

SUSE Linux Enterprise Server

10

www.novell.com

02. Juni 2006



Installation und Administration

Autorenliste: Jörg Arndt, Steve Bearnson, Stefan Behlert, Frank Bodammer, James Branam, Volker Buzek, Klara Cihlarova, Catherine Craft, Olaf Dabrunz, Stefan Dirsch, Olaf Donjak, Roman Drahtmüller, Thorsten Dubiel, Torsten Duwe, Thomas Fehr, Stefan Fent, Werner Fink, Jakub Friedl, Kurt Garloff, Joachim Gleißner, Todd Grant, Carsten Groß, Andreas Grünbacher, Berthold Gunreben, Franz Hassels, Andreas Jaeger, Jana Jaeger, Denise Jewkes, Klaus Kämpf, Andi Kleen, Hubert Mantel, Lars Marowsky-Bree, Chris Mason, Johannes Meixner, Lars Müller, Matthias Nagorni, Anas Nashif, Siegfried Olschner, Edith Parzefall, Peter Pöml, Thomas Renninger, Hannes Reinecke, Scott Rhoades, Thomas Rölz, Heiko Rommel, Tanja Roth, Marcus Schäfer, Thomas Schraitle, Kay Sievers, Klaus Singvogel, Frank Sundermeyer, Elisabeth Tobiasson, Hendrik Vogelsang, Klaus G. Wagner, Rebecca Walter, Christian Zoz

Diese Veröffentlichung ist das geistige Eigentum von Novell, Inc.

Ihr Inhalt darf ganz oder teilweise dupliziert werden, sofern jede Kopie einen sichtbaren Copyright-Hinweis trägt.

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

Novell, das Novell-Logo, das N-Logo und SUSE sind eingetragene Marken von Novell, Inc., in den Vereinigten Staaten und anderen Ländern. * Linux ist eine eingetragene Marke von Linus Torvalds. Alle anderen Drittanbieter-Marken sind das Eigentum der jeweiligen Inhaber.

Inhaltsverzeichnis

Über dieses Handbuch	xv
Teil 1 Bereitstellung	19
1 Planen der Implementierung von SUSE Linux Enterprise	21
1.1 Überlegungen vor der Implementierung von SUSE Linux Enterprise Server	23
1.2 Bereitstellung von SUSE Linux Enterprise Server	23
1.3 Ausführen von SUSE Linux Enterprise Server	24
2 Installationsstrategien	25
2.1 Einsatz von bis zu 10 Arbeitsstationen	25
2.2 Einsatz von bis zu 100 Arbeitsstationen	27
2.3 Installation auf mehr als 100 Arbeitsstationen	35
3 Installation mit YaST	37
3.1 IBM-System z: Systemstart für die Installation	37
3.2 Systemstart für die Installation	38
3.3 Der Boot-Bildschirm	41
3.4 Sprachauswahl	42
3.5 IBM-System z: Konfiguration der Festplatte	43
3.6 Lizenzvereinbarung	45
3.7 Systemanalyse	45
3.8 Zeitzone	46
3.9 Installationsüberblick	46
3.10 Konfiguration	62
3.11 Grafische Anmeldung	74

4	Installation mit entferntem Zugriff	75
4.1	Installationsszenarien für die Installation auf entfernten Systemen	76
4.2	Einrichten des Servers, auf dem sich die Installationsquellen befinden	85
4.3	Vorbereitung des Bootvorgangs für das Zielsystem	95
4.4	Booten des Zielsystems für die Installation	106
4.5	Überwachen des Installationsvorgangs	111
5	Automatisierte Installation	115
5.1	Einfache Masseninstallation	115
5.2	Regelbasierte automatische Installation	127
5.3	Weitere Informationen	132
6	Fortgeschrittene Festplattenkonfiguration	133
6.1	LVM-Konfiguration	133
6.2	Soft-RAID-Konfiguration	142
7	Systemkonfiguration mit YaST	149
7.1	YaST-Sprache	150
7.2	Das YaST-Kontrollzentrum	151
7.3	Software	152
7.4	Hardware	167
7.5	System	173
7.6	Netzwerkgeräte	185
7.7	Netzwerkdienste	186
7.8	AppArmor	194
7.9	Sicherheit und Benutzer	194
7.10	Andere	199
7.11	YaST im Textmodus	202
7.12	Aktualisierung über die Kommandozeile	206
7.13	SaX2	209
7.14	Fehlerbehebung	217
7.15	Weitere Informationen	217
8	Aktualisieren von SUSE Linux Enterprise	219
8.1	Aktualisieren von SUSE Linux Enterprise	219
8.2	Installieren von Service Packs	222
8.3	Software-Änderungen von Version 9 zu Version 10	229

Teil 2 Administration	245
9 OpenWBEM	247
9.1 Einrichten von OpenWBEM	249
9.2 Ändern der OpenWBEM CIMOM-Konfiguration	254
9.3 Weitere Informationen	275
10 Multipath-E/A	277
10.1 Unterstützte Hardware	278
10.2 Systemkonfiguration	279
10.3 Software-Konfiguration	279
10.4 Verwenden der Geräte	283
11 Massenspeicher über IP-Netzwerke – iSCSI	285
11.1 Einrichten eines iSCSI-Ziels	285
11.2 Konfigurieren eines iSCSI-Initiators	291
12 Hohe Verfügbarkeit (High Availability) unter Linux	295
12.1 Wichtige Begriffe	295
12.2 Ein Mindestszenario als Beispiel	297
12.3 Komponenten einer Lösung mit hoher Verfügbarkeit	298
12.4 Software-Anforderungen bei hoher Verfügbarkeit	299
12.5 Clustering	301
12.6 Weitere Informationen	302
13 Installieren eines Heartbeat 2-Clusters mithilfe von YaST	305
13.1 Hardware-Anforderungen	305
13.2 Software-Anforderungen	306
13.3 Voraussetzungen für ein freigegebenes Festplattensystem	306
13.4 Installieren von Heartbeat 2	307
13.5 Zusätzliche Informationen	309
14 Oracle Cluster File System 2	311
14.1 Überblick über OCFS2	311
14.2 Erstellen eines OCFS2-Volumes	318
14.3 Einhängen eines OCFS2-Volumes	324
14.4 Zusätzliche Informationen	325

15	Zugriffssteuerungslisten unter Linux	327
15.1	Traditionelle Dateiberechtigungen	327
15.2	Vorteile von ACLs	329
15.3	Definitionen	330
15.4	Arbeiten mit ACLs	330
15.5	ACL-Unterstützung in Anwendungen	339
15.6	Weitere Informationen	340
16	RPM - der Paket-Manager	341
16.1	Prüfen der Authentizität eines Pakets	342
16.2	Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren	342
16.3	RPM und Patches	344
16.4	Delta-RPM-Pakete	345
16.5	RPM-Abfragen	346
16.6	Installieren und Kompilieren von Quellpaketen	349
16.7	Kompilieren von RPM-Paketen mit "build"	351
16.8	Werkzeuge für RPM-Archive und die RPM-Datenbank	352
17	Dienstprogramme zur Systemüberwachung	353
17.1	Fehlersuche	354
17.2	Dateien und Dateisysteme	356
17.3	Hardware-Informationen	358
17.4	Netzwerke	361
17.5	Das Dateisystem <code>/proc</code>	362
17.6	Prozesse	365
17.7	Systeminformationen	369
17.8	Benutzerinformationen	374
17.9	Zeit und Datum	374
18	Arbeiten mit der Shell	375
18.1	Einführung in die Bash-Shell	376
18.2	Benutzer und Zugriffsberechtigungen	389
18.3	Wichtige Linux-Befehle	393
18.4	Der vi-Editor	405
Teil 3	System	411
19	32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung	413
19.1	Laufzeitunterstützung	414

19.2	Software-Entwicklung	415
19.3	Software-Kompilierung auf Doppelarchitektur-Plattformen	415
19.4	Kernel-Spezifikationen	417
20	Booten und Konfigurieren eines Linux-Systems	419
20.1	Der Linux-Bootvorgang	419
20.2	Der init-Vorgang	424
20.3	Systemkonfiguration über /etc/sysconfig	433
21	Der Bootloader	437
21.1	Auswählen eines Bootloaders	438
21.2	Booten mit GRUB	438
21.3	Konfigurieren des Bootloaders mit YaST	448
21.4	Deinstallieren des Linux-Bootloaders	454
21.5	Erstellen von Boot-CDs	454
21.6	Der grafische SUSE-Bildschirm	455
21.7	Fehlerbehebung	456
21.8	Weitere Informationen	458
22	Sonderfunktionen in SUSE Linux Enterprise	459
22.1	Informationen zu speziellen Softwarepaketen	459
22.2	Virtuelle Konsolen	466
22.3	Tastaturzuordnung	467
22.4	Sprach- und länderspezifische Einstellungen	468
23	Virtual Machine Server	473
23.1	Systemvoraussetzungen	474
23.2	Vorteile von virtuellen Computern	476
23.3	Terminologie	476
23.4	Virtual Machine Modi	477
23.5	Virtual Machine Server	478
23.6	Einrichten des Virtual Machine Servers	481
23.7	Erstellen virtueller Computer	484
23.8	Verwalten virtueller Computer	485
24	Druckerbetrieb	489
24.1	Workflow des Drucksystems	491
24.2	Methoden und Protokolle zum Anschließen von Druckern	491
24.3	Installieren der Software	492
24.4	Konfigurieren des Druckers	493

24.5	Konfiguration für Anwendungen	500
24.6	Spezielle Funktionen in SUSE Linux Enterprise	501
24.7	Fehlerbehebung	507
25	Gerätemanagement über dynamischen Kernel mithilfe von udev	515
25.1	Das <code>/dev</code> -Verzeichnis	515
25.2	Kernel-uevents und udev	516
25.3	Treiber, Kernel-Module und Geräte	516
25.4	Booten und erstes Einrichten des Geräts	517
25.5	Fehlersuche bei udev-Ereignissen	518
25.6	Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von udev-Regeln	519
25.7	Permanente Gerätebenennung	520
25.8	Das ersetzte <code>hotplug</code> -Paket	520
25.9	Weitere Informationen	521
26	Dateisysteme in Linux	523
26.1	Terminologie	523
26.2	Wichtige Dateisysteme in Linux	524
26.3	Weitere unterstützte Dateisysteme	530
26.4	Large File Support unter Linux	532
26.5	Weitere Informationen	533
27	Das X Window-System	535
27.1	X11-Konfiguration mit <code>SaX2</code>	535
27.2	Optimierung der X-Konfiguration	537
27.3	Installation und Konfiguration von Schriften	543
27.4	OpenGL – 3D-Konfiguration	550
28	Authentifizierung mit PAM	553
28.1	Struktur einer PAM-Konfigurationsdatei	554
28.2	PAM-Konfiguration von <code>sshd</code>	556
28.3	Konfiguration von PAM-Modulen	558
28.4	Weitere Informationen	561
29	Energieverwaltung	563
29.1	Energiesparfunktionen	564
29.2	APM	565
29.3	ACPI	567
29.4	Ruhezustand für Festplatte	575

29.5	Das powersave-Paket	577
29.6	Das YaST-Energieverwaltungsmodul	586
30	Drahtlose Kommunikation	591
30.1	Wireless LAN	591
Teil 4	Dienste	603
31	Grundlegendes zu Netzwerken	605
31.1	IP-Adressen und Routing	608
31.2	IPv6 – Das Internet der nächsten Generation	612
31.3	Namensauflösung	622
31.4	Konfigurieren von Netzwerkverbindungen mit YaST	623
31.5	Verwalten der Netzwerkverbindungen mit dem NetworkManager	644
31.6	Manuelle Netzwerkkonfiguration	647
31.7	smpppd als Einwahlhelfer	664
32	SLP-Dienste im Netzwerk	669
32.1	Installation über SLP	669
32.2	Registrieren eigener Dienste	670
32.3	SLP-Frontends in SUSE Linux Enterprise	671
32.4	SLP aktivieren	672
32.5	Weitere Informationen	672
33	Zeitsynchronisierung mit NTP	675
33.1	Konfigurieren eines NTP-Client mit YaST	675
33.2	Konfigurieren von xntp im Netzwerk	679
33.3	Einrichten einer lokalen Referenzuhr	680
34	Domain Name System (DNS)	681
34.1	DNS-Terminologie	681
34.2	Konfiguration mit YaST	682
34.3	Starten des Namenservers BIND	692
34.4	Die Konfigurationsdatei /etc/dhcpd.conf	694
34.5	Zonendateien	699
34.6	Dynamische Aktualisierung von Zonendaten	703
34.7	Sichere Transaktionen	704
34.8	DNS-Sicherheit	705
34.9	Weitere Informationen	706

35 DHCP	707
35.1 Konfigurieren eines DHCP-Servers mit YaST	708
35.2 DHCP-Softwarepakete	718
35.3 Der DHCP-Server dhcpd	719
35.4 Weitere Informationen	723
36 Arbeiten mit NIS	725
36.1 Konfigurieren von NIS-Servern	725
36.2 Konfigurieren von NIS-Clients	732
37 LDAP – Ein Verzeichnisdienst	735
37.1 LDAP und NIS	736
37.2 Struktur eines LDAP-Verzeichnisbaums	737
37.3 Serverkonfiguration mit slapd.conf	741
37.4 Datenbehandlung im LDAP-Verzeichnis	746
37.5 Konfigurieren eines LDAP-Servers mit YaST	750
37.6 Konfigurieren eines LDAP-Clients mit YaST	754
37.7 Konfigurieren von LDAP-Benutzern und -Gruppen in YaST	762
37.8 Weitere Informationen	764
38 Samba	767
38.1 Terminologie	767
38.2 Starten und Stoppen von Samba	769
38.3 Konfigurieren eines Samba-Servers	769
38.4 Konfigurieren der Clients	776
38.5 Samba als Anmeldeserver	777
38.6 Samba-Server im Netzwerk mit Active Directory	778
38.7 Migrieren eines Windows NT-Servers auf Samba	780
38.8 Weitere Informationen	782
39 Verteilte Nutzung von Dateisystemen mit NFS	785
39.1 Importieren von Dateisystemen mit YaST	785
39.2 Manuelles Importieren von Dateisystemen	786
39.3 Exportieren von Dateisystemen mit YaST	787
39.4 Weitere Informationen	788
40 Dateisynchronisierung	789
40.1 Verfügbare Software zur Datensynchronisierung	789
40.2 Kriterien für die Auswahl eines Programms	793

40.3	Einführung in Unison	797
40.4	Einführung in CVS	799
40.5	Einführung in Subversion	802
40.6	Einführung in rsync	805
40.7	Einführung in mailsync	807
41	Der HTTP-Server Apache	811
41.1	Schnellstart	811
41.2	Konfigurieren von Apache	813
41.3	Starten und Beenden von Apache	829
41.4	Installieren, Aktivieren und Konfigurieren von Modulen	831
41.5	Aktivieren von CGI-Skripts	839
41.6	Einrichten eines sicheren Webservers mit SSL	843
41.7	Vermeiden von Sicherheitsproblemen	850
41.8	Fehlerbehebung	852
41.9	Weitere Informationen	853
42	Der Proxyserver Squid	857
42.1	Einige Tatsachen zu Proxy-Caches	858
42.2	Systemvoraussetzungen	860
42.3	Starten von Squid	862
42.4	Die Konfigurationsdatei /etc/squid/squid.conf	864
42.5	Konfigurieren eines transparenten Proxy	870
42.6	cachemgr.cgi	873
42.7	squidGuard	875
42.8	Erstellung von Cache-Berichten mit Calamaris	877
42.9	Weitere Informationen	878
Teil 5	Sicherheit	879
43	Verwalten der X.509-Zertifizierung	881
43.1	Prinzipien der digitalen Zertifizierung	881
43.2	YaST-Module für die Verwaltung von Zertifizierungsstellen	886
44	Masquerading und Firewalls	899
44.1	Paketfilterung mit iptables	899
44.2	Grundlegendes zum Masquerading	902
44.3	Grundlegendes zu Firewalls	904
44.4	SuSEfirewall2	905
44.5	Weitere Informationen	910

45	SSH: Sicherer Netzwerkbetrieb	911
45.1	Das Paket OpenSSH	912
45.2	Das ssh-Programm	912
45.3	scp – sicheres Kopieren	912
45.4	sftp – sichere Dateiübertragung	913
45.5	Der SSH-Daemon (sshd) – Serverseite	913
45.6	SSH-Authentifizierungsmechanismen	915
45.7	X-, Authentifizierungs- und Weiterleitungsmechanismen	916
46	Netzwerkauthentifizierung – Kerberos	919
46.1	Kerberos-Terminologie	919
46.2	Funktionsweise von Kerberos	921
46.3	Benutzeransicht von Kerberos	925
46.4	Weitere Informationen	926
47	Installation und Administration von Kerberos	927
47.1	Auswählen der Kerberos-Bereiche	927
47.2	Einrichten der KDC-Hardware	928
47.3	Uhrensynchronisation	929
47.4	Konfigurieren des KDC	930
47.5	Manuelles Konfigurieren der Kerberos-Clients	933
47.6	Konfigurieren eines Kerberos-Clients mit YaST	936
47.7	Entfernte Kerberos-Administration	938
47.8	Erstellen der Kerberos-Host-Prinzipals	940
47.9	Aktivieren der PAM-Unterstützung für Kerberos	942
47.10	Konfigurieren von SSH für die Kerberos-Authentifizierung	943
47.11	Verwenden von LDAP und Kerberos	944
48	Verschlüsseln von Partitionen und Dateien	949
48.1	Einrichten eines verschlüsselten Dateisystems mit YaST	950
48.2	Verschlüsselung einzelner Dateien mit vi	953
49	Einschränken von Berechtigungen mit AppArmor	955
49.1	Installation von Novell AppArmor	956
49.2	Aktivieren und Deaktivieren von Novell AppArmor	957
49.3	Einführung in die Erstellung von Anwendungsprofilen	958
50	Sicherheit und Vertraulichkeit	967
50.1	Lokale Sicherheit und Netzwerksicherheit	968

50.2	Tipps und Tricks: Allgemeine Hinweise zur Sicherheit	978
50.3	Zentrale Adresse für die Meldung von neuen Sicherheitsproblemen	980
Teil 6 Fehlerbehebung		983
51 Hilfe und Dokumentation		985
51.1	Verwenden der SUSE-Hilfe	985
51.2	Manualpages	989
51.3	Infoseiten	990
51.4	Das Linux-Dokumentationsprojekt	990
51.5	Wikipedia: die kostenlose Online-Enzyklopädie	991
51.6	Handbücher und andere Literatur	991
51.7	Dokumentation zu den einzelnen Paketen	992
51.8	Usenet	993
51.9	Standards und Spezifikationen	994
52 Häufige Probleme und deren Lösung		997
52.1	Ausfindigmachen von Informationen	997
52.2	Probleme bei der Installation	999
52.3	Probleme beim Booten	1008
52.4	Probleme bei der Anmeldung	1011
52.5	Probleme mit dem Netzwerk	1018
52.6	Probleme mit Daten	1024
52.7	IBM-System z: initrd als Rettungssystem verwenden	1037
Index		1043

Über dieses Handbuch

Dieses Handbuch ist für professionelle Netzwerk- und Systemadministratoren zur Planung, Installation, Konfiguration und zum Betrieb von SUSE® Linux Enterprise konzipiert. Daher soll es nur sicherstellen, dass SUSE Linux Enterprise korrekt konfiguriert ist und die erforderlichen Dienste im Netzwerk verfügbar sind, um eine ordnungsgemäße Funktion gemäß der ursprünglichen Installation zu erlauben. Dieses Handbuch behandelt nicht, wie Sie dafür sorgen, dass SUSE Linux Enterprise die geeignete Kompatibilität mit der Anwendungssoftware Ihres Unternehmens bietet oder dass seine Kernfunktionalität diese Anforderungen erfüllt. Das Handbuch setzt voraus, dass eine vollständige Anforderungsüberprüfung durchgeführt und die Installation angefordert wurde bzw. dass eine Testinstallation zum Zwecke einer solchen Überprüfung angefordert wurde.

Dieses Handbuch enthält die folgenden Themen:

Bereitstellung

Wählen Sie vor der Installation von SUSE Linux Enterprise die Installationsstrategie und Festplattenkonfiguration, die sich am besten für Ihre Umgebung eignet. Lernen Sie, wie Sie Ihr System manuell installieren, Konfigurationen zur Netzwerkinstallation verwenden und eine automatische Installation ausführen können. Konfigurieren Sie das installierte System mit YaST, um es Ihren Anforderungen anzupassen.

Administration

SUSE Linux Enterprise bietet eine breite Palette an Werkzeugen, um verschiedene Aspekte des Systems anzupassen. In diesem Abschnitt werden einige dieser Aspekte erläutert. Mit einer Übersicht über die erhältlichen Gerätetechnologien, Konfigurationen für hohe Verfügbarkeit und fortgeschrittenen Administrationsmöglichkeiten wird dem Administrator das System vorgestellt.

System

Erfahren Sie mehr über das zugrunde liegende Betriebssystem, indem Sie diesen Abschnitt lesen. SUSE Linux Enterprise unterstützt eine Reihe von Hardware-Architekturen, damit Sie Ihre eigenen Anwendungen zur Ausführung unter SUSE Linux Enterprise anpassen können. Der Bootloader und die Informationen zum Bootvorgang unterstützen Sie dabei zu verstehen, wie Ihr Linux-System arbeitet und wie sich Ihre eigenen Skripts und Anwendungen integrieren lassen.

Dienste

SUSE Linux Enterprise ist als Netzwerkbetriebssystem konzipiert. Es bietet eine breite Palette an Netzwerkdiensten, z. B. DNS, DHCP, Web, Proxy und Authentifizierung, und fügt sich gut in heterogene Umgebungen mit MS Windows-Clients und -Servern ein.

Sicherheit

Diese Ausgabe von SUSE Linux Enterprise umfasst mehrere sicherheitsbezogene Funktionen. Im Lieferumfang ist Novell® AppArmor enthalten, mit dessen Hilfe Sie Ihre Anwendungen schützen können, indem Sie Privilegien einschränken. Sichere Anmeldung, Verwendung von Firewalls sowie Verschlüsselung des Dateisystems werden ebenfalls behandelt.

Fehlerbehebung

SUSE Linux Enterprise umfasst eine Vielzahl an Anwendungen, Tools und Dokumentation, die Ihnen bei der Lösung von Problemen helfen kann. Einige der häufigsten Probleme, die mit SUSE Linux Enterprise und dessen Lösungen auftreten können, werden ausführlich diskutiert.

1 Feedback

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

2 Updates zur Dokumentation

Informationen zur neuesten Version dieser Dokumentation erhalten Sie auf der Website von SUSE Linux Enterprise Desktop [<http://www.novell.com/documentation/sled10/index.html>].

3 Zusätzliche Dokumentation

Weitere Dokumentation zu diesem Produkt finden Sie unter <http://www.novell.com/documentation/sles10/index.html>:

Starthandbuch

Grundlegende Informationen zu Installationsarten und Arbeitsabläufen.

Architekturspezifische Informationen

Architekturspezifische Informationen zur Vorbereitung eines Installationsziels für SUSE Linux Enterprise Server.

Installation und Administration

Ausführliche Informationen zu Installation und Administration für SUSE Linux Enterprise Server.

Einen Überblick über das Produkt SUSE® Linux Enterprise Desktop erhalten Sie unter <http://www.novell.com/documentation/sled10/index.html>. Die folgenden Handbücher stehen exklusiv für SUSE Linux Enterprise Desktop zur Verfügung:

GNOME-Benutzerhandbuch

Ein umfassendes Handbuch zum GNOME-Desktop und seinen wichtigsten Anwendungen.

KDE-Benutzerhandbuch

Ein umfassendes Handbuch zum KDE-Desktop und seinen wichtigsten Anwendungen.

Handbuch zur Netzwerkkonnektivität

Eine detaillierte Einführung in die Netzwerkverwaltung mit dem NetworkManager.

Novell AppArmor 2.0 Administration Guide

Ein ausführliches Administrationshandbuch zu Novell AppArmor, das Sie in die Anwendungsbeschränkungen für höhere Sicherheit in Ihrer Umgebung einführt.

Viele Kapitel in diesem Handbuch enthalten Links zu zusätzlichen Dokumentationsressourcen. Dazu gehört auch weitere Dokumentation, die auf dem System bzw. im Internet verfügbar ist.

4 Konventionen in der Dokumentation

In diesem Handbuch werden folgende typografische Konventionen verwendet:

- `/etc/passwd`: Datei- und Verzeichnisnamen
- *Platzhalter*: Ersetzen Sie *Platzhalter* durch den tatsächlichen Wert.
- `PATH`: die Umgebungsvariable `PATH`
- `ls, --help`: Befehle, Optionen und Parameter
- `user`: Benutzer oder Gruppen
- `[Alt]`, `[Alt] + [F1]`: Eine Taste oder Tastenkombination; Tastennamen werden wie auf der Tastatur in Großbuchstaben dargestellt
- *Datei, Datei* → *Speichern unter*: Menüelemente, Schaltflächen
- ▶ **amd64 em64t ipf**: Dieser Absatz ist nur für die angegebenen Architekturen von Bedeutung. Die Pfeile kennzeichnen den Anfang und das Ende des Textblocks. ◀
 - ▶ **ipseries s390 zseries**: Dieser Absatz ist nur für die angegebenen Architekturen von Bedeutung. Die Pfeile kennzeichnen den Anfang und das Ende des Textblocks. ◀
- *Tanzende Pinguine* (Kapitel "Pinguine", ↑*Verweis*): Dies ist ein Verweis auf ein Kapitel in einem anderen Buch.

Teil 1. Bereitstellung

Planen der Implementierung von SUSE Linux Enterprise

1

Die Bereitstellung eines Betriebssystems muss sowohl in einer bestehenden IT-Umgebung als auch in einer völlig neuen Implementierung sorgfältig vorbereitet werden. Mit SUSE Linux Enterprise Server 10 erhalten Sie zahlreiche neue Funktionen, die wir an dieser Stelle unmöglich alle beschreiben können. Nachfolgend eine Aufstellung der wichtigsten Verbesserungen, die besonders von Interesse sind.

Xen 3.0-Virtualisierung

Führt mehrere virtuelle Computer auf einem einzigen Server aus, wobei jeder virtuelle Computer über sein eigenes Betriebssystem verfügt. Weitere Informationen finden Sie in [Kapitel 23, *Virtual Machine Server*](#) (S. 473).

YaST

Für YaST wurden zahlreiche neue Konfigurationsoptionen entwickelt. Diese werden meist in den entsprechenden Kapiteln beschrieben.

CIM-Verwaltung mit openWBEM

Der Common Information Model Object Manager (CIMON) ist ein Dienstprogramm für die webbasierte Unternehmensverwaltung. Der Manager bietet ein ausgereiftes Verwaltungsrahmenwerk. Weitere Informationen hierzu finden Sie in [Kapitel 9, *OpenWBEM*](#) (S. 247).

SPident

Dieses Verwaltungsprogramm gibt einen Überblick über die installierte Software und zeigt das aktuelle Service Pack-Level des Systems an.

Verzeichnisdienste

Mehrere LDAP-konforme Verzeichnisdienste stehen zur Verfügung:

- Microsoft Active Directory
- OpenLDAP

Novell AppArmor

Mit der Novell AppArmor-Technologie können Sie Ihr System härten. Dieser Dienst wird in *Novell AppArmor 2.0 Administration Guide* (↑Novell AppArmor 2.0 Administration Guide) ausführlich beschrieben.

iSCSI

iSCSI bietet eine einfache und günstige Lösung für die Verbindung von Linux-Computern mit zentralen Speichersystemen. Weitere Informationen zu iSCSI finden Sie in [Kapitel 11, *Massenspeicher über IP-Netzwerke – iSCSI*](#) (S. 285).

Network File System v4

Ab Version 10 unterstützt SUSE Linux Enterprise Server auch Version 4 von NFS. Zu den Vorteilen dieser Version zählen Leistungsverbesserungen, eine überragende Sicherheit und ein „statusbehaftetes“ Protokoll.

Oracle Cluster File System 2

OCFS2 ist ein allgemeines Journaling-Dateisystem, das vollständig in den Linux 2.6-Kernel und spätere Versionen integriert ist. Einen Überblick über OCFS2 finden Sie in [Kapitel 14, *Oracle Cluster File System 2*](#) (S. 311).

Heartbeat 2

Heartbeat 2 bietet eine Infrastruktur für die Cluster-Mitgliedschaft und die Übertragung von Meldungen in einem Cluster. Die Einrichtung eines Clusters wird in [Kapitel 13, *Installieren eines Heartbeat 2-Clusters mithilfe von YaST*](#) (S. 305) beschrieben.

MultiPath-E/A

Die Gerätezuordnung über MultiPath-E/A ermöglicht die automatische Konfiguration von Subsystemen in zahlreichen Implementierungen. Weitere Informationen hierzu finden Sie in [Kapitel 10, *Multipath-E/A*](#) (S. 277).

Absturzabbild des Linux-Kernel

Mit Kexec und Kdump ist das Debuggen von Kernel-Problemen nun wesentlich komfortabler. Diese Technologie steht auf x86-, AMD64-, Intel EM64T- und POWER-Plattformen zur Verfügung.

1.1 Überlegungen vor der Implementierung von SUSE Linux Enterprise Server

Zu Beginn Ihrer Planungen sollten Sie die Projektziele und die benötigten Funktionen festlegen. Diese Überlegungen werden bei jedem Projekt anders aussehen. Immer sollten Sie sich jedoch die folgenden Fragen stellen:

- Wie viele Installationen sind erforderlich? Von dieser Überlegung hängt die optimale Bereitstellungsmethode ab. Weitere Informationen hierzu finden Sie in [Kapitel 2, Installationsstrategien](#) (S. 25).
- Befindet sich das System in einer feindseligen Umgebung? In [Kapitel 50, Sicherheit und Vertraulichkeit](#) (S. 967) finden Sie einen Überblick über die daraus folgenden Konsequenzen.
- Wie erhalten Sie reguläre Updates? Alle Patches stehen registrierten Benutzern online zur Verfügung. Die Registrierungs- und Patch-Support-Datenbank finden Sie unter <http://www.novell.com/suselinuxportal>.
- Benötigen Sie für die lokale Installation Hilfe? Novell bietet Schulungen, Unterstützung und Beratung für alle Themen rund um SUSE Linux Enterprise Server an. Weitere Informationen hierzu finden Sie unter <http://www.novell.com/products/linuxenterpriseserver/>.
- Benötigen Sie Produkte von Drittanbietern? Vergewissern Sie sich, dass das benötigte Produkt von der gewünschten Plattform unterstützt wird. Bei Bedarf unterstützt Sie Novell auch bei der Portierung von Software auf andere Plattformen.

