

openSUSE

10.3

www.novell.com

07. November 2007

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	xiii
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	13
1.3 Vorbereitung des Bootvorgangs für das Zielsystem	24
1.4 Booten des Zielsystems für die Installation	35
1.5 Überwachen des Installationsvorgangs	47
2 Fortgeschrittene Festplattenkonfiguration	51
2.1 Verwenden der YaST-Partitionierung	51
2.2 LVM-Konfiguration	60
2.3 Soft-RAID-Konfiguration	68
Teil II Verwaltung	75
3 Online-Update	77
3.1 YaST-Online-Update	77
3.2 Aktualisierung über die Kommandozeile mit zypper	80
4 YaST im Textmodus	83
4.1 Navigation in Modulen	84
4.2 Einschränkung der Tastenkombinationen	86

4.3	YaST-Kommandozeilenoptionen	87
5	Aktualisieren des Systems und Systemänderungen	89
5.1	Aktualisieren des Systems	89
5.2	Software-Änderungen von Version zu Version	92
6	RPM – der Paket-Manager	101
6.1	Prüfen der Authentizität eines Pakets	102
6.2	Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren	102
6.3	RPM und Patches	104
6.4	Delta-RPM-Pakete	105
6.5	RPM Abfragen	106
6.6	Installieren und Kompilieren von Quellpaketen	109
6.7	Kompilieren von RPM-Paketen mit "build"	112
6.8	Werkzeuge für RPM-Archive und die RPM-Datenbank	112
7	Druckerbetrieb	115
7.1	Work-Flow des Drucksystems	117
7.2	Methoden und Protokolle zum Anschließen von Druckern	117
7.3	Installation der Software	118
7.4	Netzwerkdrucker	119
7.5	Grafische Bedienoberflächen für das Drucken	122
7.6	Drucken über die Kommandozeile	123
7.7	Spezielle Funktionen in openSUSE	123
7.8	Fehlersuche	127
8	Das X Window-System	137
8.1	Manuelles Konfigurieren des X Window-Systems	137
8.2	Installation und Konfiguration von Schriften	144
8.3	Weiterführende Informationen	150
9	Xen-Virtualisierung	151
9.1	Hauptkomponenten	151
9.2	Einrichten eines virtuellen Computerhosts	155
9.3	Einrichten virtueller Computer	160
9.4	Verwalten einer Virtualisierungsumgebung	167
10	Dienstprogramme zur Systemüberwachung	173
10.1	Fehlersuche	174

10.2	Dateien und Dateisysteme	176
10.3	Hardware-Informationen	178
10.4	Netzwerke	181
10.5	Das Dateisystem <code>/proc</code>	182
10.6	Vorgänge	186
10.7	Systemangaben	190
10.8	Benutzerinformationen	195
10.9	Zeit und Datum	195
Teil III System		197
11 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung		
199		
11.1	Laufzeitunterstützung	199
11.2	Software-Entwicklung	200
11.3	Software-Kompilierung auf Doppelarchitektur-Plattformen	201
11.4	Kernel-Spezifikationen	202
12 Booten und Konfigurieren eines Linux-Systems		203
12.1	Der Linux-Bootvorgang	203
12.2	Der init-Vorgang	207
12.3	Systemkonfiguration über <code>/etc/sysconfig</code>	217
13 Der Bootloader		221
13.1	Auswählen eines Bootloaders	222
13.2	Booten mit GRUB	222
13.3	Konfigurieren des Bootloaders mit YaST	232
13.4	Deinstallieren des Linux-Bootloaders	237
13.5	Erstellen von Boot-CDs	237
13.6	Der grafische SUSE-Bildschirm	239
13.7	Fehlersuche	240
13.8	Weiterführende Informationen	241
14 Spezielle Systemfunktionen		243
14.1	Informationen zu speziellen Softwarepaketen	243
14.2	Virtuelle Konsolen	250
14.3	Tastaturzuordnung	251
14.4	Sprach- und länderspezifische Einstellungen	252

15	Gerätemanagemet über dynamischen Kernel mithilfe von udev	257
15.1	Das /dev-Verzeichnis	257
15.2	Kernel-uevents und udev	258
15.3	Treiber, Kernel-Module und Geräte	258
15.4	Booten und erstes Einrichten des Geräts	259
15.5	Überwachen des aktiven udev-Daemons	260
15.6	Einflussnahme auf das Gerätemanagemet über dynamischen Kernel mithilfe von udev-Regeln	261
15.7	Permanente Gerätebenennung	269
15.8	Von udev verwendete Dateien	270
15.9	Weiterführende Informationen	270
16	Dateisysteme in Linux	273
16.1	Terminologie	273
16.2	Wichtige Dateisysteme in Linux	274
16.3	Weitere unterstützte Dateisysteme	280
16.4	Large File Support unter Linux	281
16.5	Weiterführende Informationen	282
17	Zugriffssteuerungslisten unter Linux	285
17.1	Traditionelle Dateiberechtigungen	285
17.2	Vorteile von ACLs	287
17.3	Definitionen	288
17.4	Arbeiten mit ACLs	288
17.5	ACL-Unterstützung in Anwendungen	298
17.6	Weiterführende Informationen	298
18	Authentifizierung mit PAM	299
18.1	Struktur einer PAM-Konfigurationsdatei	300
18.2	PAM-Konfiguration von sshd	302
18.3	Konfigurieren von PAM mit pam-config	305
18.4	Weiterführende Informationen	306
19	Arbeiten mit der Shell	309
19.1	Verwenden der Bash-Shell	309
19.2	Benutzer und Zugriffsberechtigungen	316
19.3	Wichtige Linux-Befehle	320
19.4	Der vi-Editor	332

Teil IV Services 337

20 Grundlegendes zu Netzwerken 339

20.1	IP-Adressen und Routing	342
20.2	IPv6 – Das Internet der nächsten Generation	345
20.3	Namensauflösung	355
20.4	Konfigurieren von Netzwerkverbindungen mit YaST	357
20.5	Manuelle Netzwerkkonfiguration	376
20.6	smpppd als Einwählhelfer	391

21 SLP-Dienste im Netzwerk 395

21.1	Installation	395
21.2	SLP aktivieren	396
21.3	SLP-Frontends in openSUSE	396
21.4	Installation über SLP	397
21.5	Bereitstellen von Diensten über SLP	397
21.6	Weiterführende Informationen	398

22 Domain Name System (DNS) 399

22.1	DNS-Terminologie	399
22.2	Installation	400
22.3	Konfiguration mit YaST	401
22.4	Starten des Namensservers BIND	408
22.5	Die Konfigurationsdatei /etc/dhcpd.conf	410
22.6	Zonendateien	415
22.7	Dynamische Aktualisierung von Zonendaten	420
22.8	Sichere Transaktionen	420
22.9	DNS-Sicherheit	422
22.10	Weiterführende Informationen	423

23 DHCP 425

23.1	Konfigurieren eines DHCP-Servers mit YaST	426
23.2	DHCP-Softwarepakete	437
23.3	Der DHCP-Server dhcpd	438
23.4	Weiterführende Informationen	442

24 Zeitsynchronisierung mit NTP 443

24.1	Konfigurieren eines NTP-Client mit YaST	443
24.2	Konfigurieren von xntp im Netzwerk	448
24.3	Einrichten einer lokalen Referenzuhr	449

25	Arbeiten mit NIS	451
25.1	Konfigurieren von NIS-Servern	451
25.2	Konfigurieren von NIS-Clients	458
26	LDAP – Ein Verzeichnisdienst	461
26.1	LDAP und NIS	462
26.2	Struktur eines LDAP-Verzeichnisbaums	463
26.3	Konfigurieren eines LDAP-Servers mit YaST	467
26.4	Konfigurieren eines LDAP-Client mit YaST	473
26.5	Konfigurieren von LDAP-Benutzern und -Gruppen in YaST	480
26.6	Navigieren in der LDAP-Verzeichnisstruktur	482
26.7	Manuelles Konfigurieren eines LDAP-Servers	483
26.8	Manuelles Verwalten von LDAP-Daten	490
26.9	Weiterführende Informationen	494
27	Unterstützung für Active Directory	497
27.1	Integration von Linux- und AD-Umgebungen	497
27.2	Hintergrundinformationen zur AD-Unterstützung unter Linux	498
27.3	Konfigurieren eines Linux-Client für Active Directory	504
27.4	Anmeldung bei einer AD-Domäne	507
27.5	Ändern von Passwörtern	509
28	Verteilte Nutzung von Dateisystemen mit NFS	513
28.1	Konfiguration des NFS-Client	514
28.2	Exportieren von Dateisystemen über NFS	518
28.3	Manuelles Exportieren von Dateisystemen	523
28.4	NFS mit Kerberos	526
28.5	Weiterführende Informationen	527
29	Samba	529
29.1	Terminologie	529
29.2	Installieren eines Samba-Servers	531
29.3	Starten und Stoppen von Samba	531
29.4	Konfigurieren eines Samba-Servers	531
29.5	Konfigurieren der Clients	538
29.6	Samba als Anmeldeserver	539
29.7	Weiterführende Informationen	540

30 Der HTTP-Server Apache **543**

30.1	Kurzanleitung	543
30.2	Konfigurieren von Apache	545
30.3	Starten und Beenden von Apache	561
30.4	Installieren, Aktivieren und Konfigurieren von Modulen	563
30.5	Aktivieren von CGI-Skripten	572
30.6	Einrichten eines sicheren Webservers mit SSL	575
30.7	Vermeiden von Sicherheitsproblemen	582
30.8	Fehlersuche	584
30.9	Weiterführende Informationen	585

31 Einrichten eines FTP-Servers mit YaST **589**

31.1	Starten des FTP-Servers	590
31.2	Allgemeine FTP-Einstellungen	591
31.3	FTP-Leistungseinstellungen	591
31.4	Authentifizierung	592
31.5	Einstellungen für Experten	592
31.6	Weitere Informationen	593

Teil V Mobilität **595**

32 Energieverwaltung **597**

32.1	Energiesparfunktionen	597
32.2	ACPI	599
32.3	Ruhezustand für Festplatte	607
32.4	Das Powersave-Paket	609

33 Drahtlose Kommunikation **617**

33.1	Wireless LAN	617
33.2	Bluetooth	629
33.3	Infrarot-Datenübertragung	637

34 Verwenden von Tablet PCs **641**

34.1	Installieren der Tablet PC-Pakete	642
34.2	Konfigurieren des Tablet-Geräts	643
34.3	Verwenden der virtuellen Tastatur	644
34.4	Drehen der Ansicht	644
34.5	Verwenden der Bewegungserkennung	645
34.6	Aufzeichnen von Notizen und Skizzen mit dem Pen	646
34.7	Fehlersuche	648

34.8	Weiterführende Informationen	649
Teil VI	Sicherheit	651
35	Masquerading und Firewalls	653
35.1	Paketfilterung mit iptables	653
35.2	Grundlegendes zum Masquerading	656
35.3	Grundlegendes zu Firewalls	658
35.4	SuSEfirewall2	659
35.5	Weiterführende Informationen	665
36	SSH – sichere Netzwerkoperationen	667
36.1	Das Paket OpenSSH	668
36.2	Das ssh-Programm	668
36.3	scp – Sichere Kopie	669
36.4	sftp – Sichere Dateiübertragung	669
36.5	Der SSH-Daemon (sshd) –Serverseite	670
36.6	SSH-Authentifizierungsmechanismen	671
36.7	X-, Authentifizierungs- und Weiterleitungsmechanismen	672
36.8	Konfigurieren eines SSH-Daemons mit YaST	674
37	Verwalten der X.509-Zertifizierung	677
37.1	Prinzipien der digitalen Zertifizierung	677
37.2	YaST-Module für die Verwaltung von Zertifizierungsstellen	682
38	Netzwerk-Authentifizierung – Kerberos	695
38.1	Kerberos-Terminologie	695
38.2	Funktionsweise von Kerberos	697
38.3	Benutzeransicht von Kerberos	701
38.4	Weiterführende Informationen	702
39	Installation und Administration von Kerberos	703
39.1	Kerberos-Netzwerktopologie	704
39.2	Auswählen der Kerberos-Bereiche	705
39.3	Einrichten der KDC-Hardware	706
39.4	Konfiguration der Zeitsynchronisierung	707
39.5	Konfigurieren des KDC	708
39.6	Konfigurieren von Kerberos-Clients	711
39.7	Konfigurieren der Kerberos-Remoteverwaltung	717

39.8	Erstellen der Kerberos-Dienst-Prinzipale	719
39.9	Aktivieren der PAM-Unterstützung für Kerberos	721
39.10	Konfigurieren von SSH für die Kerberos-Authentifizierung	722
39.11	Verwenden von LDAP und Kerberos	723
40	Verschlüsseln von Partitionen und Dateien	727
40.1	Einrichten von verschlüsselten Dateisystemen mit YaST	728
40.2	Verwenden von verschlüsselten Home-Verzeichnissen	732
40.3	Verschlüsselung einzelner Dateien mit vi	733
41	Einschränken von Berechtigungen mit AppArmor	735
41.1	Installieren von Novell AppArmor	736
41.2	Aktivieren und Deaktivieren von Novell AppArmor	737
41.3	Einführung in die Erstellung von Anwendungsprofilen	738
42	Sicherheit und Vertraulichkeit	747
42.1	Lokale Sicherheit und Netzwerksicherheit	748
42.2	Tipps und Tricks: Allgemeine Hinweise zur Sicherheit	757
42.3	Zentrale Adresse für die Meldung von neuen Sicherheitsproblemen . . .	760
A	Ein Beispielnetzwerk	761
B	GNU Licenses	763
B.1	GNU General Public License	763
B.2	GNU Free Documentation License	766
Index		771

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-System aktualisieren und konfigurieren und Ihr System von einem entfernten Standort aus 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

Dieser Abschnitt enthält eine Einführung in die mobile Computernutzung mit openSUSE. Außerdem erfahren Sie, wie Sie die zahlreichen Optionen für die drahtlose Computernutzung, die Energieverwaltung und die Profilverwaltung konfigurieren.

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.

KDE User Guide

Gibt eine Einführung in den KDE-Desktop von openSUSE und in die verschiedenen darin enthaltenen Anwendungen. Es begleitet Sie durch die Nutzung dieser Anwendungen und hilft Ihnen bei der Erledigung von wichtigen Aufgaben. Es richtet sich in erster Linie an Endbenutzer, die KDE effizient im Alltag nutzen möchten.

GNOME Quick Start

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

GNOME User Guide

Stellt den GNOME-Desktop für openSUSE sowie eine Vielzahl von Anwendungen vor, die Ihnen bei der Arbeit mit dem GNOME-Desktop begegnen. Es begleitet Sie durch die Nutzung dieser Anwendungen und hilft Ihnen bei der Erledigung von

wichtigen Aufgaben. Es richtet sich in erster Linie an Endbenutzer, die den GNOME-Desktop und darauf ausgeführte Anwendungen effizient im Alltag nutzen möchten.

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-Distribution. Ein Snapshot des von der Open Source-Community verfassten Handbuchs wird zusammen mit den Novell/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/opensuse103/>. 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, einer Untermenge 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

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 vollautomatische 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. 13) 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. 22).
- 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. 35) 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 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. 47) 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. 13) 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. 22).
- 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. 35) 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 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. 47) 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. 13) 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. 22) 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. 26) 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. 47) 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. 13) 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. 22).

- 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 1.4.3, „Benutzerdefinierte Boot-Optionen“](#) (S. 38) 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. 49) 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. 13) 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. 22).
- 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 1.4.3, „Benutzerdefinierte Boot-Optionen“** (S. 38).

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. 49) 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. 13) 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. 22).
- 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. 26) 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. 49) 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. 22).

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 28, Verteilte Nutzung von Dateisystemen mit NFS** (S. 513).

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. 35).

- 7 Laden Sie die Installationsdaten hoch. Der die meiste Zeit in Anspruch nehmende Schritt bei der Konfiguration eines Installationservers 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 Konfiguratio-

nen 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 `/Productversion` 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 Domännennamen 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 *instquelle* 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 21, SLP-Dienste im Netzwerk** (S. 395).

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. 16) 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 *instquelle* 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 *Pfad_zur_Instquelle* und *Instquelle* 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 *instquelle* 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 31, Einrichten eines FTP-Servers mit YaST** (S. 589) 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. 16) 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 30.1.2, „Installation“** (S. 544) 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 *instquelle* 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 Netzwerkconfiguration 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 Freigabenamen (`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. 16), [Abschnitt 1.2.3, „Manuelles Einrichten einer FTP-Installationsquelle“](#) (S. 19) 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. 16), [Abschnitt 1.2.3, „Manuelles Einrichten einer FTP-Installationsquelle“](#) (S. 19) oder [Abschnitt 1.2.4, „Manuelles Einrichten einer HTTP-Installationsquelle“](#) (S. 21) beschrieben.

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

Ein DHCP-Server wird auf openSUSE eingerichtet, indem Sie die entsprechenden Konfigurationsdateien manuell bearbeiten. In diesem Abschnitt wird beschrieben, wie eine vorhandene DHCP-Serverkonfiguration erweitert wird, sodass sie die für eine TFTP-, PXE- und WOL-Umgebung erforderlichen Daten zur Verfügung stellt.

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/tftpboot
    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 `/tftpbboot` 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/tftpbboot` und `/srv/tftpbboot/pxelinux.cfg`, sofern sie noch nicht vorhanden sind.
- 3 Fügen Sie wie in **Abschnitt 1.3.3, „Verwenden von PXE Boot“** (S. 28) 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/tftpbboot
    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. 35).

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 `sshpasword` zum Eintrag `install` hinzu. Die durch \ getrennten Zeilen müssen als fortlaufende Zeile ohne Zeilenumbruch 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 harddisk
    localboot 0

implicit      0
display      message
prompt       1
timeout      100

```

Ersetzen Sie *ip_instserver* und *Pfad_instquelle* 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.

	Beschreibung
--	---------------------

- | | |
|---|---|
| 0 | Führt einen normalen Bootvorgang aus |
| 4 | Führt einen lokalen Bootvorgang mit dem noch im Arbeitsspeicher vorhandenen UNDI-Treiber (Univer- |

 Beschrei- ung
sal Network Driver Inter- face) aus
5 Führt einen lokalen Bootvor- gang mit dem gesam- ten PXE- Stack, ein- schließlich des UNDI- Treibers aus, der sich im Arbeitsspei- cher befin- det

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_Ziel` 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. 28) 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*. Weitere Informationen zu Fehlerbehebung beim Installationsvorgang finden Sie in Abschnitt „Probleme bei der Installation“ (Kapitel 13, *Häufige Probleme und deren Lösung*, ↑Start).

1.4.2 F-Tasten

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 1.4.3, „Benutzerdefinierte Boot-Optionen“](#) (S. 38)).

Die verfügbaren Optionen finden Sie in der folgenden Tabelle.

Tabelle 1.1 *F-Tasten bei der Installation*

Tasten	Beschreibung	Verfügbare Optionen
F1	Bietet Hilfe	Keine
F2	Wählen Sie eine Sprache für die Installation aus	Alle unterstützten Sprachen

Tasten	Beschreibung	Verfügbare Optionen
F3	Ändert die Bildschirmauflösung für die Installation	<ul style="list-style-type: none"> • Expertenmodus • VESA • Auflösung 1 • Auflösung 2 • ...
F4	Wählt die Installationsquelle	<ul style="list-style-type: none"> • CD-ROM oder DVD • SLP • FTP • HTTP • NFS • SMB • Festplatte
F5	Wählen Sie die entsprechenden Kernel-Optionen aus.	<ul style="list-style-type: none"> • Standard • Keine ACPI • Keine lokale ACPI • Installations—ACPI deaktiviert • Installations—Sicherheits-einstellungen
F6	Führt die Treiberaktualisierung von Diskette aus	Treiber

la-ti-tu-di-nem Boot-
tionem

<i>ti-</i>	ten
<i>on</i>	b
<i>mit</i>	e
<i>YST</i>	a
(S)	han
	sh

Ad	-serd	infir
En	e s	frü
fa-	s e d	Pfad
de	-latsl	_zu
ht	- a l	<u>Freim</u>
la-	- i t.	reife
ti-	- sno	same
on	- res	<u>reife</u>
mit	s rev	(nur
et-	-zt eN	erfor
fin-	-kr ew	der-
ten	- e g	lich,
Zuf	t ä r	wenn
thr	- P I	meh-
VC	-serd	rere
-	e s	Netz
Sa-	-zt eN	wek-
ti-	- s am	
ste	e k	

Id **n** Boot-
la **m** Optio-
ti **B** nen
os **v**
ze **g**
m **f**
io **d**
i
h
R
ra
t

~~de~~ -latnI _zu
~~Int~~ - a l kein
~~la~~ - i t• vnc=1
~~ti~~ - sno• was
~~on~~ - res same
~~mit~~ s rev was
~~ent~~ - CNV
~~fm~~ - i tLA
~~tm~~ - e i v
~~Zuf~~ gnur
~~übr~~ - CNV
~~VC~~ -ssaP
 — t r ow
~~Dya~~
~~mi~~
~~ste~~
~~Nz~~
~~vek~~
~~kn~~
~~fi~~
~~gr~~
~~ra~~
~~ti~~
~~ot~~
 (S)

Id	B	Boot-
la	nd	Optio-
ti	B	nen
os	v	
ze	g	
m	6	
io	d	
	i	
	h	
	R	
	ra	
	t	

Ad	send	Nicht
Id	z	utref-
la	s	efend;
ti	lat	Prozess
on	a	wird
auf	i	über
ent	s	RXE
fn	r	and
ten	s r	DHCP
Ss	send	Arwal-
te	e	tst
nn	s	e d
thr	-	PIFT
VC	-	reS
-	s	rev
DE	-	CNV
Bu	-	itLA
und	-	e iv
Wie	gnur	
on	-	CNV
LAN	-	ssaP
(S7)	t	row

Ad	send	id
Id	s	ip

la-
ti-
os
ze-
na-
rio

fa-	s e d	<i>Pfad</i>
che	-latsI	<i>_zu</i>
hil-	- a l	<i>haben</i>
la-	- i t.	<i>haben</i>
ti-	- sno	<i>some</i>
on	- res	<i>haben</i>
mit	s rev	(nur
er-	-zt eN	erfor-
fin-	-krow	der-
ten	- e g	lich,
Zuf	t ä r	wenn
ühr	- P I	meh-
SH	-sera	rere
-	e s	Netz-
Sta-	-zt eN	werk-
ti-	- s am	gerä-
ste	e k	te
Nie	-et aG	ver-
vek	y a w	füg-
kon-	-HSS	bar
fi-	- i tka	sind)
gu-	-e i v.	hosp-
ra-	gnu r	<i>some</i>
ti-	-HSS	<i>_ip</i>
or“	-ssaP	
(S)	t r ow	

Id	n	Boot-
la-	m	Optio-
ti-	B	nen
os	v	
ze-	g	
m-	f	
no	d	
	i	
	h	
	R	
	ra	
	t	

- ~~retrak~~
sane
retrak
- ~~glov~~
ip
glov
- ~~uss1~~
- ~~spawl~~
sane
spawl

Ad -serd ~~retrak~~
En e s ~~ip~~
fa- s e d ~~Pfad~~
de -lats ~~zu~~
Id - a l ~~retrak~~
la- - i t. ~~uss1~~
ti- - sno 1
on - res. ~~spawl~~
mit s rev sane
et- -HSS ~~spawl~~
fm- - i tA
tm - eiv
Zg gnur
itr

Id **n** Boot-
la **m** Optio-
ti **B** nen
os **v**
ze **E**
m **C**
io **d**
i
h
R
ra
t

SSH -HSS
- -ssaP
Dra t row
mi
ste
Nz
vk
kn
fi
gr
ra
ti
or
(S)

Auf -serNicht
Jul e zutref-
la s efnd;
ti -latHrozess
on - a wird
auf - i über
er - s PXE
in - r and
ten s r DHCP
Ss -serArwal-
te e tst

```

id  n  Boot-
la-  d  Optio-
ti-  B  nen
os  v
ze  g
m-  f
no  d
    l
    h
    R
    m
    t

```

```

nm  s e d
itr -PIFT
SH  -reS
-   srev
PE  -HSS
Bu  -i tlA
ud  -eiv
We  gnur
on- -HSS
LA  -ssaP
(S) t row

```

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 1.4.3, „Benutzerdefinierte Boot-Optionen“** (S. 38)). 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 1.4.3, „Benutzerdefinierte Boot-Optionen“](#) (S. 38). 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-Adresse_Ziel* 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. Sämtliche Partitionierungsaufgaben können mit YaST erledigt werden. Wenn Sie persistente Gerätenamen für Blockgeräte erhalten möchten, verwenden Sie die Geräte unter `/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. Mithilfe seiner Snapshot-Funktionalität können Sie problemlos Daten-Backups erstellen. Ein RAID (Redundant Array of Independent Disks) bietet verbesserte Datenintegrität, Leistung und Fehlertoleranz.

2.1 Verwenden der YaST-Partitionierung

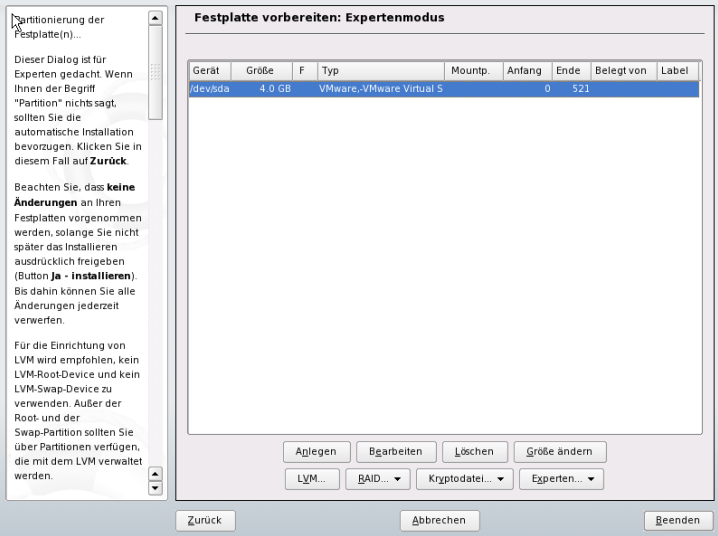
Die in [Abbildung 2.1, „Die YaST-Partitionierung“](#) (S. 52) gezeigte Expertenpartitionierung ermöglicht die manuelle Änderung der Partitionierung einer oder mehrerer Festplatten. Partitionen können hinzugefügt, gelöscht, in ihrer Größe geändert und bearbeitet werden. Außerdem können Sie über dieses 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 Einhängepunkt der Festplatten und ihrer Partitionen werden ebenfalls angezeigt. Der Einhängepunkt 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 Partition erstellen. Innerhalb der erweiterten Partition können Sie mehrere logische Partitionen erstellen (siehe [Abschnitt 2.1.1, „Partitionstypen“](#) (S. 53)).
- 3 Wählen Sie das zu verwendende Dateisystem und einen Einhängepunkt aus. YaST schlägt für jede erstellte Partition einen Einhängepunkt vor. Einzelheiten

zu den verschiedenen Dateisystemen finden Sie in **Kapitel 16, *Dateisysteme in Linux*** (S. 273).

- 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. 54).
- 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. 60) und **Abschnitt 2.3, „Soft-RAID-Konfiguration“** (S. 68).

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. Weitere Informationen zu den verschiedenen Dateisystemen finden Sie unter **Kapitel 16, *Dateisysteme in Linux*** (S. 273).

Swap ist ein Sonderformat, das die Verwendung der Partition als virtueller 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, und 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 40, *Verschlüsseln von Partitionen und Dateien*** (S. 727).

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 Einhängeoption *Geräte-ID* oder *UUID*. In openSUSE sind persistente Gerätenamen standardmäßig aktiviert.

Wenn Sie für das Dateisystem Quotas verwenden möchten, verwenden Sie die Einhängeoption *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.

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 Zylindernummer 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, Einhängpunkt und Benutzerberechtigungen.

Beispiel 2.1 *`/etc/fstab`: Partitionsdaten*

```
/dev/disk/by-id/scsi-SATA_SAMSUNG_SV4002H0413J1FR917614-part1 /data1 auto
noauto,user 0 0
/dev/disk/by-id/scsi-SATA_SAMSUNG_SV4002H0413J1FR917614-part5 /data2 auto
noauto,user 0 0
/dev/disk/by-id/scsi-SATA_SAMSUNG_SV4002H0413J1FR917614-part6 /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.

Wenn dem Kernel der Arbeitsspeicher nicht ausreicht, lagert er selten verwendete Arbeitsspeicherseiten aus. 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 verlangsamen 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 – 256 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.

System mit großem Swap (mehrere GB)

Auf einem solchen System sollten Sie besser keine Anwendung ausführen, 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 in der Regel 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. 60)). 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 `dd if=/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. 63) wird erläutert, wie LVM mit YaST eingerichtet wird.

WARNUNG

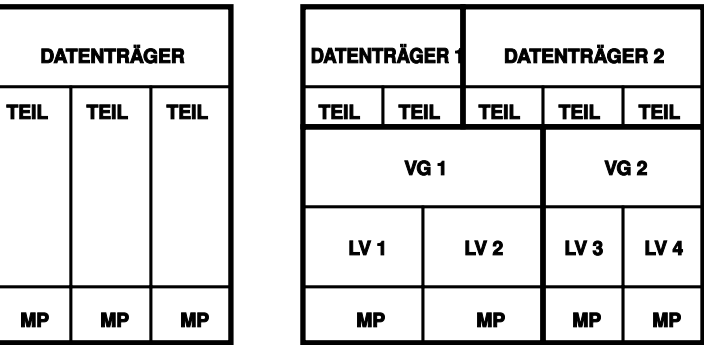
Der Einsatz von LVM kann mit einem höheren Risiko (etwa des Datenverlusts) verbunden sein. Risiken umfassen auch Anwendungsausfälle, Stromausfälle und

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. 53) und [Abschnitt 2.1, „Verwenden der YaST-Partitionierung“](#) (S. 51).

Abbildung 2.2 *Physische Partitionierung versus LVM*



[Abbildung 2.2, „Physische Partitionierung versus LVM“](#) (S. 61) 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 Parti-

tionen 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.

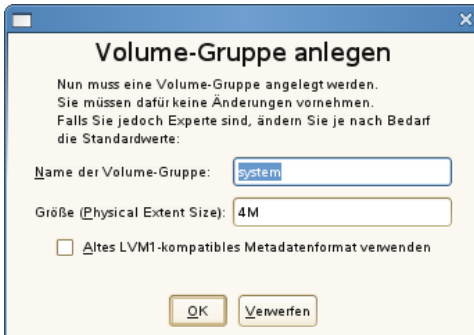
2.2.2 LVM-Konfiguration mit YaST

Zur LVM-Konfiguration mit YaST gelangen Sie über den YaST-Expertenmodus des Partitionierungsmoduls (siehe [Abschnitt 2.1, „Verwenden der YaST-Partitionierung“](#) (S. 51)). 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. 64)). 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

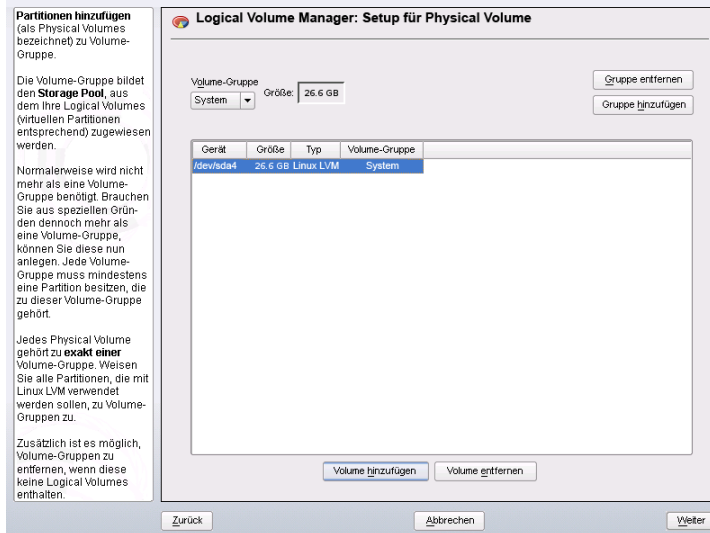


Konfigurieren von physischen Volumes

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



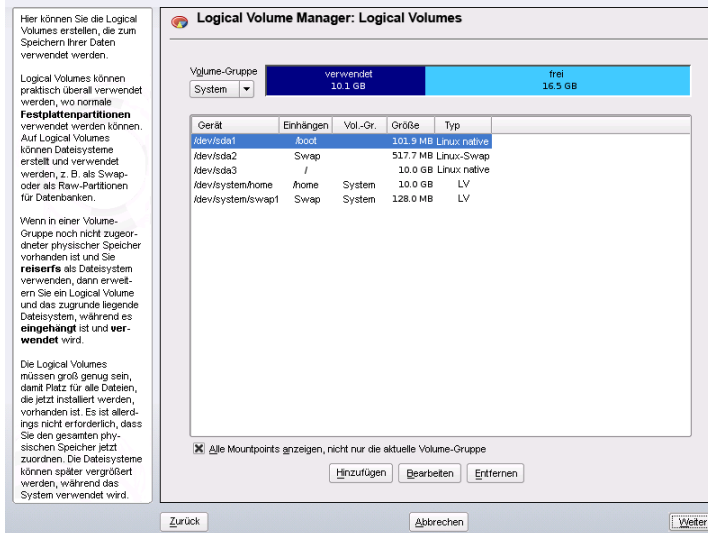
Um der ausgewählten Volume-Gruppe eine zuvor nicht zugewiesene Partition zuzuweisen, klicken Sie zuerst auf die Partition und anschließend auf *Volume hinzufügen*. Der Name der Volume-Gruppe wird dann bei der ausgewählten Partition eingetragen. Sie sollten alle Partitionen, die Sie für LVM vorgesehen 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 Popup-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

Logical Volume erstellen

Name des Logical Volume
Home
(z. B. var, opt)
Größe: (z. B. 4.0 GB 210.0 MB)
+10G
max = 26.5 GB max
Stripes
1
Stripe-Größe
64
Fstab-Optionen
Mountpoint
/home
OK Abbrechen

Formatieren
☐ Nicht formatieren
☒ Formatieren
Dateisystem
Ext3
Optionen
☐ Dateisystem verschlüsseln

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.

2.3.1 RAID-Level

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.

RAID 6

RAID 6 stellt hinsichtlich Zuverlässigkeit eine weitere Steigerung des RAID-Systems dar. Auf diesem Level kann das Array selbst nach einem Ausfall von zwei Festplatten noch rekonstruiert werden. Für ein RAID 6-Array werden mindestens vier Festplatten benötigt. Allerdings benötigt diese Konfiguration als Software-RAID sehr viel CPU-Zeit und Arbeitsspeicher.

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.

2.3.2 Soft-RAID-Konfiguration mit YaST

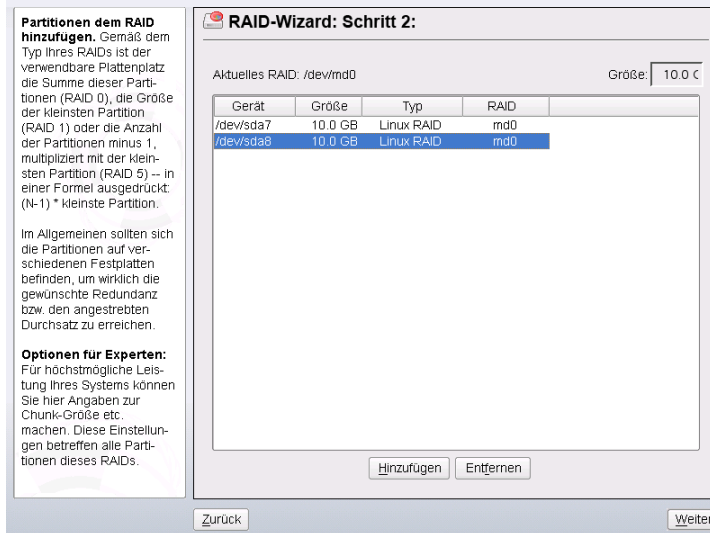
Zur Soft-RAID-Konfiguration gelangen Sie über den YaST-Expertenmodus des Partitionierungsmodus, der in [Abschnitt 2.1, „Verwenden der YaST-Partitionierung“](#) (S. 51) beschrieben ist. Mit diesem Partitionierungswerkzeug können Sie vorhandene Partitionen bearbeiten und löschen sowie neue Partitionen 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 RAID 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.

TIPP

Ab openSUSE 10.2 erkennt das System die Einstellungen von Pseudo-RAID-Adaptern auf vielen Hauptplatinen. Diese werden benutzt, um Software-RAID ohne zusätzliche Interaktion einzurichten.

Wählen Sie im nächsten Dialogfeld RAID-Level 0, 1 oder 5 (weitere Informationen hierzu finden Sie unter [Abschnitt 2.3.1, „RAID-Level“](#) (S. 68)). 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. 71)). 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. 72)).

Abbildung 2.8 Dateisystemeinstellungen

Chunk-Größe:
Dies ist die kleinste 'atomare' Datenmenge, die auf die Geräte geschrieben werden kann. Eine sinnvolle Chunk-Größe für RAID 5 ist 128 KB. Für RAID 0 ist 32 KB ein guter Anfangswert. Bei RAID 1 beeinflusst die Chunk-Größe das gesamte Plattensystem nicht wesentlich.

Parity-Algorithmus:
Hier ist der Parity-Algorithmus anzugeben, der bei RAID 5 verwendet werden soll. Links-symmetrisch (left-symmetric) ist der Algorithmus, der den maximalen Durchsatz bei typischen Platten mit rotierenden Scheiben bereitstellen kann.

RAID-Wizard: Schritt 3:

Formatieren

☐ Nicht formatieren

☒ Formatieren

Dateisystem
Ext3

Optionen

☐ Dateisystem verschlüsseln

RAID-Typ
raid1

Chunk-Größe in KB
4

Parity-Algorithmus (nur für RAID 5)
links-asymmetrisch

Fstab-Optionen

Mountpoint
/local

Zurück Beenden

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.

2.3.3 Fehlersuche

Prüfen Sie die Datei `/proc/mdstats`, um festzustellen, ob eine RAID-Partition zerstört 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.

2.3.4 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>.

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 YaST-Online-Update

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.

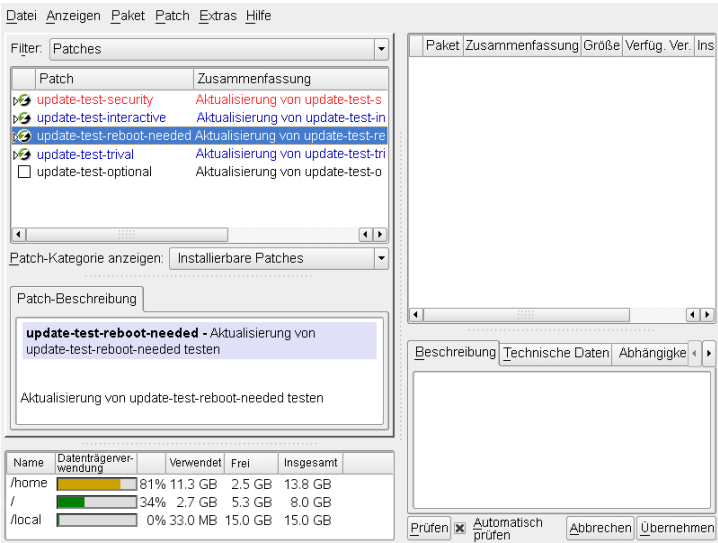
TIPP

YaST Online Update wurde in das YaST-Modul zum Installieren und Löschen von Software integriert. Damit wird sichergestellt, dass stets die neueste Version des Pakets installiert wird. Es ist nicht mehr erforderlich, nach der Installation neuer Pakete ein Online-Update durchzuführen.

3.1.1 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 Speicherplatzauslastung erscheint am Ende der linken Spalte. 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 sind nach ihrer Relevanz für die Sicherheit sortiert. Sowohl die Farbe des Patch-Namens als auch das unter dem Mauszeiger eingeblendete Fenster geben den Sicherheitsstatus eines Patches an: *Sicherheit* (rot), *Empfohlen* (blau) oder *Optional* (schwarz). Patches können in drei verschiedenen Ansichten angezeigt werden. Mit *Patch-Kategorie anzeigen* können Sie die Ansicht wechseln:

Installierbare Patches (Standardansicht)

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

Installierbare und installierte Patches

Alle Patches für Pakete, die auf Ihrem System installiert 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.

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.

3.1.2 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.

3.1.3 Hinzufügen von Update-Repositorys

Verwenden Sie zum Hinzufügen oder Entfernen von Repositorys das Modul *Software > Software Repositorys*, das unter Abschnitt „Hinzufügen von Software-Repositorys“ (Kapitel 3, *Installieren bzw. Entfernen von Software*, ↑Start) beschrieben wird.

3.2 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.

3.2.1 Installieren und Entfernen von Software mit zypper

Zur Installation eines Pakets aus einem registrierten Installations-Repository geben Sie das Kommando `zypper in Paketname` ein. Zur Deinstallation eines installierten Pakets geben Sie `zypper rm Paketname` ein.

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) mit dem Kommando `zypper --non-interactive in Paketname` angegeben werden. Mit dieser Option kann zypper auch in Skripten und Cron-Aufträgen verwendet werden.

3.2.2 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 up` aus. In diesem Fall werden alle in Ihren Installations-Repositorys vorhandenen Patches auf Relevanz überprüft und bei Bedarf installiert.

Bietet eine Installationsquelle allerdings neue Pakete, jedoch keine Patches dafür an, zeigt `zypper up` keinerlei Wirkung. Um eines dieser Pakete zu aktualisieren, müssen Sie das jeweilige Paket mit dem Kommando `zypper in Paketname` neu installieren.

3.2.3 Verwalten der Installations-Repositorys

Sämtliche Installations- und Update-Kommandos von `zypper` sind von der Liste der Installations-Repositorys abhängig, die `zypper` bekannt sind. Mit dem Kommando `zypper sl` können Sie die dem System bekannten Installations-Repositorys auflisten.

Wenn Sie ein Installations-Repository entfernen möchten, listen Sie zunächst alle Repositorys auf und geben Sie danach das Kommando `zypper sd Repository-Nummer` ein. Das zu entfernende Installations-Repository könnte beispielsweise durch folgende Zeile dargestellt sein (der Zeilenumbruch ist in diesem Dokument aus Layout-Gründen eingefügt):

```
2 | No | Yes | YaST | openSUSE FACTORY Extra 10.3 | \  
  
http://download.opensuse.org/distribution/SL-Factory-non-oss/inst-source-extra/
```

Um dieses Installations-Repository aus der Liste zu entfernen, führen Sie das Kommando `zypper sd 2` aus.

Zum Hinzufügen eines Installations-Repositorys geben Sie das Kommando `zypper sa Installations_Repository` ein. Informationen über zusätzliche Installationsquellen erhalten Sie unter http://en.opensuse.org/Installation_Sources.

3.2.4 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 mit `zypper sh` im Shell-Modus ausgeführt werden.

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

```
zypper sh  
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`.

3.2.5 Weiterführende Informationen

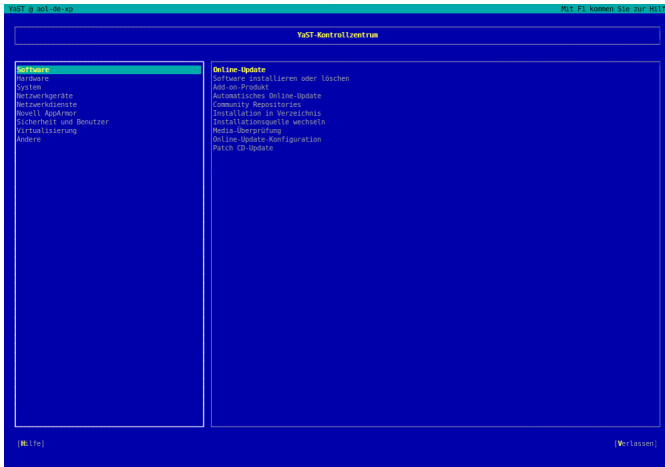
Weitere Informationen zur Aktualisierung über die Kommandozeile erhalten Sie, wenn Sie `zypper --help` eingeben oder die man-Seite `zypper(8)` aufrufen. Beispiele und ausführliche Informationen finden Sie unter http://en.opensuse.org/Using_zypper.

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.

Beim Start von YaST im Textmodus wird zuerst das YaST-Kontrollzentrum angezeigt. Weitere Informationen hierzu finden Sie unter **Abbildung 4.1, „Hauptfenster von YaST im Textmodus“** (S. 84). 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*.

Abbildung 4.1 *Hauptfenster von YaST im Textmodus*



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, wird der Modultitel mit farbigem Hintergrund angezeigt und im unteren Rahmen sehen Sie eine kurze Beschreibung.

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. 86) finden Sie Informationen zu möglichen Ausnahmen.

Navigation zwischen Schaltflächen und Auswahllisten

Mit **Tabulator** und **Alt + Tabulator** oder **Umschalt + Tabulator** können Sie zwischen den Schaltflächen und den Rahmen mit Auswahllisten navigieren.

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. 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 *OK*, *Weiter* und *Verlassen* verwendet. Mit F1 kann die YaST-Hilfe aufgerufen werden, in der die den einzelnen F-Tasten zugeordneten Funktionen angezeigt werden.

Abbildung 4.2 Das Software-Installationsmodul

[illegible]

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 Verfü-

gung. 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-Repositorys 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 Softwareverwaltungs-bibliothek, die auch die Grundlage des YaST-Paket-Managers bildet. Die grundlegende Verwendung von zypper wird unter **Abschnitt 3.2, „Aktualisierung über die Kommandozeile mit zypper“** (S. 80) erläutert.

4.3.3 Kommandozeilenparameter der YaST-Module

Um die Verwendung von YaST-Funktionen in Skripts 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 YaST2 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 (Streamer), eine Wechselfestplatte, einen USB-Stick oder ein ZIP-Laufwerk, um die Daten zu sichern. Dies gilt hauptsächlich für die in `/etc` gespeicherten Dateien sowie einige der Verzeichnisse und Dateien in `/var` und `/opt`. 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. 90) 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. 89) 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 und Repositorys“ (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. 89) 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. 77).

5.2.1 Von 9.3 auf 10.0

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

Anmelden als Superuser mit su

Standardmäßig wird durch den Aufruf von su zur Anmeldung als root der PATH für root nicht eingestellt. Rufen Sie entweder su - auf, um eine Anmelde-Shell mit der vollständigen Umgebung für root zu starten, oder stellen Sie ALWAYS_SET_PATH auf yes (ja) in /etc/default/su ein, wenn Sie das Standardverhalten von su ändern möchten.

powersave-Konfigurationsvariablen

Namen der powersave-Konfigurationsvariablen wurden aus Konsistenzgründen geändert, die sysconfig-Dateien sind unverändert. Weitere Informationen finden Sie in **Abschnitt 32.4.1, „Konfigurieren des Powersave-Pakets“** (S. 609).

PCMCIA

Mit cardmgr ist die Verwaltung von PC-Karten nicht mehr möglich. Stattdessen wird die Verwaltung, wie bei Cardbus-Karten und anderen Teilsystemen, von einem Kernel-Modul vorgenommen. Alle erforderlichen Aktionen können mit hotplug ausgeführt werden. Das Startskript pcmciawurde entfernt und cardctl wird durch pccardctl ersetzt. Weitere Informationen finden Sie in /usr/share/doc/packages/pcmciutils/README.SUSE.

Einrichten von D-BUS für die prozessübergreifende Kommunikation in `.xinitrc`

In vielen Anwendungen wird jetzt D-BUS für die prozessübergreifende Kommunikation verwendet. Durch den Aufruf `dbus-launch` wird `dbus-daemon` gestartet. Die systemweite Datei `/etc/X11/xinit/xinitrc` verwendet `dbus-launch` zum Starten des Fenster-Managers.

Falls Sie eine lokale `~/.xinitrc`-Datei verwenden, müssen Sie diese entsprechend ändern. Andernfalls können in Anwendungen, wie `f-spot`, `banshee`, `tomboy` oder `Network Manager` `banshee`, Fehler auftreten. Speichern Sie die alte Version der Datei `~/.xinitrc`. Kopieren Sie anschließend die neue Vorlagendatei mit folgendem Befehl in Ihr Home-Verzeichnis:

```
cp /etc/skel/.xinitrc.template ~/.xinitrc
```

Fügen Sie anschließend Ihre Anpassungen aus der gespeicherten `.xinitrc`-Datei hinzu.

Umbenannte NTP-bezogene Dateien

Aus Gründen der Kompatibilität mit LSB (Linux Standard Base) wurden die meisten Konfigurationsdateien und das init-Skript von `xntp` in `ntp` umbenannt. Die neuen Dateinamen lauten wie folgt:

```
/etc/slp.reg.d/ntp.reg
```

```
/etc/init.d/ntp
```

```
/etc/logrotate.d/ntp
```

```
/usr/sbin/rcntp
```

```
/etc/sysconfig/ntp
```

Über den udev-Daemon verarbeitete Hotplug-Ereignisse

Hotplug-Ereignisse werden jetzt vollständig über den udev-Daemon (`udev`) verarbeitet. Das Ereignis-Multiplexer-System unter `/etc/hotplug.d` und `/etc/dev.d` wird nicht mehr verwendet. Stattdessen werden mit `udev` alle Hotplug-Hilfswerkzeuge gemäß den entsprechenden Regeln direkt aufgerufen. Udev-Regeln und Hilfswerkzeuge werden von `udev` und verschiedenen anderen Paketen bereitgestellt.

TEI-XSL-Stylesheets

Die TEI-XSL-Stylesheets (`tei-xsl-stylesheets`) mit neuem Verzeichnislayout finden Sie in `/usr/share/xml/tei/stylesheet/rahtz/current`. Von diesem Speicherort können Sie beispielsweise `base/p4/html/tei.xsl` für die HTML-(HyperText Markup Language-)Ausgabe verwenden. Weitere Informationen finden Sie unter <http://www.tei-c.org/Stylesheets/teic/>

Benachrichtigung bezüglich Dateisystemänderung für GNOME-Anwendungen

Für eine ordnungsgemäße Funktionsweise der GNOME-Anwendungen ist die Unterstützung für Benachrichtigungen bei Dateisystemänderungen erforderlich. Installieren Sie auf ausschließlich lokalen Dateisystemen das `gamin`-Paket (bevorzugt) oder führen Sie den FAM-Daemon aus. Führen Sie für entfernte Dateisysteme sowohl auf dem Server als auch auf dem Client FAM aus und öffnen Sie die Firewall für RPC-Aufrufe durch FAM.

GNOME (`gnome-vfs2` und `libgda`) enthält einen Packer, der für die Bereitstellung der Benachrichtigung bezüglich Dateisystemänderungen `gamin` oder `fam` auswählt:

- Wenn der FAM-Daemon nicht ausgeführt wird, ist `gamin` zu bevorzugen (Grund: Inotify wird nur von `gamin` unterstützt und ist für lokale Dateisysteme effizienter).
- Wenn der FAM-Daemon ausgeführt wird, ist FAM zu bevorzugen (Grund: Mit FAM werden Sie wahrscheinlich die Remote-Benachrichtigung nutzen, die nur von FAM unterstützt wird).

5.2.2 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 30, *Der HTTP-Server Apache*** (S. 543) 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.

Entriegeln 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.

5.2.3 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.

5.2.4 Von 10.2 auf 10.3

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

RPM – der Paket-Manager

RPM (RPM Package Manager) wird für die Verwaltung von Softwarepaketen verwendet. Seine Hauptbefehle lauten `rpm` und `rpmbuild`. In der leistungsstarken RPM-Datenbank können Benutzer, Systemadministratoren und Paketersteller ausführliche Informationen zur installierten Software abfragen.

Im Wesentlichen hat `rpm` fünf Modi: Installieren, Deinstallieren oder Aktualisieren von Software-Paketen; Neuaufbauen der RPM-Datenbank, Abfragen der RPM-Basis oder individuellen RPM-Archiven, Integritätsprüfung der Pakete und Signieren von Paketen. `rpmbuild` ermöglicht das Aufbauen installierbarer Pakete von Pristine-Quellen.

Installierbare RPM-Archive sind in einem speziellen binären Format gepackt. Diese Archive bestehen aus den zu installierenden Programmdateien und aus verschiedenen Metadaten, die bei der Installation von `rpm` benutzt werden, um das jeweilige Softwarepaket zu konfigurieren, oder die zu Dokumentationszwecken in der RPM-Datenbank gespeichert werden. RPM-Archive haben für gewöhnlich die Dateinamenserweiterung `.rpm`.

TIPP: Pakete zur Software-Entwicklung

Bei etlichen Paketen sind die zur Software-Entwicklung erforderlichen Komponenten (Bibliotheken, Header- und Include-Dateien usw.) in eigene Pakete ausgelagert. Diese Entwicklungspakete werden nur benötigt, wenn Sie Software selbst kompilieren möchten – beispielsweise die neuesten GNOME-Pakete. Solche Pakete sind am Namenszusatz `-devel` zu erkennen, z. B. die Pakete `alsa-devel`, `gimp-devel` und `kdelibs3-devel`.

6.1 Prüfen der Authentizität eines Pakets

RPM-Pakete sind mit GnuPG signiert. Der Schlüssel mit dem "Fingerabdruck" lautet:

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>  
Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
```

Mit dem Befehl `rpm --checksig paket-1.2.3.rpm` können Sie die Signatur eines RPM-Pakets überprüfen und feststellen, ob es wirklich von SUSE oder einer anderen vertrauenswürdigen Quelle stammt. Dies ist insbesondere bei Update-Paketen aus dem Internet zu empfehlen. Der öffentliche Paketsignierschlüssel von SUSE ist standardmäßig in `/root/.gnupg/` hinterlegt. Der Schlüssel befindet sich zusätzlich im Verzeichnis `/usr/lib/rpm/gnupg/`, damit auch normale Benutzer die Signatur von RPM-Paketen prüfen können.

6.2 Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren

In der Regel kann ein RPM-Archiv einfach installiert werden: `rpm -i package.rpm`. Mit diesem Befehl wird das Paket aber nur dann installiert, wenn seine Abhängigkeiten erfüllt sind und keine Konflikte mit anderen Paketen bestehen. `rpm` fordert per Fehlermeldung die Pakete an, die zum Erfüllen der Abhängigkeiten installiert werden müssen. Im Hintergrund stellt die RPM-Datenbank sicher, dass keine Konflikte entstehen: Jede spezifische Datei darf nur zu einem Paket gehören. Durch die Wahl anderer Optionen können Sie `rpm` zwingen, diese Standards zu ignorieren, jedoch ist dies nur für Spezialisten gedacht. Andernfalls wird damit die Integrität des Systems gefährdet und möglicherweise die Update-Fähigkeit aufs Spiel gesetzt.

Die Optionen `-U` oder `--upgrade` und `-F` oder `--freshen` können für das Update eines Pakets benutzt werden, z. B.: `rpm -F paket.rpm`. Dieser Befehl entfernt die Dateien der alten Version und installiert sofort die neuen Dateien. Der Unterschied zwischen den beiden Versionen besteht darin, dass mit `-U` auch Pakete installiert werden, die vorher nicht im System vorhanden waren, wohingegen mit `-F` nur zuvor installierte

Pakete aktualisiert werden. Bei einem Update verwendet `rpm` zur sorgfältigen Aktualisierung der Konfigurationsdateien die folgende Strategie:

- Falls eine Konfigurationsdatei vom Systemadministrator nicht geändert wurde, installiert `rpm` die neue Version der entsprechenden Datei. Es sind keine Eingriffe seitens des Administrators nötig.
- Falls eine Konfigurationsdatei vom Systemadministrator vor dem Update geändert wurde, speichert `rpm` die geänderte Datei mit der Erweiterung `.rpmorig` oder `.rpmsave` (Sicherungsdatei) und installiert nur dann die Version aus dem neuen Paket, wenn sich die ursprünglich installierte Datei und die neue Version unterscheiden. Vergleichen Sie in diesem Fall die Sicherungsdatei (`.rpmorig` oder `.rpmsave`) mit der neu installierten Datei und nehmen Sie Ihre Änderungen erneut in der neuen Datei vor. Löschen Sie anschließend unbedingt alle `.rpmorig`- und `.rpmsave`-Dateien, um Probleme mit zukünftigen Updates zu vermeiden.
- `.rpmnew`-Dateien erscheinen immer dann, wenn die Konfigurationsdatei bereits existiert *und* wenn die Kennung `noreplace` mit der `.spec`-Datei angegeben wurde.

Im Anschluss an ein Update sollten alle `.rpmsave`- und `.rpmnew`-Dateien nach einem Abgleich entfernt werden, damit sie bei zukünftigen Updates nicht stören. Die Erweiterung `.rpmorig` wird zugewiesen, wenn die Datei zuvor nicht von der RPM-Datenbank erkannt wurde.

Andernfalls wird `.rpmsave` verwendet. Mit anderen Worten: `.rpmorig` entsteht bei einem Update von einem Fremdformat auf RPM. `.rpmsave` entsteht bei einem Update aus einem älteren RPM auf einen neueren RPM. `.rpmnew` informiert nicht darüber, ob der Systemadministrator die Konfigurationsdatei geändert hat. Eine Liste all dieser Dateien ist in `/var/adm/rpmconfigcheck` verfügbar. Einige Konfigurationsdateien (wie `/etc/httpd/httpd.conf`) werden nicht überschrieben, um den weiteren Betrieb zu ermöglichen.

Der Schalter `-U` ist *nicht* einfach gleichbedeutend mit der Deinstallation mit der Option `-e` und der Installation mit der Option `-i`. Verwenden Sie `-U`, wann immer möglich.

Geben Sie `rpm -e paket` ein, wenn Sie ein Paket entfernen möchten. `rpm` löscht das Paket nur, wenn keine nicht erfüllten Abhängigkeiten vorhanden sind. Theoretisch ist es unmöglich, beispielsweise `Tcl/Tk` zu löschen, solange eine andere Anwendung `Tcl/Tk` noch benötigt. Auch in diesem Fall nutzt RPM die Datenbank zur Unterstützung.

Falls es in Ausnahmefällen nicht möglich ist, zu löschen, obwohl *keine* zusätzlichen Abhängigkeiten bestehen, können Sie versuchen, die RPM-Datenbank mit der Option `--rebuilddb` neu aufzubauen.

6.3 RPM und Patches

Um die Betriebssicherheit eines Systems zu garantieren, müssen von Zeit zu Zeit Update-Pakete auf dem System installiert werden. Bisher konnte ein Fehler in einem Paket nur eliminiert werden, indem das vollständige Paket ersetzt wurde. Bei großen Paketen mit Fehlern in kleinen Dateien kann dies schnell zu großen Datenmengen führen. Jedoch bietet SUSE RPM nun eine Funktion, mit der Patches in Pakete installiert werden können.

Die wichtigsten Überlegungen dazu werden am Beispiel "pine" aufgezeigt:

Ist der Patch-RPM für mein System geeignet?

Um dies zu prüfen, fragen Sie zunächst die installierte Version des Pakets ab. Im Fall von pine verwenden Sie den Befehl:

```
rpm -q pine
pine-4.44-188
```

Prüfen Sie dann, ob der Patch-RPM sich für diese Version von pine eignet:

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

Dieser Patch passt zu drei verschiedenen Versionen von pine. Auch die im Beispiel installierte Version wird aufgeführt, d. h. der Patch kann installiert werden.

Welche Dateien werden durch den Patch ersetzt?

Die durch einen Patch betroffenen Dateien können leicht im Patch-RPM abgelesen werden. Der `rpm`-Parameter `-P` ermöglicht die Auswahl von speziellen Patch-Funktionen. Zeigen Sie die Dateiliste mit dem folgenden Befehl an:

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Oder verwenden Sie, falls der Patch bereits installiert ist, den folgenden Befehl:

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

Wie kann ein Patch-RPM im System installiert werden?

Patch-RPMs werden wie normale RPMs verwendet. Der einzige Unterschied liegt darin, dass ein passender RPM bereits installiert sein muss.

Welche Patches sind bereits auf dem System installiert und zu welchen Paketversionen gehören sie?

Eine Liste aller im System installierter Patches kann über den Befehl `rpm -qPa` angezeigt werden. Wenn nur ein Patch in einem neuen System installiert ist (wie in unserem Beispiel), sieht die Liste wie folgt aus:

```
rpm -qPa
pine-4.44-224
```

Wenn Sie zu einem späteren Zeitpunkt wissen möchten, welche Paketversion ursprünglich installiert war, können Sie auch diese Information der RPM-Datenbank entnehmen. Für `pine` rufen Sie diese Information mit dem folgenden Befehl ab:

```
rpm -q --basedon pine
pine = 4.44-188
```

Weitere Informationen, auch zur Patch-Funktion von RPM, stehen auf den man-Seiten von `rpm` und `rpmbuild` zur Verfügung.

6.4 Delta-RPM-Pakete

Delta-RPM-Pakete enthalten die Unterschiede zwischen einer alten und einer neuen Version eines RPM-Pakets. Wenn Sie ein Delta-RPM auf ein altes RPM anwenden, ergibt dies einen vollständig neuen RPM. Es ist nicht erforderlich, dass eine Kopie des alten RPM vorhanden ist, da ein Delta-RPM auch mit einem installierten RPM arbeiten kann. Die Delta-RPM-Pakete sind sogar kleiner als Patch-RPMs, was beim Übertragen von Update-Paketen über das Internet von Vorteil ist. Der Nachteil ist, dass Update-Vorgänge mit Delta-RPMs erheblich mehr CPU-Zyklen beanspruchen als normale oder Patch-RPMs.

Die Binärdateien `prepdeltarpm`, `writedeltarpm` und `applydeltarpm` sind Teil der Delta-RPM-Suite (Paket `deltarpm`) und helfen Ihnen beim Erstellen und Anwenden von Delta-RPM-Paketen. Mit den folgenden Befehlen erstellen Sie ein Delta-RPM mit dem Namen `new.delta.rpm`. Der folgende Befehl setzt voraus, dass `old.rpm` und `new.rpm` vorhanden sind:

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

Entfernen Sie zum Schluss die temporären Arbeitsdateien `old.cpio`, `new.cpio` und `delta`.

Mit `applydeltarpm` können Sie den neuen RPM aus dem Dateisystem rekonstruieren, wenn das alte Paket bereits installiert ist:

```
applydeltarpm new.delta.rpm new.rpm
```

Um es aus dem alten RPM abzuleiten, ohne auf das Dateisystem zuzugreifen, verwenden Sie die Option `-r`:

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

Technische Details finden Sie in `/usr/share/doc/packages/deltarpm/README`.

6.5 RPM Abfragen

Mit der Option `-q` initiiert `rpm` Abfragen und ermöglicht es, ein RPM-Archiv zu prüfen (durch Hinzufügen der Option `-p`) und auch die RPM-Datenbank nach installierten Paketen abzufragen. Zur Angabe der benötigten Informationsart stehen mehrere Schalter zur Verfügung. Weitere Informationen hierzu finden Sie unter **Tabelle 6.1**, „Die wichtigsten RPM-Abfrageoptionen“ (S. 106).

Tabelle 6.1 Die wichtigsten RPM-Abfrageoptionen

<code>-i</code>	Paketinformation
<code>-l</code>	Dateiliste

<code>-f FILE</code>	Abfrage nach Paket, das die Datei <i>FILE</i> enthält. (<i>FILE</i> muss mit dem vollständigen Pfad angegeben werden.)
<code>-s</code>	Dateiliste mit Statusinformation (impliziert <code>-l</code>)
<code>-d</code>	Nur Dokumentationsdateien auflisten (impliziert <code>-l</code>)
<code>-c</code>	Nur Konfigurationsdateien auflisten (impliziert <code>-l</code>)
<code>--dump</code>	Dateiliste mit vollständigen Details (mit <code>-l</code> , <code>-c</code> oder <code>-d</code> benutzen)
<code>--provides</code>	Funktionen des Pakets auflisten, die ein anderes Paket mit <code>--requires</code> anfordern kann
<code>--requires, -R</code>	Fähigkeiten, die das Paket benötigt
<code>--Skripten</code>	Installationsskripten (preinstall, postinstall, uninstall)

Beispielsweise gibt der Befehl `rpm -q -i wget` die in **Beispiel 6.1**, „`rpm -q -i wget`“ (S. 107) gezeigte Information aus.

Beispiel 6.1 `rpm -q -i wget`

```

Name           : wget                               Relocations: (not relocatable)
Version        : 1.9.1                             Vendor: SUSE LINUX AG,
Nuernberg, Germany
Release        : 50                                Build Date: Sat 02 Oct 2004
03:49:13 AM CEST
Install date: Mon 11 Oct 2004 10:24:56 AM CEST      Build Host: f53.suse.de
Group          : Productivity/Networking/Web/Utilities Source RPM:
wget-1.9.1-50.src.rpm
Size           : 1637514                             License: GPL
Signature      : DSA/SHA1, Sat 02 Oct 2004 03:59:56 AM CEST, Key ID
a84edae89c800aca
Packager       : http://www.suse.de/feedback
URL            : http://wget.sunsite.dk/
Summary        : A tool for mirroring FTP and HTTP servers
Description    :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

Die Option `-f` funktioniert nur, wenn Sie den kompletten Dateinamen mit dem vollständigen Pfad angeben. Sie können so viele Dateinamen wie nötig angeben. Beispielsweise führt der folgende Befehl

```
rpm -q -f /bin/rpm /usr/bin/wget
```

zum Ergebnis:

```
rpm-4.1.1-191
wget-1.9.1-50
```

Wenn nur ein Teil des Dateinamens bekannt ist, verwenden Sie ein Shell-Skript, wie in **Beispiel 6.2, „Skript für die Suche nach Paketen“** (S. 108) gezeigt. Übergeben Sie den partiellen Dateinamen als Parameter beim Aufruf des Skripts.

Beispiel 6.2 *Skript für die Suche nach Paketen*

```
#!/bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

Der Befehl `rpm -q --changelog rpm` zeigt eine detaillierte Liste der Änderungsinformation zu einem bestimmten Paket nach Datum sortiert. Dieses Beispiel zeigt Informationen zum Paket `rpm`.

Mithilfe der installierten RPM-Datenbank sind Überprüfungen möglich. Initiiieren Sie die Überprüfungen mit `-V`, `-y` oder `--verify`. Mit dieser Option zeigt `rpm` alle Dateien in einem Paket an, die seit der Installation geändert wurden. `rpm` verwendet acht verschiedene Zeichen als Hinweis auf die folgenden Änderungen:

Tabelle 6.2 *RPM-Überprüfungsoptionen*

5	MD5-Prüfsumme
S	Dateigröße
L	Symbolischer Link
T	Änderungszeit

D	Major- und Minor-Gerätenummern
U	Eigentümer
G	Gruppe
M	Modus (Berechtigungen und Dateityp)

Bei Konfigurationsdateien wird der Buchstabe `c` ausgegeben. Beispielsweise für Änderungen an `/etc/wgetrc` (`wget`):

```
rpm -V wget
S.5....T c /etc/wgetrc
```

Die Dateien der RPM-Datenbank werden in `/var/lib/rpm` abgelegt. Wenn die Partition `/usr` eine Größe von 1 GB aufweist, kann diese Datenbank beinahe 30 MB belegen, insbesondere nach einem kompletten Update. Wenn die Datenbank viel größer ist als erwartet, kann es nützlich sein, die Datenbank mit der Option `--rebuilddb` neu zu erstellen. Legen Sie zuvor eine Sicherungskopie der alten Datenbank an. Das cron-Skript `cron.daily` legt täglich (mit `gzip` gepackte) Kopien der Datenbank an und speichert diese unter `/var/adm/backup/rpmdb`. Die Anzahl der Kopien wird durch die Variable `MAX_RPMDB_BACKUPS` (Standard: 5) in `/etc/sysconfig/backup` gesteuert. Die Größe einer einzelnen Sicherungskopie beträgt ungefähr 1 MB für 1 GB in `/usr`.

6.6 Installieren und Kompilieren von Quellpaketen

Alle Quellpakete haben die Erweiterung `.src.rpm` (Source-RPM).

TIPP

Quellpakete können vom Installationsmedium auf die Festplatte kopiert und mit YaST entpackt werden. Sie werden im Paket-Manager jedoch nicht als installiert (`[i]`) gekennzeichnet. Das liegt daran, dass die Quellpakete nicht in der RPM-Datenbank eingetragen sind. Nur *installierte* Betriebssystemsoftware

wird in der RPM-Datenbank aufgeführt. Wenn Sie ein Quellpaket „installieren“, wird dem System nur der Quellcode hinzugefügt.

Die folgenden Verzeichnisse müssen für `rpm` und `rpmbuild` in `/usr/src/packages` vorhanden sein (es sei denn, Sie haben spezielle Einstellungen in einer Datei, wie `/etc/rpmmrc`, festgelegt):

SOURCES

für die originalen Quellen (`.tar.bz2` oder `.tar.gz` files, etc.) und für die distributionsspezifischen Anpassungen (meistens `.diff`- oder `.patch`-Dateien)

SPECS

für die `.spec`-Dateien, die ähnlich wie Meta-Makefiles den *build*-Prozess steuern

BUILD

Alle Quellen in diesem Verzeichnis werden entpackt, gepatcht und kompiliert.

RPMS

Speicherort der fertigen Binärpakete

SRPMS

Speicherort der Quell-RPMs

Wenn Sie ein Quellpaket mit YaST installieren, werden alle notwendigen Komponenten in `/usr/src/packages` installiert: die Quellen und Anpassungen in `SOURCES` und die relevanten `.spec`-Dateien in `SPECS`.

WARNUNG

Experimentieren Sie nicht mit Systemkomponenten (`glibc`, `rpm`, `sysvinit` usw.), da Sie damit die Funktionstüchtigkeit Ihres Systems aufs Spiel setzen.

Das folgende Beispiel verwendet das `wget.src.rpm`-Paket. Nach dem Installieren des Pakets mit YaST sollten Sie über Dateien ähnlich der in folgender Liste verfügen:

```
/usr/src/packages/SOURCES/nops_doc.diff
/usr/src/packages/SOURCES/toplev_destdir.diff
/usr/src/packages/SOURCES/wget-1.9.1+ipvmisc.patch
/usr/src/packages/SOURCES/wget-1.9.1-brokentime.patch
/usr/src/packages/SOURCES/wget-1.9.1-passive_ftp.diff
/usr/src/packages/SOURCES/wget-LFS-20040909.tar.bz2
```

```
/usr/src/packages/SOURCES/wget-wrong_charset.patch  
/usr/src/packages/SPECS/wget.spec
```

Mit `rpmbuild -b X /usr/src/packages/SPECS/wget.spec` wird die Kompilierung gestartet. `X` ist ein Platzhalter für verschiedene Stufen des build-Prozesses (Einzelheiten siehe in `--help` oder der RPM-Dokumentation). Nachfolgend wird nur eine kurze Erläuterung gegeben:

`-bp`

Bereiten Sie Quellen in `/usr/src/packages/BUILD` vor: entpacken und patchen.

`-bc`

Wie `-bp`, jedoch zusätzlich kompilieren.

`-bi`

Wie `-bp`, jedoch zusätzlich die erstellte Software installieren. Vorsicht: Wenn das Paket die Funktion `BuildRoot` nicht unterstützt, ist es möglich, dass Konfigurationsdateien überschrieben werden.

`-bb`

Wie `-bi`, jedoch zusätzlich das Binärpaket erstellen. Nach erfolgreicher Kompilierung sollte das Binärpaket in `/usr/src/packages/RPMS` sein.

`-ba`

Wie `-bb`, jedoch zusätzlich den Quell-RPM erstellen. Nach erfolgreicher Kompilierung sollte dieses in `/usr/src/packages/RPMS` liegen.

`--short-circuit`

Einige Schritte überspringen.

Der erstellte Binär-RPM kann nun mit `rpm -i` oder vorzugsweise mit `rpm -U` erstellt werden. Durch die Installation mit `rpm` wird er in die RPM-Datenbank aufgenommen.

6.7 Kompilieren von RPM-Paketen mit "build"

Bei vielen Paketen besteht die Gefahr, dass während der Erstellung ungewollt Dateien in das laufende System kopiert werden. Um dies zu vermeiden, können Sie `build` verwenden, das eine definierte Umgebung herstellt, in der das Paket erstellt wird. Zum Aufbau dieser chroot-Umgebung muss dem `build`-Skript ein kompletter Paketbaum zur Verfügung stehen. Dieser kann auf Festplatte, über NFS oder auch von DVD bereitgestellt werden. Legen Sie die Position mit `build --rpms Verzeichnis` fest. Im Unterschied zu `rpm` sucht der Befehl `build` die SPEC-Datei im Quellverzeichnis. Wenn Sie, wie im obigen Beispiel, `wget` neu erstellen möchten und die DVD unter `/media/dvd` im System eingehängt ist, verwenden Sie als Benutzer `root` folgende Befehle:

```
cd /usr/src/packages/SOURCES/  
mv ../SPECS/wget.spec .  
build --rpms /media/dvd/suse/ wget.spec
```

Anschließend wird in `/var/tmp/build-root` eine minimale Umgebung eingerichtet. Das Paket wird in dieser Umgebung erstellt. Danach befinden sich die resultierenden Pakete in `/var/tmp/build-root/usr/src/packages/RPMS`.

Das `build`-Skript bietet eine Reihe zusätzlicher Optionen. Beispielsweise können Sie das Skript veranlassen, Ihre eigenen RPMs bevorzugt zu verwenden, die Initialisierung der `build`-Umgebung auszulassen oder den Befehl `rpm` auf eine der oben erwähnten Stufen zu beschränken. Weitere Informationen erhalten Sie über `build --help` oder die Manualpage `build`.

6.8 Werkzeuge für RPM-Archive und die RPM-Datenbank

Midnight Commander (`mc`) kann den Inhalt von RPM-Archiven anzeigen und Teile daraus kopieren. Archive werden als virtuelle Dateisysteme dargestellt und bieten alle üblichen Menüoptionen von Midnight Commander. Zeigen Sie den `HEADER` mit `F3` an. Zeigen Sie die Archivstruktur mit den Cursorstasten und der Eingabetaste an. Kopieren Sie Archivkomponenten mit `F5`.

KDE bietet das Werkzeug `kpackage` als Front-End für `rpm` an. Ein Paket-Manager mit allen Funktionen ist als YaST-Modul verfügbar (siehe Kapitel 3, *Installieren bzw. Entfernen von Software* (↑Start)).

Druckerbetrieb

openSUSE® unterstützt viele Arten von Druckern, einschließlich Remote- und Netzwerkdrucker. Drucker können mit YaST oder manuell konfiguriert werden. Anleitungen zur Konfiguration finden Sie unter Abschnitt „Einrichten eines Druckers“ (Kapitel 2, *Einrichten von Hardware-Komponenten mit YaST*, ↑Start). Grafische Dienstprogramme und Dienstprogramme an der Kommandozeile sind verfügbar, um Druckaufträge zu starten und zu verwalten. Wenn Ihr Drucker nicht wie erwartet verwendet werden kann, lesen Sie die Informationen unter [Abschnitt 7.8, „Fehlersuche“](#) (S. 127).

CUPS ist das Standard-Drucksystem in openSUSE. CUPS ist stark benutzerorientiert. In vielen Fällen ist es kompatibel mit LPRng oder kann mit relativ geringem Aufwand angepasst werden. LPRng ist lediglich aus Kompatibilitätsgründen im Lieferumfang von openSUSE enthalten.

Drucker können nach Schnittstelle, z. B. USB oder Netzwerk, und nach Druckersprache unterschieden werden. Stellen Sie beim Kauf eines Druckers sicher, dass der Drucker über eine für Ihre Hardware geeignete Schnittstelle (wie USB oder einen parallelen Port) und eine geeignete Druckersprache verfügt. Drucker können basierend auf den folgenden drei Klassen von Druckersprachen kategorisiert werden:

PostScript-Drucker

PostScript ist die Druckersprache, in der die meisten Druckaufträge unter Linux und Unix vom internen Drucksystem generiert und verarbeitet werden. Diese Sprache ist bereits sehr alt und sehr effizient. Wenn PostScript-Dokumente direkt vom Drucker verarbeitet und im Drucksystem nicht in weiteren Phasen konvertiert werden müssen, reduziert sich die Anzahl der möglichen Fehlerquellen. Da PostScript-Drucker immer mit erheblichen Lizenzkosten verbunden sind, sind diese Drucker in der Regel teurer als Drucker ohne PostScript-Interpreter.

Standarddrucker (Sprachen wie PCL und ESC/P)

Obwohl diese Druckersprachen ziemlich alt sind, werden sie immer weiter entwickelt, um neue Druckerfunktionen unterstützen zu können. Bei den bekannten Druckersprachen kann das Drucksystem PostScript-Druckaufträge mithilfe von Ghostscript in die entsprechende Druckersprache konvertieren. Diese Verarbeitungsphase wird als "Interpretieren" bezeichnet. Die gängigsten Sprachen sind PCL, die am häufigsten auf HP-Druckern und ihren Klonen zum Einsatz kommt, und ESC/P, die bei Epson-Druckern verwendet wird. Diese Druckersprachen werden in der Regel von Linux unterstützt und liefern ein annehmbares Druckergebnis. Es kann sein, dass Linux einige neue Drucker mit sehr ausgefallenen Funktionen nicht unterstützt, da die Open-Source-Entwickler möglicherweise an diesen Funktionen noch arbeiten. Mit Ausnahme der von HP entwickelten `hpijs`-Treiber gibt es derzeit keinen Druckerhersteller, der Linux-Treiber entwickelt und den Linux-Distributoren unter einer Open Source-Lizenz zur Verfügung stellt. Die meisten dieser Drucker finden sich im mittleren Preisbereich.

Proprietäre Drucker (auch GDI-Drucker genannt)

Diese Drucker unterstützen keine der gängigen Druckersprachen. Sie verwenden eigene, undokumentierte Druckersprachen, die geändert werden können, wenn neue Versionen eines Modells auf den Markt gebracht werden. Für diese Drucker sind in der Regel nur Windows-Treiber verfügbar. Weitere Informationen finden Sie unter **Abschnitt 7.8.1, „Drucker ohne Unterstützung für eine Standard-Druckersprache“** (S. 128).

Vor dem Kauf eines neuen Druckers sollten Sie anhand der folgenden Quellen prüfen, wie gut der Drucker, den Sie zu kaufen beabsichtigen, unterstützt wird:

<http://www.linuxprinting.org/>

Die LinuxPrinting.org-Druckerdatenbank

<http://www.cs.wisc.edu/~ghost/>

Die Ghostscript-Website

`/usr/share/doc/packages/ghostscript/catalog.devices`

Liste der enthaltenen Treiber.

In den Online-Datenbanken wird immer der neueste Linux-Supportstatus angezeigt. Eine Linux-Distribution kann jedoch immer nur die zur Produktionszeit verfügbaren Treiber enthalten. Entsprechend ist es möglich, dass ein Drucker, der derzeit als „vollständig unterstützt“ eingestuft wird, diesen Status bei der Veröffentlichung der aktuellen

openSUSE-Version noch nicht hatte. Die Datenbank gibt daher nicht notwendigerweise den richtigen Status, sondern nur eine Annäherung an diesen an.

7.1 Work-Flow des Drucksystems

Der Benutzer erstellt einen Druckauftrag. Der Druckauftrag besteht aus den zu drucken- den Daten sowie aus Informationen für den Spooler, z. B. dem Namen des Druckers oder dem Namen der Druckwarteschlange und – optional – den Informationen für den Filter, z. B. druckerspezifische Optionen.

Mindestens eine zugeordnete Druckerwarteschlange ist für jeden Drucker vorhanden. Der Spooler hält den Druckauftrag in der Warteschlange, bis der gewünschte Drucker bereit ist, Daten zu empfangen. Wenn der Drucker druckbereit ist, sendet der Spooler die Daten über den Filter und das Backend an den Drucker.

