel*}

Gibt einen Wert an, der in ein sysfs-Attribut des Ereignisgeräts geschrieben werden soll. Wenn der Operator == verwendet wird, überprüft dieser Schlüssel, ob der Wert eines sysfs-Attributs mit dem angegebenen Wert übereinstimmt.

ENV{*Schlüssel*}

Weist udev an, eine Umgebungsvariable zu exportieren. Wenn der Operator == verwendet wird, überprüft dieser Schlüssel, ob der Wert einer Umgebungsvariable mit dem angegebenen Wert übereinstimmt.

RUN

Weist udev an, der Liste der für dieses Gerät auszuführenden Programme ein Programm hinzuzufügen. Sie sollten hier nur sehr kurze Aufgaben angeben. Anderenfalls laufen Sie Gefahr, dass weitere Ereignisse für dieses Gerät blockiert werden.

LABEL

Fügt der Regel eine Bezeichnung hinzu, zu der ein GOTO direkt wechseln kann.

GOTO

Weist udev an, eine Reihe von Regeln auszulassen und direkt mit der Regel fortzufahren, die die von GOTO angegebene Bezeichnung enthält.

IMPORT{*Typ*}

Lädt Variablen in die Ereignisumgebung, beispielsweise die Ausgabe eines externen Programms. udev kann verschiedene Variablentypen importieren. Wenn kein Typ angegeben ist, versucht udev den Typ anhand des ausführbaren Teils der Dateiberechtigungen selbst zu ermitteln.

- `program` weist udev an, ein externes Programm auszuführen und dessen Ausgabe zu importieren.
- `file` weist udev an, eine Textdatei zu importieren.
- `parent` weist udev an, die gespeicherten Schlüssel des übergeordneten Geräts zu importieren.

WAIT_FOR_SYSFS

Weist udev an, auf die Erstellung der angegebenen sysfs-Datei für ein bestimmtes Gerät zu warten. Beispiel: `WAIT_FOR_SYSFS="ioerr_cnt"` fordert udev auf, so lange zu warten, bis die Datei `ioerr_cnt` erstellt wurde.

OPTIONEN

Für den Schlüssel `OPTION` stehen verschiedene Werte zur Verfügung:

- `last_rule` weist udev an, alle nachfolgenden Regeln zu ignorieren.
- `ignore_device` weist udev an, dieses Ereignis komplett zu ignorieren.
- `ignore_remove` weist udev an, alle späteren Entfernungsereignisse für dieses Gerät zu ignorieren.
- `all_partitions` weist udev an, für alle vorhandenen Partitionen eines Blockgeräts Geräteknotten zu erstellen.

11.7 Permanente Gerätebenennung

Das dynamische Geräteverzeichnis und die Infrastruktur für die udev-Regeln ermöglichen die Bereitstellung von stabilen Namen für alle Laufwerke unabhängig von ihrer Erkennungsreihenfolge oder der für das Gerät verwendeten Verbindung. Jedes geeignete Blockgerät, das der Kernel erstellt, wird von Werkzeugen mit speziellen Kenntnissen über bestimmte Busse, Laufwerktypen oder Dateisysteme untersucht. Gemeinsam mit dem vom dynamischen Kernel bereitgestellten Geräteknottennamen unterhält udev Klassen permanenter symbolischer Links, die auf das Gerät verweisen:

```
/dev/disk
|-- by-id
| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
| |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
| |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
| `-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
| |-- Photos -> ../../sdd1
| |-- SUSE10 -> ../../sda7
| `-- devel -> ../../sda6
|-- by-path
| |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
| |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
```

```

| |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
| |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
| |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
| |-- usb-02773:0:0:2 -> ../../sdd
| |-- usb-02773:0:0:2-part1 -> ../../sdd1
|-- by-uuid
| |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
| |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
`-- 4210-8F8C -> ../../sdd1

```

11.8 Von udev verwendete Dateien

`/sys/*`

Virtuelles, vom Linux-Kernel bereitgestelltes Dateisystem, das alle zur Zeit bekannten Geräte exportiert. Diese Informationen werden von udev zur Erstellung von Geräteknoten in `/dev` verwendet.

`/dev/*`

Dynamisch erstellte Geräteknoten und statische Inhalte, die beim Booten aus `/lib/udev/devices/*` kopiert werden.

Die folgenden Dateien und Verzeichnisse enthalten die entscheidenden Elemente der udev-Infrastruktur:

`/etc/udev/udev.conf`

Wichtigste udev-Konfigurationsdatei

`/etc/udev/rules.d/*`

udev-Ereigniszuordnungsregeln

`/lib/udev/devices/*`

Statischer `/dev`-Inhalt

`/lib/udev/*`

Von den udev-Regeln aufgerufene Helferprogramme

11.9 Weiterführende Informationen

Weitere Informationen zur udev-Infrastruktur finden Sie auf den folgenden Manualpages:

udev

Allgemeine Informationen zu udev, Schlüssel, Regeln und anderen wichtigen Konfigurationsbelangen.

udevadm

udevadm kann dazu verwendet werden, das Laufzeitverhalten von udev zu kontrollieren, Kernel-Ereignisse abzurufen, die Ereigniswarteschlange zu verwalten und einfache Methoden zur Fehlersuche bereitzustellen.

udev

Informationen zum udev-Ereignisverwaltungs-Daemon.

Zugriffssteuerungslisten unter Linux

12

POSIX-ACLs (Zugriffssteuerungslisten) können als Erweiterung des traditionellen Berechtigungskonzepts für Dateisystemobjekte verwendet werden. Mit ACLs können Berechtigungen flexibler als mit dem traditionellen Berechtigungskonzept definiert werden.

Der Begriff *POSIX-ACL* suggeriert, dass es sich um einen echten Standard aus der POSIX-Familie (*Portable Operating System Interface*) handelt. Die entsprechenden Standardentwürfe POSIX 1003.1e und POSIX 1003.2c wurden aus mehreren Gründen zurückgezogen. ACLs unter vielen UNIX-artigen Betriebssystemen basieren allerdings auf diesen Entwürfen und die Implementierung der in diesem Kapitel beschriebenen Dateisystem-ACLs folgt diesen beiden Standards ebenfalls. Die Standards können unter <http://wt.xpilot.org/publications/posix.1e/> eingesehen werden.

12.1 Traditionelle Dateiberechtigungen

Detaillierte Informationen über die traditionellen Dateiberechtigungen erhalten Sie auf den Info-Seiten zu `coreutils`, Knoten *Dateiberechtigungen* (`info coreutils "File permissions"`). Erweiterte Funktionen sind das `setuid`-, das `setgid`- und das `sticky`-Bit.

12.1.1 setuid-Bit

In bestimmten Situationen sind die Zugriffsberechtigungen möglicherweise zu streng. Deshalb weist Linux zusätzliche Einstellungen auf, die das vorübergehende Ändern der aktuellen Benutzer- und Gruppenidentität für eine bestimmte Aktion ermöglichen. Für das `passwd`-Programm beispielsweise werden in der Regel `root`-Berechtigungen benötigt, um auf `/etc/passwd` zuzugreifen. Diese Datei enthält wichtige Informationen, beispielsweise die Home-Verzeichnisse von Benutzern sowie Benutzer- und Gruppen-IDs. Folglich ist es einem normalen Benutzer im Regelfall nicht möglich, `passwd` zu ändern, da es zu gefährlich wäre, allen Benutzern den direkten Zugriff auf diese Datei zu gewähren. Eine mögliche Lösung dieses Problems stellt der *setuid*-Mechanismus dar. `setuid` (set user ID (Benutzer-ID festlegen)) ist ein spezielles Dateiattribut, das das System zum Ausführen entsprechend markierter Programme unter einer bestimmten Benutzer-ID veranlasst. Betrachten wir einmal den `passwd`-Befehl:

```
-rwsr-xr-x  1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

Sie sehen das `s`, das angibt, dass das `setuid`-Bit für die Benutzerberechtigung festgelegt ist. Durch das `setuid`-Bit führen alle Benutzer, die den `passwd`-Befehl aufrufen, den entsprechenden Vorgang als `root` aus.

12.1.2 setgid-Bit

Das `setuid`-Bit hat für Benutzer Gültigkeit. Es gibt jedoch eine entsprechende Eigenschaft für Gruppen, nämlich das *setgid*-Bit. Ein Programm, für das dieses Bit festgelegt wurde, wird unter der Gruppen-ID ausgeführt, unter der es gespeichert wurde, unabhängig davon, von welchem Benutzer es gestartet wird. Folglich werden in einem Verzeichnis mit dem `setgid`-Bit alle neu erstellten Dateien und Unterverzeichnisse der Gruppe zugewiesen, der das Verzeichnis zugehörig ist. Betrachten wir einmal folgendes Beispielverzeichnis:

```
drwxrws---  2 tux archive 48 Nov 19 17:12  backup
```

Sie sehen das `s`, das angibt, dass das `setgid`-Bit für die Gruppenberechtigung festgelegt ist. Der Eigentümer des Verzeichnisses sowie Mitglieder der Gruppe `archive` dürfen auf dieses Verzeichnis zugreifen. Benutzer, die nicht Mitglied dieser Gruppe sind, werden der entsprechenden Gruppe „zugeordnet“. `archive` ist die Gruppen-ID für alle geschriebenen Dateien. Ein mit der Gruppen-ID `archive` ausgeführtes Sicherungsprogramm kann auch ohne `root`-Berechtigungen auf dieses Verzeichnis zugreifen.

12.1.3 sticky-Bit

Außerdem gibt es das *sticky-Bit*. Es macht einen Unterschied, ob es einem ausführbaren Programm oder einem Verzeichnis zugehörig ist. Wenn es einem Programm zugehörig ist, wird eine auf diese Weise markierte Datei in den RAM geladen; auf diese Weise muss sie nicht bei jeder Verwendung von der Festplatte abgerufen werden. Dieses Attribut kommt selten zum Einsatz, da moderne Festplatten schnell genug sind. Wenn dieses Bit einem Verzeichnis zugewiesen ist, hindert es einen Benutzer daran, Dateien eines anderen Benutzers zu löschen. Zu den typischen Beispielen zählen die Verzeichnisse `/tmp` und `/var/tmp`:

```
drwxrwxrwt 2 root root 1160 2002-11-19 17:15 /tmp
```

12.2 Vorteile von ACLs

Traditionell sind für jedes Dateiojekt unter Linux drei Berechtigungsgruppen definiert. Diese Gruppen enthalten die Berechtigungen zum Lesen (`r`), Schreiben (`w`) und Ausführen (`x`) für den Eigentümer der Datei, die Gruppe und andere Benutzer. Zusätzlich können noch die Bits für *set user id*, *set group id* und das *sticky-Bit* gesetzt werden. Dieses schlanke Konzept ist für die meisten in der Praxis auftretenden Fälle völlig ausreichend. Für komplexere Szenarien oder erweiterte Anwendungen mussten Systemadministratoren früher eine Reihe von Tricks anwenden, um die Einschränkungen des traditionellen Berechtigungskonzepts zu umgehen.

ACLs können als Erweiterung des traditionellen Berechtigungskonzepts verwendet werden. Sie ermöglichen es, einzelnen Benutzern oder Gruppen, bei denen es sich nicht um den ursprünglichen Eigentümer oder die ursprüngliche Eigentümergruppe handelt, Berechtigungen zuzuweisen. ACLs sind eine Funktion des Linux-Kernels und werden derzeit von ReiserFS, Ext2, Ext3, JFS und XFS unterstützt. Mithilfe von ACLs können komplexe Szenarien umgesetzt werden, ohne dass auf Anwendungsebene komplexe Berechtigungsmodelle implementiert werden müssen.

Die Vorzüge von ACLs zeigen sich, wenn Sie einen Windows-Server durch einen Linux-Server ersetzen möchten. Einige der angeschlossenen Arbeitsstationen können auch nach der Migration weiter unter Windows betrieben werden. Das Linux-System stellt den Windows-Clients Datei- und Druckdienste über Samba zur Verfügung. Da Samba ACLs unterstützt, können Benutzerberechtigungen sowohl auf dem Linux-Server als auch über eine grafische Bedienoberfläche unter Windows (nur Windows NT und

höher) konfiguriert werden. Über `winbindd`, einem Teil der Samba-Suite, ist es sogar möglich, Benutzern, die nur in der Windows-Domäne existieren und über kein Konto auf dem Linux-Server verfügen, Berechtigungen zu gewähren.

12.3 Definitionen

Benutzerklasse

Das konventionelle POSIX-Berechtigungskonzept verwendet drei *Klassen* von Benutzern, um Berechtigungen im Dateisystem zuzuordnen: den Eigentümer, die Eigentümergruppe und andere Benutzer. Pro Benutzerklasse können jeweils die drei Berechtigungsbits zum Lesen (*r*), Schreiben (*w*) und Ausführen (*x*) gesetzt werden.

Zugriffs-ACL

Die Zugriffsberechtigungen von Benutzern und Gruppen auf beliebige Dateisystemobjekte (Dateien und Verzeichnisse) werden über Access ACLs (Zugriffs-ACLs) festgelegt.

Standard-ACL

Standard-ACLs können nur auf Verzeichnisse angewendet werden. Diese legen fest, welche Berechtigungen ein Dateisystemobjekt übernimmt, wenn das Objekt von seinem übergeordneten Verzeichnis erstellt wird.

ACL-Eintrag

Jede ACL besteht aus mehreren ACL-Einträgen. Ein ACL-Eintrag enthält einen Typ, einen Bezeichner für den Benutzer oder die Gruppe, auf den bzw. die sich der Eintrag bezieht, und Berechtigungen. Für einige Eintragstypen ist der Bezeichner für die Gruppe oder die Benutzer nicht definiert.

12.4 Arbeiten mit ACLs

Tabelle 12.1, „Typen von ACL-Einträgen“ (S. 203) fasst die sechs möglichen Typen von ACL-Einträgen zusammen und beschreibt die für einen Benutzer oder eine Gruppe von Benutzern verfügbaren Berechtigungen. Der Eintrag *owner* definiert die Berechtigungen des Benutzers, der Eigentümer der Datei oder des Verzeichnisses ist. Der Eintrag *owning group* definiert die Berechtigungen der Gruppe, die Eigentümer der Datei ist. Der Superuser kann den Eigentümer (*owner*) oder die Eigentümergruppe (*owning*

group) mit `chown` oder `chgrp` ändern, in welchem Fall die Einträge "owner" und "owning group" sich auf den neuen Eigentümer bzw. die neue Eigentümergruppe beziehen. Die Einträge des Typs *named user* definieren die Berechtigungen des Benutzers, der im Bezeichnerfeld des Eintrags angegeben ist. Die Einträge des Typs *named group* definieren die Berechtigungen der im Bezeichnerfeld des Eintrags angegebenen Gruppe. Nur die Einträge des Typs "named user" und "named group" verfügen über ein Bezeichnerfeld, das nicht leer ist. Der Eintrag *other* definiert die Berechtigungen aller anderen Benutzer.

Der Eintrag *mask* schränkt die durch die Einträge "named user", "named group" und "owning group" gewährten Berechtigungen ein, indem durch ihn festgelegt werden kann, welche der Berechtigungen in diesen Einträgen wirksam und welche maskiert sind. Sind Berechtigungen sowohl in einem der oben genannten Einträge als auch in der Maske vorhanden, werden sie wirksam. Berechtigungen, die nur in der Maske oder nur im eigentlichen Eintrag vorhanden sind, sind nicht wirksam, d. h., die Berechtigungen werden nicht gewährt. Die in den Einträgen "owner" und "owning group" gewährten Berechtigungen sind immer wirksam. Dieser Mechanismus wird mit dem Beispiel in [Tabelle 12.2, „Maskierung von Zugriffsberechtigungen“](#) (S. 204) verdeutlicht.

Es gibt zwei grundlegende Klassen von ACLs: Eine *minimale* ACL enthält nur die Einträge für die Typen "owner", "owning group" und "other", die den herkömmlichen Berechtigungsbits für Dateien und Verzeichnisse entsprechen. Eine *erweiterte* ACL geht über dieses Konzept hinaus. Sie muss einen Eintrag des Typs *mask* enthalten und kann mehrere Einträge des Typs "named user" und "named group" haben.

Tabelle 12.1 Typen von ACL-Einträgen

Typ	Textformat
owner	user::rwx
named user	user:name:rwx
owning group	group::rwx
named group	group:name:rwx
mask	mask::rwx
other	other::rwx

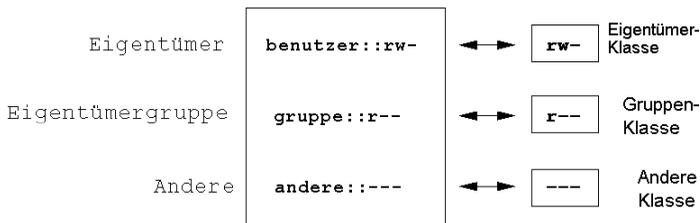
Tabelle 12.2 Maskierung von Zugriffsberechtigungen

Eintragstyp	Textformat	Berechtigungen
named user	user:geeko:r-x	r-x
mask	mask::rw-	rw-
	wirksame Berechtigungen:	r--

12.4.1 ACL-Einträge und Dateimodus-Berechtigungsbits

Abbildung 12.1, „Minimale ACL: ACL-Einträge im Vergleich zu Berechtigungsbits“ (S. 204) und [Abbildung 12.2](#), „Erweiterte ACL: ACL-Einträge im Vergleich zu Berechtigungsbits“ (S. 205) zeigen eine minimale und eine erweiterte ACL. Die Abbildungen sind in drei Blöcke unterteilt: der linke Block zeigt die Typspezifikationen der ACL-Einträge, der mittlere Block zeigt das Beispiel einer ACL und der rechte Block zeigt die entsprechenden Berechtigungsbits gemäß dem herkömmlichen Berechtigungskonzept, wie sie beispielsweise auch mit `ls -l` angezeigt werden. In beiden Fällen werden die Berechtigungen *owner class* dem ACL-Eintrag "owner" zugeordnet. *Other class*-Berechtigungen werden dem entsprechenden ACL-Eintrag zugeordnet. Die Zuordnung der Berechtigungen des Typs *group class* ist in den beiden Fällen jedoch unterschiedlich.

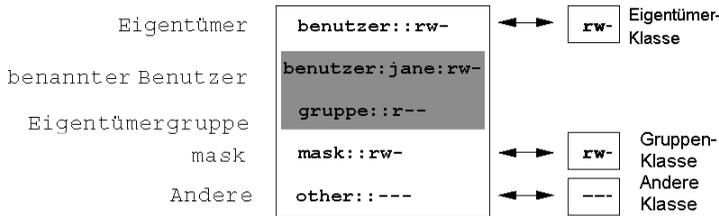
Abbildung 12.1 Minimale ACL: ACL-Einträge im Vergleich zu Berechtigungsbits



Im Fall einer minimalen ACL (ohne "mask") werden die "group class"-Berechtigungen dem ACL-Eintrag "owning group" zugeordnet. Dies ist in [Abbildung 12.1](#), „Minimale ACL: ACL-Einträge im Vergleich zu Berechtigungsbits“ (S. 204) dargestellt. Im Fall

einer erweiterten ACL (mit "mask") werden die "group class"-Berechtigungen dem "mask"-Eintrag zugeordnet. Dies ist in **Abbildung 12.2**, „Erweiterte ACL: ACL-Einträge im Vergleich zu Berechtigungsbits“ (S. 205) dargestellt.

Abbildung 12.2 *Erweiterte ACL: ACL-Einträge im Vergleich zu Berechtigungsbits*



Durch diese Art der Zuordnung ist die reibungslose Interaktion von Anwendungen mit und ohne ACL-Unterstützung gewährleistet. Die Zugriffsberechtigungen, die mittels der Berechtigungsbits festgelegt wurden, sind die Obergrenze für alle anderen „Feineinstellungen“, die per ACL vorgenommen werden. Werden Berechtigungsbits geändert, spiegelt sich dies in der ACL wider und umgekehrt.

12.4.2 Ein Verzeichnis mit einer Zugriffs-ACL

Mit `getfacl` und `setfacl` in der Kommandozeile können Sie auf ACLs zugreifen. Die Verwendung dieser Befehle wird im folgenden Beispiel erläutert:

Bevor Sie das Verzeichnis erstellen, können Sie mit dem Befehl `umask` festlegen, welche Zugriffsberechtigungen gleich beim Erstellen von Dateiobjekten maskiert werden sollen. Der Befehl `umask 027` legt die Standardberechtigungen fest: der Eigentümer erhält sämtliche Berechtigungen (0), der Gruppenschreibzugriff wird verweigert (2), alle anderen Benutzer erhalten keine Berechtigungen (7). Die entsprechenden Berechtigungsbits werden von `umask` maskiert oder deaktiviert. Weitere Informationen hierzu finden Sie auf der Manualpage `umask`.

`mkdir mydir` erstellt das Verzeichnis `mydir` mit den durch `umask` festgelegten Standardberechtigungen. Mit dem Befehl `ls -dl mydir` können Sie prüfen, ob alle Berechtigungen ordnungsgemäß zugewiesen wurden. Die Ausgabe für dieses Beispiel sieht wie folgt aus:

```
drwxr-x--- ... tux project3 ... mydir
```

Mit dem Befehl `getfacl mydir` prüfen Sie den anfänglichen Status der ACL. Es werden ähnliche Informationen wie im folgenden Beispiel zurückgegeben:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

Die ersten drei Zeilen der Ausgabe nennen Namen, Eigentümer und Eigentümergruppe des Verzeichnisses. Die drei nächsten Zeilen enthalten die drei ACL-Einträge `owner`, `owning group` und `other`. Insgesamt liefert Ihnen der Befehl `getfacl` im Fall dieser minimalen ACL keine Informationen, die Sie mit `ls` nicht auch erhalten hätten.

Ändern Sie die ACL so, dass Sie dem zusätzlichen Benutzer `geeko` und der zusätzlichen Gruppe `mascots` Lese-, Schreib- und Ausführberechtigungen gewähren, indem Sie folgenden Befehl eingeben:

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

Mit der Option `-m` kann per `setfacl` die vorhandene ACL geändert werden. Das nachfolgende Argument gibt an, welche ACL-Einträge geändert werden (mehrere Einträge werden durch Kommas voneinander getrennt). Im letzten Teil geben Sie den Namen des Verzeichnisses an, für das diese Änderungen gelten sollen. Mit dem Befehl `getfacl` können Sie sich die resultierende ACL ansehen.

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

Zusätzlich zu den von Ihnen erstellten Einträgen für den Benutzer `geeko` und die Gruppe `mascots` wurde ein "mask"-Eintrag generiert. Der `mask`-Eintrag wird automatisch gesetzt, sodass alle Berechtigungen wirksam sind. Außerdem passt `setfacl` vorhandene `mask`-Einträge automatisch an die geänderten Einstellungen an, es sei denn, Sie deaktivieren diese Funktion mit `-n`. `mask` legt die maximal wirksamen Zugriffsberechtigungen für alle Einträge innerhalb der `group class` fest. Dazu gehören `named user`, `named group` und `owning group`. Die Berechtigungsbits des Typs "group class", die mit `ls-dl mydir` ausgegeben werden, entsprechen jetzt dem `mask`-Eintrag.

```
drwxrwx---+ ... tux project3 ... mydir
```

Die erste Spalte der Ausgabe enthält ein zusätzliches +, um darauf hinzuweisen, dass für dieses Objekt eine *erweiterte* ACL vorhanden ist.

Gemäß der Ausgabe des Befehls `ls` beinhalten die Berechtigungen für den mask-Eintrag auch Schreibzugriff. Solche Berechtigungsbits bedeuten normalerweise, dass auch die Eigentümergruppe (hier `project3`) Schreibzugriff auf das Verzeichnis `mydir` erhält. Jedoch entsprechen die tatsächlich wirksamen Zugriffsberechtigungen für die Eigentümergruppe der Schnittmenge aus den für die Eigentümergruppe und den für mask definierten Berechtigungen, in unserem Beispiel also `r-x` (siehe [Tabelle 12.2, „Maskierung von Zugriffsberechtigungen“](#) (S. 204)). Was die wirksamen Berechtigungen der "owning group" in diesem Beispiel betrifft, hat sich also nach dem Hinzufügen der ACL-Einträge nichts geändert.

Bearbeiten Sie den mask-Eintrag mit `setfacl` oder `chmod`. Geben Sie beispielsweise `chmod g-w mydir` ein. `ls -dl mydir` gibt dann Folgendes aus:

```
drwxr-x---+ ... tux project3 ... mydir
```

`getfacl mydir` erzeugt die folgende Ausgabe:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx          # effective: r-x
group::r-x
group:mascots:rwx      # effective: r-x
mask::r-x
other::---
```

Nachdem Sie den Befehl `chmod` ausgeführt haben, um die Schreibberechtigung von den "group class"-Bits zu entfernen, zeigt Ihnen bereits die Ausgabe des Befehls `ls`, dass die mask-Bits entsprechend angepasst wurden: Der Schreibzugriff ist erneut auf den Eigentümer von `mydir` beschränkt. Dies wird durch die Ausgabe des Befehls `getfacl` bestätigt. Dieser Befehl fügt allen Einträgen Kommentare hinzu, deren tatsächlich wirksame Berechtigungsbits nicht mit den ursprünglich gesetzten übereinstimmen, weil sie vom mask-Eintrag herausgefiltert werden. Die ursprünglichen Berechtigungen können jederzeit mit dem Befehl `chmod g+w mydir` wiederhergestellt werden.

12.4.3 Ein Verzeichnis mit einer Standard-ACL

Verzeichnisse können über eine Standard-ACL verfügen. Dabei handelt es sich um einen speziellen Typ von ACL, der festlegt, welche Zugriffsberechtigungen neue Unterobjekte dieses Verzeichnisses bei ihrer Erstellung erben. Eine Standard-ACL wirkt sich sowohl auf Unterverzeichnisse als auch auf Dateien aus.

Auswirkungen einer Standard-ACL

Die Zugriffsberechtigungen in der Standard-ACL eines Verzeichnisses werden an Dateien und Unterverzeichnisse unterschiedlich vererbt:

- Ein Unterverzeichnis erbt die Standard-ACL des übergeordneten Verzeichnisses sowohl als seine eigene Standard-ACL als auch als Zugriffs-ACL.
- Eine Datei erbt die Standard-ACL als ihre eigene Zugriffs-ACL.

Alle Systemaufrufe, die Dateisystemobjekte anlegen, verwenden einen `mode`-Parameter, der die Zugriffsberechtigungen für das neu erstellte Dateisystemobjekt definiert. Hat das übergeordnete Verzeichnis keine Standard-ACL, werden die mit `umask` definierten Berechtigungsbits mit dem `mode`-Parameter von den Berechtigungen abgezogen und das Ergebnis wird dem neuen Objekt zugewiesen. Existiert eine Standard-ACL für das übergeordnete Verzeichnis, entsprechen die dem neuen Objekt zugewiesenen Berechtigungsbits der Schnittmenge aus den Berechtigungen des `mode`-Parameters und den in der Standard-ACL festgelegten Berechtigungen. `umask` wird in diesem Fall nicht beachtet.

Standard-ACLs in der Praxis

Die drei folgenden Beispiele führen Sie an die wichtigsten Operationen an Verzeichnissen und Standard-ACLs heran:

1. Fügen Sie dem vorhandenen Verzeichnis `mydir` eine Standard-ACL hinzu, indem Sie folgenden Befehl eingeben:

```
setfacl -d -m group:mascots:r-x mydir
```

Die Option `-d` des Befehls `setfacl` weist `setfacl` an, die folgenden Änderungen (Option `-m`) an der Standard-ACL vorzunehmen.

Sehen Sie sich das Ergebnis dieses Befehls genauer an:

```
getfacl mydir

# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other:---
default:user::rwx
default:group:r-x
default:group:mascots:r-x
default:mask:r-x
default:other:---
```

`getfacl` gibt sowohl die Zugriffs-ACL als auch die Standard-ACL zurück. Die Standard-ACL setzt sich aus allen Zeilen zusammen, die mit `default` beginnen. Obwohl Sie den Befehl `setfacl` nur mit einem Eintrag für die Gruppe `mascots` für die Standard-ACL ausgeführt haben, hat `setfacl` automatisch alle anderen Einträge aus der Zugriffs-ACL kopiert, um so eine gültige Standard-ACL zu bilden. Standard-ACLs haben keine direkten Auswirkungen auf Zugriffsberechtigungen. Sie wirken sich nur beim Erstellen von Dateisystemobjekten aus. Diese neuen Objekte übernehmen Berechtigungen nur aus der Standard-ACL ihres übergeordneten Verzeichnisses.

2. Im nächsten Beispiel wird mit `mkdir` ein Unterverzeichnis in `mydir` angelegt, das die Standard-ACL übernimmt.

```
mkdir mydir/mysubdir

getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: project3
user::rwx
group::r-x
group:mascots:r-x
mask:r-x
other:---
default:user:rwx
```

```
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other::---
```

Wie erwartet, hat das neu angelegte Unterverzeichnis `mysubdir` die Berechtigungen aus der Standard-ACL des übergeordneten Verzeichnisses geerbt. Die Zugriffs-ACL von `mysubdir` ist ein exaktes Abbild der Standard-ACL von `mydir`. Die Standard-ACL, die dieses Verzeichnis an ihre untergeordneten Objekte weitervererbt, ist ebenfalls dieselbe.

3. Legen Sie mit `touch` eine Datei im Verzeichnis `mydir` an. Beispiel: `touch mydir/myfile`. `ls -l mydir/myfile` gibt Folgendes zurück:

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

Die Ausgabe von `getfacl mydir/myfile` ist:

```
# file: mydir/myfile
# owner: tux
# group: project3
user::rw-
group::r-x          # effective:r--
group:mascots:r-x   # effective:r--
mask:r--
other::---
```

`touch` übergibt `mode` mit dem Wert `0666`. Dies bedeutet, dass neue Dateien mit Lese- und Schreibberechtigungen für alle Benutzerklassen angelegt werden, vorausgesetzt, `umask` oder die Standard-ACL enthalten keine weiteren Einschränkungen (siehe „**Auswirkungen einer Standard-ACL**“ (S. 208)). Am konkreten Beispiel heißt dies, dass alle Zugriffsberechtigungen, die nicht im `mode`-Wert enthalten sind, aus den entsprechenden ACL-Einträgen entfernt werden. Aus dem ACL-Eintrag der "group class" wurden keine Berechtigungen entfernt, allerdings wurde der `mask`-Eintrag dahin gehend angepasst, dass Berechtigungsbits, die nicht mit `mode` gesetzt werden, maskiert werden.

Auf diese Weise ist sichergestellt, dass Anwendungen, zum Beispiel Compiler, reibungslos mit ACLs interagieren können. Sie können Dateien mit beschränkten Zugriffsberechtigungen erstellen und diese anschließend als ausführbar markieren. Über den `mask`-Mechanismus ist gewährleistet, dass die richtigen Benutzer und Gruppen die Dateien wie gewünscht ausführen können.

12.4.4 Der ACL-Auswertungsalgorithmus

Bevor ein Prozess oder eine Anwendung Zugriff auf ein durch eine ACL geschütztes Dateisystemobjekt erhält, wird ein Auswertungsalgorithmus angewendet. Als grundlegende Regel werden die ACL-Einträge in der folgenden Reihenfolge geprüft: Eigentümer, benannter Benutzer, Eigentümergruppe oder benannte Gruppe und andere. Über den Eintrag, der am besten auf den Prozess passt, wird schließlich der Zugriff geregelt. Berechtigungen werden nicht akkumuliert.

Komplizierter werden die Verhältnisse, wenn ein Prozess zu mehr als einer Gruppe gehört, also potenziell auch mehrere group-Einträge dazu passen können. Aus den passenden Einträgen mit den erforderlichen Berechtigungen wird per Zufallsprinzip ein Eintrag ausgesucht. Es ist unerheblich, welcher der Einträge das Endergebnis „Zugriff gewährt“ auslöst. Ähnliches gilt, wenn keiner der passenden group-Einträge die erforderlichen Berechtigungen enthält. In diesem Fall löst ein per Zufallsprinzip ausgewählter Eintrag das Ergebnis „Zugriff verweigert“ aus.

12.5 ACL-Unterstützung in Anwendungen

Mit ACLs können sehr anspruchsvolle Berechtigungsszenarien umgesetzt werden, die den Anforderungen moderner Anwendungen gerecht werden. Das traditionelle Berechtigungskonzept und ACLs lassen sich geschickt miteinander kombinieren. Die grundlegenden Dateibefehle (`cp`, `mv`, `ls` usw.) unterstützen ACLs ebenso wie Samba und Konqueror.

Viele Editoren und Dateimanager bieten jedoch keine ACL-Unterstützung. Beim Kopieren von Dateien mit Emacs gehen die ACLs der entsprechenden Dateien beispielsweise noch verloren. Wenn Dateien mit einer Zugriffs-ACL im Editor bearbeitet werden, hängt es vom Backup-Modus des verwendeten Editors ab, ob die Zugriffs-ACL nach Abschluss der Bearbeitung weiterhin vorliegt. Schreibt der Editor die Änderungen in die Originaldatei, bleibt die Zugriffs-ACL erhalten. Legt der Editor eine neue Datei an, die nach Abschluss der Änderungen in die alte umbenannt wird, gehen die ACLs möglicherweise verloren, es sei denn, der Editor unterstützt ACLs. Mit Ausnahme von Star Archiver gibt es derzeit keine Backup-Anwendungen, bei deren Verwendung die ACLs erhalten bleiben.

12.6 Weiterführende Informationen

Ausführliche Informationen zu ACLs finden Sie unter <http://acl.bestbits.at/>. Weitere Informationen finden Sie außerdem auf den man-Seiten für `getfacl(1)`, `acl(5)` und `setfacl(1)`.

Authentifizierung mit PAM

Während des Authentifizierungsprozesses verwendet Linux PAM (Pluggable Authentication Modules, einfügbare Authentifizierungsmodule) als Schicht für die Vermittlung zwischen Benutzer und Anwendung. PAM-Module sind systemweit verfügbar, sodass sie von jeder beliebigen Anwendung angefordert werden können. In diesem Kapitel wird beschrieben, wie der modulare Authentifizierungsmechanismus funktioniert und wie er konfiguriert wird.

Häufig möchten Systemadministratoren und Programmierer den Zugriff auf bestimmte Teile des Systems einschränken oder die Nutzung bestimmter Funktionen einer Anwendung begrenzen. Ohne PAM müssen die Anwendungen bei jedem neu eingeführten Authentifizierungsmechanismus, wie LDAP, Samba oder Kerberos, angepasst werden. Dieser Prozess ist jedoch sehr zeitaufwändig und fehleranfällig. Eine Möglichkeit, diese Nachteile zu vermeiden, ist eine Trennung zwischen den Anwendungen und dem Authentifizierungsmechanismus und das Delegieren der Authentifizierung an zentral verwaltete Module. Wenn ein neues Authentifizierungsschema erforderlich ist, genügt es, ein geeigneter PAM-Modus für die Verwendung durch das betreffende Programm anzupassen oder zu schreiben.

Jedes Programm, das mit dem PAM-Mechanismus arbeitet, verfügt über eine eigene Konfigurationsdatei im Verzeichnis `/etc/pam.d/programmname`. Mit diesen Dateien werden die für die Authentifizierung verwendeten PAM-Module definiert. Darüber hinaus sind im Verzeichnis `/etc/security` globale Konfigurationsdateien für PAM-Module gespeichert, in denen die genaue Verhaltensweise der Module definiert ist (Beispiele: `pam_env.conf` und `time.conf`). Jede Anwendung, die ein PAM-Modul verwendet, ruft eine Reihe von PAM-Funktionen auf, mit denen dann die Informationen in den verschiedenen Konfigurationsdateien verarbeitet und das Ergebnis an die anfordernde Anwendung zurückgegeben wird.

Zur Vereinfachung der Erstellung und Verwaltung von PAM-Modulen stehen Dateien mit gängigen Standardkonfigurationen für die Module `auth`, `account`, `password` und `session` bereit. Diese werden den PAM-Konfigurationen der einzelnen Anwendungen entnommen. Aktualisierungen der globalen PAM-Konfigurationsmodule in `common-*` werden daher auf alle PAM-Konfigurationsdateien übertragen. Die manuelle Aktualisierung jeder einzelnen PAM-Konfigurationsdatei durch den Administrator entfällt somit.

Die globalen, allgemeinen PAM-Konfigurationsdateien werden mit dem Tool `pam-config` verwaltet. Dieses Tool fügt der Konfiguration automatisch neue Module hinzu, ändert die Konfiguration vorhandener Module oder löscht einzelne Module oder Optionen aus den Konfigurationen. Manuelle Vorgänge bei der Verwaltung der PAM-Konfigurationen werden dadurch minimiert oder gar nicht mehr benötigt.

13.1 Struktur einer PAM-Konfigurationsdatei

Jede Zeile in einer PAM-Konfigurationsdatei enthält maximal vier Spalten:

```
<Type of module> <Control flag> <Module path> <Options>
```

PAM-Module werden als Stapel verarbeitet. Die unterschiedlichen Modultypen dienen verschiedenen Zwecken. So wird beispielsweise mit einem Modul das Passwort und mit einem anderen Modul der Standort überprüft, von dem aus auf das System zugegriffen wird. Mit einem dritten Modul können beispielsweise benutzerspezifische Einstellungen abgelesen werden. PAM sind ungefähr vier verschiedene Modultypen bekannt:

`auth`

Dieser Modultyp dient der Überprüfung der Authentizität des Benutzers. Dies erfolgt in der Regel über die Abfrage des Passworts, es kann jedoch auch mithilfe einer Chipkarte oder biometrischer Daten (Fingerabdruck oder Scannen der Iris) erreicht werden.

`Konto`

Mit Modulen dieses Typs wird überprüft, ob der Benutzer allgemein zur Verwendung des angeforderten Diensts berechtigt ist. Solch eine Prüfung sollte beispielsweise durchgeführt werden, um sicherzustellen, dass keine Anmeldung mit einem Benutzernamen eines nicht mehr gültigen Kontos erfolgen kann.

password

Mit diesem Modultyp kann die Änderung eines Authentifizierungs-Token aktiviert werden. In den meisten Fällen handelt es sich hierbei um ein Passwort.

session

Mit diesem Modultyp werden Benutzersitzungen verwaltet und konfiguriert. Sie werden vor und nach der Authentifizierung gestartet, um Anmeldeversuche in Systemprotokollen aufzuzeichnen und die spezielle Umgebung des Benutzers (Mailkonten, Home-Verzeichnis, Systemgrenzen usw.) zu konfigurieren.

Die zweite Spalte enthält Steuerflaggen, mit denen das Verhalten der gestarteten Module beeinflusst wird:

required

Ein Modul mit dieser Flagge muss erfolgreich verarbeitet werden, damit die Authentifizierung fortgesetzt werden kann. Wenn ein Modul mit der Flagge `required` ausfällt, werden alle anderen Module mit derselben Flagge verarbeitet, bevor der Benutzer eine Meldung bezüglich des Fehlers beim Authentifizierungsversuch erhält.

requisite

Module mit dieser Flagge müssen ebenfalls erfolgreich verarbeitet werden, ähnlich wie Module mit der Flagge `required`. Falls jedoch ein Modul mit dieser Flagge ausfällt, erhält der Benutzer sofort eine entsprechende Rückmeldung und es werden keine weiteren Module verarbeitet. Bei einem erfolgreichen Vorgang werden die anderen Module nachfolgend verarbeitet genau wie alle Module mit der Flagge `required`. Die Flagge `requisite` kann als Basisfilter verwendet werden, um zu überprüfen, ob bestimmte Bedingungen erfüllt sind, die für die richtige Authentifizierung erforderlich sind.

sufficient

Wenn ein Modul mit dieser Flagge erfolgreich verarbeitet wurde, erhält die anfordernde Anwendung sofort eine Nachricht bezüglich des erfolgreichen Vorgangs und keine weiteren Module werden verarbeitet, vorausgesetzt, es ist zuvor kein Fehler bei einem Modul mit der Flagge `required` aufgetreten. Ein Fehler eines Moduls mit der Flagge `sufficient` hat keine direkten Auswirkungen auf die Verarbeitung oder die Verarbeitungsreihenfolge nachfolgender Module.

optional

Ein Fehler oder die erfolgreiche Verarbeitung hat bei diesem Modul keine direkten Folgen. Dies kann für Module sinnvoll sein, die nur der Anzeige einer Meldung (beispielsweise um dem Benutzer mitzuteilen, dass er eine E-Mail erhalten hat) dienen, ohne weitere Aktionen auszuführen.

include

Wenn diese Flagge festgelegt ist, wird die als Argument angegebene Datei an dieser Stelle eingefügt.

Der Modulpfad muss nicht explizit angegeben werden, solange sich das Modul im Standardverzeichnis `/lib/security` befindet (für alle von openSUSE® unterstützten 64-Bit-Plattformen lautet das Verzeichnis `/lib64/security`). Die vierte Spalte kann eine Option für das angegebene Modul enthalten, wie beispielsweise `debug` (zum Aktivieren der Fehlersuche) oder `nullok` (um die Verwendung leerer Passwörter zu ermöglichen).

13.2 PAM-Konfiguration von sshd

Betrachten Sie zum Verständnis der Theorie, auf der PAM basiert, die PAM-Konfiguration von `sshd` als praktisches Beispiel:

Beispiel 13.1 PAM-Konfiguration für sshd

```
##PAM-1.0
auth    include      common-auth
auth    required     pam_nologin.so
account include     common-account
password include    common-password
session include     common-session
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
#session optional   pam_resmgr.so fake_ttyname
```

Die typische PAM-Konfiguration einer Anwendung (in diesem Fall `sshd`) enthält vier Anweisungen, die sich auf die Konfigurationsdateien von vier Modultypen beziehen: `common-auth`, `common-account`, `common-password` und `common-session`. In diesen vier Dateien ist die Standardkonfiguration für die einzelnen Modultypen gespeichert. Wenn Sie diese Dateien aufnehmen, anstatt jedes Modul für die einzelnen PAM-Anwendungen separat aufzurufen, erhalten Sie automatisch eine aktualisierte PAM-Konfiguration, wenn der Administrator die Standardeinstellungen ändert. Vorher

mussten alle Konfigurationsdateien für alle Anwendungen manuell angepasst werden, wenn Änderungen an PAM vorgenommen oder neue Anwendungen installiert wurden. Jetzt wird die PAM-Konfiguration mithilfe von zentralen Konfigurationsdateien ausgeführt und alle Änderungen werden automatisch über die PAM-Konfiguration der einzelnen Dienste weitergegeben.

Die erste include-Datei (`common-auth`) ruft zwei Module des Typs `auth` auf: `pam_env` und `pam_unix2`. Weitere Informationen hierzu finden Sie unter **Beispiel 13.2**, „Standardkonfiguration für den Abschnitt `auth`“ (S. 217).

Beispiel 13.2 Standardkonfiguration für den Abschnitt `auth`

```
auth    required      pam_env.so
auth    required      pam_unix2.so
```

Mit dem ersten Modul, `pam_env`, wird die Datei `/etc/security/pam_env.conf` geladen, um die in dieser Datei angegebenen Variablen festzulegen. Hiermit kann die Variable `DISPLAY` auf den richtigen Wert gesetzt werden, da dem Modul `pam_env` der Standort bekannt ist, an dem der Anmeldevorgang stattfindet. Mit dem zweiten Modul, `pam_unix2`, werden der Anmelde-name und das Passwort des Benutzers mit `/etc/passwd` und `/etc/shadow` abgeglichen.

Wenn die in `common-auth` angegebenen Dateien erfolgreich aufgerufen wurden, wird mit dem dritten Modul `pam_nologin` überprüft, ob die Datei `/etc/nologin` vorhanden ist. Ist dies der Fall, darf sich kein anderer Benutzer außer `root` anmelden. Der gesamte Stapel der `auth`-Module wird verarbeitet, bevor `sshd` eine Rückmeldung darüber erhält, ob der Anmeldevorgang erfolgreich war. Wenn alle Module des Stapels die Flagge `required` aufweisen, müssen sie alle erfolgreich verarbeitet werden, bevor `sshd` eine Meldung bezüglich des positiven Ergebnisses erhält. Falls bei einem der Module ein Fehler auftritt, wird der vollständige Modulstapel verarbeitet und erst dann wird `sshd` bezüglich des negativen Ergebnisses benachrichtigt.

Nachdem alle Module vom Typ `auth` erfolgreich verarbeitet wurden, wird eine weitere include-Anweisung verarbeitet, in diesem Fall die in **Beispiel 13.3**, „Standardkonfiguration für den Abschnitt `account`“ (S. 218). Die Datei `common-account` enthält lediglich ein Modul, `pam_unix2`. Wenn `pam_unix2` als Ergebnis zurückgibt, dass der Benutzer vorhanden ist, erhält `sshd` eine Meldung mit dem Hinweis auf diesen erfolgreichen Vorgang und der nächste Modulstapel (`password`) wird verarbeitet, wie in **Beispiel 13.4**, „Standardkonfiguration für den Abschnitt `password`“ (S. 218) dargestellt.

Beispiel 13.3 Standardkonfiguration für den Abschnitt `account`

```
account required          pam_unix2.so
```

Beispiel 13.4 Standardkonfiguration für den Abschnitt `password`

```
password required       pam_pwcheck.so  nullok cracklib
password required       pam_unix2.so   nullok use_authtok
#password required      pam_make.so   /var/yp
```

Auch hier beinhaltet die PAM-Konfiguration von `sshd` nur eine `include`-Anweisung, die sich auf die Standardkonfiguration für `password`-Module in der Datei `common-password` bezieht. Diese Module müssen erfolgreich abgeschlossen werden (Steuerflagge `required`), wenn die Anwendung die Änderung eines Authentifizierungs-Token anfordert. Für die Änderung eines Passworts oder eines anderen Authentifizierungs-Token ist eine Sicherheitsprüfung erforderlich. Dies erfolgt über das Modul `pam_pwcheck`. Das anschließend verwendete Modul `pam_unix2` überträgt alle alten und neuen Paswörter von `pam_pwcheck`, sodass der Benutzer die Authentifizierung nicht erneut ausführen muss. Dadurch ist es zudem unmöglich, die von `pam_pwcheck` durchgeführten Prüfungen zu umgehen. Die Module vom Typ `password` sollten immer dann verwendet werden, wenn die vorherigen Module vom Typ `account` oder `auth` so konfiguriert sind, dass bei einem abgelaufenen Passwort eine Fehlermeldung angezeigt wird.

Beispiel 13.5 Standardkonfiguration für den Abschnitt `session`

```
session required        pam_limits.so
session required        pam_unix2.so
session optional        pam_umask.so
```

Im letzten Schritt werden die in der Datei `common-session` gespeicherten Module vom Typ `session` aufgerufen, um die Sitzung gemäß den Einstellungen für den betreffenden Benutzer zu konfigurieren. Mit dem Modul `pam_limits` wird die Datei `/etc/security/limits.conf` geladen, mit der Nutzungseinschränkungen für bestimmte Systemressourcen definiert werden können. Das Modul `pam_unix2` wird erneut verarbeitet. Das Modul `pam_umask` kann zur Festlegung der Dateimoduserstellungsmaske verwendet werden. Da dieses Modul mit dem Flag `Optional` versehen ist, wirkt sich ein Fehler in diesem Modul nicht auf die erfolgreiche Ausführung des gesamten Sitzungsmodulstapels aus. Die `session`-Module werden beim Abmelden des Benutzers ein zweites Mal aufgerufen.

13.3 Konfigurieren von PAM mit pam-config

Das Tool `pam-config` hilft bei der Konfiguration der globalen PAM-Konfigurationsdateien im Verzeichnis `/etc/pam.d/common-*-pc`. Mit dem Kommando `pam-config` können Sie Ihre PAM-Konfigurationsdateien verwalten. Sie können Ihren PAM-Konfigurationen neue Module hinzufügen oder Module löschen und die Optionen einzelner Module ändern. Da sich diese Änderungen nur auf die globalen PAM-Konfigurationsdateien auswirken, sind keine manuellen Anpassungen der PAM-Konfigurationen einzelner Anwendungen mehr nötig.

Ein einfaches Szenarium, in dem die Funktionen von `pam-config` von Nutzen sind, sieht zum Beispiel wie folgt aus:

- 1 Automatische Generierung einer neuen PAM-Konfiguration für Unix** Erstellen Sie mit `pam-config` eine möglichst einfache Konfiguration, die Sie später erweitern können. Das Kommando `pam-config --create` erstellt eine einfache UNIX-Authentifizierungskonfiguration. Bereits vorhandene, nicht von `pam-config` verwaltete Konfigurationsdateien werden überschrieben. Allerdings werden von diesen Dateien Sicherungskopien mit dem Namen `*.pam-config-backup` erstellt.
- 2 Hinzufügen einer neuen Authentifizierungsmethode** Zum Hinzufügen einer neuen Authentifizierungsmethode (z. B. LDAP) zu Ihrem PAM-Modulstapel benötigen Sie lediglich das Kommando `pam-config --add --ldap`. Die LDAP-Authentifizierungsmethode wird allen `common-*-pc`-PAM-Konfigurationsdateien hinzugefügt, auf die diese Methode anwendbar ist.
- 3 Aktivieren der Debug-Funktion für Testzwecke** Um sicherzustellen, dass die neue Authentifizierungsmethode wie geplant funktioniert, aktivieren Sie die Debug-Funktion für alle PAM-Vorgänge. Im Falle von LDAP verwenden Sie dazu das Kommando `pam-config --add --ldap-debug`. Die Debug-Ausgabe finden Sie unter `/var/log/messages`.
- 4 Abfragen der Konfiguration** Bevor Sie die neue PAM-Konfiguration anwenden, sollten Sie sicherstellen, dass sie alle gewünschten Optionen enthält. Das Modul `pam-config --query --` gibt sowohl den Typ als auch die Optionen des abgefragten PAM-Moduls zurück.

5 Entfernen der Debug-Optionen Wenn Sie mit Ihrer neuen Konfiguration zufrieden sind, entfernen Sie die Debug-Optionen. Im Falle von LDAP verwenden Sie dazu das Kommando `pam-config --delete --ldap-debug`. Falls Sie auch für andere Module Debug-Optionen hinzugefügt haben, deaktivieren Sie diese mit den betreffenden Kommandos.

Wenn Sie Ihre PAM-Konfigurationsdateien mit dem Kommando `pam-config --create` völlig neu erstellen, werden symbolische Links zwischen den `common-*`-Dateien und den `common-*-pc`-Dateien erstellt. `pam-config` bearbeitet nur die `common-*-pc`-Konfigurationsdateien. Falls Sie diese symbolischen Links entfernen, setzen Sie `pam-config` praktisch außer Kraft, da `pam-config` nur die `common-*-pc`-Dateien bearbeitet, diese aber ohne die symbolischen Links nicht verwendet werden können.

Weitere Informationen zum Kommando `pam-config` und dessen Optionen finden Sie auf der `man`-Seite von `pam-config` (`pam-config(8)`).

13.4 Weiterführende Informationen

Im Verzeichnis `/usr/share/doc/packages/pam` des installierten Systems finden Sie folgende zusätzliche Dokumentation:

READMEs

Auf der obersten Ebene dieses Verzeichnisses finden Sie einige allgemeine README-Dateien. Im Unterverzeichnis `modules` sind README-Dateien zu den verfügbaren PAM-Modulen gespeichert.

Linux-PAM-Handbuch für Systemadministratoren

Dieses Dokument enthält alle Informationen zu PAM, die ein Systemadministrator benötigt. Hier werden mehrere Themen von der Syntax der Konfigurationsdateien bis hin zu Sicherheitsaspekten von PAM behandelt. Das Dokument ist als PDF-Datei, im HTML-Format oder im reinen Textformat verfügbar.

Linux-PAM-Handbuch für Modulprogrammierer

In diesem Dokument wird das Thema aus der Sicht der Entwickler zusammengefasst. Hier erhalten Sie Informationen zum Programmieren standardkompatibler PAM-Module. Es ist als PDF-Datei, im HTML-Format oder im reinen Textformat verfügbar.

Linux-PAM-Handbuch für Anwendungsentwickler

Dieses Dokument enthält alle Informationen, die ein Anwendungsentwickler benötigt, der die PAM-Bibliotheken verwenden möchte. Es ist als PDF-Datei, im HTML-Format oder im reinen Textformat verfügbar.

Die man-Seiten zu PAM

Für PAM im Allgemeinen, aber auch für die einzelnen PAM-Module, stehen man-Seiten zur Verfügung, die einen hervorragenden Überblick über die von der jeweiligen Komponente bereitgestellten Funktionen bieten.

Thorsten Kukuk hat mehrere PAM-Module entwickelt und unter <http://www.suse.de/~kukuk/pam/> einige Informationen zu diesen Modulen zur Verfügung gestellt.

Teil IV. Services

Grundlegendes zu Netzwerken

Linux stellt die erforderlichen Netzwerkwerkzeuge und -funktionen für die Integration in alle Arten von Netzwerkstrukturen zur Verfügung. Das üblicherweise von Linux verwendete Protokoll, TCP/IP, verfügt über unterschiedliche Dienste und Sonderfunktionen, die im Folgenden beschrieben werden. Der Netzwerkzugriff über eine Netzwerkkarte, ein Modem oder ein anderes Gerät kann mit YaST konfiguriert werden. Die manuelle Konfiguration ist ebenfalls möglich. In diesem Kapitel werden nur die grundlegenden Mechanismen sowie die zugehörigen Netzwerkkonfigurationsdateien beschrieben.

Linux und andere Unix-Betriebssysteme verwenden das TCP/IP-Protokoll. Hierbei handelt es sich nicht um ein einzelnes Netzwerkprotokoll, sondern um eine Familie von Netzwerkprotokollen, die unterschiedliche Dienste zur Verfügung stellen. Die in **Tabelle 14.1, „Verschiedene Protokolle aus der TCP/IP-Familie“** (S. 226) aufgelisteten Protokolle dienen dem Datenaustausch zwischen zwei Computern über TCP/IP. Über TCP/IP verbundene Netzwerke bilden zusammen ein weltweites Netzwerk, das in seiner Gesamtheit auch als „das Internet“ bezeichnet wird.

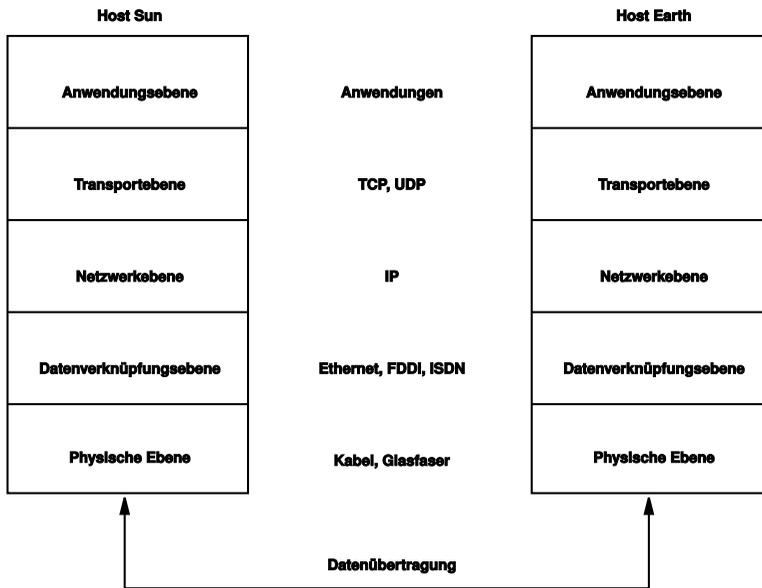
RFC steht für *Request for Comments*. RFCs sind Dokumente, die unterschiedliche Internetprotokolle und Implementierungsverfahren für das Betriebssystem und seine Anwendungen beschreiben. Die RFC-Dokumente beschreiben das Einrichten der Internetprotokolle. Weitere Informationen zu diesen Protokollen finden Sie in den entsprechenden RFC-Dokumenten. Diese sind online unter <http://www.ietf.org/rfc.html> verfügbar.

Tabelle 14.1 *Verschiedene Protokolle aus der TCP/IP-Familie*

Protokoll	Beschreibung
TCP	Transmission Control Protocol: Ein verbindungsorientiertes sicheres Protokoll. Die zu übertragenden Daten werden von der Anwendung zunächst als Datenstrom gesendet und anschließend vom Betriebssystem in das richtige Format konvertiert. Die entsprechende Anwendung auf dem Zielhost empfängt die Daten im ursprünglichen Datenstromformat, in dem sie anfänglich gesendet wurden. TCP ermittelt, ob Daten während der Übertragung verloren gegangen sind, und stellt sicher, dass keine Verwechslungen der Daten vorliegen. TCP wird immer dann implementiert, wenn die Datensequenz eine Rolle spielt.
UDP	User Datagram Protocol: Ein verbindungsloses, nicht sicheres Protokoll. Die zu übertragenden Daten werden in Form von anwendungsseitig generierten Paketen gesendet. Es ist nicht garantiert, in welcher Reihenfolge die Daten beim Empfänger eingehen, und ein Datenverlust ist immer möglich. UDP ist geeignet für datensatzorientierte Anwendungen. Es verfügt über eine kürzere Latenzzeit als TCP.
ICMP	Internet Control Message Protocol: Dies ist im Wesentlichen kein Protokoll für den Endbenutzer, sondern ein spezielles Steuerungsprotokoll, das Fehlerberichte ausgibt und das Verhalten von Computern, die am TCP/IP-Datentransfer teilnehmen, steuern kann. Außerdem bietet es einen speziellen Echomodus, der mit dem Programm "ping" angezeigt werden kann.
IGMP	Internet Group Management Protocol: Dieses Protokoll kontrolliert das Verhalten des Rechners beim Implementieren von IP Multicast.

Der Datenaustausch findet wie in **Abbildung 14.1**, „**Vereinfachtes Schichtmodell für TCP/IP**“ (S. 227) dargestellt in unterschiedlichen Schichten statt. Die eigentliche Netzwerkschicht ist der unsichere Datentransfer über IP (Internet Protocol). Oberhalb von IP gewährleistet TCP (Transmission Control Protocol) bis zu einem gewissen Grad die Sicherheit des Datentransfers. Die IP-Schicht wird vom zugrunde liegenden Hardware-abhängigen Protokoll, z. B. Ethernet, unterstützt.

Abbildung 14.1 Vereinfachtes Schichtmodell für TCP/IP



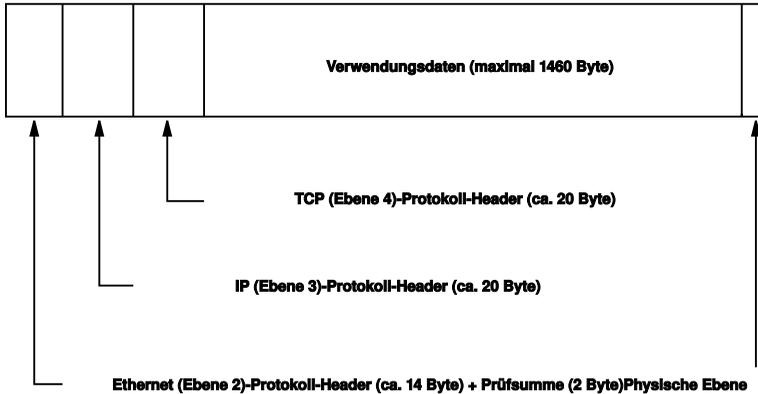
Dieses Diagramm bietet für jede Schicht ein oder zwei Beispiele. Die Schichten sind nach *Abstraktionsstufen* sortiert. Die unterste Schicht ist sehr Hardware-nah. Die oberste Schicht ist beinahe vollständig von der Hardware losgelöst. Jede Schicht hat ihre eigene spezielle Funktion. Die speziellen Funktionen der einzelnen Schichten gehen bereits aus ihrer Bezeichnung hervor. Die Datenverbindungs- und die physische Schicht repräsentieren das verwendete physische Netzwerk, z. B. das Ethernet.

Fast alle Hardwareprotokolle arbeiten auf einer paketorientierten Basis. Die zu übertragenden Daten werden in *Pakete* unterteilt, da sie nicht alle auf einmal gesendet werden können. Die maximale Größe eines TCP/IP-Pakets beträgt ca. 64 KB. Die Pakete sind in der Regel jedoch sehr viel kleiner, da die Netzwerkhardware ein einschränkender Faktor sein kann. Die maximale Größe eines Datenpakets in einem Ethernet beträgt ca. 1500 Byte. Die Größe eines TCP/IP-Pakets ist auf diesen Wert begrenzt, wenn die Daten über ein Ethernet gesendet werden. Wenn mehr Daten übertragen werden, müssen vom Betriebssystem mehr Datenpakete gesendet werden.

Damit die Schichten ihre vorgesehenen Funktionen erfüllen können, müssen im Datenpaket zusätzliche Informationen über die einzelnen Schichten gespeichert sein. Diese Informationen werden im *Header* des Pakets gespeichert. Jede Schicht stellt jedem ausgehenden Paket einen kleinen Datenblock voran, den so genannten Protokoll-

Header. Ein Beispiel für ein TCP/IP-Datenpaket, das über ein Ethernetkabel gesendet wird, ist in **Abbildung 14.2**, „TCP/IP-Ethernet-Paket“ (S. 228) dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

Abbildung 14.2 TCP/IP-Ethernet-Paket



Wenn eine Anwendung Daten über das Netzwerk sendet, werden diese Daten durch alle Schichten geleitet, die mit Ausnahme der physischen Schicht alle im Linux-Kernel implementiert sind. Jede Schicht ist für das Vorbereiten der Daten zur Weitergabe an die nächste Schicht verantwortlich. Die unterste Schicht ist letztendlich für das Senden der Daten verantwortlich. Bei eingehenden Daten erfolgt die gesamte Prozedur in umgekehrter Reihenfolge. Die Protokoll-Header werden von den transportierten Daten in den einzelnen Schichten wie die Schalen einer Zwiebel entfernt. Die Transportschicht ist schließlich dafür verantwortlich, die Daten den Anwendungen am Ziel zur Verfügung zu stellen. Auf diese Weise kommuniziert eine Schicht nur mit der direkt darüber bzw. darunter liegenden Schicht. Für Anwendungen ist es irrelevant, ob die Daten über ein 100 MBit/s schnelles FDDI-Netzwerk oder über eine 56-KBit/s-Modemleitung übertragen werden. Ähnlich spielt es für die Datenverbindung keine Rolle, welche Art von Daten übertragen wird, solange die Pakete das richtige Format haben.

14.1 IP-Adressen und Routing

Die in diesem Abschnitt enthaltenen Informationen beziehen sich nur auf IPv4-Netzwerke. Informationen zum IPv6-Protokoll, dem Nachfolger von IPv4, finden Sie in **Abschnitt 14.2**, „IPv6 – Das Internet der nächsten Generation“ (S. 231).

14.1.1 IP-Adressen

Jeder Computer im Internet verfügt über eine eindeutige 32-Bit-Adresse. Diese 32 Bit (oder 4 Byte) werden in der Regel wie in der zweiten Zeile in **Beispiel 14.1**, „**IP-Adressen schreiben**“ (S. 229) dargestellt geschrieben.

Beispiel 14.1 IP-Adressen schreiben

```
IP Address (binary): 11000000 10101000 00000000 00010100
IP Address (decimal): 192. 168. 0. 20
```

Im Dezimalformat werden die vier Byte in Dezimalzahlen geschrieben und durch Punkte getrennt. Die IP-Adresse wird einem Host oder einer Netzwerkschnittstelle zugewiesen. Diese Adresse kann weltweit nur einmal verwendet werden. Es gibt zwar Ausnahmen zu dieser Regel, diese sind jedoch für die folgenden Abschnitte nicht relevant.

Die Punkte in IP-Adressen geben das hierarchische System an. Bis in die 1990er-Jahre wurden IP-Adressen strikt in Klassen organisiert. Dieses System erwies sich jedoch als zu wenig flexibel und wurde eingestellt. Heute wird das *klassenlose Routing* (CIDR, Classless Interdomain Routing) verwendet.

14.1.2 Netzmasken und Routing

Mit Netzmasken werden Adressräume eines Subnetzes definiert. Wenn sich zwei Hosts im selben Subnetz befinden, können sie direkt kommunizieren. Anderenfalls benötigen sie die Adresse eines Gateways, das den gesamten Verkehr zwischen dem Subnetz und dem Rest der Welt handhabt. Um zu prüfen, ob sich zwei IP-Adressen im selben Subnetz befinden, wird jede Adresse bitweise mit der Netzmaske „UND“-verknüpft. Sind die Ergebnisse identisch, befinden sich beide IP-Adressen im selben lokalen Netzwerk. Wenn unterschiedliche Ergebnisse ausgegeben werden, kann die entfernte IP-Adresse, und somit die entfernte Schnittstelle, nur über ein Gateway erreicht werden.

Weitere Informationen zur Funktionsweise von Netzmasken finden Sie in **Beispiel 14.2**, „**Verknüpfung von IP-Adressen mit der Netzmaske**“ (S. 230). Die Netzmaske besteht aus 32 Bit, die festlegen, welcher Teil einer IP-Adresse zum Netzwerk gehört. Alle Bits mit dem Wert 1 kennzeichnen das entsprechende Bit in der IP-Adresse als zum Netzwerk gehörend. Alle Bits mit dem Wert 0 kennzeichnen Bits innerhalb des Subnetzes. Das bedeutet, je mehr Bits den Wert 1 haben, desto kleiner ist das Netzwerk. Da die Netzmaske immer aus mehreren aufeinander folgenden Bits mit dem Wert 1 besteht, ist es

auch möglich, einfach die Anzahl der Bits in der Netzmaske zu zählen. In **Beispiel 14.2**, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 230) könnte das erste Netz mit 24 Bit auch als 192.168.0.0/24 geschrieben werden.

Beispiel 14.2 Verknüpfung von IP-Adressen mit der Netzmaske

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0): 11111111 11111111 11111111 00000000
-----
Result of the link:      11000000 10101000 00000000 00000000
In the decimal system:   192.     168.     0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask   (255.255.255.0): 11111111 11111111 11111111 00000000
-----
Result of the link:      11010101 10111111 00001111 00000000
In the decimal system:   213.     95.      15.      0
```

Ein weiteres Beispiel: Alle Computer, die über dasselbe Ethernetkabel angeschlossen sind, befinden sich in der Regel im selben Subnetz und sind direkt zugreifbar. Selbst wenn das Subnetz physisch durch Switches oder Bridges unterteilt ist, können diese Hosts weiter direkt erreicht werden.

IP-Adressen außerhalb des lokalen Subnetzes können nur erreicht werden, wenn für das Zielnetzwerk ein Gateway konfiguriert ist. In den meisten Fällen wird der gesamte externe Verkehr über lediglich ein Gateway gehandhabt. Es ist jedoch auch möglich, für unterschiedliche Subnetze mehrere Gateways zu konfigurieren.

Wenn ein Gateway konfiguriert wurde, werden alle externen IP-Pakete an das entsprechende Gateway gesendet. Dieses Gateway versucht anschließend, die Pakete auf dieselbe Weise (von Host zu Host) weiterzuleiten, bis sie den Zielhost erreicht haben oder ihre TTL-Zeit (Time to Live) abgelaufen ist.

Tabelle 14.2 Spezifische Adressen

Adresstyp	Beschreibung
Netzwerkbasis- adresse	Dies ist die Netzmaske, die durch UND mit einer Netzwerkadresse verknüpft ist, wie in Beispiel 14.2 , „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 230) unter Ergebnis dargestellt. Diese Adresse kann keinem Host zugewiesen werden.

Adresstyp	Beschreibung
Broadcast-Adresse	Dies bedeutet im Wesentlichen „Senden an alle Hosts in diesem Subnetz.“ Um die Broadcast-Adresse zu generieren, wird die Netzmaske in die binäre Form invertiert und mit einem logischen ODER mit der Netzwerkbasisisadresse verknüpft. Das obige Beispiel ergibt daher die Adresse 192.168.0.255. Diese Adresse kann keinem Host zugeordnet werden.
Lokaler Host	Die Adresse 127.0.0.1 ist auf jedem Host dem „Loopback-Device“ zugewiesen. Mit dieser Adresse kann eine Verbindung zu Ihrem Computer hergestellt werden.

Da IP-Adressen weltweit eindeutig sein müssen, können Sie nicht einfach eine Adresse nach dem Zufallsprinzip wählen. Zum Einrichten eines privaten IP-basierten Netzwerks stehen drei Adressdomänen zur Verfügung. Diese können keine Verbindung zum Internet herstellen, da sie nicht über das Internet übertragen werden können. Diese Adressdomänen sind in RFC 1597 festgelegt und werden in **Tabelle 14.3, „Private IP-Adressdomänen“** (S. 231) aufgelistet.

Tabelle 14.3 *Private IP-Adressdomänen*

Netzwerk/Netzmaske	Domäne
10.0.0.0/255.0.0.0	10.x.x.x
172.16.0.0/255.240.0.0	172.16.x.x – 172.31.x.x
192.168.0.0/255.255.0.0	192.168.x.x

14.2 IPv6 – Das Internet der nächsten Generation

Aufgrund der Entstehung des WWW (World Wide Web) hat das Internet in den letzten 15 Jahren ein explosives Wachstum mit einer immer größer werdenden Anzahl von Computern erfahren, die über TCP/IP kommunizieren. Seit Tim Berners-Lee bei CERN

(<http://public.web.cern.ch>) 1990 das WWW erfunden hat, ist die Anzahl der Internethosts von ein paar tausend auf ca. 100 Millionen angewachsen.

Wie bereits erwähnt, besteht eine IPv4-Adresse nur aus 32 Bit. Außerdem gehen zahlreiche IP-Adressen verloren, da sie aufgrund die Organisation der Netzwerke nicht verwendet werden können. Die Anzahl der in Ihrem Subnetz verfügbaren Adressen ist zwei hoch der Anzahl der Bits minus zwei. Ein Subnetz verfügt also beispielsweise über 2, 6 oder 14 Adressen. Um beispielsweise 128 Hosts mit dem Internet zu verbinden, benötigen Sie ein Subnetz mit 256 IP-Adressen, von denen nur 254 verwendbar sind, da zwei IP-Adressen für die Struktur des Subnetzes selbst benötigt werden: die Broadcast- und die Basisnetzwerkadresse.

Unter dem aktuellen IPv4-Protokoll sind DHCP oder NAT (Network Address Translation) die typischen Mechanismen, um einem potenziellen Adressmangel vorzubeugen. Kombiniert mit der Konvention, private und öffentliche Adressräume getrennt zu halten, können diese Methoden den Adressmangel sicherlich mäßigen. Das Problem liegt in der Konfiguration der Adressen, die schwierig einzurichten und zu verwalten ist. Um einen Host in einem IPv4-Netzwerk einzurichten, benötigen Sie mehrere Adressen, z. B. die IP-Adresse des Hosts, die Subnetzmaske, die Gateway-Adresse und möglicherweise die Adresse des Namensservers. Alle diese Einträge müssen bekannt sein und können nicht von anderer Stelle her abgeleitet werden.

Mit IPv6 gehören sowohl der Adressmangel als auch die komplizierte Konfiguration der Vergangenheit an. Die folgenden Abschnitte enthalten weitere Informationen zu den Verbesserungen und Vorteilen von IPv6 sowie zum Übergang vom alten zum neuen Protokoll.

14.2.1 Vorteile

Die wichtigste und augenfälligste Verbesserung durch das neue Protokoll ist der enorme Zuwachs des verfügbaren Adressraums. Eine IPv6-Adresse besteht aus 128-Bit-Werten und nicht aus den herkömmlichen 32 Bit. Dies ermöglicht mehrere Billiarden IP-Adressen.

IPv6-Adressen unterscheiden sich nicht nur hinsichtlich ihrer Länge gänzlich von ihren Vorgängern. Sie verfügen auch über eine andere interne Struktur, die spezifischere Informationen zu den Systemen und Netzwerken enthalten kann, zu denen sie gehören. Weitere Informationen hierzu finden Sie in [Abschnitt 14.2.2, „Adresstypen und -struktur“](#) (S. 234).

In der folgenden Liste werden einige der wichtigsten Vorteile des neuen Protokolls aufgeführt:

Automatische Konfiguration

IPv6 macht das Netzwerk „Plug-and-Play“-fähig, d. h., ein neu eingerichtetes System wird ohne jegliche manuelle Konfiguration in das (lokale) Netzwerk integriert. Der neue Host verwendet die automatischen Konfigurationsmechanismen, um seine eigene Adresse aus den Informationen abzuleiten, die von den benachbarten Routern zur Verfügung gestellt werden. Dabei nutzt er ein Protokoll, das als *ND-Protokoll* (Neighbor Discovery) bezeichnet wird. Diese Methode erfordert kein Eingreifen des Administrators und für die Adresszuordnung muss kein zentraler Server verfügbar sein. Dies ist ein weiterer Vorteil gegenüber IPv4, bei dem für die automatische Adresszuordnung ein DHCP-Server erforderlich ist.

Mobilität

IPv6 ermöglicht es, einer Netzwerkschnittstelle gleichzeitig mehrere Adressen zuzuordnen. Benutzer können daher einfach auf mehrere Netzwerke zugreifen. Dies lässt sich mit den internationalen Roaming-Diensten vergleichen, die von Mobilfunkunternehmen angeboten werden: Wenn Sie das Mobilfunkgerät ins Ausland mitnehmen, meldet sich das Telefon automatisch bei einem ausländischen Dienst an, der sich im entsprechenden Bereich befindet. Sie können also überall unter der gleichen Nummer erreicht werden und können telefonieren als wären Sie zu Hause.

Sichere Kommunikation

Bei IPv4 ist die Netzwerksicherheit eine Zusatzfunktion. IPv6 umfasst IPsec als eine seiner Kernfunktionen und ermöglicht es Systemen, über einen sicheren Tunnel zu kommunizieren, um das Ausspionieren durch Außenstehende über das Internet zu verhindern.

Abwärtskompatibilität

Realistisch gesehen, ist es unmöglich, das gesamte Internet auf einmal von IPv4 auf IPv6 umzustellen. Daher ist es wichtig, dass beide Protokolle nicht nur im Internet, sondern auf einem System koexistieren können. Dies wird durch kompatible Adressen (IPv4-Adressen können problemlos in IPv6-Adressen konvertiert werden) und die Verwendung von Tunnels gewährleistet. Weitere Informationen hierzu finden Sie unter **Abschnitt 14.2.3, „Koexistenz von IPv4 und IPv6“** (S. 239). Außerdem können Systeme eine *Dual-Stack-IP*-Technik verwenden, um beide Protokolle gleichzeitig unterstützen zu können. Dies bedeutet, dass sie über zwei

Netzwerk-Stacks verfügen, die vollständig unabhängig voneinander sind, sodass zwischen den beiden Protokollversionen keine Konflikte auftreten.

Bedarfsgerechte Dienste über Multicasting

Mit IPv4 müssen einige Dienste, z. B. SMB, ihre Pakete via Broadcast an alle Hosts im lokalen Netzwerk verteilen. IPv6 ermöglicht einen sehr viel ausgefeilterten Ansatz. Server können Hosts über *Multicasting* ansprechen, d. h. sie sprechen mehrere Hosts als Teile einer Gruppe an (im Gegensatz zur Adressierung aller Hosts über *Broadcasting* oder der Einzeladressierung der Hosts über *Unicasting*). Welche Hosts als Gruppe adressiert werden, kann je nach Anwendung unterschiedlich sein. Es gibt einige vordefinierte Gruppen, mit der beispielsweise alle Namensserver (die *Multicast-Gruppe "all name servers"*) oder alle Router (die *Multicast-Gruppe "all routers"*) angesprochen werden können.

14.2.2 Adresstypen und -struktur

Wie bereits erwähnt hat das aktuelle IP-Protokoll zwei wichtige Nachteile: Es stehen zunehmend weniger IP-Adressen zur Verfügung und das Konfigurieren des Netzwerks und Verwalten der Routing-Tabellen wird komplexer und aufwändiger. IPv6 löst das erste Problem durch die Erweiterung des Adressraums auf 128 Bit. Das zweite Problem wird durch die Einführung einer hierarchischen Adressstruktur behoben, die mit weiteren hoch entwickelten Techniken zum Zuordnen von Netzwerkadressen sowie mit dem *Multihoming* (der Fähigkeit, einem Gerät mehrere Adressen zuzuordnen und so den Zugriff auf mehrere Netzwerke zu ermöglichen) kombiniert wird.

Bei der Arbeit mit IPv6 ist es hilfreich, die drei unterschiedlichen Adresstypen zu kennen:

Unicast

Adressen dieses Typs werden genau einer Netzwerkschnittstelle zugeordnet. Pakete mit derartigen Adressen werden nur einem Ziel zugestellt. Unicast-Adressen werden dementsprechend zum Übertragen von Paketen an einzelne Hosts im lokalen Netzwerk oder im Internet verwendet.

Multicast

Adressen dieses Typs beziehen sich auf eine Gruppe von Netzwerkschnittstellen. Pakete mit derartigen Adressen werden an alle Ziele zugestellt, die dieser Gruppe angehören. Multicast-Adressen werden hauptsächlich von bestimmten Netzwerkdiensten für die Kommunikation mit bestimmten Hostgruppen verwendet, wobei diese gezielt adressiert werden.

Anycast

Adressen dieses Typs beziehen sich auf eine Gruppe von Schnittstellen. Pakete mit einer derartigen Adresse werden gemäß den Prinzipien des zugrunde liegenden Routing-Protokolls dem Mitglied der Gruppe gesendet, das dem Absender am nächsten ist. Anycast-Adressen werden verwendet, damit Hosts Informationen zu Servern schneller abrufen können, die im angegebenen Netzwerkbereich bestimmte Dienste anbieten. Sämtliche Server desselben Typs verfügen über dieselbe Anycast-Adresse. Wann immer ein Host einen Dienst anfordert, erhält er eine Antwort von dem vom Routing-Protokoll ermittelten nächstgelegenen Server. Wenn dieser Server aus irgendeinem Grund nicht erreichbar ist, wählt das Protokoll automatisch den zweitnächsten Server, dann den dritten usw. aus.

Eine IPv6-Adresse besteht aus acht vierstelligen Feldern, wobei jedes 16 Bit repräsentiert, und wird in hexadezimaler Notation geschrieben. Die Felder werden ebenfalls durch Doppelpunkte (:) getrennt. Alle führenden Null-Byte innerhalb eines bestimmten Felds können ausgelassen werden, alle anderen Nullen jedoch nicht. Eine weitere Konvention ist, dass mehr als vier aufeinander folgenden Null-Byte mit einem doppelten Doppelpunkt zusammengefasst werden können. Jedoch ist pro Adresse nur ein solcher doppelter Doppelpunkt (: :) zulässig. Diese Art der Kurznotation wird in **Beispiel 14.3**, „Beispiel einer IPv6-Adresse“ (S. 235) dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

Beispiel 14.3 *Beispiel einer IPv6-Adresse*

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                : 10 : 1000 : 1a4
```

Jeder Teil einer IPv6-Adresse hat eine festgelegte Funktion. Die ersten Byte bilden das Präfix und geben den Typ der Adresse an. Der mittlere Teil ist der Netzwerkteil der Adresse, der möglicherweise nicht verwendet wird. Das Ende der Adresse bildet der Hostteil. Bei IPv6 wird die Netzmaske definiert, indem die Länge des Präfixes nach einem Schrägstrich am Ende der Adresse angegeben wird. Adressen wie in **Beispiel 14.4**, „IPv6-Adressen mit Angabe der Präfix-Länge“ (S. 235) enthalten Informationen zum Netzwerk (die ersten 64 Bit) und zum Hostteil (die letzten 64 Bit). Die 64 bedeutet, dass die Netzmaske mit 64 1-Bit-Werten von links gefüllt wird. Wie bei IPv4 wird die IP-Adresse mit den Werten aus der Netzmaske durch UND verknüpft, um zu ermitteln, ob sich der Host im selben oder einem anderen Subnetz befindet.

Beispiel 14.4 *IPv6-Adressen mit Angabe der Präfix-Länge*

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige von diesen sind in [Tabelle 14.4](#), „[Unterschiedliche IPv6-Präfixe](#)“ (S. 236) aufgeführt.

Tabelle 14.4 *Unterschiedliche IPv6-Präfixe*

Präfix (hexadezimal)	Definition
00	IPv4-über-IPv6-Kompatibilitätsadressen. Diese werden zur Erhaltung der Kompatibilität mit IPv4 verwendet. Für diesen Adresstyp wird ein Router benötigt, der IPv6-Pakete in IPv4-Pakete konvertieren kann. Mehrere spezielle Adressen, z. B. die für das Loopback-Device, verfügen ebenfalls über dieses Präfix.
2 oder 3 als erste Stelle	Aggregierbare globale Unicast-Adressen. Wie bei IPv4 kann eine Schnittstelle zugewiesen werden, um einen Teil eines bestimmten Subnetzes zu bilden. Aktuell stehen die folgenden Adressräume zur Verfügung: 2001::/16 (Adressraum Produktionsqualität) und 2002::/16 (6to4-Adressraum).
fe80::/10	Link-local-Adressen. Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.
fec0::/10	Site-local-Adressen. Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb des Organisationsnetzwerks, dem sie angehören. Damit entsprechen diese Adressen den bisherigen privaten Netzen (beispielsweise 10.x.x.x).
ff	Dies sind Multicast-Adressen.

Eine Unicast-Adresse besteht aus drei grundlegenden Komponenten:

Öffentliche Topologie

Der erste Teil, der unter anderem auch eines der oben erwähnten Präfixe enthält, dient dem Routing des Pakets im öffentlichen Internet. Hier sind Informationen zum Provider oder der Institution kodiert, die den Netzwerkzugang bereitstellen.

Site-Topologie

Der zweite Teil enthält Routing-Informationen zum Subnetz, in dem das Paket zugestellt werden soll.

Schnittstellen-ID

Der dritte Teil identifiziert eindeutig die Schnittstelle, an die das Paket gerichtet ist. Dies erlaubt, die MAC-Adresse als Adressbestandteil zu verwenden. Da diese weltweit nur einmal vorhanden und zugleich vom Hardwarehersteller fest vorgegeben ist, vereinfacht sich die Konfiguration auf diese Weise sehr. Die ersten 64 Bit werden zu einem so genannten EUI-64-Token zusammengefasst. Dabei werden die letzten 48 Bit der MAC-Adresse entnommen und die restlichen 24 Bit enthalten spezielle Informationen, die etwas über den Typ des Tokens aussagen. Das ermöglicht dann auch, Geräten ohne MAC-Adresse (z. B. PPP- und ISDN-Verbindungen) ein EUI-64-Token zuzuweisen.

Abgeleitet aus diesem Grundaufbau werden bei IPv6 fünf verschiedene Typen von Unicast-Adressen unterschieden:

:: (nicht spezifiziert)

Ein Host verwendet diese Adresse als Quelladresse, wenn seine Netzwerkschnittstelle zum ersten Mal initialisiert wird und die Adresse noch nicht anderweitig ermittelt werden kann.

:::1 (Loopback)

Adresse des Loopback-Device.

IPv4-kompatible Adressen

Die IPv6-Adresse setzt sich aus der IPv4-Adresse und einem Präfix von 96 0-Bits zusammen. Dieser Typ der Kompatibilitätsadresse wird beim Tunneling verwendet (siehe [Abschnitt 14.2.3, „Koexistenz von IPv4 und IPv6“](#) (S. 239)). IPv4/IPv6-Hosts können so mit anderen kommunizieren, die sich in einer reinen IPv4-Umgebung befinden.

IPv6-gemappte IPv4-Adressen

Dieser Adresstyp gibt die Adresse in IPv6-Notation an.

Lokale Adressen

Es gibt zwei Typen von Adressen zum rein lokalen Gebrauch:

link-local

Dieser Adresstyp ist ausschließlich für den Gebrauch im lokalen Subnetz bestimmt. Router dürfen Pakete mit solcher Ziel- oder Quelladresse nicht an das Internet oder andere Subnetze weiterreichen. Diese Adressen zeichnen sich durch ein spezielles Präfix ($\text{fe80}::/10$) und die Schnittstellen-ID der Netzwerkkarte aus. Der Mittelteil der Adresse besteht aus Null-Bytes. Diese Art Adresse wird von den Autokonfigurationsmethoden verwendet, um Hosts im selben Subnetz anzusprechen.

site-local

Pakete mit diesem Adresstyp dürfen zwischen einzelnen Subnetzen geroutet werden, jedoch nicht außerhalb einer Organisation ins Internet gelangen. Solche Adressen werden für Intranets eingesetzt und sind ein Äquivalent zu den privaten IPv4-Adressen. Neben einem definierten Präfix ($\text{fec0}::/10$) und der Schnittstellen-ID enthalten diese Adressen ein 16-Bit-Feld, in dem die Subnetz-ID kodiert ist. Der Rest wird wieder mit Null-Bytes aufgefüllt.

Zusätzlich gibt es in IPv6 eine grundsätzlich neue Funktion: Einer Netzwerkschnittstelle werden üblicherweise mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netze zur Verfügung stehen. Eines dieser Netzwerke kann mit der MAC-Adresse und einem bekannten Präfix vollautomatisch konfiguriert werden, sodass sofort nach der Aktivierung von IPv6 alle Hosts im lokalen Netz über Link-local-Adressen erreichbar sind. Durch die MAC-Adresse als Bestandteil der IP-Adresse ist jede dieser Adressen global eindeutig. Einzig die Teile der *Site-Topologie* und der *öffentlichen Topologie* können variieren, je nachdem in welchem Netz dieser Host aktuell zu erreichen ist.

Bewegt sich ein Host zwischen mehreren Netzen hin und her, braucht er mindestens zwei Adressen. Die eine, seine *Home-Adresse*, beinhaltet neben der Schnittstellen-ID die Informationen zu dem Heimatnetz, in dem der Computer normalerweise betrieben wird, und das entsprechende Präfix. Die Home-Adresse ist statisch und wird in der Regel nicht verändert. Alle Pakete, die für diesen Host bestimmt sind, werden ihm sowohl im eigenen als auch in fremden Netzen zugestellt. Möglich wird die Zustellung im Fremdnetz über wesentliche Neuerungen des IPv6-Protokolls, z. B. *Stateless Auto-configuration* und *Neighbor Discovery*. Der mobile Rechner hat neben seiner Home-Adresse eine oder mehrere weitere Adressen, die zu den fremden Netzen gehören, in denen er sich bewegt. Diese Adressen heißen *Care-of-Adressen*. Im Heimatnetz des mobilen Rechners muss eine Instanz vorhanden sein, die an seine Home-Adresse gerichtete Pakete nachsendet, sollte er sich in einem anderen Netz befinden. Diese Funktion wird in einer IPv6-Umgebung vom *Home-Agenten* übernommen. Er stellt alle

Pakete, die an die Home-Adresse des mobilen Rechners gerichtet sind, über einen Tunnel zu. Pakete, die als Zieladresse die Care-of-Adresse tragen, können ohne Umweg über den Home-Agenten zugestellt werden.

14.2.3 Koexistenz von IPv4 und IPv6

Die Migration aller mit dem Internet verbundenen Hosts von IPv4 auf IPv6 wird nicht auf einen Schlag geschehen. Vielmehr werden das alte und das neue Protokoll noch eine ganze Weile nebeneinanderher existieren. Die Koexistenz auf einem Rechner ist dann möglich, wenn beide Protokolle im *Dual Stack*-Verfahren implementiert sind. Es bleibt aber die Frage, wie IPv6-Rechner mit IPv4-Rechnern kommunizieren können und wie IPv6-Pakete über die momentan noch vorherrschenden IPv4-Netze transportiert werden sollen. Tunneling und die Verwendung von Kompatibilitätsadressen (siehe [Abschnitt 14.2.2, „Adresstypen und -struktur“](#) (S. 234)) sind hier die besten Lösungen.

IPv6-Hosts, die im (weltweiten) IPv4-Netzwerk mehr oder weniger isoliert sind, können über Tunnel kommunizieren: IPv6-Pakete werden als IPv4-Pakete gekapselt und so durch ein IPv4-Netzwerk übertragen. Ein *Tunnel* ist definiert als die Verbindung zwischen zwei IPv4-Endpunkten. Hierbei müssen die Pakete die IPv6-Zieladresse (oder das entsprechende Präfix) und die IPv4-Adresse des entfernten Hosts am Tunnelendpunkt enthalten. Einfache Tunnel können von den Administratoren zwischen ihren Netzwerken manuell und nach Absprache konfiguriert werden. Ein solches Tunneling wird *statisches Tunneling* genannt.

Trotzdem reicht manuelles Tunneling oft nicht aus, um die Menge der zum täglichen vernetzten Arbeiten nötigen Tunnel aufzubauen und zu verwalten. Aus diesem Grund wurden für IPv6 drei verschiedene Verfahren entwickelt, die das *dynamische Tunneling* erlauben:

6over4

IPv6-Pakete werden automatisch in IPv4-Pakete verpackt und über ein IPv4-Netzwerk versandt, in dem Multicasting aktiviert ist. IPv6 wird vorgespiegelt, das gesamte Netzwerk (Internet) sei ein einziges, riesiges LAN (Local Area Network). So wird der IPv4-Endpunkt des Tunnel automatisch ermittelt. Nachteile dieser Methode sind die schlechte Skalierbarkeit und die Tatsache, dass IP-Multicasting keineswegs im gesamten Internet verfügbar ist. Diese Lösung eignet sich für kleinere Netzwerke, die die Möglichkeit von IP-Multicasting bieten. Die zugrunde liegenden Spezifikationen sind in RFC 2529 enthalten.

6to4

Bei dieser Methode werden automatisch IPv4-Adressen aus IPv6-Adressen generiert. So können isolierte IPv6-Hosts über ein IPv4-Netz miteinander kommunizieren. Allerdings gibt es einige Probleme, die die Kommunikation zwischen den isolierten IPv6-Hosts und dem Internet betreffen. Diese Methode wird in RFC 3056 beschrieben.

IPv6 Tunnel Broker

Dieser Ansatz sieht spezielle Server vor, die für IPv6 automatisch dedizierte Tunnel anlegen. Diese Methode wird in RFC 3053 beschrieben.

14.2.4 IPv6 konfigurieren

Um IPv6 zu konfigurieren, müssen Sie auf den einzelnen Arbeitsstationen in der Regel keine Änderungen vornehmen. IPv6 ist standardmäßig aktiviert. Sie können IPv6 während der Installation im Schritt der Netzwerkkonfiguration deaktivieren (siehe „Netzwerkkonfiguration“ (Kapitel 1, *Installation mit YaST*, ↑Start)). Um IPv6 auf einem installierten System zu deaktivieren oder zu aktivieren, verwenden Sie das Modul *YaST-Netzwerkeinstellungen*. Aktivieren oder deaktivieren Sie auf dem Karteireiter *Globale Optionen* die Option *IPv6 aktivieren*, falls nötig. Um IPv6 manuell zu aktivieren, geben Sie `modprobe ipv6` als `root` ein.

Aufgrund des Konzepts der automatischen Konfiguration von IPv6 wird der Netzwerkkarte eine Adresse im *Link-local*-Netzwerk zugewiesen. In der Regel werden Routing-Tabellen nicht auf Arbeitsstationen verwaltet. Bei Netzwerkroutern kann von der Arbeitsstation unter Verwendung des *Router-Advertisement-Protokolls* abgefragt werden, welches Präfix und welche Gateways implementiert werden sollen. Zum Einrichten eines IPv6-Routers kann das *radvd*-Programm verwendet werden. Dieses Programm informiert die Arbeitsstationen darüber, welches Präfix und welche Router für die IPv6-Adressen verwendet werden sollen. Alternativ können Sie die Adressen und das Routing auch mit *zebra/quagga* automatisch konfigurieren.

Weitere Informationen zum Einrichten der unterschiedlichen Tunneltypen mithilfe der Dateien im Verzeichnis `/etc/sysconfig/network` finden Sie auf der man-Seite "`ifcfg-tunnel (5)`".

14.2.5 Weiterführende Informationen

Das komplexe IPv6-Konzept wird im obigen Überblick nicht vollständig abgedeckt. Weitere ausführliche Informationen zu dem neuen Protokoll finden Sie in den folgenden Online-Dokumentationen und -Büchern:

<http://www.ipv6.org/>

Alles rund um IPv6.

<http://www.ipv6day.org>

Alle Informationen, die Sie benötigen, um Ihr eigenes IPv6-Netzwerk zu starten.

<http://www.ipv6-to-standard.org/>

Die Liste der IPv6-fähigen Produkte.

<http://www.bieringer.de/linux/IPv6/>

Hier finden Sie den Beitrag "Linux IPv6 HOWTO" und viele verwandte Links zum Thema.

RFC 2640

Die grundlegenden IPv6-Spezifikationen.

IPv6 Essentials

Ein Buch, in dem alle wichtigen Aspekte zum Thema enthalten sind, ist *IPv6 Essentials* von Silvia Hagen (ISBN 0-596-00125-8).

14.3 Namensauflösung

Mithilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden und umgekehrt auch ein Name einer IP-Adresse. Unter Linux erfolgt diese Umwandlung üblicherweise durch eine spezielle Software namens `bind`. Der Computer, der diese Umwandlung dann erledigt, nennt sich *Namenserver*. Dabei bilden die Namen wieder ein hierarchisches System, in dem die einzelnen Namensbestandteile durch Punkte getrennt sind. Die Namenshierarchie ist aber unabhängig von der oben beschriebenen Hierarchie der IP-Adressen.

Nehmen Sie als Beispiel einen vollständigen Namen wie `earth.example.com`, der im Format `hostname.domain` geschrieben wurde. Ein vollständiger Name, der als

Fully Qualified Domain Name oder kurz als FQDN bezeichnet wird, besteht aus einem Host- und einem Domännennamen (`example.com`). Ein Bestandteil des Domännennamens ist die *Top Level Domain* oder TLD (`com`).

Aus historischen Gründen ist die Zuteilung der TLDs etwas verwirrend. So werden in den USA traditionell dreibuchstabile TLDs verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen. Seit 2000 stehen zusätzliche TLDs für spezielle Sachgebiete mit zum Teil mehr als drei Buchstaben zur Verfügung (z. B. `.info`, `.name`, `.museum`).

In der Frühzeit des Internets (vor 1990) gab es die Datei `/etc/hosts`, in der die Namen aller im Internet vertretenen Rechner gespeichert waren. Dies erwies sich bei der schnell wachsenden Menge der mit dem Internet verbundenen Computer als unpraktikabel. Deshalb wurde eine dezentralisierte Datenbank entworfen, die die Hostnamen verteilt speichern kann. Diese Datenbank, eben jener oben erwähnte Namensserver, hält also nicht die Daten aller Computer im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere Namensserver weiterdelegieren.