1.2 Bereitstellung von SUSE Linux Enterprise Server

Um sicherzustellen, dass Ihr System fehlerlos läuft, sollten Sie nur zertifizierte Hardware verwenden. Unsere Datenbank der zertifizierten Geräte wird regelmäßig aktualisiert.

Ein Suchformular für zertifizierte Hardware finden Sie unter <http://developer.novell.com/yesssearch/Search.jsp>.

Abhängig von der Anzahl der gewünschten Installationen empfehlen sich eventuell Installationsserver oder sogar völlig automatische Installationen. Informationen hierzu finden Sie in [Kapitel 2, Installationsstrategien](#) (S. 25). Wenn Sie die Xen-Virtualisierungstechnologien verwenden möchten, empfehlen sich eventuell Netzwerk-Root-Dateisysteme oder Netzwerkspeicherlösungen, wie iSCSI. Weitere Informationen hierzu finden Sie in [Kapitel 11, Massenspeicher über IP-Netzwerke – iSCSI](#) (S. 285).

SUSE Linux Enterprise Server bietet eine breite Palette an Diensten an. Einen Überblick über die Dokumentation zu diesen Diensten finden Sie in diesem Handbuch in [Über dieses Handbuch](#) (S. xv). Die meisten Konfigurationen lassen sich in YaST, dem Konfigurationsprogramm von SUSE, vornehmen. Darüber hinaus sind aber auch zahlreiche manuelle Konfigurationen möglich, die in den betreffenden Kapiteln beschrieben werden.

Über die Installation der Software hinaus sollten Sie in der Planung auch die Schulung der System-Endbenutzer sowie die Schulung Ihres HelpDesks berücksichtigen.

1.3 Ausführen von SUSE Linux Enterprise Server

SUSE Linux Enterprise Server ist ein sorgfältig getestetes und stabiles Betriebssystem. Dennoch lassen sich Hardware-Ausfälle oder andere Ursachen für Ausfallzeiten und Datenverluste nicht gänzlich vermeiden. Sie sollten daher für jede wichtige Arbeit, bei der es zu einem Datenverlust kommen kann, regelmäßig Sicherungskopien anfertigen.

Zur optimalen Absicherung Ihrer Arbeit sollten Sie alle verwendeten Systeme regelmäßig aktualisieren. Für einen missions-kritischen Server sollten Sie eventuell einen zweiten, identischen Server einrichten, an dem Sie alle Änderungen testen können, bevor Sie sie am echten System anwenden. Bei Hardware-Ausfällen steht Ihnen so auch immer ein redundantes System zur Verfügung, zu dem Sie jederzeit wechseln können.

Installationsstrategien

Es gibt verschiedene Installationsmöglichkeiten für SUSE® Linux Enterprise. Wählen Sie aus verschiedenen Ansätzen. Von der lokalen Installation mit physischen Medien über einen Netzwerkinstallationsserver bis zu einer Masseninstallation über eine entfernt gesteuerte, hochgradig angepasste und automatisierte Installationsmethode ist alles möglich. Wählen Sie die Methode, die Ihren Anforderungen am besten entspricht.

2.1 Einsatz von bis zu 10 Arbeitsstationen

Wenn Ihre Installation von SUSE Linux Enterprise nur 1 bis 10 Arbeitsstationen umfasst, ist es am einfachsten, wenn Sie SUSE Linux Enterprise manuell installieren. Weitere Einzelheiten erhalten Sie unter [Kapitel 3, *Installation mit YaST*](#) (S. 37). Die manuelle Installation kann auf verschiedene Arten erfolgen, je nach Ihren Anforderungen.

[Installation von den SUSE Linux Enterprise-Medien](#) (S. 26)

Dieser Ansatz kommt für Sie in Frage, wenn Sie eine einzelne, nicht verbundene Arbeitsstation installieren möchten.

[Installation von einem Netzwerkservers mit SLP](#) (S. 26)

Dieser Ansatz kommt für Sie in Frage, wenn Sie über eine einzelne Arbeitsstation oder über eine geringe Anzahl von Arbeitsstationen verfügen und wenn ein Netzwerkinstallationsserver über SLP verfügbar ist.

[Installation von einem Netzwerksver](#) (S. 27)

Dieser Ansatz kommt für Sie in Frage, wenn Sie über eine einzelne Arbeitsstation oder über eine geringe Anzahl von Arbeitsstationen verfügen und wenn ein Netzwerkinstallationsserver verfügbar ist.

Tabelle 2.1 *Installation von den SUSE Linux Enterprise-Medien*

Installationsquelle	SUSE Linux Enterprise-Medienkit
Aufgaben, die einen manuellen Eingriff erfordern	<ul style="list-style-type: none">• Einlegen der Installationsmedien• Booten des Installationsziels• Wechseln der Medien• Festlegen des YaST-Installationsbereichs• Konfigurieren des Systems mit YaST
Entfernt gesteuerte Aufgaben	Keine
Details	„Installation von den SUSE Linux Enterprise-Medien“ (S. 39)

Tabelle 2.2 *Installation von einem Netzwerksver mit SLP*

Installationsquelle	Netzwerkinstallationsserver mit den SUSE Linux Enterprise-Installationsmedien
Aufgaben, die einen manuellen Eingriff erfordern	<ul style="list-style-type: none">• Einlegen der Boot-Disk• Booten des Installationsziels• Festlegen des YaST-Installationsbereichs• Konfigurieren der Firewall mit YaST
Entfernt gesteuerte Aufgaben	Keine, aber diese Methode kann mit VNC kombiniert werden.

Tabelle 2.3 *Installation von einem Netzwerkservers*

Installationsquelle	Netzwerkinstallationsserver mit den SUSE Linux Enterprise-Installationsmedien
Aufgaben, die einen manuellen Eingriff erfordern	<ul style="list-style-type: none"> • Einlegen der Boot-Disk • Angeben von Boot-Optionen • Booten des Installationsziels • Festlegen des YaST-Installationsbereichs • Konfigurieren der Firewall mit YaST
Entfernt gesteuerte Aufgaben	Keine, aber diese Methode kann mit VNC kombiniert werden.
Details	„Installation von einem Netzwerkservers“ (S. 40)

2.2 Einsatz von bis zu 100 Arbeitsstationen

Bei einer großen Anzahl zu installierender Arbeitsstationen möchten Sie sicher nicht jede manuell einzeln installieren und konfigurieren. Es gibt viele automatisierte oder halbautomatisierte Vorgänge sowie einige Optionen zum Durchführen einer Installation mit minimalen oder gar keinen Eingriffen durch den Benutzer.

Bevor Sie einen vollautomatisierten Ansatz in Betracht ziehen, sollten Sie beachten, dass ein sehr komplexes Szenario auch sehr lange eingerichtet werden muss. Wenn es bei Ihrer Installation auf die Zeit ankommt, ist es eventuell besser, eine weniger komplexe Methode zu wählen, die schneller durchgeführt werden kann. Automatisierung

eignet sich vor allem für riesige Installationen und solche, die von einem entfernten Standort erfolgen müssen.

Wählen Sie aus folgenden Optionen:

[Einfache Installation mit entferntem Zugriff über VNC – Statische Netzwerkkonfiguration](#) (S. 29)

Dieser Ansatz kommt in einem kleinen bis mittleren Szenario mit einer statischen Netzwerkeinrichtung in Frage. Ein Netzwerk, ein Netzwerkinstallationsserver und die VNC-Anwendung sind erforderlich.

[Einfache Installation mit entferntem Zugriff über VNC – Dynamische Netzwerkkonfiguration](#) (S. 30)

Dieser Ansatz kommt in einem kleinen bis mittleren Szenario mit einer dynamischen Netzwerkeinrichtung in Frage. Ein Netzwerk, ein Netzwerkinstallationsserver und die VNC-Anwendung sind erforderlich.

[Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN](#) (S. 30)

Dieser Ansatz kommt in einem kleinen bis mittleren Szenario in Frage und sollte über das Netzwerk und ohne Eingriff auf die Installationsziele erfolgen. Ein Netzwerk, ein Netzwerkinstallationsserver, Netzwerk-Boot-Images, Netzwerk-bootfähige Zielhardware und die VNC-Anwendung sind erforderlich.

[Einfache Installation mit entferntem Zugriff über SSH – Statische Netzwerkkonfiguration](#) (S. 31)

Dieser Ansatz kommt in einem kleinen bis mittleren Szenario mit einer statischen Netzwerkeinrichtung in Frage. Ein Netzwerk, ein Netzwerkinstallationsserver und die SSH-Client-Anwendung sind erforderlich.

[Entfernte Installation über SSH – Dynamische Netzwerkkonfiguration](#) (S. 32)

Dieser Ansatz kommt in einem kleinen bis mittleren Szenario mit einer dynamischen Netzwerkeinrichtung in Frage. Ein Netzwerk, ein Netzwerkinstallationsserver und die SSH-Client-Anwendung sind erforderlich.

[Installation auf entfernten Systemen über SSH – PXE-Boot und Wake-on-LAN](#) (S. 32)

Dieser Ansatz kommt in einem kleinen bis mittleren Szenario in Frage und sollte über das Netzwerk und ohne Eingriff auf die Installationsziele erfolgen. Ein Netzwerk, ein Netzwerkinstallationsserver, Netzwerk-Boot-Images, Netzwerk-bootfähige Zielhardware und die SSH-Client-Anwendung sind erforderlich.

Einfache Masseninstallation (S. 33)

Dieser Ansatz kommt bei großen Installationen auf identischen Maschinen in Frage. Bei einer Konfiguration zum Netzwerkstart ist kein direkter Eingriff auf die Zielsysteme erforderlich. Ein Netzwerk, ein Netzwerkinstallationsserver, eine entfernte Steueranwendung, wie der VNC-Viewer oder ein SSH-Client, und ein AutoYaST-Konfigurationsprofil sind erforderlich. Wenn Sie den Netzwerk-Boot verwenden, sind außerdem ein Netzwerk-Boot-Image und Netzwerk-bootfähige Hardware erforderlich.

Regelbasierte automatische Installation (S. 34)

Dieser Ansatz eignet sich für große Installationen auf verschiedene Hardwaretypen. Bei einer Konfiguration zum Netzwerkstart ist kein direkter Eingriff auf die Zielsysteme erforderlich. Ein Netzwerk, ein Netzwerkinstallationsserver, eine entfernte Steueranwendung, wie der VNC-Viewer oder ein SSH-Client, und mehrere AutoYaST-Konfigurationsprofile sowie eine Regel für AutoYaST sind erforderlich. Wenn Sie den Netzwerk-Boot verwenden, sind außerdem ein Netzwerk-Boot-Image und Netzwerk-bootfähige Hardware erforderlich.

Tabelle 2.4 *Einfache Installation mit entferntem Zugriff über VNC – Statische Netzwerkkonfiguration*

Installationsquelle	Netzwerk
Vorbereitung	<ul style="list-style-type: none">• Einrichten einer Installationsquelle• Booten vom Installationsmedium
Steuerung und Überwachung	Entfernt: VNC
Am besten geeignet für	Kleine bis mittlere Szenarien mit verschiedener Hardware
Nachteile	<ul style="list-style-type: none">• Jede Maschine muss einzeln eingerichtet werden.• Direkter Eingriff ist zum Booten erforderlich.

Details	Abschnitt 4.1.1, „Einfache Installation mit entferntem Zugriff über VNC – Statische Netzwerkkonfiguration“ (S. 76)
---------	--

Tabelle 2.5 *Einfache Installation mit entferntem Zugriff über VNC – Dynamische Netzwerkkonfiguration*

Installationsquelle	Netzwerk
Vorbereitung	<ul style="list-style-type: none"> • Einrichten einer Installationsquelle • Booten vom Installationsmedium
Steuerung und Überwachung	Entfernt: VNC
Am besten geeignet für	Kleine bis mittlere Szenarien mit verschiedener Hardware
Nachteile	<ul style="list-style-type: none"> • Jede Maschine muss einzeln eingerichtet werden. • Direkter Eingriff ist zum Booten erforderlich.
Details	Abschnitt 4.1.2, „Einfache Installation mit entferntem Zugriff über VNC – Dynamische Netzwerkkonfiguration“ (S. 78)

Tabelle 2.6 *Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN*

Installationsquelle	Netzwerk
Vorbereitung	<ul style="list-style-type: none"> • Einrichten einer Installationsquelle • Konfigurieren von DHCP, TFTP, PXE-Boot und WOL

	<ul style="list-style-type: none"> • Booten vom Netzwerk
Steuerung und Überwachung	Entfernt: VNC
Am besten geeignet für	<ul style="list-style-type: none"> • Kleine bis mittlere Szenarien mit verschiedener Hardware • Komplett entfernte Installationen; standortübergreifende Installation
Nachteile	Jede Maschine muss manuell eingerichtet werden.
Details	Abschnitt 4.1.3, „Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN“ (S. 79)

Tabelle 2.7 *Einfache Installation mit entferntem Zugriff über SSH – Statische Netzwerkkonfiguration*

Installationsquelle	Netzwerk
Vorbereitung	<ul style="list-style-type: none"> • Einrichten einer Installationsquelle • Booten vom Installationsmedium
Steuerung und Überwachung	Entfernt: SSH
Am besten geeignet für	<ul style="list-style-type: none"> • Kleine bis mittlere Szenarien mit verschiedener Hardware • Verbindungen mit geringer Bandbreite zum Ziel
Nachteile	<ul style="list-style-type: none"> • Jede Maschine muss einzeln eingerichtet werden. • Direkter Eingriff ist zum Booten erforderlich.

Details	Abschnitt 4.1.4, „Einfache Installation mit entferntem Zugriff über SSH – Statische Netzwerkkonfiguration“ (S. 81)
---------	--

Tabelle 2.8 *Entfernte Installation über SSH – Dynamische Netzwerkkonfiguration*

Installationsquelle	Netzwerk
Vorbereitung	<ul style="list-style-type: none"> • Einrichten einer Installationsquelle • Booten vom Installationsmedium
Steuerung und Überwachung	Entfernt: SSH
Am besten geeignet für	<ul style="list-style-type: none"> • Kleine bis mittlere Szenarien mit verschiedener Hardware • Verbindungen mit geringer Bandbreite zum Ziel
Nachteile	<ul style="list-style-type: none"> • Jede Maschine muss einzeln eingerichtet werden. • Direkter Eingriff ist zum Booten erforderlich.
Details	Abschnitt 4.1.5, „Einfache entfernte Installation über SSH – Dynamische Netzwerkkonfiguration“ (S. 82)

Tabelle 2.9 *Installation auf entfernten Systemen über SSH – PXE-Boot und Wake-on-LAN*

Installationsquelle	Netzwerk
Vorbereitung	<ul style="list-style-type: none"> • Einrichten einer Installationsquelle • Konfigurieren von DHCP, TFTP, PXE-Boot und WOL

	<ul style="list-style-type: none"> • Booten vom Netzwerk
Steuerung und Überwachung	Entfernt: SSH
Am besten geeignet für	<ul style="list-style-type: none"> • Kleine bis mittlere Szenarien mit verschiedener Hardware • Komplett entfernte Installationen; standortübergreifende Installation • Verbindungen mit geringer Bandbreite zum Ziel
Nachteile	Jede Maschine muss einzeln eingerichtet werden.
Details	Abschnitt 4.1.6, „Installation auf entfernten Systemen über SSH – PXE-Boot und Wake-on-LAN“ (S. 84)

Tabelle 2.10 *Einfache Masseninstallation*

Installationsquelle	Vorzugsweise Netzwerk
Vorbereitung	<ul style="list-style-type: none"> • Sammeln von Hardwareinformationen • Erstellen des AutoYaST-Profiles • Einrichten des Installationservers • Verteilen des Profils • Einrichten des Netzwerkstarts (DHCP, TFTP, PXE, WOL) <p><i>Oder:</i></p> <p>Booten des Ziels vom Installationsmedium</p>

Steuerung und Überwachung	Lokal oder entfernt über VNC oder SSH
Am besten geeignet für	<ul style="list-style-type: none"> • Große Szenarien • Identische Hardware • Kein Zugriff auf System (Netzwerkstart)
Nachteile	Gilt nur für Maschinen mit identischer Hardware
Details	Abschnitt 5.1, „Einfache Masseninstallation“ (S. 115)

Tabelle 2.11 *Regelbasierte automatische Installation*

Installationsquelle	Vorzugsweise Netzwerk
Vorbereitung	<ul style="list-style-type: none"> • Sammeln von Hardwareinformationen • Erstellen der AutoYaST-Profile • Erstellen der AutoYaST-Regeln • Einrichten des Installationsservers • Verteilen des Profils • Einrichten des Netzwerkstarts (DHCP, TFTP, PXE, WOL) <p><i>Oder:</i></p> <p>Booten des Ziels vom Installationsmedium</p>
Steuerung und Überwachung	Lokal oder entfernt über VNC oder SSH
Am besten geeignet für	<ul style="list-style-type: none"> • Unterschiedliche Hardware

- Standortübergreifende Installationen

Nachteile

Komplexes Einrichten der Regeln

Details

[Abschnitt 5.2, „Regelbasierte automatische Installation“](#)
(S. 127)

2.3 Installation auf mehr als 100 Arbeitsstationen

Die meisten Betrachtungen für mittlere Installationsszenarien gelten [Abschnitt 2.1, „Einsatz von bis zu 10 Arbeitsstationen“](#) (S. 25) auch für große Installationen. Durch eine wachsende Anzahl von Installationszielen steigen jedoch die Vorteile einer vollautomatischen Installationsmethode. Die Nachteile dieser Methode sind vergleichsweise gering.

Der beträchtliche Zeitaufwand zum Erstellen anspruchsvoller Regeln und Class-Framework in AutoYaST lohnt sich für die Ansprüche eines riesigen Installationsstandorts. Wenn Sie nicht auf jedes Ziel einzeln zugreifen müssen, sparen Sie unter Umständen enorm viel Zeit, je nach der Größe Ihres Installationsprojekts.

Installation mit YaST

Nachdem Ihre Hardware zur Installation von SUSE Linux Enterprise Server vorbereitet wurde, wie im Handbuch *Architecture-Specific Information* beschrieben, und die Verbindung mit dem Installationssystem aufgebaut wurde, wird die Schnittstelle des SUSE Linux Enterprise-Systemassistenten YaST angezeigt. YaST kümmert sich um alle folgenden Schritte für die Konfiguration des Systems und führt Sie durch den ganzen Installations- und Konfigurationsvorgang.

3.1 IBM-System z: Systemstart für die Installation

Für IBM-System z-Plattformen wird das System initialisiert (IPL), wie im Handbuch *Architecture-Specific Information* beschrieben. SUSE Linux Enterprise Server zeigt auf diesen Systemen keinen Eröffnungsbildschirm. Laden Sie während des Installationsvorgangs den Kernel, initrd und parmfile manuell. YaST beginnt mit seinem Installationsbildschirm, sobald über VNC, X oder SSH eine Verbindung zum Installationssystem aufgebaut wurde. Da kein Eröffnungsbildschirm vorhanden ist, können Kernel- oder Boot-Parameter nicht am Bildschirm eingegeben werden, sondern müssen in einer Parameterdatei (parmfile) eingegeben werden. (Eine Beschreibung finden Sie im Kapitel "Parmfile" im Handbuch *Architecture-Specific Information*.)

TIPP: IBM-System z: Die nächsten Schritte

Folgen Sie für die Installation der Beschreibung des Installationsvorgangs mit YaST, beginnend mit [Abschnitt 3.4, „Sprachauswahl“](#) (S. 42).

3.2 Systemstart für die Installation

Legen Sie die erste SUSE Linux Enterprise-CD oder die DVD in das Laufwerk ein. Starten Sie den Computer dann neu, um das Installationsprogramm vom Datenträger im Laufwerk zu starten.

3.2.1 Boot-Optionen

Von CD oder DVD abweichende Boot-Optionen existieren und können benutzt werden, wenn beim Booten von CD oder DVD Probleme auftreten. Eine Beschreibung dieser Optionen finden Sie unter [Tabelle 3.1, „Boot-Optionen“](#) (S. 38).

Tabelle 3.1 *Boot-Optionen*

Boot-Option	Beschreibung
CD-ROM	Dies ist die einfachste Boot-Option. Diese Option kann benutzt werden, wenn das System über ein lokales CD-ROM-Laufwerk verfügt, das von Linux unterstützt wird.
Diskette	Die Images zum Generieren von Boot-Disketten befinden sich auf CD 1 im Verzeichnis <code>/boot</code> . Eine README-Datei steht im selben Verzeichnis zur Verfügung.
PXE oder BOOTP	Dies muss vom BIOS oder der Firmware des Systems unterstützt werden und ein Boot-Server muss im Netzwerk verfügbar sein. Diese Aufgabe kann auch von einem anderen SUSE Linux Enterprise-System erledigt werden.
Festplatte	SUSE Linux Enterprise lässt sich auch von der Festplatte booten. Kopieren Sie dafür den Kernel (<code>linux</code>) und das Installationssystem (<code>initrd</code>) aus dem Verzeichnis <code>/boot/loader</code> der CD 1 auf die Festplatte und fügen Sie dem Bootloader den entsprechenden Eintrag hinzu.

3.2.2 Auswählen der Quelle der Installationsdaten

Sie können die Installation von einer lokalen Installationsquelle ausführen, beispielsweise von SUSE Linux Enterprise-CDs oder DVD, oder die Installationsquellen von einem FTP-, HTTP- oder NFS-Server beziehen. Jede dieser Methoden setzt physischen Zugriff auf das zu installierende System sowie Eingriffe des Benutzers während der Installation voraus. Der Installationsvorgang ist grundsätzlich gleich, unabhängig von der bevorzugten Installationsquelle oder -methode.

Installation von den SUSE Linux Enterprise-Medien

So installieren Sie von physischen Medien (Ihrem SUSE Linux Enterprise-Medienkit):

- 1 Legen Sie das Medium in Ihr CD- oder DVD-Laufwerk ein.
- 2 Booten Sie das System neu.
- 3 Wählen Sie am Boot-Bildschirm *Installation* und folgen Sie den Anleitungen unter [Abschnitt 3.3, „Der Boot-Bildschirm“](#) (S. 41) und in den folgenden Abschnitten.

Installation von einem Netzwerkserver mit SLP

Wenn Ihre Netzwerkkonfiguration OpenSLP unterstützt und die Netzwerkinstallationsquelle so konfiguriert wurde, dass sie sich über OpenSLP (siehe [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85)) ankündigt, fahren Sie wie folgt mit der SUSE Linux Enterprise-Installation fort.

- 1 Richten Sie einen Installationsserver ein, wie unter [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85) beschrieben.
- 2 Legen Sie die erste CD des Medienkits in das CD-ROM-Laufwerk ein und booten Sie den Rechner neu.
- 3 Wählen Sie am Boot-Bildschirm *Installation*, drücken Sie **F4** und wählen Sie dann *SLP*.

Das Installationsprogramm ruft den Speicherort der Netzwerkinstallationsquelle mithilfe von OpenSLP ab und konfiguriert die Netzwerkverbindung mit DHCP. Bei einem Problem der DHCP-Netzwerkconfiguration werden Sie aufgefordert, die geeigneten Parameter manuell einzugeben. Die Installation fährt dann normal fort.

- 4 Beenden Sie die Installation so, als hätten Sie die Installation von physischen Medien gewählt.

Installation von einem Netzwerkservers

So führen Sie eine manuelle Installation mithilfe einer Netzwerkinstallationsquelle aus:

- 1 Richten Sie einen Installationsserver ein, wie unter [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85) beschrieben.
- 2 Legen Sie die erste CD bzw. DVD des Medienkits in das entsprechende Laufwerk ein und booten Sie den Rechner neu.
- 3 Wählen Sie am Boot-Bildschirm *Installation* und geben Sie an der Boot-Eingabeaufforderung die benötigten Informationen ein, beispielsweise:

- Adresse des Installationsservers:

```
install=protokoll:inst_quelle
```

Ersetzen Sie *protocol* durch das Protokollpräfix für den Dienst, den der Installationsserver benutzt (*nfs*, *http* oder *ftp*). Ersetzen Sie *inst_source* durch die IP-Adresse des Installationsservers.

- Parameter für die Netzwerkconfiguration, falls die DHCP-Konfiguration nicht unterstützt wird (siehe [Abschnitt 4.4.3, „Benutzerdefinierte Boot-Optionen“](#) (S. 108)).
- 4 Drücken Sie die Eingabetaste, um zur Installation zu booten. Wenn keine Netzwerkparameter an der Boot-Eingabeaufforderung angegeben wurden, versuchen die Installationsroutinen, das Netzwerk mit DHCP zu konfigurieren. Falls dabei ein Problem auftritt, werden Sie zur Angabe der entsprechenden Parameter aufgefordert. Nach Eingabe der Parameter wird die Installation fortgesetzt.

- 5 Schließen Sie die Installation so ab, als wäre sie von den physischen Medien erfolgt.

3.3 Der Boot-Bildschirm

Im Boot-Bildschirm werden mehrere Optionen für den Installationsvorgang angezeigt. Mit *Boot from Hard Disk* wird das installierte System gebootet. Dieser Eintrag ist standardmäßig ausgewählt, da die CD häufig im Laufwerk vergessen wird. Wählen Sie zum Installieren des Systems eine der Installationsoptionen mithilfe der Pfeiltasten aus. Folgende Optionen sind relevant:

Installation

Der normale Installationsmodus. Alle modernen Hardware-Funktionen sind aktiviert.

Installation – ACPI deaktiviert

Wenn bei der normalen Installation ein Fehler auftritt, kann dies an der fehlenden Unterstützung der ACPI (Advanced Configuration and Power Interface) durch das System liegen. Wenn dies der Fall ist, verwenden Sie diese Option, um die Installation ohne ACPI-Unterstützung durchzuführen.

Installation – Sichere Einstellungen

Startet das System mit deaktiviertem DMA-Modus (für CD-ROM-Laufwerke), Energieverwaltungsfunktionen werden ebenfalls deaktiviert. Experten können auch die Kommandozeile verwenden, um Kernel-Parameter einzugeben oder zu ändern.

Mithilfe der in der Leiste im unteren Bildschirmbereich genannten Funktionstasten können Sie eine Reihe von Installationseinstellungen ändern.

F1

Rufen Sie die kontextabhängige Hilfe für das aktive Element des Boot-Bildschirms auf.

F2

Wählen Sie die Anzeigesprache für die Installation aus.

F3

Wählen Sie verschiedene Modi für die grafische Darstellung während der Installation aus. Wählen Sie den Expertenmodus aus, wenn die grafische Installation Probleme verursacht.

F4

In der Regel wird die Installation vom eingelegten Installationsdatenträger ausgeführt. Wählen Sie hier andere Quellen, wie etwa FTP- oder NFS-Server. Wenn die Installation in einem Netzwerk mit einem SLP-Server erfolgt, wählen Sie mit dieser Option eine von den auf dem Server verfügbaren Installationsquellen. Informationen zu SLP erhalten Sie im [Kapitel 32, SLP-Dienste im Netzwerk](#) (S. 669).

F5

Hiermit geben Sie dem System an, dass Sie einen optionalen Datenträger mit einem Treiber-Update für SUSE Linux Enterprise Server verwenden. Sie werden zum gegebenen Zeitpunkt des Installationsvorgangs aufgefordert, den Datenträger für das Update in das Laufwerk einzulegen.

Einige Sekunden nach Beginn der Installation lädt SUSE Linux Enterprise ein minimales Linux-System zum Ausführen des Installationsvorgangs. Wenn Sie verfolgen möchten, welche Vorgänge beim Booten ablaufen, drücken Sie [\[ESC\]](#), um die Meldungen und Copyright-Hinweise anzuzeigen. Am Ende des Ladevorgangs wird das YaST-Installationsprogramm gestartet. Nach einigen Sekunden wird auf dem Bildschirm das grafische Installationsprogramm angezeigt.

An diesem Punkt beginnt die eigentliche Installation von SUSE Linux Enterprise. Alle YaST-Bildschirme weisen das gleiche Layout auf. Alle Schaltflächen, Eingabefelder und Listen können mit der Maus oder über die Tastatur aufgerufen werden. Wenn sich der Mauszeiger nicht bewegen lässt, wurde die Maus nicht automatisch erkannt. Verwenden Sie in diesem Fall vorübergehend die Tastatur. Die Navigation per Tastatur ähnelt der Beschreibung in [Abschnitt 7.11.1, „Navigation in Modulen“](#) (S. 203).

3.4 Sprachauswahl

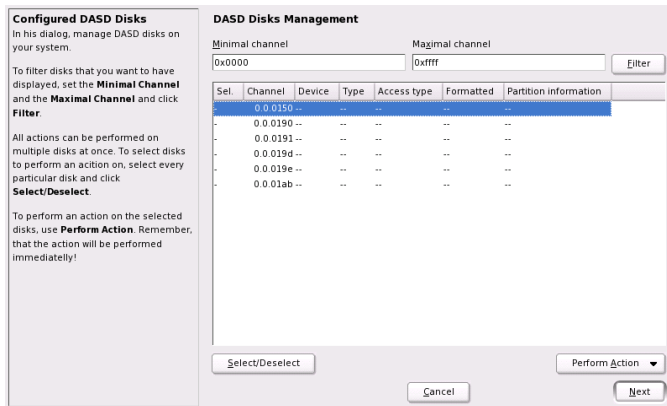
YaST und SUSE Linux Enterprise können im Allgemeinen so konfiguriert werden, dass entsprechend Ihren Anforderungen verschiedene Sprachen verwendet werden. Die hier ausgewählte Sprache wird auch für die Tastaturbelegung verwendet. YaST verwendet diese Spracheinstellung auch, um eine Zeitzone für die Systemuhr zu bestimmen. Diese Einstellungen können später bei der Auswahl sekundärer Sprachen geändert werden, die auf Ihrem System installiert werden sollen. Falls die Maus nicht funktioniert, wählen Sie die Sprache mithilfe der Pfeiltasten aus und drücken Sie so lange die [\[Tabulatortaste\]](#), bis die Option *Weiter* ausgewählt ist. Drücken Sie anschließend zum Bestätigen der Sprachauswahl die [\[Eingabetaste\]](#).