Der Filter konvertiert die von der druckenden Anwendung generierten Daten (in der Regel PostScript oder PDF, aber auch ASCII, JPEG usw.) in druckerspezifische Daten (PostScript, PCL, ESC/P usw.). Die Funktionen des Druckers sind in den PPD-Dateien beschrieben. Eine PPD-Datei enthält druckerspezifische Optionen mit den Parametern, die erforderlich sind, um die Optionen auf dem Drucker zu aktivieren. Das Filtersystem stellt sicher, dass die vom Benutzer ausgewählten Optionen aktiviert werden.

Wenn Sie einen PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten in druckerspezifische PostScript-Daten. Hierzu ist kein Druckertreiber erforderlich. Wenn Sie einen Nicht-PostScript-Drucker verwenden, konvertiert das Filtersystem die Daten mithilfe von Ghostscript in druckerspezifische Daten. Hierzu ist ein für den Drucker geeigneter Ghostscript-Druckertreiber erforderlich. Das Back-End empfängt die druckerspezifischen Daten vom Filter und leitet sie an den Drucker weiter.

7.2 Methoden und Protokolle zum Anschließen von Druckern

Es gibt mehrere Möglichkeiten, einen Drucker an das System anzuschließen. Die Konfiguration des CUPS-Drucksystems unterscheidet nicht zwischen einem lokalen Drucker und einem Drucker, der über das Netzwerk an das System angeschlossen ist. Unter Linux müssen lokale Drucker wie im Handbuch des Druckerherstellers

beschrieben angeschlossen werden. CUPS unterstützt serielle, USB-, Parallel- und SCSI-Verbindungen. Weitere Informationen zum Anschließen von Druckern finden Sie im Beitrag *CUPS in aller Kürze* in der Support-Datenbank unter http://en.opensuse.org/SDB:CUPS_in_a_Nutshell.

WARNUNG: Ändern der Anschlüsse bei einem laufenden System

Vergessen Sie beim Anschließen des Druckers an den Computer nicht, dass während des Betriebs nur USB-Geräte angeschlossen werden können. Um Ihr System oder Ihren Drucker vor Schaden zu bewahren, fahren Sie das System herunter, wenn Sie Verbindungen ändern müssen, die keine USB-Verbindungen sind.

7.3 Installation der Software

PPD (PostScript Printer Description, PostScript-Druckerbeschreibung) ist die Computersprache, die die Eigenschaften, z. B. die Auflösung und Optionen wie die Verfügbarkeit einer Duplexeinheit, beschreibt. Diese Beschreibungen sind für die Verwendung der unterschiedlichen Druckeroptionen in CUPS erforderlich. Ohne eine PPD-Datei würden die Druckdaten in einem „rohen“ Zustand an den Drucker weitergeleitet werden, was in der Regel nicht erwünscht ist. Während der Installation von openSUSE werden viele PPD-Dateien vorinstalliert, um den Einsatz von Druckern ohne PostScript-Unterstützung zu ermöglichen.

Um einen PostScript-Drucker zu konfigurieren, sollten Sie sich zunächst eine geeignete PPD-Datei beschaffen. Viele PPD-Dateien sind im Paket `manufacturer-PPDs` enthalten, das im Rahmen der Standardinstallation automatisch installiert wird. Weitere Informationen hierzu finden Sie unter **Abschnitt 7.7.3, „PPD-Dateien in unterschiedlichen Paketen“** (S. 125) und **Abschnitt 7.8.2, „Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar“** (S. 129).

Neue PPD-Dateien können im Verzeichnis `/usr/share/cups/model/` gespeichert oder dem Drucksystem mit YaST hinzugefügt werden (siehe „Hinzufügen von PPD-Dateien mit YaST“ (Kapitel 2, *Einrichten von Hardware-Komponenten mit YaST*, ↑Start)). Die PPD-Dateien lassen sich anschließend während der Installation auswählen.

Seien Sie vorsichtig, wenn ein Druckerhersteller verlangt, dass Sie zusätzlich zum Ändern der Konfigurationsdateien vollständige Softwarepakete installieren sollen. Diese

Art der Installation könnte dazu führen, dass Sie den von openSUSE verfügbaren Support verlieren. Außerdem können Druckbefehle in der Ausführung variieren, sodass das System nicht mehr in der Lage ist, Geräte anderer Hersteller anzusprechen. Aus diesem Grund wird das Installieren von Herstellersoftware nicht empfohlen.

7.4 Netzwerkdrucker

Ein Netzwerkdrucker kann unterschiedliche Protokolle - einige von diesen sogar gleichzeitig. Obwohl die meisten der unterstützten Protokolle standardisiert sind, erweitern (ändern) einige Hersteller den Standard, weil sie Systeme testen, die in den Standard noch nicht ordnungsgemäß implementiert wurden, oder weil sie bestimmte Funktionen zur Verfügung stellen möchten, die im Standard nicht enthalten sind. Hersteller stellen in diesem Fall nur für wenige Betriebssysteme Treiber zur Verfügung und eliminieren so die Schwierigkeiten mit diesen Systemen. Linux-Treiber werden leider nur sehr selten zur Verfügung gestellt. Gegenwärtig können Sie nicht davon ausgehen, dass alle Protokolle problemlos mit Linux funktionieren. Um dennoch eine funktionale Konfiguration zu erhalten, müssen Sie daher möglicherweise mit den verschiedenen Optionen experimentieren.

WICHTIG: Fernzugriffseinstellungen

`cupsd` überwacht standardmäßig nur interne Netzwerkschnittstellen (`localhost`). Wenn Sie einen CUPS-Netzwerkserver einrichten, müssen Sie die Direktive `Listen` in `/etc/cups/cupsd.conf` ändern, damit auch das äußere Netzwerk überwacht wird.

CUPS unterstützt die Protokolle `socket`, `LPD`, `IPP` und `smb`.

`socket`

Socket bezieht sich auf eine Verbindung, in der die Daten an ein Internet-Socket gesendet werden, ohne dass zuvor ein Data-Handshake erfolgt. Einige der am häufigsten verwendeten Socket-Ports sind 9100 oder 35. Die Syntax der Geräte-URI (Uniform Resource Identifier) ist `socket://IP.of.the.printer:port`, zum Beispiel `socket://192.168.2.202:9100/`.

LPD (Line Printer Daemon)

Das bewährte LPD-Protokoll wird in RFC 1179 beschrieben. Mit diesem Protokoll werden einige druckauftragsbezogene Daten, z. B. die ID der Druckwarteschlange,

vor den eigentlichen Druckdaten gesendet. Daher muss die Druckwarteschlange beim Konfigurieren des LPD-Protokolls für die Datenübertragung angegeben werden. Die Implementierungen diverser Druckerhersteller sind flexibel genug, um beliebige Namen als Druckwarteschlange zu akzeptieren. Der zu verwendende Name müsste ggf. im Druckerhandbuch angegeben sein. Es werden häufig Bezeichnungen wie LPT, LPT1, LP1 o. ä. verwendet. Eine LPD-Warteschlange kann auch auf einem anderen Linux- oder Unix-Host im CUPS-System konfiguriert werden. Die Portnummer für einen LPD-Dienst lautet 515. Ein Beispiel für einen Gerät-URI ist `lpd://192.168.2.202/LPT1`.

IPP (Internet Printing Protocol)

IPP ist ein relativ neues Protokoll (1999), das auf dem HTTP-Protokoll basiert. Mit IPP können mehr druckauftragsbezogene Daten übertragen werden als mit den anderen Protokollen. CUPS verwendet IPP für die interne Datenübertragung. Dies ist das bevorzugte Protokoll für eine Weiterleitungswarteschlange zwischen zwei CUPS-Servern. Um IPP ordnungsgemäß konfigurieren zu können, ist der Name der Druckwarteschlange erforderlich. Die Portnummer für IPP lautet 631. Beispiele für Geräte-URIs sind `ipp://192.168.2.202/ps` und `ipp://192.168.2.202/printers/ps`.

SMB (Windows-Freigabe)

CUPS unterstützt auch das Drucken auf freigegebenen Druckern unter Windows. Das für diesen Zweck verwendete Protokoll ist SMB. SMB verwendet die Portnummern 137, 138 und 139. Beispiele für Geräte-URIs sind `smb://user:password@workgroup/smb.example.com/printer`, `smb://user:password@smb.example.com/printer` und `smb://smb.example.com/printer`.

Das vom Drucker unterstützte Protokoll muss vor der Konfiguration ermittelt werden. Wenn der Hersteller die erforderlichen Informationen nicht zur Verfügung stellt, können Sie das Protokoll mit dem Befehl `nmap` ermitteln, der Bestandteil des Pakets `nmap` ist. `nmap` überprüft einen Host auf offene Ports. Beispiel:

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

7.4.1 Konfigurieren von CUPS mit Kommandozeilenwerkzeugen

Sie können beim Konfigurieren eines Netzwerkdruckers die CUPS-Optionen nicht nur mit YaST einstellen, sondern können auch auf Kommandozeilenwerkzeuge wie `lpadmin` und `lpoptions` zugreifen. Sie benötigen einen Geräte-URI, der aus einem Bac-End, z. B. USB, und Parametern wie `/dev/usb/lp0` besteht. Der vollständige URI könnte beispielsweise wie folgt lauten: `parallel:/dev/lp0` (an den ersten Parallelanschluss angeschlossener Drucker) oder `usb:/dev/usb/lp0` (erster erkannter Drucker, der an den USB-Anschluss angeschlossen ist).

Mit `lpadmin` kann der CUPS-Serveradministrator Klassen und Druckwarteschlangen hinzufügen, entfernen und verwalten. Verwenden Sie die folgende Syntax, um eine Druckwarteschlange hinzuzufügen:

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

Das Gerät (`-v`) ist anschließend als *Warteschlange* (`-p`) verfügbar und verwendet die angegebene PPD-Datei (`-P`). Das bedeutet, dass Sie die PPD-Datei und den Namen des Geräts kennen müssen, wenn Sie den Drucker manuell konfigurieren möchten.

Verwenden Sie nicht `-E` als erste Option. Für alle CUPS-Befehle legt die Option `-E` als erstes Argument die Verwendung einer verschlüsselten Verbindung fest. Zur Aktivierung des Druckers muss die Option `-E` wie im folgenden Beispiel dargestellt verwendet werden:

```
lpadmin -p ps -v parallel:/dev/lp0 -P \  
/usr/share/cups/model/Postscript.ppd.gz -E
```

Im folgenden Beispiel wird ein Netzwerkdrucker konfiguriert:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \  
/usr/share/cups/model/Postscript-levell.ppd.gz -E
```

Weitere Optionen von `lpadmin` finden Sie auf der man-Seiten von `lpadmin(1)`.

Während der Druckerkonfiguration werden bestimmte Optionen standardmäßig gesetzt. Diese Optionen können (je nach Druckwerkzeug) für jeden Druckauftrag geändert werden. Es ist auch möglich, diese Standardoptionen mit YaST zu ändern. Legen Sie die Standardoptionen mithilfe der Kommandozeilenwerkzeuge wie folgt fest:

1 Zeigen Sie zunächst alle Optionen an:

```
lpoptions -p queue -l
```

Beispiel:

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

Die aktivierte Standardoption wird durch einen vorangestellten Stern (*) gekennzeichnet.

2 Ändern Sie die Option mit lpadmin:

```
lpadmin -p queue -o Resolution=600dpi
```

3 Prüfen Sie die neue Einstellung:

```
lpoptions -p queue -l
```

```
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

Wenn ein normaler Benutzer den Befehl `lpoptions` ausführt, werden die Einstellungen in `~/.lpoptions` geschrieben. `root`-Einstellungen werden jedoch in `/etc/cups/lpoptions` geschrieben.

7.5 Grafische Bedienoberflächen für das Drucken

Werkzeuge wie `xpp` und das KDE-Programm `KPrinter` bieten eine grafische Oberfläche für die Auswahl der Warteschlangen und zum Festlegen der CUPS-Standardoptionen und druckerspezifischen Optionen, die über die PPD-Datei zur Verfügung gestellt werden. Sie können `KPrinter` sogar als Standard-Druckoberfläche für Nicht-KDE-Anwendungen benutzen. Geben Sie im Druckdialogfeld dieser Anwendungen `kprinter` oder `kprinter--stdin` als Druckbefehl an. Der geeignete Befehl hängt davon ab, wie die Anwendung die Daten überträgt. Probieren Sie einfach aus, welcher Befehl `KPrinter` startet. Wenn die Anwendung ordnungsgemäß konfiguriert ist, sollte bei jedem Druckauftrag das Dialogfeld "KPrinter" geöffnet werden, in dem Sie eine

Warteschlange wählen und andere Druckoptionen festlegen können. Hierfür dürfen keine Konflikte zwischen den Druckereinstellungen der Anwendung und KPrinter auftreten. Die Druckoptionen dürfen nur über KPrinter geändert werden, nachdem das Programm aktiviert wurde. Weitere Informationen zu KPrinter finden Sie unter Abschnitt „Printing“ (Kapitel 1, *Getting Started with the KDE Desktop*, ↑KDE User Guide).

7.6 Drucken über die Kommandozeile

Um den Druckvorgang über die Kommandozeile zu starten, geben Sie `lp -d Name_der_WarteschlangeDateiname` ein und ersetzen die entsprechenden Namen für *Name_der_Warteschlange* und *Dateiname*.

Einige Anwendungen erfordern für den Druckvorgang den Befehl `lp`. Geben Sie in diesem Fall den richtigen Befehl in das Druckdialogfeld der Anwendung ohne Angabe des *Dateinamens* ein, z. B. `lp -d Name_der_Warteschlange`.

7.7 Spezielle Funktionen in openSUSE

Für openSUSE wurden mehrere CUPS-Funktionen angepasst. Im Folgenden werden einige der wichtigsten Änderungen beschrieben.

7.7.1 CUPS und Firewall

Nach einer Standardinstallation von openSUSE ist `SuSEfirewall2` aktiv, und externe Netzwerkgeräte sind in der `externen Zone` konfiguriert, die eingehenden Datenverkehr blockiert. Diese Standardeinstellungen müssen geändert werden, wenn Sie CUPS verwenden wollen. Weitere Informationen zur `SUSEfirewall2`-Konfiguration finden Sie unter [Abschnitt 35.4, „SuSEfirewall2“](#) (S. 659).

CUPS-Client

Normalerweise wird der CUPS-Client auf einer normalen Arbeitsstation ausgeführt, die sich in einem Netzwerk hinter einer Firewall befindet. In diesem Fall empfiehlt es

sich, die externen Netzwerkgeräte in der `internen` Zone zu konfigurieren, damit die Arbeitsstation innerhalb des Netzwerks erreichbar ist.

CUPS-Server

Wenn der CUPS-Server Teil des durch eine Firewall geschützten Netzwerks ist, sollte das externe Netzwerkgerät in der `internen` Zone der Firewall konfiguriert sein. Wenn der CUPS-Server in der externen Zone eingerichtet ist, muss TCP- und UDP-Port 631 geöffnet sein, damit der CUPS-Server im Netzwerk verfügbar ist.

7.7.2 Änderungen am CUPS-Druckdienst

Allgemeinere Funktionalität für `BrowseAllow` und `BrowseDeny`

Die festgelegten Zugriffsberechtigungen für `BrowseAllow` und `BrowseDeny` gelten für alle Pakettypen, die an `cupsd` gesendet werden. Die Standardeinstellungen in `/etc/cups/cupsd.conf` lauten wie folgt:

```
BrowseAllow @LOCAL
BrowseDeny All
```

und

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

Auf diese Weise können nur `LOCAL`-Hosts auf `cupsd` auf einem CUPS-Server zugreifen. `LOCAL`-Hosts sind Hosts, deren IP-Adressen zu einer Nicht-PPP-Schnittstelle (Schnittstellen, deren `IFF_POINTOPOINT`-Flags nicht gesetzt sind) und zum selben Netzwerk wie der CUPS-Server gehören. Pakete von allen anderen Hosts werden sofort abgelehnt.

cupsd standardmäßig aktiviert

In einer Standardinstallation ist `cupsd` automatisch aktiviert und ermöglicht so den Zugriff auf die Warteschlangen des CUPS-Netzwerkserver, ohne dass ein weiteres Eingreifen erforderlich ist. Die Einstellungen in „Allgemeinere Funktionalität für `BrowseAllow` und `BrowseDeny`“ (S. 124) sind wichtige Voraussetzungen für diese Funktion, da andernfalls die Sicherheit für eine automatische Aktivierung von `cupsd` nicht ausreichend wäre.

7.7.3 PPD-Dateien in unterschiedlichen Paketen

Die YaST-Druckerkonfiguration richtet die Warteschlangen für CUPS auf dem System nur mit den in `/usr/share/cups/model/` installierten PPD-Dateien ein. Um die geeigneten PPD-Dateien für das Druckermodell zu finden, vergleicht YaST während der Hardware-Erkennung den Hersteller und das Modell mit den Herstellern und Modellen, die auf dem System in den PPD-Dateien unter `/usr/share/cups/model/` verfügbar sind. Zu diesem Zweck generiert die YaST-Druckerkonfiguration eine Datenbank mit den Hersteller- und Modelldaten, die aus den PPD-Dateien extrahiert werden. Wenn Sie in der Liste der Hersteller und Modelle einen Drucker auswählen, erhalten Sie die PPD-Dateien, die dem Hersteller und dem Modell entsprechen.

Die Konfiguration, die nur PPD-Dateien und keine weiteren Informationsquellen verwendet, hat den Vorteil, dass die PPD-Dateien in `/usr/share/cups/model/` beliebig geändert werden können. Die YaST-Druckerkonfiguration erkennt die Änderungen und generiert die Hersteller- und Modelldatenbank neu. Wenn Sie beispielsweise nur mit PostScript-Druckern arbeiten, sind die Foomatic-PPD-Dateien im Paket `cups-drivers` oder die Gimp-Print-PPD-Dateien im Paket `cups-drivers-stp` in der Regel nicht erforderlich. Stattdessen können die PPD-Dateien für die PostScript-Drucker direkt in `/usr/share/cups/model/` kopiert werden (wenn sie nicht bereits im Paket `manufacturer-PPDs` vorhanden sind), um eine optimale Konfiguration der Drucker zu erzielen.

CUPS-PPD-Dateien im Paket cups

Die generischen PPD-Dateien im Paket `cups` wurden durch angepasste Foomatic-PPD-Dateien für PostScript-Drucker der Level 1 und Level 2 ergänzt:

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

PPD-Dateien im Paket **cups-drivers**

Der Foomatic-Druckerfilter `foomatic-rip` wird in der Regel zusammen mit Ghostscript für Nicht-PostScript-Drucker verwendet. Geeignete Foomatic PPD-Dateien haben die Einträge `*NickName: ... Foomatic/Ghostscript driver` und `*cupsFilter: ... foomatic-rip`. Diese PPD-Dateien befinden sich im Paket `cups-drivers`.

YaST bevorzugt eine Foomatic PPD-Datei, wenn eine Foomatic PPD-Datei mit dem Eintrag `*NickName: ... Foomatic ... (recommended)` mit dem Druckermodell übereinstimmt und das `Hersteller-PPDs-Paket` keine geeignetere PPD-Datei enthält.

Gimp-Print-PPD-Dateien im Paket **cups-drivers-stp**

Für viele Nicht-PostScript-Drucker kann an Stelle von `foomatic-rip` der CUPS-Filter `rastertoprinter` verwendet werden. Dieser Filter und die entsprechenden Gimp-Print-PPD-Dateien befinden sich im Paket `cups-drivers-stp`. Die Gimp Print PPD-Dateien befinden sich in `/usr/share/cups/model/stp/` und haben die Einträge `*NickName: ... CUPS+Gimp-Print` und `*cupsFilter: ... rastertoprinter`.

PPD-Dateien von Druckerherstellern im Paket **manufacturer-PPDs**

Das Paket `manufacturer-PPDs` enthält PPD-Dateien von Druckerherstellern, die unter einer ausreichend freien Lizenz veröffentlicht werden. PostScript-Drucker sollten mit der entsprechenden PPD-Datei des Druckerherstellers konfiguriert werden, da diese Datei die Verwendung aller Funktionen des PostScript-Druckers ermöglicht. YaST bevorzugt eine PPD-Datei aus dem Paket `manufacturer-PPDs`, wenn folgende Bedingungen erfüllt sind:

- Der während der Hardware-Erkennung ermittelte Hersteller und das Modell entsprechen dem Hersteller und dem Modell in einer PPD-Datei im Paket `manufacturer-PPDs`.
- Die PPD-Datei aus dem Paket `manufacturer-PPDs` ist die einzige passende PPD-Datei für das Druckermodell oder es gibt eine Foomatic PPD-Datei mit dem Eintrag `*NickName: ... Foomatic/Postscript (recommended)`, der ebenfalls mit dem Druckermodell übereinstimmt.

Entsprechend verwendet YaST in den folgenden Fällen keine PPD-Datei aus dem Paket `manufacturer-PPDs` :

- Die PPD-Datei im Paket `manufacturer-PPDs` entspricht nicht dem Hersteller und dem Modell. Dies kann der Fall sein, wenn das Paket `manufacturer-PPDs` nur eine PPD-Datei für ähnliche Modelle enthält, z. B. wenn für die einzelnen Modelle einer Modellserie keine separaten PPD-Dateien vorhanden sind, sondern die Modellbezeichnungen in der PPD-Datei beispielsweise in Form von `Funprinter 1000 series` angegeben werden.
- Die Verwendung der Foomatic-PostScript-PPD-Datei wird nicht empfohlen. Der Grund dafür ist möglicherweise, dass das Druckermodell im PostScript-Modus nicht effizient genug arbeitet, weil es in diesem Modus beispielsweise aufgrund von zu wenig Speicher unzuverlässig oder wegen seines zu schwachen Prozessors zu langsam arbeitet. Des Weiteren unterstützt der Drucker möglicherweise standardmäßig kein PostScript, da die PostScript-Unterstützung nur als optionales Modul verfügbar ist.

Wenn eine PPD-Datei im Paket `manufacturer-PPDs` für einen PostScript-Drucker geeignet ist, YaST diesen aus den gegebenen Gründen jedoch nicht konfigurieren kann, müssen Sie das entsprechende Druckermodell manuell in YaST auswählen.

7.8 Fehlersuche

In den folgenden Abschnitten werden einige der am häufigsten auftretenden Probleme mit der Druckerhardware und -software sowie deren Lösungen oder Umgehung beschrieben. Unter anderem werden die Themen GDI-Drucker, PPD-Dateien und Port-Konfiguration behandelt. Darüber hinaus werden gängige Probleme mit Netzwerkdruckern, fehlerhafte Ausdrücke und die Bearbeitung der Warteschlange erläutert.

7.8.1 Drucker ohne Unterstützung für eine Standard-Druckersprache

Diese Drucker unterstützen keine der geläufigen Druckersprachen und können nur mit proprietären Steuersequenzen adressiert werden. Daher funktionieren sie nur mit den Betriebssystemversionen, für die der Hersteller einen Treiber zur Verfügung stellt. GDI ist eine von Microsoft für Grafikgeräte entwickelte Programmierschnittstelle. In der Regel liefert der Hersteller nur Treiber für Windows. Da die Windows-Treiber die GDI-Schnittstelle verwenden, werden diese Drucker auch *GDI-Drucker* genannt. Das eigentliche Problem ist nicht die Programmierschnittstelle, sondern die Tatsache, dass diese Drucker nur mit der proprietären Druckersprache des jeweiligen Druckermodells adressiert werden können.

Der Betrieb einiger GDI-Drucker kann sowohl im GDI-Modus als auch in einer der Standard-Druckersprachen ausgeführt werden. Sehen Sie im Druckerhandbuch nach, ob dies möglich ist. Einige Modelle benötigen für diese Umstellung eine spezielle Windows-Software (Beachten Sie, dass der Windows-Druckertreiber den Drucker immer zurück in den GDI-Modus schalten kann, wenn von Windows aus gedruckt wird). Für andere GDI-Drucker sind Erweiterungsmodule für eine Standarddruckersprache erhältlich.

Einige Hersteller stellen für ihre Drucker proprietäre Treiber zur Verfügung. Der Nachteil proprietärer Druckertreiber ist, dass es keine Garantie gibt, dass diese mit dem installierten Drucksystem funktionieren und für die unterschiedlichen Hardwareplattformen geeignet sind. Im Gegensatz dazu sind Drucker, die eine Standard-Druckersprache unterstützen, nicht abhängig von einer speziellen Drucksystemversion oder einer bestimmten Hardwareplattform.

Anstatt Zeit darauf zu verwenden, einen proprietären Linux-Treiber zum Funktionieren zu bringen, ist es möglicherweise kosteneffektiver, einen unterstützten Drucker zu kaufen. Dadurch wäre das Treiberproblem ein für alle Mal aus der Welt geschafft und es wäre nicht mehr erforderlich, spezielle Treibersoftware zu installieren und zu konfigurieren oder Treiber-Updates zu beschaffen, die aufgrund neuer Entwicklungen im Drucksystem benötigt würden.

7.8.2 Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar

Wenn das Paket `manufacturer-PPDs` für einen PostScript-Drucker keine geeignete PPD-Datei enthält, sollte es möglich sein, die PPD-Datei von der Treiber-CD des Druckerherstellers zu verwenden, oder eine geeignete PPD-Datei von der Webseite des Druckerherstellers herunterzuladen.

Wenn die PPD-Datei als Zip-Archiv (`.zip`) oder als selbstextrahierendes Zip-Archiv (`.exe`) zur Verfügung gestellt wird, entpacken Sie sie mit `unzip`. Lesen Sie zunächst die Lizenzvereinbarung für die PPD-Datei. Prüfen Sie dann mit dem Dienstprogramm `cupstestppd`, ob die PPD-Datei den Spezifikationen „Adobe PostScript Printer Description File Format Specification, Version 4.3.“ entspricht. Wenn das Dienstprogramm „FAIL“ zurückgibt, sind die Fehler in den PPD-Dateien schwerwiegend und werden sehr wahrscheinlich größere Probleme verursachen. Die von `cupstestppd` protokollierten Problempunkte müssen behoben werden. Fordern Sie beim Druckerhersteller ggf. eine geeignete PPD-Datei an.

7.8.3 Parallele Anschlüsse

Die sicherste Methode ist, den Drucker direkt an den ersten Parallelanschluss anzuschließen und im BIOS die folgenden Einstellungen für Parallelanschlüsse auszuwählen:

- E/A-Adresse: 378 (hexadezimal)
- Interrupt: nicht relevant
- Modus: Normal, SPP oder Nur Ausgabe
- DMA: deaktiviert

Wenn der Drucker trotz dieser Einstellungen über den Parallelanschluss nicht angesprochen werden kann, geben Sie die E/A-Adresse explizit entsprechend den Einstellungen im BIOS in der Form `0x378` in `/etc/modprobe.conf` ein. Wenn zwei Parallelanschlüsse vorhanden sind, die auf die E/A-Adressen 378 und 278 (hexadezimal) gesetzt sind, geben Sie diese in Form von `0x378, 0x278` ein.

Wenn Interrupt 7 frei ist, kann er mit dem in **Beispiel 7.1**, „`/etc/modprobe.conf`: **Interrupt-Modus für den ersten parallelen Port**“ (S. 130) dargestellten Eintrag aktiviert werden. Prüfen Sie vor dem Aktivieren des Interrupt-Modus die Datei `/proc/interrupts`, um zu sehen, welche Interrupts bereits verwendet werden. Es werden nur die aktuell verwendeten Interrupts angezeigt. Dies kann sich je nachdem, welche Hardwarekomponenten aktiv sind, ändern. Der Interrupt für den Parallelanschluss darf von keinem anderen Gerät verwendet werden. Wenn Sie sich diesbezüglich nicht sicher sind, verwenden Sie den Polling-Modus mit `irq=none`.

Beispiel 7.1 *`/etc/modprobe.conf`: Interrupt-Modus für den ersten parallelen Port*

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

7.8.4 Netzwerkdrucker-Verbindungen

Netzwerkprobleme identifizieren

Schließen Sie den Drucker direkt an den Computer an. Konfigurieren Sie den Drucker zu Testzwecken als lokalen Drucker. Wenn dies funktioniert, werden die Probleme netzwerkseitig verursacht.

TCP/IP-Netzwerk prüfen

Das TCP/IP-Netzwerk und die Namensauflösung müssen funktionieren.

Überprüfen des Fernzugriffs

`cupsd` überwacht standardmäßig nur interne Netzwerkschnittstellen (`localhost`). Prüfen Sie, ob die `Listen`-Direktiven in `/etc/cups/cupsd.conf` den Zugriff aus dem äußeren Netzwerk zulassen:

```
Listen 192.168.2, *:631
```

Überprüfen der Firewall-Einstellungen

Ein CUPS-Server muss entweder in der internen Firewall-Zone eingerichtet sein, oder, wenn er in der externen Zone eingerichtet ist, in der Lage sein, Daten an UDP- und TCP-Port 631 zu senden und zu empfangen.

Entfernten `lpd` prüfen

Geben Sie den folgenden Befehl ein, um zu testen, ob zu `lpd` (Port 515) auf `host` eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 515 && echo ok || echo failed
```

Wenn die Verbindung zu `lpd` nicht hergestellt werden kann, ist `lpd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor.

Geben Sie als `root` den folgenden Befehl ein, um einen (möglicherweise sehr langen) Statusbericht für `queue` auf dem entfernten `host` abzufragen, vorausgesetzt, der entsprechende `lpd` ist aktiv und der Host akzeptiert Abfragen:

```
echo -e "\004queue" \  
| netcat -w 2 -p 722 host 515
```

Wenn `lpd` nicht antwortet, ist er entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. Wenn `lpd` reagiert, sollte die Antwort zeigen, warum das Drucken in der `queue` auf `host` nicht möglich ist. Wenn Sie eine Antwort wie die in **Beispiel 7.2, „Fehlermeldung von `lpd`“** (S. 131) erhalten, wird das Problem durch den entfernten `lpd` verursacht.

Beispiel 7.2 Fehlermeldung von `lpd`

```
lpd: your host does not have line printer access  
lpd: queue does not exist  
printer: spooling disabled  
printer: printing disabled
```

Entfernten `cupsd` prüfen

Standardmäßig sendet der CUPS-Netzwerkserver über Broadcast alle 30 Sekunden Informationen über seine Warteschlangen an UDP-Port 631. Demzufolge kann mit dem folgenden Befehl getestet werden, ob im Netzwerk ein CUPS-Netzwerkserver vorhanden ist.

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

Wenn ein CUPS-Netzwerkserver vorhanden ist, der Informationen über Broadcasting sendet, erscheint die Ausgabe wie in **Beispiel 7.3, „Broadcast vom CUPS-Netzwerkserver“** (S. 131) dargestellt.

Beispiel 7.3 Broadcast vom CUPS-Netzwerkserver

```
ipp://192.168.2.202:631/printers/queue
```

Mit dem folgenden Befehl können Sie testen, ob mit `cupsd` (Port 631) auf *host* eine TCP-Verbindung hergestellt werden kann:

```
netcat -z host 631 && echo ok || echo failed
```

Wenn die Verbindung zu `cupsd` nicht hergestellt werden kann, ist `cupsd` entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. `lpstat -h host -l -t` gibt einen (möglicherweise sehr langen) Statusbericht für alle Warteschlangen auf *host* zurück, vorausgesetzt, dass der entsprechende `cupsd` aktiv ist und der Host Abfragen akzeptiert.

Mit dem nächsten Befehl können Sie testen, ob die *Warteschlange* auf *Host* einen Druckauftrag akzeptiert, der aus einem einzigen CR-Zeichen (Carriage-Return) besteht. In diesem Fall sollte nichts gedruckt werden. Möglicherweise wird eine leere Seite ausgegeben.

```
echo -en "\r" \  
| lp -d queue -h host
```

Fehlerbehebung für einen Netzwerkdrucker oder eine Print Server Box

Spooler, die in einer Print Server Box ausgeführt werden, verursachen gelegentlich Probleme, wenn sie viele Druckaufträge bearbeiten müssen. Da dies durch den Spooler in der Print Server Box verursacht wird, können Sie nichts dagegen tun. Sie haben jedoch die Möglichkeit, den Spooler in der Print Server-Box zu umgehen, indem Sie den an die Print Server-Box angeschlossenen Drucker über TCP-Socket direkt ansprechen. Weitere Informationen hierzu finden Sie unter [Abschnitt 7.4, „Netzwerkdrucker“](#) (S. 119).

Auf diese Weise wird die Print Server-Box auf einen Konvertierer zwischen den unterschiedlichen Formen der Datenübertragung (TCP/IP-Netzwerk und lokale Druckerverbindung) reduziert. Um diese Methode verwenden zu können, müssen Sie den TCP-Port der Print Server Box kennen. Wenn der Drucker eingeschaltet und an die Print Server Box angeschlossen ist, kann dieser TCP-Port in der Regel mit dem Dienstprogramm `nmap` aus dem Paket `nmap` ermittelt werden, wenn die Print Server Box einige Zeit eingeschaltet ist. Beispiel: `nmap IP-Adresse` gibt die folgende Ausgabe für eine Print Server-Box zurück:

Port	State	Service
23/tcp	open	telnet
80/tcp	open	http
515/tcp	open	printer

```
631/tcp      open        cups
9100/tcp     open        jetdirect
```

Diese Ausgabe gibt an, dass der an die Print Server-Box angeschlossene Drucker über TCP-Socket an Port 9100 angesprochen werden kann. `nmap` prüft standardmäßig nur eine bestimmte Anzahl der allgemein bekannten Ports, die in `/usr/share/nmap/nmap-services` aufgeführt sind. Um alle möglichen Ports zu überprüfen, verwenden Sie den Befehl `nmap -p Ausgangs-Port-Ziel-Port IP-Adresse`. Dies kann einige Zeit dauern. Weitere Informationen finden Sie auf der man-Seite zu `yplibind`.

Geben Sie einen Befehl ein wie

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port
cat file | netcat -w 1 IP-address port
```

um Zeichenketten oder Dateien direkt an den entsprechenden Port zu senden, um zu testen, ob der Drucker auf diesem Port angesprochen werden kann.

7.8.5 Fehlerhafte Ausdrücke ohne Fehlermeldung

Für das Drucksystem ist der Druckauftrag abgeschlossen, wenn das CUPS-Back-End die Datenübertragung an den Empfänger (Drucker) abgeschlossen hat. Wenn die weitere Verarbeitung auf dem Empfänger nicht erfolgt, z. B., wenn der Drucker die druckerspezifischen Daten nicht drucken kann, wird dies vom Drucksystem nicht erkannt. Wenn der Drucker die druckerspezifischen Daten nicht drucken kann, wählen Sie eine andere PPD-Datei, die für den Drucker besser geeignet ist.

7.8.6 Deaktivierte Warteschlangen

Wenn die Datenübertragung zum Empfänger auch nach mehreren Versuchen nicht erfolgreich ist, meldet das CUPS-Back-End, z. B. `USB` oder `socket`, dem Drucksystem (an `cupsd`) einen Fehler. Das Backend entscheidet, ob und wie viele Versuche sinnvoll sind, bis die Datenübertragung als nicht möglich abgebrochen wird. Da weitere Versuche vergeblich wären, deaktiviert `cupsd` das Drucken für die entsprechende Warteschlange. Nachdem der Systemadministrator das Problem behoben hat, muss er das Drucken mit dem Befehl `/usr/bin/enable` wieder aktivieren.

7.8.7 CUPS-Browsing: Löschen von Druckaufträgen

Wenn ein CUPS-Netzwerkserver seine Warteschlangen den Client-Hosts via Browsing bekannt macht und auf den Host-Clients ein geeigneter lokaler `cupsd` aktiv ist, akzeptiert der Client-`cupsd` Druckaufträge von Anwendungen und leitet sie an den `cupsd` auf dem Server weiter. Wenn `cupsd` einen Druckauftrag akzeptiert, wird diesem eine neue Auftragsnummer zugewiesen. Daher unterscheidet sich die Auftragsnummer auf dem Client-Host von der auf dem Server. Da ein Druckauftrag in der Regel sofort weitergeleitet wird, kann er mit der Auftragsnummer auf dem Client-Host nicht gelöscht werden, da der Client-`cupsd` den Druckauftrag als abgeschlossen betrachtet, sobald dieser an den Server-`cupsd` weitergeleitet wurde.

Um einen Druckauftrag auf dem Server zu löschen, geben Sie ein Kommando wie `lpstat -h cups.example.com -o` ein. Sie ermitteln damit die Auftragsnummer auf dem Server, wenn der Server den Druckauftrag nicht bereits abgeschlossen (d. h. an den Drucker gesendet) hat. Mithilfe dieser Auftragsnummer kann der Druckauftrag auf dem Server gelöscht werden:

```
cancel -h cups.example.com queue-jobnumber
```

7.8.8 Fehlerhafte Druckaufträge und Fehler bei der Datenübertragung

Druckaufträge verbleiben in den Warteschlangen und das Drucken wird fortgesetzt, wenn Sie den Drucker aus- und wieder einschalten oder den Computer während des Druckvorgangs herunterfahren und neu booten. Fehlerhafte Druckaufträge müssen mit `cancel` aus der Warteschlange entfernt werden.

Wenn ein Druckauftrag fehlerhaft ist oder während der Kommunikation zwischen dem Host und dem Drucker ein Fehler auftritt, druckt der Drucker mehrere Seiten Papier mit unleserlichen Zeichen, da er die Daten nicht ordnungsgemäß verarbeiten kann. Führen Sie die folgenden Schritte aus, um dies zu beheben:

- 1 Um den Druckvorgang zu beenden, entfernen Sie das Papier aus Tintenstrahldruckern oder öffnen Sie die Papierzufuhr bei Laserdruckern. Qualitativ hochwertige

Drucker sind mit einer Taste zum Abbrechen des aktuellen Druckauftrags ausgestattet.

- 2 Der Druckauftrag befindet sich möglicherweise noch in der Warteschlange, da die Aufträge erst dann entfernt werden, wenn sie vollständig an den Drucker übertragen wurden. Geben Sie `lpstat -o` oder `lpstat -h cups.example.com -o` ein, um zu prüfen, über welche Warteschlange aktuell gedruckt wird. Löschen Sie den Druckauftrag mit `cancel Warteschlange-Auftragsnummer` oder mit `cancel -h cups.example.com Warteschlange-Auftragsnummer`.
- 3 Auch wenn der Druckauftrag aus der Warteschlange gelöscht wurde, werden einige Daten weiter an den Drucker gesendet. Prüfen Sie, ob ein CUPS-Backend-Prozess für die entsprechende Warteschlange ausgeführt wird und wenn ja, beenden Sie ihn. Für einen an den Parallelanschluss angeschlossenen Drucker geben Sie beispielsweise den Befehl `fuser -k /dev/lp0` ein, um alle Prozesse zu beenden, die aktuell noch auf den Drucker (den parallelen Port) zugreifen.
- 4 Setzen Sie den Drucker vollständig zurück, indem Sie ihn für einige Zeit ausschalten. Legen Sie anschließend Papier ein und schalten Sie den Drucker wieder ein.

7.8.9 Fehlerbehebung beim CUPS-Drucksystem

Suchen Sie Probleme im CUPS-Drucksystem mithilfe des folgenden generischen Verfahrens:

- 1 Setzen Sie `LogLevel debug` in `/etc/cups/cupsd.conf`.
- 2 Stoppen Sie `cupsd`.
- 3 Entfernen Sie `/var/log/cups/error_log*`, um das Durchsuchen sehr großer Protokolldateien zu vermeiden.
- 4 Starten Sie `cupsd`.
- 5 Wiederholen Sie die Aktion, die zu dem Problem geführt hat.

- 6 Lesen Sie die Meldungen in `/var/log/cups/error_log*`, um die Ursache des Problems zu identifizieren.

7.8.10 Weiterführende Informationen

Lösungen zu vielen spezifischen Problemen sind in der SUSE-Support-Datenbank enthalten (<http://en.opensuse.org/SDB:SDB>). Die gesuchten Themen finden Sie am schnellsten mit einer Textsuche nach `SDB:CUPS`.

Das X Window-System

Das X Window-System (X11) ist der Industriestandard für grafische Bedienoberflächen unter UNIX. X ist netzwerkbasiert und ermöglicht es, auf einem Host gestartete Anwendungen auf einem anderen, über eine beliebige Art von Netzwerk (LAN oder Internet) verbundenen Host anzuzeigen. In diesem Kapitel werden die Einrichtung und die Optimierung der X Window-Systemumgebung beschrieben. Sie erhalten dabei Hintergrundinformationen zur Verwendung von Schriften in openSUSE®.

8.1 Manuelles Konfigurieren des X Window-Systems

Standardmäßig ist das X Windows System mit der unter Abschnitt „Einrichten von Grafikkarte und Monitor“ (Kapitel 2, *Einrichten von Hardware-Komponenten mit YaST*, ↑Start) beschriebenen SaX2-Schnittstelle konfiguriert. Alternativ kann es manuell konfiguriert werden, indem Sie die Konfigurationsdateien bearbeiten.

WARNUNG: Fehlerhafte X-Konfigurationen können Ihre Hardware beschädigen

Seien Sie sehr vorsichtig, wenn Sie die Konfiguration des X Window-Systems ändern. Starten Sie auf keinen Fall das X Window-System, bevor die Konfiguration abgeschlossen ist. Ein falsch konfiguriertes System kann Ihre Hardware irreparabel beschädigen (dies gilt insbesondere für Monitore mit fester Frequenz). Die Autoren dieses Buchs und die Entwickler von openSUSE übernehmen keine Haftung für mögliche Schäden. Die folgenden Informationen basieren

auf sorgfältiger Recherche. Es kann jedoch nicht garantiert werden, dass alle hier aufgeführten Methoden fehlerfrei sind und keinen Schaden an Ihrer Hardware verursachen können.

Das Kommando `sax2` erstellt die Datei `/etc/X11/xorg.conf`. Dabei handelt es sich um die primäre Konfigurationsdatei des X Window System. Hier finden Sie alle Einstellungen, die Grafikkarte, Maus und Monitor betreffen.

In den folgenden Abschnitten wird die Struktur der Konfigurationsdatei `/etc/X11/xorg.conf` beschrieben. Sie ist in mehrere Abschnitte gegliedert, die jeweils für bestimmte Aspekte der Konfiguration verantwortlich sind. Jeder Abschnitt beginnt mit dem Schlüsselwort `Section` <Bezeichnung> und endet mit `EndSection`. Die folgende Konvention gilt für alle Abschnitte:

```
Section "designation"
    entry 1
    entry 2
    entry n
EndSection
```

Die verfügbaren Abschnittstypen finden Sie in [Tabelle 8.1, „Abschnitte in /etc/X11/xorg.conf“](#) (S. 138).

Tabelle 8.1 *Abschnitte in /etc/X11/xorg.conf*

Typ	Bedeutung
Dateien	Die Pfade für die Schriften und die RGB-Farbtabelle.
ServerFlags	Allgemeine Schalter für das Serververhalten.
Modul	Eine Liste mit Modulen, die der Server laden sollte
InputDevice	Eingabegeräte wie Tastaturen und spezielle Eingabegeräte (Touchpads, Joysticks usw.) werden in diesem Abschnitt konfiguriert. Wichtige Parameter in diesem Abschnitt sind <code>Driver</code> und die Optionen für <code>Protocol</code> und <code>Device</code> . Normalerweise ist dem Computer ein <code>InputDevice</code> -Abschnitt pro Gerät angefügt.

Typ	Bedeutung
Monitor	Der verwendete Monitor. Wichtige Elemente dieses Abschnitts sind die Kennung (<code>Identifier</code>), auf die später in der Definition von <code>Screen</code> eingegangen wird, die Aktualisierungsrate (<code>VertRefresh</code>) und die Grenzwerte für die Synchronisierungsfrequenz (<code>HorizSync</code> und <code>VertRefresh</code>). Die Einstellungen sind in MHz, kHz und Hz angegeben. Normalerweise akzeptiert der Server nur Modeline-Werte, die den Spezifikationen des Monitors entsprechen. Dies verhindert, dass der Monitor versehentlich mit zu hohen Frequenzen angesteuert wird.
Modi	Die Modeline-Parameter für die spezifischen Bildschirmauflösungen. Diese Parameter können von <code>SaX2</code> auf Grundlage der vom Benutzer vorgegebenen Werte berechnet werden und müssen in der Regel nicht geändert werden. Nehmen Sie hier beispielsweise dann Änderungen vor, wenn Sie einen Monitor mit fester Frequenz anschließen möchten. Details zur Bedeutung der einzelnen Zahlenwerte finden Sie in den HOWTO-Dateien unter <code>/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO</code> (im Paket <code>howtoenh</code>).
Gerät	Eine spezifische Grafikkarte. Sie wird mit ihrem beschreibenden Namen angeführt.
Screen	Verbindet einen <code>Monitor</code> und ein <code>Device</code> , damit alle erforderlichen Einstellungen für <code>X.Org</code> gewährleistet sind. Geben Sie im Unterabschnitt <code>Display</code> die Größe des virtuellen Bildschirms (<code>Virtual</code>), den <code>ViewPort</code> und die für diesen Bildschirm verwendeten Modi (<code>Modes</code>) an.
ServerLayout	Das Layout einer Einzel- oder Multihead-Konfiguration. In diesem Abschnitt werden Kombinationen aus Eingabegeräten (<code>InputDevice</code>) und Anzeigegeräten (<code>Screen</code>) festgelegt.
DRI	Bietet Informationen für die Direct Rendering Infrastructure (DRI).

Monitor, Device und Screen werden im Folgenden genauer erläutert. Weitere Informationen zu den anderen Abschnitten finden Sie auf den man-Seiten von X.Org und `xorg.conf`.

Die Datei `xorg.conf` kann mehrere unterschiedliche Abschnitte vom Typ `Monitor` und `Device` enthalten. Manchmal gibt es sogar mehrere Abschnitte vom Typ `Screen`. Der Abschnitt `ServerLayout` legt fest, welche dieser Abschnitte verwendet werden.

8.1.1 Abschnitt "Screen"

Der Abschnitt "Screen" kombiniert einen Monitor mit einem Device-Abschnitt und legt fest, welche Auflösung und Farbtiefe verwendet werden sollen. Der Abschnitt "Screen" kann beispielsweise wie in [Beispiel 8.1, „Abschnitt "Screen" der Datei /etc/X11/xorg.conf“](#) (S. 140) aussehen.

Beispiel 8.1 Abschnitt "Screen" der Datei `/etc/X11/xorg.conf`

```
Section "Screen"❶
    DefaultDepth 16❷
    SubSection "Display"❸
        Depth 16❹
        Modes "1152x864" "1024x768" "800x600"❺
        Virtual 1152x864❻
    EndSubSection
    SubSection "Display"
        Depth 24
        Modes "1280x1024"
    EndSubSection
    SubSection "Display"
        Depth 32
        Modes "640x480"
    EndSubSection
    SubSection "Display"
        Depth 8
        Modes "1280x1024"
    EndSubSection
    Device "Device[0]"
    Identifier "Screen[0]"❼
    Monitor "Monitor[0]"
EndSection
```

- ❶ Section legt den Typ des Abschnitts fest, in diesem Fall `Screen`.
- ❷ `DefaultDepth` bestimmt die Farbtiefe, die standardmäßig verwendet werden soll, wenn keine andere Farbtiefe explizit angegeben wird.

- ③ Für jede Farbtiefe werden verschiedene `Display`-Unterabschnitte angegeben.
- ④ `Depth` bestimmt die Farbtiefe, die mit diesem Satz von `Display`-Einstellungen benutzt werden soll. Mögliche Werte sind 8, 15, 16, 24 und 32, obwohl möglicherweise nicht alle davon durch alle X-Server-Module oder -Auflösungen unterstützt werden.
- ⑤ Der Abschnitt `Modes` enthält eine Liste der möglichen Bildschirmauflösungen. Diese Liste wird vom X-Server von links nach rechts gelesen. Zu jeder Auflösung sucht der X-Server eine passende `Modeline` im Abschnitt `Modes`. Die `Modeline` ist von den Fähigkeiten des Monitors und der Grafikkarte abhängig. Die Einstellungen unter `Monitor` bestimmen die `Modeline`.

Die erste passende Auflösung ist der Standardmodus (`Default mode`). Mit `Strg + Alt + +` (auf dem Ziffernblock) können Sie zur nächsten Auflösung rechts in der Liste wechseln. Mit `Strg + Alt + -` (auf dem Ziffernblock) können Sie zur vorherigen Auflösung wechseln. So lässt sich die Auflösung ändern, während X ausgeführt wird.

- ⑥ Die letzte Zeile des Unterabschnitts `Display` mit `Depth 16` bezieht sich auf die Größe des virtuellen Bildschirms. Die maximal mögliche Größe eines virtuellen Bildschirms ist von der Menge des Arbeitsspeichers auf der Grafikkarte und der gewünschten Farbtiefe abhängig, nicht jedoch von der maximalen Auflösung des Monitors. Wenn Sie diese Zeile auslassen, entspricht die virtuelle Auflösung der physikalischen Auflösung. Da moderne Grafikkarten über viel Grafikspeicher verfügen, können Sie sehr große virtuelle Desktops erstellen. Gegebenenfalls ist es aber nicht mehr möglich, 3-D-Funktionen zu nutzen, wenn ein virtueller Desktop den größten Teil des Grafikspeichers belegt. Wenn die Grafikkarte beispielsweise über 16 MB RAM verfügt, kann der virtuelle Bildschirm bei einer Farbtiefe von 8 Bit bis zu 4096 x 4096 Pixel groß sein. Insbesondere bei beschleunigten Grafikkarten ist es nicht empfehlenswert, den gesamten Arbeitsspeicher für den virtuellen Bildschirm zu verwenden, weil der Kartenspeicher auch für diverse Schrift- und Grafik-Caches genutzt wird.
- ⑦ In der Zeile `Identifizier` (hier `Screen[0]`) wird für diesen Abschnitt ein Name vergeben, der als eindeutige Referenz im darauf folgenden Abschnitt `ServerLayout` verwendet werden kann. Die Zeilen `Device` und `Monitor` geben die Grafikkarte und den Monitor an, die zu dieser Definition gehören. Hierbei handelt es sich nur um Verbindungen zu den Abschnitten `Device` und `Monitor` mit ihren entsprechenden Namen bzw. Kennungen (*identifiers*). Diese Abschnitte werden weiter unten detailliert beschrieben.

8.1.2 Abschnitt "Device"

Im Abschnitt "Device" wird eine bestimmte Grafikkarte beschrieben. `xorg.conf` kann beliebig viele Grafikkarteneinträge enthalten. Jedoch muss der Name der Grafikkarten eindeutig sein. Hierfür wird das Schlüsselwort `Identifizier` verwendet. Wenn mehrere Grafikkarten installiert sind, werden die Abschnitte einfach der Reihe nach nummeriert. Die erste wird als `Device[0]`, die zweite als `Device[1]` usw. eingetragen. Die folgende Datei zeigt einen Auszug aus dem Abschnitt `Device` eines Computers mit einer Matrox Millennium PCI-Grafikkarte (wie von SaX2 konfiguriert):

```
Section "Device"
    BoardName      "MGA2064W"
    BusID          "0:19:0"❶
    Driver         "mga"❷
    Identifizier   "Device[0]"
    VendorName     "Matrox"
    Option        "sw_cursor"
EndSection
```

- ❶ Der Wert unter `BusID` steht für den PCI- oder AGP-Steckplatz, in dem die Grafikkarte installiert ist. Er entspricht der ID, die bei Eingabe des Befehls `lspci` angezeigt wird. Der X-Server benötigt Informationen im Dezimalformat, `lspci` zeigt die Informationen jedoch im Hexadezimalformat an. Der Wert von `BusID` wird von SaX2 automatisch erkannt.
- ❷ Der Wert von `Driver` wird automatisch von SaX2 eingestellt und gibt den Treiber an, der für Ihre Grafikkarte verwendet wird. Wenn es sich um eine Matrox Millennium-Grafikkarte handelt, heißt das Treibermodul `mga`. Anschließend durchsucht der X-Server den `ModulePath`, der im Abschnitt `Files` des Unterverzeichnisses `drivers` angegeben ist. Bei einer Standardinstallation handelt es sich hierbei um das Verzeichnis `/usr/lib/xorg/modules/drivers._drv.o` wird an den Namen angehängt, sodass beispielsweise im Falle des `mga`-Treibers die Treiberdatei `mga_drv.o` geladen wird.

Das Verhalten des X-Servers bzw. des Treibers kann außerdem durch weitere Optionen beeinflusst werden. Ein Beispiel hierfür ist die Option `sw_cursor`, die im Abschnitt "Device" festgelegt wird. Diese deaktiviert den Hardware-Mauszeiger und stellt den Mauszeiger mithilfe von Software dar. Je nach Treibermodul können verschiedene Optionen verfügbar sein. Diese finden Sie in den Beschreibungsdateien der Treibermodule im Verzeichnis `/usr/share/doc/paket_name`. Allgemein gültige Optionen

finden Sie außerdem auf den entsprechenden man-Seiten (`man xorg.conf`, `man X.Org` und `man 4 chips`).

Wenn die Grafikkarte über mehrere Videoanschlüsse verfügt, können die verschiedenen an der Karte angeschlossenen Geräte in SaX2 als eine Ansicht konfiguriert werden.

8.1.3 Abschnitte "Monitor" und "Modes"

So wie die Abschnitte vom Typ `Device` jeweils für eine Grafikkarte verwendet werden, beschreiben die Abschnitte `Monitor` und `Modes` jeweils einen Monitor. Die Konfigurationsdatei `/etc/X11/xorg.conf` kann beliebig viele Abschnitte vom Typ `Monitor` enthalten. Jeder `Monitor`-Abschnitt verweist, sofern verfügbar, auf einen `Modes`-Abschnitt mit der Zeile `UseModes`. Wenn für den Abschnitt `Monitor` kein `Modes`-Abschnitt zur Verfügung steht, berechnet der X-Server aus den allgemeinen Synchronisierungswerten passende Werte. Der Abschnitt "ServerLayout" gibt an, welcher `Monitor`-Abschnitt zu verwenden ist.

Monitordefinitionen sollten nur von erfahrenen Benutzern festgelegt werden. Die `Modelines` stellen einen bedeutenden Teil der `Monitor`-Abschnitte dar. `Modelines` legen die horizontalen und vertikalen Frequenzen für die jeweilige Auflösung fest. Die Monitoreigenschaften, insbesondere die zulässigen Frequenzen, werden im Abschnitt `Monitor` gespeichert.

WARNUNG

Die `Modelines` sollten Sie nur ändern, wenn Sie sich sehr gut mit den Bildschirmfunktionen und der Grafikkarte auskennen, da der Bildschirm durch eine falsche Änderung dieser Zeilen ernsthaft Schaden nehmen kann.

Falls Sie Ihre eigenen Monitorbeschreibungen entwickeln möchten, sollten Sie sich genauestens mit der Dokumentation unter `/usr/share/X11/doc` vertraut machen.

Heutzutage ist es nur sehr selten erforderlich, `Modelines` manuell festzulegen. Wenn Sie mit einem modernen Multisync-Monitor arbeiten, können die zulässigen Frequenzen und die optimalen Auflösungen in aller Regel vom X-Server direkt per DDC vom Monitor abgerufen werden, wie im SaX2-Konfigurationsabschnitt beschrieben. Ist dies aus irgendeinem Grund nicht möglich, können Sie auf einen der VESA-Modi des X-Servers zurückgreifen. Dies funktioniert in Verbindung mit fast allen Kombinationen aus Grafikkarte und Monitor.

8.2 Installation und Konfiguration von Schriften

Die Installation zusätzlicher Schriften in openSUSE ist sehr einfach. Kopieren Sie einfach die Schriften in ein beliebiges Verzeichnis im X11-Pfad für Schriften (siehe [Abschnitt 8.2.1, „X11 Core-Schriften“](#) (S. 145)). Damit die Schriften verwendet werden können, sollte das Installationsverzeichnis ein Unterverzeichnis der Verzeichnisse sein, die in `/etc/fonts/fonts.conf` konfiguriert sind (siehe [Abschnitt 8.2.2, „Xft“](#) (S. 146)), oder es sollte über `/etc/fonts/suse-font-dirs.conf` in diese Datei eingefügt worden sein.

Nachfolgend ein Ausschnitt aus der Datei `/etc/fonts/suse-font-dirs.conf`. Diese Datei ist in die Konfiguration integriert, da sie mit dem Verzeichnis `/etc/fonts/conf.d` verknüpft ist, das wiederum durch `/etc/fonts/fonts.conf` eingeschlossen wurde. Alle Dateien und symbolischen Links in diesem Verzeichnis, die mit einer zweistelligen Zahl beginnen, werden von `fontconfig` geladen. Ausführliche Erläuterungen zu dieser Funktion finden Sie in der Datei `/etc/fonts/conf.d/README`.

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/.fonts</dir>
<include ignore_missing="yes">conf.d</include>
```

`/etc/fonts/suse-font-dirs.conf` wird automatisch generiert, um Schriften abzurufen, die mit Anwendungen (meist von anderen Herstellern) wie OpenOffice.org, Java oder Adobe Acrobat Reader geliefert werden. Einige typische Einträge von `/etc/fonts/suse-font-dirs.conf` :

```
<dir>/usr/lib64/ooo-2.0/share/fonts</dir>
<dir>/usr/lib/jvm/java-1_4_2-sun-1.4.2.11/jre/lib/fonts</dir>
<dir>/usr/lib64/jvm/java-1.5.0-sun-1.5.0_07/jre/lib/fonts</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font/PFM</dir>
```

Um zusätzliche Schriften systemweit zu installieren, kopieren Sie Schriftdateien manuell (als `root`) in ein geeignetes Verzeichnis, beispielsweise `/usr/share/fonts/truetype`. Alternativ kann diese Aktion auch mithilfe des KDE-Schrift-

Installationsprogramms im KDE-Kontrollzentrum durchgeführt werden. Das Ergebnis ist dasselbe.

Anstatt die eigentlichen Schriften zu kopieren, können Sie auch symbolische Links erstellen. Beispielsweise kann dies sinnvoll sein, wenn Sie lizenzierte Schriften auf einer gemounteten Windows-Partition haben und diese nutzen möchten. Führen Sie anschließend `SuSEconfig --module fonts` aus.

`SuSEconfig --module fonts` startet das für die Schriftenkonfiguration zuständige Skript `/usr/sbin/fonts-config`. Weitere Informationen zu diesem Skript finden Sie auf der man-Seite `man fonts-config`.

Die Vorgehensweise ist für Bitmap-, TrueType- und OpenType-Schriften sowie Type1-Schriften (PostScript) dieselbe. Alle diese Schriften können in einem beliebigen Verzeichnis installiert werden.

X.Org enthält zwei komplett unterschiedliche Schriftsysteme: das alte *X11-Core-Schriftsystem* und das neu entwickelte System *Xft und fontconfig*. In den folgenden Abschnitten wird kurz auf diese beiden Systeme eingegangen.

8.2.1 X11 Core-Schriften

Heute unterstützt das X11 Core-Schriftsystem nicht nur Bitmap-Schriften, sondern auch skalierbare Schriften wie Type1-, TrueType- und OpenType-Schriften. Skalierbare Schriften werden nur ohne Antialiasing und Subpixel-Rendering unterstützt und das Laden von großen skalierbaren Schriften mit Zeichen für zahlreiche Sprachen kann sehr lange dauern. Unicode-Schriften werden ebenfalls unterstützt, aber ihre Verwendung kann mit erheblichem Zeitaufwand verbunden sein und erfordert mehr Speicher.

Das X11 Core-Schriftsystem weist mehrere grundsätzliche Schwächen auf. Es ist überholt und kann nicht mehr sinnvoll erweitert werden. Zwar muss es noch aus Gründen der Abwärtskompatibilität beibehalten werden, doch das modernere System "Xft/fontconfig" sollte immer verwendet werden, wenn es möglich ist.

Der X-Server muss die verfügbaren Schriften und deren Speicherorte im System kennen. Dies wird durch Verwendung der Variablen `FontPath` erreicht, in der die Pfade zu allen gültigen Schriftverzeichnissen des Systems vermerkt sind. In jedem dieser Verzeichnisse sind die dort verfügbaren Schriften in einer Datei mit dem Namen `fonts.dir` aufgeführt. Der `FontPath` wird vom X Server beim Systemstart erzeugt. Der

Server sucht an jedem Speicherort, auf den die `FontPath`-Einträge der Konfigurationsdatei `/etc/X11/xorg.conf` verweisen, nach einer gültigen `fonts.dir`-Datei. Diese Einträge befinden sich im Abschnitt `Files`. Der `FontPath` lässt sich mit dem Befehl `xset q` anzeigen. Dieser Pfad kann auch zur Laufzeit mit dem Befehl `xset` geändert werden. Zusätzliche Pfade werden mit `xset+fp <Pfad>` hinzugefügt. Unerwünschte Pfade können mit `xset-fp <Pfad>` gelöscht werden.

Wenn der X-Server bereits aktiv ist, können Sie neu installierte Schriften in eingehängten Verzeichnissen mit dem Befehl `xsetfp rehash` verfügbar machen. Dieser Befehl wird von `SuSEconfig--module fonts` ausgeführt. Da zur Ausführung des Befehls `xset` der Zugriff auf den laufenden X-Server erforderlich ist, ist dies nur möglich, wenn `SuSEconfig--module fonts` von einer Shell aus gestartet wird, die Zugriff auf den laufenden X-Server hat. Am einfachsten erreichen Sie dies, indem Sie `su` und das `root`-Passwort eingeben und dadurch `root`-Berechtigungen erlangen. `su` überträgt die Zugriffsberechtigungen des Benutzers, der den X Server gestartet hat, auf die `root`-Shell. Wenn Sie überprüfen möchten, ob die Schriften ordnungsgemäß installiert wurden und über das X11 Core-Schriftsystem verfügbar sind, geben Sie den Befehl `xlsfonts` ein, um alle verfügbaren Schriften aufzulisten.

Standardmäßig arbeitet openSUSE mit UTF-8-Gebietsschemata. Daher sollten nach Möglichkeit Unicode-Schriften verwendet werden (Schriftnamen, die in der von `xlsfonts` ausgegebenen Liste auf `iso10646-1` enden). Alle verfügbaren Unicode-Schriften lassen sich über den Befehl `xlsfonts | grep iso10646-1` auflisten. Fast alle Unicode-Schriften, die unter openSUSE zur Verfügung stehen, umfassen zumindest die für europäische Sprachen erforderlichen Schriftzeichen (früher als `iso-8859-*` kodiert).

8.2.2 Xft

Die Programmierer von Xft haben von Anfang an sichergestellt, dass auch skalierbare Schriften, die Antialiasing nutzen, problemlos unterstützt werden. Bei Verwendung von Xft werden die Schriften von der Anwendung, die die Schriften nutzt, und nicht vom X-Server gerendert, wie es beim X11 Core-Schriftsystem der Fall ist. Auf diese Weise hat die jeweilige Anwendung Zugriff auf die eigentlichen Schriftdateien und kann genau steuern, wie die Zeichen gerendert werden. Dies bildet eine optimale Basis für die ordnungsgemäße Textdarstellung für zahlreiche Sprachen. Direkter Zugriff auf die Schriftdateien ist sehr nützlich, wenn Schriften für die Druckausgabe eingebettet

werden sollen. So lässt sich sicherstellen, dass der Ausdruck genau der Bildschirmdarstellung entspricht.

Unter openSUSE nutzen die beiden Desktop-Umgebungen KDE und GNOME sowie Mozilla und zahlreiche andere Anwendungen bereits standardmäßig Xft. Xft wird inzwischen von mehr Anwendungen genutzt als das alte X11 Core-Schriftsystem.

Xft greift für die Suche nach Schriften und für deren Darstellung auf die fontconfig-Bibliothek zurück. Die Eigenschaften von "fontconfig" werden durch die globale Konfigurationsdatei `/etc/fonts/fonts.conf` und die benutzerspezifische Konfigurationsdatei `~/.fonts.conf` bestimmt. Jede dieser fontconfig-Konfigurationsdateien muss folgendermaßen beginnen:

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

Enden müssen die Dateien wie folgt:

```
</fontconfig>
```

Wenn Sie möchten, dass weitere Verzeichnisse nach Schriften durchsucht werden sollen, fügen Sie Zeilen in der folgenden Weise hinzu:

```
<dir>/usr/local/share/fonts/</dir>
```

Dies ist jedoch in der Regel nicht erforderlich. Standardmäßig ist das benutzerspezifische Verzeichnis `~/.fonts` bereits in die Datei `/etc/fonts/fonts.conf` eingetragen. Entsprechend müssen Sie die zusätzlichen Schriften einfach nur nach `~/.fonts` kopieren, um sie zu installieren.

Außerdem können Sie Regeln angeben, die die Darstellung der Schriften beeinflussen. Geben Sie beispielsweise Folgendes ein:

```
<match target="font">
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>
```

Hierdurch wird das Antialiasing für alle Schriften aufgehoben. Wenn Sie hingegen

```
<match target="font">
  <test name="family">
```

```

    <string>Luxi Mono</string>
    <string>Luxi Sans</string>
  </test>
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>

```

eingeben, wird das Antialiasing nur für bestimmte Schriften aufgehoben.

Standardmäßig verwenden die meisten Anwendungen die Schriftbezeichnungen `sans-serif` (bzw. `sans`), `serif` oder `monospace`. Hierbei handelt es sich nicht um eigentliche Schriften, sondern nur um Aliasnamen, die je nach Spracheinstellung in eine passende Schrift umgesetzt werden.

Benutzer können problemlos Regeln zur Datei `~/ .fonts.conf` hinzufügen, damit diese Aliasnamen in ihre bevorzugten Schriften umgesetzt werden:

```

<alias>
  <family>sans-serif</family>
  <prefer>
    <family>FreeSans</family>
  </prefer>
</alias>
<alias>
  <family>serif</family>
  <prefer>
    <family>FreeSerif</family>
  </prefer>
</alias>
<alias>
  <family>monospace</family>
  <prefer>
    <family>FreeMono</family>
  </prefer>
</alias>

```

Da fast alle Anwendungen standardmäßig mit diesen Aliasnamen arbeiten, betrifft diese Änderung praktisch das gesamte System. Daher können Sie nahezu überall sehr einfach Ihre Lieblingsschriften verwenden, ohne die Schrifteinstellungen in den einzelnen Anwendungen ändern zu müssen.

Mit dem Befehl `fc-list` finden Sie heraus, welche Schriften installiert sind und verwendet werden können. Der Befehl `fc-list` gibt eine Liste aller Schriften zurück. Wenn Sie wissen möchten, welche der skalierbaren Schriften (`:scalable=true`) alle erforderlichen Zeichen für Hebräisch (`:lang=he`) enthalten und Sie deren Namen

(family), Schnitt (style) und Stärke (weight) sowie die Namen der entsprechenden Schriftdateien anzeigen möchten, geben Sie folgenden Befehl ein:

```
fc-list ":lang=he:scalable=true" family style weight
```

Auf diesen Befehl kann beispielsweise Folgendes zurückgegeben werden:

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
FreeSans.ttf: FreeSans:style=Medium:weight=80
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

In der folgenden Tabelle finden Sie wichtige Parameter, die mit dem Befehl `fc-list` abgefragt werden können:

Tabelle 8.2 *Parameter zur Verwendung mit `fc-list`*

Parameter	Bedeutung und zulässige Werte
family	Der Name der Schriftfamilie, z. B. <code>FreeSans</code> .
foundry	Der Hersteller der Schrift, z. B. <code>urw</code> .
style	Der Schriftschnitt, z. B. <code>Medium</code> , <code>Regular</code> , <code>Bold</code> , <code>Italic</code> oder <code>Heavy</code> .
lang	Die Sprache, die von dieser Schrift unterstützt wird, z. B. <code>de</code> für Deutsch, <code>ja</code> für Japanisch, <code>zh-TW</code> für traditionelles Chinesisch oder <code>zh-CN</code> für vereinfachtes Chinesisch.
weight	Die Schriftstärke, z. B. <code>80</code> für normale Schrift oder <code>200</code> für Fettschrift.
slant	Die Schriftneigung, in der Regel <code>0</code> für gerade Schrift und <code>100</code> für Kursivschrift.

Parameter	Bedeutung und zulässige Werte
geschrieben werden	Der Name der Schriftdatei.
outline	<code>true</code> für Konturschriften oder <code>false</code> für sonstige Schriften.
scalable	<code>true</code> für skalierbare Schriften oder <code>false</code> für sonstige Schriften.
bitmap	<code>true</code> für Bitmap-Schriften oder <code>false</code> für sonstige Schriften.
pixelsize	Schriftgröße in Pixel. In Verbindung mit dem Befehl "fc-list" ist diese Option nur bei Bitmap-Schriften sinnvoll.

8.3 Weiterführende Informationen

Installieren Sie die Pakete `xorg-x11-doc` und `howtoenh` , um detailliertere Informationen zu X11 zu erhalten. Weitere Informationen zur X11-Entwicklung finden Sie auf der Startseite des Projekts unter <http://www.x.org>.

Xen-Virtualisierung

In diesem Kapitel werden die Komponenten und Technologien beschrieben, die Sie zur Einrichtung und Verwaltung einer xen-basierten Virtualisierungsumgebung kennen sollten. Es besteht aus den folgenden Abschnitten:

Die aktuellsten Dokumente von Novell zum Thema Virtualisierung finden Sie unter <http://www.novell.com/documentation/vmserver/>.

9.1 Hauptkomponenten

Die Hauptkomponenten einer xen-basierten Virtualisierungsumgebung sind der *Xen Hypervisor*, die *Desktop-Umgebung des Hosts*, eine beliebige Anzahl *xen-basierter virtueller Computer* sowie die Werkzeuge, Befehle und Konfigurationsdateien für die Verwaltung der Virtualisierung. Der physische Computer, auf dem all diese Komponenten ausgeführt werden, wird gemeinhin auch als *virtueller Computerhost* bezeichnet, da diese Komponenten gemeinsam die Hostplattform für virtuelle Computer bilden.

Der Xen Hypervisor

Der Xen Hypervisor, auch als Monitor für virtuelle Computer bezeichnet, koordiniert auf unterster Ebene die Interaktion zwischen den virtuellen Computern und der physischen Hardware.

Die Desktop-Umgebung des Hosts

Die Desktop-Umgebung des virtuellen Computerhosts, auch als *Domäne 0* bezeichnet. Sie besteht unter anderem aus folgenden Komponenten:

- openSUSE, das Administratoren zur Verwaltung der Komponenten des virtuellen Computerhosts und seiner virtuellen Computer eine grafische Desktop- und Kommandozeilenumgebung bereitstellt.

ANMERKUNG

Mit „Host-Desktop“ wird in der Regel die Verwaltungsumgebung *Domäne 0* bezeichnet, auch wenn openSUSE im Kommandozeilenmodus ohne grafisches Desktop ausgeführt werden kann.

- Der xend-Daemon (xend), der Konfigurationsdaten sämtlicher virtueller Computer speichert und die Erstellung und Verwaltung der virtuellen Computer steuert.
- Eine angepasste Version von QEMU, einem Programm, das ein vollständiges Computersystem einschließlich Prozessor und verschiedenen Peripheriegeräten emuliert. Dieses Programm ermöglicht es, Betriebssysteme vollständig im Virtualisierungsmodus zu hosten.

Xen-basierte virtuelle Computer

Ein xen-basierter virtueller Computer, auch als *Domäne* bezeichnet, besteht aus folgenden Komponenten:

- Mindestens ein virtueller Datenträger mit bootfähigem Betriebssystem. Der virtuelle Datenträger kann auf einer Datei, einer Partition, einem Volume oder einem anderen Blockgerätetyp basieren.
- Informationen zur virtuellen Computerkonfiguration, die mittels Export einer textbasierten Konfigurationsdatei aus xend oder im Virtual Machine Manager bearbeitet werden können.

Verwaltungswerkzeuge, Befehle und Konfigurationsdateien

Ihre Virtualisierungsumgebung können Sie mittels GUI-Werkzeugen, Kommandos und Konfigurationsdateien verwalten und anpassen.

9.1.1 Erläuterungen zu den Virtualisierungsmodi

Gast-Betriebssysteme werden auf virtuellen Computern entweder im vollständig virtuellen Modus oder in einem paravirtuellen Modus gehostet. Jede der beiden Virtualisierungsmodi hat Vor- und Nachteile.

- Im vollständigen Virtualisierungsmodus können virtuelle Computer Betriebssysteme wie Windows* Server 2003 und Windows XP unverändert ausführen. Allerdings muss der Computer, der als virtueller Computerhost fungiert, in diesem Modus hardware-unterstützte Virtualisierungstechnologien wie AMD* Virtualization oder Intel* Virtualization Technology unterstützen.

Einige Gast-Betriebssysteme können im vollständigen Virtualisierungsmodus so konfiguriert werden, dass sie statt der betriebssystemspezifischen Treiber die Virtual Machine-Treiber von openSUSE ausführen. Virtual Machine-Treiber verbessern die Leistung von Gast-Betriebssystemen wie Windows XP und Windows Server 2003 erheblich. Weitere Informationen finden Sie unter „Virtual Machine Driver Pack für Windows [<http://www.novell.com/documentation/vmserver/susedriversforwindows/data/b7cf074.html#b7cf074>]“.

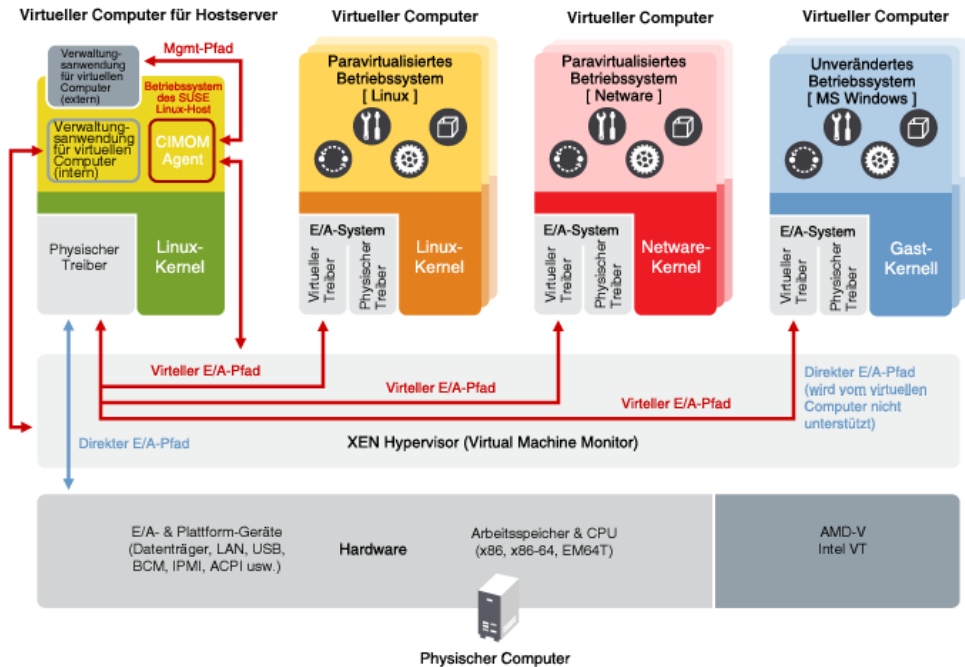
- Der paravirtuelle Modus fordert vom Hostcomputer keine Unterstützung hardware-basierter Virtualisierungstechnologien, allerdings muss sein Betriebssystem in diesem Modus an die Virtualisierungsumgebung angepasst sein. In der Regel zeigen Betriebssysteme im paravirtuellen Modus eine bessere Leistung als Betriebssysteme, für die der vollständige Virtualisierungsmodus erforderlich ist.

9.1.2 Virtualisierungsarchitektur von Xen

Folgende Abbildung zeigt einen virtuellen Computerhost mit drei virtuellen Computern. Der Xen Hypervisor wird direkt auf der physischen Hardware-Plattform ausgeführt.

Über der Ebene des Xen Hypervisor befinden sich vier virtuelle Computer.

Abbildung 9.1 Virtualisierungsarchitektur



Auf der linken Seite sehen Sie den Desktop des virtuellen Computerhosts (Domäne 0) mit dem Betriebssystem SUSE Linux. Auf den beiden virtuellen Computern in der Mitte werden paravirtuelle openSUSE-Systeme ausgeführt. Auf dem vollständig virtuellen Computer auf der rechten Seite wird ein unverändertes Betriebssystem, zum Beispiel Windows Server 2003 oder Windows XP, ausgeführt.

9.1.3 Erläuterungen zum virtuellen Computerhost

Nach der Installation der Virtualisierungskomponenten und dem Booten des Computers sollte das GRUB-Menü die Menüoption "Xen" enthalten. Durch Auswahl dieser Option werden die Virtualisierungskomponenten geladen und der Host-Desktop `Dom ne 0` wird mit openSUSE gestartet.

Unter `Dom ne 0` zeigt openSUSE die installierte Textkonsole oder die Desktop-Umgebung an (GNOME oder KDE). Nach dem Öffnen wird jeder virtuelle Computer in einem eigenen Fenster angezeigt.

9.2 Einrichten eines virtuellen Computerhosts

In diesem Abschnitt wird die Einrichtung und Verwendung von openSUSE als virtueller Computerhost beschrieben. Aktuelle Dokumente von Novell zum Thema Virtualisierung finden Sie unter <http://www.novell.com/documentation/vmserver/>.

9.2.1 Anforderungen an den virtuellen Computerhost

In den folgenden Abschnitten sind die System- und Softwareanforderungen zur Ausführung der Virtualisierung aufgeführt.

Hardwareanforderungen

In den meisten Fällen sind die Anforderungen an den virtuellen Computerhost dieselben wie für das openSUSE-System. Es sollten jedoch weitere CPU-, Festplatten-, Arbeitsspeicher- und Netzwerkressourcen hinzugefügt werden, um den Ressourcenbedarf für alle geplanten virtuellen Computer abzudecken.

TIPP

Beachten Sie, dass virtuelle Computer genau wie reale Computer bessere Leistung erbringen, wenn sie über schnellere Prozessoren verfügen und Zugriff auf mehr Systemarbeitspeicher haben.

In folgender Tabelle sind die Hardware-Mindestanforderungen für die Ausführung von openSUSE auf einem virtuellen Linux-Computer aufgelistet.

Tabelle 9.1 *Hardwareanforderungen*

Systemkomponente	Mindestanforderungen	Empfohlene Systemvoraussetzungen
Computer	Server-Computer mit Pentium* II oder AMD * K7-Prozessor, 450 MHz	Server-Computer mit Pentium III, Pentium III Xeon*, Pentium 4, Intel Xeon 700 MHz, AMD K8 CPUs (Athlon * 64 und Opteron*), Intel EM64T oder einem höheren Prozessor
Arbeitsspeicher	512 MB RAM für den Host	512 MB
	512 MB RAM für jeden virtuellen Linux-Computer	1 GB RAM
Freier Speicherplatz	7 GB freier, nicht partitionierter Festplattenspeicher für den Host	Mindestens 7 GB freier, nicht partitionierter Festplattenspeicher für den Host
	3,7 GB freier, nicht partitionierter Festplattenspeicher für jeden virtuellen Linux-Computer	Mindestens 10 GB freier, nicht partitionierter Festplattenspeicher Abhängig von den ausgewählten Komponenten und deren Verwendung ist eventuell weiterer Speicherplatz erforderlich.

Systemkomponente	Mindestanforderungen	Empfohlene Systemvoraussetzungen
CD-ROM-Laufwerk	4x CD-ROM-Laufwerk	48x CD-ROM-Laufwerk
Festplatte	20 GB	
Netzwerkkarte	Ethernet 100 Mbps	
IP-Adresse	<ul style="list-style-type: none"> • Eine IP-Adresse auf einem Subnetz für den Host • Eine IP-Adresse auf einem Subnetz für jeden virtuellen Computer • Teilnetzmaske • Standard-Gateway 	
Maus	nicht zutreffend	USB oder PS/2
BIOS des Servercomputers	Wenn Sie die Installation von CD-ROM ausführen, müssen Sie das BIOS auf dem Servercomputer zunächst so vorbereiten, das es vom CD-ROM-Laufwerk startet.	

Softwareanforderungen

Der virtuelle Computerhost erfordert die Installation der folgenden Softwarepakete und Abhängigkeiten:

- kernel-xen
- xen

- `xen-tools`
- `xen-tools-ioemu` (erforderlich für den vollständigen Virtualisierungsmodus)
- `kernel-xenpae` (wird anstelle von `kernel-xen` verwendet; dieses Paket ist zur Aktivierung eines 32-Bit-Hosts für virtuelle Computer für den Zugriff auf Arbeitsspeicher über 3 GB erforderlich)
- `yast2-vm`

Updates sind über die Update-Verbindung verfügbar. Vergewissern Sie sich, dass Sie die neuesten Update-Pakete verwenden.

9.2.2 Installieren der Xen-Software für den virtuellen Computerhost

Die Xen-Virtualisierungssoftware kann während der anfänglichen Installation von openSUSE installiert werden oder einem Computer, auf dem bereits ein Betriebssystem installiert ist, später hinzugefügt werden.

Zur Leistungsoptimierung sollten Sie auf dem virtuellen Computerhost nur diejenigen Anwendungen und Prozesse installieren, die tatsächlich für die Virtualisierung erforderlich sind.

Installieren der Virtualisierung während der anfänglichen Einrichtung von openSUSE

- 1 Wählen Sie bei der Installation von openSUSE das Softwareschema *Hostserver für Xen Virtual Machine* aus.
- 2 Wählen Sie nach Ihren Anforderungen Softwarepakete aus oder deaktivieren Sie Pakete.

Sie sollten wirklich nur diejenigen Software- und Systemaufgaben auswählen, die Sie für Ihre Virtualisierungsumgebung tatsächlich benötigen. Die Ausführung jedes weiteren Dienstes in der Verwaltungsdomäne (Domäne 0), wie Webserver, Mailserver oder Druckserver, wirkt sich auch auf die Leistung der gehosteten virtuellen Computer aus.

Eine optimale Leistung erzielen Sie, wenn Sie alle Komponenten deaktivieren, mit Ausnahme der folgenden:

- *Server-Basissystem*
- *GNOME- oder KDE-Desktop-Umgebung*
- *X Window System (für grafische Benutzerschnittstelle erforderlich)*
- *Hostserver für Xen Virtual Machine*

3 Befolgen Sie die Anweisungen auf dem Bildschirm bis zum Abschluss des Installationsprogramms.

Die Xen-Software ist nun auf dem Computer installiert. Fahren Sie mit [Abschnitt 9.2.3, „Starten des virtuellen Computerhosts“](#) (S. 159) fort.

Hinzufügen der Virtualisierung zu openSUSE

Wenn openSUSE bereits installiert ist, können Sie die Virtualisierungssoftware mit folgenden Methoden über das Desktop oder die Kommandozeilenschnittstelle nachträglich hinzufügen.

- Führen Sie auf dem Desktop *YaST > Virtualisierung > Hypervisor und Werkzeuge installieren* aus. Befolgen Sie die Anweisungen auf dem Bildschirm und starten Sie den Computer neu.
- Geben Sie an der Kommandozeile das Kommando `yast2 xen` ein. Befolgen Sie die Anweisungen auf dem Bildschirm und starten Sie den Computer neu.

9.2.3 Starten des virtuellen Computerhosts

Wenn die Virtualisierungssoftware korrekt installiert wurde, bootet der Computer, um den GRUB-Bootloader mit der Menüoption *Xen* anzuzeigen. Wählen Sie diese Option aus, um den virtuellen Computerhost zu starten.

Sie können den Bootloader auch so bearbeiten, dass die Option "Xen" standardmäßig ausgewählt ist.

- 1 Melden Sie sich als `root`-Benutzer an.
- 2 Klicken Sie in YaST auf *System > Bootloader*.
- 3 Wählen Sie für den Standardboot *Xen* aus und klicken Sie auf *Als Standard festlegen*.
- 4 Klicken Sie auf *Fertig stellen*.
- 5 Klicken Sie auf *Computer > Abmelden > Abmelden*, um das System neu zu starten. Klicken Sie danach auf *Neustart* und geben Sie das root-Passwort ein.

Wenn der GRUB-Bootloader nicht angezeigt wird oder sich die Option *Xen* nicht im Menü befindet, sollten Sie die Installationsschritte überprüfen und sich vergewissern, dass der GRUB-Bootloader aktualisiert wurde.

Nach dem Booten startet der virtuelle Verwaltungscomputer mit seiner grafischen Desktop-Umgebung. Falls keine grafische Desktop-Umgebung installiert ist, wird die Kommandozeilenumgebung angezeigt.

Weitere Informationen zur Verwaltung von virtuellen Computern finden Sie in [Abschnitt 9.4, „Verwalten einer Virtualisierungsumgebung“](#) (S. 167).

9.3 Einrichten virtueller Computer

Ein virtueller Computer besteht aus Daten- und Betriebssystemdateien, die die virtuelle Umgebung festlegen. Virtuelle Computer werden vom virtuellen Computerhost gehostet und gesteuert.

In diesem Abschnitt finden Sie allgemeine Anleitungen zur Installation virtueller Computer. Ausführliche Informationen zur Installation und Verwaltung des jeweils installierten Betriebssystems finden Sie im Artikel *Novell Virtualization Technology: Guest Operating System Guide* [http://www.novell.com/documentation/vmserver/guest_os_sp1/data/bookinfo.html#bookinfo] .

9.3.1 Systemvoraussetzungen

Für virtuelle Computer gelten keine oder nur wenige Anforderungen, die über die Anforderungen des jeweiligen Betriebssystems hinausreichen. Wenn das Betriebssystem nicht für die virtuelle Computerhost-Umgebung optimiert wurde, kann das Betriebssystem nur im vollständigen Virtualisierungsmodus und nur auf Computer-Hardware ausgeführt werden, die Virtualisierung hardware-seitig unterstützt. Außerdem müssen in diesem Fall spezielle Gerätetreiber geladen sein.

An dieser Stelle muss auch das Thema Lizenzen angesprochen werden. Nicht immer darf ein Betriebssystem mit nur einer Lizenz auf mehreren virtuellen Computern ausgeführt werden. Informieren Sie sich hierzu in der Lizenzvereinbarung zum jeweiligen Betriebssystem.

9.3.2 Systemarchitekturen für virtuelle Computer

Der virtuelle Computerhost kann nur x86-32-Bit- und x86-64-Bit-Architekturen emulieren. Andere Systemarchitekturen wie Itanium^{*} oder IBM^{*} POWER (ehemals IBM iSeries und IBM pSeries) kann der Host nicht emulieren.

9.3.3 Voraussetzungen

Zur Erstellung eines virtuellen Computers benötigen Sie Folgendes:

- Wenn Sie eine automatische Installationsdatei verwenden möchten (AutoYaST, in openSUSE), müssen Sie diese erstellen und in ein Verzeichnis auf dem virtuellen Computerserver laden oder im Netzwerk bereitstellen.
- Wenn Sie openSUSE installieren möchten, benötigen Sie eine Netzwerkinstallationsquelle. Informationen zur Erstellung von Installationsquellen finden Sie unter [Abschnitt 1.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 13).

9.3.4 Erstellen eines virtuellen Computers

Der Assistent für das Erstellen virtueller Computer führt Sie durch die erforderlichen Schritte zur Erstellung eines virtuellen Computers sowie zur Installation des Betriebssystems. Die nachfolgenden Informationen sind allgemein gehalten und gelten für jedes Betriebssystem. Spezifische Informationen zu den einzelnen Betriebssystemen erhalten Sie im *Novell Virtualization Technology: Guest Operating System Guide* [http://www.novell.com/documentation/vmserver/guest_os_spl/data/bookinfo.html#bookinfo].

Starten Sie den Assistenten für das Erstellen virtueller Computer auf eine der folgenden Weisen:

- Klicken Sie auf dem Desktop des Virtualisierungs-Hostservers auf *YaST > Virtualisierung > Virtuellen Computer erstellen*.

Falls YaST nicht in der Anwendungsliste aufgeführt ist, können Sie das Programm ausführen, indem Sie sich als `root` anmelden und `yast2` in einem Terminal ausführen.

- Klicken Sie im Virtual Machine Manager auf *Neu*.
- Geben Sie an der Kommandozeile `vm-install` ein.

Wenn der Assistent nicht angezeigt wird oder der Befehl `vm-install` nicht funktioniert, überprüfen Sie das Verfahren zum Installieren und Starten des Virtualisierungs-Hostservers. Die Virtualisierungssoftware ist eventuell nicht ordnungsgemäß installiert.

Installieren eines Betriebssystems

Zur Installation eines Betriebssystems können Sie ein Installationsprogramm ausführen oder eine Festplatte bzw. ein Festplatten-Image mit einem bereits installierten und bootfähigen Betriebssystem verwenden.

Wenn Sie ein Installationsprogramm ausführen, stehen Ihnen verschiedene Betriebssysteme zur Auswahl. Wählen Sie das zu installierende Betriebssystem aus.

Zusammenfassung

Die Informationen auf der Seite "Zusammenfassung" können Sie bearbeiten, indem Sie auf die Überschrift zu den jeweiligen Einstellungen klicken. Spezifische Informationen zu den Einstellungen der einzelnen Betriebssysteme auf dieser Seite erhalten Sie im *Novell Virtualization Technology: Guest Operating System Guide* [http://www.novell.com/documentation/vmserver/guest_os_spl/data/bookinfo.html#bookinfo].

Virtualisierungsmethode

Auf der Seite "Virtualisierungsmethode" wählen Sie die gewünschte Virtualisierungsmethode aus.

Wenn Ihr Computer die hardware-gestützte Virtualisierung unterstützt, können Sie einen virtuellen Computer einrichten, der im vollständig virtuellen Modus ausgeführt wird. Wenn Sie ein Betriebssystem installieren, das für die Virtualisierung angepasst wurde, können Sie einen virtuellen Computer einrichten, der im paravirtuellen Modus ausgeführt wird. Weitere Informationen zu den Virtualisierungsmodi finden Sie unter **Abschnitt 9.1.1, „Erläuterungen zu den Virtualisierungsmodi“** (S. 153).

Name der Virtual Machine

Jeder virtuelle Computer muss einen eindeutigen Namen haben. Der auf dieser Seite eingegebene Name wird zur Erstellung und Benennung der Konfigurationsdatei des virtuellen Computers verwendet. Die Konfigurationsdatei enthält Parameter, die den virtuellen Computer definieren. Sie wird im Verzeichnis `/etc/xen/vm/` gespeichert.

Hardware

Auf der Seite "Hardware" legen Sie die Arbeitsspeichermenge und die Anzahl der virtuellen Prozessoren für den virtuellen Computer fest.

Ursprünglicher Arbeitsspeicher:

Die dem virtuellen Computer anfänglich zugewiesene Menge an Arbeitsspeicher (in Megabyte).

Maximaler Arbeitsspeicher:

Die maximale Menge an Arbeitsspeicher, die dem virtuellen Computer zugeteilt werden kann.

Virtuelle Prozessoren:

Bei Bedarf können Sie hier festlegen, dass der virtuelle Computer über mehr virtuelle Prozessoren verfügt, als es die Anzahl der physikalischen Prozessoren zulässt. Sie können hier bis zu 32 virtuelle Prozessoren angeben. Eine bessere Leistung erzielen Sie allerdings, wenn die Anzahl der virtuellen Prozessoren die Anzahl der physikalischen Prozessoren nicht überschreitet.

Grafiken

Keine Grafikerkennung

Der virtuelle Computer arbeitet wie ein Server ohne Bildschirm. Zugriff auf das Betriebssystem erhalten Sie über Dienste, die vom Betriebssystem unterstützt werden, wie SSH oder VNC.

Paravirtualisierter Grafikadapter

Hierfür muss auf dem Betriebssystem ein geeigneter Grafiktreiber installiert sein.

Festplatten

Ein virtueller Computer muss über mindestens einen virtuellen Datenträger verfügen. Folgende Möglichkeiten stehen zur Auswahl:

- Der virtuelle Datenträger ist ein datei-gestützter Datenträger, d. h. eine einzelne Image-Datei auf einem größeren physikalischen Datenträger.
- Der virtuelle Datenträger ist eine Sparse Image-Datei, d. h. eine einzelne Image-Datei ohne fest zugewiesenen Speicherplatz.
- Der virtuelle Datenträger ist aus einem Blockgerät konfiguriert, es handelt sich also um eine ganze Festplatte, eine Partition oder ein Volume.

Die beste Leistung erzielen Sie, wenn Sie für jeden virtuellen Datenträger eine Festplatte oder Partition verwenden. Auch mit einer Image-Datei erhalten Sie eine annehmbare Leistung, solange Sie die Datei nicht als Sparse-Image-Datei erstellen. Eine Sparse-Image-Datei als virtueller Datenträger bietet zwar eine enorme Flexibilität in Sachen

Speicherplatz, allerdings ist die Installations- und Plattenzugriffsgeschwindigkeit bei dieser Option sehr stark herabgesetzt.

Standardmäßig wird ein einzelner, datei-gestützter 4 GB großer virtueller Datenträger als Sparse-Image-Datei in `/var/lib/xen/images/ VM_Name` erstellt (*VM_Name* ist der Name des virtuellen Computers). Diese Konfiguration können Sie an Ihre Anforderungen anpassen.

Bearbeiten der Eigenschaften eines virtuellen Datenträgers

Bei der Erstellung des virtuellen Datenträgers können Sie dessen Eigenschaften über die Schaltfläche *Bearbeiten* an Ihre persönlichen Konfigurationsanforderungen anpassen.

Typ:

Virtuellen Datenträgern sind Laufwerksbezeichnungen nach den Linux-Gerätenamenskonventionen zugewiesen, beispielsweise `hda`. Die Bezeichnung legt fest, wie der virtuelle Datenträger für den virtuellen Computer dargestellt wird. Beispielsweise wird ein virtueller Datenträger mit der Bezeichnung `hda` für den virtuellen Computer als erstes Datenträgergerät dargestellt. Paravirtuelle Datenträger werden als generische Datenträger dargestellt (also z. B. nicht als IDE oder SCSI). Vollständig virtuelle Datenträger werden dem Gast als IDE dargestellt. Die Benennung erfolgt in jedem Fall nach den Konventionen des Gast-Betriebssystems.

Ursprung

Je nach Anforderungen möchten Sie eventuell den Ort ändern, an dem die Datenträger-Image-Datei erstellt und gespeichert wird, oder Sie möchten die Festplatte, die Partition oder das Volume für den virtuellen Datenträger selbst bestimmen.

Sparse-Image-Datei

Ein auf einer Sparse-Image-Datei basierender virtueller Datenträger belegt nicht den gesamten für die Datei reservierten Speicherplatz, sondern nur den jeweils benötigten Speicherplatz. Diese Option empfiehlt sich durchaus, wenn Sie virtuelle Datenträger auf die Schnelle erstellen möchten. Zur Leistungsoptimierung sollten Sie den Plattenspeicher jedoch fest zuweisen, also die Option *Sparse Image-Datei anlegen* deaktivieren.

Nur-Lese-Zugriff

Aus Sicherheitsgründen sollte ein virtueller Datenträger nur dann für mehrere virtuelle Computer freigegeben werden, wenn der Zugriff auf den virtuellen Datenträger schreibgeschützt ist.

Weitere virtuelle Datenträger

Einem virtuellen Computer können mehrere virtuelle Datenträger zugewiesen sein. Bei der Erstellung eines virtuellen Computers können Sie weitere datei-gestützte virtuelle Datenträger erstellen oder vorhandene Datenträger-Images oder Blockgeräte als weitere virtuelle Datenträger zuweisen.

Netzwerkadapter

Standardmäßig wird pro virtuellen Computer eine virtuelle Netzwerkkarte erstellt. Die nach dem Zufallsprinzip generierte MAC-Adresse der Karte können Sie an die gewünschte Konfiguration anpassen. Sie können auch weitere virtuelle Netzwerkkarten erstellen. Im paravirtuellen Modus kommunizieren die virtuellen Netzwerkkarten über einen generischen, mit Xen kompatiblen Netzwerkkartentreiber.

Betriebssysteminstallation

Das Betriebssystem kann von einem CD/DVD-Gerät oder aus einer ISO-Image-Datei installiert werden. Wenn Sie ein openSUSE-System installieren, können Sie das Betriebssystem auch aus einer Netzwerkinstallationsquelle installieren.

Wenn Sie das Betriebssystem für einen paravirtuellen Computer von CD installieren, sollten Sie den virtuellen CD-Reader nach der Installation vom virtuellen Computer entfernen, da der virtuelle Computer davon ausgeht, dass die Original-CD nach wie vor im CD-Reader eingelegt ist, selbst wenn sie ausgeworfen wurde. Wenn die CD aber bereits ausgeworfen ist, erhält der virtuelle Computer I/O-Fehler, da er nicht auf die CD (und auch nicht auf eine andere eingelegte CD) zugreifen kann.

Informationen zum Entfernen des virtuellen CD-Readers finden Sie im Abschnitt „Virtual CD Readers [http://www.novell.com/documentation/vmserver/config_options/data/b9rtimf.html#b9rtimf]“ (Virtuelle CD-Reader) unter *Configuration Options and Settings* [http://www.novell.com/documentation/vmserver/config_options/data/bookinfo.html#bookinfo] (Konfigurationsoptionen und -einstellungen).

Falls das Installationsprogramm Installationsprofile, Antwortdateien oder Skripte erkennt, können Sie die Installationseinstellungen durch Angabe des gewünschten Profils, der Datei oder des Skripts automatisieren. openSUSE verwendet beispielsweise ein AutoYaST-Profil.

Über Parameter im Feld *Zusätzliche Argumente* können Sie während der Installation auch Anweisungen an den Kernel eingeben.

Wenn Sie beispielsweise unter openSUSE für den virtuellen Server die IP-Adresse 192.35.1.10, die Netzmaske 255.255.255.0 und das Gateway 192.35.1.254 angeben möchten und SSH für den Zugriff auf die Installation verwenden möchten, geben Sie im Feld *Zusätzliche Argumente* die folgenden Parameter ein:

```
hostip=192.35.1.10 netmask=255.255.255.0 gateway=192.35.1.254 \  
usessh=1 sshpassword=<password>
```

Wenn Sie auf der Seite "Betriebssysteminstallation" alle erforderlichen Einstellungen vorgenommen haben, klicken Sie auf *Anwenden*, um zur Seite "Zusammenfassung" zurückzukehren.

Fortsetzen der Installation

Wenn die Angaben auf der Seite "Zusammenfassung" korrekt sind, klicken Sie auf *OK*, um den virtuellen Computer zu erstellen. Daraufhin wird ein TightVNC-Bildschirm eingeblendet, mit dem die Installation des Betriebssystems beginnt. Folgen Sie ab jetzt den Installationsanweisungen Ihres Betriebssystems. Zusätzlich finden Sie in *Novell Virtualization Technology: Guest Operating System Guide* [http://www.novell.com/documentation/vmserver/guest_os_spl/data/bookinfo.html#bookinfo] spezifische Anweisungen zur Installation Ihres Betriebssystems in einer virtuellen Umgebung.

9.4 Verwalten einer Virtualisierungsumgebung

Zur Verwaltung Ihrer Virtualisierungsumgebung stehen Ihnen grafische Dienstprogramme, textbasierte Kommandos und angepasste Konfigurationsdateien zur Verfügung. Sie können zum Beispiel Virtual Machine Manager verwenden, ein von YaST bereitgestelltes grafisches Dienstprogramm, das vom Desktop des virtuellen Computerhosts gestartet werden kann.

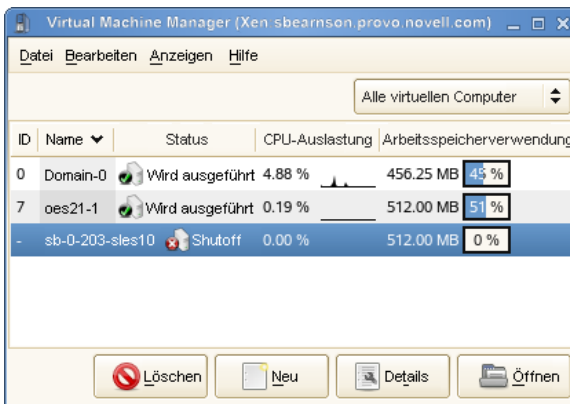
Als Kommandozeilenoptionen stehen Ihnen auf dem virtuellen Computerhost zur Erstellung und Verwaltung virtueller Computer zum Beispiel das Programm `vm-install` sowie `xm`-Kommandos zur Verfügung. Eine weitere Möglichkeit der Verwaltung virtu-

eller Computer ist die Bearbeitung der Konfigurationsdateien, in denen Sie die Einstellungen des virtuellen Computerhosts sowie die Einstellungen einzelner virtueller Computer ändern können.

9.4.1 Virtual Machine Manager

Der YaST Virtual Machine Manager ist eine grafische Benutzeroberfläche für die Erstellung und Verwaltung virtueller Computer, die Ihnen direkt auf dem Desktop des virtuellen Verwaltungscomputers zur Verfügung steht.

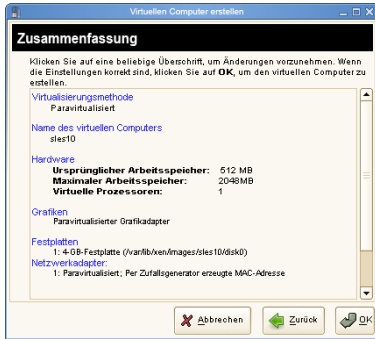
Abbildung 9.2 Hauptkonsole von Virtual Machine Manager



- Wenn Sie einen virtuellen Computer auswählen und auf *Öffnen* klicken, wird ein Fenster mit dem aktuellen Status des virtuellen Computers angezeigt.
- Wenn Sie in diesem Fenster auf *Ausführen* klicken, wird der virtuelle Computer gestartet und die auf dem virtuellen Computer aktive Benutzeroberfläche oder Textkonsole wird angezeigt.
- Wenn Sie einen virtuellen Computer auswählen und auf *Details* klicken, wird die Leistung des virtuellen Computers angezeigt. Außerdem können Sie über diese Schaltfläche die Hardware-Einstellungen des virtuellen Computers konfigurieren.
- Wenn Sie im Virtual Machine Manager auf *Neu* klicken, wird der *Assistent zum Erstellen von virtuellen Computern* gestartet, der Sie durch die einzelnen Schritte zur Einrichtung eines virtuellen Computers führt.

Der Assistent hilft Ihnen bei der Einstellung des virtuellen Computers und der Installation des Betriebssystems.

Abbildung 9.3 Seite "Zusammenfassung" für virtuelle Computer



Nachdem Sie die Einstellungen auf der Seite *Zusammenfassung* festgelegt haben, startet der Assistent den virtuellen Computer sowie das Installationsprogramm für das Betriebssystem, das Sie durch die Installation führt.

9.4.2 Das Kommando `vm-install`

Wenn Ihnen in Ihrer Umgebung keine grafische Benutzeroberfläche zur Verfügung steht, können Sie eine Textversion des Assistenten zum Erstellen von virtuellen Computern ausführen. Dazu geben Sie an der Kommandozeile das Kommando `vm-install` ein. Die Textversion führt Sie durch die gleichen Schritte wie die grafische Benutzeroberfläche.

9.4.3 Steuern des Hosts durch Bearbeiten seiner `xend`-Einstellungen

Eine wichtige Komponente der Software des virtuellen Computerhosts ist der Daemon `xend`. Er steuert, wie der virtuelle Computerhost Verwaltungsfunktionen ausführt und die für virtuelle Computer relevanten Einstellungen speichert. Durch Bearbeitung der Konfigurationsdatei von `xend` können Sie den Host an Ihre speziellen Virtualisierungsanforderungen anpassen.

Dazu bearbeiten Sie die Konfigurationsdatei `/etc/xen/xend-config.sxp` in einem Texteditor, den Sie vom Desktop des virtuellen Verwaltungscomputers aufrufen.

Danach müssen Sie den Daemon `xend` neu starten, damit die Änderungen auf dem virtuellen Computerhost wirksam werden. Zum Neustarten des Daemons geben Sie `service xend restart` ein.

Nachfolgend finden Sie einige weitere nützliche Kommandos.

- `service xend status` zeigt den Status des Daemons `xend` an.
- `service xend start` startet den Daemon `xend`.
- `service xend stop` beendet den Daemon `xend`.

9.4.4 Konfigurieren eines virtuellen Computers durch Bearbeiten seiner `xend`-Einstellungen

Die Einstellungen eines virtuellen Computers können durch Bearbeitung seiner `xend`-Konfigurationsdaten geändert werden. Die Konfigurationsdaten eines virtuellen Computers werden in der `xend`-Datenbank gespeichert und können von dort in eine Datei exportiert, geändert und wieder in die `xend`-Datenbank zurück importiert werden.

- 1 Geben Sie dazu in einem Terminal auf dem Desktop des virtuellen Verwaltungscomputers das Kommando `xm list -l Name > Dateiname` ein, um die Einstellungen des virtuellen Computers aus der `xend`-Datenbank in eine Datei zu exportieren.
 - *Name* ist der Name des virtuellen Computers.
 - *Dateiname* ist der Dateiname der Datei, in die Sie die Daten exportieren möchten.
- 2 Nehmen Sie die gewünschten Änderungen in einem Texteditor vor und speichern Sie die Datei.

- 3 Geben Sie an der Kommandozeile das kommando `xm new -F Dateiname` ein, um die geänderten Einstellungen in die xend-Datenbank zurück zu importieren.
- 4 Geben Sie `xm start VM_Name` ein, um den virtuellen Computer mit den neuen Einstellungen zu starten.

ANMERKUNG

Die Bearbeitung der Dateien in `etc/xen/vm`, die nur für die Erstellung eines neuen virtuellen Computers benötigt werden, wird nicht mehr empfohlen.

9.4.5 Das Kommando `xm`

Mit dem Kommando `xm` können Sie den Status virtueller Computer verwalten und anzeigen. Das Kommando `xm list` zeigt zum Beispiel den Status aller virtuellen Computer an.

Nachfolgend finden Sie einige weitere nützliche `xm`-Kommandos:

- `xm start` startet einen virtuellen Computer.
- `xm reboot` startet einen virtuellen Computer neu.
- `xm destroy` entfernt einen virtuellen Computer sofort.
- `xm block-list` zeigt alle virtuellen Blockgeräte eines virtuellen Computers an.

Die vollständige Liste aller `xm`-Parameter rufen Sie an der Kommandozeile mit dem Kommando `xm help` ab.

Dienstprogramme zur Systemüberwachung

10

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.

10.1 Fehlersuche

10.1.1 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-gate.so.1 => (0xffffe000)
librt.so.1 => /lib/librt.so.1 (0xb7f97000)
libacl.so.1 => /lib/libacl.so.1 (0xb7f91000)
libc.so.6 => /lib/libc.so.6 (0xb7e79000)
libpthread.so.0 => /lib/libpthread.so.0 (0xb7e67000)
/lib/ld-linux.so.2 (0xb7fb6000)
libattr.so.1 => /lib/libattr.so.1 (0xb7e63000)
```

Statische Binärdateien benötigen keine dynamischen Bibliotheken.

```
tux@mercury:~> ldd /bin/sash
not a dynamic executable
tux@mercury:~> file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for
GNU/Linux 2.6.4, statically linked, for GNU/Linux 2.6.4, stripped
```

10.1.2 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
[...]			
0.00	0.000036	36	1 textdomain

100.00	19.662715		105717 total

10.1.3 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\0\3\0\3\0\1\0\0\0000\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`.

10.2 Dateien und Dateisysteme

10.2.1 Bestimmen Sie den Dateityp: Datei

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 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
for GNU/Linux 2.2.5, 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)
```

10.2.2 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:~> df
/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
```

10.2.3 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 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                   ELF32
  Data:                    2's complement, little endian
  Version:                 1 (current)
  OS/ABI:                  UNIX - System V
  ABI Version:             0
  Type:                    EXEC (Executable file)
  Machine:                 Intel 80386
  Version:                 0x1
  Entry point address:     0x8049b60
  Start of program headers: 52 (bytes into file)
```

```

Start of section headers:      81112 (bytes into file)
Flags:                        0x0
Size of this header:          52 (bytes)
Size of program headers:      32 (bytes)
Number of program headers:     9
Size of section headers:      40 (bytes)
Number of section headers:     30
Section header string table index: 29

```

10.2.4 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

```

10.3 Hardware-Informationen

10.3.1 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.

10.3.2 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
```

10.3.3 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.

10.4 Netzwerke

10.4.1 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 BMNRRU
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
```

10.5 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     : AuthenticAMD
cpu family    : 6
model         : 8
model name    : AMD Athlon(tm) XP 2400+
stepping      : 1
cpu MHz       : 2009.343
cache size    : 256 KB
fdiv_bug      : no
[...]

```

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]

```

10.5.1 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:

10.6 Vorgänge

10.6.1 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
```

10.6.2 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 ?        Sl   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
```

10.6.3 Prozessbaum: `pstree`

Mit dem Befehl `pstree` 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`:

10.6.4 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 Programm 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	khubd
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.

10.7 Systemangaben

10.7.1 Informationen zur Systemaktivität:

sar

Damit der Befehl `sar` verwendet werden kann, muss `sadc` (system activity data collector) ausgeführt werden. Überprüfen Sie den Status oder starten Sie ihn mit dem Befehl `rcsysstat {start|status}`.

Mit `sar` können umfangreiche Berichte zu fast alle wichtigen Systemaktivitäten generiert werden, darunter CPU-, Speicher-, IRQ-Auslastung, EA oder Netzwerk. Da dieser Befehl über zahlreiche Optionen verfügt, wird er an dieser Stelle nicht näher erläutert. Eine umfassende Dokumentation mit entsprechenden Beispielen finden Sie auf der Manualpage.

10.7.2 Auslastung des Arbeitsspeichers:

frei

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:      515584        501704        13880           0        73040     334592
-/+ buffers/cache:      94072      421512
Swap:      658656           0        658656
```

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.

10.7.3 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
/mnt/notes.txt      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.

10.7.4 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
bootsplash: status on console 0 changed to on
NET: Registered protocol family 10
Disabled Privacy Extensions on device c0326ea0(10)
IPv6 over IPv4 tunneling driver
powernow: This module only works with AMD K7 CPUs
bootsplash: status on console 0 changed to on
```

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

10.7.5 Liste der geöffneten Dateien: lsof

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:~> lsof -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/nscd/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 `lsof` 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:~> lsof | 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
lsof       5673      tux      0u      CHR  136,5          7 /dev/pts/5
lsof       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
```

10.7.6 Kernel- und udev-Ereignissequenzanzeige: udevmonitor

udevmonitor 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
```

10.7.7 Von X11-Clients verwendete Serverressourcen: xrestop

Mit xrestop werden Statistiken für die serverseitigen Ressourcen der einzelnen angeschlossenen X11-Clients angegeben. Die Ausgabe ähnelt [Abschnitt 10.6.4, „Prozesse: top“](#) (S. 188).

```
xrestop - Display: localhost:0
Monitoring 40 clients. XErrors: 0
Pixmap: 42013K total, Other: 206K total, All: 42219K total
```

res-base	Wins	GCS	Fnts	Pxms	Misc	Pxm mem	Other	Total	PID	Identifizier
3e00000	385	36	1	751	107	18161K	13K	18175K	?	NOVELL: SU
4600000	391	122	1	1182	889	4566K	33K	4600K	?	amaroK - S
1600000	35	11	0	76	142	3811K	4K	3816K	?	KDE Deskto
3400000	52	31	1	69	74	2816K	4K	2820K	?	Linux Shel
2c00000	50	25	1	43	50	2374K	3K	2378K	?	Linux Shel
2e00000	50	10	1	36	42	2341K	3K	2344K	?	Linux Shel
2600000	37	24	1	34	50	1772K	3K	1775K	?	Root - Kon
4800000	37	24	1	34	49	1772K	3K	1775K	?	Root - Kon
2a00000	209	33	1	323	238	1111K	12K	1123K	?	Trekstor25
1800000	182	32	1	302	285	1039K	12K	1052K	?	kicker
1400000	157	121	1	231	477	777K	18K	796K	?	kwin
3c00000	175	36	1	248	168	510K	9K	520K	?	de.comp.la
3a00000	326	42	1	579	444	486K	20K	506K	?	[opensuse-
0a00000	85	38	1	317	224	102K	9K	111K	?	Kopete
4e00000	25	17	1	60	66	63K	3K	66K	?	YaST Contr
2400000	11	10	0	56	51	53K	1K	55K	22061	suseplugge
0e00000	20	12	1	50	92	50K	3K	54K	22016	kded
3200000	6	41	5	72	84	40K	8K	48K	?	EMACS
2200000	54	9	1	30	31	42K	3K	45K	?	SUSEWatche
4400000	2	11	1	30	34	34K	2K	36K	16489	kdesu
1a00000	255	7	0	42	11	19K	6K	26K	?	KMix
3800000	2	14	1	34	37	21K	2K	24K	22242	knotify
1e00000	10	7	0	42	9	15K	624B	15K	?	KPowerSave
3600000	106	6	1	30	9	7K	3K	11K	22236	konqueror
2000000	10	5	0	21	34	9K	1K	10K	?	klipper
3000000	21	7	0	11	9	7K	888B	8K	?	KDE Wallet

10.8 Benutzerinformationen

10.8.1 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
 16:33:03 up  3:33,  2 users,  load average: 0.14, 0.06, 0.02
USER      TTY      LOGIN@  IDLE   JCPU   PCPU WHAT
tux      :0        16:33   ?xdm?   9.42s   0.15s /bin/sh /opt/kde3/bin/startk
tux     pts/0        15:59     0.00s   0.19s   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.

10.9 Zeit und Datum

10.9.1 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

11

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.

11.1 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 Objektdaten befinden sich in Verzeichnissen mit dem Namen `lib64`. Die -Bit-Objektdaten, 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).

11.2 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.

11.3 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 Programmkonfiguration. 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"          \  
LDFLAGS="-L/usr/lib;"  \  
    .configure         \  
        --prefix=/usr  \  
        --libdir=/usr/lib  
  
make  
make install
```

11.4 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

12

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.

12.1 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 13, *Der Bootloader*](#) (S. 221).

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. In früheren Versionen von SUSE® Linux wurden diese Tasks von "initrd" bzw. "linuxrc" durchgeführt. Weitere Informationen zu initramfs finden Sie unter [Abschnitt 12.1.1, „initramfs“](#) (S. 204).
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 12.1.2, „init on initramfs“](#) (S. 205). Weitere Informationen zu udev finden Sie in [Kapitel 15, *Gerätemanagemet über dynamischen Kernel mithilfe von udev*](#) (S. 257).
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 12.2, „Der init-Vorgang“](#) (S. 207).

12.1.1 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.

12.1.2 `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 Gerätedateien

Für jedes geladene Modul generiert der Kernel Geräteergebnisse. udev verarbeitet diese Ergebnisse und generiert die erforderlichen speziellen Dateien für das Gerät auf einem RAM-Dateisystem in `/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. 68). Informationen zu LVM finden Sie in [Abschnitt 2.2, „LVM-Konfiguration“](#) (S. 60).

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 12.1.1, „initramfs“](#) (S. 204) 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.

12.2 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 12.2.1, „Runlevel“](#) (S. 208)). 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 12.2.2, „Init-Skripten“](#) (S. 211)).

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.

12.2.1 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 12.1, „Verfügbare Runlevel“** (S. 208). Alternativ kann der Runlevel auch zur Boot-Zeit (beispielsweise 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 12.1 *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
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 der Standard-Runlevel 3 ist, muss das X Window System wie unter [Kapitel 8, Das X Window-System](#) (S. 137) beschrieben 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 seine Konfigurationsdatei (`/etc/inittab`) und stellt fest, dass es `/etc/init.d/rc` mit dem neuen Runlevel als Parameter starten 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 für den Start an, da einige Abhängigkeiten zu berücksichtigen sind.
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`. Hier wird dasselbe Verfahren hinsichtlich der Startreihenfolge angewendet.

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.

12.2.2 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 Runlevels 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 12.2, „Mögliche init-Skript-Optionen“** (S. 211) erläutert. Die von `init` direkt ausgeführten Skripten verfügen nicht über diese Links. Sie werden unabhängig vom Runlevel bei Bedarf ausgeführt.

Tabelle 12.2 *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.

Option	Beschreibung
<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 gestoppt, wenn alle Aktionen, die durch diese Skripts ausgelöst wurden (z. B. das Ausführen einer bestimmten Anzahl von Subskripts), abgeschlossen sind. `blogd` schreibt alle auf dem Bildschirm ausgegebenen Informationen in die Protokolldatei `/var/log/boot.msg`, aber nur dann, wenn `/var` mit Lese- und Schreibrechten eingehängt wurde. Anderenfalls puffert `blogd` alle

Bildschirmdateien, 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.

`boot.setup`

Dieses Skript wird bei einem Wechsel vom Einzelbenutzer-Modus in einen anderen Runlevel ausgeführt. Es ist verantwortlich für eine Reihe grundlegender Einstellungen, z. B. die Tastaturbelegung und die Initialisierung der virtuellen Konsolen.

`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.

`rc`

Dieses Skript ruft die entsprechenden Stopp-Skripten des aktuellen Runlevels und die Start-Skripten des neu gewählten Runlevels auf.

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-Skripten können das System stoppen

Bei fehlerhaften init-Skripten kann es dazu kommen, dass der Computer hängt. Diese Skripten 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 12.2.1, „Runlevel“](#) (S. 208).

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 12.1, „Ein minimaler INIT INFO-Block“](#) (S. 214).

Beispiel 12.1 *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 12.2.3, „Konfigurieren von Systemdiensten (Runlevel) mit YaST“** (S. 215) beschrieben.

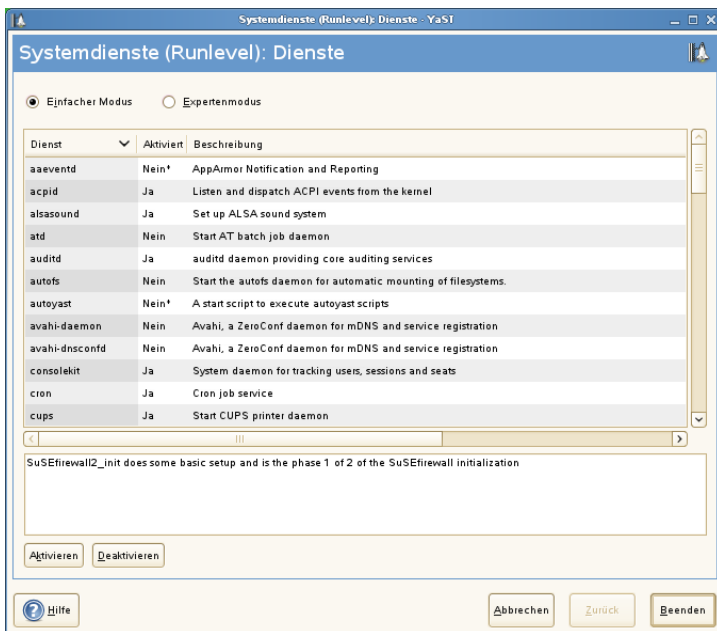
Wenn ein in `/etc/init.d/` bereits vorhandenes Skript in das vorhandene Runlevel-Schema integriert werden soll, erstellen Sie die Links in den Runlevel-Verzeichnissen direkt mit `insserv` oder indem Sie den entsprechenden Dienst im Runlevel-Editor von YaST aktivieren. Ihre Änderungen werden beim nächsten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

12.2.3 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.

Abbildung 12.1 Systemdienste (Runlevel)



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 12.1, „Verfügbare Runlevel“** (S. 208) 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.

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.

12.3 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.

12.3.1 Ändern der Systemkonfiguration mithilfe des YaST-Editors `"sysconfig"`

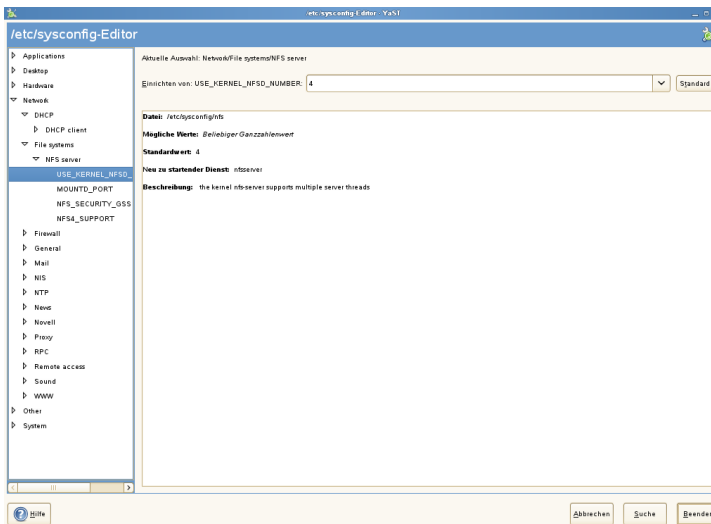
Der YaST-Editor `"sysconfig"` bietet ein benutzerfreundliches Frontend für die Systemkonfiguration. Ohne den eigentlichen Speicherort der zu ändernden Konfigurationsvariablen zu kennen, können Sie mithilfe der integrierten Suchfunktion dieses Moduls den Wert der Konfigurationsvariable wie erforderlich 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 12.2 *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 Ände-

rungen zu bestätigen und zeigt an, welche Skripten ausgeführt werden, wenn Sie *Verlassen* wählen. Außerdem können Sie die Dienste und Skripten 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.

12.3.2 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 12, *Booten und Konfigurieren eines Linux-Systems*** (S. 203). 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. 53)). 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).

13.1 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`.

13.2 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. 228)).

`/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. 228)) 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.

13.2.1 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 13.3, „Konfigurieren des Bootloaders mit YaST“](#) (S. 232) 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. 225) 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. 226).

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 Plattennummerierung, 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 13.2.2, „Die Datei `device.map`“](#) (S. 229).

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)/message
color white/blue black/light-gray
default 0
timeout 8
```

```

title linux
    kernel (hd0,4)/vmlinuz root=/dev/sda7 vga=791
    initrd (hd0,4)/initrd

title windows
    chainloader (hd0,0)+1

title floppy
    chainloader (fd0)+1

title failsafe
    kernel (hd0,4)/vmlinuz.shipped root=/dev/sda7 ide=nodma \
    apm=off acpi=off vga=normal nosmp maxcpus=0 3
    initrd (hd0,4)/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. 228).

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. Eine Abbildung finden Sie in Abbildung „US-Tastaturbelegung“ (↑Start).

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
    kernel (hd0,0)/vmlinuz root=/dev/sda3 additional parameter
    initrd (hd0,0)/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.

13.2.2 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
```

13.2.3 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.

13.2.4 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: $1$lS2dv/$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 $1$lS2dv/$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 eingeben und die Eingabetaste gedrückt haben, sollte das ausgewählte Betriebssystem (in diesem Fall Linux) gebootet werden.

13.3 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 13.1**, „**Bootloader-Einstellungen**“ (S. 233) zeigt dies die aktuelle Bootloader-Konfiguration des Systems und ermöglicht Ihnen, Änderungen vorzunehmen.

Abbildung 13.1 *Bootloader-Einstellungen*



Auf der Registerkarte *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 13.2, „Booten mit GRUB“](#) (S. 222).

Verwenden Sie die Registerkarte *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 13.2, „Booten mit GRUB“](#) (S. 222)). 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.

13.3.1 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 13.1 *Ändern des Bootloader-Typs*

- 1 Wählen Sie die Registerkarte *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.

13.3.2 Speicherort des Bootloaders

Um den Speicherort des Bootloaders zu ändern, gehen Sie wie folgt vor:

Prozedur 13.2 *Speicherort des Bootloaders ändern*

- 1 Wählen Sie die Registerkarte *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*.

13.3.3 Standardsystem

Um das System zu ändern, das standardmäßig gebootet wird, gehen Sie wie folgt vor:

Prozedur 13.3 *Standardsystem einrichten*

- 1 Öffnen Sie die Registerkarte *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.

13.3.4 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 13.4 *Ändern des Bootloader-Zeitlimits*

- 1 Öffnen Sie die Registerkarte *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.

13.3.5 Sicherheitseinstellungen

Mit diesem YaST-Modul können Sie zum Schutz des Bootvorgangs auch ein Passwort einrichten. Damit wird ein zusätzlicher Grad an Sicherheit geboten.

Prozedur 13.5 *Festlegen eines Bootloader-Passworts*

- 1 Öffnen Sie die Registerkarte *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.

13.4 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 *Ja, neu schreiben*.

13.5 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 13.6 *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 `(sd*)` aufgeführt sind, mit dem Gerätenamen des CD-ROM-Laufwerks, das mit `(cd)` angegeben wird:

```
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 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.

13.6 Der grafische SUSE-Bildschirm

Seit SUSE Linux 7.2 wird der grafische SUSE-Bildschirm 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 13, Der Bootloader](#) (S. 221). 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.

13.7 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.

13.8 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).

14.1 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.

14.1.1 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 die persönlichen Einstellungen zurück aus den `*.old`-Dateien.

14.1.2 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 14.1**, „Eintrag in `/etc/crontab`“ (S. 244), 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 14.1 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-Skripten 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 Skripten `hourly`, `daily` oder andere Skripten für regelmäßige Wartungsarbeiten zu benutzerdefinierten Zeiten auszuführen, entfernen Sie regelmäßig die Zeitstempeldateien mit `/etc/crontab`-Einträgen (siehe **Beispiel 14.2**, „`/etc/crontab`: Entfernen der Zeitstempeldateien“ (S. 245) - u. a. wird `hourly` vor jeder vollen Stunde und `daily` einmal täglich um 2:14 Uhr entfernt).

Beispiel 14.2 */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`.

14.1.3 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 14.3 *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.

14.1.4 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.

14.1.5 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 14.1, „ulimit: Einstellen von Ressourcen für Benutzer“** (S. 247) aufgeführten Optionen.

Tabelle 14.1 *ulimit: Einstellen von Ressourcen für Benutzer*

<code>-m</code>	Maximale Größe des physischen Arbeitsspeichers
<code>-v</code>	Maximale Größe des virtuellen Arbeitsspeichers
<code>-s</code>	Maximale Größe des Stapels
<code>-c</code>	Maximale Größe der Core-Dateien
<code>-a</code>	Anzeigen der festgelegten Grenzwerte

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 14.4 *ulimit: Einstellungen in ~/.bashrc*

```
# Limits of 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`.

14.1.6 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 einer *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.

14.1.7 Die Datei /etc/resolv.conf

Die Auflösung von Domännennamen erfolgt über die Datei `/etc/resolv.conf`. Weitere Informationen finden Sie im Abschnitt **Kapitel 22, Domain Name System (DNS)** (S. 399).

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.

14.1.8 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 `info info` 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 `tkinfo`, `xinfo` oder das Hilfesystem von zum Anzeigen von info-Seiten verwenden.

14.1.9 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.

14.2 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

nen 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.

14.3 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>.

14.4 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 Buchstaben 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 12.3.1](#), „Ändern der Systemkonfiguration mithilfe des YaST-Editors `sysconfig`“ (S. 217)) 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>]
```

14.4.1 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 Programmmeldungen beispielsweise nicht verwenden möchten, nehmen Sie beispielsweise `LC_MESSAGES=es_ES` auf, damit die Meldungen stattdessen auf Spanisch angezeigt werden.

14.4.2 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
```

14.4.3 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.

14.4.4 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`.

Gerätemanagemet über dynamischen Kernel mithilfe von udev

15

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 Geräteknotendateien 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.

15.1 Das `/dev`-Verzeichnis

Die Geräteknoten 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 Geräteknoten 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`.

15.2 Kernel-uevents und udev

Die erforderlichen Geräteinformationen werden vom sysfs-Dateisystem exportiert. Für jedes Gerät, das der Kernel erkannt 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 15.6, „Einflussnahme auf das Gerätemanagemet über dynamischen Kernel mithilfe von udev-Regeln“](#) (S. 261).

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.

15.3 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.

15.4 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 Geräteknoten 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.

15.5 Überwachen des aktiven udev-Daemons

Das Programm `udevmonitor` 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 Partitionseignisse möglicherweise auf die Daten angewiesen sind, die das Ereignis für den primären Datenträger von der Hardware angefordert hat.

`udevmonitor --env` zeigt die vollständige Ereignisumgebung:

```
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 Dämons kann mit `udevcontrol log_priority=level/number` geändert werden.

15.6 Einflussnahme auf das Gerätemanagemet 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 15.1 *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` 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.

15.6.1 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.

15.6.2 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

15.6.3 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-Attribut 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.

15.6.4 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 Geräteknoten Werte, Namen und Aktionen zu.

`NAME`

Der Name des zu erstellenden Geräteknotens. 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 Geräteknoten 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.

15.7 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
```

15.8 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

15.9 Weiterführende Informationen

Weitere Informationen zur udev-Infrastruktur finden Sie auf den folgenden Manualpages:

udev

Allgemeine Informationen zu udev, Schlüssel, Regeln und anderen wichtigen Konfigurationsbelangen.

udevinfo

udevinfo kann verwendet werden, um Geräteinformationen aus der udev-Datenbank abzufragen.

udev

Informationen zum udev-Ereignisverwaltungs-Daemon.

udevmonitor

udevmonitor gibt die Kernel- und udev-Ereignissequenz an der Konsole aus. Dieses Werkzeug wird hauptsächlich zur Fehlersuche verwendet.

Dateisysteme in Linux

openSUSE® wird mit einer Reihe von unterschiedlichen Dateisystemen geliefert (ReiserFS, Ext2, Ext3 und XFS), aus denen Sie bei der Installation wählen können. Jedes Dateisystem hat seine Vor- und Nachteile, durch die es sich mehr oder weniger für ein bestimmtes Szenario eignet. Für eine professionelle Hochleistungsumgebung wird wahrscheinlich ein anderes Dateisystem gewählt als für die Computerbenutzung zuhause.

16.1 Terminologie

Metadaten

Eine interne Datenstruktur des Dateisystems, die gewährleistet, dass alle Daten auf dem Datenträger ordnungsgemäß organisiert sind und darauf zugegriffen werden kann. Im Grunde sind es „Daten über die Daten.“ Nahezu jedes Dateisystem verfügt über seine eigene Struktur an Metadaten. Das ist eine der Ursachen für die unterschiedlichen Leistungsmerkmale von Dateisystemen. Es ist von größter Wichtigkeit, dass Metadaten intakt bleiben, anderenfalls können alle Daten auf dem Dateisystem unzugreifbar werden.

Inode

Inodes enthalten zahlreiche Informationen zu einer Datei, einschließlich Größe, Anzahl an Links, Zeiger auf die Plattenblöcke, auf denen der Dateiinhalt tatsächlich gespeichert wird, sowie Datum und Uhrzeit der Erstellung, der Änderung und des Zugriffs.

Journal

Im Kontext eines Dateisystems ist ein Journal eine Struktur auf dem Datenträger, die eine Art Protokoll enthält, in dem das Dateisystem speichert, was sich in den Metadaten des Dateisystems ändert. Durch Journaling verringert sich die Wiederherstellungsdauer für ein Linux-System erheblich, da es den langen Suchvorgang überflüssig macht, der beim Systemstart das ganze Dateisystem prüft. Stattdessen wird nur das Journal wiedergegeben.

16.2 Wichtige Dateisysteme in Linux

Die Wahl eines Dateisystems für ein Linux-System ist nicht mehr wie noch vor zwei oder drei Jahren eine Sache von wenigen Sekunden (Ext2 oder ReiserFS?). Kernels, die mit 2.4 beginnen, stellen eine Vielzahl von Dateisystemen zur Auswahl. Nachfolgend erhalten Sie einen Überblick über die grundlegende Funktionsweise und die Vorzüge dieser Dateisysteme.

Denken Sie daran, dass es wahrscheinlich kein Dateisystem gibt, das für alle Arten von Anwendungen optimal ist. Jedes Dateisystem hat seine Stärken und Schwächen, die berücksichtigt werden müssen. Selbst das anspruchsvollste Dateisystem kann jedoch keine vernünftige Strategie für Sicherungskopien ersetzen.

Die Begriffe *Datenintegrität* und *Datenkonsistenz* beziehen sich in diesem Kapitel nicht auf die Konsistenz der Daten auf Benutzerebene (Daten, die Ihre Anwendung in ihre Dateien schreibt). Ob diese Daten konsistent sind, muss die Anwendung selbst prüfen.

WICHTIG: Einrichten von Dateisystemen

Wenn in diesem Kapitel nichts anderes angegeben ist, können alle Schritte für das Einrichten oder Ändern von Partitionen und Dateisystemen mit YaST ausgeführt werden.

16.2.1 ReiserFS

ReiserFS, offiziell eine der wichtigsten Funktionen der Kernel-Version 2.4, war seit der Version 6.4 als Kernel-Patch für SUSE-Kernels der Version 2.2.x verfügbar. ReiserFS wurde von Hans Reiser und dem Entwicklungs-Team Namesys konzipiert. Es hat sich als leistungsstarke Alternative zu Ext2 bewährt. Seine Vorzüge sind eine bes-

sere Nutzung des Speicherplatzes, bessere Leistung beim Plattenzugriff und schnellere Wiederherstellung nach einem Absturz.

Die Stärken von ReiserFS:

Bessere Nutzung des Speicherplatzes

In ReiserFS werden alle Daten in einer Struktur namens "B*-balanced Tree" organisiert. Die Baumstruktur trägt zur besseren Nutzung des Festplattenspeichers bei, da kleine Dateien direkt in den Blättern des B*-Baums gespeichert werden können, statt sie an anderer Stelle zu speichern und einfach den Zeiger auf den tatsächlichen Ort zu verwalten. Darüber hinaus wird der Speicher nicht in Einheiten von 1 oder 4 KB zugewiesen, sondern in exakt der benötigten Größe. Ein weiterer Vorteil liegt in der dynamischen Zuweisung von Inodes. Damit bleibt das Dateisystem flexibler als traditionelle Dateisysteme wie Ext2, bei dem die Inode-Dichte bei der Erstellung des Dateisystems angegeben werden muss.

Bessere Leistung beim Festplattenzugriff

Bei kleinen Dateien werden häufig die Dateidaten und die „stat_data“ (Inode)-Informationen nebeneinander gespeichert. Sie lassen sich in einer einzigen E/A-Operation lesen, d. h., ein einziger Festplattenzugriff genügt, um alle benötigten Informationen abzurufen.

Schnelle Wiederherstellung nach einem Absturz

Durch Verwendung eines Journals zur Nachverfolgung kürzlich erfolgter Metadatenänderungen reduziert sich die Dateisystemüberprüfung sogar für große Dateisysteme auf wenige Sekunden.

Zuverlässigkeit durch Daten-Journaling

ReiserFS unterstützt auch Daten-Journaling und "ordered-data"-Modi ähnlich den Konzepten, die im Ext3-Abschnitt, [Abschnitt 16.2.3, „Ext3“](#) (S. 276), umrissen werden. Der Standardmodus ist `data=ordered`, was die Integrität von Daten und Metadaten sicherstellt, aber Journaling nur für Metadaten nutzt.

16.2.2 Ext2

Die Ursprünge von Ext2 reichen bis zu den Anfangstagen der Linux-Geschichte zurück. Sein Vorgänger, das Extended File System, wurde im April 1992 implementiert und in Linux 0.96c integriert. Das Extended File System unterzog sich einer Reihe von Änderungen und entwickelte sich als Ext2 für viele Jahre zum beliebtesten Linux-

Dateisystem. Mit der Erstellung von Journaling File Systemen und ihren verblüffend kurzen Wiederherstellungszeiten verlor Ext2 an Bedeutung.

Eine kurze Zusammenfassung der Vorzüge von Ext2, die verdeutlicht, warum es das beliebteste Linux-Dateisystem vieler Linux-Benutzer war und in einigen Bereichen immer noch ist.

Stabilität

Als wahrer „Oldtimer“ erlebte Ext2 viele Verbesserungen und wurde ausgiebig getestet. Das kann der Grund dafür sein, dass es als "unerschütterlich" gilt. Wenn nach einem Systemausfall kein ordnungsgemäßes Aushängen des Dateisystems möglich war, beginnt `e2fsck`, die Dateisystemdaten zu analysieren. Metadaten werden in einen konsistenten Zustand gebracht und schwebende Dateien oder Datenblöcke werden in ein ausgewiesenes Verzeichnis geschrieben (genannt `lost + found`). Im Unterschied zu Journaling File Systemen analysiert `e2fsck` das ganze Dateisystem und nicht nur die kürzlich geänderten Metadaten. Das dauert erheblich länger als das Überprüfen der Protokolldaten eines Journaling File Systems. Abhängig von der Größe des Dateisystems kann dies eine halbe Stunde oder länger dauern. Daher sollte Ext2 nicht für einen Server gewählt werden, der auf hohe Verfügbarkeit angewiesen ist. Da Ext2 jedoch kein Journal führt und bedeutend weniger Speicher belegt, ist es manchmal schneller als andere Dateisysteme.

Einfaches Upgrade

Der Code für Ext2 bildet die starke Grundlage, auf der sich Ext3 zu einem hoch geschätzten Dateisystem der nächsten Generation entwickeln konnte. Seine Zuverlässigkeit und Stabilität wurden geschickt mit den Vorzügen eines Journaling File Systems kombiniert.

16.2.3 Ext3

Ext3 wurde von Stephen Tweedie entwickelt. Im Unterschied zu allen anderen Dateisystemen der nächsten Generation folgt Ext3 keinem komplett neuen Entwicklungsprinzip. Es basiert auf Ext2. Diese beiden Dateisysteme sind sehr eng miteinander verwandt. Ein Ext3-Dateisystem kann einfach auf einem Ext2-Dateisystem aufgebaut werden. Der wesentlichste Unterschied zwischen Ext2 und Ext3 liegt darin, dass Ext3 Journaling unterstützt. Insgesamt bietet Ext3 drei wesentliche Vorteile:

Einfache und höchst zuverlässige Dateisystem-Upgrades von Ext2

Da Ext3 auf dem Ext2-Code basiert und dessen platteneigenes Format sowie sein Metadatenformat teilt, sind Upgrades von Ext2 auf Ext3 unglaublich einfach. Im Unterschied zur Umstellung auf andere Journaling File Systeme, wie z. B. ReiserFS oder XFS, die sich ziemlich langwierig gestalten können (Anlegen von Sicherungskopien des kompletten Dateisystems und ein kompletter Neuaufbau des Dateisystems), ist eine Umstellung auf Ext3 eine Sache von Minuten. Zudem ist es sehr sicher, da die Neuerstellung eines ganzen Dateisystems von Grund auf eventuell nicht reibungslos funktioniert. In Anbetracht der bestehenden Ext2-Systeme, die auf ein Upgrade auf ein Journaling File System warten, lässt sich leicht ausrechnen, warum Ext3 für viele Systemadministratoren eine gewisse Bedeutung hat. Ein Downgrade von Ext3 auf Ext2 ist genauso leicht wie das Upgrade. Führen Sie einfach ein sauberes Aushängen des Ext3-Dateisystems durch und hängen Sie es neu als ein Ext2-Dateisystem ein.

Zuverlässigkeit und Leistung

Einige andere Journaling File Systeme nutzen die Journaling-Methode „nur Metadaten“. Das bedeutet, Ihre Metadaten bleiben stets in einem konsistenten Zustand, jedoch kann dasselbe nicht automatisch für die eigentlichen Dateisystemdaten garantiert werden. Ext3 ist in der Lage, sich sowohl um die Metadaten als auch die Daten selbst zu kümmern. Wie eingehend sich Ext3 um Daten und Metadaten „kümmert“, ist individuell einstellbar. Maximale Sicherheit (Datenintegrität) wird durch den Start von Ext3 im Modus `data=journal` erreicht; dies kann jedoch das System verlangsamen, da sowohl Metadaten als auch Daten selbst im Journal erfasst werden. Ein relativ neuer Ansatz besteht in der Verwendung des Modus `data=ordered`, der sowohl die Daten- als auch die Metadatenintegrität gewährleistet, jedoch das Journaling nur für Metadaten verwendet. Der Dateisystemtreiber sammelt alle Datenblöcke, die einem Metadaten-Update entsprechen. Diese Datenblöcke werden vor dem Metadaten-Update auf Platte geschrieben. So wird Konsistenz für Metadaten und Daten erzielt, ohne die Leistung zu beeinträchtigen. Eine dritte Möglichkeit ist die Verwendung von `data=writeback`, bei der Daten in das Hauptdateisystem geschrieben werden können, nachdem die Metadaten im Journal festgeschrieben wurden. Diese Option wird häufig als die beste hinsichtlich der Leistung betrachtet. Sie kann jedoch ermöglichen, dass alte Daten nach einem Absturz und der Wiederherstellung erneut in Dateien auftauchen, während die interne Integrität des Dateisystems bewahrt wird. Sofern nicht anders angegeben, wird Ext3 mit der Standardeinstellung `data=ordered` gestartet

16.2.4 Konvertieren eines Ext2-Dateisystems in Ext3

Gehen Sie wie folgt vor, um ein Ext2-Dateisystem in Ext3 zu konvertieren:

- 1 Legen Sie ein Ext3-Journal an, indem Sie `tune2fs -j` als `root` ausführen. Dabei wird ein Ext3-Journal mit den Standardparametern erstellt.

Falls Sie selbst die Größe des Journals und dessen Speicherort festlegen möchten, führen Sie stattdessen `tune2fs -J` zusammen mit den entsprechenden Journaloptionen `size=` und `device=` aus. Weitere Informationen zu dem Programm `tune2fs` finden Sie auf der Manualpage "tune2fs".

- 2 Um sicherzustellen, dass das Ext3-Dateisystem als solches erkannt wird, bearbeiten Sie die Datei `/etc/fstab` als `root`, indem Sie den Dateisystemtyp für die entsprechende Partition von `ext2` in `ext3` ändern. Diese Änderung wird nach dem nächsten Neustart wirksam.
- 3 Um ein Root-Dateisystem zu booten, das als Ext3-Partition eingerichtet wurde, nehmen Sie die Module `ext3` und `jbd` in `initrd` auf. Bearbeiten Sie hierfür `/etc/sysconfig/kernel` als `root`, indem Sie der Variablen `INITRD_MODULES` `ext3` und `jbd` hinzufügen. Führen Sie nach dem Speichern der Änderungen den Befehl `mkinitrd` aus. Damit wird eine neue `initrd` aufgebaut und zur Verwendung vorbereitet.

16.2.5 XFS

Ursprünglich als Dateisystem für ihr IRIX-Betriebssystem gedacht, begann SGI die Entwicklung von XFS bereits in den frühen 1990er-Jahren. Mit XFS sollte ein leistungsstarkes 64-Bit-Journaling File System geschaffen werden, das den extremen Herausforderungen der heutigen Zeit gewachsen ist. XFS eignet sich sehr gut für den Umgang mit großen Dateien und zeigt gute Leistungen auf High-End-Hardware. Jedoch hat auch XFS einen Schwachpunkt. Wie ReiserFS legt XFS großen Wert auf Metadatenintegrität, jedoch weniger auf Datenintegrität.

Ein kurzer Blick auf die Hauptfunktionen von XFS erklärt, warum es sich möglicherweise als starke Konkurrenz zu anderen Journaling File Systemen in der High-End-Datenverarbeitung erweisen könnte.

Hohe Skalierbarkeit durch den Einsatz von Zuweisungsgruppen

Bei der Erstellung eines XFS-Dateisystems wird das dem Dateisystem zugrunde liegende Blockgerät in acht oder mehr lineare Bereiche gleicher Größe unterteilt. Diese werden als *Zuweisungsgruppen* bezeichnet. Jede Zuweisungsgruppe verwaltet Inodes und freien Speicher selbst. Zuordnungsgruppen können praktisch als Dateisysteme im Dateisystem betrachtet werden. Da Zuordnungsgruppen relativ autonom sind, kann der Kernel gleichzeitig mehrere von ihnen adressieren. Diese Funktion ist der Schlüssel zur hohen Skalierbarkeit von XFS. Das Konzept der autonomen Zuordnungsgruppen kommt natürlicherweise den Anforderungen von Multiprozessorsystemen entgegen.

Hohe Leistung durch effiziente Verwaltung des Festplattenspeichers

Freier Speicher und Inodes werden von B^+ -Bäumen innerhalb der Zuordnungsgruppen verwaltet. Der Einsatz von B^+ -Bäumen trägt wesentlich zur Leistung und Skalierbarkeit von XFS bei. XFS verwendet *Delayed Allocation* (verzögerte Speicherzuweisung). Es führt die Speicherzuweisung in zwei Schritten durch. Eine ausstehende Transaktion wird im RAM gespeichert und der entsprechende Speicherplatz reserviert. XFS entscheidet noch nicht, wo genau (d. h. in welchen Dateisystemblöcken) die Daten gespeichert werden. Diese Entscheidung wird auf den letztmöglichen Moment hinausgezögert. Einige kurzlebige, temporäre Daten werden somit niemals auf Platte gespeichert, da sie zum Zeitpunkt der Entscheidung über ihren Speicherort durch XFS bereits überholt sind. So erhöht XFS die Leistung und verringert die Fragmentierung des Dateisystems. Da jedoch eine verzögerte Zuweisung weniger Schreibvorgänge als in anderen Dateisystemen zur Folge hat, ist es wahrscheinlich, dass der Datenverlust nach einem Absturz während eines Schreibvorgangs größer ist.

Vorabzuweisung zur Vermeidung von Dateisystemfragmentierung

Vor dem Schreiben der Daten in das Dateisystem *reserviert* XFS den benötigten Speicherplatz für eine Datei (bzw. weist ihn vorab zu). Damit wird die Dateisystemfragmentierung erheblich reduziert. Die Leistung wird erhöht, da die Dateiinhalte nicht über das gesamte Dateisystem verteilt werden.

16.3 Weitere unterstützte Dateisysteme

Tabelle 16.1, „Dateisystemarten unter Linux“ (S. 280) In sind weitere von Linux unterstützte Dateisysteme aufgelistet. Sie werden hauptsächlich unterstützt, um die Kompatibilität und den Datenaustausch zwischen unterschiedlichen Medien oder fremden Betriebssystemen sicherzustellen.

Tabelle 16.1 *Dateisystemarten unter Linux*

<code>cramfs</code>	<i>Komprimiertes ROM-Dateisystem:</i> ein komprimiertes Nur-Lese-Dateisystem für ROMs
<code>hpfs</code>	<i>Hochleistungsfähiges Dateisystem:</i> Das Standarddateisystem IBM OS/2 wird nur im schreibgeschützten Modus verwendet.
<code>iso9660</code>	Standarddateisystem auf CD-ROMs.
<code>minix</code>	Dieses Dateisystem wurde ursprünglich für Forschungsprojekte zu Betriebssystemen entwickelt und war das erste unter Linux verwendete Dateisystem. Heute wird es noch für Disketten eingesetzt.
<code>msdos</code>	<i>fat</i> , das von DOS stammende Dateisystem, wird heute noch von verschiedenen Betriebssystemen verwendet.
<code>ncpfs</code>	Dateisystem zum Einhängen von Novell-Volumes über Netzwerke.
<code>nfs</code>	<i>Netzwerkdateisystem:</i> Hier können Daten auf jedem Rechner in einem Netzwerk gespeichert werden und der Zugriff kann über ein Netzwerk gewährt werden.
<code>smbfs</code>	<i>Server Message Block</i> wird von Produkten wie Windows für den Dateizugriff über ein Netzwerk verwendet.
<code>sysv</code>	Verwendet unter SCO UNIX, Xenix und Coherent (kommerzielle UNIX-Systeme für PCs).

ufs	Verwendet von BSD, SunOS und NeXTSTEP. Nur im Nur-Lese-Modus unterstützt.
umsdos	<i>UNIX auf MSDOS</i> : Aufgesetzt auf einem normalen fat-Dateisystem. Erhält UNIX-Funktionalität (Rechte, Links, lange Dateinamen) durch die Erstellung spezieller Dateien.
vfat	<i>Virtual FAT</i> : Erweiterung des FAT-Dateisystems (unterstützt lange Dateinamen).
ntfs	<i>Windows NT File System</i> , Nur-Lese-Modus.

16.4 Large File Support unter Linux

Ursprünglich unterstützte Linux eine maximale Dateigröße von 2 GB. Mit dem zunehmenden Einsatz von Linux für Multimedia und zur Verwaltung riesiger Datenbanken reichte dies nicht mehr aus. Aufgrund des immer häufigeren Einsatzes als Server-Betriebssystem wurden der Kernel und die C Library so angepasst, dass sie auch Dateien unterstützen, die größer als 2 GB sind. Dazu wurden neue Schnittstellen eingeführt, die von Anwendungen genutzt werden können. Heutzutage bieten fast alle wichtigen Dateisysteme eine Unterstützung von LFS zur High-End-Datenverarbeitung. **Tabelle 16.2, „Maximale Größe von Dateisystemen (Festplattenformat)“** (S. 281) bietet einen Überblick über die derzeitigen Beschränkungen für Linux-Dateien und -Dateisysteme.

Tabelle 16.2 *Maximale Größe von Dateisystemen (Festplattenformat)*

Dateisystem	Dateigröße (Byte)	Dateisystemgröße (Byte)
Ext2 oder Ext3 (Blockgröße (1 KB))	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 oder Ext3 (Blockgröße (2 KB))	2^{38} (256 GB)	2^{43} (8 TB)

Dateisystem	Dateigröße (Byte)	Dateisystemgröße (Byte)
Ext2 oder Ext3 (Blockgröße (4 KB))	2^{41} (2 TB)	2^{43} -4096 (16 TB-4096 Byte)
Ext2 oder Ext3 (Blockgröße (8 KB) (Systeme mit 8-KB-Seiten, wie Alpha)	2^{46} (64 TB)	2^{45} (32 TB)
ReiserFS v3	2^{46} (64 TB)	2^{45} (32 TB)
XFS	2^{63} (8 EB)	2^{63} (8 EB)
NFSv2 (Client-seitig)	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3 (Client-seitig)	2^{63} (8 EB)	2^{63} (8 EB)

WICHTIG: Linux-Kernel-Beschränkungen

Tabelle 16.2, „Maximale Größe von Dateisystemen (Festplattenformat)“ (S. 281) beschreibt die Einschränkungen in Abhängigkeit vom Festplattenformat. Der Kernel von Version 2.6 hat seine eigenen Einschränkungen für die maximale Größe von Dateien und Dateisystemen. Zulässig sind:

Dateigröße

Dateien können auf 32-Bit-Systemen nicht größer sein als 2 TB (2^{41} Byte).

Dateisystemgröße

Dateisysteme können bis zu 2^{73} Byte groß sein. Dieses Limit schöpft jedoch noch keine verfügbare Hardware aus.

16.5 Weiterführende Informationen

Jedes der oben beschriebenen Dateisystemprojekte unterhält seine eigene Homepage, wo Sie Informationen aus Mailinglisten und weitere Dokumentation sowie FAQ erhalten.

- <http://e2fsprogs.sourceforge.net/>
- <http://www.zipworld.com.au/~akpm/linux/ext3/>
- <http://www.namesys.com/>
- <http://oss.sgi.com/projects/xfst/>
- <http://oss.oracle.com/projects/ocfs2/>

Ein umfassendes mehrteiliges Tutorial zu Linux-Dateisystemen findet sich unter *IBM developerWorks*: <http://www-106.ibm.com/developerworks/library/l-fs.html>. Einen ausführlichen Vergleich der verschiedenen Dateisysteme (nicht nur Linux-Dateisysteme) steht über das folgende Wikipedia-Projekt zur Verfügung http://en.wikipedia.org/wiki/Comparison_of_file_systems#Comparison.

Zugriffssteuerungslisten unter Linux

17

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.

17.1 Traditionelle Dateiberechtigungen

Die Grundlagen der traditionellen Linux-Dateiberechtigungen werden unter **Abschnitt 19.2, „Benutzer und Zugriffsberechtigungen“** (S. 316) erläutert. Erweiterte Funktionen sind das `setuid`-, das `setgid`- und das sticky-Bit.

17.1.1 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, dass 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.

17.1.2 setgid-Bit

Das `setuid`-Bit hat für Benutzer Gültigkeit. Es gibt jedoch eine entsprechende Eigenschaft für Gruppen, nämlich das *setgid*-Bit. Ein Program, 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.

17.1.3 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
```

17.2 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.

17.3 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.

17.4 Arbeiten mit ACLs

Tabelle 17.1, „Typen von ACL-Einträgen“ (S. 289) 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 Berechti-

gungen 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 17.2, „Maskierung von Zugriffsberechtigungen“](#) (S. 290) 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 17.1 Typen von ACL-Einträgen

Typ	Textformat
owner	user::rwx
named user	user:name:rwx
owning group	group::rwx
named group	group:name:rwx

Typ	Textformat
mask	mask::rwx
other	other::rwx

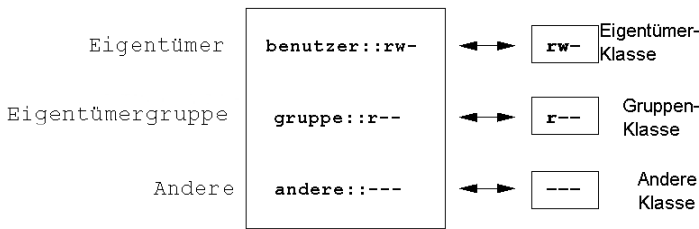
Tabelle 17.2 Maskierung von Zugriffsberechtigungen

Eintragstyp	Textformat	Berechtigungen
named user	user:geeko:r-x	r-x
mask	mask::rw-	rw-
	wirksame Berechtigungen:	r--

17.4.1 ACL-Einträge und Dateimodus-Berechtigungsbits

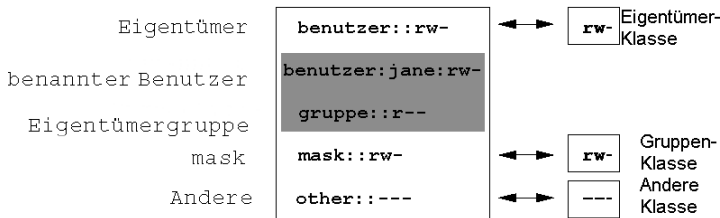
Abbildung 17.1, „Minimale ACL: ACL-Einträge im Vergleich zu Berechtigungsbits“ (S. 291) und **Abbildung 17.2, „Erweiterte ACL: ACL-Einträge im Vergleich zu Berechtigungsbits“** (S. 291) zeigen eine minimale und eine erweiterte ACL. Die Abbildungen sind in drei Blöcke unterteilt: der linke Block zeigt 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 17.1 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 17.1, „Minimale ACL: ACL-Einträge im Vergleich zu Berechtigungsbits“** (S. 291) dargestellt. Im Fall einer erweiterten ACL (mit "mask") werden die "group class"-Berechtigungen dem "mask"-Eintrag zugeordnet. Dies ist in **Abbildung 17.2, „Erweiterte ACL: ACL-Einträge im Vergleich zu Berechtigungsbits“** (S. 291) dargestellt.

Abbildung 17.2 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.

17.4.2 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 `ascots` Lese-, Schreib- und Ausführberechtigungen gewähren, indem Sie folgenden Befehl eingeben:

```
setfacl -m user:geeko:rwx,group:ascots: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 17.2, „Maskierung von Zugriffsberechtigungen“](#) (S. 290)). 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.

17.4.3 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. 294)). 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.

17.4.4 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.

17.5 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.

17.6 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.

18.1 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:

`Erforderlich`

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.

Aufnehmen

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).

18.2 PAM-Konfiguration von sshd

Betrachten Sie zum Verständnis der Theorie, auf der PAM basiert, die PAM-Konfiguration von `sshd` als praktisches Beispiel:

Beispiel 18.1 *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 18.2, „Standardkonfiguration für den Abschnitt `auth`“** (S. 303).

Beispiel 18.2 *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 18.3, „Standardkonfiguration für den Abschnitt `account`“** (S. 304). 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 18.4, „Standardkonfiguration für den Abschnitt `password`“** (S. 304) dargestellt.

Beispiel 18.3 *Standardkonfiguration für den Abschnitt account*

```
account required          pam_unix2.so
```

Beispiel 18.4 *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 18.5 *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.

18.3 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)`).

18.4 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.

Arbeiten mit der Shell

Obwohl grafische Bedienoberflächen zunehmend wichtiger und benutzerfreundlicher geworden sind, sind sie nicht die einzige Kommunikationsmöglichkeit mit Ihrem System. Ein Kommandozeilen-Interpreter, in Unix/Linux als *Shell* bezeichnet, bietet ein höchst flexibles und effizientes Mittel zur textorientierten Kommunikation mit Ihrem System.

Gerade bei der Administration spielen Shell-basierte Anwendungen eine besonders große Rolle, wenn Sie zum Beispiel Computer über langsame Netzwerkverbindungen steuern müssen oder als Administrator Aufgaben von der Kommandozeile ausführen möchten.

In diesem Kapitel werden einige grundlegende Konzepte besprochen, die Sie kennen sollten, um die Kommandozeile effizient nutzen zu können. Sie erfahren hier mehr über die Verzeichnisstruktur und das Benutzer- und Berechtigungskonzept von Linux und Sie erhalten einen Überblick über die wichtigsten Shell-Kommandos sowie eine kurze Einleitung in den Editor *vi*, der unter Unix und Linux als Standardeditor immer zur Verfügung steht.

19.1 Verwenden der Bash-Shell

Für UNIX oder Linux sind mehrere Shells verfügbar, die sich geringfügig in ihrem Verhalten und den akzeptierten Befehlen unterscheiden. Die Standard-Shell in openSUSE ist Bash (GNU Bourne-Again Shell).

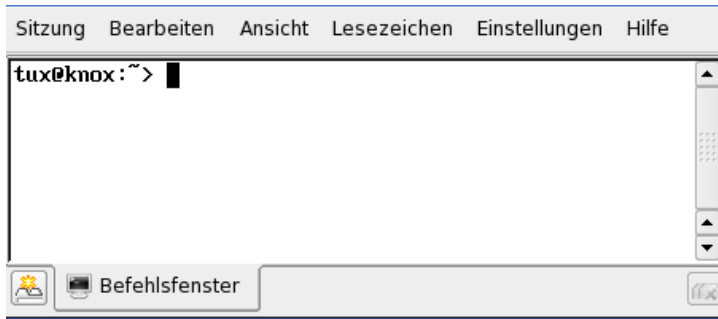
Wenn Sie an einer grafischen Bedienoberfläche angemeldet sind, können Sie eine (Anmelde-)Shell parallel zur Bedienoberfläche oder in einem Terminalfenster innerhalb

der grafischen Bedienoberfläche starten. Drücken Sie `Strg + Alt + F2`, um die grafische Bedienoberfläche zu verlassen und auf eine Anmelde-Shell zuzugreifen. Nach der Anmeldung zeigt die Anmeldung Ihren Anmeldenamen gefolgt von `@` und dem Hostnamen Ihres Computers an. Auf den Hostnamen folgt ein Doppelpunkt und der Pfad zum aktuellen Verzeichnis. Wenn Sie als Systemadministrator (`root`) angemeldet sind, kennzeichnet Bash dies mit einem Nummernzeichen (`#`). Direkt nach der Anmeldung ist gewöhnlich das aktuelle Verzeichnis das Home-Verzeichnis des Benutzerkontos, mit dem die Anmeldung erfolgte, und wird durch eine Tilde (`~`) gekennzeichnet. Wenn Sie bei einem entfernten Computer angemeldet sind, zeigen die an der Eingabeaufforderung angegebenen Informationen immer an, auf welchem System Sie gerade arbeiten. Sie können nun Befehle eingeben und Aufgaben ausführen. Sie melden sich von der Shell ab, indem Sie `exit` eingeben und `Alt + F7` drücken, um zurück zur grafischen Bedienoberfläche zu gelangen. Ihr Desktop und die darauf ausgeführten Anwendungen sind unverändert.