An der Spitze der Hierarchie befinden sich die *Root-Namensserver*. Die root-Namensserver verwalten die Domänen der obersten Ebene (Top Level Domains) und werden vom Network Information Center (NIC) verwaltet. Der Root-Namensserver kennt die jeweils für eine Top Level Domain zuständigen Namensserver. Weitere Informationen zu TLD-NICs finden Sie unter <http://www.internic.net>.

DNS kann noch mehr als nur Hostnamen auflösen. Der Namensserver weiß auch, welcher Host für eine ganze Domäne E-Mails empfängt (der *Mail Exchanger (MX)*).

Damit auch Ihr Rechner einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Namensserver mit einer IP-Adresse bekannt sein. Die Konfiguration eines Namensservers erledigen Sie komfortabel mithilfe von YaST. Falls Sie eine Einwahl über Modem vornehmen, kann es sein, dass die manuelle Konfiguration eines Namensservers nicht erforderlich ist. Das Einwahlprotokoll liefert die Adresse des Namensservers bei der Einwahl gleich mit. Die Konfiguration des Namensserverzugriffs unter openSUSE® wird unter „**Konfigurieren des Hostnamens und DNS**“ (S. 252) beschrieben. Eine Beschreibung zum Einrichten Ihres Namensservers finden Sie in **Kapitel 16, Domain Name System (DNS)** (S. 287).

Eng verwandt mit DNS ist das Protokoll `whois`. Mit dem gleichnamigen Programm `whois` können Sie schnell ermitteln, wer für eine bestimmte Domäne verantwortlich ist.

14.4 Konfigurieren von Netzwerkverbindungen mit YaST

Unter Linux gibt es viele unterstützte Netzwerktypen. Die meisten verwenden unterschiedliche Gerätenamen und die Konfigurationsdateien sind im Dateisystem an unterschiedlichen Speicherorten verteilt. Einen detaillierten Überblick über die Aspekte der manuellen Netzwerkkonfiguration finden Sie in [Abschnitt 14.6, „Manuelle Netzwerkkonfiguration“](#) (S. 264).

Bei der Installation auf einem Laptop, auf dem NetworkManager standardmäßig aktiv ist, konfiguriert YaST alle erkannten Schnittstellen. Auf anderen Computern wird nur die erste Schnittstelle mit einer Verbindung automatisch konfiguriert. Zusätzliche Hardware kann nach Abschluss der Installation jederzeit konfiguriert werden. In den folgenden Abschnitten wird die Netzwerkkonfiguration für alle von openSUSE unterstützten Netzwerkverbindungen beschrieben.

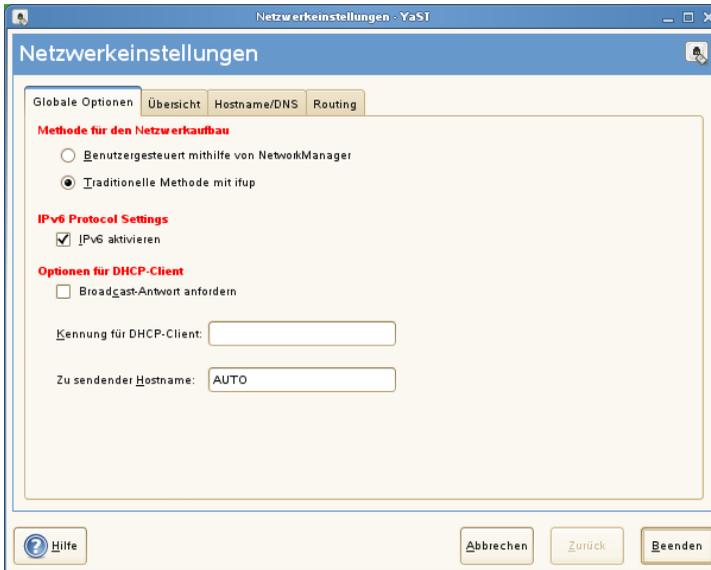
14.4.1 Konfigurieren der Netzwerkkarte mit YaST

Zur Konfiguration verkabelter oder drahtloser Netzwerkkarten in YaST wählen Sie *Netzwerkgeräte > Netzwerkeinstellungen* aus. Nach Starten des Moduls zeigt YaST das Dialogfeld *Netzwerkeinstellung* mit vier Karteireitern an. Auf dem Karteireiter *Globale Optionen* können allgemeine Netzwerkooptionen wie die Verwendung der Optionen NetworkManager, IPv6 und global DHCP festgelegt werden. Weitere Informationen finden Sie unter [„Konfigurieren globaler Netzwerkooptionen“](#) (S. 244).

Der Karteireiter *Übersicht* enthält Informationen zu den installierten Netzwerkkarten. Jede korrekt erkannte Netzwerkkarte wird dort mit ihrem Namen aufgelistet. In diesem Dialogfeld können Sie neue Karten manuell hinzufügen und deren Konfiguration entfernen oder ändern. Informationen zum manuellen Hinzufügen und Konfigurieren von Karten, die nicht automatisch erkannt wurden, finden Sie unter [„Konfigurieren einer unerkannten Netzwerkkarte“](#) (S. 251). Informationen zum Ändern der Konfiguration einer bereits konfigurierten Karte finden Sie unter [„Ändern der Konfiguration einer Netzwerkkarte“](#) (S. 245).

Auf dem Karteireiter *Hostname/DNS* können der Hostname des Computers sowie die zu verwendenden Nameserver festgelegt werden. Weitere Informationen finden Sie unter „**Konfigurieren des Hostnamens und DNS**“ (S. 252). Der Karteireiter *Routing* wird zur Konfiguration des Routings verwendet. Weitere Informationen zur Routing-Konfiguration finden Sie unter „**Konfigurieren des Routing**“ (S. 253).

Abbildung 14.3 Konfigurieren der Netzwerkeinstellungen



Konfigurieren globaler Netzwerkooptionen

Auf dem Karteireiter *Globale Optionen* des YaST-Moduls *Netzwerkeinstellungen* können wichtige globale Netzwerkooptionen wie die Verwendung der Optionen *NetworkManager*, *IPv6* und *DHCP-Client* festgelegt werden. Diese Einstellungen sind für alle Netzwerkschnittstellen anwendbar.

Unter *Netzwerkeinrichtungsmethode* wählen Sie die Methode aus, mit der Netzwerkverbindungen verwaltet werden sollen. Wenn die Verbindungen für alle Schnittstellen über das Desktop-Applet *NetworkManager* verwaltet werden sollen, wählen Sie *Benutzergesteuert mithilfe von NetworkManager* aus. Diese Option eignet sich besonders für den Wechsel zwischen verschiedenen verkabelten und drahtlosen Netzwerken. Wenn Sie keine Desktop-Umgebung (*GNOME* oder *KDE*) ausführen oder wenn Ihr Computer

ein Xen-Server oder ein virtuelles System ist oder Netzwerkdienste wie DHCP oder DNS in Ihrem Netzwerk zur Verfügung stellt, verwenden Sie die *Traditionelle Methode mit ifup*. Weitere Informationen zu NetworkManager finden Sie unter Kapitel 10, *Verwalten der Netzwerkverbindungen mit NetworkManager* (↑Start).

Geben Sie unter *IPv6 Protocol Settings* (IPv6-Protokolleinstellungen) an, ob Sie das IPv6-Protokoll verwenden möchten. IPv6 kann parallel zu IPv4 verwendet werden. IPv6 ist standardmäßig aktiviert. In Netzwerken, die das IPv6-Protokoll nicht verwenden, können die Antwortzeiten jedoch schneller sein, wenn dieses Protokoll deaktiviert ist. Zum Deaktivieren von IPv6 deaktivieren Sie die Option *IPv6 aktivieren*. Dadurch wird das automatische Laden des Kernel-Moduls von IPv6 unterbunden. Die Änderung wird erst nach einem Neustart wirksam.

Unter *Optionen für DHCP-Client* konfigurieren Sie die Optionen für den DHCP-Client. Wenn der DHCP-Client den Server anweisen soll, seine Antworten immer per Broadcast zu versenden, aktivieren Sie *Broadcast-Antwort anfordern*. Diese Einstellung ist vermutlich erforderlich, wenn Sie Ihren Computer in verschiedenen Netzwerken verwenden. Die *Kennung für DHCP-Client* muss innerhalb eines Netzwerks für jeden DHCP-Client eindeutig sein. Wenn dieses Feld leer bleibt, wird standardmäßig die Hardware-Adresse der Netzwerkschnittstelle als Kennung übernommen. Falls Sie allerdings mehrere virtuelle Computer mit der gleichen Netzwerkschnittstelle und damit der gleichen Hardware-Adresse ausführen, sollten Sie hier eine eindeutige Kennung in beliebigem Format eingeben.

Unter *Zu sendender Hostname* wird eine Zeichenkette angegeben, die für das Optionsfeld "Hostname" verwendet wird, wenn dhcpcd Nachrichten an den DHCP-Server sendet. Einige DHCP-Server aktualisieren Namensserver-Zonen gemäß diesem Hostnamen (dynamischer DNS). Bei einigen DHCP-Servern muss das Optionsfeld "Zu sendender Hostname" in den DHCP-Nachrichten der Clients zudem eine bestimmte Zeichenkette enthalten. Übernehmen Sie die Einstellung "AUTO", wenn der aktuelle, in `/etc/HOSTNAME` festgelegte Hostname gesendet werden soll. Lassen Sie das Optionsfeld leer, wenn kein Hostname gesendet werden soll. Wenn die Standardroute nicht gemäß der Informationen von DHCP geändert werden soll, deaktivieren Sie *Standardroute über DHCP ändern*.

Ändern der Konfiguration einer Netzwerkkarte

Um die Konfiguration einer Netzwerkkarte zu ändern, wählen Sie eine Karte aus der Liste der erkannten Karten auf dem Karteireiter *Übersicht* im YaST-Modul Netzwerk-

einstellungen aus und klicken Sie auf *Bearbeiten*. Das Dialogfeld *Netzwerkkarte* wird angezeigt. Hier können Sie die Kartenkonfiguration auf den Registerkarten *Allgemein*, *Adresse* und *Hardware* anpassen. Genauere Informationen zur drahtlosen Kartenkonfiguration finden Sie unter **Abschnitt 25.1.1, „Konfiguration mit YaST“** (S. 477).

IP-Adressen konfigurieren

Die IP-Adresse der Netzwerkkarte oder die Art der Festlegung dieser IP-Adresse kann auf dem Karteireiter *Adresse* im Dialogfeld *Einrichten der Netzwerkkarte* festgelegt werden. Für die Netzwerkkarte können die Einstellungen *Keine IP-Adresse* (nützlich für eingebundene Geräte), *Statisch zugewiesene IP-Adresse* oder *Dynamische Adresse* über *DHCP* und/oder *Zeroconf* zugewiesen werden.

Wenn möglich wird die erste Netzwerkkarte mit einer Verbindung, die bei der Installation verfügbar ist, automatisch zur Verwendung der automatischen Adressenkonfiguration mit *DHCP* konfiguriert. Bei Laptop-Computern, auf denen *NetworkManager* standardmäßig aktiv ist, werden alle Netzwerkkarten konfiguriert.

DHCP sollten Sie auch verwenden, wenn Sie eine *DSL*-Leitung verwenden, Ihr *ISP* (*Internet Service Provider*) Ihnen aber keine statische IP-Adresse zugewiesen hat. Wenn Sie *DHCP* verwenden möchten, konfigurieren Sie dessen Einstellungen im Dialogfeld *Netzwerkeinstellungen* des *YaST*-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Globale Optionen* unter *Optionen für DHCP-Client*. Geben Sie unter *Broadcast-Antwort anfordern* an, ob der *DHCP-Client* den Server anweisen soll, seine Antworten immer per *Broadcast* zu versenden. Diese Einstellung ist vermutlich erforderlich, wenn Sie Ihren Computer als mobilen Client in verschiedenen Netzwerken verwenden. In einer virtuellen Hostumgebung, in der mehrere Hosts über dieselbe Schnittstelle kommunizieren, müssen diese anhand der *Kennung für DHCP-Client* unterschieden werden.

DHCP eignet sich gut zur Client-Konfiguration, aber zur Server-Konfiguration ist es nicht ideal. Wenn Sie eine statische IP-Adresse festlegen möchten, gehen Sie wie folgt vor:

- 1 Wählen Sie im *YaST*-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.
- 2 Wählen Sie auf dem Karteireiter *Adresse* die Option *Statisch zugewiesene IP-Adresse* aus.

- 3 Geben Sie die *IP-Adresse* und die *Subnetzmaske* ein (normalerweise 255.255.255.0).

Optional kann ein voll qualifizierter *Hostname* für diese Adresse eingegeben werden, der in die Konfigurationsdatei `/etc/hosts` geschrieben wird.

- 4 Klicken Sie auf *Weiter*.
- 5 Klicken Sie auf *Verlassen*, um die Konfiguration zu aktivieren.

Wenn Sie die statische Adresse verwenden, werden die Namensserver und das Standard-Gateway nicht automatisch konfiguriert. Informationen zur Konfiguration von Namensservern finden Sie unter „**Konfigurieren des Hostnamens und DNS**“ (S. 252). Informationen zur Konfiguration eines Gateways finden Sie unter „**Konfigurieren des Routing**“ (S. 253).

Konfigurieren von Aliassen

Wenn NetworkManager nicht verwendet wird, kann ein einzelnes Netzwerkgerät mehrere IP-Adressen haben, die sogenannten Aliase. Wenn Sie einen Alias für Ihre Netzwerkkarte einrichten möchten, gehen Sie wie folgt vor.

- 1 Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.
- 2 Klicken Sie auf dem Karteireiter *Adresse* im Bereich *Zusätzliche Adressen* auf *Hinzufügen*.
- 3 Geben Sie den *Aliasnamen*, die *IP-Adresse* und die *Netzmaske* ein. Nehmen Sie den Schnittstellennamen nicht in den Aliasnamen auf.
- 4 Klicken Sie auf *OK*.
- 5 Klicken Sie auf *Weiter*.
- 6 Klicken Sie auf *Verlassen*, um die Konfiguration zu aktivieren.

Ändern des Gerätenamens und der Udev-Regeln

Der Geräteiname der Netzwerkkarte kann während des laufenden Betriebs geändert werden. Es kann auch festgelegt werden, ob udev die Netzwerkkarte über die Hardware-Adresse (MAC) oder die Bus-ID erkennen soll. Die zweite Option ist bei großen Servern vorzuziehen, um einen Austausch der Karten unter Spannung zu erleichtern. Mit YaST legen Sie diese Optionen wie folgt fest:

- 1 Wählen Sie im YaST-Modul *Netzwerkeinstellungen* auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.
- 2 Öffnen Sie den Karteireiter *Hardware*. Der aktuelle Geräteiname wird unter *Udev-Regeln* angezeigt. Klicken Sie auf *Ändern*.
- 3 Wählen Sie aus, ob udev die Karte über die *MAC-Adresse* oder die *BusID* erkennen soll. Die aktuelle MAC-Adresse und Bus-ID der Karte werden im Dialogfeld angezeigt.
- 4 Aktivieren Sie zum Ändern des Gerätenamens die Option *Gerätenamen ändern* und bearbeiten Sie den Namen.
- 5 Klicken Sie auf *OK* und *Weiter*.
- 6 Klicken Sie auf *Verlassen*, um die Konfiguration zu aktivieren.

Ändern des Kernel-Moduls für Netzwerkkarten

Für einige Netzwerkkarten sind eventuell verschiedene Kernel-Module (Treiber) verfügbar. Wenn die Karte bereits konfiguriert ist, ermöglicht YaST die Auswahl eines zu verwendenden Kernel-Moduls aus einer Liste verfügbarer Module. Es ist auch möglich, Optionen für das Kernel-Modul anzugeben. Mit YaST legen Sie diese Optionen wie folgt fest:

- 1 Wählen Sie im YaST-Modul *Netzwerkeinstellungen* auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.
- 2 Öffnen Sie den Karteireiter *Hardware*.

- 3 Wählen Sie das zu verwendende Kernel-Modul unter *Modulname* aus. Geben Sie die entsprechenden Optionen für das ausgewählte Modul unter *Optionen* im Format *Option=Wert* ein. Wenn mehrere Optionen verwendet werden, sollten sie durch Leerzeichen getrennt sein.
- 4 Klicken Sie auf *OK* und *Weiter*.
- 5 Klicken Sie auf *Verlassen*, um die Konfiguration zu aktivieren.

Aktivieren des Netzwerkgeräts

Wenn Sie die traditionelle Methode mit `ifup` verwenden, können Sie Ihr Gerät so konfigurieren, dass es beim Systemstart, bei der Verbindung per Kabel, beim Erkennen der Karte, manuell oder nie startet. Wenn Sie den Gerätestart ändern möchten, gehen Sie wie folgt vor:

- 1 Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten eine Karte aus der Liste der erkannten Karten und klicken Sie auf *Bearbeiten*.
- 2 In der Karteireiter *Allgemein* wählen Sie den gewünschten Eintrag unter *Geräte-Aktivierung*.

Wählen Sie *Beim Systemstart*, um das Gerät beim Booten des Systems zu starten. Wenn *Bei Kabelanschluss* aktiviert ist, wird die Schnittstelle auf physikalische Netzwerkverbindungen überwacht. Wenn *Falls hot-plugged* aktiviert ist, wird die Schnittstelle eingerichtet, sobald sie verfügbar ist. Diese Option ähnelt der Option *Bei Systemstart*, es wird jedoch kein Fehler angezeigt, wenn die Schnittstelle bei Systemstart nicht verfügbar ist. Wählen Sie *Manuell*, wenn die Schnittstelle manuell mit `ifup` oder `KInternet` gesteuert werden soll. Wählen Sie *Nie*, wenn das Gerät gar nicht gestartet werden soll. *Bei NFSroot* verhält sich ähnlich wie *Beim Systemstart*, allerdings fährt das Kommando `rcnetwork stop` die Schnittstelle bei dieser Einstellung nicht herunter. Diese Einstellung empfiehlt sich bei einem NFS- oder iSCSI-Root-Dateisystem.

- 3 Klicken Sie auf *Weiter*.
- 4 Klicken Sie auf *Verlassen*, um die Konfiguration zu aktivieren.

Normalerweise können Netzwerk-Schnittstellen nur vom Systemadministrator aktiviert und deaktiviert werden. Wenn Benutzer in der Lage sein sollen, diese Schnittstelle über

Internet zu aktivieren, wählen Sie *Gerätesteuerung für Nicht-Root-Benutzer über Internet aktivieren* aus.

Konfigurieren der Firewall

Sie müssen nicht die genaue Firewall-Konfiguration durchführen, wie unter [Abschnitt 28.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 510) beschrieben. Sie können einige grundlegende Firewall-Einstellungen für Ihr Gerät als Teil der Gerätekonfiguration festlegen. Führen Sie dazu die folgenden Schritte aus:

- 1 Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten eine Karte aus der Liste der erkannten Karten und klicken Sie auf *Bearbeiten*.
- 2 Öffnen Sie die Karteireiter *Allgemein* des Dialogfelds zur Netzwerkkonfiguration.
- 3 Legen Sie die Firewall-Zone fest, der Ihre Schnittstelle zugewiesen werden soll. Mit den zur Verfügung stehenden Optionen können Sie

Firewall deaktiviert

Diese Option ist nur verfügbar, wenn die Firewall deaktiviert ist. Die Firewall wird nicht ausgeführt. Verwenden Sie diese Option nur, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird.

Automatisches Zuweisen von Zonen

Diese Option ist nur verfügbar, wenn die Firewall aktiviert ist. Die Firewall wird ausgeführt und die Schnittstelle wird automatisch einer Firewall-Zone zugewiesen. Die Zone, die das Stichwort 'Beliebig' enthält, oder die externe Zone wird für solch eine Schnittstelle verwendet.

Interne Zone (ungeschützt)

Die Firewall wird ausgeführt, aber es gibt keine Regeln, die diese Schnittstelle schützen. Verwenden Sie diese Option, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird. Sie ist auch dann nützlich, wenn der Computer für die mit dem internen Netzwerk verbundenen Schnittstellen über mehrere Netzwerkschnittstellen verfügt.

Demilitarisierte Zone

Eine demilitarisierte Zone ist eine zusätzliche Verteidigungslinie zwischen einem internen Netzwerk und dem (feindlichen) Internet. Die dieser Zone

zugewiesenen Hosts können vom internen Netzwerk und vom Internet erreicht werden, können jedoch nicht auf das interne Netzwerk zugreifen.

Externe Zone

Die Firewall wird an dieser Schnittstelle ausgeführt und schützt sie vollständig vor anderem (möglicherweise feindlichem) Netzwerkverkehr. Dies ist die Standardoption.

4 Klicken Sie auf *Weiter*.

5 Aktivieren Sie die Konfiguration, indem Sie auf *Verlassen* klicken.

Konfigurieren einer unerkannten Netzwerkkarte

Ihre Karte wird unter Umständen nicht richtig erkannt. In diesem Fall erscheint sie nicht in der Liste der erkannten Karten. Wenn Sie sich nicht sicher sind, ob Ihr System über einen Treiber für die Karte verfügt, können Sie sie manuell konfigurieren. Zur Konfiguration einer unerkannten Netzwerkkarte gehen Sie wie folgt vor:

1 Klicken Sie auf dem Karteireiter *Übersicht* des YaST-Netzwerkkartenmoduls auf *Hinzufügen*.

2 Legen Sie den *Gerätetyp* der Schnittstelle im Dialogfeld *Hardware* mit Hilfe der verfügbaren Optionen fest und geben Sie einen *Konfigurationsnamen* ein. Wenn es sich bei der Netzwerkkarte um ein PCMCIA- oder USB-Gerät handelt, aktivieren Sie das entsprechende Kontrollkästchen und schließen Sie das Dialogfeld durch Klicken auf *Weiter*. Ansonsten können Sie den Kernel *Modulname* definieren, der für die Karte verwendet wird, sowie gegebenenfalls dessen *Optionen*.

3 Klicken Sie auf *Weiter*.

4 Konfigurieren Sie die benötigten Optionen wie die IP-Adresse, die Geräteaktivierung oder die Firewall-Zone für die Schnittstelle auf den Karteireitern *Allgemein*, *Adresse* und *Hardware*. Weitere Informationen zu den Konfigurationsoptionen finden Sie in „[Ändern der Konfiguration einer Netzwerkkarte](#)“ (S. 245).

5 Klicken Sie auf *Weiter*.

6 Klicken Sie auf *Verlassen*, um die neue Netzwerkkonfiguration zu aktivieren.

Konfigurieren des Hostnamens und DNS

Wenn Sie die Netzwerkkonfiguration während der Installation noch nicht geändert haben und die verkabelte Karte verfügbar war, wurde automatisch ein Hostname für Ihren Computer erstellt und DHCP wurde aktiviert. Dasselbe gilt für die Namensserverdaten, die Ihr Host für die Integration in eine Netzwerkkumgebung benötigt. Wenn DHCP für eine Konfiguration der Netzwerkadresse verwendet wird, wird die Liste der Domain Name Server automatisch mit den entsprechenden Daten versorgt. Falls eine statische Konfiguration vorgezogen wird, legen Sie diese Werte manuell fest.

Wenn Sie den Namen Ihres Computers und die Namensserver-Suchliste ändern möchten, gehen Sie wie folgt vor:

- 1 Öffnen Sie den Karteireiter *Hostname/DNS* im YaST-Konfigurationsmodul für Netzwerkkarten.
- 2 Geben Sie den *Hostnamen* und bei Bedarf auch den *Domänennamen* ein. Der Hostname ist global und gilt für alle eingerichteten Netzwerkschnittstellen.

Wenn Sie zum Abrufen einer IP-Adresse DHCP verwenden, wird der Hostname Ihres Computers automatisch durch DHCP festgelegt. Wenn Sie in verschiedenen Netzwerken arbeiten, die Ihrem Computer unterschiedliche Hostnamen zuweisen, empfiehlt es sich, dieses Verhalten durch Deaktivieren der Option *Hostnamen über DHCP ändern* zu unterbinden, da eine Änderung des Hostnamens während der Laufzeit zu Problemen mit dem grafischen Desktop führen kann.

Wenn Sie DHCP zum Abrufen einer IP-Adresse verwenden, wird Ihr Hostname standardmäßig in die Datei `/etc/hosts` geschrieben. Der Name kann in diesem Fall als `127.0.0.2-IP-Adresse` aufgelöst werden. Wenn Sie dieses Standardverhalten unterbinden möchten, deaktivieren Sie *Hostname in /etc/hosts schreiben*. Allerdings kann Ihr Hostname dann ohne aktives Netzwerk nicht aufgelöst werden.

- 3 Geben Sie die Namensserver und Domänensuchlisten an. Nameserver müssen in der IP-Adresse angegeben werden, wie zum Beispiel `192.168.1.116`, nicht im Hostnamen. Suchdomänen sind Domänennamen, die zur Auflösung von Hostnamen ohne angegebene Domäne verwendet werden. Wenn mehrere Suchdomänen verwendet werden, müssen die Domänen durch Kommas oder Leerzeichen getrennt werden.

- 4 Klicken Sie auf *Verlassen*, um die Konfiguration zu aktivieren.

Konfigurieren des Routing

Damit Ihre Maschine mit anderen Maschinen und Netzwerken kommuniziert, müssen Routing-Daten festgelegt werden. Dann nimmt der Netzwerkverkehr den korrekten Weg. Wird DHCP verwendet, werden diese Daten automatisch angegeben. Wird eine statische Konfiguration verwendet, müssen Sie die Daten manuell angeben.

- 1 Öffnen Sie den Karteireiter *Routing* im YaST-Konfigurationsmodul Netzwerkeinstellungen.
- 2 Geben Sie die IP des *Standard-Gateways* ein. Das Standard-Gateway passt zwar zu jedem möglichen Ziel, dies allerdings nicht besonders gut. Falls ein anderer Eintrag existiert, der besser zur benötigten Adresse passt, wird dieser statt der Standardroute verwendet.
- 3 Auf dem Karteireiter *Routing-Tabelle* können weitere Einträge vorgenommen werden. Geben Sie die IP-Adresse für das *Ziel*-Netzwerk, die IP-Adresse des *Gateways* und die *Netzmaske* ein. Wählen Sie das *Gerät* aus, durch das der Datenverkehr zum definierten Netzwerk geroutet wird (das Minuszeichen steht für ein beliebiges Gerät). Verwenden Sie das Minuszeichen `-`, um diese Werte frei zu lassen. Verwenden Sie `Standard` für *Ziel*, um in der Tabelle ein Standard-Gateway einzugeben.

ANMERKUNG

Wenn mehrere Standardrouten verwendet werden, kann die Metrik-Option verwendet werden, um festzulegen, welche Route eine höhere Priorität hat. Geben Sie zur Angabe der Metrik-Option `- MetrikNummer` unter *Optionen* ein. Die Route mit der höheren Metrik wird als Standard verwendet. Wenn das Netzwerkgerät ausgesteckt ist, wird dessen Route entfernt und die nächste Route wird verwendet. Der aktuelle Kernel verwendet jedoch keine Metrik bei statischem Routing, sondern nur Routing-Daemons wie `multipathd` do.

- 4 Falls es sich bei dem System um einen Router handelt, aktivieren Sie die Option *IP-Weiterleitung*.

5 Klicken Sie auf *Verlassen*, um die Konfiguration zu aktivieren.

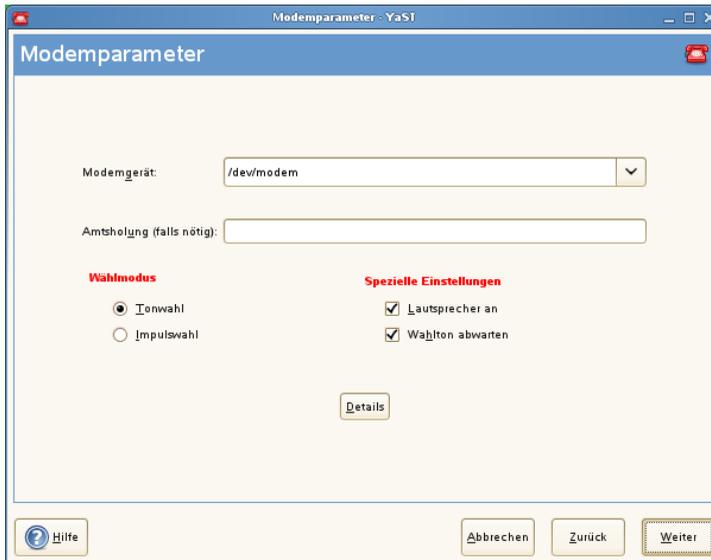
14.4.2 Modem

Im YaST-Kontrollzentrum greifen Sie mit *Netzwerkgeräte > Modem* auf die Modem-Konfiguration zu. Wenn die automatische Erkennung fehlschlägt, öffnen Sie das Dialogfeld für die manuelle Konfiguration, indem Sie auf *Hinzufügen* klicken. Geben Sie unter *Modemgerät* die Schnittstelle an, an die das Modem angeschlossen ist.

TIPP: CDMA- und GPRS-Modems

Konfigurieren Sie unterstützte CDMA- und GPRS-Modems mit dem YaST-Modem-Modul wie reguläre Modems.

Abbildung 14.4 Modemkonfiguration



Wenn eine Telefonanlage zwischengeschaltet ist, müssen Sie ggf. eine Vorwahl für die Amtsholung eingeben. Dies ist in der Regel die Null. Sie können diese aber auch in der Bedienungsanleitung der Telefonanlage finden. Zudem können Sie festlegen, ob Ton- oder Impulswahl verwendet, der Lautsprecher eingeschaltet und der Wählton abgewartet

werden soll. Letztere Option sollte nicht verwendet werden, wenn Ihr Modem an einer Telefonanlage angeschlossen ist.

Legen Sie unter *Details* die Baudrate und die Zeichenketten zur Modeminitialisierung fest. Ändern Sie die vorhandenen Einstellungen nur, wenn das Modem nicht automatisch erkannt wird oder es spezielle Einstellungen für die Datenübertragung benötigt. Dies ist vor allem bei ISDN-Terminaladaptern der Fall. Schließen Sie das Dialogfeld mit *OK*. Wenn Sie die Kontrolle des Modems an normale Benutzer ohne Root-Berechtigung abgeben möchten, aktivieren Sie *Enable Device Control for Non-root User via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen). Auf diese Weise kann ein Benutzer ohne Administratorberechtigungen eine Schnittstelle aktivieren oder deaktivieren. Geben Sie unter *Regulärer Ausdruck für Vorwahl zur Amtsholung* einen regulären Ausdruck an. Dieser muss der vom Benutzer unter *Dial Prefix* (Vorwahl) in KInternet bearbeitbaren Vorwahl entsprechen. Wenn dieses Feld leer ist, kann ein Benutzer ohne Administratorberechtigungen keine andere *Vorwahl* festlegen.

Wählen Sie im nächsten Dialogfeld den ISP (Internet Service Provider). Wenn Sie Ihren Provider aus einer Liste der für Ihr Land verfügbaren Provider auswählen möchten, aktivieren Sie *Land*. Sie können auch auf *Neu* klicken, um ein Dialogfeld zu öffnen, in dem Sie die Daten Ihres ISPs eingeben können. Dazu gehören ein Name für die Einwahlverbindung und den ISP sowie die vom ISP zur Verfügung gestellten Benutzer- und Kennwortdaten für die Anmeldung. Aktivieren Sie *Immer Passwort abfragen*, damit immer eine Passwortabfrage erfolgt, wenn Sie eine Verbindung herstellen.

Im letzten Dialogfeld können Sie zusätzliche Verbindungsoptionen angeben:

Dial-On-Demand

Wenn Sie diese Option aktivieren, müssen Sie mindestens einen Namensserver angeben. Verwenden Sie diese Funktion nur, wenn Sie über eine günstige Internet-Verbindung oder eine Flatrate verfügen, da manche Programme in regelmäßigen Abständen Daten aus dem Internet abfragen.

Während Verbindung DNS ändern

Diese Option ist standardmäßig aktiviert, d. h. die Adresse des Namensservers wird bei jeder Verbindung mit dem Internet automatisch aktualisiert.

DNS automatisch abrufen

Wenn der Provider nach dem Herstellen der Verbindung seinen DNS-Server nicht überträgt, deaktivieren Sie diese Option und geben Sie die DNS-Daten manuell ein.

Automatically Reconnect (Automatische Verbindungswiederherstellung)

Wenn aktiviert, wird nach einem Fehler automatisch versucht, die Verbindung wiederherzustellen.

Ignore prompts (Eingabeaufforderungen ignorieren)

Diese Option deaktiviert die Erkennung der Eingabeaufforderungen des Einwahlservers. Aktivieren Sie diese Option, wenn der Verbindungsaufbau sehr lange dauert oder die Verbindung nicht zustande kommt.

Externe Firewall-Schnittstelle

Durch Auswahl dieser Option wird die Firewall aktiviert und die Schnittstelle als extern festgelegt. So sind Sie für die Dauer Ihrer Internetverbindung vor Angriffen von außen geschützt.

Idle-Time-Out (Sekunden)

Mit dieser Option legen Sie fest, nach welchem Zeitraum der Netzwerkinaktivität die Modemverbindung automatisch getrennt wird.

IP-Details

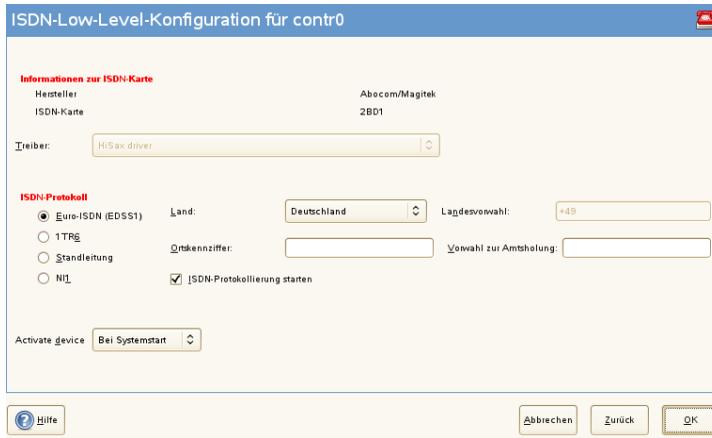
Diese Option öffnet das Dialogfeld für die Adresskonfiguration. Wenn Ihr ISP Ihrem Host keine dynamische IP-Adresse zuweist, deaktivieren Sie die Option *Dynamische IP-Adresse* und geben Sie die lokale IP-Adresse des Hosts und anschließend die entfernte IP-Adresse ein. Diese Informationen erhalten Sie von Ihrem ISP. Lassen Sie die Option *Standard-Route* aktiviert und schließen Sie das Dialogfeld mit *OK*.

Durch Auswahl von *Weiter* gelangen Sie zum ursprünglichen Dialogfeld zurück, in dem eine Zusammenfassung der Modemkonfiguration angezeigt wird. Schließen Sie dieses Dialogfeld mit *Verlassen*.

14.4.3 ISDN

Dieses Modul ermöglicht die Konfiguration einer oder mehrerer ISDN-Karten in Ihrem System. Wenn YaST Ihre ISDN-Karte nicht erkannt hat, klicken Sie auf dem Karteireiter *ISDN-Geräte* auf *Hinzufügen* und wählen Sie Ihre Karte manuell aus. Theoretisch können Sie mehrere Schnittstellen einrichten, im Normalfall ist dies aber nicht notwendig, da Sie für eine Schnittstelle mehrere Provider einrichten können. Die nachfolgenden Dialogfelder dienen dann dem Festlegen der verschiedenen ISDN-Optionen für den ordnungsgemäßen Betrieb der Karte.

Abbildung 14.5 ISDN-Konfiguration

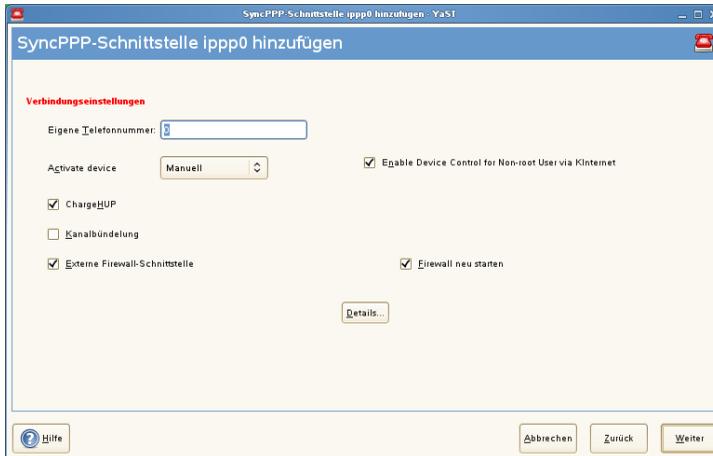


Wählen Sie im nächsten Dialogfeld, das in **Abbildung 14.5**, „ISDN-Konfiguration“ (S. 257) dargestellt ist, das zu verwendende Protokoll. Der Standard ist *Euro-ISDN (EDSS1)*, aber für ältere oder größere Telefonanlagen wählen Sie *1TR6*. Für die USA gilt *N11*. Wählen Sie das Land in dem dafür vorgesehenen Feld aus. Die entsprechende Landeskenntzahl wird im Feld daneben angezeigt. Geben Sie dann noch die *Ortsnetz-kennzahl* und ggf. die *Vorwahl zur Amtsholung* ein. Wenn nicht der gesamte ISDN-Datenverkehr protokolliert werden soll, deaktivieren Sie die Option *ISDN-Protokollie-rung starten*.

Geräte-Aktivierung definiert, wie die ISDN-Schnittstelle gestartet werden soll: *Beim Systemstart* initialisiert den ISDN-Treiber bei jedem Systemstart. Bei *Manuell* müssen Sie den ISDN-Treiber als `root` laden. Verwenden Sie hierfür den Befehl `rcisdn start`. *Falls hot-plugged* wird für PCMCIA- oder USB-Geräte verwendet. Diese Option lädt den Treiber, nachdem das Gerät eingesteckt wurde. Wenn Sie alle Einstel-lungen vorgenommen haben, klicken Sie auf *OK*.

Im nächsten Dialogfeld können Sie den Schnittstellentyp für die ISDN-Karte angeben und weitere ISPs zu einer vorhandenen Schnittstelle hinzufügen. Schnittstellen können in den Betriebsarten `SyncPPP` oder `RawIP` angelegt werden. Die meisten ISPs ver-wenden jedoch den `SyncPPP`-Modus, der im Folgenden beschrieben wird.

Abbildung 14.6 Konfiguration der ISDN-Schnittstelle



Die Nummer, die Sie unter *Eigene Telefonnummer* eingeben, ist vom jeweiligen Anschlusszenario abhängig:

ISDN-Karte direkt an der Telefondose

Eine standardmäßige ISDN-Leitung bietet Ihnen drei Rufnummern (sogenannte MSNs, Multiple Subscriber Numbers). Auf Wunsch können (auch) bis zu zehn Rufnummern zur Verfügung gestellt werden. Eine dieser MSNs muss hier eingegeben werden, allerdings ohne Ortsnetzkenzahl. Sollten Sie eine falsche Nummer eintragen, wird Ihr Netzbetreiber die erste Ihrem ISDN-Anschluss zugeordnete MSN verwenden.

ISDN-Karte an einer Telefonanlage

Auch hier kann die Konfiguration je nach installierten Komponenten variieren:

1. Kleinere Telefonanlagen für den Hausgebrauch verwenden für interne Anrufe in der Regel das Euro-ISDN-Protokoll (EDSS1). Diese Telefonanlagen haben einen internen S0-Bus und verwenden für die angeschlossenen Geräte interne Rufnummern.

Für die Angabe der MSN verwenden Sie eine der internen Rufnummern. Eine der möglichen MSNs Ihrer Telefonanlage sollte funktionieren, sofern für diese der Zugriff nach außen freigeschaltet ist. Im Notfall funktioniert eventuell auch eine einzelne Null. Weitere Informationen dazu entnehmen Sie bitte der Dokumentation Ihrer Telefonanlage.

2. Größere Telefonanlagen (z. B. in Unternehmen) verwenden für die internen Anschlüsse das Protokoll ITR6. Die MSN heißt hier EAZ und ist üblicherweise die Durchwahl. Für die Konfiguration unter Linux ist die Eingabe der letzten drei Stellen der EAZ in der Regel ausreichend. Im Notfall probieren Sie die Ziffern 1 bis 9.

Wenn die Verbindung vor der nächsten zu zahlenden Gebühreneinheit getrennt werden soll, aktivieren Sie *ChargeHUP*. Dies funktioniert unter Umständen jedoch nicht mit jedem ISP. Durch Auswahl der entsprechenden Option können Sie auch die Kanalbündelung (Multilink-PPP) aktivieren. Sie können die Firewall für die Verbindung aktivieren, indem Sie *Externe Firewall-Schnittstelle* und *Firewall neu starten* auswählen. Wenn Sie normalen Benutzern ohne Administratorberechtigung die Aktivierung und Deaktivierung der Schnittstelle erlauben möchten, aktivieren Sie *Enable Device Control for Non-root user via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen).

Details öffnet ein Dialogfeld, das für die Implementierung komplexerer Verbindungsszenarien ausgelegt und aus diesem Grund für normale Heimbenutzer nicht relevant ist. Schließen Sie das Dialogfeld *Details* mit *OK*.

Im nächsten Dialogfeld legen Sie die Einstellungen für die Vergabe der IP-Adressen fest. Wenn Ihr Provider Ihnen keine statische IP-Adresse zugewiesen hat, wählen Sie *Dynamische IP-Adresse*. Anderenfalls tragen Sie gemäß den Angaben Ihres Providers die lokale IP-Adresse Ihres Rechners sowie die entfernte IP-Adresse in die dafür vorgesehenen Felder ein. Soll die anzulegende Schnittstelle als Standard-Route ins Internet dienen, aktivieren Sie *Standard-Route*. Beachten Sie, dass jeweils nur eine Schnittstelle pro System als Standard-Route in Frage kommt. Schließen Sie das Dialogfeld mit *Weiter*.

Im folgenden Dialogfeld können Sie Ihr Land angeben und einen ISP wählen. Bei den in der Liste aufgeführten ISPs handelt es sich um Call-By-Call-Provider. Wenn Ihr ISP in der Liste nicht aufgeführt ist, wählen Sie *Neu*. Dadurch wird das Dialogfeld *Provider-Parameter* geöffnet, in dem Sie alle Details zu Ihrem ISP eingeben können. Die Telefonnummer darf keine Leerzeichen oder Kommas enthalten. Geben Sie dann den Benutzernamen und das Passwort ein, den bzw. das Sie von Ihrem ISP erhalten haben. Wählen Sie anschließend *Weiter*.

Um auf einem Einzelplatz-Arbeitsplatzrechner *Dial-On-Demand* verwenden zu können, müssen Sie auf jeden Fall den Namensserver (DNS-Server) angeben. Die meisten Provider unterstützen heute die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau

wird die IP-Adresse eines Namensservers übergeben. Bei einem Einzelplatz-Arbeitsplatz-rechner müssen Sie dennoch eine Platzhalteradresse wie 192.168.22.99 angeben. Wenn Ihr ISP keine dynamischen DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namensserver des ISPs ein. Ferner können Sie festlegen, nach wie vielen Sekunden die Verbindung automatisch getrennt werden soll, falls in der Zwischenzeit kein Datenaustausch stattgefunden hat. Bestätigen Sie die Einstellungen mit *Weiter*. YaST zeigt eine Zusammenfassung der konfigurierten Schnittstellen an. Klicken Sie zur Aktivierung dieser Einstellungen auf *Fertig stellen*.

14.4.4 Kabelmodem

In einigen Ländern wird der Zugriff auf das Internet über Kabel-TV mehr und mehr üblich. Der TV-Kabel-Abonnent erhält in der Regel ein Modem, das auf der einen Seite an die TV-Kabelbuchse und auf der anderen Seite (mit einem 10Base-TG Twisted-Pair-Kabel) an die Netzwerkkarte des Computers angeschlossen wird. Das Kabelmodem stellt dann eine dedizierte Internetverbindung mit einer statischen IP-Adresse zur Verfügung.

Richten Sie sich bei der Konfiguration der Netzwerkkarte nach den Anleitungen Ihres ISP (Internet Service Provider) und wählen Sie entweder *Dynamic Address* (Dynamische Adresse) oder *Statically assigned IP address* (Statisch zugewiesene IP-Adresse) aus. Die meisten Provider verwenden heute DHCP. Eine statische IP-Adresse ist oft Teil eines speziellen Firmenkontos.

Weitere Informationen zur Konfiguration von Kabelmodems erhalten Sie im entsprechenden Artikel der Support-Datenbank. Dieser ist online verfügbar unter http://en.opensuse.org/SDB:Setting_Up_an_Internet_Connection_via_Cable_Modem_with_SuSE_Linux_8.0_or_Higher.

14.4.5 DSL

Um das DSL-Gerät zu konfigurieren, wählen Sie das *DSL*-Modul aus dem Abschnitt YaST*Netzwerkgeräte* aus. Dieses YaST-Modul besteht aus mehreren Dialogfeldern, in denen Sie die Parameter des DSL-Zugangs basierend auf den folgenden Protokollen festlegen können:

- PPP über Ethernet (PPPoE)

- PPP über ATM (PPPoATM)
- CAPI für ADSL (Fritz-Karten)
- Tunnel-Protokoll für Point-to-Point (PPTP) – Österreich

Im Dialogfeld *DSL-Konfiguration* finden Sie auf dem Karteireiter *DSL-Geräte* eine Liste der installierten DSL-Geräte. Zur Änderung der Konfiguration eines DSL-Geräts wählen Sie das Gerät in der Liste aus und klicken Sie auf *Bearbeiten*. Wenn Sie ein neues DSL-Gerät manuell konfigurieren möchten, klicken Sie auf *Hinzufügen*.

Beachten Sie bitte, dass die Konfiguration Ihres DSL-Zugangs mit PPPoE und PPTP eine korrekte Konfiguration der Netzwerkkarte voraussetzt. Falls noch nicht geschehen, konfigurieren Sie zunächst die Karte, indem Sie *Netzwerkkarten konfigurieren* auswählen (siehe **Abschnitt 14.4.1, „Konfigurieren der Netzwerkkarte mit YaST“** (S. 243)). Bei DSL-Verbindungen können die Adressen zwar automatisch vergeben werden, jedoch nicht über DHCP. Aus diesem Grund dürfen Sie die Option *Dynamic Address* (Dynamische Adresse) nicht aktivieren. Geben Sie stattdessen eine statische Dummy-Adresse für die Schnittstelle ein, z. B. 192.168.22.1. Geben Sie unter *Subnetzmaske* 255.255.255.0 ein. Wenn Sie eine Einzelplatz-Arbeitsstation konfigurieren, lassen Sie das Feld *Standard-Gateway* leer.

TIPP

Die Werte in den Feldern *IP-Adresse* und *Subnetzmaske* sind lediglich Platzhalter. Sie haben für den Verbindungsaufbau mit DSL keine Bedeutung und werden nur zur Initialisierung der Netzwerkkarte benötigt.

Wählen Sie im ersten Dialogfeld für die DSL-Konfiguration (siehe **Abbildung 14.7, „DSL-Konfiguration“** (S. 262)) den *PPP-Modus* und die *Ethernetkarte*, mit der das DSL-Modem verbunden ist (in den meisten Fällen ist dies `eth0`). Geben Sie anschließend unter *Geräte-Aktivierung* an, ob die DSL-Verbindung schon beim Booten des Systems gestartet werden soll. Aktivieren Sie *Enable Device Control for Non-root User via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen), wenn Sie normalen Benutzern ohne Root-Berechtigung die Aktivierung und Deaktivierung der Schnittstelle via KInternet erlauben möchten.

Im nächsten Dialogfeld können Sie Ihr Land und danach in der Liste der in Ihrem Land operierenden ISPs einen Internetprovider auswählen. Die Inhalte der danach folgenden Dialogfelder der DSL-Konfiguration hängen stark von den bis jetzt festgelegten

Optionen ab und werden in den folgenden Abschnitten daher nur kurz angesprochen. Weitere Informationen zu den verfügbaren Optionen erhalten Sie in der ausführlichen Hilfe in den einzelnen Dialogfeldern.

Abbildung 14.7 DSL-Konfiguration



Um auf einem Einzelplatz-Arbeitsplatzrechner *Dial-On-Demand* verwenden zu können, müssen Sie auf jeden Fall den Namensserver (DNS-Server) angeben. Die meisten Provider unterstützen die dynamische DNS-Vergabe, d. h. beim Verbindungsaufbau wird die IP-Adresse eines Namensservers übergeben. Bei einem Einzelplatz-Arbeitsplatzrechner müssen Sie jedoch eine Platzhalteradresse wie 192.168.22.99 angeben. Wenn Ihr ISP keine dynamische DNS-Namen unterstützt, tragen Sie die IP-Adressen der Namensserver des ISPs ein.

Idle-Timeout (Sekunden) definiert, nach welchem Zeitraum der Netzwerkinaktivität die Verbindung automatisch getrennt wird. Hier sind Werte zwischen 60 und 300 Sekunden empfehlenswert. Wenn *Dial-On-Demand* deaktiviert ist, kann es hilfreich sein, das Zeitlimit auf Null zu setzen, um das automatische Trennen der Verbindung zu vermeiden.

Die Konfiguration von T-DSL entspricht weitgehend der Konfiguration von DSL. Wählen Sie einfach *T-Online* als Provider und YaST öffnet das Konfigurationsdialogfeld für T-DSL. In diesem Dialogfeld geben Sie einige zusätzliche Informationen ein, die für T-DSL erforderlich sind: die Anschlusskennung, die T-Online-Nummer, die

Benutzerkennung und Ihr Passwort. Diese Informationen finden Sie in den T-DSL-Anmeldeunterlagen.

14.5 NetworkManager

NetworkManager ist die ideale Lösung für einen mobilen Arbeitsplatzrechner. Wenn Sie viel unterwegs sind und den NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen Netzwerken zu verschwenden. NetworkManager kann automatisch Verbindungen zu den bekannten WLAN-Netzwerken herstellen. Bei zwei oder gar mehreren Verbindungsmöglichkeiten stellt der NetworkManager die Verbindung zum schnelleren Netzwerk her.

NetworkManager ist jedoch nicht in jedem Fall eine passende Lösung, daher können Sie immer noch zwischen der herkömmlichen Methode zur Verwaltung von Netzwerkverbindungen (ifup) und NetworkManager wählen. Wenn Ihre Netzwerkverbindung mit NetworkManager verwaltet werden soll, aktivieren Sie NetworkManager im Netzwerkkartenmodul von YaST wie in Abschnitt „Aktivieren von NetworkManager“ (Kapitel 10, *Verwalten der Netzwerkverbindungen mit NetworkManager*, ↑Start) beschrieben. Eine Liste der Anwendungsfälle sowie eine detaillierte Beschreibung zur Konfiguration und Verwendung von NetworkManager finden Sie unter Kapitel 10, *Verwalten der Netzwerkverbindungen mit NetworkManager* (↑Start).

Richten Sie nach Auswahl der Methode zur Verwaltung von Netzwerkverbindungen Ihre Netzwerkkarte mit der automatischen Konfiguration über DHCP oder eine statische IP-Adresse ein, oder konfigurieren Sie Ihr Modem. Eine ausführliche Beschreibung der Netzwerkkonfiguration mit YaST erhalten Sie unter [Abschnitt 14.4, „Konfigurieren von Netzwerkverbindungen mit YaST“](#) (S. 243) und [Abschnitt 25.1, „Wireless LAN“](#) (S. 477). Konfigurieren Sie die unterstützten drahtlosen Karten direkt in NetworkManager, indem Sie die NetworkManager-Miniprogramme in KDE oder GNOME verwenden.

Einige Unterschiede zwischen ifup und NetworkManager sind:

root-Berechtigungen

Wenn Sie NetworkManager zur Netzwerkeinrichtung verwenden, können Sie mithilfe eines Miniprogramms von Ihrer Desktop-Umgebung aus Ihre Netzwerkverbindung jederzeit auf einfache Weise wechseln, stoppen oder starten. NetworkManager ermöglicht zudem die Änderung und Konfiguration drahtloser Kartenver-

bindungen ohne Anforderung von `root`-Berechtigungen. Aus diesem Grund ist NetworkManager die ideale Lösung für einen mobilen Arbeitsplatzrechner.

Die herkömmliche Konfiguration mit `ifup` bietet wie die benutzerverwalteten Geräte ebenfalls verschiedene Möglichkeiten zum Wechseln, Stoppen oder Starten der Verbindung mit oder ohne Benutzereingriff. Jedoch sind `root`-Berechtigungen erforderlich, um ein Netzwerkgerät zu ändern oder zu konfigurieren. Dies stellt häufig ein Problem bei der mobilen Computernutzung dar, bei der es nicht möglich ist, alle Verbindungsmöglichkeiten vorzukonfigurieren.

Typen von Netzwerkverbindungen

Sowohl die herkömmliche Konfiguration als auch NetworkManager können Netzwerkverbindungen mit drahtlosen Netzwerken (mit WEP-, WPA-PSK- und WPA-Enterprise-Zugriff), Einwahlverbindungen und verkabelten Netzwerken herstellen und dabei DHCP oder statische Konfigurationen verwenden. Darüber hinaus unterstützen sie Verbindungen über VPN.

NetworkManager sorgt für eine zuverlässige Verbindung rund um die Uhr und verwendet dazu die beste verfügbare Verbindung. Wenn verfügbar, wird die schnellste Kabelverbindung verwendet. Wurde das Netzkabel versehentlich ausgesteckt, wird erneut versucht, eine Verbindung herzustellen. Der NetworkManager sucht in der Liste Ihrer drahtlosen Verbindungen nach dem Netzwerk mit dem stärksten Signal und stellt automatisch eine Verbindung her. Wenn Sie dieselbe Funktionalität mit `ifup` erhalten möchten, ist einiger Konfigurationsaufwand erforderlich.

14.6 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte immer die letzte Alternative sein. Wir empfehlen, YaST zu benutzen. Die folgenden Hintergrundinformationen zur Netzwerkkonfiguration können Ihnen jedoch auch bei der Arbeit mit YaST behilflich sein.

Wenn der Kernel eine Netzwerkkarte erkennt und eine entsprechende Netzwerkschnittstelle erstellt, weist er dem Gerät einen Namen zu. Dieser richtet sich nach der Reihenfolge der Geräteerkennung bzw. nach der Reihenfolge, in der die Kernel-Module geladen werden. Die vom Kernel vergebenen Standardgerätenamen lassen sich nur in sehr einfachen oder überaus kontrollierten Hardwareumgebungen vorhersagen. Auf Systemen, auf denen es möglich ist, Hardware während der Laufzeit hinzuzufügen oder zu entfer-

nen, oder die die automatische Konfiguration von Geräten zulassen, können vom Kernel über mehrere Neustarts hinaus keine stabilen Netzwerkgerätenamen erwartet werden.

Für die Systemkonfigurationstools sind jedoch dauerhafte (persistente) Schnittstellennamen erforderlich. Dieses Problem wird durch udev gelöst. udev führt eine Datenbank mit den bekannten Netzwerkschnittstellen. Das Programm teilt diesen Schnittstellen statt der vom Kernel zugewiesenen Namen persistente Namen zu und speichert diese in der Datenbank. Die udev-Datenbank mit den Netzwerkschnittstellen wird in der Datei `/etc/udev/rules.d/70-persistent-net.rules` gespeichert. Pro Zeile dieser Datei wird eine Netzwerkschnittstelle beschrieben und deren persistenter Name angegeben. Die zugewiesenen Namen können vom Systemadministrator im Eintrag `NAME=""` geändert werden. Nachdem udev ein Netzwerkgerät auf den konfigurierten Namen umbenannt hat, können Sie die Systemkonfiguration mittels des Kommandos `ifup` auf die Schnittstelle anwenden.

Tabelle 14.5, „Skripten für die manuelle Netzwerkkonfiguration“ (S. 265) zeigt die wichtigsten an der Netzwerkkonfiguration beteiligten Skripten.

Tabelle 14.5 *Skripten für die manuelle Netzwerkkonfiguration*

Befehl	Funktion
<code>if{up,down,status}</code>	Die <code>if*</code> -Skripten starten vorhandene Netzwerkschnittstellen oder setzen den Status der angegebenen Schnittstelle zurück. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl <code>ifup</code> .
<code>rcnetwork</code>	Mit dem Skript <code>rcnetwork</code> können alle Netzwerkschnittstellen oder nur eine bestimmte Netzwerkschnittstelle gestartet, gestoppt oder neu gestartet werden. Mit <code>rcnetwork stop</code> stoppen Sie Netzwerkschnittstellen, mit <code>rcnetwork start</code> starten Sie Netzwerkschnittstellen und mit <code>rcnetwork restart</code> führen Sie einen Neustart der Netzwerkschnittstellen durch. Wenn Sie nur eine Netzwerkschnittstelle stoppen, starten oder neu starten möchten, geben Sie nach dem jeweiligen Kommando den Namen der Schnittstelle ein, zum Beispiel <code>rcnetwork restart eth0</code> . Wenn keine Schnittstelle angegeben ist, werden die

Befehl	Funktion
	<p>Firewall und alle Netzwerkschnittstellen gestoppt, gestartet bzw. neu gestartet. Das Kommando <code>rcnetwork status</code> zeigt den Status und die IP-Adressen der Netzwerkschnittstellen an. Außerdem gibt das Kommando an, ob auf den Schnittstellen ein DHCP-Client ausgeführt wird. Mit <code>rcnetwork stop-all-dhcp-clients</code> und <code>rcnetwork restart-all-dhcp-clients</code> können Sie die auf den Netzwerkschnittstellen ausgeführten DHCP-Clients stoppen und wieder starten.</p>

Weitere Informationen zu `udev` und persistenten Gerätenamen finden Sie in [Kapitel 11, *Gerätemanagement über dynamischen Kernel mithilfe von udev*](#) (S. 183).

14.6.1 Konfigurationsdateien

Dieser Abschnitt bietet einen Überblick über die Netzwerkkonfigurationsdateien und erklärt ihren Zweck sowie das verwendete Format.

`/etc/sysconfig/network/ifcfg-*`

Diese Dateien enthalten die Konfigurationsdaten für Netzwerkschnittstellen. Sie enthalten Informationen wie den Startmodus und die IP-Adresse. Mögliche Parameter sind auf der `man`-Seite für den Befehl `ifup` beschrieben. Wenn nur eine einzelne allgemeine Einstellung nur für eine bestimmte Schnittstelle verwendet werden soll, können außerdem alle Variablen aus den Dateien `dhcp`, `wireless` und `config` in den `ifcfg-*`-Dateien verwendet werden.

`/etc/sysconfig/network/{config, dhcp, wireless}`

Die Datei `config` enthält allgemeine Einstellungen für das Verhalten von `ifup`, `ifdown` und `ifstatus`. `dhcp` enthält DHCP-Einstellungen und `wireless` Einstellungen für Wireless-LAN-Karten. Die Variablen in allen drei Konfigurationsdateien

sind kommentiert und können auch in den `ifcfg-*`-Dateien verwendet werden, wo sie mit einer höheren Priorität verarbeitet werden.

`/etc/sysconfig/network/{routes,ifroute-*}`

Hier wird das statische Routing von TCP/IP-Paketen festgelegt. Alle statischen Routen, die für verschiedenen Systemaufgaben benötigt werden, können in die Datei `/etc/sysconfig/network/routes` eingegeben werden: Routen zu einem Host, Routen zu einem Host über Gateways und Routen zu einem Netzwerk. Definieren Sie für jede Schnittstelle, die individuelles Routing benötigt, eine zusätzliche Konfigurationsdatei: `/etc/sysconfig/network/ifroute-*`. Ersetzen Sie `*` durch den Namen der Schnittstelle. Die folgenden Einträge werden in die Routing-Konfigurationsdatei aufgenommen:

# Destination	Dummy/Gateway	Netmask	Device
#			
127.0.0.0	0.0.0.0	255.255.255.0	lo
204.127.235.0	0.0.0.0	255.255.255.0	eth0
default	204.127.235.41	0.0.0.0	eth0
207.68.156.51	207.68.145.45	255.255.255.255	eth1
192.168.0.0	207.68.156.51	255.255.0.0	eth1

Das Routenziel steht in der ersten Spalte. Diese Spalte kann die IP-Adresse eines Netzwerks oder Hosts bzw., im Fall von *erreichbaren* Namensservern, den voll qualifizierten Netzwerk- oder Hostnamen enthalten.

Die zweite Spalte enthält das Standard-Gateway oder ein Gateway, über das der Zugriff auf einen Host oder ein Netzwerk erfolgt. Die dritte Spalte enthält die Netzmaske für Netzwerke oder Hosts hinter einem Gateway. Die Maske `255.255.255.255` gilt beispielsweise für einen Host hinter einem Gateway.

Die vierte Spalte ist nur für Netzwerke relevant, die mit dem lokalen Host verbunden sind, z. B. Loopback-, Ethernet-, ISDN-, PPP- oder Dummy-Geräte. In diese Spalte muss der Gerätenamen eingegeben werden.

In einer (optionalen) fünften Spalte kann der Typ einer Route angegeben werden. Nicht benötigte Spalten sollten ein Minuszeichen `-` enthalten, um sicherzustellen, dass der Parser den Befehl korrekt interpretiert. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `routes(5)`.

`/etc/resolv.conf`

In dieser Datei wird die Domäne angegeben, zu der der Host gehört (Schlüsselwort `search`). Ebenfalls aufgeführt ist der Status des Namenservers, auf den der Zugriff erfolgt (Schlüsselwort `nameserver`). Es können mehrere Domännennamen angegeben werden. Bei der Auflösung eines Namens, der nicht voll qualifiziert ist, wird versucht, einen solchen zu generieren, indem die einzelnen `search`-Einträge angehängt werden. Wenn Sie mehrere Namenserver verwenden, geben Sie mehrere Zeilen ein, wobei jede Zeile mit `nameserver` beginnt. Stellen Sie Kommentaren ein `#`-Zeichen voran. YaST trägt den angegebenen Namenserver in diese Datei ein. **Beispiel 14.5**, „`/etc/resolv.conf`“ (S. 268) zeigt, wie `/etc/resolv.conf` aussehen könnte.

Beispiel 14.5 `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

Einige Dienste, zum Beispiel `pppd` (`wvdial`), `ippd` (`isdn`), `dhcp` (`dhcpcd` und `dhclient`) und `pcmcia` bearbeiten die Datei `/etc/resolv.conf` über das Skript `modify_resolvconf`. Wenn die Datei `/etc/resolv.conf` von diesem Skript vorübergehend geändert wurde, enthält sie einen vordefinierten Kommentar mit Informationen zu dem Dienst, der sie geändert hat, dem Speicherort, an dem die ursprüngliche Datei gesichert wurde, sowie Informationen dazu, wie der automatische Änderungsmechanismus deaktiviert werden kann. Wenn `/etc/resolv.conf` mehrmals geändert wird, enthält die Datei die Änderungen in verschachtelter Form. Diese können auf saubere Weise auch dann wieder rückgängig gemacht werden, wenn dieser Umkehrvorgang in einer anderen Reihenfolge ausgeführt wird, als die Änderungen vorgenommen wurden. Dienste, die diese Flexibilität möglicherweise benötigen, sind beispielsweise `isdn` und `pcmcia`.

Wenn ein Dienst auf unnormale Weise beendet wurde, kann die ursprüngliche Datei mit `modify_resolvconf` wiederhergestellt werden. Zudem wird beispielsweise nach einem Systemabsturz beim Booten des Systems ein Test ausgeführt, um zu ermitteln, ob eine unsaubere, geänderte `resolv.conf` vorhanden ist (z. B. durch einen Systemabsturz), in welchem Fall die ursprüngliche (unveränderte) `resolv.conf` wiederhergestellt wird.

YaST ermittelt mit dem Befehl `modify_resolvconf check`, ob `resolv.conf` geändert wurde, und warnt den Benutzer, dass Änderungen nach dem Wiederherstellen der Datei verloren gehen. Abgesehen davon verlässt sich YaST nicht auf `modify_resolvconf`, d. h. die Auswirkungen der Änderung von `resolv.conf` mit YaST sind identisch mit allen anderen manuellen Änderungen. Die Änderungen sind in beiden Fällen permanent. Die von den genannten Diensten vorgenommenen Änderungen sind nur temporärer Natur.

/etc/hosts

In dieser Datei werden, wie in [Beispiel 14.6](#), „`/etc/hosts`“ (S. 269) gezeigt, IP-Adressen zu Hostnamen zugewiesen. Wenn kein Namensserver implementiert ist, müssen alle Hosts, für die IP-Verbindungen eingerichtet werden sollen, hier aufgeführt sein. Geben Sie für jeden Host in die Datei eine Zeile ein, die aus der IP-Adresse, dem voll qualifizierten Hostnamen und dem Hostnamen besteht. Die IP-Adresse muss am Anfang der Zeile stehen und die Einträge müssen durch Leerzeichen und Tabulatoren getrennt werden. Kommentaren wird immer das #-Zeichen vorangestellt.

Beispiel 14.6 `/etc/hosts`

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

/etc/networks

Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen. Weitere Informationen hierzu finden Sie unter [Beispiel 14.7](#), „`/etc/networks`“ (S. 269).

Beispiel 14.7 `/etc/networks`

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

Diese Datei steuert das Auflösen von Namen, d. h. das Übersetzen von Host- und Netzwerknamen über die `resolver`-Bibliothek. Diese Datei wird nur für Programme verwendet, die mit `libc4` oder `libc5` gelinkt sind. Weitere Informationen zu aktuellen

glibc-Programmen finden Sie in den Einstellungen in `/etc/nsswitch.conf`. Jeder Parameter muss in einer eigenen Zeile stehen. Kommentare werden durch ein `#`-Zeichen eingeleitet. Die verfügbaren Parameter sind in [Tabelle 14.6](#), „Parameter für `/etc/host.conf`“ (S. 270) aufgeführt. Ein Beispiel für `/etc/host.conf` wird in [Beispiel 14.8](#), „`/etc/host.conf`“ (S. 270) gezeigt.

Tabelle 14.6 Parameter für `/etc/host.conf`

<code>order hosts, bind</code>	Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente (getrennt durch Leerzeichen oder Kommas): <i>Hosts</i> : Sucht die <code>/etc/hosts</code> -Datei <i>bind</i> : Greift auf einen Namensserver zu <i>nis</i> : Verwendet NIS
<code>multi on/off</code>	Legt fest, ob ein in <code>/etc/hosts</code> eingegebener Host mehrere IP-Adressen haben kann.
<code>nospoof on</code> <code>spoofalert on/off</code>	Diese Parameter beeinflussen das <i>spoofing</i> des Namensservers, haben aber weiter keinen Einfluss auf die Netzwerkkonfiguration.
<code>trim Domänenna- me</code>	Der angegebene Domänenname wird vor dem Auflösen des Hostnamens von diesem abgeschnitten (insofern der Hostname diesen Domännennamen enthält). Diese Option ist dann von Nutzen, wenn in der Datei <code>/etc/hosts</code> nur Namen aus der lokalen Domäne stehen, diese aber auch mit angehängtem Domännennamen erkannt werden sollen.

Beispiel 14.8 `/etc/host.conf`

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

`/etc/nsswitch.conf`

Mit der GNU C Library 2.0 wurde *Name Service Switch* (NSS) eingeführt. Weitere Informationen hierzu finden Sie auf der Manualpage für `nsswitch.conf(5)` und im Dokument *The GNU C Library Reference Manual*.

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Beispiel für `nsswitch.conf` ist in **Beispiel 14.9**, „`/etc/nsswitch.conf`“ (S. 271) dargestellt. Kommentare werden durch ein `#`-Zeichen eingeleitet. Der Eintrag unter der `hosts`-Datenbank bedeutet, dass Anfragen über DNS an `/etc/hosts(files)` gehen.

Beispiel 14.9 `/etc/nsswitch.conf`

```
passwd:      compat
group:       compat

hosts:       files dns
networks:    files dns

services:    db files
protocols:   db files

netgroup:    files
automount:   files nis
```

Die über NSS verfügbaren „Datenbanken“ sind in **Tabelle 14.7**, „Über `/etc/nsswitch.conf` verfügbare Datenbanken“ (S. 271) aufgelistet. Zusätzlich sind in Zukunft zudem `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten. Die Konfigurationsoptionen für NSS-Datenbanken sind in **Tabelle 14.8**, „Konfigurationsoptionen für NSS-„Datenbanken““ (S. 272) aufgelistet.

Tabelle 14.7 Über `/etc/nsswitch.conf` verfügbare Datenbanken

<code>aliases</code>	Mail-Aliasse, die von <code>sendmail</code> implementiert werden. Siehe <code>man5 aliases</code> .
<code>ethers</code>	Ethernet-Adressen
Gruppe	Für Benutzergruppen, die von <code>getgrent</code> verwendet werden. Weitere Informationen hierzu finden Sie auch auf der Manualpage für den Befehl <code>group</code> .

<code>hosts</code>	Für Hostnamen und IP-Adressen, die von <code>gethostbyname</code> und ähnlichen Funktionen verwendet werden.
<code>netgroup</code>	Im Netzwerk gültige Host- und Benutzerlisten zum Steuern von Zugriffsrechten. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>netgroup(5)</code> .
<code>networks</code>	Netzwerknamen und -adressen, die von <code>getnetent</code> verwendet werden.
<code>passwd</code>	Benutzerpasswörter, die von <code>getpwent</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage <code>passwd(5)</code> .
<code>protocols</code>	Netzwerkprotokolle, die von <code>getprotoent</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>protocols(5)</code> .
<code>rpc</code>	Remote Procedure Call-Namen und -Adressen, die von <code>getrpcbyname</code> und ähnlichen Funktionen verwendet werden.
<code>services</code>	Netzwerkdienste, die von <code>getservent</code> verwendet werden.
<code>shadow</code>	Shadow-Passwörter der Benutzer, die von <code>getspnam</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>shadow(5)</code> .

Tabelle 14.8 *Konfigurationsoptionen für NSS-„Datenbanken“*

Dateien	Direkter Dateizugriff, z. B. <code>/etc/aliases</code>
<code>db</code>	Zugriff über eine Datenbank
<code>nis, nisplus</code>	NIS, siehe auch Kapitel 19, Arbeiten mit NIS (S. 339)
<code>dns</code>	Nur bei <code>hosts</code> und <code>networks</code> als Erweiterung verwendbar

compat

Nur bei `passwd`, `shadow` und `group` als Erweiterung
verwendbar

/etc/nscd.conf

Mit dieser Datei wird `nscd` (Name Service Cache Daemon) konfiguriert. Weitere Informationen hierzu finden Sie auf den man-Seiten `nscd(8)` und `nscd.conf(5)`. Standardmäßig werden die Systemeinträge von `passwd` und `groups` von `nscd` gecacht. Dies ist wichtig für die Leistung der Verzeichnisdienste, z. B. NIS und LDAP, da anderenfalls die Netzwerkverbindung für jeden Zugriff auf Namen oder Gruppen verwendet werden muss. `hosts` wird standardmäßig nicht gecacht, da der Mechanismus in `nscd` dazu führen würde, dass das lokale System keine Trust-Forward- und Reverse-Lookup-Tests mehr ausführen kann. Statt `nscd` das Cachen der Namen zu übertragen, sollten Sie einen DNS-Server für das Cachen einrichten.

Wenn das Caching für `passwd` aktiviert wird, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten von `nscd` mit dem Befehl `rcnscd restart` kann diese Wartezeit verkürzt werden.

/etc/HOSTNAME

Hier steht der Name des Computers, also nur der Hostname ohne den Domännennamen. Diese Datei wird von verschiedenen Skripten beim Booten des Computers gelesen. Sie darf nur eine Zeile enthalten, in der der Hostname steht.

14.6.2 Testen der Konfiguration

Bevor Sie Ihre Konfiguration in den Konfigurationsdateien speichern, können Sie sie testen. Zum Einrichten einer Testkonfiguration verwenden Sie den Befehl `ip`. Zum Testen der Verbindung verwenden Sie den Befehl `ping`. Ältere Konfigurationswerkzeuge, `ifconfig` und `route`, sind ebenfalls verfügbar.

Die Befehle `ip`, `ifconfig` und `route` ändern die Netzwerkkonfiguration direkt, ohne sie in der Konfigurationsdatei zu speichern. Wenn Sie die Konfiguration nicht in die korrekten Konfigurationsdateien eingeben, geht die geänderte Netzwerkkonfiguration nach dem Neustart verloren.

Konfigurieren einer Netzwerkschnittstelle mit ip

`ip` ist ein Werkzeug zum Anzeigen und Konfigurieren von Routing, Netzwerkgeräten, Richtlinien-Routing und Tunneln. Er wurde als Ersatz für die älteren Werkzeuge `ifconfig` und `route` gedacht.

`ip` ist ein sehr komplexes Werkzeug. Seine allgemeine Syntax ist `ip options object command`. Sie können mit folgenden Objekten arbeiten:

Verbindung

Dieses Objekt stellt ein Netzwerkgerät dar.

Adresse

Dieses Objekt stellt die IP-Adresse des Geräts dar.

neighbour

Dieses Objekt stellt einen ARP- oder NDISC-Cache-Eintrag dar.

route

Dieses Objekt stellt den Routing-Tabelleneintrag dar.

Regel

Dieses Objekt stellt eine Regel in der Routing-Richtlinien-Datenbank dar.

maddress

Dieses Objekt stellt eine Multicast-Adresse dar.

mroute

Dieses Objekt stellt einen Multicast-Routing-Cache-Eintrag dar.

tunnel

Dieses Objekt stellt einen Tunnel über IP dar.

Wird kein Befehl angegeben, wird der Standardbefehl verwendet. Normalerweise ist das `list`.

Ändern Sie den Gerätestatus mit dem Befehl `ip link set device_name command`. Wenn Sie beispielsweise das Gerät `eth0` deaktivieren möchten, geben Sie `ip link set eth0 down` ein. Um es wieder zu aktivieren, verwenden Sie `ip link set eth0 up`.

Nach dem Aktivieren eines Geräts können Sie es konfigurieren. Verwenden Sie zum Festlegen der IP-Adresse `ip addr add ip_address + dev device_name`. Wenn Sie beispielsweise die Adresse der Schnittstelle `eth0` mit dem standardmäßigen Broadcast (Option `brd`) auf `192.168.12.154/30` einstellen möchten, geben Sie `ip addr add 192.168.12.154/30 brd + dev eth0` ein.

Damit die Verbindung funktioniert, müssen Sie außerdem das Standard-Gateway konfigurieren. Geben Sie `ip route add gateway_ip_address` ein, wenn Sie ein Gateway für Ihr System festlegen möchten. Um eine IP-Adresse in eine andere Adresse zu übersetzen, verwenden Sie `nat: ip route add nat ip_address via other_ip_address`.

Zum Anzeigen aller Geräte verwenden Sie `ip link ls`. Wenn Sie nur die aktiven Schnittstellen abrufen möchten, verwenden Sie `ip link ls up`. Um Schnittstellenstatistiken für ein Gerät zu drucken, geben Sie `ip -s link ls device_name` ein. Um die Adressen Ihrer Geräte anzuzeigen, geben Sie `ip addr` ein. In der Ausgabe von `ip addr` finden Sie auch Informationen zu MAC-Adressen Ihrer Geräte. Wenn Sie alle Routen anzeigen möchten, wählen Sie `ip route show`.

Weitere Informationen zur Verwendung von `ip` erhalten Sie, indem Sie `iphelp` eingeben oder die man-Seite `ip(8)` aufrufen. Die Option `help` ist zudem für alle `ip`-Objekte verfügbar. Wenn Sie beispielsweise Hilfe zu `ipaddr` benötigen, geben Sie `ipaddr help` ein. Suchen Sie die IP-Manualpage in der Datei `/usr/share/doc/packages/iproute2/ip-cref.pdf`.

Testen einer Verbindung mit ping

Der `ping`-Befehl ist das Standardwerkzeug zum Testen, ob eine TCP/IP-Verbindung funktioniert. Er verwendet das ICMP-Protokoll, um ein kleines Datenpaket, das `ECHO_REQUEST`-Datagramm, an den Ziel-Host zu senden. Dabei wird eine sofortige Antwort angefordert. Funktioniert dies, erhalten Sie eine Meldung, die Ihnen `best tigt`, dass die Netzwerkverbindung grunds tzlich funktioniert.

`ping` testet nicht nur die Funktion der Verbindung zwischen zwei Computern, es bietet darüber hinaus grundlegende Informationen zur Qualität der Verbindung. In **Beispiel 14.10**, „Ausgabe des `ping`-Befehls“ (S. 276) sehen Sie ein Beispiel der `ping`-Ausgabe. Die vorletzte Zeile enthält Informationen zur Anzahl der übertragenen Pakete, der verlorenen Pakete und der Gesamtlaufzeit von `ping`.

Als Ziel können Sie einen Hostnamen oder eine IP-Adresse verwenden, z. B. `ping example.com` oder `ping 192.168.3.100`. Das Programm sendet Pakete, bis Sie auf `Strg + C` drücken.

Wenn Sie nur die Funktion der Verbindung überprüfen möchten, können Sie die Anzahl der Pakete durch die Option `-c` beschränken. Wenn die Anzahl beispielsweise auf drei Pakete beschränkt werden soll, geben Sie `ping -c 3 example.com` ein.

Beispiel 14.10 *Ausgabe des ping-Befehls*

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

Das Standardintervall zwischen zwei Paketen beträgt eine Sekunde. Zum Ändern des Intervalls bietet der ping-Befehl die Option `-i`. Wenn beispielsweise das Ping-Intervall auf zehn Sekunden erhöht werden soll, geben Sie `ping -i 10 example.com` ein.

In einem System mit mehreren Netzwerkgeräten ist es manchmal nützlich, wenn der ping-Befehl über eine spezifische Schnittstellenadresse gesendet wird. Verwenden Sie hierfür die Option `-I` mit dem Namen des ausgewählten Geräts. Beispiel: `ping -I wlan1 example.com`.

Weitere Optionen und Informationen zur Verwendung von ping erhalten Sie, indem Sie `ping -h` eingeben oder die man-Seite `ping (8)` aufrufen.

Konfigurieren des Netzwerks mit dem ifconfig-Befehl

`ifconfig` ist ein herkömmliches Werkzeug zur Netzwerkkonfiguration. Im Gegensatz zu `ip`, können Sie diesen Befehl nur für die Schnittstellenkonfiguration verwenden. Das Routing konfigurieren Sie mit `route`.

ANMERKUNG: ifconfig und ip

Das `ifconfig`-Programm ist veraltet. Verwenden Sie stattdessen `ip`.

Ohne Argumente zeigt `ifconfig` den Status der gegenwärtig aktiven Schnittstellen an. Unter **Beispiel 14.11**, „Ausgabe des `ifconfig`-Befehls“ (S. 277) sehen Sie, dass `ifconfig` über eine gut angeordnete, detaillierte Ausgabe verfügt. Die Ausgabe enthält außerdem in der ersten Zeile Informationen zur MAC-Adresse Ihres Geräts, dem Wert von `HWaddr`.

Beispiel 14.11 Ausgabe des `ifconfig`-Befehls

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1    Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 Mb)
```

Weitere Optionen und Informationen zur Verwendung von `ifconfig` erhalten Sie, wenn Sie `ifconfig-h` eingeben oder die `man`-Seite `ifconfig(8)` aufrufen.

Konfigurieren des Routing mit `route`

`route` ist ein Programm zum Ändern der IP-Routing-Tabelle. Sie können damit Ihre Routing-Konfiguration anzeigen und Routen hinzufügen oder entfernen.

ANMERKUNG: route und ip

Das route-Programm ist veraltet. Verwenden Sie stattdessen ip.

route ist vor allem dann nützlich, wenn Sie schnelle und übersichtliche Informationen zu Ihrer Routing-Konfiguration benötigen, um Routing-Probleme zu ermitteln. Sie sehen Ihre aktuelle Routing-Konfiguration unter `route -n` als `root`.

Beispiel 14.12 Ausgabe des route -n-Befehls

```
route -n
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
10.20.0.0        *                255.255.248.0   U        0  0        0 eth0
link-local       *                255.255.0.0     U        0  0        0 eth0
loopback         *                255.0.0.0       U        0  0        0 lo
default          styx.exam.com    0.0.0.0         UG       0  0        0 eth0
```

Weitere Optionen und Informationen zur Verwendung von `route` erhalten Sie, indem Sie `v-h` eingeben oder die man-Seite `route (8)` aufrufen.

14.6.3 Startup-Skripten

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripten, die beim Booten des Computers die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Mehrbenutzer-Runlevel* wechselt. Einige der Skripten sind in [Tabelle 14.9](#), „Einige Start-Skripten für Netzwerkprogramme“ (S. 278) beschrieben.

Tabelle 14.9 Einige Start-Skripten für Netzwerkprogramme

<code>/etc/init.d/network</code>	Dieses Skript übernimmt die Konfiguration der Netzwerkschnittstellen. Wenn der Netzwerkdienst nicht gestartet wurde, werden keine Netzwerkschnittstellen implementiert.
<code>/etc/init.d/xinetd</code>	Startet <code>xinetd</code> . Mit <code>xinetd</code> können Sie Serverdienste auf dem System verfügbar machen. Beispielsweise kann er <code>vsftpd</code> starten, sobald eine FTP-Verbindung initiiert wird.

<code>/etc/init.d/portmap</code>	Startet den Portmapper, der für einen RPC-Server benötigt wird, z. B. für einen NFS-Server.
<code>/etc/init.d/nfsserver</code>	Startet den NFS-Server.
<code>/etc/init.d/postfix</code>	Steuert den postfix-Prozess.
<code>/etc/init.d/ypserv</code>	Startet den NIS-Server.
<code>/etc/init.d/ypbind</code>	Startet den NIS-Client.

14.7 smpppd als Einwählhelfer

Einige Heimanwender besitzen keine gesonderte Leitung für das Internet, sondern wählen sich bei Bedarf ein. Je nach Einwählart (ISDN oder DSL) wird die Verbindung von `ippdd` oder `pppd` gesteuert. Im Prinzip müssen nur diese Programme korrekt gestartet werden, um online zu sein.

Sofern Sie über eine Flatrate verfügen, die bei der Einwahl keine zusätzlichen Kosten verursacht, starten Sie einfach den entsprechenden Daemon. Sie können die Einwählverbindung über ein KDE-Applet oder eine Kommandozeilen-Schnittstelle steuern. Wenn das Internet-Gateway nicht der eigentliche Arbeitscomputer ist, besteht die Möglichkeit, die Einwählverbindung über einen Host im Netzwerk zu steuern.

An dieser Stelle kommt `smpppd` ins Spiel. Der Dienst bietet den Hilfsprogrammen eine einheitliche Schnittstelle, die in zwei Richtungen funktioniert. Zum einen programmiert er den jeweils erforderlichen `pppd` oder `ippdd` und steuert deren Einwählverhalten. Zum anderen stellt er den Benutzerprogrammen verschiedene Provider zur Verfügung und übermittelt Informationen zum aktuellen Status der Verbindung. Da der `smpppd`-Dienst auch über das Netzwerk gesteuert werden kann, eignet er sich für die Steuerung von Einwählverbindungen ins Internet von einer Arbeitsstation in einem privaten Subnetzwerk.

14.7.1 Konfigurieren von smpppd

Die von smpppd bereitgestellten Verbindungen werden automatisch von YaST konfiguriert. Die eigentlichen Einwählprogramme KInternet und cinternet werden ebenfalls vorkonfiguriert. Manuelle Einstellungen sind nur notwendig, wenn Sie zusätzliche Funktionen von smpppd, z. B. die Fernsteuerung, einrichten möchten.

Die Konfigurationsdatei von smpppd ist `/etc/smpppd.conf`. Sie ist so eingestellt, dass standardmäßig keine Fernsteuerung möglich ist. Die wichtigsten Optionen dieser Konfigurationsdatei sind:

`open-inet-socket = yes/no`

Wenn smpppd über das Netzwerk gesteuert werden soll, muss diese Option auf `yes` (ja) eingestellt werden. Der Port, auf dem smpppd lauscht, ist 3185. Wenn dieser Parameter auf `yes` (ja) gesetzt ist, sollten auch die Parameter `bind-address`, `host-range` und `password` entsprechend eingestellt werden.

`bind-address = IP-Adresse`

Wenn ein Host mehrere IP-Adressen hat, können Sie mit dieser Einstellung festlegen, über welche IP-Adresse smpppd Verbindungen akzeptiert. Standard ist die Überwachung an allen Adressen.

`host-range = Anfangs-IPEnd-IP`

Der Parameter `host-range` definiert einen Netzbereich. Hosts, deren IP-Adressen innerhalb dieses Bereichs liegen, wird der Zugriff auf smpppd gewährt. Alle Hosts, die außerhalb dieses Bereichs liegen, werden abgewiesen.

`password = Passwort`

Mit der Vergabe eines Passworts wird der Client-Zugriff auf autorisierte Hosts beschränkt. Da es lediglich ein reines Textpasswort ist, sollte die Sicherheit, die es bietet, nicht überbewertet werden. Wenn kein Passwort vergeben wird, sind alle Clients berechtigt, auf smpppd zuzugreifen.

`slp-register = yes/no`

Mit diesem Parameter kann der smpppd-Dienst per SLP im Netzwerk bekannt gegeben werden.

Weitere Informationen zu smpppd finden Sie in den man-Seiten zu `smpppd(8)` und `smpppd.conf(5)`.

14.7.2 Konfigurieren von KInternet und cinternet für die Fernsteuerung

KInternet und cinternet können zur Steuerung eines lokalen smpppd verwendet werden. cinternet mit Kommandozeilen ist das Gegenstück zum grafischen KInternet. Wenn Sie diese Dienstprogramme zum Einsatz mit einem entfernten smpppd-Dienst vorbereiten möchten, bearbeiten Sie die Konfigurationsdatei `/etc/smpppd-c.conf` manuell oder mithilfe von KInternet. Diese Datei enthält nur vier Optionen:

`sites = Liste der Sites`

Hier weisen Sie die Frontends an, wo sie nach smpppd suchen sollen. Die Frontends testen die Optionen in der hier angegebenen Reihenfolge. Die Option `Lokal` verlangt den Verbindungsaufbau zum lokalen smpppd. Die Option `Gateway` verweist auf ein smpppd am Gateway. Die Option `config-file` gibt an, dass die Verbindung zum smpppd hergestellt werden sollte, der in den Optionen `Server` und `Port` in der Datei `/etc/smpppd-c.conf` angegeben ist. `slp` veranlasst, dass die Front-Ends eine Verbindung zu einem über SLP gefundenen smpppd aufbauen.

`server = Server`

Geben Sie hier den Host an, auf dem smpppd läuft.

`port = Port`

Geben Sie hier den Host an, auf dem smpppd ausgeführt wird.

`password = Passwort`

Geben Sie das Passwort für smpppd ein.

Wenn smpppd aktiv ist, können Sie jetzt versuchen, darauf zuzugreifen, z. B. mit dem Befehl `ccinternet--verbose --interface-list`. Sollten Sie an dieser Stelle Schwierigkeiten haben, finden Sie weitere Informationen in den man-Seiten zu `smpppd-c.conf(5)` und `ccinternet(8)`.

SLP-Dienste im Netzwerk

Das *Service Location Protocol* (SLP) wurde entwickelt, um die Konfiguration vernetzter Clients innerhalb eines lokalen Netzwerks zu vereinfachen. Zur Konfiguration eines Netzwerk-Clients inklusive aller erforderlichen Dienste benötigt der Administrator traditionell detailliertes Wissen über die im Netzwerk verfügbaren Server. SLP teilt allen Clients im lokalen Netzwerk die Verfügbarkeit ausgewählter Dienste mit. Anwendungen mit SLP-Unterstützung können diese Informationen verarbeiten und können automatisch konfiguriert werden.

openSUSE® unterstützt die Installation von mit SLP bereitgestellten Installationsquellen und beinhaltet viele Systemdienste mit integrierter Unterstützung für SLP. YaST und Konqueror verfügen beide über SLP-fähige Frontends. Nutzen Sie SLP, um vernetzten Clients zentrale Funktionen wie Installationsserver, YOU-Server, Dateiserver oder Druckserver auf Ihrem System zur Verfügung zu stellen.

WICHTIG: SLP-Unterstützung in openSUSE

Dienste, die SLP-Unterstützung bieten, sind u. a. cupsd, rsyncd, ypserv, openldap2, openwbem (CIM), ksysguardd, saned, kdm vnc login, smpppd, rpasswd, postfix und sshd (über fish).

15.1 Installation

Nur ein SLP-Client und slptools werden standardmäßig installiert. Wenn Sie Dienste über SLP bereitstellen möchten, installieren Sie das Paket `openslp-server`. Zur Installation des Pakets starten Sie YaST und wählen Sie *Software > Software-Manage-*

ment aus. Wählen Sie dann *Filter > Schemata* und klicken Sie auf *Verschiedene Server*. Wählen Sie `openslp-server`. Bestätigen Sie die Installation der erforderlichen Pakete, um den Installationsvorgang abzuschließen.

15.2 SLP aktivieren

`slpd` muss auf Ihrem System ausgeführt werden, damit Dienste mit SLP angeboten werden können. Für das bloße Abfragen von Diensten ist ein Start dieses Daemons nicht erforderlich. Wie die meisten Systemdienste unter openSUSE wird der `slpd`-Dämon über ein separates `init`-Skript gesteuert. Standardmäßig ist der Daemon inaktiv. Wenn Sie ihn für die Dauer einer Sitzung aktivieren möchten, führen Sie `rcslpd start` als `root` aus, um ihn zu starten. Mit dem Befehl `rcslpd stop` können Sie ihn stoppen. Mit `restart` oder `status` lösen Sie einen Neustart oder eine Statusabfrage aus. Wenn `slpd` standardmäßig aktiv sein soll, aktivieren Sie `slpd` in YaST *System > Systemdienste (Runlevel)* oder führen Sie den Befehl `insserv slpd` einmalig als `root` aus. Dadurch wird `slpd` automatisch zu den Diensten hinzugefügt, die beim Booten eines Systems gestartet werden.

15.3 SLP-Frontends in openSUSE

Verwenden Sie ein SLP-Frontend, um in Ihrem Netzwerk von SLP bereitgestellte Dienste zu finden. openSUSE enthält mehrere Frontends:

`slptool`

`slptool` ist ein einfaches Kommandozeilenprogramm, mit dem proprietäre Dienste oder SLP-Anfragen im Netzwerk bekannt gegeben werden können. Mit `slptool --help` werden alle verfügbaren Optionen und Funktionen aufgelistet. `slptool` kann auch aus Skripten aufgerufen werden, die SLP-Informationen verarbeiten. Um beispielsweise alle Netzwerk-Zeitserver zu finden, die sich selbst im aktuellen Netzwerk ankündigen, führen Sie folgendes Kommando aus:

```
slptool findsrvs service:ntp
```

Konqueror

Als Netzwerkbrowser kann Konqueror alle im lokalen Netz verfügbaren SLP-Dienste unter `slp:/` anzeigen. Klicken Sie auf die Symbole im Hauptfenster, um ausführlichere Informationen zum entsprechenden Dienst zu erhalten. Wenn Sie

Konqueror mit `service : /` aufrufen, können Sie mit einem Klick auf das entsprechende Symbol im Browserfenster eine Verbindung zum ausgewählten Dienst aufbauen.

15.4 Installation über SLP

Wenn Sie einen Installationsserver mit openSUSE-Installationsmedien in Ihrem Netzwerk anbieten, kann dieser mit SLP registriert werden. Weitere Informationen finden Sie in [Abschnitt 1.2.1, „Einrichten eines Installationservers mithilfe von YaST“](#) (S. 14). Wenn die SLP-Installation ausgewählt wurde, startet `linuxrc` eine SLP-Anfrage, nachdem das System vom ausgewählten Startmedium gestartet wurde, und zeigt die gefundenen Quellen an.

15.5 Bereitstellen von Diensten über SLP

Viele Anwendungen in openSUSE verfügen durch die `libslp`-Bibliothek bereits über eine integrierte SLP-Unterstützung. Falls ein Dienst ohne SLP-Unterstützung kompiliert wurde, können Sie ihn mit einer der folgenden Methoden per SLP verfügbar machen:

Statische Registrierung über `/etc/slp.reg.d`

Legen Sie für jeden neuen Dienst eine separate Registrierungsdatei an. Dies ist ein Beispiel einer solchen Datei für die Registrierung eines Scannerdiensts:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

Die wichtigste Zeile dieser Datei ist die *Dienst-URL*, die mit `service :` beginnt. Sie enthält den Dienstyp (`scanner.sane`) und die Adresse, unter der der Dienst auf dem Server verfügbar ist. `$HOSTNAME` wird automatisch durch den vollständigen Hostnamen ersetzt. Abgetrennt durch einen Doppelpunkt folgt nun der Name des TCP-Ports, auf dem der entsprechende Dienst gefunden werden kann. Geben Sie nun die Sprache an, in der der Dienst angekündigt werden soll, und die Gültig-

keitsdauer der Registrierung in Sekunden. Diese Angaben müssen durch Kommas von der Dienst-URL getrennt werden. Wählen Sie für die Registrierungsdauer einen Wert zwischen 0 und 65535. 0 verhindert die Registrierung. Mit 65535 werden alle Einschränkungen aufgehoben.

Die Registrierungsdatei enthält außerdem die beiden Variablen `watch-port-tcp` und `description.watch-port-tcp` koppelt die SLP-Dienstankündigung daran, ob der entsprechende Dienst aktiv ist, indem `slpd` den Status des Diensts überprüft. Die zweite Variable enthält eine genauere Beschreibung des Diensts, die in den entsprechenden Browsern angezeigt wird.

Statische Registrierung über `/etc/slp.reg`

Der einzige Unterschied zum Verfahren mit `/etc/slp.reg.d` ist die Gruppierung aller Dienste innerhalb einer zentralen Datei.

Dynamische Registrierung über `slptool`

Verwenden Sie zur SLP-Registrierung eines Diensts aus proprietären Skripten das Kommandozeilen-Frontend `slptool`.

15.6 Weiterführende Informationen

Weitere Informationen zu SLP finden Sie in folgenden Quellen:

RFC 2608, 2609, 2610

RFC 2608 befasst sich mit der Definition von SLP im Allgemeinen. RFC 2609 geht näher auf die Syntax der verwendeten Dienst-URLs ein und RFC 2610 thematisiert DHCP über SLP.

<http://www.openslp.org/>

Die Homepage des OpenSLP-Projekts.

`/usr/share/doc/packages/openslp`

Dieses Verzeichnis enthält alle verfügbaren Dokumentationen zu SLP, einschließlich einer `README.SuSE`-Datei mit Details zu openSUSE, den oben genannten RFCs und zwei einleitenden HTML-Dokumenten. Programmierer, die SLP-Funktionen verwenden möchten, sollten das Paket `openslp-devel` installieren und im darin enthaltenen *Programmers Guide* nachschlagen.

Domain Name System (DNS)

DNS (Domain Name System) ist zur Auflösung der Domänen- und Hostnamen in IP-Adressen erforderlich. Auf diese Weise wird die IP-Adresse 192.168.2.100 beispielsweise dem Hostnamen `jupiter` zugewiesen. Bevor Sie Ihren eigenen Namensserver einrichten, sollten Sie die allgemeinen Informationen zu DNS in [Abschnitt 14.3](#), „Namensauflösung“ (S. 241) lesen. Die folgenden Konfigurationsbeispiele beziehen sich auf BIND.

16.1 DNS-Terminologie

Zone

Der Domänen-Namespace wird in Regionen, so genannte Zonen, unterteilt. So ist beispielsweise `example.com` der Bereich oder die Zone `example` der Domäne `com`.

DNS-Server

Der DNS-Server ist ein Server, auf dem der Name und die IP-Informationen für eine Domäne gespeichert sind. Sie können einen primären DNS-Server für die Masterzone, einen sekundären Server für die Slave-Zone oder einen Slave-Server ohne jede Zone für das Caching besitzen.

DNS-Server der Masterzone

Die Masterzone beinhaltet alle Hosts aus Ihrem Netzwerk und der DNS-Server der Masterzone speichert die aktuellen Einträge für alle Hosts in Ihrer Domäne.

DNS-Server der Slave-Zone

Eine Slave-Zone ist eine Kopie der Masterzone. Der DNS-Server der Slave-Zone erhält seine Zonendaten mithilfe von Zonentransfers von seinem Master-server. Der DNS-Server der Slave-Zone antwortet autorisiert für die Zone, solange er über gültige (nicht abgelaufene) Zonendaten verfügt. Wenn der Slave keine neue Kopie der Zonendaten erhält, antwortet er nicht mehr für die Zone.

Forwarder

Forwarders sind DNS-Server, an die der DNS-Server Abfragen sendet, die er nicht bearbeiten kann.

Datensatz

Der Eintrag besteht aus Informationen zu Namen und IP-Adresse. Die unterstützten Einträge und ihre Syntax sind in der BIND-Dokumentation beschrieben. Einige spezielle Einträge sind beispielsweise:

NS-Eintrag

Ein NS-Eintrag informiert die Namenserver darüber, welche Computer für eine bestimmte Domänenzone zuständig sind.

MX-Eintrag

Die MX (Mailaustausch)-Einträge beschreiben die Computer, die für die Weiterleitung von Mail über das Internet kontaktiert werden sollen.

SOA-Eintrag

Der SOA (Start of Authority)-Eintrag ist der erste Eintrag in einer Zonendatei. Der SOA-Eintrag wird bei der Synchronisierung von Daten zwischen mehreren Computern über DNS verwendet.

16.2 Installation

Zur Installation eines DNS-Servers starten Sie YaST und wählen Sie *Software > Software-Management* aus. Wählen Sie *Filter > Schemata* und schließlich *DHCP- und DNS-Server* aus. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

16.3 Konfiguration mit YaST

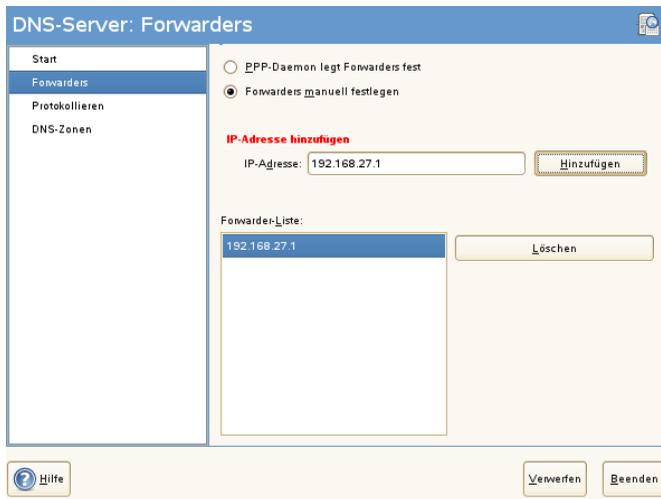
Mit dem DNS-Modul von YaST können Sie einen DNS-Server für Ihr lokales Netzwerk konfigurieren. Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Nach Abschluss der anfänglichen Konfiguration ist eine grundlegende Serverkonfiguration verfügbar, die für einfache Szenarien ausreichend ist. Komplexere Konfigurationsaufgaben können im Expertenmodus ausgeführt werden.

16.3.1 Assistentenkonfiguration

Der Assistent besteht aus drei Schritten bzw. Dialogfeldern. An den entsprechenden Stellen in den Dialogfeldern haben Sie die Möglichkeit, in den Expertenkonfigurationsmodus zu wechseln.

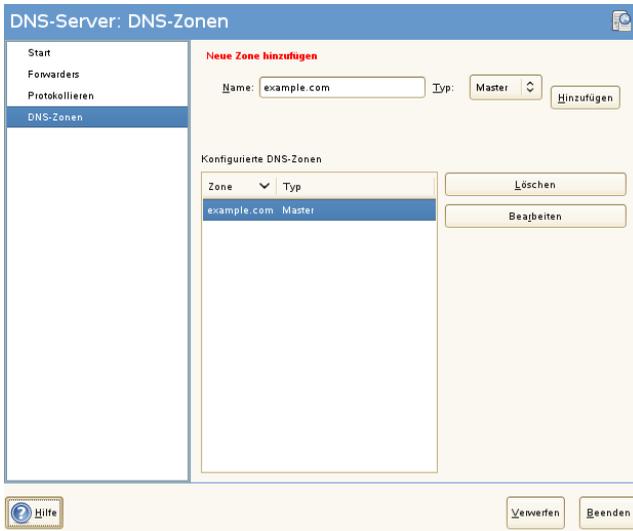
- 1 Wenn Sie das Modul zum ersten Mal starten, wird das Dialogfeld *Forwarder-Einstellungen* (siehe **Abbildung 16.1**, „DNS-Server-Installation: Forwarder-Einstellungen“ (S. 290)) geöffnet. Legen Sie hier fest, ob der PPP-Daemon eine Liste von Forwarders bei der Einwahl über DSL oder ISDN eine Liste von Forwarders bereitstellen soll (*PPP-Daemon legt Forwarders fest*) oder ob Sie Ihre eigene Liste angeben möchten (*Forwarders manuell festlegen*).

Abbildung 16.1 DNS-Server-Installation: Forwarder-Einstellungen



- Das Dialogfeld *DNS-Zonen* besteht aus mehreren Teilen und ist für die Verwaltung von Zonendateien zuständig, wie in [Abschnitt 16.6, „Zonendateien“](#) (S. 304) beschrieben. Bei einer neuen Zone müssen Sie unter *Name der Zone* einen Namen angeben. Um eine Reverse Zone hinzuzufügen, muss der Name auf `.in-addr.arpa` enden. Wählen Sie schließlich den *Zonentyp* (Master oder Slave) aus. Weitere Informationen hierzu finden Sie unter [Abbildung 16.2, „DNS-Server-Installation: DNS-Zonen“](#) (S. 291). Klicken Sie auf *Zone bearbeiten*, um andere Einstellungen für eine bestehende Zone zu konfigurieren. Zum Entfernen einer Zone klicken Sie auf *Zone löschen*.

Abbildung 16.2 DNS-Server-Installation: DNS-Zonen



- 3 Im letzten Dialogfeld können Sie den DNS-Port in der Firewall öffnen, indem Sie auf *Firewall-Port öffnen* klicken. Legen Sie dann fest, ob der DNS-Server gestartet werden soll (*Ein* oder *Aus*). Außerdem können Sie die LDAP-Unterstützung aktivieren. Weitere Informationen hierzu finden Sie unter **Abbildung 16.3**, „DNS-Server-Installation: Wizard beenden“ (S. 292).

Abbildung 16.3 DNS-Server-Installation: Wizard beenden



16.3.2 Konfiguration für Experten

Nach dem Starten des Moduls öffnet YaST ein Fenster, in dem mehrere Konfigurationsoptionen angezeigt werden. Nach Abschluss dieses Fensters steht eine DNS-Server-Konfiguration mit Grundfunktionen zur Verfügung:

Starten des DNS-Servers

Legen Sie unter *Service starten* fest, ob der DNS-Server beim Booten des Systems oder manuell gestartet werden soll. Um den DNS-Server sofort zu starten, wählen Sie *DNS-Server nun starten*. Um den DNS-Server anzuhalten, wählen Sie *DNS-Server nun anhalten*. Zum Speichern der aktuellen Einstellungen wählen Sie *Einstellungen speichern und DNS-Server nun neu starten*. Sie können den DNS-Anschluss in der Firewall mit *Firewall-Port öffnen* öffnen und die Firewall-Einstellungen mit *Firewall-Details* bearbeiten.

Wenn Sie *LDAP-Unterstützung aktiv* wählen, werden die Zone-Dateien von einer LDAP-Datenbank verwaltet. Alle Änderungen an Zonendaten, die in der LDAP-Datenbank gespeichert werden, werden vom DNS-Server gleich nach dem Neustart erfasst oder er wird aufgefordert, seine Konfiguration neu zu laden.

DNS-Server: Grundlegende Optionen

In diesem Abschnitt werden grundlegende Serveroptionen festgelegt. Wählen Sie im Menü *Option* das gewünschte Element und geben Sie dann den Wert im entsprechenden Eintragsfeld an. Nehmen Sie den neuen Eintrag auf, indem Sie auf *Hinzufügen* klicken.

Protokollierung

Um festzulegen, was und wie der DNS-Server protokollieren soll, wählen Sie *Protokollieren* aus. Geben Sie unter *Protokolltyp* an, wohin der DNS-Server die Protokolldaten schreiben soll. Verwenden Sie die systemweite Protokolldatei `/var/log/messages`, indem Sie *Systemprotokoll* auswählen oder geben Sie eine andere Datei an, indem Sie *Datei* auswählen. In letzterem Fall müssen Sie außerdem einen Namen, die maximale Dateigröße in Megabyte und die Anzahl der zu speichernden Versionen von Protokolldateien angeben.

Weitere Optionen sind unter *Zusätzliches Protokollieren* verfügbar. Durch Aktivieren von *Alle DNS-Abfragen protokollieren* wird *jede* Abfrage protokolliert. In diesem Fall kann die Protokolldatei extrem groß werden. Daher sollte diese Option nur zur Fehlersuche aktiviert werden. Um den Datenverkehr zu protokollieren, der während Zonenaktualisierungen zwischen dem DHCP- und dem DNS-Server stattfindet, aktivieren Sie *Zonen-Updates protokollieren*. Um den Datenverkehr während eines Zonentransfers von Master zu Slave zu protokollieren, aktivieren Sie *Zonen-Transfer protokollieren*. Weitere Informationen hierzu finden Sie unter [Abbildung 16.4, „DNS-Server: Protokollieren“](#) (S. 294).

Abbildung 16.4 DNS-Server: Protokollieren



Verwenden von ACLs

In diesem Fenster legen Sie ACLs (Access Control Lists = Zugriffssteuerungslisten) fest, mit denen Sie den Zugriff einschränken. Nach der Eingabe eines eindeutigen Namens unter *Name* geben Sie unter *Wert* eine IP-Adresse (mit oder ohne Netzmaske) wie folgt an:

```
{ 10.10/16; }
```

Die Syntax der Konfigurationsdatei erfordert, dass die Adresse mit einem Strichpunkt endet und in geschwungenen Klammern steht.

TSIG-Schlüssel

Der Hauptzweck von TSIG-Schlüsseln (Transaction Signatures = Transaktionssignaturen) ist die Sicherung der Kommunikation zwischen DHCP- und DNS-Servern. Diese werden unter **Abschnitt 16.8, „Sichere Transaktionen“** (S. 309) beschrieben.

Zum Erstellen eines TSIG-Schlüssels geben Sie einen eindeutigen Namen im Feld mit der Beschriftung *Schlüssel-ID* ein und geben die Datei an, in der der Schlüssel gespeichert werden soll (*Dateiname*). Bestätigen Sie Ihre Einstellung mit *Hinzufügen*.

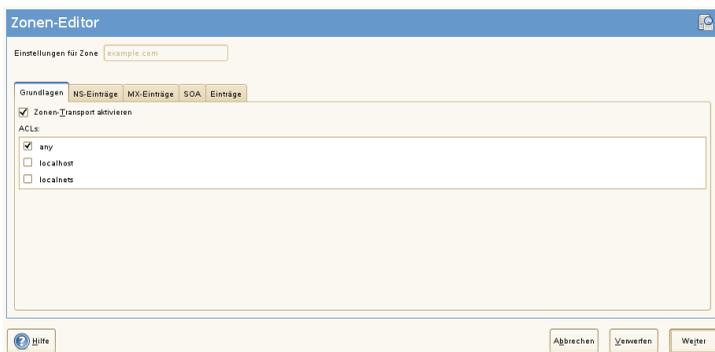
Wenn Sie einen vorher erstellten Schlüssel verwenden möchten, lassen Sie das Feld *Schlüssel-ID* leer und wählen die Datei, in der der gewünschten Schlüssel gespeichert wurde unter *Dateiname*. Dann bestätigen Sie die Auswahl mit *Hinzufügen*.

Hinzufügen einer Slave-Zone

Wenn Sie eine Slave-Zone hinzufügen möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Slave* aus, geben Sie den Namen der neuen Zone ein und klicken Sie auf *Hinzufügen*.

Geben Sie im *Zonen-Editor* unter *IP des Master DNS-Servers* den Master an, von dem der Slave die Daten abrufen soll. Um den Zugriff auf den Server zu beschränken, wählen Sie eine der ACLs aus der Liste aus. Weitere Informationen hierzu finden Sie unter [Abbildung 16.5](#), „*DNS-Server: Slave-Zonen-Editor*“ (S. 295).

Abbildung 16.5 *DNS-Server: Slave-Zonen-Editor*



Hinzufügen einer Masterzone

Wenn Sie eine Masterzone hinzufügen möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Master* aus, geben Sie den Namen der neuen Zone ein und klicken Sie auf *Hinzufügen*.

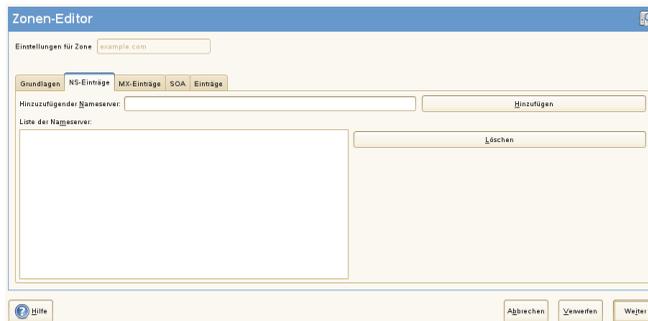
Bearbeiten einer Masterzone

Wenn Sie eine Masterzone bearbeiten möchten, klicken Sie auf *DNS-Zonen*, wählen Sie die Masterzone in der Tabelle aus und klicken Sie auf *Bearbeiten*. Dieses Dialogfeld besteht aus mehreren Seiten: *Grundlagen* (die zuerst geöffnete Seite), *DNS-Einträge*, *MX-Einträge*, *SOA* und *Einträge*.

Zonen-Editor (NS-Einträge)

In diesem Dialogfeld können Sie alternative Namensserver für die angegebenen Zonen definieren. Vergewissern Sie sich, dass Ihr eigener Namensserver in der Liste enthalten ist. Um einen Eintrag hinzuzufügen, geben Sie seinen Namen unter *Hinzuzufügender Namensserver* ein und bestätigen Sie den Vorgang anschließend mit *Hinzufügen*. Weitere Informationen hierzu finden Sie unter **Abbildung 16.6**, „DNS-Server: Zonen-Editor (DNS-Einträge)“ (S. 296).

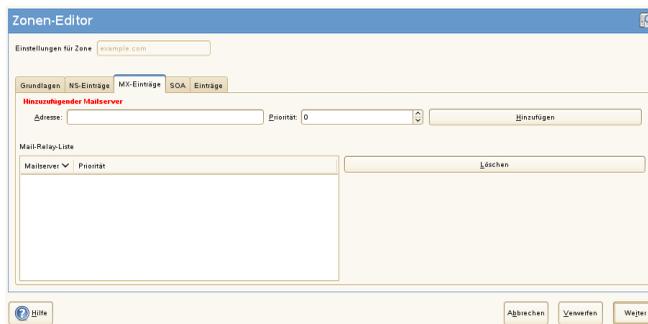
Abbildung 16.6 DNS-Server: Zonen-Editor (DNS-Einträge)



Zonen-Editor (MX-Einträge)

Um einen Mailserver für die aktuelle Zone zur bestehenden Liste hinzuzufügen, geben Sie die entsprechende Adresse und den entsprechenden Prioritätswert ein. Bestätigen Sie den Vorgang anschließend durch Auswahl von *Hinzufügen*. Weitere Informationen hierzu finden Sie unter **Abbildung 16.7**, „DNS-Server: Zonen-Editor (MX-Einträge)“ (S. 296).

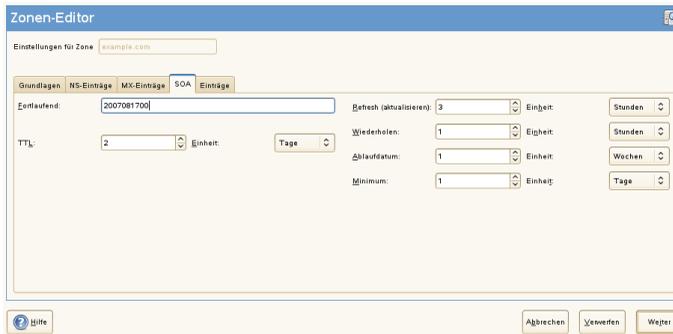
Abbildung 16.7 DNS-Server: Zonen-Editor (MX-Einträge)



Zonen-Editor (SOA)

Auf dieser Seite können Sie SOA (Start of Authority)-Einträge erstellen. Eine Erklärung der einzelnen Optionen finden Sie in [Beispiel 16.6](#), „Datei `/var/lib/named/example.com.zone`“ (S. 305).

Abbildung 16.8 DNS-Server: Zonen-Editor (SOA)



Zonen-Editor (Einträge)

In diesem Dialogfeld wird die Namensauflösung verwaltet. Geben Sie unter *Eintragsschlüssel* den Hostnamen an und wählen Sie anschließend den Typ aus. *A-Record* steht für den Haupteintrag. Der Wert hierfür sollte eine IP-Adresse sein. *CNAME* ist ein Alias. Verwenden Sie die Typen *NS* und *MX* für detaillierte oder partielle Einträge, mit denen die Informationen aus den Registerkarten *NS-Einträge* und *MX-Einträge* erweitert werden. Diese drei Typen werden in einen bestehenden A-Eintrag aufgelöst. *PTR* dient für Reverse Zones. Es handelt sich um das Gegenteil eines A-Eintrags.

16.4 Starten des Namensservers BIND

Bei openSUSE®-Systemen ist der Namensserver BIND (*Berkeley Internet Name Domain*) vorkonfiguriert, sodass er problemlos unmittelbar nach der Installation gestartet werden kann. Wenn Sie bereits über eine funktionierende Internetverbindung verfügen und 127.0.0.1 als Namenserveradresse für localhost in `/etc/resolv.conf` eingegeben haben, verfügen Sie normalerweise bereits über eine funktionierende Namensauflösung, ohne dass Ihnen der DNS des Anbieters bekannt sein muss. BIND führt die Namensauflösung über den Root-Namensserver durch. Dies ist ein wesentlich langsamerer Prozess. Normalerweise sollte der DNS des Anbieters zusammen mit der

zugehörigen IP-Adresse in die Konfigurationsdatei `/etc/named.conf` unter `forwarders` eingegeben werden, um eine effektive und sichere Namensauflösung zu gewährleisten. Wenn dies so weit funktioniert, wird der Namenserver als reiner *Nur-Cache*-Namenserver ausgeführt. Nur wenn Sie seine eigenen Zonen konfigurieren, wird er ein richtiger DNS. Ein einfaches Beispiel hierfür ist in der Dokumentation unter `/usr/share/doc/packages/bind/config` enthalten.

TIPP: Automatische Anpassung der Namenserverinformationen

Je nach Typ der Internet- bzw. Netzwerkverbindung können die Namenserverinformationen automatisch an die aktuellen Bedingungen angepasst werden. Setzen Sie hierfür die Variable `MODIFY_NAMED_CONF_DYNAMICALY` in der Datei `/etc/sysconfig/network/config` auf `yes`.

Richten Sie jedoch noch keine offiziellen Domänen ein. Warten Sie, bis Ihnen eine von der verantwortlichen Institution zugewiesen wird. Selbst wenn Sie eine eigene Domäne besitzen und diese vom Anbieter verwaltet wird, sollten Sie sie besser nicht verwenden, da BIND ansonsten keine Anforderungen für diese Domäne weiterleitet. Beispielsweise könnte in diesem Fall für diese Domäne der Zugriff auf den Webserver beim Anbieter nicht möglich sein.

Geben Sie zum Starten des Namensservers den Befehl `rndcstart` als `root` ein. Falls rechts in grüner Schrift „done“ angezeigt wird, wurde `named`, wie der Namenserverprozess hier genannt wird, erfolgreich gestartet. Testen Sie den Namenserver umgehend auf dem lokalen System mit den Programmen `host` oder `dig`. Sie sollten `localhost` als Standardserver mit der Adresse `127.0.0.1` zurückgeben. Ist dies nicht der Fall, enthält `/etc/resolv.conf` einen falschen Namenservereintrag oder die Datei ist nicht vorhanden. Geben Sie beim ersten Test `host 127.0.0.1` ein. Dieser Eintrag sollte immer funktionieren. Wenn Sie eine Fehlermeldung erhalten, prüfen Sie mit `rndcstatus`, ob der Server tatsächlich ausgeführt wird. Wenn der Namenserver sich nicht starten lässt oder unerwartetes Verhalten zeigt, finden Sie die Ursache normalerweise in der Protokolldatei `/var/log/messages`.

Um den Namenserver des Anbieters oder einen bereits in Ihrem Netzwerk ausgeführten Server als Forwarder zu verwenden, geben Sie die entsprechende IP-Adresse(n) im Abschnitt `options` unter `forwarders` ein. Bei den Adressen in **Beispiel 16.1**, „Weiterleitungsoptionen in `named.conf`“ (S. 299) handelt es sich lediglich um Beispiele. Passen Sie diese Einträge an Ihr eigenes Setup an.

Beispiel 16.1 Weiterleitungsoptionen in *named.conf*

```
options {
    directory "/var/lib/named";
    forwarders { 10.11.12.13; 10.11.12.14; };
    listen-on { 127.0.0.1; 192.168.1.116; };
    allow-query { 127/8; 192.168/16 };
    notify no;
};
```

Auf den Eintrag `options` folgen Einträge für die Zone, `localhost` und `0.0.127.in-addr.arpa`. Der Eintrag `type hint` unter „`„` sollte immer vorhanden sein. Die entsprechenden Dateien müssen nicht bearbeitet werden und sollten so funktionieren, wie sie sind. Achten Sie außerdem darauf, dass jeder Eintrag mit einem „`„` abgeschlossen ist und dass sich die geschweiften Klammern an der richtigen Position befinden. Wenn Sie die Konfigurationsdatei `/etc/named.conf` oder die Zonendateien geändert haben, teilen Sie BIND mit, die Datei erneut zu lesen. Verwenden Sie hierfür den Befehl `rndc reload`. Sie erzielen dasselbe Ergebnis, wenn Sie den Namensserver mit `rndc restart` stoppen und erneut starten. Sie können den Server durch Eingabe von `rndc stop` jederzeit stoppen.

16.5 Die Konfigurationsdatei /etc/dhcpd.conf

Alle Einstellungen für den BIND-Namensserver selbst sind in der Datei `/etc/named.conf` gespeichert. Die Zonendaten für die zu bearbeitenden Domänen, die aus Hostnamen, IP-Adressen usw. bestehen, sind jedoch in gesonderten Dateien im Verzeichnis `/var/lib/named` gespeichert. Einzelheiten hierzu werden weiter unten beschrieben.

`/etc/named.conf` lässt sich grob in zwei Bereiche untergliedern. Der eine ist der Abschnitt `options` für allgemeine Einstellungen und der zweite besteht aus `zone`-Einträgen für die einzelnen Domänen. Der Abschnitt `logging` und die Einträge unter `acl` (access control list, Zugriffssteuerungsliste) sind optional. Kommentarzeilen beginnen mit `#` oder mit `//`. Eine Minimalversion von `/etc/named.conf` finden Sie in [Beispiel 16.2](#), „Eine Grundversion von `/etc/named.conf`“ (S. 300).

Beispiel 16.2 Eine Grundversion von `/etc/named.conf`

```
options {
    directory "/var/lib/named";
    forwarders { 10.0.0.1; };
    notify no;
};

zone "localhost" in {
    type master;
    file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};

zone "." in {
    type hint;
    file "root.hint";
};
```

16.5.1 Wichtige Konfigurationsoptionen

`directory "Dateiname";`

Gibt das Verzeichnis an, in dem BIND die Dateien mit den Zonendaten finden kann. In der Regel ist dies `/var/lib/named`.

`forwarders \{ ip-adresse; \};`

Gibt die Namenserver (zumeist des Anbieters) an, an die DNS-Anforderungen weitergeleitet werden sollen, wenn sie nicht direkt aufgelöst werden können.

Ersetzen Sie *IP-Adresse* durch eine IP-Adresse wie `192.168.1.116`.

`forward first;`

Führt dazu, dass DNS-Anforderungen weitergeleitet werden, bevor versucht wird, sie über die Root-Namenserver aufzulösen. Anstatt `forward first` kann `forward only` verwendet werden. Damit werden alle Anforderungen weitergeleitet, ohne dass sie an die Root-Namenserver gesendet werden. Dies ist bei Firewall-Konfigurationen sinnvoll.

`listen-on port 53 \{ 127.0.0.1; IP-Adresse; \};`

Informiert BIND darüber, an welchen Netzwerkschnittstellen und Ports Client-Abfragen akzeptiert werden sollen. `port 53` muss nicht explizit angegeben wer-

den, da 53 der Standardport ist. Geben Sie `127.0.0.1` ein, um Anforderungen vom lokalen Host zuzulassen. Wenn Sie diesen Eintrag ganz auslassen, werden standardmäßig alle Schnittstellen verwendet.

`listen-on-v6 port 53 {any;};`

Informiert BIND darüber, welcher Port auf IPv6-Client-Anforderungen überwacht werden soll. Die einzige Alternative zu `any` ist `none`. Bei IPv6 akzeptiert der Server nur Wildcard-Adressen.

`query-source address * port 53;`

Dieser Eintrag ist erforderlich, wenn eine Firewall ausgehende DNS-Anforderungen blockiert. Dadurch wird BIND angewiesen, Anforderungen extern von Port 53 und nicht von einem der Ports mit den hohen Nummern über 1024 aufzugeben.

`query-source-v6 address * port 53;`

Informiert BIND darüber, welcher Port für IPv6-Abfragen verwendet werden soll.

`allow-query \{ 127.0.0.1; net;};`

Definiert die Netzwerke, von denen aus Clients DNS-Anforderungen aufgeben können. Ersetzen Sie *Netz* durch Adressinformationen wie `192.168.2.0/24`. Der Wert `/24` am Ende ist ein abgekürzter Ausdruck für die Netzmaske, hier `255.255.255.0`.

`allow-transfer ! *;`

Legt fest, welche Hosts Zonentransfers anfordern können. Im vorliegenden Beispiel werden solche Anforderungen mit `! *` vollständig verweigert. Ohne diesen Eintrag können Zonentransfer ohne Einschränkungen von jedem beliebigen Ort angefordert werden.

`statistics-interval 0;`

Ohne diesen Eintrag generiert BIND in der Datei `/var/log/messages` pro Stunde mehrere Zeilen mit statistischen Informationen. Setzen Sie diesen Wert auf `"0"`, um diese Statistiken vollständig zu unterdrücken, oder legen Sie ein Zeitintervall in Minuten fest.

`cleaning-interval 720;`

Diese Option legt fest, in welchen Zeitabständen BIND den Cache leert. Jedes Mal, wenn dies geschieht, wird ein Eintrag in `/var/log/messages` ausgelöst. Die verwendete Einheit für die Zeitangabe ist Minuten. Der Standardwert ist 60 Minuten.

interface-interval 0;

BIND durchsucht die Netzwerkschnittstellen regelmäßig nach neuen oder nicht vorhandenen Schnittstellen. Wenn dieser Wert auf 0 gesetzt ist, wird dieser Vorgang nicht durchgeführt und BIND überwacht nur die beim Start erkannten Schnittstellen. Anderenfalls wird das Zeitintervall in Minuten angegeben. Der Standardwert ist 60 Minuten.

notify no;

no verhindert, dass anderen Namenserver informiert werden, wenn Änderungen an den Zonendaten vorgenommen werden oder wenn der Namenserver neu gestartet wird.

16.5.2 Protokollierung

Der Umfang, die Art und Weise und der Ort der Protokollierung kann in BIND extensiv konfiguriert werden. Normalerweise sollten die Standardeinstellungen ausreichen. In [Beispiel 16.3](#), „Eintrag zur Deaktivierung der Protokollierung“ (S. 302) sehen Sie die einfachste Form eines solchen Eintrags, bei dem jegliche Protokollierung unterdrückt wird.

Beispiel 16.3 Eintrag zur Deaktivierung der Protokollierung

```
logging {  
    category default { null; };  
};
```

16.5.3 Zoneneinträge

Beispiel 16.4 Zoneneintrag für "example.com"

```
zone "example.com" in {  
    type master;  
    file "example.com.zone";  
    notify no;  
};
```

Geben Sie nach `zone` den Namen der zu verwaltenden Domäne (`example.com`) an, gefolgt von `in` und einem Block relevanter Optionen in geschweiften Klammern, wie in [Beispiel 16.4](#), „Zoneneintrag für "example.com"“ (S. 302) gezeigt. Um eine *Slave-Zone* zu definieren, ändern Sie den Wert von `type` in `slave` und geben Sie einen Namenserver an, der diese Zone als `master` verwaltet (dieser kann wiederum ein

Slave eines anderen Masters sein), wie in [Beispiel 16.5](#), „Zoneneintrag für `example.net`“ (S. 303) gezeigt.

Beispiel 16.5 Zoneneintrag für `example.net`

```
zone "example.net" in {
    type slave;
    file "slave/example.net.zone";
    masters { 10.0.0.1; };
};
```

Zonenooptionen:

`type master;`

Durch die Angabe `master` wird BIND darüber informiert, dass der lokale Namensserver für die Zone zuständig ist. Dies setzt voraus, dass eine Zonendatei im richtigen Format erstellt wurde.

`type slave;`

Diese Zone wird von einem anderen Namensserver übertragen. Sie muss zusammen mit `masters` verwendet werden.

`type hint;`

Die Zone `.` vom Typ `hint` wird verwendet, um den root-Namensserver festzulegen. Diese Zonendefinition kann unverändert beibehalten werden.

Datei `example.com.zone` oder Datei `„slave/example.net.zone“`;

In diesem Eintrag wird die Datei angegeben, in der sich die Zonendaten für die Domäne befinden. Diese Datei ist für einen Slave nicht erforderlich, da die betreffenden Daten von einem anderen Namensserver abgerufen werden. Um zwischen Master- und Slave-Dateien zu unterscheiden, verwenden Sie das Verzeichnis `slave` für die Slave-Dateien.

`masters { server-ip-adresse; };`

Dieser Eintrag ist nur für Slave-Zonen erforderlich. Er gibt an, von welchem Namensserver die Zonendatei übertragen werden soll.

`allow-update {! *; };`

Mit dieser Option wird der externe Schreibzugriff gesteuert, der Clients das Anlegen von DNS-Einträgen gestattet. Aus Sicherheitsgründen wird davon abgeraten, den Clients Schreibzugriff zu gewähren. Ohne diesen Eintrag sind überhaupt keine

Zonenaktualisierungen zulässig. Der oben stehende Eintrag hat dieselbe Wirkung, da ! * solche Aktivitäten effektiv unterbindet.

16.6 Zonendateien

Zwei Arten von Zonendateien sind erforderlich. Eine Art ordnet IP-Adressen Hostnamen zu, die andere stellt Hostnamen für IP-Adressen bereit.

TIPP: Verwenden des Punktes in Zonendateien

Die `.` hat eine wichtige Bedeutung in den Zonendateien. Wenn Hostnamen ohne `.` am Ende angegeben werden, wird die Zone angefügt. Vollständige Hostnamen, die mit einem vollständigen Domännennamen angegeben werden, müssen mit `.` abgeschlossen werden, um zu verhindern, dass die Domäne ein weiteres Mal angefügt wird. Ein fehlender oder falsch platzierter Punkt ist wahrscheinlich die häufigste Ursache von Fehlern bei der Namenserverkonfiguration.

Der erste zu betrachtende Fall ist die Zonendatei `example.com.zone`, die für die Domäne `example.com` zuständig ist (siehe [Beispiel 16.6, „Datei /var/lib/named/example.com.zone“](#) (S. 305)).

Beispiel 16.6 Datei `/var/lib/named/example.com.zone`

```
1. $TTL 2D
2. example.com. IN SOA      dns root.example.com. (
3.      2003072441 ; serial
4.      1D        ; refresh
5.      2H        ; retry
6.      1W        ; expiry
7.      2D )      ; minimum
8.
9.      IN NS      dns
10.     IN MX      10 mail
11.
12. gate      IN A      192.168.5.1
13.          IN A      10.0.0.1
14. dns       IN A      192.168.1.116
15. mail      IN A      192.168.3.108
16. jupiter  IN A      192.168.2.100
17. venus    IN A      192.168.2.101
18. saturn   IN A      192.168.2.102
19. mercury  IN A      192.168.2.103
20. ntp      IN CNAME   dns
21. dns6     IN A6      0      2002:c0a8:174::
```

Zeile 1:

\$TTL legt die Standardlebensdauer fest, die für alle Einträge in dieser Datei gelten soll. In diesem Beispiel sind die Einträge zwei Tage lang gültig (2 D).

Zeile 2:

Hier beginnt der SOA (Start of Authority)-Steuereintrag:

- Der Name der zu verwaltenden Datei ist `example.com` an der ersten Stelle. Dieser Eintrag endet mit `.`, da anderenfalls die Zone ein zweites Mal angefügt würde. Alternativ kann hier `@` eingegeben werden. In diesem Fall wird die Zone aus dem entsprechenden Eintrag in `/etc/named.conf` extrahiert.
- Nach `IN SOA` befindet sich der Name des Namensservers, der als Master für diese Zone fungiert. Der Name wird von `dns` zu `dns.example.com` erweitert, da er nicht mit `.` endet.
- Es folgt die E-Mail-Adresse der für diesen Namensserver zuständigen Person. Da das Zeichen `@` bereits eine besondere Bedeutung hat, wird hier stattdessen `.` eingegeben. Für `root@example.com` muss der Eintrag wie folgt lauten: `root.example.com..` Der Punkt `.` muss angehängt werden, damit die Zone nicht hinzugefügt wird.

- Durch (werden alle Zeilen bis einschließlich) in den SOA-Eintrag aufgenommen.

Zeile 3:

Die Seriennummer (`serial`) ist eine beliebige Nummer, die sich bei jeder Änderung der Datei erhöht. Sie wird benötigt, um die sekundären Namenserver (Slave-Server) über Änderungen zu informieren. Hierfür hat sich eine 10-stellige Nummer aus Datum und Ausführungsnummer in der Form `JJJJMMTTNN` als übliches Format etabliert.

Zeile 4:

Die Aktualisierungsrate (`refresh rate`) gibt das Zeitintervall an, in dem die sekundären Namenserver die Seriennummer (`serial`) der Zone überprüfen. In diesem Fall beträgt dieses Intervall einen Tag.

Zeile 5:

Die Wiederholungsrate (`retry`) gibt das Zeitintervall an, nach dem ein sekundärer Namenserver bei einem Fehler erneut versucht, Kontakt zum primären Server herzustellen. In diesem Fall sind dies zwei Stunden.

Zeile 6:

Die Ablaufzeit (`expiry`) gibt den Zeitraum an, nach dem ein sekundärer Server die im Cache gespeicherten Daten verwirft, wenn er keinen erneuten Kontakt zum primären Server herstellen konnte. In diesem Fall ist dies eine Woche.

Zeile 7:

Die letzte Angabe im SOA-Eintrag gibt die negative Cache-Lebensdauer (`negative caching TTL`) an. Sie legt fest, wie lange Ergebnisse nicht aufgelöster DNS-Abfragen anderer Server im Cache gespeichert werden können.

Zeile 9:

`IN NS` gibt den für diese Domäne verantwortlichen Namenserver an. `dns` wird zu `dns.example.com` erweitert, da der Eintrag nicht mit einem `.` endet. Es können mehrere solcher Zeilen vorhanden sein - eine für den primären und eine für die einzelnen sekundären Namenserver. Wenn `notify` in `/etc/named.conf` nicht auf `no` gesetzt ist, werden alle hier aufgeführten Namenserver über die Änderungen an den Zonendaten informiert.

Zeile 10:

Der MX-Eintrag gibt den Mailserver an, der E-Mails für die Domäne `example.com` annimmt, verarbeitet und weiterleitet. In diesem Beispiel ist dies der Host `mail.example.com`. Die Zahl vor dem Hostnamen ist der Präferenzwert. Wenn mehrere MX-Einträge vorhanden sind, wird zunächst der Mailserver mit dem kleinsten Wert verwendet. Wenn die Mailzustellung an diesen Server nicht möglich ist, wird ein Versuch mit dem nächsthöheren Wert unternommen.

Zeilen 12 – 19:

Dies sind die eigentlichen Adresseinträge, in denen den Hostnamen eine oder mehrere IP-Adressen zugewiesen werden. Die Namen werden hier ohne `.` aufgelistet, da sie ihre Domäne nicht enthalten. Daher wird ihnen allen `example.com` hinzugefügt. Dem Host `gate` werden zwei IP-Adressen zugewiesen, weil er zwei Netzwerkkarten aufweist. Bei jeder traditionellen Hostadresse (IPv4) wird der Eintrag mit `A` gekennzeichnet. Wenn es sich um eine IPv6-Adresse handelt, wird der Eintrag mit `A6 0` gekennzeichnet. Das frühere Token für IPv6-Adressen war `AAAA`. Es ist inzwischen veraltet.

ANMERKUNG: IPv6-Syntax

Die Syntax des IPv6-Eintrags unterscheidet sich geringfügig von der Syntax von IPv4. Aufgrund der Möglichkeit einer Fragmentierung müssen Informationen zu fehlenden Bits vor der Adresse angegeben werden. Sie müssen diese Informationen angeben, selbst wenn Sie vorhaben, eine völlig unfragmentierte Adresse zu verwenden. Für den AAAA-Datensatz mit der Syntax

```
pluto IN          AAAA 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto IN          AAAA 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

müssen Sie Informationen über fehlende Bits im IPv6-Format hinzufügen. Da das obige Beispiel vollständig ist (es fehlen keine Bits), lautet das `A6`-Format des Eintrags:

```
pluto IN          A6 0 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto IN          A6 0 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

Zeile 20:

Der Alias `ntp` kann zur Adressierung von `dns` (`CNAME` steht für *canonical name* (kanonischer Name)) verwendet werden.

Die Pseudodomäne `in-addr.arpa` wird für Reverse-Lookups zur Auflösung von IP-Adressen in Hostnamen verwendet. Sie wird in umgekehrter Notation an den Netzwerk-Teil der Adresse angehängt. `192.168` wird also in `168.192.in-addr.arpa` aufgelöst. Weitere Informationen hierzu finden Sie unter [Beispiel 16.7, „Reverse-Lookup“](#) (S. 308).

Beispiel 16.7 *Reverse-Lookup*

```
1. $TTL 2D
2. 168.192.in-addr.arpa.    IN SOA dns.example.com. root.example.com. (
3.                          2003072441      ; serial
4.                          1D              ; refresh
5.                          2H              ; retry
6.                          1W              ; expiry
7.                          2D )            ; minimum
8.
9.                          IN NS          dns.example.com.
10.
11. 1.5                      IN PTR   gate.example.com.
12. 100.3                    IN PTR   www.example.com.
13. 253.2                    IN PTR   cups.example.com.
```

Zeile 1:

\$TTL definiert die Standard-TTL, die für alle Einträge hier gilt.

Zeile 2:

Die Konfigurationsdatei muss Reverse-Lookup für das Netzwerk `192.168` aktivieren. Angenommen, die Zone heißt `168.192.in-addr.arpa`, sollte sie nicht zu den Hostnamen hinzugefügt werden. Daher werden alle Hostnamen in ihrer vollständigen Form eingegeben, d. h. mit der Domäne und einem abschließenden Punkt (`.`). Die restlichen Einträge entsprechen den im vorherigen Beispiel (`example.com`) beschriebenen Einträgen.

Zeilen 3 – ;7:

Sehen Sie sich hierzu das Beispiel für `example.com` an.

Zeile 9:

Diese Zeile gibt wieder den für diese Zone verantwortlichen Namensserver an. Diesmal wird der Name allerdings in vollständiger Form mit Domäne und `.` am Ende eingegeben.

Zeilen 11 – ;13:

Dies sind die Zeigereinträge, die auf die IP-Adressen auf den entsprechenden Hosts verweisen. Am Anfang der Zeile wird nur der letzte Teil der IP-Adresse eingegeben,

ohne `.` am Ende. Wenn daran die Zone angehängt wird (ohne `.in-addr.arpa`), ergibt sich die vollständige IP-Adresse in umgekehrter Reihenfolge.

Normalerweise sollten Zonentransfers zwischen verschiedenen Versionen von BIND problemlos möglich sein.

16.7 Dynamische Aktualisierung von Zonendaten

Der Ausdruck *dynamische Aktualisierung* bezieht sich auf Vorgänge, bei denen Einträge in den Zonendateien eines Masterservers hinzugefügt, geändert oder gelöscht werden. Dieser Mechanismus wird in RFC 2136 beschrieben. Die dynamische Aktualisierung wird individuell für jeden Zoneneintrag durch Hinzufügen einer optionalen `allow-update-` bzw. `update-policy-`Regel konfiguriert. Dynamisch zu aktualisierende Zonen sollten nicht von Hand bearbeitet werden.

Die zu aktualisierenden Einträge werden mit dem Befehl `nsupdate` an den Server übermittelt. Die genaue Syntax dieses Befehls können Sie der `man`-Seite für `nsupdate` (`man8 nsupdate`) entnehmen. Aus Sicherheitsgründen sollten solche Aktualisierungen mithilfe von TSIG-Schlüsseln durchgeführt werden, wie in [Abschnitt 16.8](#), „**Sichere Transaktionen**“ (S. 309) beschrieben.

16.8 Sichere Transaktionen

Sichere Transaktionen können mithilfe von Transaktionssignaturen (TSIGs) durchgeführt werden, die auf gemeinsam genutzten geheimen Schlüsseln (TSIG-Schlüssel) beruhen. In diesem Abschnitt wird die Erstellung und Verwendung solcher Schlüssel beschrieben.

Sichere Transaktionen werden für die Kommunikation zwischen verschiedenen Servern und für die dynamische Aktualisierung von Zonendaten benötigt. Die Zugriffssteuerung von Schlüsseln abhängig zu machen, ist wesentlich sicherer, als sich lediglich auf IP-Adressen zu verlassen.

Erstellen Sie mit dem folgenden Befehl einen TSIG-Schlüssel (genauere Informationen finden Sie unter `mandnssec-keygen`):

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

Dadurch werden zwei Schlüssel mit ungefähr folgenden Namen erstellt:

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

Der Schlüssel selbst (eine Zeichenkette, wie beispielsweise `ejIkuCyyGJwwuN3xAteKgg==`) ist in beiden Dateien enthalten. Um ihn für Transaktionen zu verwenden, muss die zweite Datei (`Khost1-host2.+157+34265.key`) auf den entfernten Host übertragen werden, möglichst auf eine sichere Weise (z. B. über SCP). Auf dem entfernten Server muss der Schlüssel in der Datei `/etc/named.conf` enthalten sein, damit eine sichere Kommunikation zwischen `host1` und `host2` möglich ist:

```
key host1-host2. {
    algorithm hmac-md5;
    secret "ejIkuCyyGJwwuN3xAteKgg==";
};
```

WARNUNG: Dateiberechtigungen von `/etc/named.conf`

Vergewissern Sie sich, dass die Berechtigungen von `/etc/named.conf` ordnungsgemäß eingeschränkt sind. Der Standardwert für diese Datei lautet `0640`, mit `root` als Eigentümer und `named` als Gruppe. Alternativ können Sie die Schlüssel in eine gesonderte Datei mit speziell eingeschränkten Berechtigungen verschieben, die dann aus `/etc/named.conf` eingefügt werden. Zum Einschließen einer externen Datei verwenden Sie:

```
include "filename"
```

Ersetzen Sie `filename` durch einen absoluten Pfad zu Ihrer Datei mit den Schlüsseln.

Damit Server `host1` den Schlüssel für `host2` verwenden kann (in diesem Beispiel mit der Adresse `10.1.2.3`), muss die Datei `/etc/named.conf` des Servers folgende Regel enthalten:

```
server 10.1.2.3 {
    keys { host1-host2. };
};
```

Analoge Einträge müssen in die Konfigurationsdateien von `host2` aufgenommen werden.

Fügen Sie TSIG-Schlüssel für alle ACLs (Access Control Lists, Zugriffssteuerungslisten, nicht zu verwechseln mit Dateisystem-ACLs) hinzu, die für IP-Adressen und -Adress-

bereiche definiert sind, um Transaktionssicherheit zu gewährleisten. Der entsprechende Eintrag könnte wie folgt aussehen:

```
allow-update { key host1-host2. ;};
```

Dieses Thema wird eingehender im *Referenzhandbuch für BIND-Administratoren* (unter `update-policy`) erörtert.

16.9 DNS-Sicherheit

DNSSEC (DNS-Sicherheit) wird in RFC 2535 beschrieben. Die für DNSSEC verfügbaren Werkzeuge werden im BIND-Handbuch erörtert.

Einer als sicher betrachteten Zone müssen ein oder mehrere Zonenschlüssel zugeordnet sein. Diese werden mit `dnssec-keygen` erstellt, genau wie die Host-Schlüssel. Zurzeit wird der DSA-Verschlüsselungsalgorithmus zum Erstellen dieser Schlüssel verwendet. Die generierten öffentlichen Schlüssel sollten mithilfe einer `$INCLUDE`-Regel in die entsprechende Zonendatei aufgenommen werden.

Mit dem Befehl `dnssec-makekeyset` werden alle erstellten Schlüssel zu einem Satz zusammengefasst, der dann auf sichere Weise in die übergeordnete Zone übertragen werden muss. In der übergeordneten Zone wird der Satz mit `dnssec-signkey` signiert. Die durch diesen Befehl erstellten Dateien werden anschließend verwendet, um die Zonen mit `dnssec-signzone` zu signieren, wodurch wiederum die Dateien erstellt werden, die für die einzelnen Zonen in `/etc/named.conf` aufgenommen werden sollen.

16.10 Weiterführende Informationen

Weitere Informationen können Sie dem *Referenzhandbuch für BIND-Administratoren* aus Paket `bind-doc` entnehmen, das unter `/usr/share/doc/packages/bind/` installiert ist. Außerdem könnten Sie die RFCs zurate ziehen, auf die im Handbuch verwiesen wird, sowie die in BIND enthaltenen man-Seiten. `/usr/share/doc/packages/bind/README.SuSE` enthält aktuelle Informationen zu BIND in openSUSE.

DHCP

Das *DHCP* (Dynamic Host Configuration Protocol) dient dazu, Einstellungen in einem Netzwerk zentral von einem Server aus zuzuweisen. Einstellungen müssen also nicht dezentral an einzelnen Arbeitsplatzcomputern konfiguriert werden. Ein für DHCP konfigurierter Host verfügt nicht über eine eigene statische Adresse. Er konfiguriert sich stattdessen vollständig und automatisch nach den Vorgaben des DHCP-Servers. Wenn Sie auf der Client-Seite den NetworkManager verwenden, brauchen Sie den Client überhaupt nicht zu konfigurieren. Das ist nützlich, wenn Sie in wechselnden Umgebungen arbeiten und nur jeweils eine Schnittstelle aktiv ist. Verwenden Sie den NetworkManager nie auf einem Computer, der einen DHCP-Server ausführt.

Eine Möglichkeit zur Konfiguration von DHCP-Servern besteht darin, jeden Client mithilfe der Hardwareadresse seiner Netzwerkkarte zu identifizieren (die in den meisten Fällen statisch ist) und anschließend diesen Client bei jeder Verbindung zum Server mit identischen Einstellungen zu versorgen. Zum anderen kann DHCP aber auch so konfiguriert werden, dass der Server jedem Client, der eine Verbindung zu ihm herstellt, eine Adresse aus einem dafür vorgesehenen Adresspool dynamisch zuweist. In diesem Fall versucht der DHCP-Server, dem Client bei jeder Anforderung dieselbe Adresse zuzuweisen - auch über einen längeren Zeitraum hinweg. Das ist nur möglich, wenn die Anzahl der Clients im Netzwerk nicht die Anzahl der Adressen übersteigt.

DHCP erleichtert Systemadministratoren das Leben. Alle (selbst umfangreiche) Änderungen der Netzwerkadressen oder der -konfiguration können zentral in der Konfigurationsdatei des DHCP-Servers vorgenommen werden. Dies ist sehr viel komfortabler als das Neukonfigurieren zahlreicher Arbeitsstationen. Außerdem können vor allem neue Computer sehr einfach in das Netzwerk integriert werden, indem sie aus dem Adresspool eine IP-Adresse zugewiesen bekommen. Das Abrufen der entsprechen-

den Netzwerkeinstellungen von einem DHCP-Server ist auch besonders interessant für Notebooks, die regelmäßig in unterschiedlichen Netzwerken verwendet werden.

In diesem Kapitel wird der DHCP-Server im gleichen Subnetz wie die Workstations (192.168.2.0/24) mit 192.168.2.1 als Gateway ausgeführt. Er hat die feste IP-Adresse 192.168.2.254 und bedient die beiden Adressbereiche 192.168.2.10 bis 192.168.2.20 und 192.168.2.100 bis 192.168.2.200;.

Neben IP-Adresse und Netzmaske werden dem Client nicht nur der Computer- und Domänenname, sondern auch das zu verwendende Gateway und die Adressen der Namenserver mitgeteilt. Im Übrigen können auch etliche andere Parameter zentral konfiguriert werden, z. B. ein Zeitserver, von dem die Clients die aktuelle Uhrzeit abrufen können, oder ein Druckserver.

17.1 Konfigurieren eines DHCP-Servers mit YaST

WICHTIG: LDAP-Unterstützung

In dieser Version von openSUSE kann das DHCP-Modul von YaST so eingestellt werden, dass die Serverkonfiguration lokal gespeichert wird (auf dem Host, der den DHCP-Server ausführt) oder so, dass die Konfigurationsdaten von einem LDAP-Server verwaltet werden. Wenn Sie LDAP verwenden möchten, müssen Sie vor der Konfiguration des DHCP-Servers die LDAP-Umgebung einrichten.

Das DHCP-Modul von YaST ermöglicht die Einrichtung Ihres eigenen DHCP-Servers für das lokale Netzwerk. Das Modul kann im einfachen oder im Expertenmodus ausgeführt werden.

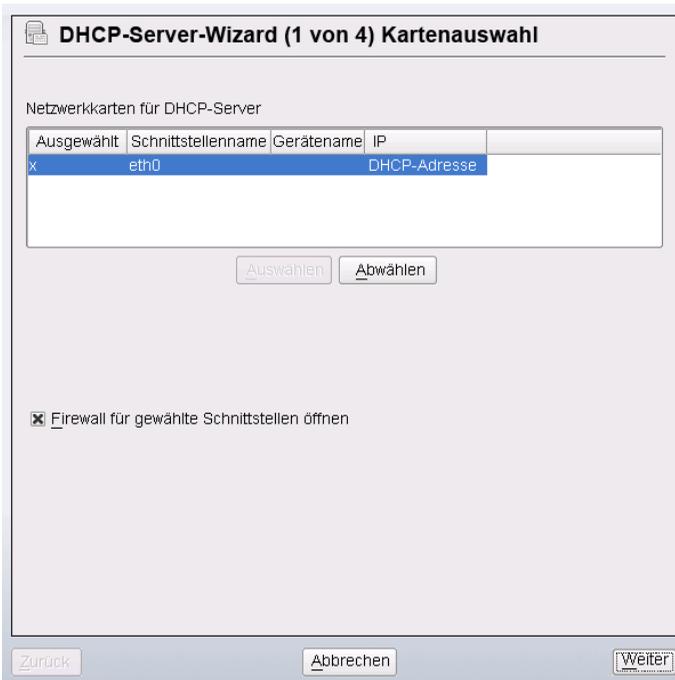
17.1.1 Anfängliche Konfiguration (Assistent)

Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Nach Abschluss der anfänglichen Konfiguration ist eine grundlegende Serverkonfiguration verfügbar, die für einfache Szenarien ausreichend ist. Komplexere Konfigurationaufgaben können im Expertenmodus ausgeführt werden.

Kartenauswahl

Im ersten Schritt ermittelt YaST die in Ihr System eingebundenen Netzwerkschnittstellen und zeigt sie anschließend in einer Liste an. Wählen Sie in dieser Liste die Schnittstelle aus, auf der der DHCP-Server lauschen soll, und klicken Sie auf *Hinzufügen*. Wählen Sie anschließend die Option *Firewall für gewählte Schnittstelle öffnen*, um die Firewall für diese Schnittstelle zu öffnen. Weitere Informationen hierzu finden Sie unter [Abbildung 17.1, „DHCP-Server: Kartenauswahl“](#) (S. 315).

Abbildung 17.1 DHCP-Server: Kartenauswahl



Globale Einstellungen

Geben Sie anhand des Kontrollkästchens an, ob Ihre DHCP-Einstellungen automatisch von einem LDAP-Server gespeichert werden sollen. In den Eingabefeldern legen Sie die Netzwerkinformationen fest, die jeder von diesem DHCP-Server verwaltete Client erhalten soll. Diese sind: Domänenname, Adresse eines Zeitervers, Adressen der primären und sekundären Namenserver, Adressen eines Druck- und WINS-Servers (für gemischte Netzwerkumgebungen mit Windows- und Linux-Clients), Gateway-Adressen und Leasing-Zeit. Weitere Informationen hierzu finden Sie unter [Abbildung 17.2, „DHCP-Server: Globale Einstellungen“](#) (S. 316).

Abbildung 17.2 DHCP-Server: Globale Einstellungen

DHCP-Server-Wizard (2 von 4) Globale Einstellungen

LDAP-Unterstützung

Name des DHCP-Servers (optional)

Domain-Name: beispiel.com

NTP-Zeitserver: 192.168.1.116

IP des primären Nameservers: 192.168.1.116

Druckserver:

IP des sekundären Nameservers:

WINS-Server: 192.168.1.110

Standard-Gateway (Router): 192.168.2.1

Standard-Leasing-Zeit: 4

Einheiten: Stunden

Zurück Abbrechen Weiter

Dynamisches DHCP

In diesem Schritt konfigurieren Sie die Vergabe der dynamischen IP-Adressen an Clients. Hierzu legen Sie einen Bereich von IP-Adressen fest, in dem die zu vergebenden Adressen der DHCP-Clients liegen dürfen. Alle zu vergebenden Adressen müssen unter eine gemeinsame Netzmaske fallen. Legen Sie abschließend die Leasing-Zeit fest, für die ein Client seine IP-Adresse behalten darf, ohne eine Verlängerung der Leasing-Zeit beantragen zu müssen. Legen Sie optional auch die maximale Leasing-Zeit fest, innerhalb derer eine bestimmte IP-Adresse auf dem Server für einen bestimmten Client reserviert bleibt. Weitere Informationen hierzu finden Sie unter [Abbildung 17.3, „DHCP-Server: Dynamisches DHCP“](#) (S. 317).

Abbildung 17.3 DHCP-Server: Dynamisches DHCP

The screenshot shows the 'DHCP-Server-Wizard (3 von 4) Dynamisches DHCP' window. It is divided into three main sections:

- Subnetzinformationen:** Contains fields for 'Aktuelles Netzwerk', 'Aktuelle Netzmaske', and 'Netzmasken-Bits' (set to 32). Below these are fields for 'Minimale IP-Adresse' and 'Maximale IP-Adresse'.
- IP-Adressbereich:** Contains fields for 'Erste IP-Adresse' (192.168.2.100) and 'Letzte IP-Adresse' (192.168.2.128). There is a checkbox for 'Dynamisches BOOTP zulassen' which is currently unchecked.
- Leasing-Zeit:** Contains a 'Standard' field (4), a unit dropdown menu (Stunden), a 'Maximum' field (2), and another unit dropdown menu (Tage).

At the bottom of the window, there is a 'DNS-Server synchronisieren' dropdown menu and three buttons: 'Zurück', 'Abbrechen', and 'Weiter'.

Fertigstellen der Konfiguration und Auswahl des Startmodus

Nachdem Sie den dritten Teil des Konfigurationsassistenten abgeschlossen haben, gelangen Sie in ein letztes Dialogfeld, das sich mit den Startoptionen des DHCP-Servers befasst. Hier können Sie festlegen, ob der DHCP-Server automatisch beim Booten des Systems oder bei Bedarf (z. B. zu Testzwecken) manuell gestartet werden soll. Klicken Sie auf *Verlassen*, um die Konfiguration des Servers abzuschließen. Weitere Informationen hierzu finden Sie unter [Abbildung 17.4, „DHCP-Server: Start“](#) (S. 318). Alternativ können Sie *Host-Verwaltung* links aus der Baumstruktur auswählen, um zusätzlich zur grundlegenden Konfiguration bestimmte Host-Verwaltungsfunktionen zu konfigurieren (siehe [Abbildung 17.5, „DHCP-Server: Host-Verwaltung“](#) (S. 319)).

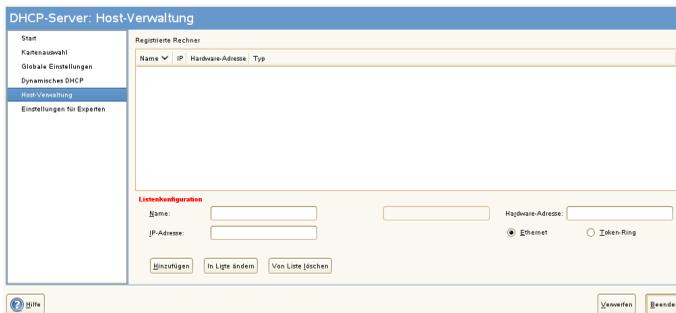
Abbildung 17.4 DHCP-Server: Start



Host-Verwaltung

Statt der Verwendung des dynamischen DHCP, wie in den vorigen Abschnitten beschrieben, können Sie den Server auch so konfigurieren, dass Adressen in fast statischer Weise zugewiesen werden. Dafür geben Sie in den Eintragsfeldern im unteren Teil eine Liste der in dieser Art zu verwaltenden Clients ein. Geben Sie vor allem *Name* und *IP-Adresse* für einen solchen Client an, die *Hardware-Adresse* und den *Netzwerktyp* (Token-Ring oder Ethernet). Ändern Sie die oben angezeigte Liste der Clients mit *Hinzufügen*, *Bearbeiten* und *Löschen*. Weitere Informationen hierzu finden Sie unter [Abbildung 17.5](#), „DHCP-Server: Host-Verwaltung“ (S. 319).

Abbildung 17.5 DHCP-Server: Host-Verwaltung



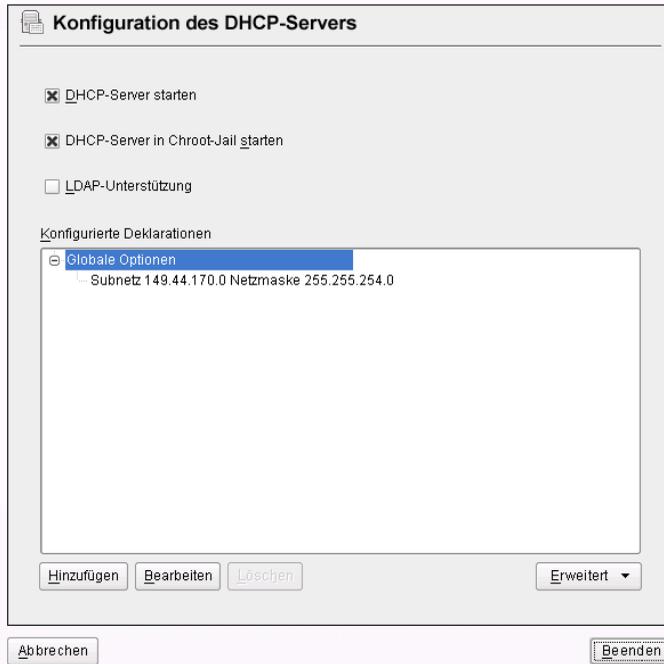
17.1.2 Konfiguration für Experten

Zusätzlich zu den bisher erwähnten Konfigurationsmethoden gibt es einen Expertenkonfigurationsmodus, mit dem Sie die Einrichtung des DHCP-Servers detailgenau ändern können. Starten Sie die Expertenkonfiguration, indem Sie *Einstellungen für Experten* in der Baumstruktur links im Dialogfeld wählen.

Chroot-Umgebung und Deklarationen

Im ersten Dialogfeld bearbeiten Sie die vorhandene Konfiguration, indem Sie *DHCP-Server starten* wählen. Eine wichtige Funktion des Verhaltens eines DHCP-Servers ist, dass er in einer Chroot-Umgebung (oder einem Chroot-Jail) ausgeführt werden kann und so den Server-Host schützt. Sollte der DHCP-Server durch einen Angriff von außen beeinträchtigt werden, bleibt der Angreifer gefangen im Chroot-Jail und kann auf den Rest des Systems nicht zugreifen. Im unteren Bereich des Dialogfelds sehen Sie eine Baumstruktur mit den bereits definierten Deklarationen. Diese verändern Sie mit *Hinzufügen*, *Löschen* und *Bearbeiten*. Wenn Sie *Erweitert* wählen, werden zusätzliche Experten-Dialogfelder angezeigt. Weitere Informationen hierzu finden Sie unter **Abbildung 17.6**, „**DHCP-Server: Chroot Jail und Deklarationen**“ (S. 320). Nach der Auswahl von *Hinzufügen* legen Sie den hinzuzufügenden Deklarationstyp fest. Mit *Erweitert* zeigen Sie die Protokolldatei des Servers an, konfigurieren die TSIG-Schlüsselverwaltung und passen die Konfiguration der Firewall an die Einrichtung des DHCP-Servers an.

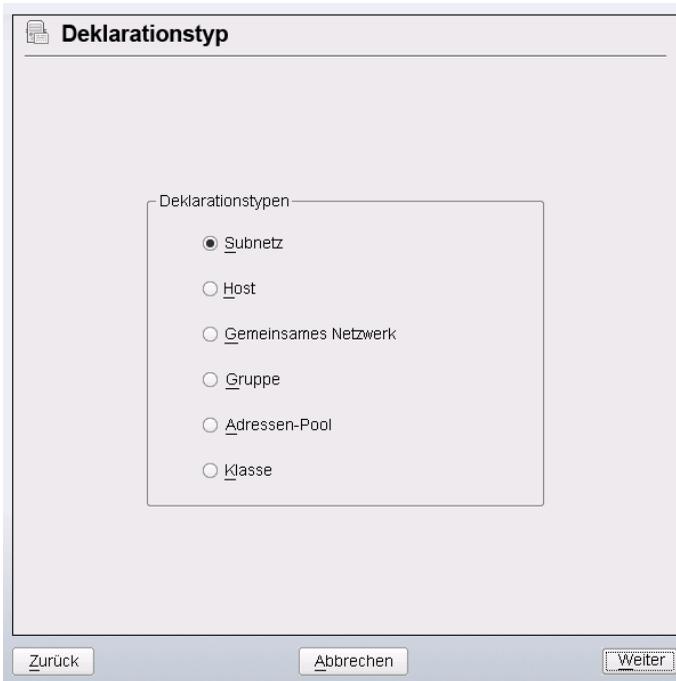
Abbildung 17.6 DHCP-Server: Chroot Jail und Deklarationen



Auswählen des Deklarationstyps

Die *Globalen Optionen* des DHCP-Servers bestehen aus einer Reihe von Deklarationen. In diesem Dialogfeld legen Sie die Deklarationstypen *Subnetz*, *Host*, *Gemeinsames Netzwerk*, *Gruppe*, *Adressen-Pool* und *Klasse* fest. In diesem Beispiel sehen Sie die Auswahl eines neuen Subnetzwerks (siehe [Abbildung 17.7](#), „**DHCP-Server: Wählen eines Deklarationstyps**“ (S. 321)).

Abbildung 17.7 DHCP-Server: Wählen eines Deklarationstyps



Konfiguration des Subnetzes

In diesem Dialogfeld können Sie ein neues Subnetz mit seiner IP-Adresse und Netzmaske angeben. In der Mitte des Dialogfelds ändern Sie die Startoptionen des DHCP-Servers für das ausgewählte Subnetz mit den Optionen *Hinzufügen*, *Bearbeiten* und *Löschen*. Um einen dynamischen DNS für das Subnetz einzurichten, wählen Sie *Dynamisches DNS*.

Abbildung 17.8 DHCP-Server: Konfigurieren von Subnetzen

Konfiguration des Subnetzes

Netzwerkadresse: 192.168.2.0 Netzwerkmáske: 255.255.255.0

Option	Wert
default-lease-time	14400
max-lease-time	172800

Hinzufügen Bearbeiten Löschen Dynamisches DNS

Zurück Abbrechen OK

TSIG-Schlüsselverwaltung

Wenn Sie im vorigen Dialogfeld die Konfiguration des dynamischen DNS vorgenommen haben, können Sie jetzt die Schlüsselverwaltung für einen sicheren Zonentransfer konfigurieren. Wenn Sie *OK* wählen, gelangen Sie zu einem weiteren Dialogfeld, in dem Sie die Schnittstelle für das dynamische DNS konfigurieren können (siehe **Abbildung 17.10**, „DHCP-Server: Schnittstellenkonfiguration für dynamisches DNS“ (S. 324)).

Abbildung 17.9 DHCP Server: TSIG-Konfiguration



Dynamisches DNS: Schnittstellenkonfiguration

Jetzt können Sie das dynamische DNS für das Subnetz aktivieren, indem Sie *Dynamisches DNS für dieses Subnetz aktivieren* wählen. Danach wählen Sie in der Dropdown-Liste die TSIG-Schlüssel für Forward und Reverse Zones. Vergewissern Sie sich dabei, dass die Schlüssel für den DNS- und den DHCP-Server dieselben sind. Mit der Option *Globale dynamische DNS-Einstellungen aktualisieren* aktivieren Sie die automatische Aktualisierung und Einstellung der globalen DHCP-Servereinstellungen entsprechend der dynamischen DNS-Umgebung. Nun legen Sie fest, welche Forward und Reverse Zones über das dynamische DNS aktualisiert werden sollen. Dafür geben Sie den primären Namensserver für beide Zonen an. Wenn der Namensserver auf demselben Host wie der DHCP-Server ausgeführt wird, können Sie diese Felder leer lassen. Wenn Sie *OK* wählen, gelangen Sie wieder zum Dialogfeld für die Subnetzkonfiguration (siehe [Abbildung 17.8](#), „*DHCP-Server: Konfigurieren von Subnetzen*“ (S. 322)). Wenn Sie noch einmal auf *OK* klicken, gelangen Sie wieder zum ursprünglichen Dialogfeld für die Expertenkonfiguration.

Abbildung 17.10 DHCP-Server: Schnittstellenkonfiguration für dynamisches DNS

The screenshot shows a window titled "Konfiguration der Schnittstelle". It contains the following elements:

- A checked checkbox: Dynamisches DNS für dieses Subnetz aktivieren
- A dropdown menu for "TSIG-Schlüssel der Forward-Zone" with the value "examplecom".
- A dropdown menu for "TSIG-Schlüssel der Reverse-Zone" with the value "examplecom".
- An unchecked checkbox: Globale dynamische DNS-Einstellungen aktualisieren
- Four text input fields arranged in a 2x2 grid:
 - Top-left: "Zone"
 - Top-right: "Primärer DNS-Server"
 - Bottom-left: "Reverse-Zone"
 - Bottom-right: "Primärer DNS-Server"
- At the bottom, three buttons: "Zurück", "Abbrechen", and "OK".

Netzwerkschnittstellenkonfiguration

Wenn Sie die Schnittstellen festlegen möchten, die vom DHCP-Server überwacht werden sollen, und die Firewall-Konfiguration anpassen, wählen Sie im Dialogfeld für die Expertenkonfiguration *Erweitert* > *Schnittstellenkonfiguration*. Aus der Liste der angezeigten Schnittstellen wählen Sie die gewünschte(n) Schnittstelle(n) für den DHCP-Server aus. Falls Clients in allen Subnetzen mit dem Server kommunizieren sollen und der Server-Host eine Firewall ausführt, passen Sie die Einstellungen der Firewall entsprechend an. Dafür wählen Sie *Firewall-Einstellungen anpassen*. YaST passt dann die Regeln der SuSEfirewall2 an die neuen Bedingungen an (siehe [Abbildung 17.11](#), „DHCP-Server: Netzwerkschnittstelle und Firewall“ (S. 325)). Jetzt können Sie zum ursprünglichen Dialogfeld zurückkehren, indem Sie auf *OK* klicken.

Abbildung 17.11 DHCP-Server: Netzwerkschnittstelle und Firewall



Nach Abschluss aller Konfigurationsschritte schließen Sie das Dialogfeld mit *OK*. Der Server wird jetzt mit seiner neuen Konfiguration gestartet.

17.2 DHCP-Softwarepakete

Für openSUSE stehen sowohl ein DHCP-Server als auch DHCP-Clients bereit. Der vom Internet Systems Consortium (ISC) herausgegebene DHCP-Server `dhcpd` stellt die Serverfunktionalität zur Verfügung. Wählen Sie auf der Client-Seite zwischen zwei verschiedenen DHCP-Client-Programmen: `DHCP-Client` (auch von ISC) und `DHCP-Client-Daemon` im Paket `dhcpcd`.

openSUSE installiert standardmäßig `dhcpcd`. Das Programm ist sehr einfach in der Handhabung und wird beim Booten des Computers automatisch gestartet, um nach einem DHCP-Server zu suchen. Es kommt ohne eine Konfigurationsdatei aus und funktioniert im Normalfall ohne weitere Konfiguration. Verwenden Sie für komplexere

Situationen das Programm `dhcp-client` von ISC, das sich über die Konfigurationsdatei `/etc/dhclient.conf` steuern lässt.

17.3 Der DHCP-Server `dhcpd`

Das Kernstück des DHCP-Systems ist der `dhcpd`-Daemon. Dieser Server *least* Adressen und überwacht deren Nutzung gemäß den Vorgaben in der Konfigurationsdatei `/etc/dhcpd.conf`. Über die dort definierten Parameter und Werte stehen dem Systemadministrator eine Vielzahl von Möglichkeiten zur Verfügung, das Verhalten des Programms anforderungsgemäß zu beeinflussen. Sehen Sie sich die einfache Beispieldatei `/etc/dhcpd.conf` in [Beispiel 17.1](#), „Die Konfigurationsdatei `/etc/dhcpd.conf`“ (S. 326) an.

Beispiel 17.1 Die Konfigurationsdatei `/etc/dhcpd.conf`

```
default-lease-time 600;           # 10 minutes
max-lease-time 7200;             # 2 hours

option domain-name "example.com";
option domain-name-servers 192.168.1.116;
option broadcast-address 192.168.2.255;
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0
{
    range 192.168.2.10 192.168.2.20;
    range 192.168.2.100 192.168.2.200;
}
```

Diese einfache Konfigurationsdatei reicht bereits aus, damit der DHCP-Server im Netzwerk IP-Adressen zuweisen kann. Bitte achten Sie insbesondere auf die Semikolons am Ende jeder Zeile, ohne die `dhcpd` nicht startet.

Die Beispieldatei lässt sich in drei Abschnitte unterteilen. Im ersten Abschnitt wird definiert, wie viele Sekunden eine IP-Adresse standardmäßig an einen anfragenden Client geleast wird, bevor dieser eine Verlängerung anfordern sollte (`default-lease-time`). Hier wird auch festgelegt, wie lange ein Computer maximal eine vom DHCP-Server vergebene IP-Adresse behalten darf, ohne für diese eine Verlängerung anfordern zu müssen (`max-lease-time`).

Im zweiten Abschnitt werden einige grundsätzliche Netzwerkparameter global festgelegt:

- Die Zeile `option domain-name` enthält die Standarddomäne des Netzwerks.
- Mit dem Eintrag `option domain-name-servers` können Sie bis zu drei Werte für die DNS-Server angeben, die zur Auflösung von IP-Adressen in Hostnamen (und umgekehrt) verwendet werden sollen. Idealerweise sollten Sie vor dem Einrichten von DHCP einen Namensserver auf dem Computer oder im Netzwerk konfigurieren. Dieser Namensserver sollte für jede dynamische Adresse jeweils einen Hostnamen und umgekehrt bereithalten. Weitere Informationen zum Konfigurieren eines eigenen Namensservers finden Sie in [Kapitel 16, Domain Name System \(DNS\)](#) (S. 287).
- Die Zeile `option broadcast-address` definiert die Broadcast-Adresse, die der anfragende Client verwenden soll.
- Mit `option routers` wird festgelegt, wohin der Server Datenpakete schicken soll, die (aufgrund der Adresse von Quell- und Zielhost sowie der Subnetzmaske) nicht im lokalen Netzwerk zugestellt werden können. Gerade bei kleineren Netzwerken ist dieser Router auch meist mit dem Internet-Gateway identisch.
- Mit `option subnet-mask` wird die den Clients zugewiesene Netzmaske angegeben.

Im letzten Abschnitt der Datei werden ein Netzwerk und eine Subnetzmaske angegeben. Abschließend muss noch ein Adressbereich gewählt werden, aus dem der DHCP-Daemon IP-Adressen an anfragende Clients vergeben darf. In [Beispiel 17.1, „Die Konfigurationsdatei `/etc/dhcpd.conf`“](#) (S. 326) können Clients Adressen zwischen `192.168.2.10` und `192.168.2.20` sowie `192.168.2.100` und `192.168.2.200` zugewiesen werden.

Nachdem Sie diese wenigen Zeilen bearbeitet haben, können Sie den DHCP-Daemon bereits mit dem Befehl `rcdhcpd start` aktivieren. Der DHCP-Daemon ist sofort einsatzbereit. Mit dem Befehl `rcdhcpd check-syntax` können Sie eine kurze Überprüfung der Konfigurationsdatei vornehmen. Wenn ein unerwartetes Problem mit der Konfiguration auftritt (der Server wird mit einem Fehler abgebrochen oder gibt beim Starten nicht `done` zurück), lesen Sie die Informationen in der zentralen Systemprotokolldatei `/var/log/messages` oder auf der Konsole `10` (Strg + Alt + F10).

Auf einem openSUSE-Standardsystem wird der DHCP-Dämon aus Sicherheitsgründen in einer chroot-Umgebung gestartet. Damit der Daemon die Konfigurationsdateien

finden kann, müssen diese in die chroot-Umgebung kopiert werden. In der Regel müssen Sie dazu nur den Befehl `rcdhcpd start` eingeben, um die Dateien automatisch zu kopieren.

17.3.1 Clients mit statischen IP-Adressen

DHCP lässt sich auch verwenden, um einem bestimmten Client eine vordefinierte statische Adresse zuzuweisen. Solche expliziten Adresszuweisungen haben Vorrang vor dynamischen Adressen aus dem Pool. Im Unterschied zu den dynamischen verfallen die statischen Adressinformationen nie, z. B. wenn nicht mehr genügend freie Adressen zur Verfügung stehen und deshalb eine Neuverteilung unter den Clients erforderlich ist.

Zur Identifizierung eines mit einer statischen Adresse konfigurierten Clients verwendet `dhcpd` die Hardware-Adresse. Dies ist eine global eindeutige, fest definierte Zahl aus sechs Oktettpaaren, über die jedes Netzwerkgerät verfügt, z. B. `00:30:6E:08:EC:80`. Werden die entsprechenden Zeilen, wie z. B. in [Beispiel 17.2](#), „Ergänzungen zur Konfigurationsdatei“ (S. 328) zur Konfigurationsdatei von [Beispiel 17.1](#), „Die Konfigurationsdatei `/etc/dhcpd.conf`“ (S. 326) hinzugefügt, weist der DHCP-Daemon dem entsprechenden Client immer dieselben Daten zu.

Beispiel 17.2 *Ergänzungen zur Konfigurationsdatei*

```
host jupiter {
hardware ethernet 00:30:6E:08:EC:80;
fixed-address 192.168.2.100;
}
```

Der Name des entsprechenden Clients (`host Hostname`, hier `jupiter`) wird in die erste Zeile, und die MAC-Adresse wird in die zweite Zeile eingegeben. Auf Linux-Hosts kann die MAC-Adresse mit dem Befehl `iplink show` gefolgt vom Netzwerkgerät (z. B. `eth0`) ermittelt werden. Die Ausgabe sollte in etwa wie folgt aussehen:

```
link/ether 00:30:6E:08:EC:80
```

Im vorherigen Beispiel wird also dem Client, dessen Netzwerkkarte die MAC-Adresse `00:30:6E:08:EC:80` hat, automatisch die IP-Adresse `192.168.2.100` und der Hostname `jupiter` zugewiesen. Als Hardwaretyp kommt heutzutage in aller Regel `ethernet` zum Einsatz, wobei durchaus auch das vor allem bei IBM-Systemen häufig zu findende `token-ring` unterstützt wird.

17.3.2 Die Version von openSUSE

Aus Sicherheitsgründen enthält bei openSUSE Linux der DHCP-Server von ISC den non-root/chroot-Patch von Ari Edelkind. Damit kann `dhcpd` mit der Benutzer-ID `nobody` und in einer `chroot`-Umgebung (`/var/lib/dhcp`) ausgeführt werden. Um dies zu ermöglichen, muss sich die Konfigurationsdatei `dhcpd.conf` im Verzeichnis `/var/lib/dhcp/etc` befinden. Sie wird vom Init-Skript beim Start automatisch dorthin kopiert.

Dieses Verhalten lässt sich über Einträge in der Datei `/etc/sysconfig/dhcpd` steuern. Um den `dhcpd` ohne `chroot`-Umgebung laufen zu lassen, setzen Sie die Variable `DHCPD_RUN_CHROOTED` in der Datei `/etc/sysconfig/dhcpd` auf „no“.

Damit der `dhcpd` auch in der `chroot`-Umgebung Hostnamen auflösen kann, müssen außerdem einige weitere Konfigurationsdateien kopiert werden:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Diese Dateien werden beim Starten des Init-Skripts in das Verzeichnis `/var/lib/dhcp/etc/` kopiert. Berücksichtigen Sie die Kopien bei Aktualisierungen, die benötigt werden, wenn sie durch ein Skript wie `/etc/ppp/ip-up` dynamisch modifiziert werden. Falls in der Konfigurationsdatei anstelle von Hostnamen nur IP-Adressen verwendet werden, sind jedoch keine Probleme zu erwarten.

Wenn in Ihrer Konfiguration weitere Dateien in die `chroot`-Umgebung kopiert werden müssen, können Sie diese mit der Variablen `DHCPD_CONF_INCLUDE_FILES` in der Datei `/etc/sysconfig/dhcpd` festlegen. Damit der `dhcp`-Daemon aus der `chroot`-Umgebung heraus auch nach einem Neustart des `Syslog-ng`-Daemons weiter protokollieren kann, befindet sich der zusätzliche Eintrag `SYSLOGD_ADDITIONAL_SOCKET_DHCP` in der Datei `/etc/sysconfig/syslog`.

17.4 Weiterführende Informationen

Weitere Informationen zu DHCP finden Sie auf der Website des *Internet Systems Consortium* (<http://www.isc.org/products/DHCP/>). Weitere Informationen finden Sie zudem auf den man-Seiten `dhcpd`, `dhcpd.conf`, `dhcpd.leases` und `dhcp-options`.

Zeitsynchronisierung mit NTP

Der NTP-(Network Time Protocol-)Mechanismus ist ein Protokoll für die Synchronisierung der Systemzeit über das Netzwerk. Erstens kann ein Computer die Zeit von einem Server abrufen, der als zuverlässige Zeitquelle gilt. Zweitens kann ein Computer selbst für andere Computer im Netzwerk als Zeitquelle fungieren. Zwei Ziele sollen erreicht werden: die absolute Zeit beizubehalten und die Systemzeit aller Computer im Netzwerk zu synchronisieren.

Das Aufrechterhalten der genauen Systemzeit ist in vielen Situationen wichtig. Die integrierte Hardware-Uhr (BIOS-Uhr) erfüllt häufig nicht die Anforderungen bestimmter Anwendungen, beispielsweise Datenbanken. Die manuelle Korrektur der Systemzeit würde schwerwiegende Probleme nach sich ziehen; das Zurückstellen kann beispielsweise zu Fehlfunktionen wichtiger Anwendungen führen. Die Systemzeiten der in einem Netzwerk zusammengeschlossenen Computer müssen in der Regel synchronisiert werden. Es empfiehlt sich aber nicht, die Zeiten manuell anzugleichen. Vielmehr sollten Sie dazu `xntp` verwenden. Er passt die Systemzeit ständig anhand zuverlässiger Zeitserver im Netzwerk an. Zudem ermöglicht er die Verwaltung lokaler Referenzuhren, beispielsweise funkgesteuerter Uhren.

18.1 Konfigurieren eines NTP-Client mit YaST

`xntp` ist so voreingestellt, dass die lokale Computeruhr als Zeitreferenz verwendet wird. Das Verwenden der (BIOS-) Uhr ist jedoch nur eine Ausweidlösung, wenn keine genauere Zeitquelle verfügbar ist. YaST erleichtert die Konfiguration von NTP-Clients.

Verwenden Sie für Systeme, die keine Firewall ausführen, entweder die schnelle oder die erweiterte Konfiguration. Bei einem durch eine Firewall geschützten System kann die erweiterte Konfiguration die erforderlichen Ports in SuSEfirewall2 öffnen.

18.1.1 Schnelle NTP-Client-Konfiguration

Die schnelle NTP-Client-Konfiguration (*Netzwerkdienste > NTP-Konfiguration*) benötigt zwei Dialogfelder. Im ersten Dialogfeld legen Sie den Start-Modus für xntpd und den abzufragenden Server fest. Wenn xntpd automatisch beim Booten des Systems gestartet werden soll, klicken Sie auf *Jetzt und beim Systemstart*. Geben Sie anschließend die *NTP-Server-Konfiguration* an. Klicken Sie auf *Use Random Server from pool.ntp.org* (Zufallsserver von pool.ntp.org verwenden), wenn Sie keinen lokalen Zeitserver verwenden können, oder auf *Wählen*, um in einem zweites Dialogfeld einen geeigneten Zeitserver für Ihr Netzwerk auszuwählen.

Abbildung 18.1 YaST: NTP-Konfiguration

NTP-Konfiguration

NTP-Daemon automatisch starten

Niemaals

Während des Bootens

NTP-Server-Konfiguration

Zufällig ausgewählte Server von pool.ntp.org verwenden

Adresse

Wählen... ▾

Test

Erweiterte Konfiguration

Verwerfen

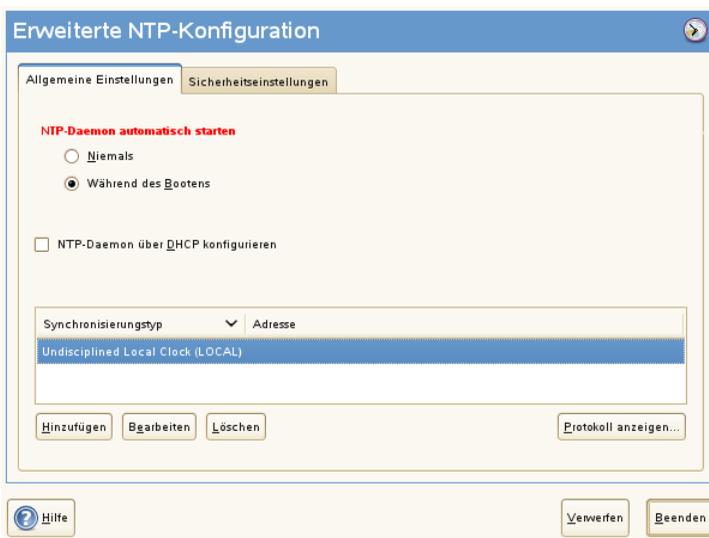
Beenden

Geben Sie in der Pulldown-Liste unter *Auswählen* an, ob die Zeitsynchronisierung anhand eines Zeitservers in Ihrem lokalen Netzwerk (*Lokaler NTP-Server*) oder eines Zeitservers im Internet erfolgen soll, der Ihre Zeitzone verwaltet (*Öffentlicher NTP-Server*). Bei einem lokalen Zeitserver klicken Sie auf *Lookup*, um eine SLP-Abfrage für verfügbare Zeitserver in Ihrem Netzwerk zu starten. Wählen Sie den am besten geeigneten Zeitserver in der Liste der Suchergebnisse aus und schließen Sie das Dialogfeld mit *OK*. Bei einem öffentlichen Zeitserver wählen Sie in der Liste unter *Öffentlicher NTP-Server* Ihr Land (Ihre Zeitzone) sowie einen geeigneten Server aus und schließen das Dialogfeld dann mit *OK*. Im Hauptdialogfeld testen Sie die Verfügbarkeit des ausgewählten Servers mit *Test* und schließen das Dialogfeld mit *Verlassen*.

18.1.2 Erweiterte NTP-Client-Konfiguration

Die erweiterte Konfiguration eines NTP-Clients kann unter *Erweiterte Konfiguration* im Hauptdialogfeld des Moduls *NTP-Konfiguration* aufgerufen werden (siehe [Abbildung 18.1](#), „*YaST: NTP-Konfiguration*“ (S. 332)). Zunächst müssen Sie jedoch einen Start-Modus auswählen wie bei der schnellen Konfiguration beschrieben.

Abbildung 18.2 *Erweiterte NTP-Konfiguration: Allgemeine Einstellungen*



Sie können den NTP-Client entweder manuell oder automatisch konfigurieren, um eine Liste der NTP-Server zu erhalten, die über DHCP in Ihrem Netzwerk verfügbar sind.

Wenn Sie auf *NTP-Daemon über DHCP konfigurieren* klicken, sind die unten erklärten Optionen nicht verfügbar.

Die Server und anderen Zeitquellen für die Abfrage durch den Client sind im unteren Bereich im Karteireiter *Allgemeine Einstellungen* aufgelistet. Bearbeiten Sie diese Liste nach Bedarf mithilfe der Optionen *Hinzufügen*, *Bearbeiten* und *Löschen*. Mit *Protokoll anzeigen* können die Protokolldateien Ihres Clients angezeigt werden.

Klicken Sie auf *Hinzufügen*, um eine neue Quelle für Zeitinformationen hinzuzufügen. Wählen Sie im nachfolgenden Dialogfeld den Quellentyp aus, mit dem die Zeitsynchronisierung vorgenommen werden soll. Mit den zur Verfügung stehenden Optionen können Sie

Server

In einem anderen Dialogfeld können Sie einen NTP-Server auswählen (siehe Beschreibung unter [Abschnitt 18.1.1, „Schnelle NTP-Client-Konfiguration“](#) (S. 332)). Aktivieren Sie *Für initiale Synchronisierung verwenden*, um die Synchronisierung der Zeitinformationen zwischen dem Server und dem Client auszulösen, wenn das System gebootet wird. Unter *Optionen* können Sie weitere Optionen für `xntpd` einstellen.

Mit den *Access Control Options* (Zugriffskontrolloptionen) können Sie die Aktionen einschränken, die der entfernte Computer mit dem Daemon Ihres Computers ausführen kann. Dieses Feld ist nur aktiviert, wenn die Option *Restrict NTP Service to Configured Servers Only* (NTP-Dienst auf konfigurierte Server beschränken) auf dem Karteireiter *Sicherheitseinstellungen* aktiviert ist. Die Optionen entsprechen den `restrict`-Klauseln der Datei `/etc/ntp.conf`. Die Klausel `nomodify notrap noquery` verhindert beispielsweise, dass der Server die NTP-Einstellungen Ihres Computers ändern und die `Trap`-Funktion (eine Fernprotokollierungsfunktion für Ereignisse) Ihres NTP-Daemons verwenden kann. Diese Einschränkungen werden besonders für Server außerhalb Ihrer Kontrolle empfohlen (z. B. im Internet).

Ziehen Sie bezüglich detaillierter Informationen `/usr/share/doc/packages/xntp-doc` zurate (Bestandteil des `xntp-doc`-Pakets).

Peer

Ein Peer ist ein Computer, mit dem eine symmetrische Beziehung eingerichtet wird: Er fungiert sowohl als Zeitserver als auch als Client. Wenn Sie einen Peer im selben Netzwerk anstelle eines Servers verwenden möchten, geben Sie die

Adresse des Systems ein. Der Rest des Dialogfelds ist mit dem Dialogfeld *Server* identisch.

Funkuhr

Wenn eine Funkuhr für die Zeitsynchronisierung in Ihrem System verwendet werden soll, geben Sie Uhrtyp, Gerätezahl, Geräte-Name und weitere Optionen in diesem Dialogfeld ein. Klicken Sie auf *Treiber-Kalibrierung*, um den Treiber genauer einzustellen. Detaillierte Informationen zum Betrieb einer lokalen Funkuhr finden Sie in `/usr/share/doc/packages/xntp-doc/refclock.html`.

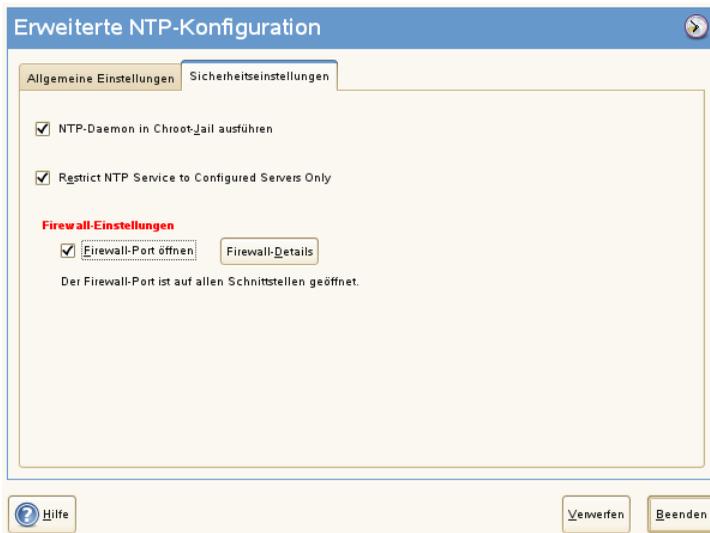
Ausgangs-Broadcast

Zeitinformationen und Abfragen können im Netzwerk auch per Broadcast übermittelt werden. Geben Sie in diesem Dialogfeld die Adresse ein, an die Broadcasts gesendet werden sollen. Die Option für Broadcasts sollte nur aktiviert werden, wenn Ihnen eine zuverlässige Zeitquelle, etwa eine funkgesteuerte Uhr, zur Verfügung steht.

Eingangs-Broadcast

Wenn Ihr Client die entsprechenden Informationen per Broadcast erhalten soll, geben Sie in diesen Feldern die Adresse ein, von der die jeweiligen Pakete akzeptiert werden sollen.

Abbildung 18.3 *Erweiterte NTP-Konfiguration: Sicherheitseinstellungen*



Legen Sie auf dem Karteireiter *Sicherheitseinstellungen* fest, ob `xntpd` in einem "Chroot-Jail" gestartet werden soll. Standardmäßig ist *DHCP-Daemon in Chroot-Jail starten* aktiviert. Hierdurch wird die Sicherheit im Falle eines Angriffs über `xntpd` erhöht, da der Angreifer daran gehindert wird, das gesamte System zu beeinträchtigen.

Die Option *Restrict NTP Service to Configured Servers Only* (NTP-Dienst auf konfigurierte Server beschränken) erhöht die Sicherheit Ihres Systems. Wenn gewählt, verhindert diese Option, dass entfernte Computer die NTP-Einstellungen Ihres Computers anzeigen und ändern und die Trap-Funktion für die Fernprotokollierung von Ereignissen verwenden können. Wenn gewählt, gelten diese Einschränkungen für alle entfernten Computer, es sei denn, Sie überschreiben die Zugriffskontrolloptionen für einzelne Computer in der Liste der Zeitquellen auf dem Karteireiter *Allgemeine Einstellungen*. Allen anderen entfernten Computern wird nur die Abfrage der lokalen Zeit erlaubt.

Aktivieren Sie *Firewall-Port öffnen*, wenn `SuSEfirewall2` aktiviert ist (Standardeinstellung). Wenn Sie den Port geschlossen lassen, können Sie keine Verbindung zum Zeitserver herstellen.

18.2 Konfigurieren von `xntp` im Netzwerk

Die einfachste Art der Verwendung eines Zeitservers im Netzwerk besteht darin, Serverparameter festzulegen. Beispiel: Wenn der Zeitserver `ntp.example.com` über das Netzwerk erreichbar ist, fügen Sie seinen Namen in die Datei `/etc/ntp.conf` ein, indem Sie folgende Zeile einfügen.