3.5 IBM-System z: Konfiguration der Festplatte

Bei der Installation auf IBM-System z-Plattformen folgt auf das Dialogfeld für Sprachauswahl ein Dialogfeld zur Konfiguration der angeschlossenen Festplatten. Wählen Sie DASD, zFCP (per Fiber-Channel angeschlossene SCSI-Platten) oder iSCSI für die Installation von SUSE Linux Enterprise Server.

Nachdem Sie *Configure DASD Disks* (DASD-Partitionen konfigurieren) gewählt haben, werden in einer Übersicht alle verfügbaren DASDs aufgelistet. Geben Sie für ein klareres Bild der verfügbaren Geräte einen Bereich der anzuzeigenden Kanäle in das Eingabefeld über der Liste ein. Um die Liste nach einem solchen Bereich zu filtern, wählen Sie *Filtern*. Siehe [Abbildung 3.1](#), „IBM-System z: Wählen einer DASD-Partition“ (S. 43).

Abbildung 3.1 IBM-System z: Wählen einer DASD-Partition



Geben Sie nun die DASD-Partitionen für die Installation an, indem Sie die entsprechenden Einträge durch einen Klick auf *Auswählen* bzw. *Abwählen* festlegen. Aktivieren Sie anschließend die DASD-Partitionen und stellen Sie sie bereit, indem Sie *Aktion ausführen* → *Aktivieren* wählen (siehe [Abbildung 3.2](#), „IBM-System z: Aktivieren einer DASD-Partition“ (S. 44)). Wählen Sie zur Formatierung der DASD-Partitionen sofort *Aktion ausführen* → *Format (Formatieren)* oder verwenden Sie später das YaST-Partitionierungsprogramm, wie in „[Partitionierung mit YaST](#)“ (S. 50) beschrieben.

Abbildung 3.2 IBM-System z: Aktivieren einer DASD-Partition

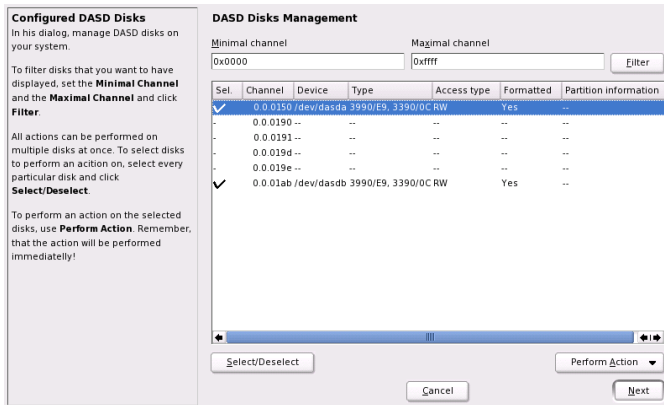
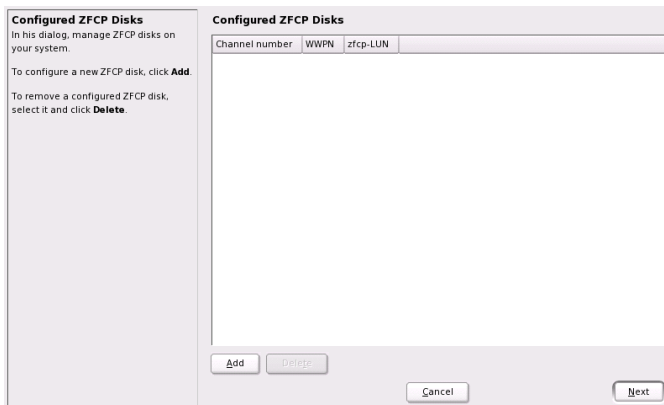


Abbildung 3.3 IBM-System z: Überblick über verfügbare ZFCP-Partitionen



Zur Verwendung von ZFCP-Partitionen für die SUSE Linux Enterprise Server-Installation wählen Sie *Configure ZFCP Disks* (ZFCP-Partitionen konfigurieren) im Auswahldialogfeld. Dadurch wird ein Dialogfeld mit einer Liste der ZFCP-Partitionen geöffnet, die auf dem System verfügbar sind. Wählen Sie in diesem Dialogfeld *Hinzufügen*, um ein weiteres Dialogfeld zu öffnen, in dem Sie ZFCP-Parameter eingeben können (siehe [Abbildung 3.3](#), „IBM-System z: Überblick über verfügbare ZFCP-Partitionen“ (S. 44)).

Damit eine ZFCP-Partition für die SUSE Linux Enterprise Server-Installation verfügbar ist, verwenden Sie die Eingabefelder *Channel Number* (Kanalnummer), *WWPN* (World

Wide Port Number) und *FCP-LUN*, um die Parameter für die entsprechende Partition anzugeben. Schließen Sie am Ende das ZFCP-Dialogfeld mit *Weiter* und das Dialogfeld zur allgemeinen Festplattenkonfiguration mit *Beenden*, um mit der weiteren Konfiguration fortzufahren.

3.6 Lizenzvereinbarung

Lesen Sie die auf dem Bildschirm angezeigte Lizenzvereinbarung genau durch. Wenn Sie den darin aufgeführten Bedingungen zustimmen, wählen Sie *Ja, ich akzeptiere diese Lizenzvereinbarung* und klicken Sie zum Bestätigen der Auswahl auf *Weiter*. Wenn Sie die Lizenzvereinbarung nicht akzeptieren, dürfen Sie SUSE Linux Enterprise nicht installieren und die Installation wird beendet.

3.7 Systemanalyse

Wählen Sie *Neuinstallation* oder *Update des bestehenden Systems* aus. Das Update ist nur möglich, wenn bereits ein SUSE Linux Enterprise-System installiert ist. Wenn bereits ein SUSE Linux Enterprise-System installiert ist, können Sie mit *Andere* auf zwei erweiterte Optionen zugreifen: Sie können mit *Installiertes System starten* das installierte System booten, oder, wenn es sich nicht booten lässt, können Sie versuchen, das Problem mit *Reparatur des installierten Systems* zu beheben. Wenn kein SUSE Linux Enterprise-System installiert ist, können Sie nur eine Neuinstallation ausführen.

In den folgenden Abschnitten wird die Installation eines neuen Systems beschrieben. Detaillierte Anweisungen für eine Systemaktualisierung finden Sie in [Abschnitt 7.3.7, „Aktualisieren des Systems“](#) (S. 163). Eine Beschreibung Optionen für die Systemreparatur finden Sie in [„Verwenden der YaST-Systemreparatur“](#) (S. 1027).

Um zusammen mit dem System ein Zusatzprodukt, eine Erweiterung für Ihr SUSE Linux Enterprise, zu installieren, wählen Sie *Add-on-Produkte aus separaten Medien einschließen* und klicken Sie auf *Weiter*. Klicken Sie im nächsten Dialogfeld auf *Hinzufügen*, um zusätzliche Medien hinzuzufügen.

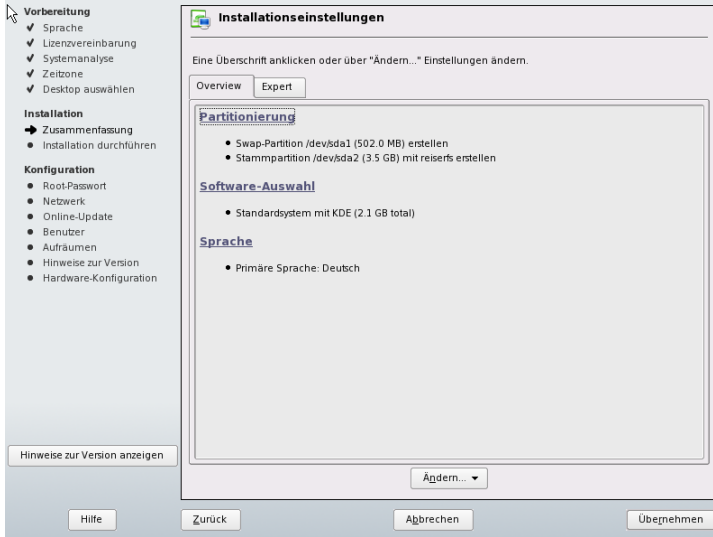
3.8 Zeitzone

Wählen Sie in diesem Dialogfeld Ihre Region und die entsprechende Zeitzone in den Listen aus. Während der Installation werden beide Werte entsprechend der ausgewählten Installationssprache festgelegt. Sie können zwischen *Lokale Zeit* und *UTC (GMT)* unter *Rechneruhr eingestellt auf* wählen. Die Auswahlmöglichkeit ist von den Einstellungen der Hardware-Uhr im BIOS Ihres Computers abhängig. Wenn Sie die Hardware-Uhr auf GMT (entspricht UTC) festlegen, schaltet SUSE Linux Enterprise automatisch von Standardzeit auf Sommerzeit und zurück um. Klicken Sie auf *Ändern*, um das aktuelle Datum und die Uhrzeit festzulegen. Klicken Sie anschließend auf *Weiter*, um die Installation fortzusetzen.

3.9 Installationsüberblick

Nach einer eingehenden Systemanalyse zeigt YaST sinnvolle Vorschläge für alle Installationseinstellungen an. Die Optionen, die in den gängigen Installationssituationen gelegentlich ein manuelles Eingreifen erfordern, werden auf der Registerkarte *Überblick* dargestellt. Speziellere Optionen finden Sie auf der Registerkarte *Erweitert*. Nach der Konfiguration der in diesen Dialogfeldern dargestellten Elemente kehren Sie immer zum Überblicksfenster zurück, das entsprechend aktualisiert wird. Die einzelnen Einstellungen werden in den folgenden Abschnitten beschrieben.

Abbildung 3.4 *Installationseinstellungen*



3.9.1 Partitionierung

In den meisten Fällen schlägt YaST ein passendes Partitionierungsschema vor, das ohne Änderungen übernommen werden kann. Darüber hinaus besteht die Möglichkeit, die Partitionierung mit YaST anzupassen. In diesem Abschnitt werden die erforderlichen Schritte beschrieben.

Partitionstypen

TIPP: IBM-System z: Festplatten

Auf den IBM-System z-Plattformen unterstützt SUSE Linux Enterprise Server SCSI-Festplatten sowie DASD-Partitionen (Direct Access Storage Devices). Während sich SCSI-Datenträger wie unten beschrieben partitionieren lassen, sind für DASDs maximal drei Partitionseinträge in den entsprechenden Partitionstabellen möglich.

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, eine erweiterte Partition kann 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.

TIPP: Festplatten mit GPT-Festplattenkennung

Für Architekturen, in denen die GPT-Festplattenkennung verwendet wird, ist die Anzahl der primären Partitionen nicht begrenzt. Folglich sind keine logischen Partitionen vorhanden.

Erforderlicher Festplattenspeicher

In der Regel schlägt YaST ein sinnvolles Partitionierungsschema mit ausreichend Festplattenspeicher vor. Wenn Sie ein eigenes Partitionierungsschema implementieren möchten, sollten Sie folgende Empfehlungen bezüglich der Anforderungen der unterschiedlichen Systemtypen berücksichtigen.

Minimalinstallation: 500 MB

Es wird keine grafische Bedienoberfläche (X-Windows-System) installiert. Dies bedeutet, dass ausschließlich Konsolenanwendungen verwendet werden können. Darüber hinaus wird nur sehr grundlegende Software installiert.

Minimalinstallation mit grafischer Bedienoberfläche 700 MB

Dies beinhaltet das X-Window-System und einige Anwendungen.

Standardsystem: 1,5 GB

Diese Installation umfasst eine moderne Desktop-Umgebung, wie KDE oder GNOME, und bietet ausreichend Speicher für umfangreiche Anwendungs-Suites, wie Netscape oder Mozilla.

Vollständige Installation: 2,5 GB

Sämtliche mit SUSE Linux Enterprise gelieferten Pakete werden installiert.

Die zu erstellenden Partitionen sind vom verfügbaren Speicherplatz abhängig. Nachfolgend einige grundlegende Partitionierungsrichtlinien:

Bis zu 4 GB:

Eine Partition für den Swap-Speicherplatz und eine Root-Partition (/). In diesem Fall muss die Root-Partition genügend Platz für die Verzeichnisse bieten, die sich bei größeren Festplatten häufig auf ihren eigenen Partitionen befinden.

4 GB oder mehr:

Eine Swap-Partition, eine root-Partition (1 GB) und eine Partition für jedes der folgenden Verzeichnisse ist erforderlich: /usr (4 GB oder mehr), /opt (4 GB oder mehr) und /var (1 GB). Wenn Sie für diese Verzeichnisse keine separaten Partitionen verwenden möchten, fügen Sie der Root-Partition den empfohlenen Festplattenspeicher hinzu. Der restliche verfügbare Speicher kann für das Verzeichnis /home verwendet werden.

Je nach Hardware kann es sinnvoll sein, eine Boot-Partition (/boot) zu erstellen, in der der Boot-Mechanismus und der Linux-Kernel gespeichert sind. Diese Partition sollte sich am Anfang der Festplatte befinden und mindestens 8 MB bzw. einen Zylinder belegen. Als Faustregel gilt, dass immer eine solche Partition erstellt werden sollte, wenn dies von YaST ursprünglich vorgeschlagen wurde. Wenn Sie sich hierbei nicht sicher sind, erstellen Sie vorsichtshalber eine Boot-Partition.

Denken Sie immer daran, dass die Daten einiger (handelsüblicher) Programme in /opt installiert werden. Erstellen Sie daher entweder eine separate Partition für /opt oder weisen Sie der Root-Partition genügend Speicher zu.

Partitionierung mit YaST

Wenn Sie den Partitionierungseintrag im Vorschlagsfenster zum ersten Mal auswählen, werden im Dialogfeld für die YaST-Partitionierung die vorgeschlagenen Partitionseinstellungen angezeigt. Übernehmen Sie die aktuellen Einstellungen oder ändern Sie sie, bevor Sie fortfahren. Alternativ können Sie alle Einstellungen verwerfen und ganz von vorne beginnen.

Wenn Sie *Vorschlag annehmen* auswählen, wird die Partitionskonfiguration nicht geändert. Wenn Sie *Partitions-Setup basierend auf diesem Vorschlag ausführen* auswählen, wird *Festplatte vorbereiten: Expertenmodus* geöffnet. Hier können Sie die Partitionskonfiguration detailliert anpassen. Dieses Dialogfeld wird in [Abschnitt 7.5.8, „Partitionierung“](#) (S. 176) erläutert. Hier wird die ursprüngliche von YaST vorgeschlagene Konfiguration als Ausgangspunkt angezeigt.

Durch Auswahl von *Benutzerdefiniertes Partitions-Setup erstellen* wird das Dialogfeld für die Festplattenauswahl geöffnet. Verwenden Sie die Liste, um zwischen den bestehenden Festplatten auf Ihrem System zu wählen. SUSE Linux Enterprise wird auf der in diesem Dialogfeld ausgewählten Festplatte installiert.

Im nächsten Schritt wird festgelegt, ob eine vollständige Festplatte (*Gesamte Festplatte*) oder eine der vorhandenen Partitionen (sofern verfügbar) für die Installation verwendet werden soll. Wenn ein Windows-Betriebssystem auf der Festplatte gefunden wurde, werden Sie gefragt, ob die Partition gelöscht oder ihre Größe geändert werden soll. Lesen Sie [„Ändern der Größe einer Windows-Partition“](#) (S. 51), bevor Sie den Vorgang ausführen. Wenn Sie möchten, rufen Sie das Dialogfeld *Festplatte vorbereiten: Expertenmodus* auf, um eine benutzerdefinierte Partitionskonfiguration zu erstellen, wie in [Abschnitt 7.5.8, „Partitionierung“](#) (S. 176) beschrieben.

WARNUNG: Verwenden der gesamten Festplatte für die Installation

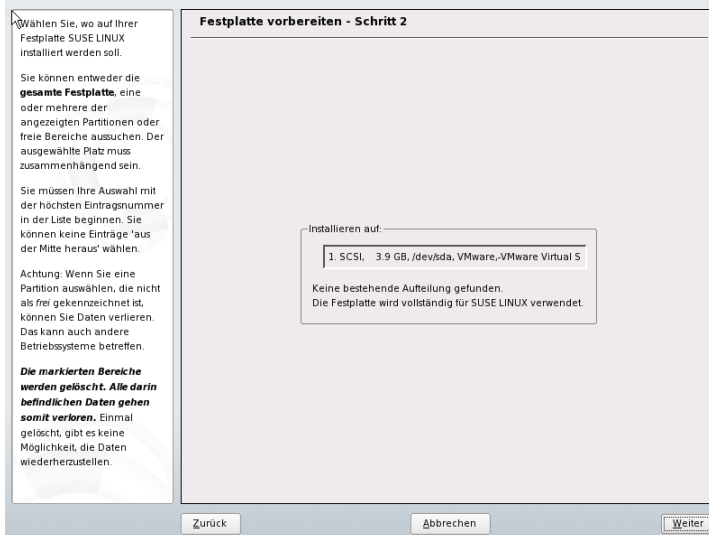
Wenn Sie *Gesamte Festplatte* auswählen, werden alle vorhandenen Daten auf der Festplatte zu einem späteren Zeitpunkt während der Installation vollständig gelöscht und gehen verloren.

YaST überprüft während der Installation, ob der Festplattenspeicher für die ausgewählte Software ausreicht. Ist dies nicht der Fall, ändert YaST die Auswahl der Software automatisch. Im Dialogfeld mit den Vorschlägen wird ein entsprechender Hinweis angezeigt. Solange genügend Festplattenspeicher verfügbar ist, übernimmt YaST Ihre Einstellungen und partitioniert die Festplatte entsprechend.

Ändern der Größe einer Windows-Partition

Wenn eine Festplatte, auf der eine Windows FAT- oder NTFS-Partition vorhanden ist, als Installationsziel ausgewählt wird, bietet YaST die Option, diese Partition zu löschen oder zu verkleinern. Auf diese Weise können Sie SUSE® Linux Enterprise auch dann installieren, wenn zurzeit nicht ausreichend Festplattenspeicher verfügbar ist. Diese Funktion ist besonders dann sinnvoll, wenn auf der ausgewählten Festplatte nur eine Windows-Partition vorhanden ist, die die gesamte Festplatte in Anspruch nimmt. Dies ist gelegentlich auf Computern der Fall, auf denen Windows bereits vorinstalliert ist. Wenn YaST feststellt, dass auf der ausgewählten Festplatte nicht genügend Speicherplatz vorhanden ist, der Speicher jedoch durch Löschen oder Verkleinern der Windows-Partition verfügbar gemacht werden kann, wird ein Dialogfeld angezeigt, in dem eine der beiden Optionen ausgewählt werden kann.

Abbildung 3.5 Mögliche Optionen für Windows-Partitionen



Wenn Sie *Windows komplett löschen* wählen, wird die Windows-Partition zum Löschen markiert und der entsprechende Speicherplatz wird für die Installation von SUSE Linux Enterprise verwendet.

WARNUNG: Löschen von Windows

Wenn Sie Windows löschen, werden alle Daten mit Beginn der Formatierung unwiederbringlich gelöscht.

Wenn Sie die Windows-Partition verkleinern möchten, brechen Sie die Installation ab und booten Sie Windows, um die Partition entsprechend vorzubereiten. Zwar ist dieser Schritt für FAT-Partitionen nicht zwingend erforderlich, er beschleunigt jedoch den Vorgang der Größenänderung und sorgt für mehr Sicherheit. Auf NTFS-Partitionen spielen diese Schritte eine entscheidende Rolle.

FAT-Dateisystem

Führen Sie unter Windows zunächst Scandisk aus, um sicherzustellen, dass auf der FAT-Partition keine einzelnen Dateifragmente oder Querverbindungen vorhanden sind. Führen Sie anschließend eine Defragmentierung aus, um die Dateien an den Anfang der Partition zu verschieben. Dadurch wird die Größenänderung in Linux beschleunigt.

Wenn Sie die Einstellungen des virtuellen Speichers für Windows optimiert haben, sodass eine zusammenhängende Swap-Datei mit derselben ursprünglichen (minimalen) und maximalen Größenbeschränkung verwendet wird, sollten Sie einen weiteren Schritt ausführen. Mit diesen Windows-Einstellungen kann es vorkommen, dass die Swap-Datei bei der Größenänderung in mehrere kleinere über die FAT-Partition verstreute Teile unterteilt wird. Zudem müsste die vollständige Swap-Datei während der Größenänderung verschoben werden. Hierdurch würde der Prozess stark verlangsamt. Daher ist es sinnvoll, diese Windows-Optimierungen vorübergehend zu deaktivieren und sie nach Abschluss der Größenänderung erneut zu aktivieren.

NTFS-Dateisystem

Führen Sie unter Windows Scandisk und dann eine Defragmentierung aus, um die Dateien an den Anfang der Festplatte zu verschieben. Im Gegensatz zum FAT-Dateisystem müssen die Schritte für dieses Dateisystem ausgeführt werden. Ansonsten kann die Größe der NTFS-Partition nicht geändert werden.

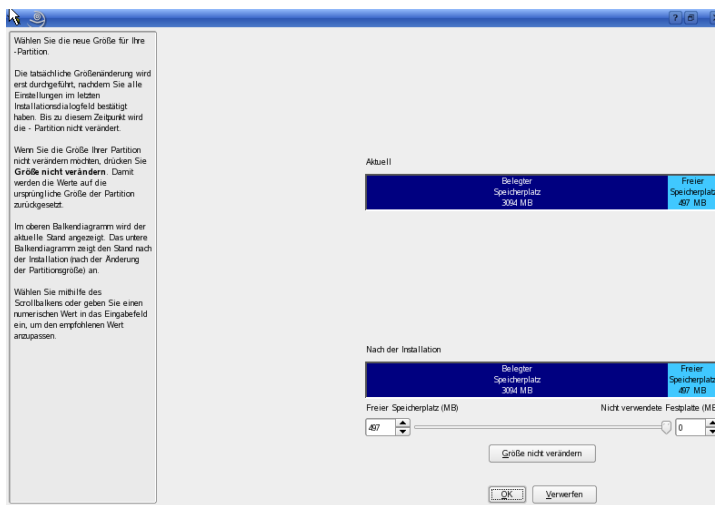
WICHTIG: Deaktivieren der Windows-Swap-Datei

Wenn Sie das System mit einer dauerhaften Swap-Datei auf einem NTFS-Dateisystem verwenden, befindet sich die Datei möglicherweise am Ende der Festplatte und verbleibt dort trotz der Defragmentierung. Daher ist unter

Umständen eine Verkleinerung der Partition erforderlich. Deaktivieren Sie in diesem Fall vorübergehend die Swap-Datei (den virtuellen Arbeitsspeicher unter Windows). Konfigurieren Sie den virtuellen Arbeitsspeicher nach der Änderung der Partitionsgröße erneut.

Kehren Sie, nachdem Sie diese Vorbereitungen getroffen haben, zur Konfiguration der Linux-Partitionierung zurück und wählen Sie *Windows-Partition verkleinern*. Nach einer kurzen Überprüfung der Partition öffnet YaST ein Dialogfeld mit einem Vorschlag für die Größenänderung der Windows-Partition.

Abbildung 3.6 Größe der Windows-Partition wird geändert



Im ersten Balkendiagramm wird dargestellt, wie viel Festplattenspeicher momentan von Windows belegt und wie viel Speicher noch verfügbar ist. Im zweiten Balkendiagramm wird dargestellt, wie der Speicherplatz nach der Größenänderung gemäß dem aktuellen Vorschlag von YaST verteilt wäre. Siehe [Abbildung 3.6, „Größe der Windows-Partition wird geändert“](#) (S. 53). Übernehmen Sie die vorgeschlagenen Einstellungen oder ändern Sie die Partitionsgröße (innerhalb bestimmter Grenzen) mithilfe des Schiebereglers.

Wenn Sie dieses Dialogfeld durch Auswahl von *Weiter* verlassen, werden die Einstellungen gespeichert und Sie gelangen zurück zum vorherigen Dialogfeld. Die tatsächliche Größenänderung findet später vor der Formatierung der Festplatte statt.

WICHTIG: Auf NTFS-Partitionen installierte Windows-Systeme

Für die Windows-Versionen NT, 2000 und XP wird das Dateisystem NTFS verwendet. Im Gegensatz zu FAT-Dateisystemen können NTFS-Dateisysteme von Linux nicht gelesen werden. Dies bedeutet, dass Sie Ihre Windows-Dateien unter Linux anzeigen, jedoch nicht bearbeiten können. Wenn Sie Schreibzugriff für Ihre Windows-Daten wünschen und das NTFS-Dateisystem nicht benötigen, installieren Sie Windows erneut auf einem FAT32-Dateisystem. In diesem Fall erhalten Sie unter SUSE Linux Enterprise vollständigen Zugriff auf Ihre Windows-Daten.

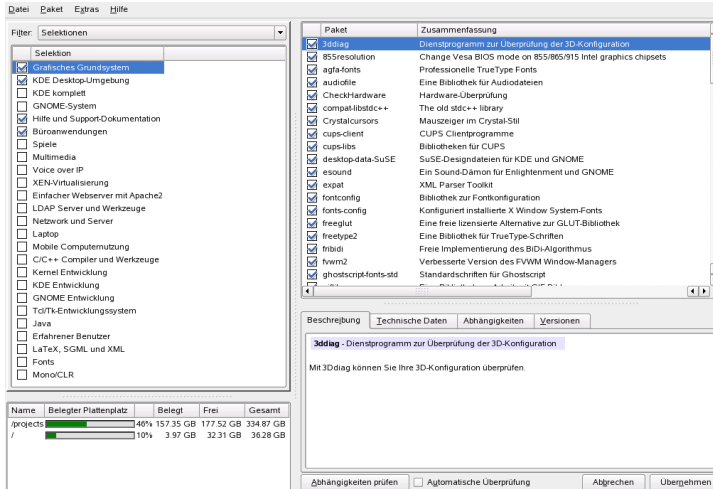
3.9.2 Software

SUSE Linux Enterprise enthält mehrere Software-Pakete für verschiedene Anwendungszwecke. Klicken Sie im Vorschlagsfenster auf *Software*, um die Softwareauswahl zu starten und den Installationsbereich entsprechend Ihren Bedürfnissen anzupassen. Wählen Sie die gewünschten Kategorien in der Liste in der Mitte aus und lesen Sie die Beschreibung im rechten Fenster. Jede Kategorie enthält eine Anzahl an Softwarepaketen, die die meisten Bedingungen für die entsprechende Kategorie erfüllen. Eine detailliertere Auswahl an zu installierenden Softwarepaketen erhalten Sie wenn Sie auf *Details* klicken, um zum YaST-Paket-Manager zu wechseln. Siehe [Abbildung 3.7, „Installieren und Entfernen der Software mit dem YaST-Paket-Manager“](#) (S. 55).

ANMERKUNG: Standard-Desktop

Der Standard-Desktop von SUSE Linux Enterprise ist GNOME. Klicken Sie zur Installation von KDE auf *Software* und wählen Sie *KDE Desktop-Umgebung* aus *Grafische Umgebungen*.

Abbildung 3.7 *Installieren und Entfernen der Software mit dem YaST-Paket-Manager*



Ändern des Installationsumfangs

Falls Sie bestimmte Softwareanforderungen erfüllen müssen, ändern Sie die aktuelle Auswahl im Paket-Manager, der diese Aufgabe wesentlich erleichtert. Im Paket-Manager stehen verschiedene Filterkriterien zur Vereinfachung der Auswahl mehrerer Pakete in SUSE Linux Enterprise zur Verfügung.

Das Feld für die Filterauswahl befindet sich links oben unterhalb der Menüleiste. Der Standardfilter ist *Schemata*. Schemainstallationspakete basieren auf der vorgesehenen Verwendung oder Aufgabe Ihres Systems. Wählen Sie beispielsweise *Dateiserver*, um Ihr System als NFS-Server einzurichten, oder *Web- und LAMP-Server*, um den Apache-Webserver zu installieren. Die bereits im aktuellen Systemtyp enthaltenen Gruppen sind vorausgewählt. Klicken Sie auf die Kontrollkästchen, um Gruppen für die Installation auszuwählen oder ihre Auswahl aufzuheben.

Im rechten Teil des Fensters wird eine Tabelle mit einzelnen in der aktuellen Gruppe enthaltenen Paketen angezeigt. In der äußersten linken Tabellenspalte wird der aktuelle Status der einzelnen Pakete angezeigt. Für die Installation sind insbesondere zwei Statusflags relevant: *Installieren* (das Kontrollkästchen vor dem Paketnamen ist aktiviert) und *Nicht installieren* (das Kontrollkästchen ist leer). Klicken Sie zum Auswählen oder zum Aufheben der Auswahl einzelner Software-Pakete auf das Statusfeld, bis der

gewünschte Status angezeigt wird. Alternativ klicken Sie mit der rechten Maustaste auf die Paketzeile, um ein Popup-Menü mit allen möglichen Statuseinstellungen anzuzeigen. Weitere Informationen hierzu erhalten Sie in der detaillierten Beschreibung des Moduls in [Abschnitt 7.3.1, „Installieren und Entfernen von Software“](#) (S. 152).

Andere Filter

Klicken Sie auf das Filterauswahlfeld, um die anderen möglichen Filter anzuzeigen. Auch die Auswahl unter *Paketgruppen* kann für die Installation verwendet werden. Dieser Filter führt zu einer thematischen Sortierung in der Baumstruktur auf der linken Seite. Je stärker die Zweige erweitert werden, desto spezifischer ist die Auswahl und desto weniger Pakete werden in der Liste der zugeordneten Pakete auf der rechten Seite angezeigt.

Mit *Suche* können Sie nach einem bestimmten Paket suchen. Dies wird in [Abschnitt 7.3.1, „Installieren und Entfernen von Software“](#) (S. 152) detailliert beschrieben.