Sie starten ein Terminalfenster *in* der grafischen Bedienoberfläche von KDE oder GNOME, indem Sie `Alt + F2` drücken und `xterm` eingeben (oder auf das Konsole- oder GNOME-Terminalsymbol in der Kontrollleiste klicken). Auf Ihrem Desktop wird ein Terminalfenster geöffnet. Da Sie bereits an Ihrem Desktop angemeldet sind, zeigt die Eingabeaufforderung die gewöhnliche Anmelde- und Pfadinformation. Sie können nun Befehle eingeben und Aufgaben ausführen wie in jeder beliebigen Shell, die parallel zu Ihrem Desktop ausgeführt wird. Um das Terminalfenster zu schließen, drücken Sie `Alt + F4`

Das Konsole-Fenster bzw. das GNOME-Terminalfenster wird geöffnet. Es enthält die Eingabeaufforderung (Prompt) in der ersten Zeile, wie in **Abbildung 19.1, „Beispiel eines Bash-Terminalfensters“** (S. 311). Die Eingabeaufforderung zeigt normalerweise folgende Informationen an: Ihren Anmeldenamen (in diesem Fall `tux`), den Hostnamen Ihres Rechners (hier `knox`) und den aktuellen Pfad (in diesem Fall Ihr durch das Tilde-Symbol `~` gekennzeichnetes Home-Verzeichnis). Wenn Sie bei einem entfernten Computer angemeldet sind, zeigen diese Informationen immer an, auf welchem System Sie gerade arbeiten. Wenn sich der Cursor hinter diesen Angaben befindet, können Sie direkt Befehle eingeben und an das Computersystem senden.

Abbildung 19.1 *Beispiel eines Bash-Terminalfensters*



Da die Shell keinen grafischen Überblick über die Verzeichnisse und Dateien bietet, wie beispielsweise eine Baumansicht in einem Dateimanager, ist es hilfreich, wenn Sie einige Grundkenntnisse zur Standardverzeichnisstruktur in Linux besitzen.

19.1.1 Die Verzeichnisstruktur

Die folgende Tabelle bietet eine kurze Übersicht über die wichtigsten Verzeichnisse der höheren Ebene auf einem Linux-System. Ausführlichere Informationen über die Verzeichnisse und wichtige Unterverzeichnisse erhalten Sie in der folgenden Liste.

Tabelle 19.1 *Überblick über eine Standardverzeichnisstruktur*

Verzeichnis	Inhalt
/	Root-Verzeichnis – Startpunkt der Verzeichnisstruktur.
/bin	Grundlegende binäre Dateien, z. B. Befehle, die der Systemadministrator und normale Benutzer brauchen. Enthält gewöhnlich auch die Shells, z. B. Bash.
/boot	Statische Dateien des Bootloaders.
/dev	Erforderliche Dateien für den Zugriff auf Host-spezifische Geräte.
/etc	Host-spezifische Systemkonfigurationsdateien.

Verzeichnis	Inhalt
/home	Enthält die Home-Verzeichnisse aller Benutzer, die ein Konto auf dem System haben. Nur das Home-Verzeichnis von <code>root</code> befindet sich nicht unter <code>/home</code> , sondern unter <code>/root</code> .
/lib	Grundlegende freigegebene Bibliotheken und Kernel-Module.
/media	Einhängpunkte für Wechselmedien.
/mnt	Einhängpunkt für das temporäre Einhängen eines Dateisystems.
/opt	Add-On-Anwendungssoftwarepakete.
/root	Home-Verzeichnis für den Superuser <code>root</code> .
/sbin	Grundlegende Systembinärdateien.
/srv	Daten für Dienste, die das System bereitstellt.
/tmp	Temporäre Dateien.
/usr	Sekundäre Hierarchie mit Nur-Lese-Daten.
/var	Variable Daten wie Protokolldateien.
/windows	Nur verfügbar, wenn sowohl Microsoft Windows* als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten.

Die folgende Liste bietet detailliertere Informationen und bietet einige Beispiele für die Dateien und Unterverzeichnisse, die in den Verzeichnissen gefunden werden können:

`/bin`

Enthält die grundlegenden Shell-Befehle, die `root` und andere Benutzer verwenden können. Zu diesen Kommandos gehören `ls`, `mkdir`, `cp`, `mv`, `rm` und `rmdir`.
`/bin` enthält auch `Bash`, die Standard-Shell in openSUSE.

`/boot`

Enthält Daten, die zum Booten erforderlich sind, z. B. den Bootloader, den Kernel und andre Daten, die verwendet werden, bevor der Kernel mit der Ausführung von Programmen im Benutzermodus beginnt.

`/dev`

Enthält Gerätedateien, die Hardware-Komponenten darstellen.

`/etc`

Enthält lokale Konfigurationsdateien, die den Betrieb von Programmen wie das X Window System steuern können. Das Unterverzeichnis `/etc/init.d` enthält Skripten, die während des Bootvorgangs ausgeführt werden.

`/home/Benutzername`

Enthält die privaten Daten aller Benutzer, die ein Konto auf dem System haben. Die Dateien, die hier gespeichert sind, können nur durch den Besitzer oder den Systemadministrator geändert werden. Standardmäßig befinden sich hier Ihr E-Mail-Verzeichnis und Ihre persönliche Desktopkonfiguration in Form von verborgenen Dateien und Verzeichnissen. KDE-Benutzer finden die persönlichen Konfigurationsdaten für den Desktop unter `.kde`, GNOME-Benutzer unter `.gconf`. Informationen zu verborgenen Dateien finden Sie unter Abschnitt „Wichtigste Merkmale“ (Kapitel 7, *Grundlegende Konzepte*, ↑Start).

ANMERKUNG: Home-Verzeichnis in einer Netzwerkumgebung

Wenn Sie in einer Netzwerkumgebung arbeiten, kann Ihr Home-Verzeichnis einem von `/home` abweichenden Verzeichnis zugeordnet sein.

`/lib`

Enthält grundlegende freigegebene Bibliotheken, die zum Booten des Systems und zur Ausführung der Befehle im Root-Dateisystem erforderlich sind. Freigegebene Bibliotheken entsprechen in Windows DLL-Dateien.

`/media`

Enthält Einhängepunkte für Wechselmedien, z. B. CD-ROMs, USB-Sticks und Digitalkameras (sofern sie USB verwenden). Unter `/media` sind beliebige Laufwerktypen gespeichert, mit Ausnahme der Festplatte Ihres Systems. Sobald Ihr Wechselmedium eingelegt bzw. mit dem System verbunden und eingehängt wurde, können Sie von hier darauf zugreifen.

`/mnt`

Dieses Verzeichnis bietet einen Einhängepunkt für ein temporär eingehängtes Dateisystem. `root` kann hier Dateisysteme einhängen.

`/opt`

Reserviert für die Installation zusätzlicher Software. Hier finden Sie Software- und größere Addon-Programmpakete. KDE3 befindet sich hier, während KDE4 und GNOME nach `/usr` verschoben wurden.

`/root`

Home-Verzeichnis für den Benutzer `root`. Hier befinden sich persönliche Daten von "`root`".

`/sbin`

Wie durch das `s` angegeben, enthält dieses Verzeichnis Dienstprogramme für den Superuser. `/sbin` enthält Binärdateien, die zusätzlich zu den Dateien in `/bin` wesentlich für Booten und Wiederherstellen des Systems erforderlich sind.

`/srv`

Enthält Daten für Dienste, die das System bereitstellt, z. B. FTP und HTTP.

`/tmp`

Dieses Verzeichnis wird von Programmen benutzt, die eine temporäre Speicherung von Dateien verlangen.

`/usr`

`/usr` hat nichts mit Benutzern ("`user`") zu tun, sondern ist das Akronym für UNIX-Systemressourcen. Die Daten in `/usr` sind statische, schreibgeschützte Daten, die auf verschiedenen Hosts freigegeben sein können, die den Filesystem Hierarchy Standard (FHS) einhalten. Dieses Verzeichnis enthält alle Anwendungsprogramme und bildet eine sekundäre Hierarchie im Dateisystem. `/usr` enthält eine Reihe von Unterverzeichnissen, z. B. `/usr/bin`, `/usr/sbin`, `/usr/local` und `/usr/share/doc`.

`/usr/bin`

Enthält Programme, die für den allgemeinen Zugriff verfügbar sind.

`/usr/sbin`

Enthält Programme, die für den Systemadministrator reserviert sind, z. B. Reparaturfunktionen.

`/usr/local`

In diesem Verzeichnis kann der Systemadministrator lokale, verteilungsunabhängige Erweiterungen installieren.

`/usr/share/doc`

Enthält verschiedene Dokumentationsdateien und die Versionshinweise für Ihr System. Im Unterverzeichnis `manual` befindet sich eine Online-Version dieses Handbuchs. Wenn mehrere Sprachen installiert sind, kann dieses Verzeichnis die Handbücher für verschiedene Sprachen enthalten.

Im Verzeichnis `packages` befindet sich die Dokumentation zu den auf Ihrem System installierten Software-Paketen. Für jedes Paket wird ein Unterverzeichnis `/usr/share/doc/packages/Paketname` angelegt, das häufig README-Dateien für das Paket und manchmal Beispiele, Konfigurationsdateien oder zusätzliche Skripten umfasst.

Wenn HOWTOs (Verfahrensbeschreibungen) auf Ihrem System installiert sind, enthält `/usr/share/doc` auch das Unterverzeichnis `howto` mit zusätzlicher Dokumentation zu vielen Aufgaben bei Setup und Betrieb von Linux-Software.

`/var`

Während `/usr` statische, schreibgeschützte Daten enthält, ist `/var` für Daten, die während des Systembetriebs geschrieben werden und daher variabel sind, z. B. Protokolldateien oder Spooling-Daten. Beispielsweise befinden sich die Protokolldateien Ihres Systems in `/var/log/messages` (nur für "root" zugreifbar).

`/windows`

Nur verfügbar, wenn sowohl Microsoft Windows als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten, die auf der Windows-Partition Ihres Systems verfügbar sind. Ob Sie die Daten in diesem Verzeichnis bearbeiten können, hängt vom Dateisystem ab, das Ihre Windows-Partition verwendet. Falls es sich um FAT32 handelt, können Sie die Dateien in diesem Verzeichnis öffnen und bearbeiten. In einem NTFS-Dateisystem können Sie jedoch Ihre Windows-Dateien

nur von Linux aus lesen, aber nicht ändern. Weitere Informationen dazu finden Sie unter Abschnitt „Zugreifen auf Dateien auf verschiedenen Betriebssystemen am selben Computer“ (Kapitel 11, *Kopieren und Freigeben von Dateien*, ↑Start).

19.2 Benutzer und Zugriffsberechtigungen

Seit den Anfängen, also Anfang 1990, wurde Linux als Mehrbenutzersystem entwickelt. Es kann also von mehreren Benutzern gleichzeitig bearbeitet werden. Bevor Benutzer auf ihrer Arbeitsstation eine Sitzung starten können, müssen Sie sich beim System anmelden. Jeder Benutzer verfügt über einen Benutzernamen mit einem zugehörigen Passwort. Durch diese Abgrenzung kann gewährleistet werden, dass nicht autorisierte Benutzer keine Dateien anzeigen können, für die sie keine Berechtigung aufweisen. Umfassendere Änderungen des Systems, beispielsweise das Installieren neuer Programme, sind im Regelfall für normale Benutzer entweder gar nicht oder nur beschränkt möglich. Nur der Benutzer "root", auch *Superuser* genannt, kann uneingeschränkt Änderungen am System vornehmen und uneingeschränkt auf alle Dateien zugreifen. Diejenigen Benutzer, die hinsichtlich dieses Konzepts überlegt vorgehen, sich also nur als Benutzer `root` mit uneingeschränkten Rechten anmelden, wenn dies erforderlich ist, können dazu beitragen, dass Risiko versehentlicher Datenverluste zu minimieren. Da unter normalen Umständen nur "root" Systemdateien löschen oder Festplatten formatieren kann, kann die Bedrohung durch *Trojanische Pferde* bzw. durch die versehentliche Eingabe zerstörender Befehle deutlich verringert werden.

19.2.1 Dateisystemberechtigungen

Grundsätzlich ist jede Datei in einem Linux-Dateisystem einem Benutzer und einer Gruppe zugehörig. Sowohl diese Gruppen (die Eigentümer) als auch alle anderen können zum Schreiben, Lesen oder Ausführen dieser Dateien autorisiert werden.

Eine Gruppe kann, in diesem Fall, als eine Reihe verbundener Benutzer mit bestimmten gemeinsamen Rechten definiert werden. Nennen Sie eine Gruppe, die an einem bestimmten Projekt arbeitet, beispielsweise `project3`. Jeder Benutzer in einem Linux-System ist Mitglied mindestens einer eigenen Gruppe, normalerweise `users`. In einem System können so viele Gruppen wie erforderlich vorhanden sein, jedoch kann nur

`root` Gruppen hinzufügen. Jeder Benutzer kann mithilfe des Befehls `groups` ermitteln, in welchen Gruppen er Mitglied ist.

Dateizugriff

Berechtigungen werden im Dateisystem für Dateien und Verzeichnisse unterschiedlich organisiert. Informationen zu Dateiberechtigungen können über den Befehl `ls -l` angezeigt werden. Die Ausgabe sieht u. U. wie in **Beispiel 19.1, „Beispielausgabe mit Dateiberechtigungen“** (S. 317) aus.

Beispiel 19.1 *Beispielausgabe mit Dateiberechtigungen*

```
-rw-r----- 1 tux project3 14197 Jun 21 15:03 Roadmap
```

Wie aus der dritten Spalte hervorgeht, gehört diese Datei Benutzer `tux`. Sie ist der Gruppe `project3` zugewiesen. Um die Benutzerberechtigungen für die Datei `Roadmap` zu ermitteln, muss die erste Spalte genauer untersucht werden.

-	rw-	r--	---
Typ	Benutzerberechtigungen	Gruppenberechtigungen	Berechtigungen für andere Benutzer

Diese Spalte besteht aus einem vorangestellten Zeichen, auf das neun in Dreiergruppen aufgeteilte Zeichen folgen. Der erste der zehn Buchstaben steht für den Typ der Dateisystemkomponente. Der Bindestrich (`-`) weist darauf hin, dass es sich um eine Datei handelt. Es kann auch auf ein Verzeichnis (`d`), einen Link (`l`), ein Blockgerät (`b`) oder ein zeichenorientiertes Gerät hingewiesen werden.

Die nachfolgenden drei Blöcke folgen einem Standardschema. Die ersten drei Zeichen geben an, ob die Datei gelesen werden kann (`r`) oder nicht (`-`). Ein `w` im mittleren Teil gibt an, dass das entsprechende Objekt bearbeitet werden kann, ein Bindestrich (`-`) weist darauf hin, dass die Datei schreibgeschützt ist. Ein `x` an dritter Stelle gibt an, dass das Objekt ausgeführt werden kann. Da es sich bei der Datei in diesem Beispiel um eine Textdatei handelt, nicht um eine ausführbare Datei, ist der Zugriff zum Ausführen für diese bestimmte Datei nicht erforderlich.

In diesem Beispiel verfügt `tux` als Eigentümer der Datei `Roadmap`, über Lese- (`r`) und Schreibzugriff (`w`) für die Datei, kann sie jedoch nicht ausführen (`x`). Die Mitglieder der Gruppe `project3` können die Datei lesen, sie jedoch nicht bearbeiten oder ausführen. Andere Benutzer dürfen auf diese Datei nicht zugreifen.

Weitere Berechtigungen können über Zugriffssteuerungslisten (Access Control Lists, ACLs) zugewiesen werden.

Verzeichnisberechtigungen

Zugriffsberechtigungen für Verzeichnisse haben den Typ `d`. Für Verzeichnisse weicht die Bedeutung der einzelnen Berechtigungen geringfügig voneinander ab.

Beispiel 19.2 *Beispielausgabe mit Verzeichnisberechtigungen*

```
drwxrwxr-x 1 tux project3 35 Jun 21 15:15 ProjectData
```

In **Beispiel 19.2**, „**Beispielausgabe mit Verzeichnisberechtigungen**“ (S. 318) sind der Eigentümer (`tux`) und die Eigentümergruppe (`project3`) des Verzeichnisses `ProjectData` leicht zu identifizieren. Im Gegensatz zu den Dateizugriffsberechtigungen unter **Dateizugriff** (S. 317) gibt die festgelegte Leseberechtigung (`r`) an, dass der Inhalt des Verzeichnisses angezeigt werden kann. Die Schreibberechtigung (`w`) ermöglicht die Erstellung neuer Dateien. Die Berechtigung für das Ausführen (`x`) ermöglicht dem Benutzer den Wechsel zu diesem Verzeichnis. Im obigen Beispiel können der Benutzer `tux` sowie die Mitglieder der Gruppe `project3` zum Verzeichnis `ProjectData` wechseln (`x`), den Inhalt anzeigen (`r`) sowie Dateien hinzufügen oder löschen (`w`). Die restlichen Benutzer verfügen hingegen über weniger Zugriffsrechte. Sie können zum Verzeichnis wechseln (`x`) und es durchsuchen (`r`), jedoch keine neuen Dateien hinzufügen (`w`).

19.2.2 Bearbeiten von Dateiberechtigungen

Ändern von Zugriffsberechtigungen

Die Zugriffsberechtigungen für eine Datei und ein Verzeichnis können vom Eigentümer und natürlich von `root` geändert werden. Hierfür wird der Befehl `chmod` verwendet. Ihm folgen die Parameter, die die Berechtigungen ändern sowie mindestens ein Dateiname. Die Parameter fallen in unterschiedliche Kategorien:

1. Hinsichtlich der Benutzer

- `u` (*user (Benutzer)*): Eigentümer der Datei
- `g` (*group (Gruppe)*): Gruppe, der die Datei gehört
- `o` (*others (andere)*): zusätzliche Benutzer (wenn kein Parameter angegeben ist, gelten die Änderungen für alle Kategorien)

2. Ein Zeichen für Löschen (-), Einstellen (=) oder Einfügen (+)

3. Die Abkürzungen

- *r – lesen*
- *w – schreiben*
- *x – ausführen*

4. Dateiname oder durch Leerzeichen voneinander getrennte Dateinamen

Wenn der Benutzer `tux` in **Beispiel 19.2, „Beispielausgabe mit Verzeichnisberechtigungen“** (S. 318) beispielsweise auch anderen Benutzern Schreibzugriff (*w*) für das Verzeichnis `ProjectData` gewähren möchte, ist dies über den Befehl `chmod o+w ProjectData` möglich.

Wenn er jedoch allen Benutzern außer sich selbst keine Schreibberechtigung gewähren möchte, kann er den Befehl `chmod go-w ProjectData` eingeben. Um allen Benutzern das Hinzufügen einer neuen Datei zu dem Ordner `ProjectData` zu verwehren, geben Sie `chmod -w ProjectData` ein. Nun kann selbst der Eigentümer keine neue Datei mehr im Verzeichnis erstellen, ohne zuvor die Schreibberechtigungen wieder einzurichten.

Ändern von Eigentumsberechtigungen

Weitere wichtige Befehle für das Steuern von Eigentümerschaft und Berechtigungen der Dateisystemkomponenten sind `chown` (change owner (Eigentümer ändern)) und `chgrp` (change group (Gruppe ändern)). Mithilfe des Befehls `chown` kann die Eigentümerschaft einer Datei auf einen anderen Benutzer übertragen werden. Diese Änderung darf jedoch nur von Benutzer `root` vorgenommen werden.

Angenommen, die Datei `Roadmap` aus **Beispiel 19.2, „Beispielausgabe mit Verzeichnisberechtigungen“** (S. 318) soll nicht mehr Eigentum von `tux`, sondern von Benutzer `geeko` sein. In diesem Fall sollte `root chown geeko Roadmap` eingeben.

Mit `chgrp` wird die Gruppeneigentümerschaft der Datei geändert. Der Eigentümer der Datei muss jedoch Mitglied der neuen Gruppe sein. Auf diese Weise kann Benutzer `tux` aus **Beispiel 19.1, „Beispielausgabe mit Dateiberechtigungen“** (S. 317) die Eigentümerschaft der Datei `ProjectData` in `project4` ändern (mithilfe

des Befehls `chgrp project4 ProjectData`), wenn er Mitglied dieser neuen Gruppe ist.

19.3 Wichtige Linux-Befehle

Dieser Abschnitt gibt Ihnen einen Überblick über die wichtigsten Befehle. Die Liste der Befehle in diesem Abschnitt ist keineswegs vollständig. Neben der grundlegenden Funktion der einzelnen Befehle werden in diesem Abschnitt auch die wichtigsten Parameter und Optionen erläutert. Weitere Informationen über die zahlreichen zur Verfügung stehenden Befehle erhalten Sie auf den zugehörigen `man`-Seiten, die Sie mit dem Befehl `man` gefolgt von dem Namen des jeweiligen Befehls öffnen (z. B. `man ls`).

In den `man`-Seiten navigieren Sie mit den Tasten `Bild auf` und `Bild ab` nach oben bzw. nach unten. Mit `Pos1` und `Ende` gelangen Sie an den Anfang oder das Ende des Dokuments und mit `Q` schließen Sie die `man`-Seiten. Weitere Informationen über den Befehl `man` erhalten Sie durch Eingabe von `man man`.

In der folgenden Übersicht sind die einzelnen Befehlselemente durch verschiedene Schriften hervorgehoben. Der eigentliche Befehl und die erforderlichen Parameter werden in der Form `Befehl Option` dargestellt. Nicht zwingend erforderliche Angaben und Parameter sind in `[eckigen Klammern]` eingeschlossen.

Passen Sie die Angaben Ihren Anforderungen an. Die Eingabe von `ls Datei(en)` ergibt keinen Sinn, wenn es keine Datei namens `Datei(en)` gibt, was vermutlich kaum der Fall sein dürfte. In der Regel können Sie mehrere Parameter kombinieren, indem Sie zum Beispiel statt `ls -l -a` einfach `ls -la` eingeben.

19.3.1 Dateibefehle

Im folgenden Abschnitt werden die wichtigsten Befehle für die Dateiverwaltung vorgestellt. Mit diesen Befehlen können sämtliche Aufgaben von der allgemeinen Dateiverwaltung bis hin zur Bearbeitung der Dateisystem-ACLs (Access Control Lists) ausgeführt werden.

Dateiverwaltung

`ls [Optionen] [Dateien]`

Ohne Angabe von Parametern listet dieser Befehl den Inhalt des aktuellen Verzeichnisses in Kurzform auf.

`-l`

Zeigt eine detaillierte Liste an.

`-a`

Zeigt versteckte Dateien an.

`cp [Optionen] Quelle - Ziel`

Kopiert die `Quelle` zum `Ziel`.

`-i`

Fragt den Benutzer, ob das `Ziel` überschrieben werden soll, falls es bereits vorhanden ist.

`-r`

Kopiert rekursiv (mit Unterverzeichnissen).

`mv [Optionen] Quelle - Ziel`

Kopiert die `Quelle` zum `Ziel` und löscht die `Quelle` danach.

`-b`

Erstellt vor dem Verschieben eine Sicherungskopie der `Quelle`.

`-i`

Fragt den Benutzer, ob das `Ziel` überschrieben werden soll, falls es bereits vorhanden ist.

`rm [Optionen] Dateien`

Entfernt die angegebenen Dateien aus dem Dateisystem. Verzeichnisse werden nicht durch `rm` entfernt, wenn die Option `-r` angegeben ist.

`-r`

Löscht auch eventuell vorhandene Unterverzeichnisse.

-i

Fordert den Benutzer vor dem Löschen jeder einzelnen Datei zur Bestätigung auf.

`ln [Optionen] Quelle Ziel`

Erstellt eine interne Verknüpfung (Link) zwischen `Quelle` und `Ziel`. Normalerweise verweist ein solcher Link unmittelbar auf die `Quelle` im gleichen Dateisystem. Mit der Option `-s` erstellt `ln` jedoch eine symbolische Verknüpfung (Symlink), die lediglich auf das Verzeichnis verweist, in dem sich `Quelle` befindet. Damit sind auch Verknüpfungen über mehrere Dateisysteme hinweg möglich.

-s

Erstellt eine symbolische Verknüpfung.

`cd [Optionen] [Verzeichnis]`

Wechselt das aktuelle Verzeichnis. Ohne Angabe von Parametern wechselt `cd` in das Home-Verzeichnis des Benutzers.

`mkdir [Optionen] Verzeichnis`

Erstellt ein neues Verzeichnis.

`rmdir [Optionen] Verzeichnis`

Löscht das angegebene Verzeichnis, sofern es leer ist.

`chown [Optionen] Benutzername[:[Gruppe]] Dateien`

Übergibt das Eigentum an den angegebenen Datei(en) an den angegebenen Benutzer.

-R

Ändert die Dateien und Verzeichnisse in allen Unterverzeichnissen.

`chgrp [Optionen] Gruppenname Dateien`

Übergibt das Gruppeneigentum an den angegebenen Datei(en) an die angegebene Gruppe. Der Eigentümer einer Datei kann die Gruppeneigenschaft nur dann ändern, wenn er sowohl Mitglied der aktuellen als auch der neuen Gruppe ist.

`chmod [Optionen] Modus Dateien`

Ändert die Zugriffsberechtigungen.

Der Parameter `Modus` besteht aus drei Teilen: `Gruppe`, `Zugriff` und `Zugriffstyp`. `Gruppe` akzeptiert die folgenden Zeichen:

u
Benutzer

g
Gruppe

o
Andere

Der Zugriff wird durch + (Zugriff) bzw. – (kein Zugriff) gesteuert.

Der Zugriffstyp wird durch folgende Optionen gesteuert:

r
Finden Sie unter

w
Schreiben

x
Ausführen – Ausführen der Dateien oder Wechseln in das Verzeichnis

s
Setuid-Bit – Das Programm wird ausgeführt, als ob es vom Eigentümer der Datei gestartet worden wäre.

Alternativ kann ein Zahlencode verwendet werden. Die vier Stellen dieses Codes setzen sich jeweils aus der Summe der Werte 4, 2 und 1 zusammen – dem Dezimalergebnis einer Binärmaske. Die erste Stelle bestimmt die Set User-ID (SUID) (4), die Set Group-ID (2) und die Sticky Bits (1). Die zweite Stelle legt die Berechtigungen des Dateieigentümers fest. Die dritte Stelle bestimmt die Berechtigungen der Gruppenmitglieder und die letzte Stelle bestimmt die Berechtigungen aller anderen Benutzer. Der Berechtigung zum Lesen ist die Zahl 4 zugewiesen, der Berechtigung zum Schreiben die Zahl 2 und der Berechtigung zum Ausführen die Zahl 1. Der Eigentümer einer Datei erhält normalerweise also eine 6 bzw. bei ausführbaren Dateien eine 7 (die Summe aller Berechtigungen).

`gzip [Parameter] Dateien`

Dieser Befehl komprimiert den Inhalt von Dateien mit komplexen mathematischen Algorithmen. Die komprimierten Dateien erhalten die Erweiterung `.gz` und müssen

vor einer erneuten Verwendung dekomprimiert werden. Zur Komprimierung mehrerer Dateien oder ganzer Verzeichnisse verwenden Sie besser den Befehl `tar`.

`-d`

Dekomprimiert gzip-Dateien zu ihrer ursprünglichen Größe. Danach können die Dateien wieder normal bearbeitet werden. Der Befehl entspricht etwa dem Befehl `gunzip`.

`tar` Optionen Archiv Dateien

Dieser Befehl stellt eine oder mehrere Dateien mit oder ohne Komprimierung in einer Archivdatei zusammen. `tar` ist mit seinen zahlreichen Optionen ein recht komplexer Befehl. Meist werden die folgenden Optionen verwendet:

`-f`

Schreibt die Ausgabe in eine Datei, nicht wie üblich auf den Bildschirm.

`-c`

Erstellt ein neues tar-Archiv.

`-r`

Fügt die angegebenen Dateien einem vorhandenen Archiv hinzu.

`-t`

Gibt den Inhalt eines Archivs aus.

`-u`

Fügt die angegebenen Dateien nur hinzu, wenn sie noch nicht im Archiv enthalten sind oder aktuelleren Datums sind, als gleichnamige, bereits im Archiv enthaltene Dateien.

`-x`

Entpackt und dekomprimiert die Dateien eines Archivs (*Extraktion*).

`-z`

Komprimiert das entstandene Archiv mit `gzip`.

`-j`

Komprimiert das entstandene Archiv mit `bzip2`.

-v

Listet die verarbeiteten Dateien auf.

Mit `tar` erstellte Archivdateien erhalten die Erweiterung `.tar`. Falls das `tar`-Archiv gleichzeitig mit `gzip` komprimiert wurde, lautet die Erweiterung `.tgz` oder `.tar.gz`. Bei einer Komprimierung mit `bzip2` lautet die Erweiterung `.tar.bz2`.

`locate` Schemata

Dieser Befehl steht nur zur Verfügung, wenn das Paket `findutils-locate` installiert ist. Mit `locate` finden Sie den Speicherort der angegebenen Datei. Zur Angabe des gesuchten Dateinamens können Sie auch verwenden. Das Programm ist sehr schnell, da es die Dateien in einer speziell für diesen Zweck erstellten Datenbank sucht, also nicht das gesamte Dateisystem durchsuchen muss. Hierdurch ergibt sich auch ein wesentlicher Nachteil: `locate` kann keine Dateien finden, die nach der letzten Aktualisierung der Datenbank erstellt wurden. Die Datenbank wird mit `updatedb` aktualisiert. Dazu benötigen Sie allerdings `Root`-Berechtigungen.

`updatedb` [Optionen]

Dieser Befehl führt eine Aktualisierung der von `locate` verwendeten Datenbank aus. Um die Dateien aller vorhandenen Verzeichnisse aufzunehmen, müssen Sie den Befehl als `Root`-Benutzer ausführen. Es empfiehlt sich, den Befehl mit einem Ampersand (&) im Hintergrund auszuführen (`updatedb &`). Sie können dann sofort mit der gleichen Kommandozeile weiterarbeiten. Normalerweise wird dieser Befehl als täglicher `cron`-Auftrag ausgeführt (siehe `cron.daily`).

`find` [Optionen]

Mit diesem Befehl können Sie ein bestimmtes Verzeichnis nach einer Datei durchsuchen. Das erste Argument gibt das Verzeichnis an, in dem die Suche beginnt. Nach der Option `-name` muss der gesuchte Dateiname eingegeben werden (eventuell auch mit Platzhaltern). Im Gegensatz zu `locate`, das eine Datenbank durchsucht, sucht `find` nur im angegebenen Verzeichnis.

Zugriff auf Dateiinhalte

`Datei` [Optionen] [Dateien]

Mit `file` wird der Inhalt der angegebenen Dateien ermittelt.

-Z

Versucht, den Inhalt komprimierter Dateien zu ermitteln.

`cat [Optionen] Dateien`

Dieser Befehl gibt den gesamten Inhalt einer Datei ohne Unterbrechung auf dem Bildschirm aus.

-n

Nummeriert die Ausgabe am linken Rand.

`less [Options] Datei`

Mit diesem Befehl können Sie den Inhalt der angegebenen Datei am Bildschirm durchsuchen. Mit `Bild auf` und `Bild ab` blättern Sie jeweils eine halbe Seite nach oben oder unten, mit der `Leertaste` blättern Sie eine ganze Seite nach unten. Mit `Pos1` bzw. `Ende` gelangen Sie zum Anfang bzw. zum Ende der Datei. Mit `Q` beenden Sie das Programm.

`grep [Optionen] searchstring Dateien`

Mit diesem Befehl können Sie die angegebenen Dateien nach einer bestimmten Suchzeichenfolge durchsuchen. Wird das gesuchte Wort gefunden, dann wird die Zeile, in der sich die Suchzeichenfolge befindet, mit dem Namen der betreffenden Datei angezeigt.

-i

Ignoriert die Groß-/Kleinschreibung.

-H

Zeigt nur die Namen der Dateien an, in der die Suchzeichenfolge gefunden wurde, nicht aber die Textzeilen selbst.

-n

Zeigt zusätzlich die Nummern der Zeilen an, in denen sich die Suchzeichenfolge befindet.

-l

Listet nur die Dateien auf, in denen die Suchzeichenfolge nicht vorkommt.

`diff [Optionen] Datei1 Datei2`

Dieser Befehl vergleicht den Inhalt zweier Dateien. Das Programm gibt alle nicht übereinstimmenden Zeilen aus. Es wird häufig von Programmierern verwendet,

die nur Programmänderungen, nicht aber den gesamten Quellcode verschicken möchten.

-q

Meldet lediglich, ob sich die beiden Dateien unterscheiden.

-u

Fasst die Unterschiede in einer „gemeinsamen“ Diff-Datei zusammen, wodurch die Ausgabe lesbarer wird.

Dateisysteme

`mount [Optionen] [Gerät] Einhängpunkt`

Mit diesem Befehl können Sie jeden Datenträger wie Festplatten, CD-ROM-Laufwerke und andere Laufwerke in ein Verzeichnis des Linux-Dateisystems einhängen. Dies wird gelegentlich auch als "Mounten" bezeichnet.

-r

Hängt das Laufwerk mit Schreibschutz ein.

-t Dateisystem

Geben Sie das Dateisystem an. Die gebräuchlichsten sind `ext2` für Linux-Festplatten, `msdos` für MS-DOS-Medien, `vfat` für das Windows-Dateisystem und `iso9660` für CDs.

Bei Festplatten, die nicht in der Datei `/etc/fstab` deklariert sind, muss auch der Laufwerktyp angegeben werden. In diesem Fall kann das Einhängen nur durch den Root-Benutzer erfolgen. Soll ein Dateisystem auch von anderen Benutzern eingehängt werden, geben Sie in der betreffenden Zeile der Datei `/etc/fstab` die Option `user` ein (getrennt durch Kommata) und speichern Sie diese Änderung. Weitere Informationen zu diesem Befehl finden Sie auf der Manualpage `mount(1)`.

`umount [Optionen] Einhängpunkt`

Mit diesem Befehl hängen Sie ein eingehängtes Laufwerk aus dem Dateisystem aus. Dies wird gelegentlich auch als "Unmounten" bezeichnet. Diesen Befehl sollten Sie nur aufrufen, bevor Sie den Datenträger aus dem Laufwerk entfernen. Andernfalls besteht die Gefahr eines Datenverlustes! Normalerweise können die Befehle `mount` und `umount` nur vom Root-Benutzer ausgeführt werden. Wenn Laufwerke auch von anderen Benutzern ein- und ausgehängt werden sollen, geben

Sie in der Datei `/etc/fstab` für die betreffenden Laufwerke die Option `user` ein.

19.3.2 Systembefehle

Im folgenden Abschnitt werden die wichtigsten Befehle zum Abrufen von Systeminformationen, zur Steuerung von Prozessen und zur Kontrolle von Netzwerken vorgestellt.

Systemangaben

`df [Optionen] [Verzeichnis]`

Ohne Angabe von Optionen zeigt der Befehl `df` (Disk free) Informationen zu dem gesamten, dem belegten und dem verfügbaren Speicherplatz aller eingehängten Laufwerke an. Wenn ein Verzeichnis angegeben ist, werden die Informationen nur für das Laufwerk angezeigt, auf dem sich das Verzeichnis befindet.

`-h`

Zeigt die Anzahl der belegten Blöcke in allgemein lesbarer Form in Giga-, Mega- oder Kilobyte an.

`-T`

Gibt den Dateisystemtyp an (z. B. `ext2` oder `nfs`).

`du [Optionen] [Pfad]`

Ohne Angabe von Parametern zeigt dieser Befehl den Speicherplatz an, der von den Dateien und Unterverzeichnissen des aktuellen Verzeichnisses insgesamt belegt ist.

`-a`

Gibt die Größe jeder einzelnen Datei an.

`-h`

Zeigt die Ausgabe in menschenlesbarer Form an.

`-s`

Zeigt nur die errechnete Gesamtgröße an.

`free [Optionen]`

Dieser Befehl zeigt den gesamten und den belegten Arbeits- und Swap-Speicher an. Weitere Informationen finden Sie unter [Abschnitt 14.1.6, „Der Befehl "free"“](#) (S. 248).

`-b`

Gibt die Werte in Byte an.

`-k`

Gibt die Werte in Kilobyte an.

`-m`

Gibt die Werte in Megabyte an.

`date [Optionen]`

Dieses einfache Programm gibt die aktuelle Systemzeit aus. Als `Root`-Benutzer können Sie die Systemzeit mit diesem Befehl auch ändern. Weitere Informationen zu diesem Befehl finden Sie auf der Manualpage "`date(1)`".

Prozesse

`top [Optionen]`

Dieser Befehl gibt einen schnellen Überblick über die laufenden Prozesse. Mit `H` öffnen Sie eine Seite mit kurzen Erläuterungen zu den wichtigsten Optionen dieses Programms.

`ps [Optionen] [Prozess-ID]`

Wenn keine Optionen angegeben sind, zeigt dieser Befehl die von Ihnen gestarteten Programme und Prozesse in einer Tabelle an. Den Optionen dieses Befehls wird kein Bindestrich vorangestellt.

`aux`

Zeigt eine detaillierte Liste aller Prozesse unabhängig von ihren Eigentümern an.

`kill [Optionen] Prozess-ID`

Gelegentlich lässt sich ein Programm nicht auf die übliche Weise beenden. In den meisten Fällen sollte sich ein solches Programm aber mit dem Befehl `kill` unter Angabe der betreffenden Prozess-ID beenden lassen (die IDs aller laufenden Prozesse ermitteln Sie mit den Befehlen `top` und `ps`). `kill` fordert das Programm

mit einem *TERM*-Signal auf, sich selbst herunterzufahren. Falls sich das Programm auf diese Weise nicht beenden lässt, sollten Sie es mit dem folgenden Parameter versuchen:

-9

Sendet statt des *TERM*-Signals ein *KILL*-Signal, mit dem sich nahezu jeder Prozess beenden lässt.

`killall [Optionen] Prozessname`

Dieser Befehl entspricht dem Befehl `kill`, akzeptiert aber statt der Prozess-ID den Prozessnamen als Argument. Der Befehl beendet alle Prozesse mit dem angegebenen Namen.

Netzwerk

`ping [Optionen] Hostname oder IP-Adresse`

Ping ist ein Standardtool zum Testen der grundsätzlichen Funktionsfähigkeit von TCP/IP-Netzwerken. Der Befehl sendet ein kleines Datenpaket an den Zielhost mit der Aufforderung, dieses sofort zu beantworten. Funktioniert dies, erhalten Sie eine Meldung, die Ihnen bestätigt, dass die Netzwerkverbindung grundsätzlich funktioniert.

-c *Zahl*

Ermittelt die Gesamtzahl der zu sendenden Pakete und endet erst, wenn diese zugestellt sind (standardmäßig ist keine Beschränkung vorgegeben).

-f

flood ping: sendet so viele Pakete wie möglich. Dies ist für `root`-Benutzer eine gängige Methode zum Testen von Netzwerken.

-i *Wert*

Legt das Intervall zwischen zwei Datenpaketen in Sekunden fest (Standard: eine Sekunde).

`nslookup`

Für die Zuordnung von Domännennamen zu IP-Adressen ist das DNS (Domain Name System) zuständig. Mit diesem Befehl können Sie entsprechende Auskünfte von Namensservern (DNS-Servern) anfordern.

`telnet [Optionen] Hostname oder IP-Adresse [Port]`

Im eigentlichen Sinne ist Telnet ein Internet-Protokoll, mit dem Sie über ein Netzwerk auf entfernten Hosts arbeiten können. Der Name wird aber auch von einem Linux-Programm verwendet, das dieses Protokoll für die Arbeit auf entfernten Computern nutzt.

WARNUNG

Verwenden Sie Telnet nicht in einem Netzwerk, das von Dritten „abgehört werden kann.“ Gerade im Internet sollten Sie verschlüsselte Übertragungsmethoden verwenden, beispielsweise `ssh`, um das Risiko des Passwortmissbrauchs zu vermindern (siehe Manualpage zu `ssh`).

Sonstige

`passwd [Optionen] [Benutzername]`

Mit diesem Befehl kann ein Benutzer sein Passwort jederzeit ändern. Der Administrator (Root-Benutzer) kann mit diesem Befehl die Passwörter aller Benutzer des Systems ändern.

`su [Optionen] [Benutzername]`

Mit diesem Befehl können Sie sich innerhalb einer laufenden Sitzung unter einem anderen Benutzernamen anmelden. Geben Sie dazu einen Benutzernamen und das zugehörige Passwort ein. Der Root-Benutzer muss kein Passwort eingeben, da er die Identität jedes Benutzers annehmen darf. Wenn Sie das Kommando ohne Benutzernamen eingeben, werden Sie nach dem Root-Passwort gefragt. Können Sie dieses bereitstellen, werden Sie automatisch zum Root-Benutzer. Mit `su -` öffnen Sie ein Anmeldefenster für einen anderen Benutzer.

`halt [Optionen]`

Um keinen Datenverlust zu riskieren, sollten Sie Ihr System immer mit diesem Programm herunterfahren.

`reboot [Optionen]`

Fährt das System wie mit dem Befehl `halt` herunter, startet es aber unmittelbar danach wieder.

`clear`

Dieser Befehl löscht den Inhalt des sichtbaren Konsolenausschnitts. Er verfügt über keine Optionen.

19.3.3 Weiterführende Informationen

Die Liste der Befehle in diesem Abschnitt ist keineswegs vollständig. Informationen zu weiteren Befehlen und ausführliche Erläuterungen zu den bereits genannten Befehlen finden Sie in der sehr empfehlenswerten Publikation *Linux in a Nutshell* von O'Reilly.

19.4 Der vi-Editor

Texteditoren werden nach wie vor für viele Systemverwaltungsaufgaben und zur Programmierung verwendet. Im Unix-Bereich bietet der Editor vi komfortable Bearbeitungsfunktionen und ist praktischer in der Handhabung als viele Editoren mit Mausunterstützung.

19.4.1 Betriebsmodi

ANMERKUNG: Anzeige der Tasten

Im Folgenden finden Sie mehrere Befehle, die Sie in vi einfach durch das Drücken von Tasten eingeben können. Diese werden in Großbuchstaben angezeigt, wie auf einer Tastatur. Wenn Sie einen Tastenbuchstaben als Großbuchstaben eingeben müssen, wird dies explizit angegeben: Es wird eine Tastenkombination mit der Taste Umschalttaste angezeigt.

vi verwendet drei Betriebsmodi: *Einfügemodus*, *Befehlsmodus* und *erweiterter Modus*. Je nachdem, in welchem Modus Sie arbeiten, haben die Tasten unterschiedliche Funktionen. Beim Systemstart wird vi in der Regel in den *Befehlsmodus* versetzt. Zuerst müssen Sie lernen, wie man zwischen den Modi umschaltet:

Befehlsmodus in Einfügemodus

Hierfür stehen mehrere Möglichkeiten zur Verfügung, darunter A für Anfügen, I für Einfügen oder O für eine neue Zeile unterhalb der aktuellen Zeile.

Einfügemodus in Befehlsmodus

Drücken Sie Esc, um den *Einfügemodus* zu verlassen. vi kann im *Einfügemodus* nicht beendet werden, sodass Sie sich mit der Verwendung der Taste Esc vertraut machen sollten.

Befehlsmodus in erweiterten Modus

Der *erweiterte* Modus von vi kann durch Eingabe eines Doppelpunkts (:) aktiviert werden. Der *erweiterte* oder *ex*-Modus ähnelt einem unabhängigen zeilenorientierten Editor, der für verschiedene einfache und komplexere Aufgaben eingesetzt werden kann.

Erweiterter Modus in Befehlsmodus

Nach der Ausführung eines Befehls im *erweiterten* Modus kehrt der Editor automatisch in den *Befehlsmodus* zurück. Wenn Sie keinen Befehl im *erweiterten* Modus ausführen möchten, löschen Sie den Doppelpunkt mit <— . Der Editor kehrt in den *Befehlsmodus* zurück.

Es ist nicht möglich, direkt vom *Einfügemodus* in den *erweiterten* Modus umzuschalten, ohne vorher in den *Befehlsmodus* gewechselt zu haben.

Wie andere Editoren verfügt auch vi über ein eigenes Verfahren zum Beenden des Programms. vi kann im *Einfügemodus* nicht beendet werden. Verlassen Sie zuerst den *Einfügemodus* mit Esc. Anschließend haben Sie zwei Möglichkeiten:

1. *Verlassen ohne zu speichern*: Um den Editor zu beenden, ohne die Änderungen zu speichern, geben Sie : – Q – ! im *Befehlsmodus* ein. Durch das Ausrufezeichen (!) ignoriert vi alle Änderungen.
2. *Speichern und beenden*: Es gibt mehrere Möglichkeiten, die Änderungen zu speichern und den Editor zu beenden. Verwenden Sie im *Befehlsmodus* Umschalttaste + Z Umschalttaste + Z. Um das Programm zu beenden und alle Änderungen im *erweiterten* Modus zu speichern, geben Sie : – W – Q ein. Im *erweiterten* Modus steht w für Schreiben und q für Beenden.

19.4.2 vi in Aktion

vi kann als normaler Editor verwendet werden. Im *Einfügemodus* können Sie über die Tasten <— und Entf Text eingeben und löschen. Bewegen Sie den Cursor mithilfe der Pfeiltasten.

Diese Steuertasten verursachen jedoch häufig Probleme, da auf vielen Terminaltypen spezielle Tastenkombinationen verwendet werden. An dieser Stelle wird der *Befehlsmodus* relevant. Drücken Sie Esc, um vom *Einfüge-* in den *Befehlsmodus* zu wechseln. Im *Befehlsmodus* verschieben Sie den Cursor mit H, J, K und L. Mit den Tasten werden folgende Funktionen ausgeführt:

- H
Ein Zeichen nach links
- J
Eine Zeile nach unten
- K
Eine Zeile nach oben
- L
Ein Zeichen nach rechts

Die Befehle im *Befehlsmodus* können auf verschiedene Arten variiert werden. Wenn Sie einen Befehl mehrfach ausführen möchten, geben Sie einfach die Anzahl der Wiederholungen ein, bevor Sie den tatsächlichen Befehl eingeben. Geben Sie beispielsweise 5L ein, um den Cursor um fünf Zeichen nach rechts zu verschieben.

Eine Auswahl wichtiger Befehle wird in [Tabelle 19.2, „Einfache Befehle im vi-Editor“](#) (S. 334) aufgeführt. Diese Liste ist nicht vollständig. Umfangreichere Listen finden Sie in der Dokumentation in [Abschnitt 19.4.3, „Weiterführende Informationen“](#) (S. 335)

Tabelle 19.2 *Einfache Befehle im vi-Editor*

Esc	In den Befehlsmodus wechseln
I	In den Einfügemodus wechseln (die Zeichen werden an der aktuellen Cursorposition angezeigt)
A	In den Einfügemodus wechseln (die Zeichen werden hinter der aktuellen Cursorposition angezeigt)
Umschalttaste + A	In den Einfügemodus wechseln (die Zeichen werden am Ende der Zeile hinzugefügt)

Umschalttaste + R	In den Ersetzungsmodus wechseln (alter Text wird überschrieben)
R	Das Zeichen unter dem Cursor ersetzen
O	In den Einfügemodus wechseln (unterhalb der aktuellen Zeile wird eine neue Zeile eingefügt)
Umschalttaste + O	In den Einfügemodus wechseln (oberhalb der aktuellen Zeile wird eine neue Zeile eingefügt)
X	Aktuelles Zeichen löschen
D – D	Aktuelle Zeile löschen
D – W	Zeichen bis zum Ende des aktuellen Worts löschen
C – W	In den Einfügemodus wechseln (der Rest des aktuellen Worts wird mit den nächsten Einträgen überschrieben)
U	Letzten Befehl rückgängig machen
Strg + F	Rückgängig gemachte Änderung erneut ausführen
Umschalttaste + J	Folgende Zeile an die aktuelle Zeile anfügen
.	Letzten Befehl wiederholen

19.4.3 Weiterführende Informationen

vi unterstützt viele verschiedene Befehle. Es ermöglicht die Verwendung von Makros, Schnellverfahren, benannten Puffern und viele andere nützliche Funktionen. Eine detaillierte Beschreibung der verschiedenen Optionen ist nicht Bestandteil dieses Handbuchs. Im Lieferumfang von openSUSE ist vim (vi improved) enthalten, eine verbesserte Version von vi. Für diese Anwendungen stehen zahlreiche Informationsquellen zur Verfügung:

- vimtutor ist ein interaktives Tutorial für vim.

- Hilfe zu vielen Themen erhalten Sie, indem Sie in vim den Befehl `:help` eingeben.
- Ein Buch über vim ist online unter <http://www.truth.sk/vim/vimbook-OPL.pdf> verfügbar.
- Die Webseiten des vim-Projekts unter <http://www.vim.org> enthalten verschiedene Arten von Nachrichten, Mailinglisten und sonstiger Dokumentation.
- Im Internet stehen zahlreiche Informationsquellen zu vim zur Verfügung: <http://www.selflinux.org/selflinux/html/vim.html> und http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html. Links zu weiteren Tutorials finden Sie unter <http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html>.

WICHTIG: VIM-Lizenz

Bei vim handelt es sich um „Charityware“. Dies bedeutet, dass die Autoren keine Gebühren für die Software erheben, sondern Sie auffordern, ein gemeinnütziges Projekt mit einem finanziellen Beitrag zu unterstützen. Bei diesem Projekt wird um Hilfe für Kinder in Uganda gebeten. Weitere Informationen hierzu erhalten Sie online unter <http://iccf-holland.org/index.html>, <http://www.vim.org/iccf/> und <http://www.iccf.nl/>.

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 20.1, „Verschiedene Protokolle aus der TCP/IP-Familie“** (S. 340) 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.

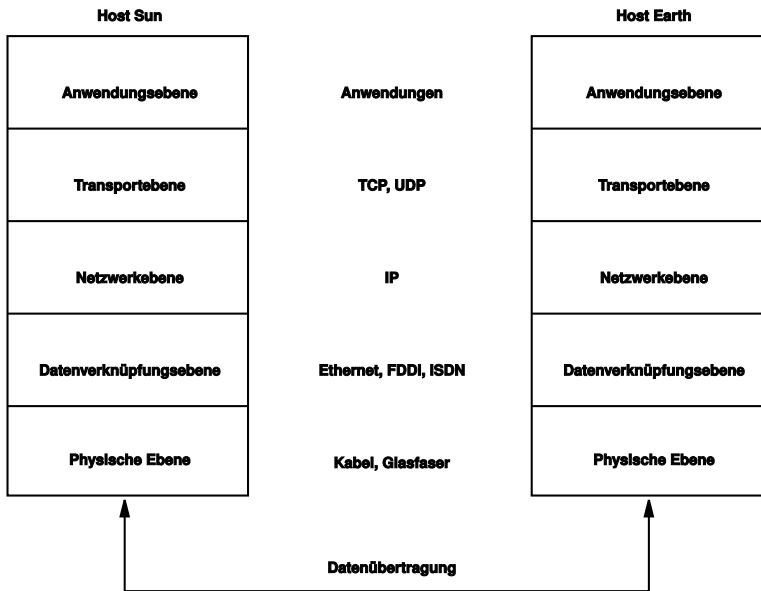
RFC steht für *Request for Comments*. RFCs sind Dokumente, die unterschiedliche Internetprotokolle und Implementierungsverfahren für das Betriebssystem und seine Anwendungen beschreiben. Die RFC-Dokumente beschreiben das Einrichten der Internetprotokolle. Weitere Informationen zu diesen Protokollen finden Sie in den entsprechenden RFC-Dokumenten. Diese sind online unter <http://www.ietf.org/rfc.html> verfügbar.

Tabelle 20.1 *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 20.1, „Vereinfachtes Schichtmodell für TCP/IP“** (S. 341) 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 20.1 Vereinfachtes Schichtmodell für TCP/IP



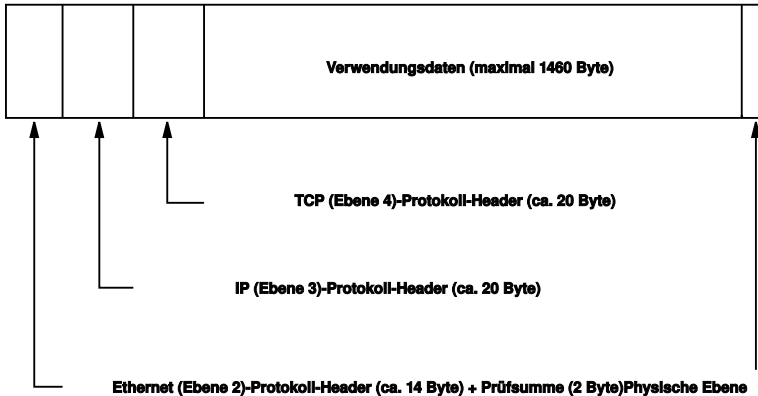
Dieses Diagramm bietet für jede Schicht ein oder zwei Beispiele. Die Schichten sind nach *Abstraktionsstufen* sortiert. Die unterste Schicht ist sehr Hardware-nah. Die oberste Schicht ist beinahe vollständig von der Hardware losgelöst. Jede Schicht hat ihre eigene spezielle Funktion. Die speziellen Funktionen 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 20.2, „TCP/IP-Ethernet-Paket“** (S. 342) dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

Abbildung 20.2 *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.

20.1 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 20.2, „IPv6 – Das Internet der nächsten Generation“** (S. 345).

20.1.1 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 20.1**, „IP-Adressen schreiben“ (S. 343) dargestellt geschrieben.

Beispiel 20.1 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.

20.1.2 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 20.2**, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 344). 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 20.2, „Verknüpfung von IP-Adressen mit der Netzmaske“** (S. 344) könnte das erste Netz mit 24 Bit auch als 192.168.0.0/24 geschrieben werden.

Beispiel 20.2 *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 20.2 *Spezifische Adressen*

Adresstyp	Beschreibung
Netzwerkbasis- adresse	Dies ist die Netzmaske, die durch UND mit einer Netzwerkadresse verknüpft ist, wie in Beispiel 20.2, „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 344) 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 20.3, „Private IP-Adressdomänen“** (S. 345) aufgelistet.

Tabelle 20.3 *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

20.2 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 der 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.

20.2.1 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 Milliarden 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 20.2.2, „Adresstypen und -struktur“** (S. 348).

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 20.2.3, „Koexistenz von IPv4 und IPv6“** (S. 353). 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.

20.2.2 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 zweithöchsten 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 20.3**, „Beispiel einer IPv6-Adresse“ (S. 349) dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

Beispiel 20.3 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 20.4**, „IPv6-Adressen mit Angabe der Präfix-Länge“ (S. 349) 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 20.4 IPv6-Adressen mit Angabe der Präfix-Länge

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige von diesen sind in **Tabelle 20.4**, „**Unterschiedliche IPv6-Präfixe**“ (S. 350) aufgeführt.

Tabelle 20.4 *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 20.2.3, „Koexistenz von IPv4 und IPv6“** (S. 353)). 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 Netzwerkarte 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.

20.2.3 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 20.2.2, „Adresstypen und -struktur“](#) (S. 348)) 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.

20.2.4 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 Abschnitt „Netzwerk“ (Kapitel 1, *Installation mit YaST*, ↑Start)). Zur Deaktivierung oder Aktivierung von IPv6 auf einem installierten System starten Sie YaST, öffnen Sie das Dialogfeld *Netzwerkgeräte > Netzwerkkarte*, klicken Sie auf den Karteireiter *Globale Optionen* und aktivieren bzw. deaktivieren Sie dort *IPv6 aktivieren*. 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* automatisch konfigurieren.

Weitere Informationen zum Einrichten der unterschiedlichen Tunneltypen mithilfe der Dateien im Verzeichnis `/etc/sysconfig/network` finden Sie auf der Manualpage "ifup(8)".

20.2.5 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).

20.3 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 **Kapitel 22, Domain Name System (DNS)** (S. 399) beschrieben.

Eng verwandt mit DNS ist das Protokoll `whois`. Mit dem gleichnamigen Programm `whois` können Sie schnell ermitteln, wer für eine bestimmte Domäne verantwortlich ist.

20.4 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 20.5, „Manuelle Netzwerkkonfiguration“](#) (S. 376).

Während der Installation können sämtliche erkannte Schnittstellen mit YaST automatisch konfiguriert werden. Zusätzliche Hardware kann nach Abschluss der Installation jederzeit konfiguriert werden. In den folgenden Abschnitten wird die Netzwerkkonfiguration für alle von openSUSE unterstützten Netzwerkverbindungen beschrieben.

20.4.1 Konfigurieren der Netzwerkkarte mit YaST

Zur Konfiguration verkabelter oder drahtloser Netzwerkkarten in YaST wählen Sie *Netzwerkgeräte > Netzwerkkarte*. Nach dem Öffnen des Moduls zeigt YaST das Dialogfeld "Netzwerkeinstellungen" mit den vier Karteireitern *Globale Optionen*, *Übersicht*, *Hostname/DNS* und *Routing* an.

Der Karteireiter *Übersicht* enthält Informationen zu den installierten Netzwerkkarten. Jede korrekt erkannte Netzwerkkarte wird dort mit ihrem Namen aufgelistet. In diesem Dialogfeld können Sie Karten manuell hinzufügen, entfernen oder ihre Konfiguration ändern. Informationen zum manuellen Hinzufügen und Konfigurieren von Karten, die nicht automatisch erkannt wurden, finden Sie unter [„Konfigurieren einer unerkannten Netzwerkkarte“](#) (S. 365).

Auf dem Karteireiter *Globale Optionen* können Sie wichtige globale Netzwerkoptionen einstellen. 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) verwenden

oder mehrere Schnittstellen sofort benötigen, empfiehlt sich die *Traditionelle Methode mit ifup*. Weitere Informationen zu NetworkManager finden Sie unter Kapitel 10, *Verwalten der Netzwerkverbindungen mit NetworkManager* (↑Start).

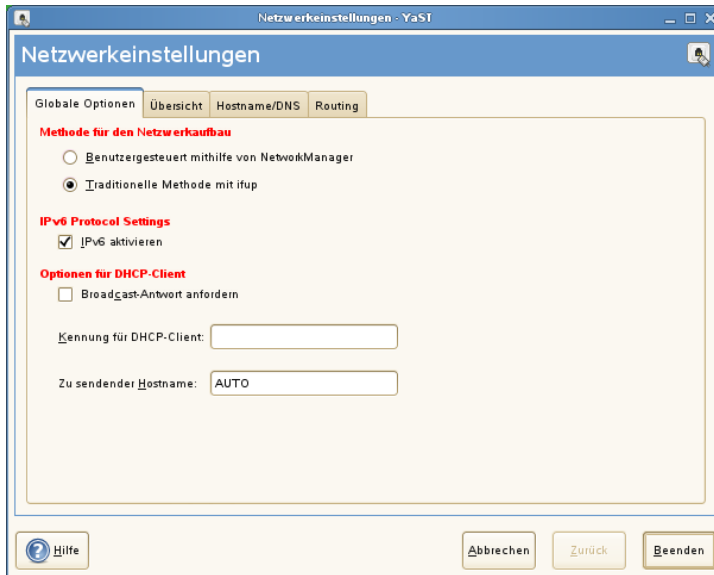
Geben Sie unter *IPv6 Protocol Settings* (IPv6-Protokolleinstellungen) an, ob Sie das IPv6-Protokoll verwenden möchten. IPv6 kann parallel zu IPv4 verwendet werden. IPv6 ist standardmäßig aktiviert. In Netzwerken, die das IPv6-Protokoll nicht verwenden, können die Antwortzeiten jedoch schneller sein, 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.

Abbildung 20.3 Konfigurieren der Netzwerkeinstellungen



Auf dem Karteireiter *Hostname/DNS* können der Hostname des Computers sowie die zu verwendenden Namensserver festgelegt werden. Weitere Informationen zu diesen Optionen finden Sie unter „**Konfigurieren des Hostnamens und DNS**“ (S. 361). Auf dem Karteireiter *Routing* legen Sie das Standard-Gateway und die Routing-Einstellungen fest. Weitere Informationen finden Sie unter „**Konfigurieren des Routing**“ (S. 362).

Ändern der Konfiguration einer Netzwerkkarte

Wenn Sie die Konfiguration einer Netzwerkkarte ändern möchten, wählen Sie die Karte im YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* aus der Liste der erkannten Karten aus und klicken Sie auf *Konfigurieren*. 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 33.1.3, „Konfiguration mit YaST“** (S. 622).

IP-Adressen konfigurieren

Wenn möglich, werden die während der Installation erkannten, verkabelten Netzwerkkarten automatisch für die automatische Adresseneinrichtung DHCP 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 *Konfigurieren*.
- 2 Wählen Sie auf dem Karteireiter *Adresse* die Option *Statically assigned IP address* (Statisch zugewiesene IP-Adresse) aus.
- 3 Geben Sie die *IP-Adresse* und die *Subnetzmaske* ein.
- 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. 361). Informationen zur Konfiguration eines Gateways finden Sie unter „**Konfigurieren des Routing**“ (S. 362).

Konfigurieren von Aliassen

Ein Netzwerkgerät kann mehrere IP-Adressen haben, die Aliasse genannt werden. 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 *Konfigurieren*.
- 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.

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.
- 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 für Netzwerkkarten.
- 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 Wenn Sie der *Routing-Tabelle* weitere Einträge hinzufügen möchten, aktivieren Sie die Option *Konfiguration für Experten*. Fügen Sie danach den gewünschten Eintrag mit *Hinzufügen* hinzu. Geben Sie das *Ziel* und die *Netzmaske* ein und wählen Sie optional das zu verwendende *Gerät*.
- 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.

Ändern der Hardware-Optionen

Bei Bedarf können Sie den Gerätenamen der Netzwerkkarte während des laufenden Betriebs ändern. Genauso können Sie auch den Treiber wechseln. Mit YaST legen Sie diese Optionen wie folgt fest:

- 1 Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Konfigurieren*.
- 2 Öffnen Sie den Karteireiter *Hardware*. Die *Matching rule* (Übereinstimmungsregel) unter *Udev rules* (Udev-Regeln) kann nicht bearbeitet werden. Udev nutzt zur Identifizierung der Netzwerkkarte die Hardware-Adresse (MAC) oder die Bus-ID. Allerdings können Sie den Gerätenamen der Karte unter *Gerätename* ändern.
- 3 Unter *Treibername* können Sie den Treiber festlegen, der für die Netzwerkkarte verwendet werden soll.
- 4 Klicken Sie auf *Weiter*.
- 5 Um die Konfiguration zu aktivieren, klicken Sie auf *Verlassen*.

Starten des Geräts

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 aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Konfigurieren*.
- 2 In der Registerkarte *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. Wählen Sie *Manuell*, wenn Sie die Schnittstelle manuell mit `ifup` steuern möchten. 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.

Konfigurieren der Firewall

Sie müssen nicht die genaue Firewall-Konfiguration durchführen, wie unter [Abschnitt 35.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 660) 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 aus der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Konfigurieren*.
- 2 Öffnen Sie die Registerkarte *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

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.

Interne Zone (ungeschützt)

Die Firewall wird ausgeführt, aber es gibt keine Regeln, die diese Schnittstelle schützen. Verwenden Sie diese Option nur, wenn Ihre Maschine Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird.

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*. Wählen Sie andernfalls über die Option *Auswahl aus Liste* das Modell Ihrer Netzwerkkarte aus. YaST wählt dann automatisch das geeignete Kernelmodul für die Karte aus. Falls Ihre Karte nicht in der Liste aufgeführt ist, wählen Sie den *Namen des Moduls* manuell aus.

3 Klicken Sie auf *Weiter*.

4 In der Registerkarte *Adresse* legen Sie den Gerätetyp der Schnittstelle, den Konfigurationsnamen und die IP-Adresse fest. Wenn Sie eine statische Adresse verwenden möchten, wählen Sie *Statically assigned IP Address* (Statisch zugewiesene IP-Adresse). Geben Sie dann die *IP-Adresse* und *Subnetzmaske* ein. Hier können Sie auch den Hostnamen und zusätzliche Schnittstellenadressen einrichten (siehe „**Konfigurieren von Aliassen**“ (S. 361)).

Wenn Sie für den Gerätetyp der Schnittstelle die Option *Drahtlos* gewählt haben, konfigurieren Sie im nächsten Dialogfeld die drahtlose Verbindung. Weitere Informationen zur Konfiguration drahtloser Geräte erhalten Sie unter **Abschnitt 33.1, „Wireless LAN“** (S. 617).

5 Legen Sie auf dem Karteireiter *Allgemein* die *Firewall-Zone* und die *Geräte-Aktivierung* fest. Mit *Enable Device Control for Non-root User via KInternet* (Gerätesteuerung für Nicht-Root-Benutzer via KInternet ermöglichen) erlauben Sie auch normalen Benutzern die Kontrolle über die Verbindung.

6 Klicken Sie auf *Weiter*.

7 Klicken Sie auf *Verlassen*, um die neue Netzwerkkonfiguration zu aktivieren.

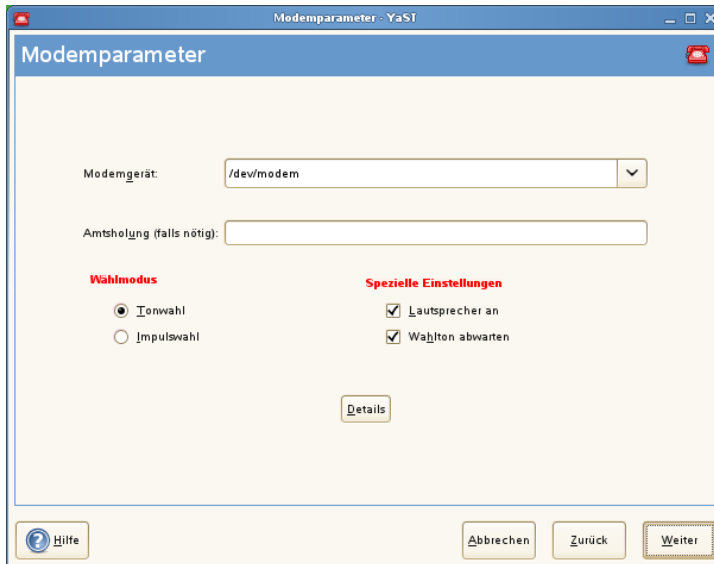
20.4.2 Modem

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 20.4 *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-Terminaladaptoren 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 Einwahl-servers. Aktivieren Sie diese Option, wenn der Verbindungsaufbau sehr lange dauert oder die Verbindung nicht zustande kommt.

Externe Firewall-Schnittstelle

Durch Auswahl dieser Option wird SUSEfirewall2 aktiviert und die Schnittstelle als extern eingestellt. 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

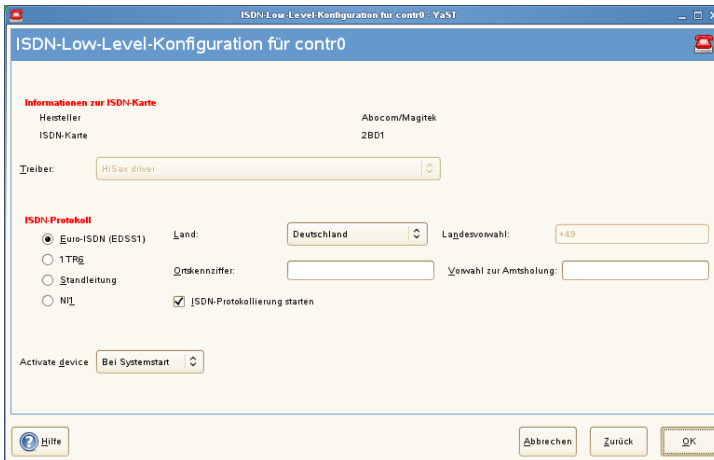
Diese Option öffnet das Dialogfeld für die Adresskonfiguration. Wenn Ihr ISP Ihrem Host keine dynamische IP-Adresse zuweist, deaktivieren Sie die Option *Dynamische IP-Adresse* und geben Sie die lokale IP-Adresse des Hosts und anschließend die entfernte IP-Adresse ein. Diese Informationen erhalten Sie 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*.

20.4.3 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 20.5 ISDN-Konfiguration

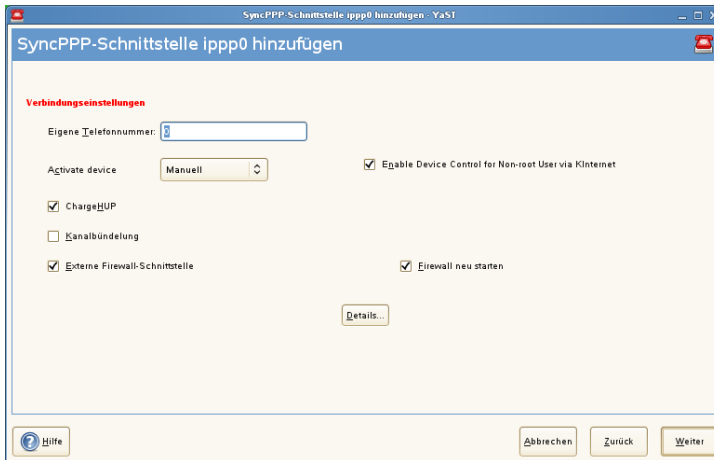


Wählen Sie im nächsten Dialogfeld, das in **Abbildung 20.5**, „ISDN-Konfiguration“ (S. 370) dargestellt ist, das zu verwendende Protokoll. Der Standard ist *Euro-ISDN (EDSS1)*, aber für ältere oder größere Telefonanlagen wählen Sie *1TR6*. Für die USA gilt *N11*. Wählen Sie das Land in dem dafür vorgesehenen Feld aus. Die entsprechende Landeskennung wird im Feld daneben angezeigt. Geben Sie dann noch die *Ortsnetz-kennzahl* und ggf. die *Vorwahl zur Amtsholung* ein.

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 Einstellungen 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 verwenden jedoch den `SyncPPP`-Modus, der im Folgenden beschrieben wird.

Abbildung 20.6 Konfiguration der ISDN-Schnittstelle



Die Nummer, die Sie unter *Eigene Telefonnummer* eingeben, ist vom jeweiligen Anschlussszenario 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 SuSEfirewall2 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*.

20.4.4 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.

20.4.5 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

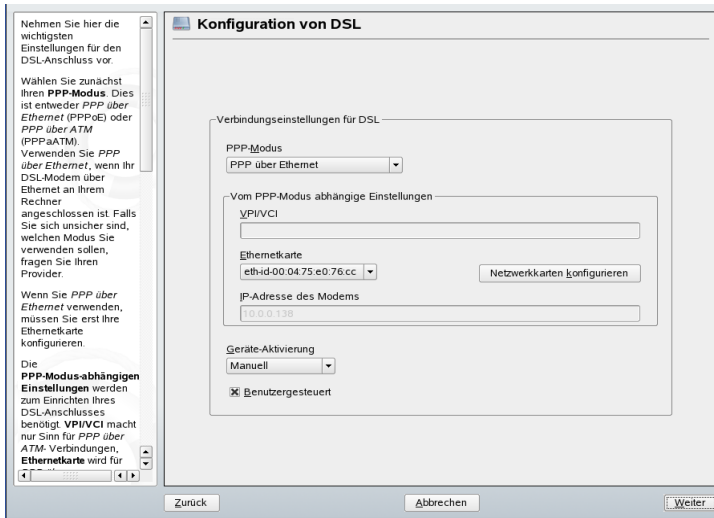
Im Dialogfeld *DSL-Konfiguration* finden Sie auf dem Karteireiter *DSL-Geräte* eine Liste der installierten DSL-Geräte. Zur Änderung der Konfiguration eines DSL-Geräts wählen Sie das Gerät in der Liste aus und klicken Sie auf *Bearbeiten*. Wenn Sie ein neues DSL-Gerät manuell konfigurieren möchten, klicken 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 20.4.1, „Konfigurieren der Netzwerkkarte mit YaST“** (S. 357)). 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.

Abbildung 20.7 DSL-Konfiguration



Wählen Sie im ersten Dialogfeld für die DSL-Konfiguration (siehe [Abbildung 20.7](#), „DSL-Konfiguration“ (S. 375)) 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* (Gerätestuerung 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.

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.

20.5 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 entfernen, 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 20.5, „Skripten für die manuelle Netzwerkkonfiguration“ (S. 377) zeigt die wichtigsten an der Netzwerkkonfiguration beteiligten Skripten.

Tabelle 20.5 *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 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.

Weitere Informationen zu udev und persistenten Gerätenamen finden Sie in **Kapitel 15, *Gerätemanagemet über dynamischen Kernel mithilfe von udev*** (S. 257).

20.5.1 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 angegeben 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 Namensservers, 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 Namensserver verwenden, geben Sie mehrere Zeilen ein, wobei jede Zeile mit `nameserver` beginnt. Stellen Sie Kommentaren ein `#`-Zeichen voran. YaST trägt den angegebenen Namensserver in diese Datei ein. **Beispiel 20.5**, „`/etc/resolv.conf`“ (S. 380) zeigt, wie `/etc/resolv.conf` aussehen könnte.

Beispiel 20.5 */etc/resolv.conf*

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

Einige Dienste, zum Beispiel `pppd` (`wvdial`), `ipppd` (`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 20.6**, „/etc/hosts“ (S. 381) 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 20.6 /etc/hosts

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.1 earth.example.com earth
```

/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 20.7**, „/etc/networks“ (S. 381).

Beispiel 20.7 /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 20.6**, „Parameter für

`/etc/host.conf`“ (S. 382) aufgeführt. Ein Beispiel für `/etc/host.conf` wird in **Beispiel 20.8**, „`/etc/host.conf`“ (S. 382) gezeigt.

Tabelle 20.6 *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 20.8 *`/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 20.9**, „`/etc/nsswitch.conf`“ (S. 383) dargestellt. Kommentare werden durch ein `#`-Zeichen eingeleitet. Der Eintrag unter der `hosts`-Datenbank bedeutet, dass Anfragen über DNS an `/etc/hosts(files)` gehen.

Beispiel 20.9 `/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 20.7**, „Über `/etc/nsswitch.conf` verfügbare Datenbanken“ (S. 383) aufgelistet. Zusätzlich sind in Zukunft zudem `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten. Die Konfigurationsoptionen für NSS-Datenbanken sind in **Tabelle 20.8**, „Konfigurationsoptionen für NSS-„Datenbanken““ (S. 384) aufgelistet.

Tabelle 20.7 Über `/etc/nsswitch.conf` verfügbare Datenbanken

<code>aliases</code>	Mail-Aliasze, 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> .
hosts	Für Hostnamen und IP-Adressen, die von <code>gethostbyname</code> und ähnlichen Funktionen verwendet werden.
netgroup	Im Netzwerk gültige Host- und Benutzerlisten zum Steuern von Zugriffsrechten. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>netgroup(5)</code> .
networks	Netzwerknamen und -adressen, die von <code>getnetent</code> verwendet werden.
passwd	Benutzerpasswörter, die von <code>getpwent</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage <code>passwd(5)</code> .
protocols	Netzwerkprotokolle, die von <code>getprotoent</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>protocols(5)</code> .
rpc	Remote Procedure Call-Namen und -Adressen, die von <code>getrpcbyname</code> und ähnlichen Funktionen verwendet werden.
services	Netzwerkdienste, die von <code>getservent</code> verwendet werden.
shadow	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 20.8 *Konfigurationsoptionen für NSS-„Datenbanken“*

Dateien	Direkter Dateizugriff, z. B. <code>/etc/aliases</code>
db	Zugriff über eine Datenbank
nis, nisplus	NIS, siehe auch Kapitel 25, Arbeiten mit NIS (S. 451)

<code>dns</code>	Nur bei <code>hosts</code> und <code>networks</code> als Erweiterung verwendbar
<code>compat</code>	Nur bei <code>passwd</code> , <code>shadow</code> und <code>group</code> 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 Domänennamen. Diese Datei wird von verschiedenen Skripten beim Booten des Computers gelesen. Sie darf nur eine Zeile enthalten, in der der Hostname steht.

20.5.2 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 bestätigt, dass die Netzwerkverbindung grundsätzlich funktioniert.

`ping` testet nicht nur die Funktion der Verbindung zwischen zwei Computern, es bietet darüber hinaus grundlegende Informationen zur Qualität der Verbindung. In **Beispiel 20.10**, „Ausgabe des `ping`-Befehls“ (S. 388) 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, zum Beispiel `ping venus.example.com` oder `ping 192.168.2.101`. 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 Sie die Anzahl beispielsweise auf drei Pakete beschränken möchten, geben Sie `ping -c 3 192.168.2.101` ein.

Beispiel 20.10 *Ausgabe des ping-Befehls*

```
ping -c 3 venus.example.com
PING venus.example.com (192.168.2.101) 56(84) bytes of data.
64 bytes from venus.example.com (192.168.2.101): icmp_seq=1 ttl=49 time=188
ms
64 bytes from venus.example.com (192.168.2.101): icmp_seq=2 ttl=49 time=184
ms
64 bytes from venus.example.com (192.168.2.101): icmp_seq=3 ttl=49 time=183
ms
--- venus.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 Sie beispielsweise das Ping-Intervall auf zehn Sekunden erhöhen möchten, geben Sie `ping -i 10 192.168.2.101` 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, zum Beispiel `ping -I wlan1 192.168.2.101`.

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 20.11**, „Ausgabe des `ifconfig`-Befehls“ (S. 389) 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 20.11 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 20.12 *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.

20.5.3 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 20.9, „Einige Start-Skripten für Netzwerkprogramme“](#) (S. 391) beschrieben.

Tabelle 20.9 *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 xinetd. Mit xinetd können Sie Serverdienste auf dem System verfügbar machen. Beispielsweise kann er vsftpd 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.

20.6 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 ippd 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 Einwahlverbindung über ein KDE-Applet oder eine Kommandozeilen-Schnittstelle steuern. Wenn das Internet-Gateway nicht der eigentliche Arbeitscomputer ist, besteht die Möglichkeit, die Einwahlverbindung 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 `ipppd` 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.

20.6.1 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)`.

20.6.2 Konfigurieren von KInternet, cinternet und qinternet für die Fernsteuerung

Mit den Programmen KInternet, cinternet und qinternet kann sowohl ein lokaler als auch ein entfernter smpppd-Dienst gesteuert werden. cinternet ist die Kommandozeilenvariante von KInternet, das eine grafische Oberfläche bietet. qinternet ist im Grunde das Gleiche wie KInternet, verwendet aber nicht die KDE-Bibliotheken, sodass es ohne KDE verwendet werden kann und separat installiert werden muss. 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 drei 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 `local` weist den Verbindungsaufbau dem lokalen smpppd-Dienst zu und `gateway` verweist auf einen smpppd-Dienst auf dem Gateway. Die Verbindung wird nach den in der Datei `config-file` unter `server` spezifizierten Einstellungen hergestellt. `slp` weist die Frontends an, sich mit einem per SLP gefundenen smpppd-Dienst zu verbinden.

`server = Server`

Geben Sie hier den Host an, auf dem smpppd läuft.

`password = Passwort`

Geben Sie das Passwort für smpppd ein.

Wenn smpppd aktiv ist, können Sie jetzt versuchen, darauf zuzugreifen, z. B. mit dem Befehl `cinternet--verbose --interface-list`. Sollten Sie an dieser Stelle Schwierigkeiten haben, finden Sie weitere Informationen in den man-Seiten zu `smpppd-c.conf(5)` und `cinternet(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).

21.1 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.

21.2 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.

21.3 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.

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.

21.4 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 Installationsservers 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.

21.5 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 sane 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 Gültigkeitsdauer 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`.

21.6 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)

22

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 20.3](#), „Namensauflösung“ (S. 355) lesen. Die folgenden Konfigurationsbeispiele beziehen sich auf BIND.

22.1 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 Namensserver 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.

22.2 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.