```
server ntp.example.com
```

Wenn Sie weitere Zeitserver hinzufügen möchten, fügen Sie zusätzliche Zeilen mit dem Schlüsselwort `server` ein. Nach der Initialisierung von `xntpd` mit dem Befehl `rcntpstart` dauert es etwa eine Stunde, bis die Zeit stabil ist und die Drift-Datei für das Korrigieren der lokalen Computeruhr erstellt wird. Mithilfe der Drift-Datei kann der systematische Fehler der Hardware-Uhr berechnet werden, sobald der Computer eingeschaltet wird. Die Korrektur kommt umgehend zum Einsatz und führt zu einer größeren Stabilität der Systemzeit.

Es gibt zwei Möglichkeiten, den NTP-Mechanismus als Client zu verwenden: Erstens kann der Client in regelmäßigen Abständen die Zeit von einem bekannten Server

abfragen. Wenn viele Clients vorhanden sind, kann dies zu einer starken Auslastung des Servers führen. Zweitens kann der Client auf NTP-Broadcasts warten, die von Broadcast-Zeitservern im Netzwerk gesendet werden. Dieser Ansatz hat den Nachteil, dass die Qualität des Servers unbekannt ist und dass ein Server, der falsche Informationen sendet, zu schwerwiegenden Problemen führen kann.

Wenn die Zeit per Broadcast ermittelt wird, ist der Servername nicht erforderlich. Geben Sie in diesem Fall die Zeile `broadcastclient` in die Konfigurationsdatei `/etc/ntp.conf` ein. Wenn ein oder mehrere bekannte Zeitserver exklusiv verwendet werden sollen, geben Sie die Namen in der Zeile ein, die mit `servers` beginnt.

18.3 Einrichten einer lokalen Referenzuhr

Das Software-Paket `xntp` enthält Treiber für das Verbinden lokaler Referenzuhren. Eine Liste unterstützter Uhren steht im Paket `xntp-doc` in der Datei `/usr/share/doc/packages/xntp-doc/refclock.html` zur Verfügung. Jeder Treiber ist mit einer Nummer verknüpft. In `xntp` wird die eigentliche Konfiguration mit Pseudo-IP-Adressen durchgeführt. Die Uhren werden so in die Datei `/etc/ntp.conf` eingegeben, als ob sie im Netzwerk vorhanden wären. Zu diesem Zweck werden Ihnen spezielle IP-Adressen im Format `127.127.t.u` zugewiesen. Hierbei steht `t` für den Uhrentyp und legt fest, welcher Treiber verwendet wird und `u` steht für die Einheit (unit), die die verwendete Schnittstelle bestimmt.

Im Regelfall verfügen die einzelnen Treiber über spezielle Parameter, die die Konfigurationsdetails beschreiben. Die Datei `/usr/share/doc/packages/xntp-doc/drivers/driverNN.html` (`NN` steht für die Anzahl der Treiber) bietet Informationen zum jeweiligen Uhrentyp. Für die Uhr vom „Typ 8“ (Funkuhr über serielle Schnittstelle) ist ein zusätzlicher Modus erforderlich, der die Uhr genauer angibt. Das Conrad DCF77-Empfängermodul weist beispielsweise Modus 5 auf. Wenn diese Uhr als bevorzugte Referenz verwendet werden soll, geben Sie das Schlüsselwort `prefer` an. Die vollständige `server`-Zeile für ein Conrad DCF77-Empfängermodul sieht folgendermaßen aus:

```
server 127.127.8.0 mode 5 prefer
```

Für andere Uhren gilt dasselbe Schema. Nach der Installation des Pakets `xntp-doc` steht die Dokumentation für `xntp` im Verzeichnis `/usr/share/doc/packages/`

xntp-doc zur Verfügung. Die Datei `/usr/share/doc/packages/xntp-doc/refclock.html` enthält Links zu den Treiberseiten, auf denen die Treiberparameter beschrieben werden.

Arbeiten mit NIS

Sobald mehrere Unix-Systeme in einem Netzwerk auf gemeinsame Ressourcen zugreifen, muss sichergestellt sein, dass alle Benutzer- und Gruppen-IDs auf allen Computern in diesem Netzwerk identisch sind. Das Netzwerk muss für Benutzer transparent sein: unabhängig davon, welchen Rechner sie verwenden, befinden sie sich immer in derselben Umgebung. Dies erreichen Sie über NIS- und NFS-Dienste. NFS dient der Verteilung von Dateisystemen im Netzwerk und wird in [Kapitel 21, Verteilte Nutzung von Dateisystemen mit NFS](#) (S. 385) beschrieben.

NIS (Network Information Service) kann als datenbankähnlicher Dienst verstanden werden, der den netzwerkübergreifenden Zugriff auf den Inhalt der Dateien `/etc/passwd`, `/etc/shadow` und `/etc/group` ermöglicht. NIS kann auch für andere Zwecke eingesetzt werden (beispielsweise, um den Inhalt von Dateien wie `/etc/hosts` oder `/etc/services` verfügbar zu machen). Darauf wird hier jedoch nicht im Detail eingegangen, da dies den Rahmen dieser Einführung sprengen würde. Für NIS wird vielfach synonym der Begriff *YP* (Yellow Pages) verwendet, da es sich bei dem Dienst quasi um die „Gelben Seiten“ des Netzwerks handelt.

19.1 Konfigurieren von NIS-Servern

Zur Verteilung von NIS-Informationen in Netzwerken können Sie entweder einen einzelnen Server (einen *Master*) verwenden, der allen Clients Daten bereitstellt, oder Sie verwenden NIS-Slave-Server, die diese Informationen vom Master anfordern und dann an ihre jeweiligen Clients weiterleiten.

- Um nur einen NIS-Server für Ihr Netzwerk zu konfigurieren, fahren Sie mit [Abschnitt 19.1.1, „Konfigurieren eines NIS-Master-Servers“](#) (S. 340) fort.
- Wenn Ihr NIS-Master-Server seine Daten an Slave-Server exportieren soll, richten Sie den Master-Server ein, wie unter [Abschnitt 19.1.1, „Konfigurieren eines NIS-Master-Servers“](#) (S. 340) beschrieben, und richten Sie die Slave-Server in den Subnetzen ein, wie unter [Abschnitt 19.1.2, „Konfigurieren eines NIS-Slave-Servers“](#) (S. 345) beschrieben.

19.1.1 Konfigurieren eines NIS-Master-Servers

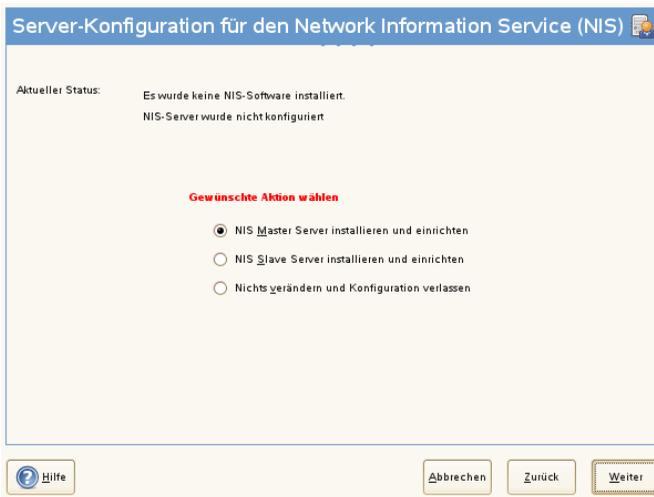
Gehen Sie wie folgt vor, um einen NIS-Master-Server für Ihr Netzwerk zu konfigurieren:

- 1 Starten Sie *YaST > Netzwerkdienste > NIS-Server*.
- 2 Falls Sie nur einen NIS-Server in Ihrem Netzwerk benötigen oder dieser Server als Master für NIS-Slave-Server fungieren soll, wählen Sie *NIS Master Server installieren und einrichten*. YaST installiert die erforderlichen Pakete.

TIPP

Wenn bereits NIS-Serversoftware auf Ihrem Computer installiert ist, klicken Sie auf *NIS Master Server einrichten*, um die Erstellung eines NIS-Master-Servers zu initiieren.

Abbildung 19.1 NIS-Serverkonfiguration



3 Legen Sie die grundlegenden Optionen für das NIS-Setup fest:

3a Geben Sie den NIS-Domännennamen ein.

3b Definieren Sie, ob der Host auch ein NIS-Client sein soll, an dem sich Benutzer anmelden und auf Daten vom NIS-Server zugreifen können, indem Sie *Dieser Rechner ist zugleich NIS-Client* auswählen.

Wählen Sie *Ändern der Passwörter zulassen*, um Benutzern in Ihrem Netzwerk (sowohl lokalen als auch den vom NIS-Server verwalteten Benutzern) das Ändern ihres Passworts auf dem NIS-Server zu ermöglichen (mit dem Befehl `yppasswd`).

Dadurch werden die Optionen *Ändern des GECOS-Eintrags zulassen* und *Ändern der Login-SHELL zulassen* verfügbar. „GECOS“ bedeutet, dass Benutzer mit dem Befehl `ypchfn` auch ihre Namens- und Adresseinstellungen ändern können. „SHELL“ erlaubt Benutzern, mit dem Befehl `ypchsh` ihre Standard-Shell zu ändern, z. B. von `bash` zu `sh`. Die neue Shell muss einer der vordefinierten Einträge in `/etc/shells` sein.

3c Wenn Ihr NIS-Server als Master-Server für NIS-Slave-Server in anderen Subnetzen fungieren soll, wählen Sie *Aktiver Slave-Server für NIS vorhanden*.

Die Option *Schnelle Map-Verteilung* ist nur nützlich in Verbindung mit *Aktive Slave NIS-Server vorhanden*. Dadurch wird die Geschwindigkeit bei der Übertragung von Maps an die Slaves erhöht.

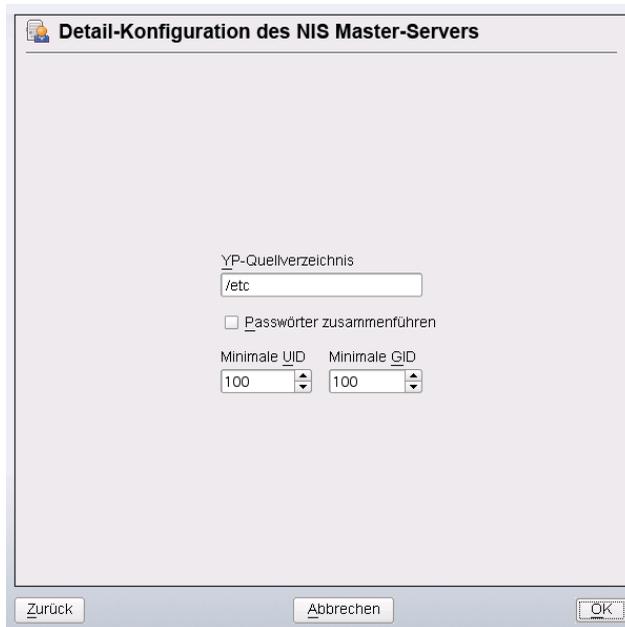
- 3d** Wählen Sie *Firewall-Ports öffnen*, damit YaST die Firewall-Einstellungen für den NIS-Server anpasst.

Abbildung 19.2 *Konfiguration des Masterservers*



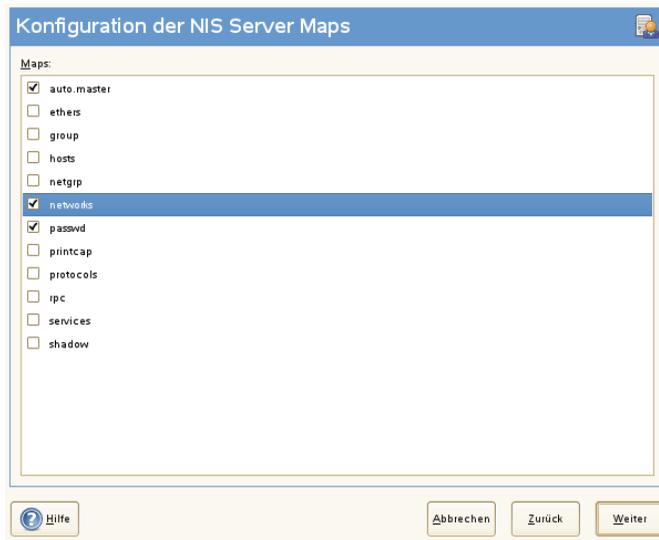
- 3e** Schließen Sie dieses Dialogfeld mit *Weiter* oder klicken Sie auf *Andere globale Einstellungen*, um zusätzliche Einstellungen vorzunehmen. *Andere globale Einstellungen* umfassen das Ändern des Quellverzeichnisses für den NIS-Server (standardmäßig `/etc`). Außerdem können hier Passwörter zusammengeführt werden. Die Einstellung sollte auf *Ja* gesetzt sein, damit die Dateien (`/etc/passwd`, `/etc/shadow` und `/etc/group`) zum Erstellen der Benutzerdatenbank verwendet werden. Legen Sie auch die kleinste Benutzer- und Gruppen-ID fest, die NIS anbieten soll. Klicken Sie auf *OK*, um Ihre Einstellungen zu bestätigen und in das vorherige Fenster zurückzukehren.

Abbildung 19.3 Ändern des Verzeichnisses und Synchronisieren von Dateien für einen NIS-Server



- 4 Wenn Sie zuvor die Option *Aktiver Slave-Server für NIS vorhanden* aktiviert haben, geben Sie die entsprechenden Hostnamen der Slaves ein und klicken Sie auf *Weiter*.
- 5 Werden keine Slave-Server verwendet, wird die Slave-Konfiguration übersprungen und Sie gelangen direkt zum Dialogfeld für die Datenbankkonfiguration. Hier geben Sie die *Maps* an, d. h. die Teildatenbanken, die vom NIS-Server auf den jeweiligen Client übertragen werden sollen. Die hier angezeigten Voreinstellungen sind für die meisten Fälle ausreichend. Schließen Sie das Dialogfeld mit *Weiter*.
- 6 Legen Sie fest, welche Maps (Teildatenbanken) verfügbar sein sollen, und klicken Sie auf *Weiter*, um fortzufahren.

Abbildung 19.4 Konfiguration der NIS Server Maps

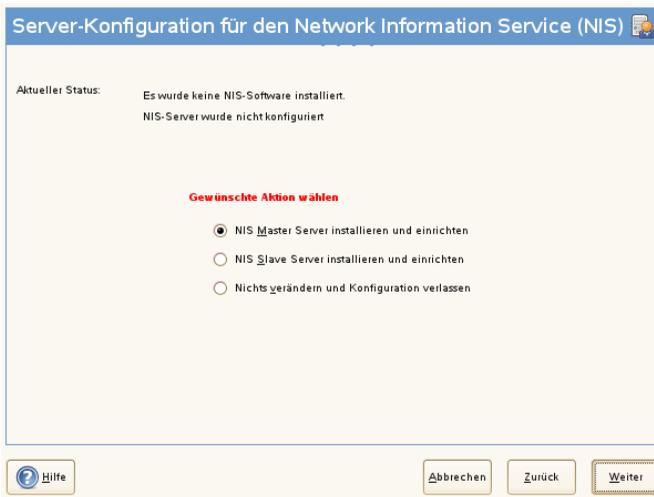


- 7 Geben Sie die Hosts ein, die den NIS-Server abfragen dürfen. Mithilfe der entsprechenden Schaltflächen können Sie Hosts hinzufügen, bearbeiten oder entfernen. Legen Sie fest, aus welchen Netzwerken Anforderungen an den NIS-Server gesendet werden dürfen. Dies ist in der Regel nur das interne Netzwerk. In diesem Fall sollten die beiden folgenden Einträge vorhanden sein:

```
255.0.0.0      127.0.0.0
0.0.0.0        0.0.0.0
```

Der erste Eintrag ermöglicht Verbindungen vom eigenen Host, bei dem es sich um den NIS-Server handelt. Der zweite erlaubt allen Hosts, Anforderungen an den Server zu senden.

Abbildung 19.5 Einrichten von Anforderungsberechtigungen für einen NIS-Server



- 8 Klicken Sie auf *Verlassen*, um die Änderungen zu speichern und das Setup abzuschließen.

19.1.2 Konfigurieren eines NIS-Slave-Servers

Gehen Sie wie folgt vor, um zusätzliche *NIS-Slave-Server* in Ihrem Netzwerk zu konfigurieren:

- 1 Starten Sie *YaST* > *Netzwerkdienste* > *NIS-Server*.
- 2 Wählen Sie *NIS Slave Server installieren und einrichten* und klicken Sie auf *Weiter*.

TIPP

Wenn bereits NIS-Serversoftware auf Ihrem Computer installiert ist, klicken Sie auf *NIS Slave Server einrichten*, um die Erstellung eines NIS-Slave-Servers zu initiieren.

- 3 Vervollständigen Sie das grundlegende Setup Ihres NIS-Slave-Servers:

- 3a** Geben Sie die NIS-Domäne ein.
 - 3b** Geben Sie den Hostnamen oder die IP-Adresse des Master-Servers ein.
 - 3c** Aktivieren Sie *Dieser Rechner ist zugleich NIS-Client*, wenn Sie Benutzeranmeldungen auf diesem Server ermöglichen möchten.
 - 3d** Passen Sie die Firewall-Einstellungen mit *Ports in Firewall öffnen* an.
 - 3e** Klicken Sie auf *Weiter*.
- 4** Geben Sie die Hosts ein, die den NIS-Server abfragen dürfen. Mithilfe der entsprechenden Schaltflächen können Sie Hosts hinzufügen, bearbeiten oder entfernen. Legen Sie fest, aus welchen Netzwerken Anforderungen an den NIS-Server gesendet werden dürfen. Gewöhnlich sind das alle Hosts. In diesem Fall sollten die beiden folgenden Einträge vorhanden sein:

```
255.0.0.0      127.0.0.0
0.0.0.0        0.0.0.0
```

Der erste Eintrag ermöglicht Verbindungen vom eigenen Host, bei dem es sich um den NIS-Server handelt. Der zweite Eintrag ermöglicht allen Hosts, die Zugriff auf das Netzwerk haben, Anforderungen an den Server zu senden.

- 5** Klicken Sie auf *Verlassen*, um die Änderungen zu speichern und das Setup abzuschließen.

19.2 Konfigurieren von NIS-Clients

Verwenden Sie das YaST-Modul *NIS-Client*, um eine Arbeitsstation für den Einsatz von NIS zu konfigurieren. Legen Sie fest, ob der Host eine statische IP-Adresse hat oder ob er eine Adresse vom DHCP-Server erhält. DHCP kann auch die NIS-Domäne und den NIS-Server angeben. Weitere Informationen zu DHCP finden Sie in [Kapitel 17, DHCP](#) (S. 313). Falls eine statische IP-Adresse verwendet wird, geben Sie die NIS-Domäne und den NIS-Server manuell an. Weitere Informationen hierzu finden Sie unter [Abbildung 19.6, „Festlegen der Domäne und Adresse eines NIS-Servers“](#) (S. 347). *Suchen* weist YaST an, in Ihrem gesamten Netzwerk nach einem aktiven NIS-Server zu suchen. Abhängig von der Größe Ihres lokalen Netzwerks kann das ein sehr zeitrau-

bendes Verfahren sein. *Broadcast* verlangt einen NIS-Server im lokalen Netzwerk, wenn der angegebene Server nicht reagiert.

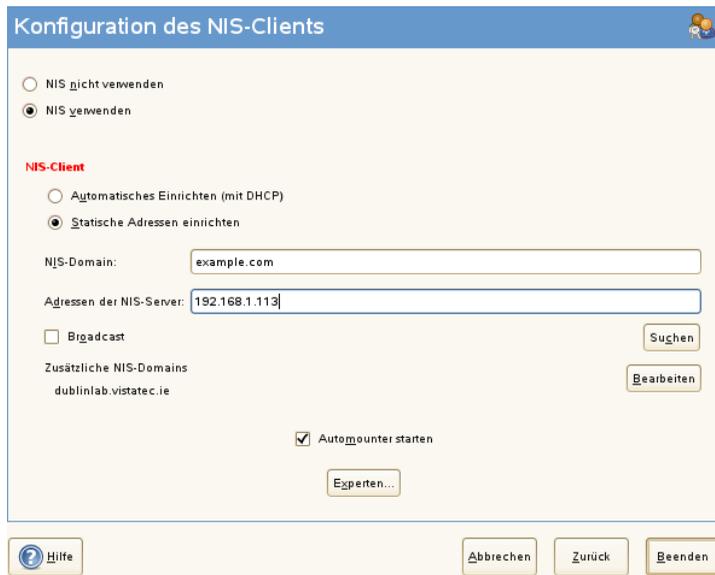
Sie können auch mehrere Server angeben, indem Sie ihre Adressen durch Leerzeichen getrennt unter *Adressen der NIS-Server* angeben.

Abhängig von Ihrer lokalen Installation können Sie auch den Automounter aktivieren. Diese Option installiert bei Bedarf auch zusätzliche Software.

Deaktivieren Sie in den Experteneinstellungen die Option *Entfernten Hosts antworten*, wenn Hosts nicht abfragen dürfen, welchen Server Ihr Client verwendet. Wenn Sie *Fehlerhafter Server* aktivieren, wird der Client für das Empfangen von Antworten von einem Server aktiviert, der über einen nicht berechtigten Port kommuniziert. Weitere Informationen finden Sie auf der man-Seite `manypbind`.

Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *Verlassen*, um sie zu speichern und zum YaST-Kontrollzentrum zurückzukehren.

Abbildung 19.6 Festlegen der Domäne und Adresse eines NIS-Servers



The screenshot shows the 'Konfiguration des NIS-Clients' window. At the top, there are two radio buttons: 'NIS nicht verwenden' (unselected) and 'NIS verwenden' (selected). Below this, under the 'NIS-Client' section, there are two radio buttons: 'Automatisches Einrichten (mit DHCP)' (unselected) and 'Statische Adressen einrichten' (selected). The 'NIS-Domain:' field contains 'example.com'. The 'Adressen der NIS-Server:' field contains '192.168.1.113'. There is a 'Broadcast' checkbox (unselected) and a 'Suchen' button. Below that, the 'Zusätzliche NIS-Domains' section lists 'dublinlab.vistatec.ie' with a 'Bearbeiten' button. At the bottom, there is a checked checkbox for 'Automounter starten' and an 'Experten...' button. The footer contains a 'Hilfe' button, an 'Abbrechen' button, a 'Zurück' button, and a 'Beenden' button.

LDAP – Ein Verzeichnisdienst

20

Bei Lightweight Directory Access Protocol (LDAP) handelt es sich um eine Reihe von Protokollen für den Zugriff auf und die Verwaltung von Datenverzeichnissen. LDAP kann für viele Zwecke, wie Benutzer- und Gruppenverwaltung, Systemkonfigurationsverwaltung und Adressverwaltung eingesetzt werden. Dieses Kapitel enthält die Grundlagen zum Verständnis der Funktionsweise von OpenLDAP und zur Verwaltung von LDAP-Daten mit YaST. Es sind zwar mehrere Implementierungen des LDAP-Protokolls möglich, in diesem Kapitel wird jedoch ausschließlich die OpenLDAP-Implementierung behandelt.

In einer Netzwerkumgebung ist es entscheidend, die wichtigen Informationen strukturiert anzuordnen und schnell zur Verfügung zu stellen. Dies kann mit einem Verzeichnisdienst erreicht werden, der Informationen wie die Gelben Seiten in gut strukturierter und schnell durchsuchbarer Form enthält.

Im Idealfall sind die Daten auf einem zentralen Server in einem Verzeichnis gespeichert, von dem aus sie über ein bestimmtes Protokoll an alle Clients verteilt werden. Die Daten sind so strukturiert, dass zahlreiche Anwendungen darauf zugreifen können. Auf diese Weise ist es nicht erforderlich, für jedes einzelne Kalenderwerkzeug und jeden Email-Client eine eigene Datenbank zu speichern, da auf ein zentrales Repository zugegriffen werden kann. Dadurch wird der Verwaltungsaufwand für die Daten erheblich reduziert. Mithilfe eines offenen und standardisierten Protokolls wie LDAP wird sichergestellt, dass so viele verschiedene Client-Anwendungen wie möglich auf diese Informationen zugreifen können.

In diesem Kontext ist ein Verzeichnis eine Art Datenbank, die für schnelle und effektive Lese- und Suchvorgänge optimiert wurde:

- Damit mehrere gleichzeitige Lesevorgänge möglich sind, ist der Schreibzugriff nur auf eine geringe Anzahl an Aktualisierungen durch den Administrator beschränkt. Herkömmliche Datenbanken sind speziell dafür bestimmt, ein möglichst großes Datenvolumen in kurzer Zeit verarbeiten zu können.
- Da der Schreibzugriff nur eingeschränkt möglich ist, wird ein Verzeichnisdienst zur Verwaltung der statischen Informationen eingesetzt, die sich normalerweise nicht ändern. Daten in einer herkömmlichen Datenbank werden in der Regel häufig geändert (*dynamische* Daten). So werden die Telefonnummern in einem Unternehmensverzeichnis beispielsweise nicht so häufig geändert wie die in der Buchhaltung verwalteten Zahlen.
- Bei der Verwaltung statischer Daten werden die vorhandenen Datengruppen nur selten aktualisiert. Beim Arbeiten mit dynamischen Daten, insbesondere wenn daran Datengruppen wie Bankkonten oder Buchhaltung beteiligt sind, kommt der Datenkonsistenz höchste Priorität zu. Wenn ein Betrag an einer Stelle subtrahiert und an einer anderen Stelle addiert werden soll, müssen beide Vorgänge innerhalb einer *Transaktion* gleichzeitig erfolgen, um das Gleichgewicht des Datenbestandes aufrecht zu erhalten. Diese Art von Transaktionen wird von Datenbanken unterstützt. In Verzeichnissen ist dies jedoch nicht der Fall. Kurzfristige Inkonsistenzen der Daten sind in Verzeichnissen in gewissem Maße akzeptabel.

Das Design eines Verzeichnisdiensts wie LDAP ist nicht für die Unterstützung solcher komplexer Aktualisierungs- und Abfragemechanismen bestimmt. Alle Anwendungen, die auf diesen Dienst zugreifen, müssen ihn schnell und einfach aufrufen können.

20.1 LDAP und NIS

Der Unix-Systemadministrator verwendet für die Namensauflösung und die Datenverteilung in einem Netzwerk in der Regel NIS. Die in den Dateien unter `/etc` und in den Verzeichnissen `group`, `hosts`, `mail`, `netgroup`, `networks`, `passwd`, `printcap`, `protocols`, `rpc` und `services` enthaltenen Konfigurationsdaten werden über Clients im ganzen Netzwerk verteilt. Diese Dateien können ohne größeren Aufwand verwaltet werden, da es sich hierbei um einfache Textdateien handelt. Die Verarbeitung größerer Datenmengen wird aufgrund der fehlenden Strukturierung jedoch immer schwieriger. NIS ist nur für Unix-Plattformen bestimmt. Es eignet sich nicht als Tool zur zentralen Datenadministration in heterogenen Netzwerken.

Im Gegensatz zu NIS ist die Verwendung des LDAP-Diensts nicht auf reine Unix-Netzwerke beschränkt. Windows-Server (ab 2000) unterstützen LDAP als Verzeichnisdienst. Die oben erwähnten Anwendungsaufgaben werden zusätzlich in Nicht-Unix-Systemen unterstützt.

Das LDAP-Prinzip lässt sich auf jede beliebige Datenstruktur anwenden, die zentral verwaltet werden soll. Nachfolgend einige Anwendungsbeispiele:

- Verwendung als Ersatz für den NIS-Dienst
- Mail-Routing (postfix, sendmail)
- Adressbücher für Mail-Clients, wie Mozilla, Evolution und Outlook
- Verwaltung von Zonenbeschreibungen für einen BIND9-Namensserver
- Benutzerauthentifizierung mit Samba in heterogenen Netzwerken

Diese Liste lässt sich erweitern, da LDAP im Gegensatz zu NIS erweiterungsfähig ist. Durch die klar definierte hierarchische Datenstruktur wird die Verwaltung großer Datenmengen erleichtert, da die Daten einfacher durchsucht werden können.

20.2 Struktur eines LDAP-Verzeichnisbaums

Um ein tieferes Hintergrundwissen zur Funktionsweise eines LDAP-Servers und dem Speichern der Daten zu erhalten, ist es wichtig, die Art und Weise zu verstehen, in der Daten auf dem Server organisiert werden, und wie es LDAP ermöglicht wird, schnellen Zugriff auf die benötigten Daten bereitzustellen. Für eine erfolgreiche LDAP-Einrichtung müssen Sie außerdem die grundlegende LDAP-Terminologie kennen. Dieser Abschnitt erläutert das grundlegende Layout eines LDAP-Verzeichnisbaumes und stellt die im LDAP-Kontext verwendete grundlegende Terminologie bereit. Überspringen Sie diesen einführenden Abschnitt, wenn Sie bereits über LDAP-Hintergrundwissen verfügen und nur erfahren möchten, wie eine LDAP-Umgebung in openSUSE eingerichtet wird. Lesen Sie unter [Abschnitt 20.3, „Konfigurieren eines LDAP-Servers mit YaST“](#) (S. 355) bzw. [Abschnitt 20.7, „Manuelles Konfigurieren eines LDAP-Servers“](#) (S. 373) weiter.

Ein LDAP-Verzeichnis weist eine Baumstruktur auf. Alle Einträge (auch "Objekte" genannt) des Verzeichnisses verfügen über eine festgelegte Position innerhalb dieser Hierarchie. Diese Hierarchie wird als *Verzeichnisinformationsbaum* (Directory Information Tree, DIT) bezeichnet. Der vollständige Pfad zum gewünschten Eintrag, durch den der Eintrag eindeutig identifiziert wird, wird als *eindeutiger Name* oder DN (Distinguished Name) bezeichnet. Ein einzelner Knoten im Pfad dieses Eintrags wird *relativer eindeutiger Name* oder RDN (relative distinguished name) genannt. Objekte können im Allgemeinen einem von zwei möglichen Typen zugewiesen werden:

Container

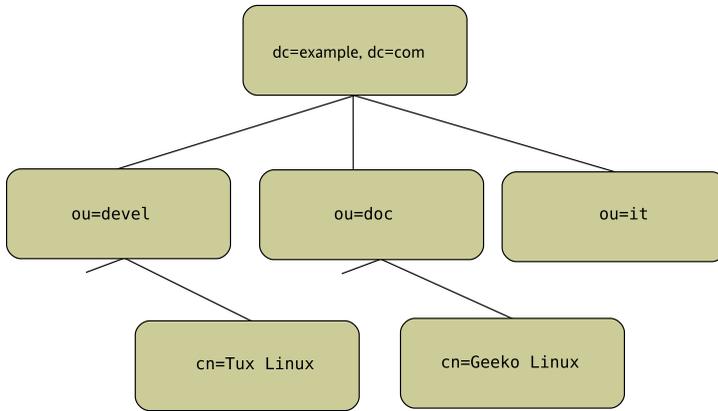
Diese Objekte können wiederum andere Objekte enthalten. Solche Objektklassen sind beispielsweise `root` (das Stammelement des Verzeichnisbaums, das in der Regel nicht vorhanden ist), `c` (Land), `ou` (organisatorische Einheit) und `dc` (Domänenkomponente). Dieses Modell ist mit Verzeichnissen (Ordern) in einem Dateisystem vergleichbar.

Blatt

Diese Objekte befinden sich am Ende einer Verzweigung und verfügen nicht über untergeordnete Objekte. Beispiele: `person`, `InetOrgPerson` oder `groupofNames`.

Auf der obersten Ebene in der Verzeichnishierarchie steht das Stammelement `root`. Hierin können die untergeordneten Elemente `c` (Land), `dc` (Domänenkomponente) oder `o` (Organisation) enthalten sein. Die Bezüge innerhalb eines LDAP-Verzeichnisbaums werden im folgenden Beispiel verdeutlicht, das in **Abbildung 20.1, „Struktur eines LDAP-Verzeichnisses“** (S. 353) gezeigt wird.

Abbildung 20.1 Struktur eines LDAP-Verzeichnisses



Das vollständige Diagramm stellt einen Beispiel-Verzeichnisbaum dar. Die Einträge auf allen drei Ebenen werden dargestellt. Jeder Eintrag entspricht einem Feld im Bild. Der vollständige, gültige *eindeutige Name* für den fiktiven Mitarbeiter `Geeko Linux` lautet in diesem Fall `cn=Geeko Linux, ou=doc, dc=example, dc=com`. Er wird zusammengesetzt, indem dem RDN `cn=Geeko Linux` des DN des vorhergehenden Eintrags `ou=doc, dc=example, dc=com` hinzugefügt wird.

Die Objekttypen, die im DIT gespeichert werden sollen, werden global anhand eines *Schemas* bestimmt. Der Objekttyp wird durch die *Objektklasse* bestimmt. Mit der Objektklasse wird festgelegt, welche Attribute des betreffenden Objekts zugewiesen werden müssen bzw. können. Daher muss ein Schema die Definitionen aller Objektklassen und Attribute enthalten, die im gewünschten Anwendungsszenario verwendet werden. Es gibt einige häufig verwendeten Schemata (siehe RFC 2252 und 2256). Es besteht jedoch die Möglichkeit, benutzerdefinierte Schemata zu erstellen oder mehrere einander ergänzende Schemata zu verwenden, sofern die Umgebung, in der der LDAP-Server verwendet werden soll, dies erfordert.

In **Tabelle 20.1**, „Häufig verwendete Objektklassen und Attribute“ (S. 354) erhalten Sie einen kurzen Überblick über die Objektklassen von `core.schema` und `inetorgperson.schema`, die im Beispiel verwendet werden, und über die erforderlichen Attribute und gültigen Attributswerte.

Tabelle 20.1 Häufig verwendete Objektklassen und Attribute

Object Class	Bedeutung	Beispieleintrag	Obligatorische Attribute
dcObject	<i>domainComponent</i> (Name der Domänenkomponenten)	Beispiel	dc
organizationalUnit	<i>organizationalUnit</i> (organisatorische Einheit)	doc	ou
inetOrgPerson	<i>inetOrgPerson</i> (personenbezogene Daten für das Intranet oder Internet)	Geeko Linux	sn und cn

In **Beispiel 20.1**, „Ausschnitt aus *schema.core*“ (S. 354) wird ein Ausschnitt einer Schemadirektive mit entsprechenden Erklärungen dargestellt (die Zeilen sind für Erklärungszwecke nummeriert).

Beispiel 20.1 Ausschnitt aus *schema.core*

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2     DESC 'RFC2256: organizational unit this object belongs to'
#3     SUP name )
...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5     DESC 'RFC2256: an organizational unit'
#6     SUP top STRUCTURAL
#7     MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory
    $ x121Address $ registeredAddress $ destinationIndicator
    $ preferredDeliveryMethod $ telexNumber
    $ teletexTerminalIdentifier $ telephoneNumber
    $ internationaliSDNNumber $ facsimileTelephoneNumber
    $ street $ postOfficeBox $ postalCode $ postalAddress
    $ physicalDeliveryOfficeName
    $ st $ l $ description) )
...
```

Der Attributtyp *organizationalUnitName* und die entsprechende Objektklasse *organizationalUnit* dienen hier als Beispiel. Zeile 1 enthält den Namen des Attributs, den eindeutigen OID (*Object Identifier*) (numerisch) und die Abkürzung des Attributs.

Zeile 2 enthält eine kurze, mit `DESC` gekennzeichnete, Beschreibung des Attributs. Hier wird der entsprechende RFC, auf dem die Definition basiert, erwähnt. Der Ausdruck `SUP` in Zeile 3 weist auf einen untergeordneten Attributtyp an, dem das Attribut angehört.

Die Definition der Objektklasse `organizationalUnit` beginnt in Zeile 4 wie die Definition des Attributs mit einem OID und dem Namen der Objektklasse. Zeile 5 enthält eine kurze Beschreibung der Objektklasse. In Zeile 6 mit dem Eintrag `SUP top` wird angegeben, dass diese Objektklasse keiner anderen Objektklasse untergeordnet ist. In Zeile 7 werden, mit `MUST` beginnend, alle Attributtypen aufgeführt, die in Verbindung mit einem Objekt vom Typ `organizationalUnit` verwendet werden müssen. In der mit `MAY` beginnenden Zeile 8 werden die Attribute aufgeführt, die im Zusammenhang mit dieser Objektklasse zulässig sind.

Eine sehr gute Einführung in die Verwendung von Schemata finden Sie in der Dokumentation zu OpenLDAP. Wenn Sie OpenLDAP installiert haben, ist sie unter `/usr/share/doc/packages/openldap2/admin-guide/index.html` zu finden.

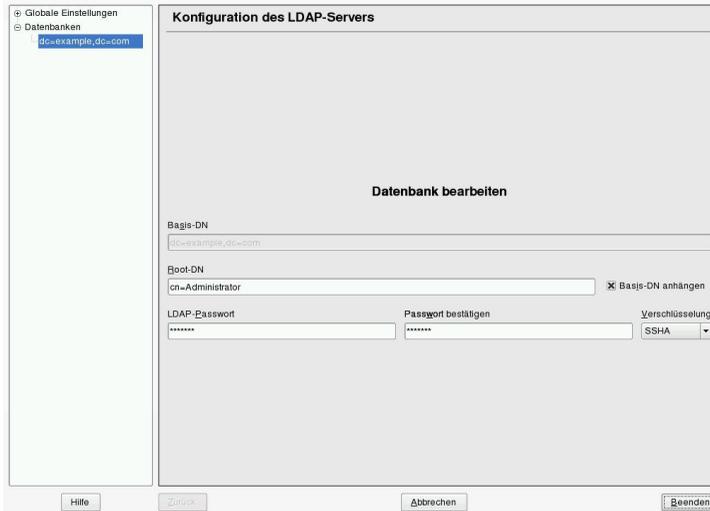
20.3 Konfigurieren eines LDAP-Servers mit YaST

Verwenden Sie YaST zum Einrichten eines LDAP-Servers. Typische Einsatzbereiche für LDAP-Server sind die Verwaltung von Benutzerkontodaten und die Konfiguration von Mail-, DNS- und DHCP-Servern.

TIPP

Vergewissern Sie sich, dass das Paket `yast2-ldap-server` sowie die Pakete, von denen es abhängt, installiert sind.

Abbildung 20.2 *YaST-LDAP-Server-Konfiguration*



Zum Einrichten eines LDAP-Servers für Benutzerkontodaten gehen Sie wie folgt vor:

- 1 Melden Sie sich als `root` an.
- 2 Starten Sie YaST und wählen Sie *Netzwerkdienste > LDAP-Server*.
- 3 Legen Sie fest, dass LDAP beim Systemstart gestartet wird.
- 4 Wenn der LDAP-Server seine Dienste per SLP ankündigt, aktivieren Sie *Register at an SLP Daemon* (Bei einem SLP-Daemon registrieren).
- 5 Wählen Sie *Konfigurieren*, um die *Allgemeinen Einstellungen* und die *Datenbanken* zu konfigurieren.

Gehen Sie zum Konfigurieren der *Globalen Einstellungen* Ihres LDAP-Servers wie folgt vor:

- 1 Akzeptieren oder Verändern Sie die Schemadateien in der Server-Konfiguration, indem Sie links im Dialogfeld *Schemadateien* wählen. Die Standardauswahl an Schemadateien wird auf den Server angewendet und bietet eine Quelle für YaST-Benutzerkontodaten.

- 2 Mit der Option *Protokollebeneinstellungen* konfigurieren Sie die Protokollaktivität (Ausführlichkeit) des LDAP-Servers. Aktivieren oder deaktivieren Sie in der vordefinierten Liste die Protokolloptionen nach Ihren Wünschen. Je mehr Optionen aktiviert sind, desto größer werden Ihre Protokolldateien.
- 3 Legen Sie unter *Allow-Einstellungen* die Verbindungsarten fest, die der LDAP-Server zulassen sollte. Folgende Möglichkeiten stehen zur Auswahl:

LDAPv2-Bind-Anforderungen

Diese Option aktiviert Verbindungsanforderungen (Bind-Anforderungen) von Clients mit der vorigen Version des Protokolls (LDAPv2).

Anonyme Verbindung, wenn Berechtigungen nicht leer sind

In der Regel weist der LDAP-Server alle Authentifizierungsversuche mit leeren Berechtigungen (DN oder Passwort) zurück. Wenn Sie diese Option aktivieren, wird eine anonyme Verbindung mit Passwort, aber ohne DN möglich.

Nicht authentifizierte Verbindung, wenn DN nicht leer ist

Wenn Sie diese Option aktivieren, kann eine Verbindung ohne Authentifizierung (anonym) mit einem DN, aber ohne Passwort erfolgen.

Nicht authentifizierte Aktualisierungsoptionen zur Verarbeitung

Durch Aktivieren dieser Option können nicht authentifizierte (anonyme) Aktualisierungsvorgänge ausgeführt werden. Der Zugriff ist gemäß ACLs und anderen Regeln beschränkt (siehe [Abschnitt 20.7.1](#), „**Globale Direktiven in slapd.conf**“ (S. 374)).

- 4 Zum Konfigurieren der sicheren Kommunikation von Client und Server fahren Sie mit *TLS-Einstellungen* fort:

4a Setzen Sie *TLS Active* auf *Yes*, um die TLS und SSL-Verschlüsselung der Client/Server-Kommunikation zu aktivieren.

4b Klicken Sie auf *Zertifikat auswählen* und bestimmen Sie, wie ein gültiges Zertifikat erhalten wird. Wählen Sie *Zertifikat importieren* (Zertifikat wird von externer Quelle importiert) oder *Allgemeines Server-Zertifikat verwenden* (das bei der Installation erstellte Zertifikat wird verwendet).

- Wenn Sie ein Zertifikat importieren möchten, werden Sie von YaST aufgefordert, den genauen Pfad zum Standort anzugeben.

- Wenn Sie sich für das gemeinsame Serverzertifikat entschieden haben und dieses während der Installation nicht erstellt wurde, wird es anschließend erstellt.

Gehen Sie zum Konfigurieren der Datenbanken Ihres LDAP-Servers wie folgt vor:

- 1** Wählen Sie die Option *Datenbanken* links im Dialogfeld.
- 2** Klicken Sie auf *Datenbanken hinzufügen*, um die neue Datenbank hinzuzufügen.
- 3** Geben Sie die erforderlichen Daten ein:

Basis-DN

Geben Sie den Basis-DN Ihres LDAP-Servers an.

Root-DN

Geben Sie den DN des verantwortlichen Server-Administrators an. Wenn Sie die Option *Basis-DN anhängen* aktivieren, müssen Sie nur den `cn` des Administrators eingeben. Das System macht die restlichen Angaben automatisch.

LDAP-Passwort

Geben Sie das Passwort für den Datenbankadministrator ein.

Verschlüsselung

Legen Sie den Verschlüsselungsalgorithmus zum Sichern des Passworts für den Root-DN fest. Wählen Sie *crypt*, *sm5*, *sha* oder *sha*. Im Dialogfeld ist auch die Option *plain* verfügbar, um die Verwendung von reinen Textpasswörtern zu ermöglichen. Aus Sicherheitsgründen wird diese Option jedoch nicht empfohlen. Wählen Sie *OK*, um Ihre Einstellungen zu bestätigen und zum vorigen Dialogfeld zurückzukehren.

- 4** Aktivieren Sie die Durchsetzung der Passwortrichtlinien, um Ihrem LDAP-Server zusätzliche Sicherheit zur Verfügung zu stellen:
 - 4a** Aktivieren Sie *Einstellungen für Passwortrichtlinien*, um eine Passwortrichtlinie angeben zu können.

- 4b Aktivieren Sie *Hash-Vorgang für unverschlüsselte Passwörter*, damit hinzugefügte oder bearbeitete unverschlüsselte Passwörter vor dem Schreiben in die Datenbank verschlüsselt werden.
- 4c Die Option *Status "Konto gesperrt" offenlegen* stellt eine aussagekräftige Fehlermeldung zur Verfügung, um Anforderungen an gesperrte Konten zu binden.

WARNUNG: Gesperrte Konten in sicherheitssensitiven Umgebungen

Verwenden Sie die Option *Status "Konto gesperrt" offenlegen* nicht, wenn Ihre Umgebung für Sicherheitsprobleme anfällig ist. Die Fehlermeldung für „Gesperrtes Konto“ stellt sicherheitsrelevante Informationen bereit, die von einem potenziellen Angreifer ausgenutzt werden können.

- 4d Geben Sie den DN des Standard-Richtlinienobjekts ein. Um ein DN zu verwenden, der nicht von YaST vorgeschlagen wurde, geben Sie Ihre Auswahl an. Übernehmen Sie andernfalls die Standardeinstellung.

- 5 Schließen Sie die Datenbankkonfiguration ab, indem Sie auf *Verlassen* klicken.

Wenn Sie keine Passwortrichtlinien festgelegt haben, kann Ihr Server an diesem Punkt ausgeführt werden. Wenn Sie Passwortrichtlinien aktivieren möchten, fahren Sie mit der Konfiguration der Passwortrichtlinien fort. Wenn Sie ein Passwortrichtlinienobjekt auswählen, das noch nicht vorhanden ist, wird es von YaST erstellt:

- 1 Geben Sie das LDAP-Serverpasswort ein.
- 2 Konfigurieren Sie die Passwortänderungsrichtlinien:
 - 2a Legen Sie fest, wie viele Passwörter in der Password-History gespeichert werden sollen. Gespeicherte Passwörter können von Benutzern nicht wiederverwendet werden.
 - 2b Legen Sie fest, ob Benutzer ihre Passwörter ändern können und ob die Passwörter nach einem Zurücksetzen durch den Administrator geändert werden müssen. Optional kann das alte Passwort bei Passwortänderungen angefragt werden.

2c Legen Sie fest, ob und in welchem Ausmaß die Qualität von Passwörtern geprüft werden muss. Legen Sie fest, wie viele Zeichen ein gültiges Passwort umfassen muss. Wenn Sie die Option *Nicht überprüfbare Passwörter akzeptieren* aktivieren, können Benutzer verschlüsselte Passwörter verwenden auch wenn keine Überprüfung der Qualität ausgeführt werden kann. Wenn Sie die Option *Nur überprüfte Passwörter akzeptieren* aktivieren, werden nur die Passwörter als gültig akzeptiert, die die Qualitätstests bestehen.

3 Konfigurieren Sie die Passwortablaufrichtlinien:

3a Legen Sie die mindestens einzuhaltende Passwortdauer (die Zeit, die zwischen zwei gültigen Passwortänderungen ablaufen muss) und die maximale Passwortdauer fest.

3b Legen Sie fest, wie viel Zeit zwischen der Warnmeldung zu einem ablaufenden Passwort und dem eigentlichen Passwortablauf liegen soll.

3c Legen Sie für ein abgelaufenes Passwort die Verlängerungsfrist fest, nach der das Passwort endgültig abläuft.

4 Konfigurieren Sie die Sperrrichtlinien:

4a Aktivieren Sie die Passwortsperrung.

4b Legen Sie fest, nach wie vielen Bindungsfehlern eine Passwortsperrung ausgelöst werden soll.

4c Legen Sie die Dauer der Passwortsperrung fest.

4d Legen Sie fest, wie lange Passwortfehler im Cache bleiben, bevor sie gelöscht werden.

5 Wenden Sie Ihre Einstellungen zu den Passwortrichtlinien mit *OK* an.

Zum Bearbeiten einer vorher erstellten Datenbank wählen Sie Ihren Basis-DN links im Baum aus. Im rechten Teil des Fensters zeigt YaST ein Dialogfeld an, das weitgehend dem zum Erstellen einer neuen Datenbank entspricht. Allerdings ist der grundlegende DN-Eintrag grau abgeblendet und kann nicht bearbeitet werden.

Nach dem Beenden der LDAP-Serverkonfiguration mit *Verlassen* können Sie mit einer grundlegenden Arbeitskonfiguration für Ihren LDAP-Server beginnen. Wenn Sie die Einrichtung noch genauer abstimmen möchten, bearbeiten Sie die Datei `/etc/openldap/slapd.conf` entsprechend und starten den Server neu.

20.4 Konfigurieren eines LDAP-Client mit YaST

YaST enthält ein Modul zum Einrichten der LDAP-basierten Benutzerverwaltung. Wenn Sie diese Funktion bei der Installation nicht aktiviert haben, starten Sie das Modul, indem Sie *Netzwerkdienste > LDAP-Client* wählen. YaST aktiviert alle PAM- und NSS-bezogenen Änderungen, die für LDAP erforderlich sind, und installiert die benötigten Dateien. Verbinden Sie einfach Client und Server miteinander und lassen Sie YaST Benutzer über LDAP verwalten. Das grundlegende Setup wird in [Abschnitt 20.4.1, „Konfigurieren der grundlegenden Einstellungen“](#) (S. 361) beschrieben.

Verwenden Sie für die weitere Konfiguration der YaST-Gruppe und der Benutzerkonfigurationsmodule den YaST-LDAP-Client. Dies beinhaltet die Änderung der Standardeinstellungen für neue Benutzer und Gruppen und der Anzahl und Art von Attributen, die einem Benutzer bzw. einer Gruppe zugewiesen sind. Mit der LDAP-Benutzerverwaltung können Sie Benutzern und Gruppen mehrere und verschiedene Attribute zuweisen als bei herkömmlichen Lösungen zur Gruppen- oder Benutzerverwaltung. Die Konfiguration eines solchen Servers wird in [Abschnitt 20.4.2, „Konfigurieren der YaST-Gruppe und der Benutzerverwaltungsmodule“](#) (S. 366) beschrieben.

20.4.1 Konfigurieren der grundlegenden Einstellungen

Das Dialogfeld für die grundlegende Konfiguration des LDAP-Clients ([Abbildung 20.3, „YaST: Konfiguration des LDAP-Client“](#) (S. 362)) wird während der Installation geöffnet, wenn Sie die LDAP-Benutzerverwaltung oder im YaST-Kontrollzentrum des installierten Systems *Netzwerkdienste > LDAP-Client* auswählen.

Abbildung 20.3 YaST: Konfiguration des LDAP-Client

The screenshot shows the 'Konfiguration des LDAP-Clients' window. It is divided into two main sections: 'Benutzerauthentifikation' and 'LDAP-Client'. In the 'Benutzerauthentifikation' section, there are three radio buttons: 'LDAP nicht verwenden', 'LDAP verwenden' (which is selected), and 'LDAP verwenden, jedoch Anmeldungen deaktivieren'. The 'LDAP-Client' section contains a text input field for 'Adressen von LDAP-Servern' with the value '127.0.0.1' and a 'Suchen' button. Below it is another text input field for 'LDAP base DN' with the value 'dc=example,dc=com' and a 'DN holen' button. There are two checkboxes: 'LDAP TLS/SSL' (checked) and 'LDAP Version 2' (unchecked). At the bottom of the main configuration area, there is a checkbox for 'Automounter starten' and a button for 'Erweiterte Konfiguration...'. The window has a title bar with a close button and a footer with 'Zurück', 'Abbrechen', and 'Beenden' buttons.

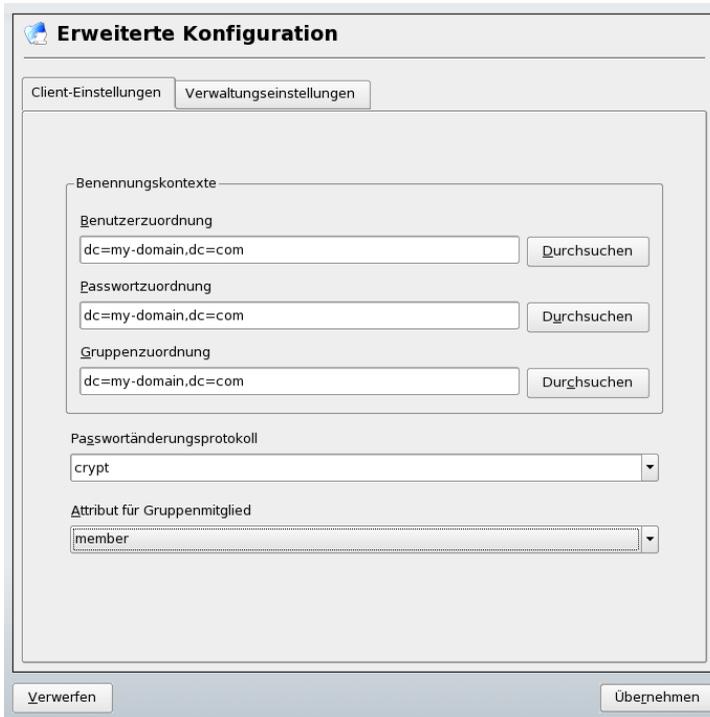
Gehen Sie wie folgt vor, um die Benutzer Ihres Computers bei einem OpenLDAP-Server zu authentifizieren und die Benutzerverwaltung über OpenLDAP zu aktivieren:

- 1 Klicken Sie zum Aktivieren von LDAP auf *LDAP verwenden*. Wählen Sie *LDAP verwenden, jedoch Anmeldungen deaktivieren* aus, wenn LDAP für die Authentifizierung verwendet werden soll, Sie jedoch verhindern möchten, dass sich Benutzer bei diesem Client anmelden.
- 2 Geben Sie die IP-Adresse des zu verwendenden LDAP-Servers ein.
- 3 Geben Sie den *LDAP Base DN* ein, um die Suchbasis auf dem LDAP-Server auszuwählen. Wenn Sie den Basis-DN automatisch abrufen möchten, klicken Sie auf *DN holen*. YaST prüft dann, ob eine oder mehrere LDAP-Datenbanken an der oben angegebenen Serveradresse vorhanden sind. Wählen Sie den geeigneten "Base DN" aus den Suchergebnissen, die YaST liefert.
- 4 Wenn eine durch TLS oder SSL geschützte Kommunikation mit dem Server erforderlich ist, wählen Sie *LDAP TLS/SSL*.

- 5 Falls auf dem LDAP-Server noch LDAPv2 verwendet wird, muss die Verwendung dieser Protokollversion durch Auswahl von *LDAP Version 2* ausdrücklich aktiviert werden.
- 6 Wählen Sie *Automounter starten* aus, um die entfernten Verzeichnisse, wie beispielsweise ein entfernt verwaltetes */home*-Verzeichnis auf dem Client einzuhängen.
- 7 Aktivieren Sie die Option *Home-Verzeichnis bei Anmeldung erstellen*, um beim ersten Anmelden des Benutzers automatisch ein Home-Verzeichnis zu erstellen.
- 8 Klicken Sie zum Anwenden der Einstellungen auf *Verlassen*.

Wenn Sie als Administrator Daten auf einem Server ändern möchten, klicken Sie auf *Erweiterte Konfiguration*. Das folgende Dialogfeld verfügt über zwei Registerkarten. Weitere Informationen hierzu finden Sie unter **Abbildung 20.4, „YaST: Erweiterte Konfiguration“** (S. 364).

Abbildung 20.4 YaST: Erweiterte Konfiguration



- 1** Passen Sie auf der Karteireiter *Client-Einstellungen* die folgenden Einstellungen je nach Bedarf an:
 - 1a** Wenn sich die Suchbasis für Benutzer, Passwörter und Gruppen von der im *LDAP Base DN* angegebenen globalen Suchbasis unterscheidet, geben Sie diese anderen Benennungskontexte unter *Benutzerzuordnung*, *Passwortzuordnung* und *Gruppenzuordnung* ein.
 - 1b** Geben Sie das Passwortänderungsprotokoll an. Die Standardmethode, die bei Passwortänderungen verwendet wird, lautet `crypt`. Dies bedeutet, dass mit `crypt` erstellte Passwort-Hashes verwendet werden. Detaillierte Informationen zu dieser und anderen Optionen finden Sie auf der Manualpage `pam_ldap`.
 - 1c** Geben Sie die LDAP-Gruppe an, die mit *Attribut für Gruppenmitglied* verwendet werden soll. Der Standardwert ist `member`.

2 Passen Sie unter *Verwaltungseinstellungen* folgende Einstellungen an:

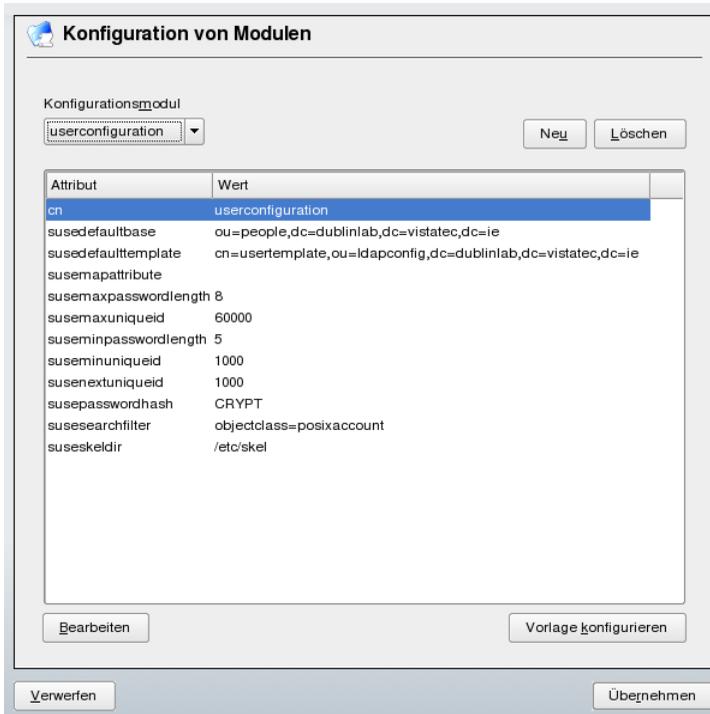
- 2a** Legen Sie die Basis zum Speichern der Benutzerverwaltungsdaten mit *Konfigurations-Base DN* fest.
- 2b** Geben Sie die entsprechenden Werte für *Administrator-DN* ein. Dieser DN muss dem in `/etc/openldap/slapd.conf` angegebenen Wert für `rootdn` entsprechen, damit dieser spezielle Benutzer die auf einem LDAP-Server gespeicherten Daten bearbeiten kann. Geben Sie den vollen DN ein (z. B. `cn=Administrator,dc=example,dc=com`) oder aktivieren Sie *Basis-DN anhängen*, damit der Basis-DN automatisch angehängt wird, wenn Sie `cn=Administrator` eingeben.
- 2c** Aktivieren Sie die Option *Standardkonfigurationsobjekte erzeugen*, um die Standardkonfigurationsobjekte auf dem Server zu erstellen und so die Benutzerverwaltung über LDAP zu ermöglichen.
- 2d** Wenn der Client-Computer als Dateiserver für die Home-Verzeichnisse in Ihrem Netzwerk fungieren soll, aktivieren Sie *Home-Verzeichnisse auf diesem Computer*.
- 2e** Im Abschnitt *Passwortrichtlinie* können Sie die zu verwendenden Einstellungen für die Passwortrichtlinie wählen, hinzufügen, löschen oder ändern. Die Konfiguration der Passwortrichtlinien mit YaST gehört zur Einrichtung des LDAP-Servers.
- 2f** Klicken Sie zum Verlassen der Option *Erweiterte Konfiguration* auf *OK* und anschließend zum Zuweisen der Einstellungen auf *Beenden*.

Mit *Einstellungen für die Benutzerverwaltung konfigurieren* bearbeiten Sie Einträge auf dem LDAP-Server. Der Zugriff auf die Konfigurationsmodule auf dem Server wird anschließend entsprechend den auf dem Server gespeicherten ACLs und ACIs gewährt. Befolgen Sie die in **Abschnitt 20.4.2, „Konfigurieren der YaST-Gruppe und der Benutzerverwaltungsmodule“** (S. 366) beschriebenen Schritte.

20.4.2 Konfigurieren der YaST-Gruppe und der Benutzerverwaltungsmodule

Verwenden Sie den YaST-LDAP-Client, um die YaST-Module für die Benutzer- und Gruppenverwaltung anzupassen und sie nach Bedarf zu erweitern. Definieren Sie die Vorlagen mit Standardwerten für die einzelnen Attribute, um die Datenregistrierung zu vereinfachen. Die hier vorgenommenen Voreinstellungen werden als LDAP-Objekte im LDAP-Verzeichnis gespeichert. Die Registrierung von Benutzerdaten erfolgt weiterhin über reguläre YaST-Module für die Benutzer- und Gruppenverwaltung. Die registrierten Daten werden als LDAP-Objekte auf dem Server gespeichert.

Abbildung 20.5 YaST: Modulkonfiguration



Im Dialogfeld für die Modulkonfiguration (**Abbildung 20.5**, „YaST: Modulkonfiguration“ (S. 366)) können Sie neue Module erstellen, vorhandene Konfigurationsmodule auswählen und ändern sowie Vorlagen für solche Module entwerfen und ändern.

Zum Erstellen eines neuen Konfigurationsmoduls gehen Sie wie folgt vor:

- 1** Klicken Sie in *Konfiguration des LDAP-Clients* auf *Erweiterte Konfiguration* und öffnen Sie anschließend den Karteireiter *Verwaltungseinstellungen*. Klicken Sie auf *Einstellungen für Benutzerverwaltung konfigurieren* und geben Sie die Berechtigungen für den LDAP-Server ein.
- 2** Klicken Sie auf *Neu* und wählen Sie den gewünschten Modultyp aus. Wählen Sie für ein Benutzerkonfigurationsmodul `suseuserconfiguration` und für eine Gruppenkonfiguration `susegroupconfiguration` aus.
- 3** Legen Sie einen Namen für die neue Vorlage fest. In der Inhaltsansicht wird dann eine Tabelle mit allen in diesem Modul zulässigen Attributen und den entsprechenden zugewiesenen Werten angezeigt. Neben allen festgelegten Attributen enthält die Liste auch alle anderen im aktuellen Schema zulässigen jedoch momentan nicht verwendeten Attribute.
- 4** Akzeptieren Sie die voreingestellten Werte oder passen Sie die Standardwerte an, die in der Gruppen- und Benutzerkonfiguration verwendet werden sollen, indem Sie *Bearbeiten* wählen und den neuen Wert eingeben. Ein Modul können Sie umbenennen, indem Sie einfach das Attribut `cn` des Moduls ändern. Durch Klicken auf *Löschen* wird das ausgewählte Modul gelöscht.
- 5** Mit *OK* fügen Sie das neue Modul dem Auswahlménü hinzu.

Mit den YaST-Modulen für die Gruppen- und Benutzerverwaltung werden Vorlagen mit sinnvollen Standardwerten eingebettet. Zum Bearbeiten einer Vorlage für ein Konfigurationsmodul führen Sie folgende Schritte aus:

- 1** Klicken Sie im Dialogfeld *Konfiguration von Modulen* auf *Vorlage konfigurieren*.
- 2** Legen Sie die Werte der allgemeinen dieser Vorlage zugewiesenen Attribute gemäß Ihren Anforderungen fest oder lassen Sie einige nicht benötigte Attribute leer. Leere Attribute werden auf dem LDAP-Server gelöscht.
- 3** Ändern, löschen oder fügen Sie neue Standardwerte für neue Objekte hinzu (Benutzer- oder Gruppenkonfigurationsobjekte im LDAP-Baum).

Abbildung 20.6 YaST Konfiguration einer Objektvorlage

Attribut	Wert
cn	grouptemplate
susenamingattribute	cn
suseplugin	UsersPluginLDAPAll

Bearbeiten

Standardwerte für neue Objekte

Objektattribut	Standardwert
businesscategory	/home/%uid
loginshell	/bin/bash

Hinzufügen Bearbeiten Löschen

Verwerfen Übernehmen

Verbinden Sie die Vorlage mit dem entsprechenden Modul, indem Sie den Wert des Attributs `susedefaulttemplate` für das Modul auf den DN der angepassten Vorlage setzen.

TIPP

Die Standardwerte für ein Attribut können anhand von anderen Attributen mithilfe einer Variablen anstelle eines absoluten Werts erstellt werden. Wenn Sie beispielsweise einen neuen Benutzer erstellen, wird `cn=%sn %givenName` automatisch anhand der Attributwerte für `sn` und `givenName` erstellt.

Nachdem alle Module und Vorlagen richtig konfiguriert wurden und zum Ausführen bereit sind, können neue Gruppen und Benutzer wie gewohnt mit YaST registriert werden.

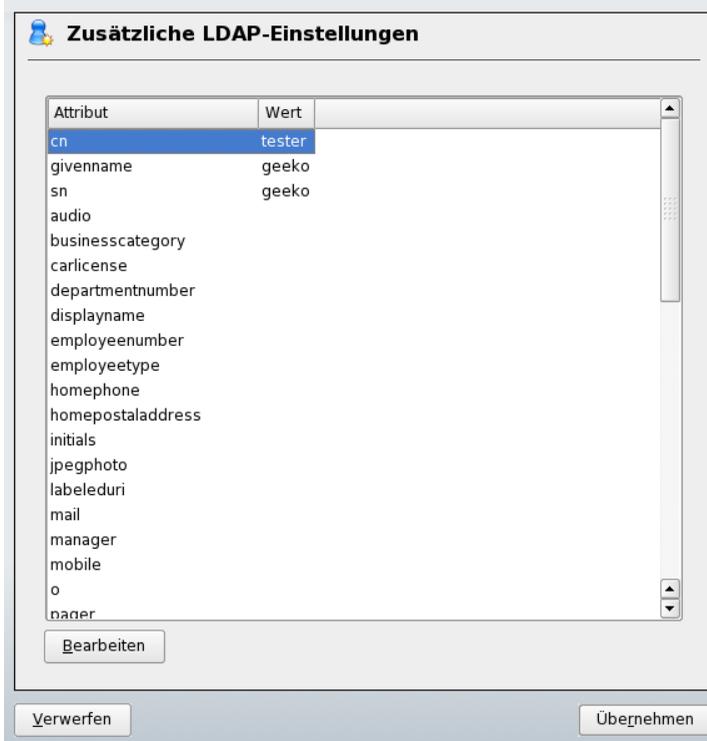
20.5 Konfigurieren von LDAP-Benutzern und -Gruppen in YaST

Die tatsächliche Registrierung der Benutzer- und Gruppendaten weicht nur geringfügig von dem Vorgang ohne Verwendung von LDAP ab. Die folgenden kurzen Anweisungen betreffen die Benutzerverwaltung. Das Verfahren für die Gruppenverwaltung entspricht dieser Vorgehensweise.

- 1 Greifen Sie auf die YaST-Benutzerverwaltung mit *Sicherheit und Benutzer > Verwaltung von Benutzern und Gruppen* zu.
- 2 Mit *Filter festlegen* können Sie die Anzeige der Benutzer auf LDAP-Benutzer beschränken und das Passwort für "Root-DN" eingeben.
- 3 Klicken Sie auf *Hinzufügen* und geben Sie die Konfiguration für einen neuen Benutzer ein. Daraufhin wird ein Dialogfeld mit vier Registerkarten geöffnet:
 - 3a Geben Sie auf der Karteireiter *Benutzerdaten* den Benutzernamen, die Anmeldeinformationen und das Passwort an.
 - 3b Wählen Sie die Karteireiter *Details* aus, um die Gruppenmitgliedschaft, die Anmelde-Shell und das Home-Verzeichnis für den neuen Benutzer anzugeben. Falls erforderlich, ändern Sie den Standardwert entsprechend Ihren Anforderungen. Die Standardwerte und die Passworteinstellungen können mit den in [Abschnitt 20.4.2, „Konfigurieren der YaST-Gruppe und der Benutzerverwaltungsmodule“](#) (S. 366) beschriebenen Schritten definiert werden.
 - 3c Ändern oder akzeptieren Sie die standardmäßigen *Passworteinstellungen*.
 - 3d Rufen Sie die Karteireiter *Plug-Ins* auf, wählen Sie das LDAP-Plugin und klicken Sie zum Konfigurieren zusätzlicher LDAP-Attribute für den neuen Benutzer auf *Starten* (siehe [Abbildung 20.7, „YaST: Zusätzliche LDAP-Einstellungen“](#) (S. 370)).

- 4 Klicken Sie zum Zuweisen der Einstellungen und zum Beenden der Benutzerkonfiguration auf *OK*.

Abbildung 20.7 *YaST: Zusätzliche LDAP-Einstellungen*



Im ersten Eingabeformular der Benutzerverwaltung stehen *LDAP-Optionen* zur Verfügung. Hier haben Sie die Möglichkeit, LDAP-Suchfilter auf die Gruppe der verfügbaren Benutzer anzuwenden oder das Modul zur Konfiguration von LDAP-Benutzern und -Gruppen durch die Auswahl von *Verwaltung von Benutzern und Gruppen* aufzurufen.

20.6 Navigieren in der LDAP-Verzeichnisstruktur

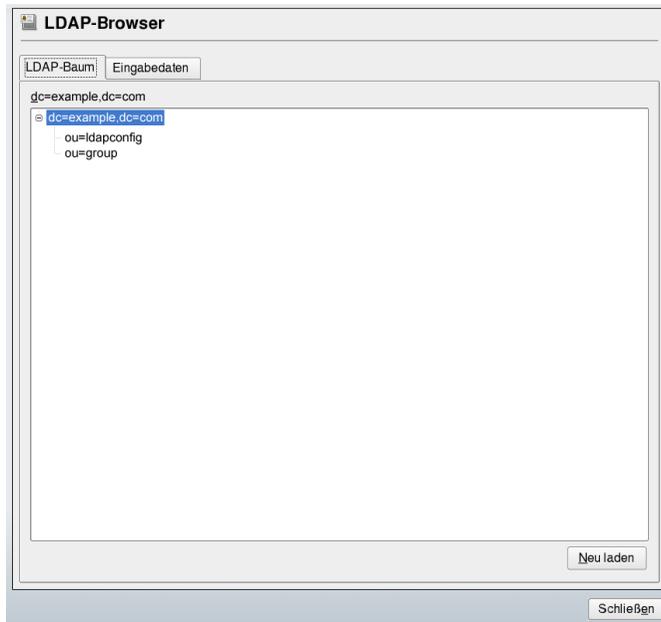
Um mühelos in der LDAP-Verzeichnisstruktur und ihren Einträgen zu navigieren, verwenden Sie den YaST-LDAP-Browser:

- 1 Melden Sie sich als `root` an.
- 2 Starten Sie *YaST > Netzwerkdienste > LDAP-Browser*.
- 3 Geben Sie die Adresse des LDAP-Servers, den AdministratorDN und das Passwort für den RootDN dieses Servers ein, wenn Sie auf dem Server gespeicherte Daten lesen und schreiben müssen.

Wählen Sie alternativ *Anonymer Zugriff* und geben Sie kein Passwort an, um Lesezugriff auf das Verzeichnis zu erhalten.

Der Karteireiter *LDAP-Baum* zeigt den Inhalt des LDAP-Verzeichnisses an, mit dem Ihr Rechner verbunden ist. Klicken Sie auf Einträge, um deren Untereinträge einzublenden.

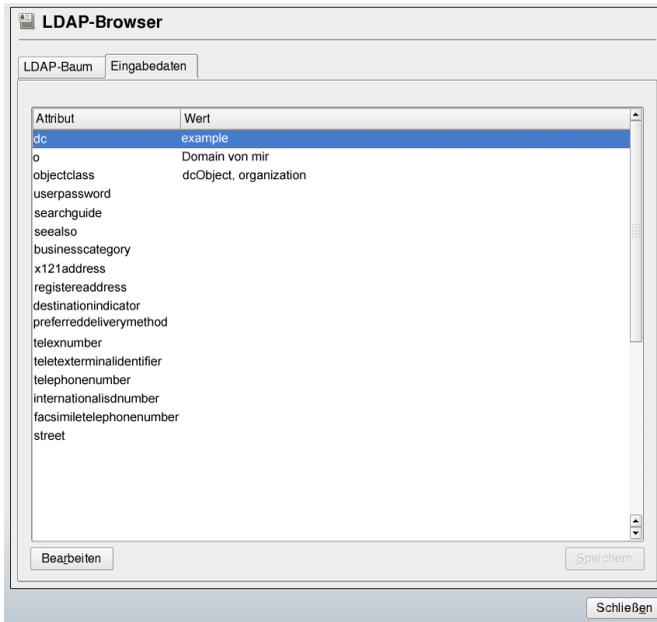
Abbildung 20.8 Navigieren in der LDAP-Verzeichnisstruktur



- 4 Um einen Eintrag im Detail anzuzeigen, wählen Sie ihn in der Ansicht *LDAP-Baum* aus und öffnen Sie den Karteireiter *Eingabedaten*.

Alle Attribute und Werte, die mit diesem Eintrag verbunden sind, werden angezeigt.

Abbildung 20.9 Navigieren in den Eingabedaten



- 5 Um den Wert eines dieser Attribute zu ändern, wählen Sie das Attribut aus und klicken Sie auf *Bearbeiten*. Geben Sie den neuen Wert ein und klicken Sie auf *Speichern*. Geben Sie anschließend das RootDN-Passwort ein, wenn Sie dazu aufgefordert werden.
- 6 Beenden Sie den LDAP-Browser mit *Schließen*.

20.7 Manuelles Konfigurieren eines LDAP-Servers

Das installierte System enthält unter `/etc/openldap/slapd.conf` eine vollständige Konfigurationsdatei für den LDAP-Server. Die einzelnen Einträge und die erforderlichen Anpassungen werden hier kurz beschrieben. Einträge, denen ein Rautenzeichen (#) vorangestellt wurde, sind nicht aktiv. Dieses Kommentarzeichen muss entfernt werden, um sie zu aktivieren.

20.7.1 Globale Direktiven in slapd.conf

Beispiel 20.2 *slapd.conf: Include-Direktive für Schemata*

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/rfc2307bis.schema
include /etc/openldap/schema/yast.schema
```

Diese erste in **Beispiel 20.2**, „**slapd.conf: Include-Direktive für Schemata**“ (S. 374) dargestellte Direktive in `slapd.conf` gibt das Schema an, anhand dessen das LDAP-Verzeichnis organisiert wird. Der Eintrag `core.schema` ist erforderlich. Dieser Direktive werden zusätzliche erforderliche Schemata angefügt. Weitere Informationen erhalten Sie in der im Lieferumfang enthaltenen OpenLDAP-Dokumentation.

Beispiel 20.3 *slapd.conf: pidfile und argsfile*

```
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
```

Diese beiden Dateien enthalten die PID (Prozess-ID) und einige Argumente, mit denen der `slapd`-Prozess gestartet wird. Hier müssen keine Änderungen vorgenommen werden.

Beispiel 20.4 *slapd.conf: Zugriffssteuerung*

```
# Sample Access Control
#   Allow read access of root DSE
# Allow self write access
#   Allow authenticated users read access
#   Allow anonymous users to authenticate
# access to dn="" by * read
#   access to * by self write
#       by users read
#       by anonymous auth
#
# if no access controls are present, the default is:
#   Allow read by all
#
# rootdn can always write!
```

In **Beispiel 20.4**, „**slapd.conf: Zugriffssteuerung**“ (S. 374) ist der Ausschnitt der Datei `slapd.conf` dargestellt, mit dem die Zugriffsberechtigungen für das LDAP-Verzeichnis auf dem Server gesteuert werden. Die hier im globalen Abschnitt von `slapd.conf` vorgenommenen Einträge sind gültig, sofern keine benutzerdefinierten Zugriffsregeln

im datenbankspezifischen Abschnitt festgelegt werden. Durch diese Regeln würden die globalen Deklarationen außer Kraft gesetzt. Wie hier dargestellt, verfügen alle Benutzer über Lesezugriff auf das Verzeichnis, nur der Administrator (`rootdn`) hat jedoch Schreibberechtigung für dieses Verzeichnis. Die Zugriffssteuerung in LDAP ist ein hochkomplexer Prozess. Folgende Tipps dienen als Unterstützung:

- Jede Zugriffsregel weist folgende Struktur auf:

```
access to <what> by <who> <access>
```

- *what* ist ein Platzhalter für das Objekt oder Attribut, auf das Zugriff gewährt wird. Einzelne Verzweigungen des Verzeichnisses können explizit mit separaten Regeln geschützt werden. Darüber hinaus besteht die Möglichkeit, Bereiche des Verzeichnisbaums mit einer Regel durch die Verwendung regulärer Ausdrücke zu verarbeiten. `slapd` wertet alle Regeln in der Reihenfolge aus, in der sie in der Konfigurationsdatei angegeben sind. Allgemeine Regeln sollten nach den spezifischeren Regeln angegeben werden. Die erste von `slapd` als gültig eingestufte Regel wird bewertet, alle folgenden Einträge werden ignoriert.
- Mit *who* wird festgelegt, wer Zugriff auf die mit *what* angegebenen Bereiche erhalten soll. Hier können reguläre Ausdrücke verwendet werden. Auch hier bricht `slapd` die Bewertung nach der ersten Übereinstimmung ab, sodass die spezifischeren Regeln vor den allgemeineren Regeln angegeben werden sollten. Die in [Tabelle 20.2, „Benutzergruppen und ihre Zugriffsberechtigungen“](#) (S. 375) dargestellten Einträge sind möglich.

Tabelle 20.2 Benutzergruppen und ihre Zugriffsberechtigungen

Tag	Scope
*	Alle Benutzer ohne Ausnahme
anonymous	Nicht authentifizierte („anonyme“) Benutzer
Benutzer	Authentifizierte Benutzer
self	Mit dem Zielobjekt verbundene Benutzer
dn.regex=<regex>	Alle Benutzer, die mit dem regulären Ausdruck übereinstimmen

- Mit `access` wird der Zugriffstyp angegeben. Verwenden Sie die in [Tabelle 20.3](#), „Zugriffstypen“ (S. 376) angegebenen Optionen.

Tabelle 20.3 Zugriffstypen

Tag	Umfang des Zugriffs
Keine	Kein Zugriff
auth	Für die Verbindung zum Server
compare	Für Objekt für Vergleichszugriff
Suchen	Für den Einsatz von Suchfiltern
Lesen	Lesezugriff
write	Schreibzugriff

`slapd` vergleicht das vom Client angeforderte Zugriffsrecht mit den in `slapd.conf` gewährten Rechten. Dem Client wird Zugriff gewährt, wenn in den Regeln ein höheres als das angeforderte Recht oder gleichwertiges Recht festgelegt ist. Wenn der Client ein höheres Recht als die in den Regeln deklarierten Rechte anfordert, wird ihm der Zugriff verweigert.

In [Beispiel 20.5](#), „`slapd.conf`: Beispiel für Zugriffskontrolle“ (S. 376) ist ein Beispiel für eine einfache Zugriffssteuerung dargestellt, die mithilfe von regulären Ausdrücken beliebig entwickelt werden kann.

Beispiel 20.5 `slapd.conf`: Beispiel für Zugriffskontrolle

```
access to dn.regex="ou=([^,]+),dc=example,dc=com"
by dn.regex="cn=Administrator,ou=$1,dc=example,dc=com" write
by user read
by * none
```

Mit dieser Regel wird festgelegt, dass nur der jeweilige Administrator Schreibzugriff auf einen einzelnen `ou`-Eintrag erhält. Alle anderen authentifizierten Benutzer verfügen über Lesezugriff und alle sonstigen Benutzer haben kein Zugriffsrecht.

TIPP: Festlegen von Zugriffsregeln

Falls keine `access to`-Regel oder keine passende `by`-Direktive vorhanden ist, wird der Zugriff verweigert. Nur explizit deklarierte Zugriffsrechte werden erteilt. Wenn gar keine Regeln deklariert sind, wird das Standardprinzip mit Schreibzugriff für den Administrator und Lesezugriff für alle anderen Benutzer angewendet.

Detaillierte Informationen hierzu und eine Beispielkonfiguration für LDAP-Zugriffsrechte finden Sie in der Online-Dokumentation zum installierten `openldap2`-Paket.

Neben der Möglichkeit, Zugriffsberechtigungen über die zentrale Serverkonfigurationsdatei (`slapd.conf`) zu verwalten, stehen Zugriffssteuerungsinformationen (ACI, Access Control Information) zur Verfügung. Mit ACI können Zugriffsdaten für einzelne Objekte innerhalb des LDAP-Baums gespeichert werden. Diese Art der Zugriffssteuerung wird noch selten verwendet und von Entwicklern als experimentell betrachtet. Weitere Informationen hierzu erhalten Sie unter <http://www.openldap.org/faq/data/cache/758.html>.

20.7.2 Datenbankspezifische Direktiven in `slapd.conf`

Beispiel 20.6 `slapd.conf`: Datenbankspezifische Direktiven

```
database bdb❶
suffix "dc=example,dc=com"❷
checkpoint 1024 5❸
cachesize 10000❹
rootdn "cn=Administrator,dc=example,dc=com"❺
# Cleartext passwords, especially for the rootdn, should
# be avoided. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret❻
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap❼
# Indices to maintain
index objectClass eq❸
overlay ppolicy❹
ppolicy_default "cn=Default Password Policy,dc=example,dc=com"
ppolicy_hash_cleartext
ppolicy_use_lockout
```

- ❶ In der ersten Zeile dieses Abschnitts wird der Datenbanktyp, in diesem Fall eine Berkeley-Datenbank, festgelegt (siehe [Beispiel 20.6](#), „[slapd.conf: Datenbankspezifische Direktiven](#)“ (S. 377)). Mit
- ❷ `suffix` geben Sie an, für welchen Teil des LDAP-Baums der Server verantwortlich sein soll. Mit
- ❸ `checkpoint` legen Sie die Datenmenge (in KB) fest, die im Transaktionsprotokoll gespeichert wird, bevor die Daten in die tatsächliche Datenbank geschrieben werden sowie die Zeit (in Minuten) zwischen zwei Schreibvorgängen. Mit
- ❹ `cachesize` legen Sie die Anzahl der im Cache der Datenbank gespeicherten Objekte fest.
- ❺ Mit dem darauf folgenden `rootdn` wird festgelegt, wer für diesen Server über Administratorrechte verfügt. Der hier angegebene Benutzer muss nicht über einen LDAP-Eintrag verfügen und nicht als regulärer Benutzer vorhanden sein.
- ❻ `rootpw` stellt das Administratorpasswort ein. Anstelle von `secret` kann hier auch der mit `slappasswd` erstellte Hash-Wert des Administratorpassworts eingegeben werden.
- ❼ Die `directory`-Direktive gibt das Verzeichnis im Dateisystem an, in dem die Datenbankverzeichnisse auf dem Server gespeichert sind.
- ❽ Die letzte Direktive, `index objectClass eq` veranlasst die Wartung eines Indizes aller Objektklassen. Attribute, nach denen die Benutzer am häufigsten suchen, können hier je nach Erfahrung hinzugefügt werden.
- ❾ `overlay ppolicy` fügt einen Layer der Passwortsteuermechanismen hinzu. `ppolicy_default` gibt den DN des `pwdPolicy`-Objekts an, der verwendet werden soll, wenn für einen gegebenen Benutzereintrag keine spezifische Richtlinie festgelegt wurde. Wenn für einen Eintrag keine spezifische Richtlinie und kein Standardwert vorgegeben ist, werden keine Richtlinien durchgesetzt. `ppolicy_hash_cleartext` gibt an, dass unverschlüsselte Passwörter in Hinzufüge- oder Bearbeitungsanforderungen vor dem Speichern in die Datenbank verschlüsselt werden. Bei Verwendung dieser Option wird empfohlen, allen Verzeichnisbenutzern den Zugriff zum Vergleichen, Suchen und Lesen des Attributs `userPassword` zu verweigern, da `ppolicy_hash_cleartext` das Informationsmodell X.500/LDAP verletzt. `ppolicy_use_lockout` sendet einen spezifischen Fehlercode, wenn ein Client versucht, sich bei einem gesperrten Konto anzumelden. Wenn Ihre Site für Sicherheitsprobleme anfällig ist, deaktivieren Sie diese Option, da der Fehlercode Angreifern nützliche Informationen zur Verfügung stellt.

Die an dieser Stelle für die Datenbank festgelegten benutzerdefinierten Regeln für `Access` können anstelle der globalen `Access`-Regeln verwendet werden.

20.7.3 Starten und Anhalten der Server

Nachdem der LDAP-Server vollständig konfiguriert und alle gewünschten Einträge gemäß dem in [Abschnitt 20.8, „Manuelles Verwalten von LDAP-Daten“](#) (S. 379) beschriebenen Schema vorgenommen wurden, starten Sie den LDAP-Server als `root`, indem Sie den Befehl `rclldap start` eingeben. Um den Server manuell zu stoppen, geben Sie den Befehl `rclldap stop` ein. Fragen Sie den Status des laufenden LDAP-Servers mit `rclldap status` ab.

Mit dem in [Abschnitt 8.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 141) beschriebenen Runlevel-Editor von YaST kann der Server beim Booten und Stoppen des Systems automatisch gestartet bzw. angehalten werden. Darüber hinaus besteht die Möglichkeit, wie in [Abschnitt 8.2.2, „Init-Skripten“](#) (S. 137) beschrieben, die entsprechenden Verknüpfungen zu den Start- und Anhaltenskripten mit dem Befehl `insserv` über die Kommandozeile zu erstellen.

20.8 Manuelles Verwalten von LDAP-Daten

In OpenLDAP stehen eine Reihe von Werkzeugen für die Datenverwaltung im LDAP-Verzeichnis zur Verfügung. Die vier wichtigsten Werkzeuge für Hinzufüge-, Lösch-, Such- und Änderungsvorgänge im Datenbestand werden im Folgenden beschrieben.

20.8.1 Einfügen von Daten in ein LDAP-Verzeichnis

Sobald die Konfiguration des LDAP-Servers in `/etc/openldap/slapd.conf` richtig und einsatzbereit ist (sie enthält die richtigen Einträge für `suffix`, `directory`, `rootdn`, `rootpw` und `index`), fahren Sie mit der Eingabe von Datensätzen fort. In OpenLDAP steht hierfür der Befehl `ldapadd` zur Verfügung. Wenn möglich, sollten Sie aus praktischen Gründen die Objekte als Bundle in der Datenbank hinzufügen. Zu

diesem Zweck kann LDAP das LDIF-Format (LDAP Data Interchange Format) verarbeiten. Bei einer LDIF-Datei handelt es sich um eine einfache Textdatei, die eine beliebige Anzahl an Attribut-Wert-Paaren enthalten kann. In den in `slapd.conf` deklarierten Schemadateien finden Sie die verfügbaren Objektklassen und Attribute. Die LDIF-Datei zur Erstellung eines groben Framework für das Beispiel in [Abbildung 20.1](#), „Struktur eines LDAP-Verzeichnisses“ (S. 353) würde der Datei in [Beispiel 20.7](#), „Beispiel für eine LDIF-Datei“ (S. 380) ähneln.

WICHTIG: Codierung von LDIF-Dateien

LDAP arbeitet mit UTF-8 (Unicode). Umlaute müssen richtig kodiert werden. Verwenden Sie einen Editor mit UTF-8-Unterstützung, wie beispielsweise Kate oder neuere Versionen von Emacs. Ansonsten sollten Sie Umlaute und andere Sonderzeichen vermeiden oder `recode` verwenden, um die Eingabe in UTF-8 neu zu kodieren.

Beispiel 20.7 *Beispiel für eine LDIF-Datei*

```
# The Organization
dn: dc=example,dc=com
objectClass: dcObject
objectClass: organization
o: Example dc: example

# The organizational unit development (devel)
dn: ou=devel,dc=example,dc=com
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=example,dc=com
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=example,dc=com
objectClass: organizationalUnit
ou: it
```

Speichern Sie die Datei mit der Erweiterung `.ldif` und geben Sie sie mit folgendem Befehl an den Server weiter:

```
ldapadd -x -D <dn of the administrator> -W -f <file>.ldif
```

`-x` deaktiviert in diesem Fall die Authentifizierung mit SASL. `-D` deklariert den Benutzer, der den Vorgang aufruft. Der gültige DN des Administrators wird hier so

eingetragen, wie er in `slapd.conf` konfiguriert wurde. Im aktuellen Beispiel lautet er `cn=Administrator,dc=example,dc=com`. Mit `-W` wird die Passwordeingabe in der Kommandozeile (unverschlüsselt) umgangen und eine separate Passwordeingabeaufforderung aktiviert. Das Passwort wurde zuvor in `slapd.conf` mit `rootpw` festgelegt. Mit der Option `-f` wird der Dateiname weitergegeben. Detaillierte Informationen zum Ausführen von `ldapadd` erhalten Sie in [Beispiel 20.8](#), „`ldapadd` mit `example.ldif`“ (S. 381).

Beispiel 20.8 *ldapadd mit example.ldif*

```
ldapadd -x -D cn=Administrator,dc=example,dc=com -W -f example.ldif
```

```
Enter LDAP password:
adding new entry "dc=example,dc=com"
adding new entry "ou=devel,dc=example,dc=com"
adding new entry "ou=doc,dc=example,dc=com"
adding new entry "ou=it,dc=example,dc=com"
```

Die Benutzerdaten einzelner Personen können in separaten LDIF-Dateien vorbereitet werden. In [Beispiel 20.9](#), „LDIF-Daten für Tux“ (S. 381) wird dem neuen LDAP-Verzeichnis Tux hinzugefügt.

Beispiel 20.9 *LDIF-Daten für Tux*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@example.com
uid: tux
telephoneNumber: +49 1234 567-8
```

Eine LDIF-Datei kann eine beliebige Anzahl an Objekten enthalten. Es können ganze Verzeichnisverzweigungen oder nur Teile davon in einem Vorgang an den Server weitergegeben werden, wie im Beispiel der einzelnen Objekte dargestellt. Wenn bestimmte Daten relativ häufig geändert werden müssen, wird eine detaillierte Unterteilung der einzelnen Objekte empfohlen.

20.8.2 Ändern von Daten im LDAP-Verzeichnis

Mit dem Werkzeug `ldapmodify` kann der Datenbestand geändert werden. Am einfachsten können Sie dies durch die Änderung der entsprechenden LDIF-Datei und der Weiterleitung der geänderten Datei an den LDAP-Server erreichen. Wenn Sie die Telefonnummer des Kollegen Tux von +49 1234 567-8 in +49 1234 567-10 ändern möchten, bearbeiten Sie die LDIF-Datei, wie in [Beispiel 20.10](#), „Geänderte LDIF-Datei `tux.ldif`“ (S. 382) angegeben.