Paketabhängigkeiten und -konflikte

Sie können nicht einfach eine beliebige Kombination an Software-Paketen installieren. Die verschiedenen Software-Pakete müssen miteinander kompatibel sein. Anderenfalls können sie sich gegenseitig beeinträchtigen und Konflikte mit Auswirkungen auf das gesamte System verursachen. Daher werden möglicherweise Warnmeldungen bezüglich nicht aufgelöster Paketabhängigkeiten oder Konflikte angezeigt, nachdem Sie Software-Pakete in diesem Dialogfeld ausgewählt oder die Auswahl von Paketen aufgehoben haben. Wenn Sie SUSE Linux Enterprise zum ersten Mal installieren oder Sie die Warnmeldungen nicht verstehen, lesen Sie [Abschnitt 7.3.1, „Installieren und Entfernen von Software“](#) (S. 152). Dort erhalten Sie detaillierte Informationen zur Funktionsweise des Paket-Managers.

Beenden der Software-Auswahl

Wenn die Software-Auswahl Ihren Vorstellungen entspricht und alle Paketabhängigkeiten oder Konflikte gelöst sind, klicken Sie zum Übernehmen der Änderungen und zum Beenden des Moduls auf *Übernehmen*. Während der Installation werden die Änderungen intern aufgezeichnet und später zu Beginn des Installationsvorgangs angewendet.

3.9.3 Sprache

Die Sprache wurde zu Beginn der Installation, wie in [Abschnitt 3.4, „Sprachauswahl“](#) (S. 42) beschrieben, ausgewählt. Diese Einstellungen können hier jedoch geändert werden und Sie können alle zusätzlichen Sprachen auswählen, die in Ihrem System installiert werden sollen. Wählen Sie im oberen Teil des Dialogfelds die Hauptsprache aus. Diese Sprache wird nach der Installation aktiviert. Passen Sie die Tastatur- und Zeitzoneneinstellungen an die ausgewählte Hauptsprache an, indem Sie gegebenenfalls die entsprechenden Optionen aktivieren. Optional können Sie mit *Details* die Sprache für den Benutzer `root` festlegen. Drei Optionen stehen zur Verfügung:

Nur `ctype`

Der Wert der Variablen `LC_CTYPE` in der Datei `/etc/sysconfig/language` wird für den Benutzer `root` angepasst. Hiermit wird die Lokalisierung für sprachspezifische Funktionsaufrufe festgelegt.

`ja`

Für den Benutzer `root` sind dieselben Spracheinstellungen festgelegt wie für den lokalen Benutzer.

`no`

Die Spracheinstellungen für den Benutzer `root` sind unabhängig von der Sprachauswahl. Die Festlegung aller `locale`-Variablen wird aufgehoben.

Treffen Sie die Einstellung für das Locale explizit mit *Detaillierte Locale-Einstellung*.

In der Liste im unteren Teil des Dialogfelds für die Sprachauswahl können Sie zusätzliche zu installierende Sprachen auswählen. YaST überprüft für alle in dieser Liste ausgewählten Sprachen, ob in der aktuellen Software-Auswahl sprachspezifische Pakete vorhanden sind. Ist dies der Fall, werden die entsprechenden Pakete installiert.

Klicken Sie zum Beenden der Konfiguration auf *Übernehmen*.

3.9.4 System

In diesem Dialogfeld werden alle Informationen angezeigt, die YaST von Ihrem Computer abrufen konnte. Wählen Sie einen beliebigen Eintrag in der Liste aus und klicken Sie auf *Details*, um detaillierte Informationen zum ausgewählten Eintrag anzuzeigen. In diesem Dialogfeld können Sie auch PCI-IDs zu den Treibern hinzufügen.

3.9.5 Tastaturbelegung

TIPP: IBM-System z: Konfiguration von Tastatur und Maus

Auf den IBM-System z-Plattformen erfolgt die Installation von einem entfernten Terminal. Der Host als solcher verfügt über keine lokal angeschlossene Tastatur oder Maus.

Wählen Sie die Tastaturbelegung in der Liste aus. Standardmäßig entspricht das Layout der ausgewählten Sprache. Testen Sie nach dem Ändern der Tastaturbelegung die besonderen Zeichen für die ausgewählte Tastaturbelegung, um sicherzustellen, dass Sie die richtige Auswahl getroffen haben. Klicken Sie zum Festlegen von speziellen Optionen für das Verhalten der Tastatur auf *Einstellungen für Experten*. Weitere Informationen hierzu finden Sie in [Abschnitt 7.4.8, „Tastaturbelegung“](#) (S. 169). Wenn Sie den Vorgang abgeschlossen haben, klicken Sie auf *Übernehmen*, um zum Dialogfeld mit den Installationseinstellungen zurückzukehren.

3.9.6 Booten

TIPP: IBM-System z: Konfiguration des Bootloaders

Das unten beschriebene Modul darf nicht zur Konfiguration des Bootloaders (zipl) auf IBM-System z-Plattformen benutzt werden.

Bei der Installation schlägt YaST eine Boot-Konfiguration für das System vor. Diese Einstellungen müssen in der Regel nicht geändert werden. Falls Sie jedoch ein benutzerdefiniertes Setup ausführen müssen, ändern Sie den Vorschlag für Ihr System.

Sie können den Boot-Mechanismus so konfigurieren, dass er eine spezielle Boot-Diskette verwendet. Obwohl dies den Nachteil hat, dass die Diskette sich beim Booten immer im Laufwerk befinden muss, wird ein vorhandener Boot-Mechanismus davon nicht berührt. In der Regel ist dies jedoch nicht erforderlich, da YaST den Bootloader so konfigurieren kann, dass auch andere vorhandene Betriebssysteme gebootet werden. In der Konfiguration besteht zudem die Möglichkeit, den Speicherort des Boot-Mechanismus auf die Festplatte zu ändern.

Wenn Sie die von YaST vorgeschlagene Boot-Konfiguration ändern möchten, wählen Sie *Systemstart*, um das Dialogfeld zu öffnen, in dem Sie die Details zum Boot-

Mechanismus ändern können. Weitere Informationen finden Sie in [Abschnitt 21.3](#), „[Konfigurieren des Bootloaders mit YaST](#)“ (S. 448).

3.9.7 Standard-Runlevel

SUSE Linux Enterprise kann mit verschiedenen Runlevels gebootet werden. Normalerweise ist an dieser Stelle keine Änderung erforderlich, wenn Sie jedoch einen anderen Runlevel festlegen müssen, tun Sie dies in diesem Dialogfeld. Informationen zur Runlevel-Konfiguration finden Sie in [Abschnitt 7.5.13](#), „[Systemdienste \(Runlevel\)](#)“ (S. 183).

3.9.8 Zeitzone

Ändern Sie in diesem Dialogfeld Ihre Region und die entsprechende Zeitzone, indem Sie sie in den Listen auswählen. Sie können zwischen *Lokale Zeit* und *UTC (GMT)* unter *Rechneruhr eingestellt auf* wählen. Die Auswahlmöglichkeit ist von den Einstellungen der Hardware-Uhr im BIOS Ihres Computers abhängig. Wenn Sie die Hardware-Uhr auf GMT (entspricht UTC) festlegen, schaltet SUSE Linux Enterprise automatisch von Standardzeit auf Sommerzeit und zurück um. Klicken Sie auf *Ändern*, um das aktuelle Datum und die Uhrzeit festzulegen. Wenn Sie den Vorgang abgeschlossen haben, klicken Sie auf *Übernehmen*, um zum Dialogfeld mit den Installationseinstellungen zurückzukehren.

3.9.9 Ausführen der Installation

Wenn Sie alle Installationseinstellungen vorgenommen haben, klicken Sie im Vorschlagsfenster zum Starten der Installation auf *Übernehmen*. Bestätigen Sie den Vorgang im daraufhin angezeigten Dialogfeld mit *Installieren*. Die Installation dauert ca. 15 bis 30 Minuten, abhängig von der Leistung des Systems und der ausgewählten Software. Wenn alle Pakete installiert wurden, bootet YaST mit dem neuen Linux-System. Anschließend können Sie die Hardware konfigurieren und Systemdienste einrichten.

3.9.10 IBM-System z: Ausführen von IPL für das installierte System

Auf den IBM-System z-Plattformen muss nach der Installation der ausgewählten Softwarepakete ein weiteres IPL ausgeführt werden. Die Prozedur variiert abhängig vom Typ der Installation:

LPAR-Installation

Wählen Sie in IBM-System z HMC *LADEN*, dann *Löschen* und geben Sie die Ladeadresse (die Geräteadresse des Root-Device) ein. Wenn Sie eine ZFCP-Festplatte als Boot-Device verwenden, wählen Sie *LOAD from SCSI* (Von SCSI LADEN) und geben Sie sowohl ZFCP WWPN als auch LUN des Boot-Device an. Beginnen Sie nun den Ladevorgang.

z/VM-Installation

Fahren Sie das installierte System mit dem Befehl `halt` herunter. Melden Sie sich als der VM-Gast unter dem Kontonamen `LINUX1` an und führen Sie dann IPL für das installierte System aus. Wenn Sie eine ZFCP-Festplatte als Boot-Device verwenden, geben Sie vor der Initialisierung des IPL sowohl ZFCP WWPN als auch LUN des Boot-Device an. Beachten Sie, dass die Parameterlänge auf acht Zeichen beschränkt ist. Längere Werte müssen durch Leerzeichen getrennt werden:

```
SET LOADDEV PORT 50050763 00C590A9 LUN 50010000 00000000
```

Starten Sie dann IPL:

```
IPL 151 CLEAR
```

3.9.11 IBM-System z: Herstellen der Verbindung mit dem installierten System

Bauen Sie nach dem Ausführen von IPL für das installierte System eine Verbindung mit dem System auf, um die Installation abzuschließen. Die erforderlichen Schritte variieren abhängig vom anfangs verwendeten Verbindungstyp.

Verbindung mithilfe von VNC

Eine Meldung im 3270-Terminal fordert Sie auf, eine Verbindung zum Linux-System mithilfe eines VNC-Clients herzustellen. Diese Meldung wird leicht übersehen, da sie mit Kernel-Meldungen gemischt ist und der Terminalprozess eventuell beendet wird, bevor Sie die Meldung bemerken. Wenn fünf Minuten lang nichts geschieht, initiieren Sie mithilfe eines VNC-Viewers eine Verbindung zum Linux-System.

Wenn die Verbindung mit einem Java-fähigen Browser erfolgt, geben Sie die vollständige URL, bestehend aus der IP-Adresse des installierten Systems und der Portnummer, wie folgt ein:

```
http://<IP of installed system>:5801/
```

Verbindung mithilfe von X

Stellen Sie beim Ausführen von IPL für das installierte System sicher, dass der für die erste Installationsphase verwendete X-Server immer noch verfügbar ist. YaST wird auf diesem X-Server geöffnet, um die Installation abzuschließen.

Verbindung mithilfe von SSH

WICHTIG: IBM-System z: Verbindung von einem Linux- oder UNIX-System

Starten Sie `ssh` in einem `xterm`. Andere Terminalemulatoren unterstützen die textbasierte Oberfläche von YaST nicht vollständig.

Eine Meldung im 3270-Terminal fordert Sie auf, eine Verbindung zum Linux-System mithilfe eines SSH-Clients herzustellen. Diese Meldung wird leicht übersehen, da sie mit Kernel-Meldungen gemischt ist und der Terminalprozess eventuell beendet wird, bevor Sie die Meldung bemerken.

Führen Sie nun die folgenden Schritte aus, um die Installation abzuschließen:

- 1 Verwenden Sie SSH, um sich als `root` beim Linux-System anzumelden. Wenn die Verbindung abgewiesen wird oder eine Zeitüberschreitung eintritt, warten Sie ein paar Minuten und versuchen Sie es dann erneut.

- 2 Führen Sie den Befehl `/usr/lib/YaST2/startup/YaST2.ssh` aus. In diesem Fall genügt `yast` nicht.

Anschließend startet YaST, um die Installation der verbleibenden Pakete abzuschließen und eine erste Systemkonfiguration auszuführen.

3.10 Konfiguration

Nach dem Abschluss des grundlegenden System-Setups und der Installation aller ausgewählten Software-Pakete geben Sie ein Passwort für das Konto des Systemadministrators (den Benutzer `root`) an. Anschließend können Sie den Internetzugang und die Netzwerkverbindung konfigurieren. Mit einer funktionierenden Internetverbindung können Sie das System im Rahmen der Installation aktualisieren. Zudem besteht die Möglichkeit, einen Authentifizierungsserver für die zentralisierte Benutzerverwaltung in einem lokalen Netzwerk zu konfigurieren. Zum Schluss konfigurieren Sie die an den Computer angeschlossenen Hardware-Geräte.

3.10.1 Hostname

Der Hostname ist der Name des Computers im Netzwerk. Der vollständig qualifizierte Domänenname, der hier erforderlich ist, umfasst den Namen der Domäne, zu der der Computer gehört. Jeder Server und Client im Netzwerk muss über einen eindeutigen Hostnamen verfügen.

Wenn der Rechner in ein lokales Netzwerk eingebunden ist, erhalten Sie den Hostnamen möglicherweise über DHCP. In diesem Fall sollte der Name nicht geändert werden. Um den Hostnamen über DHCP zu empfangen, wählen Sie *Hostnamen über DHCP ändern*.

3.10.2 root-Passwort

`root` ist der Name für den Superuser, den Administrator des Systems. Anders als normale Benutzer, die nicht über die Berechtigung zum Ausführen bestimmter Vorgänge im System verfügen, kann `root` alle beliebigen Vorgänge ausführen: Ändern der Systemkonfiguration, Installieren von Programmen und Konfigurieren neuer Hardware. Wenn Benutzer ihre Passwörter vergessen oder Probleme im System auftreten, kann

`root` ihnen helfen. Das `root`-Konto sollte nur für die Systemadministration, Wartung und Reparaturen verwendet werden. Die Anmeldung als `root` für tägliche Aufgaben ist relativ riskant: Ein einziger Fehler kann dazu führen, dass Systemdateien unwiederbringlich verloren gehen.

Zur Überprüfung muss das Passwort für `root` zweimal eingegeben werden. Das Passwort für `root` sollten Sie nicht vergessen. Wenn das Passwort einmal eingegeben wurde, kann es nicht mehr abgerufen werden.

3.10.3 Netzwerkkonfiguration

TIPP: IBM-System z: Netzwerkkonfiguration

Für die IBM-System z-Plattformen ist zum Zeitpunkt der Installation eine funktionierende Netzwerkverbindung erforderlich, um eine Verbindung zum Zielsystem, der Installationsquelle und dem YaST-Terminal herzustellen, das den Prozess steuert. Die Schritte zum Einrichten des Netzwerks werden im Kapitel zur Netzwerkkonfiguration im Handbuch *Architecture-Specific Information* (Kapitel *Vorbereitung der Installation* (↑Architekturspezifische Informationen)) behandelt. Die IBM-System z-Plattformen unterstützen nur die Typen von Netzwerkschnittstellen, die in diesem Kapitel erwähnt sind (OSA Token Ring, OSA Ethernet, OSA Gigabit Ethernet, OSA Express Fast Ethernet, Escon, IUCV, OSA Express High-Speed Token Ring). Das YaST-Dialogfeld zeigt einfach die Schnittstelle mit ihren zuvor konfigurierten Einstellungen an. Bestätigen Sie dieses Dialogfeld, um fortzufahren.

Sie können nun entscheiden, ob der NetworkManager oder die herkömmliche Methode für die Verwaltung all Ihrer Netzwerkgeräte verwendet werden soll. Der NetworkManager ist das neue Werkzeug, das automatischen Verbindungsaufbau mit minimalen Benutzereingriffen ermöglicht. Es eignet sich ideal für den mobilen Computereinsatz. Konfigurieren Sie auch die Netzwerkgeräte Ihres Systems und nehmen Sie Sicherheitseinstellungen vor, beispielsweise für eine Firewall oder einen Proxy. Informationen zum Konfigurieren der Netzwerk-Hardware in dieser Phase erhalten Sie in [Abschnitt 31.4, „Konfigurieren von Netzwerkverbindungen mit YaST“](#) (S. 623). Anderenfalls wählen Sie *Konfiguration überspringen* und klicken Sie auf *Weiter*. Netzwerk-Hardware kann auch nach dem Abschluss der Systeminstallation konfiguriert werden.

ANMERKUNG: Netzwerkgeräte und Update

Wenn Sie die Konfiguration der Netzwerkgeräte überspringen, ist Ihr System offline und kann keine Updates abrufen oder in die Installation aufnehmen.

Konfigurieren Sie wie bei der Gerätekonfiguration auch die Einstellungen im Zusammenhang mit den Netzwerk-Eingabehilfen:

Firewall-Konfiguration

Wenn Sie eine Verbindung zu einem Netzwerk herstellen, wird auf der konfigurierten Oberfläche automatisch eine Firewall gestartet. Der Konfigurationsvorschlag für die Firewall wird immer dann automatisch aktualisiert, wenn die Konfiguration der Oberflächen oder Dienste geändert wird. Um die automatischen Einstellungen an Ihre eigenen Voreinstellungen anzupassen, klicken Sie auf *Ändern* → *Firewall*. Legen Sie im anschließend geöffneten Dialogfeld fest, ob die Firewall gestartet werden soll. Wenn Sie die Firewall nicht starten möchten, wählen Sie die entsprechende Option aus und schließen Sie das Dialogfeld. Klicken Sie zum Starten und Konfigurieren der Firewall auf *Weiter*, um eine Reihe von Dialogfeldern anzuzeigen, die den in [Abschnitt 44.4.1](#), „Konfigurieren der Firewall mit YaST“ (S. 906) beschriebenen Dialogfeldern ähneln.

Entfernte Administration mit VNC

Um Ihren Rechner entfernt mit VNC zu verwalten, klicken Sie auf *Ändern* → *VNC Remote Administration (Entfernte Administration mit VNC)*, aktivieren Sie die entfernte Administration und öffnen Sie den Port in der Firewall. Wenn Sie über mehrere Netzwerkgeräte verfügen und festlegen möchten, auf welchem der Port geöffnet werden soll, klicken Sie auf *Firewall-Details* und wählen Sie das gewünschte Netzwerkgerät aus. Sie können für die entfernte Netzwerkadministration auch SSH, eine sicherere Option, verwenden.

Proxy

Wenn in Ihrem Netzwerk ein Proxy-Server den Netzwerkzugriff steuert, geben Sie den Servernamen und alle erforderlichen Informationen ein, um den Zugriff auf das Internet zu ermöglichen.

Internetverbindungstest

Wenn Sie eine Internetverbindung konfiguriert haben, können Sie sie jetzt testen. Zu diesem Zweck stellt YaST eine Verbindung zum SUSE Linux Enterprise-Server her

und überprüft, ob Produkt-Updates für Ihre SUSE Linux Enterprise-Version verfügbar sind. Falls Updates vorhanden sind, können sie in die Installation integriert werden. Darüber hinaus werden die neuesten Versionshinweise heruntergeladen. Sie können sie nach Abschluss der Installation lesen.

Wählen Sie zum Start des Tests *Ja, Internetverbindung testen* und klicken Sie auf *Weiter*. Im nächsten Dialogfeld sehen Sie den Testverlauf und das Ergebnis des Tests. Wenn der Test nicht erfolgreich ist, klicken Sie auf *Zurück*, um in das vorherige Dialogfeld zurückzukehren, und korrigieren Sie die Konfiguration oder überspringen Sie den Test. Falls Sie weitere Informationen zu dem Testvorgang benötigen, klicken Sie auf *Protokolle anzeigen*.

Wenn Sie die Verbindung jetzt nicht überprüfen möchten, wählen Sie *Nein, diesen Test überspringen* und anschließend *Weiter*. Hiermit wird auch das Herunterladen von Produkt-Updates und Versionshinweisen übersprungen.

Wenn Ihr System mehrere Netzwerkschnittstellen hat, stellen Sie sicher, dass die korrekte Karte für die Verbindung zum Internet verwendet wird. Klicken Sie dazu auf *Gerät ändern*.

3.10.4 Kundenzentrum

Damit Sie technischen Support und Produkt-Updates erhalten, registrieren und aktivieren Sie zuerst Ihr Produkt. *Konfiguration für Novell-Kundenzentrum* unterstützt Sie dabei. Wenn Sie offline arbeiten oder diesen Schritt überspringen möchten, wählen Sie *Später konfigurieren*.

Wählen Sie unter *Für besseren Service aufnehmen*, ob Sie einen Teil der erforderlichen Informationen von Ihrem System beziehen möchten. Dies vereinfacht die Registrierung. Wenn Sie sehen möchten, was zur Registrierung Ihres Systems nötig ist oder mit Ihren Daten geschieht, verwenden Sie *Details*.

TIPP: Technischer Support

Weitere Informationen zum technischen Support finden Sie unter <http://www.novell.com/support/products/linuxenterpriseserver/>.

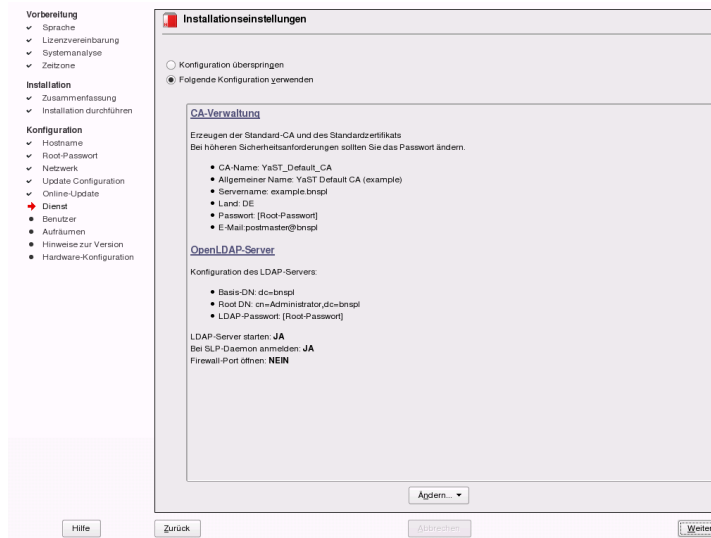
3.10.5 Online-Update

Wenn YaST eine Verbindung zu den SUSE Linux Enterprise-Servern herstellen konnte, wählen Sie aus, ob ein YaST-Online-Update ausgeführt werden soll. Wenn Pakete mit Patches auf den Servern vorhanden sind, laden Sie sie jetzt herunter, um bekannte Fehler oder Sicherheitslücken zu beheben.

3.10.6 Dienst

Nach dem Test der Internetverbindung und dem Herunterladen der ersten Updates wird ein Dialogfeld geöffnet, in dem Sie zwei wichtige Netzwerkdienste aktivieren und konfigurieren können. Siehe [Abbildung 3.8](#), „Vorgeschlagene Konfiguration für Netzwerkdienste“ (S. 66).

Abbildung 3.8 Vorgeschlagene Konfiguration für Netzwerkdienste



Zertifikatverwaltung

Der Zweck eines Zertifikats (von einer Zertifizierungsstelle) ist es, eine verbürgte Beziehung zwischen allen miteinander kommunizierenden Netzwerkdiensten zu garantieren. Wenn Sie sich dafür entscheiden, dass Sie keine Zertifizierungsstelle einrichten möchten, sichern Sie die Server-Kommunikation mit SSL und TLS,

allerdings separat für jeden einzelnen Dienst. Standardmäßig wird während der Installation ein Zertifikat erstellt und aktiviert. Einzelheiten über das Erstellen eines Zertifikats mit YaST sowie einige Hintergrundinformationen erhalten Sie unter [Kapitel 43, *Verwalten der X.509-Zertifizierung*](#) (S. 881).

LDAP-Server

Sie können einen LDAP-Dienst auf Ihrem Host ausführen, damit eine zentrale Einrichtung zur Verwaltung von Konfigurationsdateien zur Verfügung steht. Typischerweise verwaltet ein LDAP-Server Daten von Benutzerkonten, aber in SUSE Linux Enterprise Server lässt er sich auch für Mail-, DHCP- und DNS-Daten verwenden. Standardmäßig wird während der Installation ein LDAP-Server eingerichtet. Wenn Sie sich gegen die Verwendung eines LDAP-Servers entscheiden, funktioniert das YaST-Mailservermodul nicht, da es von LDAP-Funktionalität abhängt. Sie können dennoch auf Ihrem System mithilfe des Moduls *Mail Transfer Agent* einen Mailserver einrichten. Detaillierte Informationen zu LDAP und der Konfiguration mit YaST finden Sie in [Kapitel 37, *LDAP – Ein Verzeichnisdienst*](#) (S. 735).

Wie die allgemeine Netzwerkkonfiguration können Sie vorerst auch diese Konfiguration überspringen. Nach Abschluss der Installation können Sie mithilfe von YaST immer noch dieselben Dienste konfigurieren und starten.

3.10.7 Benutzer

Dieser Schritt besteht aus zwei Teilen. Im ersten Teil wählen Sie die Methode für die Benutzerauthentifizierung. Der zweite Teil hängt von der gewählten Authentifizierungsmethode ab.

Benutzerauthentifizierung

Wenn der Netzwerkzugang in den vorherigen Schritten erfolgreich konfiguriert wurde, stehen Ihnen jetzt vier Möglichkeiten zum Verwalten von Benutzerkonten in Ihrem System zur Verfügung.

Lokal (/etc/passwd)

Die Benutzer werden lokal auf dem installierten Host verwaltet. Dies ist eine geeignete Option für eigenständige Arbeitsstationen. Die Benutzerdaten werden über die lokale Datei `/etc/passwd` verwaltet. Alle Benutzer, die in dieser Datei

eingetragen sind, können sich beim System anmelden, selbst wenn kein Netzwerk verfügbar ist.

LDAP

Die Benutzer werden zentral auf einem LDAP-Server für alle Systeme im Netzwerk verwaltet.

NIS

Die Benutzer werden zentral auf einem NIS-Server für alle Systeme im Netzwerk verwaltet.

Windows-Domäne

Die SMB-Authentifizierung wird häufig in heterogenen Linux- und Windows-Netzwerken verwendet.

ANMERKUNG: Inhalt des Authentifizierungsmenüs

Wenn Sie die benutzerdefinierte Paketauswahl verwenden und eine oder mehrere Authentifizierungsmethoden im Menü fehlen, haben Sie wahrscheinlich nicht die dafür erforderlichen Pakete ausgewählt.

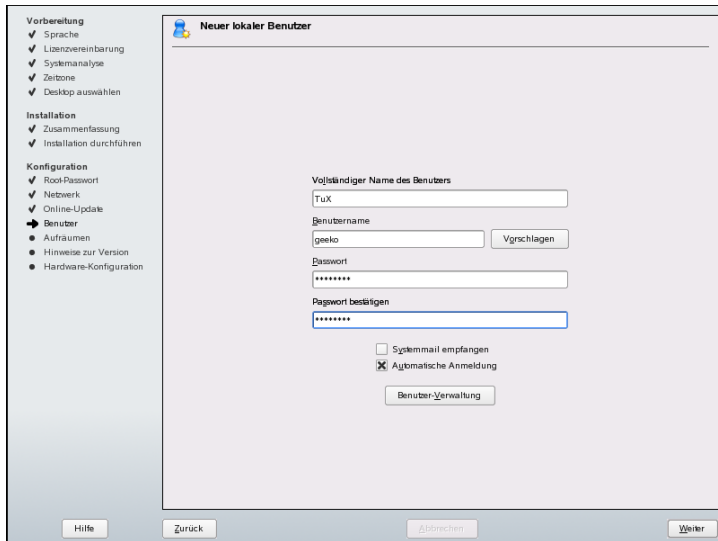
Wenn alle Anforderungen erfüllt sind, wird in YaST ein Dialogfeld zur Auswahl der Benutzerverwaltungsmethode geöffnet. Wenn Sie nicht über die erforderliche Netzwerkverbindung verfügen, erstellen Sie lokale Benutzerkonten.

Erstellen lokaler Benutzerkonten

Linux ist ein Betriebssystem, in dem mehrere Benutzer gleichzeitig im selben System arbeiten können. Jeder Benutzer benötigt ein Benutzerkonto für die Anmeldung beim System. Die Benutzerkonten tragen wesentlich zur Sicherheit des Systems bei. Normale Benutzer können beispielsweise keine Dateien ändern oder löschen, die für die ordnungsgemäße Funktionsweise des Systems erforderlich sind. Gleichzeitig können die persönlichen Daten eines bestimmten Benutzers von anderen Benutzern nicht geändert oder angezeigt werden. Benutzer können ihre eigene Arbeitsumgebung einrichten und bekommen sie unverändert nach jedem erneuten Anmeldevorgang angezeigt.

Wenn Sie sich gegen einen Authentifizierungsserver für Benutzerauthentifizierungen entscheiden, erstellen Sie lokale Benutzer. Alle Daten, die sich auf Benutzerkonten beziehen (Name, Anmeldedaten, Passwort usw.) werden auf dem installierten System gespeichert und verwaltet.

Abbildung 3.9 *Eingabe von Benutzername und Passwort*



Ein lokales Benutzerkonto kann in dem in [Abbildung 3.9](#), „Eingabe von Benutzername und Passwort“ (S. 69) dargestellten Dialogfeld erstellt werden. Geben Sie nach der Eingabe des Vornamens und des Nachnamens einen Benutzernamen ein. Mit *Vorschlagen* können Sie vom System automatisch einen Benutzernamen erstellen lassen.

Geben Sie schließlich das Passwort für den Benutzer ein. Geben Sie es zur Bestätigung erneut ein (um sicherzustellen, dass sie nicht versehentlich etwas anderes eingegeben haben).

Um ausreichend Sicherheit zu gewährleisten, sollten Passwörter zwischen fünf und acht Zeichen lang sein. Die maximal zulässige Länge für ein Passwort ist 128 Zeichen. Wenn jedoch keine speziellen Sicherheitsmodule geladen werden, werden die ersten acht Zeichen für die Erkennung des Passworts verwendet. Bei Passwörtern muss die Groß- und Kleinschreibung berücksichtigt werden. Sonderzeichen, wie Umlaute, sind nicht zulässig. Andere Sonderzeichen (7-Bit ASCII) und die Ziffern 0 bis 9 sind zulässig.

Für lokale Benutzer stehen zwei zusätzliche Optionen zur Verfügung:

Empfangen von Systemmeldungen per E-Mail

Wenn Sie dieses Kontrollkästchen aktivieren, werden dem Benutzer die vom Systemdienst erstellten Meldungen zugesendet. Diese Meldungen werden in der Regel nur an den Systemadministrator `root` gesendet. Die Option ist sinnvoll für das am häufigsten verwendete Konto, da die Anmeldung als `root` nur in speziellen Fällen empfohlen wird.