22.3 Konfiguration mit YaST

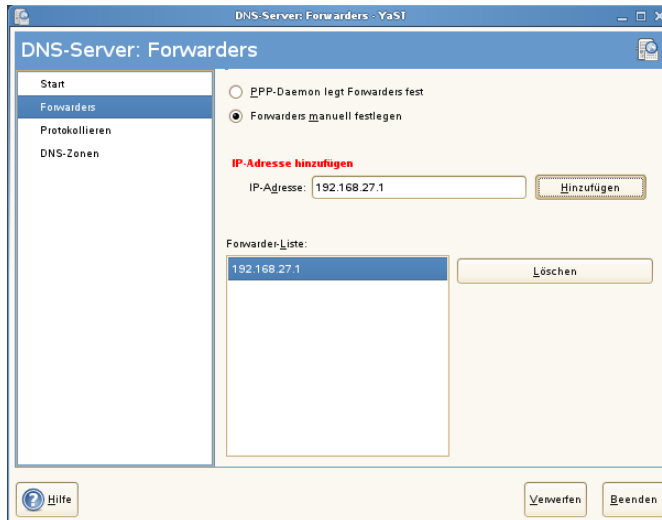
Mit dem DNS-Modul von YaST können Sie einen DNS-Server für Ihr lokales Netzwerk konfigurieren. Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Nach Abschluss der anfänglichen Konfiguration ist eine grundlegende Serverkonfiguration verfügbar, die für einfache Szenarien ausreichend ist. Komplexere Konfigurationsaufgaben können im Expertenmodus ausgeführt werden.

22.3.1 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.

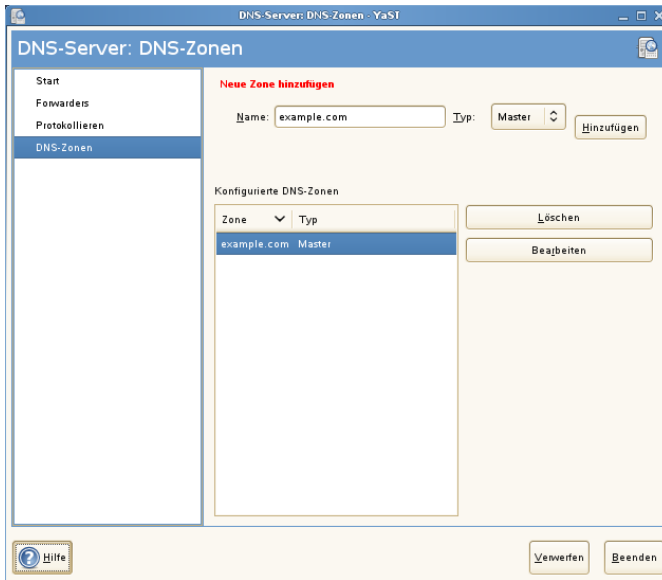
- 1 Wenn Sie das Modul zum ersten Mal starten, wird das Dialogfeld *Forwarder-Einstellungen* (siehe **Abbildung 22.1**, „DNS-Server-Installation: Forwarder-Einstellungen“ (S. 402)) geöffnet. Legen Sie hier fest, ob der PPP-Daemon eine Liste von Forwarders bei der Einwahl über DSL oder ISDN eine Liste von Forwarders bereitstellen soll (*PPP-Daemon legt Forwarders fest*) oder ob Sie Ihre eigene Liste angeben möchten (*Forwarders manuell festlegen*).

Abbildung 22.1 DNS-Server-Installation: Forwarder-Einstellungen



- 2 Das Dialogfeld *DNS-Zonen* besteht aus mehreren Teilen und ist für die Verwaltung von Zonendateien zuständig, wie in [Abschnitt 22.6, „Zonendateien“](#) (S. 415) 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 22.2, „DNS-Server-Installation: DNS-Zonen“](#) (S. 403). Klicken Sie auf *Zone bearbeiten*, um andere Einstellungen für eine bestehende Zone zu konfigurieren. Zum Entfernen einer Zone klicken Sie auf *Zone löschen*.

Abbildung 22.2 DNS-Server-Installation: DNS-Zonen



- 3** Im abschließenden Dialogfeld können Sie die Ports für den DNS-Dienst in der Firewall öffnen, die während der Installation aktiviert wird, und angeben, ob DNS gestartet werden soll. Die Expertenkonfiguration lässt sich ebenfalls über dieses Dialogfeld aufrufen. Weitere Informationen hierzu finden Sie unter [Abbildung 22.3, „DNS-Server-Installation: Assistent beenden“](#) (S. 404).

Abbildung 22.3 *DNS-Server-Installation: Assistent beenden*



22.3.2 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

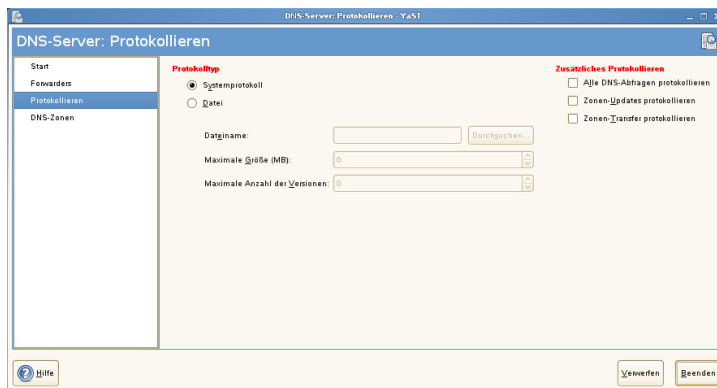
Legen Sie unter *Service starten* fest, ob der DNS-Server beim Booten des Systems oder manuell gestartet werden soll. Um den DNS-Server sofort zu starten, wählen Sie *DNS-Server nun starten*. Um den DNS-Server anzuhalten, wählen Sie *DNS-Server nun anhalten*. Zum Speichern der aktuellen Einstellungen 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.

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 22.4, „DNS-Server: Protokollieren“** (S. 405).

Abbildung 22.4 DNS-Server: Protokollieren

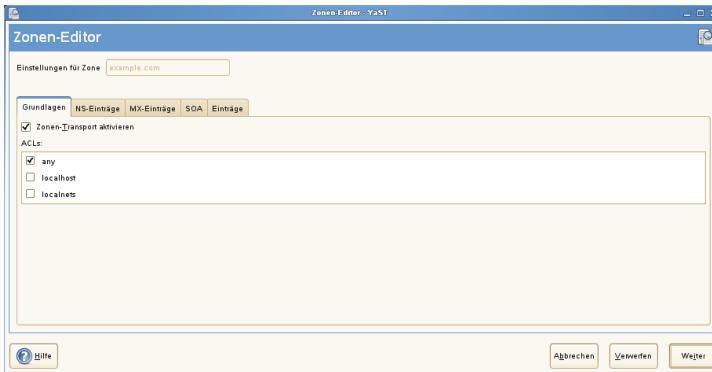


Hinzufügen einer Slave-Zone

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 22.5**, „DNS-Server: Slave-Zonen-Editor“ (S. 406).

Abbildung 22.5 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*.

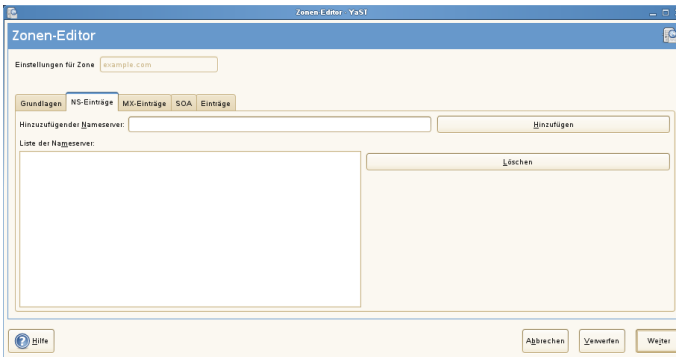
Bearbeiten einer Masterzone

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 22.6**, „DNS-Server: Zonen-Editor (DNS-Einträge)“ (S. 407).

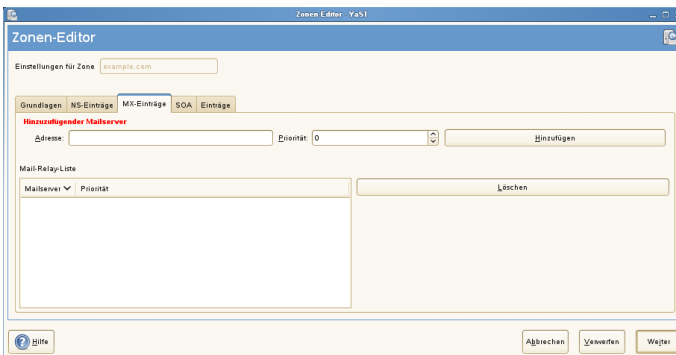
Abbildung 22.6 DNS-Server: Zonen-Editor (DNS-Einträge)



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 22.7, „DNS-Server: Zonen-Editor \(MX-Einträge\)“](#) (S. 407).

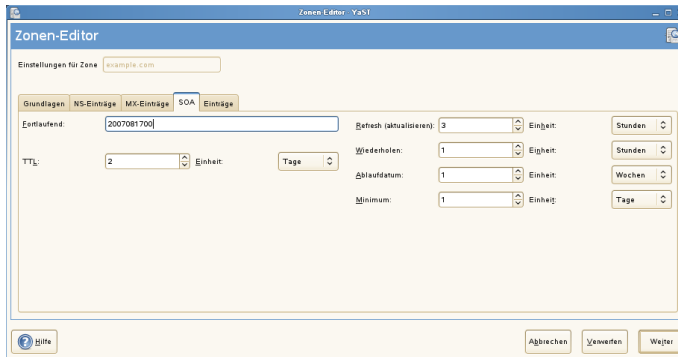
Abbildung 22.7 DNS-Server: Zonen-Editor (MX-Einträge)



Zonen-Editor (SOA)

Auf dieser Seite können Sie SOA (Start of Authority)-Einträge erstellen. Eine Erklärung der einzelnen Optionen finden Sie in [Beispiel 22.6, „Datei /var/lib/named/example.com.zone“](#) (S. 416).

Abbildung 22.8 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.

22.4 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 Namensserveradresse 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 Namensserver als reiner *Nur-Cache*-Namensserver 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 `rcnamedstart` als `root` ein. Falls rechts in grüner Schrift „done“ angezeigt wird, wurde `named`, wie der Namenserverprozess hier genannt wird, erfolgreich gestartet. Testen Sie den Namensserver 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 `rcnamed status`, ob der Server tatsächlich ausgeführt wird. Wenn der Namensserver sich nicht starten lässt oder unerwartetes Verhalten zeigt, finden Sie die Ursache normalerweise in der Protokolldatei `/var/log/messages`.

Um den Namensserver 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 22.1**, „Weiterleitungsoptionen in `named.conf`“ (S. 410) handelt es sich lediglich um Beispiele. Passen Sie diese Einträge an Ihr eigenes Setup an.

Beispiel 22.1 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.

22.5 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 22.2, „Eine Grundversion von `/etc/named.conf`“** (S. 411).

Beispiel 22.2 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";
};
```

22.5.1 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 Namensserver (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 *10.0.0.1*.

`forward first;`

Führt dazu, dass DNS-Anforderungen weitergeleitet werden, bevor versucht wird, sie über die Root-Namensserver aufzulösen. Anstatt `forward first` kann `forward only` verwendet werden. Damit werden alle Anforderungen weitergeleitet, ohne dass sie an die Root-Namensserver 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 192.168/16. Der Wert /16 am Ende ist ein abgekürzter Ausdruck für die Netzmaske, hier 255.255.0.0.

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 aus 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 Namensserver informiert werden, wenn Änderungen an den Zonendaten vorgenommen werden oder wenn der Namensserver neu gestartet wird.

22.5.2 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 22.3, „Eintrag zur Deaktivierung der Protokollierung“](#) (S. 413) sehen Sie die einfachste Form eines solchen Eintrags, bei dem jegliche Protokollierung unterdrückt wird.

Beispiel 22.3 *Eintrag zur Deaktivierung der Protokollierung*

```
logging {  
    category default { null; };  
};
```

22.5.3 Zoneneinträge

Beispiel 22.4 *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 22.4, „Zoneneintrag für "example.com"“](#) (S. 413) gezeigt. Um eine *Slave-Zone* zu definieren, ändern Sie den Wert von `type` in `slave` und geben Sie einen

Namensserver an, der diese Zone als `master` verwaltet (dieser kann wiederum ein Slave eines anderen Masters sein), wie in **Beispiel 22.5**, „Zoneneintrag für `example.net`“ (S. 414) gezeigt.

Beispiel 22.5 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.

22.6 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 22.6](#), „Datei `/var/lib/named/example.com.zone`“ (S. 416)).

Beispiel 22.6 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
```

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 Namensserver (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 Namensserver 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 Namensserver 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 Namensserver 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 Namensserver. Wenn `notify` in `/etc/named.conf` nicht auf `no` gesetzt ist, werden alle hier aufgeführten Namensserver 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 allen traditionellen Hostadressen (IPv4) wird der Eintrag mit `AAAA` gekennzeichnet. Wenn es sich um eine IPv6-Adresse handelt, wird der Eintrag mit `AAAA 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 IPv4-Eintrag 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 IPv6-Format des Eintrags:

```
pluto IN          AAAA 0 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto IN          AAAA 0 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

Verwenden Sie keine IPv4-Adressen mit IPv6-Zuordnung.

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 22.7, „Reverse-Lookup“** (S. 419).

Beispiel 22.7 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.

22.7 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` (`man 8 nsupdate`) entnehmen. Aus Sicherheitsgründen sollten solche Aktualisierungen mithilfe von TSIG-Schlüsseln durchgeführt werden, wie in [Abschnitt 22.8](#), „Sichere Transaktionen“ (S. 420) beschrieben.

22.8 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 -Adressbereiche 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.

22.9 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.

22.10 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.

Zum einen kann ein DHCP-Server so konfiguriert werden, dass er jeden Client anhand der Hardware-Adresse seiner Netzwerkkarte (die unveränderlich sein sollte) identifiziert und ständig mit denselben Einstellungen versorgt, sobald der Client eine Verbindung herstellt. 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 Namensserver 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.

23.1 Konfigurieren eines DHCP-Servers mit YaST

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.

23.1.1 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 23.1, „DHCP-Server: Kartenauswahl“** (S. 427).

Abbildung 23.1 DHCP-Server: Kartenauswahl

Auswahl der Netzwerkkarte
Wählen Sie eine oder mehrere der aufgeführten Netzwerkkarten aus, die für den DHCP-Server verwendet werden soll(en).

Firewall-Einstellungen
Zum Öffnen der Firewall, damit entfernte Rechner über die ausgewählte Schnittstelle auf den Dienst zugreifen können, wählen Sie **Firewall für gewählte Schnittstelle öffnen** aus. Diese Option ist nur dann verfügbar, wenn die Firewall aktiviert ist.

DHCP-Server-Wizard (1 von 4) Kartenauswahl

Netzwerkkarten für DHCP-Server

Ausgewählt	Schnittstellenname	Gerätename	IP
x	eth0		DHCP-Adresse

☒ Firewall für gewählte Schnittstellen öffnen

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 Namensserver, Adressen eines Druck- und WINS-Servers (für gemischte Netzwerkkumgebungen mit Windows- und Linux-Clients), Gateway-Adressen und Leasing-Zeit. Weitere Informationen hierzu finden Sie unter **Abbildung 23.2, „DHCP-Server: Globale Einstellungen“** (S. 428).

Abbildung 23.2 *DHCP-Server: Globale Einstellungen*

DHCP-Server-Wizard (2 von 4) Globale Einstellungen

☐ LDAP-Unterstützung

Name des DHCP-Servers (optional)

Domain-Name:

NTP-Zeitserver:

IP des primären Nameservers:

Druckserver:

IP des sekundären Nameservers:

WINS-Server:

Standard-Gateway (Router):

Standard-Leasing-Zeit: Einheiten:

Zurück **Abbrechen** **Weiter**

Optional kann auch der Name des DHCP-Servers (der Name des dhcpServer-LDAP-Objekts) angegeben werden, wenn er von Ihrem Hostnamen abweicht.

Globale Einstellungen Nehmen Sie hier verschiedene DHCP-Einstellungen vor.

Mit **Domainname** wird die Domäne festgelegt, für die der DHCP-Server per Leasing IPs an Clients vergibt.

IP des primären Nameservers und IP des sekundären Nameservers bieten den DHCP-Clients folgende Nameserver an. Bei diesen Werten

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 23.3, „DHCP-Server: Dynamisches DHCP“** (S. 429).

Abbildung 23.3 DHCP-Server: Dynamisches DHCP

The screenshot shows the 'DHCP-Server-Wizard (3 von 4) Dynamisches DHCP' window. On the left is a sidebar with 'Subnetzinformationen' and 'IP-Adressbereich'. The main area contains three sections: 'Subnetzinformationen' with fields for 'Aktuelles Netzwerk', 'Aktuelle Netzmaske', and 'Netzmasken-Bits'; 'IP-Adressbereich' with 'Erste IP-Adresse' (192.168.2.100) and 'Letzte IP-Adresse' (192.168.2.128), and a checkbox for 'Dynamisches BOOTP zulassen'; and 'Leasing-Zeit' with 'Standard' (4) and 'Maximum' (2) values and unit dropdowns. At the bottom are 'Zurück', 'Abbrechen', and 'Weiter' buttons, and a 'DHCP-Server synchronisieren' button.

Subnetzinformationen

Hier stehen die Informationen zum aktuellen Subnetz, wie die Adresse, die Netzmaske und die für die Clients verfügbaren minimalen und maximalen IP-Adressen.

IP-Adressbereich

Legen Sie die **Erste IP-Adresse** und die **Letzte IP-Adresse** fest, die per Leasing an die Clients vergeben werden dürfen. Diese Adressen müssen dieselbe Netzmaske aufweisen. Beispiel: 192.168.1.1 und 192.168.1.64. Bei Aktivierung des Flags **Dynamisches BOOTP** zulassen kann im festgelegten Bereich eine dynamische Zuordnung zu BOOTP-Clients und DHCP-Clients erfolgen

DHCP-Server-Wizard (3 von 4) Dynamisches DHCP

Subnetzinformationen

Aktuelles Netzwerk: Aktuelle Netzmaske: Netzmasken-Bits:

Minimale IP-Adresse: Maximale IP-Adresse:

IP-Adressbereich

Erste IP-Adresse: Letzte IP-Adresse:

☐ Dynamisches BOOTP zulassen

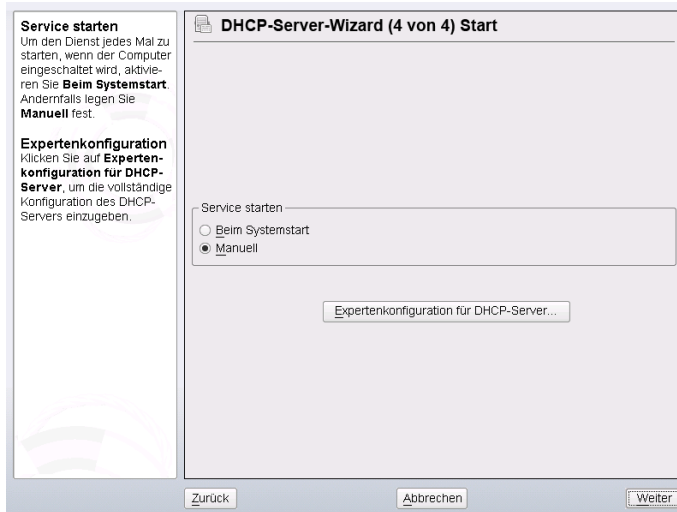
Leasing-Zeit

Standard: Einheiten: Maximum: Einheiten:

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 23.4, „DHCP-Server: Start“** (S. 430). Alternativ können Sie *Host-Verwaltung* links aus der Baumstruktur auswählen, um zusätzlich zur grundlegenden Konfiguration bestimmte Host-Verwaltungsfunktionen zu konfigurieren (siehe **Abbildung 23.5, „DHCP-Server: Host-Verwaltung“** (S. 431)).

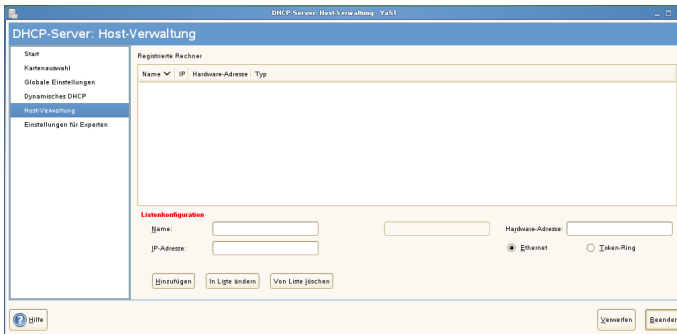
Abbildung 23.4 DHCP-Server: Start



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 23.5, „DHCP-Server: Host-Verwaltung“** (S. 431).

Abbildung 23.5 DHCP-Server: Host-Verwaltung



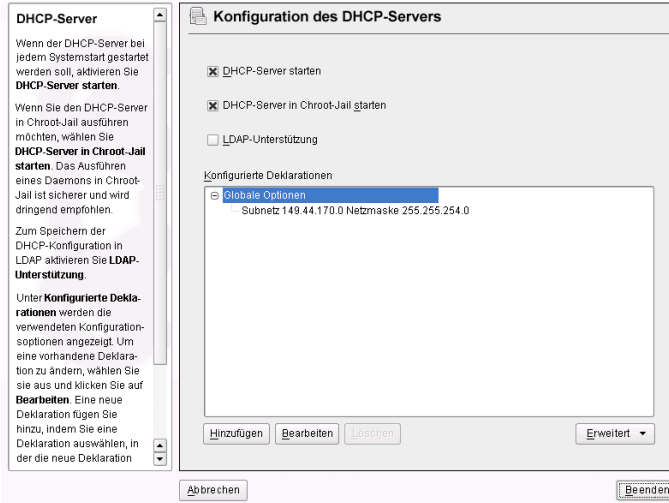
23.1.2 Konfiguration für Experten

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 23.6, „DHCP-Server: Chroot Jail und Deklarationen“** (S. 432). 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.

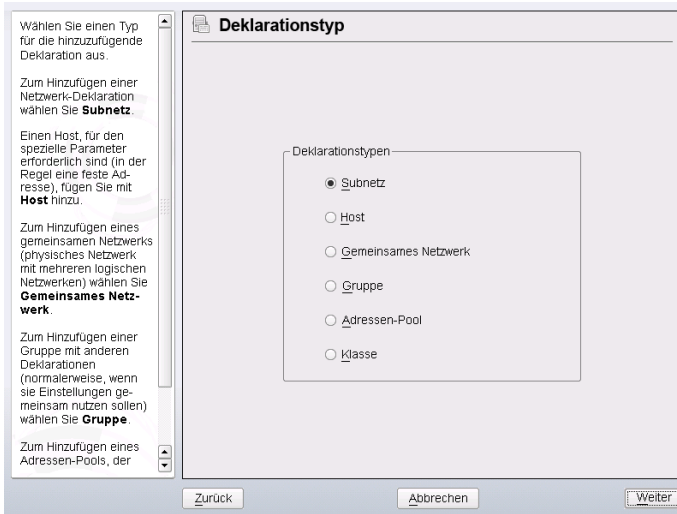
Abbildung 23.6 *DHCP-Server: Chroot Jail und Deklarationen*



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 23.7](#), „**DHCP-Server: Wählen eines Deklarationstyps**“ (S. 433)).

Abbildung 23.7 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 23.8 DHCP-Server: Konfigurieren von Subnetzen

Konfiguration des Subnetzes
Legen Sie hier die **Netzwerkadresse** und die **Netzwerkmaske** des Subnetzes fest.

Zum Bearbeiten der DHCP-Optionen wählen Sie den entsprechenden Tabelleneintrag aus und klicken Sie auf **Bearbeiten**. Mit **Hinzufügen** können Sie eine neue Option hinzufügen. Um eine Option zu entfernen, wählen Sie sie aus und klicken Sie auf **Löschen**.

Möchten Sie für Rechner dieses Subnetzes dynamisches DNS anpassen, verwenden Sie **Dynamisches DNS**.

Konfiguration des Subnetzes

Netzwerkadresse: 192.168.2.0 Netzwerkmaske: 255.255.255.0

Option	Wert
default-lease-time	14400
max-lease-time	172800

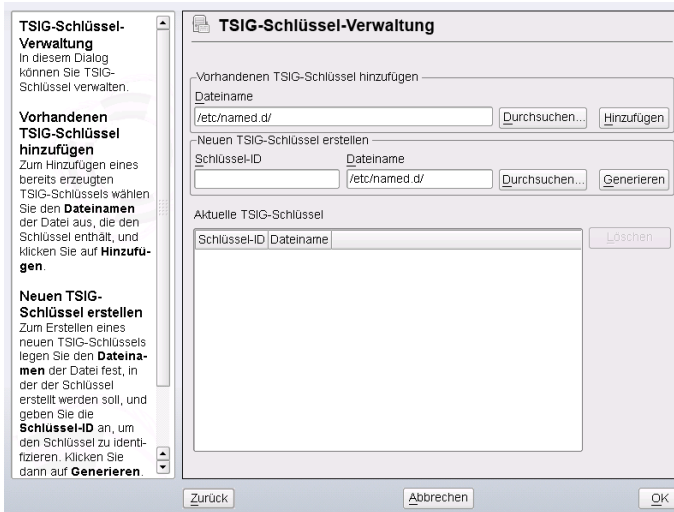
Hinzufügen Bearbeiten Löschen ☐ Dynamisches DNS

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 23.10**, „DHCP-Server: Schnittstellenkonfiguration für dynamisches DNS“ (S. 436)).

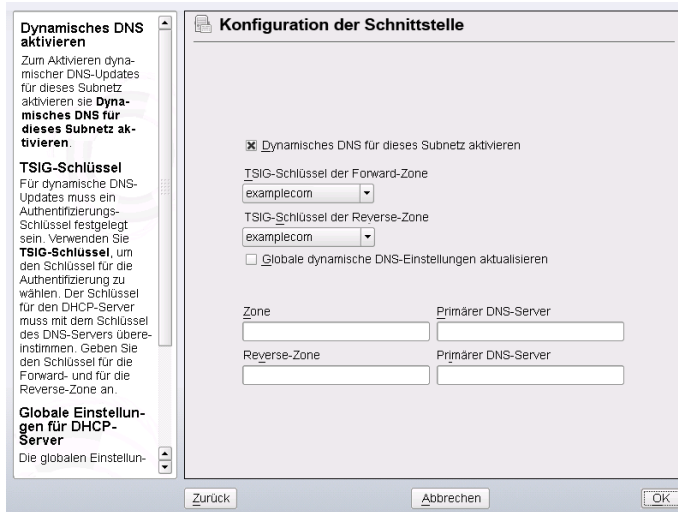
Abbildung 23.9 *DHCP Server: TSIG-Konfiguration*



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 23.8, „DHCP-Server: Konfigurieren von Subnetzen“** (S. 434)). Wenn Sie noch einmal auf **OK** klicken, gelangen Sie wieder zum ursprünglichen Dialogfeld für die Expertenkonfiguration.

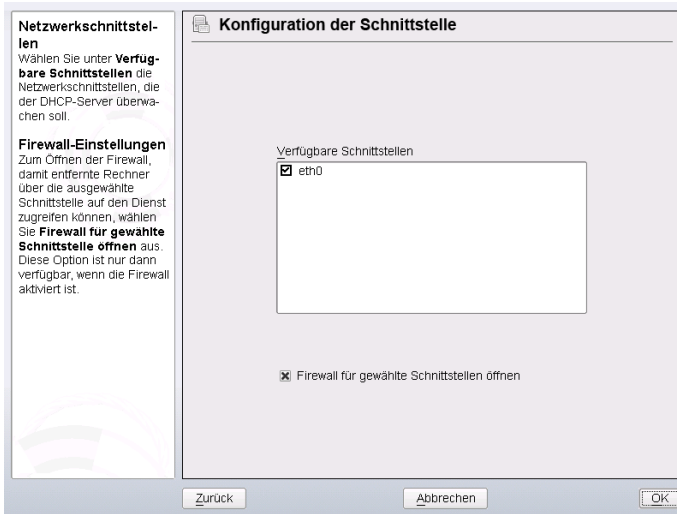
Abbildung 23.10 DHCP-Server: Schnittstellenkonfiguration für dynamisches DNS



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 23.11**, „**DHCP-Server: Netzwerkschnittstelle und Firewall**“ (S. 437)). Jetzt können Sie zum ursprünglichen Dialogfeld zurückkehren, indem Sie auf *OK* klicken.

Abbildung 23.11 *DHCP-Server: Netzwerkschnittstelle und Firewall*



Nach Abschluss aller Konfigurationsschritte schließen Sie das Dialogfeld mit *OK*. Der Server wird nun mit seiner neuen Konfiguration gestartet. Konfiguration.

23.2 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.

23.3 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 23.1**, „Die Konfigurationsdatei `/etc/dhcpd.conf`“ (S. 438) an.

Beispiel 23.1 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 22, Domain Name System (DNS)** (S. 399).
- 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 23.1, „Die Konfigurationsdatei `/etc/dhcpd.conf`“** (S. 438) 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 `rcdhcpdcheck-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 `redhcpdstart` eingeben, um die Dateien automatisch zu kopieren.

23.3.1 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 23.2, „Ergänzungen zur Konfigurationsdatei“](#) (S. 440) zur Konfigurationsdatei von [Beispiel 23.1, „Die Konfigurationsdatei `/etc/dhcpd.conf`“](#) (S. 438) hinzugefügt, weist der DHCP-Daemon dem entsprechenden Client immer dieselben Daten zu.

Beispiel 23.2 *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.

23.3.2 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`.

23.4 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.

24.1 Konfigurieren eines NTP-Client mit YaST

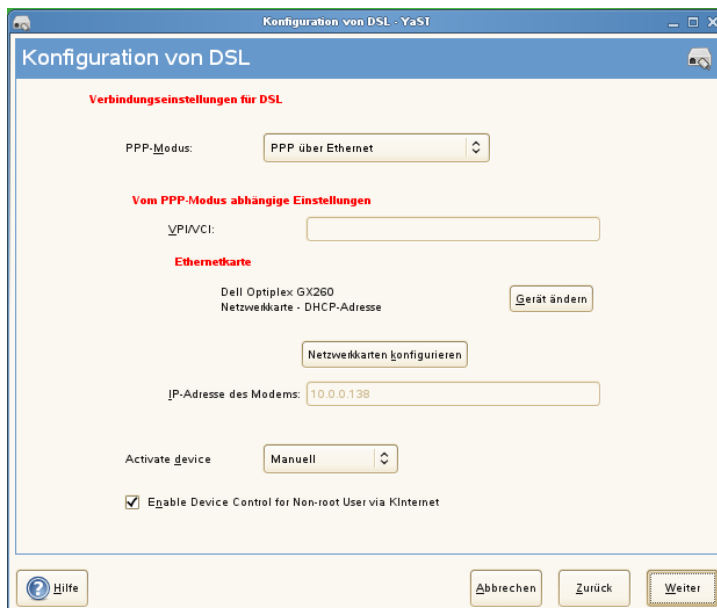
`xntp` ist so voreingestellt, dass die lokale Computeruhr als Zeitreferenz verwendet wird. Das Verwenden der (BIOS-) Uhr ist jedoch nur eine Ausweidlösung, wenn keine genauere Zeitquelle verfügbar ist. YaST erleichtert die Konfiguration von NTP-Clients.

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.

24.1.1 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 *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 24.1 YaST: Konfigurieren eines NTP-Client



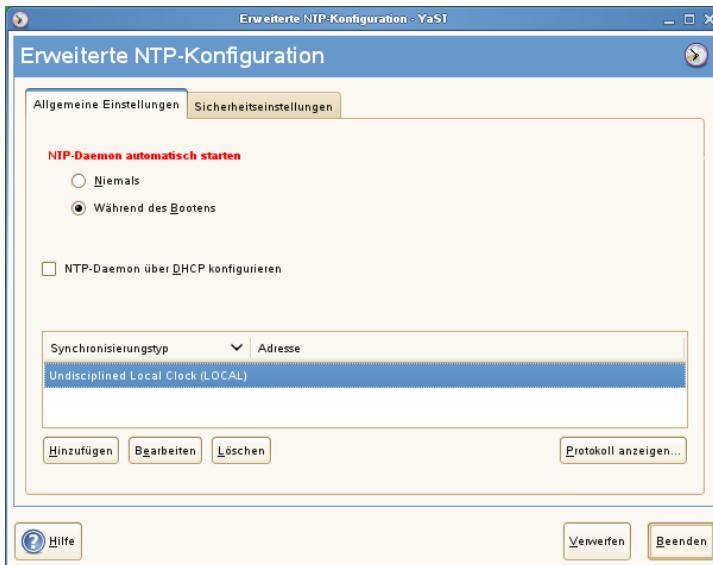
Geben Sie im Dialogfeld für die detaillierte Serverauswahl an, ob die Zeitsynchronisierung anhand eines Zeitserver in Ihrem lokalen Netzwerk (*Lokaler NTP-Server*) oder eines Zeitserver im Internet erfolgen soll, der Ihre Zeitzone verwaltet (*Öffentlicher*

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*.

24.1.2 Erweiterte NTP-Client-Konfiguration

Die erweiterte Konfiguration eines NTP-Clients kann unter *Erweiterte Konfiguration* im Hauptdialogfeld des Moduls *NTP-Konfiguration* aufgerufen werden (siehe [Abbildung 24.1](#), „*YaST: Konfigurieren eines NTP-Client*“ (S. 444)). Zunächst müssen Sie jedoch einen Start-Modus auswählen wie bei der schnellen Konfiguration beschrieben.

Abbildung 24.2 *Erweiterte NTP-Client-Konfiguration: Allgemeine Einstellungen*



Konfigurieren Sie auf dem Karteireiter *Allgemeine Einstellungen* den Betriebsmodus von *xntpd*. Mit NTP-Daemon über DHCP konfigurieren wird der NTP-Client so eingerichtet, dass eine Liste der in Ihrem Netzwerk verfügbaren NTP-Server über DHCP (Dynamic Host Configuration Protocol) abgerufen wird.

Die Server und anderen Zeitquellen für die Abfrage durch den Client sind im unteren Bereich 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 24.1.1, „Schnelle NTP-Client-Konfiguration“** (S. 444)). 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`.

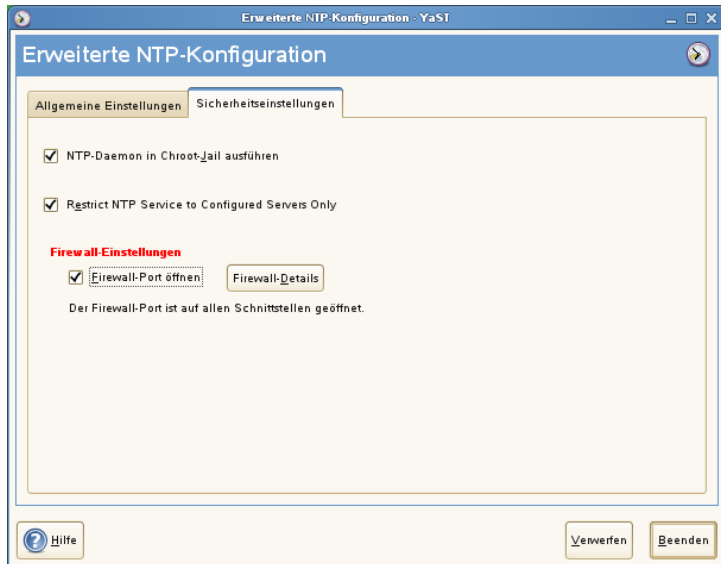
Ausgangs-Broadcast

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 24.3 *Erweiterte NTP-Client-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.

24.2 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.

24.3 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 28, Verteilte Nutzung von Dateisystemen mit NFS** (S. 513) 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.

25.1 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 25.1.1, „Konfigurieren eines NIS-Master-Servers“** (S. 452) fort.
- Wenn Ihr NIS-Master-Server seine Daten an Slave-Server exportieren soll, richten Sie den Master-Server ein, wie unter **Abschnitt 25.1.1, „Konfigurieren eines NIS-Master-Servers“** (S. 452) beschrieben, und richten Sie die Slave-Server in den Subnetzen ein, wie unter **Abschnitt 25.1.2, „Konfigurieren eines NIS-Slave-Servers“** (S. 457) beschrieben.

25.1.1 Konfigurieren eines NIS-Master-Servers

Gehen Sie wie folgt vor, um einen NIS-Master-Server für Ihr Netzwerk zu konfigurieren:

- 1 Starten Sie *YaST > Netzerkdienste > 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 25.1 NIS-Serverkonfiguration



3 Legen Sie die grundlegenden Optionen für das NIS-Setup fest:

3a Geben Sie den NIS-Domännennamen ein.

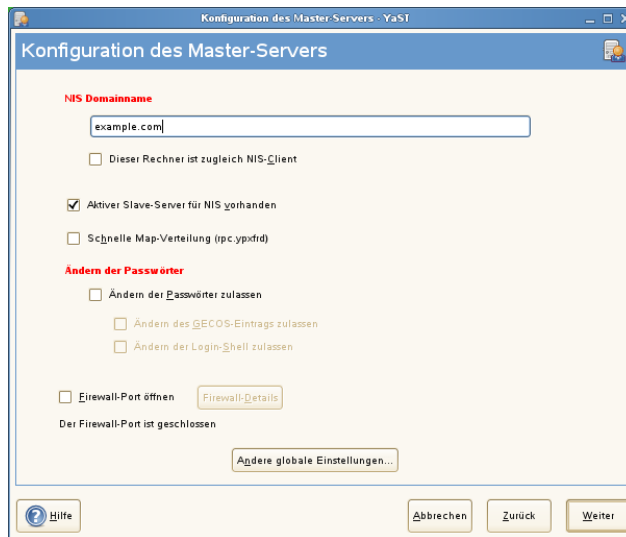
3b Definieren Sie, ob der Host auch ein NIS-Client sein soll, an dem sich Benutzer anmelden und auf Daten vom NIS-Server zugreifen können, indem Sie *Dieser Rechner ist zugleich NIS-Client* auswählen.

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.

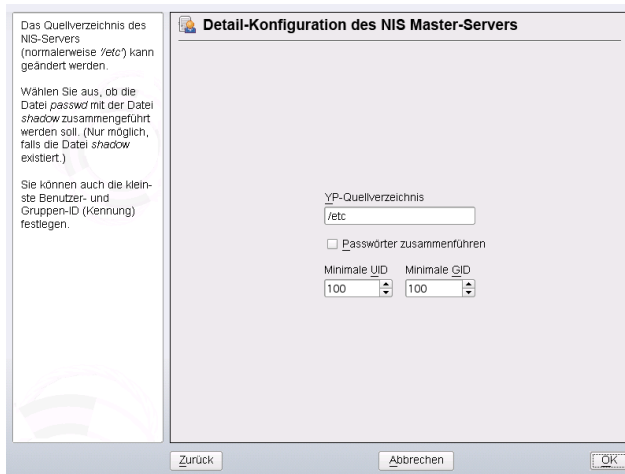
- 3c** Wenn Ihr NIS-Server als Master-Server für NIS-Slave-Server in anderen Subnetzen fungieren soll, wählen Sie *Aktiver Slave-Server für NIS vorhanden*.
- 3d** Wählen Sie *Firewall-Ports öffnen*, damit YaST die Firewall-Einstellungen für den NIS-Server anpasst.

Abbildung 25.2 *Konfiguration des Masterservers*



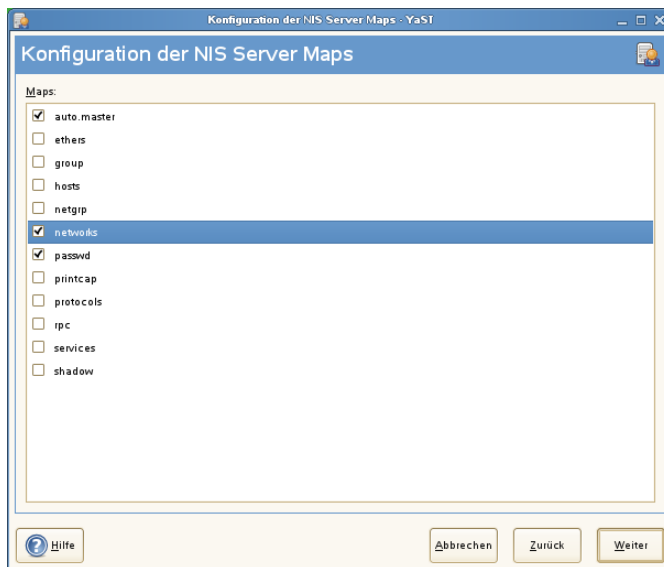
- 3e** Schließen Sie dieses Dialogfeld mit *Weiter* oder klicken Sie auf *Andere globale Einstellungen*, um zusätzliche Einstellungen vorzunehmen. *Andere globale Einstellungen* umfassen das Ändern des Quellverzeichnis für den NIS-Server (standardmäßig `/etc`). Außerdem können hier Passwörter zusammengeführt 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 25.3 *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 25.4 *Konfiguration der NIS Server Maps*

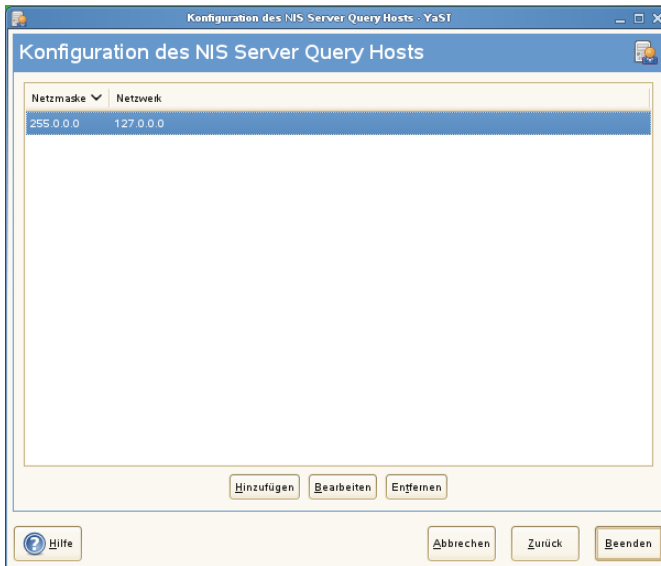


- 7** Geben Sie die Hosts ein, die den NIS-Server abfragen dürfen. Mithilfe der entsprechenden Schaltflächen können Sie Hosts hinzufügen, bearbeiten oder entfernen. Legen Sie fest, aus welchen Netzwerken Anforderungen an den NIS-Server gesendet werden dürfen. Dies ist in der Regel nur das interne Netzwerk. 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 25.5 Einrichten von Anforderungsberechtigungen für einen NIS-Server



- 8 Klicken Sie auf *Verlassen*, um die Änderungen zu speichern und das Setup abzuschließen.

25.1.2 Konfigurieren eines NIS-Slave-Servers

Gehen Sie wie folgt vor, um zusätzliche NIS-Slave-Server in Ihrem Netzwerk zu konfigurieren:

- 1 Starten Sie *YaST > Netwerkdienste > 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.

25.2 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 23, DHCP](#) (S. 425). 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 25.6, „Festlegen der Domäne und Adresse eines NIS-Servers“](#) (S. 459).

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 zeitraubendes Verfahren sein. *Broadcast* verlangt einen NIS-Server im lokalen Netzwerk, wenn der angegebene Server nicht reagiert.

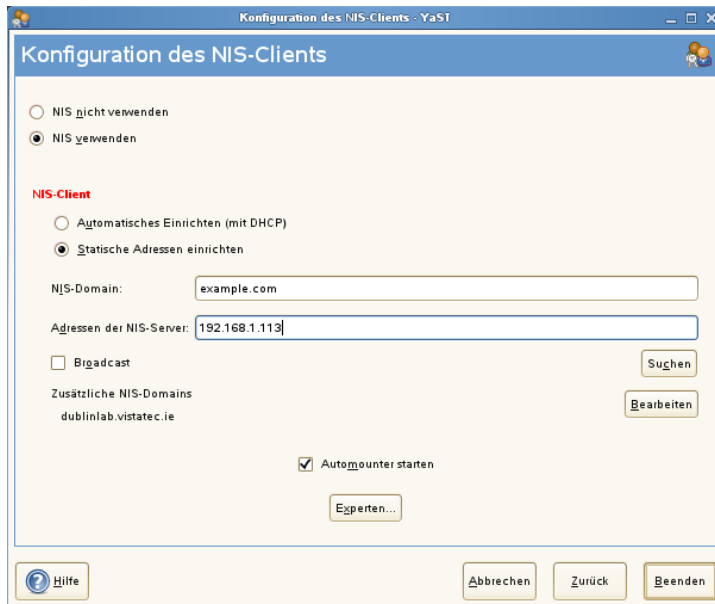
Sie können auch mehrere Server angeben, indem Sie ihre Adressen durch Leerzeichen getrennt unter *Adressen der NIS-Server* angeben.

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 25.6 Festlegen der Domäne und Adresse eines NIS-Servers



LDAP – Ein Verzeichnisdienst

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.

26.1 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.

26.2 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 26.3, „Konfigurieren eines LDAP-Servers mit YaST“](#) (S. 467) bzw. [Abschnitt 26.7, „Manuelles Konfigurieren eines LDAP-Servers“](#) (S. 483) 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

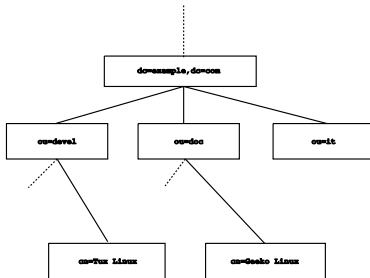
Diese Objekte können wiederum andere Objekte enthalten. Solche Objektklassen sind beispielsweise `root` (das Stammelement des Verzeichnisbaums, das in der Regel nicht vorhanden ist), `c` (Land), `ou` (organisatorische Einheit) und `dc` (Domänenkomponente). Dieses Modell ist mit Verzeichnissen (Ordern) 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 26.1, „Struktur eines LDAP-Verzeichnisses“** (S. 465) gezeigt wird.

Abbildung 26.1 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 26.1**, „Häufig verwendete Objektklassen und Attribute“ (S. 466) 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 26.1 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 26.1**, „Ausschnitt aus *schema.core*“ (S. 466) wird ein Ausschnitt einer Schemadirektive mit entsprechenden Erklärungen dargestellt (die Zeilen sind für Erklärungszwecke nummeriert).

Beispiel 26.1 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.

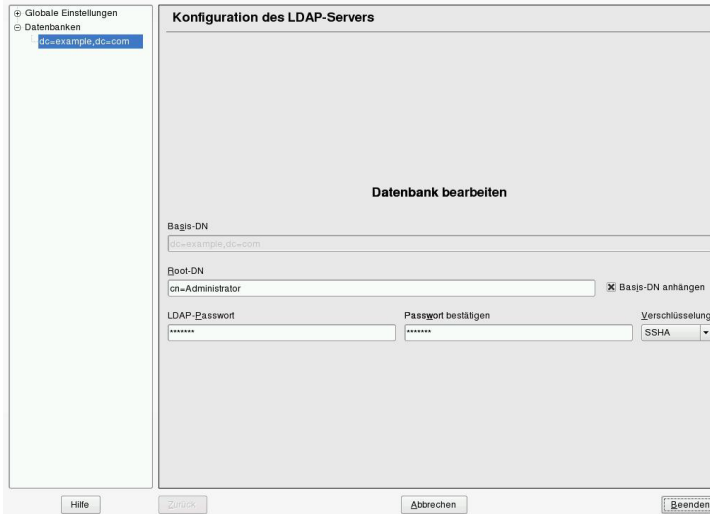
Die Definition der Objektklasse `organizationalUnit` beginnt in Zeile 4 wie die Definition des Attributs mit einem OID und dem Namen der Objektklasse. Zeile 5 enthält eine kurze Beschreibung der Objektklasse. In Zeile 6 mit dem Eintrag `SUP top` wird angegeben, dass diese Objektklasse keiner anderen 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.

26.3 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.

Abbildung 26.2 *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 die Verbindungstypen fest, die der LDAP-Server erlauben soll. Folgende Möglichkeiten stehen zur Auswahl:

`bind_v2`

Diese Option aktiviert Verbindungsanforderungen (Bind-Anforderungen) von Clients mit der vorigen Version des Protokolls (LDAPv2).

`bind_anon_cred`

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.

`bind_anon_dn`

Wenn Sie diese Option aktivieren, kann eine Verbindung ohne Authentifizierung (anonym) mit einem DN, aber ohne Passwort erfolgen.

`update_anon`

Durch Aktivieren dieser Option können nicht authentifizierte (anonyme) Aktualisierungsvorgänge ausgeführt werden. Der Zugriff ist gemäß ACLs und anderen Regeln beschränkt (siehe [Abschnitt 26.7.1, „Globale Direktiven in slapd.conf“](#) (S. 484)).

- 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*, *smd5*, *ssha* 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 Passwortsrichtlinien festgelegt haben, kann Ihr Server an diesem Punkt ausgeführt werden. Wenn Sie Passwortsrichtlinien aktivieren möchten, fahren Sie mit der Konfiguration der Passwortsrichtlinien fort. Wenn Sie ein Passwortsrichtlinienobjekt 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 *Übernehmen* 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.

26.4 Konfigurieren eines LDAP-Client mit YaST

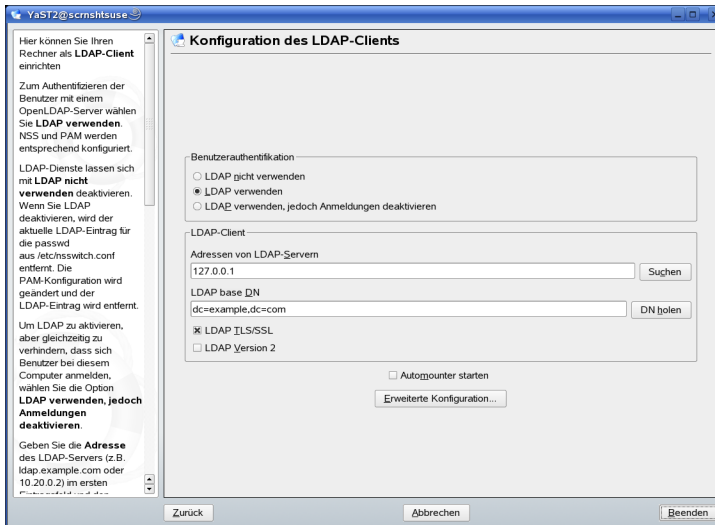
YaST enthält ein Modul zum Einrichten der LDAP-basierten Benutzerverwaltung. Wenn Sie diese Funktion bei der Installation nicht aktiviert haben, starten Sie das Modul, indem Sie *Netzwerkdienste* > *LDAP-Client* wählen. YaST aktiviert alle PAM- und NSS-bezogenen Änderungen, die für LDAP erforderlich 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 26.4.1, „Konfigurieren der grundlegenden Einstellungen“** (S. 473) 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 26.4.2, „Konfigurieren der YaST-Gruppe und der Benutzerverwaltungsmodule“** (S. 477) beschrieben.

26.4.1 Konfigurieren der grundlegenden Einstellungen

Das Dialogfeld für die grundlegende Konfiguration des LDAP-Clients (**Abbildung 26.3, „YaST: Konfiguration des LDAP-Client“** (S. 474)) wird während der Installation geöffnet, wenn Sie die LDAP-Benutzerverwaltung oder im YaST-Kontrollzentrum des installierten Systems *Netzwerkdienste* > *LDAP-Client* auswählen.

Abbildung 26.3 YaST: Konfiguration des LDAP-Client



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*.

Abbildung 26.4 *YaST: Erweiterte Konfiguration*

Erweiterte Einstellungen für LDAP-Client

Geben Sie die für die Suchbasen zu verwendenden speziellen Zuordnungen an (Benutzer, Passwörter und Gruppen), wenn Sie vom Basis-DN abweichen. Diese Werte werden in der Datei `/etc/ldap.conf` auf die Attribute `nss_base_passwd`, `nss_base_shadow`, und `nss_base_group` gesetzt.

Passwortänderungsprotokoll bezieht sich auf das Attribut `pam_password` der Datei `/etc/ldap.conf`. Informationen zur Bedeutung dieser Werte finden Sie unter `man pam_ldap`.

Legen Sie den Typ Ihrer verwendeten LDAP-Gruppen fest. Der Standardwert für **Attribut für Gruppenmitglied** ist `member`.

Erweiterte Konfiguration

Client-Einstellungen Verwaltungseinstellungen

Benennungskontexte

Benutzerzuordnung

Passwortzuordnung

Gruppenzuordnung

Passwortänderungsprotokoll

Attribut für Gruppenmitglied

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 26.4**, „YaST: Erweiterte Konfiguration“ (S. 475).

- 1 Passen Sie auf der Registerkarte *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 *Erweiterten Konfiguration* auf *Übernehmen* und anschließend zum Zuweisen der Einstellungen auf *Verlassen*.

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 26.4.2, „Konfigurieren der YaST-Gruppe und der Benutzerverwaltungsmodule“** (S. 477) beschriebenen Schritte.

26.4.2 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 26.5 *YaST: Modulkonfiguration*

Hier können Sie die im LDAP-Verzeichnis gespeicherte Konfiguration verwalten.

Eine Konfigurationsgruppe wird **Konfigurationsmodul** genannt. Ist im angegebenen Pfad (Base Configuration) kein Konfigurationsmodul vorhanden, dann erstellen Sie eines mit **Neu**. Löschen Sie das aktuelle Modul mit **Löschen**.

Falls Sie die Werte der Attribute aus der Tabelle bearbeiten wollen, drücken Sie **Bearbeiten**. Einige Werte haben besondere Bedeutungen, so wird z. B. beim Ändern des Werts **cn** das aktuelle Modul umbenannt.

Zum Konfigurieren der Standardvorlage des aktuellen Moduls klicken Sie auf **Vorlage konfigurieren**.

Konfiguration von Modulen

Konfigurationsmodul: **userconfiguration** Neu Löschen

Attribut	Wert
cn	userconfiguration
susedefaultbase	ou=people,dc=dublinlab,dc=vistatec,dc=ie
susedefaulttemplate	cn=usertemplate,ou=ldapconfig,dc=dublinlab,dc=vistatec,dc=ie
susemapattribute	
susemaxpasswordlength	8
susemaxuniqueid	60000
suseminpasswordlength	5
suseminuniqueid	1000
suseextuniqueid	1000
susepasswordhash	CRYPT
susesearchfilter	objectclass=posixaccount
suseaskelir	/etc/skel

Bearbeiten Vorlage konfigurieren

Verwerfen Übernehmen

Im Dialogfeld für die Modulkonfiguration (**Abbildung 26.5, „YaST: Modulkonfiguration“** (S. 477)) 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 auf *Neu* und wählen Sie den gewünschten Modultyp aus. Wählen Sie für ein Benutzerkonfigurationsmodul `suseuserconfiguration` und für eine Gruppenkonfiguration `susegroupconfiguration` aus.
- 2** 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.
- 3** 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.
- 4** Mit *Übernehmen* fügen Sie das neue Modul dem Auswahlmenü 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 26.6 *YaST Konfiguration einer Objektvorlage*

Konfigurieren Sie hier die Vorlage zum Anlegen neuer Objekte (wie z. B. Benutzer oder Gruppen).

Mit **Bearbeiten** lassen sich die Attributwerte der Vorlage bearbeiten. Beim Ändern des Werts **cn** wird die Vorlage umbenannt.

Die zweite Tabelle enthält eine Liste mit **Standardwerten**, die für neue Objekte verwendet werden. Ändern Sie die Liste durch Hinzufügen neuer Werte oder durch Entfernen vorhandener Werte.

Konfiguration der Objektvorlage

Attribut	Wert
cn	grouptemplate
suseNamingAttribute	cn
susePlugin	UsersPluginLDAPUI

Standardwerte für neue Objekte

Objektattribut	Standardwert
businesscategory	/home/%uid
loginshell	/bin/bash

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.

26.5 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** Rufen Sie die YaST-Benutzerverwaltung über *Sicherheit und Benutzer > Benutzerverwaltung* auf.
- 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 Registerkarte *Benutzerdaten* den Benutzernamen, die Anmeldeinformationen und das Passwort an.
 - 3b** Wählen Sie die Registerkarte *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 26.4.2, „Konfigurieren der YaST-Gruppe und der Benutzerverwaltungsmodule“** (S. 477) beschriebenen Schritten definiert werden.
 - 3c** Ändern oder akzeptieren Sie die standardmäßigen *Passworteinstellungen*.
 - 3d** Rufen Sie die Registerkarte *Plug-Ins* auf, wählen Sie das LDAP-Plugin und klicken Sie zum Konfigurieren zusätzlicher LDAP-Attribute für den neuen Benutzer auf *Starten* (siehe **Abbildung 26.7, „YaST: Zusätzliche LDAP-Einstellungen“** (S. 481)).

- 4 Klicken Sie zum Zuweisen der Einstellungen und zum Beenden der Benutzerkonfiguration auf *Übernehmen*.

Abbildung 26.7 YaST: Zusätzliche LDAP-Einstellungen

Hier sehen Sie eine Tabelle mit allen erlaubten Attributen für den aktuellen LDAP-Eintrag, die in den vorangegangenen Dialogen nicht festgelegt wurden.

Die Liste der Attribute wird von dem Wert von "objectClass" bestimmt. (Dieser ist derzeit: inetOrgPerson, posixAccount, shadowAccount, top).

Bearbeiten Sie die einzelnen Attribute mit **Bearbeiten**. Einige Attribute könnten erforderlich sein. Dies wird in der Benutzervorlage im **LDAP-Client-Modul** festgelegt.

Attribut	Wert
cn	faster
givenname	geeko
sn	geeko
audio	
businesscategory	
carlicense	
departmentnumber	
displayname	
employeenumber	
employeetype	
homephone	
homepostaladdress	
initials	
jpegphoto	
labeleduri	
mail	
manager	
mobile	
o	
ou	

Bearbeiten

Übernehmen

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.

26.6 Navigieren in der LDAP-Verzeichnisstruktur

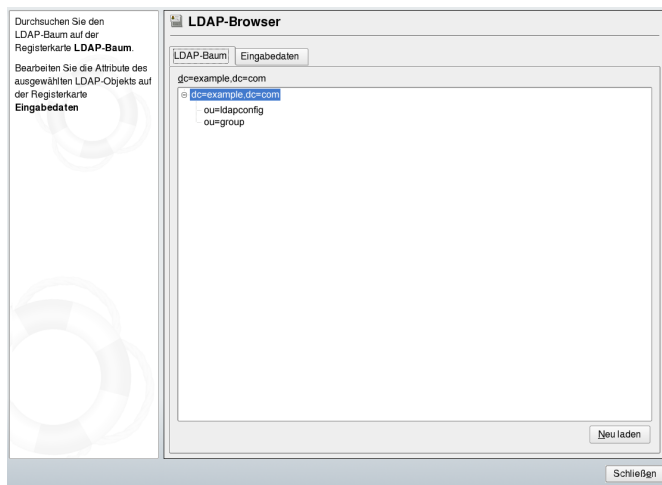
Um mühelos in der LDAP-Verzeichnisstruktur und ihren Einträgen zu navigieren, verwenden Sie den YaST-LDAP-Browser:

- 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.

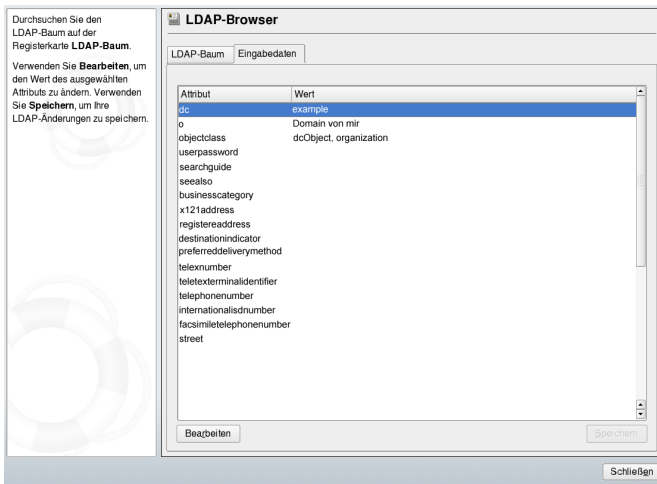
Abbildung 26.8 Navigieren in der LDAP-Verzeichnisstruktur



- 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 26.9 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*.

26.7 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.

26.7.1 Globale Direktiven in slapd.conf

Beispiel 26.2 *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 26.2, „slapd.conf: Include-Direktive für Schemata“** (S. 484) 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 Information erhalten Sie in der im Lieferumfang enthaltenen OpenLDAP-Dokumentation.

Beispiel 26.3 *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 26.4 *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 26.4, „slapd.conf: Zugriffssteuerung“** (S. 484) 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 26.2, „Benutzergruppen und ihre Zugriffsberechtigungen“** (S. 485) dargestellten Einträge sind möglich.

Tabelle 26.2 Benutzergruppen und ihre Zugriffsberechtigungen

Tag	Scope
*	Alle Benutzer ohne Ausnahme
anonymous	Nicht authentifizierte („anonyme“) Benutzer
Benutzer	Authentifizierte Benutzer

Tag	Scope
<code>self</code>	Mit dem Zielobjekt verbundene Benutzer
<code>dn.regex=<regex></code>	Alle Benutzer, die mit dem regulären Ausdruck übereinstimmen

- Mit `access` wird der Zugriffstyp angegeben. Verwenden Sie die in [Tabelle 26.3, „Zugriffstypen“](#) (S. 486) angegebenen Optionen.

Tabelle 26.3 Zugriffstypen

Tag	Umfang des Zugriffs
<code>Keine</code>	Kein Zugriff
<code>auth</code>	Für die Verbindung zum Server
<code>compare</code>	Für Objekt für Vergleichszugriff
<code>Suchen</code>	Für den Einsatz von Suchfiltern
<code>Lesen</code>	Lesezugriff
<code>write</code>	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 26.5, „slapd.conf: Beispiel für Zugriffskontrolle“](#) (S. 487) ist ein Beispiel für eine einfache Zugriffssteuerung dargestellt, die mithilfe von regulären Ausdrücken beliebig entwickelt werden kann.

Beispiel 26.5 *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>.

26.7.2 Datenbankspezifische Direktiven in slapd.conf

Beispiel 26.6 *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 slapasswd(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 ppolicy❾
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 26.6**, „**slapd.conf: Datenbankspezifische Direktiven**“ (S. 488)).
- ❷ Mit `suffix` geben Sie an, für welchen Teil des LDAP-Baums der Server verantwortlich sein soll.
- ❸ Mit `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.
- ❹ Mit `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 `slapasswd` erstellte Hash-Wert des Administratorpassworts eingegeben werden.

- ⑦ Die `directory`-Direktive gibt das Verzeichnis im Dateisystem an, in dem die Datenbankverzeichnisse auf dem Server gespeichert sind.
- ⑧ 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.
- ⑨ `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.

26.7.3 Starten und Anhalten der Server

Nachdem der LDAP-Server vollständig konfiguriert und alle gewünschten Einträge gemäß dem in **Abschnitt 26.8, „Manuelles Verwalten von LDAP-Daten“** (S. 490) beschriebenen Schema vorgenommen wurden, starten Sie den LDAP-Server als `root`, indem Sie den Befehl `rcldap start` eingeben. Um den Server manuell zu stoppen, geben Sie den Befehl `rcldap stop` ein. Fragen Sie den Status des laufenden LDAP-Servers mit `rcldap status` ab.

Mit dem in [Abschnitt 12.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 215) 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 12.2.2, „Init-Skripten“](#) (S. 211) beschrieben, die entsprechenden Verknüpfungen zu den Start- und Anhaltsskripten mit dem Befehl `insserv` über die Kommandozeile zu erstellen.

26.8 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.

26.8.1 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 26.1, „Struktur eines LDAP-Verzeichnisses“](#) (S. 465) würde der Datei in [Beispiel 26.7, „Beispiel für eine LDIF-Datei“](#) (S. 491) ähneln.

Beispiel 26.7 *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
```

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.

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 eingegeben, wie er in `slapd.conf` konfiguriert wurde. Im aktuellen Beispiel lautet `cn=Administrator,dc=example,dc=com`. Mit `-W` wird die Passworтеingabe in der Kommandozeile (unverschlüsselt) umgangen und eine separate Passworтеingabeaufforderung aktiviert. Das Passwort wurde zuvor in `slapd.conf` mit `rootpw` festgelegt. Mit der Option `-f` wird der Dateiname weitergegeben. Detaillierte Informa-

tionen zum Ausführen von `ldapadd` erhalten Sie in **Beispiel 26.8**, „`ldapadd` mit `example.ldif`“ (S. 492).

Beispiel 26.8 *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 26.9**, „LDIF-Daten für Tux“ (S. 492) wird dem neuen LDAP-Verzeichnis Tux hinzugefügt.

Beispiel 26.9 *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.

26.8.2 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 26.10**, „Geänderte LDIF-Datei `tux.ldif`“ (S. 493) angegeben.

Beispiel 26.10 *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`.

26.8.3 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)`).

26.8.4 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
```

26.9 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.

Unterstützung für Active Directory

27

Active Directory* (AD) ist ein Verzeichnisdienst auf der Basis von LDAP, Kerberos und anderen Diensten, der von Microsoft Windows zur Verwaltung von Ressourcen, Diensten und Benutzern eingesetzt wird. In einem MS Windows-Netzwerk bietet AD Informationen über diese Objekte, beschränkt den Zugriff darauf und setzt Richtlinien durch. openSUSE® ermöglicht es Ihrem Linux-Computer, bestehenden AD-Domänen beizutreten und sich in eine Windows-Umgebung zu integrieren.

27.1 Integration von Linux- und AD-Umgebungen

Sobald ein Linux-Client, der als Active Directory-Client konfiguriert wurde, einer bestehenden Active Directory-Domäne beitrifft, kann er von einer großen Anzahl von Funktionen profitieren, die auf einem reinen openSUSE Linux-Client nicht verfügbar sind:

Blättern in freigegebenen Dateien und Ordnern mit SMB

Sowohl Nautilus, der GNOME-Dateimanager, als auch Konqueror, seine KDE-Entsprechung, unterstützen die Anzeige freigegebener Ressourcen mit SMB.

Freigabe von Dateien und Ordnern mit SMB

Sowohl Nautilus, der GNOME-Datei-Manager, als auch Konqueror, sein KDE-Gegenstück, unterstützen die Freigabe von Ordnern und Dateien wie unter Windows.

Zugriff auf und Änderung von Benutzerdaten auf dem Windows-Server

Mithilfe von Nautilus und Konqueror können die Benutzer auf ihre Windows-Benutzerdaten zugreifen sowie Dateien und Ordner auf dem Windows-Server bearbeiten, erstellen und löschen. Benutzer können auf ihre Daten zugreifen, ohne ständig ihr Passwort neu eingeben zu müssen.

Offline-Authentifizierung

Benutzer können sich auf dem Linux-Computer anmelden und auf ihre lokalen Daten zugreifen, selbst wenn sie offline sind (z. B. an einem Laptop) oder der AD-Server aus anderen Gründen nicht verfügbar ist.

Windows-Passwortänderung

Dieser Teil der AD-Unterstützung unter Linux erzwingt die Anwendung firmeninterner Passwortrichtlinien, die in Active Directory gespeichert sind. Die Anzeiger-Manager und Konsolen unterstützen Passwortänderungsnachrichten und akzeptieren Ihre Eingabe. Sie können sogar das Linux-Kommando `passwd` verwenden, um Windows-Passwörter festzulegen.

Einmalige Anmeldung über kerberisierte Anwendungen

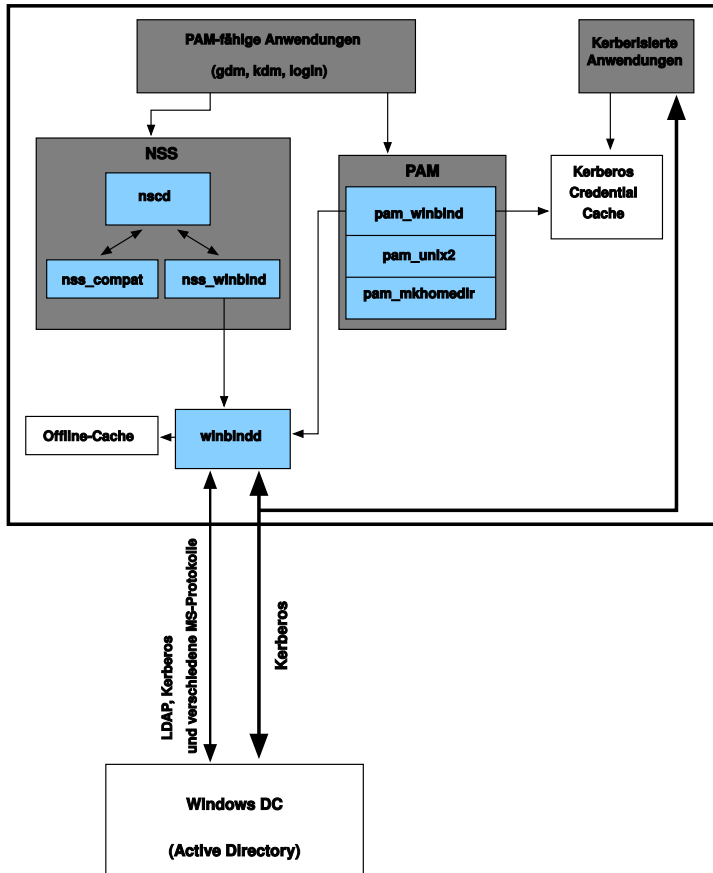
Viele Anwendungen beider Arbeitsoberflächen wurden für Kerberos aktiviert (*kerberisiert*). Dies bedeutet, dass sie die Autorisierung für den Benutzer transparenter gestalten und er bei Webservern, Proxies, Groupware-Anwendungen usw. nicht mehr erneut sein Passwort eingeben muss.

Der folgende Abschnitt enthält kurze technische Hintergrundinformationen zu den meisten der genannten Funktionen. Anleitungen zur Datei- und Druckerfreigabe finden Sie im *GNOME User Guide* sowie im *KDE User Guide*. Darin erfahren Sie mehr zur AD-Aktivierung in der Anwendungswelt von GNOME und KDE.

27.2 Hintergrundinformationen zur AD-Unterstützung unter Linux

Viele Systemkomponenten müssen fehlerfrei zusammenarbeiten, um einen Linux-Client in eine bestehende Windows Active Directory-Domäne zu integrieren. **Abbildung 27.1, „Active Directory-Authentifizierungsschema“** (S. 499) markiert die wichtigsten. Die folgenden Abschnitte konzentrieren sich auf die zugrunde liegenden Prozesse der Schlüsselereignisse bei der Interaktion zwischen AD-Server und -Client.

Abbildung 27.1 Active Directory-Authentifizierungsschema



Damit der Client mit dem Verzeichnisdienst kommunizieren kann, muss er mindestens zwei Protokolle mit dem Server gemeinsam verwenden:

LDAP

LDAP ist ein Protokoll, das für die Verwaltung von Verzeichnisinformationen optimiert ist. Ein Windows-Domain Controller mit AD kann das LDAP-Protokoll für den Austausch von Verzeichnisinformationen mit den Clients verwenden. Wenn Sie mehr über LDAP und den zugehörigen Open Source-Port, OpenLDAP, erfahren möchten, lesen Sie unter **Kapitel 26, LDAP – Ein Verzeichnisdienst** (S. 461) nach.

Kerberos

Kerberos ist ein verbürgter Authentifizierungsdienst eines Drittanbieters. Alle Clients von Kerberos vertrauen dessen Beurteilung der Identität eines anderen Client, wodurch kerberisierte Single-Sign-On-(SSO-)Lösungen ermöglicht werden. Windows unterstützt eine Kerberos-Implementierung und ermöglicht somit den Kerberos-SSO auch für Linux-Clients.

Die folgenden Client-Komponenten verarbeiten Konto- und Authentifizierungsdaten:

Winbind

Das Kernstück dieser Lösung ist der winbind-Dämon, der Teil des Samba-Projekts ist und die gesamte Kommunikation mit dem AD-Server abwickelt.

NSS (*Name Service Switch*)

NSS-Routinen bieten Namendienstinformationen. Ein Benennungsdienst für Benutzer und Gruppen wird durch `nss_winbind` bereitgestellt. Dieses Modul arbeitet direkt mit dem winbind-Dämon zusammen.

PAM (*Pluggable Authentication Modules*)

Die Benutzerauthentifizierung für AD-Benutzer wird vom Modul `pam_winbind` durchgeführt. Die Erstellung von Home-Verzeichnissen für die AD-Benutzer auf dem Linux-Client wird vom Modul `pam_mkhomedir` durchgeführt. Das Modul `pam_winbind` interagiert direkt mit `winbindd`. Weitere Informationen zu PAM finden Sie unter **Kapitel 18, Authentifizierung mit PAM** (S. 299).

PAM-fähige Anwendungen wie die Anmelderoutinen und die GNOME- und KDE-Anzeige-Manager interagieren mit der PAM- und NSS-Schicht zur Authentifizierung beim Windows-Server. Anwendungen, die die Kerberos-Authentifizierung unterstützten, beispielsweise Datei-Manager, Webbrowser oder E-Mail-Clients, verwenden den Kerberos-Berechtigungszwischenspeicher für den Zugriff auf die Kerberos-Tickets des Benutzers und sind somit Teil des SSO-Framework.

27.2.1 Domänenbeitritt

Beim Domänenbeitritt stellen der Server und der Client eine sichere Beziehung her. Auf dem Client müssen die folgenden Aufgaben ausgeführt werden, damit dieser der bestehenden LDAP- und Kerberos-SSO-Umgebung beitreten kann, die durch den Windows-Domain Controller bereitgestellt wird. Der gesamte Beitrittsvorgang wird

vom YaST-Modul für die Domänenmitgliedschaft gesteuert, das während der Installation oder im installierten System ausgeführt werden kann:

- 1 Der Windows-Domain Controller, der LDAP- und KDC-(Key Distribution Center-)Dienste bereitstellt, wird ermittelt.
- 2 Im Verzeichnisdienst wird ein Computerkonto für den beitretenden Client erstellt.
- 3 Ein erstes Ticket-Granting-Ticket (TGT) für den Client wird abgerufen und in seinem lokalen Kerberos-Berechtigungszwischenspeicher abgelegt. Der Client benötigt dieses TGT, um weitere Tickets anzufordern, die den Kontakt mit anderen Diensten ermöglichen, etwa zum Kontaktieren des Verzeichnisseservers für LDAP-Anfragen.
- 4 Die NSS- und PAM-Konfigurationen werden so angepasst, dass der Client sich beim Domänencontroller authentifizieren kann.

Während des Client-Bootvorgangs wird der winbind-Dämon gestartet und ruft das erste Kerberos-Ticket für das Computerkonto ab. Das Ticket wird von winbindd automatisch aktualisiert, damit es seine Gültigkeit nicht verliert. winbindd fragt regelmäßig den Domain Controller ab, um den Überblick über die aktuellen Kontorichtlinien zu behalten.

27.2.2 Domänenanmeldung und Home-Verzeichnisse

Die Anmelde-Manager von GNOME und KDE (GDM und KDM) wurden erweitert, um die Anmeldung bei einer AD-Domäne zu ermöglichen. Die Benutzer können wählen, ob sie sich bei der Primärdomäne Ihres Computers oder bei einer der verbürgten Domänen anmelden möchten, zu denen der Domain Controller der Primärdomäne in einem Verbürgungsverhältnis steht.

Die Benutzerauthentifizierung wird durch eine Reihe von PAM-Modulen ausgehandelt, wie unter [Abschnitt 27.2, „Hintergrundinformationen zur AD-Unterstützung unter Linux“](#) (S. 498) beschrieben. Das Modul `pam_winbind`, das zur Authentifizierung von Clients bei Active Directory- oder NT4-Domänen verwendet wird, kennt die Windows-Fehlerbedingungen, die eine Anmeldung eines Benutzers verhindern können. Die Windows-Fehlercodes werden in entsprechende vom Benutzer lesbare Fehlermel-

dungen übersetzt, die PAM bei der Anmeldung mit einer der unterstützten Methoden (GDM, KDM, Konsole und SSH) ausgibt:

Passwort ist abgelaufen

Der Benutzer sieht eine Meldung, die besagt, dass sein Passwort abgelaufen ist und geändert werden muss. Das System fordert ihn direkt zur Eingabe eines neuen Passworts auf und informiert ihn, wenn sein neues Passwort nicht mit den firmen-internen Passwortrichtlinien übereinstimmt, beispielsweise, wenn es zu kurz oder zu einfach ist oder bereits verwendet wurde. Wenn das Passwort eines Benutzers fehlschlägt, wird der Grund angegeben und ein neues Passwort angefordert.

Zugang deaktiviert

Der Benutzer sieht eine Fehlermeldung, die besagt, dass sein Konto deaktiviert wurde und er sich an den Systemadministrator wenden soll.

Konto gesperrt

Der Benutzer sieht eine Fehlermeldung, die besagt, dass sein Konto gesperrt wurde und er sich an den Systemadministrator wenden soll.

Passwort muss geändert werden

Der Benutzer kann sich anmelden, erhält aber die Warnmeldung, dass sein Passwort bald geändert werden muss. Diese Warnung wird drei Tage vor Ablauf des Passworts gezeigt. Nach Ablauf kann sich der Benutzer nicht mehr anmelden.

Ungültiger Arbeitsplatzrechner

Wenn sich ein Benutzer nur von einem bestimmten Arbeitsplatzrechner aus anmelden darf und der aktuelle openSUSE-Computer nicht in dieser Liste aufgeführt ist, teilt eine Meldung mit, dass sich dieser Benutzer nicht von diesem Arbeitsplatzrechner aus anmelden kann.

Ungültige Anmeldezeit

Wenn sich ein Benutzer nur während der Arbeitsstunden anmelden darf und außerhalb der Arbeitszeit eine Anmeldung versucht, teilt eine Meldung mit, dass die Anmeldung zu diesem Zeitpunkt nicht möglich ist.

Konto abgelaufen

Ein Administrator kann eine Ablaufzeit für ein bestimmtes Benutzerkonto festlegen. Wenn dieser Benutzer versucht, sich nach Ablauf dieser Zeit anzumelden, teilt ihm eine Meldung mit, dass das Konto abgelaufen ist und nicht für eine Anmeldung benutzt werden kann.

Während einer erfolgreichen Authentifizierung erhält `pam_winbind` ein Ticket-Granting-Ticket (TGT) vom Kerberos-Server von Active Directory und speichert dieses im Berechtigungszwischenspeicher des Benutzers. Darüber hinaus kümmert sich die Datei um die Erneuerung des TGT im Hintergrund, sodass hierfür kein Benutzereingriff erforderlich ist.

openSUSE unterstützt lokale Home-Verzeichnisse für AD-Benutzer. Wenn die Konfiguration mit YaST durchgeführt wurde (siehe [Abschnitt 27.3, „Konfigurieren eines Linux-Client für Active Directory“](#) (S. 504)), wird bei der ersten Anmeldung eines Windows-(AD-)Benutzers beim Linux-Client ein Home-Verzeichnis für den Benutzer erstellt. Dieses Home-Verzeichnis unterscheidet sich äußerlich nicht von den standardmäßigen Home-Verzeichnissen der Linux-Benutzer und funktioniert unabhängig vom AD-Domain Controller. Durch Verwendung eines lokalen Home-Verzeichnisses kann der Benutzer auf seine Daten auf dem Computer zugreifen, selbst wenn keine Verbindung zum AD-Server besteht, sofern der Linux-Client für Offline-Authentifizierung konfiguriert wurde.

27.2.3 Offline-Dienst und Richtlinienunterstützung

Benutzer in einer Firmenumgebung müssen in der Lage sein, ein Roaming-Benutzer zu werden, d. h., die Netzwerke zu wechseln oder auch einige Zeit ohne Netzwerkverbindung zu arbeiten. Damit sich die Benutzer bei einem Computer ohne aktive Netzwerkverbindung anmelden können, wurde ein umfangreicher Zwischenspeicher in den `winbind`-Dämon integriert. Der `winbind`-Dämon erzwingt die Passwortrichtlinien auch im Offline-Status. Er verfolgt die Anzahl der fehlgeschlagenen Anmeldeversuche und reagiert entsprechend der in Active Directory konfigurierten Richtlinien. Die Offline-Unterstützung ist standardmäßig deaktiviert und muss im YaST-Modul für die Domänenmitgliedschaft ausdrücklich aktiviert werden.

Wie unter Windows, wenn der Domain Controller nicht mehr verfügbar ist, kann der Benutzer mit gültigen Kerberos-Tickets, die er vor dem Verbindungsverlust erworben hat, immer noch auf (vom AD-Server abweichende) Netzwerkressourcen zugreifen. Passwortänderungen können nur ausgeführt werden, wenn der Domain Controller online ist. Ohne Verbindung zum AD-Server kann ein Benutzer auf keine Daten zugreifen, die auf diesem Server gespeichert sind. Wenn ein Arbeitsplatzrechner vollständig vom Netzwerk getrennt wurde und später wieder mit dem Unternehmensnetzwerk verbunden wird, erhält openSUSE ein neues Kerberos-Ticket, sobald der Benutzer den

Desktop gesperrt und entsperrt hat (beispielsweise mithilfe eines Desktop-Bildschirmschoners).

27.3 Konfigurieren eines Linux-Client für Active Directory

Bevor Ihr Client einer AD-Domäne beitreten kann, sind einige Anpassungen an der Netzwerkkonfiguration erforderlich, um eine fehlerfreie Interaktion von Client und Server zu gewährleisten.

DNS

Konfigurieren Sie Ihren Client-Computer für die Verwendung eines DNS-Servers, der DNS-Anfragen an den AD-DNS-Server weiterleiten kann. Konfigurieren Sie Ihren Computer alternativ für die Verwendung des AD-DNS-Servers als Quelle für Namensdienstdaten.

NTP

Für eine erfolgreiche Kerberos-Authentifizierung muss die Zeit auf dem Client präzise eingestellt sein. Es wird dringend geraten, zu diesem Zweck einen zentralen NTP-Zeitserver zu verwenden. (Dies kann auch der NTP-Server sein, der auf Ihrem Active Directory-Domänencontroller ausgeführt wird.) Wenn der Zeitversatz zwischen Ihrem Linux-Host und dem Domain Controller eine bestimmte Grenze überschreitet, schlägt die Kerberos-Authentifizierung fehl und der Client wird nur mit der schwächeren NTLM-(NT LAN Manager-)Authentifizierung angemeldet.

DHCP

Wenn Ihr Client eine dynamische Netzwerkkonfiguration über DHCP verwendet, müssen Sie DHCP so konfigurieren, dass der Client stets dieselbe IP und denselben Hostnamen erhält. Verwenden Sie zur Sicherheit möglichst statische IP-Adressen.

Firewall

Für das Browsen in Ihrer Netzwerkumgebung müssen Sie entweder die Firewall vollständig deaktivieren oder die verwendete Schnittstelle als Bestandteil der internen Zone kennzeichnen.

Zur Änderung der Firewall-Einstellungen auf Ihrem Client melden Sie sich als "root" an und starten Sie das YaST-Firewall-Modul. Wählen Sie *Interfaces* (Schnittstellen) aus. Wählen Sie Ihre Netzwerkschnittstelle aus der Liste der

Schnittstellen aus, und klicken Sie auf *Change* (Ändern). Wählen Sie *Internal Zone* (interne Zone) aus und übernehmen Sie die Einstellungen mit *OK*. Schließen Sie die Firewall-Einstellungen mit *Next (Weiter) > Accept (Übernehmen)*. Zur Deaktivierung der Firewall legen Sie einfach *Service Start* (Service starten) auf *manually* (manuell) fest und schließen Sie das Firewall-Modul mit *Next (Weiter) > Accept (Übernehmen)*

AD-Konto

Sie können sich erst bei einer AD-Domäne anmelden, wenn Ihnen der AD-Administrator ein gültiges Benutzerkonto für die Domäne eingerichtet hat. Verwenden Sie den AD-Benutzernamen und das AD-Passwort, um sich auf Ihrem Linux-Client bei der AD-Domäne anzumelden.

Binden Sie eine vorhandene AD-Domäne während der Installation an oder indem Sie später die SMB-Benutzerauthentifizierung mit YaST im installierten System aktivieren.

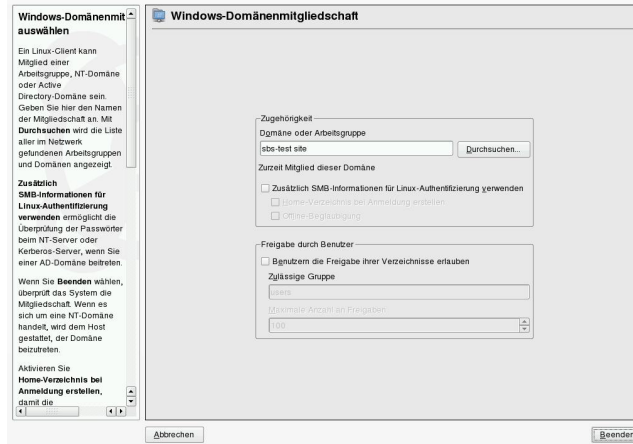
ANMERKUNG

Zurzeit kann nur ein Domänenadministratorkonto wie `Administrator` openSUSE an Active Directory anbinden.

Zum Anbinden einer AD-Domäne in einem laufenden System gehen Sie wie folgt vor:

- 1 Melden Sie sich als "`root`" an und starten Sie YaST.
- 2 Starten Sie *Netzwerkdienste > Windows-Domänenmitgliedschaft*.
- 3 Geben Sie unter *Domain or Workgroup* (Domain oder Arbeitsgruppe) im Bildschirm *Windows Domain Membership* (Windows-Domänenmitgliedschaft) die Domäne an, der Sie beitreten möchten (siehe **Abbildung 27.2, „Festlegen der Windows-Domänenmitgliedschaft“** (S. 506)). Wenn die DNS-Einstellungen auf Ihrem Host korrekt in den Windows DNS-Server integriert sind, geben Sie den AD-Domännennamen in seinem DNS-Format ein (`domain.firma.com`). Wenn Sie den Kurznamen Ihrer Domäne eingeben (auch als Domänenname vor Windows 2000 bekannt), muss sich YaST auf die NetBIOS-Namensauflösung anstelle von DNS verlassen, um den korrekten Domänen-Controller zu finden. Soll stattdessen aus einer Liste der verfügbaren Domänen ausgewählt werden, listen Sie mithilfe von *Durchsuchen* die NetBIOS-Domänen auf und wählen Sie dann die gewünschte Domäne aus.

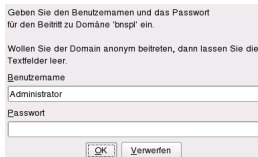
Abbildung 27.2 Festlegen der Windows-Domänenmitgliedschaft



- 4 Aktivieren Sie *Zusätzlich SMB-Informationen für Linux-Authentifizierung verwenden*, um die SMB-Quelle für die Linux-Authentifizierung zu verwenden.
- 5 Aktivieren Sie die Option *Create Home Directory on Login* (Home-Verzeichnis bei Anmeldung erstellen), um automatisch ein Home-Verzeichnis für den AD-Benutzer auf dem Linux-Computer zu erstellen.
- 6 Aktivieren Sie die Option *Offline-Authentifizierung*, damit sich Ihre Domänenbenutzer anmelden können, selbst wenn der AD-Server vorübergehend nicht verfügbar oder keine Netzwerkverbindung vorhanden ist.
- 7 Wählen Sie *Experteneinstellungen* aus, wenn Sie die UID- und GID-Bereiche für die Samba-Benutzer und -Gruppen ändern möchten. Let DHCP retrieve the WINS server (WINS-Server von DHCP abrufen lassen) (Standardeinstellung).
- 8 Konfigurieren Sie die NTP-Zeit-Synchronisierung für Ihre AD-Umgebung, indem Sie *NTP-Konfiguration* auswählen und einen entsprechenden Servernamen oder eine Ip-Adresse eingeben. Dieser Schritt entfällt, wenn Sie bereits die entsprechenden Einstellungen im eigenständigen YaST NTP-Konfigurationsmodul eingegeben haben.

- 9 Klicken Sie auf *Verlassen* und bestätigen Sie nach Aufforderung die Domänenverbindung.
- 10 Geben Sie das Passwort für den Windows-Administrator auf dem AD-Server ein und klicken Sie auf *OK* (siehe **Abbildung 27.3**, „**Angeben von Administratorberechtigungen**“ (S. 507)).

Abbildung 27.3 *Angeben von Administratorberechtigungen*



Geben Sie den Benutzernamen und das Passwort für den Beitritt zu Domäne 'bripi' ein.

Wollen Sie der Domain anonym beitreten, dann lassen Sie die Textfelder leer.

Benutzername
Administrator

Passwort

OK Verwerfen

Nachdem Sie der AD-Domäne beigetreten sind, können Sie sich auf Ihrer Arbeitsstation über den Anzeige-Manager der Arbeitsoberfläche oder über die Konsole bei der Domäne anmelden.

27.4 Anmeldung bei einer AD-Domäne

Wenn Ihr Computer für die Authentifizierung bei Active Directory konfiguriert wurde und Sie über eine gültige Windows-Benutzeridentität verfügen, können Sie sich unter Verwendung der AD-Berechtigungen bei Ihrem Computer anmelden. Die Anmeldung ist über beide Desktop-Umgebungen (GNOME und KDE), die Konsole, SSH und eine beliebige andere PAM-fähige Anwendung möglich.

WICHTIG: Offline-Authentifizierung

openSUSE unterstützt die Offline-Authentifizierung, wodurch Sie bei Ihrem Client-Computer angemeldet bleiben, selbst wenn der Client-Computer vom Netzwerk getrennt wird. Dies ermöglicht Ihnen Mobilität bei der Arbeit, d. h., Sie können Ihre Arbeit fortsetzen, selbst wenn Sie sich in einem Flugzeug befinden und keine Netzwerkverbindung haben.

27.4.1 GDM und KDM

Zur Authentifizierung eines GNOME-Client-Computers bei einem AD-Server gehen Sie wie folgt vor:

- 1** Wählen Sie die Domäne aus.
- 2** Geben Sie Ihren Windows-Benutzernamen ein und drücken Sie die Eingabetaste.
- 3** Geben Sie Ihr Windows-Passwort ein und drücken Sie dann die Eingabetaste.

Zur Authentifizierung eines KDE-Client-Computers bei einem AD-Server gehen Sie wie folgt vor:

- 1** Wählen Sie die Domäne aus.
- 2** Geben Sie Ihren Windows-Benutzernamen ein.
- 3** Geben Sie Ihr Windows-Passwort ein und drücken Sie dann die Eingabetaste.

Mit der entsprechenden Konfiguration erstellt openSUSE bei der ersten Anmeldung jedes AD-authentifizierten Benutzers ein Home-Verzeichnis auf dem lokalen Computer. Dadurch können Sie die Vorteile der AD-Unterstützung von openSUSE nutzen und haben dennoch einen voll einsatzfähigen Linux-Computer zur Verfügung.

27.4.2 Konsolenanmeldung

Sie können sich über eine grafische Bedienoberfläche beim AD-Client-Computer anmelden oder stattdessen eine textbasierte Konsolenanmeldung oder sogar eine Fernanmeldung per SSH durchführen.

Für eine Konsolenanmeldung bei Ihrem AD-Client geben Sie *DOMÄNE\Benutzer* an der Eingabeaufforderung `login:` und anschließend das Passwort ein.

Zur entfernten Anmeldung bei Ihrem AD-Client-Computer mittels SSH gehen Sie wie folgt vor:

- 1 Geben Sie an der Eingabeaufforderung Folgendes ein:

```
ssh DOMAIN\\user@hostname
```

Kennzeichnen Sie das Domänen- und Anmeldetrennzeichen `\` durch ein weiteres `\`-Zeichen.

- 2 Geben Sie das Benutzerpasswort ein.

27.5 Ändern von Passwörtern

openSUSE kann einen Benutzer bei der Wahl eines geeigneten neuen Passworts, das die Sicherheitsrichtlinien des Unternehmens einhält, unterstützen. Das zugrundeliegende PAM-Modul ruft die aktuellen Einstellungen der Passwortsicherheitsrichtlinie vom Domain Controller ab. Es informiert bei der Anmeldung über die spezifischen Qualitätsanforderungen an das Passwort, die typischerweise für ein Benutzerkonto gelten. Wie seine Windows-Entsprechung zeigt openSUSE eine Meldung, die Folgendes beschreibt:

- Passwort-History-Einstellungen
- Geforderte Mindestlänge des Passworts
- Mindestalter des Passworts
- Passwortkomplexität

Eine Passwortänderung kann nur erfolgreich sein, wenn alle entsprechenden Anforderungen erfüllt wurden. Feedback über den Passwortstatus erhalten Sie über Anzeige-Manager und die Konsole.

GDM und KDM melden, wenn Ihr altes Passwort abgelaufen ist, und fordern Sie interaktiv zur Eingabe eines neuen Passworts auf. Zur Änderung von Passwörtern über die Anzeige-Manager geben Sie einfach die angeforderten Passwortinformationen ein.

Zur Änderung Ihres Windows-Passworts können Sie das standardmäßige Linux-Dienstprogramm, `passwd`, verwenden, anstatt diese Daten auf dem Server zu bearbeiten. Gehen Sie wie folgt vor, um Ihr NT-Passwort zu ändern:

- 1 Melden Sie sich an der Konsole an.
- 2 Geben Sie `passwd` ein.
- 3 Geben Sie Ihr aktuelles Passwort ein, wenn Sie dazu aufgefordert werden.
- 4 Geben Sie das neue Passwort ein.
- 5 Geben Sie das neue Passwort zur Bestätigung erneut ein. Wenn Ihr neues Passwort nicht den Richtlinien auf dem Windows-Server entspricht, werden Sie darüber informiert und zur Eingabe eines anderen Passworts aufgefordert.

Gehen Sie wie folgt vor, um Ihr Windows-Passwort am GNOME-Desktop zu ändern:

- 1 Klicken Sie auf das *Computer*-Symbol am linken Rand der Kontrollleiste.
- 2 Wählen Sie *Kontrollzentrum* aus.
- 3 Wählen Sie im Bereich *persönlich* die Option *Passwort ändern* aus.
- 4 Geben Sie das alte Paßwort ein.
- 5 Geben Sie das neue Passwort ein und bestätigen Sie es.
- 6 Schließen Sie dieses Dialogfeld mit *OK*, um Ihre Einstellungen anzuwenden.

Gehen Sie wie folgt vor, um Ihr Windows-Passwort am KDE-Desktop zu ändern:

- 1 Wählen Sie im Hauptmenü die Option *Persönliche Einstellungen* aus.
- 2 Wählen Sie *Sicherheit & Privatsphäre* aus.
- 3 Klicken Sie auf *Passwort & Benutzerkonto*.
- 4 Klicken Sie auf *Passwort ändern*.

- 5** Geben Sie Ihr aktuelles Passwort ein.
- 6** Geben Sie das neue Passwort ein, bestätigen Sie es und übernehmen Sie die Einstellungen mit *OK*.
- 7** Schließen Sie *Persönliche Einstellungen* mit *Datei > Beenden*.

Verteilte Nutzung von Dateisystemen mit NFS

28

Eine Möglichkeit, Dateien über das Netzwerk zu verteilen, ist NFS (Network File System). NFS greift auf Netzwerkinformationsdienste wie NIS (siehe [Kapitel 25, Arbeiten mit NIS](#) (S. 451)) oder Verzeichnisdienste wie LDAP (siehe [Kapitel 26, LDAP – Ein Verzeichnisdienst](#) (S. 461)) zurück, um festzustellen, wie die verfügbaren Dienste verwendet werden. Zur Verhinderung nicht autorisierter Zugriffe ermöglicht NFSv4 die Authentifizierung mit Kerberos (siehe auch [Kapitel 39, Installation und Administration von Kerberos](#) (S. 703)). Bei einer korrekten Konfiguration finden die Anwender unabhängig davon, an welchem Terminal sie angemeldet sind, stets die gleiche Umgebung vor.

Wie NIS ist NFS ein Client-Server-System. Ein Computer kann beides gleichzeitig sein – er kann Dateisysteme im Netzwerk zur Verfügung stellen (exportieren) und Dateisysteme anderer Hosts einhängen (importieren).

Im Prinzip können alle Exporte allein mit IP-Adressen vorgenommen werden. Es ist jedoch ratsam, über ein funktionierendes DNS-System zu verfügen, um Zeitüberschreitungen zu vermeiden. Dies ist zumindest für die Protokollierung erforderlich, weil der eingehängte Daemon Reverse-Lookups ausführt.

Für Netzwerkdienste ist die korrekte Einstellung der Systemzeit besonders wichtig. Wenn Sie die Einrichtung solcher Dienste planen, sollten Sie an erster Stelle auch an die Zeitsynchronisierung denken (siehe [Kapitel 24, Zeitsynchronisierung mit NTP](#) (S. 443)).

28.1 Konfiguration des NFS-Client

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.

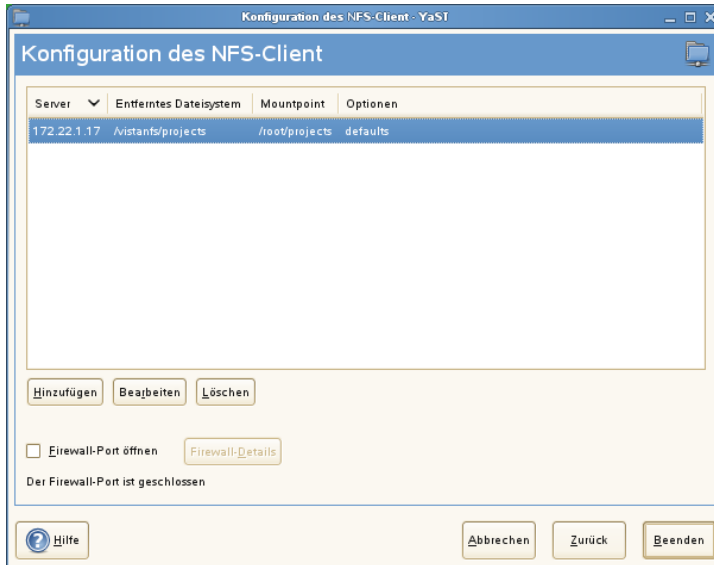
28.1.1 Importieren von Dateisystemen mit YaST

Autorisierte Benutzer können NFS-Verzeichnisse von NFS-Servern in ihre eigenen Dateibäume einhängen. Dies geschieht am einfachsten 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. Diese Eingaben werden im ersten Dialogfeld nach einem Klick auf *Hinzufügen* eingegeben. Aktivieren Sie *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 28.1, „Konfiguration des NFS-Clients mit YaST“](#) (S. 515).

Dadurch werden die Änderungen unter `/etc/fstab` gespeichert und die angegebenen Dateisysteme importiert. Wenn Sie den Client zu einem späteren Zeitpunkt starten, werden die Informationen von ihm aus dieser Datei gelesen.

Zur Zeit ist mit YaST noch kein Import von NFSv4-Dateisystemen möglich. Diese Dateisysteme könne manuell oder mit dem Automounter importiert werden. Erläuterungen hierzu finden Sie in [Abschnitt 28.1.3, „Manuelles Importieren von NFSv4-Dateisystemen“](#) (S. 516) und [Abschnitt 28.1.4, „Verwenden des Diensts zum automatischen Einhängen“](#) (S. 517).

Abbildung 28.1 Konfiguration des NFS-Clients mit YaST



28.1.2 Manuelles Importieren von NFSv3-Dateisystemen

Die einzige Voraussetzung für das Einhängen von NFSv3-Dateisystemen ist die Ausführung des RPC-Port Mapper. Diesen Dienst starten Sie durch Eingabe des Kommandos `rreportmap start` als `root`. 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 das Verzeichnis `/home` vom Computer `nfs.example.com` importiert werden soll, erstellen Sie zunächst ein lokales `/home`-Verzeichnis und geben Sie danach folgendes Kommando ein:

```
mount nfs.example.com:/home /home
```

28.1.3 Manuelles 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 `rpc.idmapd`. Überprüfen Sie den Status von `idmapd` durch Eingabe von `ps x | grep rpc.idmapd`.

Die `idmapd`-Dienste erhalten ihre Konfigurationsparameter aus der Datei `/etc/idmapd.conf`. Der Wert des Parameters `Domain` muss auf allen NFSv4-Servern und -Clients der Domäne identisch sein. Er kann zum Beispiel `localdomain` lauten. 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
```

Der Pfad des entfernten Dateisystems, der auf den Servernamen und einen Doppelpunkt folgt, wird immer 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 28.2, „Exportieren von Dateisystemen über NFS“](#) (S. 518) erläutert wird.

28.1.4 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:/
```

Stellen Sie sicher, dass `auto.nfs` mit dem Kommando `chmod 755 auto.nfs` ausgeführt werden kann. Aktivieren Sie die Einstellungen danach 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`.

28.1.5 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 Einhängepunkt angeben:

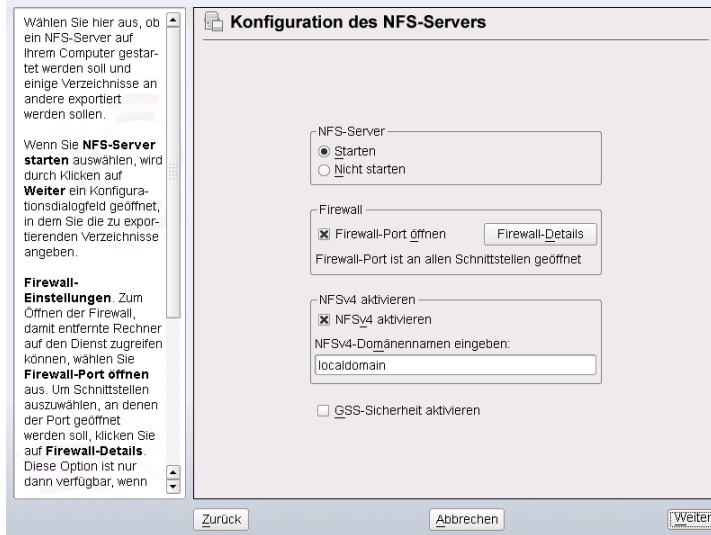
```
mount /local/path
```

Wenn die Option "noauto" nicht angegeben ist, wird das Einhängen dieser Dateisysteme beim Start durch die Initialisierungsskripten des Systems geregelt.

28.2 Exportieren von Dateisystemen über NFS

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 28.2, „Konfiguration des NFS-Servers“** (S. 519).

Abbildung 28.2 Konfiguration des NFS-Servers



Aktivieren Sie nun *NFS-Server: Start*. Wenn Sie NFSv4 verwenden möchten, aktivieren Sie *NFSv4 aktivieren* und geben Sie den *NFSv4-Domännennamen* ein. Der NFSv4-Domännennamen muss mit dem Domännennamen auf den Clients identisch sein, die mit dem Server verbunden werden sollen.

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 die Hosts fest, die auf die jeweiligen Verzeichnisse Zugriff erhalten sollen. Dieses Dialogfeld ist in **Abbildung 28.3, „Konfigurieren eines NFS-Servers mit YaST“** (S. 521) abgebildet. In der Abbildung wird das Szenario dargestellt, bei dem NFSv4 im vorherigen Dialogfeld aktiviert wurde.

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.

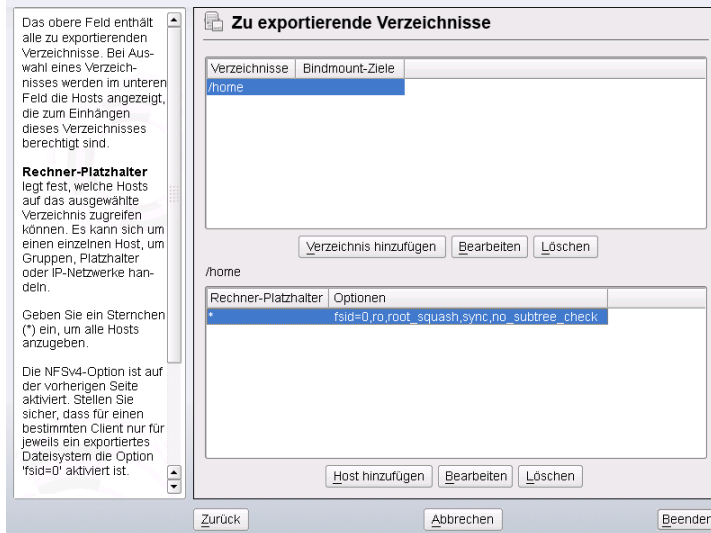
Nach dem Hinzufügen eines Verzeichnisses in der oberen Hälfte wird automatisch ein weiteres Dialogfeld zum Eingeben von Client- und Optionsinformationen geöffnet. Wenn Sie später einen oder auch mehrere neue Clients hinzufügen möchten, klicken Sie auf *Host hinzufügen*.

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. Diese Spalte kann nicht direkt bearbeitet werden. Sie enthält vielmehr eine Zusammenfassung der Verzeichnisse und deren Eigenschaften. Nachdem die Informationen vollständig sind, klicken Sie auf *Beenden*, um die Konfiguration abzuschließen, oder auf *Start*, um den Dienst neu zu starten.

Weitere Informationen zu den Optionen für den Verzeichnisexport finden Sie auf der man-Seite von `exports`. Klicken Sie zum Beenden der Konfiguration auf *Beenden*.

Abbildung 28.3 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.

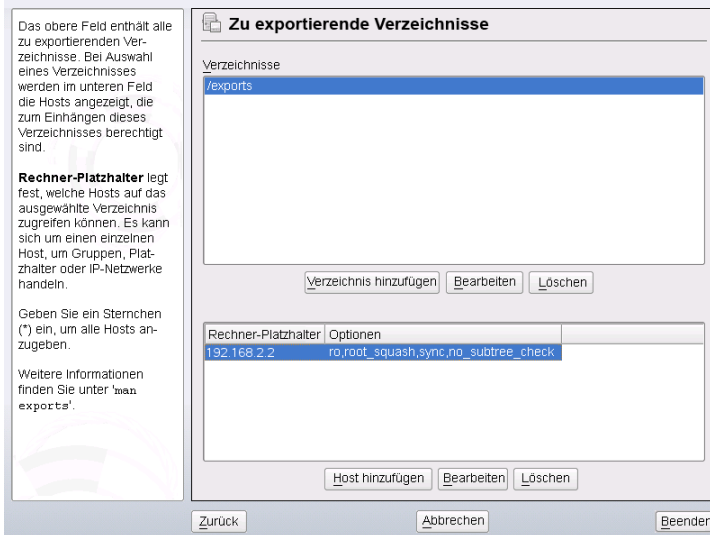
28.2.1 NFSv3- und NFSv2-Exporte

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 28.4**, „Exportieren von Verzeichnissen mit NFSv2 und v3“ (S. 522) abgebildet. Eine ausführlichere Erläuterung dieser Optionen finden Sie unter `man exports`. Klicken Sie zum Abschließen der Konfiguration auf *Beenden*.

Abbildung 28.4 Exportieren von Verzeichnissen mit NFSv2 und v3



28.2.2 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 28.3**, „Konfigurieren eines NFS-Servers mit YaST“ (S. 521) 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.

28.3 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.

28.3.1 Exportieren von Dateisystemen mit NFSv4

Für den Export von Dateisystemen mit NFSv4 sind einige spezielle Einstellungen erforderlich. Diese werden in den folgenden Abschnitten ausführlich behandelt.

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.

28.3.2 Exportieren von Dateisystemen mit NFSv2 und NFSv3

Dies gilt speziell für NFSv3- und NFSv2-Exporte. Informationen zum Exportieren mit NFSv4 finden Sie unter [Abschnitt 28.3.1, „Exportieren von Dateisystemen mit NFSv4“](#) (S. 523).

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.

28.4 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 Standardspeicherort 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 28.5, „Weiterführende Informationen“** (S. 527).

28.5 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.

Samba

Mit Samba kann ein Unix-Computer als Datei- und Druckserver für DOS-, Windows- und OS/2-Computer konfiguriert werden. Samba ist mittlerweile ein sehr umfassendes und komplexes Produkt. Konfigurieren Sie Samba mit YaST, SWAT (eine Web-Schnittstelle) oder der Konfigurationsdatei.

29.1 Terminologie

Im Folgenden werden einige Begriffe erläutert, die in der Samba-Dokumentation und im YaST-Modul verwendet werden.

SMB-Protokoll

Samba verwendet das SMB-Protokoll (Server Message Block), das auf den NetBIOS-Diensten basiert. Auf Drängen von IBM gab Microsoft das Protokoll frei, sodass auch andere Softwarehersteller Anbindungen an ein Microsoft-Domänen-netzwerk einrichten konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das TCP/IP-Protokoll installiert sein.

CIFS-Protokoll

Das CIFS-Protokoll (Common Internet File System) ist ein weiteres von Samba unterstütztes Protokoll. CIFS definiert ein Standardprotokoll für den Fernzugriff auf Dateisysteme über das Netzwerk, das Benutzergruppen die netzwerkweite Zusammenarbeit und gemeinsame Dokumentbenutzung ermöglicht.

NetBIOS

NetBIOS ist eine Softwareschnittstelle (API), die die Kommunikation zwischen Computern ermöglicht. Dabei wird ein Namensdienst bereitgestellt. Mit diesem Dienst können die an das Netzwerk angeschlossenen Computer Namen für sich reservieren. Nach dieser Reservierung können die Computer anhand ihrer Namen adressiert werden. Für die Überprüfung der Namen gibt es keine zentrale Instanz. Jeder Computer im Netzwerk kann beliebig viele Namen reservieren, solange die Namen noch nicht Gebrauch sind. Die NetBIOS-Schnittstelle kann in unterschiedlichen Netzwerkarchitekturen implementiert werden. Eine Implementierung, die relativ eng mit der Netzwerkhardware arbeitet, ist NetBEUI (häufig auch als NetBIOS bezeichnet). Mit NetBIOS implementierte Netzwerkprotokolle sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

Die per TCP/IP übermittelten NetBIOS-Namen haben nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun. NetBIOS ist ein eigener, vollständig unabhängiger Namensraum. Es empfiehlt sich jedoch, für einfachere Administration NetBIOS-Namen zu vergeben, die den jeweiligen DNS-Hostnamen entsprechen. Für einen Samba-Server ist dies die Voreinstellung.

Samba-Server

Samba-Server ist ein Server, der SMB/CIFS-Dienste sowie NetBIOS over IP-Namensdienste für Clients zur Verfügung stellt. Für Linux gibt es zwei Daemone für Samba-Server: `smnd` für SMB/CIFS-Dienste und `nmbd` für Namensdienste.

Samba-Client

Samba-Client ist ein System, das Samba-Dienste von einem Samba-Server über das SMB-Protokoll nutzt. Das Samba-Protokoll wird von allen gängigen Betriebssystemen wie Mac OS X, Windows und OS/2 unterstützt. Auf den Computern muss das TCP/IP-Protokoll installiert sein. Für die verschiedenen UNIX-Versionen stellt Samba einen Client zur Verfügung. Für Linux gibt es zudem ein Dateisystem-Kernel-Modul für SMB, das die Integration von SMB-Ressourcen auf Linux-Systemebene ermöglicht. Sie brauchen für Samba-Client keinen Daemon auszuführen.

Freigaben

SMB-Server stellen den Clients Plattenplatz in Form von Freigaben (Shares) zur Verfügung. Freigaben sind Drucker und Verzeichnisse mit ihren Unterverzeichnissen auf dem Server. Eine Freigabe wird unter einem eigenen Namen exportiert und kann von Clients unter diesem Namen angesprochen werden. Der Freigabename kann frei vergeben werden. Er muss nicht dem Namen des exportierten Verzeich-

nisses entsprechen. Ebenso wird einem Drucker ein Name zugeordnet. Clients können mit diesem Namen auf den Drucker zugreifen.

29.2 Installieren eines Samba-Servers

Zur Installation eines Samba-Servers starten Sie YaST und wählen Sie *Software > Software-Management* aus. Wählen Sie *Filter > Schemata* und schließlich *Dateiserver* aus. Bestätigen Sie die Installation der erforderlichen Pakete, um den Installationsvorgang abzuschließen.

29.3 Starten und Stoppen von Samba

Sie können den Samba-Server automatisch beim Booten oder manuell starten bzw. stoppen. Start- und Stopprichtlinien sind Teil der Samba-Serverkonfiguration mit YaST, die in [Abschnitt 29.4.1, „Konfigurieren eines Samba-Servers mit YaST“](#) (S. 532) beschrieben wird.

Um die Ausführung von Samba-Diensten mit YaST zu starten oder zu stoppen, verwenden Sie *System > Systemdienste (Runlevel)*. In der Kommandozeile stoppen Sie für Samba erforderliche Dienste mit `rcsmb stop && rcnmb stop` und starten sie mit `rcnmb start && rcsmb start`.

29.4 Konfigurieren eines Samba-Servers

Es gibt zwei Möglichkeiten, Samba-Server 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.

29.4.1 Konfigurieren eines Samba-Servers mit YaST

Um einen Samba-Server zu konfigurieren, starten Sie YaST und wählen Sie *Netzwerkdienste > Samba-Server*. Beim ersten Start des Moduls wird das Dialogfeld *Samba-Server-Installation* geöffnet, das Sie auffordert, ein paar grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen, und Sie am Ende der Konfiguration nach dem Passwort für Samba-root fragt. Bei späteren Starts wird das Dialogfeld *Samba-Server-Konfiguration* geöffnet.

Das Dialogfeld *Samba-Server-Installation* besteht aus zwei Teilen:

Arbeitsgruppe oder Domäne

Wählen Sie unter *Arbeitsgruppe oder Domäne* eine Arbeitsgruppe oder Domäne aus oder geben Sie eine neue ein und klicken Sie auf *Weiter*.

Samba-Servertyp

Geben Sie im nächsten Schritt an, ob Ihr Server als PDC fungieren soll, und klicken Sie auf *Weiter*.

Sie können später alle Einstellungen von *Samba-Server-Installation* im Dialogfeld *Samba-Server-Konfiguration* auf der Registerkarte *Identität* ändern.

Erweiterte Samba-Konfiguration mit YaST

Beim ersten Start des Samba-Servermoduls wird das Dialogfeld *Samba-Server-Konfiguration* unmittelbar nach dem Dialogfeld *Samba-Server-Installation* geöffnet. Hier passen Sie Ihre Samba-Server-Konfiguration an.

Nach dem Bearbeiten Ihrer Konfiguration klicken Sie auf *Verlassen*, um die Konfiguration abzuschließen.

Starten des Servers

Auf der Registerkarte *Start* können Sie den Start des Samba-Servers konfigurieren. Um den Dienst bei jedem Systemboot zu starten, wählen Sie *During Boot* (Beim Systemstart). Um den manuellen Start zu aktivieren, wählen Sie *Manually* (Manuell). Weitere Informationen zum Starten eines Samba-Servers erhalten Sie in [Abschnitt 29.3, „Starten und Stoppen von Samba“](#) (S. 531).

Auf dieser Registerkarte können Sie auch Ports in Ihrer Firewall öffnen. Wählen Sie hierfür *Open Port in Firewall* (Firewall-Port öffnen). Wenn mehrere Netzwerkschnittstellen vorhanden sind, wählen Sie die Netzwerkschnittstelle für Samba-Dienste, indem Sie auf *Firewall-Details* klicken, die Schnittstellen auswählen und dann auf *OK* klicken.

Freigaben

Legen Sie auf der Registerkarte *Freigaben* die zu aktivierenden Samba-Freigaben fest. Es gibt einige vordefinierte Freigaben wie Home-Verzeichnisse und Drucker. Mit *Status wechseln* können Sie zwischen den Statuswerten *Aktiviert* und *Deaktiviert* wechseln. Klicken Sie auf *Hinzufügen*, um neue Freigaben hinzuzufügen, bzw. auf *Löschen*, um die ausgewählte Freigabe zu entfernen.

Identität

Auf dem Karteireiter *Identität* legen Sie fest, zu welcher Domäne der Host gehört (*Grundeinstellungen*) und ob ein alternativer Hostname im Netzwerk (*NetBIOS-Hostname*) verwendet werden soll. Globale Einstellungen für Experten oder die Benutzerauthentifizierung können Sie festlegen, wenn Sie auf *Erweiterte Einstellungen* klicken.

29.4.2 Web-Administration mit SWAT

SWAT (Samba Web Administration Tool) ist ein alternatives Werkzeug für die Administrationsaufgaben von Samba. Es stellt eine einfache Webschnittstelle zur Verfügung, mit der Sie den Samba-Server konfigurieren können. Sie können SWAT verwenden, indem Sie in einem Webbrowser <http://localhost:901> aufrufen und sich als `root` anmelden. Wenn Sie über kein spezielles root-Konto für Samba verfügen, verwenden Sie das `root`-Systemkonto.

ANMERKUNG: Aktivieren von SWAT

Nach der Installation von Samba-Server ist SWAT nicht aktiviert. Um SWAT zu aktivieren, öffnen Sie in YaST *Netzwerkdienste > Netzwerkdienste (xinetd)*, wählen Sie *swat* aus der Tabelle und klicken Sie auf *Status wechseln (Ein oder Aus)*.

29.4.3 Manuelles Konfigurieren des Servers

Wenn Sie Samba als Server verwenden möchten, installieren Sie `samba`. Die Hauptkonfigurationsdatei von Samba ist `/etc/samba/smb.conf`. Diese Datei kann in zwei logische Bereiche aufgeteilt werden. Der Abschnitt `[global]` enthält die zentralen und globalen Einstellungen. Die Abschnitte `[share]` enthalten die einzelnen Datei- und Druckerfreigaben. Mit dieser Vorgehensweise können Details der Freigaben unterschiedlich oder im Abschnitt `[global]` übergreifend festgelegt werden. Letzteres trägt zur Übersichtlichkeit der Konfigurationsdatei bei.

Der Abschnitt "global"

Die folgenden Parameter im Abschnitt `[global]` sind den Gegebenheiten Ihres Netzwerkes anzupassen, damit Ihr Samba-Server in einer Windows-Umgebung von anderen Computern über SMB erreichbar ist.

`workgroup = TUX-NET`

Mit dieser Zeile wird der Samba-Server einer Arbeitsgruppe zugeordnet. Ersetzen Sie `TUX-NET` durch eine entsprechende Arbeitsgruppe Ihrer Netzwerkumgebung. Der Samba-Server erscheint mit seinem DNS-Namen, sofern der Name noch nicht vergeben ist. Wenn der DNS-Name nicht verfügbar ist, kann der Servername mithilfe von `netbiosname=MEINNAME` festgelegt werden. Weitere Informationen zu diesem Parameter finden Sie auf der Manualpage `mansmb.conf`.

`os level = 2`

Anhand dieses Parameters entscheidet Ihr Samba-Server, ob er versucht, LMB (Local Master Browser) für seine Arbeitsgruppe zu werden. Wählen Sie bewusst einen niedrigen Wert, damit ein vorhandenes Windows-Netz nicht durch einen falsch konfigurierten Samba-Server gestört wird. Weitere Informationen zu diesem wichtigen Thema finden Sie in den Dateien `BROWSING.txt` und `BROWSING-Config.txt` im Unterverzeichnis `textdocs` der Paketdokumentation.

Wenn im Netzwerk kein anderer SMB-Server (z. B. ein Windows NT- oder 2000-Server) vorhanden ist und der Samba-Server eine Liste aller in der lokalen Umgebung vorhandenen Systeme verwalten soll, setzen Sie den Parameter `os level` auf einen höheren Wert (z. B. 65). Der Samba-Server wird dann als LMB für das lokale Netzwerk ausgewählt.

Beim Ändern dieses Werts sollten Sie besonders vorsichtig sein, da dies den Betrieb einer vorhandenen Windows-Netzwerkumgebung stören könnte. Testen Sie Änderungen zuerst in einem isolierten Netzwerk oder zu unkritischen Zeiten.

wins support und wins server

Wenn Sie den Samba-Server in ein vorhandenes Windows-Netzwerk integrieren möchten, in dem bereits ein WINS-Server betrieben wird, aktivieren Sie den Parameter `wins server` und setzen Sie seinen Wert auf die IP-Adresse des WINS-Servers.

Sie müssen einen WINS-Server einrichten, wenn Ihre Windows-Systeme in getrennten Subnetzen betrieben werden und sich gegenseitig erkennen sollen. Um einen Samba-Server als WINS-Server festzulegen, setzen Sie die Option `wins support = Yes`. Stellen Sie sicher, dass diese Einstellung nur auf einem einzigen Samba-Server im Netzwerk aktiviert wird. Die Optionen `wins server` und `wins support` dürfen in der Datei `smb.conf` niemals gleichzeitig aktiviert sein.

Freigaben

In den folgenden Beispielen werden einerseits das CD-ROM-Laufwerk und andererseits die Verzeichnisse der Nutzer (`homes`) für SMB-Clients freigegeben.

[cdrom]

Um die versehentliche Freigabe eines CD-ROM-Laufwerks zu verhindern, sind alle erforderlichen Zeilen dieser Freigabe durch Kommentarzeichen (hier Semikolons) deaktiviert. Entfernen Sie die Semikolons in der ersten Spalte, um das CD-ROM-Laufwerk für Samba freizugeben.

Beispiel 29.1 *Eine CD-ROM-Freigabe*

```
;[cdrom]
;      comment = Linux CD-ROM
;      path = /media/cdrom
;      locking = No
```

[cdrom] und comment

Der Eintrag `[cdrom]` ist der Name der Freigabe, die von allen SMB-Clients im Netzwerk gesehen werden kann. Zur Beschreibung dieser Freigabe kann ein zusätzlicher `comment` hinzugefügt werden.

```
path = /media/cdrom
path exportiert das Verzeichnis /media/cdrom.
```

Diese Art der Freigabe ist aufgrund einer bewusst restriktiv gewählten Voreinstellung lediglich für die auf dem System vorhandenen Benutzer verfügbar. Soll die Freigabe für alle Benutzer bereitgestellt werden, fügen Sie der Konfiguration die Zeile `guest ok = yes` hinzu. Durch diese Einstellung erhalten alle Benutzer im Netzwerk Leseberechtigungen. Es wird empfohlen, diesen Parameter sehr vorsichtig zu verwenden. Dies gilt umso mehr für die Verwendung dieses Parameters im Abschnitt `[global]`.

`[homes]`

Eine besondere Stellung nimmt die Freigabe `[homes]` ein. Hat der Benutzer auf dem Linux-Dateiserver ein gültiges Konto und ein eigenes Home-Verzeichnis, so kann er eine Verbindung zu diesem herstellen.

Beispiel 29.2 *homes-Freigabe*

```
[homes]
comment = Home Directories
valid users = %S
browseable = No
read only = No
create mask = 0640
directory mask = 0750
```

`[homes]`

Insoweit keine ausdrückliche Freigabe mit dem Freigabenamen des Benutzers existiert, der die Verbindung zum SMB-Server herstellt, wird aufgrund der `[homes]`-Freigabe dynamisch eine Freigabe erzeugt. Dabei ist der Freigabename identisch mit dem Benutzernamen.

```
valid users = %S
```

`%S` wird nach erfolgreichem Verbindungsaufbau durch den konkreten Freigabennamen ersetzt. Bei einer `[homes]`-Freigabe ist dies immer der Benutzername. Aus diesem Grund werden die Zugriffsberechtigungen auf die Freigabe eines Benutzers immer exklusiv auf den Eigentümer des Benutzerverzeichnis beschränkt.

```
browseable = No
```

Durch diese Einstellung wird die Freigabe in der Netzwerkumgebung unsichtbar gemacht.

```
read only = No
```

Samba untersagt Schreibzugriff auf exportierte Freigaben standardmäßig mit dem Parameter `read only = Yes`. Soll also ein Verzeichnis als schreibbar freigegeben werden, muss der Wert `read only = No` festgesetzt werden, was dem Wert `writable = Yes` entspricht.

```
create mask = 0640
```

Nicht auf MS Windows NT basierende Systeme kennen das Konzept der Unix-Zugriffsberechtigungen nicht, sodass sie beim Erstellen einer Datei keine Berechtigungen zuweisen können. Der Parameter `create mask` legt fest, welche Zugriffsberechtigungen neu erstellten Dateien zugewiesen werden. Dies gilt jedoch nur für Freigaben mit Schreibberechtigung. Konkret wird hier dem Eigentümer das Lesen und Schreiben und den Mitgliedern der primären Gruppe des Eigentümers das Lesen erlaubt. `valid users = %S` verhindert den Lesezugriff auch dann, wenn die Gruppe über Leseberechtigungen verfügt. Um der Gruppe Lese- oder Schreibzugriff zu gewähren, deaktivieren Sie die Zeile `valid users = %S`.

Sicherheitsstufen (Security Levels)

Jeder Zugriff auf eine Freigabe kann für mehr Sicherheit durch ein Passwort geschützt werden. SMB kennt drei verschiedene Möglichkeiten der Berechtigungsprüfung:

Share Level Security (security = share)

Einer Freigabe wird ein Passwort fest zugeordnet. Jeder Benutzer, der dieses Passwort kennt, hat Zugriff auf die Freigabe.

User Level Security (security = user)

Diese Variante führt das Konzept des Benutzers in SMB ein. Jeder Benutzer muss sich bei einem Server mit einem Passwort anmelden. Nach der Authentifizierung kann der Server dann abhängig vom Benutzernamen Zugriff auf die einzelnen exportierten Freigaben gewähren.

Server Level Security (security = server):

Seinen Clients gibt Samba vor, im User Level Mode zu arbeiten. Allerdings übergibt es alle Passwortanfragen an einen anderen User Level Mode Server, der die Authentifizierung übernimmt. Diese Einstellung erwartet einen weiteren Parameter (`password server`).

Die Sicherheit auf Freigabe-, Benutzer- und Serverebene (Share, User und Server Level Security) gilt für den gesamten Server. Es ist nicht möglich, einzelne Freigaben einer Serverkonfiguration mit Share Level Security und andere mit User Level Security zu exportieren. Sie können jedoch auf einem System für jede konfigurierte IP-Adresse einen eigenen Samba-Server ausführen.

Weitere Informationen zu diesem Thema finden Sie in der Samba-HOWTO-Collection. Wenn sich mehrere Server auf einem System befinden, beachten Sie die Optionen `interfaces` und `bind interfaces only`.

29.5 Konfigurieren der Clients

Clients können auf den Samba-Server nur über TCP/IP zugreifen. NetBEUI oder NetBIOS über IPX können mit Samba nicht verwendet werden.

29.5.1 Konfigurieren eines Samba-Clients mit YaST

Konfigurieren Sie einen Samba-Client, um auf Ressourcen (Dateien oder Drucker) auf dem Samba-Server zuzugreifen. Geben Sie im Dialogfeld *Netzwerkdienste > Windows-Domänenmitgliedschaft* die Domäne oder Arbeitsgruppe an. Klicken Sie auf *Durchsuchen*, um alle verfügbaren Gruppen und Domänen anzuzeigen, und wählen Sie die gewünschte Gruppe bzw. Domäne mit einem Mausklick aus. Wenn Sie *Zusätzlich SMB-Informationen für Linux-Authentifikation verwenden* aktivieren, erfolgt die Benutzerauthentifizierung über den Samba-Server. Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *Verlassen*, um die Konfiguration abzuschließen.

29.5.2 Windows 9x und ME

Die Unterstützung für TCP/IP ist in Windows 9x und ME bereits integriert. Sie wird jedoch nicht standardmäßig installiert. Um TCP/IP zu installieren, wählen Sie *Systemsteuerung > System* und wählen Sie anschließend *Hinzufügen > Protokolle > TCP/IP von Microsoft*. Nach dem Neustart des Windows-Computers finden Sie den Samba-Server durch Doppelklicken auf das Desktopsymbol für die Netzwerkumgebung.

TIPP

Um einen Drucker auf dem Samba-Server zu nutzen, sollten Sie den Standard- oder den Apple-PostScript-Druckertreiber der entsprechenden Windows-Version installieren. Am besten verbinden Sie diesen anschließend mit der Linux-Druckwarteschlange, die PostScript als Eingabeformat akzeptiert.

29.6 Samba als Anmeldeserver

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich Benutzer nur mit einem gültigen Konto und zugehörigem Passwort anmelden dürfen. In einem Windows-basierten Netzwerk wird diese Aufgabe von einem Primary Domain Controller (PDC) übernommen. Sie können einen Windows NT-Server verwenden, der als PDC konfiguriert wurde, aber diese Aufgabe kann auch mithilfe eines Samba-Servers erfolgen. Es müssen Einträge im Abschnitt `[global]` von `smb.conf` vorgenommen werden. Diese werden in **Beispiel 29.3**, „Abschnitt `global`“ in `smb.conf`“ (S. 539) beschrieben.

Beispiel 29.3 Abschnitt `global` in `smb.conf`

```
[global]
workgroup = TUX-NET
domain logons = Yes
domain master = Yes
```

Wenn Sie verschlüsselte Passwörter zur Verifizierung verwenden (Standard bei gut verwalteten MS Windows 9x-Installationen, MS Windows NT 4.0 ab Service Pack 3 und allen späteren Produkten), müssen die Passwörter vom Samba-Server verarbeitet werden können. Dies wird durch den Eintrag `encrypt passwords = yes` im Abschnitt `[global]` aktiviert (ab Samba Version 3 ist dies Standard). Außerdem müssen die Benutzerkonten bzw. die Passwörter in eine Windows-konforme Verschlüsselungsform gebracht werden. Verwenden Sie hierfür den Befehl `smbpasswd -a name`. Da nach dem Windows NT-Domänenkonzept auch die Computer selbst ein Domänenkonto benötigen, wird dieses mit den folgenden Befehlen angelegt:

Beispiel 29.4 Einrichten eines Computerkontos

```
useradd hostname\%
smbpasswd -a -m hostname
```

Mit dem Befehl `useradd` wird ein Dollarzeichen hinzugefügt. Der Befehl `smbpasswd` fügt dieses bei der Verwendung des Parameters `-m` automatisch hinzu. In der kommentierten Beispielfunktion (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) sind Einstellungen enthalten, die diese Arbeiten automatisieren.

Beispiel 29.5 *Automatisiertes Einrichten eines Computerkontos*

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\%
```

Damit dieses Skript von Samba richtig ausgeführt werden kann, benötigen Sie noch einen Samba-Benutzer mit Administratorrechten. Fügen Sie hierzu der Gruppe `ntadmin` einen entsprechenden Benutzer hinzu. Anschließend können Sie allen Mitgliedern der Linux-Gruppe den Status `Domain Admin` zuweisen, indem Sie folgenden Befehl eingeben:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

Weitere Informationen zu diesem Thema finden Sie in Kapitel 12 der Samba-HOWTO-Collection (`/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`).

29.7 Weiterführende Informationen

Ausführliche Informationen zu Samba finden Sie in der digitalen Dokumentation. Wenn Samba installiert ist, können Sie in der Kommandozeile `apropos samba` eingeben, um einige `man`-Seiten aufzurufen. Alternativ dazu finden Sie im Verzeichnis `/usr/share/doc/packages/samba` weitere Online-Dokumentationen und Beispiele. Eine kommentierte Beispielfunktion (`smb.conf.SuSE`) finden Sie im Unterverzeichnis `examples`.

Das Samba-Team liefert in der Samba-HOWTO-Collection einen Abschnitt zur Fehlerbehebung. In Teil V ist außerdem eine ausführliche Anleitung zum Überprüfen der Konfiguration enthalten. Nach der Installation des Pakets `samba-doc` finden Sie die HOWTO-Informationen im Verzeichnis `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf`.

Detaillierte Informationen zu LDAP und der Migration von Windows NT oder 2000 finden Sie in `/usr/share/doc/packages/samba/examples/LDAP/smbldap-tools-*/doc`, wobei `*` Ihre `smbldap-tools`-Version ist.

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.

30.1 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.

30.1.1 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 20, Grundlegendes zu Netzwerken** (S. 339).

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 24, Zeit-synchronisierung mit NTP](#) (S. 443).
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 Webserver (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 35.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 660).

30.1.2 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 30.4, „Installieren, Aktivieren und Konfigurieren von Modulen“](#) (S. 563).

30.1.3 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 12.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 215).

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/>. Nun sollte eine Apache-Testseite mit folgendem Text geöffnet werden: „If you can see this, it means that the installation of the Apache Web server software on this system was successful (Wenn diese Seite angezeigt wird, wurde die Apache-Webserver-Software erfolgreich auf diesem System installiert).“ Wenn diese Seite nicht angezeigt wird, lesen Sie den Abschnitt **Abschnitt 30.8, „Fehlersuche“** (S. 584).

Nachdem der Webserver nun läuft, können Sie eigene Dokumente hinzufügen, die Konfiguration an Ihre Anforderungen anpassen und weitere Module mit den benötigten Funktionen installieren.

30.2 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 30.3, „Starten und Beenden von Apache“** (S. 561) beschrieben. Für die meisten Konfigurationsänderungen ist allerdings nur eine Aktualisierung mit `rcapache2 reload` erforderlich.

30.2.1 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. 550)).

`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 30.4, „Installieren, Aktivieren und Konfigurieren von Modulen“** (S. 563). Die Konfigurationsdateien optionaler Module befinden sich im Verzeichnis `conf.d`.

`server-tuning.conf`

Diese Datei enthält Konfigurationsdirektiven für verschiedene MPMs (siehe **Abschnitt 30.4.4, „Multiprocessing-Module“** (S. 568)) 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-Zertifikatsdaten. Weitere Informationen hierzu erhalten Sie unter **Abschnitt 30.6, „Einrichten eines sicheren Webservers mit SSL“** (S. 575).

`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. 549).

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. 557)) 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 30.1 *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 30.2 *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 30.3 *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 30.4 *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>
```

30.2.2 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 Einstellungen vornehmen. Nach Ausführung des Assistenten wird das unter „**HTTP-Server-Konfiguration**“ (S. 558) 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 Standardeinstellung 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

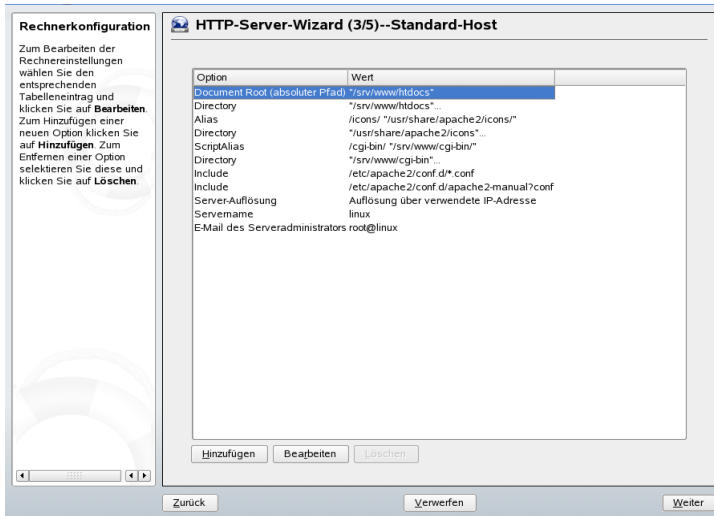
Mit dieser *Konfigurationsoption aktivieren bzw. deaktivieren Sie die vom Webserver unterstützten Skriptsprachen*. Informationen zur Aktivierung bzw. Deaktivierung anderer Module erhalten Sie unter „**Servermodule**“ (S. 560). Klicken Sie auf *Weiter*, um das nächste Dialogfeld zu öffnen.

Standardhost

Diese Option betrifft den Standard-Webserver. Wie in „**Virtuelle Hostkonfiguration**“ (S. 549) 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 30.1 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 Anzeigoptionen 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. 549)). 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 30.6.2, „Konfigurieren von Apache mit SSL“** (S. 581). 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.

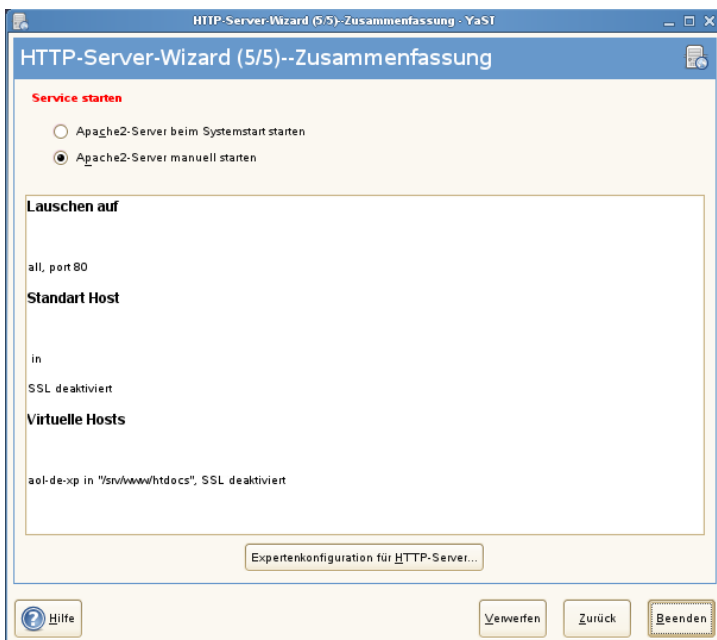
WICHTIG: Erstellen virtueller Hosts

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. 558) beschriebene Dialogfeld öffnen.

Abbildung 30.2 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 Konfigurations-

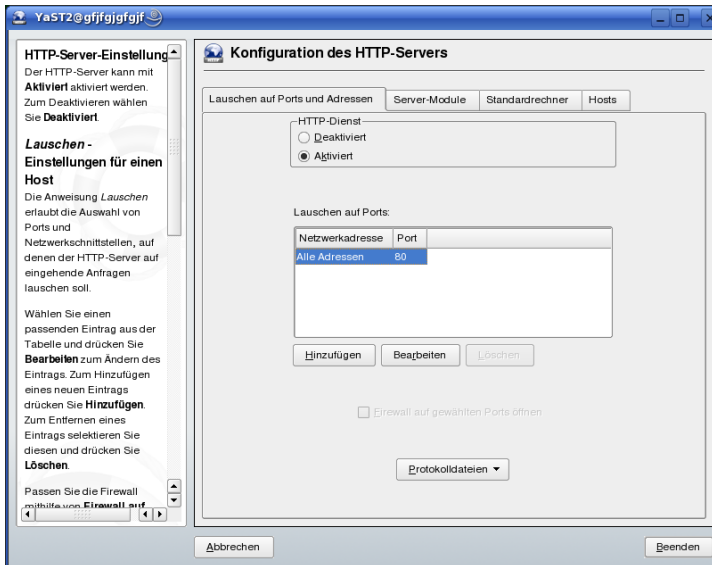
änderungen wird sofort wirksam. Die Änderungen werden erst wirksam, wenn Sie das Dialogfeld mit *Verlassen* schließen. Klicken Sie hingegen auf *Abbrechen*, so werden Ihre Konfigurationsänderungen verworfen.

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 30.3, „Starten und Beenden von Apache“** (S. 561)). Diese Befehle werden sofort ausgeführt.

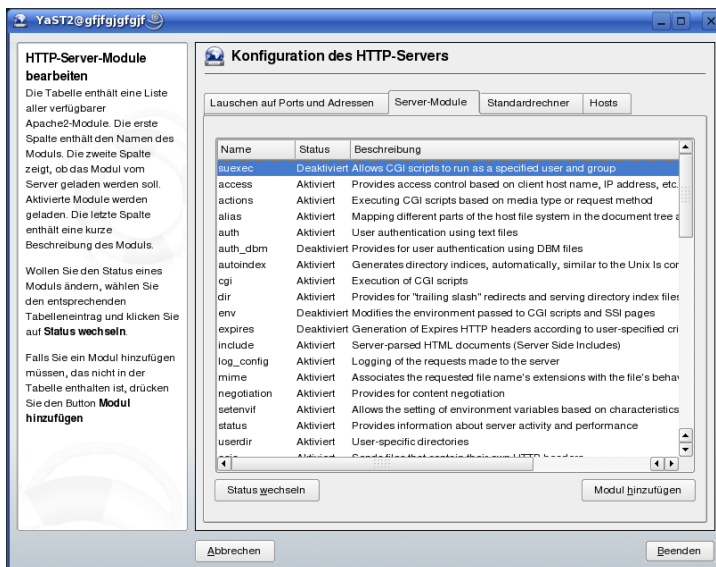
Abbildung 30.3 *Konfiguration des HTTP-Servers: Überwachen von Ports und Adressen*



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 30.4, „Installieren, Aktivieren und Konfigurieren von Modulen“** (S. 563).

Abbildung 30.4 Konfiguration des HTTP-Servers: Server-Module



Haupthost oder Hosts

Diese Dialogfelder sind mit den bereits beschriebenen identisch. in „Standardhost“ (S. 555) und „Virtuelle Hosts“ (S. 557) beschriebenen Dialogfeldern.

30.3 Starten und Beenden von Apache

Bei einer Konfiguration in YaST (siehe [Abschnitt 30.2.2, „Konfigurieren von Apache mit YaST“](#) (S. 554)) 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 12.2.2, „Init-Skripten“](#) (S. 211)). Der Befehl `rcapache2` akzeptiert folgende Parameter:

`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 30.6, „Einrichten eines sicheren Webservers mit SSL“](#) (S. 575).

`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`

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.

`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.

30.4 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 30.4.2, „Aktivieren und Deaktivieren von Modulen“](#) (S. 564).

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. open-SUSE 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.

30.4.1 Installieren von Modulen

Wenn Sie das Standardinstallationsverfahren für Apache durchgeführt haben (siehe [Abschnitt 30.1.2, „Installation“](#) (S. 544)), 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.

30.4.2 Aktivieren und Deaktivieren von Modulen

Die Skriptsprachenmodule PHP5, Perl, Python und Ruby können Sie in YaST mit der im [Abschnitt „HTTP-Server-Wizard“](#) (S. 554) beschriebenen Modulkonfiguration aktivieren oder deaktivieren. Alle anderen Module werden, wie im [Abschnitt „Servermodule“](#) (S. 560) 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`.

30.4.3 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`.

[<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 30.6, „Einrichten eines sicheren Webservers mit SSL“](#) (S. 575). 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.

30.4.4 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 Webservers 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.

30.4.5 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_fcgid`

`mod_fcgid` ist eine binäre, kompatible Alternative zu `mod_fastcgi`. Es ist eine sprachunabhängige, skalierbare Erweiterung zu CGI, die erstklassige Leistung ohne die Einschränkungen serverspezifischer APIs bietet. `mod_fcgid`-Anwendungen liegen persistent vor und sind daher äußerst schnell. Bei einer Anforderung kommt es zu keiner Verzögerung durch den Start und die Initialisierung der Anwendung.

Paketname: `apache2-mod_fcgid`

Konfigurationsdatei: `/etc/apache2/conf.d/mod_fcgid.conf`

Weitere Informationen: `/usr/share/doc/packages/apache2-mod_fastcgi`

`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_jk-ap20`

Dieses Modul stellt Konnektoren zwischen Apache und einem Tomcat Servlet-Container bereit.

Paketname: `mod_jk-ap20`

Weitere Informationen: `/usr/share/doc/packages/mod_jk-ap20`

30.4.6 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 von `apxs2` installierten Module können für alle MPMs verwendet werden. Die anderen beiden Programme installieren ihre Module so, dass sie nur für die jeweiligen

MPMs (also Prefork bzw. Worker) verwendet werden können. `apxs2` installiert seine Module in `/usr/lib/apache2`. `apxs2-prefork` und `apxs2-worker` installieren ihre Module hingegen in `/usr/lib/apache2-prefork` bzw. in `/usr/lib/apache2-worker`.

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.

30.5 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 30.4.2, „Aktivieren und Deaktivieren von Modulen“](#) (S. 564).

WARNUNG: CGI-Sicherheit

Die Zulassung der CGI-Skriptausführung auf dem Server ist ein Sicherheitsrisiko. Weitere Informationen finden Sie in [Abschnitt 30.7, „Vermeiden von Sicherheitsproblemen“](#) (S. 582).

30.5.1 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. 549)) und Ihre CGI-Skripten in einem Host-spezifischen Verzeichnis ablegen möchten, müssen Sie das betreffende Verzeichnis entsperren und für CGI-Skripten konfigurieren.

Beispiel 30.5 CGI-Konfiguration für VirtualHost

```
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.

30.5.2 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 30.7](#), „Vermeiden von Sicherheitsproblemen“ (S. 582)). 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.

30.5.3 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.

30.6 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://`).

30.6.1 Erstellen eines SSL-Zertifikats

Wenn Sie SSL/TLS 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 30.1 *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-Zertifikatssignierungsanforderung 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 Webserver eingeben. Dies macht den automatischen Start des Webserver beim Hochfahren des Computers oder einen Neustart des Webserver 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 unbekannten 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`.

30.6.2 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 35.4.1](#), „Konfigurieren der Firewall mit YaST“ (S. 660)).

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. 549).

Für den Anfang sollte es ausreichen, die Werte der folgenden Direktiven einzustellen:

- `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.

30.7 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.

30.7.1 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

30.7.2 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.

30.7.3 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. 552)). Achten Sie dabei darauf, dass keine unbefugten Personen auf kritische Dateien wie Passwort- oder Systemkonfigurationsdateien zugreifen können.

30.7.4 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.

30.7.5 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`).

30.8 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 30.3, „Starten und Beenden von Apache“](#) (S. 561)) 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 30.2.2, „Konfigurieren von Apache mit YaST“](#) (S. 554)). 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.

30.9 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 Befehl `yast -i 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.*`.

30.9.1 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>.

30.9.2 Apache Module

Weitere Informationen zu der in **Abschnitt 30.4.5, „Externe Module“** (S. 569) beschriebenen, externen Apache-Module finden Sie unter folgenden Adressen:

mod_apparmor

<http://en.opensuse.org/AppArmor>

mod_fcgid

<http://fastcgi.coremail.cn/>

mod_perl

<http://perl.apache.org/>

mod_php5

<http://www.php.net/manual/en/install.unix.apache2.php>

mod_python

<http://www.modpython.org/>

30.9.3 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/>

30.9.4 Verschiedene Informationsquellen

Wenn Sie in openSUSE Probleme mit Apache haben, werfen Sie einen Blick auf die openSUSE-Wiki unter <http://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

31

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.

vsftpd und pure-ftpd verfügen über leicht unterschiedliche Konfigurationsoptionen, besonders im Dialogfeld *Experteneinstellungen*. In diesem Kapitel werden die Einstellungen von vsftpd als Standardserver für openSUSE beschrieben.

Um den FTP-Server durch die Ausführung von YaST zu konfigurieren, wählen Sie *Netzwerkdienste > FTP-Server* aus. Wenn kein FTP-Server installiert ist, werden Sie gefragt, welcher Server installiert werden soll. Wählen Sie einen Server aus und bestätigen Sie den Dialog.

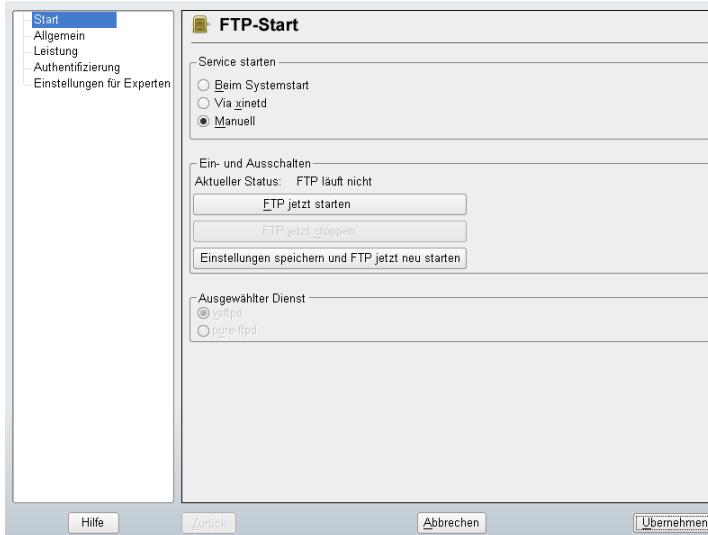
31.1 Starten des FTP-Servers

Im Bereich *Dienststart* des Dialogfelds *Start* können Sie die Art und Weise festlegen, 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 *Ein- und ausschalten* 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 auswählen. 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 31.1 *FTP-Serverkonfiguration - Start*



31.2 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.

Legen Sie unter *Umask for Anonymous* (Maske für anonyme Benutzer) und *Umask for Authenticated Users* (Maske für authentifizierte Benutzer) die Dateierstellungsmaske für anonyme bzw. autorisierte Benutzer fest.

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

pure-ftpd 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.

31.3 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.

31.4 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 authentifzierten 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 Sie möchten, dass anonyme Benutzer Dateien hochladen oder Verzeichnisse erstellen können, muss ein Unterverzeichnis mit Schreibberechtigung für alle Benutzer in diesem Verzeichnis erstellt werden.

31.5 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 *Passiver Modus* 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 for Pas. Mode* (Min.

Port für Pass.-Modus) und *Max Port for Pas Mode* (Max. Port für Pass.-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 entsprechenden 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.

31.6 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.

32.1 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.

Stromsparmodus (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 Lade-status 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.

32.2 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 32.2.4, „Fehlersuche“](#) (S. 605).

32.2.1 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 Netzsalters 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 `acpidmp`, `acpidisasm` und `dmdecode` gelesen werden. Diese Programme und ihre Dokumentation befinden sich im Paket `pmttools`. Beispiel: `acpidmp DSDT | acpidisasm`.

`/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 vollst ndigen Ladung mit der mit `state` angegebenen verbleibenden Ladung verglichen wird. Einfacher lässt sich der Ladezustand mit einem speziellen Programm ermitteln, das in [Abschnitt 32.2.3, „ACPI-Werkzeuge“](#) (S. 605) 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 32.2.3](#), „ACPI-Werkzeuge“ (S. 605).

32.2.2 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 32.4](#), „Das Powersave-Paket“ (S. 609) erläutert.

32.2.3 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`, `wmacpimon`, 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 `pmtools`).

32.2.4 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.

Überwachen Sie nach dem Booten die Bootmeldungen des Systems mit dem Befehl `dmesg | grep -zi 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 32.4.3, „Fehlersuche“](#) (S. 613) erläutert.

In der Kernel-Konfiguration gibt es einen Schalter zur Aktivierung der ACPI-Fehler-suchmeldungen. 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

Weitere Dokumentation und Hilfe zu ACPI:

- <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://acpi.sourceforge.net/> (das ACPI4Linux-Projekt von Sourceforge)
- <http://www.poupinou.org/acpi/> (DSDT-Patches von Bruno Ducrot)

32.3 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 moderenen 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 einen 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 Geräuscentwicklung 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 Kernel-Aktualisierungs-Daemon (kupdated) 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 kupdated kurze Intervalle festgelegt, um maximale Datenintegrität zu erreichen. Der Puffer wird alle 5 Sekunden überprüft und der bdfush-Daemon wird benachrichtigt, wenn Daten älter als 30 Sekunden sind oder der Puffer einen Füllstand von 30 % erreicht. Der bdfush-Daemon schreibt die Daten anschließend auf die Festplatte. Außerdem schreibt er unabhängig von kupdated, beispielsweise wenn der Puffer voll ist.

WARNUNG: Beeinträchtigung der Datenintegrität

Änderungen an den Einstellungen für den Kernel-Aktualisierungs-Daemon gefährden die Datenintegrität.

Abgesehen von diesen Prozessen schreiben protokollierende Journaling-Dateisysteme, wie ReiserFS und Ext3, ihre Metadaten unabhängig von bdfush, 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. Dies ist jedoch irrelevant, wenn das Intervall für kupdated erhöht wurde.

32.4 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`, `ospm` 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.

32.4.1 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
- Benachrichtigen
- 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.

32.4.2 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.

32.4.3 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.aml` an einen beliebigen Speicherort (`/etc/DSDT.aml` 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 Modulooption 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>.

32.4.4 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. Über Bluetooth können einzelne Systemkomponenten (Maus, Tastatur), periphere Geräte, Mobiltelefone, PDAs und einzelne Computer untereinander verbunden werden. IrDA wird in der Regel für die Kommunikation mit PDAs oder Mobiltelefonen verwendet. In diesem Kapitel werden diese drei Technologien und ihre Konfiguration vorgestellt.

33.1 Wireless LAN

Wireless LANs sind zu einem unverzichtbaren Aspekt der mobilen Computernutzung geworden. Heutzutage verfügen die meisten Notebooks über eingebaute WLAN-Karten. Standard 802.11 für die drahtlose Kommunikation mit WLAN-Karten wurde von der Organisation IEEE erarbeitet. Ursprünglich sah dieser Standard eine maximale Übertragungsrate von 2 MBit/s vor. Inzwischen wurden jedoch mehrere Ergänzungen hinzugefügt, um die Datenrate zu erhöhen. Diese Ergänzungen definieren Details wie Modulation, Übertragungsleistung und Übertragungsraten:

Tabelle 33.1 *Überblick über verschiedene WLAN-Standards*

Name	Band (GHz)	Maximale Übertragungsrate (MBit/s)	Hinweis
802.11	2.4	2	Veraltet; praktisch keine Endgeräte verfügbar
802.11b	2.4	11	Weit verbreitet
802.11a	5	54	Weniger üblich
802.11g	2.4	54	Rückwärtskompatibel mit 11b

Außerdem gibt es proprietäre Standards, beispielsweise die 802.11b-Variation von Texas Instruments mit einer maximalen Übertragungsrate von 22 MBit/s (manchmal als 802.11b+ bezeichnet). Die Karten, die diesen Standard verwenden, erfreuen sich allerdings nur begrenzter Beliebtheit.

33.1.1 Hardware

802.11-Karten werden von openSUSE® nicht unterstützt. Die meisten Karten, die 802.11a, 802.11b und 802.11g verwenden, werden unterstützt. Neuere Karten entsprechen in der Regel dem Standard 802.11g, Karten, die 802.11b verwenden, sind jedoch noch immer erhältlich. Normalerweise werden Karten mit folgenden Chips unterstützt:

- ADMTek ADM8211
- Aironet 4500, 4800
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Broadcom BCM43xx
- Intel PRO/Wireless 2100, 2200BG, 2915ABG, 3945ABG

- Intel Wireless WiFi Link 4965GN
- Intersil Prism2/2.5/3
- Intersil PrismGT
- Lucent/Agere Hermes
- Ralink RT2400, RT2500, RT2570, RT61, RT73
- Realtek RTL8187
- Texas Instruments ACX100, ACX111
- ZyDAS zd1201

Außerdem wird eine Reihe älterer Karten unterstützt, die nur noch selten verwendet werden und nicht mehr erhältlich sind. Eine umfangreiche Liste der WLAN-Karten und verwendeten Chips ist auf der Website von *AbsoluteValue Systems* unter http://www.linux-wlan.org/docs/wlan_adapters.html.gz verfügbar. Einen Überblick über die verschiedenen WLAN-Chips finden Sie unter <http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz>.

Einige Karten benötigen ein Firmware-Image, das bei der Initialisierung des Treibers in die Karte geladen werden muss. Dies ist der Fall bei Intersil PrismGT, Atmel und TI ACX100 and ACX111. Die Firmware kann problemlos mit dem YaST-Online-Update installiert werden. Die Firmware für Intel PRO/Wireless-Karten ist im Lieferumfang von openSUSE enthalten und wird automatisch von YaST installiert, sobald eine Karte dieses Typs gefunden wurde. Weitere Informationen zu diesem Thema finden Sie im installierten System unter `/usr/share/doc/packages/wireless-tools/README.firmware`.

33.1.2 Funktion

Bei der Arbeit mit drahtlosen Netzwerken werden verschiedene Verfahren und Konfigurationen verwendet, um schnelle, qualitativ hochwertige und sichere Verbindungen herzustellen. Verschiedene Betriebstypen passen zu verschiedenen Einrichtungen. Die Auswahl der richtigen Authentifizierungsmethode kann sich schwierig gestalten. Die verfügbaren Verschlüsselungsmethoden weisen unterschiedliche Vor- und Nachteile auf.

Betriebsmodus

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.

Da ein drahtloses Netzwerk wesentlich leichter abgehört und manipuliert werden kann als ein Kabelnetzwerk, beinhalten die verschiedenen Standards Authentifizierungs- und Verschlüsselungsmethoden. In der ursprünglichen Version von Standard IEEE 802.11 werden diese Methoden unter dem Begriff WEP beschrieben. Da sich WEP jedoch als unsicher herausgestellt hat (siehe „Sicherheit“ (S. 627)), hat die WLAN-Branche (gemeinsam unter dem Namen *Wi-Fi Alliance*) die neue Erweiterung WPA definiert, bei dem die Schwächen von WEP ausgemerzt sein sollen. Der spätere Standard IEEE 802.11i (auch als WPA2 bezeichnet, da WPA auf einer Entwurfsfassung von 802.11i beruht) beinhaltet WPA sowie einige andere Authentifizierungs- und Verschlüsselungsmethoden.

Authentifizierung

Um sicherzugehen, dass nur authentifizierte Stationen eine Verbindung herstellen können, werden in verwalteten Netzwerken verschiedene Authentifizierungsmechanismen verwendet.

Geöffnet

Ein offenes System ist ein System, bei dem keinerlei Authentifizierung erforderlich ist. Jede Station kann dem Netzwerk beitreten. Dennoch kann WEP-Verschlüsselung (siehe „Verschlüsselung“ (S. 622)) verwendet werden.

Gemeinsamer Schlüssel (gemäß IEEE 802.11)

In diesem Verfahren wird der WEP-Schlüssel zur Authentifizierung verwendet. Dieses Verfahren wird jedoch nicht empfohlen, da es den WEP-Schlüssel anfälliger für Angriffe macht. Angreifer müssen lediglich lang genug die Kommunikation

zwischen Station und Zugriffspunkt abhören. Während des Authentifizierungsvorgangs tauschen beide Seiten dieselben Informationen aus, einmal in verschlüsselter, und einmal in unverschlüsselter Form. Dadurch kann der Schlüssel mit den geeigneten Werkzeugen rekonstruiert werden. Da bei dieser Methode der WEP-Schlüssel für Authentifizierung und Verschlüsselung verwendet wird, wird die Sicherheit des Netzwerks nicht erhöht. Eine Station, die über den richtigen WEP-Schlüssel verfügt, kann Authentifizierung, Verschlüsselung und Entschlüsselung durchführen. Eine Station, die den Schlüssel nicht besitzt, kann keine empfangenden Pakete entschlüsseln. Sie kann also nicht kommunizieren, unabhängig davon, ob sie sich authentifizieren musste.

WPA-PSK (gemäß IEEE 802.1x)

WPA-PSK (PSK steht für "preshared key") funktioniert ähnlich wie das Verfahren mit gemeinsamen Schlüssel. Alle teilnehmenden Stationen sowie der Zugriffspunkt benötigen denselben Schlüssel. Der Schlüssel ist 256 Bit lang und wird normalerweise als Passwortsatz eingegeben. Dieses System benötigt keine komplexe Schlüsselverwaltung wie WPA-EAP und ist besser für den privaten Gebrauch geeignet. Daher wird WPA-PSK zuweilen als WPA "Home" bezeichnet.,“

WPA-EAP (gemäß IEEE 802.1x)

Eigentlich ist WPA-EAP kein Authentifizierungssystem, sondern ein Protokoll für den Transport von Authentifizierungsinformationen. WPA-EAP dient zum Schutz drahtloser Netzwerke in Unternehmen. Bei privaten Netzwerken wird es kaum verwendet. Aus diesem Grund wird WPA-EAP zuweilen als WPA „Enterprise“ bezeichnet.

WPA-EAP benötigt einen Radius-Server zur Authentifizierung von Benutzern. EAP bietet drei verschiedene Methoden zum Verbinden und Authentifizieren des Servers: TLS (Transport Layer Security), TTLS (Tunneled Transport Layer Security) und PEAP (Protected Extensible Authentication Protocol). Kurz gesagt, funktionieren diese Optionen wie folgt:

EAP-TLS

TLS-Authentifizierung beruht auf dem gegenseitigen Austausch von Zertifikaten für Server und Client. Zuerst legt der Server sein Zertifikat dem Client vor, der es auswertet. Wenn das Zertifikat als gültig betrachtet wird, legt im Gegenzug der Client sein eigenes Zertifikat dem Server vor. TLS ist zwar sicher, erfordert jedoch eine funktionierende Infrastruktur zur Zertifikatsverwaltung im Netzwerk. Diese Infrastruktur ist in privaten Netzwerken selten gegeben.