Beispiel 20.10 *Geänderte LDIF-Datei `tux.ldif`*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Importieren Sie die geänderte Datei mit folgendem Befehl in das LDAP-Verzeichnis:

```
ldapmodify -x -D cn=Administrator,dc=example,dc=com -W -f tux.ldif
```

Alternativ können Sie die zu ändernden Attribute direkt an `ldapmodify` weitergeben. Die entsprechende Vorgehensweise wird nachfolgend beschrieben:

1 Starten Sie `ldapmodify` und geben Sie Ihr Passwort ein:

```
ldapmodify -x -D cn=Administrator,dc=example,dc=com -W
Enter LDAP password:
```

2 Geben Sie die Änderungen ein und halten Sie sich dabei genau in die unten angegebene Syntax-Reihenfolge:

```
dn: cn=Tux Linux,ou=devel,dc=example,dc=com
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Detaillierte Informationen zu `ldapmodify` und der zugehörigen Syntax finden Sie auf der [Manualpage `ldapmodify`](#).

20.8.3 Suchen und Lesen von Daten in einem LDAP-Verzeichnis

Mit `ldapsearch` steht in OpenLDAP ein Kommandozeilenwerkzeug zum Suchen von Daten innerhalb eines LDAP-Verzeichnisses und zum Lesen von Daten aus dem Verzeichnis zur Verfügung. Eine einfache Abfrage weist folgende Syntax auf:

```
ldapsearch -x -b dc=example,dc=com "(objectClass=*)"
```

Mit der Option `-b` wird die Suchbasis festgelegt, d. h. der Abschnitt des Baums, in dem die Suche durchgeführt werden soll. Im aktuellen Fall lautet er `dc=example,dc=com`. Wenn Sie eine feiner abgestufte Suche in speziellen Unterabschnitten des LDAP-Verzeichnisses durchführen möchten (beispielsweise nur innerhalb der Abteilung `devel`), geben Sie diesen Abschnitt mit `-b` an `ldapsearch` weiter. Mit `-x` wird die Aktivierung der einfachen Authentifizierung angefordert. `(objectClass=*)` deklariert, dass alle im Verzeichnis enthaltenen Objekte gelesen werden sollen. Diese Befehlsoption kann nach der Erstellung eines neuen Verzeichnisbaums verwendet werden, um zu prüfen, ob alle Einträge richtig aufgezeichnet wurden und ob der Server wie gewünscht reagiert. Weitere Informationen zur Verwendung von `ldapsearch` finden Sie auf der entsprechenden Manualpage (`ldapsearch(1)`).

20.8.4 Löschen von Daten in einem LDAP-Verzeichnis

Mit `ldapdelete` werden unerwünschte Einträge gelöscht. Die Syntax ist ähnlich wie die der anderen Befehle. Wenn Sie beispielsweise den vollständigen Eintrag für `Tux Linux` löschen möchten, erteilen Sie folgenden Befehl:

```
ldapdelete -x -D cn=Administrator,dc=example,dc=com -W cn=Tux \
Linux,ou=devel,dc=example,dc=com
```

20.9 Weiterführende Informationen

Komplexere Themen, wie die SASL-Konfiguration oder das Einrichten eines LDAP-Servers für die Reproduktion, der die Auslastung auf mehrere Slaves verteilt, wurden in diesem Kapitel bewusst nicht behandelt. Detaillierte Informationen zu diesen beiden Themen erhalten Sie im *OpenLDAP 2.2 Administrator's Guide*.

Auf der Website des OpenLDAP-Projekt stehen umfangreiche Dokumentationen für Einsteiger und fortgeschrittene LDAP-Benutzer zur Verfügung:

OpenLDAP Faq-O-Matic

Eine umfangreiche Sammlung von Fragen und Antworten zur Installation, Konfiguration und Verwendung von OpenLDAP. Es steht unter <http://www.openldap.org/faq/data/cache/1.html> zur Verfügung.

Quick Start Guide

Kurze Schritt-für-Schritt-Anleitung zur Installation des ersten LDAP-Servers. Dieses Dokument finden Sie unter <http://www.openldap.org/doc/admin22/quickstart.html> oder in einem installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`.

OpenLDAP 2.2 Administrator's Guide

Eine detaillierte Einführung in alle wichtigen Aspekte der LDAP-Konfiguration einschließlich der Zugriffssteuerung und der Verschlüsselung. Dieses Dokument finden Sie unter <http://www.openldap.org/doc/admin22/> oder in einem installierten System unter `/usr/share/doc/packages/openldap2/admin-guide/index.html`.

Informationen zu LDAP

Detaillierte allgemeine Einführung in die Grundlagen von LDAP: <http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf>.

Literatur zu LDAP:

- *LDAP System Administration* von Gerald Carter (ISBN 1-56592-491-6)
- *Understanding and Deploying LDAP Directory Services* von Howes, Smith und Good (ISBN 0-672-32316-8)

Das ausführlichste und wichtigste Referenzmaterial zum Thema LDAP sind die entsprechenden RFCs (Request for Comments), 2251 bis 2256.

Verteilte Nutzung von Dateisystemen mit NFS

21

Das Verteilen und Freigeben von Dateisystemen über ein Netzwerk ist eine Standardaufgabe in Unternehmensumgebungen. NFS ist ein bewährtes System, das auch mit dem Yellow Pages-Protokoll NIS zusammenarbeitet. Wenn Sie ein sichereres Protokoll wünschen, das mit LDAP zusammenarbeitet und auch kerberisiert werden kann, aktivieren Sie NFSv4.

NFS dient neben NIS dazu, ein Netzwerk für den Benutzer transparent zu machen. Mit NFS ist es möglich, arbiträre Dateisysteme über das Netzwerk zu verteilen. Bei entsprechendem Setup befinden sich Benutzer in derselben Umgebung, unabhängig vom gegenwärtig verwendeten Terminal.

Wie NIS ist NFS ein Client-Server-System. Ein Computer kann jedoch beides gleichzeitig sein – er kann Dateisysteme im Netzwerk zur Verfügung stellen (exportieren) und Dateisysteme anderer Hosts einhängen (importieren).

WICHTIG: DNS-Bedarf

Im Prinzip können alle Exporte allein mit IP-Adressen vorgenommen werden. Es ist ratsam, über ein funktionierendes DNS-System zu verfügen, um Zeitüberschreitungen zu vermeiden. Dies ist zumindest für die Protokollierung erforderlich, weil der mountd-Daemon Reverse-Lookups ausführt.

21.1 Installieren der erforderlichen Software

Wenn Sie Ihren Host als NFS-Client konfigurieren möchten, müssen Sie keine zusätzliche Software installieren. Alle erforderlichen Pakete für die Konfiguration eines NFS-Client werden standardmäßig installiert.

NFS-Server-Software ist kein Bestandteil der Standardinstallation. Zur Installation der NFS-Server-Software starten Sie YaST und wählen Sie *Software > Software installieren oder löschen* aus. Wählen Sie nun *Filter > Schemata* und anschließend *Verschiedene Server* aus. Oder verwenden Sie die Option *Suchen* und suchen Sie nach *NFS-Server*. Bestätigen Sie die Installation der Pakete, um den Installationsvorgang abzuschließen.

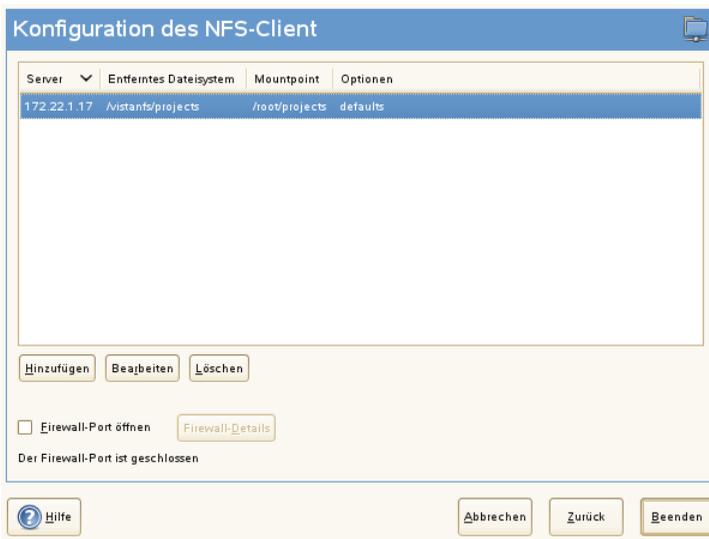
21.2 Importieren von Dateisystemen mit YaST

Autorisierte Benutzer können NFS-Verzeichnisse von NFS-Servern in ihre eigenen Dateibäume einhängen. Dies geschieht mit dem YaST-Modul *NFS-Client*. Geben Sie nur den Hostnamen des NFS-Servers, das zu importierende Verzeichnis und den Einhängpunkt an, an dem das Verzeichnis lokal eingehängt werden soll. Die Änderungen werden wirksam, nachdem im ersten Dialogfeld auf *Hinzufügen* geklickt wird. Klicken Sie auf *Firewall-Port öffnen*, um die Firewall zu öffnen und entfernten Computern den Zugriff auf den Dienst zu gewähren. Der Status der Firewall wird neben dem Kontrollkästchen angezeigt. Klicken Sie auf *Beenden*, um die Änderungen zu speichern. Weitere Informationen hierzu finden Sie in [Abbildung 21.1, „Konfiguration des NFS-Clients mit YaST“](#) (S. 387).

Die Konfiguration wird in `/etc/fstab` geschrieben und die angegebenen Dateisysteme werden eingehängt. Wenn Sie den YaST-Konfigurationsclient zu einem späteren Zeitpunkt starten, wird auch die vorhandene Konfiguration aus dieser Datei gelesen.

Ein NFSv4-Dateisystem kann zurzeit nur manuell importiert werden. Dies wird in [Abschnitt 21.3, „Manuelles Importieren von Dateisystemen“](#) (S. 387) erläutert.

Abbildung 21.1 Konfiguration des NFS-Clients mit YaST



21.3 Manuelles Importieren von Dateisystemen

Dateien können auch manuell von einem NFS-Server importiert werden. Die einzige Voraussetzung hierfür besteht darin, dass ein RPC-Portmapper ausgeführt wird, der durch die Eingabe von `rpcportmap start` vom Benutzer `root` gestartet werden kann. Sobald diese Voraussetzung erfüllt ist, können entfernt exportierte Dateisysteme genau wie lokale Festplatten mithilfe des Befehls `mount` auf folgende Weise im Dateisystem eingehängt werden:

```
mount host:remote-path local-path
```

Wenn beispielsweise Benutzerverzeichnisse vom Computer `nfs.example.com` importiert werden sollen, lautet das Kommando:

```
mount nfs.example.com:/home /home
```

21.3.1 Importieren von NFSv4-Dateisystemen

Der `idmapd`-Dienst muss verfügbar sein und auf dem Client ausgeführt werden, damit ein NFSv4-Import durchgeführt werden kann. Starten Sie den `idmapd`-Dienst an der Eingabeaufforderung durch Eingabe von `rcidmapd start`. Verwenden Sie `rcidmapd status`, um den Status von `idmapd` zu überprüfen.

Die Parameter des `idmapd`-Dienstes werden in der Datei `/etc/idmapd.conf` gespeichert. Behalten Sie den Wert `localdomain` für den Parameter `Domain` bei. Stellen Sie sicher, dass der angegebene Wert für den NFS-Client und den NFS-Server identisch ist.

Führen Sie NFSv4-Importe durch Eingabe eines Befehls an der Shell-Eingabeaufforderung aus. Geben Sie folgenden Befehl ein, um entfernte NFSv4-Dateisysteme zu importieren:

```
mount -t nfs4 host:/ local-path
```

Ersetzen Sie `host` durch den NFS-Server, auf dem ein oder mehrere NFSv4-Exporte gehostet werden, und ersetzen Sie `local-path` durch den Verzeichnisspeicherort auf dem Client-Computer, an dem der Export eingehängt werden soll. Um beispielsweise `/home`, das mit NFSv4 auf `nfs.example.com` exportiert wurde, nach `/local/home` zu importieren, verwenden Sie folgendes Kommando:

```
mount -t nfs4 nfs.example.com:/ /local/home
```

Der Pfad des entfernten Dateisystems, der auf den Servernamen und einen Doppelpunkt folgt, wird durch einen Schrägstrich („/“) dargestellt. Dies unterscheidet sich von der Angabe bei v3-Importen, bei denen der genaue Pfad des entfernten Dateisystems angegeben ist. Dieses Konzept wird als *Pseudo-Dateisystem* bezeichnet, das in [Abschnitt 21.4, „Exportieren von Dateisystemen mit YaST“](#) (S. 390) erläutert wird.

21.3.2 Verwenden des Diensts zum automatischen Einhängen

Genau wie die regulären Einhängungen für lokale Geräte kann auch der `autofs`-Daemon zum automatischen Einhängen von entfernten Dateisystemen verwendet werden. Fügen Sie dazu den folgenden Eintrag in der Datei `/etc/auto.master` hinzu:

```
/nfsmounts /etc/auto.nfs
```

Nun fungiert das Verzeichnis `/nfsmounts` als Root-Verzeichnis für alle NFS-Einhängungen auf dem Client, wenn die Datei `auto.nfs` entsprechend beendet wurde. Der Name `auto.nfs` wurde nur der Einfachheit halber ausgewählt – Sie können einen beliebigen Namen auswählen. Fügen Sie der ausgewählten Datei (erstellen Sie diese, wenn sie nicht vorhanden ist) Einträge für alle NFS-Einhängungen wie im folgenden Beispiel dargestellt hinzu:

```
localdata -fstype=nfs server1:/data  
nfs4mount -fstype=nfs4 server2:/
```

Aktivieren Sie die Einstellungen mit `rcautofs start`. In diesem Beispiel wird `/nfsmounts/localdata`, das Verzeichnis `/data` von `server1`, mit NFS eingehängt und `/nfsmounts/nfs4mount` von `server2` wird mit NFSv4 eingehängt.

Wenn die Datei `/etc/auto.master` während dem Ausführen des Diensts `autofs` bearbeitet wird, muss die automatische Einhängung erneut gestartet werden, damit die Änderungen wirksam werden. Verwenden Sie dazu den Befehl `rcautofs restart`.

21.3.3 Manuelles Bearbeiten von `/etc/fstab`

Ein typischer NFSv3-Einhängeeintrag in `/etc/fstab` sieht folgendermaßen aus:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

NFSv4-Einhängungen können der Datei `/etc/fstab` auch manuell hinzugefügt werden. Verwenden Sie für diese Einhängungen in der dritten Spalte `nfs4` statt `nfs` und stellen Sie sicher, dass das entfernte Dateisystem in der ersten Spalte nach `nfs.example.com` als `//` angegeben ist. Eine typische Zeile für eine NFSv4-Einhängung in `/etc/fstab` sieht zum Beispiel wie folgt aus:

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

Mit der Option `noauto` wird verhindert, dass das Dateisystem beim Starten automatisch eingehängt wird. Wenn Sie das jeweilige Dateisystem manuell einhängen möchten, können Sie das Einhängekommando auch kürzen. Es muss in diesem Fall wie das folgende Kommando nur den Einhängpunkt angeben:

```
mount /local/path
```

Beachten Sie, dass das Einhängen dieser Dateisysteme beim Start durch die Initialisierungsskripte des Systems geregelt wird, wenn die Option `noauto` nicht angegeben ist.

21.4 Exportieren von Dateisystemen mit YaST

Mit YaST können Sie einen Computer im Netzwerk als NFS-Server bereitstellen. Dies ist ein Server, der Verzeichnisse und Dateien an alle Hosts exportiert, die ihm Zugriff gewähren. Auf diese Weise können Anwendungen für alle Mitglieder einer Gruppe zur Verfügung gestellt werden, ohne dass sie lokal auf deren Hosts installiert werden müssen. Starten Sie zum Installieren eines solchen Servers YaST und wählen Sie *Netzwerkdienste > NFS-Server* aus. Es erscheint ein Dialogfeld wie in **Abbildung 21.2**, „**Konfiguration des NFS-Servers**“ (S. 391).

Abbildung 21.2 Konfiguration des NFS-Servers



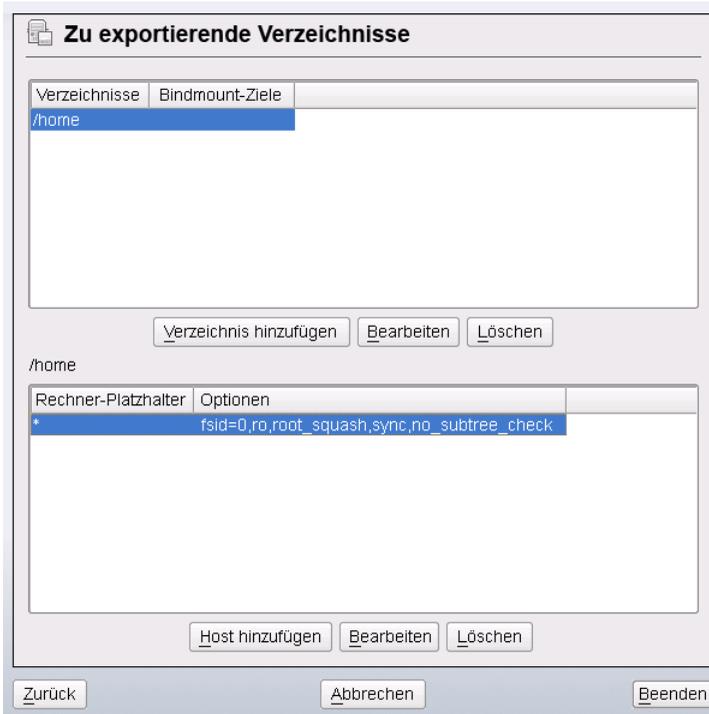
Aktivieren Sie dann *NFS-Server starten* und geben Sie den *NFSv4-Domännennamen* ein.

Klicken Sie auf *GSS-Sicherheit aktivieren*, wenn Sie einen sicheren Zugriff auf den Server benötigen. Als Voraussetzung hierfür muss Kerberos in der Domäne installiert sein und sowohl der Server als auch der Client müssen kerberisiert sein. Klicken Sie auf *Weiter*.

Geben Sie im oberen Textfeld die zu exportierenden Verzeichnisse an. Legen Sie darunter Hosts fest, die darauf Zugriff erhalten sollen. Dieses Dialogfeld ist in **Abbildung 21.3**, „**Konfigurieren eines NFS-Servers mit YaST**“ (S. 392) abgebildet. In der Abbildung wird das Szenario dargestellt, bei dem NFSv4 im vorherigen Dialogfeld aktiviert wurde. Ein `ngeziele` binden wird in der rechten Leiste angezeigt. Weitere Details finden Sie in der Hilfe auf der rechten Leiste. In der unteren Hälfte des Dialogfelds befinden sich vier Optionen, die für jeden Host festgelegt werden können: `single host` (Einzelhost), `netgroups` (Netzgruppen), `wildcards`

(Platzhalterzeichen) und IP-Netzwerke. Eine ausführlichere Erläuterung zu diesen Optionen finden Sie unter `Exporte` auf der `man`-Seite. Klicken Sie zum Beenden der Konfiguration auf *Beenden*.

Abbildung 21.3 Konfigurieren eines NFS-Servers mit YaST



WICHTIG: Automatische Firewall-Konfiguration

Wenn auf Ihrem System eine Firewall aktiviert ist (SuSEfirewall2), wird deren Konfiguration von YaST für den NFS-Server angepasst, indem der `nfs`-Dienst aktiviert wird, wenn *Firewall-Ports öffnen* ausgewählt ist.

21.4.1 Exportieren für NFSv4-Clients

Aktivieren Sie *NFSv4 aktivieren*, um NFSv4-Clients zu unterstützen. Clients mit NFSv3 können immer noch auf die exportierten Verzeichnisse des Servers zugreifen, wenn

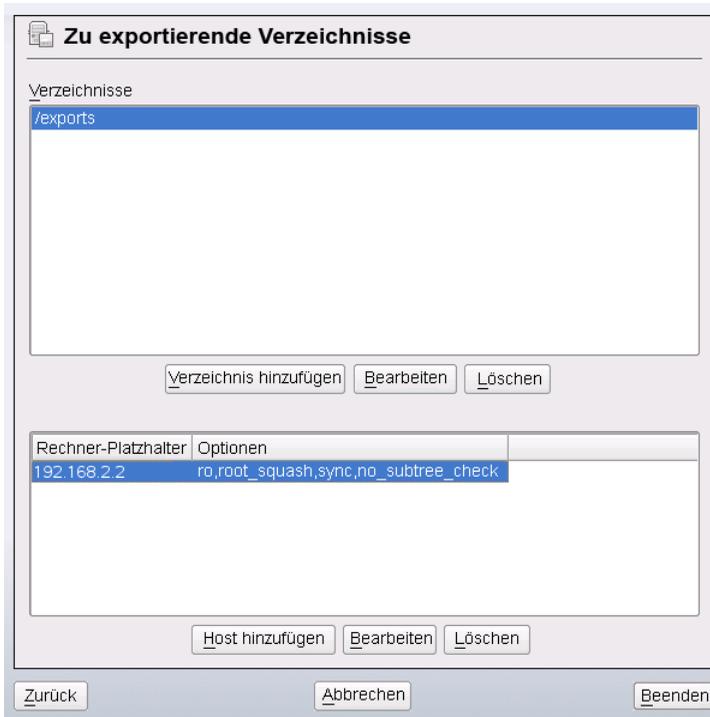
diese entsprechend exportiert wurden. Dies wird in [Abschnitt 21.4.3, „Gleichzeitig vorhandene v3-Exporte und v4-Exporte“](#) (S. 396) detailliert beschrieben.

Geben Sie nach dem Aktivieren von NFSv4 einen geeigneten Domännennamen an. Stellen Sie sicher, dass der eingegebene Name dem Namen in der Datei `/etc/idmapd.conf` eines beliebigen NFSv4-Client entspricht, der auf diesen speziellen Server zugreift. Dieser Parameter wird für den idmapd-Dienst verwendet, der für die NFSv4-Unterstützung (auf dem Server und dem Client) erforderlich ist. Behalten Sie den Wert `localdomain` (der Standardwert) bei, wenn Sie keine speziellen Anforderungen haben. Weitere Informationen finden Sie in [Abschnitt 21.7, „Weiterführende Informationen“](#) (S. 401).

Klicken Sie auf *Weiter*. Das darauf folgende Dialogfeld ist in zwei Abschnitte unterteilt. Die obere Hälfte besteht aus zwei Spalten mit den Namen *Verzeichnisse* und *Einhängeziele binden*. Bei *Verzeichnisse* handelt es sich um eine direkt bearbeitbare Spalte, in der die zu exportierenden Verzeichnisse aufgelistet werden.

Bei einer festen Gruppe von Clients gibt es zwei Arten von Clients, die exportiert werden können – Verzeichnisse, die als Pseudo-Root-Dateisysteme fungieren, und solche, die an ein Unterverzeichnis eines Pseudo-Dateisystems gebunden sind. Dieses Pseudo-Dateisystem stellt den Basispunkt dar, unter dem alle Dateisysteme angeordnet werden, die für dieselbe Gruppe von Clients exportiert wurden. Bei einem Client oder einer Gruppe von Clients kann nur ein Verzeichnis auf dem Server als Pseudo-Root-Verzeichnis für den Export konfiguriert werden. Exportieren Sie für denselben Client mehrere Verzeichnisse, indem Sie sie an vorhandene Unterverzeichnisse im Pseudo-Root-Verzeichnis binden.

Abbildung 21.4 Exportieren von Verzeichnissen mit NFSv4



Geben Sie in der unteren Hälfte des Dialogfelds die Export- und Client-Optionen (Platzhalterzeichen) für ein bestimmtes Verzeichnis ein. Nach dem Hinzufügen eines Verzeichnisses in der oberen Hälfte wird automatisch ein weiteres Dialogfeld zum Eingeben von Client- und Optionsinformationen geöffnet. Klicken Sie danach zum Hinzufügen eines neuen Client (einer Gruppe von Clients) auf *Host hinzufügen*.

Geben Sie im kleinen Dialogfeld, das geöffnet wird, das Platzhalterzeichen für den Host ein. Es gibt vier mögliche Typen von Platzhalterzeichen für den Host, die für jeden Host festgelegt werden können: ein einzelner Host (Name oder IP-Adresse), Netzgruppen, Platzhalterzeichen (wie *, womit angegeben wird, dass alle Computer auf den Server zugreifen können) und IP-Netzwerke. Schließen Sie dann unter *Optionen* die Zeichenfolge `fsid=0` in die kommasetrennte Liste der Optionen ein, um das Verzeichnis als Pseudo-Root-Verzeichnis zu konfigurieren. Wenn dieses Verzeichnis an ein anderes Verzeichnis unter einem bereits konfigurierten Pseudo-Root-Verzeichnis

gebunden werden soll, stellen Sie sicher, dass ein Zielpfad zum Binden mit der Struktur `bind=/target/path` in der Optionsliste angegeben ist.

Nehmen Sie beispielsweise an, dass das Verzeichnis `/exports` als Pseudo-Root-Verzeichnis für alle Clients ausgewählt wurde, die auf den Server zugreifen können. Fügen Sie dies in der oberen Hälfte hinzu und stellen Sie sicher, dass die für dieses Verzeichnis eingegebenen Optionen `fsid=0` einschließen. Wenn Sie über ein anderes Verzeichnis, `/data`, verfügen, das auch mit NFSv4 exportiert werden muss, fügen Sie dieses Verzeichnis der oberen Hälfte hinzu. Stellen Sie beim Eingeben von Optionen für dieses Verzeichnis sicher, dass `bind=/exports/data` in der Liste enthalten ist und dass es sich bei `/exports/data` um ein bereits bestehendes Unterverzeichnis von `/exports` handelt. Alle Änderungen an der Option `bind=/target/path` werden unter *Einhängeziele binden* angezeigt, unabhängig davon, ob ein Wert hinzugefügt, gelöscht oder geändert wurde. Bei dieser Spalte handelt es sich nicht um eine direkt bearbeitbare Spalte. In ihr werden stattdessen Verzeichnisse und deren Ursprung zusammengefasst. Nachdem die Informationen vollständig sind, klicken Sie auf *Beenden*, um die Konfiguration abzuschließen, oder auf *Start*, um den Dienst neu zu starten.

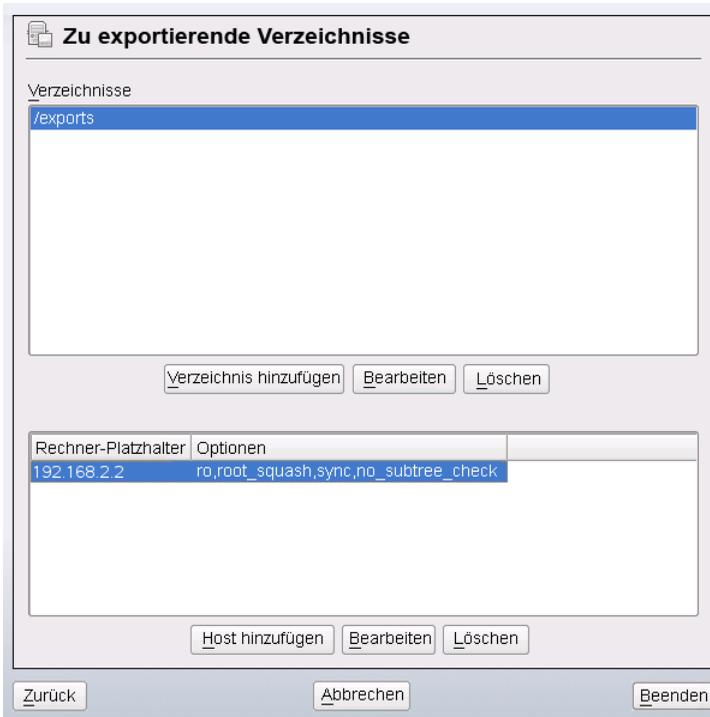
21.4.2 NFSv3- und NFSv2-Exporte

Stellen Sie vor dem Klicken auf *Weiter* sicher, dass *NFSv4 aktivieren* im ersten Dialogfeld nicht aktiviert ist.

Das nächste Dialogfeld besteht aus zwei Bereichen. Geben Sie im oberen Textfeld die zu exportierenden Verzeichnisse an. Legen Sie darunter Hosts fest, die darauf Zugriff erhalten sollen. Es können vier Arten von Host-Platzhalterzeichen für jeden Host festgelegt werden: ein einzelner Host (Name oder IP-Adresse), Netzwerkgruppen, Platzhalterzeichen (z. B. *, womit angegeben wird, dass alle Rechner auf den Server zugreifen können) und IP-Netzwerke.

Dieses Dialogfeld ist in **Abbildung 21.5, „Exportieren von Verzeichnissen mit NFSv2 und v3“** (S. 396) abgebildet. Eine ausführlichere Erläuterung dieser Optionen finden Sie unter `man exports`. Klicken Sie zum Abschließen der Konfiguration auf *Beenden*.

Abbildung 21.5 Exportieren von Verzeichnissen mit NFSv2 und v3



21.4.3 Gleichzeitig vorhandene v3-Exporte und v4-Exporte

NFSv3-Exporte und NFSv4-Exporte können gleichzeitig auf einem Server vorhanden sein. Nach dem Aktivieren der Unterstützung für NFSv4 im ersten Konfigurationsdialogfeld werden diese Exporte, für die `fsid=0` und `bind=/target/path` nicht in der Optionsliste enthalten sind, als v3-Exporte angesehen. Sehen Sie sich das Beispiel in [Abbildung 21.3](#), „Konfigurieren eines NFS-Servers mit YaST“ (S. 392) an. Wenn Sie ein weiteres Verzeichnis (z. B. `/data2`) mit *Hinzufügen: Verzeichnis* hinzufügen und anschließend weder `fsid=0` noch `bind=/target/path` in der entsprechenden Optionsliste aufgeführt wird, fungiert dieser Export als v3-Export.

WICHTIG

Automatische Firewall-Konfiguration

Wenn auf Ihrem System SuSEfirewall2 aktiviert ist, passt YaST deren Konfiguration für den NFS-Server an, indem der Dienst aktiviert wird, wenn *Firewall-Ports öffnen* ausgewählt ist.

21.5 Manuelles Exportieren von Dateisystemen

Die Konfigurationsdateien für den NFS-Exportdienst lauten `/etc/exports` und `/etc/sysconfig/nfs`. Zusätzlich zu diesen Dateien ist `/etc/idmapd.conf` für die NFSv4-Serverkonfiguration erforderlich. Führen Sie zum Starten bzw. Neustarten der Dienste das Kommando `rcnfsserver restart` aus. Dieser startet auch `rpc.idmapd`, wenn NFSv4 in `/etc/sysconfig/nfs` konfiguriert ist. Der NFS-Server ist von einem laufenden RPC-Portmapper abhängig. Starten Sie aus diesem Grund mit `rcportmap restart` auch den Portmapper-Dienst bzw. starten Sie ihn neu.

21.5.1 Exportieren von Dateisystemen mit NFSv4

NFSv4 ist die neueste Version des NFS-Protokolls, das mit openSUSE zur Verfügung gestellt wird. Das Konfigurieren der Verzeichnisse für den Export mit NFSv4 unterscheidet sich geringfügig von den früheren NFS-Versionen.

Die `/etc/exports`-Datei

Diese Datei enthält eine Liste mit Einträgen. Mit jedem Eintrag wird ein Verzeichnis angegeben, das freigegeben wird. Zudem wird angegeben, wie das Verzeichnis freigegeben wird. Ein typischer Eintrag in `/etc/exports` besteht aus:

```
/shared/directory host(option_list)
```

Beispiel:

```
/export 192.168.1.2(rw,fsid=0, sync)
/data 192.168.1.2(rw,bind=/export/data, sync)
```

Die Verzeichnisse, für die `fsid=0` in der Optionsliste angegeben ist, werden als Pseudo-Root-Dateisysteme bezeichnet. In diesem Fall wird die IP-Adresse `192.168.1.2` verwendet. Sie können den Namen des Hosts, ein Platzhalterzeichen, mit dem mehrere Hosts angegeben werden (`*.abc.com`, `* usw.`) oder Netzwerkgruppen verwenden.

Für eine feste Gruppe von Clients stehen nur zwei Arten von Verzeichnissen zur Verfügung, die NFSv4-exportiert sein können:

- Ein einzelnes Verzeichnis, das als Pseudo-Root-Dateisystem ausgewählt wird. In diesem Beispiel ist `/export` das Pseudo-Root-Verzeichnis, da `fsid=0` in der Optionsliste für diesen Eintrag angegeben ist.
- Verzeichnisse, die für die Bindung an ein vorhandenes Unterverzeichnis des Pseudo-Dateisystems ausgewählt werden. In den oben angegebenen Beispieleinträgen ist `/data` solch ein Verzeichnis, das an ein vorhandenes Unterverzeichnis (`/export/data`) des Pseudo-Dateisystems `/export` gebunden ist.

Das Pseudo-Dateisystem ist das Verzeichnis der obersten Ebene, unter dem alle Dateisysteme, die NFSv4-exportiert werden müssen, ihren Platz einnehmen. Für einen Client bzw. eine Clientgruppe kann nur ein Verzeichnis auf dem Server vorhanden sein, das als Pseudo-Root-Verzeichnis für den Export konfiguriert ist. Für den gleichen Client bzw. für die gleiche Clientgruppe können zahlreiche weitere Verzeichnisse exportiert werden, indem sie an ein vorhandenes Unterverzeichnis im Pseudo-Root-Verzeichnis gebunden werden.

/etc/sysconfig/nfs

Diese Datei enthält einige Parameter, mit denen das Verhalten des NFSv4-Server-Daemons bestimmt wird. Es ist wichtig, dass der Parameter `NFSv4_SUPPORT` auf "yes" festgelegt ist. Mit diesem Parameter wird bestimmt, ob der NFS-Server NFSv4-Exporte und -Clients unterstützt.

/etc/idmapd.conf

Jeder Benutzer eines Linux-Rechners verfügt über einen Namen und eine ID. `idmapd` führt die Name-zu-ID-Zuordnung für NFSv4-Anforderungen an den Server aus und sendet Antworten an den Client. Dies muss auf dem Server und dem Client für NFSv4 ausgeführt werden, da NFSv4 nur Namen für die eigene Kommunikation verwendet.

Stellen Sie sicher, dass Benutzernamen und IDs (uid) Benutzern auf eine einheitliche Weise auf allen Rechnern zugewiesen werden, auf denen möglicherweise Dateisysteme mit NFS freigegeben werden. Dies kann mit NIS, LDAP oder einem beliebigen einheitlichen Domänenauthentifizierungsmechanismus in Ihrer Domäne erreicht werden.

Für eine ordnungsgemäße Funktionsweise muss der Parameter `Domain` für den Client und den Server in dieser Datei identisch festgelegt sein. Wenn Sie sich nicht sicher sind, belassen Sie die Domäne in den Server- und den Clientdateien als `localdomain`. Eine Beispielkonfigurationsdatei sieht folgendermaßen aus:

```
[General]
Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]
Nobody-User = nobody
Nobody-Group = nobody
```

Ändern Sie diese Parameter nur, wenn Sie sicher sind, welche Auswirkungen diese Aktion hat. Weitere Informationen finden Sie auf der `man`-Seite zu `idmapd` und `idmapd.conf`; `man idmapd`, `man idmapd.conf`.

Starten und Beenden von Apache

Starten Sie den NFS-Serverdienst nach dem Ändern von `/etc/exports` oder `/etc/sysconfig/nfs` mit `rcnfsserver restart` bzw. starten Sie den Dienst neu. Starten Sie den `idmapd`-Dienst nach dem Ändern von `/etc/idmapd.conf` mit `rcidmapd restart` bzw. starten Sie den Dienst neu. Stellen Sie sicher, dass beide Dienste ausgeführt werden.

Wenn dieser Dienst beim Booten gestartet werden soll, führen Sie das Kommando `chkconfig nfsserver on` aus.

21.5.2 Exportieren von Dateisystemen mit NFSv2 und NFSv3

Dies gilt speziell für NFSv3- und NFSv2-Exporte. Informationen zum Exportieren mit NFSv4 finden Sie unter [Abschnitt 21.4.1, „Exportieren für NFSv4-Clients“](#) (S. 392).

Beim Exportieren von Dateisystemen mit NFS werden zwei Konfigurationsdateien verwendet: `/etc/exports` und `/etc/sysconfig/nfs`. Ein typischer `/etc/exports`-Dateieintrag weist folgendes Format auf:

```
/shared/directory host(list_of_options)
```

Beispiel:

```
/export 192.168.1.2(rw, sync)
```

Hier wird das Verzeichnis `/export` gemeinsam mit dem Host `192.168.1.2` mit der Optionsliste `rw, sync` verwendet. Diese IP-Adresse kann durch einen Clientnamen oder mehrere Clients mit einem Platzhalterzeichen (z. B. `*.abc.com`) oder auch durch Netzwerkgruppen ersetzt werden.

Eine detaillierte Erläuterung aller Optionen und der entsprechenden Bedeutungen finden Sie auf der `man`-Seite zu `exports` (`man exports`).

Starten Sie den NFS-Server nach dem Ändern von `/etc/exports` oder `/etc/sysconfig/nfs` mit dem Befehl `rcnfsserver restart` bzw. starten Sie ihn neu.

21.6 NFS mit Kerberos

Wenn die Kerberos-Authentifizierung für NFS verwendet werden soll, muss die GSS-Sicherheit aktiviert werden. Wählen Sie dazu *GSS-Sicherheit aktivieren* im ersten YaST-Dialogfeld. Zur Installation dieser Funktion muss ein funktionierender Kerberos-Server zur Verfügung stehen. YaST richtet diesen Server nicht ein, sondern nutzt lediglich die über den Server bereitgestellten Funktionen. Wenn Sie die Authentifizierung mittels Kerberos verwenden möchten, müssen Sie zusätzlich zur YaST-Konfiguration mindestens die nachfolgend beschriebenen Schritte ausführen, bevor Sie die NFS-Konfiguration ausführen:

- Stellen Sie sicher, dass sich Server und Client in derselben Kerberos-Domäne befinden. Dies bedeutet, dass beide auf denselben KDC-Server (Key Distribution Center) zugreifen und die Datei `krb5.keytab` gemeinsam verwenden (der Standard Speicherort auf allen Rechnern lautet `/etc/krb5.keytab`).
- Starten Sie den `gssd`-Dienst auf dem Client mit `rcgssd start`.
- Starten Sie den `svcgssd`-Dienst auf dem Server mit `rcsvcgssd start`.

Weitere Informationen zum Konfigurieren eines kerberisierten NFS finden Sie über die Links in **Abschnitt 21.7, „Weiterführende Informationen“** (S. 401).

21.7 Weiterführende Informationen

Genau wie für die man-Seiten zu `exports`, `nfs` und `mount` stehen Informationen zum Konfigurieren eines NFS-Servers und -Clients unter `/usr/share/doc/packages/nfs-tls/README` zur Verfügung. Online-Dokumentation wird über die folgenden Web-Dokumente bereitgestellt:

- Die detaillierte technische Dokumentation finden Sie online unter SourceForge [<http://nfs.sourceforge.net/>].
- Anweisungen zum Einrichten eines kerberisierten NFS finden Sie unter NFS Version 4 Open Source Reference Implementation [<http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html>].
- Wenn Sie Fragen zu NFSv4 haben, lesen Sie in den Linux NFSv4-FAQ [<http://www.citi.umich.edu/projects/nfsv4/linux/faq/>] nach.

Der HTTP-Server Apache

Mit einem Marktanteil von mehr als 70 % ist der Apache HTTP-Server (Apache) laut einer <http://www.netcraft.com/>-Umfrage im der weltweit am häufigsten eingesetzte Webserver. Der von Apache Software Foundation (<http://www.apache.org/>) entwickelte Apache-Server läuft auf fast allen Betriebssystemen. openSUSE® umfasst Apache, Version 2.2. In diesem Kapitel erfahren Sie, wie Apache installiert, konfiguriert und eingerichtet wird. Sie lernen SSL, CGI und weitere Module kennen und erfahren, wie Sie bei Problemen mit dem Webserver vorgehen.

22.1 Kurzanleitung

In diesem Abschnitt erfahren Sie, wie Sie Apache in kürzester Zeit installieren und einrichten. Zur Installation und Konfiguration von Apache müssen Sie als `root`-Benutzer angemeldet sein.

22.1.1 Anforderungen

Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind, bevor Sie den Apache-Webserver einrichten:

1. Das Netzwerk des Computers ist ordnungsgemäß konfiguriert. Weitere Informationen zu diesem Thema finden Sie unter **Kapitel 14, *Grundlegendes zu Netzwerken*** (S. 225).

2. Durch Synchronisierung mit einem Zeitserver ist sichergestellt, dass die Systemzeit des Computers genau ist. Die exakte Uhrzeit ist für Teile des HTTP-Protokolls nötig. Weitere Informationen zu diesem Thema finden Sie unter [Kapitel 18, Zeit-synchronisierung mit NTP](#) (S. 331).
3. Die neuesten Sicherheitsaktualisierungen sind installiert. Falls Sie sich nicht sicher sind, führen Sie ein YaST-Online-Update aus.
4. In der Firewall ist der Standardport des Webservers (Port 80) geöffnet. Lassen Sie dazu in SUSEFirewall2 den Service *HTTP-Server* in der externen Zone zu. Diese Konfiguration können Sie in YaST vornehmen. Weitere Informationen erhalten Sie unter [Abschnitt 28.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 510).

22.1.2 Installation

Apache ist in der Standardinstallation von openSUSE nicht enthalten. Um Apache zu installieren, starten Sie YaST und wählen Sie *Software > Software installieren oder löschen*. Wählen Sie dann *Filter > Schemata* und schließlich *Web and LAM Server* unter *Serverfunktionen* aus. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

Apache wird mit einer voreingestellten Standardkonfiguration installiert, die „sofort“ ausgeführt werden kann. Hierzu zählt sowohl das Multiprocessing-Modul (MPM) `apache2-prefork` als auch das Modul PHP5. Weitere Informationen zu Modulen erhalten Sie unter [Abschnitt 22.4, „Installieren, Aktivieren und Konfigurieren von Modulen“](#) (S. 423).

22.1.3 Start

Um Apache zu starten und sicherzustellen, dass Apache automatisch bei jedem Systemstart gestartet wird, öffnen Sie YaST und wählen Sie *System > Systemdienste (Runlevel)* aus. Suchen Sie dann nach `apache2` und aktivieren Sie den Service. Der Webserver wird sofort gestartet. Wenn Sie Ihre Änderungen nun mit *Verlassen* speichern, wird Apache beim Systemstart automatisch in Runlevel 3 und 5 gestartet. Weitere Informationen zu den Runlevels in openSUSE und eine Beschreibung des YaST-Runlevel-Editors finden Sie in [Abschnitt 8.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 141).

Über die Shell starten Sie Apache mit dem Befehl `rcapache2 start`. Mit dem Befehl `chkconfig -a apache2` stellen Sie sicher, dass Apache beim Systemstart automatisch in Runlevel 3 und 5 gestartet wird.

Sofern Sie beim Start von Apache keine Fehlermeldungen erhalten haben, müsste der Webserver nun laufen. Starten Sie einen Webbrowser und öffnen Sie <http://localhost/>. Daraufhin wird eine Apache-Testseite angezeigt, die besagt: „Es funktioniert!“ Wenn diese Seite nicht angezeigt wird, lesen Sie den Abschnitt [Abschnitt 22.8, „Fehlersuche“](#) (S. 444).

Nachdem der Webserver nun läuft, können Sie eigene Dokumente hinzufügen, die Konfiguration an Ihre Anforderungen anpassen und weitere Module mit den benötigten Funktionen installieren.

22.2 Konfigurieren von Apache

Sie haben zwei Möglichkeiten, Apache in openSUSE zu konfigurieren: mit YaST oder manuell. Bei der manuellen Konfiguration können Sie mehr Details einstellen, allerdings müssen Sie ohne den Komfort der Bedienoberfläche von YaST zurechtkommen.

WICHTIG: Konfigurationsänderungen

Die meisten Konfigurationsänderungen werden erst nach einem Neustart bzw. nach dem Neuladen von Apache wirksam. Wenn Sie YaST zur Konfiguration verwenden und die Konfiguration mit aktiviertem *HTTP-Dienst* abschließen, wird der Rechner automatisch neu gestartet. Der manuelle Neustart wird unter [Abschnitt 22.3, „Starten und Beenden von Apache“](#) (S. 421) beschrieben. Für die meisten Konfigurationsänderungen ist allerdings nur eine Aktualisierung mit `rcapache2 reload` erforderlich.

22.2.1 Manuelle Konfiguration von Apache

Wenn Sie den Apache-Webserver manuell konfigurieren möchten, müssen Sie die Klartext-Konfigurationsdateien als `Root`-Benutzer bearbeiten.

Konfigurationsdateien

Die Konfigurationsdateien von Apache befinden sich in zwei verschiedenen Verzeichnissen:

- `/etc/sysconfig/apache2`
- `/etc/apache2/`

`/etc/sysconfig/apache2`

`/etc/sysconfig/apache2` steuert einige globale Einstellungen von Apache, beispielsweise die zu ladenden Module, die einzuschließenden Konfigurationsdateien, die beim Serverstart zu verwendenden Flags sowie Flags, die der Kommandozeile hinzugefügt werden sollen. Die Konfigurationsoptionen dieser Datei sind hinreichend dokumentiert und werden daher an dieser Stelle nicht näher erläutert. Für die Konfigurationsanforderungen eines typischen Webservers dürften die Einstellungen der Datei `/etc/sysconfig/apache2` ausreichen.

`/etc/apache2/`

`/etc/apache2/` enthält alle Konfigurationsdateien für Apache. In diesem Abschnitt wird der Zweck jeder einzelnen Datei erklärt. Jede Datei enthält mehrere Konfigurationsoptionen (auch als *Direktiven* bezeichnet). Die Konfigurationsoptionen dieser Dateien sind hinreichend dokumentiert und werden daher an dieser Stelle nicht näher erläutert.

Die Apache-Konfigurationsdateien gliedern sich wie folgt:

```
/etc/apache2/  
|  
|- charset.conv  
|- conf.d/  
| |  
| |- *.conf  
|  
|- default-server.conf  
|- errors.conf  
|- httpd.conf  
|- listen.conf  
|- magic  
|- mime.types  
|- mod_*.conf  
|- server-tuning.conf
```

```

|- ssl.*
|- ssl-global.conf
|- sysconfig.d
|   |
|   |- global.conf
|   |- include.conf
|   |- loadmodule.conf . .
|
|- uid.conf
|- vhosts.d
|   |- *.conf

```

Apache-Konfigurationsdateien in /etc/apache2/

`charset.conf`

In dieser Datei ist festgelegt, welche Zeichensätze für die verschiedenen Sprachen verwendet werden. Bearbeiten Sie diese Datei nicht.

`conf.d/*.conf`

Dies sind Konfigurationsdateien anderer Module. Bei Bedarf können die Konfigurationsdateien in Ihre virtuellen Hostkonfigurationen eingeschlossen werden. Beispiele finden Sie in `vhosts.d/vhost.template`. Sie können damit unterschiedliche Modulsätze für verschiedene virtuelle Hosts bereitstellen.

`default-server.conf`

Diese Datei enthält eine globale Konfiguration für virtuelle Hosts mit vernünftigen Standardeinstellungen. Statt die Werte in dieser Datei zu ändern, sollten Sie sie in der virtuellen Hostkonfiguration überschreiben.

`errors.conf`

Diese Datei legt fest, wie Apache auf Fehler reagiert. Wenn Sie die Meldungen für alle virtuellen Hosts ändern möchten, können Sie diese Datei bearbeiten. Anderenfalls sollten Sie die entsprechenden Direktiven in den virtuellen Hostkonfigurationen überschreiben.

`httpd.conf`

Dies ist die Hauptkonfigurationsdatei des Apache-Servers. Diese Datei sollten Sie nicht bearbeiten. Sie enthält in erster Linie Include-Anweisungen und globale Einstellungen. Globale Einstellungen können Sie in den in diesem Abschnitt aufgelisteten Konfigurationsdateien ändern. Host-spezifische Einstellungen wie `DocumentRoot` (absoluter Pfad) ändern Sie in der virtuellen Hostkonfiguration.

`listen.conf`

Diese Datei bindet Apache an bestimmte IP-Adressen und Ports. Außerdem konfiguriert diese Datei das namensbasierte virtuelle Hosting (siehe „[Namensbasierte virtuelle Hosts](#)“ (S. 410)).

`magic`

Diese Datei enthält Daten für das Modul `mime_magic`, mit dessen Hilfe Apache den MIME-Typ unbekannter Dateien ermittelt. Bearbeiten Sie diese Datei nicht.

`mime.types`

Diese Datei enthält die dem System bekannten MIME-Typen (genau genommen ist diese Datei eine Verknüpfung mit `/etc/mime.types`). Bearbeiten Sie diese Datei nicht. MIME-Typen, die hier nicht aufgelistet sind, sollten Sie der Datei `mod_mime-defaults.conf` hinzufügen.

`mod_*.conf`

Dies sind die Konfigurationsdateien der in der Standardinstallation enthaltenen Module. Weitere Informationen hierzu erhalten Sie unter [Abschnitt 22.4, „Installieren, Aktivieren und Konfigurieren von Modulen“](#) (S. 423). Die Konfigurationsdateien optionaler Module befinden sich im Verzeichnis `conf.d`.

`server-tuning.conf`

Diese Datei enthält Konfigurationsdirektiven für verschiedene MPMs (siehe [Abschnitt 22.4.4, „Multiprocessing-Module“](#) (S. 428)) und allgemeine Konfigurationsoptionen, die sich auf die Leistung von Apache auswirken. Sie können diese Datei bearbeiten, sollten den Webserver anschließend aber gründlich testen.

`ssl-global.conf` und `ssl.*`

Diese Dateien enthalten die globale SSL-Konfiguration und die SSL-Zertifikatdaten. Weitere Informationen hierzu erhalten Sie unter [Abschnitt 22.6, „Einrichten eines sicheren Webservers mit SSL“](#) (S. 435).

`sysconfig.d/*.conf`

Diese Konfigurationsdateien werden automatisch aus `/etc/sysconfig/apache2` generiert. Ändern Sie diese Dateien nicht. Bearbeiten Sie stattdessen die Dateien unter `/etc/sysconfig/apache2`. Fügen Sie diesem Verzeichnis auch keine weiteren Konfigurationsdateien hinzu.

`uid.conf`

Diese Datei gibt die Benutzer- und Gruppen-ID an, unter der Apache läuft. Bearbeiten Sie diese Datei nicht.

`vhosts.d/*.conf`

In diese Dateien sollte Ihre virtuelle Hostkonfiguration gespeichert werden. Das Verzeichnis enthält Vorlagen für virtuelle Hosts mit und ohne SSL. Jede Datei in diesem Verzeichnis mit der Erweiterung `.conf` ist automatisch Bestandteil der Apache-Konfiguration. Weitere Informationen finden Sie unter „**Virtuelle Hostkonfiguration**“ (S. 409).

Virtuelle Hostkonfiguration

Virtueller Host *bezieht sich auf die Fähigkeit von Apache, mehrere URIs (Universal Resource Identifiers) vom gleichen physischen Computer aus bedienen zu können.* Dies bedeutet, dass mehrere Domänen wie `www.example.com` und `www.example.net` von einem einzigen Webserver auf einem physischen Rechner ausgeführt werden können.

Virtuelle Hosts werden häufig eingesetzt, um Verwaltungsaufwand (nur ein Webserver muss verwaltet werden) und Hardware-Kosten (für die einzelnen Domänen ist kein dedizierter Server erforderlich) zu sparen. Virtuelle Hosts können auf Namen, IP-Adressen oder Ports basieren.

Virtuelle Hosts können mit YaST (siehe „**Virtuelle Hosts**“ (S. 417)) oder manuell durch Bearbeitung einer Konfigurationsdatei konfiguriert werden. In openSUSE ist Apache unter `/etc/apache2/vhosts.d/` standardmäßig für eine Konfigurationsdatei pro virtuellen Host vorbereitet. Alle Dateien in diesem Verzeichnis mit der Erweiterung `.conf` sind automatisch Bestandteil der Konfiguration. Außerdem enthält dieses Verzeichnis eine grundlegende Vorlage für virtuelle Hosts (`vhost.template` bzw. `vhost-ssl.template` für einen virtuellen Host mit SSL-Unterstützung).

TIPP: Erstellen Sie immer eine virtuelle Hostkonfiguration.

Es empfiehlt sich, immer eine virtuelle Hostkonfiguration zu erstellen, selbst dann, wenn der Webserver nur eine Domäne enthält. Dadurch fassen Sie nicht nur die gesamte domänenspezifische Konfiguration in einer einzigen Datei zusammen, sondern Sie können auch jederzeit auf eine funktionierende Basis-konfiguration zurückgreifen, indem Sie einfach die Konfigurationsdatei des virtuellen Hosts verschieben, löschen oder umbenennen. Aus dem gleichen

Grund sollten Sie auch für jeden virtuellen Host eine eigene Konfigurationsdatei erstellen.

Der `<VirtualHost></VirtualHost>`-Block enthält die Informationen zu einer bestimmten Domäne. Wenn Apache eine Client-Anforderung für einen definierten virtuellen Host empfängt, verwendet es die in diesem Block angegebenen Direktiven. Nahezu alle Direktiven können auch im Kontext eines virtuellen Hosts verwendet werden. Weitere Informationen zu den Konfigurationsdirektiven von Apache finden Sie unter <http://httpd.apache.org/docs/2.2/mod/quickreference.html>.

Namensbasierte virtuelle Hosts

Namensbasierte virtuelle Hosts können an jeder IP-Adresse mehrere Websites bedienen. Apache verwendet das Hostfeld in dem vom Client übersandten HTTP-Header, um die Anforderung mit einem übereinstimmenden `ServerName`-Eintrag der virtuellen Hostdeklarationen zu verbinden. Wird kein übereinstimmender `ServerName` gefunden, dann wird der erste angegebene virtuelle Host als Standard verwendet.

Die Direktive `NameVirtualHost` teilt Apache mit, welche IP-Adresse (und optional welcher Port) auf Client-Anforderungen mit dem Domänennamen im HTTP-Header überwacht werden soll. Diese Option wird in der Konfigurationsdatei `/etc/apache2/listen.conf` konfiguriert.

Als erstes Argument kann der vollständig qualifizierte Domänenname eingegeben werden – empfohlen wird aber die IP-Adresse. Das zweite, optionale Argument ist der Port. Dieser ist standardmäßig Port 80 und wird mit der `Listen`-Direktive konfiguriert.

Sowohl für die IP-Adresse als auch für die Portnummer kann ein Platzhalterzeichen (*) eingegeben werden. In diesem Fall werden die Anforderungen an allen Schnittstellen empfangen. IPv6-Adressen müssen in eckigen Klammern eingeschlossen sein.

Beispiel 22.1 *Beispiele für namensbasierte VirtualHost-Einträge*

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.3.100:80
NameVirtualHost 192.168.3.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:364::]:80
```

In einer namensbasierten virtuellen Hostkonfiguration übernimmt das `VirtualHost`-Anfangstag die zuvor unter `NameVirtualHost` deklarierte IP-Adresse (bzw. den vollständig qualifizierten Domännennamen) als Argument. Eine mit der `NameVirtualHost`-Direktive deklarierte Portnummer ist optional.

Anstelle der IP-Adresse wird auch ein Platzhalterzeichen (*) akzeptiert. Diese Syntax ist allerdings nur in Verbindung mit einem Platzhalter in `NameVirtualHost` * zulässig. IPv6-Adressen müssen in eckige Klammern eingeschlossen werden.

Beispiel 22.2 Namensbasierte `VirtualHost`-Direktiven

```
<VirtualHost 192.168.3.100:80>
...
</VirtualHost>

<VirtualHost 192.168.3.100>
...
</VirtualHost>

<VirtualHost *:80>
...
</VirtualHost>

<VirtualHost *>
...
</VirtualHost>

<VirtualHost [2002:c0a8:364::]>
...
</VirtualHost>
```

IP-basierte virtuelle Hosts

Bei dieser alternativen virtuellen Hostkonfiguration werden auf einem Computer mehrere IPs eingerichtet. Auf einer Apache-Instanz befinden sich mehrere Domänen, denen jeweils eine eigene IP zugewiesen ist.

Auf dem physischen Server muss für jeden IP-basierten virtuellen Host eine eigene IP-Adresse eingerichtet sein. Falls der Computer nicht über die entsprechende Anzahl an Netzwerkkarten verfügt, können auch virtuelle Netzwerkschnittstellen verwendet werden (IP-Aliasing).

Das folgende Beispiel zeigt Apache auf einem Computer mit der IP `192.168.3.100`, auf dem sich zwei Domänen mit den zusätzlichen IPs `192.168.3.101` und

192.168.3.102 befinden. Für jeden virtuellen Server wird ein eigener `VirtualHost`-Block benötigt.

Beispiel 22.3 *IP-basierte VirtualHost-Direktiven*

```
<VirtualHost 192.168.3.101>
  ...
</VirtualHost>

<VirtualHost 192.168.3.102>
  ...
</VirtualHost>
```

In diesem Beispiel sind die `VirtualHost`-Direktiven nur für Schnittstellen angegeben, die nicht `192.168.3.100` sind. Wenn für `192.168.3.100` auch eine `Listen`-Direktive konfiguriert ist, muss ein eigener IP-basierter Host eingerichtet werden, um die HTTP-Anforderungen an diese Schnittstelle zu erfüllen. Andernfalls werden die Direktiven aus der Standardserverkonfiguration (`/etc/apache2/default-server.conf`) angewendet.

Basiskonfiguration eines virtuellen Hosts

Die Konfiguration eines virtuellen Hosts sollte mindestens die folgenden Direktiven enthalten. Weitere Optionen finden Sie in `/etc/apache2/vhosts.d/vhost.template`.

`ServerName`

Der vollständig qualifizierte Domänenname, unter dem der Host angesprochen wird.

`DocumentRoot`

Der absolute Pfad des Verzeichnisses, aus dem Apache die Dateien für diesen Host bedient. Aus Sicherheitsgründen ist standardmäßig auf das gesamte Dateisystem kein Zugriff möglich. Sie müssen dieses Verzeichnis daher explizit innerhalb eines `Directory`-Containers entsperren.

`ServerAdmin`

Hier geben Sie die E-Mail-Adresse des Serveradministrators ein. Diese Adresse ist beispielsweise auf den von Apache erstellten Fehlerseiten angegeben.

ErrorLog

Das Fehlerprotokoll dieses virtuellen Hosts. Ein eigenes Fehlerprotokoll für jeden virtuellen Host ist zwar nicht zwingend erforderlich, jedoch durchaus üblich, da dies die Fehlersuche erleichtert. `/var/log/apache2/` ist das Standardverzeichnis für die Protokolldateien von Apache.

CustomLog

Das Zugriffsprotokoll dieses virtuellen Hosts. Ein eigenes Zugriffsprotokoll für jeden virtuellen Host ist zwar nicht zwingend erforderlich, jedoch durchaus üblich, da dies eine separate Analyse der Zugriffsdaten für jeden einzelnen Host ermöglicht. `/var/log/apache2/` ist das Standardverzeichnis für die Protokolldateien von Apache.

Wie bereits erwähnt, ist standardmäßig auf das gesamte Dateisystem kein Zugriff möglich. Die Verzeichnisse, in die Sie die Dateien gestellt haben, mit denen Apache arbeiten soll – zum Beispiel das Verzeichnis `DocumentRoot` –, müssen daher explizit entsperrt werden:

```
<Directory "/srv/www/www.example.com/htdocs">
  Order allow,deny
  Allow from all
</Directory>
```

Die vollständige Basiskonfiguration eines virtuellen Hosts sieht wie folgt aus:

Beispiel 22.4 *Basiskonfiguration eines virtuellen Hosts*

```
<VirtualHost 192.168.3.100>
  ServerName www.example.com;
  DocumentRoot /srv/www/www.example.com/htdocs
  ServerAdmin webmaster@example.com
  ErrorLog /var/log/apache2/www.example.com_log
  CustomLog /var/log/apache2/www.example.com-access_log common
  <Directory "/srv/www/www.example.com/htdocs">
    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

22.2.2 Konfigurieren von Apache mit YaST

Um Ihren Webserver mit YaST zu konfigurieren, starten Sie YaST und wählen Sie *Netzwerkdienste > HTTP-Server*. Wenn Sie dieses Modul zum ersten Mal starten, wird der `HTTP-Server-Wizard` geöffnet. Dort müssen Sie einige administrative Einstel-

lungen vornehmen. Nach Ausführung des Assistenten wird das unter „**HTTP-Server-Konfiguration**“ (S. 418) beschriebene Dialogfeld geöffnet, sobald Sie das *HTTP-Server*-Modul aufrufen.

HTTP-Server-Wizard

Der HTTP-Server-Wizard besteht aus fünf Schritten. Im letzten Schritt des Assistenten haben Sie die Möglichkeit, den Expertenkonfigurationsmodus aufzurufen, in dem Sie weitere spezielle Einstellungen vornehmen können.

Netzwerkgeräteauswahl

Geben Sie hier die Netzwerkschnittstellen und -ports an, die von Apache auf eingehende Anfragen überwacht werden. Sie können eine beliebige Kombination aus bestehenden Netzwerkschnittstellen und zugehörigen IP-Adressen auswählen. Sie können Ports aus allen drei Bereichen (Well-Known-Ports, registrierte Ports und dynamische oder private Ports) verwenden, sofern diese nicht für andere Dienste reserviert sind. Die Standard-einstellung ist die Überwachung aller Netzwerkschnittstellen (IP-Adressen) an Port 80.

Aktivieren Sie *Firewalls für gewählte Ports öffnen*, um die vom Webserver überwachten Ports in der Firewall zu öffnen. Dies ist erforderlich, um den Webserver im Netzwerk (LAN, WAN oder Internet) verfügbar zu machen. Das Schließen des Ports ist nur in Testsituationen sinnvoll, in denen kein externer Zugriff auf den Webserver erforderlich ist.

Klicken Sie auf *Weiter*, um mit der Konfiguration fortzufahren.

Module

Mit dieser *Konfigurationsoption aktivieren bzw. deaktivieren Sie die vom Webserver unterstützten Skriptsprachen*. Informationen zur Aktivierung bzw. Deaktivierung anderer Module erhalten Sie unter „**Servermodule**“ (S. 420). Klicken Sie auf *Weiter*, um das nächste Dialogfeld zu öffnen.

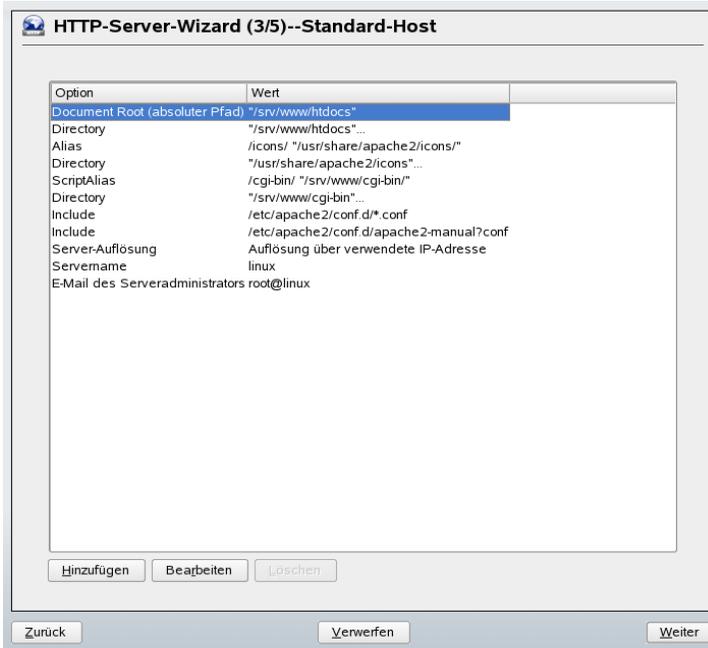
Standardhost

Diese Option betrifft den Standard-Webserver. Wie in „**Virtuelle Hostkonfiguration**“ (S. 409) beschrieben, kann Apache von einem einzigen Computer mehrere virtuelle Hosts bedienen. Der erste in der Konfigurationsdatei deklarierte virtuelle Host wird im

Allgemeinen als *Standardhost* bezeichnet. Alle nachfolgenden virtuellen Hosts übernehmen die Konfiguration des Standardhosts.

Wenn Sie die Hosteinstellungen (auch als *Direktiven* bezeichnet) bearbeiten möchten, wählen Sie den entsprechenden Eintrag in der Tabelle aus und klicken Sie auf *Bearbeiten*. Zum Hinzufügen neuer Direktiven klicken Sie auf *Hinzufügen*. Zum Löschen einer Direktive wählen Sie die Direktive aus und klicken Sie auf *Löschen*.

Abbildung 22.1 HTTP-Server-Wizard: Standardhost



Für den Server gelten folgende Standardeinstellungen:

Document-Root

Der absolute Pfad des Verzeichnisses, aus dem Apache die Dateien für diesen Host bedient. Dies ist standardmäßig `/srv/www/htdocs`.

Alias

Mithilfe von Alias-Direktiven können URL-Adressen physischen Speicherorten im Dateisystem zugeordnet werden. Dies bedeutet, dass über eine URL sogar auf

Pfade im Dateisystem außerhalb des `Document Root` zugegriffen werden kann, sofern die URL via Aliasing auf diesen Pfad verweist.

Der vorgegebene `openSUSE-Alias` für die in der Verzeichnisindex-Ansicht angezeigten Apache-Symbole, `/icons`, verweist auf `/usr/share/apache2/icons`.

`ScriptAlias`

Ähnlich wie die `Alias`-Direktive ordnet die `ScriptAlias`-Direktive eine URL einem Speicherort im Dateisystem zu. Der Unterschied besteht darin, dass `ScriptAlias` als Zielverzeichnis einen CGI-Speicherort für die Ausführung von CGI-Skripten festlegt.

`Verzeichnis`

Unter dieser Einstellung können Sie mehrere Konfigurationsoptionen zusammenfassen, die nur für das angegebene Verzeichnis gelten.

Hier werden auch die Zugriffs- und Anzeigooptionen für die Verzeichnisse `/usr/share/apache2/icons` und `/srv/www/cgi-bin` konfiguriert. Eine Änderung dieser Standardeinstellungen sollte nicht erforderlich sein.

`Einbeziehen`

Hier können weitere Konfigurationsdateien hinzugefügt werden. Zwei `Include`-Direktiven sind bereits vorkonfiguriert: `/etc/apache2/conf.d/` ist das Verzeichnis für die Konfigurationsdateien externer Module. Durch diese Direktive werden alle Dateien in diesem Verzeichnis mit der Erweiterung `.conf` eingeschlossen. Durch die zweite Direktive, `/etc/apache2/conf.d/apache2-manual.conf`, wird die Konfigurationsdatei `apache2-manual` eingeschlossen.

`Servername`

Hier wird die Standard-URL festgelegt, über die Clients den Webserver kontaktieren. Verwenden Sie einen qualifizierten Domännennamen (FQDN), um den Webserver unter `http://FQDN/` zu erreichen. Alternativ können Sie auch die IP-Adresse verwenden. Sie können hier keinen willkürlichen Namen eingeben. Der Server muss unter diesem Namen „bekannt“ sein.

`E-Mail des Serveradministrators`

Hier geben Sie die E-Mail-Adresse des Serveradministrators ein. Diese Adresse ist beispielsweise auf den von Apache erstellten Fehlerseiten angegeben.

Klicken Sie am Ende der Seite *Standardhost* auf *Weiter*, um mit der Konfiguration fortzufahren.

Virtuelle Hosts

In diesem Schritt zeigt der Assistent eine Liste der bereits konfigurierten virtuellen Hosts an (siehe „[Virtuelle Hostkonfiguration](#)“ (S. 409)). Wenn Sie vor dem Starten des YaST-HTTP-Assistenten keine manuellen Änderungen vorgenommen haben, ist kein virtueller Host vorhanden.

Zum Hinzufügen eines Hosts klicken Sie auf *Hinzufügen* und geben Sie im daraufhin geöffneten Dialogfeld die grundlegenden Informationen über den neuen Host ein. *Unter* Server-Identifikation geben Sie den Servernamen, das root-Verzeichnis für die Serverinhalte (`DocumentRoot`) und die E-Mail-Adresse des Administrators an. *Unter* Server-Auflösung legen Sie fest, wie der Host identifiziert wird (nach seinem Namen oder nach seiner IP-Adresse). Geben Sie den Namen oder die IP-Adresse unter *Change Virtual Host ID* (Virtuelle Host-ID ändern) an.

Klicken Sie auf *Weiter*, um mit dem zweiten Teil der virtuellen Hostkonfiguration fortzufahren.

Im zweiten Teil der virtuellen Hostkonfiguration legen Sie fest, ob CGI-Skripten zugelassen sind und welches Verzeichnis für diese Skripten verwendet wird. Dort können Sie auch SSL aktivieren. Wenn Sie SSL aktivieren, müssen Sie auch den Zertifikatpfad angeben. Informationen über SSL und Zertifikate finden Sie in [Abschnitt 22.6.2, „Konfigurieren von Apache mit SSL“](#) (S. 441). Mit der Option *Verzeichnisindex* geben Sie an, welche Datei angezeigt wird, wenn der Client ein Verzeichnis anfordert (standardmäßig ist dies die Datei `index.html`). Statt der Standardeinstellung können Sie aber auch ein oder mehrere andere Dateinamen (jeweils getrennt durch ein Leerzeichen) angeben. Mit *Öffentliches HTML aktivieren* stellen Sie den Inhalt der öffentlichen Benutzerverzeichnisse (`~user/public_html/`) auf dem Server unter `http://www.example.com/~user` bereit.

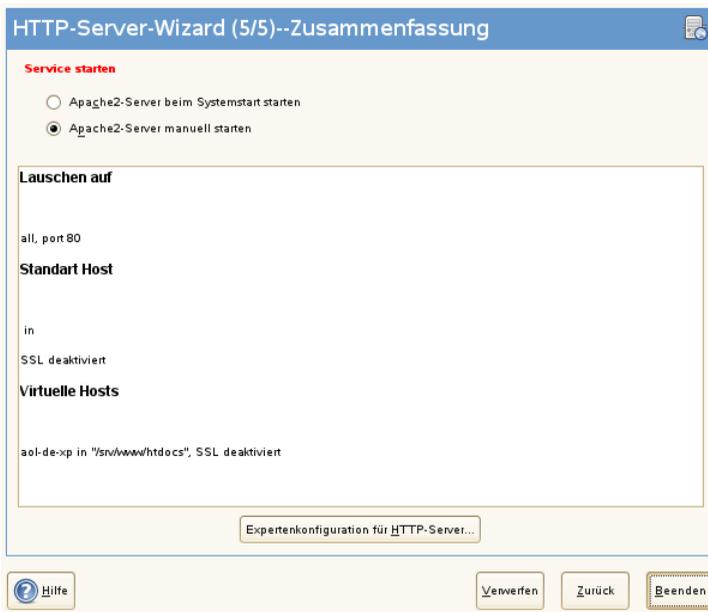
WICHTIG: Erstellen virtueller Hosts

Virtuelle Hosts können Sie nicht völlig willkürlich hinzufügen. Wenn Sie namensbasierte virtuelle Hosts hinzufügen möchten, müssen die Hostnamen im Netzwerk aufgelöst sein. Bei IP-basierten virtuellen Hosts darf jeder verfügbaren IP-Adresse nur ein Host zugewiesen sein.

Zusammenfassung

Dies ist der abschließende Schritt des Assistenten. Legen Sie hier fest, wie und wann der Apache-Server gestartet werden soll: beim Boot-Vorgang oder manuell. Außerdem erhalten Sie in diesem Schritt eine kurze Zusammenfassung Ihrer bisherigen Konfiguration. Wenn Sie mit den Einstellungen zufrieden sind, schließen Sie die Konfiguration mit *Verlassen* ab. Möchten Sie Einstellungen ändern, dann klicken Sie so oft auf *Zurück*, bis das entsprechende Dialogfeld angezeigt wird. Über *Expertenkonfiguration für HTTP-Server* können Sie hier auch das in „**HTTP-Server-Konfiguration**“ (S. 418) beschriebene Dialogfeld öffnen.

Abbildung 22.2 *HTTP-Server-Wizard: Zusammenfassung*



HTTP-Server-Konfiguration

Im Dialogfeld *HTTP-Server-Konfiguration* können Sie weitaus mehr Einstellungen vornehmen als im Assistenten (dieser wird ohnehin nur bei der Anfangskonfiguration des Webservers ausgeführt). Das Dialogfeld enthält vier Registerkarten, die nachfolgend beschrieben werden. Keine der in diesem Dialogfeld vorgenommenen Konfigurationsänderungen wird sofort wirksam. Die Änderungen werden erst wirksam, wenn Sie das

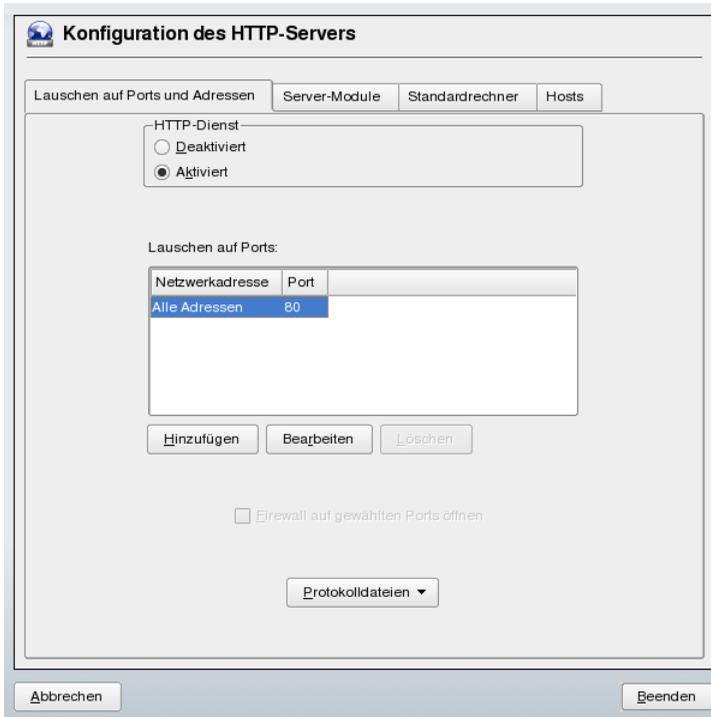
Dialogfeld mit *Verlassen* schließen. Klicken Sie hingegen auf *Abbrechen*, so verlassen Sie das Konfigurationsmodul und Ihre Konfigurationsänderungen werden verworfen.

Listen Ports and Addresses (Überwachte Ports und Adressen)

Geben Sie unter *HTTP-Dienst* an, ob Apache laufen soll (*Aktiviert*) oder beendet werden soll (*Deaktiviert*). Mit den Schaltflächen *Hinzufügen*, *Bearbeiten* und *Löschen* geben Sie unter *Ports überwachen* die Adressen und Ports an, die vom Server überwacht werden sollen. Standardmäßig werden alle Schnittstellen an Port 80 überwacht. Vergessen Sie nicht, das Kontrollkästchen *Firewall auf gewählten Ports öffnen* zu aktivieren. Anderenfalls wäre der Webserver von außen nicht erreichbar. Das Schließen des Ports ist nur in Testsituationen sinnvoll, in denen kein externer Zugriff auf den Webserver erforderlich ist.

Über die Schaltfläche *Protokolldateien* können Sie das Zugriffs- oder das Fehlerprotokoll überwachen. Diese Funktion ist besonders beim Testen der Konfiguration hilfreich. Die Protokolldatei wird in einem eigenen Fenster geöffnet, aus dem Sie den Webserver auch neu starten oder neu laden können (siehe **Abschnitt 22.3, „Starten und Beenden von Apache“** (S. 421)). Diese Befehle werden sofort ausgeführt.

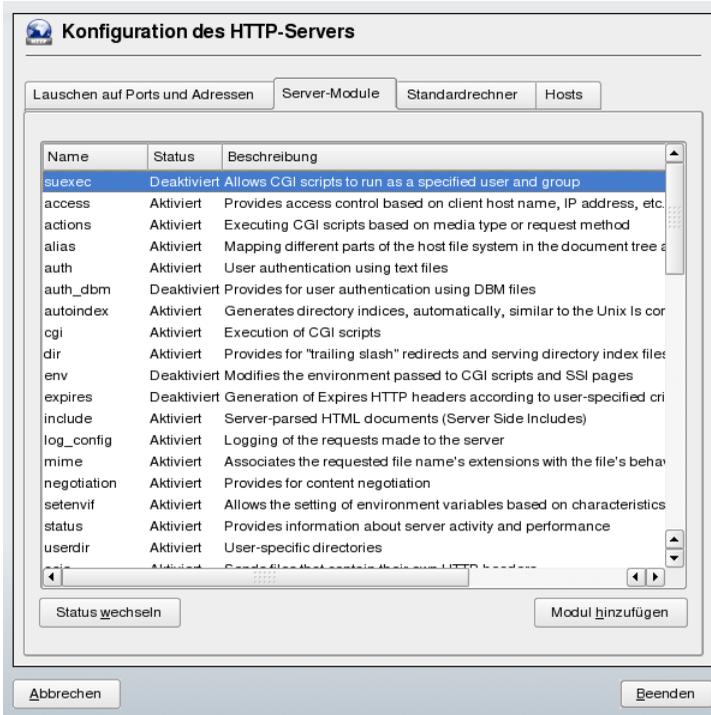
Abbildung 22.3 *Konfiguration des HTTP-Servers: Überwachen von Ports und Adressen*



Servermodule

Über *Status wechseln* können Sie Apache2-Module aktivieren und deaktivieren. Über *Modul hinzufügen* können Sie weitere Module hinzufügen, die zwar bereits installiert, aber noch nicht in dieser Liste aufgeführt sind. Weitere Informationen über Module finden Sie in [Abschnitt 22.4, „Installieren, Aktivieren und Konfigurieren von Modulen“](#) (S. 423).

Abbildung 22.4 Konfiguration des HTTP-Servers: Server-Module



Haupthost oder Hosts

Diese Dialogfelder sind mit den bereits beschriebenen identisch. in „Standardhost“ (S. 414) und „Virtuelle Hosts“ (S. 417) beschriebenen Dialogfeldern.

22.3 Starten und Beenden von Apache

Bei einer Konfiguration in YaST (siehe [Abschnitt 22.2.2, „Konfigurieren von Apache mit YaST“](#) (S. 413)) wird Apache beim Systemstart in Runlevel 3 und 5 gestartet und in Runlevel 0, 1, 2 und 6 beendet. Dieses Verhalten können Sie im Runlevel-Editor von YaST oder mit dem Kommandozeilenprogramm `chkconfig` ändern.

Zum Starten, Beenden oder Manipulieren von Apache auf einem laufenden System verwenden Sie das init-Skript `/usr/sbin/rcapache2` (allgemeine Informationen

zu init-Skripten erhalten Sie unter [Abschnitt 8.2.2, „Init-Skripten“](#) (S. 137)). Der Befehl `rcapache2` akzeptiert folgende Parameter:

`status`

Überprüft, ob Apache gestartet wurde.

`start`

Startet Apache, sofern es noch nicht läuft.

`startssl`

Startet Apache mit SSL-Unterstützung, sofern es noch nicht läuft. Weitere Informationen zu der SSL-Unterstützung finden Sie unter [Abschnitt 22.6, „Einrichten eines sicheren Webservers mit SSL“](#) (S. 435).

`stop`

Stoppt Apache durch Beenden des übergeordneten Prozesses.

`restart`

Beendet Apache und startet es danach neu. Falls der Webserver noch nicht gelaufen ist, wird er nun gestartet.

`try-restart`

Beendet Apache und startet es danach neu, sofern der Webserver bereits gelaufen ist.

`reload` oder `graceful`

Beendet den Webserver erst, nachdem alle durch Forking erstellten Apache-Prozesse aufgefordert wurden, ihre Anforderungen vor dem Herunterfahren zu Ende zu führen. Anstelle der beendeten Prozesse werden neue Prozesse gestartet. Dies führt zu einem vollständigen „Neustart“ von Apache.

TIPP

In Produktionsumgebungen ist `rcapache2 reload` die bevorzugte Methode für einen Neustart von Apache (der z. B. ausgeführt wird, damit eine Konfigurationsänderung wirksam wird). Für die Clients kommt es dabei zu keinen Verbindungsabbrüchen.

`configtest` oder `extreme-configtest`

Überprüft die Syntax der Konfigurationsdateien, ohne den laufenden Webserver zu beeinträchtigen. Da dieser Test beim Starten, Neuladen oder Neustarten des Servers automatisch durchgeführt wird, ist eine explizite Ausführung des Tests in der Regel nicht notwendig (bei einem Konfigurationsfehler wird der Webserver ohnehin nicht gestartet, neu geladen oder neu gestartet). Mithilfe der Option `extreme-configtest` wird der Webserver unter dem Benutzernamen `nobody` gestartet und die Konfiguration wird geladen, sodass mehr Fehler gefunden werden können. Beachten Sie, dass die SSL-Einrichtung nicht getestet werden kann, obwohl die Konfiguration geladen wurde, da SSL-Zertifikate nicht von `nobody` gelesen werden können.

`probe`

Überprüft, ob ein Neuladen des Webservers erforderlich ist (d. h., ob sich die Konfiguration geändert hat), und schlägt die erforderlichen Argumente für den Befehl `rcapache2` vor.

`server-status` und `full-server-status`

Erstellt einen Dump des kurzen oder vollständigen Statusfensters. Zur Ausführung des `rcapache2`-Befehls mit diesem Parameter muss entweder `lynx` oder `w3m` installiert sein und das `mod_status`-Modul muss aktiviert sein. Außerdem muss `/etc/sysconfig/apache2` unter `APACHE_SERVER_FLAGS` das Flag `status` enthalten.

TIPP: Weitere Flags

Weitere Flags, die Sie mit dem Befehl `rcapache2` angeben, werden direkt an den Webserver weitergeleitet.

22.4 Installieren, Aktivieren und Konfigurieren von Modulen

Die Apache-Software ist modular aufgebaut. Alle Funktionen außer einigen Kernaufgaben werden von Modulen durchgeführt. Dies geht sogar so weit, dass selbst HTTP durch ein Modul verarbeitet wird (`http_core`).

Apache-Module können bei der Entwicklung in die Apache-Binaries kompiliert oder während der Laufzeit dynamisch geladen werden. Informationen zum dynamischen Laden von Modulen erhalten Sie unter [Abschnitt 22.4.2, „Aktivieren und Deaktivieren von Modulen“](#) (S. 425).

Apache-Module lassen sich in vier Kategorien einteilen:

Basismodule

Basismodule sind standardmäßig in Apache enthalten. In Apache in SUSE Linux sind nur `mod_so` (zum Laden anderer Module) und `http_core` kompiliert. Alle anderen Module sind als gemeinsam genutzte Objekte verfügbar: Sie sind nicht in der Server-Binärdatei enthalten, sondern können zur Laufzeit eingebunden werden.

Erweiterungsmodule

Im Allgemeinen sind Erweiterungsmodule im Apache-Softwarepaket enthalten, jedoch nicht statisch im Server kompiliert. In openSUSE stehen diese Module als gemeinsame Objekte zur Verfügung, die während der Laufzeit in Apache geladen werden können.

Externe Module

Externe Module sind nicht in der offiziellen Apache-Distribution enthalten. openSUSE bietet jedoch einige externe Module an, die ohne großen Aufwand sofort verwendet werden können.

Multiprocessing-Module

Multiprocessing-Module (MPMs) sind dafür verantwortlich, Anforderungen an den Webserver anzunehmen und zu verarbeiten, und stellen damit das Kernstück der Webserver-Software dar.

22.4.1 Installieren von Modulen

Wenn Sie das Standardinstallationsverfahren für Apache durchgeführt haben (siehe [Abschnitt 22.1.2, „Installation“](#) (S. 404)), wird Apache mit allen Basis- und Erweiterungsmodulen sowie dem Multiprocessing-Modul Prefork und den externen Modulen `mod_php5` und `mod_python` installiert.

Sie können weitere externe Module installieren. Starten Sie dazu YaST und wählen Sie *Software > Software installieren oder löschen*. Wählen Sie danach *Filter > Suche* und suchen Sie nach *apache*. Die Ergebnisliste zeigt nun neben anderen Paketen alle verfügbaren externen Apache-Module an.

22.4.2 Aktivieren und Deaktivieren von Modulen

Die Skriptsprachenmodule PHP5, Perl, Python und Ruby können Sie in YaST mit der im Abschnitt „**HTTP-Server-Wizard**“ (S. 414) beschriebenen Modulkonfiguration aktivieren oder deaktivieren. Alle anderen Module werden, wie im Abschnitt „**Servermodule**“ (S. 420) beschrieben, aktiviert oder deaktiviert.

Manuell können Sie die Module mit den Befehlen `a2enmod mod_foo` oder `a2dismod mod_foo` aktivieren bzw. deaktivieren. `a2enmod -l` gibt eine Liste aller zurzeit aktiven Module aus.

WICHTIG: Einschließen der Konfigurationsdateien externer Module

Wenn Sie externe Module manuell aktivieren, müssen Sie sicherstellen, dass auch ihre Konfigurationsdateien in allen virtuellen Hostkonfigurationen geladen werden. Die Konfigurationsdateien externer Module befinden sich im Verzeichnis `/etc/apache2/conf.d/` und werden standardmäßig nicht geladen. Wenn Sie auf allen virtuellen Hosts die gleichen Module benötigen, können Sie die Konfigurationsdateien aus diesem Verzeichnis mit `*.conf` einschließen. Anderenfalls müssen Sie die Dateien einzeln einschließen. Beispiele hierzu finden Sie in der Datei `/etc/apache2/vhosts.d/vhost.template`.

22.4.3 Basis- und Erweiterungsmodule

Alle Basis- und Erweiterungsmodule werden ausführlich in der Apache-Dokumentation beschrieben. An dieser Stelle gehen wir daher nur kurz auf die wichtigsten Module ein. Informationen zu den einzelnen Modulen erhalten Sie auch unter <http://httpd.apache.org/docs/2.2/mod/>.

`mod_actions`

Bietet Methoden zur Ausführung eines Skripts, wenn ein bestimmter MIME-Typ (z. B. `application/pdf`), eine Datei mit einer bestimmten Erweiterung (z. B. `.rpm`) oder eine bestimmte Anforderungsmethode (z. B. `GET`) verlangt wird. Dieses Modul ist standardmäßig aktiviert.

mod_alias

Dieses Modul stellt die Direktiven `Alias` und `Redirect` bereit. Damit können Sie eine URI einem bestimmten Verzeichnis zuordnen (`Alias`) bzw. eine angeforderte URL umleiten. Dieses Modul ist standardmäßig aktiviert.

mod_auth*

Die Authentifizierungsmodule bieten verschiedene Methoden zur Authentifizierung: grundlegende Authentifizierung mit `mod_auth_basic` oder Digest-Authentifizierung mit `mod_auth_digest`. Die Digest-Authentifizierung in Apache 2.2 befindet sich noch im Versuchsstadium.

`mod_auth_basic` und `mod_auth_digest` müssen gemeinsam mit einem Authentifizierungsanbietermodul `mod_authn_*` (z. B. `mod_authn_file` für die Authentifizierung auf Basis einer Textdatei) und einem Autorisierungsmodul `mod_authz_*` (z. B. `mod_authz_user` für die Benutzerautorisierung) verwendet werden.

Weitere Informationen zu diesem Thema erhalten Sie im Artikel „Gewusst wie: Authentifizierung“ unter <http://httpd.apache.org/docs/2.2/howto/auth.html>.

mod_autoindex

Wenn keine Indexdatei vorhanden ist (z. B. `index.html`), generiert `mod_autoindex` Verzeichnislisten. Das Aussehen dieser Indizes kann konfiguriert werden. Dieses Modul ist standardmäßig aktiviert. Verzeichnislisten sind jedoch durch die `Options`-Direktive standardmäßig deaktiviert. Sie müssen diese Einstellung daher in Ihrer virtuellen Hostkonfiguration ändern. Die Standardkonfigurationsdatei dieses Moduls befindet sich unter `/etc/apache2/` und heißt `mod_autoindex-defaults.conf`.

mod_cgi

`mod_cgi` wird zur Ausführung von CGI-Skripten benötigt. Dieses Modul ist standardmäßig aktiviert.

mod_deflate

Mit diesem Modul kann Apache so konfiguriert werden, dass bestimmte Dateitypen automatisch vor der Bereitstellung komprimiert werden.

mod_dir

`mod_dir` stellt die `DirectoryIndex`-Direktive bereit, mit der Sie festlegen können, welche Dateien bei Anforderung eines Verzeichnisses automatisch

zurückgegeben werden (standardmäßig `index.html`). Außerdem leitet dieses Modul automatisch zur korrekten URI um, wenn in einer Verzeichnisanforderung der nachgestellte Schrägstrich fehlt. Dieses Modul ist standardmäßig aktiviert.

`mod_env`

Steuert die Umgebungsvariablen, die an CGI-Skripten oder SSI-Seiten übergeben werden. Sie können Umgebungsvariablen festlegen oder aufheben oder von der Shell übergeben, die den `httpd`-Prozess aufgerufen hat. Dieses Modul ist standardmäßig aktiviert.

`mod_expires`

Mit `mod_expires` legen Sie fest, wie häufig Ihre Dokumente über Proxy- und Browser-Caches durch Zustellung eines `Expires`-Header aktualisiert werden. Dieses Modul ist standardmäßig aktiviert.

`mod_include`

`mod_include` ermöglicht die Verwendung von serverseitigen Includes (SSI), die die grundlegende Funktionalität für die dynamische Generierung von HTML-Seiten bereitstellen. Dieses Modul ist standardmäßig aktiviert.

`mod_info`

Dieses Modul stellt unter `http://localhost/server-info/` eine umfassende Übersicht über die Serverkonfiguration bereit. Aus Sicherheitsgründen sollte der Zugriff auf diese URL generell eingeschränkt sein. Standardmäßig erhält nur `localhost` Zugriff auf diese URL. `mod_info` wird in der Datei `/etc/apache2/mod_info.conf` konfiguriert.

`mod_log_config`

Mit diesem Modul konfigurieren Sie den Aufbau der Apache-Protokolldateien. Dieses Modul ist standardmäßig aktiviert.

`mod_mime`

Dieses Modul sorgt dafür, dass eine Datei auf Basis seiner Dateinamenerweiterung mit dem korrekten MIME-Header bereitgestellt wird (z. B. `text/html` für HTML-Dokumente). Dieses Modul ist standardmäßig aktiviert.

`mod_negotiation`

Dieses Modul ist für die Inhaltsverhandlung erforderlich. Weitere Informationen erhalten Sie unter <http://httpd.apache.org/docs/2.2/content-negotiation.html>. Dieses Modul ist standardmäßig aktiviert.

mod_rewrite

Dieses Modul stellt die gleiche Funktionalität wie mod_alias bereit, bietet aber mehr Funktionen und ist somit flexibler. Mit mod_rewrite können Sie URLs auf Basis verschiedener Regeln umleiten, Header anfordern und einiges mehr.

mod_setenvif

Legt Umgebungsvariablen auf der Basis von Details aus der Client-Anforderung fest, z. B. die Browserzeichenfolge, die der Client sendet, oder die IP-Adresse des Clients. Dieses Modul ist standardmäßig aktiviert.

mod_speling

mod_speling versucht, typografische Fehler in URLs, beispielsweise die Groß-/Kleinschreibung, automatisch zu korrigieren.

mod_ssl

Dieses Modul ermöglicht verschlüsselte Verbindungen zwischen dem Webserver und den Clients. Weitere Informationen finden Sie in [Abschnitt 22.6, „Einrichten eines sicheren Webservers mit SSL“](#) (S. 435). Dieses Modul ist standardmäßig aktiviert.

mod_status

Dieses Modul stellt unter `http://localhost/server-status/` Informationen über die Aktivität und Leistung des Servers bereit. Aus Sicherheitsgründen sollte der Zugriff auf diese URL generell eingeschränkt sein. Standardmäßig erhält nur localhost Zugriff auf diese URL. mod_status wird in der Datei `/etc/apache2/mod_status.conf` konfiguriert.

mod_suexec

Dieses Modul ermöglicht die Ausführung von CGI-Skripten unter einem anderen Benutzer oder einer anderen Gruppe. Dieses Modul ist standardmäßig aktiviert.

mod_userdir

Dieses Modul ermöglicht benutzerspezifische Verzeichnisse unter `~user/`. In der Konfiguration muss die `UserDir`-Direktive angegeben sein. Dieses Modul ist standardmäßig aktiviert.

22.4.4 Multiprocessing-Module

openSUSE bietet zwei Multiprocessing-Module (MPMs) für Apache.

Prefork-MPM

Das Prefork-MPM implementiert einen Prefork-Webserver, der keine Threads verwendet. Mit diesem Modul verhält sich der Webserver, was die Handhabung von Anforderungen betrifft, ähnlich wie Apache Version 1.x: Er isoliert jede einzelne Anforderung und verarbeitet sie in einem separaten untergeordneten Prozess (Forking). Eine Beeinträchtigung aller Anforderungen durch wenige problematische Anforderungen und somit eine Sperre des Webserver lassen sich dadurch vermeiden.

Die prozessbasierte Vorgehensweise des Prefork-MPM bietet zwar Stabilität, konsumiert aber mehr Systemressourcen wie das Worker-MPM. Für UNIX-basierte Betriebssysteme gilt das Prefork-MPM als Standard-MPM.

WICHTIG: MPMs in diesem Dokument

In diesem Dokument wird davon ausgegangen, dass Apache mit dem Prefork-MPM verwendet wird.

Worker-MPM

Das Worker-MPM implementiert einen Multithread-Webserver. Ein Thread ist die „Lightweight-Version“ eines Prozesses. Der Vorteil von Threads gegenüber Prozessen ist deren geringerer Ressourcenkonsum. Anstatt lediglich untergeordnete Prozesse zu erstellen (Forking), verarbeitet das Worker-MPM Anforderungen durch Threads mit Serverprozessen. Die untergeordneten Prefork-Prozesse sind auf mehrere Threads verteilt (Multithreading). Diese Ansatzweise macht den Apache-Server durch den geringeren Ressourcenkonsum leistungsfähiger als mit dem Prefork-MPM.

Ein Hauptnachteil ist die Instabilität des Worker-MPM: Ein fehlerhafter Thread kann sich auf alle Threads eines Prozesses auswirken. Im schlimmsten Fall fällt der Server dadurch aus. Besonders bei gleichzeitiger Verwendung der Common Gateway Interface (CGI) auf einem überlasteten Apache-Server kann es zu internen Serverfehlern kommen, da Threads in diesem Fall unter Umständen nicht in der Lage sind, mit den Systemressourcen zu kommunizieren. Gegen die Verwendung des Worker-MPM in Apache spricht auch die Tatsache, dass nicht alle verfügbaren Apache-Module Thread-sicher sind und daher nicht in Verbindung mit dem Worker-MPM eingesetzt werden können.

WARNUNG: Verwendung von PHP-Modulen mit MPMs

Nicht alle verfügbaren PHP-Module sind Thread-sicher. Von einer Verwendung des Worker-MPM in Verbindung mit mod_php wird daher abgeraten.

22.4.5 Externe Module

Nachfolgend finden Sie eine Liste aller externen Module, die mit openSUSE ausgeliefert werden. Die Dokumentation zu den einzelnen Modulen finden Sie in den jeweils genannten Verzeichnissen.

mod_apparmor

Unterstützt Apache bei der Novell AppArmor-Einschränkung auf einzelne cgi-Skripten, die von Modulen wie mod_php5 und mod_perl benutzt werden.

Paketname: `apache2-mod_apparmor`

Weitere Informationen: *Novell AppArmor Administration Guide* (↑Novell AppArmor Administration Guide)

mod_mono

Mithilfe von mod_mono können Sie ASP.NET-Seiten auf Ihrem Server ausführen.

Paketname: `apache2-mod_mono`

Konfigurationsdatei: `/etc/apache2/conf.d/mod_mono.conf`

mod_perl

mod_perl ermöglicht die Ausführung von Perl-Skripten in einem eingebetteten Interpreter. Durch den dauerhaften, im Server eingebetteten Interpreter lassen sich Verzögerungen durch den Start eines externen Interpreters und den Start von Perl vermeiden.

Paketname: `apache2-mod_perl`

Konfigurationsdatei: `/etc/apache2/conf.d/mod_perl.conf`

Weitere Informationen: `/usr/share/doc/packages/apache2-mod_perl`

mod_php5

PHP ist eine serverseitige, plattformübergreifende, in HTML eingebettete Skriptsprache.

Paketname: `apache2-mod_php5`
Konfigurationsdatei: `/etc/apache2/conf.d/php5.conf`
Weitere Informationen: `/usr/share/doc/packages/apache2-mod_php5`

`mod_python`

`mod_python` bettet Python in den Apache-Webserver ein. Dies bringt Ihnen einen erheblichen Leistungsgewinn und zusätzliche Flexibilität bei der Entwicklung webbasierter Anwendungen.

Paketname: `apache2-mod_python`
Weitere Informationen: `/usr/share/doc/packages/apache2-mod_python`

`mod_tidy`

`mod_tidy` überprüft jede Ausgangs-HTML-Seite mithilfe der TidyLib. Im Falle eines Bestätigungsfehlers wird eine Seite mit einer Fehlerliste ausgegeben, andernfalls wird die Original-HTML-Seite ausgegeben.

Paketname: `apache2-mod_tidy`
Konfigurationsdatei: `/etc/apache2/mod_tidy.conf`
Weitere Informationen: `/usr/share/doc/packages/apache2-mod_tidy`

22.4.6 Kompilieren von Modulen

Apache kann von erfahrenen Benutzern durch selbst entwickelte Module erweitert werden. Für die Entwicklung eigener Apache-Module und für die Kompilierung von Drittanbieter-Modulen sind neben dem Paket `apache2-devel` auch die entsprechenden Entwicklungstools erforderlich. `apache2-devel` enthält unter anderem die `apxs2`-Tools, die zur Kompilierung von Apache-Erweiterungsmodulen erforderlich sind.

`apxs2` ermöglicht die Kompilierung und Installation von Modulen aus dem Quellcode (einschließlich der erforderlichen Änderungen an den Konfigurationsdateien). Dadurch ergeben sich *Dynamic Shared Objects* (DSOs), die während der Laufzeit in Apache geladen werden können.

Die Binaries von `apxs2` befinden sich unter `/usr/sbin`:

- `/usr/sbin/apxs2`: Für die Entwicklung von Erweiterungsmodulen, die mit allen MPMs verwendbar sind. Die Module werden im Verzeichnis `/usr/lib/apache2` installiert.
- `/usr/sbin/apxs2-prefork`: Für die Entwicklung von Prefork-MPM-Modulen geeignet. Die Module werden im Verzeichnis `/usr/lib/apache2-prefork` installiert.
- `/usr/sbin/apxs2-worker`: Für die Entwicklung von Worker-MPM-Modulen geeignet. Die Module werden im Verzeichnis `/usr/lib/apache2-worker` installiert.

Zur Installation und Aktivierung eines Moduls aus dem Quellcode verwenden Sie den Befehl `cd /Pfad/der/Modulquelle; apxs2 -cia mod_foo.c (-c kompiliert das Modul, -i installiert es und -a aktiviert es)`. Alle weiteren Optionen von `apxs2` werden auf der Manualpage `apxs2(1)` beschrieben.

22.5 Aktivieren von CGI-Skripten

Die Common Gateway Interface (CGI) von Apache ermöglicht die dynamische Erstellung von Inhalten mit Programmen bzw. so genannten CGI-Skripten. CGI-Skripten können in jeder beliebigen Programmiersprache geschrieben sein. In der Regel werden aber die Skriptsprachen Perl oder PHP verwendet.

Damit Apache in der Lage ist, die von CGI-Skripten erstellten Inhalte bereitzustellen, muss das Modul `mod_cgi` aktiviert sein. Außerdem ist `mod_alias` erforderlich. Beide Module sind standardmäßig aktiviert. Informationen zur Aktivierung von Modulen finden Sie unter [Abschnitt 22.4.2, „Aktivieren und Deaktivieren von Modulen“](#) (S. 425).

WARNUNG: CGI-Sicherheit

Die Zulassung der CGI-Skriptauführung auf dem Server ist ein Sicherheitsrisiko. Weitere Informationen finden Sie in [Abschnitt 22.7, „Vermeiden von Sicherheitsproblemen“](#) (S. 442).

22.5.1 Konfiguration in Apache

In openSUSE ist die Ausführung von CGI-Skripten nur im Verzeichnis `/srv/www/cgi-bin/` erlaubt. Dieses Verzeichnis ist bereits für die Ausführung von CGI-Skripten konfiguriert. Wenn Sie eine virtuelle Hostkonfiguration erstellt haben (siehe „**Virtuelle Hostkonfiguration**“ (S. 409)) und Ihre CGI-Skripten in einem Host-spezifischen Verzeichnis ablegen möchten, müssen Sie das betreffende Verzeichnis entsperren und für CGI-Skripten konfigurieren.

Beispiel 22.5 CGI-Konfiguration für virtuelle Hosts