Automatische Anmeldung

Diese Option ist nur verfügbar, wenn KDE als Standard-Desktop verwendet wird. Hiermit wird der aktuelle Benutzer beim Starten automatisch beim System angemeldet. Dies ist besonders dann sinnvoll, wenn der Computer nur von einem Benutzer verwendet wird. Damit die automatische Anmeldung funktioniert, muss die Option explizit aktiviert werden.

WARNUNG: Automatische Anmeldung

Wenn die automatische Anmeldung aktiviert ist, wird nach dem Booten des Systems direkt ohne Authentifizierung der Desktop angezeigt. Wenn auf Ihrem System vertrauliche Daten gespeichert sind, sollten Sie diese Option nicht aktivieren, sofern auch andere Benutzer auf den Computer zugreifen können.

Klicken Sie zum Erstellen mehrerer Benutzer auf *Benutzerverwaltung*. Weitere Informationen zur Benutzerverwaltung finden Sie in [Abschnitt 7.9.1, „Benutzerverwaltung“](#) (S. 194).

Konfigurieren des Host als LDAP-Client

Zum Implementieren der Benutzerverwaltung über LDAP konfigurieren Sie im nächsten Schritt einen LDAP-Client. In diesem Abschnitt wird nur die Konfiguration auf Client-Seite beschrieben. Informationen zur Konfiguration eines LDAP-Servers erhalten Sie in [Kapitel 37, LDAP – Ein Verzeichnisdienst](#) (S. 735).

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. Geben Sie die IP-Adresse des LDAP-Servers ein, der verwendet werden soll, sowie den "LDAP Base DN", 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

angegebenen Serveradresse vorhanden sind. Wählen Sie den geeigneten "Base DN" aus den Suchergebnissen, die YaST liefert. Wenn eine durch TLS oder SSL geschützte Kommunikation mit dem Server erforderlich ist, wählen Sie *LDAP TLS/SSL*. Falls auf dem LDAP-Server noch LDAPv2 verwendet wird, muss die Verwendung dieser Protokollversion durch Auswahl von *LDAP Version 2* ausdrücklich aktiviert werden. Wählen Sie *Automounter starten* aus, um die entfernten Verzeichnisse, wie beispielsweise ein entfernt verwaltetes Home-Verzeichnis, auf dem Client einzuhängen. Klicken Sie zum Anwenden der Einstellungen auf *Beenden*. Die LDAP-Client-Konfiguration wird ausführlich in [Abschnitt 37.6](#), „[Konfigurieren eines LDAP-Clients mit YaST](#)“ (S. 754) beschrieben.

Konfigurieren des Host als NIS-Client

Zum Implementieren der Benutzerverwaltung über NIS konfigurieren Sie im nächsten Schritt einen NIS-Client. In diesem Abschnitt wird nur die Konfiguration auf Client-Seite beschrieben. Informationen zur Konfiguration eines NIS-Servers mit YaST erhalten Sie in [Kapitel 36](#), [Arbeiten mit NIS](#) (S. 725).

Im NIS-Client-Dialogfeld wählen Sie zunächst aus, ob der Host über eine statische IP-Adresse verfügt oder eine Adresse über DHCP erhält. Wenn Sie DHCP auswählen, können Sie keine NIS-Domäne oder NIS-Serveradresse angeben, da diese vom DHCP-Server bereitgestellt werden. Informationen zu DHCP erhalten Sie in [Kapitel 35](#), [DHCP](#) (S. 707). Falls eine statische IP-Adresse verwendet wird, geben Sie die NIS-Domäne und den NIS-Server manuell an.

Aktivieren Sie die entsprechende Option, um nach NIS-Servern zu suchen, die im Netzwerk Versende-Vorgänge ausführen. Sie können zudem mehrere NIS-Domänen angeben und eine Standarddomäne festlegen. Wählen Sie für jede Domäne *Bearbeiten* aus, um mehrere Serveradressen anzugeben oder die Versende-Funktion für einzelne Domänen festzulegen.

Verwenden Sie in den Experteneinstellungen die Option *Entfernten Hosts antworten*, um anderen Netzwerk-Hosts zu gestatten, abzufragen, welchen Server Ihr Client verwendet. Wenn Sie *Fehlerhafter Server* aktivieren, werden auch Antworten von Servern an nicht berechtigten Ports akzeptiert. Weitere Informationen finden Sie auf der Manualpage zu `ypbind`.

Konfigurieren des Host als Mitglied der Windows-Domäne

Zum Implementieren der Benutzerverwaltung mit einem Samba- oder Windows-Server konfigurieren Sie im nächsten Schritt einen Samba-Client. In diesem Abschnitt wird nur die Konfiguration auf Client-Seite beschrieben. Die Samba-Konfiguration wird ausführlich in [Kapitel 38, Samba](#) (S. 767) beschrieben.

Geben Sie im Dialogfeld *Windows-Domänenmitgliedschaft* die gewünschte NT- oder Active Directory-Domäne oder Samba-Arbeitsgruppe ein oder klicken Sie auf *Durchsuchen*, um aus einer Liste der verfügbaren Domänen zu wählen. Wählen Sie *Home-Verzeichnis bei Anmeldung erstellen*, wenn Sie Home-Verzeichnisse für jeden Benutzer anlegen möchten, der sich von Ihrem lokalen Computer bei der Domäne anmeldet. Klicken Sie auf *Beenden*, um die Einstellungen zu übernehmen und die erforderlichen Daten anzugeben.

3.10.8 Bereinigung

Dieser Schritt erfordert keine Eingriffe des Benutzers. Das Installationsprogramm startet das SuSEconfig-Skript, um die Systemkonfiguration zu schreiben. Abhängig von der CPU und dem verfügbaren Speicher kann dieser Vorgang einige Zeit in Anspruch nehmen.

3.10.9 Versionshinweise

Wenn Sie die Einrichtung der Benutzerauthentifizierung abgeschlossen haben, werden in YaST die Versionshinweise angezeigt. Es empfiehlt sich, sie zu lesen, da sie wichtige aktuelle Informationen enthalten, die bei Drucklegung der Handbücher noch nicht zur Verfügung standen. Wenn Sie Aktualisierungspakete installiert haben, lesen Sie die neueste Version der Versionshinweise, die Sie von den SUSE Linux Enterprise-Servern abgerufen haben.

3.10.10 Hardware-Konfiguration

Am Ende der Installation wird in YaST ein Dialogfeld für die Konfiguration der Grafikkarte und anderer mit dem System verbundenen Hardware-Komponenten geöffnet.

Klicken Sie auf die einzelnen Komponenten, um mit der Hardware-Konfiguration zu starten. In der Regel erkennt und konfiguriert YaST die Geräte automatisch.

TIPP: IBM-System z: Hardware-Konfiguration

Auf IBM-System z gibt es keine Anzeige, die von XFree unterstützt wird. Daher finden Sie auf diesen Systemen den Eintrag *Grafikkarten* nicht.

Sie können die peripheren Geräte überspringen und zu einem späteren Zeitpunkt konfigurieren. Um die Konfiguration auszulassen, wählen Sie *Konfiguration überspringen* und klicken Sie auf *Weiter*.

Die Grafikkarte sollte jedoch sofort konfiguriert werden. Die automatisch konfigurierten Anzeige-Einstellungen von YaST können in der Regel übernommen werden. Viele Benutzer möchten jedoch Auflösung, Farbtiefe und andere Grafikfunktionen selbst anpassen. Wählen Sie zum Ändern dieser Einstellungen den jeweiligen Eintrag aus und legen Sie die Werte nach Wunsch fest. Um Ihre neue Konfiguration zu testen, klicken Sie auf *Konfiguration testen*.

3.10.11 Abschließen der Installation

Nach einer erfolgreichen Installation zeigt YaST das Dialogfeld *Installation abgeschlossen*. Wählen Sie in diesem Dialogfeld, ob Ihr neu installiertes System für AutoYaST geklont werden soll. Um Ihr System zu klonen, wählen Sie *Dieses System für Autoyast klonen*. Das Profil des aktuellen Systems wird in `/root/autoyast.xml` gespeichert.

AutoYaST ist ein System zur automatischen Installation von einem oder mehreren SUSE Linux Enterprise-Systemen ohne Eingriffe des Benutzers. AutoYaST-Installationen werden mithilfe einer Steuerdatei mit Installations- und Konfigurationsdaten ausgeführt. Detaillierte Informationen finden Sie in [Kapitel 5, Automatisierte Installation](#) (S. 115).

Beenden Sie die Installation von SUSE Linux Enterprise im abschließenden Dialogfeld mit *Beenden*.

3.11 Grafische Anmeldung

TIPP: IBM-System z: Keine grafische Anmeldung

Die grafische Anmeldung steht auf IBM-System z-Plattformen nicht zur Verfügung.

SUSE Linux Enterprise ist nun installiert. Sofern Sie nicht die automatische Anmeldefunktion aktiviert haben, sollte die grafische Anmeldung an Ihrem Bildschirm angezeigt werden, in der Sie Anmeldenamen und Passwörter für die Anmeldung beim System eingeben können. Wenn die automatische Anmeldung aktiviert ist, startet der Desktop automatisch.

Installation mit entferntem Zugriff

Es gibt mehrere Möglichkeiten, SUSE® Linux Enterprise zu installieren. Abgesehen von der normalen Installation von CD oder DVD, die in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben wird, können Sie aus mehreren netzwerkbasierten Ansätzen auswählen oder eine vollautomatische Installation von SUSE Linux Enterprise ausführen.

Die einzelnen Methoden werden mithilfe zweier kurzer Checklisten erläutert: In der einen Liste sind die Voraussetzungen für die jeweilige Methode aufgeführt und in der anderen Liste wird das grundlegende Verfahren beschrieben. Anschließend werden alle in diesen Installationsszenarien verwendeten Techniken ausführlicher erläutert.

ANMERKUNG

In den folgenden Abschnitten wird das System, auf dem die neue SUSE Linux Enterprise-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 Netzwerkservers, die die Installationsdaten im Netzwerk verteilen.

4.1 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 Grafikhardware, wie in [Abschnitt 27.1, „X11-Konfiguration mit SaX2“](#) (S. 535) beschrieben, zu konfigurieren.

4.1.1 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 3, *Installation mit YaST*](#) (S. 37)).

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

- Quelle der Installation mit entferntem Zugriff: NFS, HTTP, FTP oder SMB mit funktionierender Netzwerkverbindung

- 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 wie in [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zu SMB-Installationsquellen finden Sie in [Abschnitt 4.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 94).
- 2** Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des SUSE Linux Enterprise-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 4.4, „Booten des Zielsystems für die Installation“](#) (S. 106) 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 4.5.1, „VNC-Installation“](#) (S. 111) beschrieben eine Verbindung zum Zielsystem her.
- 5** Führen Sie die Installation wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.

6 Schließen Sie die Installation ab.

4.1.2 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:

- Quelle der Installation mit entferntem Zugriff: NFS, HTTP, FTP oder SMB mit funktionierender Netzwerkverbindung
- 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 wie in [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zu SMB-Installationsquellen finden Sie in [Abschnitt 4.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 94).
- 2 Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des SUSE Linux Enterprise-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 4.4](#), „[Booten des Zielsystems für die Installation](#)“ (S. 106) 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 4.5.1](#), „[VNC-Installation](#)“ (S. 111) beschrieben eine Verbindung zum Zielsystem her.
- 5 Führen Sie die Installation wie in [Kapitel 3](#), [Installation mit YaST](#) (S. 37) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6 Schließen Sie die Installation ab.

4.1.3 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:

- Quelle der Installation mit entferntem Zugriff: NFS, HTTP, FTP oder SMB mit funktionierender Netzwerkverbindung
- 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 wie in [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver aus oder konfigurieren Sie eine SMB-Installationsquelle wie in [Abschnitt 4.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 94) 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 4.3.2, „Einrichten eines TFTP-Servers“](#) (S. 97) 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 4.3.1, „Einrichten eines DHCP-Servers“](#) (S. 95) beschrieben.
- 4** Bereiten Sie das Zielsystem für PXE-Boot vor. Dies wird ausführlich in [Abschnitt 4.3.5, „Vorbereiten des Zielsystems für PXE-Boot“](#) (S. 105) beschrieben.
- 5** Initiieren Sie den Bootvorgang des Zielsystems mithilfe von Wake-on-LAN. Die Konfiguration eines solchen Servers wird in [Abschnitt 4.3.7, „Wake-on-LAN“](#) (S. 105) beschrieben.
- 6** Öffnen Sie auf der steuernden Arbeitsstation eine VNC-Viewer-Anwendung oder einen Webbrowser und stellen Sie wie in [Abschnitt 4.5.1, „VNC-Installation“](#) (S. 111) beschrieben eine Verbindung zum Zielsystem her.
- 7** Führen Sie die Installation wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.

8 Schließen Sie die Installation ab.

4.1.4 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 3, *Installation mit YaST*](#) (S. 37)).

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

- Quelle der Installation mit entferntem Zugriff: NFS, HTTP, FTP oder SMB mit funktionierender Netzwerkverbindung
- 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 wie in [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zu

SMB-Installationsquellen finden Sie in [Abschnitt 4.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 94).

- 2 Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des SUSE Linux Enterprise-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 4.4.3, „Benutzerdefinierte Boot-Optionen“](#) (S. 108) 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. 114) beschrieben eine Verbindung zum Zielsystem her.
- 5 Führen Sie die Installation wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 6 Schließen Sie die Installation ab.

4.1.5 Einfache entfernte Installation 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:

- Quelle der Installation mit entferntem Zugriff: NFS, HTTP, FTP oder SMB mit funktionierender Netzwerkverbindung
- 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 wie in [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zu SMB-Installationsquellen finden Sie in [Abschnitt 4.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 94).
- 2** Booten Sie das Zielsystem mithilfe der ersten CD oder DVD des SUSE Linux Enterprise-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 4.4.3, „Benutzerdefinierte Boot-Optionen“](#) (S. 108).

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. 114) beschrieben eine Verbindung zum Zielsystem her.
- 5** Führen Sie die Installation wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.

6 Schließen Sie die Installation ab.

4.1.6 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:

- Quelle der Installation mit entferntem Zugriff: NFS, HTTP, FTP oder SMB mit funktionierender Netzwerkverbindung
- 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 wie in [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85) beschrieben ein. Wählen Sie einen NFS-, HTTP- oder FTP-Netzwerkserver. Weitere Informationen zur Konfiguration einer SMB-Installationsquelle finden Sie in [Abschnitt 4.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 94).
- 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 4.3.2, „Einrichten eines TFTP-Servers“](#) (S. 97) 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 4.3.1, „Einrichten eines DHCP-Servers“](#) (S. 95) beschrieben.
- 4 Bereiten Sie das Zielsystem für PXE-Boot vor. Dies wird ausführlich in [Abschnitt 4.3.5, „Vorbereiten des Zielsystems für PXE-Boot“](#) (S. 105) beschrieben.
- 5 Initiieren Sie den Bootvorgang des Zielsystems mithilfe von Wake-on-LAN. Die Konfiguration eines solchen Servers wird in [Abschnitt 4.3.7, „Wake-on-LAN“](#) (S. 105) beschrieben.
- 6 Starten Sie auf der steuernden Arbeitsstation einen SSH-Client und stellen Sie wie in [Abschnitt 4.5.2, „SSH-Installation“](#) (S. 114) beschrieben eine Verbindung zum Zielsystem her.
- 7 Führen Sie die Installation wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben aus. Stellen Sie die Verbindung zum Zielsystem wieder her, nachdem dieses neu gebootet wurde.
- 8 Schließen Sie die Installation ab.

4.2 Einrichten des Servers, auf dem sich die Installationsquellen befinden

Je nachdem, welches Betriebssystem auf dem Computer ausgeführt wird, der als Netzwerkinstallationsquelle für SUSE Linux Enterprise verwendet werden soll, stehen für die Serverkonfiguration mehrere Möglichkeiten zur Verfügung. Am einfachsten lässt sich ein Installationsserver mit YaST auf SUSE Linux Enterprise Server 9 oder 10 oder SUSE Linux 9.3 und höher einrichten. Bei anderen Versionen von SUSE Linux Enterprise Server oder SUSE Linux müssen Sie die Installationsquelle manuell einrichten.

TIPP

Für die Linux-Implementierung kann auch ein Microsoft Windows-Computer als Installationsserver verwendet werden. Weitere Einzelheiten finden Sie unter [Abschnitt 4.2.5, „Verwalten einer SMB-Installationsquelle“](#) (S. 94).

4.2.1 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 Starten Sie *YaST* → *Verschiedenes* → *Installationsserver*.
- 3 Wählen Sie *Serverkonfiguration*.
- 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 39, Verteilte Nutzung von Dateisystemen mit NFS](#) (S. 785).

- 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 für die vollständige Produktinstallation mehrere Zusatz-CDs oder Service-Pack-CDs erforderlich sein. Wenn Sie die Option *Nach zusätzlichen CDs verlangen* aktivieren, werden Sie von YaST automatisch daran erinnert, diese Medien zur Verfügung zu stellen. 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 4.4, „Booten des Zielsystems für die Installation“](#) (S. 106).

- 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 *Beenden* 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 in der Übersicht die Option *Ändern*, um die Liste der verfügbaren Installationsquellen zu öffnen. Wählen Sie den zu entfernenden Eintrag und wählen Sie anschließend die Option *Löschen*. Dieses Löschverfahren bezieht sich nur auf das Deaktivieren des Serverdienstes. Die Installationsdaten selbst verbleiben im ausgewählten Verzeichnis. Sie können sie jedoch manuell entfernen.

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 *Konfigurieren*, um die Installationsquelle zu konfigurieren.

4.2.2 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`-Benutzer an.
- 2 Erstellen Sie ein Verzeichnis, in dem die Installationsdaten gespeichert werden sollen, und wechseln Sie in dieses Verzeichnis. Beispiel:

```
mkdir install/produkt/produktversion  
cd install/produkt/produktversion
```

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:

- a** Kopieren Sie den gesamten Inhalt der Installations-CD in das Server-Installationsverzeichnis:

```
cp -a /media/pfad_zu_ihrem_CD-ROM-laufwerk.
```

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.

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

```
mv pfad_zu_ihrem_CD-ROM-laufwerk CDx
```

Ersetzen Sie *x* durch die Nummer der CD.

Bei SUSE Linux und SUSE Linux Enterprise Server können Sie die Installationsquellen über NFS mit YaST exportieren. Führen Sie dazu die folgenden Schritte aus:

- 1** Melden Sie sich als *root*-Benutzer an.
- 2** Starten Sie *YaST* → *Netzwerkdienste* → *NFS-Server*.
- 3** Wählen Sie *NFS-Server starten* und *Firewall-Port öffnen* und klicken Sie auf *Weiter*.
- 4** Wählen Sie *Verzeichnis hinzufügen* und geben Sie den Pfad des Verzeichnisses ein, in dem sich die Installationsdaten befinden. In diesem Fall lautet es */Produktversion*.
- 5** Wählen Sie *Host hinzufügen* und geben Sie die Hostnamen der Computer ein, auf die die Installationsdaten exportiert werden sollen. An Stelle der Hostnamen können Sie hier auch Platzhalter, Netzwerkadressbereiche oder einfach den Domänennamen Ihres Netzwerks eingeben. Geben Sie die gewünschten Exportoptionen an oder übernehmen Sie die Vorgabe, die für die meisten Konfigurationen ausreichend ist. Weitere Informationen dazu, welche Syntax beim Exportieren von NFS-Freigaben verwendet wird, finden Sie auf der Manualpage zu *exports*.

- 6 Klicken Sie auf *Beenden*. Der NFS-Server, auf dem sich die SUSE Linux Enterprise-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`-Benutzer an.
- 2 Öffnen Sie die Datei `/etc/exports` und geben Sie die folgende Zeile ein:

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

Dadurch wird das Verzeichnis `/Produktversion` auf alle Hosts exportiert, die Teil dieses Netzwerks sind oder eine Verbindung zu diesem Server herstellen können. Um den Zugriff auf diesen Server zu beschränken, geben Sie an Stelle des allgemeinen Platzhalters `*` Netzmasken oder 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`-Benutzer 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/pfad_instquelle/CD1,en,65535
description=NFS Installation Source
```

Ersetzen Sie *Pfad_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 32, SLP-Dienste im Netzwerk](#) (S. 669).

4.2.3 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 4.2.2, „Manuelles Einrichten einer NFS-Installationsquelle“](#) (S. 88) beschrieben ein Verzeichnis für die Installationsquellen.
- 2 Konfigurieren Sie den FTP-Server für die Verteilung des Inhalts des Installationsverzeichnisses:
 - a Melden Sie sich als `root` an und installieren Sie mithilfe des YaST-Paket-Managers das Paket `pure-ftpd` (ein einfacher FTP-Server).

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

```
cd/srv/ftp
```

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

```
mkdir instquelle
```

Ersetzen Sie *instquelle* durch den Produktnamen.

- d Kopieren Sie den Inhalt der Installations-CDs in das root-Verzeichnis des FTP-Servers (ähnlich wie in [Abschnitt 4.2.2](#), „[Manuelles Einrichten einer NFS-Installationsquelle](#)“ (S. 88), [Schritt 3](#) (S. 88) beschrieben).

Alternativ dazu können Sie den Inhalt des bereits vorhandenen Installations-Repositorys auch in der `change-root`-Umgebung des FTP-Servers einhängen:

```
mount --bind pfad_zur_instquelle /srv/ftp/instquelle
```

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.

- e Starten Sie `pure-ftpd` mit `pure-ftpd &`.

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

- a 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/instquelle/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 `service:` sollte als eine fortlaufende Zeile eingegeben werden.

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

4.2.4 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 4.2.2, „Manuelles Einrichten einer NFS-Installationsquelle“](#) (S. 88) beschrieben ein Verzeichnis für die Installationsquellen.

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

a Installieren Sie den Webserver Apache, wie in [Abschnitt 4.1.2, „Installation“](#) (S. 812) beschrieben.

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

```
mkdir instquelle
```

Ersetzen Sie `instquelle` durch den Produktnamen.

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

```
ln -s /pfad_instquelle /srv/www/htdocs/instquelle
```

d 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
```

durch

```
Options Indexes FollowSymLinks
```

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

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

a 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/instquelle/CD1/,en,65535
description=HTTP Installation Source
```

Ersetzen Sie *instquelle* durch den eigentlichen Pfad der Installationsquelle auf dem Server. Die Zeile *service*: sollte als eine fortlaufende Zeile eingegeben werden.

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

4.2.5 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 SUSE Linux Enterprise-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** Kopieren Sie den Inhalt aller SUSE Linux Enterprise-CDs oder -DVDs in das Verzeichnis `INSTALL/Produkt`.

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-Computers, den Freigabenamen (`INSTALL` in diesem Beispiel), den Benutzernamen und das Passwort ein.

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

4.3 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.

4.3.1 Einrichten eines DHCP-Servers

Es gibt zwei Möglichkeiten zum Einrichten eines DHCP-Servers. Für SUSE Linux Enterprise Server 9 und höher bietet YaST eine grafische Schnittstelle für den Prozess. Die Benutzer anderer SUSE Linux-basierter Produkte und Benutzer ohne SUSE Linux sollten die Konfigurationsdateien manuell bearbeiten oder das Frontend ihrer Betriebssysteme verwenden.

Einrichten eines DHCP-Servers mit YaST

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

- 1 Melden Sie sich als `root` auf dem Computer an, der den DHCP-Server bereitstellt.
- 2 Starten Sie *YaST* → *Netzwerkdienste* → *DHCP-Server*.

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

Wenn Sie DHCP zum Angeben einer statischen IP-Adresse für einen bestimmten Host konfigurieren möchten, fügen Sie unter *Einstellungen für Experten* im DHCP-Serverkonfigurationsmodul ([Schritt 4](#) (S. 96)) eine neue Deklaration für den Hosttyp hinzu. Fügen Sie dieser Hostdeklaration die Optionen `hardware` und `fixed-address` hinzu und bieten Sie die entsprechenden Werte an.

Manuelles Einrichten eines DHCP-Servers

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

- 1 Melden Sie sich als `root` auf dem Computer an, der den DHCP-Server bereitstellt.
- 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_adresse;
            fixed-address beliebige_ip_adresse; }
}

```

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.

4.3.2 Einrichten eines TFTP-Servers

Richten Sie einen TFTP-Server auf SUSE Linux Enterprise Server und SUSE Linux mit YaST ein oder richten Sie ihn manuell auf allen anderen Linux-Betriebssystemen

ein, die `xinetd` und `tftp` unterstützen. 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`-Benutzer an.
- 2 Starten Sie *YaST* → *Netzwerkdienste* → *TFTP-Server* und installieren Sie das erforderliche Paket.
- 3 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.
- 4 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.
- 5 Klicken Sie auf *Durchsuchen*, um nach dem Verzeichnis mit dem Boot-Image zu suchen. Das Standardverzeichnis `/tftpboot` wird erstellt und automatisch ausgewählt.
- 6 Klicken Sie auf *Beenden*, um die Einstellungen zu übernehmen und den Server zu starten.

Manuelles Einrichten eines TFTP-Servers

- 1 Melden Sie sich als `root` an und installieren Sie die Pakete `tftp` und `xinetd`.
- 2 Erstellen Sie die Verzeichnisse `/srv/tftpboot` und `/srv/tftpboot/pxelinux.cfg`, sofern sie noch nicht vorhanden sind.
- 3 Fügen Sie wie in [Abschnitt 4.3.3, „Verwenden von PXE Boot“](#) (S. 99) 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:

a Erstellen Sie, sofern noch nicht vorhanden, eine Datei namens `tftp` in diesem Verzeichnis, indem Sie `touch tftp` eingeben. Führen Sie anschließend folgenden Befehl aus: `chmod 755 tftp`.

b 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 /tftpboot
    disable              = no
}
```

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

4.3.3 Verwenden von PXE Boot

Einige technische Hintergrundinformationen sowie die vollständigen PXE-Spezifikationen finden Sie in der PXE-(Preboot Execution Environment-)Spezifikation (<ftp://download.intel.com/labs/manage/wfm/download/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 unter Verwendung von 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 Installationservers. `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 4.4, „Booten des Zielsystems für die Installation“](#) (S. 106).

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, indem Sie die Optionen `vnc` und `vncpassword` oder `ssh` und `sshpassword` zum Eintrag `install` hinzufügen. 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/pfad_instquelle/produkt

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

# apic
label apic
kernel linux
    append initrd=initrd ramdisk_size=65536 apic insmod=e100 \
        install=nfs://ip_instserver/pfad_instquelle/produkt

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

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

# memory test
label memtest
kernel memtest

# hard disk
label hddisk
kernel
```

```
linux append SLX=0x202

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.

4.3.4 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 eigener_kernel optionen_eigener_kernel
  initrd eigenerinitrd
```

PXELINUX verwendet die folgende Syntax:

```
label eigenebezeichnung
  kernel eigenerkernel
  append eigeneoptionen
```

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

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

APPEND

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

LOCALBOOT *Typ*

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

Argument	Beschreibung
0	Führt einen normalen Bootvorgang aus
4	Führt einen lokalen Bootvorgang mit dem noch im Arbeitsspeicher vorhandenen UNDI-Treiber (Universal Network Driver Interface) aus

Argument	Beschreibung
5	Führt einen lokalen Bootvorgang mit dem gesamten PXE-Stack, einschließlich des UNDI-Treibers aus, der sich im Arbeitsspeicher befindet

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

TIMEOUT *Zeitlimit*

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

PROMPT *flag_val*

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

```
F2 dateiname
F1 dateiname
..etc...
F9 dateiname
F10dateiname
```

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.

4.3.5 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.

4.3.6 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.

4.3.7 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.

Benutzer von SUSE Linux Enterprise Server 9 und höher können zur einfachen Konfiguration von Wake-on-LAN ein YaST-Modul namens WOL verwenden. Die Benutzer anderer Betriebssysteme mit der Basis SUSE Linux können ein Kommandozeilenwerkzeug verwenden.

4.3.8 Wake-on-LAN mit YaST

- 1 Melden Sie sich als `root`-Benutzer an.
- 2 Starten Sie *YaST* → *Netzwerkdienste* → *WOL*.
- 3 Klicken Sie auf *Hinzufügen* und geben Sie den Hostnamen und die MAC-Adresse des Zielsystems ein.
- 4 Wählen Sie zum Einschalten dieser Maschine den entsprechenden Eintrag und klicken Sie auf *Wake up* (Aufwachen).