EAP-TTLS und PEAP

TTLS und PEAP sind zweistufige Protokolle. In der ersten Stufe wird eine sichere Verbindung hergestellt und in der zweiten werden die Daten zur Client-Authentifizierung ausgetauscht. Sie erfordern einen wesentlich geringeren Zertifikatsverwaltungs-Overhead als TLS, wenn überhaupt.

Verschlüsselung

Es gibt verschiedene Verschlüsselungsmethoden, mit denen sichergestellt werden soll, dass keine nicht autorisierten Personen die in einem drahtlosen Netzwerk ausgetauschten Datenpakete lesen oder Zugriff auf das Netzwerk erlangen können:

WEP (in IEEE 802.11 definiert)

Dieser Standard nutzt den Verschlüsselungsalgorithmus RC4, der ursprünglich eine Schlüssellänge von 40 Bit aufwies, später waren auch 104 Bit möglich. Die Länge wird häufig auch als 64 Bit bzw. 128 Bit angegeben, je nachdem, ob die 24 Bit des Initialisierungsvektors mitgezählt werden. Dieser Standard weist jedoch eigene Schwächen auf. Angriffe gegen von diesem System erstellte Schlüssel können erfolgreich sein. Nichtsdestoweniger ist es besser, WEP zu verwenden, als das Netzwerk überhaupt nicht zu verschlüsseln.

TKIP (in WPA/IEEE 802.11i definiert)

Dieses im WPA-Standard definierte Schlüsselverwaltungsprotokoll verwendet denselben Verschlüsselungsalgorithmus wie WEP, weist jedoch nicht dessen Schwächen auf. Da für jedes Datenpaket ein neuer Schlüssel erstellt wird, sind Angriffe gegen diese Schlüssel vergebens. TKIP wird in Verbindung mit WPA-PSK eingesetzt.

CCMP (in IEEE 802.11i definiert)

CCMP beschreibt die Schlüsselverwaltung. Normalerweise wird sie in Verbindung mit WPA-EAP verwendet, sie kann jedoch auch mit WPA-PSK eingesetzt werden. Die Verschlüsselung erfolgt gemäß AES und ist stärker als die RC4-Verschlüsselung des WEP-Standards.

33.1.3 Konfiguration mit YaST

Um Ihre WLAN-Karte zu konfigurieren, starten Sie das YaST-Modul *Netzwerkkarte*. Hier können Sie auch angeben, ob YaST oder der NetworkManager für die Verwaltung der Netzwerkkarte verwendet werden soll. Wenn Sie YaST auswählen, wählen Sie

unter *Konfiguration der Netzwerkadresse* den Gerätetyp *Drahtlos* aus und klicken Sie auf *Weiter*. Nehmen Sie unter *Konfiguration der drahtlosen Netzwerkkarte* (siehe **Abbildung 33.1**, „YaST: Konfigurieren der WLAN-Karte“ (S. 623)) die Grundeinstellungen für den WLAN-Betrieb vor:

Abbildung 33.1 YaST: Konfigurieren der WLAN-Karte

Nehmen Sie hier die wichtigsten Einstellungen für Funknetzwerke vor.

Der **Betriebsmodus** hängt von der Netzwerktopologie ab. Es gibt den Modus **Ad-hoc** (Peer-to-Peer-Netzwerk ohne Zugriffspunkt), **Verwaltet** (das Netzwerk versorgt von einem Zugriffspunkt, bisweilen wird das auch *Infrastrukturmodus* genannt) oder **Master** (die Netzwerkkarte fungiert als Zugriffspunkt).

Legen Sie den Netzwerknamen (ESSID) fest, der zum Identifizieren von Zellen verwendet wird, die Teil desselben virtuellen Netzwerks sind. Alle Stationen in einem Funk-LAN benötigen dieselbe ESSID zur Kommunikation untereinander. Wenn Sie den Betriebsmodus **Verwaltet**

Konfiguration der drahtlosen Netzwerkkarte

Einstellungen für Funkgeräte

Betriebsmodus
Verwaltet

Netzwerkname (ESSID)
[]

Authentifizierungsmodus
WEP - Offen

Schlüsseleingabetyp
☒ Passwortsatz ☐ ASCII ☐ Hexadezimal

Verschlüsselungs-Key
[]

[Einstellungen für Experten...] [WEP-Schlüssel]

[Zurück] [Abbrechen] [Weiter]

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 geeignete Authentifizierungsmethode für Ihr Netzwerk: *Open*, *Shared Key*, *WPA-PSK* oder *WPA-EAP*. Bei Auswahl der WPA-Authentifizierung, muss ein Netzwerkname festgelegt werden.

Einstellungen für Experten

Mit dieser Schaltfläche wird ein Dialogfeld für die detaillierte Konfiguration der WLAN-Verbindung geöffnet. Eine detaillierte Beschreibung dieses Dialogfelds finden Sie weiter unten.

Nach Abschluss der Grundeinstellungen kann die Station im WLAN bereitgestellt werden.

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. Weitere Informationen hierzu erhalten Sie in „**Verschlüsselung**“ (S. 622) und „**Sicherheit**“ (S. 627).

Je nach der ausgewählten Authentifizierungsmethode werden Sie von YaST aufgefordert, eine Feinabstimmung der Einstellungen in einem anderen Dialogfeld vorzunehmen. Bei *Offen* ist keinerlei Konfigurierung erforderlich, da diese Einstellung unverschlüsselten Betrieb ohne Authentifizierung implementiert.

Gemeinsam genutzter Schlüssel

Legen Sie die Art der Schlüsseleingabe fest. Zur Auswahl stehen *Passwortsatz*, *ASCII* und *Hexadezimal*. Bis zu vier verschiedene Schlüssel zur Verschlüsselung der übertragenen Daten sind zulässig. Klicken Sie auf *WEP-Schlüssel*, um das Dialogfeld zur Schlüsselkonfiguration aufzurufen. Legen Sie die Länge des Schlüssels fest: *128 Bit* oder *64 Bit*. Die Standardeinstellung ist *128 Bit*. Im Listebereich 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.

WPA-EAP

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 nach allen Zertifikaten unter `/etc/cert`. Daher müssen Sie die erhaltenen Zertifikate in diesem Verzeichnis speichern und den Zugriff auf die Dateien auf `0600` (Lesen und Schreiben nur für Eigentümer) beschränken.

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.

Klicken Sie auf *Einstellungen für Experten*, um das Dialogfeld für die Grundkonfiguration der WLAN-Verbindung zu verlassen und die Konfiguration für Experten einzugeben. In diesem Dialogfeld sind folgende Optionen verfügbar:

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 Energiespartetechnologien maximieren. Weitere Informationen über die Energieverwaltung finden Sie in **Kapitel 32, *Energieverwaltung*** (S. 597).

33.1.4 Dienstprogramme

hostap (Paket `hostap`) wird zum Betrieb einer WLAN-Karte als Zugriffspunkt verwendet. Weitere Informationen zu diesem Paket finden Sie auf der Homepage des Projekts (<http://hostap.epitest.fi/>).

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.

33.1.5 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 Übertragungsreichweite 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.

33.1.6 Fehlersuche

Wenn Ihre WLAN-Karte nicht reagiert, überprüfen Sie, ob Sie die benötigte Firmware heruntergeladen haben. Weitere Informationen finden Sie unter [Abschnitt 33.1.1, „Hardware“](#) (S. 618). In den folgenden Abschnitten werden einige bekannte Probleme behandelt.

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`.

33.1.7 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.

33.2 Bluetooth

Bluetooth ist eine drahtlose Technologie für den Anschluss verschiedener Geräte, wie beispielsweise Mobiltelefone, PDAs, Notebooks oder Systemkomponenten wie Tastatur oder Maus. Der Name leitet sich vom dänischen König Harald Blauzahn (engl. Name Harold Bluetooth) ab, der mehrere sich bekriegende Fraktionen in Skandinavien einte. Das Bluetooth-Logo basiert auf den Runen für „H“ (sternähnlich) und „B“.

Bluetooth unterscheidet sich durch eine Reihe wichtiger Aspekte von IrDA. Zum einen müssen sich die einzelnen Geräte nicht in optischer Reichweite voneinander befinden und zum anderen können mehrere Geräte zu einem Netzwerk zusammengeschlossen werden. „Die maximale Datenübertragungsrate beträgt allerdings nur 2.1 Mbps (in der aktuellen Version 2.0). Theoretisch ist mit Bluetooth sogar eine Kommunikation durch Wände möglich. In der Praxis hängt dies jedoch von den Eigenschaften der Wand und der Geräteklasse ab. Es gibt drei Geräteklassen mit Übertragungsbereichen zwischen zehn und hundert Metern.

33.2.1 Grundlagen

In den folgenden Abschnitten werden die Grundprinzipien umrissen, nach denen Bluetooth funktioniert. Sie erfahren, welche Software-Anforderungen erfüllt sein müssen, wie Bluetooth mit dem System interagiert und wie Bluetooth-Profiles funktionieren.

Software

Zur Verwendung von Bluetooth benötigen Sie einen Bluetooth-Adapter (eingebauter Adapter oder externes Gerät), Treiber sowie einen Bluetooth-Protokollstapel. Der Linux-Kernel weist bereits die wichtigsten Treiber für die Verwendung von Bluetooth auf. Das BlueZ-System wird als Protokollstapel verwendet. Um sicherzustellen, dass die Anwendungen mit Bluetooth zusammenarbeiten, müssen die Basispakete `bluez-libs` und `bluez-utils` installiert sein. Diese Pakete enthalten mehrere benötigte Dienste und Dienstprogramme. Außerdem muss für einige Adapter, wie Broadcom bzw. AVM BlueFritz!, das Paket `bluez-firmware` installiert sein. Das Paket `bluez-cups` ermöglicht das Drucken über Bluetooth-Verbindungen. Für die Fehlersuche bei Problemen mit Bluetooth-Verbindungen installieren Sie die Pakete `bluez-hcidump` und `bluez-test`.

Allgemeines Zusammenspiel

Bluetooth-Systeme bestehen aus vier miteinander verzahnten Schichten, die die gewünschte Funktionalität bereitstellen:

Hardware

Adapter und geeigneter Treiber zur Unterstützung durch den Linux-Kernel.

Konfigurationsdateien

Dienen zur Steuerung des Bluetooth-Systems.

Daemons

Dienste, die von den Konfigurationsdateien gesteuert werden und die Funktionalität bereitstellen.

Anwendungen

Durch die Anwendungen kann der Benutzer die von den Daemons bereitgestellte Funktionalität nutzen und steuern.

Beim Einstecken eines Bluetooth-Adapters wird der zugehörige Treiber in das Hotplug-System geladen. Nachdem der Treiber geladen wurde, überprüft das System die Konfigurationsdateien, um zu ermitteln, ob Bluetooth gestartet werden sollte. Wenn dies der Fall ist, wird ermittelt, welche Dienste gestartet werden sollen. Auf der Grundlage dieser Informationen werden die entsprechenden Daemons gestartet.

Profile

In Bluetooth werden die Dienste über Profile definiert, beispielsweise das Dateiübertragungsprofil, das Profil für grundlegende Druckvorgänge und das Profil für das persönliche Netzwerk (Personal Area Network). Damit ein Gerät die Dienste eines anderen Gerätes nutzen kann, müssen beide dasselbe Profil verstehen. Diese Information fehlt häufig auf der Verpackung und im Handbuch des Geräts. Leider halten sich einige Hersteller nicht streng an die Definitionen der einzelnen Profile. Dennoch funktioniert die Kommunikation zwischen den Geräten normalerweise reibungslos.

Im folgenden Text sind die lokalen Geräte diejenigen, die physisch mit dem Computer verbunden sind. Alle anderen Geräte, auf die nur über drahtlose Verbindungen zugegriffen werden kann, werden als entfernte Geräte bezeichnet.

33.2.2 Konfiguration

Dieser Abschnitt bietet eine Einführung in die Bluetooth-Konfiguration. Sie erfahren, welche Konfigurationsdateien beteiligt sind, welche Werkzeuge benötigt werden und wie Bluetooth konfiguriert wird.

Die Konfigurationsdateien für die einzelnen Komponenten des Bluez-Systems befinden sich im Verzeichnis `/etc/bluetooth`. Die einzige Ausnahme hiervon ist die Datei `/etc/sysconfig/bluetooth`, die die Komponenten startet.

Die im Folgenden beschriebenen Konfigurationsdateien können nur vom Benutzer `root` bearbeitet werden. Zurzeit gibt es keine grafische Bedienoberfläche zum Ändern aller Einstellungen. Die meisten dieser Einstellungen sind allerdings nur für erfahrene Benutzer mit speziellen Anwendungsfällen interessant. Normalerweise sollten die Standardeinstellungen angemessen sein.

Verschiedene Einstellungen, beispielsweise Gerätenamen und Sicherheitsmodus, können in der Konfigurationsdatei `/etc/bluetooth/hcid.conf` geändert werden. Normalerweise sollten die Standardeinstellungen angemessen sein. Die Datei enthält Kommentare, in denen die Optionen für die verschiedenen Einstellungen beschrieben werden. Die meisten Einstellungen dieser Datei können jedoch auch mit `kbluetooth` oder `bluez-gnome` festgelegt werden.

Zwei Abschnitte in der eingeschlossenen Datei heißen `options` und `device`. Der erste enthält allgemeine Informationen, die `hcid` zum Starten verwendet. Der zweite enthält Einstellungen für einzelne lokale Bluetooth-Geräte.

Eine der wichtigsten Einstellungen im Abschnitt `options` ist `security auto;`. Wenn dieser Wert auf `auto` gesetzt ist, versucht `hcid`, die lokale PIN für eingehende Verbindungen zu verwenden. Wenn dies nicht erfolgreich ist, wird auf `none` umgeschaltet und die Verbindung ohne PIN hergestellt. Um eine höhere Sicherheit zu erreichen, sollte diese Standardeinstellung auf `user` gesetzt werden, um sicherzustellen, dass der Benutzer jedes Mal, wenn eine Verbindung hergestellt wird, eine PIN eingeben muss.

Legen Sie den Namen, unter dem der Computer auf der anderen Seite angezeigt wird, im Abschnitt `device` fest. Die Geräteklasse, beispielsweise `Desktop`, `Laptop` oder `Server` wird in diesem Abschnitt definiert. Authentifizierung und Verschlüsselung werden ebenfalls hier aktiviert bzw. deaktiviert.

33.2.3 Systemkomponenten und Dienstprogramme

Die Funktionsfähigkeit von Bluetooth hängt vom Zusammenspiel verschiedener Dienste ab. `hcid` (Host Controller Interface Daemon) fungiert als Schnittstelle für das Bluetooth-Gerät, über die das Gerät gesteuert wird. `hcid` stellt auch den `sdpsd`-Daemon (Service Discovery Protocol Daemon) bereit, mit dessen Hilfe ein Gerät die auf dem Host bereitgestellten Dienste erkennt. `hcid` wird automatisch beim Systemstart oder beim Einstecken des Bluetooth-Adapters am System aktiviert. Falls `hcid` nicht automatisch gestartet wird, können Sie das Bluetooth-Subsystem manuell mit `rcbluetooth start` starten. Dieser Befehl muss als `root` ausgeführt werden.

In den folgenden Absätzen werden kurz die wichtigsten Shell-Werkzeuge beschrieben, die für die Arbeit mit Bluetooth verwendet werden können. Mittlerweile stehen zwar verschiedene grafische Komponenten für die Steuerung von Bluetooth zur Verfügung, aber dennoch kann es sich lohnen, einen Blick auf diese Programme zu werfen.

Einige der Kommandos können nur als `root` ausgeführt werden. Dazu gehört das Kommando `l2ping device_address` zum Testen der Verbindung mit einem entfernten Gerät.

hcitool

Mit `hcitool` kann bestimmt werden, ob lokale und entfernte Geräte erkannt wurden. Mit dem Kommando `hcitool dev` werden die lokalen Geräte aufgeführt. Für jedes erkannte lokale Gerät wird in der Ausgabe eine Zeile in der Form *Schnittstellename Geräteadresse* erstellt.

Nach entfernten Geräten wird mit dem Kommando `hcitool inq` gesucht. Dieses Kommando gibt für jedes erkannte Gerät drei Werte zurück: die Geräteadresse, die Uhrzeitverschiebung und die Geräteklasse. Die Geräteklasse ist wichtig, da andere Befehle sie zur Ermittlung des Zielgeräts verwenden. Das Uhren-Offset dient hauptsächlich technischen Zwecken. Die Klasse gibt Geräte- und Dienstyp als Hexadezimalwert an.

Mit `hcitool name Geräteadresse` kann der Gerätenamen eines entfernten Geräts ermittelt werden. Bei einem entfernten Computer entsprechen Klasse und Gerätenamen

den Informationen in der Datei `/etc/bluetooth/hcid.conf`. Lokale Geräteadressen führen zu einer Fehlerausgabe.

hciconfig

Der Befehl `/usr/sbin/hciconfig` liefert weitere Informationen zum lokalen Gerät. Wenn `hciconfig` ohne Argumente ausgeführt wird, werden in der Ausgabe Geräteinformationen, beispielsweise Gerätenamen (`hciX`), physikalische Geräteadresse (12-stellige Nummer in der Form `00:12:34:56:78`) und Informationen zum Umfang der übertragenen Daten angezeigt.

`hciconfig hci0 name` zeigt den Namen an, der von Ihrem Computer zurückgegeben wird, wenn er Anforderungen von entfernten Geräten erhält. Mit `hciconfig` können die Einstellungen des lokalen Geräts nicht nur abgefragt, sondern auch bearbeitet werden. Mit `hciconfig hci0 name TEST` beispielsweise wird der Name auf `TEST` gesetzt.

sdptool

Mit `sdptool` kann überprüft werden, welche Dienste von einem bestimmten Gerät zur Verfügung gestellt werden. Das Kommando `sdptool browse Geräteadresse` gibt alle Dienste eines Geräts zurück. Mit `sdptool search Dienstcode` wird nach einem bestimmten Dienst gesucht. Dieser Befehl scannt alle erreichbaren Geräte nach dem angeforderten Dienst. Wenn eines der Geräte den Dienst anbietet, gibt das Programm den vollständigen Dienstnamen, der vom Gerät zurückgegeben wurde, sowie eine kurze Beschreibung aus. Eine Liste aller möglichen Dienstcodes lässt sich durch Eingabe von `sdptool` ohne Parameter anzeigen.

33.2.4 Grafische Anwendungen

Geben Sie in Konqueror die URL `bluetooth:/` ein, um lokale und entfernte Bluetooth-Geräte aufzuführen. Durch Doppelklicken auf ein Gerät erhalten Sie einen Überblick über die von dem betreffenden Gerät bereitgestellten Dienste. Wenn Sie mit der Maus über einen der angegebenen Dienste fahren, wird in der Statusleiste des Browsers angezeigt, welches Profil für den Dienst verwendet wird. Wenn Sie auf einen Dienst klicken, wird ein Dialogfeld geöffnet, in dem Sie den gewünschten Vorgang auswählen können: Speichern, den Dienst verwenden (dazu muss eine Anwendung

gestartet werden) oder den Vorgang abbrechen. Aktivieren Sie das betreffende Kontrollkästchen, wenn der Dialog nicht mehr angezeigt und immer die ausgewählte Aktion durchgeführt werden soll. Für einige Dienste ist noch keine Unterstützung verfügbar. Weitere grafische Front-Ends für Bluetooth sind in den Paketen `kbluetooth`, `bluez-gnome` und `gnome-bluetooth` enthalten.

33.2.5 Beispiel – Einrichten einer Netzwerkverbindung via Bluetooth

In diesem Beispiel wird eine Netzwerkverbindung zwischen den Hosts *H1* und *H2* eingerichtet. Diese beiden Hosts haben die Bluetooth-Geräteadressen *baddr1* und *baddr2* (auf beiden Hosts mit dem Kommando `hcitool dev` bestimmt, wie oben beschrieben). Die Hosts sollten mit den IP-Adressen `192.168.1.3` (*H1*) und `192.168.1.4` (*H2*) identifiziert sein.

Die Bluetooth-Verbindung wird mithilfe von `pand` (Personal Area Networking Daemon) hergestellt. Die folgenden Kommandos müssen vom Benutzer `root` ausgeführt werden. Die Beschreibung konzentriert sich auf die Bluetooth-spezifischen Aktionen und bietet keine detaillierte Beschreibung des Netzwerkbefehls `ip`.

Geben Sie `pand -s` ein, um `pand` auf Host *H1* zu starten. Anschließend kann auf Host *H2* mit `pand -c baddr1` eine Verbindung hergestellt werden. Wenn Sie auf einem der Hosts `ip link show` eingeben, um die verfügbaren Netzwerkschnittstellen aufzulisten, sollte die Ausgabe etwa folgenden Eintrag enthalten:

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

Statt `00:12:34:56:89:90` sollte die Ausgabe die lokale Geräteadresse *baddr1* bzw. *baddr2* enthalten. Nun muss diese Schnittstelle einer IP-Adresse zugewiesen und aktiviert werden. Auf *H1* führen Sie dies mit den folgenden beiden Kommandos durch:

```
ip addr add 192.168.1.3/24 dev bnep0
ip link set bnep0 up
```

Verwenden Sie auf *H2* die folgenden Kommandos:

```
ip addr add 192.168.1.4/24 dev bnep0
ip link set bnep0 up
```

Nun ist ein Zugriff auf *H1* von *H2* aus unter der IP-Adresse 192.168.1.3 möglich. Mit dem Kommando `ssh 192.168.1.4` können Sie von *H1* aus auf *H2* zugreifen, vorausgesetzt *H2* führt einen `sshd` aus, der standardmäßig in openSUSE® aktiviert ist. Die Ausführung des Kommandos `ssh 192.168.1.4` ist auch als normaler Benutzer möglich.

33.2.6 Fehlersuche

Wenn Sie Schwierigkeiten bei der Herstellung einer Verbindung haben, sollten Sie die folgende Liste abarbeiten. Bedenken Sie, dass der Fehler auf jeder der beiden Seiten einer Verbindung liegen kann, zuweilen liegt sogar auf beiden Seiten ein Fehler vor. Rekonstruieren Sie das Problem nach Möglichkeit mit einem anderen Bluetooth-Gerät, um sicherzustellen, dass das Gerät nicht defekt ist.

Wird das lokale Gerät in der Ausgabe von `hcitool dev` aufgeführt?

Wenn das lokale Gerät nicht in dieser Ausgabe aufgeführt ist, wurde entweder `hcid` nicht gestartet oder das Gerät wird nicht als Bluetooth-Gerät erkannt. Dies kann verschiedene Ursachen haben. Das Gerät könnte beschädigt sein oder der richtige Treiber könnte fehlen. Notebooks mit integriertem Bluetooth haben häufig einen Ein-/Aus-Schalter für drahtlose Geräte, wie WLAN- oder Bluetooth-Geräte. Überprüfen Sie im Handbuch Ihres Notebooks, ob Ihr Gerät einen solchen Schalter aufweist. Starten Sie das Bluetooth-System mit dem Befehl `rcbluetooth restart` neu und überprüfen Sie, ob unter `/var/log/messages` Fehler gemeldet werden.

Benötigt Ihr Bluetooth-Adapter eine Firmware-Datei?

Falls ja, installieren Sie `bluez-bluefw` und starten Sie das Bluetooth-System mit `rcbluetooth restart` neu.

Gibt die Ausgabe von `hcitool inq` andere Geräte zurück?

Testen Sie diesen Befehl mehrmals. Die Verbindung weist möglicherweise Interferenzen auf, da das Bluetooth-Frequenzband auch von anderen Geräten verwendet wird.

Kann das entfernte Gerät den Computer „sehen“?

Versuchen Sie, die Verbindung vom Remote-Gerät aus herzustellen. Überprüfen Sie, ob das Gerät den Computer sieht.

Kann eine Netzwerkverbindung hergestellt werden (siehe **Abschnitt 33.2.5, „Beispiel – Einrichten einer Netzwerkverbindung via Bluetooth“** (S. 634))?

Die in **Abschnitt 33.2.5, „Beispiel – Einrichten einer Netzwerkverbindung via Bluetooth“** (S. 634) beschriebene Einrichtung funktioniert möglicherweise nicht. Dafür kann es mehrere Gründe geben. Beispielsweise unterstützt einer der beiden Computer möglicherweise nicht SSH. Versuchen Sie es mit `ping 192.168.1.3` oder `ping 192.168.1.4`. Wenn dies funktioniert, überprüfen Sie, ob `sshd` aktiv ist. Ein weiteres Problem könnte darin bestehen, dass eines der beiden Geräte bereits Netzwerkeinstellungen aufweist, die mit der im Beispiel genannten Adresse `192.168.1.X` in Konflikt stehen. Versuchen Sie es in diesem Fall mit anderen Adressen, beispielsweise `10.123.1.2` und `10.123.1.3`.

Wenn Sie das `bluez-hcidump`-Paket installiert haben, können Sie mithilfe von `hcidump -X` überprüfen, was zwischen den Geräten versendet wird. Manchmal gibt die Ausgabe einen Hinweis auf das Problem. Beachten Sie aber, dass nur teilweise „Klartext“ ausgegeben wird.

33.2.7 Weiterführende Informationen

Zusätzliche (kurz vor Veröffentlichung eingegangene) Dokumentationen erhalten Sie unter `/usr/share/doc/packages/bluez-utils/` (deutschsprachige und englischsprachige Version verfügbar).

Einen umfassenden Überblick über die verschiedenen Anweisungen für Verwendung und Konfiguration von Bluetooth finden Sie unter <http://www.bluez.org/>. Weitere nützliche Informationen und Anweisungen:

- Offizielle Anleitungssseite für den in den Kernel integrierten Bluetooth-Protokollstapel: <http://bluez.sourceforge.net/howto/index.html>
- Verbindung mit PalmOS PDA: <http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html>

33.3 Infrarot-Datenübertragung

IrDA (Infrared Data Association) ist ein Industriestandard für die kabellose Kommunikation über Infrarotlicht. Viele Notebooks sind heute mit einem IrDA-kompatiblen Transceiver ausgestattet, der die Kommunikation mit anderen Geräten, wie Druckern, Modems, LANs oder anderen Notebooks, ermöglicht. Die Übertragungsgeschwindigkeit reicht von 2400 bps bis 4 Mbps.

Es gibt zwei IrDA-Betriebsmodi. Im Standardmodus, SIR, wird über eine serielle Schnittstelle auf den Infrarot-Port zugegriffen. Dieser Modus funktioniert auf fast allen Systemen und ist für die meisten Anforderungen ausreichend. Für den schnelleren Modus, FIR, ist ein besonderer Treiber für den IrDA-Chip erforderlich. Im FIR-Modus werden aufgrund des Fehlens geeigneter Treiber nicht alle Chiptypen unterstützt. Den gewünschten IrDA-Modus legen Sie im BIOS Ihres Computers fest. Im BIOS wird angezeigt, welche serielle Schnittstelle im SIR-Modus verwendet wird.

Informationen zu IrDA finden Sie im Dokument "IrDA how-to" von Werner Heuser unter <http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html>. Zusätzlich können Sie die Website des Linux IrDA-Projekts unter <http://irda.sourceforge.net/> als Referenz verwenden.

33.3.1 Software

Die erforderlichen Kernel-Module sind im Kernel-Paket enthalten. Im Paket `irda` sind die erforderlichen Hilfsanwendungen für die Unterstützung der Infrarotschnittstelle enthalten. Nach der Installation des Pakets finden Sie die entsprechende Dokumentation unter `/usr/share/doc/packages/irda/readme`.

33.3.2 Konfiguration

Der IrDA-Systemdienst wird beim Booten des Systems nicht automatisch gestartet. Zur Aktivierung verwenden Sie das YaST IrDA-Modul. Nur eine Einstellung in diesem Modul kann geändert werden: die serielle Schnittstelle des Infrarotgeräts. Im Testfenster werden zwei Ausgaben angezeigt. Die eine ist die Ausgabe von `irdadump`, mit der alle gesendeten und empfangenen IrDA-Pakete protokolliert werden. Diese Ausgabe sollte den Namen des Computers und den Namen aller Infrarotgeräte im Übertragungsbereich enthalten. Im Abschnitt **Abschnitt 33.3.4, „Fehlersuche“** (S. 639) wird ein Beispiel

für diese Meldungen angegeben. Alle Geräte, mit denen eine IrDA-Verbindung besteht, werden im unteren Bereich des Fensters aufgeführt.

IrDA nimmt sehr viel Batterieleistung in Anspruch, da im Abstand von wenigen Sekunden ein Erkennungspaket zur Erkennung anderer peripherer Geräte gesendet wird. Aus diesem Grund sollte IrDA nur bei Bedarf gestartet werden, wenn Sie Ihr Gerät mit Batterie betreiben müssen. Geben Sie zum Aktivieren das Kommando `rcirda start` und zum Deaktivieren `rcirda stop` ein. Alle erforderlichen Kernel-Module werden automatisch beim Aktivieren der Schnittstelle geladen.

In der Datei `/etc/sysconfig/irda` kann nach Wunsch eine manuelle Konfiguration vorgenommen werden. Die Datei enthält nur eine Variable, `IRDA_PORT`, mit der die im SIR-Modus zu verwendende Schnittstelle bestimmt wird.

33.3.3 Verwendung

An die Gerätedatei `/dev/irldpt0` können Daten zum Drucken gesendet werden. Die Gerätedatei `/dev/irldpt0` fungiert genau wie die normale Kableschnittstelle `/dev/lp0` mit dem Unterschied, dass die Daten kabellos per Infrarot gesendet werden. Zum Drucken stellen Sie sicher, dass sich der Drucker in Sichtweite der Infrarotschnittstelle des Computers befindet und dass die Infrarotunterstützung gestartet wurde.

Ein Drucker, der über die Infrarotschnittstelle betrieben wird, kann mit dem YaST-Druckermodule konfiguriert werden. Da er nicht automatisch erkannt wird, konfigurieren Sie ihn manuell, indem Sie auf *Hinzufügen > Direkt angeschlossene Drucker* klicken. Wählen Sie *IrDA-Drucker* aus und klicken Sie auf *Weiter*, um den Drucker zu konfigurieren. In der Regel ist `irldpt0` die richtige Verbindung. Klicken Sie zum Anwenden der Einstellungen auf *Verlassen*. Detaillierte Informationen zum Betrieb von Druckern unter Linux erhalten Sie in **Kapitel 7, Druckerbetrieb** (S. 115).

Die Kommunikation mit anderen Hosts und Mobiltelefonen oder ähnlichen Geräten erfolgt über die Gerätedatei `/dev/ircomm0`. Mit den Mobiltelefonen Siemens S25 und Nokia 6210 kann beispielsweise über die Infrarotschnittstelle mit der Anwendung `wvdial` eine Verbindung zum Internet hergestellt werden. Auch die Synchronisierung von Daten mit einem Palm Pilot ist möglich, vorausgesetzt, die Geräteeinstellungen der entsprechenden Anwendung wurden auf `/dev/ircomm0` gesetzt.

Wenn Sie möchten, können Sie nur Geräte adressieren, die den Drucker oder IrCOMM-Protokolle unterstützen. Auf Geräte, die das IROBEX-Protokoll unterstützen, wie der

3Com Palm Pilot, kann mit speziellen Anwendungen wie irobexpalm und irobexreceive zugegriffen werden. Weitere Informationen hierzu erhalten Sie im Dokument *IR-HOWTO* (<http://tldp.org/HOWTO/Infrared-HOWTO/>). Die vom Gerät unterstützten Protokolle werden hinter dem Namen des Geräts in der Ausgabe von `irdadump` in Klammern aufgeführt. Die Unterstützung des IrLAN-Protokolls steht momentan noch nicht zur Verfügung.

33.3.4 Fehlersuche

Falls an den Infrarot-Port angeschlossene Geräte nicht reagieren, können Sie mit dem Befehl `irdadump` (als Benutzer `root`) überprüfen, ob das andere Gerät vom Computer erkannt wird. Ein ähnliches Problem wie in **Beispiel 33.1**, „Ausgabe von `irdadump`“ (S. 639) tritt häufig auf, wenn ein Canon BJC-80-Drucker sich in der Reichweite des Computers befindet:

Beispiel 33.1 Ausgabe von `irdadump`

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                    hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* earth
                    hint=0500 [ PnP Computer ] (21)
```

Überprüfen Sie die Konfiguration der Schnittstelle, wenn keine Ausgabe vorhanden ist oder das andere Gerät nicht reagiert. Überprüfen Sie, ob die richtige Schnittstelle verwendet wird. Gelegentlich befindet sich die Infrarotschnittstelle in `/dev/ttyS2` oder `/dev/ttyS3` und manchmal wird ein anderer Interrupt als IRQ 3 verwendet. Diese Einstellungen können auf nahezu alle Notebooks im BIOS-Setup-Menü überprüft und geändert werden.

Auch mithilfe einer einfachen Videokamera kann festgestellt werden, ob die Infrarot-LED leuchtet. Mit den meisten Videokameras kann Infrarotlicht aufgenommen werden, das für das menschliche Auge nicht sichtbar ist.

Verwenden von Tablet PCs

openSUSE® unterstützt Tablet PCs mit seriellen Wacom-Geräten (z. B. IBM/Lenovo X41, ACER TM C300/C301/C302 Series, Fujitsu Lifebook T Series (T3010/T4010), HP Compaq TC4200, Motion M1200) und FinePoint-Geräten (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 Zeigegeräte (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.

34.1 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
- `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.

34.2 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 den Hersteller und den Namen Ihres Tablets aus und aktivieren Sie *Dieses Tablet aktivieren*.
- 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.

34.3 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 Anmeldefelds 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 34.1 Virtuelle Tastatur von xvkbd

F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	Backspace	xvkbd (v2.7)						
Esc	!	@	#	\$	%	^	&	*	()	_	=		~	Num Lock	/	*	Focus	
Tab	Q	W	E	R	T	Y	U	I	O	P	{	}	Del	7 Home	8 Up	9 PgUp	+		
Control	A	S	D	F	G	H	J	K	L	:	"	'	Return	4 Left	5	6 Right	-		
Shift	Z	X	C	V	B	N	M	<	>	?	,	.	/	Com pose	Shift	1 End	2 Down	3 PgDn	Enter
xvkbd	Caps Lock	Alt	Meta				Meta	Alt	←	→	↑	↓	Focus	0 Ins	.	Del			

Wenn Sie xvkbd nach der Anmeldung verwenden möchten, starten Sie es aus dem Hauptmenü oder über das Shell-Kommando *xvkbd*.

34.4 Drehen der Ansicht

Wenn Sie den Bildschirm Ihres Tablet PCs drehen, wird die Ausrichtung der Ansicht und Ihres Grafiktablets nicht automatisch angepasst. Auf dem KDE-Desktop können Sie die Ansicht mit dem Applet KRandRTray manuell drehen und skalieren. KRandRTray ist ein KDE-Applet für die RANDR-Erweiterung von X Server.

- 1 Starten Sie KRandRTray aus dem Hauptmenü oder über das Shell-Kommando *krandrtray*. Dadurch wird dem Systemabschnitt der Kontrollleiste das KRandRTray-Symbol hinzugefügt.
- 2 Zum Drehen der Ansicht klicken Sie auf das Symbol und wählen Sie die gewünschte Ausrichtung aus dem Kontextmenü 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 34.7, „Fehlersuche“** (S. 648).

34.5 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.

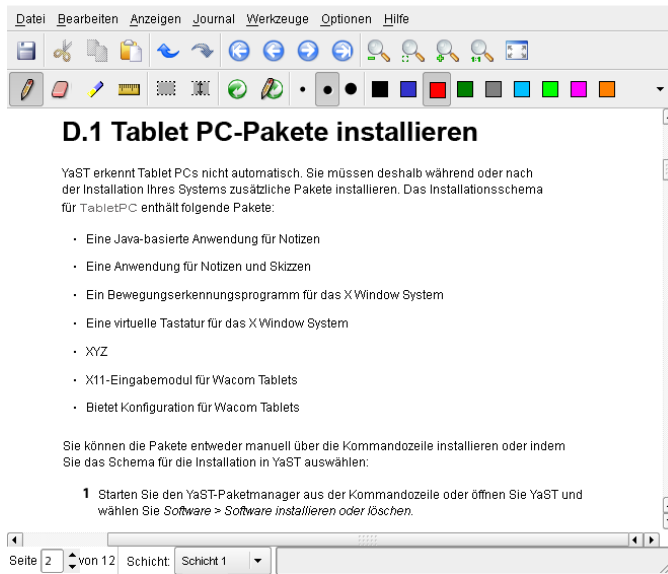
- 1 Starten Sie xstroke aus dem Hauptmenü oder über das Shell-Kommando `xstroke`. Dadurch wird dem Systemabschnitt der Kontrollleiste ein Bleistiftsymbol hinzugefügt.
- 2 Starten Sie die Anwendung, in die Sie mittels des Pens einen Text eingeben möchten (z. B. ein Terminalfenster, einen Texteditor oder 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.

34.6 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)*.

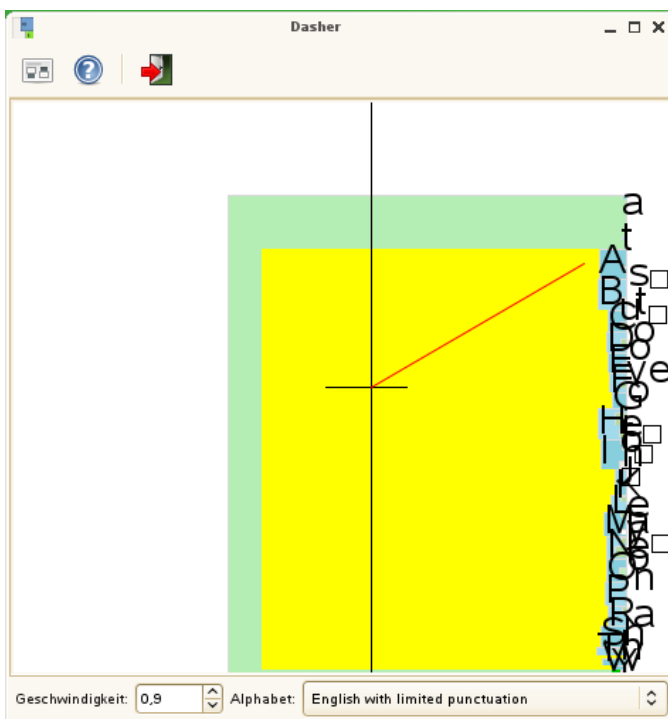
Abbildung 34.2 *Kommentieren einer PDF-Datei mit Xournal*



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 34.3 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/>

34.7 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 in GNOME 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 34.2, „Konfigurieren des Tablet-Geräts“](#) (S. 643) beschrieben, mit SaX2 konfiguriert haben, sollten die Kommandos wie angegeben funktionieren. Wenn Sie den Parameter `Identifizier` des Tablet Stylus-Eingabegeräts in der Datei `xorg.conf` manuell geändert haben, müssen Sie `"Mouse[7]"` durch den neuen `Identifizier` ersetzen.

34.8 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/tc1000/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/>

Teil VI. Sicherheit

Masquerading und Firewalls

Wann immer Linux in einer Netzwerkkumgebung 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.

35.1 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.

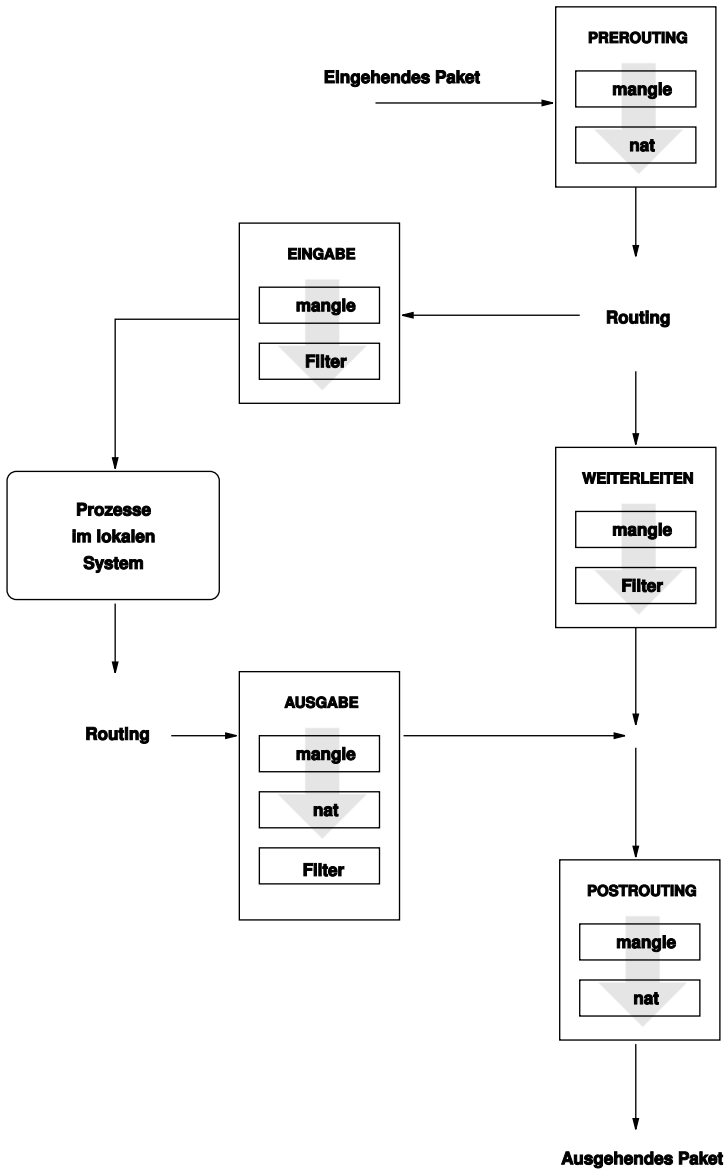
nat

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).

Abbildung 35.1 *iptables: Die möglichen Wege eines Pakets*



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 35.1, „**iptables: Die möglichen Wege eines Pakets**“ (S. 655) 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.

35.2 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 20.1.2, „Netzmasken und Routing“** (S. 343)) 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.

35.3 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.
```

35.4 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 20.1.2, „Netzmasken und Routing“](#) (S. 343)) 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 35.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 660)). 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.

35.4.1 Konfigurieren der Firewall mit YaST

WICHTIG: Automatische Firewall-Konfiguration

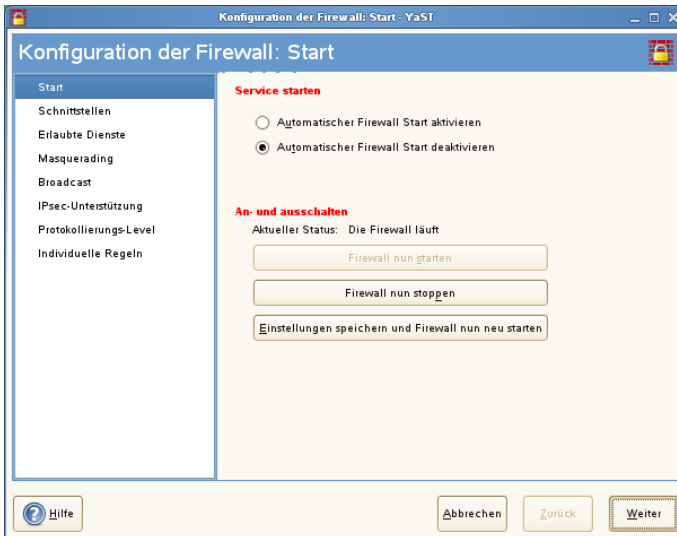
Im Anschluss an die Installation startet YaST automatisch eine Firewall für alle konfigurierten Schnittstellen. Wenn ein Server auf dem System konfiguriert und aktiviert ist, kann YaST die automatisch generierte Firewall-Konfiguration mit den Optionen *Firewall-Ports auf ausgewählten Schnittstellen öffnen* 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 35.2 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 ausgege-

ben, 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 verbürgt 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.

35.4.2 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. 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`.

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 (020405B40402080A061AFEB0000000001030300)
```

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.

35.5 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 – sichere Netzwerkoperationen

36

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.

36.1 Das Paket OpenSSH

openSUSE installiert das Paket OpenSSH standardmäßig. Daher stehen Ihnen die Programme `ssh`, `scp` und `sftp` als sichere Alternativen 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.

36.2 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 Kommando `ssh venus` auf dem Host `venus` anmelden. Der Host fordert Sie dann zur Eingabe des Passworts am `venus` 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 venus` oder `ssh augustine@venus`.

Darüber hinaus bietet `ssh` die von `rsh` bekannte Möglichkeit, Befehle auf einem entfernten System auszuführen. Im folgenden Beispiel wird das Kommando `uptime` auf dem Host `venus` ausgeführt und ein Verzeichnis mit dem Namen `tmp` wird angelegt. Die Programmausgabe erfolgt auf dem lokalen Terminal des Hosts `jupiter`.

```
ssh venus "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 das zweite Kommando auf dem Host `venus` ausgeführt.

36.3 scp – Sichere Kopie

scp kopiert Dateien auf einen entfernten Computer. Es ist ein sicherer und verschlüsselter Ersatz für rcp. Beispielsweise kopiert `scp MyLetter.tex venus:` die Datei `MyLetter.tex` vom Host `jupiter` auf den Host `venus`. Wenn sich die Benutzernamen auf `jupiter` und `venus` unterscheiden, geben Sie den letzteren im Format `benutzername@host` an. Verwenden Sie für die Angabe des Benutzernamens mit diesem Kommando nicht die Option `-l`; sie hat eine andere Bedeutung.

Nach Eingabe des richtigen Passworts startet scp die Datenübertragung. Am rechten Rand des Fortschrittsbalkens wird die geschätzte Restübertragungszeit (bis zum Erreichen des Balkenendes) angezeigt. Jegliche Ausgabe kann durch die Option `-q` unterdrückt werden.

scp bietet auch ein rekursives Kopierverfahren für ganze Verzeichnisse. Das Kommando `scp -r src/ venus:backup/` kopiert den kompletten Inhalt des Verzeichnisses `src` einschließlich aller Unterverzeichnisse in das Unterverzeichnis `backup` auf den Host `venus`. 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.

36.4 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.

36.5 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.

36.6 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.

36.7 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 beste-

henden 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:mail.example.com:25 jupiter.example.com
```

Mit diesem Kommando wird jede Verbindung zu Port 25 (SMTP) von `jupiter.example.com` auf den SMTP-Port von `mail.example.com` 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. Analog können mit folgendem Kommando alle POP3-Anfragen (Port 110) an `jupiter.example.com` auf den POP3-Port von `mail.example.com` weitergeleitet werden:

```
ssh -L 110:mail.example.com:110 jupiter.example.com
```

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`.

36.8 Konfigurieren eines SSH-Daemons mit YaST

Zur Konfiguration eines sshd-Servers mit YaST wählen Sie in YaST *Netzwerkdienste* > *SSHD-Konfiguration* aus. Führen Sie danach die folgenden Schritte aus:

- 1 Wählen Sie in der Tabelle *SSHD TCP-Ports* diejenigen Ports aus, die sshd überwachen soll. Die Standardanschlussnummer lautet 22. Sie können auch mehrere Ports auswählen. Zum Hinzufügen eines neuen Ports klicken Sie auf *Hinzufügen*, geben Sie die Nummer des Ports ein und klicken Sie auf *OK*. Zum Löschen eines Ports wählen Sie den Port in der Tabelle aus, klicken Sie auf *Löschen* und bestätigen Sie den Vorgang.
- 2 Wählen Sie die Funktionen aus, die der sshd-Daemon unterstützen soll. Zum Deaktivieren der TCP-Weiterleitung deaktivieren Sie die Option *Allow TCP Forwarding* (TCP-Weiterleitung zulassen). Durch Deaktivieren der TCP-Weiterleitung wird die Sicherheit nicht erhöht, sofern nicht auch der Shell-Zugriff unterbunden wird; andernfalls haben die Benutzer immer noch die Möglichkeit, eigene Weiterleitungsmechanismen zu installieren. Weitere Informationen zur TCP-Weiterleitung finden Sie unter **Abschnitt 36.7, „X-, Authentifizierungs- und Weiterleitungsmechanismen“** (S. 672).

Zum Deaktivieren der X-Weiterleitung deaktivieren Sie die Option *Allow X11 Forwarding* (X11-Weiterleitung zulassen). Wenn diese Option deaktiviert ist, verursacht jede X11-Weiterleitungsanforderung seitens des Clients einen Fehler. Die Benutzer haben aber nach wie vor die Möglichkeit, eigene Weiterleitungsmechanismen zu installieren. Weitere Informationen zur X-Weiterleitung finden Sie unter **Abschnitt 36.7, „X-, Authentifizierungs- und Weiterleitungsmechanismen“** (S. 672).

Geben Sie unter *Allow Compression* (Komprimierung zulassen) an, ob die Verbindung zwischen dem Server und den Clients komprimiert werden soll. Klicken Sie nach der Einstellung dieser Optionen auf *Weiter*.

- 3 Geben Sie unter *Print Message of the day After Login* (Nach Anmeldung Nachricht des Tages ausgeben) an, ob sshd eine Nachricht aus */etc/motd* ausgeben soll, wenn sich ein Benutzer interaktiv anmeldet. Wenn Sie Verbindungen vom

Benutzer `root` unterbinden möchten, deaktivieren Sie die Option *Permit Root Login* (Root-Anmeldung zulassen).

Geben Sie unter *Maximum Authentication Tries* (Maximale Anzahl der Authentifizierungsversuche) die maximal zulässige Anzahl an Authentifizierungsversuchen pro Verbindung ein. *Password Authentication* (Passwortauthentifizierung) legt fest, ob die Authentifizierung mittels eines Passworts erlaubt ist. *RSA Authentication* (RSA-Authentifizierung) legt fest, ob die reine RSA-Authentifizierung erlaubt ist. Diese Option gilt nur für Version 1 des SSH-Protokolls. *Public Key Authentication* (Authentifizierung mit öffentlichem Schlüssel) legt fest, ob die Authentifizierung mittels eines öffentlichen Schlüssels erlaubt ist. Diese Option gilt nur für Version 2 des Protokolls.

- 4 Klicken Sie zum Speichern der Konfiguration auf *Übernehmen*.

Verwalten der X.509-Zertifizierung

37

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>.

37.1 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.

37.1.1 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.

37.1.2 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 37.1 zeigt die Felder eines grundlegenden X.509-Zertifikats der Version 3 an.

Tabelle 37.1 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“.

37.1.3 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 37.2, „X.509-Zertifikatswiderrufsliste (CRL)“** (S. 681) werden die grundlegenden Bestandteile einer X.509-CRL dargestellt.

Tabelle 37.2 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

37.1.4 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 26, LDAP – Ein Verzeichnisdienst** (S. 461). **Kapitel 30, Der HTTP-Server Apache** (S. 543) enthält Informationen zu HTTP-Servern.

37.1.5 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.

37.2 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.

37.2.1 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 37.1**, „YaST-CA-Modul: Grunddaten für eine Stammzertifizierungsstelle“ (S. 683) gezeigten Dialogfeld ein. Die Textfelder haben folgende Bedeutungen:

Abbildung 37.1 YaST-CA-Modul: Grunddaten für eine Stammzertifizierungsstelle

Zum Erstellen einer neuen CA sind einige Einträge erforderlich.

Diese hängen von der in der Konfigurationsdatei definierten Richtlinie ab.

CA-Name ist der Name des CA-Zertifikats. Verwenden Sie ausschließlich ASCII-Zeichen sowie "-" und ".".

Allgemeiner Name ist der Name der CA.

E-Mail-Adressen sind gültige E-Mail-Adressen des Benutzers oder des Serveradministrators.

Organisation, Organisatorische Einheit, Ort und Bundesland sind häufig optional.

Neue Root-CA erstellen (Schritt 1/3)

CA-Name:

Allgemeiner Name:

E-Mail-Adressen: ☒

Organisation: Organisatorische Einheit:

Ort: Bundesland:

Land:

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.

Eigennamen

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 37.4, „YaST-CA-Modul: Erweiterte Einstellungen“** (S. 689)). 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.

37.2.2 Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle

Eine untergeordnete Zertifizierungsstelle wird auf dieselbe Weise erstellt wie eine Stammzertifizierungsstelle. Führen Sie folgende Schritte aus:

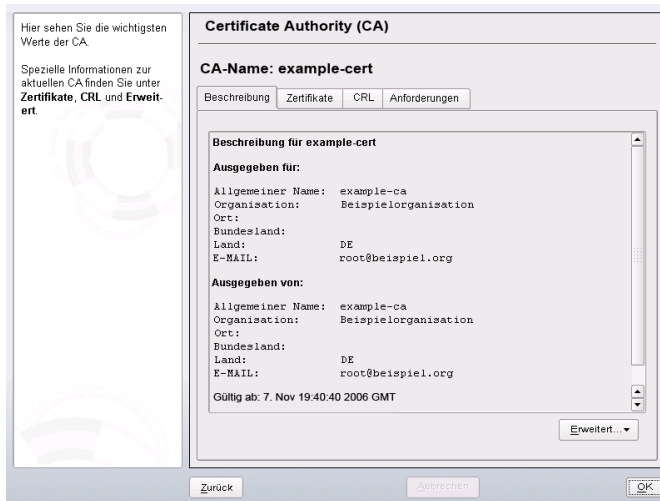
- 1 Starten Sie YaST und öffnen Sie das CA-Modul.
- 2 Wählen Sie die erforderliche Zertifizierungsstelle aus und klicken Sie auf *CA betreten*.

ANMERKUNG

Die Gültigkeitsdauer der untergeordneten Zertifizierungsstelle muss vollständig in die Gültigkeitsdauer der „übergeordneten“ Zertifizierungsstelle fallen. Da die untergeordnete Zertifizierungsstelle immer nach der „übergeordneten“ Zertifizierungsstelle erstellt wird, 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 37.2](#)).

Abbildung 37.2 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 37.2.1, „Erstellen einer Stammzertifizierungsstelle“** (S. 682) 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 37.2.5, „Erstellen von CRLs“** (S. 690) beschrieben.
- 7 Klicken Sie abschließend auf *OK*.

37.2.3 Erstellen oder Widerrufen von Benutzerzertifikaten

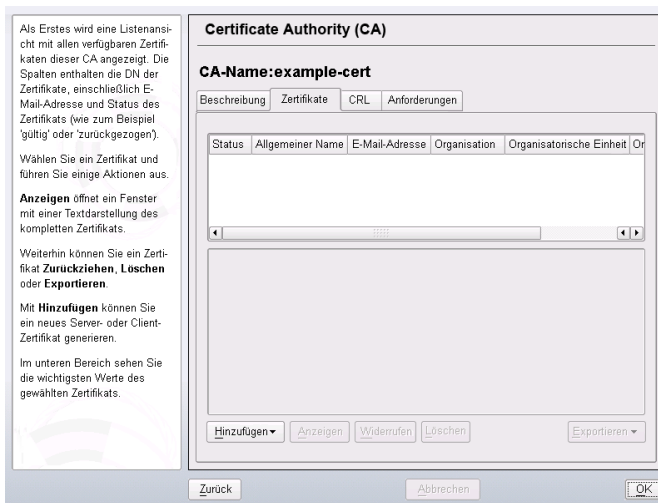
Die Erstellung von Client- und Server-Zertifikaten ähnelt der Erstellung des Zertifikats zum Erstellen von Zertifizierungsstellen in **Abschnitt 37.2.1, „Erstellen einer Stamm-**

zertifizierungsstelle“ (S. 682). 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 *Eigennamen* 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 Zertifizierungsstelle 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 37.3**, „Zertifikate einer Zertifizierungsstelle“ (S. 687)).

Abbildung 37.3 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 Zertifizierungsstelle 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 37.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“** (S. 685)).
- 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

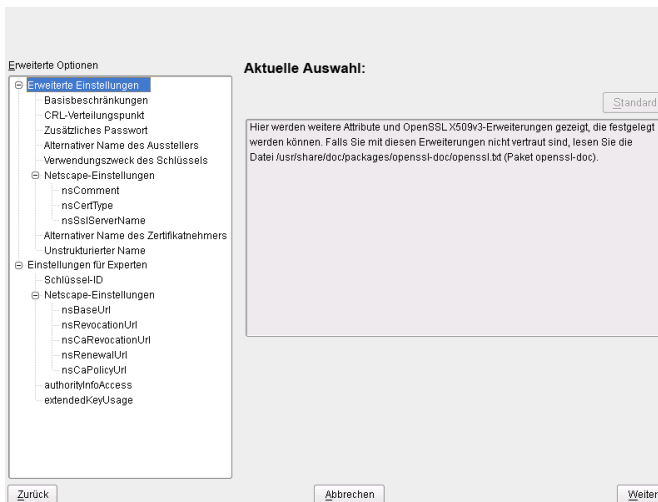
Ein Widerruf allein reicht zur Deaktivierung eines Zertifikats nicht aus. Widerrufene Zertifikate müssen zudem in einer CRL veröffentlicht werden. In **Abschnitt 37.2.5, „Erstellen von CRLs“** (S. 690) wird die Erstellung von CRLs erläutert. Nach der Veröffentlichung in einer CRL können widerrufene Zertifikate vollständig mit *Löschen* entfernt werden.

37.2.4 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 Zertifizierungsstelle ein, wie in [Abschnitt 37.2.2](#), „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“ (S. 685) 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 37.4](#), „YaST-CA-Modul: Erweiterte Einstellungen“ (S. 689) gezeigte Dialogfeld zum Ändern der Standardeinstellungen geöffnet.

Abbildung 37.4 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.

37.2.5 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 37.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“](#) (S. 685) (für untergeordnete Zertifizierungsstellen) und in [Abschnitt 37.2.3, „Erstellen oder Widerrufen von Benutzerzertifikaten“](#) (S. 686) (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 37.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“](#) (S. 685) 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.

37.2.6 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 37.3**, „Passwörter beim LDAP-Export“ (S. 691)).

Tabelle 37.3 *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 37.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“** (S. 685) 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 dann ggf. eine neue CRL und exportieren Sie sie mit *Nach LDAP > exportieren*. Die LDAP-Daten werden hier ebenfalls so eingegeben wie für Zertifizierungsstellen. Die Einträge werden in LDAP an derselben Stelle eingefügt wie die zugehörige Zertifizierungsstelle, hier wird jedoch das Attribut „certificateRevocationList“ verwendet.

37.2.7 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.

Dateien werden für Zertifikate, Zertifizierungsstellen und CRLs auf die gleiche Weise exportiert wie mit LDAP (in **Abschnitt 37.2.6, „Exportieren von Zertifizierungsstellenobjekten in LDAP“** (S. 691) 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 mit *OK* im erforderlichen Verzeichnis gespeichert.

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.

37.2.8 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*.

Netzwerk-Authentifizierung – Kerberos

38

Bei einem offenen Netzwerk gibt es keine Garantie dafür, dass eine Arbeitsstation ihre Benutzer korrekt identifiziert, außer die üblichen Passwortmechanismen. Bei gewöhnlichen Installationen muss der Benutzer bei jedem Zugriff auf einen Dienst im Netzwerk ein Passwort eingeben. Kerberos bietet eine Authentifizierungsmethode, mit der ein Benutzer sich einmal registriert. Anschließend wird ihm im ganzen Netzwerk für den Rest der Sitzung vertraut. Damit das Netzwerk sicher ist, müssen folgende Anforderungen gegeben sein:

- Alle Benutzer müssen Ihre Identität für jeden gewünschten Dienst beweisen und sicherstellen, dass niemand die Identität eines anderen übernehmen kann.
- Stellen Sie sicher, dass jeder Netzwerkservers ebenfalls eine Identität beweist. Anderenfalls kann ein Angreifer die Identität des Servers übernehmen und auf wichtige Informationen, die über den Server übertragen werden, zugreifen. Dieses Konzept nennt man *gegenseitige Authentifizierung*, weil sich der Client beim Server authentifiziert und umgekehrt.

Kerberos hilft Ihnen bei diesen Anforderungen, da es eine stark verschlüsselte Authentifizierung bietet. Im Folgenden sehen Sie, wie das erreicht wird. Hier werden nur die grundlegenden Prinzipien von Kerberos erläutert. Genauere technische Informationen erhalten Sie aus der Dokumentation Ihrer Kerberos-Installation.

38.1 Kerberos-Terminologie

Im folgenden Glossar wird die Kerberos-Terminologie erläutert.

Berechtigung

Benutzer oder Clients müssen bestimmte Berechtigungen vorweisen, die Sie autorisieren, Dienste anzufordern. Kerberos kennt zwei Arten von Berechtigungen: Tickets und Authentifikatoren.

Ticket

Ein Ticket ist eine Berechtigung, die pro Server vergeben wird. Clients verwenden es, um sich bei einem Server zu authentifizieren, von dem sie einen Dienst anfordern möchten. Es enthält den Namen des Servers, des Clients, die Internetadresse des Clients, einen Zeitstempel, eine Lebensdauer und einen zufälligen Sitzungsschlüssel. Alle diese Daten sind über den Serverschlüssel verschlüsselt.

Authentifikator

Gemeinsam mit dem Ticket stellt ein Authentifikator sicher, dass der das Ticket vorlegende Client tatsächlich der vorgegebene Client ist. Ein Authentifikator besteht aus dem Client-Namen, der IP-Adresse der Arbeitsstation und der aktuellen Zeit der Arbeitsstation. Alle sind verschlüsselt mit dem Sitzungsschlüssel, der nur dem Client und dem Server bekannt ist, von dem der Dienst angefordert wurde. Ein Authentifikator kann, anders als ein Ticket, nur einmal verwendet werden. Ein Client kann einen Authentifikator selbst generieren.

Prinzipal

Ein Kerberos Prinzipal ist eine eindeutige Einheit (ein Benutzer oder ein Dienst), dem ein Ticket zugewiesen werden kann. Ein Prinzipal besteht aus folgenden Komponenten:

- **Primär:** Der erste Teil des Prinzipals. Im Falle eines Benutzer kann dies der Benutzername sein,
- **Instanz:** Zusätzliche Informationen zur genaueren Bestimmung des Primärs. Dieser String wird vom Primär durch einen / getrennt.
- **Bereich:** Gibt den Kerberos-Bereich an. Normalerweise ist der Bereich der Domänenname in Großbuchstaben.

Gegenseitige Authentifizierung

Kerberos stellt sicher, dass Client und Server sich ihrer gegenseitigen Identität sicher sein können. Sie teilen sich einen Sitzungsschlüssel, über den sie sicher kommunizieren können.

Sitzungsschlüssel

Sitzungsschlüssel sind temporäre private Schlüssel, die von Kerberos erstellt werden. Sie sind dem Client bekannt und werden zur Verschlüsselung der Kommunikation zwischen dem Client und dem Server, der angefordert und für den ein Ticket erhalten wurde, verwendet.

Replay

Fast alle in einem Netzwerk versendeten Nachrichten können belauscht, gestohlen und erneut versendet werden. Bei Kerberos wäre es sehr gefährlich, wenn ein Angreifer auf Ihre Dienstanforderung zugreifen könnte, die Ihr Ticket und Ihren Authentifikator enthält. Er könnte sie dann erneut senden (*Replay*) und Ihre Identität übernehmen. Kerberos verwendet jedoch mehrere Mechanismen, um dieses Problem zu umgehen.

Server oder Dienst

Dienst ist eine bestimmte durchzuführende Aktion. Der dieser Aktion zugrunde liegende Prozess ist ein *Server*.

38.2 Funktionsweise von Kerberos

Kerberos wird meist als vertrauenswürdiger Authentifizierungsdienst eines Drittanbieters bezeichnet. Das bedeutet, alle Clients vertrauen Kerberos' Beurteilung der Identität eines anderen Clients. Kerberos verwaltet eine Datenbank aller Benutzer mit deren privaten Schlüsseln.

Wenn Sie die absolute Sicherheit von Kerberos garantieren möchten, sollten Sie sowohl den Authentifizierungs- sowie den Tickets ausstellenden Server auf einer dedizierten Maschine ausführen. Stellen Sie sicher, dass nur der Administrator direkt auf diese Maschine und über das Netzwerk zugreifen kann. Reduzieren Sie die darauf ausgeführten (Netzwerk-)Dienste auf das absolute Minimum. Führen Sie auch nicht `sshd` aus.

38.2.1 Erster Kontakt

Ihr erster Kontakt mit Kerberos ähnelt einem beliebigen Anmeldevorgang bei einem normalen Netzwerksystem. Geben Sie Ihren Benutzernamen ein. Diese Informationen und der Name des Dienstes, welcher das Ticket ausstellt, werden an den Authentifizierungsserver (Kerberos) gesendet. Wenn Sie dem Authentifizierungsserver bekannt sind, wird ein zufälliger Sitzungsschlüssel zur Verwendung zwischen Ihrem Client und dem

Ticket ausstellenden Server generiert. Jetzt bereitet der Authentifizierungsserver ein Ticket für den Ticket ausstellenden Server vor. Das Ticket enthält die folgenden Informationen, die alle mit einem Sitzungsschlüssel verschlüsselt sind, der nur dem Authentifizierungsserver und dem Server bekannt ist, welcher das Ticket ausstellt:

- Die Namen des Clients und des Ticket ausstellenden Servers
- Die aktuelle Zeit
- Eine Lebensdauer für dieses Ticket
- Die Client-IP-Adresse
- Der neu generierte Sitzungsschlüssel

Dieses Ticket wird dann gemeinsam mit dem Sitzungsschlüssel zurück an den Client gesendet. Das geschieht wieder in verschlüsselter Form. Dieses Mal wird jedoch der private Schlüssel des Clients verwendet. Dieser private Schlüssel ist nur Kerberos und dem Client bekannt, da er vom Benutzerpasswort abgeleitet wird. Jetzt hat der Client eine Antwort erhalten und Sie werden zur Eingabe Ihres Passworts aufgefordert. Das Passwort wird in den Schlüssel umgewandelt, der das vom Authentifizierungsserver gesendete Paket entschlüsselt. Das Paket wird „ausgepackt“ und das Passwort und der Schlüssel werden aus dem Speicher der Arbeitsstation gelöscht. Solange die Lebensdauer Ihres Tickets, das zum Erstellen anderer Tickets verwendet wird, nicht erlöscht, kann Ihre Arbeitsstation Ihre Identität nachweisen.

38.2.2 Anfordern eines Diensts

Zum Anfordern eines Diensts von einem beliebigen Netzwerkserver, muss die Client-Anwendung dem Server ihre Identität beweisen. Daher generiert die Anwendung einen Authentifikator. Ein Authentifikator besteht aus folgenden Komponenten:

- Der Prinzipal des Client
- Die Client-IP-Adresse
- Die aktuelle Zeit
- Eine Prüfsumme (gewählt vom Client)

Alle diese Informationen werden mithilfe des Sitzungsschlüssels, den der Client bereits für diesen bestimmten Server erhalten hat, verschlüsselt. Der Authentifikator und das Ticket für den Server werden an den Server gesendet. Der Server verwendet seine Kopie des Sitzungsschlüssels zum Entschlüsseln des Authentifikators. So erhält der Server alle erforderlichen Informationen zur Anforderung des Clients und kann sie mit denen im Ticket vergleichen. Der Server prüft, ob das Ticket und der Authentifikator vom selben Client stammen.

Ohne serverseitige Sicherheitsmaßnahmen wäre dieser Prozessabschnitt ein ideales Ziel für Replay-Angriffe. Jemand könnte versuchen, eine vorher aus dem Netzwerk gestohlene Anforderung erneut zu versenden. Um das zu verhindern, akzeptiert der Server keine Anforderungen mit einem Zeitstempel und Ticket, die bereits vorher empfangen wurden. Außerdem wird eine Anforderung mit einem sehr unterschiedlichen Zeitstempel zur empfangenen Anforderung ignoriert.

38.2.3 Beiderseitige Authentifizierung

Die Kerberos-Authentifizierung kann in beide Richtungen verwendet werden. Es geht nicht nur um die korrekte Identität des Client. Der Server sollte sich außerdem selbst beim Client identifizieren, der seinen Dienst anfordert. Daher sendet er ebenfalls eine Art Authentifikator. Er fügt einen Authentifikator zur Prüfsumme des Client-Authentifikators hinzu und verschlüsselt ihn mit dem Sitzungsschlüssel, der gemeinsam von Server und Client verwendet wird. Der Client nimmt diese Antwort als Beweis für die Serverauthentizität und beide beginnen die Zusammenarbeit.

38.2.4 Ticket-Ausstellung: Alle Server werden kontaktiert

Tickets können jeweils nur von einem Server verwendet werden. Das bedeutet, Sie benötigen für jede Anforderung eines weiteren Diensts ein neues Ticket. Kerberos verwendet einen Mechanismus, um Tickets für einzelne Server zu erhalten. Dieser Dienst wird als „Ticket-Granting Service“ (Ticket-Ausstellung) bezeichnet. Der Ticket ausstellende Dienst gehört zu den zuvor erwähnten Diensten. Daher verwendet er dieselben Zugriffsprotokolle, die bereits erläutert wurden. Jedes Mal, wenn eine Anwendung ein Ticket benötigt, das noch nicht angefordert wurde, wird ein Kontakt mit dem Ticket ausstellenden Server hergestellt. Die Anforderung besteht aus folgenden Komponenten:

- Der angeforderte Prinzipal
- Das Ticket ausstellende Ticket
- Ein Authentifikator

Wie jeder andere Server überprüft der Ticket ausstellende Server jetzt das Ticket ausstellende Ticket und den Authentifikator. Wenn diese gültig sind, erstellt der Ticket ausstellende Server einen neuen Sitzungsschlüssel zur Verwendung durch den ursprünglichen Client und den neuen Server. Darauf wird das Ticket für den neuen Server erstellt. Es enthält folgende Informationen:

- Der Prinzipal des Client
- Der Prinzipal des Servers
- Die aktuelle Zeit
- Die Client-IP-Adresse
- Der neu generierte Sitzungsschlüssel

Das neue Ticket erhält eine Lebensdauer, die geringer ist als die restliche Lebensdauer des Ticket ausstellenden Tickets und des Standards für den Dienst. Der Client erhält dieses Ticket und den Sitzungsschlüssel, die durch den Ticket ausstellenden Dienst versendet werden. Aber dieses Mal ist die Antwort mit dem Sitzungsschlüssel verschlüsselt, der zum ursprünglichen Ticket ausstellenden Ticket gehört. Der Client kann die Antwort ohne ein Benutzerpasswort entschlüsseln, wenn ein neuer Dienst kontaktiert wird. So kann Kerberos Ticket um Ticket für den Client erwerben, ohne dass der Benutzer mehr als einmal bei der Anmeldung belästigt wird.

38.2.5 Kompatibilität mit Windows 2000

Windows 2000 enthält eine Microsoft-Implementierung von Kerberos 5. Da openSUSE® die MIT-Implementierung von Kerberos 5 verwendet, finden Sie in der MIT-Dokumentation nützliche Informationen und Hilfestellungen. Weitere Informationen hierzu finden Sie unter [Abschnitt 38.4, „Weiterführende Informationen“](#) (S. 702).

38.3 Benutzeransicht von Kerberos

Der einzige Kontakt eines Benutzers mit Kerberos findet idealerweise nur während der Anmeldung bei der Arbeitsstation statt. Der Anmeldevorgang beinhaltet den Erhalt eines Ticket ausstellenden Tickets. Bei der Abmeldung werden die Kerberos-Tickets eines Benutzers automatisch vernichtet. Dadurch wird eine Identitätsübernahme durch andere erschwert. Durch den automatischen Ablauf eines Tickets kann es zu der seltenen Situation kommen, dass die Anmeldesitzung des Benutzers länger dauert als die maximale Lebensdauer des Ticket ausstellenden Tickets (die übliche Einstellung beträgt 10 Stunden). Der Benutzer kann jedoch ein neues Ticket ausstellendes Ticket erhalten, indem `kinit` ausgeführt wird. Geben Sie erneut das Passwort ein. Kerberos erhält ohne zusätzliche Authentifizierung Zugriff auf die gewünschten Dienste. Wenn Sie eine Liste aller im Hintergrund erworbenen Tickets von Kerberos sehen möchten, führen Sie `klist` aus.

Hier sehen Sie eine kurze Liste einiger Anwendungen, die die Kerberos-Authentifizierung verwenden. Diese Anwendungen finden Sie unter `/usr/lib/mit/bin` oder `/usr/lib/mit/sbin`. Sie alle verfügen über die volle Funktionalität der gemeinsamen UNIX- und Linux-Systeme und der zusätzlichen transparenten Authentifizierung durch Kerberos.

- `telnet`, `telnetd`
- `rlogin`
- `rsh`, `rcp`, `rshd`
- `ftp`, `ftpd`
- `ksu`

Sie müssen zur Nutzung dieser Anwendungen kein Passwort mehr eingeben, da Kerberos Ihre Identität bereits bewiesen hat. Wenn `ssh` mit Kerberos-Unterstützung kompiliert wird, können alle für eine Arbeitsstation erworbenen Tickets sogar an eine andere weitergeleitet werden. Wenn Sie zur Anmeldung bei einer weiteren Arbeitsstation `ssh` verwenden, stellt `ssh` sicher, dass die verschlüsselten Ticket-Inhalte der neuen Situation angepasst werden. Einfaches Kopieren von Tickets zwischen Arbeitsplatzrechnern ist nicht ausreichend, da das Ticket arbeitsstationsspezifische Informationen (die IP-Adresse) enthält. XDM, GDM und KDM bieten ebenfalls Kerberos-Unterstützung. Im

Benutzerhandbuch zu Kerberos V5 UNIX unter <http://web.mit.edu/kerberos> erfahren Sie mehr zu den Kerberos-Netzwerkanwendungen.

38.4 Weiterführende Informationen

Die offizielle Website von MIT Kerberos lautet <http://web.mit.edu/kerberos>. Hier finden Sie Links zu anderen wichtigen Kerberos-Ressourcen, z. B. die Kerberos-Installation, die Benutzer- und Administratorhandbücher.

Unter <ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS> erhalten Sie einen umfassenden und einfach gestalteten Einblick in die grundlegenden Funktionen von Kerberos. Außerdem erhalten Sie zusätzliche Hinweise zu genaueren Informationen zu Kerberos.

Häufige Fragen zu Kerberos finden Sie auf der offiziellen Website <http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>. Das Buch *Kerberos – A Network Authentication System* von Brian Tung (ISBN 0-201-37924-4) liefert umfassende Informationen.

Installation und Administration von Kerberos

39

Eine Kerberos-Umgebung, wie sie unter **Kapitel 38, *Netzwerk-Authentifizierung – Kerberos*** (S. 695) beschrieben wird, besteht aus verschiedenen Komponenten. Ein Key Distribution Center (KDC) enthält die zentrale Datenbank mit allen Kerberos-relevanten Daten. Alle Clients benötigen das KDC für die ordnungsgemäße Authentifizierung im Netzwerk. Das KDC und die Clients müssen konfiguriert werden, um Ihrem Setup zu entsprechen:

Allgemeine Vorbereitungen

Überprüfen Sie Ihr Netzwerk-Setup und stellen Sie sicher, dass es die unter **Abschnitt 39.1, „Kerberos-Netzwerktopologie“** (S. 704) beschriebenen Mindestvoraussetzungen erfüllt. Wählen Sie einen passenden Bereich für das Kerberos-Setup aus, siehe **Abschnitt 39.2, „Auswählen der Kerberos-Bereiche“** (S. 705). Richten Sie den Computer, der als KDC fungieren soll, mit Bedacht ein und wenden Sie strenge Sicherheitsvorkehrungen an, siehe **Abschnitt 39.3, „Einrichten der KDC-Hardware“** (S. 706). Richten Sie eine verlässliche Zeitquelle im Netzwerk ein und stellen Sie sicher, dass alle Tickets gültige Zeitstempel enthalten, siehe **Abschnitt 39.4, „Konfiguration der Zeitsynchronisierung“** (S. 707).

Grundlegende Konfiguration

Konfigurieren Sie das KDC und die Clients, siehe **Abschnitt 39.5, „Konfigurieren des KDC“** (S. 708) und **Abschnitt 39.6, „Konfigurieren von Kerberos-Clients“** (S. 711). Aktivieren Sie die Remoteverwaltung für den Kerberos-Dienst, damit Sie keinen physikalischen Zugriff auf den KDC-Computer benötigen, siehe **Abschnitt 39.7, „Konfigurieren der Kerberos-Remoteverwaltung“** (S. 717). Erstellen Sie Dienstprinzipalnamen für alle Dienste im Bereich, siehe **Abschnitt 39.8, „Erstellen der Kerberos-Dienst-Prinzipale“** (S. 719).

Aktivieren der Kerberos-Authentifizierung

Verschiedene Dienste im Netzwerk können Kerberos nutzen. Gehen Sie wie in [Abschnitt 39.9, „Aktivieren der PAM-Unterstützung für Kerberos“](#) (S. 721) erläutert vor, um Kerberos-Passwortüberprüfung zu Anwendungen, die PAM verwenden, hinzuzufügen. Um SSH oder LDAP mit Kerberos-Authentifizierung zu konfigurieren, gehen Sie wie unter [Abschnitt 39.10, „Konfigurieren von SSH für die Kerberos-Authentifizierung“](#) (S. 722) und [Abschnitt 39.11, „Verwenden von LDAP und Kerberos“](#) (S. 723) beschrieben vor.

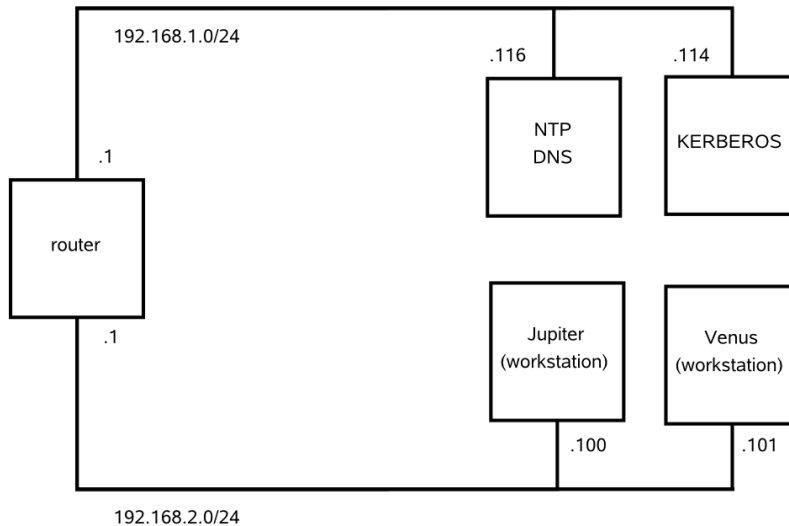
39.1 Kerberos-Netzwerktopologie

Alle Kerberos-Umgebungen müssen den folgenden Anforderungen entsprechen, um voll funktionsfähig zu sein:

- Geben Sie einen DNS-Server für die Namensauflösung im Netzwerk an, damit Clients und Server sich gegenseitig finden können. Informationen zum DNS-Setup finden Sie unter [Kapitel 22, *Domain Name System \(DNS\)*](#) (S. 399).
- Stellen Sie einen Zeitserver im Netzwerk bereit. Das Verwenden exakter Zeitstempel ist beim Kerberos-Setup von zentraler Bedeutung, da gültige Kerberos-Tickets korrekte Zeitstempel enthalten müssen. Informationen zum NTP-Setup finden Sie unter [Kapitel 24, *Zeitsynchronisierung mit NTP*](#) (S. 443).
- Stellen Sie ein Key Distribution Center (KDC) als Zentralstück der Kerberos-Architektur bereit. Es enthält die Kerberos-Datenbank. Verwenden Sie die auf diesem Computer höchstmögliche Sicherheitsrichtlinie, um Angriffe auf diesen Computer zu verhindern, die Ihre gesamte Infrastruktur beschädigen könnten.
- Konfigurieren Sie die Clientcomputer für die Verwendung der Kerberos-Authentifizierung.

Die folgende Abbildung zeigt ein einfaches Beispielnetzwerk mit den für das Erstellen einer Kerberos-Infrastruktur mindestens erforderlichen Komponenten. Je nach Größe und Topologie Ihrer Bereitstellung müssen Sie möglicherweise ein anderes Setup verwenden.

Abbildung 39.1 Kerberos-Netzwerktopologie



TIPP: Konfigurieren des Teilnetz-Routings

Für ein Setup ähnlich dem in [Abbildung 39.1](#), „Kerberos-Netzwerktopologie“ (S. 705) müssen Sie ein Routing zwischen den beiden Teilnetzen (192.168.1.0/24 and 192.168.2.0/24) konfigurieren. Weitere Informationen zum Konfigurieren des Routings mit YaST finden Sie unter [„Konfigurieren des Routing“](#) (S. 362).

39.2 Auswählen der Kerberos-Bereiche

Die Domäne einer Kerberos-Installation wird als Bereich bezeichnet und mit einem Namen identifiziert, z. b. `EXAMPLE.COM` oder einfach `BUCHHALTUNG`. Kerberos unterstützt die Groß-/Kleinschreibung, daher ist `example.com` ein anderer Bereich als `EXAMPLE.COM`. Verwenden Sie nach Ihrem Belieben Groß- oder Kleinschreibung. Gewöhnlich verwendet man jedoch Bereichsnamen in Großbuchstaben.

Daher ist ihr DNS-Domänenname (oder eine Unterdomäne, wie `ACCOUNTING.EXAMPLE.COM`) eine gute Wahl. Wie Sie im Folgenden sehen werden, wird Ihre Arbeit als Administrator wesentlich einfacher, wenn Sie Ihre Kerberos-Clients so konfigurieren, dass die KDC- und andere Kerberos-Dienste über DNS gesucht werden. Dafür ist es hilfreich, wenn Ihr Bereichsname eine Unterdomäne Ihres DNS Domain Name ist.

Anders als der DNS-Namespace ist Kerberos nicht hierarchisch. Es ist nicht möglich, einen Bereich `EXAMPLE.COM` einzurichten und diesem zwei „Bereiche“ `ENTWICKLUNG` und `BUCHHALTUNG` unterzuordnen, die automatisch die Prinzipale von `EXAMPLE.COM` erben. Stattdessen benötigen Sie drei separate Bereiche, für die Sie eine bereichsübergreifende Authentifizierung konfigurieren müssen, damit Benutzer mit Servern oder Benutzern aus anderen Bereichen kommunizieren können.

Lassen Sie uns der Einfachheit halber annehmen, Sie richten für Ihr gesamtes Unternehmen nur einen Bereich ein. Im Weiteren wird daher der Bereichsname `BEISPIEL.COM` für alle Beispiele verwendet.

39.3 Einrichten der KDC-Hardware

Zum Einsatz von Kerberos benötigen Sie zuallererst eine Maschine, die als Schlüsselverteilungszentrum (Key Distribution Center = KDC) fungiert. Diese Maschine enthält die gesamte Kerberos-Benutzerdatenbank mit Passwörtern und allen Informationen.

Das KDC ist der wichtigste Teil Ihrer Sicherheitsinfrastruktur. Bei einem unberechtigten Zugriff sind alle Benutzerkonten und Ihre gesamte, von Kerberos geschützte, Infrastruktur gefährdet. Ein Angreifer mit Zugriff auf die Kerberos-Datenbank kann die Identität jedes Prinzipals in der Datenbank übernehmen. Erhöhen Sie die Sicherheit für diese Maschine so weit wie möglich:

- 1 Stellen Sie den Server an einen sicheren Ort, beispielsweise in einen verschlossenen Serverraum, zu dem nur sehr wenige Personen Zugang haben.
- 2 Führen Sie keine Netzwerkanwendungen darauf aus, außer dem KDC. Dies gilt auch für Server und Clients. Das KDC sollte beispielsweise keine Dateisysteme über NFS importieren oder DHCP zum Abrufen der Netzwerkkonfiguration verwenden.

- 3 Installieren Sie zuerst ein minimales System. Wählen Sie dann die Liste der installierten Pakete aus und entfernen Sie alle unnötigen. Dazu gehören Server, wie `inetd`, `portmap` und `cups` sowie alle Programme auf X-Basis. Sogar die Installation eines SSH-Servers ist ein potenzielles Sicherheitsrisiko.
- 4 Auf dieser Maschine ist keine grafische Anmeldung möglich, da ein X-Server ein potenzielles Sicherheitsrisiko darstellt. Kerberos bietet seine eigene administrative Schnittstelle.
- 5 Konfigurieren Sie `/etc/nsswitch.conf` so, dass nur lokale Dateien zur Suche nach Benutzern und Gruppen verwendet werden. Ändern Sie die Zeilen für `passwd` und `group`, damit sie wie folgt aussehen:

```
passwd:      files
group:       files
```

Bearbeiten Sie die Dateien `passwd`, `group`, und `shadow` unter `/etc` und entfernen Sie die Zeilen, die mit einem `+`-Zeichen beginnen (diese werden für NIS-Suchen verwendet).

- 6 Deaktivieren Sie alle Benutzerkonten außer das Konto des `root`, indem Sie die Datei `/etc/shadow` bearbeiten und die Rautezeichen für Passwörter durch die Zeichen `*` oder `!` ersetzen.

39.4 Konfiguration der Zeitsynchronisierung

Beim Einsatz von Kerberos sollten Sie sich vergewissern, dass alle Systemuhren Ihrer Organisation innerhalb eines gewissen Bereichs synchronisiert sind. Das ist wichtig, weil Kerberos vor dem erneuten Senden der Zugangsdaten schützt. Ein Angreifer könnte die Kerberos-Zugangsdaten im Netzwerk beobachten und dann für den Angriff auf den Server verwenden. Kerberos verwendet mehrere Verteidigungsstrategien, um das zu verhindern. Eine davon sind die Zeitstempel der Tickets. Wenn ein Server ein Ticket mit einem Zeitstempel erhält, der sich von der aktuellen Zeit unterscheidet, weist er das Ticket zurück.

Kerberos erlaubt eine geringfügige Abweichung beim Vergleichen der Zeitstempel. Systemuhren können jedoch bei der Zeitmessung enorm fehlerhaft sein. Es kommt vor,

dass PC-Uhren innerhalb von einer Woche eine halbe Stunde vor- oder nachgehen. Aus diesem Grund sollten Sie festlegen, dass alle Hosts im Netzwerk ihre Uhren mit einer zentralen Zeitquelle synchronisieren.

Ein einfacher Weg ist die Installation eines NTP-Zeitserver auf einer Maschine, mit dem alle Clients ihre Uhren synchronisieren. Hierfür führen Sie entweder einen NTP-Daemon im Client-Modus auf diesen Rechnern aus oder führen einmal pro Tag `ntpdate` auf allen Clients aus (diese Lösung eignet sich nur bei einer geringen Anzahl von Clients). Das KDC selbst muss ebenfalls mit der gemeinsamen Zeitquelle synchronisiert werden. Da es ein Sicherheitsrisiko wäre, einen NTP-Daemon auf dieser Maschine auszuführen, sollten Sie das tun, indem Sie `ntpdate` über einen cron-Eintrag ausführen. Zum Konfigurieren Ihrer Maschine als NTP-Client, gehen Sie vor wie unter [Abschnitt 24.1, „Konfigurieren eines NTP-Client mit YaST“](#) (S. 443) erläutert.

Außerdem ist es möglich, die maximale Abweichung von Kerberos beim Überprüfen der Zeitstempel anzupassen. Dieser Wert (genannt *Zeitdifferenz*) kann in der Datei `krb5.conf` eingestellt werden, wie unter [„Anpassen der Zeitdifferenz“](#) (S. 717) beschrieben.

39.5 Konfigurieren des KDC

In diesem Abschnitt wird die anfängliche Konfiguration und Installation des KDC erläutert, einschließlich dem Erstellen eines administrativen Prinzipals. Dieser Vorgang besteht aus mehreren Schritten:

- 1 Installieren der RPMs** Auf einer als KDC bestimmten Maschine installieren Sie spezielle Softwarepakete. Verwenden Sie YaST für die Installation der `krb5`-, `krb5-Server`- und `krb5-Client`-Pakete
- 2 Anpassen der Konfigurationsdateien** Die Konfigurationsdateien `/etc/krb5.conf` und `/var/lib/kerberos/krb5kdc/kdc.conf` müssen Ihrem Szenario angepasst werden. Diese Dateien enthalten alle Informationen zum KDC.
- 3 Erstellen der Kerberos-Datenbank** Kerberos unterhält eine Datenbank aller Prinzipal-Kennungen und die geheimen Schlüssel aller Prinzipals, die beglaubigt werden müssen. Weitere Informationen finden Sie unter [Abschnitt 39.5.1, „Einrichten der Datenbank“](#) (S. 709).

- 4 Anpassen der ACL-Dateien: Hinzufügen von Administratoren** Die Kerberos-Datenbank des KDC kann entfernt verwaltet werden. Damit der Zugriff auf die Datenbank durch unberechtigte Prinzipale verhindert wird, verwendet Kerberos Zugriffskontrolllisten. Sie müssen den entfernten Zugriff für den Administrator-Prinzipal zum Verwalten der Datenbank explizit erlauben. Die Kerberos-ACL-Datei befindet sich unter `/var/lib/kerberos/krb5kdc/kadm5.acl`. Weitere Informationen finden Sie unter [Abschnitt 39.7, „Konfigurieren der Kerberos-Remoteverwaltung“](#) (S. 717).
- 5 Anpassen der Kerberos-Datenbank: Hinzufügen von Administratoren** Sie benötigen zum Ausführen und Verwalten von Kerberos mindestens einen Administrator-Prinzipal. Dieser Prinzipal muss hinzugefügt werden, bevor das KDC gestartet wird. Weitere Informationen finden Sie unter [Abschnitt 39.5.2, „Erstellen eines Prinzipals“](#) (S. 710).
- 6 Starten des Kerberos-Daemons** Sobald die KDC-Software installiert und korrekt konfiguriert ist, starten Sie den Kerberos-Daemon, damit die Dienste von Kerberos in Ihrem Bereich zur Verfügung stehen. Weitere Informationen finden Sie unter [Abschnitt 39.5.3, „Starten des KDC“](#) (S. 711).
- 7 Erstellen eines Prinzipals für Sie selbst** Sie selbst benötigen einen Prinzipal. Weitere Informationen finden Sie unter [Abschnitt 39.5.2, „Erstellen eines Prinzipals“](#) (S. 710).

39.5.1 Einrichten der Datenbank

Ihr nächster Schritt ist die Initialisierung der Datenbank, in der Kerberos alle Informationen zu Prinzipalen speichert. Richten Sie den Datenbank-Master-Schlüssel ein, der die Datenbank vor versehentlicher Offenlegung schützt, vor allem wenn sie auf ein Band gesichert wird. Der Master-Schlüssel besteht aus einem Passwortsatz, der in einer Datei namens Stapeldatei gespeichert wird. So müssen Sie das Passwort nicht bei jedem Start des KDC erneut eingeben. Wählen Sie unbedingt eine gute Passphrase, wie einen Satz aus einem Buch, das Sie auf einer willkürlichen Seite öffnen.

Wenn Sie die Kerberos-Datenbank auf Band sichern (`/var/lib/kerberos/krb5kdc/principal`), sollten Sie die Stapeldatei nicht mitsichern (Sie befindet sich unter `/var/lib/kerberos/krb5kdc/.k5.EXAMPLE.COM`). Anderenfalls kann jeder, der das Band liest, auch die Datenbank entschlüsseln. Daher sollten Sie eine Kopie der Passphrase in einem Safe oder an einem anderen sicheren Ort aufbewah-

ren. Sie brauchen sie zum Wiederherstellen Ihrer Datenbank vom Band nach einem Absturz.

Zum Erstellen der Stapeldatei und der Datenbank führen Sie Folgendes aus:

```
$> kdb5_util create -r EXAMPLE.COM -s
Initializing database '/var/lib/kerberos/krb5kdc/principal' for realm
'EXAMPLE.COM',
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key: <= Type the master password.
Re-enter KDC database master key to verify: <= Type it again.
$>
```

Zum Überprüfen der Funktion verwenden Sie den Befehl "list":

```
$>kadmin.local
kadmin> listprincs
K/M@EXAMPLE.COM
kadmin/admin@EXAMPLE.COM
kadmin/changepw@EXAMPLE.COM
krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

Sie sehen, dass es eine Reihe von Prinzipalen in der Datenbank gibt. Alle sind für den internen Gebrauch von Kerberos bestimmt.

39.5.2 Erstellen eines Prinzipals

Erstellen Sie als nächstes zwei Kerberos-Prinzipale für sich selbst: einen normalen Prinzipal für die täglich anfallenden Arbeiten und einen für auf Kerberos- bezogene Verwaltungsaufgaben. Nehmen wir an, Ihr Anmeldename sei *newbie*. Gehen Sie wie folgt vor:

```
kadmin.local

kadmin> ank newbie
newbie@EXAMPLE.COM's Password: <type password here>
Verifying password: <re-type password here>
```

Erstellen Sie einen weiteren Prinzipal mit dem Namen *newbie/admin*, indem Sie an der Eingabeaufforderung *kadmin* den Eintrag *ank newbie/admin* eingeben. Das Suffix *admin* nach Ihrem Benutzernamen ist eine *Rolle*. Später verwenden wir

diese Rolle bei der Verwaltung der Kerberos-Datenbank. Ein Benutzer kann für verschiedene Zwecke verschiedene Rollen haben. Rollen sind komplett verschiedene Konten mit ähnlichen Namen.

39.5.3 Starten des KDC

Starten Sie den KDC-Daemon und den kadmind-Daemon. Um die Daemons manuell zu starten, geben Sie `rckrb5kdc start` und `rckadmind start` ein. Stellen Sie darüber hinaus sicher, dass KDC und kadmind standardmäßig gestartet werden, wenn der Server mit den Befehlen `insserv krb5kdc` und `insserv kadmind` neu gebootet wird.

39.6 Konfigurieren von Kerberos-Clients

Sobald die unterstützende Infrastruktur (DNS, NTP) eingerichtet und das KDC ordnungsgemäß konfiguriert und gestartet wurde, konfigurieren Sie die Clientcomputer. Sie können entweder YaST zum Konfigurieren eines Kerberos-Clients oder eine der beiden unten beschriebenen manuellen Vorgehensweisen verwenden.

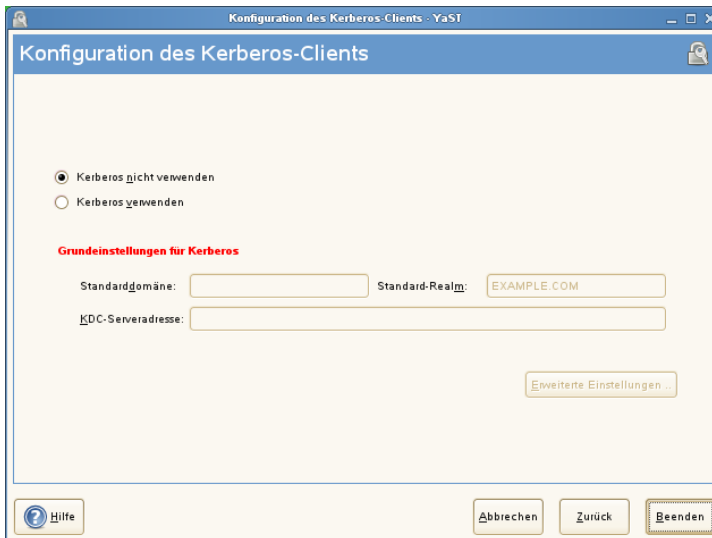
39.6.1 Konfigurieren von Kerberos-Clients mit YaST

Anstatt beim Konfigurieren eines Kerberos-Clients alle relevanten Konfigurationsdateien manuell zu bearbeiten, können Sie YaST diese Aufgabe für Sie erledigen lassen. Sie können die Clientkonfiguration entweder während der Installation auf Ihrem Computer oder im installierten System durchführen:

- 1 Melden Sie sich als `root` an und wählen Sie *Netzwerkdienste > Kerberos-Client*.
- 2 Wählen Sie *Kerberos verwenden*.
- 3 Zur Konfiguration eines DNS-basierten Kerberos-Clients gehen Sie wie folgt vor:

- 3a** Bestätigen Sie die angezeigten *Kerberos-Grundeinstellungen*.
- 3b** Klicken Sie auf *Erweiterte Einstellungen*, um die Einzelheiten in Bezug auf Tickets, Unterstützung von OpenSSH und Zeitsynchronisation zu konfigurieren.
- 4** Zur Konfiguration eines statischen Kerberos-Clients gehen Sie wie folgt vor:
- 4a** Legen Sie die *Standarddomäne*, den *Standardbereich* und die *KDC-Serveradresse* fest, sodass sie zu Ihrer Installation passen.
- 4b** Klicken Sie auf *Erweiterte Einstellungen*, um die Einzelheiten in Bezug auf Tickets, Unterstützung von OpenSSH und Zeitsynchronisation zu konfigurieren.

Abbildung 39.2 *YaST: Grundlegende Konfiguration von Kerberos-Clients*



Wenn Sie die Ticket-Optionen im Dialogfeld *Erweiterte Einstellungen* konfigurieren, können Sie aus folgenden Optionen wählen:

- Geben Sie die *Standardlebensdauer* des Tickets und den *Standardwert für erneuerbare Lebensdauer* in Tagen, Stunden oder Minuten an (Verwenden Sie die Maßeinheiten *d*, *h* und *m* ohne Leerzeichen zwischen dem Wert und der Maßeinheit).
- Wenn Sie Ihre vollständige Identität weiterleiten möchten, um Ihre Tickets auf anderen Hosts zu verwenden, wählen Sie *Weiterleitbar*.
- Aktivieren Sie den Transfer bestimmter Tickets mit *Weitervermittelbar*.
- Mit einem PAM-Modul bleiben die Tickets verfügbar, auch nach dem Ende einer Sitzung, wenn Sie *Beibehalten* aktivieren.
- Aktivieren Sie die Kerberos-Authentifizierungsunterstützung für Ihren OpenSSH-Client, indem Sie das entsprechende Kontrollkästchen auswählen. Der Client verwendet dann Kerberos-Tickets zur Authentifizierung bei dem SSH-Server.
- Schließen Sie eine Reihe von Benutzerkonten von der Nutzung der Kerberos-Authentifizierung aus, indem Sie einen Wert für die *Minimum UID* (Minimale UID) festlegen, über die ein Benutzer dieser Funktion verfügen muss. Eventuell möchten Sie z. B. den Systemadministrator (`root`) ausschließen.
- Verwenden Sie die *Zeitdifferenz*, um einen Wert für die zulässige Differenz zwischen Zeitstempel und der Systemzeit des Hosts festzulegen.
- Damit das System mit einem NTP-Server synchronisiert bleibt, können Sie den Host als NTP-Client einrichten, indem Sie *NTP-Konfiguration* wählen. Das unter [Abschnitt 24.1, „Konfigurieren eines NTP-Client mit YaST“](#) (S. 443) beschriebene NTP-Client-Dialogfeld von YaST wird geöffnet. Nach Abschluss der Konfiguration führt YaST alle erforderlichen Änderungen durch und der Kerberos-Client kann verwendet werden.

Abbildung 39.3 *YaST: Erweiterte Konfiguration von Kerberos-Clients*

39.6.2 Manuelles Konfigurieren der Kerberos-Clients

Bei der Konfiguration von Kerberos gibt es zwei verschiedene Ansätze: die statische Konfiguration in der Datei `/etc/krb5.conf` oder die dynamische Konfiguration mit DNS. Bei der DNS-Konfiguration suchen die Kerberos-Anwendungen die KDC-Dienste über DNS-Einträge. Bei der statischen Konfiguration fügen Sie die Hostnamen Ihres KDC-Servers der Datei `krb5.conf` hinzu (und aktualisieren Sie die Datei, wenn Sie das KDC verschieben oder Ihren Bereich anderweitig neu konfigurieren).

Die DNS-basierte Konfiguration ist meist viel flexibler und der Arbeitsaufwand pro Maschine ist wesentlich geringer. Ihr Bereichsname muss hierfür jedoch entweder Ihrer DNS-Domäne oder einer Unterdomäne davon entsprechen. Die Konfiguration mit DNS führt zu einem gewissen Sicherheitsrisiko. Ein Angreifer kann Ihre Infrastruktur über den DNS ernsthaft stören (durch Shoot-Down des Namensservers, Spoofing von DNS-Datensätzen usw.). Meistens führt das jedoch zu einem Denial of Service. Ein ähnliches Szenario gilt für die statische Konfiguration, es sei denn, Sie geben IP-Adressen in die Datei `krb5.conf` statt Hostnamen ein.

Statische Konfiguration

Eine Konfigurationsweise von Kerberos ist die Bearbeitung der Konfigurationsdatei `/etc/krb5.conf`. Die standardmäßig installierte Datei enthält verschiedene Beispieleinträge. Löschen Sie alle Einträge vor dem Start. `krb5.conf` besteht aus mehreren Abschnitten. Jeder beginnt mit dem Abschnittsnamen in Klammern, das sieht z. B. `[so aus]`.

Zur Konfiguration Ihrer Kerberos-Clients fügen Sie der Datei `krb5.conf` den folgenden Absatz hinzu (wobei `kdc.example.com` der Hostname des KDC ist):

```
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
    EXAMPLE.COM = {
        kdc = kdc.example.com
        admin_server = kdc.example.com
    }
```

Die Zeile `default_realm` bestimmt den Standardbereich für Kerberos-Anwendungen. Wenn Sie mehrere Bereiche haben, fügen Sie zusätzliche Anweisungen im Abschnitt `[realms]` hinzu.

Fügen Sie der Datei außerdem eine Anweisung hinzu, die bestimmt, wie Anwendungen Hostnamen einem Bereich zuordnen. Beispiel: Wenn Sie sich bei einem entfernten Host anmelden, muss die Kerberos-Bibliothek wissen, in welchem Bereich sich der Host befindet. Das muss im Abschnitt `[domain_realms]` konfiguriert werden:

```
[domain_realm]
    .example.com = EXAMPLE.COM
    www.foobar.com = EXAMPLE.COM
```

Dadurch weiß die Bibliothek, dass alle Hosts in der Datei `example.com` DNS-Domänen im Kerberos-Bereich `EXAMPLE.COM` sind. Außerdem sollte ein externer Host mit dem Namen `www.foobar.com` als Mitglied des Bereichs `EXAMPLE.COM` betrachtet werden.

DNS-basierte Konfiguration

Die DNS-basierte Kerberos-Konfiguration verwendet die SRV-Datensätze. Siehe (RFC2052) *A DNS RR for specifying the location of services* unter <http://www.ietf.org>. Diese Datensätze werden in früheren Installationen des BIND-Namensservers nicht unterstützt. Dafür ist mindestens die BIND-Version 8 erforderlich.

Der Name eines SRV-Datensatzes ist für Kerberos immer im Format `_service._proto.realm`, wobei "realm" für den Kerberos-Bereich steht. Die Groß-/Kleinschreibung wird bei Domännennamen in DNS nicht beachtet. Daher würden Kerberos-Bereiche mit Groß-/Kleinschreibung bei dieser Konfigurationsmethode zerstört. `_service` ist ein Dienstname (beim Verbindungsversuch mit dem KDC oder dem Passwortdienst werden beispielsweise verschiedene Namen verwendet). `_proto` kann entweder `_udp` oder `_tcp` sein, aber nicht alle Dienste unterstützen beide Protokolle.

Der Datenteil der SRV-Ressourcen-Datensätze besteht aus einem Wert für die Priorität, einer Gewichtung, einer Port-Nummer und einem Hostnamen. Die Priorität legt die Reihenfolge fest, in der die Hosts versucht werden (ein niedriger Wert bedeutet eine niedrigere Priorität). Die Gewichtung unterstützt eine Art Lastenausgleich zwischen Servern mit gleicher Priorität. Sie brauchen diese Werte wahrscheinlich nicht und können sie daher auf Null setzen.

MIT Kerberos sucht derzeit bei der Suche nach Diensten die folgenden Namen:

`_kerberos`

Definiert den Standort des KDC-Daemons (die Authentifizierung und der Ticket ausstellende Server). Ein typischer Datensatz sieht wie folgt aus:

```
_kerberos._udp.EXAMPLE.COM. IN SRV 0 0 88 kdc.example.com.  
_kerberos._tcp.EXAMPLE.COM. IN SRV 0 0 88 kdc.example.com.
```

`_kerberos-adm`

Beschreibt den Standort des entfernten Administrationsdiensts. Ein typischer Datensatz sieht wie folgt aus:

```
_kerberos-adm._tcp.EXAMPLE.COM. IN SRV 0 0 749 kdc.example.com.
```

Da kadmind UDP nicht unterstützt, sollte kein `_udp`-Datensatz vorhanden sein.

Wie bei der statischen Konfigurationsdatei gibt es eine Methode, den Clients mitzuteilen, dass sich ein bestimmter Host im Bereich `EXAMPLE.COM` befindet, auch wenn dieser

nicht zur `example.com`-DNS-Domäne gehört. Das geschieht, indem ein TXT-Datensatz an `_kerberos.hostname` angehängt wird, wie im Folgenden:

```
_kerberos.www.foobar.com. IN TXT "EXAMPLE.COM"
```

Anpassen der Zeitdifferenz

Die *Zeitdifferenz* ist die Toleranz, in der Tickets mit Zeitstempeln akzeptiert werden, die nicht genau der Systemuhr des Hosts entsprechen. Die Zeitdifferenz wird in der Regel auf 300 Sekunden (fünf Minuten) festgelegt. Das bedeutet, ein Ticket kann einen Zeitstempel zwischen fünf Minuten vorher und fünf Minuten nach der Server-Uhr haben.

Wenn Sie NTP zum Synchronisieren aller Hosts einsetzen, können Sie diesen Wert auf ca. eine Minute verringern. Der Wert für die Zeitdifferenz wird in der Datei `/etc/krb5.conf` wie folgt festgelegt:

```
[libdefaults]
    clockskew = 120
```

39.7 Konfigurieren der Kerberos-Remoteverwaltung

Wenn Sie der Kerberos-Datenbank Prinzipale hinzufügen und entfernen möchten, ohne direkt auf die KDC-Konsole zuzugreifen, müssen Sie dem Kerberos-Administrationsserver mitteilen, welche Berechtigungen bestimmte Prinzipale haben. Bearbeiten Sie hierfür die Datei `/var/lib/kerberos/krb5kdc/kadm5.acl`. Die ACL (Zugriffskontrollliste)-Datei ermöglicht die Angabe von Berechtigungen mit einer guten Kontrolle. Weitere Informationen finden Sie auf der man-Seite mit `man 8 kadmind`.

Gewähren Sie sich selbst die absolute Berechtigung für die Datenbank, indem Sie der Datei folgende Zeile hinzufügen:

```
newbie/admin *
```

Ersetzen Sie den Benutzernamen `newbie` durch Ihren eigenen. Starten Sie `kadmind` neu, damit die Änderung wirksam wird.

Jetzt sollten Sie Kerberos-Administrationsaufgaben von einem entfernten Standort mit dem kadmin-Werkzeug durchführen können. Zuerst müssen Sie ein Ticket für Ihre Administrationsrolle abholen und das Ticket bei der Verbindung mit dem kadmin-Server verwenden:

```
kadmin -p newbie/admin
Authenticating as principal newbie/admin@EXAMPLE.COM with password.
Password for newbie/admin@EXAMPLE.COM:
kadmin: getprivs
current privileges: GET ADD MODIFY DELETE
kadmin:
```

Verwenden Sie den Befehl `getprivs`, um Ihre Berechtigungen zu überprüfen. Die obige Liste enthält alle Berechtigungen.

Als Beispiel, ändern Sie `newbie`:

```
kadmin -p newbie/admin
Authenticating as principal newbie/admin@EXAMPLE.COM with password.
Password for newbie/admin@EXAMPLE.COM:

kadmin: getprinc newbie
Principal: newbie@EXAMPLE.COM
Expiration date: [never]
Last password change: Wed Jan 12 17:28:46 CET 2005
Password expiration date: [none]
Maximum ticket life: 0 days 10:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Wed Jan 12 17:47:17 CET 2005 (admin/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, Triple DES cbc mode with HMAC/shal, no salt
Key: vno 1, DES cbc mode with CRC-32, no salt
Attributes:
Policy: [none]

kadmin: modify_principal -maxlife "8 hours" newbie
Principal "newbie@EXAMPLE.COM" modified.
kadmin: getprinc joe
Principal: newbie@EXAMPLE.COM
Expiration date: [never]
Last password change: Wed Jan 12 17:28:46 CET 2005
Password expiration date: [none]
Maximum ticket life: 0 days 08:00:00
Maximum renewable life: 7 days 00:00:00
Last modified: Wed Jan 12 17:59:49 CET 2005 (newbie/admin@EXAMPLE.COM)
Last successful authentication: [never]
```

```
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 2
Key: vno 1, Triple DES cbc mode with HMAC/sha1, no salt
Key: vno 1, DES cbc mode with CRC-32, no salt
Attributes:
Policy: [none]
kadmin:
```

Dadurch wird die maximale Ticketlebensdauer auf acht Stunden geändert. Weitere Informationen zum Befehl `kadmin` und den verfügbaren Optionen finden Sie unter <http://web.mit.edu/kerberos/www/krb5-1.4/krb5-1.4/doc/krb5-admin.html#Kadmin%20Options> oder auf der man-Seite `man8 kadmin`.

39.8 Erstellen der Kerberos-Dienst-Prinzipale

Bis jetzt wurden nur Benutzerberechtigungen erläutert. Kerberos-kompatible Dienste müssen sich jedoch selbst beim Client-Benutzer authentifizieren. Daher müssen spezielle Dienst-Prinzipale in der Kerberos-Datenbank für jeden im Bereich angebotenen Dienst vorhanden sein. Wenn `ldap.example.com` beispielsweise einen LDAP-Dienst anbietet, benötigen Sie einen Dienst-Prinzipal, `ldap/ldap.example.com@EXAMPLE.COM`, um diesen Dienst bei allen Clients zu authentifizieren.

Die Namenkonvention für Dienst-Prinzipale lautet *Dienst/Hostname@BEREICH*, wobei der *Hostname* dem vollständig qualifizierten Hostnamen entspricht.

Gültige Dienst-Deskriptoren sind:

Dienst-Deskriptor	Dienst
host	Telnet, RSH, SSH
nfs	NFSv4 (mit Kerberos-Unterstützung)
HTTP	HTTP (mit Kerberos-Authentifizierung)

Dienst-Deskriptor	Dienst
imap	IMAP
pop	POP3
ldap	LDAP

Dienst-Prinzipale ähneln Benutzer-Prinzipalen, aber es gibt wesentliche Unterschiede. Im Gegensatz zum Schlüssel des Dienst-Prinzipals ist der Schlüssel des Benutzer-Prinzipals durch ein Passwort geschützt. Wenn ein Benutzer ein Ticket zur Ticketausstellung vom KDC erhält, muss er sein Passwort eingeben, damit Kerberos das Ticket entschlüsseln kann. Für den Systemadministrator wäre es ziemlich unpraktisch, wenn alle acht Stunden für den SSH-Daemon neue Tickets ausgestellt werden müssten.

Stattdessen extrahiert der Administrator den Schlüssel zur Entschlüsselung des anfänglichen Tickets für den Dienst-Prinzipal einmal aus dem KDC und speichert ihn in einer lokalen Datei namens *keytab*. Dienste, wie der SSH-Daemon, lesen diesen Schlüssel und nutzen ihn, falls erforderlich, zum automatischen Erhalt neuer Tickets. Die standardmäßige *keytab*-Datei befindet sich im Pfad `/etc/krb5.keytab`.

Zum Erstellen eines Dienst-Prinzipals für `jupiter.example.com` geben Sie die folgenden Kommandos während der *kadmin*-Sitzung ein:

```
kadmin -p newbie/admin
Authenticating as principal newbie/admin@EXAMPLE.COM with password.
Password for newbie/admin@EXAMPLE.COM:
kadmin: addprinc -randkey host/jupiter.example.com
WARNING: no policy specified for host/jupiter.example.com@EXAMPLE.COM;
defaulting to no policy
Principal "host/jupiter.example.com@EXAMPLE.COM" created.
```

Statt ein neues Passwort für den neuen Prinzipal einzurichten, bedeutet das Flag `-randkey` für *kadmin* eine Aufforderung zum Generieren eines willkürlichen Schlüssels. Diese Funktion wird verwendet, weil keine Benutzeraktion für diesen Prinzipal gewünscht ist. Es handelt sich um ein Serverkonto für die Maschine.

Extrahieren Sie nun den Schlüssel und speichern Sie ihn in der lokalen *keytab*-Datei `/etc/krb5.keytab`. Diese Datei gehört dem Superuser. Daher müssen Sie als `root` angemeldet sein, um den nächsten Befehl in der *kadmin*-Shell auszuführen:

```
kadmin: ktadd host/jupiter.example.com
Entry for principal host/jupiter.example.com with kvno 3, encryption type
Triple
DES cbc mode with HMAC/shal added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/jupiter.example.com with kvno 3, encryption type DES
cbc mode with CRC-32 added to keytab WRFILE:/etc/krb5.keytab.
kadmin:
```

Vergewissern Sie sich nach der Fertigstellung, dass Sie das admin-Ticket, das Sie mit `kinit` erhalten haben, mit `kdestroy` vernichten.

39.9 Aktivieren der PAM-Unterstützung für Kerberos

Im Lieferumfang von openSUSE® ist das PAM-Modul `pam_krb5` enthalten, das die Kerberos-Anmeldung und das Kennwort-Update unterstützt. Dieses Modul kann von Anwendungen verwendet werden, wie der Konsolenanmeldung, `su` und grafischen Anmeldeanwendungen, wie KDM, bei der der Benutzer ein Passwort eingeben muss und verlangt, dass die authentifizierende Anwendung ein anfängliches Kerberos-Ticket für ihn abholt. Verwenden Sie das folgende Kommando, um die PAM-Unterstützung für Kerberos zu konfigurieren:

```
pam-config --add --krb5
```

Mit dem obigen Kommando wird das Modul `pam_krb5` zu den vorhandenen PAM-Konfigurationsdateien hinzugefügt und sichergestellt, dass es in der richtigen Reihenfolge aufgerufen wird. Wenn Sie die Verwendung der Datei `pam_krb5` optimieren möchten, bearbeiten Sie die Datei `/etc/krb5.conf` und fügen Sie `pam` die Standardanwendungen hinzu. Genauere Einzelheiten finden Sie auf der Handbuchseite `man 5 pam_krb5`.

Das `pam_krb5`-Modul ist nicht für Netzwerkdienste geeignet, die Kerberos-Tickets als Teil der Benutzerauthentifizierung verwenden. Das ist ein völlig anderes Thema und wird im Folgenden behandelt.

39.10 Konfigurieren von SSH für die Kerberos-Authentifizierung

OpenSSH unterstützt die Kerberos-Authentifizierung in beiden Protokollversionen 1 und 2. Bei Version 1 gibt es spezielle Protokollmeldungen zur Übertragung von Kerberos-Tickets. Bei Version 2 wird Kerberos nicht mehr direkt verwendet, sondern GSSAPI, das General Security Services API. Hierbei handelt es sich um eine Programmierschnittstelle, die nicht Kerberos-spezifisch ist. Sie wurde konzipiert, um die Eigenheiten des zugrunde liegenden Authentifizierungssystems (Kerberos, Public-Key-Authentifizierungssysteme wie SPKM oder andere) zu kaschieren. Die im Lieferumfang enthaltene GSSAPI-Bibliothek unterstützt jedoch nur Kerberos.

Zur Verwendung von `sshd` mit der Kerberos-Authentifizierung bearbeiten Sie `/etc/ssh/sshd_config` und legen folgende Optionen fest:

```
# These are for protocol version 1
#
# KerberosAuthentication yes
# KerberosTicketCleanup yes

# These are for version 2 - better to use this
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

Starten Sie dann Ihren SSH-Daemon mit dem Befehl `rcsshd restart` neu.

Wenn Sie die Kerberos-Authentifizierung mit der Protokollversion 2 verwenden möchten, aktivieren Sie sie auch auf der Client-Seite. Verwenden Sie hierfür entweder die systemweite Konfigurationsdatei `/etc/ssh/ssh_config` oder bearbeiten Sie die Datei `~/.ssh/config` für einzelne Benutzer. Fügen Sie in beiden Fällen die Option `GSSAPIAuthentication yes` hinzu.

Jetzt sollten Sie sich mithilfe der Kerberos-Authentifizierung verbinden können. Verwenden Sie `klist`, um sicherzustellen, dass Sie ein gültiges Ticket haben, und verbinden Sie sich dann mit dem SSH-Server. Wenn Sie die SSH-Protokollversion 1 erzwingen möchten, geben Sie bei der Kommandozeile die Option `-1` an.

TIPP: Weitere Informationen

Die Datei `/usr/share/doc/packages/openssh/README.kerberos` erläutert die Interaktion von OpenSSH und Kerberos genauer.

39.11 Verwenden von LDAP und Kerberos

Wenn Sie Kerberos einsetzen, können Sie die Benutzerinformationen (wie Benutzer-ID, Gruppen und Home-Verzeichnis) in Ihrem lokalen Netzwerk mithilfe von LDAP verteilen. Dafür ist ein starker Authentifizierungsmechanismus erforderlich, der Paket-Spoofing und andere Angriffe verhindert. Eine Lösung ist die Nutzung von Kerberos für die LDAP-Kommunikation.

OpenLDAP implementiert die meisten Authentifizierungsarten über SASL, die einfache Authentifizierungs-Sitzungsschicht. SASL ist eigentlich ein Netzwerkprotokoll für die Authentifizierung. Die SASL-Installation ist `cyrus-sasl`, das eine Reihe verschiedener Authentifizierungsarten unterstützt. Die Kerberos-Authentifizierung wird mithilfe von GSSAPI durchgeführt (General Security Services API). Standardmäßig ist das SASL-Plugin für GSSAPI nicht installiert. Installieren Sie es manuell mit `rpm -ivh cyrus-sasl-gssapi-*.rpm`.

Wenn Sie Kerberos den Bind mit dem OpenLDAP-Server ermöglichen möchten, müssen Sie einen Prinzipal `ldap/earth.example.com` erstellen und der `keytab`-Datei hinzufügen.

Standardmäßig wird der LDAP-Server `slapd` als Benutzer- und Gruppen-`ldap` ausgeführt, während die `keytab`-Datei nur von `root` gelesen werden kann. Sie können daher entweder die LDAP-Konfiguration ändern, damit der Server als `root` ausgeführt wird, oder die `keytab`-Datei für die Gruppe `ldap` lesbar machen. Letzteres wird automatisch vom OpenLDAP-Startskript (`/etc/init.d/ldap`) ausgeführt, wenn die `keytab`-Datei in der Variable `OPENLDAP_KRB5_KEYTAB` in `/etc/sysconfig/openldap` angegeben wurde und wenn die Variable `OPENLDAP_CHOWN_DIRS` auf `yes` eingestellt ist (die Standardeinstellung). Wenn `OPENLDAP_KRB5_KEYTAB` leer gelassen wird, wird die standardmäßige `keytab`-Datei unter `/etc/krb5.keytab` verwendet und Sie müssen die Berechtigungen, wie im Folgenden beschrieben, selbst anpassen.

Wenn Sie `slapd` als `root` ausführen möchten, bearbeiten Sie `/etc/sysconfig/openldap`. Deaktivieren Sie die Variablen `OPENLDAP_USER` und `OPENLDAP_GROUP`, indem Sie ein Kommentarzeichen davor setzen.

Um die `keytab`-Datei für die Gruppe LDAP lesbar zu machen, führen Sie Folgendes aus:

```
chgrp ldap /etc/krb5.keytab
chmod 640 /etc/krb5.keytab
```

Eine dritte und vielleicht die beste Lösung ist es, wenn Sie OpenLDAP anweisen, eine spezielle `keytab`-Datei zu verwenden. Dafür starten Sie `kadmin` und geben Sie den folgenden Befehl ein, nachdem Sie den Prinzipal `ldap/earth.example.com` hinzugefügt haben:

```
ktadd -k /etc/openldap/ldap.keytab ldap/earth.example.com@EXAMPLE.COM
```

Auf der Shell führen Sie dann Folgendes aus:

```
chown ldap.ldap /etc/openldap/ldap.keytab
chmod 600 /etc/openldap/ldap.keytab
```

Wenn Sie OpenLDAP anweisen möchten, eine andere `keytab`-Datei zu verwenden, ändern Sie die folgende Variable in `/etc/sysconfig/openldap`:

```
OPENLDAP_KRB5_KEYTAB="/etc/openldap/ldap.keytab"
```

Starten Sie schließlich den LDAP-Server mit `rcldaprestart` neu.

39.11.1 Verwenden der Kerberos-Authentifizierung mit LDAP

Jetzt sollten Sie Werkzeuge, wie `ldapsearch`, mit der Kerberos-Authentifizierung automatisch verwenden können.

```
ldapsearch -b ou=people,dc=example,dc=com '(uid=newbie)'

SASL/GSSAPI authentication started
SASL SSF: 56
SASL installing layers
[...]

# newbie, people, example.com
dn: uid=newbie,ou=people,dc=example,dc=com
uid: newbie
cn: Olaf Kirch
[...]
```

Wie Sie sehen, gibt `ldapsearch` eine Meldung aus, dass die GSSAPI-Authentifizierung gestartet wurde. Die nächste Meldung ist sehr unverständlich, aber sie zeigt, dass der *Security Strength Factor* (SSF) 56 beträgt. (Der Wert 56 ist etwas willkürlich. Wahrscheinlich wurde er gewählt, weil diese Anzahl an Bits in einem DES-Verschlüsselungsschlüssel enthalten ist.) Das bedeutet, dass die GSSAPI-Authentifizierung erfolgreich war und dass der Datenschutz und die Vertraulichkeit der LDAP-Verbindung mittels Verschlüsselung gewährleistet ist.

In Kerberos ist die Authentifizierung immer gegenseitig. Das bedeutet, dass Sie sich nicht nur selbst beim LDAP-Server authentifiziert haben, sondern dass sich der LDAP-Server auch bei Ihnen selbst authentifiziert hat. Nun wissen Sie, dass die Kommunikation wirklich mit dem gewünschten LDAP-Server stattfindet und nicht mit einem falschen Dienst, den ein Hacker eingerichtet hat.

39.11.2 Kerberos-Authentifizierung und LDAP-Zugriffskontrolle

Jetzt können Sie jedem Benutzer erlauben, das Anmelde-Shell-Attribut seines LDAP-Benutzerdatensatzes zu ändern. Angenommen Sie haben ein Schema, bei dem der LDAP-Eintrag des Benutzers `joe` sich unter `uid=joe,ou=people,dc=example,dc=com` befindet, richten Sie die folgende Zugriffskontrolle in `/etc/openldap/slapd.conf` ein:

```
# This is required for things to work _at all_
access to dn.base="" by * read
# Let each user change their login shell
access to dn="*,ou=people,dc=example,dc=com" attrs=loginShell
by self write
```

```
# Every user can read everything
access to *
    by users read
```

Die zweite Anweisung gewährt authentifizierten Benutzern Schreibzugriff auf das `loginShell`-Attribut des eigenen LDAP-Eintrags. Die dritte Anweisung gibt allen authentifizierten Benutzern Lesezugriff auf das gesamte LDAP-Verzeichnis.

Es fehlt jedoch ein Puzzle-Teil. Wie findet der LDAP-Server heraus, dass der Kerberos-Benutzer `joe@EXAMPLE.COM` dem LDAP-DN `uid=joe,ou=people,dc=example,dc=com` entspricht? Diese Art der Zuweisung muss manuell konfiguriert werden mit der `saslExpr`-Direktive. In diesem Beispiel fügen Sie Folgendes der Datei `slapd.conf` hinzu:

```
authz-regexp
    uid=(.*),cn=GSSAPI,cn=auth
    uid=$1,ou=people,dc=example,dc=com
```

Um die Funktionsweise zu verstehen, müssen Sie zunächst wissen, dass OpenLDAP bei der Benutzerauthentifizierung über SASL einen DN aus dem von SASL angegebenen Namen (z. B. `joe`) und dem Namen der SASL-Funktion (`GSSAPI`) erstellt. Das Ergebnis lautet: `uid=joe,cn=GSSAPI,cn=auth`.

Wenn ein `authz-regexp` konfiguriert wurde, überprüft er den DN der SASL-Informationen und nimmt dabei das erste Argument als regulären Ausdruck. Wenn dieser reguläre Ausdruck passt, wird der Name durch das zweite Argument der `authz-regexp`-Anweisung ersetzt. Der Platzhalter `$1` wird durch den Substring ersetzt, der dem `(.*)`-Ausdruck entspricht.

Es sind auch kompliziertere Entsprechungsausdrücke möglich. Wenn Sie über eine kompliziertere Verzeichnisstruktur oder ein Schema verfügen, in dem der Benutzername kein Teil des DN ist, können Sie sogar Suchausdrücke verwenden, um den SASL-DN dem Benutzer-DN zuzuweisen.

Verschlüsseln von Partitionen und Dateien

40

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 40.1.1, „Anlegen einer verschlüsselten Partition während der Installation“](#) (S. 729) und [Abschnitt 40.1.2, „Einrichten einer verschlüsselten Partition im laufenden System“](#) (S. 730). Diese Option kann auch für Wechseldatenträger, wie externe Festplatten, verwendet werden (siehe [Abschnitt 40.1.4, „Verschlüsseln des Inhalts von Wechselmedien“](#) (S. 731)).

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 40.1.3, „Erstellen einer verschlüsselten Datei als Container“](#) (S. 731).

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 40.2, „Verwenden von verschlüsselten Home-Verzeichnissen“](#) (S. 732).

Verschlüsselung einzelner Dateien

Wenn Sie nur über eine geringe Anzahl von Dateien mit sensiblen oder vertraulichen Daten verfügen, können Sie diese mithilfe des vi-Editors einzeln verschlüsseln und mit einem Passwort schützen. Weitere Informationen finden Sie unter [Abschnitt 40.3, „Verschlüsselung einzelner Dateien mit vi“](#) (S. 733).

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.

40.1 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.

40.1.1 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 `umountName_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 40.1.2, „Einrichten einer verschlüsselten Partition im laufenden System“** (S. 730) und bedenken Sie, dass durch diese Aktion alle Daten in der bestehenden Partition, die Sie verschlüsseln möchten, gelöscht werden.

40.1.2 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 40.1.1, „Anlegen einer verschlüsselten Partition während der Installation“** (S. 729) beschrieben aus.

40.1.3 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 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.

40.1.4 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 entfernbare Gerät mit LUKS (Linux Unified Key Setup) verschlüsselt haben, erkennen die KDE- und GNOME-Desktops dies automatisch und fordern zur Eingabe des Passwortes auf, sobald das Gerät erkannt wird. Wenn Sie Ihr entfernbare Medium mit einem FAT-Dateisystem formatiert haben, wird der am Desktop angemeldete Benutzer, der das Passwort für die Verschlüsselung eingibt, automatisch zum Eigentümer des Gerätes und kann die Dateien auf diesem Gerät 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.

40.2 Verwenden von verschlüsselten Home-Verzeichnissen

Zum Schutz der Daten in den Home-Verzeichnissen der Benutzer vor Diebstahl (z. B. durch Entfernen der Festplatte) sollten Sie die Home-Verzeichnisse mit dem LUKS-Framework verschlüsseln. LUKS erstellt ein Image sowie einen Image-Schlüssel. Der Image-Schlüssel ist durch das Anmeldepasswort des Benutzers geschützt. Standardmäßig befinden sich Image und Image-Schlüssel im Home-Verzeichnis des entsprechenden Benutzers. Der Schlüssel kann auch an einer anderen Stelle im Dateisystem abgelegt sein, beispielsweise auf einem entfernbaren Gerät, das manuell eingefügt werden kann.

Verwenden Sie das Modul zur Benutzerverwaltung von YaST oder das Werkzeug an der Kommandozeile `cryptconfig`, um die Verschlüsselung von Home-Verzeichnissen zu aktivieren. Sie können verschlüsselte Home-Verzeichnisse für neue oder vorhandene Benutzer erstellen. Um verschlüsselte Home-Verzeichnisse von bereits vorhandenen Benutzern zu verschlüsseln oder zu bearbeiten, geben Sie das aktuelle Anmeldepasswort des Benutzers ein. Informationen über die Benutzerverwaltung mit YaST finden Sie in Kapitel 5, *Verwalten von Benutzern mit YaST* (↑Start).

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 40.1.1, „Anlegen einer verschlüsselten Partition während der Installation“](#) (S. 729) und [Abschnitt 40.1.3, „Erstellen einer verschlüsselten Datei als Container“](#) (S. 731) beschrieben. Zusätzlich zu den Optionen von YaST können Sie für einige spezielle Aufgaben auch das Kommandozeilenwerkzeug `cryptconfig` verwenden.

Sie können damit zum Beispiel einen zusätzlichen Schlüssel für das Image erstellen.

1 Melden Sie sich als `root` an einer Shell an

2 Führen Sie

```
cryptconfig create-key admin.key
```

aus, um einen Schlüssel für Administratoren zu erstellen.

3 Um ein verschlüsseltes Home-Verzeichnis für den Benutzer `tux` zu erstellen und ihm den Administrationsschlüssel hinzuzufügen, geben Sie Folgendes ein

```
cryptconfig make-ehd --extra-key-file=admin.key tux 200
```

Es wird ein Home-Verzeichnis mit einer Ausgangsgröße von 200 MB erstellt.

4 Um die Größe des Home-Verzeichnisses jederzeit zu ändern, verwenden Sie

```
cryptconfig enlarge-size image  
size_to_add_in_MB
```

Weitere Informationen zum Kommandozeilenwerkzeug rufen Sie mit dem Kommando `cryptconfig --help` ab.

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 vermutlich der jeweiligen Konfigurationsdatei in `/etc/pam.d/` hinzufügen. Weitere Informationen finden Sie in [Kapitel 18, Authentifizierung mit PAM](#) (S. 299) sowie auf der man-Seite von `pam_mount`.

40.3 Verschlüsselung einzelner Dateien 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

41

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 Sicherheitsprofil 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*.

41.1 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-parser`
- `libapparmor`
- `apparmor-docs`
- `yast2-apparmor`
- `apparmor-profiles`
- `apparmor-utils`
- `audit`

41.2 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 Melden Sie sich als "`root`" an und 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 Melden Sie sich als "root" an und starten Sie YaST.
- 2 Wählen Sie *Novell AppArmor > AppArmor-Kontrollleiste*.
- 3 Wählen Sie *&aa aktivieren* aus. Um AppArmor zu deaktivieren, heben Sie die Auswahl dieser Option auf.
- 4 Beenden Sie die AppArmor-Kontrollleiste mit *Fertig*.

41.3 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 41.3.1, „Wählen der Anwendungen, die ein Profil erhalten sollen“** (S. 739).
- 2 Erstellen Sie die erforderlichen Profile wie in **Abschnitt 41.3.2, „Erstellen und Ändern von Profilen“** (S. 740) 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 41.3.3, „Konfigurieren von Novell AppArmor-Ereignisbenachrichtigung und -Berichten“** (S. 743).
- 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 41.3.4, „Aktualisieren Ihrer Profile“** (S. 745).

41.3.1 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 41.1 *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).

41.3.2 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 41.3.1, „Wählen der Anwendungen, die ein Profil erhalten sollen“](#) (S. 739) 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. 740) generiert wurden, indem Sie `S` in `aa-genprof` eingeben.

oder

Analysieren Sie die Protokolle, indem Sie im *Assistenten zum Hinzufügen von Profilen* auf *Systemprotokoll nach AppArmor-Ereignissen absuchen* 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. 740) und **Schritt 3** (S. 741) 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 msg=audit(1140325305.502:1407): REJECTING w access to
/usr/lib/firefox/update.test (firefox-bin(9469) profile
/usr/lib/firefox/firefox-bin active /usr/lib/firefox/firefox-bin)
```

```
/var/log/messages
```

Wird `auditd` nicht verwendet, werden die AppArmor-Ereignisse im Standardsystemprotokoll unter `/var/log/messages` protokolliert. Ein Beispieleintrag würde wie folgt aussehen:

```
Feb 22 18:29:14 dhcp-81 klogd: audit(1140661749.146:3): REJECTING w access
to /dev/console (mdnsd(3239) profile /usr/sbin/mdnsd active
/usr/sbin/mdnsd)
```

```
dmesg
```

Wird `auditd` nicht ausgeführt, können AppArmor-Ereignisse auch mit dem Befehl `dmesg` überprüft werden:

```
audit(1140661749.146:3): REJECTING w access to /dev/console (mdnsd(3239)
profile /usr/sbin/mdnsd active /usr/sbin/mdnsd)
```

Analysieren Sie die Protokollmeldungen für diese Anwendung erneut, wie in **Schritt 3** (S. 741) 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).

41.3.3 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 Melden Sie sich als `root` an und starten Sie YaST. Wählen Sie dann *Novell AppArmor > AppArmor-Kontrollleiste*.
- 3 Wählen Sie unter *Sicherheitsereignisbenachrichtigung aktivieren* die Option *Konfigurieren*.
- 4 Stellen Sie für jeden Eintragsstyp (*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 unbekannten 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 Melden Sie sich als `root` an und 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).

41.3.4 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 Melden Sie sich als `root` an und 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

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.

42.1 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.

42.1.1 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.

42.1.2 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.

42.1.3 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 13, Der Bootloader** (S. 221)). 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.

42.1.4 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`).

42.1.5 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 42.1.4, „Dateiberechtigungen“](#) (S. 751)).

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 42.1.4, „Dateiberechtigungen“](#) (S. 751)).

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.

42.1.6 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.

42.1.7 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.

42.1.8 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 36, SSH – sichere Netzwerkkoperationen](#) (S. 667).

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.

42.1.9 Pufferüberläufe und Format-String-Programmfehler

Wie in [Abschnitt 42.1.5, „Pufferüberläufe und Format-String-Programmfehler“](#) (S. 752) 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.

42.1.10 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.

42.1.11 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.

42.1.12 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.

42.1.13 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.

42.2 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#Mailing_Lists 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`).
- Als zusätzlichen Schutz zu `tcpd` (`tcp_wrapper`) könnten Sie SuSEfirewall verwenden.
- Entwickeln Sie redundante Sicherheitsmaßnahmen: Eine doppelt angezeigte Meldung ist besser als keine Meldung.

42.3 Zentrale Adresse für die Meldung von neuen Sicherheitsproblemen

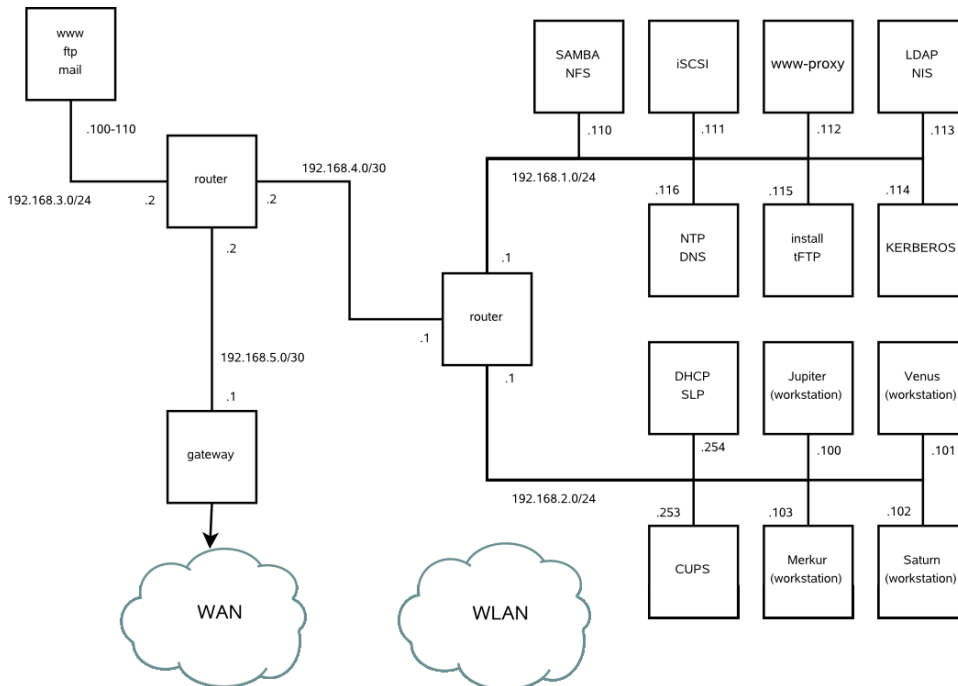
Wenn Sie ein Sicherheitsproblem finden (bitte überprüfen Sie zunächst die zur Verfügung stehenden Update-Pakete), schreiben Sie an die E-Mail-Adresse security@suse.de. Bitte fügen Sie eine genaue Beschreibung des Problems bei, zusammen mit den Versionsnummern der verwendeten Pakete. SUSE bemüht sich, 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 that 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 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. 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.

Index

Symbole

64-Bit-Linux, 199

Kernel-Spezifikationen, 202

Laufzeitunterstützung, 199

Software-Entwicklung, 200

A

ACLs, 285-298

Algorithmus prüfen, 297

Auswirkungen, 294

Berechtigungsbits, 290

Definitionen, 288

Masken, 293

Standard, 288, 294

Struktur, 288

Unterstützung, 298

Verarbeiten, 288

Zugriff, 288, 291

Add-On-Medium

Sprachunterstützung, 99

Aktualisieren, 89-93

Online

Kommandozeile, 80

Aktualisierung

Online, 77

passwd und group, 90

Probleme, 90

YaST , 91

Apache, 543-587

CGI-Skripten, 572

Fehlersuche, 584

installieren, 544

konfigurieren, 545

Dateien, 546

manuell, 545-553

virtueller Host, 549

YaST, 554-561

Module, 563-572

erstellen, 571

externe, 569

installieren, 564

Multiprocessing, 568

verfügbar, 565

Schnelleinführung, 543

Sicherheit, 582

SSL, 575-582

Apache mit SSL konfigurieren, 581

SSL-Zertifikat erstellen, 575

Starten, 561

Stoppen, 561

Arbeitsspeicher

RAM, 248

Authentifizierung

PAM, 299-307

B

Bash

.bashrc, 244

.profile, 244

Profil, 243

Befehle, 320-332

cat, 326

cd, 322

chgrp, 319, 322

chmod, 318, 322

chown, 319, 322

clear, 332

cp, 321

date, 329

df, 328

diff, 326

du, 328

find, 325

fonts-config, 145

free, 248, 329

- getfacl, 292
- grep, 326
- grub, 222
- gzip, 323
- halt, 331
- ifconfig, 389
- ip, 386
- kadmin, 710
- kill, 329
- killall, 330
- kinit, 718
- ktadd, 721
- ldapadd, 491
- ldapdelete, 494
- ldapmodify, 493
- ldapsearch, 494, 725
- less, 326
- ln, 322
- locate, 325
- lp, 123
- ls, 321
- man, 320
- mkdir, 322
- mount, 327
- mv, 321
- nslookup, 330
- passwd, 331
- ping, 330, 387
- ps, 329
- reboot, 331
- rm, 321
- rmdir, 322
- route, 390
- rpm, 101
- rpmbuild, 101
- scp, 669
- setfacl, 292
- sftp, 669
- slptool, 396
- ssh, 668

- ssh-agent, 672
- ssh-keygen, 671
- su, 331
- tar, 324
- telnet, 331
- top, 329
- umount, 327
- updatedb, 325

Benutzer

- /etc/passwd, 303

Berechtigungen, 316

- ACLs, 285-298
- Ändern, 318, 322
- Anzeigen, 318
- Dateiberechtigungen, 247
- Dateien, 316
- Dateisysteme, 316
- Verzeichnisse, 318

Bildschirm

- Auflösung, 141

BIND, 408-420

Bluetooth, 629

- hciconfig, 633
- hcidtool, 632
- pand, 634
- sdptool, 633

Booten, 203

- Bootsektoren, 221-222
- Grafisch, 239
- GRUB, 222
- initramfs, 205
- initrd, 205
- Konfigurieren
 - YaST, 232

Booting

- GRUB, 221

C

- cat, 326

- cd, 322
- chgrp, 319, 322
- chmod, 318, 322
- chown, 319, 322
- CJK, 252
- clear, 332
- commands
 - smbpasswd, 539
- Core-Dateien, 247
- cp, 321
- cpuspeed, 609
- cron, 244

D

- date, 329
- Datei, 325
 - Vergleichen, 326
- Dateien
 - anzeigen, 325
 - Archivieren, 324
 - Durchsuchen des Inhalts, 326
 - Komprimieren, 323
 - Kopieren, 321
 - Löschen, 321
 - Suchen, 247
 - suchen, 325
 - Suchen nach, 325
 - verschieben, 321
 - Verschlüsseln, 731
- Dateisysteme, 273-283
 - ACLs, 285-298
 - Ändern, 54
 - auswählen, 274
 - Begriffe, 273
 - Beschränkungen, 281
 - cryptofs, 727
 - Ext2, 275-276
 - Ext3, 276-278
 - LFS, 281

- ReiserFS, 274-275
 - unterstützt, 280-281
 - Verschlüsseln, 727
 - XFS, 278-279
- Datenträger
 - booten, 237
- Deinstallieren
 - GRUB, 237
 - Linux, 237
- deltarpm, 105
- df, 328
- DHCP, 425-442
 - dhcpcd, 438-440
 - Konfigurieren mit YaST, 426
 - Pakete, 437
 - Server, 438-440
 - Zuweisung statischer Adressen, 440
- diff, 326
- DNS, 355
 - BIND, 408-420
 - Domänen, 379
 - Fehlersuche, 409
 - Konfigurieren, 399
 - Mail Exchanger, 356
 - Namensserver, 379
 - NIC, 356
 - Optionen, 411
 - Protokollieren, 413
 - Reverse-Lookup, 419
 - Sicherheit und, 757
 - Starten, 409
 - Terminologie, 399
 - Top Level Domain, 356
 - Weiterleiten, 409
 - Zonen
 - Dateien, 415
- Domain Name System (Siehe DNS)
- DOS
 - Dateien freigeben, 529
- Drahtlose Verbindungen

- Bluetooth, 629
- Druck, 115
- Drucken
 - CUPS, 122
 - Fehlerbehebung
 - Netzwerk, 130
 - GDI-Drucker, 128
 - Kommandozeile, 123
 - kprinter, 122
 - Netzwerk, 130
 - Samba, 531
 - xpp, 122
- drucken
 - Irda, 638
- du, 328

E

- Editoren
 - Emacs, 249-250
 - vi, 332
- Emacs, 249-250
 - .emacs, 249
 - default.el, 250
- encoding
 - ISO-8859-1, 254
- Energieverwaltung, 597-615
 - ACPI, 597, 599-607
 - Akku-Überwachung, 598
 - cpufrequency, 609
 - cpuspeed, 609
 - Powersave, 609
 - Standby, 597
 - Stromsparmodus, 597
 - Tiefschlaf, 598

F

- Fehlermeldungen
 - Berechtigung verweigert, 57
 - Fehlerhafter Interpreter, 57

- find, 325
- Firefox
 - Befehl zum Öffnen von URLs, 96
- Firewalls, 653
 - Paketfilter, 653, 658
 - SuSEfirewall2, 653, 659
- free, 329
- FTP-Server
 - konfigurieren, 589

G

- GNOME
 - shell, 310
- Grafik
 - Karten
 - Treiber, 142
- grep, 326
- GRUB, 221
 - Befehle, 222
 - boot Passwort, 231
 - Booten, 222
 - Bootmenü, 224
 - Bootsektoren, 222
 - Deinstallieren, 237
 - device.map, 223, 229
 - Einschränkungen, 222
 - Fehlerbehebung, 240
 - Gerätenamen, 225
 - GRUB Geom Error, 240
 - grub.conf, 223, 230
 - Master Boot Record (MBR), 221
 - Menü-Editor, 228
 - menu.lst, 223-224
 - Partitionsnamen, 225
- gzip, 323

H

- halt, 331
- Hardware

- ISDN, 369
- hciconfig, 633
- hcitool, 632
- Hilfe
 - info-Seiten, 249
 - man-Seiten, 249, 320
 - Novell/SUSE-Handbücher, xiv
 - X, 143

I

- I18N, 252
- info-Seiten, 249
- init, 207-208
 - inittab, 207
 - Skripten, 211-215
 - Skripten hinzufügen, 213
- Installieren
 - GRUB, 222
 - Pakete, 102
- Internationalisierung, 252
- Internet
 - cinternet, 393
 - DSL, 373
 - Einwahl, 391-394
 - ISDN, 369
 - KInternet, 393
 - qinternet, 393
 - smpppd, 391-394
 - TDSL, 376
- IP-Adressen, 342
 - Dynamische Zuweisung, 425
- IPv6, 345
 - Konfigurieren, 354
- Klassen, 343
- Masquerading, 656
- privat, 345

IrDA, 637-639

- anhalten, 637
- konfigurieren, 637
- Problembehandlung, 639
- starten, 637

K

- Karten
 - Grafik, 142
 - Netzwerk, 357
- KDE
 - shell, 310
- Kerberos, 695-702
 - Administration, 703-726
 - Authentifikatoren, 696
 - Berechtigungen, 696
 - Bereiche, 705
 - Erstellen, 710
 - Clients
 - Konfigurieren, 714-717
 - Installieren, 703-726
- KDC, 706-711
 - nsswitch.conf, 707
 - Starten, 711
 - Verwalten, 717
- keytab, 720
- Konfiguring
 - Clients, 714-717
- LDAP und, 723-726
- Master-Schlüssel, 709
- PAM-Unterstützung, 721
- Prinzipale, 696
 - Dienst, 719
 - Erstellen, 710
 - Host, 719
- Sitzungsschlüssel, 697
- SSH-Konfiguration, 722
- Stapeldatei, 709
- Ticket ausstellen, 699
- Tickets, 696, 699
- Uhrensynchronisation, 707
- Zeitdifferenz, 717

- Kernel
 - Caches, 248
 - Einschränkungen, 282
 - Standard-Kernel, 99
- kill, 329
- killall, 330
- Konfigurationsdatei
 - Dienste, 533
- Konfigurationsdateien, 378
 - .bashrc, 244, 248
 - .emacs, 249
 - .profile, 244
 - .xsession, 672
 - acpi, 600
 - Berechtigungen, 758
 - crontab, 244
 - cs.cshrc, 254
 - dhclient.conf, 437
 - dhcp, 378
 - dhcpd.conf, 438
 - fstab, 57, 327
 - group , 90
 - grub.conf, 230
 - host.conf, 381
 - HOSTNAME, 385
 - Hosts, 356, 381
 - ifcfg-*, 378
 - inittab, 207-208, 210, 251
 - inputrc, 251
 - irda, 638
 - Kernel, 205
 - krb5.conf, 714-715, 717, 721
 - krb5.keytab, 720
 - language, 252, 254
 - logrotate.conf, 246
 - menu.lst, 224
 - named.conf, 409-420
 - Netzwerk, 378
 - Netzwerke, 381
 - nscd.conf, 385
 - nsswitch.conf, 383
 - openldap, 724
 - passwd, 90
 - Powersave, 599
 - Profil , 243
 - Profile, 247
 - profile, 254
 - resolv.conf, 249, 379, 409
 - Routen, 378
 - Samba, 533
 - slapd.conf, 483, 725-726
 - smb.conf, 534, 540
 - smppd.conf, 392
 - smpppd-c.conf, 393
 - sshd_config, 673, 722
 - ssh_config, 722
 - suseconfig, 220
 - sysconfig, 217-220
 - termcap, 251
 - wireless, 378
 - xorg.conf, 137
 - Device, 142
 - Monitor, 143
 - Screen, 140
- Konfigurieren, 217
 - DNS, 399
 - DSL, 373
 - GRUB, 222, 230
 - IPv6, 354
 - ISDN, 369
 - Kabelmodem, 373
 - Modems, 366
 - Netzwerke, 357
 - manuell, 376-391
 - Routing, 378
 - Samba, 531-538
 - SSH, 667
 - T-DSL, 376
- konfigurieren
 - FTP-Server, 589

- IrDA, 637
- Konfigurieren
 - Samba
 - Clients, 538
- Konsolen
 - Grafische , 239
 - Umschalten, 250
 - Zuweisen, 251

L

- L10N, 252
- Laptops
 - Energieverwaltung, 597-608
 - IrDA, 637-639
- Laufwerke
 - Aushängen, 327
 - Einhängen, 327
- LDAP, 461-495
 - ACLs, 485
 - Ändern von Daten, 492
 - Benutzer verwalten, 480
 - Gruppen verwalten, 480
 - Hinzufügen von Daten, 490
 - Kerberos und, 723-726
 - Konfigurieren
 - YaST, 467
 - ldapadd, 490
 - ldapdelete, 494
 - ldapmodify, 492
 - ldapsearch, 493
 - Löschen von Daten, 494
 - Serverkonfiguration
 - manuell, 483
 - YaST, 467
 - Suchen von Daten, 493
 - Verzeichnisbaum, 463
 - YaST
 - Client, 473
 - Module, 473

- Vorlagen, 473
- Zugriffskontrolle, 487
- less, 326
- LFS, 281
- Lightweight Directory Access Protocol (Siehe LDAP)
- Linux
 - Dateien mit anderen Betriebssystemen gemeinsam nutzen, 529
 - Deinstallieren, 237
 - Netzwerke und, 339
- ln, 322
- locate, 247, 325
- Logical Volume Manager (Siehe LVM)
- logrotate, 245
- Lokalisierung, 252
- ls, 321
- LSB
 - Installieren von Paketen, 101
- LVM
 - YaST, 60

M

- man-Seiten, 249, 320
- Masquerading, 656
 - Konfigurieren mit SuSEfirewall2, 659
- Master Boot Record (Siehe MBR)
- MBR, 221-222
- mkdir, 322
- Modems
 - Kabel, 373
 - YaST, 366
- mount, 327
- mv, 321

N

- Namensserver (Siehe DNS)
- NAT (Siehe Masquerading)
- NetBIOS, 530

Network Information Service (Siehe NIS)

Netzwerk

- Konfigurieren, 376-391

Netzwerkdateisystem (Siehe NFS)

Netzwerke, 339

- Authentifizierung

 - Kerberos, 695-702

- Basisnetzwerkadresse, 344

- Broadcast-Adresse, 345

- DHCP, 425

- DNS, 355

- Konfigurationsdateien, 378-385

- Konfigurieren, 357-376

 - IPv6, 354

- localhost, 345

- Netzmasken, 343

- Routing, 342-343

- SLP, 395

- TCP/IP, 339

- YaST, 357

 - Alias, 361

 - Gateway, 362

 - Hostname, 361

 - IP-Adresse, 360

 - Starten, 364

NFS, 513

- Clients, 514

- Einhängen, 515

- exportieren, 523

- Importieren, 515

- Server, 518

NIS, 451-459

- Clients, 458

- Masters, 451-458

- Slaves, 451-458

Novell/SUSE-Handbücher, xiv

nslookup, 330

NSS, 383

- Datenbanken, 383

O

OpenLDAP (Siehe LDAP)

OpenSSH (Siehe SSH)

OS/2

- Dateien freigeben, 529

P

Pakete

- Deinstallieren, 102

- Installieren, 102

- Kompilieren, 109

- Kompilieren mit build, 112

- LSB, 101

- Paketmanager, 101

- Prüfen, 102

- RPMs, 101

Paketfilter (Siehe Firewalls)

PAM, 299-307

pand, 634

Partitionen

- Erstellen, 51, 53

- fstab, 57

- LVM, 54

- Neuformatieren, 54

- Parameter, 54

- Partitionstabelle, 221

- RAID, 54

- Swap, 54

- Typen, 53

- Verschlüsseln, 729

passwd, 331

Passwörter

- Ändern, 331

PCMCIA

- IrDA, 637-639

ping, 330, 387

Platzhalter, 325

Pluggable Authentication Modules (Siehe PAM)

- Ports
 - 53, 411
- PostgreSQL
 - aktualisieren, 90
- Powersave, 609
 - Konfigurieren, 609
- protocols
 - SMB, 529
- Protokolldateien, 245
 - boot.msg, 599
 - Meldungen, 409, 664
- Protokolle
 - CIFS, 529
 - IPv6, 345
 - LDAP, 461
 - SLP, 395
- Prozesse, 329
 - Terminieren, 329
 - Überblick, 329
- ps, 329

Q

- Quelle
 - Kompilieren, 109

R

- RAID
 - YaST, 68
- reboot, 331
- RFCs, 339
- rm, 321
- rmdir, 322
- Routing, 342, 378-379
 - Masquerading, 656
 - Netzmasken, 343
 - Routen, 378
 - statisch, 378
- RPM, 101-113
 - Abfragen, 106

- Abhängigkeiten, 102
- Aktualisieren, 103
- database
 - Neu aufbauen, 104
- Datenbank
 - Neu erstellen, 109
- Deinstallieren, 104
- deltarpm, 105
- Patches, 104
- Prüfen, 102
- rpmnew, 102
- rpmorig, 102
- rpmsave, 102
- Sicherheit, 759
- SRPMS, 110
- überprüfen, 108
- Werkzeuge, 112
- rpmbuild, 101
- Runlevel
 - ändern, 210
 - in YaST bearbeiten, 215
- Runlevels, 208-210

S

- Samba, 529-541
 - Anmelden, 539
 - Berechtigungen, 537
 - CIFS, 529
 - Clients, 530-531, 538-539
 - Drucken, 539
 - Drucker, 531
 - Freigaben, 530, 535
 - Installieren, 531
 - Konfigurieren, 531-538
 - Namen, 530
 - Server, 530-538
 - Sicherheit, 537-538
 - SMB, 529
 - Starten, 531

- Stoppen, 531
- swat, 533
- TCP/IP und, 529
- Schriften, 145
 - TrueType, 144
 - X11-Core, 145
 - Xft, 146
- scripts
 - init.d
 - network, 391
- sdptool, 633
- Service Location Protocol (Siehe SLP)
- Shells, 309-336
 - Bash, 309
 - Befehle, 320-332
- Sicherheit, 747-760
 - Angriffe, 755-757
 - Berechtigungen, 751-752
 - Berichterstellungsprobleme, 760
 - Booten, 748-751
 - DNS, 757
 - Engineering, 748
 - Firewalls, 653
 - lokal, 749-753
 - Netzwerk, 753-757
 - Passwörter, 749-750
 - Programmfehler und, 752, 755
 - RPM-Signaturen, 759
 - Samba, 537
 - Serielle Terminals, 748-749
 - SSH, 667-675
 - tcpd, 760
 - telnet, 667
 - Tipps und Tricks, 757
 - Viren, 753
 - Würmer, 757
 - X und, 754
- Skripten
 - init.d, 207, 211-215, 390
 - boot, 212
 - boot.local, 213
 - boot.setup, 213
 - halt, 213
 - nfsserver, 391
 - portmap, 391
 - postfix, 391
 - rc, 211, 213
 - ypbind, 391
 - ypserv, 391
 - mkinitrd, 205
 - modify_resolvconf, 249, 380
 - SuSEconfig, 217-220
 - Deaktivieren, 220
- Skripts
 - init.d
 - rc, 210
 - xinetd, 391
 - irda, 638
- SLP, 395
 - Bereitstellen von Diensten, 397
 - Konqueror, 396
 - Registrieren von Diensten, 397
 - slptool, 396
- SMB (Siehe Samba)
- smbd, 529
- Soft-RAID (Siehe RAID)
- Software
 - Kompilieren, 109
- spm, 109
- SSH, 667-675
 - Authentifizierungsmechanismen, 671
 - Daemon, 670
 - Schlüsselpaare, 670-671
 - scp, 669
 - sftp, 669
 - ssh, 668
 - ssh-agent, 672-673
 - ssh-keygen, 671
 - sshd, 670
 - X und, 672

su, 331

System

Aktualisieren, 89-93

Beschränken der Ressourcenauslastung, 247

Herunterfahren, 331

Lokalisierung, 252

Neubooten, 331

T

Tablet PCs, 641-650

Dasher, 647

installieren, 642

Jamal, 646

konfigurieren, 643

KRandRTray, 644

Xournal, 646

xstroke, 645

xvkbd, 644

tar, 324

Tastatur

Asiatische Zeichen, 252

Belegung, 251

Multi-Key, 251

X-Tastaturerweiterung, 251

XKB, 251

Zuordnung, 251

Compose, 251

TCP/IP, 339

ICMP, 340

IGMP, 340

Pakete, 341-342

Schichtmodell, 340

TCP, 340

UDP, 340

TEI-XSL-Stylesheets

neuer Speicherort, 95

Telefonanlage, 371

telnet, 331

top, 329

U

ulimit, 247

Optionen, 247

umount, 327

updatedb, 325

V

Variablen

Umgebung, 252

Verschlüsseln, 727-731

Dateien, 731-734

Dateien mit vi, 733

Entfernbare Medien, 731

Erstellen von Partitionen, 729

Partitionen, 728-730

YaST, mit, 728

Verzeichnisse

/, 311

/bin, 311, 313

/boot, 311, 313

/dev, 311, 313

/etc, 311, 313

/home, 312-313

/lib, 312-313

/media, 312, 314

/mnt, 312, 314

/opt, 312, 314

/root, 312, 314

/sbin, 312, 314

/srv, 312, 314

/tmp, 312, 314

/usr, 312, 314

/var, 312, 315

/windows, 312, 315

Ändern, 322

Erstellen, 322

Löschen, 322

Verzeichnisstruktur
 , 311
Virtueller Arbeitsspeicher, 54

W

whois, 356
Windows
 Dateien freigeben, 529

X

X
 Hilfe, 143
 Konfigurieren, 137-143
 SaX2, 138
 Schriften, 144
 Schriftsysteme, 145
 Sicherheit, 754
 SSH und, 672
 Treiber, 142
 TrueType-Schriften, 144
 Virtueller Bildschirm, 141
 X11-Core-Schriften, 145
 xft, 144
 Xft, 146
 xorg.config, 138
 Zeichensätze, 144
X Window System (Siehe X)
X-Tastaturerweiterung (Siehe Tastatur,
XKB)
X.509-Zertifizierung
 Prinzipien, 677
 Repository, 681-682
 Widerrufsliste, 680
 YaST, 677
 Zertifikate, 679
X.Org, 137
Xft, 146
XKB (Siehe Tastatur, XKB)
xorg.conf

Dateien, 138
Depth, 141
Device, 141
Display, 141
Farbtiefe, 141
InputDevice, 138
Modeline, 141
Modelines, 139
Modes, 139, 141
Module, 138
Monitor, 139-140
ServerFlags, 138

Y

YaST
 Aktualisierung, 91
 Bootkonfiguration, 232
 Sicherheit, 236
 Standardsystem, 236
 Timeout, 236
 Bootlader
 Typ, 234
 Bootloader
 Passwort, 236
 Speicherort, 235
 CA-Management, 682
 DHCP, 426
 DSL, 373
 GRUB, 234
 ISDN, 369
 Kabelmodem, 373
 Kommandozeile, 87
 LDAP
 Clients, 473
 Server, 467
 LILO, 234
 LVM, 60
 Modems, 366
 ncurses, 83

- Netzwerkkarte, 357
- NIS-Clients, 458
- Online-Update, 77-79
- Partitionierung, 51
- RAID, 68
- Runlevel, 215
- Samba
 - Clients, 538
- sysconfig editor, 217
- T-DSL, 376
- Textmodus, 83-88
 - Module, 87
- X.509-Zertifizierung
 - Ändern von Standardwerten, 689
 - CRLs erstellen, 690
- X.509-Zertifizierung, 677
 - Exportieren von Zertifizierungsstellenobjekten als Datei, 692
 - Exportieren von Zertifizierungsstellenobjekten in LDAP, 691
 - Importieren von allgemeinen Server-Zertifikaten, 693
 - root CA, 682
 - sub-CA, 685
 - Zertifikate, 686
- YP (Siehe NIS)

Z

- Zugriffsberechtigungen (Siehe Berechtigungen)
- zypper, 80-82