```
ScriptAlias /cgi-bin/ "/srv/www/www.example.com/cgi-bin/"❶

<Directory "/srv/www/www.example.com/cgi-bin/">
  Options +ExecCGI❷
  AddHandler cgi-script .cgi .pl❸
  Order allow,deny❹
  Allow from all
</Directory>
```

- ❶ Fordert Apache auf, alle Dateien in diesem Verzeichnis als CGI-Skripten zu behandeln
- ❷ Aktiviert die Ausführung von CGI-Skripten
- ❸ Fordert den Server auf, Dateien mit den Erweiterungen `.pl` und `.cgi` als CGI-Skripten zu behandeln. passen Sie diese Anweisung entsprechend Ihren Anforderungen an
- ❹ Die `Order`- und `Allow`-Anweisungen legen den Standardzugriffsstatus sowie die Reihenfolge fest, in der `Allow`- und `Deny`-Anweisungen ausgewertet werden. in diesem Beispiel werden „deny“-Anweisungen vor „allow“-Anweisungen ausgewertet und der Zugriff ist von jedem Ort aus möglich.

22.5.2 Ausführen eines Beispielskripten

Die CGI-Programmierung unterscheidet sich von der herkömmlichen Programmierung insoweit, als CGI-Programmen und -Skripten ein MIME-Typ-Header wie `Content-type: text/html` vorangestellt werden muss. Dieser Header wird an den Client gesendet, damit er weiß, welchen Inhaltstyp er empfängt. Darüber hinaus muss die Skriptausgabe vom Client, in der Regel einem Webbrowser, verstanden werden.

In den meisten Fällen ist dies HTML, manchmal aber auch Klartext, Bilder oder Ähnliches.

Unter `/usr/share/doc/packages/apache2/test-cgi` stellt Apache ein einfaches Testskript bereit. Dieses Skript gibt den Inhalt einiger Umgebungsvariablen als Klartext aus. Wenn Sie dieses Skript ausprobieren möchten, kopieren Sie es in das Verzeichnis `/srv/www/cgi-bin/` bzw. in das Skriptverzeichnis Ihres virtuellen Hosts (`/srv/www/www.example.com/cgi-bin/`) und benennen Sie es in `test.cgi` um.

Über den Webserver zugängliche Dateien sollten dem `root`-Benutzer gehören (siehe auch [Abschnitt 22.7](#), „Vermeiden von Sicherheitsproblemen“ (S. 442)). Da der Webserver unter einem anderen Benutzer ausgeführt wird, müssen CGI-Skripten von jedermann ausgeführt und gelesen werden können. Wechseln Sie daher in das CGI-Verzeichnis und führen Sie den Befehl `chmod 755 test.cgi` aus, um die entsprechenden Berechtigungen einzurichten.

Rufen Sie danach `http://localhost/cgi-bin/test.cgi` oder `http://www.example.com/cgi-bin/test.cgi` auf. Nun sollte der „CGI/1.0-Testskriptbericht“ angezeigt werden.

22.5.3 Fehlersuche

Wenn Sie nach der Ausführung des CGI-Testskripten statt des Testskriptberichts eine Fehlermeldung erhalten, überprüfen Sie Folgendes:

CGI-Fehlerbehebung

- Haben Sie den Server nach der Konfigurationsänderung neu geladen? Überprüfen Sie dies mit `rcapache2 probe`.
- Falls Sie ein benutzerdefiniertes CGI-Verzeichnis eingerichtet haben, ist dieses richtig konfiguriert? Falls Sie sich nicht sicher sind, führen Sie das Skript im CGI-Standardverzeichnis `/srv/www/cgi-bin/` aus. Rufen Sie das Skript dazu mit `http://localhost/cgi-bin/test.cgi` auf.
- Wurden die richtigen Berechtigungen zugewiesen? Wechseln Sie in das CGI-Verzeichnis und führen Sie `ls -l test.cgi` aus. Die Befehlsausgabe sollte mit folgender Zeile beginnen:

```
-rwxr-xr-x 1 root root
```

- Überprüfen Sie das Skript auf Programmierfehler. Wenn Sie die Datei `test.cgi` nicht bearbeitet haben, dürfte sie keine Programmierfehler enthalten. Falls Sie aber eigene Programme verwenden, sollten Sie diese immer auf Programmierfehler untersuchen.

22.6 Einrichten eines sicheren Webservers mit SSL

Vertrauliche Daten wie Kreditkarteninformationen sollten nur über eine sichere, verschlüsselte Verbindung mit Authentifizierung zwischen Webserver und Client übertragen werden. `mod_ssl` bietet mittels der Protokolle Secure Sockets Layer (SSL) und Transport Layer Security (TLS) eine sichere Verschlüsselung für die HTTP-Kommunikation zwischen einem Client und dem Webserver. Wenn Sie SSL/TLS verwenden, wird zwischen dem Webserver und dem Client eine private Verbindung eingerichtet. Die Datenintegrität bleibt dadurch gewährleistet und Client und Server können sich gegenseitig authentifizieren.

Zu diesem Zweck sendet der Server vor der Beantwortung von Anforderungen an eine URL ein SSL-Zertifikat mit Informationen, die die Identität des Servers nachweisen. Dies garantiert, dass der Server eindeutig der richtige Endpunkt der Kommunikation ist. Außerdem wird durch das Zertifikat eine verschlüsselte Verbindung zwischen dem Client und dem Server hergestellt, die sicherstellt, dass Informationen ohne das Risiko der Freigabe sensibler Klartextinhalte übertragen werden.

`mod_ssl` implementiert die SSL/TLS-Protokolle nicht selbst, sondern fungiert als Schnittstelle zwischen Apache und einer SSL-Bibliothek. In openSUSE wird die OpenSSL-Bibliothek verwendet. OpenSSL wird bei der Installation von Apache automatisch installiert.

Die Verwendung von `mod_ssl` in Apache erkennen Sie in URLs am Präfix `https://` (statt `http://`).

22.6.1 Erstellen eines SSL-Zertifikats

Wenn Sie SSL/TSL mit dem Webserver einsetzen möchten, müssen Sie ein SSL-Zertifikat erstellen. Dieses Zertifikat ist für die Autorisierung zwischen Webserver und Client erforderlich, damit beide Endpunkte jeweils die Identität des anderen Endpunkts überprüfen können. Zum Nachweis der Zertifikatintegrität muss das Zertifikat von einer Organisation signiert sein, der jeder der beteiligten Benutzer vertraut.

Sie können drei Zertifikatsarten erstellen: ein „Dummy“-Zertifikat, das nur zu Testzwecken verwendet wird, ein selbst signiertes Zertifikat für einen bestimmten Benutzerkreis, der Ihnen vertraut, und ein Zertifikat, das von einer unabhängigen, öffentlich bekannten Zertifizierungsstelle (CA) signiert wurde.

Die Zertifikaterstellung besteht im Grunde nur aus zwei Schritten: Zunächst wird ein privater Schlüssel für die Zertifizierungsstelle generiert und danach wird das Serverzertifikat mit diesem Schlüssel signiert.

TIPP: Weiterführende Informationen

Weitere Informationen über das Konzept von SSL/TSL und diesbezügliche Festlegungen finden Sie unter http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html.

Erstellen eines „Dummy“-Zertifikats

Die Erstellung eines Dummy-Zertifikats ist einfach. Rufen Sie lediglich das Skript `/usr/bin/gensslcert` auf. Dieses Skript erstellt oder überschreibt die folgenden Dateien:

- `/etc/apache2/ssl.crt/ca.crt`
- `/etc/apache2/ssl.crt/server.crt`
- `/etc/apache2/ssl.key/server.key`
- `/etc/apache2/ssl.csr/server.csr`

Außerdem wird eine Kopie der Datei `ca.crt` im Verzeichnis `/srv/www/htdocs/CA.crt` zum Herunterladen bereitgestellt.

WICHTIG

Verwenden Sie Dummy-Zertifikate niemals in Produktionsumgebungen, sondern nur zum Testen.

Erstellen eines selbst signierten Zertifikats

Wenn Sie einen sicheren Webserver für Ihr Intranet oder einen bestimmten Benutzerkreis einrichten, reicht unter Umständen ein von Ihrer eigenen Zertifizierungsstelle signiertes Zertifikat aus.

Die Erstellung eines selbst signierten Zertifikats ist ein interaktiver Vorgang, der aus neun Schritten besteht. Wechseln Sie dazu zunächst in das Verzeichnis `/usr/share/doc/packages/apache2` und führen Sie den folgenden Befehl aus: `./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/custom`. Diesen Befehl sollten Sie keinesfalls außerhalb dieses Verzeichnisses ausführen. Das Programm gibt eine Reihe von Eingabeaufforderungen aus, von denen einige Benutzereingaben erfordern.

Prozedur 22.1 *Erstellen eines selbst signierten Zertifikats mit `mkcert.sh`*

- 1** Festlegen des für Zertifikate zu verwendenden Signaturalgorithmus

Wählen Sie RSA aus (R, die Standardeinstellung), da einige ältere Browser Probleme mit DSA haben.

- 2** Generating RSA private key for CA (1024 bit) (Privaten RSA-Schlüssel für CA (1024 Bit) erstellen)

Keine Eingabe erforderlich.

- 3** Generating X.509 certificate signing request for CA (X.509-Zertifikatsignierungsanforderung für CA erstellen)

Hier erstellen Sie den DN (Distinguished Name) der Zertifizierungsstelle. Dazu müssen Sie einige Fragen, z. B. nach dem Land oder der Organisation, beantworten. Geben Sie an dieser Stelle nur gültige Daten ein. Schließlich wird alles, was Sie hier eingeben, später im Zertifikat angezeigt. Sie müssen nicht alle Fragen

beantworten. Wenn eine Frage nicht auf Sie zutrifft oder Sie eine Antwort offen lassen möchten, geben Sie „“ ein. Allgemeiner Name ist der Name der CA selbst. Wählen Sie einen aussagekräftigen Namen wie *CA mein Unternehmen*.

- 4 Generating X.509 certificate for CA signed by itself
(Von CA selbst signiertes X.509-Zertifikat für CA erstellen)

Wählen Sie Zertifikatversion 3 aus (die Standardeinstellung).

- 5 Generating RSA private key for SERVER (1024 bit)
(Privaten RSA-Schlüssel für SERVER (1024 Bit) erstellen)

Keine Eingabe erforderlich.

- 6 Generating X.509 certificate signing request for SERVER
(X.509-Zertifikatsignierungsanforderung für SERVER erstellen)

Hier erstellen Sie den DN für den Serverschlüssel. Es werden nahezu die gleichen Fragen gestellt wie für den DN der Zertifizierungsstelle. Ihre Antworten betreffen jedoch den Webserver und müssen nicht unbedingt identisch mit den für die Zertifizierungsstelle eingegebenen Daten sein (der Server kann sich z. B. an einem anderen Standort befinden).

WICHTIG: Auswahl eines Common Name

Als Common Name (allgemeiner Name) müssen Sie hier den vollständig qualifizierten Hostnamen des sicheren Servers eingeben (z. B. www.example.com). Anderenfalls gibt der Browser beim Zugriff auf den Webserver eine Warnung mit dem Hinweis aus, dass das Zertifikat nicht mit dem Server übereinstimmt.

- 7 Generating X.509 certificate signed by own CA (Von eigener CA signiertes X.509-Zertifikat erstellen)

Wählen Sie Zertifikatversion 3 aus (die Standardeinstellung).

- 8 Encrypting RSA private key of CA with a pass phrase for security (Privaten RSA-Schlüssel der CA aus Sicherheitsgründen mit einem Passwort verschlüsseln)

Aus Sicherheitsgründen empfiehlt es sich, den privaten Schlüssel der Zertifizierungsstelle mit einem Passwort zu verschlüsseln. Wählen Sie daher J aus und geben Sie ein Passwort ein.

- 9 Encrypting RSA private key of SERVER with a pass phrase for security (Privaten RSA-Schlüssel des SERVERS aus Sicherheitsgründen mit einem Passwort verschlüsseln)

Wenn Sie den Serverschlüssel mit einem Passwort verschlüsseln, müssen Sie dieses Passwort bei jedem Start des Webservers eingeben. Dies macht den automatischen Start des Webservers beim Hochfahren des Computers oder einen Neustart des Webservers nahezu unmöglich. Aus diesem Grund sollten Sie diese Frage mit N beantworten. Denken Sie aber daran, dass Ihr Schlüssel in diesem Fall ungeschützt ist, und stellen Sie sicher, dass nur autorisierte Personen Zugriff auf den Schlüssel haben.

WICHTIG: Verschlüsseln des Serverschlüssels

Wenn Sie den Serverschlüssel mit einem Passwort verschlüsseln möchten, erhöhen Sie den Wert für `APACHE_TIMEOUT` in `/etc/sysconfig/apache2`. Anderenfalls bleibt Ihnen unter Umständen nicht genügend Zeit für die Eingabe des Passworts, bevor der Startversuch des Servers wegen Zeitüberschreitung abgebrochen wird.

Die Ergebnisseite des Skripts enthält eine Liste der generierten Zertifikate und Schlüssel. Die Dateien wurden allerdings nicht, wie im Skript angegeben, im lokalen Verzeichnis `conf` erstellt, sondern in den passenden Verzeichnissen unter `/etc/apache2/`.

Der letzte Schritt besteht darin, die Zertifikatdatei der Zertifizierungsstelle aus dem Verzeichnis `/etc/apache2/ssl.crt/ca.crt` in ein Verzeichnis zu kopieren, in dem die Benutzer auf die Datei zugreifen können. Aus diesem Verzeichnis können die Benutzer die Zertifizierungsstelle in ihren Webbrowsern der Liste der bekannten und vertrauenswürdigen Zertifizierungsstellen hinzufügen. Wäre die Zertifizierungsstelle nicht in dieser Liste enthalten, würde der Browser melden, dass das Zertifikat von einer unbekanntem Zertifizierungsstelle ausgegeben wurde. Das neu erstellte Zertifikat ist ein Jahr lang gültig.

WICHTIG: Eigensignierte Zertifikate

Verwenden Sie selbst signierte Zertifikate nur auf einem Webserver, auf den Benutzer zugreifen, denen Sie bekannt sind und die Ihnen als Zertifizierungsstelle vertrauen. Für einen öffentlichen Online-Versand wäre ein solches Zertifikat z. B. nicht geeignet.

Anfordern eines offiziell signierten Zertifikats

Es gibt verschiedene offizielle Zertifizierungsstellen, die Ihre Zertifikate signieren. Zertifizierungsstellen sind vertrauenswürdige unabhängige Parteien. Einem Zertifikat, das durch eine solche Zertifizierungsstelle signiert wurde, kann daher voll und ganz vertraut werden. Sichere Webserver, deren Inhalte für die Öffentlichkeit bereitstehen, verfügen in der Regel über ein offiziell signiertes Zertifikat.

Die bekanntesten offiziellen Zertifizierungsstellen sind Thawte (<http://www.thawte.com/>) und Verisign (<http://www.verisign.com>). Diese und andere Zertifizierungsstellen sind bereits in Browsern kompiliert. Zertifikate, die von diesen Zertifizierungsstellen signiert wurden, werden daher von Browsern automatisch akzeptiert.

Wenn Sie ein offiziell signiertes Zertifikat anfordern, senden Sie kein Zertifikat an die Zertifizierungsstelle, sondern eine CSR (Certificate Signing Request, Zertifikatsignierungsanforderung). Zur Erstellung einer CSR rufen Sie das Skript `/usr/share/ssl/misc/CA.sh -newreq` auf.

Das Skript fragt zunächst nach dem Passwort für die Verschlüsselung der CSR. Danach müssen Sie einen Distinguished Name (DN) eingeben. Dazu müssen Sie einige Fragen, z. B. nach dem Land oder der Organisation, beantworten. Geben Sie an dieser Stelle nur gültige Daten ein. Alles, was Sie hier eingeben, wird überprüft und später im Zertifikat angezeigt. Sie müssen nicht alle Fragen beantworten. Wenn eine Frage nicht auf Sie zutrifft oder Sie eine Antwort offen lassen möchten, geben Sie „`„`“ ein. Allgemeiner Name ist der Name der CA selbst. Wählen Sie einen aussagekräftigen Namen wie *CA Mein Unternehmen*. Zum Schluss müssen Sie noch ein Challenge Passwort (zur Vernichtung des Zertifikats, falls der Schlüssel kompromittiert wird) und einen alternativen Unternehmensnamen eingeben.

Die CSR wird in dem Verzeichnis erstellt, aus dem Sie das Skript aufgerufen haben. Der Name der CSR-Datei lautet `newreq.pem`.

22.6.2 Konfigurieren von Apache mit SSL

Port 443 ist auf dem Webserver der Standardport für SSL- und TLS-Anforderungen. Zwischen einem „normalen“ Apache-Webserver, der Port 80 überwacht, und einem SSL/TLS-aktivierten Apache-Server, der Port 443 überwacht, kommt es zu keinen Konflikten. In der Tat kann die gleiche Apache-Instanz sowohl HTTP als auch HTTPS ausführen. In der Regel verteilen separate virtuelle Hosts die Anforderungen für Port 80 und Port 443 an separate virtuelle Server.

WICHTIG: Firewall-Konfiguration

Vergessen Sie nicht, die Firewall für den SSL-aktivierten Apache-Webserver an Port 443 zu öffnen. Sie können dazu YaST verwenden (siehe [Abschnitt 28.4.1](#), „Konfigurieren der Firewall mit YaST“ (S. 510)).

Zur Verwendung von SSL muss SSL in der globalen Serverkonfiguration aktiviert sein. Zur Aktivierung öffnen Sie `/etc/sysconfig/apache2` in einem Editor und suchen Sie nach `APACHE_MODULES`. Fügen Sie der Modulliste „ssl“ hinzu, sofern dieser Eintrag noch nicht vorhanden ist (`mod_ssl` ist standardmäßig aktiviert). Suchen Sie anschließend nach `APACHE_SERVER_FLAGS` und fügen Sie „SSL“ hinzu. Wenn Sie sich zuvor entschieden haben, Ihr Serverzertifikat durch ein Passwort zu verschlüsseln, sollten Sie nun den Wert von `APACHE_TIMEOUT` heraufsetzen, damit Ihnen beim Start von Apache genügend Zeit für die Eingabe des Passworts bleibt. Starten Sie den Server anschließend neu, damit die Änderungen wirksam werden. Ein Neuladen des Servers reicht dazu nicht aus.

Das Verzeichnis der virtuellen Hostkonfiguration enthält die Vorlage `/etc/apache2/vhosts.d/vhost-ssl.template`. Diese enthält SSL-spezifische Direktiven, die bereits an anderer Stelle hinreichend dokumentiert sind. Informationen über die Basiskonfiguration eines virtuellen Hosts finden Sie unter „[Virtuelle Hostkonfiguration](#)“ (S. 409).

Kopieren Sie zum Starten die Vorlage zu `/etc/apache2/vhosts.d/mySSL-host.conf` und bearbeiten Sie diese. Es sollte ausreichen, die Werte für die folgenden Anweisungen anzupassen:

- `DocumentRoot`
- `ServerName`

- ServerAdmin
- ErrorLog
- TransferLog

WICHTIG: Namensbasierte virtuelle Hosts und SSL

Auf einem Server mit nur einer IP-Adresse können nicht mehrere SSL-aktivierte virtuelle Hosts laufen. Benutzer, die versuchen, eine Verbindung mit einer solchen Konfiguration herzustellen, erhalten bei jedem Besuch der URL eine Warnung mit dem Hinweis, dass das Zertifikat nicht mit dem Namen des Servers übereinstimmt. Für die Kommunikation auf Grundlage eines gültigen SSL-Zertifikats ist eine separate IP-Adresse bzw. ein separater Port für jede SSL-aktivierte Domäne erforderlich.

22.7 Vermeiden von Sicherheitsproblemen

Ein dem öffentlichen Internet ausgesetzter Webserver erfordert ständige Wartungs- und Verwaltungsarbeiten. Sicherheitsprobleme, verursacht durch die Software wie auch durch versehentliche Fehlkonfigurationen, sind kaum zu vermeiden. Im Folgenden einige Tipps zur Verbesserung der Sicherheit.

22.7.1 Stets aktuelle Software

Bei Bekanntwerden von Sicherheitsrisiken in der Apache-Software veröffentlicht SUSE sofort einen entsprechenden Sicherheitshinweis. Dieser enthält Anleitungen zur Behebung der Risiken, die möglichst frühzeitig ausgeführt werden sollten. Die Sicherheitsankündigungen von SUSE stehen unter folgenden Adressen zur Verfügung:

- **Webseite** <http://www.novell.com/linux/security/securitysupport.html>
- **Mailingliste** <http://en.opensuse.org/Communicate#Mailinglists>

- **RSS-Newsticker** http://www.novell.com/linux/security/suse_security.xml

22.7.2 DocumentRoot-Berechtigungen

In openSUSE sind das `DocumentRoot`-Verzeichnis `/srv/www/htdocs` und das `CGI`-Verzeichnis `/srv/www/cgi-bin` standardmäßig dem Benutzer bzw. der Gruppe `root` zugeordnet. Diese Berechtigungen sollten nicht geändert werden. Wenn diese Verzeichnisse für alle Benutzer modifizierbar wären, könnte jeder Benutzer Dateien darin ablegen. Diese Dateien würden dann von Apache mit `wwwrun`-Berechtigungen ausgeführt werden, was wiederum dem Benutzer unbeabsichtigt Zugriff auf die Ressourcen des Dateisystems gewähren würde. Das `DocumentRoot`-Verzeichnis und die `CGI`-Verzeichnisse Ihrer virtuellen Hosts sollten Sie als Unterverzeichnisse im Verzeichnis `/srv/www` anlegen. Stellen Sie auch bei diesen Verzeichnissen sicher, dass die Verzeichnisse und die darin enthaltenen Dateien dem Benutzer bzw. der Gruppe `root` zugeordnet sind.

22.7.3 Zugriff auf das Dateisystem

Standardmäßig wird in `/etc/apache2/httpd.conf` der Zugriff auf das gesamte Dateisystem verweigert. Sie sollten diese Anweisungen nicht überschreiben. Stattdessen sollten Sie explizit den Zugriff auf die Verzeichnisse aktivieren, die Apache lesen muss (siehe „**Basiskonfiguration eines virtuellen Hosts**“ (S. 412)). Achten Sie dabei darauf, dass keine unbefugten Personen auf kritische Dateien wie Passwort- oder Systemkonfigurationsdateien zugreifen können.

22.7.4 CGI-Skripten

Interaktive Skripten in Perl, PHP, SSI oder anderen Programmiersprachen können im Prinzip jeden beliebigen Befehl ausführen und stellen damit generell ein Sicherheitsrisiko dar. Skripten, die vom Server ausgeführt werden, sollten nur aus Quellen stammen, denen der Serveradministrator vertraut. Es wird davon abgeraten, den Benutzern die Ausführung eigener Skripten zu erlauben. Zusätzlich empfiehlt es sich, die Sicherheit aller Skripten zu überprüfen.

Es ist durchaus üblich, sich die Skriptverwaltung durch eine Einschränkung der Skriptausführung zu vereinfachen. Dabei wird die Ausführung von CGI-Skripten auf bestimmte Verzeichnisse eingeschränkt, statt sie global zuzulassen. Die Direktiven `ScriptAlias` und `Option ExecCGI` werden zur Konfiguration verwendet. In der Standardkonfiguration von openSUSE ist es generell nicht gestattet, CGI-Skripten von jedem beliebigen Ort aus auszuführen.

Alle CGI-Skripten werden unter dem gleichen Benutzer ausgeführt. Es kann daher zu Konflikten zwischen verschiedenen Skripten kommen. Abhilfe schafft hier das Modul `suEXEC`, das die Ausführung von CGI-Skripten unter einem anderen Benutzer oder einer anderen Gruppe ermöglicht.

22.7.5 Benutzerverzeichnisse

Bei der Aktivierung von Benutzerverzeichnissen (mit `mod_userdir` oder `mod_rewrite`) sollten Sie unbedingt darauf achten, keine `.htaccess`-Dateien zuzulassen. Durch diese Dateien wäre es den Benutzern möglich, die Sicherheitseinstellungen zu überschreiben. Zumindest sollten Sie die Möglichkeiten des Benutzers durch die Direktive `AllowOverride` einschränken. In openSUSE sind `.htaccess`-Dateien standardmäßig aktiviert. Den Benutzern ist es allerdings nicht erlaubt, mit `mod_userdir` `Option`-Anweisungen zu überschreiben (siehe Konfigurationsdatei `/etc/apache2/mod_userdir.conf`).

22.8 Fehlersuche

Wenn sich Apache nicht starten lässt, eine Webseite nicht angezeigt werden kann oder Benutzer keine Verbindung zum Webserver herstellen können, müssen Sie die Ursache des Problems herausfinden. Im Folgenden werden einige nützliche Ressourcen vorgestellt, die Ihnen bei der Fehlersuche behilflich sein können.

An erster Stelle sei hier das Skript `rcapache2` (siehe [Abschnitt 22.3, „Starten und Beenden von Apache“](#) (S. 421)) genannt, das sich sehr ausführlich mit Fehlern und deren Ursachen befasst und bei Problemen mit Apache wirklich hilfreich ist. Manchmal ist es eine Versuchung, die Binärdatei `/usr/sbin/httpd2` zum Starten oder Beenden des Webserver zu verwenden. Vermeiden Sie dies aber und verwenden Sie stattdessen besser das Skript `rcapache2`. `rcapache2` gibt sogar Tipps und Hinweise zur Behebung von Konfigurationsfehlern.

An zweiter Stelle möchten wir auf die Bedeutung von Protokolldateien hinweisen. Sowohl bei geringfügigen als auch bei schwerwiegenden Fehlern sind die Protokolldateien von Apache, in erster Linie das Fehlerprotokoll, der beste Ort, um nach Fehlerursachen zu fahnden. Mit der Direktive `LogLevel` können Sie im Übrigen die Ausführlichkeit der protokollierten Meldungen einstellen. Dies ist z. B. nützlich, wenn Sie mehr Details benötigen. Standardmäßig befindet sich das Fehlerprotokoll in `/var/log/apache2/error_log`.

TIPP: Ein einfacher Test

Sie können die Apache-Protokollmeldungen mit dem Befehl `tail -F /var/log/apache2/my_error_log` überwachen. Führen Sie anschließend den Befehl `rcapache2 restart` aus. Versuchen Sie anschließend eine Verbindung mit einem Browser herzustellen und überprüfen Sie dort die Ausgabe.

Häufig wird vergessen, die Ports für Apache in der Firewall-Konfiguration des Servers zu öffnen. YaST bietet bei der Konfiguration von Apache eine eigene Option, die sich dieses speziellen Themas annimmt (siehe [Abschnitt 22.2.2, „Konfigurieren von Apache mit YaST“](#) (S. 413)). Bei der manuellen Konfiguration von Apache können Sie die Ports für HTTP und HTTPS in der Firewall über das Firewall-Modul von YaST öffnen.

Falls sich Ihr Problem nicht mithilfe der vorgenannten Ressourcen beheben lässt, finden Sie weitere Informationen in der Apache-Fehlerdatenbank, die online unter http://httpd.apache.org/bug_report.html zur Verfügung steht. Sie können sich auch an die Apache-Benutzer-Community wenden, die Sie über eine Mailingliste unter <http://httpd.apache.org/userslist.html> erreichen. Des Weiteren empfehlen wir die Newsgroup comp.infosystems.www.servers.unix.

22.9 Weiterführende Informationen

Das Paket `apache2-doc`, das an verschiedenen Orten bereitgestellt wird, enthält das vollständige Apache-Handbuch für die lokale Installation und Referenz. Das Handbuch ist nicht in der Standardinstallation enthalten. Am schnellsten installieren Sie es mit dem Kommando `zypper in apache2-doc`. Nach der Installation steht das Apache-Handbuch unter <http://localhost/manual/> zur Verfügung. Unter <http://httpd.apache.org/docs-2.2/> können Sie auch im Web darauf zugreifen. SUSE-spezifische Konfigurationstipps finden Sie im Verzeichnis `/usr/share/doc/packages/apache2/README.*`.

22.9.1 Apache 2.2

Eine Liste der neuen Funktionen in Apache 2.2 finden Sie unter http://httpd.apache.org/docs/2.2/new_features_2_2.html. Upgrade-Informationen von Version 2.0 auf Version 2.2 erhalten Sie unter <http://httpd.apache.org/docs-2.2/upgrading.html>.

22.9.2 Apache Module

Weitere Informationen zu der in **Abschnitt 22.4.5, „Externe Module“** (S. 430) beschriebenen, externen Apache-Module finden Sie unter folgenden Adressen:

mod_apparmor

<http://en.opensuse.org/AppArmor>

mod_mono

http://www.mono-project.com/Mod_mono

mod_perl

<http://perl.apache.org/>

mod_php5

<http://www.php.net/manual/en/install.unix.apache2.php>

mod_python

<http://www.modpython.org/>

mod_tidy

<http://mod-tidy.sourceforge.net/>

22.9.3 Entwicklung

Weitere Informationen zur Entwicklung von Apache-Modulen sowie zur Teilnahme am Apache-Webserver-Projekt finden Sie unter folgenden Adressen:

Informationen für Apache-Entwickler

<http://httpd.apache.org/dev/>

Dokumentation für Apache-Entwickler

<http://httpd.apache.org/docs/2.2/developer/>

Entwickeln von Apache-Modulen mit Perl und C

<http://www.modperl.com/>

22.9.4 Verschiedene Informationsquellen

Wenn Sie in openSUSE Probleme mit Apache haben, werfen Sie einen Blick auf die openSUSE-Wiki unter <http://en.opensuse.org/Apache>. Die Entstehungsgeschichte von Apache finden Sie unter http://httpd.apache.org/ABOUT_APACHE.html. Auf dieser Seite erfahren Sie auch, weshalb dieser Server Apache genannt wird.

Einrichten eines FTP-Servers mit YaST

23

Mithilfe des YaST-*FTP-Server*-Moduls können Sie Ihren Computer für die Funktion als FTP-Server konfigurieren. Anonyme und/oder authentifizierte Benutzer können eine Verbindung zu Ihrem Computer herstellen und, je nach Konfiguration, Dateien mit dem FTP-Protokoll hoch- und herunterladen. YaST stellt eine einheitliche Konfigurationsschnittstelle für verschiedene auf dem System installierte FTP-Server-Daemons bereit.

Das YaST-*FTP-Server*-Konfigurationsmodul kann zum Konfigurieren zweier verschiedener FTP-Server-Daemons verwendet werden: vsftpd (Very Secure FTP Daemon) und pure-ftpd. Nur installierte Server können konfiguriert werden. Standardmäßige openSUSE -Medien enthalten das pure-ftpd-Paket nicht. Wenn das pure-ftpd-Paket allerdings von einer anderen Repository installiert wird, kann es mithilfe des YaST-Moduls konfiguriert werden.

Die vsftpd- und pure-ftpd-Server verfügen über leicht unterschiedliche Konfigurationsoptionen, besonders im Dialogfeld *Experteneinstellungen*. In diesem Kapitel werden die Einstellungen von vsftpd als Standardserver für openSUSE beschrieben.

Wenn das YaST FTP Server-Modul in Ihrem System nicht verfügbar ist, installieren Sie das Paket `yast2-ftp-server`.

Führen Sie zum Konfigurieren des FTP-Servers mit YaST die folgenden Schritte aus:

- 1 Öffnen Sie das YaST-Kontrollzentrum und wählen Sie *Netzwerkdienste* > *FTP-Server* oder führen Sie das Kommando `yast2 ftp-server` als root aus.

- 2 Wenn auf Ihrem System kein FTP-Server installiert ist, werden Sie gefragt, welcher Server installiert werden soll, wenn das YaST FTP Server-Modul gestartet wird. Wählen Sie einen Server (vsftpd ist der Standard-Server für openSUSE) und bestätigen Sie das Dialogfeld.
- 3 Konfigurieren Sie im Dialogfeld *Start* den Startvorgang des FTP-Servers. Weitere Informationen finden Sie unter [Abschnitt 23.1, „Starten des FTP-Servers“](#) (S. 450).

Konfigurieren Sie im Dialogfeld *Allgemein* die FTP-Verzeichnisse, eine Begrüßung, die Masken zum Erstellen von Dateien sowie verschiedene andere Parameter. Weitere Informationen finden Sie unter [Abschnitt 23.2, „Allgemeine FTP-Einstellungen“](#) (S. 451).

Legen Sie im Dialogfeld *Leistung* die Parameter fest, die sich auf das Laden des FTP-Servers auswirken. Weitere Informationen finden Sie unter [Abschnitt 23.3, „FTP-Leistungseinstellungen“](#) (S. 452).

Legen Sie im Dialogfeld *Authentifizierung* fest, ob der FTP-Server für anonyme und/oder authentifizierte Benutzer verfügbar sein soll. Weitere Informationen finden Sie unter [Abschnitt 23.4, „Authentifizierung“](#) (S. 453).

Konfigurieren Sie im Dialogfeld *Einstellungen für Expertenden* Betriebsmodus des FTP-Servers, der SSL-Verbindungen sowie die Firewall-Einstellungen. Weitere Informationen finden Sie unter [Abschnitt 23.5, „Einstellungen für Experten“](#) (S. 453).

- 4 Drücken Sie *Übernehmen*, um die Konfigurationen zu speichern.

23.1 Starten des FTP-Servers

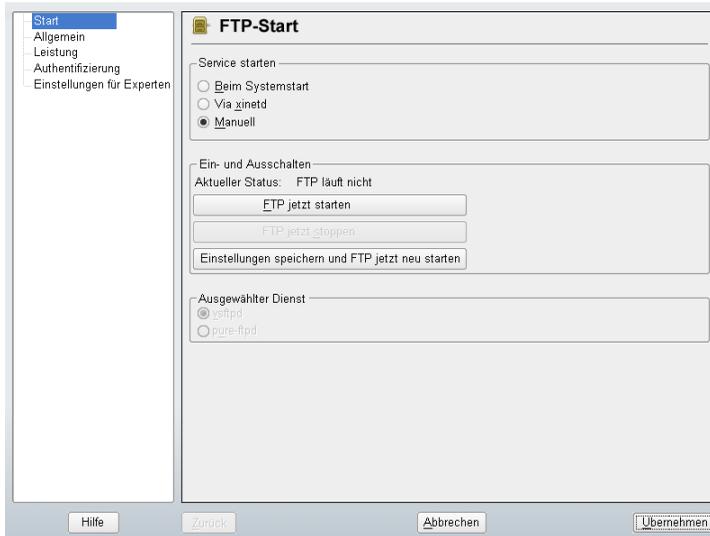
Legen Sie im Bereich *Dienststart* des Dialogfelds *FTP-Start* die Art und Weise fest, in der der FTP-Server gestartet wird. Sie können den Server entweder automatisch während des Systemstarts oder manuell starten. Wenn der FTP-Server erst bei einer FTP-Verbindungsanfrage gestartet werden soll, wählen Sie *Via xinetd* aus.

Der aktuelle Status des FTP-Servers wird im Bereich *An- und ausschalten* im Dialogfeld *FTP-Start* angezeigt. Starten Sie den FTP-Server, indem Sie auf *FTP-Server jetzt starten* klicken. Um den Server zu stoppen, klicken Sie auf *Stoppen FTP*. Nachdem Sie

die Servereinstellungen geändert haben, klicken Sie auf *Einstellungen speichern und FTP jetzt neu starten*. Ihre Konfigurationen werden gespeichert, indem für das Konfigurationsmodul *Akzeptieren* beibehalten wird.

Im Bereich *Dienst auswählen* des Dialogfelds *FTP-Start* wird der verwendete FTP-Server angezeigt. Entweder vsftpd (Very Secure FTP Daemon) oder pure-ftpd können verwendet werden. Wenn beide Server installiert sind, können Sie zwischen ihnen umschalten. Das pure-ftpd-Paket ist in den standardmäßigen openSUSE-Medien nicht enthalten, daher müssen Sie es aus einer anderen Installationsquelle installieren, wenn Sie es verwenden möchten.

Abbildung 23.1 *FTP-Serverkonfiguration - Start*



23.2 Allgemeine FTP-Einstellungen

Im Bereich *Allgemeine Einstellungen* des Dialogfelds *Allgemeine FTP-Einstellungen* können Sie die *Willkommensnachricht* festlegen, die nach der Verbindungsherstellung zum FTP-Server angezeigt wird.

Wenn Sie die Option *Chroot Everyone* (Alle platzieren) aktivieren, werden alle lokalen Benutzer nach der Anmeldung in einem Chroot Jail in ihrem Home-Verzeichnis platziert

Diese Option hat Auswirkungen auf die Sicherheit, besonders wenn die Benutzer über Uploadberechtigungen oder Shellzugriff verfügen, daher sollten Sie beim Aktivieren dieser Option mit Bedacht vorgehen.

Wenn Sie die Option *Ausführliche Protokollierung* aktivieren, werden alle FTP-Anfragen und -Antworten protokolliert.

Sie können die Berechtigungen für Dateien, die von anonymen und/oder authentifizierten Benutzern erstellt wurden, mit `umask` einschränken. Die in `umask` festgelegten Bits stellen die Berechtigungen dar, die immer für neu erstellte Dateien deaktiviert werden müssen. Legen Sie die Dateierstellungsmaske für anonyme Benutzer in *Umask für anonyme Benutzer* fest und die Dateierstellungsmaske für authentifizierte Benutzer in *Umask für authentifizierte Benutzer*. Die Masken sollten als Oktalzahlen mit führender Null eingegeben werden.

Legen Sie im Bereich *FTP-Verzeichnisse* die für anonyme und autorisierte Benutzer verwendeten Verzeichnisse fest. Das standardmäßige FTP-Verzeichnis für anonyme Benutzer ist `/srv/ftp`. Beachten Sie, dass `vsftpd` keine Verzeichnisschreibrechte für alle Benutzer erteilt. Stattdessen wird das Unterverzeichnis `upload` mit Schreibberechtigungen für anonyme Benutzer erstellt.

ANMERKUNG

Der `pure-ftpd`-Server ermöglicht es, dass anonyme Benutzer über Schreibberechtigungen für dieses FTP-Verzeichnis verfügen. Stellen Sie sicher, dass Sie die Schreibberechtigungen im Verzeichnis, das mit `pure-ftpd` verwendet wurde, entfernen, bevor Sie zum `vsftpd`-Server zurückschalten.

23.3 FTP-Leistungseinstellungen

Unter *FTP-Leistungseinstellungen* legen Sie die Parameter fest, die sich auf das Laden des FTP-Servers auswirken. *Max. Lerrlaufzeit* entspricht der Maximalzeit (in Minuten), die der Remote-Client zwischen FTP-Kommandos pausieren darf. Bei einer längeren Inaktivität wird die Verbindung zum Remote-Client getrennt. *Max. Clients für eine IP* bestimmt die maximale Clientanzahl, die von einer einzelnen IP-Adresse aus verbunden sein können. *Max. Clients* bestimmt die maximale Clientanzahl, die verbunden sein können. Alle zusätzlichen Clients erhalten eine Fehlermeldung.

Die maximale Datenübertragungsrate (in KB/s) wird in *Lovale Max Rate* (Lokale max. Rate) für lokale authentifizierte Benutzer und in *Anonymous Max Rate* (Anonyme max. Rate) für anonyme Benutzer festgelegt. Der Standardwert für diese Einstellung ist 0, was für eine unbegrenzte Datenübertragungsrate steht.

23.4 Authentifizierung

Im Bereich *Enable/Disable Anonymous and Local Users* (Anonyme und lokale Benutzer aktivieren/deaktivieren) des Dialogfelds *Authentifizierung* können Sie festlegen, welche Benutzer auf Ihren FTP-Server zugreifen dürfen. Sie können nur anonymen Benutzern, nur authentifizierte Benutzern mit Konten im System oder beiden Benutzertypen den Zugriff gewähren.

Wenn Sie es Benutzern ermöglichen möchten, Dateien auf den FTP-Server hochzuladen, aktivieren Sie die Option *Hochladen aktivieren* im Bereich *Hochladen* des Dialogfelds *Authentifizierung*. Hier können Sie das Hochladen und das Erstellen von Verzeichnissen sogar für anonyme Benutzer zulassen, indem Sie das entsprechende Kontrollkästchen aktivieren.

ANMERKUNG

Wenn ein vsftpd-Server verwendet wird und anonyme Benutzer Dateien hochladen oder Verzeichnisse erstellen dürfen, muss ein Unterverzeichnis mit Schreibberechtigung für alle Benutzer im anonymen FTP-Verzeichnis erstellt werden.

23.5 Einstellungen für Experten

Ein FTP-Server kann im aktiven oder passiven Modus ausgeführt werden. Standardmäßig wird der Server im passiven Modus ausgeführt. Um in den aktiven Modus zu wechseln, deaktivieren Sie einfach die Option *Passiven Modus aktivieren* im Dialogfeld *Einstellungen für Experten*. Sie können außerdem den Portbereich ändern, der auf dem Server für den Datenstrom verwendet wird, indem Sie die Optionen *Min Port für Pas.-Modus* und *Max Port für Pas.-Modus* bearbeiten.

Wenn Sie eine verschlüsselte Kommunikation zwischen den Clients und dem Server wünschen, können Sie das FTPS-Protokoll (FTP/SSH) verwenden. Beachten Sie aber,

dass sich FTPS von dem häufiger verwendeten SFTP (SSH File Transport Protocol) unterscheidet. Wenn Sie das FTPS-Protokoll verwenden möchten, können Sie die SSL-Optionen im Dialogfeld *Einstellungen für Experten* festlegen.

Wenn Ihr System von einer Firewall geschützt wird, aktivieren Sie *Port in Firewall öffnen*, um eine Verbindung zum FTP-Server zu ermöglichen.

23.6 Weitere Informationen

Weitere Informationen zum vsftpd-Server finden Sie in den Handbuchseiten zu `vsftpd` und `vsftpd.conf`.

Teil V. Mobilität

Energieverwaltung

Die Energieverwaltung ist insbesondere bei Notebook-Computern von großer Wichtigkeit, sie ist jedoch auch für andere Systeme sinnvoll. ACPI (Advanced Configuration and Power Interface) steht auf allen modernen Computern (Laptops, Desktops und Servern) zur Verfügung. Für Energieverwaltungstechnologien sind geeignete Hardware- und BIOS-Routinen erforderlich. Die meisten Notebooks und modernen Desktops und Server erfüllen diese Anforderungen. Es ist außerdem möglich, die CPU-Frequenzskalierung zu steuern, um Energie zu sparen oder den Geräuschpegel zu senken.

24.1 Energiesparfunktionen

Energiesparfunktionen sind nicht nur für die mobile Verwendung von Notebooks von Bedeutung, sondern auch für Desktop-Systeme. Die Hauptfunktionen und ihre Verwendung im ACPI sind:

Standby

Bei diesem Betriebsmodus wird der Bildschirm ausgeschaltet. Bei einigen Computern wird die Prozessorleistung gedrosselt. Diese Funktion entspricht ACPI-Zustand S1 bzw. S2.

Stromsparmmodus (in Speicher)

In diesem Modus wird der gesamte Systemstatus in den RAM geschrieben. Anschließend wird das gesamte System mit Ausnahme des RAM in den Ruhezustand versetzt. In diesem Zustand verbraucht der Computer sehr wenig Energie. Der Vorteil dieses Zustands besteht darin, dass innerhalb weniger Sekunden die Arbeit nahtlos wieder aufgenommen werden kann, ohne dass ein Booten des Systems

oder ein Neustart der Anwendungen erforderlich ist. Diese Funktion entspricht ACPI-Zustand S3. Die Unterstützung für diesen Zustand befindet sich noch in der Entwicklungsphase und hängt daher weitgehend von der Hardware ab.

Tiefschlaf (Suspend to Disk)

In diesem Betriebsmodus wird der gesamte Systemstatus auf die Festplatte geschrieben und das System wird von der Energieversorgung getrennt. Es muss eine Swap-Partition vorhanden sein, die mindestens die Größe des RAM hat, damit alle aktiven Daten geschrieben werden können. Die Reaktivierung von diesem Zustand dauert ungefähr 30 bis 90 Sekunden. Der Zustand vor dem Suspend-Vorgang wird wiederhergestellt. Einige Hersteller bieten Hybridvarianten dieses Modus an, beispielsweise RediSafe bei IBM Thinkpads. Der entsprechende ACPI-Zustand ist S4. In Linux wird "suspend to disk" über Kernel-Routinen durchgeführt, die von ACPI unabhängig sind.

Akku-Überwachung

ACPI überprüft den Akkuladestatus und stellt entsprechende Informationen bereit. Außerdem koordiniert es die Aktionen, die beim Erreichen eines kritischen Ladezustand durchzuführen sind.

Automatisches Ausschalten

Nach dem Herunterfahren wird der Computer ausgeschaltet. Dies ist besonders wichtig, wenn der Computer automatisch heruntergefahren wird, kurz bevor der Akku leer ist.

Herunterfahren von Systemkomponenten

Das Ausschalten der Festplatte ist der wichtigste Einzelaspekt des Energiesparpotentials des gesamten Systems. Je nach der Zuverlässigkeit des Gesamtsystems, kann die Festplatte für einige Zeit in den Ruhezustand versetzt werden. Das Risiko eines Datenverlusts steigt jedoch mit der Dauer der Ruhephase. Andere Komponenten, wie PCI-Geräte, die in einen bestimmten Energiesparmodus versetzt werden können, können (zumindest theoretisch) mithilfe von ACPI deaktiviert oder dauerhaft in der BIOS-Einrichtung deaktiviert werden.

Steuerung der Prozessorgeschwindigkeit

In Verbindung mit der CPU gibt es drei Möglichkeiten, Energie zu sparen: Frequenz- und Spannungsskalierung (auch PowerNow! oder Speedstep), Drosselung und Versetzen des Prozessors in den Ruhezustand (C-Status). Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden.

24.2 ACPI

ACPI (Advanced Configuration and Power Interface, erweiterte Konfigurations- und Energieschnittstelle) wurde entwickelt, um dem Betriebssystem die Einrichtung und Steuerung der einzelnen Hardware-Komponenten zu ermöglichen. ACPI ersetzt PnP und APM. Diese Schnittstelle bietet Informationen zu Akku, Netzteil, Temperatur, Ventilator und Systemereignissen wie dem Schließen des Deckels oder einem niedrigen Akkuladestand.,“,“

Das BIOS bietet Tabellen mit Informationen zu den einzelnen Komponenten und Hardware-Zugriffsmethoden. Das Betriebssystem verwendet diese Informationen für Aufgaben wie das Zuweisen von Interrupts oder das Aktivieren bzw. Deaktivieren von Komponenten. Da das Betriebssystem die in BIOS gespeicherten Befehle ausführt, hängt die Funktionalität von der BIOS-Implementierung ab. Die Tabellen, die ACPI erkennen und laden kann, werden in `/var/log/boot.msg` gemeldet. Weitere Informationen zur Fehlersuche bei ACPI-Problemen finden Sie in [Abschnitt 24.2.4](#), „Fehlersuche“ (S. 465).

24.2.1 ACPI in Aktion

Wenn der Kernel beim Booten des Systems ein ACPI BIOS entdeckt, wird ACPI automatisch aktiviert. Bei einigen älteren Computern kann der Bootparameter `acpi=force` erforderlich sein. Der Computer muss ACPI 2.0 oder höher unterstützen. Überprüfen Sie anhand der Bootmeldungen unter `/var/log/boot.msg`, ob ACPI aktiviert wurde.

Anschließend muss eine Reihe von Modulen geladen werden. Dies erfolgt über das Startskript des `acpid`-Skripts. Wenn eines dieser Module Probleme verursacht, kann das betreffende Modul unter `/etc/sysconfig/powersave/common` aus dem Lade- bzw. Entladevorgang ausgeschlossen werden. Das Systemprotokoll (`/var/log/messages`) enthält die Meldungen der Module, denen Sie entnehmen können, welche Komponenten erkannt wurden.

`/proc/acpi` enthält nun eine Nummer der Dateien, die Informationen zum Systemzustand bieten oder zum Ändern einiger Zustände verwendet werden können. Einige Funktionen funktionieren noch nicht, da sie sich noch in der Entwicklungsphase befinden, und die Unterstützung einiger Funktionen hängt weitgehend von der Implementierung durch den Hersteller ab.

Alle Dateien (mit Ausnahme von `dsdt` und `fadt`) können mit `cat` gelesen werden. In einigen Dateien können die Einstellungen mit `echo` geändert werden, beispielsweise `echo X > file` zur Angabe geeigneter Werte für `X`. Eine Möglichkeit für den einfachen Zugriff auf diese Werte ist der `Powersave`-Befehl, der als Frontend für den `Powersave`-Daemon dient. Im Folgenden werden die wichtigsten Dateien beschrieben:

```
/proc/acpi/info
```

Allgemeine Informationen zu ACPI.

```
/proc/acpi/alarm
```

Hier können Sie angeben, wann das System aus einem Ruhezustand wieder aktiviert werden soll. Zurzeit wird diese Funktion nicht vollständig unterstützt.

```
/proc/acpi/sleep
```

Bietet Informationen zu möglichen Ruhezuständen.

```
/proc/acpi/event
```

Hier werden alle Ereignisse gemeldet und vom `Powersave`-Daemon (`Powersaved`) verarbeitet. Wenn kein Daemon auf diese Datei zugreift, können Ereignisse, wie ein kurzes Antippen des Netzschalters oder das Schließen des Deckels mit `cat /proc/acpi/event` gelesen werden (Beenden mit `Strg + C`).

```
/proc/acpi/dsdt und /proc/acpi/fadt
```

Diese Dateien enthalten die ACPI-Tabellen `DSDT` (Differentiated System Description Table) und `FADT` (Fixed ACPI Description Table). Sie können mit `acpidump`, `iasl` und `dmidecode` gelesen werden. Diese Programme und ihre Dokumentation befinden sich im Paket `pmttools`. Um zum Beispiel ein nicht verbundenes `DSDT` in der Datei `dsdt.dsl` abzurufen, verwenden Sie Folgendes:

```
acpidump > acpidump.out
acpixtract acpidump.out
iasl -d DSDT.dat
```

```
/proc/acpi/ac_adapter/AC/state
```

Zeigt an, ob das Netzteil angeschlossen ist.

```
/proc/acpi/battery/BAT*/\{alarm,info,state}
```

Detaillierte Informationen zum Ladezustand des Akkus. Der Ladezustand wird ermittelt, indem der mit `info` angegebene letzte Zustand der vollständigen Ladung mit der mit `state` angegebenen verbleibenden Ladung verglichen wird. Einfacher lässt sich der Ladezustand mit einem speziellen

Programm ermitteln, das in [Abschnitt 24.2.3](#), „ACPI-Werkzeuge“ (S. 465) beschrieben wurde. Der Ladezustand, bei dem ein Akku-Ereignis (z. B. Warnung, niedrige oder kritische Kapazität) ausgelöst wird, kann unter `alarm` (Alarm) angegeben werden.

```
/proc/acpi/button
```

Dieses Verzeichnis enthält Informationen zu verschiedenen Schaltern.

```
/proc/acpi/fan/FAN/state
```

Zeigt, ob der Ventilator zurzeit aktiv ist. Sie können den Ventilator manuell aktivieren bzw. deaktivieren, indem Sie 0 (ein) bzw. 3 (aus) in diese Datei schreiben. Diese Einstellung wird jedoch sowohl vom ACPI-Code im Kernel als auch von der Hardware (bzw. BIOS) überschrieben, wenn die Temperatur des Systems zu hoch wird.

```
/proc/acpi/processor/*
```

Für jede CPU im System wird ein gesondertes Unterverzeichnis geführt.

```
/proc/acpi/processor/*/info
```

Informationen zu den Energiesparoptionen des Prozessors.

```
/proc/acpi/processor/*/power
```

Informationen zum aktuellen Prozessorzustand. Ein Sternchen neben `C2` zeigt an, dass der Prozessor zurzeit nicht genutzt wird. Dies ist der häufigste Zustand, wie aus dem Wert `usage` (Nutzung) ersichtlich ist.

```
/proc/acpi/processor/*/throttling
```

Hiermit kann die Drosselung der Prozessoruhr festgelegt werden. Normalerweise ist eine Drosselung in acht Stufen möglich. Dies hängt von der Frequenzsteuerung der CPU ab.

```
/proc/acpi/processor/*/limit
```

Wenn Leistung (obsolet) und Drosselung automatisch von einem Daemon gesteuert werden, können hier die Obergrenzen angegeben werden. Einige der Grenzwerte werden durch das System bestimmt. Andere können vom Benutzer angepasst werden.

```
/proc/acpi/thermal_zone/
```

Für jede Thermalzone ist ein eigenes Unterverzeichnis vorhanden. Eine Thermalzone ist ein Bereich mit ähnlichen thermischen Eigenschaften. Ihre Anzahl und Bezeichnungen werden vom Hardware-Hersteller festgelegt. Viele der von ACPI

gebotenen Möglichkeiten werden jedoch kaum implementiert. Stattdessen wird die Temperatursteuerung üblicherweise dem BIOS überlassen. Das Betriebssystem hat kaum Gelegenheit, einzugreifen, da die Lebensdauer der Hardware in Gefahr ist. Daher weisen einige der Dateien nur einen theoretischen Wert auf.

```
/proc/acpi/thermal_zone/*/temperature
```

Aktuelle Temperatur der thermalen Zone.

```
/proc/acpi/thermal_zone/*/state
```

Dieser Status zeigt an, ob alles ok (OK) ist bzw. ob ACPI *active* (aktive) oder *passive* (passive) Kühlung durchführt. Bei ACPI-unabhängiger Ventilatorsteuerung ist dieser Zustand immer ok (OK)

```
/proc/acpi/thermal_zone/*/cooling_mode
```

Wählen Sie die von ACPI gesteuerte Kühlmethode aus. Wählen Sie einen passiven (weniger Leistung, sparsamer) oder aktiven (volle Leistung, Ventilatorgeräusche) Kühlmodus aus.

```
/proc/acpi/thermal_zone/*/trip_points
```

Aktiviert die Ermittlung von Temperaturgrenzen zur Auslösung spezieller Vorgänge, wie passive oder aktive Kühlung, Suspend-Modus (beim Zustand *hot* (heiß)) oder Herunterfahren (beim Zustand *critical* kritisch)). Die möglichen Aktionen sind in der DSDT definiert (geräteabhängig). In der ACPI-Spezifikation werden die folgenden Schwellenwerte festgelegt: *critical* (kritisch), *hot* (heiß), *passive* (passiv), *active1* (aktiv1) und *active2* (aktiv2). Auch wenn sie nicht alle implementiert sind, müssen sie stets in dieser Reihenfolge in die Datei eingegeben werden. Der Eintrag `echo 90:0:70:0:0 > trip_points` setzt die Temperatur für *critical* (kritisch) auf 90 und die Temperatur für *passive* (passiv) auf 70 Grad Celsius.

```
/proc/acpi/thermal_zone/*/polling_frequency
```

Wenn der Wert in *temperature* bei Temperaturänderungen nicht automatisch aktualisiert wird, können Sie hier auf einen anderen Erhebungsmodus umschalten. Der Befehl `echo X >`

`/proc/acpi/thermal_zone/*/polling_frequency` führt zu einer Abfrage der Temperatur alle X Sekunden. Um die Erhebung zu deaktivieren, setzen Sie `X=0`.

Keine dieser Einstellungen, Informationen und Ereignisse muss manuell bearbeitet werden. Dies ist über den Powersave-Daemon (Powersaved) und verschiedene Frontends,

wie Powersave, kpowersave und wmpowersave, möglich. Weitere Informationen hierzu finden Sie unter [Abschnitt 24.2.3, „ACPI-Werkzeuge“](#) (S. 465).

24.2.2 Steuern der CPU-Leistung

Mit der CPU sind Energieeinsparungen auf drei verschiedene Weisen möglich. Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden. Energiesparen bedeutet auch, dass sich das System weniger erhitzt und die Ventilatoren seltener in Betrieb sind.

Frequenz- und Spannungsskalierung

ADM und Intel bezeichnen diese Technologie als PowerNow! und Speedstep. Doch auch in die Prozessoren anderer Hersteller ist diese Technologie integriert. Taktfrequenz und Kernspannung der CPU werden gleichzeitig verringert, was zu mehr als linearen Energieeinsparungen führt. Eine Halbierung der Frequenz (halbe Leistung) führt also dazu, dass wesentlich weniger als die Hälfte der Energie verbraucht wird. Diese Technologie ist unabhängig von ACPI. Es gibt zwei Möglichkeiten, die CPU-Frequenz zu skalieren: über den Kernel selbst oder über eine Userspace-Anwendung. Aus diesem Grund gibt es verschiedene Kernel-Governors, die in `/sys/devices/system/cpu/cpu*/cpufreq/` festgelegt werden können.

userspace governor

Wenn der Userspace Governor eingerichtet wird, steuert der Kernel die CPU-Frequenz durch die Skalierung auf eine Userspace-Anwendung (normalerweise ein Daemon). In openSUSE-Distributionen besteht dieser Daemon im `Powersaved`-Paket. Wenn diese Implementierung verwendet wird, wird die CPU-Frequenz gemäß der aktuellen Systemlast angepasst. Standardmäßig wird eine der Kernel-Implementierungen verwendet. Bei mancher Hardware oder in Bezug auf bestimmte Prozessoren oder Treiber ist die userspace-Implementierung jedoch nach wie vor die einzige funktionierende Lösung.

ondemand governor

Es handelt sich hierbei um die Kernel-Implementierung einer dynamischen CPU-Frequenz-Richtlinie und sollte auf den meisten Systemen funktionieren. Sobald eine hohe Systemlast vorliegt, wird die CPU-Frequenz sofort erhöht. Sie wird bei einer niedrigeren Systemlast herabgesetzt.

conservative governor

Dieser Regler ähnelt der On Demand-Implementierung, außer dass eine konservativere Richtlinie verwendet wird. Die Auslastung des Systems muss über einen bestimmten Zeitraum hoch sein, damit die CPU-Frequenz erhöht wird.

powersave governor

Die CPU-Frequenz wird statisch auf den niedrigsten möglichen Wert gesetzt.

performance governor

Die CPU-Frequenz wird statisch auf den höchstmöglichen Wert gesetzt.

Drosseln der Taktfrequenz

Bei dieser Technologie wird ein bestimmter Prozentsatz der Taktsignalimpulse für die CPU ausgelassen. Bei einer Drosselung von 25 % wird jeder vierte Impuls ausgelassen. Bei 87.5 % erreicht nur jeder achte Impuls den Prozessor. Die Energieeinsparungen sind allerdings ein wenig geringer als linear. Normalerweise wird die Drosselung nur verwendet, wenn keine Frequenzskalierung verfügbar ist oder wenn maximale Energieeinsparungen erzielt werden sollen. Auch diese Technologie muss von einem speziellen Prozess gesteuert werden. Die Systemschnittstelle lautet `/proc/acpi/processor/*/throttling`.

Versetzen des Prozessors in den Ruhezustand

Das Betriebssystem versetzt den Prozessor immer dann in den Ruhezustand, wenn keine Arbeiten anstehen. In diesem Fall sendet das Betriebssystem den Befehl `halt` an die CPU. Es gibt drei Statusmöglichkeiten: C1, C2 und C3. Im Zustand mit der höchsten Energieeinsparung, C3, wird sogar die Synchronisierung des Prozessor-Cache mit dem Hauptspeicher angehalten. Daher ist dieser Zustand nur möglich, wenn der Inhalt des Hauptspeichers von keinem anderen Gerät über Busmaster-Aktivitäten bearbeitet wird. Einige Treiber verhindern die Verwendung von C3. Der aktuelle Zustand wird unter `/proc/acpi/processor/*/throttling` angezeigt.

Frequenzskalierung und Drosselung sind nur relevant, wenn der Prozessor belegt ist, da der sparsamste C-Zustand ohnehin gilt, wenn sich der Prozessor im Wartezustand befindet. Wenn die CPU belegt ist, ist die Frequenzskalierung die empfohlene Energiesparmethode. Häufig arbeitet der Prozessor nur im Teillast-Betrieb. In diesem Fall kann er mit einer niedrigeren Frequenz betrieben werden. Normalerweise ist eine dynamische Frequenzskalierung, die von dem On Demand-Governor des Kernels oder einem Daemon (z. B. `powersaved`) gesteuert wird, der beste Ansatz. Eine statische Einstellung auf eine

niedrige Frequenz ist sinnvoll bei Akkubetrieb oder wenn der Computer kühl oder geräuscharm arbeiten soll.

Drosselung sollte nur als letzter Ausweg verwendet werden, um die Betriebsdauer des Akkus trotz hoher Systemlast zu verlängern. Einige Systeme arbeiten bei zu hoher Drosselung jedoch nicht reibungslos. Außerdem hat die CPU-Drosselung keinen Sinn, wenn die CPU kaum ausgelastet ist.

Unter openSUSE werden diese Technologien vom Powersave-Daemon gesteuert. Die Konfiguration wird in [Abschnitt 24.4](#), „Das Powersave-Paket“ (S. 469) erläutert.

24.2.3 ACPI-Werkzeuge

Zu der Palette der mehr oder weniger umfassenden ACPI-Dienstprogramme gehören Werkzeuge, die lediglich Informationen anzeigen, wie beispielsweise Akku-Ladezustand und Temperatur (`acpi`, `klaptopdaemon`, usw.), Werkzeuge, die den Zugriff auf die Strukturen unter `/proc/acpi` ermöglichen oder Überwachungsänderungen erleichtern (`akpi`, `acpiw`, `gtkacpiw`), sowie Werkzeuge zum Bearbeiten der ACPI-Tabellen im BIOS (Paket `pmttools`).

24.2.4 Fehlersuche

Es gibt zwei verschiedene Arten von Problemen. Einerseits kann der ACPI-Code des Kernel Fehler enthalten, die nicht rechtzeitig erkannt wurden. In diesem Fall wird eine Lösung zum Herunterladen bereitgestellt. Häufiger jedoch werden die Probleme vom BIOS verursacht. Manchmal werden Abweichungen von der ACPI-Spezifikation absichtlich in das BIOS integriert, um Fehler in der ACPI-Implementierung in anderen weit verbreiteten Betriebssystemen zu umgehen. Hardware-Komponenten, die ernsthafte Fehler in der ACPI-Implementierung aufweisen, sind in einer Blacklist festgehalten, die verhindert, dass der Linux-Kernel ACPI für die betreffenden Komponenten verwendet.

Der erste Schritt, der bei Problemen unternommen werden sollte, ist die Aktualisierung des BIOS. Wenn der Computer sich überhaupt nicht booten lässt, kann eventuell einer der folgenden Bootparameter Abhilfe schaffen:

`pci=noacpi`

ACPI nicht zum Konfigurieren der PCI-Geräte verwenden.

acpi=ht

Nur eine einfache Ressourcenkonfiguration durchführen. ACPI nicht für andere Zwecke verwenden.

acpi=off

ACPI deaktivieren.

WARNUNG: Probleme beim Booten ohne ACPI

Einige neuere Computer (insbesondere SMP- und AMD64-Systeme) benötigen ACPI zur korrekten Konfiguration der Hardware. Bei diesen Computern kann die Deaktivierung von ACPI zu Problemen führen.

Manchmal ist der Computer durch Hardware gestört, die über USB oder FireWire angeschlossen ist. Wenn ein Computer nicht hochfährt, stecken Sie nicht benötigte Hardware aus und versuchen Sie es erneut.

Überwachen Sie nach dem Booten die Bootmeldungen des Systems mit dem Befehl `dmesg | grep -2i acpi` (oder überwachen Sie alle Meldungen, da das Problem möglicherweise nicht durch ACPI verursacht wurde). Wenn bei der Analyse einer ACPI-Tabelle ein Fehler auftritt, kann die wichtigste Tabelle, DSDT, durch eine verbesserte Version ersetzt werden. In diesem Fall wird die fehlerhafte DSDT des BIOS ignoriert. Das Verfahren wird in [Abschnitt 24.4.3, „Fehlersuche“](#) (S. 473) erläutert.

In der Kernel-Konfiguration gibt es einen Schalter zur Aktivierung der ACPI-Fehlermeldung. Wenn ein Kernel mit ACPI-Fehlersuche kompiliert und installiert wurde, können Experten, die nach einem Fehler suchen, mit detaillierten Informationen unterstützt werden.

Wenn Sie Probleme mit dem BIOS oder der Hardware feststellen, sollten Sie stets Kontakt mit den betreffenden Herstellern aufweisen. Insbesondere Hersteller, die nicht immer Hilfe für Linux anbieten, sollten mit den Problemen konfrontiert werden. Die Hersteller nehmen das Problem nur dann ernst, wenn sie feststellen, dass eine nennenswerte Zahl ihrer Kunden Linux verwendet.

Weiterführende Informationen

- <http://www.cpqlinux.com/acpi-howto.html> (detailliertes ACPI HOWTO, enthält DSDT-Patches)

- <http://www.intel.com/technology/iapc/acpi/faq.htm> (ACPI FAQ @Intel)
- <http://www.lesswatts.org/projects/acpi/> (das ACPI4Linux-Projekt von Sourceforge)
- <http://www.poupinou.org/acpi/> (DSDT-Patches von Bruno Ducrot)

24.3 Ruhezustand für Festplatte

In Linux kann die Festplatte vollständig ausgeschaltet werden, wenn sie nicht benötigt wird, oder sie kann in einem energiesparenderen oder ruhigeren Modus betrieben werden. Bei modereren Notebooks müssen die Festplatten nicht manuell ausgeschaltet werden, da sie automatisch in einen Sparbetriebsmodus geschaltet werden, wenn sie nicht benötigt werden. Um die Energieeinsparungen zu maximieren, sollten Sie jedoch einige der folgenden Verfahren ausprobieren.

Mit der Anwendung `hdparm` können verschiedene Festplatteneinstellungen bearbeitet werden. Die Option `-y` schaltet die Festplatte sofort in den Stand-by-Modus. `-Y` versetzt sie in den Ruhezustand. `hdparm -S x` führt dazu, dass die Festplatte nach einem bestimmten Inaktivitätszeitraum abgeschaltet wird. Ersetzen Sie `x` wie folgt: 0 deaktiviert diesen Mechanismus, sodass die Festplatte kontinuierlich ausgeführt wird. Werte von 1 bis 240 werden mit 5 Sekunden multipliziert. Werte von 241 bis 251 entsprechen 1- bis 11-mal 30 Minuten.

Die internen Energiesparoptionen der Festplatte lassen sich über die Option `-B` steuern. Wählen Sie einen Wert 0 (maximale Energieeinsparung) bis 255 (maximaler Durchsatz). Das Ergebnis hängt von der verwendeten Festplatte ab und ist schwer einzuschätzen. Die Geräuschentwicklung einer Festplatte können Sie mit der Option `-M` reduzieren. Wählen Sie einen Wert von 128 (ruhig) bis 254 (schnell).

Häufig ist es nicht so einfach, die Festplatte in den Ruhezustand zu versetzen. Bei Linux führen zahlreiche Prozesse Schreibvorgänge auf der Festplatte durch, wodurch diese wiederholt aus dem Ruhezustand reaktiviert wird. Daher sollten Sie unbedingt verstehen, wie Linux mit Daten umgeht, die auf die Festplatte geschrieben werden müssen. Zunächst werden alle Daten im RAM-Puffer gespeichert. Dieser Puffer wird vom `pdflush`-Daemon überwacht. Wenn die Daten ein bestimmtes Alter erreichen oder wenn der Puffer bis zu einem bestimmten Grad gefüllt ist, wird der Pufferinhalt auf die Festplatte übertragen. Die Puffergröße ist dynamisch und hängt von der Größe des

Arbeitsspeichers und von der Systemlast ab. Standardmäßig werden für `pdflush` kurze Intervalle festgelegt, um maximale Datenintegrität zu erreichen. Das Programm überprüft den Puffer alle fünf Sekunden und schreibt die Daten auf die Festplatte. Die folgenden Variablen sind interessant:

`/proc/sys/vm/dirty_writeback_centisecs`

enthält die Verzögerung bis ein `pdflush`-Thread in Hundertstel Sekunden reaktiviert wird.

`/proc/sys/vm/dirty_expire_centisecs`

definiert, nach welchem Zeitabschnitt eine schlechte Seite spätestens ausgeschrieben werden sollte. Der Standardwert ist 3000, was 30 Sekunden bedeutet.

`/proc/sys/vm/dirty_background_ratio`

maximaler Prozentsatz an schlechten Seiten bis `pdflush` damit beginnt, sie zu schreiben. Der Standardwert ist 5%.

`/proc/sys/vm/dirty_ratio`

wenn die schlechten Seiten diesen Prozentsatz des gesamten Arbeitsspeichers überschreiten, werden Prozesse gezwungen, während ihres Zeitabschnitts Puffer mit schlechten Seiten anstelle von weiteren Daten zu schreiben.

WARNUNG: Beeinträchtigung der Datenintegrität

Änderungen an den Einstellungen für den `pdflush`-Aktualisierungs-Daemon gefährden die Datenintegrität.

Abgesehen von diesen Prozessen schreiben protokollierende Journaling-Dateisysteme, wie ReiserFS und Ext3, ihre Metadaten unabhängig von `pdflush`, was ebenfalls das Abschalten der Festplatte verhindert. Um dies zu vermeiden, wurde eine spezielle Kernel-Erweiterung für mobile Geräte entwickelt. Details finden Sie unter `/usr/src/linux/Documentation/laptop-mode.txt`.

Ein weiterer wichtiger Faktor ist die Art und Weise, wie sich die Programme verhalten. Gute Editoren beispielsweise schreiben regelmäßig verborgene Sicherungskopien der aktuell bearbeiteten Datei auf die Festplatte, wodurch die Festplatte wieder aktiviert wird. Derartige Funktionen können auf Kosten der Datenintegrität deaktiviert werden.

In dieser Verbindung verwendet der Mail-Daemon postfix die Variable `POSTFIX_LAPTOP`. Wenn diese Variable auf `yes` (ja) gesetzt wird, greift postfix wesentlich seltener auf die Festplatte zu.

24.4 Das Powersave-Paket

Das `Powersave`-Paket enthält alle zuvor erwähnten Stromsparfunktionen. Aufgrund der allgemein wachsenden Forderung nach geringerem Energieverbrauch sind einige der enthaltenen Funktionen auch auf Arbeitsstationen und Servern wichtig. Beispielsweise der Suspend- oder Standby-Modus oder die CPU-Frequenzskalierung.

Dieses Paket enthält alle Energieverwaltungsfunktionen für Ihren Computer. Es unterstützt Hardware, die ACPI, IDE-Festplatten und PowerNow!- oder SpeedStep-Technologien verwendet. Die Funktionen der Pakete `apmd`, `acpid`, `ospmd` und `cpufreqd` (jetzt `cpuspeed`) wurden im `Powersave`-Paket zusammengeführt. Die Daemons aus diesen Paketen sollten nicht gleichzeitig mit dem Powersave-Daemon ausgeführt werden (mit Ausnahme von `acpid`, der als Multiplexer für ACPI-Ereignisse fungiert).

Selbst wenn Ihr System nicht alle oben aufgeführten Hardware-Elemente beinhaltet, sollten Sie den Powersave-Daemon zur Steuerung der Energiesparfunktion verwenden. Da sich ACPI und APM gegenseitig ausschließen, können Sie nur eines dieser Systeme auf Ihrem Computer verwenden. Der Daemon erkennt automatisch etwaige Änderungen in der Hardware-Konfiguration.

24.4.1 Konfigurieren des Powersave-Pakets

Die Konfiguration von Powersave wird auf mehrere Dateien verteilt: Jede hier aufgelistete Konfigurationsoption enthält eine zusätzliche Dokumentation zur eigenen Funktionalität.

`/etc/sysconfig/powersave/common`

Diese Datei enthält allgemeine Einstellungen für den Powersave-Daemon. Der Umfang der Fehlersuchmeldungen in `/var/log/messages` lässt sich beispielsweise durch Heraufsetzen des Werts der Variablen `DEBUG` erhöhen.

`/etc/sysconfig/powersave/events`

Der Powersave-Daemon benötigt diese Datei zur Verarbeitung von Systemereignissen. Einem Ereignis können externe Aktionen oder vom Daemon selbst ausgeführte Aktionen zugewiesen werden. Bei externen Aktionen versucht der Daemon eine ausführbare Datei (normalerweise ein Bash-Skript) in `/usr/lib/powersave/scripts/` auszuführen. Vordefinierte interne Aktionen:

- `ignore`
- `throttle`
- `dethrottle`
- `suspend_to_disk`
- `suspend_to_ram`
- `standby`
- `notify`
- `screen_saver`
- `reread_cpu_capabilities`

`throttle` verlangsamt den Prozessor um den in `MAX_THROTTLING` festgelegten Wert. Dieser Wert hängt vom aktuellen Schema ab. `dethrottle` setzt den Prozessor auf volle Leistung. `suspend_to_disk`, `suspend_to_ram` und `standby` lösen das Systemereignis für einen Energiesparmodus aus. Diese drei Aktionen sind in der Regel für die Auslösung des Energiesparmodus zuständig, sie sollten jedoch stets mit bestimmten Systemereignissen verknüpft sein.

Das Verzeichnis `/usr/lib/powersave/scripts` enthält Skripten zum Verarbeiten von Ereignissen:

`switch_vt`

Hilfreich, wenn der Bildschirm nach einem Suspend- oder Stand-by-Vorgang verschoben ist.

`wm_logout`

Speichert die Einstellungen und Protokolle aus GNOME, KDE oder anderen Fenstermanagern.

`wm_shutdown`

Speichert die GNOME- bzw. KDE-Einstellungen und fährt das System herunter.

Wenn beispielsweise die Variable