4.3.9 Manuelles Wake-on-LAN

- 1 Melden Sie sich als `root`-Benutzer an.
- 2 Starten Sie *YaST* → *Software Management (Software-Management)* 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_des_ziels
```

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

4.4 Booten des Zielsystems für die Installation

Abgesehen von der in [Abschnitt 4.3.7](#), „Wake-on-LAN“ (S. 105) und [Abschnitt 4.3.3](#), „Verwenden von PXE Boot“ (S. 99) beschriebenen Vorgehensweise gibt es im

Wesentlichen zwei unterschiedliche Möglichkeiten, den Bootvorgang für die Installation anzupassen. Sie können entweder die standardmäßigen Boot-Optionen und Funktions-tasten 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.

4.4.1 Standardmäßige Boot-Optionen

Die Boot-Optionen werden genauer unter [Kapitel 3, *Installation mit YaST*](#) (S. 37) erläutert. In der Regel wird durch die Auswahl von *Installation* der Bootvorgang für die Installation gestartet.

Verwenden Sie bei Problemen *Installation - ACPI deaktiviert* bzw. *Installation - Sichere Einstellungen*. Weitere Informationen zu Fehlerbehebung beim Installationsvorgang finden Sie in [Abschnitt 52.2, „Probleme bei der Installation“](#) (S. 999).

4.4.2 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 4.4.3, „Benutzerdefinierte Boot-Optionen“](#) (S. 108)).

Die verfügbaren Optionen finden Sie in der folgenden Tabelle.

Tabelle 4.1 *F-Tasten bei der Installation*

Schlüssel	Zweck	Verfügbare Optionen	Standardwert
F1	Bietet Hilfe	Keine	Keine
F2	Wählt die Installations-sprache	Alle unterstützten Sprachen	Englisch

Schlüssel	Zweck	Verfügbare Optionen	Standardwert
F3	Ändert die Bildschirmauflösung für die Installation	<ul style="list-style-type: none"> • Expertenmodus • VESA • Auflösung 1 • Auflösung 2 • ... 	<ul style="list-style-type: none"> • Die Standardwerte sind abhängig von der Grafikkarte
F4	Wählt die Installationsquelle	<ul style="list-style-type: none"> • CD-ROM oder DVD • SLP • FTP • HTTP • NFS • SMB • Festplatte 	CD-ROM oder DVD
F5	Führt die Treiberaktualisierung von Diskette aus	Treiber	Keine

4.4.3 Benutzerdefinierte Boot-Optionen

Mithilfe geeigneter Boot-Optionen können Sie den Installationsvorgang vereinfachen. Viele Parameter können mit den `linuxrc`-Routinen auch zu einem späteren Zeitpunkt konfiguriert werden, das Verwenden der Boot-Optionen ist jedoch viel einfacher. In einigen automatisierten Setups können die Boot-Optionen über die Datei `initrd` oder eine `info`-Datei bereit gestellt werden.

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

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

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

Tabelle 4.2 *In diesem Kapitel verwendete Installationsszenarien (Boot-Szenarien)*

Installationsszenario	Für den Bootvorgang erforderliche Parameter	Boot-Optionen
Kapitel 3, <i>Installation mit YaST</i> (S. 37)	Keine: System bootet automatisch	Nicht erforderlich
Abschnitt 4.1.1, „Einfache Installation mit entferntem Zugriff über VNC – Statische Netzwerkkonfiguration“ (S. 76)	<ul style="list-style-type: none"> • Adresse des Installationservers • Netzwerkgerät • IP-Adresse • Netzmaske • Gateway • VNC-Aktivierung • VNC-Passwort 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb)://Pfad_zu_Instmedium</code> • <code>netdevice=some_netdevice</code> (nur erforderlich, wenn mehrere Netzwerkgeräte verfügbar sind) • <code>hostip=some_ip</code> • <code>netmask=some_netmask</code> • <code>gateway=ip_gateway</code> • <code>vnc=1</code> • <code>vncpassword=some_password</code>
Abschnitt 4.1.2, „Einfache Installation mit	<ul style="list-style-type: none"> • Adresse des Installationservers 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb)://Pfad_zu_Instmedium</code>

Installationsszenario	Für den Bootvorgang erforderliche Parameter	Boot-Optionen
entferntem Zugriff über VNC – Dynamische Netzwerkkonfiguration“ (S. 78)	<ul style="list-style-type: none"> • VNC-Aktivierung • VNC-Passwort 	<ul style="list-style-type: none"> • <code>vnc=1</code> • <code>vncpassword=some_password</code>
Abschnitt 4.1.3, „Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN“ (S. 79)	<ul style="list-style-type: none"> • Adresse des Installationservers • Adresse des TFTP-Servers • VNC-Aktivierung • VNC-Passwort 	Nicht zutreffend; Prozess wird über PXE und DHCP verwaltet
Abschnitt 4.1.4, „Einfache Installation mit entferntem Zugriff über SSH – Statische Netzwerkkonfiguration“ (S. 81)	<ul style="list-style-type: none"> • Adresse des Installationservers • Netzwerkgerät • IP-Adresse • Netzmaske • Gateway • SSH-Aktivierung • SSH-Passwort 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb):://Pfad_zu_Instmedium</code> • <code>netdevice=some_netdevice</code> (nur erforderlich, wenn mehrere Netzwerkgeräte verfügbar sind) • <code>hostip=some_ip</code> • <code>netmask=some_netmask</code> • <code>gateway=ip_gateway</code> • <code>usessh=1</code> • <code>sshpassword=some_password</code>
Abschnitt 4.1.5, „Einfache entfernte Installation über SSH – Dynamische	<ul style="list-style-type: none"> • Adresse des Installationservers • SSH-Aktivierung • SSH-Passwort 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb):://Pfad_zu_Instmedium</code> • <code>usessh=1</code>

Installationsszenario	Für den Bootvorgang erforderliche Parameter	Boot-Optionen
Netzwerkconfiguration“ (S. 82)		<ul style="list-style-type: none"> • <code>sshpassword=some_password</code>
Abschnitt 4.1.6, „Installation auf entfernten Systemen über SSH – PXE-Boot und Wake-on-LAN“ (S. 84)	<ul style="list-style-type: none"> • Adresse des Installationsservers • Adresse des TFTP-Servers • SSH-Aktivierung • SSH-Passwort 	Nicht zutreffend; Prozess wird über PXE und DHCP verwaltet

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`.

4.5 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.

4.5.1 VNC-Installation

Mithilfe einer beliebigen VNC-Viewer-Software können Sie die Installation von SUSE Linux Enterprise 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 4.4.3, „Benutzerdefinierte Boot-Optionen“](#) (S. 108)). 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 (dem Installationsziel in diesem Fall) 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_adresse:anzeige_nummer
```

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 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_adresse_des_ziels: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.

4.5.2 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 Einzelheiten finden Sie unter [Abschnitt 4.4.3, „Benutzerdefinierte Boot-Optionen“](#) (S. 108). 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_adresse_des_ziels
```

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. Es wird ein Fenster geöffnet, in dem die üblichen YaST-Bildschirme wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben angezeigt werden.

Automatisierte Installation

AutoYaST ermöglicht es Ihnen, SUSE® Linux Enterprise auf einer großen Anzahl von Computern gleichzeitig zu installieren. Die AutoYaST-Technologie bietet große Flexibilität zur Anpassung von Implementierungen für heterogene Hardware. In diesem Kapitel erfahren Sie, wie eine einfache automatisierte Installation vorbereitet wird und ein komplexeres Szenario mit unterschiedlichen Hardwaretypen und Installationszwecken gehandhabt wird.

5.1 Einfache Masseninstallation

WICHTIG: Identische Hardware

Dieses Szenario setzt voraus, dass Sie SUSE Linux Enterprise auf einer Reihe von Computern mit genau derselben Hardware-Konfiguration installieren.

Zur Vorbereitung einer AutoYaST-Masseninstallation gehen Sie wie folgt vor:

- 1 Erstellen Sie ein AutoYaST-Profil mit den erforderlichen Installationsdetails für Ihr Szenario, wie unter [Abschnitt 5.1.1, „Erstellen eines AutoYaST-Profiles“](#) (S. 116) beschrieben.
- 2 Bestimmen Sie die Quelle für das AutoYaST-Profil und den Parameter, der an die Installationsroutinen übergeben werden soll (siehe [Abschnitt 5.1.2, „Verteilen des Profils und Festlegen der autoyast-Parameter“](#) (S. 118)).

- 3 Bestimmen Sie die Quelle für die SUSE Linux Enterprise-Installationsdaten, wie unter [Abschnitt 5.1.3, „Bereitstellung der Installationsdaten“](#) (S. 121) beschrieben.
- 4 Richten Sie das Boot-Szenario für die automatische Installation, wie unter [Abschnitt 5.1.4, „Einrichten des Boot-Szenarios“](#) (S. 121) beschrieben ein.
- 5 Übergeben Sie die Kommandozeile an die Installationsroutinen, indem Sie die Parameter manuell hinzufügen oder eine `info`-Datei erstellen (siehe [Abschnitt 5.1.5, „Erstellen der info-Datei“](#) (S. 124)).
- 6 Starten Sie die automatische Installation, wie unter [Abschnitt 5.1.6, „Initialisierung und Überwachung der automatischen Installation“](#) (S. 127) beschrieben.

5.1.1 Erstellen eines AutoYaST-Profiles

Ein AutoYaST-Profil weist AutoYaST an, was installiert und wie das installierte System konfiguriert werden soll, um am Ende ein voll funktionsbereites System zu ergeben. Ein solches Profil kann auf verschiedene Weisen erstellt werden:

- Klonen einer frischen Installation von einem Referenzcomputer auf einer Reihe von identischen Computern
- Erstellung und Änderung eines Profils mithilfe der AutoYaST GUI nach Ihren Anforderungen
- Verwendung eines XML-Editors zur Erstellung eines ganz neuen Profils

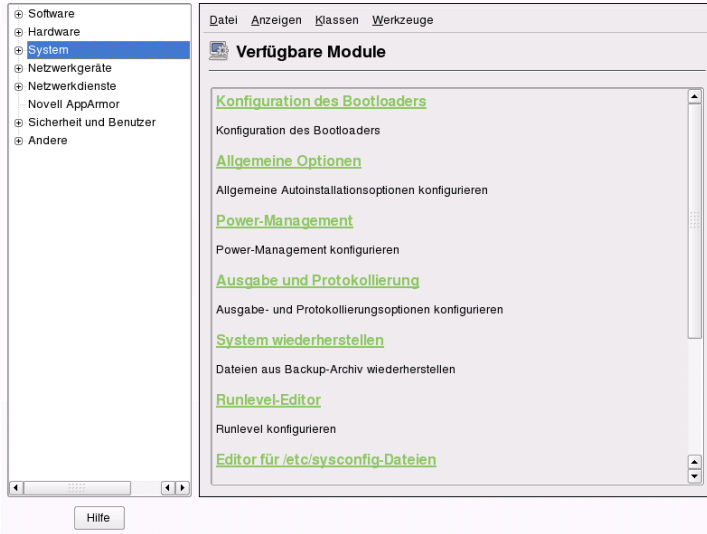
Gehen Sie wie folgt vor, um eine frische Referenzinstallation zu klonen:

- 1 Führen Sie eine normale Installation aus.
- 2 Nachdem Sie die Hardware-Konfiguration abgeschlossen und die Versionshinweise gelesen haben, aktivieren Sie die Option *Create Profile For AutoYaST* (Profil für AutoYaST erstellen), falls diese nicht standardmäßig aktiviert ist. Dadurch wird ein einsatzbereites Profil namens `/root/autoyast.xml` erstellt, das zur Erstellung mehrerer Klone dieser speziellen Installation eingesetzt werden kann.

Gehen Sie wie folgt vor, um über die AutoYaST GUI aus einer bestehenden Systemkonfiguration ein Profil zu erstellen und dieses nach Bedarf zu verändern:

- 1 Starten Sie YaST als `root`.
- 2 Wählen Sie *Miscellaneous (Andere)* → *Autoinstallation*, um die AutoYaST-Bedienoberfläche zu starten.
- 3 Wählen Sie *Werkzeuge* → *Create Reference Control File (Referenzkontrolldatei erstellen)*, um AutoYaST für die Spiegelung der aktuellen Systemkonfiguration in ein AutoYaST-Profil vorzubereiten.
- 4 Zusätzlich zu den Standardressourcen, wie Bootloader, Partitionierung und Software-Auswahl, können Sie dem Profil zahlreiche andere Aspekte Ihres Systems hinzufügen, indem Sie die Elemente in der Liste *Create a Reference Control File (Referenzkontrolldatei erstellen)* aktivieren.
- 5 Klicken Sie auf *Erstellen*, damit YaST alle Systeminformationen sammelt und in ein neues Profil schreibt.
- 6 Wählen Sie eine der folgenden Möglichkeiten, um fortzufahren:
 - Wenn das Profil abgeschlossen ist und Ihren Anforderungen entspricht, wählen Sie *Datei* → *Speichern unter* und geben Sie einen Dateinamen für das Profil ein, beispielsweise `autoyast.xml`.
 - Ändern Sie das Referenzprofil durch Auswahl der entsprechenden Konfigurationsaspekte (wie „Hardware/Drucker“) in der Baumansicht auf der linken Seite und klicken Sie dann auf *Konfigurieren*. Das entsprechende YaST-Modul wird gestartet, aber die Einstellungen werden nicht auf Ihr System angewendet, sondern in das AutoYaST-Profil geschrieben. Wählen Sie nach Abschluss dieses Vorgangs *Datei* → *Speichern unter* und geben Sie einen passenden Namen für das Profil ein.
- 7 Schließen Sie das AutoYaST-Modul mit *Datei* → *Beenden*.

Abbildung 5.1 Bearbeiten eines AutoYaST-Profiles in der AutoYaST-Bedienoberfläche



5.1.2 Verteilen des Profils und Festlegen der autoyast-Parameter

Das AutoYaST-Profil kann auf verschiedene Weisen verteilt werden. Je nachdem, welches Protokoll zur Verteilung der Profildaten eingesetzt wird, werden verschiedene AutoYaST-Parameter verwendet, um den Installationsroutinen auf dem Client den Profilspeicherort bekannt zu geben. Der Speicherort des Profils wird an die Installationsroutinen durch die Boot-Eingabeaufforderung oder eine `info`-Datei übergeben, die beim Booten geladen wird. Die folgenden Optionen stehen zur Verfügung:

Profilspeicherort	Parameter	Beschreibung
Datei	<code>autoyast=file:// pfad</code>	Bewirkt, dass die Installationsroutinen im angegebenen Pfad nach der Kontrolldatei suchen (relativ zum Quellen-root-Verzeichnis – <code>file:///autoyast.xml</code> ,

Profilspeicherort	Parameter	Beschreibung
		ausgehend vom root-Verzeichnis einer CD-ROM).
Gerät	<code>autoyast=device:// pfad</code>	Bewirkt, dass die Installationsroutinen auf einem Speichergerät nach der Kontrolldatei suchen. Es wird nur der Gerätename benötigt – <code>/dev/sda1</code> ist falsch, verwenden Sie stattdessen <code>sda1</code> .
Diskette	<code>autoyast=floppy:// pfad</code>	Bewirkt, dass die Installationsroutinen auf einer Diskette im Diskettenlaufwerk nach der Kontrolldatei suchen. Diese Option ist besonders hilfreich, wenn Sie von einer CD-ROM booten möchten.
NFS	<code>autoyast=nfs:// server/pfad</code>	Lässt die Installationsroutinen die Kontrolldatei von einem NFS-Server abrufen.
HTTP	<code>autoyast=http:// server/pfad</code>	Lässt die Installationsroutinen die Kontrolldatei von einem HTTP-Server abrufen.
HTTPS	<code>autoyast=https:// server/pfad</code>	Lässt die Installationsroutinen die Kontrolldatei von einem HTTPS-Server abrufen.
TFTP	<code>autoyast=tftp:// server/pfad</code>	Lässt die Installationsroutinen die Kontrolldatei von einem TFTP-Server abrufen.
FTP	<code>autoyast=ftp:// server/pfad</code>	Lässt die Installationsroutinen die Kontrolldatei von einem FTP-Server abrufen.

Ersetzen Sie die Platzhalter *server* und *pfad* durch die entsprechenden Werte für Ihre Konfiguration.

AutoYaST enthält eine Funktion, die eine Bindung bestimmter Profile an die MAC-Adresse des Client ermöglicht. Dadurch können Sie verschiedene Instanzen derselben Konfiguration mit unterschiedlichen Profilen installieren, ohne den Parameter `autoyast=` zu ändern.

Gehen Sie hierfür wie folgt vor:

1 Erstellen Sie separate Profile mit der MAC-Adresse des Client als Dateiname und speichern Sie diese auf dem HTTP-Server mit Ihren AutoYaST-Profilen.

2 Lassen Sie den exakten Pfad leer und geben Sie bei Erstellung des Parameters `autoyast=` den Dateinamen an. Zum Beispiel:

```
autoyast=http://192.0.2.91/
```

3 Starten Sie die automatische Installation.

YaST versucht, den Speicherort des Profils auf folgende Weise zu ermitteln:

1. YaST sucht nach dem Profil unter Verwendung seiner eigenen IP-Adresse in Hexadezimalzahlen mit Großbuchstaben, z. B. `192.0.2.91` ist `C000025B`.
2. Wird diese Datei nicht gefunden, entfernt YaST eine Hexadezimalstelle und versucht es dann erneut. Diese Aktion wird achtmal wiederholt, bis die Datei mit dem korrekten Namen gefunden wird.
3. Wenn dies weiterhin fehlschlägt, sucht YaST nach einer Datei mit der MAC-Adresse des Client als Dateiname. Die MAC-Adresse des Beispiel-Client ist `0080C8F6484C`.
4. Wenn die mit der MAC-Adresse benannte Datei nicht gefunden wird, sucht YaST nach einer Datei namens `default` (in Kleinbuchstaben). Ein Beispiel für eine Reihe von Adressen, in denen YaST nach dem AutoYaST-Profil sucht, sieht wie folgt aus:

```
C000025B
C000025
C00002
C0000
C000
C000
```

```
C00
C0
C
0080C8F6484C
default
```

5.1.3 Bereitstellung der Installationsdaten

Die Installationsdaten können in Form von Produkt-CDs oder -DVDs oder über eine Netzwerkinstallationsquelle bereitgestellt werden. Wenn die Produkt-CDs als Installationsquelle verwendet werden, ist zur Installation ein physischer Zugriff auf den Client erforderlich, da der Boot-Vorgang manuell gestartet werden muss und die CDs gewechselt werden müssen.

Zur Bereitstellung der Installationsquellen über das Netzwerk müssen Sie einen Netzwerkinstallationsserver (HTTP, NFS, FTP) einrichten, wie unter [Abschnitt 4.2.1](#), „[Einrichten eines Installationservers mithilfe von YaST](#)“ (S. 86) beschrieben. Verwenden Sie eine `info`-Datei, um den Installationsroutinen den Standort des Servers bekannt zu geben.

5.1.4 Einrichten des Boot-Szenarios

Der Client kann auf verschiedene Weisen gebootet werden:

Network-Boot

Wie bei einer normalen entfernten Installation ist es möglich, die automatische Installation mit Wake-on-LAN und PXE zu initialisieren, das Boot-Image und die Kontrolldatei über TFTP abzurufen und die Installationsquellen von einem Netzwerkinstallationsserver zu laden.

Bootfähige CD-ROM

Sie können den SUSE Linux Enterprise-Originaldatenträger verwenden, um das System für die automatische Installation zu booten und die Kontrolldatei von einem Netzlaufwerk oder einer Diskette zu laden. Alternativ dazu können Sie auch eine eigene CD-ROM mit den Installationsquellen und dem AutoYaST-Profil erstellen.

In den folgenden Abschnitten werden die Verfahren für das Booten über das Netzwerk oder von der CD-ROM kurz umrissen.

Vorbereitung auf einen Netzwerk-Boot

Das Netzwerk-Booten mit Wake-on-LAN, PXE und TFTP wird in [Abschnitt 4.1.3, „Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN“](#) (S. 79) beschrieben. Damit die dort vorgestellte Konfiguration für die automatische Installation eingesetzt werden kann, müssen Sie die angegebene PXE-Linux-Konfigurationsdatei (`/srv/tftp/pxelinux.cfg/default`) so ändern, dass der Parameter `autoyast` auf den Speicherort des AutoYaST-Profiles verweist. Ein Beispiel für eine Standardinstallation sieht wie folgt aus:

```
default linux

# default label linux
kernel linux append initrd=initrd ramdisk_size=65536 insmod=e100 \
install=http://192.168.0.22/install/suse-enterprise/
```

Dasselbe Beispiel für die automatische Installation sieht wie folgt aus:

```
default linux

# default label linux
kernel linux append initrd=initrd ramdisk_size=65536 insmod=e100 \
install=http://192.168.0.22/install/suse-enterprise/ \
autoyast=nfs://192.168.0.23/profiles/autoyast.xml
```

Ersetzen Sie die Beispiel-IP-Adressen und -pfade durch die Daten aus Ihrer Konfiguration.

Vorbereitung auf das Booten von CD-ROM

Das Booten von CD-ROM kann bei AutoYaST-Installationen auf verschiedene Weisen eingesetzt werden. Folgende Szenarien stehen zur Auswahl:

Booten von SUSE Linux Enterprise-Datenträgern, Abrufen des Profils über das Netzwerk
Verwenden Sie diesen Ansatz, wenn ein vollständig netzwerkbasiertes Szenario nicht möglich ist (beispielsweise, wenn Ihre Hardware PXE nicht unterstützt) und Sie ausreichenden physischen Zugriff auf das zu installierende System haben.

Sie benötigen:

- Die SUSE Linux Enterprise-Datenträger

- Ein Netzwerkservers, der die Profildaten bereitstellt (Einzelheiten siehe [Abschnitt 5.1.2, „Verteilen des Profils und Festlegen der autoyast-Parameter“](#) (S. 118))
- Eine Diskette mit der `info`-Datei, die den Installationsroutinen den Speicherort des Profils angibt

Oder:

Zugriff auf die Boot-Eingabeaufforderung des zu installierenden Systems zur manuellen Eingabe des Parameters `autoyast=`

Booten und Installation von SUSE Linux Enterprise-Datenträgern, Abrufen des Profils von einer Diskette

Verwenden Sie diesen Ansatz, wenn ein vollständig netzwerkbasierendes Installationszenario nicht möglich ist. Er erfordert den physischen Zugriff auf das zu installierende System zum Einschalten des Zielcomputers oder, wie im zweiten Fall, zur Eingabe des Speicherorts des Profils an der Boot-Eingabeaufforderung. In beiden Fällen müssen Sie je nach Umfang der Installation möglicherweise auch die Datenträger wechseln.

Sie benötigen:

- Die SUSE Linux Enterprise-Datenträger
- Eine Diskette mit dem Profil und der `info`-Datei

Oder:

Zugriff auf die Boot-Eingabeaufforderung des Ziels zur Eingabe des Parameters `autoyast=`

Booten und Installation von benutzerdefinierten Datenträgern, Abrufen des Profils von den Datenträgern

Wenn Sie nur eine beschränkte Anzahl von Softwarepaketen installieren müssen und die Anzahl der Ziele relativ gering ist, empfiehlt es sich möglicherweise, eine eigene benutzerdefinierte CD mit den Installationsdaten und dem Profil zu erstellen. Dies empfiehlt sich vor allem, wenn in Ihrer Konfiguration kein Netzwerk verfügbar ist.

5.1.5 Erstellen der `info`-Datei

Die Installationsroutinen auf dem Zielcomputer müssen auf die vielen verschiedenen Komponenten des AutoYaST-Framework aufmerksam gemacht werden. Dies geschieht durch Erstellung einer Kommandozeile mit allen Parametern, die zum Auffinden der AutoYaST-Komponenten, Installationsquellen und Parameter erforderlich sind, die zur Steuerung des Installationsvorgangs benötigt werden.

Sie können dies bewerkstelligen, indem Sie diese Parameter an der Boot-Eingabeaufforderung der Installation manuell eingeben oder indem Sie eine Datei namens `info` bereitstellen, die von den Installationsroutinen (`linuxrc`) gelesen wird. Ersteres erfordert den physischen Zugriff auf jeden zu installierenden Client, was diesen Ansatz für umfangreiche Implementierungen ungeeignet macht. Letzteres ermöglicht Ihnen die Bereitstellung der `info`-Datei auf einem Datenträger, der vorbereitet und vor der automatischen Installation in das entsprechende Laufwerk des Client eingelegt wird. Alternativ dazu können Sie auch einen PXE-Boot durchführen und die `linuxrc`-Parameter in die Datei `pxelinux.cfg/default` einfügen (siehe „[Vorbereitung auf einen Netzwerk-Boot](#)“ (S. 122)).

Die folgenden Parameter werden häufig für `linuxrc` verwendet. Weitere Informationen finden Sie in der Dokumentation zu AutoYaST unter `/usr/share/doc/packages/autoyast`.

WICHTIG: Trennung von Parametern und Werten

Verwenden Sie bei der Übergabe von Parametern an `linuxrc` an der Boot-Eingabeaufforderung ein Gleichheitszeichen (=), um Parameter und Wert voneinander zu trennen. Bei Verwendung einer `info`-Datei müssen Parameter und Wert durch einen Doppelpunkt (:) getrennt sein.

Schlüsselwort	Wert
<code>netdevice</code>	Das Netzwerkgerät, das für die Netzwerkeinrichtung verwendet werden soll (für BOOTP/DHCP-Anforderungen). Nur erforderlich, wenn mehrere Netzwerkgeräte verfügbar sind.

Schlüsselwort	Wert
hostip	Beim Fehlen einer Angabe sendet der Client eine BOOTP-Anforderung. Anderenfalls wird der Client mithilfe der angegebenen Daten konfiguriert.
netmask	Netzmaske.
gateway	Gateway.
nameserver	Namenserver.
autoyast	Speicherort der Kontrolldatei, die für die automatische Installation verwendet wird, beispielsweise autoyast=http://192.168.2.1/profiles/.
install	Speicherort der Installationsquelle, beispielsweise install=nfs://192.168.2.1/CDs/.
vnc	Der Wert 1 aktiviert die ferngesteuerte VNC-Installation.
vncpassword	Das Passwort für VNC.
usessh	Der Wert 1 aktiviert die ferngesteuerte SSH-Installation.

Wenn Ihr Szenario für die automatische Installation eine Client-Konfiguration über DHCP und eine Netzwerkinstallationsquelle aufweist und Sie den Installationsvorgang mit VNC überwachen möchten, würde Ihre `info`-Datei wie folgt aussehen:

```
autoyast:profil_quelle install:installations_quelle vnc:1
vncpassword:beliebiges_passwort
```

Wenn Sie eine statische Netzwerkkonfiguration bevorzugen, würde Ihre `info`-Datei wie folgt aussehen:

```
autoyast:profil_quelle \
install:installations_quelle \
hostip:beliebige_ip \
netmask:beliebige_netzmaske \
gateway:beliebiges_gateway
```

Umgekehrte Schrägstriche (\) geben an, dass die Zeilenumbrüche nur zur Verbesserung der Lesbarkeit hinzugefügt wurden. Alle Optionen müssen als eine fortlaufende Zeichenkette eingegeben werden.

Die `info`-Daten können `linuxrc` auf verschiedene Weisen bereitgestellt werden:

- Als Datei im `root`-Verzeichnis einer Diskette, die sich zum Installationszeitpunkt im Diskettenlaufwerk des Client befindet.
- Als Datei im `root`-Verzeichnis der Initial RAM-Disk, die zum Booten des Systems verwendet wird und entweder von einem benutzerdefinierten Installationsdatenträger oder von PXE-Boot stammt.
- Als Teil des AutoYaST-Profiles. In diesem Fall muss die AutoYaST-Datei `info` genannt werden, damit `linuxrc` sie analysieren kann. Ein Beispiel für diesen Ansatz sehen Sie unten.

`linuxrc` sucht im Profil nach einer Zeichenkette (`start_linuxrc_conf`), die den Anfang der Datei angibt. Wird diese gefunden, wird der Inhalt der Datei zwischen dieser Zeichenkette und der Zeichenkette `end_linuxrc_conf` analysiert. Die Optionen werden im Profil wie folgt gespeichert:

```
....
  <install>
....
  <init>
    <info_file>
<![CDATA[
#
# Don't remove the following line:
# start_linuxrc_conf
#
install: nfs:server/pfad
vnc: 1
vncpassword: test
autoyast: file:///info