```
EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk  
do_suspend_to_disk"
```

 festgelegt wird, werden die beiden Skripten oder Aktionen in der angegebenen Reihenfolge verarbeitet, sobald der Benutzer Powersaved den Befehl für den Energiesparmodus Suspend to Disk erteilt. Der Daemon führt das externe Skript `/usr/lib/powersave/scripts/prepare_suspend_to_disk` aus. Nach der erfolgreichen Verarbeitung dieses Skripts führt der Daemon die interne Aktion `do_suspend_to_disk` aus und versetzt den Computer in den Energiesparmodus, nachdem kritische Module mithilfe des Skripts entladen und Dienste gestoppt wurden.

Die Aktionen für das durch einen Energiespar-Schalter ausgelöste Ereignis können wie in `EVENT_BUTTON_SLEEP="notify_suspend_to_disk"` geändert werden. In diesem Fall wird der Benutzer durch ein Popup-Fenster in X oder eine Meldung auf der Konsole über den Suspend-Vorgang informiert. Anschließend wird das Ereignis `EVENT_GLOBAL_SUSPEND2DISK` generiert, was zur Ausführung der erwähnten Aktionen und einem sicheren Suspend-Modus für das System führt. Die interne Aktion `notify` kann mithilfe der Variablen `NOTIFY_METHOD` in `/etc/sysconfig/powersave/common` angepasst werden.

`/etc/sysconfig/powersave/cpufreq`

Enthält Variablen für die Optimierung der dynamischen CPU-Frequenzeinstellungen und legt fest, ob die userspace- oder die Kernel-Implementierung verwendet werden soll.

`/etc/sysconfig/powersave/battery`

Enthält Grenzwerte für den Akku und andere akkuspezifische Einstellungen.

`/etc/sysconfig/powersave/thermal`

Aktiviert Kühlung und Wärmesteuerung. Einzelheiten zu diesem Thema finden Sie in der Datei `/usr/share/doc/packages/powersave/README.thermal`.

/etc/sysconfig/powersave/scheme_*

Dies sind die verschiedenen Schemata, die den Energieverbrauch an bestimmte Bereitstellungsszenarien anpassen. Eine Anzahl von Schemata werden vorkonfiguriert und können unverändert verwendet werden. Außerdem können hier benutzerdefinierte Schemata gespeichert werden.

24.4.2 Weitere ACPI-Funktionen

Wenn Sie ACPI verwenden, können Sie steuern, wie Ihr System auf *ACPI-Schalter* (Ein/Aus, Energiesparen, Deckel offen, Deckel geschlossen) reagieren soll. Die Ausführung der Aktionen wird in `/etc/sysconfig/powersave/events` konfiguriert. In dieser Konfigurationsdatei finden Sie auch eine Erklärung der einzelnen Optionen.

TIPP: Konfigurieren von ACPI-Schaltflächen

Die Einstellungen in `/etc/sysconfig/powersave/event` werden nur berücksichtigt, wenn auf dem Desktop des Benutzers kein Energieverwaltungs-Applet (KPowerSave oder GNOME Power Manager) ausgeführt wird.

`EVENT_BUTTON_POWER="wm_shutdown"`

`EVENT_BUTTON_POWER="wm_shutdown"` Wenn der Netzschalter gedrückt wird, reagiert das System mit Herunterfahren des jeweiligen Fenstermanagers (KDE, GNOME, fvwm usw.).

`EVENT_BUTTON_SLEEP="suspend_to_disk"`

Wenn der Energiespar-Schalter gedrückt wird, wird das System in den Modus "Suspend to Disk" versetzt.

`EVENT_BUTTON_LID_OPEN="ignore"`

Das Öffnen des Deckels hat keine Wirkung.

`EVENT_BUTTON_LID_CLOSED="screen_saver"`

Beim Schließen des Deckels wird der Bildschirmschoner aktiviert.

`EVENT_OTHER="ignore"`

Dieses Ereignis tritt ein, wenn ein unbekanntes Ereignis vom Daemon erkannt wird. Unbekannte Ereignisse sind beispielsweise ACPI-Tastenkombinationen auf einigen Rechnern.

Eine weitere Drosselung der CPU-Leistung ist möglich, wenn die CPU-Last über einen bestimmten Zeitraum einen angegebenen Wert nicht übersteigt. Geben Sie die Lastgrenze in `PROCESSOR_IDLE_LIMIT` und den Wert für die Zeitüberschreitung in `CPU_IDLE_TIMEOUT` an. Wenn die CPU-Last länger als unterhalb des Grenzwerts bleibt, als für die Zeitüberschreitung festgelegt, wird das in `EVENT_PROCESSOR_IDLE` konfigurierte Ereignis aktiviert. Wenn die CPU erneut belegt ist, wird `EVENT_PROCESSOR_BUSY` ausgeführt.

24.4.3 Fehlersuche

Alle Fehler- und Alarmmeldungen werden in der Datei `/var/log/messages` protokolliert. Wenn Sie die benötigten Informationen nicht finden können, erhöhen Sie die Ausführlichkeit der Powersave-Meldungen mithilfe von `DEBUG` in der Datei `/etc/sysconfig/powersave/common`. Erhöhen Sie den Wert der Variablen auf 7 oder sogar 15 und starten Sie den Daemon erneut. Mithilfe der detaillierteren Fehlermeldungen in `/var/log/messages` sollten Sie den Fehler leicht finden können. In den folgenden Abschnitten werden die häufigsten Probleme mit Powersave und den verschiedenen Energiesparmodi behandelt.

ACPI mit Hardware-Unterstützung aktiviert, bestimmte Funktionen sind jedoch nicht verfügbar

Bei Problemen mit ACPI können Sie mit dem Befehl `dmesg|grep -i acpi` die Ausgabe von `dmesg` nach ACPI-spezifischen Meldungen durchsuchen. Zur Behebung des Problems kann eine BIOS-Aktualisierung erforderlich sein. Rufen Sie die Homepage Ihres Notebookherstellers auf, suchen Sie nach einer aktualisierten BIOS-Version und installieren Sie sie. Bitten Sie den Hersteller, die aktuellsten ACPI-Spezifikationen einzuhalten. Wenn der Fehler auch nach der BIOS-Aktualisierung noch besteht, gehen Sie wie folgt vor, um die fehlerhafte DSDT-Tabelle im BIOS mit einer aktualisierten DSDT zu ersetzen:

- 1 Laden Sie die DSDT für Ihr System von der Seite <http://acpi.sourceforge.net/dsdt/index.php> herunter. Prüfen Sie, ob die Datei dekomprimiert und kompiliert ist. Dies wird durch die Dateinamenserweiterung `.aml` (ACPI Machine Language) angezeigt. Wenn dies der Fall ist, fahren Sie mit Schritt 3 fort.

- 2 Wenn die Dateierweiterung der heruntergeladenen Tabelle `.asl` (ACPI Source Language) lautet, kompilieren Sie sie mit `iasl` (Paket `pmttools`). Geben Sie den Befehl `iasl -sa file.asl` ein. Die aktuellste Version von `asl` (Intel ACPI Compiler) ist unter <http://developer.intel.com/technology/iapc/acpi/downloads.htm> verfügbar.
- 3 Kopieren Sie die Datei `DSDT.asl` an einen beliebigen Speicherort (`/etc/DSDT.asl` wird empfohlen). Bearbeiten Sie `/etc/sysconfig/kernel` und passen Sie den Pfad zur `DSDT`-Datei entsprechend an. Starten Sie `mkinitrd` (Paket `mkinitrd`). Immer wenn Sie den Kernel installieren und `mkinitrd` verwenden, um `initrd` zu erstellen, wird die bearbeitete `DSDT` beim Booten des Systems integriert und geladen.

CPU-Frequenzsteuerung funktioniert nicht

Rufen Sie die Kernel-Quelle (`kernel-source`) auf, um festzustellen, ob der verwendete Prozessor unterstützt wird. Möglicherweise ist ein spezielles Kernel-Modul bzw. eine Moduloption erforderlich, um die CPU-Frequenzsteuerung zu aktivieren. Diese Informationen erhalten Sie unter `/usr/src/linux/Documentation/cpu-freq/*`.

Suspend und Stand-by funktionieren nicht

ACPI-Systeme können Probleme mit dem Stromspar- und Standby-Modus haben, wenn die `DSDT`-Implementierung (BIOS) fehlerhaft ist. Aktualisieren Sie in diesem Fall das BIOS.

Beim Versuch fehlerhafte Module zu entladen, reagiert das System nicht mehr oder das Suspend-Ereignis wird nicht ausgelöst. Dies kann auch dann passieren, wenn Sie keine Module entladen oder Dienste stoppen, die ein erfolgreiches Suspend-Ereignis verhindern. In beiden Fällen müssen Sie versuchen, das fehlerhafte Modul zu ermitteln, das den Energiesparmodus verhindert hat. Die Protokolldatei `/var/log/pm-suspend.log` enthält ausführliche Informationen über die einzelnen Vorgänge und mögliche Fehlerursachen. Ändern Sie die Variable `SUSPEND_MODULES` in `/usr/lib/pm-utils/defaults`, um problematische Module vor einem Suspend- oder Standby-Vorgang zu entladen.

Ausführliche Informationen zur Änderung des Suspend- und Resume-Prozesses finden Sie unter <http://www.opensuse.org/Pm-utils> und <http://www.opensuse.org/S2ram>.

24.4.4 Weiterführende Informationen

- `/usr/share/doc/packages/powersave` – Lokale Dokumentation zum Powersave-Daemon
- <http://powersave.sourceforge.net> – Aktuelle Dokumentation zum Powersave-Daemon
- http://www.opensuse.org/Projects_Powersave – Projektseite auf openSUSE-Wiki
- <http://www.opensuse.org/S2ram> – Anleitung zur Einstellung von "Suspend to RAM"
- <http://www.opensuse.org/Pm-utils> – Anleitung zur Änderung des allgemeinen Suspend-Frameworks

Drahtlose Kommunikation

Sie können Ihr Linux-System auf verschiedene Arten für die Kommunikation mit anderen Computern, Mobiltelefonen oder peripheren Geräten nutzen. Mit WLAN (Wireless LAN) können Notebooks in einem Netzwerk miteinander verbunden werden.

25.1 Wireless LAN

Wireless LANs sind zu einem unverzichtbaren Aspekt der mobilen Computernutzung geworden. Heutzutage verfügen die meisten Notebooks über eingebaute WLAN-Karten. Grundsätzlich lassen sich drahtlose Netzwerke in verwaltete Netzwerke und Ad-hoc-Netzwerke unterteilen. Verwaltete Netzwerke verfügen über ein verwaltendes Element: den Zugriffspunkt. In diesem Modus (auch als Infrastrukturmodus bezeichnet) laufen alle Verbindungen der WLAN-Stationen im Netzwerk über den Zugriffspunkt, der auch als Verbindung zu einem Ethernet fungieren kann. Ad-hoc-Netzwerke weisen keinen Zugriffspunkt auf. Die Stationen kommunizieren unmittelbar miteinander. Übertragungsbereich und Anzahl der teilnehmenden Stationen sind in Ad-hoc-Netzwerken stark eingeschränkt. Daher ist ein Zugriffspunkt normalerweise effizienter. Es ist sogar möglich, eine WLAN-Karte als Zugriffspunkt zu verwenden. Die meisten Karten unterstützen diese Funktionen.

25.1.1 Konfiguration mit YaST

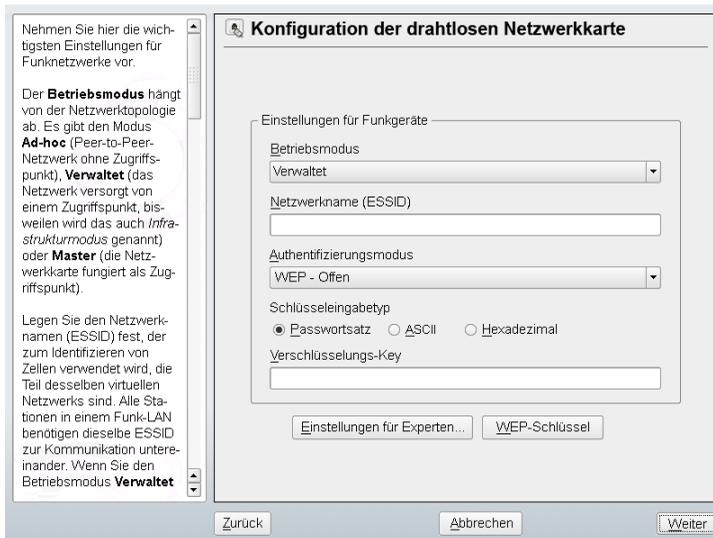
Zum Konfigurieren der drahtlosen Netzwerkkarte wählen Sie im YaST-Kontrollzentrum die Optionen *Netzwerkgeräte* > *Netzwerkeinstellungen* aus. Das Dialogfeld "Netzwerkeinstellungen" wird geöffnet, in dem Sie allgemeine Netzwerkeinstellungen konfigurieren

können. Weitere Informationen zur Netzwerkkonfiguration allgemein finden Sie unter [Abschnitt 14.4, „Konfigurieren von Netzwerkverbindungen mit YaST“](#) (S. 243). Alle vom System erkannten Netzwerkkarten werden auf dem Karteireiter *Übersicht* aufgelistet.

Wählen Sie die drahtlose Karte aus der Liste aus und klicken Sie auf *Bearbeiten*, um das Dialogfeld "Einrichten von Netzwerkkarten" zu öffnen. Nehmen Sie auf dem Karteireiter *Adresse* die Konfiguration zur Verwendung einer dynamischen oder einer statischen IP-Adresse vor. Sie können auch die Einstellungen unter *Allgemein* und *Hardware* wie zum Beispiel *Geräte-Aktivierung* oder *Firewall-Zone* sowie die Treibereinstellungen anpassen. In den meisten Fällen ist es nicht erforderlich, die vorkonfigurierten Werte zu ändern.

Klicken Sie auf *Weiter*, um mit der Konfiguration der drahtlosen Netzwerkkarten im dafür vorgesehenen Dialogfeld fortzufahren. Wenn Sie NetworkManager verwenden (weitere Informationen dazu finden Sie unter [Abschnitt 14.5, „NetworkManager“](#) (S. 263)), ist es nicht erforderlich, die Einstellungen für drahtlose Gerät anzupassen, da diese von NetworkManager nach Bedarf festgelegt werden – fahren Sie mit *Weiter* und *Ja* fort, um die Konfiguration fertig zu stellen. Wenn Sie Ihren Computer nur in einem speziellen drahtlosen Netzwerk verwenden, nehmen Sie hier die grundlegenden Einstellungen für den WLAN-Betrieb vor.

Abbildung 25.1 YaST: Konfigurieren der WLAN-Karte



Betriebsmodus

Eine Station kann in drei verschiedenen Modi in ein WLAN integriert werden. Der geeignete Modus hängt vom Netzwerk ab, in dem kommuniziert werden soll: *Ad-hoc* (Peer-to-Peer-Netzwerk ohne Zugriffspunkt), *Verwaltet* (Netzwerk wird über Zugriffspunkt verwaltet) oder *Master* (Ihre Netzwerkkarte soll als Zugriffspunkt verwendet werden). Um einen der WPA-PSK- oder WPA-EAP-Modi zu verwenden, muss der Betriebsmodus auf *Verwaltet* gesetzt sein.

Netzwerkname (ESSID)

Alle Stationen in einem drahtlosen Netzwerk benötigen dieselbe ESSID zur Kommunikation untereinander. Wenn nichts angegeben ist, wählt die Karte automatisch einen Zugriffspunkt aus, der möglicherweise von dem von Ihnen vorgesehenen abweicht.

Authentifizierungsmodus

Wählen Sie eine passende Authentifizierungsmethode für Ihr Netzwerk aus: *Keine Verschlüsselung*, *WEP-Open*, *WEP-Shared Key*, *WPA-EAP* oder *WPA-PSK*. Bei Auswahl der WPA-Authentifizierung muss ein Netzwerkname (ESSID) festgelegt werden.

Art der Schlüsseleingabe

Die WEP- und WPA-PSK-Authentifizierung verlangt die Eingabe eines Schlüssels. Der Schlüssel muss entweder als *Passwortsatz*, als *ASCII-String* oder als *Hexadezimal-String* eingegeben werden.

WEP-Schlüssel

Geben Sie hier entweder den Standardschlüssel ein oder klicken Sie auf *WEP-Schlüssel*, um das erweiterte Dialogfeld für die Schlüsselkonfiguration zu öffnen. Legen Sie die Länge des Schlüssels auf *128 Bit* oder *64 Bit* fest. Die Standardeinstellung ist *128 Bit*. Im Listenbereich unten im Dialogfeld können bis zu vier verschiedene Schlüssel angegeben werden, die Ihre Station für die Verschlüsselung verwenden soll. Wählen Sie *Als Standard festlegen*, um einen davon als Standardschlüssel festzulegen. Wenn Sie hier keine Auswahl treffen, verwendet YaST den als erstes eingegebenen Schlüssel als Standardschlüssel. Wenn der Standardschlüssel gelöscht wird, muss einer der anderen Schlüssel manuell als Standardschlüssel gekennzeichnet werden. Klicken Sie auf *Bearbeiten*, um bestehende Listeneinträge zu bearbeiten oder neue Schlüssel zu erstellen. In diesem Fall werden Sie über ein Popup-Fenster dazu aufgefordert, einen Eingabetyp auszuwählen (*Passwortsatz*, *ASCII* oder *Hexadezimal*). Geben Sie bei Verwendung von *Passwortsatz* ein Wort oder eine Zeichenkette ein,

aus der ein Schlüssel mit der zuvor festgelegten Länge erstellt wird. *ASCII* erfordert die Eingabe von 5 Zeichen für einen 64-Bit-Schlüssel und von 13 Zeichen für einen 128-Bit-Schlüssel. Bei *Hexadezimal* geben Sie 10 Zeichen für einen 64-Bit-Schlüssel bzw. 26 Zeichen für einen 128-Bit-Schlüssel in Hexadezimalnotation ein.

WPA-PSK

Um einen Schlüssel für WPA-PSK einzugeben, stehen die Eingabemethoden *Passwortsatz* bzw. *Hexadezimal* zur Auswahl. Im Modus *Passwortsatz* muss die Eingabe 8 bis 63 Zeichen betragen. Im Modus *Hexadezimal* geben Sie 64 Zeichen ein.

Einstellungen für Experten

Mit dieser Schaltfläche wird ein Dialogfeld für die detaillierte Konfiguration der WLAN-Verbindung geöffnet. Normalerweise sollte es nicht erforderlich sein, die vorkonfigurierten Einstellungen zu ändern.

Channel

Die Spezifikation eines Kanals, über den die WLAN-Station arbeiten soll, ist nur in den Modi *Ad-hoc* und *Master* erforderlich. Im Modus *Verwaltet* durchsucht die Karte automatisch die verfügbaren Kanäle nach Zugriffspunkten. Im Modus *Ad-hoc* müssen Sie einen der 12 angebotenen Kanäle für die Kommunikation zwischen Ihrer Station und den anderen Stationen auswählen. Im Modus *Master* müssen Sie festlegen, auf welchem Kanal Ihre Karte die Funktionen des Zugriffspunkts anbieten soll. Die Standardeinstellung für diese Option lautet *Auto*.

Bitrate

Je nach der Leistungsfähigkeit Ihres Netzwerks können Sie eine bestimmte Bitrate für die Übertragung von einem Punkt zum anderen festlegen. Bei der Standardeinstellung, *Auto*, versucht das System, die höchstmögliche Datenübertragungsrate zu verwenden. Einige WLAN-Karten unterstützen die Festlegung von Bitraten nicht.

Zugriffspunkt

In einer Umgebung mit mehreren Zugriffspunkten kann einer davon durch Angabe der MAC-Adresse vorausgewählt werden.

Energieverwaltung verwenden

Wenn Sie Ihr Notebook unterwegs verwenden, sollten Sie die Akku-Betriebsdauer mithilfe von Energiespartechnologien maximieren. Weitere Informationen über die Energieverwaltung finden Sie in **Kapitel 24, Energieverwaltung** (S. 457).

Klicken Sie auf "Weiter", um die Einrichtung fertig zu stellen. Wenn Sie die WPA-EAP-Authentifizierung gewählt haben, ist ein weiterer Konfigurationsschritt erforderlich, bevor Ihr Arbeitsplatzrechner im WLAN bereitgestellt werden kann. Geben Sie den Berechtigungsnachweis ein, den Sie von Ihrem Netzwerkadministrator erhalten haben. Geben Sie für TLS *Identität*, *Client-Zertifikat*, *Client-Schlüssel* und *Server-Zertifikat* an. Für TTLS und PEAP sind *Identität* und *Passwort* erforderlich. Die Optionen *Server-Zertifikat* und *Anonyme Identität* sind optional. YaST sucht unter `/etc/cert` nach einem Zertifikat. Speichern Sie daher die erhaltenen Zertifikate an diesem Ort und schränken Sie den Zugriff zu diesen Dateien auf 0600 (Lese- und Schreibzugriff des Eigentümers) ein. Klicken Sie auf *Details*, um das Dialogfeld für die erweiterte Authentifizierung für die WPA-EAP-Einrichtung aufzurufen. Wählen Sie die Authentifizierungsmethode für die zweite Phase der EAP-TTLS- oder EAP-PEAP-Kommunikation aus. Wenn Sie im vorherigen Dialogfeld TTLS ausgewählt haben, wählen Sie `any`, `MD5`, `GTC`, `CHAP`, `PAP`, `MSCHAPv1` oder `MSCHAPv2`. Wenn Sie PEAP ausgewählt haben, wählen Sie `any`, `MD5`, `GTC` oder `MSCHAPv2`. *PEAP-Version* kann verwendet werden, um die Verwendung einer bestimmten PEAP-Implementierung zu erzwingen, falls die automatisch festgelegte Einstellung für Sie nicht funktioniert.

WICHTIG: Sicherheit in drahtlosen Netzwerken.

Sie sollten unbedingt eine der unterstützten Authentifizierungs- und Verschlüsselungsmethoden für den Schutz Ihres Netzwerks verwenden. Bei nicht verschlüsselten WLAN-Verbindungen können Dritte alle Netzwerkdaten abfangen. Selbst eine schwache Verschlüsselung (WEP) ist besser als gar keine.

25.1.2 Dienstprogramme

kismet (Paket `kismet`) ist ein Werkzeug zur Netzwerkd Diagnose, mit dem Sie den WLAN-Paketverkehr überwachen können. Auf diese Weise können Sie auch etwaige Versuche einer unbefugten Benutzung des Netzwerks durch Dritte feststellen. Weitere Informationen finden Sie unter <http://www.kismetwireless.net/> und auf der entsprechenden Handbuchseite.

25.1.3 Tipps und Tricks zur Einrichtung eines WLAN

Mit diesen Tipps können Sie Geschwindigkeit und Stabilität sowie Sicherheitsaspekte Ihres WLAN optimieren.

Stabilität und Geschwindigkeit

Leistungsfähigkeit und Zuverlässigkeit eines drahtlosen Netzwerks hängen in erster Linie davon ab, ob die teilnehmenden Stationen ein sauberes Signal von den anderen Stationen empfangen. Hindernisse, wie beispielsweise Wände, schwächen das Signal erheblich ab. Je weiter die Signalstärke sinkt, desto langsamer wird die Übertragung. Während des Betriebs können Sie die Signalstärke mit dem Dienstprogramm `iwconfig` in der Kommandozeile (Feld `Link-Qualität`) oder mit `NetworkManager` oder `KNetworkManager` überprüfen. Bei Problemen mit der Signalqualität sollten Sie versuchen, die Geräte an einer anderen Position einzurichten oder die Antennen der Zugriffspunkte neu zu positionieren. Hilfsantennen, die den Empfang erheblich verbessern sind für eine Reihe von PCMCIA-WLAN-Karten erhältlich. Die vom Hersteller angegebene Rate, beispielsweise 54 MBit/s, ist ein Nennwert, der für das theoretische Maximum steht. IN der Praxis beträgt der maximale Datendurchsatz nicht mehr als die Hälfte dieses Werts.

Sicherheit

Wenn Sie ein drahtloses Netzwerk einrichten möchten, sollten Sie bedenken, dass jeder, der sich innerhalb der Übertragungreichweite befindet, problemlos auf das Netzwerk zugreifen kann, sofern keine Sicherheitsmaßnahmen implementiert sind. Daher sollten Sie auf jeden Fall eine Verschlüsselungsmethode aktivieren. Alle WLAN-Karten und Zugriffspunkte unterstützen WEP-Verschlüsselung. Dieses Verfahren bietet zwar keine absolute Sicherheit, es stellt jedoch durchaus ein Hindernis für mögliche Angreifer dar. WEP ist für den privaten Gebrauch in der Regel ausreichend. WPA-PSK bietet noch größere Sicherheit, es ist jedoch in älteren Zugriffspunkten und Routern mit WLAN-Funktionen nicht implementiert. Auf einigen Geräten kann WPA mithilfe einer Firmware-Aktualisierung implementiert werden. Außerdem unterstützt Linux WPA nicht auf allen Hardware-Komponenten. Wenn WPA nicht verfügbar ist, sollten Sie lieber WEP verwenden, als völlig auf Verschlüsselung zu verzichten. Bei Unternehmen mit

erhöhten Sicherheitsanforderungen sollten drahtlose Netzwerke ausschließlich mit WPA betrieben werden.

25.1.4 Fehlersuche

Wenn Ihre WLAN-Karte nicht automatisch erkannt wird oder wenn sie nicht antwortet, prüfen Sie, ob die Karte von openSUSE unterstützt wird. Eine Liste der unterstützten WLAN-Netzwerkkarten finden Sie unter [http://en.opensuse.org/HCL/Network_Adapters_\(Wireless\)](http://en.opensuse.org/HCL/Network_Adapters_(Wireless))

Mehrere Netzwerkgeräte

Moderne Laptops verfügen normalerweise über eine Netzwerkkarte und eine WLAN-Karte. Wenn Sie beide Geräte mit DHCP (automatische Adresszuweisung) konfiguriert haben, können Probleme mit der Namensauflösung und dem Standard-Gateway auftreten. Dies können Sie daran erkennen, dass Sie dem Router ein Ping-Signal senden, jedoch nicht das Internet verwenden können. In der Support-Datenbank finden Sie unter http://en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with_Several_Concurrent_DHCP_Clients einen Artikel zu diesem Thema.

Probleme mit Prism2-Karten

Für Geräte mit Prism2-Chips sind mehrere Treiber verfügbar. Die verschiedenen Karten funktionieren mit den einzelnen Treibern mehr oder weniger reibungslos. Bei diesen Karten ist WPA nur mit dem `hostap`-Treiber möglich. Wenn eine solche Karte nicht einwandfrei oder überhaupt nicht funktioniert oder Sie WPA verwenden möchten, lesen Sie nach unter `/usr/share/doc/packages/wireless-tools/README.prism2`.

25.1.5 Weiterführende Informationen

Auf den Internetseiten von Jean Tourrilhes, dem Entwickler der *Wireless Tools* für Linux finden Sie ein breites Spektrum an nützlichen Informationen zu drahtlosen Netzwerken. Weitere Informationen hierzu finden Sie unter http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html.

Verwenden von Tablet PCs

openSUSE® unterstützt Tablet PCs mit seriellen Wacom-Geräten (z. B. IBM/Lenovo X300, ACER TM C301/C302/C3010 Series, Fujitsu Lifebook T Series (T4010/T4200), HP Compaq TC1200, Motion M1200/M1400) und FinePoint-Geräte (z. B. Gateway-Tablet PCs) sowie Fujitsu Siemens Computers P-Series. Sie erfahren hier, wie Sie Ihren Tablet PC installieren und konfigurieren. Außerdem werden Ihnen einige Linux*-Anwendungen vorgestellt, die die Eingabe über digitale Pens akzeptieren.

Nach der Installation der Tablet PC-Pakete und der Konfiguration Ihres Grafiktablets können Sie Ihren Pen (auch als Stylus bezeichnet) für folgende Aktionen und Anwendungen verwenden:

- Anmelden bei KDM oder GDM
- Aufheben der Bildschirmsperre auf KDE- und GNOME-Desktops
- Aktionen, die auch durch andere Zeigeegeräte (z. B. Maus oder Touch Pad) ausgelöst werden können, wie das Verschieben des Cursors auf dem Bildschirm, das Starten von Anwendungen, das Schließen, Skalieren und Verschieben von Fenstern, den Fokuswechsel in ein anderes Fenster oder das Ziehen und Ablegen von Objekten
- Verwenden der Bewegungserkennung in Anwendungen des X Window System
- Zeichnen mit The GIMP
- Aufzeichnen von Notizen oder Skizzen mit Anwendungen wie Jarnal oder Xournal oder Bearbeiten größerer Textmengen mit Dasher

ANMERKUNG: Tastatur oder Maus für Installation erforderlich

Während der Installation von openSUSE kann der Pen nicht als Eingabegerät verwendet werden. Falls Ihr Tablet PC weder über Tastatur noch Touch Pad verfügt, schließen Sie für die Systeminstallation eine externe Tastatur oder Maus an den Tablet PC an.

26.1 Installieren der Tablet PC-Pakete

Die für Tablet PCs benötigten Pakete sind im Installationsschema `Laptop` enthalten – wenn dieses Schema während der Installation ausgewählt wurde, sollten die folgenden Pakete bereits auf dem System installiert sein:

- `jarnal`: Eine Java-basierte Anwendung für die Aufzeichnung von Notizen
- `xournal`: Eine Anwendung für die Aufzeichnung von Notizen und Skizzen
- `xstroke`: Ein Bewegungserkennungsprogramm für das X Window System
- `xvkbd`: Eine virtuelle Tastatur für das X Window System
- `cellwriter`: eine auf Zeichen basierende Kontrollleiste für handschriftliche Eingabe
- `x11-input-wacom`: Das X-Eingabemodul für Wacom-Tablets
- `x11-input-wacom-tools`: Konfiguration, Diagnose und Bibliotheken für Wacom-Tablets
- `x11-input-fujitsu`: Das X-Eingabemodul für Fujitsu P-Series-Tablets

Falls diese Pakete noch nicht installiert sind, installieren Sie diejenigen Pakete, die Sie benötigen, manuell über die Kommandozeile oder wählen Sie das Schema `Laptop` in YaST zur Installation aus.

26.2 Konfigurieren des Tablet-Geräts

Konfigurieren Sie das (interne oder externe) Tablet-Gerät nach der Installation der Tablet PC-Pakete mit SaX2.

- 1 Starten Sie SaX2 an der Kommandozeile oder drücken Sie Alt + F2 und geben Sie `sax2` ein.
- 2 Klicken Sie bei einem Wacom-Gerät auf *Tablet*, um die *Tablet-Eigenschaften* anzuzeigen.

Bei einem Fujitsu P-Series-Gerät klicken Sie stattdessen auf *Touchscreen*.

- 3 Wählen Sie in der Liste auf der rechten Seite *TABLET PCs* als Hersteller und den Namen Ihres Tablets aus und aktivieren Sie *Dieses Tablet aktivieren*.

Wenn Ihr Computer nicht aufgelistet ist und Sie nicht sicher sind, ob Sie ein Wacom-Gerät besitzen, wählen Sie *Wacom ISDV4 TABLET PC (SERIAL)* aus.

- 4 Öffnen Sie den Karteireiter *Elektronische Stifte* und aktivieren Sie dort die folgenden Optionen: *Stift hinzufügen* und *Radierer hinzufügen*.
- 5 Klicken Sie zum Speichern der Änderungen auf *OK*.

Starten Sie Ihren X Server nach Abschluss der X Window System-Konfiguration neu, indem Sie sich abmelden. Alternativ können Sie die Benutzeroberfläche auch geöffnet lassen und `init 3 && init 5` in einer virtuellen Konsole ausführen.

Nach der Konfiguration Ihres Tablet-Geräts können Sie den Pen als Eingabegerät verwenden.

26.3 Verwenden der virtuellen Tastatur

Zur Anmeldung beim KDE- oder GNOME-Desktop und zum Entsperren des Bildschirms können Sie Ihren Benutzernamen und Ihr Passwort wie gewohnt eingeben oder Sie können dazu die virtuelle Tastatur (`xvkbd`) verwenden, die sich unterhalb des Anmelde-

felds befindet. Zur Konfiguration der Tastatur und zum Aufrufen der integrierten Hilfe klicken Sie links unten auf das Feld *xvkbd*, um das xvkbd-Hauptmenü zu öffnen.

Abbildung 26.1 Virtuelle Tastatur von xvkbd



Wenn Sie xvkbd nach der Anmeldung verwenden möchten, starten Sie es aus dem Hauptmenü oder über das Shell-Kommando *xvkbd*.

26.4 Drehen der Ansicht

Verwenden Sie KRandRTray (KDE) oder resapplet (GNOME), um Ihre Anzeige manuell interaktiv zu drehen oder die Größe zu verändern. Sowohl KRandRTray als auch resapplet sind Miniprogramme für die RANDR-Erweiterung von X Server. Nach Starten des entsprechenden Miniprogramms wird das Symbol für das Miniprogramm zum Systemabschnitt der Kontrolleiste hinzugefügt.

Starten Sie KRandRTray oder resapplet im Hauptmenü oder geben Sie *krandrtray* oder *resapplet* ein, um das Miniprogramm von einer Shell aus zu starten. Zum Drehen Ihrer Anzeige mit KRandRTray klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie *Anzeige konfigurieren*. Wählen Sie die gewünschte Ausrichtung im Konfigurations-Dialogfeld aus.

Zum Drehen Ihrer Anzeige mit resapplet klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie die gewünschte Ausrichtung unterhalb von *Bildschirmdrehung* aus. Die Ansicht wird sofort gedreht. Gleichzeitig ändert sich auch die Ausrichtung des Grafiktablets. Es kann daher die Bewegungen des Pens nach wie vor richtig interpretieren.

Bei Problemen mit der Ausrichtung Ihres Desktops finden Sie weitere Informationen unter [Abschnitt 26.7, „Fehlersuche“](#) (S. 492).

26.5 Verwenden der Bewegungserkennung

xstroke erkennt Bewegungen des Pens oder anderer Zeigegeräte als Eingabe für Anwendungen des X Window System. Das xstroke-Alphabet ist ein mit dem Graffiti*-Alphabet vergleichbares Unistroke-Alphabet. Wenn aktiviert, sendet xstroke die Eingabe an das Fenster, das aktuell den Fokus hält.

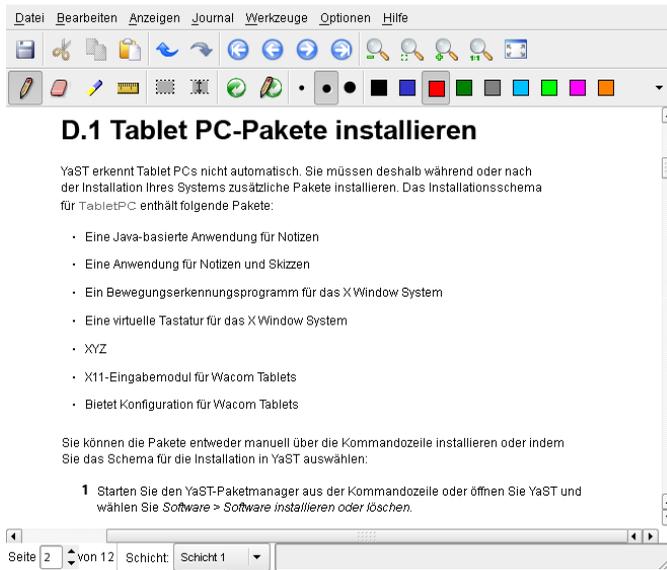
- 1 Starten Sie xstroke aus dem Hauptmenü oder über das Shell-Kommando `xstroke`. Dadurch wird dem Systemabschnitt der Kontrollleiste ein Bleistiftsymbol hinzugefügt.
- 2 Starten Sie die Anwendung, in die Sie mittels des Pens einen Text eingeben möchten (z. B. ein Terminalfenster, einen Texteditor oder einen OpenOffice.org Writer).
- 3 Zum Aktivieren der Bewegungserkennung klicken Sie einmal auf das Bleistiftsymbol.
- 4 Führen Sie auf dem Grafiktablett einige Bewegungen mit dem Pen oder einem anderen Zeigegerät aus. xstroke erfasst die Bewegungen und überträgt sie als Text in das fokussierte Anwendungsfenster.
- 5 Wenn Sie den Fokus in ein anderes Fenster wechseln möchten, klicken Sie mit dem Pen auf das betreffende Fenster und warten Sie einen Moment (oder verwenden Sie dazu das im Kontrollzentrum des Desktops festgelegte Tastenkürzel).
- 6 Zum Deaktivieren der Bewegungserkennung klicken Sie erneut auf das Bleistiftsymbol.

26.6 Aufzeichnen von Notizen und Skizzen mit dem Pen

Zum Anfertigen von Zeichnungen mit dem Pen können Sie einen professionellen Grafikeditor wie The GIMP oder eine Notizenanwendung wie Xournal oder Jarnal verwenden. Sowohl mit Xournal als auch mit Jarnal können Sie mittels Pen Notizen aufzeichnen, Zeichnungen erstellen oder PDF-Dateien kommentieren. Die Java-basierte Anwendung Jarnal ist für verschiedene Plattformen verfügbar und bietet grundlegende Funktionen der Zusammenarbeit. Weitere Informationen hierzu finden Sie in <http://www.dklevine.com/general/software/tc1000/jarnal-net.htm>. Jarnal speichert den Inhalt in einem Archiv mit der Erweiterung .jaj. Dieses Archiv enthält auch eine Datei im SVG-Format.

Starten Sie Jarnal oder Xournal aus dem Hauptmenü oder über das Shell-Kommando `jarnal` bzw. `xournal`. Wenn Sie zum Beispiel in Xournal eine PDF-Datei kommentieren möchten, wählen Sie *File (Datei) > Annotate PDF (PDF kommentieren)* und öffnen Sie dann die PDF-Datei in Ihrem Dateisystem. Tragen Sie Ihre Kommentare mit dem Pen oder einem anderen Zeigegerät in die PDF-Datei ein und speichern Sie die Änderungen mit *File (Datei) > Print to PDF (PDF-Ausgabe)*.

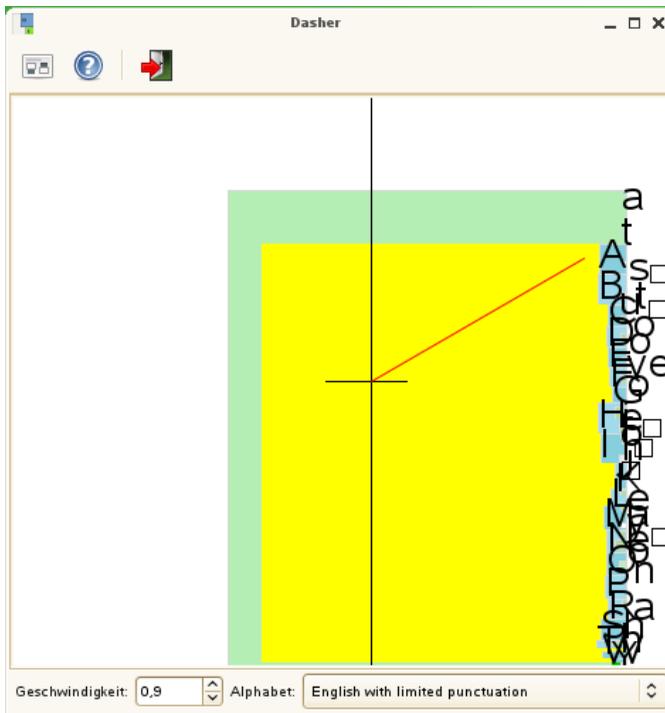
Abbildung 26.2 *Kommentieren einer PDF-Datei mit Xournal*



Dasher ist eine weitere nützliche Anwendung. Sie wurde speziell für Situationen entwickelt, in denen die Eingabe über die Tastatur unpraktisch oder unmöglich ist. Mit ein wenig Übung gelingt es recht bald, auch große Textmengen nur mit dem Pen (oder einem anderen Eingabegerät – selbst mit einem Eye Tracker) einzugeben.

Starten Sie Dasher aus dem Hauptmenü oder über das Shell-Kommando `dasher`. Sobald Sie den Pen in eine Richtung verschieben, beginnen die Buchstaben auf der rechten Seite vorbeizuzoomen. Aus den Buchstaben, die an dem Fadenkreuz in der Mitte vorbeilaufen, wird der Text erstellt bzw. vorausgesagt und im oberen Teil des Fensters angezeigt. Zum Beenden oder Starten der Texteingabe klicken Sie einmal mit dem Pen auf die Anzeige. Die Zoom-Geschwindigkeit können Sie unten im Fenster einstellen.

Abbildung 26.3 Bearbeiten von Text mit Dasher



Das Konzept von Dasher funktioniert in vielen Sprachen. Weitere Informationen finden Sie auf der Website von Dasher, auf der Sie eine umfassende Dokumentation, Demonstrationen und Schulungsdokumente vorfinden. Die Adresse der Website lautet <http://www.inference.phy.cam.ac.uk/dasher/>

26.7 Fehlersuche

Die virtuelle Tastatur wird im Anmeldefenster nicht angezeigt

Gelegentlich wird die virtuelle Tastatur im Anmeldefenster nicht angezeigt. Zur Behebung dieses Problems starten Sie X Server durch Drücken von Strg + Alt + ← neu bzw. drücken Sie die entsprechende Taste auf Ihrem Tablet PC (falls Sie ein schlankes Modell ohne integrierte Tastatur verwenden). Wenn sich das Problem dadurch nicht beheben lässt, schließen Sie eine externe Tastatur an Ihr Modell an und melden Sie sich über diese Tastatur an.

Die Ausrichtung des Grafiktablets wird nicht geändert

Mit dem Kommando `xrandr` können Sie die Ausrichtung der Ansicht über eine Shell ändern. Geben Sie `xrandr --help` ein, um die verfügbaren Optionen dieses Kommandos anzuzeigen. Wenn Sie gleichzeitig die Ausrichtung des Grafiktablets ändern möchten, müssen Sie das Kommando wie folgt eingeben:

- Normale Ausrichtung (Drehung um 0°):

```
xrandr -o 0 && xsetwacom set "Mouse[7]" Rotate 0
```

- Drehung um 90° (im Uhrzeigersinn, Hochformat):

```
xrandr -o 3 && xsetwacom set "Mouse[7]" Rotate 1
```

- Drehung um 180° (Querformat):

```
xrandr -o 2 && xsetwacom set "Mouse[7]" Rotate 3
```

- Drehung um 270° (gegen den Uhrzeigersinn, Hochformat):

```
xrandr -o 1 && xsetwacom set "Mouse[7]" Rotate 2
```

Allerdings wirken sich auf diese Kommandos auch die Einstellungen der Konfigurationsdatei `/etc/X11/xorg.conf` aus. Wenn Sie Ihr Gerät, wie unter [Abschnitt 26.2, „Konfigurieren des Tablet-Geräts“](#) (S. 487) beschrieben, mit SaX2 konfiguriert haben, sollten die Kommandos wie angegeben funktionieren. Wenn Sie den Parameter `Identifier` des Tablet Stylus-Eingabegeräts in der Datei `xorg.conf` manuell geändert haben, müssen Sie `"Mouse[7]"` durch den neuen Identifier ersetzen.

26.8 Weiterführende Informationen

Einige der beschriebenen Anwendungen verfügen über keine integrierte Online-Hilfe. Informationen über deren Verwendung und Konfiguration finden Sie jedoch auf dem installierten System unter `/usr/share/doc/package/Paketname` bzw. im Web:

- Das Xournal-Handbuch finden Sie unter <http://xournal.sourceforge.net/manual.html>
- Die Jarnal-Dokumentation finden Sie unter <http://www.dklevine.com/general/software/tcl1000/jarnal.htm#documentation>
- Die man-Seite zu xstroke finden Sie unter <http://davesource.com/Projects/xstroke/xstroke.txt>
- Eine HOWTO-Anleitung zur Konfiguration von X finden Sie auf der Linux Wacom-Website unter <http://linuxwacom.sourceforge.net/index.php/howto/x11>
- Eine überaus informative Website zum Dasher-Projekt finden Sie unter <http://www.inference.phy.cam.ac.uk/dasher/>
- Informationen zu CellWriter finden Sie unter <http://risujin.org/cellwriter/>

Verwendung des Fingerabdrucklesers

27

Mit dem ThinkFinger-Treiber unterstützt openSUSE® den Fingerabdruckleser von UPEK/SGS Thomson Microelectronics, der im Lieferumfang einiger ThinkPads von IBM und Lenovo enthalten ist. Dieser Fingerabdruckleser kann auch in anderen Laptops entweder als eigenständiges Gerät oder eingebaut in einige USB-Tastaturen gefunden werden. Weitere Einzelheiten finden Sie unter http://thinkfinger.svn.sourceforge.net/viewvc/*checkout*/thinkfinger/README.in. Wenn Ihr System den Fingerabdruckleser enthält, können Sie die biometrische Authentifizierung zusätzlich zur Standardauthentifizierung über Benutzername und Passwort verwenden. Nachdem ihr Fingerabdruck registriert wurde, können sich die Benutzer beim System anmelden, indem sie entweder einen Finger über das Fingerabdruck-Lesegerät ziehen oder ein Passwort eingeben.

Wenn bei der Hardwareprüfung der Fingerabdruckleser in Ihrem Laptop (oder der an Ihr System angeschlossene Fingerabdruckleser) erkannt wird, werden die Pakete `libthinkfinger`, `pam_thinkfinger` und `yast2-fingerprint-reader` automatisch installiert.

Zurzeit kann nur ein Fingerabdruck pro Benutzer registriert werden. Die Fingerabdruckdaten des Benutzers werden unter `/etc/pam_thinkfinger/login.bir` gespeichert. Verwenden Sie zur Verwaltung der Authentifizierung über Fingerabdruck entweder YaST (siehe [Abschnitt 27.2, „Verwalten der Fingerabdrücke mit YaST“](#) (S. 496)) oder das Kommandozeilenwerkzeug `tf-tool`, das außerdem noch zusätzliche Optionen bietet (siehe [Abschnitt 27.3, „Verwalten von Fingerabdrücken mit tf-tool“](#) (S. 498)).

27.1 Unterstützte Anwendungen und Aktionen

Das PAM-Modul `pam_thinkfinger` unterstützt die Authentifizierung über Fingerabdruck für die folgenden Anwendungen und Aktionen (obwohl Sie möglicherweise nicht in jedem Fall dazu aufgefordert werden, Ihren Finger aufzudrücken):

- Anmelden bei GDM/KDM oder einer Anmelde-Shell
- Entsperren des Bildschirms auf dem GNOME/KDE-Desktop
- Starten von YaST und den YaST-Modulen
- Starten einer Anwendung mit `root`-Berechtigung: `sudo` oder `gnomesu`
- Einrichten einer anderen Benutzerkennung mit `su` or `su - Benutzername`

27.2 Verwalten der Fingerabdrücke mit YaST

Prozedur 27.1 Aktivieren der Authentifizierung über Fingerabdruck

Sie können die biometrische Authentifizierung nur dann verwenden, wenn PAM entsprechend konfiguriert ist. Dies erfolgt normalerweise bei der Installation der Pakete, wenn bei der Hardwareprüfung ein unterstützter Fingerabdruckleser erkannt wird. Aktivieren Sie andernfalls die Fingerabdruckunterstützung in YaST wie folgt:

- 1 Starten Sie YaST und wählen Sie *Hardware > Fingerabdruckleser* aus.
- 2 Aktivieren Sie im Konfigurationsdialogfeld die Option *Fingerabdruckleser verwenden* und klicken Sie auf *Fertig stellen*, um die Änderungen zu speichern und das Dialogfeld zu schließen.

Nun können Sie Fingerabdrücke für verschiedene Benutzer registrieren.

Prozedur 27.2 Registrieren eines Fingerabdrucks

- 1 Klicken Sie in YaST auf *Sicherheit und Benutzer > Benutzerverwaltung*, um das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu öffnen. Eine Liste der Benutzer oder Gruppen im System wird angezeigt.
- 2 Wählen Sie den Benutzer aus, für den ein Fingerabdruck registriert werden soll und klicken Sie auf *Bearbeiten*.
- 3 Wählen Sie auf dem Karteireiter *Plugins* den Fingerabdruckeintrag aus und klicken Sie dann auf *Aufrufen*, um das Dialogfeld *Fingerabdruckkonfiguration* zu öffnen.
- 4 YaST fordert den Benutzer auf, den Finger aufzudrücken, bis drei lesbare Fingerabdrücke gesammelt wurden.



- 5 Wenn der Fingerabdruck erfolgreich genommen wurde, klicken Sie auf *Übernehmen*, um das Dialogfeld *Fingerabdruckkonfiguration* und das Dialogfeld für den Benutzer zu schließen.
- 6 Wenn die Authentifizierung über Fingerabdruck auch zum Starten von YaST oder der YaST-Module verwendet werden soll, müssen Sie auch einen Fingerabdruck für `root` registrieren.

Setzen Sie dazu den Filter im Dialogfeld *Verwaltung von Benutzern und Gruppen* auf *Systembenutzer*, wählen Sie den Eintrag `root` aus und registrieren Sie einen Fingerabdruck für `root` wie oben beschrieben.

- 7 Klicken Sie nach der Registrierung der Fingerabdrücke für die gewünschten Benutzer auf *Fertig stellen*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern.

Nachdem der Fingerabdruck des Benutzers erfolgreich registriert wurde, kann der Benutzer wählen, ob er sich für die unter **Abschnitt 27.1, „Unterstützte Anwendungen und Aktionen“** (S. 496) aufgelisteten Aktionen und Anwendungen über Fingerabdruck oder über Passwort authentifizieren will.

Mit YaST können Fingerabdrücke zurzeit weder überprüft noch entfernt werden, doch Sie können Fingerabdrücke auf der Kommandozeile überprüfen oder entfernen. Weitere Informationen finden Sie unter **Überprüfen oder Entfernen eines Fingerabdrucks** (S. 499).

Mit YaST können Sie auch in Ihrem Dateisystem gespeicherte Fingerabdruckdateien (**.bir*) importieren. Klicken Sie auf *Hardware > Fingerabdruckleser* und wählen Sie das *Verzeichnis mit Fingerabdruckdateien* aus oder geben Sie den entsprechenden Pfad ein. Klicken Sie auf *Fertig stellen*, um den Import zu starten. Die Fingerabdruckdateien werden nach */etc/pam_thinkfinger/login.bir*, das Standardverzeichnis für Fingerabdruckdateien, kopiert.

27.3 Verwalten von Fingerabdrücken mit `tf-tool`

Prozedur 27.3 Registrieren eines Fingerabdrucks

- 1 Öffnen Sie eine Shell und melden Sie sich als `root` an.
- 2 Um einen Fingerabdruck für einen bestimmten Benutzer zu registrieren, geben Sie Folgendes ein:

```
tf-tool --add-user login
```

`tf-tool` fordert den Benutzer auf, seinen Finger aufzudrücken, bis drei lesbare Fingerabdrücke gesammelt wurden.

- 3 Wenn die Authentifizierung über Fingerabdruck auch zum Starten von YaST oder der YaST-Module verwendet werden soll, müssen Sie auch einen Fingerabdruck für `root` registrieren.

Nachdem der Fingerabdruck des Benutzers erfolgreich registriert wurde, kann der Benutzer wählen, ob er sich für die unter **Abschnitt 27.1, „Unterstützte Anwendungen und Aktionen“** (S. 496) aufgelisteten Aktionen und Anwendungen über Fingerabdruck oder über Passwort authentifizieren will.

Prozedur 27.4 *Überprüfen oder Entfernen eines Fingerabdrucks*

- 1** Öffnen Sie eine Shell und melden Sie sich als `root` an.
- 2** Führen Sie zur Überprüfung eines vorhandenen Fingerabdrucks für einen bestimmten Benutzer das folgende Kommando aus:

```
tf-tool --verify-user login
```

- 3** Fordern Sie den Benutzer auf, seinen Finger aufzudrücken. `tf-tool` vergleicht den Fingerabdruck mit dem für diesen Benutzer gespeicherten Fingerabdruck und gibt eine Meldung aus, wenn die Fingerabdrücke identisch sind.
- 4** Um den Fingerabdruck eines Benutzers zu entfernen, löschen Sie die entsprechende Fingerabdruckdatei für diesen Benutzer mit dem folgenden Kommando:

```
shred /etc/pam_thinkfinger/login.bir
```

Mit `tf-tool --acquire` können Sie einen Probelauf mit `tf-tool` durchführen. Der Fingerabdruck wird als `/tmp/test.bir` gespeichert und kann mit `tf-tool --verify` überprüft werden.

27.4 Weiterführende Informationen

- Die Startseite für das Projekt finden Sie unter <http://thinkfinger.sourceforge.net/>
- Weitere technische Details finden Sie unter `/usr/share/doc/packages/libthinkfinger/README` in Ihrem installierten System.
- Dort stehen auch Man-Seiten für `pam_thinkfinger` und `tf-tool` zur Verfügung.

Teil VI. Sicherheit

Masquerading und Firewalls

Wann immer Linux in einer Netzwerkumgebung eingesetzt wird, können Sie die Kernel-Funktionen verwenden, mit denen Netzwerkpakete so bearbeitet werden können, dass zwischen internen und externen Netzwerkbereichen unterschieden wird. Das Linux-Netfilter-Framework ermöglicht die Einrichtung einer wirksamen Firewall, die die verschiedenen Netzwerke voneinander trennt. Mithilfe von iptables, einer generischen Tabellenstruktur für die Definition von Regelsätzen, können Sie präzise steuern, welche Pakete eine Netzwerkschnittstelle passieren dürfen. Ein derartiger Paketfilter kann schnell und einfach mithilfe von SuSEfirewall2 und dem entsprechenden YaST-Modul eingerichtet werden.

28.1 Paketfilterung mit iptables

Die Komponenten netfilter und iptables sind verantwortlich für das Filtern und Bearbeiten von Netzwerkpaketen sowie für NAT (Network Address Translation, Übersetzung der Netzwerkadressen). Die Filterkriterien und alle dazugehörigen Aktionen werden in Ketten gespeichert, die nacheinander mit den einzelnen eingehenden Netzwerkpaketen verglichen werden müssen. Die für den Vergleich zu verwendenden Ketten werden in Tabellen gespeichert. Mit dem Befehl `iptables` können Sie diese Tabellen und Regelsätze bearbeiten.

Der Linux-Kernel verwaltet drei Tabellen, wobei jede einzelne für eine bestimmte Kategorie von Funktionen des Paketfilters dient:

Filter

Diese Tabelle enthält die meisten Filterregeln, da sie die eigentliche *Paketfilterung* implementiert. Hier wird u. a. entschieden, welche Pakete durchgelassen (ACCEPT) oder abgelehnt (DROP) werden.

nat

In dieser Tabelle werden alle Änderungen an den Quell- und Zieladressen von Paketen definiert. Mithilfe dieser Funktionen können Sie das *Masquerading* implementieren, bei dem es sich um einen Spezialfall von NAT handelt und der eingesetzt wird, um private Netzwerke mit dem Internet zu verbinden.

mangle

Die Regeln in dieser Tabelle ermöglichen das Bearbeiten von Werten, die in IP-Headern gespeichert sind (z. B. den Typ des Diensts).

Diese Tabellen enthalten mehrere vordefinierte Ketten, mit denen die Pakete verglichen werden:

PREROUTING

Diese Kette wird auf eingehende Pakete angewendet.

EINGABE

Diese Kette wird auf Pakete angewendet, die an interne Prozesse des Systems adressiert sind.

WEITERLEITEN

Diese Kette wird auf Pakete angewendet, die durch das System nur weitergeleitet werden.

AUSGABE

Diese Kette wird auf Pakete angewendet, die aus dem System selbst stammen.

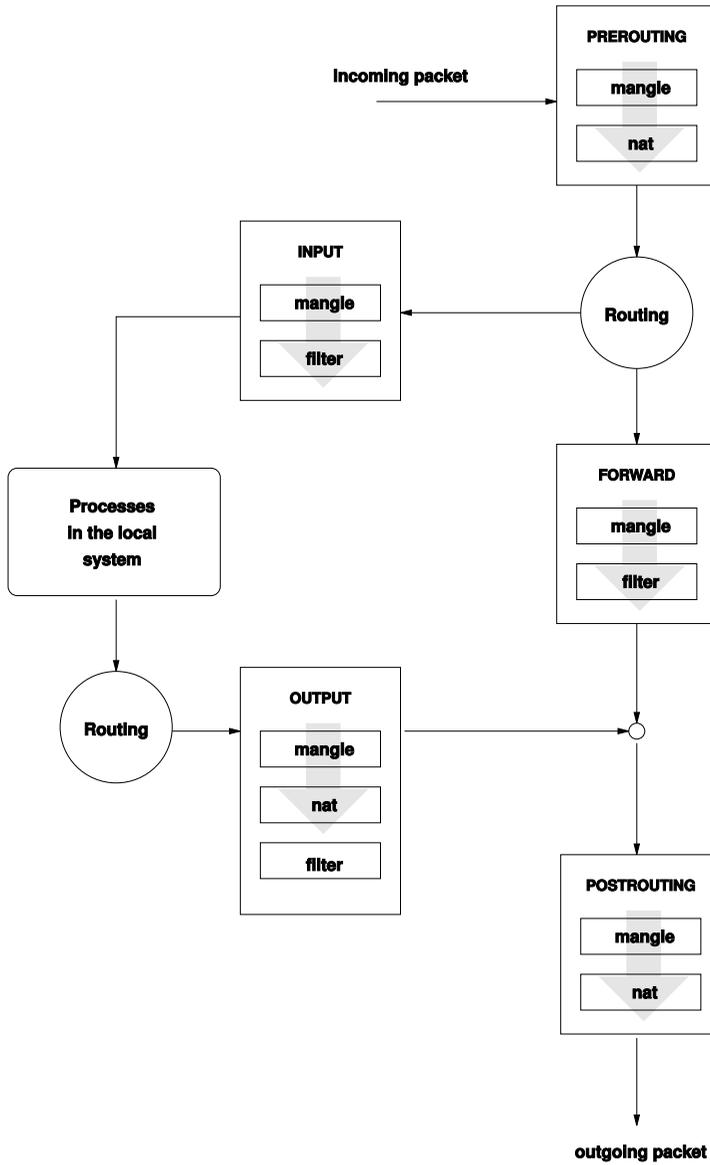
POSTROUTING

Diese Kette wird auf alle ausgehenden Pakete angewendet.

Abbildung 28.1, „iptables: Die möglichen Wege eines Pakets“ (S. 506) zeigt die Wege, die ein Netzwerkpaket auf einem System durchlaufen kann. Der Einfachheit halber werden in dieser Abbildung die Tabellen als Teile von Ketten dargestellt. In Wirklichkeit sind diese Ketten jedoch in den Tabellen selbst enthalten.

Im einfachsten aller möglichen Fälle geht ein eingehendes Paket, das an das System selbst adressiert ist, an der Schnittstelle `eth0` ein. Das Paket wird zunächst an die Kette `PREROUTING` der Tabelle `mangle` und anschließend an die Kette `PREROUTING` der Tabelle `nat` weitergegeben. Im folgenden Schritt des Paket-Routings wird ermittelt, dass das tatsächliche Ziel des Pakets ein Prozess des Systems selbst ist. Nach den `INPUT`-Ketten der Tabellen `mangle` und `filter` erreicht das Paket schließlich sein Ziel, vorausgesetzt, dass es tatsächlich den Regeln der Tabelle `filter` entspricht.

Abbildung 28.1 iptables: Die möglichen Wege eines Pakets



28.2 Grundlegendes zum Masquerading

Masquerading ist eine Linux-spezifische Form von NAT (Network Address Translation). Es kann verwendet werden, um ein kleines LAN (Hosts verwenden IP-Adressen aus dem privaten Bereich, siehe [Abschnitt 14.1.2, „Netzmasken und Routing“](#) (S. 229)) mit dem Internet (offizielle IP-Adressen) zu verbinden. Damit die LAN-Hosts eine Verbindung zum Internet herstellen können, müssen ihre privaten Adressen in eine offizielle Adresse übersetzt werden. Dies geschieht auf dem Router, der als Gateway zwischen dem LAN und dem Internet agiert. Das zugrunde liegende Prinzip ist einfach: Der Router verfügt über mehrere Netzwerkschnittstellen, in der Regel eine Netzwerkkarte und eine getrennte Schnittstelle zur Verbindung mit dem Internet. Letztere verbindet den Router mit der Außenwelt und eine oder mehrere andere Schnittstellen verbinden ihn mit den LAN-Hosts. Wenn diese Hosts im lokalen Netzwerk mit der Netzwerkkarte (z. B. `eth0`) des Routers verbunden sind, senden Sie alle Pakete, die nicht an das lokale Netzwerk adressiert sind, an ihr Standard-Gateway (den Router).

WICHTIG: Verwenden der richtigen Netzmaske

Stellen Sie beim Konfigurieren des Netzwerks sicher, dass sowohl die Broadcast-Adresse als auch die Netzmaske für alle lokalen Hosts identisch sind. Anderenfalls können die Pakete nicht ordnungsgemäß weitergeleitet werden.

Wenn einer der LAN-Hosts ein Paket an eine Internetadresse sendet, wird es zunächst zum Standardrouter weitergeleitet. Bevor der Router jedoch derartige Pakete weiterleiten kann, muss er entsprechend konfiguriert werden. In einer Standardinstallation ist dies aus Sicherheitsgründen nicht aktiviert. Um den Router entsprechend zu aktivieren, setzen Sie die Variable `IP_FORWARD` in der Datei `/etc/sysconfig/sysctl` auf `IP_FORWARD=yes`.

Der Zielhost der Verbindung kann Ihren Router sehen, erfährt aber nichts über den Host im internen Netzwerk, von dem die Pakete stammen. Aus diesem Grund wird diese Technik als Masquerading bezeichnet. Die Zieladresse für Antwortpakete ist wegen der Adressübersetzung wieder der Router. Der Router muss die eingehenden Pakete identifizieren und ihre Zieladressen übersetzen, sodass die Pakete an den richtigen Host im Netzwerk weitergeleitet werden können.

Da das Routing des eingehenden Verkehrs von der Masquerading-Tabelle abhängig ist, ist es nicht möglich, von außen eine Verbindung zu einem internen Host herzustellen. Für eine derartige Verbindung gibt es in der Tabelle keinen Eintrag. Zudem verfügt eine eingerichtete Verbindung in der Tabelle über einen zugeordneten Status, sodass dieser Tabelleneintrag nicht von einer zweiten Verbindung genutzt werden kann.

Als Folge können bei einigen Anwendungsprotokollen, z. B. ICQ, cucme, IRC (DCC, CTCP) und FTP (im PORT-Modus) Probleme auftreten. Webbrowser, das Standard-FTP-Programm und viele andere Programme verwenden den PASV-Modus. Dieser passive Modus ist in Bezug auf die Paketfilterung und das Masquerading weitaus problemloser.

28.3 Grundlegendes zu Firewalls

Firewall ist wohl der am weitesten verbreitete Begriff für einen Mechanismus, der zwei Netze miteinander verbindet und gleichzeitig für möglichst kontrollierten Datenverkehr sorgt. Genau genommen ist die in diesem Abschnitt beschriebene Firewall eigentlich ein *Paketfilter*. Ein Paketfilter regelt den Datenfluss anhand von bestimmten Kriterien wie Protokollen, Ports und IP-Adressen. Auf diese Weise können Sie Pakete blockieren, die aufgrund ihrer Adressierung Ihr Netz nicht erreichen sollen. Wenn Sie beispielsweise den öffentlichen Zugriff auf Ihren Webserver zulassen möchten, müssen Sie den entsprechenden Port explizit öffnen. Ein Paketfilter untersucht jedoch nicht den Inhalt dieser Pakete, sofern sie legitim adressiert sind, also beispielsweise mit Ihrem Webserver als Ziel. Das Paket könnte insofern einen Angriff auf ein CGI-Programm auf Ihrem Webserver enthalten und wird vom Paketfilter trotzdem durchgelassen.

Ein effektiverer, wenn auch komplexerer Mechanismus ist die Kombination mehrerer Systeme, z. B. ein Paketfilter, der mit einem Anwendungs-Gateway bzw. -Proxy interagiert. In diesem Fall lehnt der Paketfilter alle Pakete ab, die an deaktivierte Ports adressiert sind. Es werden nur die Pakete angenommen, die an das Anwendungs-Gateway adressiert sind. Dieses Gateway bzw. dieser Proxy gibt vor, der eigentliche Client des Servers zu sein. In diesem Sinn kann ein solcher Proxy auf der Protokollebene der jeweiligen Anwendung als Masquerading-Host angesehen werden. Ein Beispiel für einen derartigen Proxy ist Squid, ein HTTP-Proxyserver. Um Squid verwenden zu können, muss der Browser für die Kommunikation über den Proxy konfiguriert sein. Alle angeforderten HTTP-Seiten werden aus dem Proxy-Cache bedient und Seiten, die im Cache nicht gefunden werden, werden vom Proxy aus dem Internet geholt. Ein

weiteres Beispiel ist die SUSE-Proxy-Suite (`proxy-suite`), die einen Proxy für das FTP-Protokoll zur Verfügung stellt.

Im folgenden Abschnitt wird der zum Lieferumfang von openSUSE gehörende Paketfilter beschrieben. Weitere Informationen zu Paketfiltern und Firewalls finden Sie in der Datei "Firewall HOWTO", die im Paket `howto` enthalten ist. Wenn dieses Paket installiert ist, lesen Sie die HOWTO-Informationen mit dem Kommando

```
less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz
```

28.4 SuSEfirewall2

SuSEfirewall2 ist ein Skript, das die in `/etc/sysconfig/SuSEfirewall2` gesetzten Variablen ausliest, um mehrere iptables-Regeln zu generieren. Es definiert drei Sicherheitszonen, obwohl nur die erste und die zweite Zone in der folgenden Beispielkonfiguration berücksichtigt werden:

Externe Zone

Davon ausgehend, dass es keine Möglichkeit gibt, Vorgänge im externen Netzwerk zu steuern, muss der Host vor diesem geschützt werden. In den meisten Fällen handelt es sich bei dem externen Netzwerk um das Internet, es könnte aber auch ein anderes unsicheres Netzwerk sein, z. B. ein WLAN.

Interne Zone

Diese Zone bezieht sich auf das private Netzwerk, wobei es sich in den meisten Fällen um ein LAN handelt. Wenn die Hosts in diesem Netzwerk IP-Adressen aus dem privaten Bereich (siehe [Abschnitt 14.1.2, „Netzmasken und Routing“](#) (S. 229)) verwenden, müssen Sie NAT (Network Address Translation) aktivieren, damit Hosts im internen Netzwerk auf externe Hosts zugreifen können.

Demilitarisierte Zone (DMZ)

Während Hosts, die sich in dieser Zone befinden, sowohl vom externen als auch vom internen Netzwerk aus erreicht werden können, können sie selbst nicht auf das interne Netzwerk zugreifen. Diese Konfiguration kann als zusätzliche Verteidigungslinie vor das interne Netzwerk gesetzt werden, da die DMZ-Systeme vom internen Netzwerk isoliert sind.

Jegliche Art von Netzwerkverkehr, der gemäß der Filterregel nicht explizit erlaubt ist, wird durch iptables unterdrückt. Daher muss jede Schnittstelle mit eingehendem Verkehr einer der drei Zonen zugeordnet werden. Legen Sie für alle Zonen die zulässigen

Dienste und Protokolle fest. Diese Regelsätze gelten jedoch nur für Pakete, die von entfernten Hosts stammen. Lokal generierte Pakete werden von der Firewall nicht erfasst.

Die Konfiguration kann mit YaST ausgeführt werden (siehe [Abschnitt 28.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 510)). Sie lässt sich jedoch auch manuell in der Datei `/etc/sysconfig/SuSEfirewall2` vornehmen, die sehr gut kommentiert ist. Zudem stehen weitere Beispielszenarien in `/usr/share/doc/packages/SuSEfirewall2/EXAMPLES` zur Verfügung.

28.4.1 Konfigurieren der Firewall mit YaST

WICHTIG: Automatische Firewall-Konfiguration

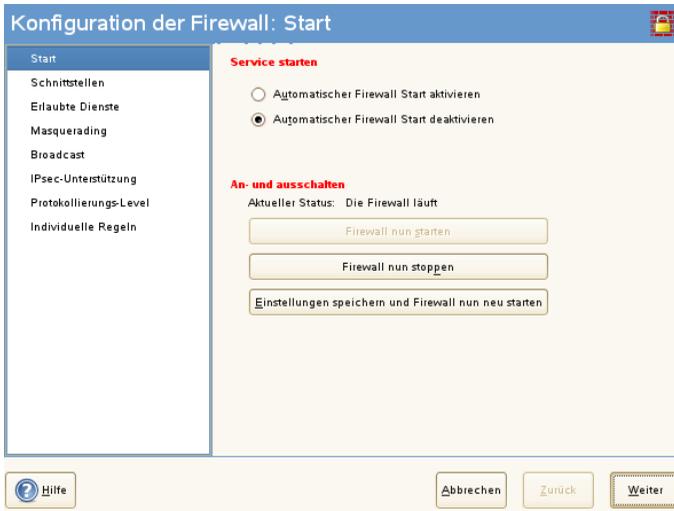
Im Anschluss an die Installation startet YaST automatisch eine Firewall für alle konfigurierten Schnittstellen. Wenn ein Server auf dem System konfiguriert und aktiviert ist, kann YaST die automatisch generierte Firewall-Konfiguration mit den Optionen *Firewall-Ports auf ausgewählten Schnittstellen öffnen* oder *Firewall-Port öffnen* in den Serverkonfigurationsmodulen ändern. Einige Servermodul-Dialogfelder enthalten die Schaltfläche *Firewall-Details* zum Aktivieren zusätzlicher Dienste und Ports. Die Firewall kann mit dem YaST-Firewall-Konfigurationsmodul aktiviert, deaktiviert oder neu konfiguriert werden.

Der Zugriff auf die YaST-Dialogfelder für die grafische Konfiguration erfolgt über das YaST-Kontrollzentrum. Wählen Sie *Sicherheit und Benutzer > Firewall*. Die Konfiguration ist in sieben Abschnitte aufgeteilt, auf die Sie über die Baumstruktur auf der linken Seite direkt zugreifen können.

Start

In diesem Dialogfeld legen Sie das Startverhalten fest. In einer Standardinstallation wird SuSEfirewall2 automatisch gestartet. Außerdem können Sie in diesem Dialogfeld die Firewall starten und stoppen. Um die neuen Einstellungen für eine aktive Firewall zu übernehmen, wählen Sie *Einstellungen speichern und Firewall nun neu starten*.

Abbildung 28.2 Die YaST-Firewall-Konfiguration



Schnittstellen

Hier werden alle bekannten Netzwerkschnittstellen aufgelistet. Um eine Schnittstelle aus einer Zone zu entfernen, markieren Sie sie, klicken Sie auf *Bearbeiten* und wählen Sie *Keine Zone zugewiesen*. Um eine Schnittstelle zu einer Zone hinzuzufügen, markieren Sie sie, klicken Sie auf *Bearbeiten* und wählen Sie anschließend eine der verfügbaren Zonen. Mit der Option *Benutzerdefiniert* können Sie auch eine spezielle Schnittstelle mit eigenen Einstellungen erstellen.

Erlaubte Dienste

Diese Option benötigen Sie, um einer Zone Dienste Ihres Systems zur Verfügung zu stellen, vor der es geschützt ist. Das System ist standardmäßig nur vor externen Zonen geschützt. Sie müssen alle Dienste explizit zulassen, die den externen Hosts zur Verfügung stehen sollen. Aktivieren Sie nach der Auswahl der gewünschten Zone die Dienste unter *Erlaubte Dienste für gewählte Zone*.

Masquerading

Mit der Masquerading-Funktionalität verbergen Sie das interne Netzwerk vor externen Netzwerken, z. B. dem Internet, und ermöglichen den Hosts im internen Netzwerk gleichzeitig den transparenten Zugriff auf das externe Netzwerk. Anforderungen vom externen an das interne Netzwerk werden blockiert. Anforderungen aus dem internen Netzwerk werden scheinbar vom Masquerading-Server ausgegeben, der extern sichtbar ist. Wenn dem externen Netzwerk spezielle Dienste eines

internen Computers zur Verfügung gestellt werden sollen, fügen Sie für den Dienst eine spezielle Umadressierungsregel hinzu.

Broadcast

In diesem Dialogfeld konfigurieren Sie die UDP-Ports, die Broadcasts zulassen sollen. Fügen Sie die erforderlichen Nummern der Ports oder Dienste getrennt durch Leerzeichen für die entsprechende Zone hinzu. Weitere Informationen hierzu finden Sie in der Datei `/etc/services`.

Hier können Sie auch das Protokollieren von Broadcasts aktivieren, die nicht akzeptiert werden. Dies kann problematisch sein, da sich Windows-Hosts über Broadcasts miteinander bekannt machen und daher viele Pakete generieren, die nicht akzeptiert werden.

IPsec-Unterstützung

In diesem Dialogfeld konfigurieren Sie, ob dem externen Netzwerk der IPsec-Dienst zur Verfügung stehen soll. Unter *Details* konfigurieren Sie, welche Pakete als vertrauenswürdig angesehen werden sollen.

Protokollierumfang

Es gibt zwei Regeln für die Protokollierung: akzeptierte und nicht akzeptierte Pakete. Nicht akzeptierte Pakete werden verworfen (DROPPED) oder abgelehnt (REJECTED). Wählen Sie die Option *Alles protokollieren*, *Nur kritische protokollieren* oder *Keine protokollieren* für beide Regeln.

Benutzerdefinierte Regeln

Legen Sie hier spezielle Firewall-Regeln fest, die nach bestimmten Kriterien Verbindungen zulassen.

Wenn Sie die Firewall-Konfiguration abgeschlossen haben, wählen Sie *Weiter*, um dieses Dialogfeld zu schließen. Anschließend wird eine zonenbezogene Zusammenfassung der Firewall-Konfiguration geöffnet. Aktivieren Sie darin alle Einstellungen. In dieser Zusammenfassung sind alle zulässigen Dienste, Ports und Protokolle aufgelistet. Mit der Option *Zurück* können Sie die Konfiguration ändern. Wählen Sie *Übernehmen*, um die Konfiguration zu speichern.

28.4.2 Manuelle Konfiguration

In den folgenden Abschnitten sind detaillierte Anweisungen für eine erfolgreiche Konfiguration enthalten. Für jeden Konfigurationsschritt wird angegeben, ob er sich auf die Firewall- oder Masquerading-Konfiguration bezieht. Verwenden Sie den Portbereich 500 : 510, sofern passend. Die in der Konfigurationsdatei erwähnten Aspekte, die mit der DMZ (Demilitarisierte Zone) in Zusammenhang stehen, werden hier nicht näher erläutert. Sie sind nur für komplexere Netzwerkinfrastrukturen größerer Unternehmen (Corporate Networks) relevant, die eine aufwändige Konfiguration und umfassende Kenntnisse erfordern.

Aktivieren Sie zunächst mit dem YaST-Runlevel-Editor SuSEfirewall2 für Ihr Runlevel (wahrscheinlich 3 oder 5). Dadurch werden symbolische Links für die SuSEfirewall2_*-Skripten in den Verzeichnissen unter `/etc/init.d/rc?.d/` angelegt.

FW_DEV_EXT (Firewall, Masquerading)

Das mit dem Internet verbundene Gerät. Geben Sie für eine Modemverbindung `ppp0` ein. Verwenden Sie für eine ISDN-Verbindung `ipp0`. DSL-Verbindungen verwenden `dsl0`. Um die der Standardroute entsprechende Schnittstelle zu verwenden, geben Sie `auto` an.

FW_DEV_INT (Firewall, Masquerading)

Das mit dem internen, privaten Netzwerk verbundene Gerät (z. B. `eth0`). Wenn es kein internes Netzwerk gibt und die Firewall nur den Host schützt, auf dem sie ausgeführt wird, machen Sie keine Angaben.

FW_ROUTE (Firewall, Masquerading)

Wenn Sie die Masquerading-Funktion benötigen, setzen Sie diese Variable auf `yes`. Die internen Hosts sind von außen nicht sichtbar, da ihre private Netzwerkadressen (z. B. `192.168.x.x`) von Internetroutern ignoriert werden.

Setzen Sie diese Variable für Firewalls ohne Masquerading auf `yes`, wenn der Zugriff auf das interne Netzwerk zugelassen werden soll. In diesem Fall müssen die internen Computer offiziell registrierte IP-Adressen verwenden. Sie sollten den externen Zugriff auf das interne Netzwerk in der Regel jedoch *nicht* zulassen.

FW_MASQUERADE (Masquerading)

Setzen Sie diese Variable auf `yes`, wenn Sie die Masquerading-Funktion benötigen. Dadurch wird den internen Hosts eine virtuelle direkte Verbindung zum Internet zur Verfügung gestellt. Es ist jedoch weitaus sicherer, wenn zwischen den Hosts

des internen Netzwerks und dem Internet ein Proxyserver geschaltet ist. Für die von einem Proxyserver zur Verfügung gestellten Dienste ist das Masquerading nicht erforderlich.

FW_MASQ_NETS (Masquerading)

Geben Sie die Hosts oder Netzwerke, für die die Masquerading-Funktion aktiviert werden soll, durch Leerzeichen getrennt an. Beispiel:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (Firewall)

Setzen Sie diese Variable auf *yes*, um den Firewall-Host vor Angriffen aus dem internen Netzwerk zu schützen. Dem internen Netzwerk stehen nur die explizit aktivierten Dienste zur Verfügung. Weitere Informationen hierzu finden Sie auch unter `FW_SERVICES_INT_TCP` und `FW_SERVICES_INT_UDP`.

FW_SERVICES_EXT_TCP (Firewall)

Geben Sie die zu öffnenden TCP-Ports an. Für eine normale Arbeitsstation, die in der Regel keine Dienste benötigt, müssen Sie hier keine Angaben machen.

FW_SERVICES_EXT_UDP (Firewall)

Lassen Sie dieses Feld leer, es sei denn, Sie möchten einen aktiven UDP-Dienst verfügbar machen. UDP wird von Diensten wie DNS-Servern, IPSec, TFTP, DHCP und anderen verwendet. Geben Sie in diesem Fall die zu verwendenden UDP-Ports an.

FW_SERVICES_INT_TCP (Firewall)

Mit dieser Variablen legen Sie die für das interne Netzwerk verfügbaren Dienste fest. Die Notation ist dieselbe wie für `FW_SERVICES_EXT_TCP`, aber die Einstellungen werden auf das *interne* Netzwerk angewendet. Diese Variable muss nur gesetzt werden, wenn `FW_PROTECT_FROM_INT` auf *yes* gesetzt ist.

FW_SERVICES_INT_UDP (Firewall)

Siehe `FW_SERVICES_INT_TCP`.

FW_SERVICES_ACCEPT_RELATED_* (Firewall)

SuSEfirewall2 führt nun eine kleine Änderung ein hinsichtlich der Pakete, die vom Netzfilter als `RELATED` betrachtet werden.

Um beispielsweise eine feinere Filterung der Samba Broadcast-Pakete zu erlauben, werden `RELATED`-Pakete nicht mehr bedingungslos akzeptiert. Die neuen Variablen,

die mit `FW_SERVICES_ACCEPT_RELATED_` beginnen, wurden eingeführt, um die Verarbeitung von `RELATED`-Paketen auf bestimmte Netzwerke, Protokolle und Ports zu beschränken.

Das bedeutet, dass ein Hinzufügen von Modulen zur Verbindungsverfolgung (conntrack-Modulen) zu `FW_LOAD_MODULES` nicht mehr automatisch dazu führt, dass die Pakete, die durch diese Module markiert werden, übernommen werden. Zusätzlich müssen Sie Variablen, die mit `FW_SERVICES_ACCEPT_RELATED_` beginnen, auf einen passenden Wert festlegen.

Testen Sie ihre Einrichtung, nachdem Sie die Firewall konfiguriert haben. Die Firewall-Regelsätze werden erstellt, indem Sie `SuSEfirewall2 start` als `root` eingeben. Testen Sie auf einem externen Host anschließend beispielsweise mit `telnet`, ob die Verbindung tatsächlich abgelehnt wird. Prüfen Sie anschließend `/var/log/messages`, wo Sie ähnliche Einträge wie die folgenden sehen sollten:

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFLT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEBEC0000000001030300)
```

Weitere Pakete zum Testen der Firewall-Konfiguration sind "nmap" oder "nessus". Die Dokumentation von `nmap` befindet sich im Verzeichnis `/usr/share/doc/packages/nmap` und die Dokumentation von `nessus` ist nach der Installation des entsprechenden Pakets im Verzeichnis `/usr/share/doc/packages/nessus-core` enthalten.

28.5 Weiterführende Informationen

Die aktuellsten Informationen sowie weitere Dokumentationen zum Paket `SuSEfirewall2` finden Sie im Verzeichnis `/usr/share/doc/packages/SuSEfirewall2`. Die Homepage der Projekte "netfilter" und "iptables" unter der Adresse <http://www.netfilter.org> bietet eine umfassende Sammlung von Dokumenten in zahlreichen Sprachen.

SSH: Secure Network Operations

29

Mit der steigenden Anzahl installierter Computer in Netzwerkumgebungen wird es häufig nötig, auf Hosts von einem entfernten Standort aus zuzugreifen. Das bedeutet gewöhnlich, dass ein Benutzer zur Authentifizierung Zeichenfolgen für Anmeldung und Passwort sendet. Solange diese Zeichenfolgen als Klartext übertragen werden, können sie abgefangen und missbraucht werden, um Zugriff auf dieses Benutzerkonto zu erhalten, sogar ohne dass der autorisierte Benutzer etwas davon bemerkt. Damit wären nicht nur alle Dateien des Benutzers für einen Angreifer zugänglich, das illegale Konto könnte auch benutzt werden, um Administrator- oder `root`-Zugriff zu erhalten oder in andere Systeme einzudringen. In der Vergangenheit wurden Fernverbindungen mit `telnet` aufgebaut, das gegen Ausspionierung keine Vorkehrungen in Form von Verschlüsselung oder anderen Sicherheitsmechanismen trifft. Es gibt andere ungeschützte Kommunikationskanäle, z. B. das traditionelle FTP-Protokoll und einige Kopierverbindungen zwischen Computern.

Die SSH-Software liefert den gewünschten Schutz. Die komplette Authentifizierung (gewöhnlich Benutzername und Passwort) und Kommunikation sowie sämtlicher Datenaustausch zwischen den Hosts erfolgen hier verschlüsselt. Zwar ist auch mit SSH weiterhin das Abfangen der übertragenen Daten möglich, doch ist der Inhalt verschlüsselt und kann nur entziffert werden, wenn der Schlüssel bekannt ist. So wird durch SSH sichere Kommunikation über unsichere Netze wie das Internet möglich. openSUSE bietet SSH-Funktionen mit dem Paket OpenSSH an.

29.1 Das Paket OpenSSH

openSUSE installiert das Paket OpenSSH standardmäßig. Daher stehen Ihnen die Programme `ssh`, `scp` und `sftp` als Alternative für `telnet`, `rlogin`, `rsh`, `rcp` und `ftp` zur Verfügung. In der Standardkonfiguration ist der Zugriff auf ein openSUSE-System nur mit den OpenSSH-Dienstprogrammen möglich und nur, wenn dies die Firewall erlaubt.

29.2 Das ssh-Programm

Mit `ssh` können Sie Verbindung zu einem entfernten System aufnehmen und dort interaktiv arbeiten. Es ersetzt somit gleichermaßen `telnet` und `rlogin`. Das Programm `slogin` ist lediglich ein symbolischer Link, der auf `ssh` weist. Sie können sich z. B. mit dem Befehl `ssh sun` auf dem Host `sun` anmelden. Der Host fordert Sie dann zur Eingabe des Passworts am System `sun` auf.

Nach erfolgreicher Authentifizierung können Sie dort in der Kommandozeile oder interaktiv arbeiten, z. B. mit YaST. Wenn sich der lokale Benutzername vom Namen auf dem entfernten System unterscheidet, können Sie einen anderen Namen angeben, z. B. `ssh-l augustine sun` oder `ssh augustine@sun`.

Darüber hinaus bietet `ssh` die von `rsh` bekannte Möglichkeit, Befehle auf einem entfernten System auszuführen. Im folgenden Beispiel wird der Befehl `uptime` auf dem Host `sun` ausgeführt und ein Verzeichnis mit dem Namen `tmp` wird angelegt. Die Programmausgabe erfolgt auf dem lokalen Terminal des Hosts `earth`.

```
ssh otherplanet "uptime; mkdir tmp"
Password:
1:21pm up 2:17, 9 users, load average: 0.15, 0.04, 0.02
```

Anführungszeichen sind hier zum Zusammenfassen der beiden Anweisungen in einem Befehl erforderlich. Nur so wird auch der zweite Befehl auf dem Host `sun` ausgeführt.

29.3 scp – Sichere Kopie

`scp` kopiert Dateien auf einen entfernten Computer. Es ist ein sicherer und verschlüsselter Ersatz für `rcp`. Beispielsweise kopiert `scp MyLetter.tex sun:` die Datei `MyLetter.tex` vom Host `earth` auf den Host `sun`. Wenn sich die Benutzernamen auf

earth und sun unterscheiden, geben Sie letzteren im Format `benutzername@host` an. Die Option `-l` hat bei diesem Kommando eine andere Bedeutung.

Nachdem das Passwort eingegeben wurde, beginnt `scp` mit der Datenübertragung und zeigt dabei den Fortschritt durch einen von links nach rechts anwachsenden Balken aus Sternen an. Zudem wird am rechten Rand die geschätzte Restübertragungszeit (bis zum Erreichen des rechten Balkenendes) angezeigt. Jegliche Ausgabe kann durch die Option `-q` unterdrückt werden.

`scp` bietet auch ein rekursives Kopierverfahren für ganze Verzeichnisse. Der Befehl `scp -r src/ sun:backup/` kopiert den kompletten Inhalt des Verzeichnisses `src` einschließlich aller Unterverzeichnisse in das Unterverzeichnis `backup` auf den Host `sun`. Das Unterverzeichnis wird automatisch angelegt, wenn es noch nicht existiert.

Die Option `-p` weist `scp` an, den Zeitstempel von Dateien unverändert zu belassen. `-C` sorgt für komprimierte Datenübertragung. Dadurch wird das zu übertragende Datenvolumen minimiert, aber der Prozessor stärker belastet.

29.4 sftp – Sichere Dateiübertragung

Das Programm `sftp` kann anstelle von `scp` zur sicheren Dateiübertragung verwendet werden. Bei einer `sftp`-Sitzung können Sie viele bereits von `ftp` bekannte Befehle verwenden. Das Programm `sftp` ist gegenüber `scp` vor allem beim Übertragen von Daten, deren Dateinamen unbekannt sind, von Vorteil.

29.5 Der SSH-Daemon (sshd) –Serverseite

Damit die SSH-Clientprogramme `ssh` und `scp` eingesetzt werden können, muss im Hintergrund der SSH-Daemon laufen und an `TCP/IP-Port 22` auf Verbindungen warten. Während des ersten Starts generiert der Daemon drei Schlüsselpaare. Die Schlüsselpaare bestehen jeweils aus einem privaten und einem öffentlichen (engl. public) Teil. Deshalb wird dies als ein Public-Key-basiertes Verfahren bezeichnet. Um die Sicherheit der Kommunikation über SSH zu gewährleisten, darf ausschließlich der Systemadministrator die Dateien der privaten Schlüssel einsehen. Die Dateirechte werden durch die Standardinstallation entsprechend eingestellt. Die privaten Schlüssel

werden lediglich lokal vom SSH-Daemon benötigt und dürfen an niemanden weitergegeben werden. Demgegenüber werden die öffentlichen Schlüsselbestandteile (an der Namensendung `.pub` erkennbar) an den Client weitergegeben, der die Verbindung anfordert. Sie sind für alle Benutzer lesbar.

Eine Verbindung wird vom SSH-Client eingeleitet. Der wartende SSH-Daemon und der anfragende SSH-Client tauschen Identifikationsdaten aus, um die Protokoll- und Softwareversion abzugleichen und eine Verbindung durch den falschen Port auszuschließen. Da ein untergeordneter Prozess des ursprünglichen SSH-Daemons antwortet, sind gleichzeitig viele SSH-Verbindungen möglich.

OpenSSH unterstützt zur Kommunikation zwischen SSH-Server und SSH-Client das SSH-Protokoll in den Versionen 1 und 2. Version 2 des SSH-Protokolls wird standardmäßig verwendet. Jedoch kann mit dem Schalter `-1` auch Version 1 des SSH-Protokolls erzwungen werden. Möchten Sie nach einem System-Update weiterhin Version 1 beibehalten, folgen Sie den Anweisungen in `/usr/share/doc/packages/openssh/README.SuSE`. Dort ist ebenfalls beschrieben, wie Sie in wenigen Schritten eine SSH 1-Umgebung in eine funktionierende SSH 2-Umgebung umwandeln.

Bei Verwendung der SSH Protokoll-Version 1 sendet der Server dann seinen öffentlichen Host-Schlüssel und einen stündlich vom SSH-Daemon neu generierten Server-Schlüssel. Anhand dieser beiden verschlüsselt der SSH-Client einen von ihm frei gewählten Sitzungsschlüssel und sendet diesen an den SSH-Server. Der SSH-Client teilt dem Server zudem die gewählte Verschlüsselungsmethode (engl. `cipher`) mit.

Version 2 des SSH-Protokolls kommt ohne den Server-Schlüssel aus. Beide Seiten verwenden einen Algorithmus nach Diffie-Hellman, um ihre Schlüssel auszutauschen.

Die zur Entschlüsselung des Sitzungsschlüssels zwingend erforderlichen privaten Host- und Server-Schlüssel können nicht aus den öffentlichen Teilen abgeleitet werden. Nur der kontaktierte SSH-Daemon kann den Sitzungsschlüssel mit seinen privaten Schlüsseln entziffern (siehe `man/usr/share/doc/packages/openssh/RFC.nroff`). Diese einleitende Phase der Verbindung lässt sich mithilfe der Fehlersuchoption `-v` des SSH-Clients genau beobachten.

Der Client legt nach der ersten Kontaktaufnahme mit einem entfernten Host alle öffentlichen Host-Schlüssel in `~/.ssh/known_hosts` ab. Auf diese Weise können so genannte "Man-in-the-Middle"-Angriffe, Versuche fremder SSH-Server, Name und IP-Adresse eines anderen Servers vorzutäuschen, verhindert werden. Derartige Angriffe fallen entweder durch einen Host-Schlüssel auf, der nicht in `~/.ssh/known`

`_hosts` enthalten ist, oder durch die Unfähigkeit des Servers, den Sitzungsschlüssel mangels des passenden privaten Gegenstücks zu entschlüsseln.

Es empfiehlt sich, die in `/etc/ssh/` abgelegten privaten und öffentlichen Schlüssel extern und gut geschützt zu archivieren. So können Änderungen der Schlüssel erkannt und nach einer Neuinstallation die alten wieder eingespielt werden. Dies erspart den Benutzern beunruhigende Warnungen. Wenn sichergestellt ist, dass es sich trotz der Warnung um den korrekten SSH-Server handelt, muss der vorhandene Eintrag zu diesem System aus `~/.ssh/known_hosts` entfernt werden.

29.6 SSH-Authentifizierungsmechanismen

Nun erfolgt die eigentliche Authentifizierung, die in ihrer einfachsten Form aus der Eingabe eines Passworts besteht, wie bereits oben erwähnt. Ziel von SSH war die Einführung einer sicheren, aber zugleich bedienerfreundlichen Software. Wie bei den abzulösenden Programmen `rsh` und `rlogin` muss deshalb auch SSH eine im Alltag einfach zu nutzende Authentifizierungsmethode bieten. SSH realisiert dies mithilfe eines weiteren Schlüsselpaares, das vom Benutzer erzeugt wird. Dazu liefert das SSH-Paket ein Hilfsprogramm: `ssh-keygen`. Nachdem Sie `ssh-keygen -t rsa` oder `ssh-keygen -t dsa` eingegeben haben, wird das Schlüsselpaar generiert und der Basisdateiname zur Ablage der Schlüssel erfragt.

Bestätigen Sie die Voreinstellung und beantworten Sie die Frage nach einem Passwortsatz. Auch wenn die Software einen leeren Passwortsatz vorschlägt, sollte bei der hier beschriebenen Vorgehensweise ein Text von 10 bis 30 Zeichen Länge gewählt werden. Verwenden Sie keine kurzen und einfachen Wörter oder Phrasen. Bestätigen Sie die Eingabe, indem Sie den Passwortsatz wiederholen. Anschließend wird der Speicherort des privaten und öffentlichen Schlüssels, in unserem Beispiel der Dateien `id_rsa` und `id_rsa.pub`, ausgegeben.

Verwenden Sie `ssh-keygen -p -t rsa` oder `ssh-keygen -p -t dsa`, um Ihren alten Passwortsatz zu ändern. Kopieren Sie den öffentlichen Teil des Schlüssels (in unserem Beispiel `id_rsa.pub`) auf den entfernten Computer und speichern Sie ihn dort unter `~/.ssh/authorized_keys`. Zur Authentifizierung werden Sie beim nächsten Verbindungsaufbau nach Ihrem Passwortsatz gefragt. Sollte dies nicht der Fall sein, überprüfen Sie bitte Ort und Inhalt dieser Dateien.

Auf Dauer ist diese Vorgehensweise mühsamer als die Eingabe eines Passworts. Entsprechend liefert das SSH-Paket ein weiteres Werkzeug, `ssh-agent`, das für die Dauer einer X-Sitzung private Schlüssel bereithält. Dazu wird die gesamte X-Sitzung als untergeordneter Prozess von `ssh-agent` gestartet. Sie erreichen dies am einfachsten, indem Sie am Anfang der Datei `.xsession` die Variable `usessh` auf `yes` setzen und sich über einen Display-Manager, z. B. KDM oder XDM, anmelden. Alternativ können Sie `ssh-agent startx` verwenden.

Nun können Sie `ssh` oder `scp` wie gewohnt verwenden. Sofern Sie Ihren öffentlichen Schlüssel wie oben beschrieben verteilt haben, werden Sie jetzt nicht mehr nach Ihrem Passwort gefragt. Beenden Sie beim Verlassen Ihres Computers Ihre X-session unbedingt oder sperren Sie ihn durch eine entsprechende Anwendung, z. B. `xlock`.

Alle wichtigen Änderungen, die sich mit der Einführung von Version 2 des SSH-Protokolls ergeben haben, sind auch in der Datei `/usr/share/doc/packages/openssh/README.SuSE` dokumentiert.

29.7 X-, Authentifizierungs- und Weiterleitungsmechanismen

Über die zuvor beschriebenen sicherheitsbezogenen Verbesserungen hinaus erleichtert SSH auch die Verwendung von entfernten X-Anwendungen. Insoweit Sie `ssh` mit der Option `-X` aufrufen, wird auf dem entfernten Computer automatisch die Variable `DISPLAY` gesetzt und alle X-Ausgaben werden durch die bestehende SSH-Verbindung an den entfernten Computer exportiert. Gleichzeitig unterbindet dies die bisher bestehenden Abhörmöglichkeiten bei entfernt aufgerufenen und lokal betrachteten X-Anwendungen.

Durch Hinzufügen der Option `-A` wird der Authentifizierungsmechanismus von `ssh-agent` auf den nächsten Computer mit übernommen. So können Sie an unterschiedlichen Computern arbeiten, ohne ein Passwort eingeben zu müssen. Allerdings ist das nur möglich, wenn Sie zuvor Ihren öffentlichen Schlüssel auf die beteiligten Zielhosts verteilt und dort korrekt gespeichert haben.

Beide Mechanismen sind in der Voreinstellung deaktiviert, können jedoch in der systemweiten Konfigurationsdatei `/etc/ssh/sshd_config` oder der benutzereigenen Datei `~/.ssh/config` permanent aktiviert werden.

ssh kann auch zur Umleitung von TCP/IP-Verbindungen benutzt werden. In den folgenden Beispielen wird SSH angewiesen, den SMTP- bzw. POP3-Port umzuleiten:

```
ssh -L 25:sun:25 earth
```

Mit diesem Befehl wird jede Verbindung zu Port 25 (SMTP) von earth auf den SMTP-Port von sun über den verschlüsselten Kanal weitergeleitet. Dies ist insbesondere für Benutzer von SMTP-Servern ohne SMTP-AUTH oder POP-before-SMTP-Funktionen von Nutzen. E-Mail kann so von jedem beliebigen Ort mit Netzanschluss zur Auslieferung durch den „home“-Mailserver übertragen werden. Entsprechend können mit dem folgenden Befehl alle POP3-Anfragen (Port 110) an earth auf den POP3-Port von sun weitergeleitet werden:

```
ssh -L 110:sun:110 earth
```

Beide Befehle müssen Sie als Benutzer `root` ausführen, da die Verbindung zu privilegierten, lokalen Ports erfolgt. Bei bestehender SSH-Verbindung wird E-Mail wie gewohnt als normaler Benutzer verschickt und abgerufen. Der SMTP- und POP3-Host muss für diese Aufgabe auf `localhost` konfiguriert werden. Zusätzliche Informationen entnehmen Sie den man-Seiten für die einzelnen Programme und den Dateien unter `/usr/share/doc/packages/openssh`.

Verwalten der X.509-Zertifizierung

30

Eine zunehmende Anzahl an Authentifizierungsmechanismen basieren auf kryptografischen Verfahren. In diesem Zusammenhang spielen digitale Zertifikate, mit denen kryptografische Schlüssel ihren jeweiligen Eigentümern zugewiesen werden, eine wichtige Rolle. Diese Zertifikate werden für die Kommunikation, beispielsweise auf ID-Karten in Unternehmen, verwendet. Die Generierung und Verwaltung von Zertifikaten wird meistens von offiziellen Einrichtungen geregelt, die dies als Dienstleistung anbieten. In einigen Fällen kann es jedoch sinnvoll sein, diese Aufgaben selbst auszuführen, beispielsweise wenn ein Unternehmen keine persönlichen Daten an Dritte weitergeben möchte.

In YaST stehen zwei Module für die Zertifizierung zur Verfügung, die grundlegende Verwaltungsfunktionen für digitale X.509-Zertifikate zur Verfügung stellen. In den nachfolgenden Abschnitten werden die Grundlagen der digitalen Zertifizierung und die Erstellung und Verwaltung von Zertifikaten dieses Typs mit YaST erläutert. Weitere Informationen finden Sie unter <http://www.ietf.org/html.charters/pkix-charter.html>.

30.1 Prinzipien der digitalen Zertifizierung

Bei der digitalen Zertifizierung werden kryptografische Prozesse für die Verschlüsselung von Daten verwendet, um die Daten vor Zugriffen durch unbefugte Personen zu schützen. Die Benutzerdaten werden mithilfe eines zweiten Datensatzes oder *Schlüssels* verschlüsselt. Der Schlüssel wird in einem mathematischen Prozess auf die Benutzer-

daten angewendet, sodass ein geänderter Datensatz entsteht, dessen ursprünglicher Inhalt nicht mehr ermittelt werden kann. Mittlerweile wird die asymmetrische Verschlüsselung am häufigsten verwendet (*öffentliche Schlüsselmethode*). Schlüssel kommen immer paarweise vor:

Private Key

Der private Schlüssel muss vom Schlüsseleigentümer sicher aufbewahrt werden. Durch eine versehentliche Veröffentlichung des privaten Schlüssels wird das Schlüsselpaar nutzlos.

Öffentlicher Schlüssel

Der Schlüsseleigentümer bringt den öffentlichen Schlüssel in Umlauf, damit er von Dritten verwendet werden kann.

30.1.1 Schlüsselauthentizität

Da der öffentliche Schlüsselprozess eine gängige Methode ist, befinden sich zahlreiche öffentliche Schlüssel im Umlauf. Für eine erfolgreiche Nutzung dieses Systems muss jeder Benutzer sicher sein, dass sich ein öffentlicher Schlüssel tatsächlich im Besitz des angenommenen Eigentümers befindet. Die Zuweisung von Benutzern zu öffentlichen Schlüsseln wird durch vertrauenswürdige Organisationen durch Zertifikate mit öffentlichen Schlüsseln bestätigt. Diese Zertifikate enthalten den Namen des Schlüsseleigentümers, den entsprechenden öffentlichen Schlüssel und die elektronische Signatur der Person, die das Zertifikat ausstellt.

Vertrauenswürdige Organisationen, die Zertifikate mit öffentlichen Schlüsseln ausstellen und signieren, gehören in der Regel einer Zertifizierungsinfrastruktur an, die auch für andere Bereiche der Zertifikatsverwaltung, wie die Veröffentlichung, Rücknahme und Erneuerung von Zertifikaten, verantwortlich sind. Eine Infrastruktur dieser Art wird allgemein als *PKI (Public Key Infrastructure)*, Infrastruktur für öffentliche Schlüssel) bezeichnet. Eine bekannte PKI ist der Standard *OpenPGP*, in dem Benutzer ihre Zertifikate selbst ohne zentrale Autorisierungspunkte veröffentlichen. Diese Zertifizierungen werden vertrauenswürdig, wenn Sie von anderen Personen im „Verbürgungsnetz“ signiert werden.

Die *Public Key Infrastructure X.509 (PKIX)* ist ein alternatives, von der *IETF (Internet Engineering Task Force)* definiertes Modell, das heute als Vorlage für beinahe alle öffentlich verwendeten PKIs dient. In diesem Modell erfolgt die Authentifizierung über *Zertifizierungsstellen* in einer hierarchischen Baumstruktur. Der Stamm des Baums ist

die Stammzertifizierungsstelle, mit der alle untergeordneten Zertifizierungsstellen zertifiziert werden. Über die unterste Ebene der untergeordneten Zertifizierungsstellen werden Benutzerzertifikate ausgestellt. Die Benutzerzertifikate sind aufgrund der Zertifizierung vertrauenswürdig, die bis zur Stammzertifizierungsstelle zurückverfolgt werden kann.

Die Sicherheit einer solchen PKI ist von der Vertrauenswürdigkeit der Zertifizierungsstellenzertifikate abhängig. Um den PKI-Kunden die Zertifizierungspraxis zu verdeutlichen, definiert der PKI-Operator ein *Certification Practice Statement (CPS)*, in dem die Vorgehensweisen für die Zertifikatsverwaltung festgelegt werden. Auf diese Weise soll sichergestellt werden, dass von der PKI nur vertrauenswürdige Zertifikate ausgestellt werden.

30.1.2 X.509-Zertifikate

Bei einem X.509-Zertifikat handelt es sich um eine Datenstruktur mit mehreren festen Feldern und optionalen zusätzlichen Erweiterungen. Die Textfelder enthalten hauptsächlich den Namen des Schlüsseleigentümers, den öffentlichen Schlüssel und die Daten zur ausstellenden Zertifizierungsstelle (Name und Signatur). Aus Sicherheitsgründen sollte ein Zertifikat nur über eine begrenzte Zeit gültig sein, sodass auch für dieses Datum ein Feld zur Verfügung steht. Die Zertifizierungsstelle garantiert die Gültigkeit des Zertifikats über den angegebenen Zeitraum. Gemäß CPS ist in der Regel die PKI (die ausstellende Zertifizierungsstelle) erforderlich, um vor dem Ablauf ein neues Zertifikat zu erstellen.

Die Erweiterungen können beliebige zusätzliche Informationen enthalten. Eine Anwendung muss nur dann eine Erweiterung bewerten können, wenn sie als *kritisch* definiert ist. Wenn eine Anwendung eine kritische Erweiterung nicht erkennt, muss sie das Zertifikat ablehnen. Einige Erweiterungen, wie Signatur oder Verschlüsselung, sind nur für bestimmte Anwendungen nützlich.

Tabelle 30.1 zeigt die Felder eines grundlegenden X.509-Zertifikats der Version 3 an.

Tabelle 30.1 X.509v3-Zertifikat

Feld	Inhalt
Version	Die Version des Zertifikats, beispielsweise v3

Feld	Inhalt
Seriennummer	Eindeutige Zertifikats-ID (eine Ganzzahl)
Signatur	Die ID des zum Signieren des Zertifikats verwendeten Algorithmus
Aussteller	Der eindeutige Name (DN) der ausstellenden Stelle (CA)
Gültigkeit	Die Gültigkeitsdauer
Betreff	Der eindeutige Name (DN) des Eigentümers
Subject Public Key Info (Betreff: Info zu öffentlichem Schlüssel)	Der öffentliche Schlüssel des Eigentümers und die ID des Algorithmus
Issuer Unique ID (Eindeutige ID des Ausstellers)	Die eindeutige ID der ausstellenden Zertifizierungsstelle (optional)
Subject Unique ID (Betreff: Eindeutige ID)	Die eindeutige ID des Eigentümers (optional)
Extensions	Optionale zusätzliche Informationen, wie „KeyUsage“ oder „BasicConstraints“

30.1.3 Blockieren von X.509-Zertifikaten

Wenn ein Zertifikat vor seinem Ablauf nicht vertrauenswürdig wird, muss es umgehend blockiert werden. Dies ist unter Umständen erforderlich, wenn der private Schlüssel beispielsweise versehentlich veröffentlicht wurde. Das Blockieren von Zertifikaten ist besonders dann wichtig, wenn der private Schlüssel einer Zertifizierungsstelle und nicht zu einem Benutzerzertifikat gehört. In diesem Fall müssen alle von der relevanten Zertifizierungsstelle ausgestellten Zertifikate umgehend blockiert werden. Wenn ein Zertifikat blockiert wird, muss die PKI (die verantwortliche Zertifizierungsstelle) diese Informationen allen beteiligten Personen über eine *Zertifikatswiderrufsliste* (CRL, Certificate Revocation List) zur Verfügung stellen.

Diese Listen werden von der Zertifizierungsstelle in regelmäßigen Abständen an öffentlichen CRL-Veröffentlichungspunkten bereitgestellt. Optional kann der CRL-Veröffentlichungspunkt als Erweiterung im Zertifikat benannt werden, sodass ein Prüfer die aktuelle CRL zur Validierung abrufen kann. Eine Möglichkeit, dies zu tun, ist das *Online Certificate Status-Protokoll* (OCSP). Die Authentizität der CRLs wird über die Signatur der ausstellenden Zertifizierungsstelle gewährleistet. In **Tabelle 30.2**, „**X.509-Zertifikatswiderrufsliste (CRL)**“ (S. 529) werden die grundlegenden Bestandteile einer X.509-CRL dargestellt.

Tabelle 30.2 X.509-Zertifikatswiderrufsliste (CRL)

Feld	Inhalt
Version	Die Version der CRL, beispielsweise v2
Signatur	Die ID des zum Signieren der CRL verwendeten Algorithmus
Aussteller	Eindeutiger Name (DN) des Veröffentlichers der CRL (in der Regel die ausstellende Zertifizierungsstelle)
This Update (Diese Aktualisierung)	Der Zeitpunkt der Veröffentlichung dieser CRL (Datum und Uhrzeit)
Nächste Aktualisierung	Der Zeitpunkt der Veröffentlichung der nächsten CRL (Datum und Uhrzeit)
Liste der widerrufenen Zertifikate	Jeder Eintrag enthält die Seriennummer des Zertifikats, den Widerrufszeitpunkt und optionale Erweiterungen (CRL-Eintragserweiterungen)
Extensions	Optionale CRL-Erweiterungen

30.1.4 Repository für Zertifikate und CRLs

Die Zertifikate und CRLs für eine Zertifizierungsstelle müssen über ein *Repository* öffentlich verfügbar gemacht werden. Da die Zertifikate und die CRLs durch die Signatur vor Fälschungen geschützt werden, muss das Repository selbst nicht besonders

geschützt werden. Stattdessen wird versucht, einen möglichst einfachen und schnellen Zugriff zu ermöglichen. Aus diesem Grund werden Zertifikate häufig auf LDAP- oder HTTP-Servern bereitgestellt. Erläuterungen zu LDAP finden Sie in [Kapitel 20, LDAP – Ein Verzeichnisdienst](#) (S. 349). [Kapitel 22, Der HTTP-Server Apache](#) (S. 403) enthält Informationen zu HTTP-Servern.

30.1.5 Proprietäre PKI

YaST enthält Module für die grundlegende Verwaltung von X.509-Zertifikaten. Dies beinhaltet hauptsächlich die Erstellung von Zertifizierungsstellen, untergeordneten Zertifizierungsstellen und Ihrer jeweiligen Zertifikate. Die Dienste einer PKI gehen weit über die einfache Erstellung und Verteilung von Zertifikaten und CRLs hinaus. Der Betrieb einer PKI erfordert eine gut strukturierte Verwaltungsinfrastruktur, über die kontinuierliche Aktualisierungen von Zertifikaten und CRLs möglich sind. Diese Infrastruktur wird durch kommerzielle PKI-Produkte bereitgestellt und kann auch teilweise automatisiert werden. YaST enthält Werkzeuge für die Erstellung und Verteilung von Zertifizierungsstellen und Zertifikaten, die entsprechende Hintergrund-Infrastruktur kann momentan jedoch nicht bereitgestellt werden. Zum Einrichten einer kleinen PKI können die verfügbaren YaST-Module verwendet werden. Sie sollten eine „offizielle“ oder kommerzielle PKI jedoch über kommerzielle Produkte erstellen.

30.2 YaST-Module für die Verwaltung von Zertifizierungsstellen

YaST enthält zwei Module für die grundlegende Verwaltung von Zertifizierungsstellen. Hier werden die primären Verwaltungsaufgaben beschrieben, die mit diesen Modulen ausgeführt werden können.

30.2.1 Erstellen einer Stammzertifizierungsstelle

Der erste Schritt bei der Einrichtung einer PKI ist die Erstellung einer Stammzertifizierungsstelle. Führen Sie folgende Schritte aus:

- 1 Starten Sie YaST und wählen Sie *Sicherheit und Benutzer > CA Management*.
- 2 Klicken Sie auf *Root-CA erstellen*.
- 3 Geben Sie die Grunddaten für die Zertifizierungsstelle im ersten in **Abbildung 30.1**, „YaST-CA-Modul: Grunddaten für eine Stammzertifizierungsstelle“ (S. 531) gezeigten Dialogfeld ein. Die Textfelder haben folgende Bedeutungen:

Abbildung 30.1 YaST-CA-Modul: Grunddaten für eine Stammzertifizierungsstelle

The screenshot shows a dialog box titled "Neue Root-CA erstellen (Schritt 1/3)". It contains the following fields and controls:

- CA-Name:** Text input field containing "example-cert".
- Allgemeiner Name:** Text input field containing "example-ca".
- E-Mail-Adressen:** A list box containing "root@beispiel.org" with a checkmark in the "Standard" column. There are "Löschen" and "Standard" buttons to the right.
- Buttons:** "Hinzufügen" button below the email list.
- Organisation:** Text input field containing "Beispielorganisation".
- Organisatorische Einheit:** Text input field containing "Beispiel".
- Ort:** Text input field.
- Bundesland:** Text input field.
- Land:** Dropdown menu with "Deutschland" selected.
- Navigation:** "Zurück", "Abbrechen", and "Weiter" buttons at the bottom.

CA-Name

Geben Sie den technischen Namen der Zertifizierungsstelle ein. Verzeichnisnamen werden unter anderem von diesem Namen abgeleitet. Aus diesem Grund können nur die in der Hilfe angegebenen Zeichen verwendet werden. Der technische Name wird zudem beim Starten des Moduls in der Übersicht angezeigt.

Eigenname

Geben Sie den Namen ein, der für Verweise auf die Zertifizierungsstelle verwendet werden soll.

E-Mail-Adresse

Hier können mehrere E-Mail-Adressen eingegeben werden, die vom Zertifizierungsstellenbenutzer angezeigt werden können. Dies kann für Anfragen nützlich sein.

Land

Geben Sie das Land an, in der die Zertifizierungsstelle betrieben wird.

Organisation, Organisational Unit (Organisationseinheit), Ort, Status

Optionale Werte

- 4 Klicken Sie auf *Weiter*.
- 5 Geben Sie im zweiten Dialogfeld ein Passwort ein. Das Passwort ist immer erforderlich, wenn Sie die Zertifizierungsstelle verwenden, um eine untergeordnete Zertifizierungsstelle zu erstellen oder Zertifikate zu generieren. Die Textfelder haben folgende Bedeutungen:

Schlüssellänge

Das Feld *Schlüssellänge* enthält einen aussagekräftigen Standardwert und muss in der Regel nicht geändert werden, es sei denn, eine Anwendung kann die Schlüssellänge nicht verarbeiten.

Gültiger Zeitraum (Tage)

Als *Gültiger Zeitraum* werden für eine Zertifizierungsstelle standardmäßig 3.650 Tage (ca. 10 Jahre) festgelegt. Dieser lange Zeitraum ist sinnvoll, da mit dem Austausch einer gelöschten Zertifizierungsstelle ein erheblicher Verwaltungsaufwand verbunden ist.

Wenn Sie auf *Erweiterte Optionen* klicken, wird ein Dialogfeld geöffnet, in dem Sie die verschiedenen Attribute der X.509-Erweiterungen festlegen können (**Abbildung 30.4, „YaST-CA-Modul: Erweiterte Einstellungen“** (S. 538)). Für diese Werte sind sinnvolle Standardeinstellungen festgelegt, die Sie nur ändern sollten, wenn Sie sich auf dem Gebiet genau auskennen.

- 6 YaST zeigt zur Bestätigung die aktuellen Einstellungen an. Klicken Sie auf *Erstellen*. Die Stammzertifizierungsstelle wird erstellt und anschließend in der Übersicht angezeigt.

TIPP

Es empfiehlt sich, die Ausstellung von Benutzerzertifikaten durch die Stammzertifizierungsstelle nicht zuzulassen. Es sollte mindestens eine untergeordnete Zertifizierungsstelle zur Ausstellung der Benutzerzertifikate erstellt werden. Dies bietet den Vorteil, dass die Stammzertifizierungsstelle isoliert und sicher bleibt, beispielsweise auf einem separaten Computer in einem sicheren Raum. So kann die Stammzertifizierungsstelle sehr schwer angegriffen werden.

30.2.2 Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle

Eine untergeordnete Zertifizierungsstelle wird auf dieselbe Weise erstellt wie eine Stammzertifizierungsstelle. Führen Sie folgende Schritte aus:

- 1 Starten Sie YaST und öffnen Sie das CA-Modul.
- 2 Wählen Sie die erforderliche Root-CA aus und klicken Sie auf *CA betreten*.

ANMERKUNG

Die Gültigkeitsdauer der untergeordneten Zertifizierungsstelle muss vollständig in die Gültigkeitsdauer der „übergeordneten“ Zertifizierungsstelle fallen. Eine untergeordnete CA wird immer nach der „übergeordneten“ CA erstellt, daher wird durch den Standardwert eine Fehlermeldung verursacht. Geben Sie, um dies zu vermeiden, einen zulässigen Wert für die Gültigkeitsdauer ein.

- 3 Geben Sie das Passwort ein, wenn Sie erstmalig eine Zertifizierungsstelle aufrufen. YaST zeigt die wichtigsten Informationen zur Zertifizierungsstelle auf dem Karteireiter *Beschreibung* an (siehe [Abbildung 30.2](#)).

Abbildung 30.2 *YaST-CA-Modul: Verwenden einer Zertifizierungsstelle*



- 4 Klicken Sie auf *Erweitert* und wählen Sie *SubCA erstellen*. Hiermit wird dasselbe Dialogfeld wie bei der Erstellung einer Stammzertifizierungsstelle geöffnet.
- 5 Fahren Sie entsprechend den Anweisungen in [Abschnitt 30.2.1](#), „Erstellen einer Stammzertifizierungsstelle“ (S. 530) fort.
- 6 Wählen Sie den Karteireiter *Zertifikate*. Setzen Sie beschädigte oder sonstige unerwünschte untergeordnete Zertifizierungsstellen mit *Widerrufen* zurück. Ein Widerruf allein reicht zur Deaktivierung einer untergeordneten Zertifizierungsstelle nicht aus. Widerrufene untergeordnete Zertifizierungsstellen müssen zudem in einer CRL veröffentlicht werden. Die Erstellung von CRLs wird in [Abschnitt 30.2.5](#), „Erstellen von CRLs“ (S. 539) beschrieben.
- 7 Klicken Sie abschließend auf *OK*.

30.2.3 Erstellen oder Widerrufen von Benutzerzertifikaten

Die Erstellung von Client- und Server-Zertifikaten ähnelt der Erstellung des Zertifikats zum Erstellen von Zertifizierungsstellen in **Abschnitt 30.2.1, „Erstellen einer Stamm-zertifizierungsstelle“** (S. 530). Hier gelten dieselben Prinzipien. In Zertifikaten, die für E-Mail-Signaturen bestimmt sind, sollte die E-Mail-Adresse des Absenders (Eigentümer des privaten Schlüssels) im Zertifikat enthalten sein, damit das E-Mail-Programm das richtige Zertifikat zuweisen kann. Für die Zertifikatszuweisung während der Verschlüsselung muss die E-Mail-Adresse des Empfängers (Eigentümer des öffentlichen Schlüssels) im Zertifikat enthalten sein. Bei Server- und Client-Zertifikaten muss der Hostname des Servers in das Feld *Eigename* eingegeben werden. Die standardmäßige Gültigkeitsdauer für Zertifikate beträgt 365 Tage.

Gehen Sie zum Erstellen von Client- und Server-Zertifikaten wie folgt vor:

- 1 Starten Sie YaST und öffnen Sie das CA-Modul.
- 2 Wählen Sie die erforderliche Root-CA aus und klicken Sie auf *CA betreten*.
- 3 Geben Sie das Passwort ein, wenn Sie erstmalig eine Zertifizierungsstelle aufrufen. YaST zeigt die wichtigsten Informationen zur Zertifizierungsstelle auf dem Karteireiter *Beschreibung* an.
- 4 Klicken Sie auf *Zertifikate* (siehe **Abbildung 30.3, „Zertifikate einer Zertifizierungsstelle“** (S. 536)).

Abbildung 30.3 Zertifikate einer Zertifizierungsstelle



- 5 Klicken Sie auf *Hinzufügen > Server-Zertifikat hinzufügen* und erstellen Sie ein Server-Zertifikat.
- 6 Klicken Sie auf *Hinzufügen > Client-Zertifikat hinzufügen* und erstellen Sie ein Client-Zertifikat. Vergessen Sie hierbei nicht die Eingabe einer E-Mail-Adresse.
- 7 Klicken Sie abschließend auf *OK*.

Gehen Sie zum Widerrufen beschädigter oder sonstiger unerwünschter Zertifikate wie folgt vor:

- 1 Starten Sie YaST und öffnen Sie das CA-Modul.
- 2 Wählen Sie die erforderliche Root-CA aus und klicken Sie auf *CA betreten*.

- 3 Geben Sie das Passwort ein, wenn Sie erstmalig eine Zertifizierungsstelle aufrufen. YaST zeigt die wichtigsten Informationen zur Zertifizierungsstelle auf dem Karteireiter *Beschreibung* an.
- 4 Klicken Sie auf *Zertifikate* (siehe [Abschnitt 30.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“](#) (S. 533)).
- 5 Wählen Sie das zu widerrufende Zertifikat aus und klicken Sie auf *Widerrufen*.
- 6 Wählen Sie einen Grund für das Widerrufen des Zertifikats aus.
- 7 Klicken Sie abschließend auf *OK*.

ANMERKUNG

Ein Widerruf allein reicht zur Deaktivierung eines Zertifikats nicht aus. Widerrufene Zertifikate müssen zudem in einer CRL veröffentlicht werden. In [Abschnitt 30.2.5, „Erstellen von CRLs“](#) (S. 539) wird die Erstellung von CRLs erläutert. Nach der Veröffentlichung in einer CRL können widerrufene Zertifikate vollständig mit *Löschen* entfernt werden.

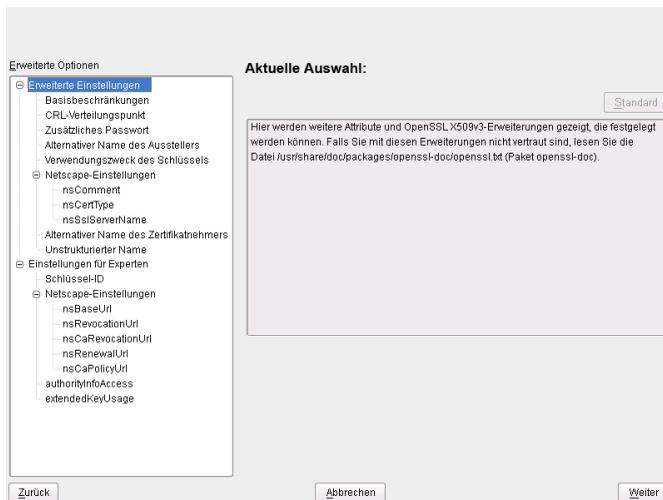
30.2.4 Ändern von Standardwerten

In den vorherigen Abschnitten wurde die Erstellung von untergeordneten Zertifizierungsstellen, Client- und Server-Zertifikaten beschrieben. In den Erweiterungen des X.509-Zertifikats werden spezielle Einstellungen verwendet. Für diese Einstellungen wurden für die einzelnen Zertifikatstypen sinnvolle Standardwerte festgelegt, die in der Regel nicht geändert werden müssen. Es kann jedoch sein, dass bei Ihnen bestimmte Anforderungen für diese Erweiterungen gelten. In diesem Fall kann eine Anpassung der Standardwerte sinnvoll sein. Anderenfalls beginnen Sie bei jeder Zertifikaterstellung von vorne.

- 1 Starten Sie YaST und öffnen Sie das CA-Modul.
- 2 Geben Sie die erforderliche Root-CA ein, wie in [Abschnitt 30.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“](#) (S. 533) beschrieben.
- 3 Klicken Sie auf *Erweitert > Standardeinstellungen bearbeiten*.

- 4 Wählen Sie den Typ der Einstellungen aus, die geändert werden sollen. Daraufhin wird das in **Abbildung 30.4**, „**YaST-CA-Modul: Erweiterte Einstellungen**“ (S. 538) gezeigte Dialogfeld zum Ändern der Standardeinstellungen geöffnet.

Abbildung 30.4 YaST-CA-Modul: Erweiterte Einstellungen



- 5 Ändern Sie den entsprechenden Wert auf der rechten Seite und legen Sie für die kritische Einstellung *Kritisch* fest oder löschen Sie sie.
- 6 Klicken Sie zum Anzeigen einer kurzen Zusammenfassung auf *Weiter*.
- 7 Schließen Sie die Änderungen mit *Speichern* ab.

TIPP

Alle Änderungen an den Standardeinstellungen gelten nur für nach diesem Zeitpunkt erstellte Objekte. Bereits bestehende Zertifizierungsstellen und Zertifikate bleiben unverändert.

30.2.5 Erstellen von CRLs

Wenn beschädigte oder sonstige unerwünschte Zertifikate von der weiteren Verwendung ausgeschlossen werden sollen, müssen sie zuerst widerrufen werden. Die entsprechende Vorgehensweise wird in [Abschnitt 30.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“](#) (S. 533) (für untergeordnete Zertifizierungsstellen) und in [Abschnitt 30.2.3, „Erstellen oder Widerrufen von Benutzerzertifikaten“](#) (S. 535) (für Benutzerzertifikate) beschrieben. Anschließend muss ein CRL mit diesen Informationen erstellt und veröffentlicht werden.

Im System wird für jede Zertifizierungsstelle jeweils nur eine CRL gespeichert. Gehen Sie zum Erstellen oder Aktualisieren dieser CRL wie folgt vor:

- 1 Starten Sie YaST und öffnen Sie das CA-Modul.
- 2 Geben Sie die erforderliche Zertifizierungsstelle ein, wie in [Abschnitt 30.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“](#) (S. 533) beschrieben.
- 3 Klicken Sie auf *CRL*. Das daraufhin angezeigte Dialogfeld enthält eine Zusammenfassung der letzten CRL dieser Zertifizierungsstelle.
- 4 Erstellen Sie eine neue CRL mit *CRL erzeugen*, wenn Sie seit der Erstellung neue untergeordnete CAs oder Zertifikate widerrufen haben.
- 5 Geben Sie die Gültigkeitsdauer für die neue CRL an (Standard: 30 Tage).
- 6 Klicken Sie zum Erstellen und Anzeigen der CRL auf *OK*. Anschließend muss die CRL veröffentlicht werden.

TIPP

Anwendungen, mit denen CRLs überprüft werden, lehnen alle Zertifikate ab, wenn die CRL nicht verfügbar oder nicht mehr gültig ist. Als PKI-Anbieter sind Sie verpflichtet, immer eine neue CRL zu erstellen und zu veröffentlichen, bevor die aktuelle CRL abläuft (Gültigkeitsdauer). In YaST steht keine Funktion zur Automatisierung dieses Vorgangs zur Verfügung.

30.2.6 Exportieren von Zertifizierungsstellenobjekten in LDAP

Der Computer, auf dem der Export ausgeführt wird, sollte für den LDAP-Export mit dem YaST-LDAP-Client konfiguriert werden. Hiermit werden während der Laufzeit Informationen zum LDAP-Server bereitgestellt, die zum Ausfüllen der Dialogfelder verwendet werden können. Ansonsten müssen alle LDAP-Daten manuell eingegeben werden, selbst wenn der Export möglich ist. Sie müssen immer mehrere Passwörter eingeben (siehe [Tabelle 30.3](#), „Passwörter beim LDAP-Export“ (S. 540)).

Tabelle 30.3 *Passwörter beim LDAP-Export*

Passwort	Bedeutung
LDAP-Passwort	Berechtigt den Benutzer, Einträge im LDAP-Baum hinzuzufügen.
Zertifikatpasswort	Berechtigt den Benutzer zum Exportieren des Zertifikats.
Neues Zertifikatpasswort	Beim LDAP-Export wird das Format PKCS12 verwendet. Mit diesem Format wird die Zuweisung eines neuen Passworts für das exportierte Zertifikat erzwungen.

Zertifikate, Zertifizierungsstellen und CRLs können in LDAP exportiert werden.

Exportieren von Zertifizierungsstellen in LDAP

Geben Sie die zu exportierende Zertifizierungsstelle wie unter [Abschnitt 30.2.2](#), „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“ (S. 533) beschrieben ein. Wählen Sie im aufgerufenen Dialogfeld die Optionsfolge *Erweitert* > *Nach LDAP exportieren*, um das Dialogfeld zur Eingabe der LDAP-Daten zu öffnen. Wenn das System mit dem YaST-LDAP-Client konfiguriert wurde, sind die Felder bereits teilweise ausgefüllt. Anderenfalls geben Sie alle Daten manuell ein. Einträge werden in LDAP in einem separaten Baum mit dem Attribut „caCertificate“ erstellt.

Exportieren von Zertifikaten in LDAP

Geben Sie die Zertifizierungsstelle ein, die das zu exportierende Zertifikat enthält, und wählen Sie dann *Zertifikate* aus. Wählen Sie in der Liste der Zertifikate im oberen Bereich des Dialogfelds das erforderliche Zertifikat und anschließend die Optionsfolge *Exportieren > Nach LDAP exportieren* aus. Die LDAP-Daten werden hier so eingegeben wie für Zertifizierungsstellen. Das Zertifikat wird zusammen mit dem entsprechenden Benutzerobjekt und mit den Attributen „userCertificate“ (PEM-Format) und „userPKCS12“ (PKCS12-Format) gespeichert.

Exportieren von CRLs in LDAP

Geben Sie die Zertifizierungsstelle ein, die die zu exportierende CRL enthält, und wählen Sie dann *CRL* aus. Erstellen Sie bei Bedarf eine neue CRL und klicken Sie auf *Exportieren*. Es wird ein Dialogfeld mit den Exportparametern geöffnet. Sie können die CRL für diese CA entweder auf ein Mal oder in regelmäßigen Zeitabständen exportieren. Aktivieren Sie den Export durch Auswählen von *Nach LDAP exportieren* und geben Sie die entsprechenden LDAP-Daten ein. Um diesen Vorgang in regelmäßigen Abständen durchzuführen, wählen Sie das Optionsfeld *Erneute Erstellung und Export wiederholen* und ändern ggf. den Zeitabstand.

30.2.7 Exportieren von Zertifizierungsstellenobjekten als Datei

Wenn Sie auf Ihrem Computer ein Repository für die Verwaltung von Zertifizierungsstellen eingerichtet haben, können Sie diese Option verwenden, um die Zertifizierungsstellenobjekte direkt als Datei am richtigen Speicherort zu erstellen. Es stehen verschiedene Ausgabeformate zur Verfügung, beispielsweise PEM, DER und PKCS12. Bei PEM können Sie auswählen, ob ein Zertifikat mit oder ohne Schlüssel exportiert werden soll und ob der Schlüssel verschlüsselt sein soll oder nicht. Bei PKCS12 besteht zudem die Möglichkeit, den Zertifizierungspfad zu exportieren.

Der Export von Zertifikaten und Zertifizierungsstellen in eine Datei erfolgt auf die gleiche Weise wie bei LDAP (in [Abschnitt 30.2.6, „Exportieren von Zertifizierungsstellenobjekten in LDAP“](#) (S. 540) beschrieben). Sie wählen jedoch anstelle der Option *Nach LDAP exportieren* die Option *Als Datei exportieren*. Hiermit gelangen Sie zu einem Dialogfeld zur Auswahl des erforderlichen Ausgabeformats und zur Eingabe

des Passworts und des Dateinamens. Das Zertifikat wird im erforderlichen Speicherort gespeichert, nachdem Sie auf *OK* klicken.

Klicken Sie bei CRLs auf *Exportieren*, wählen Sie *In Datei exportieren*, wählen Sie ein Exportformat (PEM oder DER) und geben Sie den Pfad ein. Fahren Sie mit *OK* fort, um das Element im entsprechenden Speicherort zu speichern.

TIPP

Sie können einen beliebigen Speicherort im Dateisystem auswählen. Diese Option kann auch zum Speichern von Zertifizierungsstellenobjekten auf einem Wechseldatenträger, wie beispielsweise einem USB-Stick, verwendet werden. Im Verzeichnis `/media` sind beliebige Laufwerktypen gespeichert, mit Ausnahme der Festplatte Ihres Systems.

30.2.8 Importieren von Common Server Certificates

Wenn Sie ein Server-Zertifikat mit YaST auf einen Datenträger auf einem isolierten Zertifizierungsstellen-Verwaltungscomputer exportiert haben, können Sie das betreffende Zertifikat als *Common Server Certificate* auf einen Server importieren. Führen Sie diesen Vorgang während der Installation oder zu einem späteren Zeitpunkt in YaST aus.

ANMERKUNG

Für den erfolgreichen Import des Zertifikats benötigen Sie eines der PKCS12-Formate.

Das allgemeine Server-Zertifikat wird unter `/etc/ssl/servercerts` gespeichert und kann dort von allen von Zertifizierungsstellen unterstützten Diensten verwendet werden. Wenn das Zertifikat abgelaufen ist, kann es leicht mit denselben Mechanismen ersetzt werden. Starten Sie die entsprechenden Dienste neu, damit das neue Zertifikat funktioniert.

TIPP

Wenn Sie hier *Importieren* wählen, können Sie die Quelle im Dateisystem auswählen. Diese Option kann auch zum Importieren von Zertifikaten auf einem Wechseldatenträger, wie beispielsweise einem USB-Stick, verwendet werden.

Gehen Sie zum Importieren eines Common Server Certificate wie folgt vor:

- 1 Starten Sie YaST und öffnen Sie *Common Server Certificate* unter *Sicherheit und Benutzer*.
- 2 Zeigen Sie die Daten für das aktuelle Zertifikat nach dem Starten von YaST im Beschreibungsfeld an.
- 3 Wählen Sie *Importieren* und dann die Zertifikatsdatei aus.
- 4 Geben Sie das Passwort ein und klicken Sie auf *Weiter*. Das Zertifikat wird importiert und anschließend im Beschreibungsfeld angezeigt.
- 5 Schließen Sie YaST mit *Verlassen*.

Verschlüsseln von Partitionen und Dateien

31

Vertrauliche Daten, die kein unberechtigter Dritter einsehen sollte, hat jeder Benutzer. Je mehr Sie sich auf die mobile Arbeit am Computer und verschiedene Umgebungen und Netzwerke verlassen, desto sorgfältiger sollten Sie mit Ihren Daten umgehen. Die Verschlüsselung einzelner Dateien oder gar ganzer Partitionen wird dringend empfohlen, wenn andere Personen direkt oder über das Netzwerk auf Ihr System zugreifen können. Laptops und Wechseldatenträger wie externe Festplatten oder USB-Sticks gehen sehr schnell verloren oder werden gestohlen. Daher sollten Sie Dateien mit vertraulichen Daten unbedingt verschlüsseln.

Es gibt mehrere Möglichkeiten, Ihre Daten mittels Verschlüsselung zu schützen:

Verschlüsselung einer Festplattenpartition

Sie können eine verschlüsselte Partition mit YaST während der Installation oder in einem bereits installierten System erstellen. Einzelheiten finden Sie unter [Abschnitt 31.1.1, „Anlegen einer verschlüsselten Partition während der Installation“](#) (S. 547) und [Abschnitt 31.1.2, „Einrichten einer verschlüsselten Partition im laufenden System“](#) (S. 548). Diese Option kann auch für Wechseldatenträger, wie externe Festplatten, verwendet werden (siehe [Abschnitt 31.1.4, „Verschlüsseln des Inhalts von Wechselmedien“](#) (S. 549)).

Erstellen einer verschlüsselten Datei als Container

Mit YaST können Sie jederzeit eine verschlüsselte Datei auf Ihrer Festplatte oder auf einem Wechseldatenträger erstellen. Die verschlüsselte Datei kann dann verwendet werden, um darin andere Dateien oder Ordner zu *verwahren*. Weitere Informationen hierzu finden Sie in [Abschnitt 31.1.3, „Erstellen einer verschlüsselten Datei als Container“](#) (S. 549).

Verschlüsseln von Home-Verzeichnissen

Mit openSUSE können Sie auch verschlüsselte Home-Verzeichnisse für Benutzer erstellen. Wenn sich der Benutzer am System anmeldet, wird das verschlüsselte Home-Verzeichnis eingehängt und die Inhalte werden dem Benutzer verfügbar gemacht. Weitere Informationen finden Sie unter [Abschnitt 31.2, „Verwenden von verschlüsselten Home-Verzeichnissen“](#) (S. 550).

Verschlüsseln von einzelnen ASCII-Textdateien

Wenn Sie nur wenige ASCII-Textdateien mit vertraulichen Daten haben, können Sie sie einzeln verschlüsseln und mithilfe des vi-Editors mit einem Passwort verschlüsseln. Weitere Informationen finden Sie unter [Abschnitt 31.3, „Verschlüsselung einzelner ASCII-Textdateien mit vi“](#) (S. 551).

WARNUNG: Das Verschlüsseln von Medien bietet nur eingeschränkten Schutz

Die in diesem Kapitel beschriebenen Methoden bieten nur eingeschränkten Schutz. Ein laufendes System können Sie nicht vor Manipulation und Beschädigung schützen. Nachdem ein verschlüsseltes Medium erfolgreich eingehängt wurde, können alle Benutzer mit den entsprechenden Berechtigungen darauf zugreifen. Die Verwendung verschlüsselter Medien ist jedoch von Vorteil, wenn Ihr Computer verloren geht oder gestohlen wird oder um zu verhindern, dass unbefugte Personen Ihre vertraulichen Daten lesen.

31.1 Einrichten von verschlüsselten Dateisystemen mit YaST

Verwenden Sie YaST zur Verschlüsselung von Partitionen oder Teilen Ihres Dateisystems bei der Installation oder in einem bereits installierten System. Das Verschlüsseln einer Partition in einem bereits installierten System ist jedoch schwieriger, da Sie hierbei die Größe der bestehenden Partitionen bzw. die Partitionen selbst ändern müssen. In solchen Fällen ist es oft einfacher, eine verschlüsselte Datei mit einer festgelegten Größe zu erstellen, in der andere Dateien oder Teile des Dateisystems *verwahrt* werden können. Zum Verschlüsseln einer gesamten Partition legen Sie eine zu verschlüsselnde Partition im Partitionsschema fest. Die Standardpartitionierung, wie sie YaST bei der Installation vorschlägt, sieht keine verschlüsselte Partition vor. Sie müssen sie im Partitionsdialogfeld manuell hinzufügen.

31.1.1 Anlegen einer verschlüsselten Partition während der Installation

WARNUNG: Passworтеingabe

Merken Sie sich das Passwort für Ihre verschlüsselten Partitionen. Ohne dieses Passwort haben Sie keine Möglichkeit, auf die verschlüsselten Daten zuzugreifen oder diese wiederherzustellen.

Das YaST-Expertendialogfeld für die Partitionierung bietet die Möglichkeit zum Anlegen einer verschlüsselten Partition. Zum Erstellen einer neuen verschlüsselten Partition gehen Sie wie folgt vor:

- 1 Wählen Sie im YaST-Kontrollzentrum *System > Partitionieren* aus, um das Partitionierungsprogramm von YaST zu starten.
- 2 Klicken Sie auf *Erstellen* und wählen Sie eine primäre oder eine logische Partition aus.
- 3 Wählen Sie das gewünschte Dateisystem, die Größe und den Einhängepunkt für die Partition aus.
- 4 Wenn das verschlüsselte Dateisystem nur bei Bedarf eingehängt werden soll, aktivieren Sie die Option *Nicht beim Systemstart mounten* im Dialogfeld *Optionen für Fstab*.
- 5 Aktivieren Sie das Kontrollkästchen *Dateisystem verschlüsseln*.
- 6 Klicken Sie auf *OK*. Sie werden zur Eingabe eines Passworts zur Verschlüsselung dieser Partition aufgefordert. Das Passwort wird nicht angezeigt. Um auszuschließen, dass Sie sich bei der Eingabe verschrieben haben, müssen Sie das Passwort ein zweites Mal eingeben.
- 7 Schließen Sie den Vorgang mit *OK* ab. Die neue verschlüsselte Partition wird nun erstellt.

Wenn Sie das Kontrollkästchen *Nicht beim Systemstart mounten* deaktiviert gelassen haben, wird das Passwort beim Starten des Computers vor dem Einhängen der Partition abgefragt. Nach dem Einhängen steht die Partition allen Benutzern zur Verfügung.

Um das Einhängen der verschlüsselten Partition während des Starts zu überspringen, drücken Sie die Eingabetaste, wenn Sie aufgefordert werden, das Passwort einzugeben. Verneinen Sie anschließend die Nachfrage, ob Sie das Passwort erneut eingeben möchten. Das verschlüsselte Dateisystem wird in diesem Fall nicht eingehängt, das Betriebssystem setzt den Boot-Vorgang wie gewohnt fort und blockiert somit den Zugriff auf Ihre Daten.

Um auf eine verschlüsselte Partition zuzugreifen, die während des Bootens nicht eingehängt wird, hängen Sie die Partition manuell ein, indem Sie `mount name_of_partition mount_point` eingeben. Geben Sie das Passwort auf Aufforderung ein. Wenn Sie die Partition nicht mehr benötigen, hängen Sie sie mit `umount Name_der_Partition` aus. So verhindern Sie, dass andere Benutzer auf die Partition zugreifen können.

Wenn Sie Ihr System auf einem Computer installieren, auf dem bereits mehrere Partitionen vorhanden sind, können Sie auch entscheiden, während der Installation eine bestehende Partition zu verschlüsseln. Befolgen Sie in diesem Fall die Anweisungen unter **Abschnitt 31.1.2, „Einrichten einer verschlüsselten Partition im laufenden System“** (S. 548) und bedenken Sie, dass durch diese Aktion alle Daten in der bestehenden Partition, die Sie verschlüsseln möchten, gelöscht werden.

31.1.2 Einrichten einer verschlüsselten Partition im laufenden System

WARNUNG: Aktivieren der Verschlüsselung auf einem laufenden System

Das Erstellen verschlüsselter Partitionen ist auch auf einem laufenden System möglich. Durch das Verschlüsseln einer bestehenden Partition werden jedoch alle darin enthaltenen Daten gelöscht und die bestehenden Partitionen müssen in der Größe verändert und neu strukturiert werden.

Wählen Sie auf einem laufenden System im YaST-Kontrollzentrum die Option *System > Partitionierung*. Klicken Sie auf *Ja*, um fortzufahren. Wählen Sie im *Expert Partitioner* die zu verschlüsselnde Partition aus und klicken Sie auf *Bearbeiten*. Führen Sie alle verbleibenden Schritte wie in **Abschnitt 31.1.1, „Anlegen einer verschlüsselten Partition während der Installation“** (S. 547) beschrieben aus.

31.1.3 Erstellen einer verschlüsselten Datei als Container

Anstatt eine Partition zu verwenden, können Sie eine verschlüsselte Datei mit einer bestimmten Größe erstellen, in der andere Dateien oder Ordner mit vertraulichen Daten verwahrt werden können. Solche so genannten Containerdateien werden in YaST im Dialogfeld "Festplatte vorbereiten: Expertenmodus" erstellt. Wählen Sie *Kryptodatei* aus und geben Sie den vollständigen Pfad der Datei und ihre Größe ein. Übernehmen oder ändern Sie die Voreinstellungen für die Formatierung und den Dateisystemtyp. Geben Sie den Einhängepunkt an und legen Sie fest, ob das verschlüsselte Dateisystem beim Booten des Systems eingehängt werden soll.

Der Vorteil verschlüsselter Containerdateien gegenüber verschlüsselten Partitionen besteht darin, dass sie dem System hinzugefügt werden können, ohne dass die Festplatte neu partitioniert werden muss. Sie werden mithilfe eines Loop-Device eingehängt und verhalten sich wie normale Partitionen.

31.1.4 Verschlüsseln des Inhalts von Wechselmedien

Wechselmedien, wie externe Festplatten oder USB-Flash-Laufwerke, werden von YaST auf dieselbe Weise behandelt wie herkömmliche Festplatten. Containerdateien oder Partitionen auf solchen Medien können, wie oben beschrieben, verschlüsselt werden. Aktivieren Sie jedoch *Nicht beim Systemstart mounten* (Während des Bootens nicht einhängen) im Dialogfeld *Optionen für Fstab*, da entfernbare Medien in der Regel erst verbunden werden, wenn das System ausgeführt wird.

Wenn Sie Ihr Wechselgerät mit YaST verschlüsselt haben, erkennen die KDE- und GNOME-Desktops automatisch die verschlüsselte Partition und fordern zur Eingabe des Passwortes auf, sobald das Gerät erkannt wird. Wenn Sie ein FAT-formatiertes entfernbare Gerät verbinden, während KDE oder GNOME ausgeführt wird, ist der Desktop-Benutzer, der das Passwort eingibt, automatisch der Eigentümer des Geräts und kann Dateien lesen und schreiben. Bei Geräten, deren Dateisystem nicht FAT ist, müssen Sie die Eigentümerschaft explizit für alle Benutzer außer dem `root` ändern, damit diese Benutzer Dateien auf dem Gerät lesen oder schreiben können.

31.2 Verwenden von verschlüsselten Home-Verzeichnissen

Um Daten in Home-Verzeichnissen gegen Diebstahl und das Entfernen der Festplatte zu schützen, verwenden Sie das Benutzerverwaltungsmodul, um die Verschlüsselung von Home-Verzeichnissen zu aktivieren. Sie können verschlüsselte Home-Verzeichnisse für neue oder vorhandene Benutzer erstellen. Um Home-Verzeichnisse von bereits vorhandenen Benutzern zu ver- oder entschlüsseln, müssen Sie deren Passwörter für die Anmeldung kennen. Weitere Anleitungen dazu finden Sie unter Kapitel 5, *Verwalten von Benutzern mit YaST* (↑Start).

Verschlüsselte Home-Partitionen werden in einem Dateicontainer wie in [Abschnitt 31.1.3, „Erstellen einer verschlüsselten Datei als Container“](#) (S. 549) beschrieben erstellt. Es werden zwei Dateien unter `/home` für jedes verschlüsselte Home-Verzeichnis erstellt:

`LOGIN.img`

Das Image mit dem Verzeichnis

`LOGIN.key`

Der Image-Schlüssel ist durch das Anmeldepasswort des Benutzers geschützt.

Bei der Anmeldung wird das Home-Verzeichnis automatisch entschlüsselt. Intern wird das Home-Verzeichnis über das PAM-Modul "pam_mount" bereitgestellt. Wenn Sie eine zusätzliche Anmeldemethode hinzufügen möchten, die verschlüsselte Home-Verzeichnisse bereitstellt, müssen Sie dieses Modul der jeweiligen Konfigurationsdatei in `/etc/pam.d/` hinzufügen. Weitere Informationen finden Sie in [Kapitel 13, Authentifizierung mit PAM](#) (S. 213) sowie auf der man-Seite von `pam_mount`.

WARNUNG: Sicherheitsbeschränkungen

Das Verschlüsseln des Home-Verzeichnisses eines Benutzers bietet keinen umfassenden Schutz vor anderen Benutzern. Wenn Sie einen umfassenden Schutz benötigen, sollten nicht mehrere Benutzer an einem Rechner arbeiten.

Um die Sicherheit zu erhöhen, verschlüsseln Sie auch die `Swap`-Partition sowie die Verzeichnisse `/tmp` und `/var/tmp`, da diese temporäre Images kritischer Daten enthalten können. Sie können `swap`, `/tmp` und `/var/tmp` mit dem

YaST-Partitioner verschlüsseln wie in [Abschnitt 31.1.1](#), „Anlegen einer verschlüsselten Partition während der Installation“ (S. 547) und [Abschnitt 31.1.3](#), „Erstellen einer verschlüsselten Datei als Container“ (S. 549) beschrieben.

31.3 Verschlüsselung einzelner ASCII-Textdateien mit vi

Der Nachteil verschlüsselter Partitionen ist, dass bei eingehängter Partition `root` immer auf die Daten zugreifen kann. Um dies zu verhindern, kann `vi` im verschlüsselten Modus verwendet werden.

Geben Sie zur Bearbeitung einer neuen Datei `vi -xDateiname` ein. `vi` fordert Sie auf, ein neues Passwort festzulegen und verschlüsselt anschließend den Inhalt der Datei. Bei jedem Zugriff auf die Datei fordert `vi` das richtige Passwort an.

Um die Sicherheit noch mehr zu erhöhen, können Sie die verschlüsselte Textdatei in einer verschlüsselten Partition ablegen. Dies wird empfohlen, da die `vi`-Verschlüsselung nicht sehr stark ist.

Einschränken von Berechtigungen mit AppArmor

32

Viele Sicherheitsrisiken resultieren aus Fehlern in *verbürgten* Programmen. Ein verbürgtes Programm läuft mit einer Berechtigung, die ein Angreifer gerne hätte. Das Programm kann dieses Vertrauen nicht rechtfertigen, wenn ein Fehler dem Angreifer erlaubt, diese Berechtigung zu beziehen.

Novell® AppArmor ist eine Lösung für Anwendungssicherheit, die insbesondere konzipiert wurde, um verdächtige Programme auf die geringste Berechtigungsstufe einzuschränken. Mit AppArmor kann der Administrator die Domäne der Aktivitäten angeben, die das Programm ausführen darf. Hierzu entwickelt er ein Sicherheits*profil* für diese Anwendung, d. h. eine Liste der Dateien, auf die das Programm zugreifen darf, und der Operationen, die das Programm ausführen darf.

Für wirksame Immunisierung eines Computersystems muss die Anzahl der Programme minimiert werden, die Berechtigungen vermitteln. Dann müssen die Programme so gut wie möglich abgesichert werden. Mit Novell AppArmor brauchen Sie für die Programme, die in Ihrer Umgebung Angriffen ausgesetzt sind, nur Profile zu erstellen und verringern damit den Aufwand für die Immunisierung Ihres Computers erheblich. AppArmor-Profile erzwingen die Einhaltung von Richtlinien und stellen damit sicher, dass Programme ihre Aufgaben erfüllen und keine anderen Aktionen ausführen.

Administratoren müssen sich nur um die Anwendungen kümmern, die durch Angriffe gefährdet sind, und Profile für diese Anwendungen generieren. Die Immunisierung eines Systems besteht im Wesentlichen aus dem Erstellen und Pflegen des AppArmor-Profilsatzes und der Überwachung aller Richtlinienverstöße oder Ausnahmen, die durch die Protokollfunktion von AppArmor aufgezeichnet werden.

Das Erstellen von AppArmor-Profilen zur Einschränkung einer Anwendung ist einfach und intuitiv. AppArmor wird mit mehreren Werkzeugen ausgeliefert, die Sie bei der Profilerstellung unterstützen. AppArmor verlangt keine Programmierung oder den Einsatz von Skripts. Als einzige Aufgabe muss der Administrator eine strenge Zugriffsrichtlinie und Ausführungsberechtigungen für jede Anwendung festlegen, die immunisiert werden muss.

Aktualisierungen oder Änderungen der Anwendungsprofile sind nur erforderlich, wenn sich die Softwarekonfiguration oder der gewünschte Aktionsumfang ändert. AppArmor stellt intuitive Werkzeuge für Profilaktualisierungen oder -änderungen zur Verfügung.

Den Benutzern sollte AppArmor nicht weiter auffallen. Es läuft „hinter den Kulissen“ und erfordert keinerlei Benutzereingriffe. Die Leistung wird durch AppArmor nicht merklich eingeschränkt. Wenn eine Aktivität der Anwendung nicht durch ein AppArmor-Profil abgedeckt ist oder durch AppArmor verhindert wird, muss der Administrator das Profil dieser Anwendung für die entsprechende Verhaltensweise anpassen.

Diese Anleitung umreißt die grundlegenden Aufgaben, die mit AppArmor ausgeführt werden müssen, um ein System wirksam zu schützen. Ausführlichere Informationen finden Sie im *Novell AppArmor -Administrationshandbuch*.

32.1 Installieren von Novell AppArmor

Novell AppArmor wird bei jeder Installation von openSUSE® standardmäßig installiert und ausgeführt, unabhängig davon, welche Schemata installiert sind. Die unten aufgeführten Pakete sind für eine voll funktionsfähige Instanz von AppArmor erforderlich.

- `apparmor-docs`
- `apparmor-parser`
- `apparmor-profiles`
- `apparmor-utils`
- `audit`
- `libapparmor1`
- `perl-libapparmor`
- `yast2-apparmor`

32.2 Aktivieren und Deaktivieren von Novell AppArmor

Novell AppArmor ist für die standardmäßige Ausführung auf jeder neuen Installation von openSUSE konfiguriert. Es gibt zwei Möglichkeiten, den Status von AppArmor zu ändern:

Mithilfe der YaST-Systemdienste (Runlevel)

Aktivieren oder deaktivieren Sie AppArmor, indem Sie dessen Startskript zur Abfolge der Skripts hinzufügen, die beim Systemstart ausgeführt werden, bzw. dieses daraus entfernen. Statusänderungen werden beim nächsten Systemstart übernommen.

Verwenden der Novell AppArmor-Kontrollleiste

Ändern Sie den Status von Novell AppArmor auf einem laufenden System, indem Sie es mithilfe der YaST- Novell AppArmor-Kontrollleiste aktivieren oder deaktivieren. Änderungen, die hier vorgenommen werden, werden sofort übernommen. Die Kontrollleiste löst ein Stopp- oder Startereignis für AppArmor aus und entfernt dessen Startskript aus der Startsequenz des Systems bzw. fügt dessen Startskript hinzu.

Wenn Sie AppArmor dauerhaft deaktivieren möchten, indem Sie es aus der Abfolge der beim Systemstart ausgeführten Skripten entfernen, gehen Sie wie folgt vor:

- 1 Starten Sie YaST.
- 2 Wählen Sie *System > Systemdienste (Runlevel)*.
- 3 Wählen Sie *Expertenmodus*.
- 4 Wählen Sie `boot . apparmor` und klicken Sie auf *Festlegen/Zurücksetzen > Dienst deaktivieren*.
- 5 Beenden Sie das YaST-Runlevel-Werkzeug mit *Fertig stellen*.

AppArmor wird beim nächsten Systemstart nicht initialisiert und bleibt inaktiv, bis Sie es wieder ausdrücklich aktivieren. Die erneute Aktivierung eines Diensts mithilfe des YaST-Runlevel-Werkzeugs funktioniert auf dieselbe Weise wie die Deaktivierung.

In einem laufenden System ändern Sie den Status von AppArmor mithilfe der AppArmor-Kontrollleiste. Diese Änderungen werden wirksam, sobald sie angewendet werden, und überdauern auch den Neustart des Systems. Gehen Sie zur Änderung des AppArmor-Status wie folgt vor:

- 1 Starten Sie YaST.
- 2 Wählen Sie *Novell AppArmor > AppArmor-Kontrollleiste*.
- 3 Wählen Sie *AppArmor aktivieren* aus. Um AppArmor zu deaktivieren, heben Sie die Auswahl dieser Option auf.
- 4 Beenden Sie die AppArmor-Kontrollleiste mit *Fertig*.

32.3 Einführung in die Erstellung von Anwendungsprofilen

Bereiten Sie Ihr System für einen erfolgreichen Einsatz von Novell AppArmor vor, indem Sie die folgenden Punkte genau beachten:

- 1 Ermitteln Sie die Anwendungen, die ein Profil brauchen. Weitere Informationen dazu finden Sie unter [Abschnitt 32.3.1, „Wählen der Anwendungen, die ein Profil erhalten sollen“](#) (S. 557).
- 2 Erstellen Sie die erforderlichen Profile wie in [Abschnitt 32.3.2, „Erstellen und Ändern von Profilen“](#) (S. 558) umrissen. Prüfen Sie die Ergebnisse und passen Sie die Profile bei Bedarf an.
- 3 Bleiben Sie auf dem Laufenden über die Vorgänge auf Ihrem System, indem Sie AppArmor-Berichte erzeugen und auf Sicherheitsereignisse reagieren. Weitere Informationen finden Sie unter [Abschnitt 32.3.3, „Konfigurieren von Novell AppArmor-Ereignisbenachrichtigung und -Berichten“](#) (S. 561).
- 4 Aktualisieren Sie Ihre Profile, wenn sich Ihre Umgebung ändert. Andernfalls müssen Sie auf Sicherheitsereignisse reagieren, die das AppArmor-Berichtswerkzeug protokolliert. Weitere Informationen finden Sie unter [Abschnitt 32.3.4, „Aktualisieren Ihrer Profile“](#) (S. 563).

32.3.1 Wählen der Anwendungen, die ein Profil erhalten sollen

Sie müssen nur die Programme schützen, die in Ihrer speziellen Konfiguration Angriffen ausgesetzt sind. Verwenden Sie also nur Profile für die Anwendungen, die Sie wirklich ausführen. Ermitteln Sie anhand der folgenden Liste die wahrscheinlichsten Kandidaten:

Netzwerkagenten

Programme (Server und Clients) mit offenen Netzwerkports. Benutzer-Clients, wie Mail-Clients und Webbrowser, haben bestimmte Privilegien. Diese Programme werden mit der Berechtigung ausgeführt, in das Home-Verzeichnis des Benutzers zu schreiben, und sie verarbeiten Eingaben von potenziell feindseligen entfernten Quellen, wie feindseligen Websites und per E-Mail gesendeten böartigen Code.

Webanwendungen

Programme, die sich durch einen Webbrowser aufrufen lassen, einschließlich CGI-Skripten in Perl, PHP-Seiten und komplexere Webanwendungen.

Cronjobs

Programme, die der cron-Daemon regelmäßig ausführt, lesen Eingaben aus einer Vielzahl von Quellen.

Um die Prozesse zu ermitteln, die derzeit mit offenen Netzwerkports laufen und eventuell ein Profil zur Beschränkung brauchen, führen Sie den Befehl `aa-unconfined` als `root` aus.

Beispiel 32.1 *Ausgabe von aa-unconfined*

```
19848 /usr/sbin/cupsd not confined
19887 /usr/sbin/sshd not confined
19947 /usr/lib/postfix/master not confined
29205 /usr/sbin/sshd confined by '/usr/sbin/sshd (enforce)'
```

In obigem Beispiel brauchen die Prozesse mit der Beschriftung `not confined` eventuell ein benutzerdefiniertes Profil zur Einschränkung. Die Prozesse mit der Angabe `confined by` sind bereits durch AppArmor geschützt.

TIPP: Weiterführende Informationen

Weitere Informationen zur Auswahl der richtigen Anwendungen für die Profilerstellung finden Sie unter Abschnitt „Determining Programs to Immunize“ (Kapitel 1, *Immunizing Programs*, ↑Novell AppArmor Administration Guide).

32.3.2 Erstellen und Ändern von Profilen

Novell AppArmor auf openSUSE wird mit einem vorkonfigurierten Satz von Profilen für die wichtigsten Anwendungen geliefert. Zusätzlich können Sie mit AppArmor Ihre eigenen Profile für jede beliebige Anwendung erstellen.

Es gibt zwei verschiedene Möglichkeiten, Profile zu verwalten. Die eine verwendet das grafische Frontend der YaST Novell AppArmor-Module und die andere nutzt die Befehlszeilen-Werkzeuge, die in der AppArmor-Suite zur Verfügung stehen. Beide Methoden arbeiten grundsätzlich auf dieselbe Weise.

Die Ausführung von `aa-unconfined` (wie in [Abschnitt 32.3.1](#), „Wählen der Anwendungen, die ein Profil erhalten sollen“ (S. 557) beschrieben) identifiziert eine Liste von Anwendungen, die eventuell ein Profil benötigen, um in einem sicheren Modus abzu-
laufen.

Führen Sie für jede Anwendung die folgenden Schritte aus, um ein Profil zu erstellen:

- 1 Melden Sie sich als `root` an und lassen Sie AppArmor das Profil der Anwendung grob umreißen, indem Sie `aa-genprof Programmname` ausführen.

oder

Umreißen Sie das grundlegende Profil, indem Sie `YaST > Novell AppArmor > Assistent zum Hinzufügen von Profilen` ausführen und den vollständigen Pfad der Anwendung angeben, für die ein Profil erstellt werden soll.

Ein grundlegendes Profil wird umrissen und AppArmor wird in den Lernmodus gebracht, d. h., es protokolliert jede Aktivität des ausgeführten Programms, schränkt es aber noch nicht ein.

- 2 Führen Sie die vollständige Palette der Anwendungsaktionen aus, damit AppArmor ein sehr genaues Bild der Aktivitäten ermittelt.

- 3 Lassen Sie AppArmor die Protokolldateien analysieren, die in **Schritt 2** (S. 558) generiert wurden, indem Sie `S` in `aa-genprof` eingeben.

oder

Analysieren Sie die Protokolle, indem Sie im *Assistenten zum Hinzufügen von Profilen* auf *Systemprotokoll auf AppArmor-Ereignisse prüfen* klicken und den Anweisungen des Assistenten folgen, bis das Profil fertig gestellt ist.

AppArmor prüft die Protokolle, die während der Ausführung der Anwendung aufgezeichnet wurden, und fordert Sie auf, für jedes protokollierte Ereignis die Zugriffsberechtigungen festzulegen. Legen Sie die Zugriffsberechtigungen für jede Datei fest oder verwenden Sie Platzhalterzeichen.

- 4 Abhängig von der Komplexität Ihrer Anwendung müssen **Schritt 2** (S. 558) und **Schritt 3** (S. 559) eventuell wiederholt werden. Begrenzen Sie die Anwendung, führen Sie sie unter diesen neuen Bedingungen aus und verarbeiten Sie sämtliche neuen Protokollereignisse. Um die ganzen Möglichkeiten einer Anwendung richtig einzugrenzen, müssen Sie diese Vorgehensweise möglicherweise oft wiederholen.
- 5 Sobald alle Berechtigungen festgelegt sind, wird Ihr Profil in den Erzwingen-Modus gesetzt. Das Profil wird angewendet und AppArmor schränkt die Anwendung gemäß dem soeben erstellten Profil ein.

Wenn `aa-genprof` für eine Anwendung gestartet wurde, die über ein vorhandenes Profil im Meldungsmodus verfügte, bleibt dieses Profil beim Verlassen dieses Lernzyklus im Lernmodus. Weitere Informationen zum Ändern des Modus eines Profils finden Sie unter „`aa-complain—Entering Complain or Learning Mode`“ (Kapitel 4, *Building Profiles from the Command Line*, ↑Novell AppArmor Administration Guide) und „`aa-enforce—Entering Enforce Mode`“ (Kapitel 4, *Building Profiles from the Command Line*, ↑Novell AppArmor Administration Guide).

Testen Sie Ihre Profileinstellungen, indem Sie jede benötigte Aufgabe mit der soeben eingeschränkten Anwendung ausführen. Normalerweise funktioniert das eingeschränkte Programm reibungslos und die AppArmor-Aktivitäten verlaufen unbemerkt. Wenn Sie jedoch in Ihrer Anwendung ein gewisses Fehlverhalten erkennen, prüfen Sie anhand der Systemprotokolle, ob AppArmor Ihre Anwendung zu stark einschränkt. Je nachdem, welcher Protokollierungsmechanismus in Ihrem System eingesetzt wird, müssen Sie an mehreren Stellen nach AppArmor-Protokolleinträgen suchen:

```
/var/log/audit/audit.log
```

Wenn das Paket `audit` installiert ist und `auditd` ausgeführt wird, werden AppArmor-Ereignisse wie folgt protokolliert:

```
type=APPARMOR_DENIED msg=audit(1210347212.123:18):
operation="inode_permission" requested_mask=":w" denied_mask=":w"
fsuid=1000 name="/tmp/.X11-unix/X0" pid=9160 profile="/usr/bin/kmsserver"
```

```
/var/log/messages
```

Wird `auditd` nicht verwendet, werden die AppArmor-Ereignisse im Standardsystemprotokoll unter `/var/log/messages` protokolliert. Ein Beispieleintrag würde wie folgt aussehen:

```
May  9 17:39:56 neovirt klogd: type=1503 audit(1210347596.146:23):
operation="inode_permission" requested_mask=":w" denied_mask=":w"
fsuid=1000 name="/tmp/.X11-unix/X0" pid=9347 profile="/usr/bin/kmsserver"
```

```
dmesg
```

Wird `auditd` nicht ausgeführt, können AppArmor-Ereignisse auch mit dem Befehl `dmesg` überprüft werden:

```
type=1503 audit(1210347596.146:23): operation="inode_permission"
requested_mask=":w" denied_mask=":w" fsuid=1000 name="/tmp/.X11-unix/X0"
pid=9347 profile="/usr/bin/kmsserver"
```

Analysieren Sie die Protokollmeldungen für diese Anwendung erneut, wie in **Schritt 3** (S. 559) beschrieben, um das Profil anzupassen. Bestimmen Sie die Zugriffsberechtigungen oder Einschränkungen, wenn Sie dazu aufgefordert werden.

TIPP: Weiterführende Informationen

Weitere Informationen zum Erstellen und Ändern von Profilen finden Sie in Kapitel 2, *Profile Components and Syntax* (↑Novell AppArmor Administration Guide), Kapitel 3, *Building and Managing Profiles with YaST* (↑Novell AppArmor Administration Guide) und Kapitel 4, *Building Profiles from the Command Line* (↑Novell AppArmor Administration Guide).

32.3.3 Konfigurieren von Novell AppArmor-Ereignisbenachrichtigung und -Berichten

Richten Sie eine Ereignisbenachrichtigung in Novell AppArmor ein, damit Sie Sicherheitsereignisse überprüfen können. Ereignisbenachrichtigung ist eine Novell AppArmor-Funktion, die einen angegebenen Email-Empfänger benachrichtigt, wenn im System eine Novell AppArmor-Aktivität unter der gewählten Sicherheitsebene auftritt. Diese Funktion steht derzeit über die YaST-Schnittstelle zur Verfügung.

Zum Einrichten der Ereignisbenachrichtigung in YaST gehen Sie wie folgt vor:

- 1 Stellen Sie sicher, dass ein Mailserver auf Ihrem System ausgeführt wird, der die Ereignismitteilungen liefert.
- 2 Starten Sie YaST. Wählen Sie dann *Novell AppArmor > AppArmor-Kontrollleiste* aus.
- 3 Wählen Sie unter *Sicherheitsereignisbenachrichtigung* die Option *Konfigurieren* aus.
- 4 Stellen Sie für jeden Eintragstyp (*Knapp*, *Zusammenfassung* und *Ausführlich*) eine Berichthäufigkeit ein, geben Sie die E-Mail-Adresse ein, an welche die Berichte gesendet werden, und legen Sie den Schweregrad der aufzuzeichnenden Ereignisse fest. Zur Aufnahme von unbekanntem Ereignissen in die Ereignisberichte aktivieren Sie *Ereignisse mit unbekanntem Schweregrad aufnehmen*.

ANMERKUNG: Auswahl der zu protokollierenden Ereignisse

Wenn Sie nicht mit der Ereigniskategorisierung von AppArmor vertraut sind, lassen Sie sich über alle Ereignisse in allen Sicherheitsstufen benachrichtigen.

- 5 Schließen Sie dieses Dialogfeld mit *OK > Fertig*, um Ihre Einstellungen anzuwenden.

Mithilfe von Novell AppArmor-Berichten können Sie wichtige Novell AppArmor-Sicherheitsereignisse nachlesen, die in Protokolldateien aufgezeichnet wurden, ohne

mühselig alle Meldungen zu durchsuchen, die nur für das aa-logprof-Werkzeug nützlich sind. Sie können die Größe des Berichts reduzieren, indem Sie nach Datumsbereich oder Programmname filtern.

Gehen Sie zur Konfiguration der AppArmor-Berichte wie folgt vor:

- 1 Starten Sie YaST. Wählen Sie *Novell AppArmor > AppArmor-Berichte*.
- 2 Wählen Sie den Berichtstyp, den Sie prüfen oder konfigurieren möchten, aus *Zusammenfassungsbericht der Ausführungssicherheit, Anwendungsprüfbericht* und *Sicherheitsereignisbericht*.
- 3 Bearbeiten Sie die Häufigkeit der Berichtgenerierung, E-Mail-Adresse, Exportformat und Speicherort der Berichte, indem Sie *Bearbeiten* wählen und die erforderlichen Daten angeben.
- 4 Um einen Bericht des ausgewählten Typs zu generieren, klicken Sie auf *Jetzt ausführen*.
- 5 Blättern Sie durch die archivierten Berichte eines bestimmten Typs, indem Sie *Archiv anzeigen* auswählen und den gewünschten Berichtstyp angeben.

oder

Löschen Sie nicht mehr benötigte Berichte oder fügen Sie neue Berichte hinzu.

TIPP: Weiterführende Informationen

Weitere Informationen zum Konfigurieren der Ereignisbenachrichtigung in Novell AppArmor finden Sie in Abschnitt „Configuring Security Event Notification“ (Kapitel 6, *Managing Profiled Applications*, ↑Novell AppArmor Administration Guide). Weitere Informationen zur Berichtskonfiguration finden Sie in Abschnitt „Configuring Reports“ (Kapitel 6, *Managing Profiled Applications*, ↑Novell AppArmor Administration Guide).

32.3.4 Aktualisieren Ihrer Profile

Software- und Systemkonfigurationen ändern sich im Lauf der Zeit. Daher kann Ihre Profileinstellung für AppArmor gelegentliche Anpassungen erfordern. AppArmor prüft Ihr Systemprotokoll auf Verletzungen der Richtlinien oder andere AppArmor-Ereignisse und ermöglicht es Ihnen, Ihren Profilsatz entsprechend anzupassen. Jedes Anwendungsverhalten, das außerhalb einer Profildefinition liegt, kann auch über den *Assistenten zum Aktualisieren von Profilen* behandelt werden.

Gehen Sie wie folgt vor, um Ihren Profilsatz zu aktualisieren:

- 1 Starten Sie YaST.
- 2 Starten Sie in *Novell AppArmor > Assistenten zum Aktualisieren von Profilen*.
- 3 Passen Sie Zugriffs- oder Ausführungsberechtigungen für jede protokollierte Ressource oder jedes protokollierte ausführbare Programm an, wenn Sie dazu aufgefordert werden.
- 4 Beenden Sie YaST, nachdem Sie alle Fragen beantwortet haben. Ihre Änderungen werden auf die jeweiligen Profile angewendet.

TIPP: Weiterführende Informationen

Weitere Informationen zur Aktualisierung Ihrer Profile über die Systemprotokolle finden Sie in Abschnitt „Updating Profiles from Log Entries“ (Kapitel 3, *Building and Managing Profiles with YaST*, ↑*Novell AppArmor Administration Guide*).

Sicherheit und Vertraulichkeit

33

Eines der grundlegendsten Leistungsmerkmale eines Linux- oder Unix-Systems ist, dass mehrere Benutzer (Multiuser) mehrere Aufgaben zur gleichen Zeit auf demselben Computer (Multitasking) ausführen können. Darüber hinaus ist das Betriebssystem netzwerktransparent. Dies bedeutet, dass Benutzer oftmals gar nicht wissen, ob sich die Daten oder Anwendungen, mit denen sie arbeiten, lokal auf dem Rechner befinden oder über das Netzwerk bereitgestellt werden.

Damit mehrere Benutzer auf einem System arbeiten können, müssen ihre jeweiligen Daten auch voneinander getrennt gespeichert werden können. Sicherheit und der Schutz privater Daten müssen gewährleistet sein. Datensicherheit war auch schon relevant, als Computer noch nicht miteinander vernetzt waren. Bei Verlust oder Defekt der Datenträger (im Allgemeinen Festplatten) mussten wichtige Daten genau wie heute verfügbar sein.

Auch wenn sich dieses Kapitel in der Hauptsache mit der Vertraulichkeit von Daten beschäftigt, sei betont, dass bei einem umfassenden Sicherheitskonzept immer dafür gesorgt werden muss, dass ein regelmäßig aktualisiertes, funktionierendes und getestetes Backup verfügbar ist. Ohne Sicherung kann es äußerst schwierig sein, Daten wiederherzustellen, die durch Hardwaredefekte verloren gehen oder von nicht autorisierten Personen manipuliert werden.

33.1 Lokale Sicherheit und Netzwerksicherheit

Es gibt verschiedene Möglichkeiten, auf Daten zuzugreifen:

- persönliche Kommunikation mit jemandem, der über die gewünschten Informationen verfügt bzw. Zugang zu den Daten auf einem Computer hat
- direkt über die Konsole eines Computers (physischer Zugriff)
- über eine serielle Schnittstelle oder
- über eine Netzwerkverbindung

In allen Fällen sollten sich die Benutzer authentifizieren müssen, bevor sie Zugriff auf die entsprechenden Ressourcen oder Daten erhalten. Ein Webserver mag diesbezüglich weniger restriktiv sein, aber Sie möchten sicherlich nicht, dass er Ihre persönlichen Daten an andere Surfer preisgibt.

Bei dem ersten Fall in der obigen Liste ist die zwischenmenschliche Kommunikation erforderlich. Dies gilt beispielsweise, wenn Sie sich an einen Bankangestellten wenden und nachweisen müssen, dass Sie der rechtmäßige Eigentümer eines bestimmten Kontos sind. Sie werden aufgefordert, eine Unterschrift, eine Signatur, eine PIN oder ein Passwort anzugeben, die bzw. das belegt, dass Sie die Person sind, die Sie vorgeben zu sein. In einigen Fällen ist es möglich, Personen wichtige Informationen zu entlocken, indem man beiläufig einige bekannte Details erwähnt und unter Verwendung geschickter Rhetorik ihr Vertrauen gewinnt. Das Opfer kann so möglicherweise nach und nach dazu gebracht werden, weitere Informationen Preis zu geben, ohne sich dessen bewusst zu sein. Unter Hackern wird dies als *Social Engineering* bezeichnet. Dagegen können Sie sich nur schützen, indem Sie Benutzer aufklären und bewusst mit Sprache und Informationen umgehen. Bevor Angreifer in Computersysteme einbrechen, versuchen sie häufig, Empfangsmitarbeiter, Dienstleister des Unternehmens oder sogar Familienmitglieder anzusprechen. In vielen Fällen werden solche Angriffe, die auf Social Engineering basieren, erst sehr viel später entdeckt.

Ein Person, die unbefugt auf Ihre Daten zugreifen möchte, könnte auch auf herkömmliche Weise versuchen, auf die entsprechende Hardware direkt zuzugreifen. Daher sollte der Computer so geschützt sein, dass niemand dessen Komponenten entfernen, ersetzen und beschädigen kann. Dies gilt auch für Backups sowie Netzwerk- und

Netzkabel. Zudem sollte der Bootvorgang gesichert werden, da hier einige bekannte Tastenkombinationen unerwünschtes Verhalten zur Folge haben könnten. Schützen Sie sich davor, indem Sie Passwörter für das BIOS und den Bootloader einrichten.

An vielen Standorten werden serielle Terminals verwendet, die an serielle Anschlüsse angeschlossen sind. Anders als Netzwerkschnittstellen benötigen diese für die Kommunikation mit dem Host kein Netzwerkprotokoll. Um zwischen den Geräten einfache Zeichen hin und her zu übertragen, wird ein einfaches Kabel oder ein Infrarotanschluss verwendet. Das Kabel selbst ist der schwächste Punkt des Systems. Ist ein älterer Drucker angeschlossen, lässt sich mühelos alles aufzeichnen, was über die Kabel versendet wird. Was mit einem Drucker möglich ist, geht selbstverständlich mit entsprechendem Aufwand auch anders.

Das lokale Lesen einer Datei auf einem lokalen Host unterliegt anderen Zugriffsbeschränkungen als das Öffnen einer Netzwerkverbindung zu einem Dienst auf einem anderen Host. Daher ist es nötig, zwischen lokaler Sicherheit und Netzwerksicherheit zu unterscheiden. Die Trennlinie wird da gezogen, wo Daten in Pakete verschlüsselt werden müssen, um verschickt zu werden.

33.1.1 Lokale Sicherheit

Die lokale Sicherheit beginnt bei der Umgebung, in der der Computer aufgestellt ist. Stellen Sie Ihren Computer so auf, dass das Maß an Sicherheit Ihrem Anspruch und Ihren Anforderungen genügt. Das wichtigste bei der lokalen Sicherheit ist, darauf zu achten, die einzelnen Benutzer voneinander zu trennen, sodass kein Benutzer die Rechte oder die Identität eines anderen Benutzers annehmen kann. Dies gilt für alle Benutzer, besonders aber für den Benutzer `root`, der alle Rechte im System besitzt. `root` kann unter anderem ohne Passwordeingabe die Identität aller Benutzer annehmen und jede lokal gespeicherte Datei lesen.

33.1.2 Passwörter

Auf einem Linux-System werden Passwörter nicht etwa im Klartext gespeichert, damit eingegebene Passwörter mit den gespeicherten verglichen werden können. In einem solchen Fall wären alle Konten auf dem System gefährdet, wenn jemand auf die entsprechende Datei zugreifen könnte. Das gespeicherte Passwort wird stattdessen verschlüsselt und jedes Mal, wenn es eingegeben wird, erneut verschlüsselt. Anschließend werden die beiden verschlüsselten Zeichenketten miteinander verglichen. Dies macht

natürlich nur dann Sinn, wenn man aus dem verschlüsselten Passwort nicht die ursprüngliche Textzeichenkette errechnen kann.

Dies erreicht man durch so genannte *Falltüralgorithmen*, die nur in eine Richtung funktionieren. Ein Angreifer, der das verschlüsselte Passwort in seinen Besitz gebracht hat, kann nicht einfach den Algorithmus erneut anwenden und das Passwort sehen. Stattdessen muss er alle möglichen Zeichenkombinationen für ein Passwort durchprobieren, bis er dasjenige findet, welches verschlüsselt so aussieht wie das Original. Bei acht Buchstaben pro Passwort gibt es ziemlich viele Kombinationen.

In den 1970er Jahren galt diese Methode als sicherer als andere, da der verwendete Algorithmus recht langsam war und Zeit im Sekundenbereich für das Verschlüsseln eines Passworts brauchte. Heutige PCs dagegen schaffen ohne weiteres mehrere hunderttausend bis Millionen Verschlüsselungen pro Sekunde. Aus diesem Grund darf die Passwortdatei nicht für jeden Benutzer sichtbar sein (`/etc/shadow` ist für einen normalen Benutzer nicht lesbar). Noch wichtiger ist, dass Passwörter nicht leicht zu erraten sind, für den Fall, dass die Passwortdatei wegen eines Fehlers doch sichtbar wird. Es hilft daher nicht viel, „ein“ Passwort wie „tantalize“ in „t@nt@1lz3“ umzuschreiben.

Das Ersetzen einiger Buchstaben in einem Wort durch ähnliche Zahlen ist nicht sicher. Dies kann von Knackprogrammen, die Wörterbücher zum Raten verwenden, sehr leicht aufgelöst werden. Besser sind Kombinationen von Buchstaben, die kein bekanntes Wort bilden und nur für den Benutzer eine persönliche Bedeutung haben, etwa die Anfangsbuchstaben der Wörter eines Satzes, z. B. „Der Name der Rose“ von Umberto Eco. Sie erhalten das folgende sichere Passwort „DNdRvUE“. Im Gegensatz dazu können Passwörter wie „Saufkumpan“ oder „Jasmin76“ schon von jemandem erraten werden, der Sie oberflächlich gut kennt.

33.1.3 Der Bootvorgang

Verhindern Sie, dass mit einer Diskette oder einer CD-ROM gebootet werden kann, indem Sie die Laufwerke ausbauen oder indem Sie ein BIOS-Passwort setzen und im BIOS ausschließlich das Booten von Festplatte erlauben. Linux-Systeme werden in der Regel mit einem Bootloader gestartet, der es ermöglicht, zusätzliche Optionen an den gestarteten Kernel weiterzugeben. Um zu verhindern, dass andere Personen diese Parameter während des Bootvorgangs verwenden, können Sie in `/boot/grub/menu.lst` ein zusätzliches Passwort festlegen (siehe **Kapitel 9, *Der Bootloader*** (S. 147)). Dies ist für die Sicherheit des Systems unerlässlich. Nicht nur, weil der Kernel selbst

mit `root`-Berechtigungen läuft, sondern auch weil er `root`-Berechtigungen bei Systemstart vergibt.

33.1.4 Dateiberechtigungen

Es gilt das Prinzip, immer mit den niedrigst möglichen Privilegien für die jeweilige Aufgabe zu arbeiten. Es ist beispielsweise definitiv nicht nötig, seine E-Mails als `root` zu lesen und zu schreiben. Wenn das Mail-Programm, mit dem Sie arbeiten, einen Fehler hat, der für einen Angriff ausgenutzt wird, erfolgt dieser genau mit den Berechtigungen, die Sie zum Zeitpunkt des Angriffs hatten. Durch Anwenden der obigen Regel minimieren Sie also den möglichen Schaden.

Die Berechtigungen der in der openSUSE-Verteilung enthaltenen Dateien wurden sorgfältig ausgewählt. Der Administrator eines Systems sollte zusätzliche Software oder andere Dateien mit größtmöglicher Sorgfalt installieren und besonders gut auf die vergebenen Berechtigungen achten. Erfahrene und sicherheitsbewusste Administratoren verwenden die Option `-l` mit dem Befehl `ls`, um eine detaillierte Dateiliste zu erhalten, anhand der sie eventuell falsch gesetzte Dateiberechtigungen gleich erkennen können. Ein falsch gesetztes Attribut bedeutet nicht nur, dass Dateien überschrieben oder gelöscht werden können. Diese geänderten Dateien könnten vom `root` oder, im Fall von Konfigurationsdateien, von Programmen mit `root`-Berechtigung ausgeführt werden. Damit könnte ein Angreifer beträchtlichen Schaden anrichten. Solche Angriffe werden als Kuckuckseier bezeichnet, weil das Programm (das Ei) von einem fremden Benutzer (Vogel) ausgeführt (ausgebrütet) wird, ähnlich wie der Kuckuck seine Eier von fremden Vögeln ausbrüten lässt.

Ein openSUSE®-System verfügt über die Dateien `permissions`, `permissions.easy`, `permissions.secure` und `permissions.paranoid`, die sich alle im Verzeichnis `/etc` befinden. In diesen Dateien werden besondere Berechtigungen wie etwa allgemein schreibbare Verzeichnisse oder, wie im Fall von Dateien, Setuser-ID-Bits festgelegt. (Programme mit gesetztem Setuser-ID-Bit laufen nicht mit der Berechtigung des Benutzers, der sie gestartet hat, sondern mit der Berechtigung des Eigentümers der Datei. Dies ist in der Regel `root`). Für den Administrator steht die Datei `/etc/permissions.local` zur Verfügung, in der er seine eigenen Einstellungen hinzufügen kann.

Um zu definieren, welche der obigen Dateien von den Konfigurationsprogrammen von openSUSE verwendet werden, um entsprechende Berechtigungen festzulegen, wählen Sie *Lokale Sicherheit* im Abschnitt *Sicherheit und Benutzer* von YaST. Weitere Infor-

mationen zu diesem Thema finden Sie in den Kommentaren in `/etc/permissions` oder auf der `man`-Seite für den Befehl `chmod` (`manchmod`).

33.1.5 Pufferüberläufe und Format-String-Programmfehler

Wann immer ein Programm Daten verarbeiten soll, die von einem Benutzer geändert werden können oder könnten, ist besondere Vorsicht geboten. Diese Vorsicht gilt in der Hauptsache für den Programmierer der Anwendung. Er muss sicherstellen, dass die Daten durch das Programm richtig interpretiert werden und die Daten zu keinem Zeitpunkt in Speicherbereiche geschrieben werden, die eigentlich zu klein sind. Außerdem sollten die Daten in konsistenter Art und Weise vom Programm über die dafür vorgegebenen Schnittstellen weitergereicht werden.

Ein *Pufferüberlauf* kann dann passieren, wenn beim Beschreiben eines Pufferspeicherbereichs nicht darauf geachtet wird, wie groß der Puffer tatsächlich ist. Es kann vorkommen, dass die vom Benutzer generierten Daten etwas mehr Platz erfordern, als im Puffer zur Verfügung steht. Durch dieses Überschreiben des Puffers über seine Grenzen hinaus ist es unter Umständen möglich, dass ein Programm Programmsequenzen ausführt, die vom Benutzer und nicht vom Programmierer generiert wurden, anstatt nur Benutzerdaten zu verarbeiten. Dies ist ein schwerer Fehler, insbesondere wenn das Programm mit besonderen Berechtigungen ausgeführt wird (siehe [Abschnitt 33.1.4, „Dateiberechtigungen“](#) (S. 569)).

Format-String-Programmfehler funktionieren etwas anders, auch hierbei kann über die Benutzereingabe das Programm von seinem eigentlichen Weg abgebracht werden. Diese Programmierfehler werden normalerweise von Programmen ausgenutzt, die mit besonderen Berechtigungen ausgeführt werden, also `setuid`- und `setgid`-Programme. Sie können sich und Ihr System also vor solchen Fehlern schützen, indem Sie die besonderen Ausführungsrechte aus den Programmen entfernen. Auch hier gilt wieder das Prinzip der geringstmöglichen Privilegien (siehe [Abschnitt 33.1.4, „Dateiberechtigungen“](#) (S. 569)).

Da Pufferüberläufe und Format-String-Fehler bei der Verarbeitung von Benutzerdaten auftreten, sind sie nicht notwendigerweise nur ausnutzbar, wenn man bereits Zugriff auf ein lokales Konto hat. Viele der bekannt gewordenen Fehler können auch über eine Netzwerkverbindung ausgenutzt werden. Deswegen sollten Pufferüberläufe und Format-

String-Fehler sowohl für die lokalen Computer als auch für das Netzwerk als sicherheitsrelevant klassifiziert werden.

33.1.6 Viren

Entgegen anders lautenden Behauptungen gibt es tatsächlich Viren für Linux. Die bekannten Viren sind von ihren Autoren als *Proof of Concept* geschrieben worden, d. h. als Beweis, dass die Technik funktioniert. Allerdings ist bis jetzt noch keiner dieser Viren *in freier Wildbahn* beobachtet worden.

Viren benötigen zur Ausbreitung einen Wirt (Host), ohne den sie nicht überlebensfähig sind. In diesem Fall ist der Host ein Programm oder ein wichtiger Speicherbereich für das System, etwa der Master-Boot-Record, und er muss für den Programmcode des Virus beschreibbar sein. Linux hat aufgrund seiner Mehrbenutzer-Funktionalität die Möglichkeit, den Schreibzugriff auf Dateien einzuschränken, was insbesondere für Systemdateien wichtig ist. Wenn Sie bei der Arbeit als `root` angemeldet sind, erhöhen Sie also die Wahrscheinlichkeit, dass Ihr System von solch einem Virus infiziert wird. Berücksichtigen Sie aber die Regel der geringstmöglichen Privilegien, ist es schwierig, unter Linux ein Virus zu bekommen.

Darüber hinaus sollten Sie nie leichtfertig ein Programm ausführen, das Sie aus dem Internet bezogen haben und dessen genaue Herkunft Sie nicht kennen. openSUSE-RPM-Pakete sind kryptographisch signiert und tragen mit dieser digitalen Unterschrift das Markenzeichen der Sorgfalt, mit der die Pakete entwickelt wurden. Viren sind klassische Symptome dafür, dass auch ein hochsicheres System unsicher wird, wenn der Administrator oder auch der Benutzer ein mangelndes Sicherheitsbewusstsein hat.

Viren sind nicht mit Würmern zu verwechseln, die ausschließlich in Netzwerken Probleme verursachen. Sie benötigen keinen Host, um sich zu verbreiten.

33.1.7 Netzwerksicherheit

Die Netzwerksicherheit ist wichtig, um das gesamte System gegen Angriffe von außen zu schützen. Das typische Anmeldeverfahren mit Benutzernamen und Passwort für die Benutzerauthentifizierung gehört weiter zur lokalen Sicherheit. Beim Anmelden über eine Netzwerkverbindung muss zwischen diesen beiden Sicherheitsaspekten differenziert werden: bis zur erfolgten Authentifizierung geht es um Netzwerksicherheit, nach der Anmeldung um lokale Sicherheit.

33.1.8 X Window-System und X-Authentifizierung

Wie bereits erwähnt ist Netzwerktransparenz eine grundlegende Eigenschaft eines Unix-Systems. Bei X, dem Windowing-System von Unix, gilt dies in besonderem Maße. Sie können sich ohne Weiteres auf einem entfernten Computer anmelden und dort ein Programm starten, dessen grafische Oberfläche dann über das Netzwerk auf Ihrem Computer angezeigt wird.

Wenn ein X-Client mithilfe eines X-Servers über das Netzwerk angezeigt werden soll, dann muss der Server die Ressource, die er verwaltet (die Anzeige), vor unberechtigten Zugriffen schützen. Konkret heißt das hier, dass dem Client-Programm bestimmte Berechtigungen gewährt werden müssen. Bei X Windows geschieht dies auf zwei verschiedene Arten: Hostbasierte und Cookie-basierte Zugriffskontrolle. Erstere basiert auf der IP-Adresse des Computers, auf dem das Client-Programm laufen soll. Dies wird mit dem Programm "xhost" gesteuert. xhost trägt eine IP-Adresse eines legitimen Client in eine Mini-Datenbank auf dem X-Server ein. Eine Authentifizierung einzig und allein auf einer IP-Adresse aufzubauen gilt jedoch nicht gerade als sicher. Wenn beispielsweise ein zweiter Benutzer auf dem Host arbeitet, der das Client-Programm sendet, hätte dieser ebenfalls Zugriff auf den X-Server als würde er die IP-Adresse stehlen. Aufgrund dieser Nachteile wird auf diese Authentifizierungsmethode nicht näher eingegangen. Weitere Informationen finden Sie jedoch auf der [Manualpage für xhost](#).

Bei der Cookie-basierten Zugriffskontrolle wird eine Zeichenkette, die nur der X-Server und der berechtigte Benutzer kennen, wie ein Ausweis verwendet. Dieses Cookie (das englische Wort "cookie" bedeutet Keks. Gemeint sind hier die chinesischen Glückskekse, die ein Epigramm enthalten) wird bei der Anmeldung in der Datei `.Xauthority` im Home-Verzeichnis des Benutzers gespeichert und steht somit jedem X-Client, der auf dem X-Server ein Fenster anzeigen möchte, zur Verfügung. Die Datei `.Xauthority` kann vom Benutzer mit dem Programm `xauth` untersucht werden. Wenn Sie `.Xauthority` in Ihrem Home-Verzeichnis versehentlich umbenennen oder löschen, können Sie keine neuen Fenster oder X-Clients mehr öffnen.

Mit SSH (Secure Shell) können Netzverbindungen vollständig verschlüsselt und offen an den X-Server weitergeleitet werden, ohne dass der Benutzer die Verschlüsselung wahrnimmt. Dies wird auch als X-Forwarding bezeichnet. Dabei wird serverseitig ein X-Server simuliert und bei der Shell auf dem entfernten Host die `DISPLAY`-Variable gesetzt. Weitere Informationen zu SSH finden Sie in [Kapitel 29, SSH: Secure Network Operations](#) (S. 517).

WARNUNG

Wenn Sie den Host, auf dem Sie sich anmelden, nicht als sicher einstufen, dann sollten Sie X-Forwarding nicht verwenden. Mit aktiviertem X-Forwarding könnten sich Angreifer über Ihre SSH-Verbindung mit Ihrem X-Server authentifiziert verbinden und beispielsweise Ihre Tastatureingaben abhören.

33.1.9 Pufferüberläufe und Format-String-Programmfehler

Wie in [Abschnitt 33.1.5](#), „Pufferüberläufe und Format-String-Programmfehler“ (S. 570) beschrieben, sollten Pufferüberläufe und Format-String-Fehler sowohl für die lokalen Computer als auch das Netzwerk als sicherheitsrelevant klassifiziert werden. Wie auch bei den lokalen Varianten dieser Programmierfehler nutzen Angreifer Pufferüberläufe bei Netzwerkprogrammen meistens aus, um `root`-Berechtigungen zu erhalten. Selbst wenn dies nicht der Fall ist, könnte sich der Angreifer zumindest Zugang zu einem unprivilegierten lokalen Konto verschaffen, mit dem er dann weitere Schwachstellen ausnutzen kann, sofern diese vorhanden sind.

Über das Netzwerk ausbeutbare Pufferüberläufe und Format-String-Fehler sind wohl die häufigsten Varianten von entfernten Angriffen überhaupt. Über Sicherheits-Mailing-Listen werden so genannte Exploits bekannt gemacht, d. h., Programme, die die gerade entdeckten Sicherheitslücken ausnutzen. Auch jemand, der nicht die genauen Details des Codes kennt, kann damit die Sicherheitslücken ausnutzen. Im Laufe der Jahre hat sich herausgestellt, dass die freie Verfügbarkeit von Exploit-Code generell die Sicherheit von Betriebssystemen erhöht hat, was sicherlich daran liegt, dass Betriebssystemhersteller dazu gezwungen waren, die Probleme in ihrer Software zu beseitigen. Bei kostenloser Software haben alle Benutzer Zugriff auf den Quellcode (im Lieferumfang von openSUSE ist der gesamte verfügbare Quellcode enthalten). Jeder der eine Sicherheitslücke und den entsprechenden Exploit-Code entdeckt, kann ein Patch zur Behebung des entsprechenden Bugs anbieten.

33.1.10 Denial-of-Service

Ein Dienstverweigerungsangriff (Denial of Service, DoS) soll ein Server-Programm oder sogar ein gesamtes System blockieren. Dies kann durch verschiedene Methoden erreicht werden: Überbelastung des Servers, Auslastung des Servers mit Garbage-

Paketen oder Ausnutzen eines Remote-Puffer-Überlaufs. Der Zweck eines DoS-Angriffs ist häufig, dafür zu sorgen, dass der Dienst nicht mehr verfügbar ist. Wenn ein bestimmter Dienst jedoch fehlt, kann die Kommunikation Angriffen wie *Man-in-the-Middle-Angriffen* (Sniffing, TCP-Connection-Hijacking, Spoofing) und DNS-Poisoning ausgesetzt sein.

33.1.11 Man in the Middle: Sniffing, Hijacking, Spoofing

Im Allgemeinen wird ein Remote-Angriff, bei dem der Angreifer zwischen zwei kommunizierenden Hosts positioniert ist, als *Man-in-the-Middle-Angriff* bezeichnet. Solche Angriffe haben in der Regel eines gemeinsam: Das Opfer merkt nichts davon. Viele Varianten sind denkbar, z. B.: Der Angreifer nimmt eine Verbindungsanforderung entgegen und stellt selbst eine Verbindung zum Ziel her. Das Opfer hat also, ohne es zu wissen, eine Netzwerkverbindung zum falschen Host geöffnet, weil dieser sich als das Ziel ausgibt.

Die einfachste Form des "Man-in-the-Middle-Angriff" wird als *Sniffer* bezeichnet. Dabei überwacht der Angreifer „lediglich“ den im Netzwerk übertragenen Datenverkehr. Komplexer wird es, wenn der „Man-in-the-Middle“-Angreifer versucht, eine bereits eingerichtete Verbindung zu übernehmen (Connection-Hijacking). Dafür muss der Angreifer die Pakete, die an ihm vorbeigeführt werden, eine Weile analysiert haben, damit er die richtigen TCP-Sequenznummern der TCP-Verbindung vorhersagen kann. Wenn er dann die Rolle des Zielhosts der Verbindung übernimmt, merkt das das Opfer, weil es die Meldung erhält, dass die Verbindung wegen eines Fehlers beendet wird. Der Angreifer profitiert dabei insbesondere bei Protokollen, die nicht kryptographisch gegen Hijacking gesichert sind und bei denen zu Beginn der Verbindung nur eine einfache Authentifizierung stattfindet.

Spoofing ist ein Angriff, bei dem Pakete mit falschen Absenderdaten, in der Regel der IP-Adresse, versendet werden. Bei den meisten aktiven Angriffsvarianten müssen solche gefälschten Pakete versendet werden. Unter Linux darf dies nur der Superuser (`root`).

Viele der hier erwähnten Angriffsmöglichkeiten kommen in Kombination mit einem DoS vor. Gibt es eine Möglichkeit, einen Rechner abrupt vom Netzwerk zu trennen (wenn auch nur für kurze Zeit), dann wirkt sich das förderlich auf einen aktiven Angriff aus, weil seitens des Hosts keine Störungen des Angriffs mehr erwartet werden müssen.

33.1.12 DNS-Poisoning

Beim DNS-Poisoning versucht der Angreifer, mit gefälschten (gespoofen) DNS-Antwortpaketen den Cache eines DNS-Servers zu "vergiften" (poisoning), sodass dieser bestimmte Daten an ein Opfer weitergibt, das Informationen vom Server anfordert. Viele Server haben, basierend auf IP-Adressen oder Hostnamen, ein verbürgtes Verhältnis zu anderen Hosts. Der Angreifer benötigt allerdings gute Kenntnisse der Vertrauensstruktur zwischen diesen Hosts, um sich selbst als einer der verbürgten Hosts ausgeben zu können. Der Angreifer analysiert in der Regel einige vom Server gesendete Pakete, um die erforderlichen Informationen zu erhalten. Ein zeitlich genau abgestimmter DoS-Angriff gegen den Namensserver ist aus Sicht des Angreifers ebenfalls unerlässlich. Sie können sich selbst schützen, indem Sie verschlüsselte Verbindungen verwenden, die die Identität des Zielhosts der Verbindung verifizieren können.

33.1.13 Würmer

Würmer werden häufig mit Viren gleichgesetzt. Es gibt aber einen markanten Unterschied. Anders als Viren müssen Würmer kein Hostprogramm infizieren, um überleben zu können. Stattdessen sind sie darauf spezialisiert, sich so schnell wie möglich in Netzwerken zu verbreiten. Bekannte Würmer wie Ramen, Lion oder Adore nutzen bekannte Sicherheitslücken von Serverprogrammen wie bind8 oder lprNG. Man kann sich relativ einfach gegen Würmer schützen. Weil zwischen dem Zeitpunkt des Bekanntwerdens der Sicherheitslücken bis zum Auftauchen des Wurms auf dem Server in der Regel einige Zeit vergeht, ist es gut möglich, dass dann bereits Update-Versionen des betroffenen Programms zur Verfügung stehen. Natürlich setzt dies voraus, dass der Administrator die Sicherheits-Updates auch auf den entsprechenden Systemen installiert.

33.2 Tipps und Tricks: Allgemeine Hinweise zur Sicherheit

Für einen kompetenten Umgang mit dem Bereich Sicherheit ist es nötig, mit neuen Entwicklungen Schritt zu halten und auf dem Laufenden zu sein, was die neuesten Sicherheitsprobleme angeht. Ein sehr guter Schutz gegen Fehler aller Art ist das schnellstmögliche Installieren von Update-Paketen, die in Sicherheitsmitteilungen empfohlen werden. SUSE-Sicherheitsmitteilungen werden in der Liste

opensuse-security-announce@opensuse.org veröffentlicht. Die Liste, die u. a. von Mitgliedern des SUSE-Sicherheitsteams erstellt wird, ist eine Informationsquelle für Update-Pakete aus erster Hand. Sie können die Liste auf Seite <http://en.opensuse.org/Communicate/Mailinglists> abonnieren.

Diese Mailingliste opensuse-security@opensuse.org ist ein informatives Diskussionsforum für den Bereich Sicherheit. Sie können sie auf derselben Webseite abonnieren.

bugtraq@securityfocus.com ist eine der bekanntesten Sicherheits-Mailinglisten der Welt. Die Lektüre dieser Liste mit durchschnittlich 15-20 Beiträgen am Tag wird empfohlen. Weitere Informationen finden Sie unter <http://www.securityfocus.com>.

Im Folgenden sind einige Grundregeln für die Sicherheit aufgeführt:

- In Übereinstimmung mit dem Prinzip, immer nur mit den eingeschränktesten Berechtigungen für die einzelnen Aufgaben zu arbeiten, sollten Sie Ihre täglichen Routine-Aufgaben nicht als `root` erledigen. Das verringert das Risiko, sich ein Kuckucksei oder einen Virus einzufangen, und schützt Sie vor eigenen Fehlern.
- Verwenden Sie nach Möglichkeit immer verschlüsselte Verbindungen, um Arbeiten von einem entfernten Standort aus durchzuführen. Verwenden Sie standardmäßig `ssh` (secure shell) anstelle von `telnet`, `ftp`, `rsh` und `rlogin`.
- Benutzen Sie keine Authentifizierungsmethoden, die allein auf der IP-Adresse basieren.
- Halten Sie Ihre wichtigsten Pakete für den Netzwerkbereich immer auf dem neuesten Stand und abonnieren Sie die entsprechenden Mailinglisten, um neue Versionen der jeweiligen Software (`bind`, `postfix`, `ssh` usw.) zu erhalten. Dasselbe gilt für Software, die nur lokale Sicherheitsrelevanz hat.
- Optimieren Sie die Zugriffsrechte für sicherheitskritische Dateien im System, indem Sie die Datei `/etc/permissions` an die Sicherheitsanforderungen des Systems anpassen. Wenn Sie das `setuid`-Bit aus einem Programm entfernen, kann dieses seine Aufgabe möglicherweise nicht mehr ordnungsgemäß erledigen. Auf der anderen Seite stellt das Programm dann aber in der Regel auch kein Sicherheitsproblem mehr dar. Mit einer ähnlichen Vorgehensweise können Sie auch allgemein schreibbare Dateien (Berechtigungsstufe "world") und Verzeichnisse bearbeiten.

- Deaktivieren Sie jegliche Netzwerkdienste, die Sie auf Ihrem Server nicht zwingend brauchen. Das macht Ihr System sicherer. Offene Ports (mit Socket-Status LISTEN) finden Sie mit dem Programm `netstat`. Als Optionen bieten sich `netstat -ap` oder `netstat -anp` an. Mit der Option `-p` können Sie sehen, welcher Prozess einen Port unter welchem Namen belegt.

Vergleichen Sie die Ergebnisse von `netstat` mit einem vollständigen Portscan des Hosts von außen. Das Programm `nmap` ist dafür hervorragend geeignet. Es überprüft nicht nur jeden einzelnen Port des Hosts, sondern kann anhand der Antwort des Hosts Schlüsse über einen hinter dem Port wartenden Dienst ziehen. Scannen Sie niemals einen Rechner ohne das direkte Einverständnis des Administrators, denn dies könnte als aggressiver Akt aufgefasst werden. Denken Sie daran, dass Sie nicht nur TCP-Ports scannen sollten, sondern auf jeden Fall auch UDP-Ports (Optionen `-sS` und `-sU`).

- Um die Integrität der Dateien in Ihrem System zuverlässig zu überwachen, verwenden Sie das Programm `AIDE` (Advanced Intrusion Detection Environment), das unter openSUSE verfügbar ist. Verschlüsseln Sie die von AIDE erstellte Datenbank, um unbefugte Zugriffe auf diese zu verhindern. Bewahren Sie außerdem ein Backup dieser Datenbank an einem sicheren Ort auf. Verwenden Sie dazu jedoch ein externes Speichermedium, das nicht über eine Netzwerkverbindung mit Ihrem Computer verbunden ist.
- Seien Sie vorsichtig beim Installieren von Drittanbietersoftware. Es gab schon Fälle, wo ein Angreifer tar-Archive einer Sicherheitssoftware mit einem trojanischen Pferd versehen hat. Zum Glück wurde dies schnell bemerkt. Wenn Sie ein Binärpaket installieren, sollten Sie sicher sein, woher das Paket kommt.

SUSE-RPM-Pakete sind mit GPG signiert. Der von SUSE zum Signieren verwendete Schlüssel lautet wie folgt:

```
ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
```

Der Befehl `rpm --checksig package.rpm` zeigt an, ob die Prüfsumme und die Signatur eines (nicht installierten) Pakets korrekt sind. Sie finden den Schlüssel auf der ersten CD der Distribution oder auf den meisten Schlüsselserversn der Welt.

- Überprüfen Sie regelmäßig die Backups der Benutzer- und Systemdateien. Ohne eine zuverlässige Aussage über die Qualität des Backups ist das Backup unter Umständen wertlos.

- Überprüfen Sie die Protokolldateien. Nach Möglichkeit sollten Sie sich ein kleines Skript schreiben, welches die Protokolldateien nach ungewöhnlichen Einträgen absucht. Diese Aufgabe ist alles andere als trivial. Schließlich wissen nur Sie, was ungewöhnlich ist und was nicht.
- Verwenden Sie `tcp_wrapper`, um den Zugriff auf die einzelnen Dienste Ihres Computers einzuschränken, und explizit anzugeben, welchen IP-Adressen der Zugriff gestattet ist. Weitere Informationen zu `tcp_wrapper` finden Sie auf den man-Seiten zu `tcpd` und `hosts_access` (`man 8 tcpd`, `man hosts_access`).
- Verwenden Sie `SUSEfirewall`, um die durch `tcpd` (`tcp_wrapper`) zur Verfügung gestellte Sicherheit zu verbessern.
- Entwickeln Sie redundante Sicherheitsmaßnahmen: Eine doppelt angezeigte Meldung ist besser als keine Meldung.

33.3 Zentrale Adresse für die Meldung von neuen Sicherheitsproblemen

Wenn Sie ein Sicherheitsproblem finden (bitte überprüfen Sie zunächst die zur Verfügung stehenden Update-Pakete), schreiben Sie an die E-Mail-Adresse security@suse.de. Bitte fügen Sie eine genaue Beschreibung des Problems bei, zusammen mit den Versionsnummern der verwendeten Pakete. SUSE bemüht sich, Ihnen so schnell wie möglich zu antworten. Eine `pgp`-Verschlüsselung Ihrer E-Mail ist erwünscht. SUSE verwendet folgenden PGP-Schlüssel:

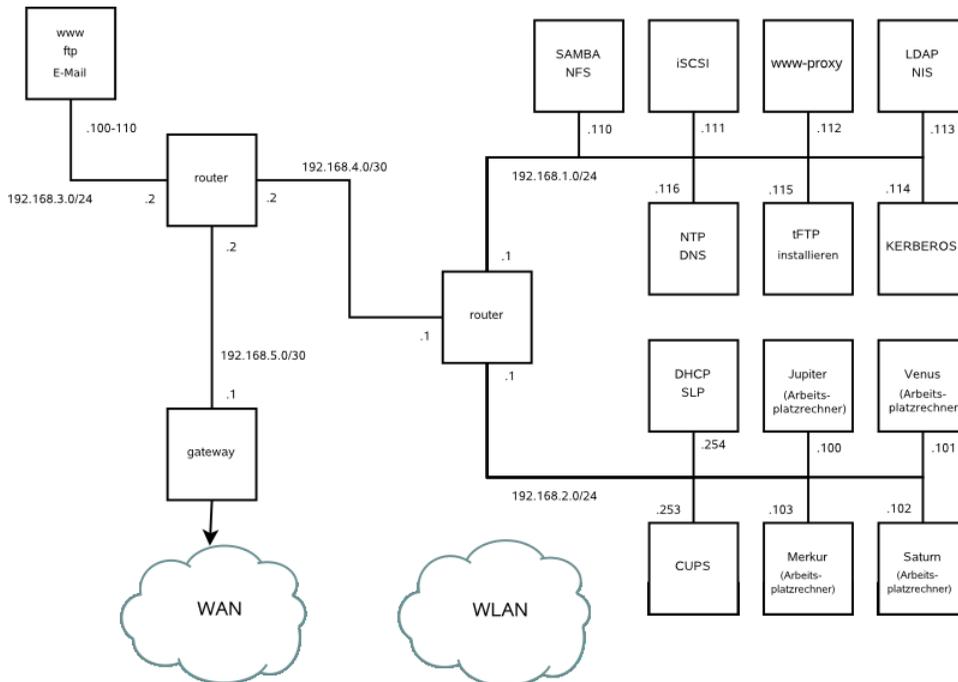
```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

Dieser Schlüssel kann auch unter folgender URL heruntergeladen werden: <http://www.novell.com/linux/security/securitysupport.html>.



Ein Beispielnetzwerk

Dieses Beispielnetzwerk wird in der openSUSE®-Dokumentation in allen Kapiteln verwendet, die sich mit Netzwerken befassen.





GNU Licenses

This appendix contains the GNU General Public License and the GNU Free Documentation License.

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does. Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w`. This is free software, and you are welcome
to redistribute it under certain conditions; type `show c`
for details.
```

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.
```

```
signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License [<http://www.fsf.org/licenses/lgpl.html>] instead of this License.

GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “Document”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “you”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “Modified Version” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “Secondary Section” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “Invariant Sections” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “Cover Texts” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “Transparent” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “Opaque”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “Title Page” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section “Entitled XYZ” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “Acknowledgements”, “Dedications”, “Endorsements”, or “History”.) To “Preserve the Title” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or of the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled “History” in the various original documents, forming one section Entitled “History”; likewise combine any sections Entitled “Acknowledgements”, and any sections Entitled “Dedications”. You must delete all sections Entitled “Endorsements”.

COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright (c) YEAR YOUR NAME.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 only as published by the Free Software Foundation; with the Invariant Section being this copyright notice and license. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.