# end_linuxrc_conf
# Do not remove the above comment
#
]]>

    </info_file>
  </init>
....
</install>
....
```

linuxrc lädt das Profil mit den Boot-Parametern anstelle der herkömmlichen `info`-Datei. Der Parameter `installieren`: verweist auf den Speicherort der Installationsquellen. `vnc` und `vncpassword` geben die Verwendung von VNC für die Installationsüberwachung an. Der Parameter `autoyast` weist linuxrc an, die `info`-Datei als AutoYaST-Profil zu behandeln.

5.1.6 Initialisierung und Überwachung der automatischen Installation

Nachdem Sie die gesamte oben genannte Infrastruktur bereitgestellt haben (Profil, Installationsquelle und `info`-Datei), können Sie die automatische Installation starten. Je nach gewähltem Szenario für das Booten und Überwachen des Vorgangs kann eine physische Interaktion mit dem Client erforderlich sein:

- Wenn das Client-System von physischen Datenträgern bootet (entweder von Produktdatenträgern oder benutzerdefinierten CDs), müssen Sie diese in das entsprechende Laufwerk des Client einlegen.
- Wenn der Client nicht mittels Wake-on-LAN eingeschaltet wird, müssen Sie zumindest den Client-Computer einschalten.
- Wenn Sie sich nicht für eine ferngesteuerte automatische Installation entschieden haben, werden die visuellen Rückmeldungen von AutoYaST an den angeschlossenen Bildschirm bzw. an eine serielle Konsole gesendet, falls der Client über keinen Bildschirm verfügt.

Zur Aktivierung einer ferngesteuerten automatischen Installation verwenden Sie die unter beschriebenen [Abschnitt 5.1.5, „Erstellen der `info`-Datei“](#) (S. 124) VNC- oder SSH-Parameter und stellen Sie von einem anderen Computer aus eine Verbindung zum Client her (siehe [Abschnitt 4.5, „Überwachen des Installationsvorgangs“](#) (S. 111)).

5.2 Regelbasierte automatische Installation

In den folgenden Abschnitten werden die grundlegenden Konzepte der regelbasierten automatischen Installation mit AutoYaST vorgestellt und anhand der Beispielszenarien

können Sie eigene benutzerdefinierte Konfigurationen für die automatische Installation erstellen.

5.2.1 Informationen zur regelbasierten automatischen Installation

Die regelbasierte AutoYaST-Installation ermöglicht Ihnen den Einsatz heterogener Hardware-Umgebungen:

- Gibt es an Ihrem Standort Hardware verschiedener Hersteller?
- Weisen die Computer an Ihrem Standort eine unterschiedliche Hardware-Konfiguration auf (beispielsweise verschiedene Geräte oder Arbeitsspeicher- und Festplattengrößen)?
- Beabsichtigen Sie eine Installation über verschiedene Domänen hinweg und müssen Sie zwischen diesen unterscheiden?

Das Ziel der regelbasierten automatischen Installation besteht im Grunde darin, ein benutzerdefiniertes Profil für ein heterogenes Szenario durch Zusammenführung verschiedener Profile zu erstellen. Jede Regel beschreibt hierbei ein bestimmtes Merkmal Ihrer Konfiguration (z. B. die Festplattengröße) und weist AutoYaST an, welches Profil verwendet werden soll, wenn die Regel übereinstimmt. Mehrere Regeln, die die verschiedenen Merkmale Ihrer Konfiguration beschreiben, werden in einer AutoYaST-Datei namens `rules.xml` zusammengefasst. Der Regelstapel wird dann verarbeitet und AutoYaST generiert das endgültige Profil durch Zusammenführung der verschiedenen Profile, die mit den AutoYaST-Regeln übereinstimmen. Eine Illustration dieses Vorgangs finden Sie unter [Abschnitt 5.2.2, „Beispielszenario für die regelbasierte automatische Installation“](#) (S. 130).

Die regelbasierte AutoYaST-Installation bietet Ihnen große Flexibilität bei der Planung und Durchführung der SUSE Linux Enterprise-Implementierung. Sie können:

- Regeln für die Übereinstimmung mit den vordefinierten Systemattributen in AutoYaST erstellen
- Mehrere Systemattribute (wie die Festplattengröße und die Kernel-Architektur) mithilfe logischer Operatoren zu einer Regel zusammenfassen

- Durch Ausführung von Shell-Skripten und die Übergabe des Ergebnisses an das AutoYaST-Framework benutzerdefinierte Regeln erstellen. Die Anzahl der benutzerdefinierten Regeln ist auf fünf beschränkt.

ANMERKUNG

Weitere Informationen zur Erstellung und Verwendung von Regeln mit AutoYaST finden Sie in der Dokumentation zum Paket unter `/usr/share/doc/packages/autoyast2/html/index.html` im Kapitel *Regeln und Klassen*.

Zur Vorbereitung einer regelbasierten AutoYaST-Masseninstallation gehen Sie wie folgt vor:

- 1 Erstellen Sie mehrere AutoYaST-Profilen mit den erforderlichen Installationsdetails für Ihre heterogene Konfiguration, wie unter [Abschnitt 5.1.1, „Erstellen eines AutoYaST-Profiles“](#) (S. 116) beschrieben.
- 2 Definieren Sie Regeln für die Übereinstimmung der Systemattribute Ihrer Hardware-Konfiguration (siehe [Abschnitt 5.2.2, „Beispielszenario für die regelbasierte automatische Installation“](#) (S. 130)).
- 3 Bestimmen Sie die Quelle für das AutoYaST-Profil und den Parameter, der an die Installationsroutinen übergeben werden soll (siehe [Abschnitt 5.1.2, „Verteilen des Profils und Festlegen der autoyast-Parameter“](#) (S. 118)).
- 4 Bestimmen Sie die Quelle für die SUSE Linux Enterprise-Installationsdaten, wie unter [Abschnitt 5.1.3, „Bereitstellung der Installationsdaten“](#) (S. 121) beschrieben.
- 5 Übergeben Sie die Kommandozeile an die Installationsroutinen, indem Sie die Parameter manuell hinzufügen oder eine `info`-Datei erstellen (siehe [Abschnitt 5.1.5, „Erstellen der info-Datei“](#) (S. 124)).
- 6 Richten Sie das Boot-Szenario für die automatische Installation, wie unter [Abschnitt 5.1.4, „Einrichten des Boot-Szenarios“](#) (S. 121) beschrieben ein.
- 7 Starten Sie die automatische Installation, wie unter [Abschnitt 5.1.6, „Initialisierung und Überwachung der automatischen Installation“](#) (S. 127) beschrieben.

5.2.2 Beispielszenario für die regelbasierte automatische Installation

Zur Erlangung eines Grundverständnisses der Vorgehensweise für die Erstellung von Regeln sollten Sie das folgende Beispiel beachten, das unter [Abbildung 5.2, „AutoYaST-Regeln“](#) (S. 130) dargestellt ist. In einem AutoYaST-Durchlauf wird die folgende Konfiguration installiert:

Ein Druckserver

Dieser Computer erfordert nur eine minimale Installation ohne Desktop-Umgebung sowie einen eingeschränkten Satz von Softwarepaketen.

Arbeitsstationen in der technischen Abteilung

Diese Computer benötigen eine Desktop-Umgebung und eine breite Palette von Entwicklungssoftware.

Laptops in der Verkaufsabteilung

Diese Computer benötigen eine Desktop-Umgebung und eine eingeschränkte Palette spezialisierter Anwendungen, wie Büro- und Terminverwaltungsprogramme.

Abbildung 5.2 *AutoYaST-Regeln*



Verwenden Sie in einem ersten Schritt eine der unter [Abschnitt 5.1.1, „Erstellen eines AutoYaST-Profiles“](#) (S. 116) beschriebenen Methoden, um Profile für jeden Anwendungsfall zu erstellen. In diesem Beispiel würden Sie die Profile `print.xml`, `engineering.xml` und `sales.xml` erstellen.

Erstellen Sie in einem zweiten Schritt Regeln zur Unterscheidung zwischen den drei Hardwaretypen sowie zur Anweisung von AutoYaST, welches Profil verwendet werden soll. Verwenden Sie zur Erstellung der Regeln einen Algorithmus, der dem folgenden ähnelt:

1. Hat der Computer die IP-Adresse `192.168.27.11`? Dann mache ihn zum Druckserver.

2. Verfügt der Computer über PCMCIA-Hardware und einen Intel-Chipsatz? Dann betrachte ihn als Intel-Laptop und installiere darauf die Software-Auswahl für die Verkaufsabteilung.
3. Wenn keine dieser Bedingungen wahr ist, betrachte den Computer als Entwickler-Arbeitsstation und installiere ihn entsprechend.

Dies kann, grob umrissen, in eine Datei namens `rules.xml` mit folgendem Inhalt übersetzt werden:

```
<?xml version="1.0"?>
<!DOCTYPE autoinstall SYSTEM "/usr/share/autoinstall/dtd/rules.dtd">
<autoinstall xmlns="http://www.suse.com/1.0/yast2ns"
xmlns:config="http://www.suse.com/1.0/configs">
  <rules config:type="list">
    <rule>
      <hostaddress>
        <match>192.168.27.11</match>
        <match_type>exact</match_type>
      </hostaddress>
      <result>
        <profile>print.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
    </rule>
    <rule>
      <haspcmcia>
        <match>1</match>
        <match_type>exact</match_type>
      </haspcmcia>
      <custom1>
        <script>
if grep -i intel /proc/cpuinfo > /dev/null; then
echo -n "intel"
else
echo -n "non_intel"
fi;
          </script>
        <match>*</match>
        <match_type>exact</match_type>
      </custom1>
      <result>
        <profile>sales.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
      <operator>and</operator>
    </rule>
    <rule>
      <haspcmcia>
        <match>0</match>
        <match_type>exact</match_type>
```

```
        </haspcmcia>
    </result>
        <profile>engineering.xml</profile>
        <continue config:type="boolean">false</continue>
    </result>
</rule>
</rules>
</autoinstall>
```

Stellen Sie bei der Verteilung der Regeldatei sicher, dass sich das Verzeichnis `rules` unterhalb des Verzeichnisses `profiles` befindet, das in der URL `autoyast=protocol:serverip/profiles/` angegeben ist. AutoYaST sucht nach einem Unterverzeichnis namens `rules`, das eine Datei namens `rules.xml` enthält, lädt dann die in der Regeldatei angegebenen Profile und führt sie zusammen.

Der Rest des Verfahrens zur automatischen Installation wird wie üblich ausgeführt.

5.3 Weitere Informationen

Ausführlichere Informationen zur AutoYaST-Technologie finden Sie in der zusammen mit der Software installierten Dokumentation. Sie finden diese unter `/usr/share/doc/packages/autoyast2`. Die neueste Ausgabe dieser Dokumentation finden Sie unter http://www.suse.de/~ug/autoyast_doc/index.html.

Fortgeschrittene Festplattenkonfiguration

6

Komplexe Systemkonfigurationen erfordern besondere Festplattenkonfigurationen. Um eine persistente Gerätebenennung für SCSI-Geräte zu ermöglichen, verwenden Sie ein bestimmtes Startskript oder udev. 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. SUSE® Linux Enterprise Server unterstützt auch die Mehrfachpfad-E/A. Weitere Informationen finden Sie in [Kapitel 10, Multipath-E/A](#) (S. 277). Ab SUSE Linux Enterprise Server 10 besteht auch die Möglichkeit zur Verwendung von iSCSI als vernetzte Festplatte. Weitere Informationen zu iSCSI finden Sie unter [Kapitel 11, Massenspeicher über IP-Netzwerke – iSCSI](#) (S. 285).

6.1 LVM-Konfiguration

Dieser Abschnitt erläutert kurz die Prinzipien von LVM und seinen grundlegenden Funktionen, mit denen es in vielen Situationen nützlich ist. In [Abschnitt 6.1.2, „LVM-Konfiguration mit YaST“](#) (S. 136) erfahren Sie, wie LVM mit YaST eingerichtet wird.

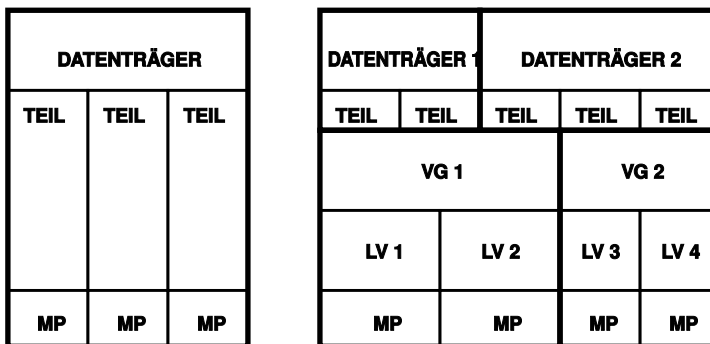
WARNUNG

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.

6.1.1 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 „[Partitionstypen](#)“ (S. 47) und [Abschnitt 7.5.8, „Partitionierung“](#) (S. 176).

Abbildung 6.1 *Physische Partitionierung versus LVM*



[Abbildung 6.1, „Physische Partitionierung versus LVM“](#) (S. 134) stellt die physische Partitionierung (links) der LVM-Segmentierung (rechts) gegenüber. Auf der linken Seite wurde eine einzelne Festplatte in drei physische Partitionen (PART) aufgeteilt, von denen jede einen Einhängepunkt (MP) hat, auf den das Betriebssystem zugreifen kann. Auf der rechten Seite wurden zwei Festplatten in zwei bzw. drei physische Partitionen aufgeteilt. Es wurden zwei LVM-Volume-Gruppen (VG 1 und VG 2) angelegt. VG 1 enthält zwei Partitionen von DISK 1 und eine von DISK 2. VG 2 enthält die restlichen zwei Partitionen von DISK 2. In LVM werden die physischen Festplattenpartitionen, die in einer Volume-Gruppe zusammengefasst sind, als physische Volumes

(PV) bezeichnet. In den Volume-Gruppen wurden vier logische Volumes (LV 1 bis LV 4) angelegt, die vom Betriebssystem über die zugewiesenen Einhängpunkte 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 den Device-Mapper, der in Kernel 2.6

integriert ist. Beginnend mit diesem Kernel kann LVM nur noch in der Version 2 verwendet werden. In diesem Kapitel ist mit LVM daher immer LVM in der Version 2 gemeint.

Statt LVM 2 können Sie EVMS (Enterprise Volume Management System) verwenden, das eine einheitliche Schnittstelle für logische Volumes und RAID-Volumes bietet. Wie LVM 2 verwendet EVMS den Device-Mapper in Kernel 2.6.

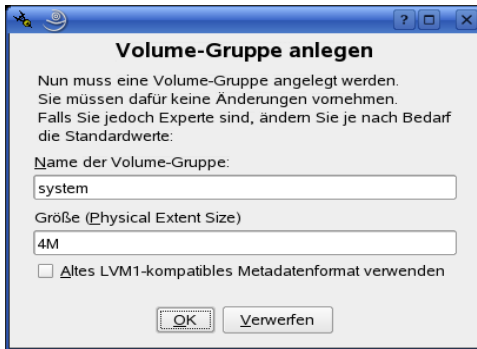
6.1.2 LVM-Konfiguration mit YaST

Zur LVM-Konfiguration mit YaST gelangen Sie über den YaST-Expertenmodus des Partitionierungsmoduls (siehe [Abschnitt 7.5.8](#), „[Partitionierung](#)“ (S. 176)). 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 6.2](#), „[Anlegen einer Volume-Gruppe](#)“ (S. 137)). 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 SUSE® Linux Enterprise-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 6.2 Anlegen einer Volume-Gruppe

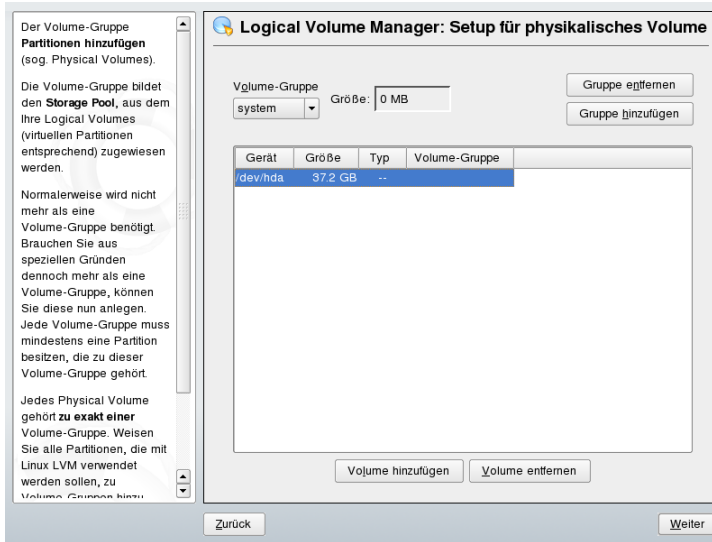


Konfigurieren von physischen Volumes

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 6.3 Setup für physische Volumes



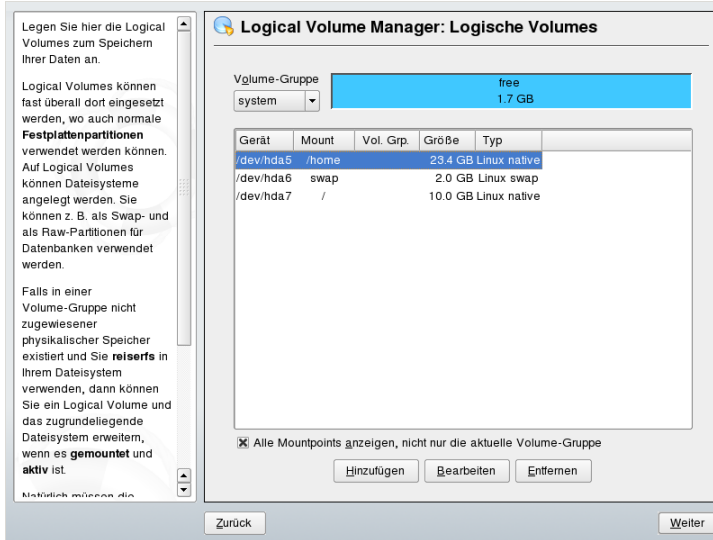
Um der ausgewählten Volume-Gruppe eine zuvor nicht zugewiesene Partition zuzuweisen, klicken Sie zuerst auf die Partition und anschließend auf *Volume hinzufügen*. Der Name der Volume-Gruppe wird dann bei der ausgewählten Partition eingetragen. Sie sollten alle Partitionen, die Sie für LVM vorgesehen 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 6.4 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 6.5 Erstellen logischer Volumes

The screenshot shows a dialog box titled "Logische Partition auf /dev/hda erstellen". It is divided into two main sections: "Formatieren" and "Größe".

- Formatieren:** Contains radio buttons for "Nicht formatieren" (unselected) and "Formatieren" (selected). Below "Formatieren" is a dropdown menu for "Dateisystem-ID:" with "tx83 Linux" selected. Below "Nicht formatieren" is a dropdown menu for "Dateisystem" with "Reiser" selected. There are buttons for "Optionen" and "Dateisystem verschlüsseln" (unchecked).
- Größe:** Shows "Zylindergröße: 7.84 M". Below it is a text input for "Startzylinder:" with "4635" entered. Below that is a text input for "Ende: (9 oder +9M oder +3.2GB)" with "4862" entered. There is a button for "Fstab-Optionen".

At the bottom, there is a "Mountpoint" dropdown menu with "/home" selected, and "OK" and "Verwerfen" buttons.

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.

6.1.3 Speicherplatzverwaltung mit EVMS

Das Enterprise Volume Management System 2 (EVMS2) ist ein vielseitiger, erweiterbarer Volume-Manager mit integrierter Cluster-Fähigkeit. Durch den Plugin-Aufbau können zusätzliche Funktionen durch Plugins zur Unterstützung und Informationen zu beliebigen Partitionstypen hinzugefügt werden. Die Cluster-Fähigkeit von EVMS2 stellt sicher, dass verwaltete Geräte an jedem Knoten im Cluster identisch benannt werden und so einfacher verwaltet werden können.

EVMS2 bietet eine einheitliche Schnittstelle (`evmsgui` und Kommandozeile) zur Verwaltung der folgenden Speicherplatzressourcen:

- Physische Festplatten und logische Geräte bei lokalen Medien und SAN-basierten Medien, einschließlich iSCSI
- Software RAIDs 0, 1, 4 und 5 für eine hohe Verfügbarkeit
- Cluster-fähiger Multipath-E/A zur Fehlertoleranz
- Cluster von Speicherplatzobjekten mit dem Plugin Cluster Segment Manager (CSM)
- Volumes für alle Dateisysteme mit einem Dateisystem-Schnittstellenmodul (FSIM) für EVMS2
- Aufnahmen von Volumes

In SUSE Linux Enterprise Server 10 sind u. a. folgende neue Funktionen verfügbar:

- EVMS2 und CLVM2 (Cluster Linux Volume Manager 2) verwenden dieselben Multidisk (MD)-Treiber und Device-Mapper (DM)-Treiber im Kernel.
- Dateisystem-Plugins sind verfügbar für Heartbeat 2 Cluster Manager und Oracle Cluster File System 2.

EVMS-Geräte

Das Administrationsdienstprogramm von EVMS unterscheidet fünf verschiedene Gerätestufen:

Festplatten

Das ist die niedrigste Gerätestufe. Alle Geräte, auf die als physische Festplatte zugegriffen werden kann, werden als Festplatten behandelt.

Segmente

Segmente bestehen aus Partitionen und anderen Speicherbereichen auf einer Festplatte, wie beispielsweise dem Master Boot Record (MBR).

Container

Container sind die Gegenstücke zu Volume-Gruppen in LVM.

Bereiche

Die verfügbaren Geräte werden hier in LVM2 und RAID aufgeteilt.

Volumes

Alle Geräte, ganz gleich, ob sie von einer realen Partition, einem logischen Volume oder einem RAID-Gerät dargestellt werden, sind mit ihren entsprechenden Einhängpunkten verfügbar.

Wenn Sie EVMS verwenden, müssen Sie Ihre Gerätenamen mit den EVMS-Gerätenamen ersetzen. Einfache Partitionen finden Sie in `/dev/evms/`, logische Volumes in `/dev/evms/lvm/` und RAID-Geräte in `/dev/evms/md`. Zum Aktivieren von EVMS beim Systemstart, fügen Sie den Startskripts im YaST-Runlevel-Editor `boot.evms` hinzu. Weitere Informationen hierzu finden Sie in [Abschnitt 20.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 431).

Weitere Informationen

Weitere Einzelheiten zur Verwendung von EVMS zur Verwaltung von Speicherplatzressourcen finden Sie im EVMS User Guide [http://evms.sourceforge.net/users_guide/] (EVMS-Benutzerhandbuch) im EVMS-Projekt [<http://evms.sourceforge.net/>] auf SourceForge*.

6.2 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.

6.2.1 RAID-Level

SUSE® Linux Enterprise bietet Ihnen die Möglichkeit, mithilfe von YaST mehrere Festplatten zu einem Soft-RAID-System zu vereinen – eine sehr günstige Alternative zu einem Hardware-RAID. 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 die Daten, weil diese 1:1 auf eine andere Festplatte kopiert werden. Dies wird als *Festplattenspiegelung* bezeichnet. Ist eine Festplatte zerstört, steht eine Kopie des Inhalts auf einer anderen zur Verfügung. Solange noch eine Festplatte intakt ist, können alle anderen fehlerhaft sein, ohne dass Daten verloren gehen. Wird der Schaden jedoch nicht festgestellt, kann es passieren, dass die beschädigten Daten auf die intakte Festplatte gespiegelt werden. Erst dadurch geht die Integrität der Daten wirklich verloren. Die Schreibleistung leidet durch den Kopiervorgang im Vergleich zu einer normalen physischen Festplatte ein wenig (10 bis 20 % langsamer), dafür ist der Lesezugriff deutlich schneller, weil die Daten doppelt vorhanden sind und somit parallel ausgelesen werden können. Im Allgemeinen kann gesagt werden, dass RAID 1 fast

eine doppelt so schnelle Transaktionsrate und nahezu dieselbe Schreibgeschwindigkeit wie einzelne Festplatten bieten.

RAID 2 und RAID 3

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

RAID 4

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

RAID 5

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

Weitere RAID-Level

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

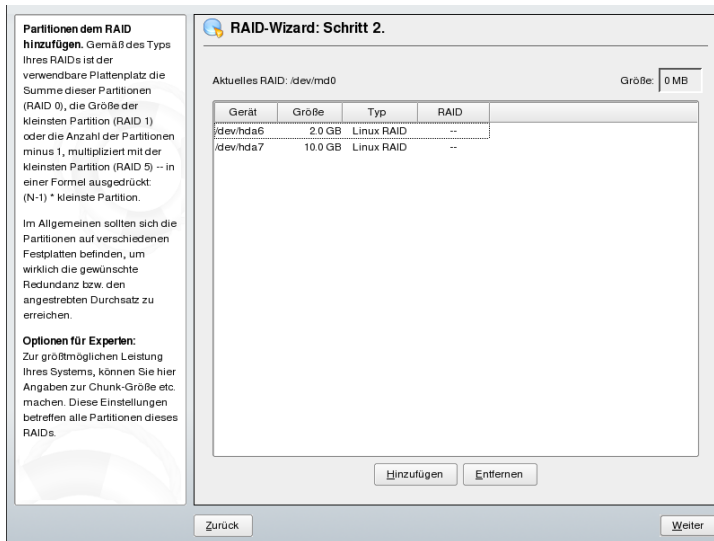
6.2.2 Soft-RAID-Konfiguration mit YaST

Zur Soft-RAID-Konfiguration gelangen Sie über den YaST-Expertenmodus des Partitionierungsmoduls, der in [Abschnitt 7.5.8, „Partitionierung“](#) (S. 176) 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 *Anlegen* → *Nicht formatieren* klicken und anschließend *0xFD Linux RAID* als Partitions-ID wählen. Für RAID 0 und RAID 1 sind mindestens zwei Partitionen erforderlich, für RAID 1 in der Regel exakt zwei. Für RAID 5 sind mindestens drei Partitionen erforderlich. Es wird empfohlen, nur Partitionen gleicher Größe zu verwenden. Die einzelnen Partitionen eines RAIDs sollten auf verschiedenen Festplatten liegen, damit das Risiko eines Datenverlusts durch den Defekt einer Festplatte (bei RAID 1 und 5) verhindert bzw. die Leistung bei RAID 0 optimiert wird. Wenn Sie alle gewünschten Partitionen erstellt haben, klicken Sie auf *RAID* → *RAID anlegen*, um die RAID-Konfiguration zu starten.

Wählen Sie im nächsten Dialogfeld zwischen RAID-Level 0, 1 und 5 (weitere Informationen hierzu finden Sie in [Abschnitt 6.2.1, „RAID-Level“](#) (S. 143)). Wenn Sie auf *Weiter* klicken, werden im folgenden Dialogfeld alle Partitionen entweder mit dem Typ „Linux RAID“ oder „Linux native“ angezeigt (siehe [Abbildung 6.6, „RAID-Partitionen“](#) (S. 145)). 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.

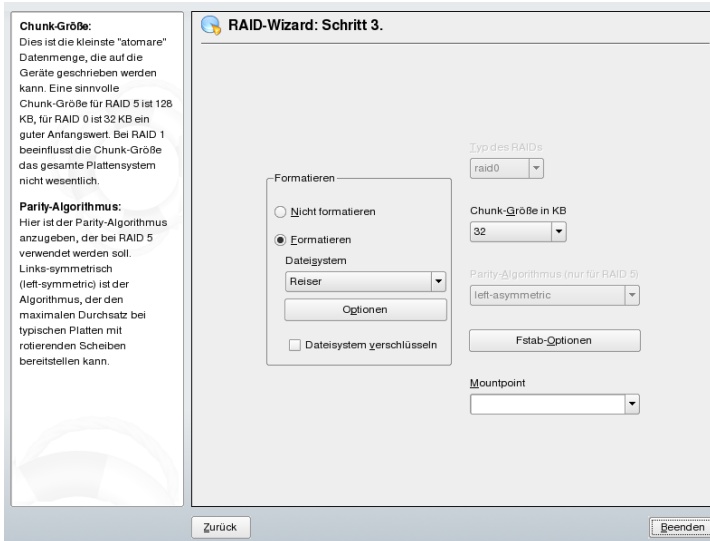
Abbildung 6.6 RAID-Partitionen



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 6.7](#), „Dateisystemeinstellungen“ (S. 146)).

Abbildung 6.7 Dateisystemeinstellungen



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

6.2.3 Fehlerbehebung

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.

6.2.4 Weitere Informationen

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

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

Linux-RAID-Mailinglisten sind beispielsweise unter folgender URL verfügbar:

<http://marc.theaimsgroup.com/?l=linux-raid&r=1&w=2>.

Systemkonfiguration mit YaST

In SUSE Linux Enterprise Server übernimmt YaST die Installation und Konfiguration Ihres Systems. In diesem Kapitel wird die Konfiguration der Systemkomponenten (Hardware), des Netzwerkzugriffs, der Sicherheitseinstellungen und der Benutzerverwaltung beschrieben. Eine kurze Einführung zur textbasierten YaST-Bedienoberfläche finden Sie unter [Abschnitt 7.11, „YaST im Textmodus“](#) (S. 202). Eine Beschreibung der manuellen Systemkonfiguration finden Sie unter [Abschnitt 20.3, „Systemkonfiguration über /etc/sysconfig“](#) (S. 433).

Konfigurieren Sie das System mit YaST unter Verwendung verschiedener YaST-Module. Je nach Hardware-Plattform und installierter Software gibt es verschiedene Möglichkeiten für den Zugriff auf YaST im installierten System.

In KDE oder GNOME starten Sie das YaST-Kontrollzentrum über das Hauptmenü. Außerdem sind die einzelnen YaST-Konfigurationsmodule im KDE-Kontrollzentrum integriert. Vor dem Start von YaST werden Sie zur Eingabe eines `root`-Passworts aufgefordert, da YaST zur Änderung der Systemdateien Systemadministratorberechtigungen benötigt.

Um YaST über die Kommandozeile zu starten, geben Sie die Befehle `su` (zum Wechsel zum Benutzer `root`) und `yast2` ein. Um die Textversion zu starten, geben Sie statt `yast2` den Befehl `yast` ein. Mit `yast` können Sie das Programm außerdem von einer der virtuellen Konsolen starten.

Bei Hardware-Plattformen, die kein eigenes Anzeigegerät unterstützen, und zur entfernten Verwaltung auf anderen Hosts führen Sie YaST auf einem entfernten Host aus. Öffnen Sie zuerst eine Konsole auf dem Host, auf dem YaST angezeigt werden soll, und geben Sie den Befehl

`ssh -X root@<zu-konfigurierendes-System>` ein, um sich bei dem zu konfigurierenden System als `root` anzumelden und die X-Server-Ausgabe auf Ihr Terminal umzuleiten. Geben Sie nach der erfolgreichen SSH-Anmeldung `yast2` ein, um YaST im Grafikmodus zu starten.

Um YaST auf einem anderen System im Textmodus zu starten, öffnen Sie die Verbindung mit `ssh root@<zu-konfigurierendes-System>`. Starten Sie anschließend YaST mit `yast`.

Um Zeit zu sparen können die einzelnen YaST-Module direkt gestartet werden. Zum Starten eines Moduls geben Sie `yast2 Modulname` ein. Eine Liste aller auf Ihrem System verfügbaren Modulnamen können Sie mit `yast2 -l` oder `yast2 --list` anzeigen. Das Netzwerkmodul beispielsweise wird mit `yast2 lan` gestartet.

7.1 YaST-Sprache

Um die Sprache von YaST zu ändern, wählen Sie im YaST-Kontrollzentrum *System* → *Sprachauswahl*. Wählen Sie die gewünschte Sprache aus, beenden Sie das YaST-Kontrollzentrum, melden Sie sich beim System ab und anschließend erneut wieder an. Beim nächsten Start von YaST wird die neue Spracheinstellung verwendet. Außerdem wird dadurch die Sprache für das gesamte System geändert.

Wenn Sie in einer anderen Sprache arbeiten müssen, jedoch nicht die Spracheinstellung für das System ändern möchten, können Sie die Variable `LANG` vorübergehend ändern. Exportieren Sie dazu `LANG` mit der gewünschten Sprache. Verwenden Sie beispielsweise für Deutsch den Befehl:

```
export LANG="en_US"; yast2
```

Mit diesem Befehl wird die Einstellung für `LANG` nur für die aktuelle Sitzung geändert. Die Spracheinstellung für andere Benutzer und andere Sitzungen, wie beispielsweise Terminalfenster, bleibt unverändert.

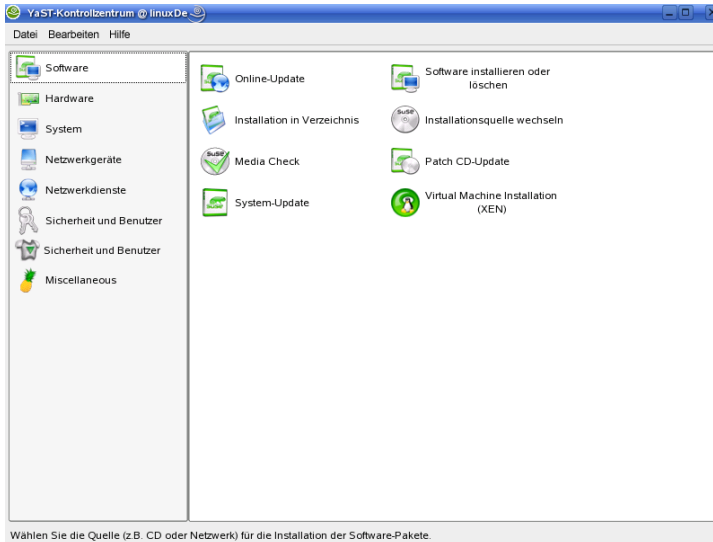
Wenn Sie YaST über SSH entfernt ausführen, verwendet YaST die Spracheinstellungen des lokalen Systems.

7.2 Das YaST-Kontrollzentrum

Wenn Sie YaST im Grafikmodus starten, öffnet sich das YaST-Kontrollzentrum, wie in [Abbildung 7.1](#), „Das YaST-Kontrollzentrum“ (S. 151) gezeigt. Der linke Rahmen enthält die verfügbaren Kategorien. Wenn Sie auf eine Kategorie klicken, wird ihr Inhalt im rechten Rahmen angezeigt. Wählen Sie anschließend das gewünschte Modul aus. Wenn Sie beispielsweise *Hardware* auswählen und im rechten Rahmen auf *Sound* klicken, wird ein Konfigurationsdialogfeld für die Soundkarte geöffnet. Die Konfiguration der einzelnen Elemente besteht in der Regel aus mehreren Schritten. Mit *Weiter* wechseln Sie zum nächsten Schritt.

Bei den meisten Modulen wird im linken Rahmen ein Hilfetext angezeigt, der Vorschläge für die Konfiguration bietet und die erforderlichen Einträge erläutert. Um Hilfe für Module ohne Hilferahmen zu erhalten, drücken Sie **F1** oder wählen Sie die Option *Hilfe*. Nach der Auswahl der gewünschten Einstellungen schließen Sie den Vorgang auf der letzten Seite des Konfigurationsdialogfelds mit *Übernehmen* ab. Die Konfiguration wird dann gespeichert.

Abbildung 7.1 Das YaST-Kontrollzentrum

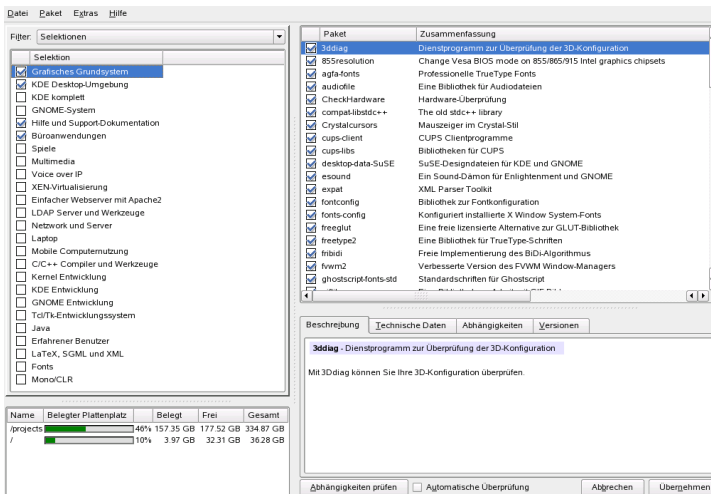


7.3 Software

7.3.1 Installieren und Entfernen von Software

Verwenden Sie zum Installieren, Deinstallieren und Aktualisieren von Software auf Ihrem Computer die Option *Software* → *Software installieren oder löschen*. Dadurch wird ein Paket-Manager-Dialogfeld geöffnet, wie in [Abbildung 7.2](#), „YaST-Paket-Manager“ (S. 152) gezeigt.

Abbildung 7.2 YaST-Paket-Manager



Bei SUSE® Linux Enterprise ist Software in Form von RPM-Paketen erhältlich. Normalerweise enthält ein Paket alles, was für ein Programm benötigt wird: das Programm selbst, die Konfigurationsdateien und alle Dokumentationen. Eine Liste der einzelnen Pakete wird rechts im Einzelpaketfenster angezeigt. Der Inhalt dieser Liste wird durch den aktuell ausgewählten Filter bestimmt. Wenn beispielsweise der Filter *Schemata* ausgewählt wurde, werden im Einzelpaketfenster alle Pakete der aktuellen Auswahl angezeigt.

Im Paket-Manager weist jedes Paket einen Status auf, der bestimmt, was mit dem Paket geschehen soll, beispielsweise „Installieren“ oder „Löschen“. Dieser Status wird durch

ein Symbol in einem Statusfeld am Anfang der Zeile angezeigt. Sie können den Status durch Klicken ändern oder indem Sie den gewünschten Status aus dem Menü auswählen, das sich öffnet, wenn mit der rechten Maustaste auf das Element geklickt wird. Je nach der aktuellen Situation stehen einige der möglichen Status-Flaggen eventuell nicht zur Auswahl zur Verfügung. So kann beispielsweise ein Paket, das noch nicht installiert wurde, nicht auf „Löschen“ gesetzt werden. Mit *Hilfe* → *Symbole* können Sie die verfügbaren Status-Flaggen anzeigen.

Die für die verschiedenen Pakete im Einzelpaketfenster verwendeten Schriftfarben bieten zusätzliche Informationen. Installierte Pakete, für die eine neuere Version auf den Installationsmedien verfügbar ist, werden in blauer Farbe angezeigt. Installierte Pakete, deren Versionsnummern höher sind als die auf den Installationsmedien, werden in roter Farbe angezeigt. Da die Versionsnummern für Pakete nicht immer in linear aufsteigender Reihenfolge vergeben werden, sind diese Informationen nicht immer perfekt. Sie sollten jedoch ausreichen, um problematische Pakete anzuzeigen. Falls erforderlich, überprüfen Sie die Versionsnummern.

Installieren von Paketen

Zur Installation von Paketen wählen Sie die gewünschten Pakete aus und klicken Sie auf *Übernehmen*. Die ausgewählten Pakete sollten das Statussymbol *Installation* aufweisen. Der Paket-Manager überprüft automatisch die Abhängigkeiten und wählt gegebenenfalls alle anderen erforderlichen Pakete aus (Auflösung von Abhängigkeiten). Um andere Pakete anzuzeigen, die für die Installation benötigt werden, wählen Sie vor dem Klicken auf *Übernehmen* im Hauptmenü die Optionsfolge *Extras* → *Automatische Paketänderungen anzeigen*. Fahren Sie nach der Installation der Pakete mit Ihrer Arbeit im Paket-Manager fort, indem Sie auf *Weitere installieren* klicken, oder schließen Sie den Paket-Manager mithilfe von *Beenden*.

Der Paket-Manager zeigt vorausgewählte Gruppen für die Installation an. Sie können statt einzelner Pakete eine ganze Gruppe auswählen. Verwenden Sie zur Anzeige dieser Gruppe die Option *Filter* im linken Rahmen.

TIPP: Liste aller verfügbaren Pakete

Um alle Pakete auf Ihrem Installationsmedium anzuzeigen, verwenden Sie den Filter *Paketgruppen* und wählen unten in der Struktur die Option *zzz All* aus. SUSE Linux Enterprise enthält eine Vielzahl von Paketen, und es kann einige Zeit dauern, bis diese lange Liste angezeigt werden kann.

Der Filter Schemata gruppiert die Programmpakete nach ihrem Anwendungszweck, beispielsweise Multimedia- oder Büroanwendungen. Die verschiedenen Gruppen des Filters Schemata sind zusammen mit den vorausgewählten installierten Paketen aufgelistet. Klicken Sie auf das Statusfeld am Anfang einer Zeile, um das betreffende Schema zu installieren bzw. deinstallieren. Wählen Sie direkt einen Status aus, indem Sie mit der rechten Maustaste auf das Schema klicken und dann das Kontextmenü verwenden. Im Überblick über die einzelnen Pakete auf der rechten Seite, in dem die im aktuellen Schema eingeschlossenen Pakete angezeigt werden, können Sie einzelne Pakete auswählen bzw. ihre Auswahl aufheben.

Um sprachspezifische Pakete zu finden, beispielsweise übersetzte Texte für die Bedienoberfläche von Programmen, Dokumentation und Schriftarten, verwenden Sie den Filter *Sprache*. In diesem Filter wird eine Liste aller Sprachen angezeigt, die von SUSE Linux Enterprise unterstützt werden. Wenn Sie eine davon auswählen, werden im rechten Rahmen alle Pakete angezeigt, die für diese Sprache verfügbar sind. Von diesen Paketen werden alle, die Ihre derzeitige Software-Auswahl betreffen, automatisch mit einem Tag für die Installation versehen.

ANMERKUNG

Da sprachspezifische Pakete von anderen Paketen abhängen können, wählt der Paket-Manager möglicherweise zusätzliche Pakete für die Installation aus.

Pakete und Installationsquellen

Wenn Sie nur Pakete aus der angegebenen Quelle finden möchten, verwenden Sie den Filter *Installationsquellen*. In der Standardkonfiguration zeigt dieser Filter eine Liste aller Pakete in der ausgewählten Quelle an. Verwenden Sie einen Sekundärfilter, um die Liste einzuschränken.

Um eine Liste aller installierten Pakete aus der ausgewählten Installationsquelle anzuzeigen, wählen Sie unter *Sekundärfilter* den Filter *Installationsquellen* und anschließend *Installationsüberblick* aus und deaktivieren Sie alle Kontrollkästchen mit Ausnahme von *Beibehalten*.

Der Paketstatus im Einzelpaketfenster kann wie gewöhnlich geändert werden. Es ist jedoch möglich, dass das geänderte Paket nicht mehr den Suchkriterien entspricht. Um solche Pakete aus der Liste zu entfernen, aktualisieren Sie die Liste mit *Aktualisierungsliste*.

Installation von Quellpaketen

Normalerweise ist ein Paket mit den Quelldateien für das Programm verfügbar. Die Quellen sind für die Ausführung des Programms nicht erforderlich, können jedoch installiert werden, um eine angepasste Version des Programms zu kompilieren.

Um Quellen für das ausgewählte Programm zu installieren, aktivieren Sie das Kontrollkästchen in der Spalte *Quelle*. Wenn kein Kontrollkästchen angezeigt wird, ist die Quelle für das Paket nicht in Ihren Installationsquellen vorhanden.

Entfernen von Paketen

Um Pakete zu entfernen, weisen Sie den betreffenden Paketen den richtigen Status zu und klicken Sie auf *Übernehmen*. Die ausgewählten Pakete sollten den Status *Löschen* aufweisen. Wenn ein Paket zum Löschen ausgewählt wurde, das von anderen Installationspaketen benötigt wird, gibt der Paket-Manager eine Warnmeldung mit detaillierten Informationen und alternativen Lösungen aus.

Erneutes Installieren von Paketen

Wenn Sie beschädigte Dateien finden, die zum Paket gehören, oder wenn Sie die ursprüngliche Version eines Pakets erneut vom Installationsdatenträger installieren möchten, müssen Sie das Paket neu installieren. Zur erneuten Installation von Paketen wählen Sie die gewünschten Pakete aus und klicken Sie auf *Übernehmen*. Die ausgewählten Pakete sollten den Status *Update* (Update) aufweisen. Sollten Abhängigkeitsprobleme bei installierten Paketen auftreten, gibt der Paket-Manager eine Warnmeldung mit detaillierten Informationen und alternativen Lösungen aus.

Suche nach Paketen, Anwendungen und Dateien

Wenn Sie ein bestimmtes Paket suchen, verwenden Sie den Filter *Suche*. Geben Sie eine Suchzeichenkette ein und klicken Sie auf *Suche*. Durch Eingabe verschiedener Suchkriterien kann die Suche soweit eingegrenzt werden, dass nur einige wenige Pakete angezeigt werden oder sogar nur ein einziges Paket angezeigt wird. Außerdem können Sie im *Suchmodus* mithilfe von Platzhaltern und regulären Ausdrücken spezielle Suchschemata definieren.

TIPP: Schnellsuche

Neben dem Filter *Suche* bieten alle Listen des Paket-Managers eine Schnellsuche. Geben Sie einfach einen Buchstaben ein, um den Cursor zum ersten Paket in der Liste zu steuern, dessen Name mit dem betreffenden Buchstaben beginnt. Der Cursor muss sich in der Liste befinden (durch Klicken auf die Liste).

Um ein Paket anhand seines Namens zu suchen, wählen Sie *Name*, geben Sie den Namen des gewünschten Pakets im Suchfeld ein und klicken Sie auf *Suche*. Um ein Paket anhand des Texts in der Beschreibung zu suchen, wählen Sie *Zusammenfassung* und *Beschreibung*, geben Sie eine Suchzeichenkette ein und klicken Sie auf *Suche*.

Um nach dem Paket zu suchen, das eine bestimmte Datei enthält, geben Sie den Namen der Datei ein, wählen Sie *RPM "Provides"* (RPM "Beinhaltet") und klicken Sie auf *Suche*. Um alle Pakete zu finden, die von einem bestimmten Paket abhängen, wählen Sie *RPM "Requires"* (RPM "Benötigt"), geben Sie den Namen des Pakets ein und klicken Sie auf *Suche*.

Wenn Sie mit der Paketstruktur von SUSE Linux Enterprise vertraut sind, können Sie mithilfe des Filters *Paketgruppen* Pakete anhand des Betreffs suchen. Dieser Filter führt zu einer thematischen Sortierung der Programmpakete (z. B. nach Anwendungen, Entwicklung und Hardware) in einer Baumstruktur auf der linken Seite. Je stärker Sie die Zweige erweitern, desto spezifischer ist die Auswahl. Es werden also weniger Pakete im Einzelpaketfenster angezeigt.

Installationsüberblick

Nach Auswahl der Pakete für Installation, Aktualisierung oder Löschung können Sie unter *Installationsüberblick* einen Überblick anzeigen lassen. Er zeigt, welche Auswirkungen das Klicken auf *Übernehmen* auf die Pakete hat. Mit den Kontrollkästchen auf der linken Seite können Sie die im Einzelpaketfenster anzuzeigenden Pakete filtern. Um beispielsweise zu überprüfen, welche Pakete bereits installiert sind, deaktivieren Sie alle Kontrollkästchen mit Ausnahme von *Behalten*.

Der Paketstatus im Einzelpaketfenster kann wie gewöhnlich geändert werden. Es ist jedoch möglich, dass das betreffende Paket nicht mehr den Suchkriterien entspricht. Um solche Pakete aus der Liste zu entfernen, aktualisieren Sie die Liste mit *Aktualisierungsliste*.

Informationen zu Paketen

Informationen zum ausgewählten Paket erhalten Sie über die Registerkarten im unteren rechten Rahmen. Wenn eine andere Version des Pakets verfügbar ist, erhalten Sie Informationen zu beiden Versionen.

Die Registerkarte *Beschreibung* mit der Beschreibung des ausgewählten Pakets ist automatisch aktiv. Um Informationen zu Paketgröße, Version, Installationsdatenträger und anderen technischen Details anzuzeigen, wählen Sie die Option *Technische Daten*. Informationen zu bereitgestellten und erforderlichen Dateien finden Sie unter *Abhängigkeiten*. Um die verfügbaren Versionen sowie die zugehörigen Installationsquellen anzuzeigen, klicken Sie auf *Versionen*.

Speicherplatzauslastung

Während der Auswahl der Software wird im Ressourcenfenster links unten im Modul die voraussichtliche Speicherplatzauslastung aller eingehängten Dateisysteme angezeigt. Das farbige Balkendiagramm wächst mit jeder Auswahl. Solange es grün ist, ist genügend Speicherplatz vorhanden. Die Balkenfarbe ändert sich langsam zu rot, je mehr die Speicherkapazität des Datenträgers ausgelastet ist. Wenn Sie zu viele Pakete für die Installation auswählen, wird eine Warnmeldung angezeigt.

Überprüfen der Abhängigkeiten

Einige Pakete sind von anderen Paketen abhängig. Das bedeutet, dass die Software des Pakets nur dann ordnungsgemäß funktioniert, wenn ein weiteres Paket ebenfalls installiert wird. Einige Pakete weisen identische oder ähnliche Funktionen auf. Wenn diese Pakete dieselbe Systemressource verwenden, ist eine gleichzeitige Installation nicht ratsam (Paketkonflikt).

Beim Start des Paket-Managers wird das System untersucht und die installierten Pakete werden angezeigt. Wenn Sie auswählen, dass weitere Pakete installiert bzw. entfernt werden sollen, überprüft der Paket-Manager automatisch die Abhängigkeiten und wählt gegebenenfalls alle anderen erforderlichen Pakete aus (Auflösung von Abhängigkeiten). Wenn Sie in Konflikt stehende Pakete auswählen bzw. deren Auswahl aufheben, wird dies vom Paket-Manager angezeigt und es werden Vorschläge zur Lösung des Problems (Auflösung von Konflikten) übermittelt.

Abhängigkeiten prüfen und *Automatische Überprüfung* finden Sie unter dem Informationsfenster. Wenn Sie auf *Abhängigkeiten prüfen* klicken, überprüft der Paket-Manager, ob die aktuelle Paketauswahl zu nicht aufgelösten Paketabhängigkeiten oder Konflikten führt. Bei nicht aufgelösten Abhängigkeiten werden die erforderlichen zusätzlichen Pakete automatisch ausgewählt. Bei Paketkonflikten öffnet der Paket-Manager ein Dialogfeld, in dem der Konflikt angezeigt wird und verschiedene Optionen zur Lösung des Problems angeboten werden.

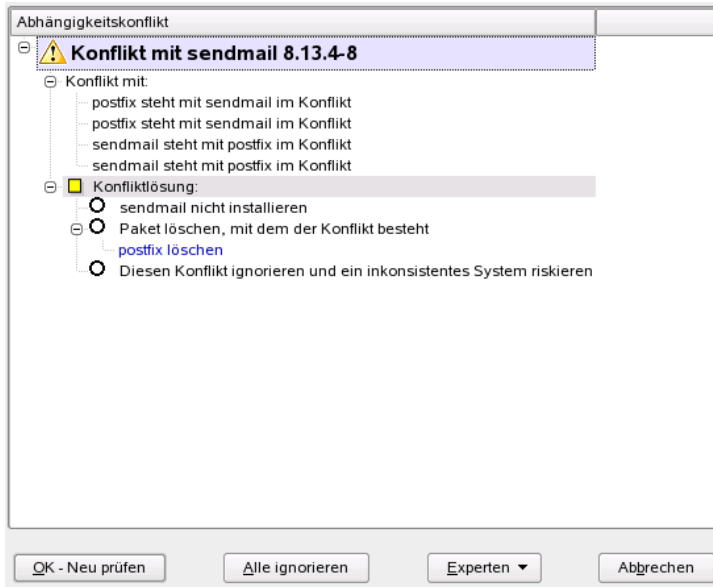
Wenn Sie *Automatische Überprüfung* aktivieren, löst jede Änderung eines Paketstatus eine automatische Überprüfung aus. Diese Funktion ist sehr nützlich, da die Konsistenz der Paketauswahl permanent überwacht wird. Der Vorgang verbraucht jedoch Ressourcen und kann den Paket-Manager verlangsamen. Aus diesem Grund ist die automatische Überprüfung standardmäßig nicht aktiviert. In jedem Fall wird eine Konsistenzprüfung durchgeführt, wenn Sie die Auswahl mit *Übernehmen* bestätigen.

Beispielsweise können `sendmail` und `postfix` nicht gleichzeitig installiert sein. [Abbildung 7.3](#), „Konfliktverwaltung des Paket-Managers“ (S. 159) zeigt die Konfliktmeldung, in der Sie aufgefordert werden, eine Entscheidung zu treffen. `postfix` ist bereits installiert. Sie können also auf die Installation von `sendmail` verzichten, `postfix` entfernen oder das Risiko eingehen und den Konflikt ignorieren.

WARNUNG: Umgang mit Paketkonflikten

Wenn Sie nicht ein besonders erfahrener Benutzer sind, sollten Sie beim Umgang mit Paketkonflikten die Vorschläge von YaST befolgen, da andernfalls die Stabilität und Funktionalität Ihres Systems durch den bestehenden Konflikt gefährdet werden könnten.

Abbildung 7.3 *Konfliktverwaltung des Paket-Managers*



Installieren von -devel-Paketen

Der Paket-Manager bietet Funktionen für eine schnelle und einfache Installation von devel- und debug-Paketen. Um alle devel-Pakete für das installierte System zu installieren, wählen Sie *Extras* → *Alle passenden -devel-Pakete installieren*. Um alle debug-Pakete für das installierte System zu installieren, wählen Sie *Extras* → *Alle passenden -debuginfo-Pakete installieren*.

7.3.2 Installieren von Add-On-Produkten

Add-On-Produkte sind Erweiterungen für Ihr System. Sie können ein Add-On-Produkt eines Drittanbieters oder eine spezielle Erweiterung für SUSE Linux Enterprise installieren, beispielsweise das SDK-Add-On oder eine CD mit Binärtreibern. Verwenden Sie zur Installation eines neuen Add-On die Option *Software* → *Add-On-Produkt*. Sie können verschiedene Typen von Produktmedien, wie eine CD, FTP oder ein lokales Verzeichnis, auswählen. Darüber hinaus können Sie direkt mit ISO-Dateien arbeiten. Wählen Sie zum Hinzufügen eines Add-On als ISO-Dateiemedium die Option *Lokales Verzeichnis* und dann *ISO-Images*.

Nachdem Sie das Add-On-Medium hinzugefügt haben, wird das Paket-Manager-Fenster angezeigt. Wenn das Add-On ein neues Schema enthält, sehen Sie das neue Element im Filter *Schemata*. Zum Anzeigen einer Liste aller Pakete in den ausgewählten Installationsquellen wählen Sie den Filter *Installationsquellen* und wählen Sie die Installationsquelle, die angezeigt werden soll. Zum Anzeigen von Paketen aus einem ausgewählten Add-On nach Paketgruppen wählen Sie den Sekundärfilter *Paketgruppen*.

Binärtreiber

Bestimmte Hardware erfordert für eine korrekte Funktion ausschließlich Binärtreiber. Wenn Sie über solche Hardware verfügen, suchen Sie in den Versionshinweisen Informationen zur Verfügbarkeit von Binärtreibern für Ihr System. Zum Lesen der Versionshinweise öffnen Sie YaST und wählen Sie *Verschiedenes* → *Versionshinweise*.

SUSE Software Development Kit (SDK) 10

Das SUSE Software Development Kit 10 ist ein Add-On für SUSE Linux Enterprise 10 und stellt einen vollständigen Werkzeugsatz für die Anwendungsentwicklung dar. In der Tat umfasst das SUSE Software Development Kit 10 zur Bereitstellung eines umfassenden Entwicklungssystems sämtliche Open-Source-Werkzeuge, die zur Erstellung des SUSE Linux Enterprise Server-Produkts verwendet wurden. Als Entwickler, unabhängiger Softwarehersteller (ISV) oder unabhängiger Hardwarehersteller (IHV) stehen Ihnen somit alle Werkzeuge zur Verfügung, die Sie zum Portieren von Anwendungen auf sämtliche Plattformen, die von SUSE Linux Enterprise Desktop und SUSE Linux Enterprise Server unterstützt werden, benötigen.

Darüber hinaus enthält das SUSE Software Development Kit integrierte Entwicklungsumgebungen (IDEs), Debugger, Code-Editoren und andere verwandte Werkzeuge. Es unterstützt die wichtigsten Programmiersprachen (einschl. C, C++, Java und die meisten Skriptsprachen) und umfasst mehrere Perl-Pakete, die nicht in SUSE Linux Enterprise enthalten sind.

Detaillierte Informationen finden Sie unter <http://developer.novell.com/ndk/susesdk.htm>. Verwenden Sie das YaST-Installationsprogramm für Add-Ons und den Paket-Manager, um das SUSE Software Development Kit 10 zu installieren.

7.3.3 Auswahl der Installationsquelle

Sie können mehrere Installationsquellen unterschiedlichen Typs verwenden. Wählen Sie sie aus und aktivieren Sie ihre Verwendung für die Installation bzw. Aktualisierung mithilfe von *Software* → *Installationsquelle*. Sie können beispielsweise das SUSE Software Development Kit als Installationsquelle angeben. Nach dem Start wird eine Liste aller zuvor registrierten Quellen angezeigt. Nach einer normalen Installation von CD wird nur die Installations-CD aufgelistet. Klicken Sie auf *Hinzufügen*, um weitere Quellen in diese Liste aufzunehmen. Bei den Quellen kann es sich um CDs, DVDs oder Netzwerkressourcen, wie NFS- und FTP-Server, handeln. Sogar Verzeichnisse auf der lokalen Festplatte können als Installationsmedium ausgewählt werden. Weitere Einzelheiten finden Sie im detaillierten YaST-Hilfetext.

Alle registrierten Quellen weisen in der ersten Spalte der Liste einen Aktivierungsstatus auf. Sie können einzelne Installationsquellen durch Klicken auf *Aktivieren/Deaktivieren* aktivieren bzw. deaktivieren. Während der Installation von Software-Paketen oder -Updates wählt YaST einen geeigneten Eintrag aus der Liste der aktivierten Installationsquellen aus. Wenn Sie das Modul mit *Schließen* beenden, werden die aktuellen Einstellungen gespeichert und auf die Konfigurationsmodule *Software Management* (Software-Management) und *System-Update* angewendet.

7.3.4 Online-Aktualisierung von Software

Wichtige Aktualisierungen und Verbesserungen können Sie mit YaST Online Update (YOU) installieren. Die aktuellen Patches für Ihr SUSE-Produkt sind in den SUSE-Katalogen verfügbar. Verwenden Sie zum Hinzufügen oder Entfernen von Katalogen das Modul *Software* → *Installationsquelle*, das unter [Abschnitt 7.3.3, „Auswahl der Installationsquelle“](#) (S. 161) beschrieben ist.

Die Liste der verfügbaren Patches befindet sich auf der linken Seite. Die Patches sind nach ihrer Bedeutung für die Sicherheit sortiert:

Sicherheit

Sie müssen diese Patches installieren. Wenn Sie die Patches nicht installieren, ist die Sicherheit ernsthaft gefährdet.

Empfohlen

Sie sollten diese Patches installieren, da Ihr Computer gefährdet sein könnte.

Optional

Sie können diese Patches installieren, Ihr Computer ist jedoch auch sicher, wenn Sie es nicht tun.

Wählen Sie zum Installieren von Patches ein Patch in der Liste aus und klicken Sie auf *Akzeptieren*. Die Auswahl mehrerer Patches ist zulässig. Zum Verwerfen der Änderungen klicken Sie auf *Abbrechen*.

Wenn Sie spezielle Einstellungen benötigen, beispielsweise wenn Ihr Computer sich hinter einem Proxyserver befindet, verwenden Sie das Kommandozeilenwerkzeug *rug*. Dies wird ausführlich in [Abschnitt 7.12](#), „Aktualisierung über die Kommandozeile“ (S. 206) beschrieben.

7.3.5 Automatische Online-Updates

Software → *Einrichten von Online-Updates* ermöglicht Ihnen die Planung automatischer Online-Updates. Aktivieren Sie zunächst die automatischen Online-Updates durch Auswahl von *Automatische Updates aktivieren* und legen Sie dann den Zeitpunkt für das Update fest. Wenn Sie jedoch volle Kontrolle über die installierten Patches behalten möchten, können Sie auch nur das Herunterladen der Patches planen und die Patches später manuell installieren. Aktivieren Sie *Only Download Patches* (Patches nur herunterladen), wenn Sie die Patches nur herunterladen möchten.

Bestimmte Patches erfordern weitere Aktionen. So erfordern beispielsweise Patches für den Kernel, dass der Computer neu gebootet wird. Informationen zu weiteren erforderlichen Aktionen finden Sie in den Vorinstallationsinformationen. Zur Verwendung automatischer Updates für normale Patches ohne Vorinstallationsinformationen aktivieren Sie *Skip Patches with Preinstall Information* (Patches mit Vorinstallationsinformationen übergehen). Beenden Sie das Dialogfeld mit *Beenden*.

7.3.6 Aktualisieren über eine Patch-CD

Über das Modul *Patch CD-Update* im Abschnitt *Software* werden Patches von einer CD installiert und nicht von einem FTP-Server. Der Vorteil besteht in einer wesentlich schnelleren Aktualisierung mit CD. Nach dem Einlegen der Patch-CD werden alle auf der CD befindlichen Patches im Dialogfeld angezeigt. Wählen Sie die für die Installation gewünschten Pakete aus der Liste der Patches aus. Das Modul gibt eine Fehlermeldung

aus, wenn keine Patch-CD vorhanden ist. Legen Sie die Patch-CD ein und starten Sie das Modul anschließend neu.

7.3.7 Aktualisieren des Systems

Aktualisieren Sie die auf Ihrem System installierte Version von SUSE Linux Enterprise mithilfe von *Software* → *System-Update*. Während des Betriebs können Sie nur Anwendungs-Software aktualisieren, nicht jedoch das Basissystem. Zur Aktualisierung des Basissystems müssen Sie den Computer von einem Installationsmedium, beispielsweise einer CD, booten. Bei der Auswahl des Installationsmodus in YaST müssen Sie *Update* auswählen.

Das Verfahren zur Systemaktualisierung weist Ähnlichkeiten zu einer Neuinstallation auf. Zunächst untersucht YaST das System, ermittelt eine geeignete Aktualisierungsstrategie und gibt die Ergebnisse in einem Vorschlagsdialogfeld aus. Klicken Sie auf *Ändern* bzw. auf die einzelnen Elemente, um Details zu ändern.

Optionen für das Update

Legen Sie die Aktualisierungsmethode für Ihr System fest. Es stehen zwei Optionen zur Verfügung.

Update mit Installation neuer Software und Funktionen gemäß der getroffenen Auswahl

Um das gesamte System auf die neuesten Software-Versionen zu aktualisieren, wählen Sie eine der vordefinierten Auswahlmöglichkeiten aus. Diese Auswahlmöglichkeiten stellen sicher, dass auch Pakete installiert werden, die vorher nicht vorhanden waren.

Nur installierte Pakete aktualisieren

Mit dieser Option werden nur Pakete aktualisiert, die bereits auf dem System vorhanden sind. Es werden keine neuen Funktionen installiert.

Außerdem können Sie mit *Obsolete Pakete löschen* Pakete entfernen, die in der neuen Version nicht vorhanden sind. Standardmäßig wird diese Option vorausgewählt, um zu verhindern, dass obsoletere Pakete unnötig Festplattenspeicher blockieren.

Pakete

Klicken Sie auf *Pakete*, um den Paket-Manager zu starten oder einzelne Pakete für die Aktualisierung auszuwählen bzw. ihre Auswahl aufzuheben. Etwaige Paketkonflikte sollten durch die Konsistenzprüfung behoben werden. Die Verwendung des Paket-Managers wird detailliert in [Abschnitt 7.3.1, „Installieren und Entfernen von Software“](#) (S. 152) beschrieben.

Sicherung

Während der Aktualisierung können die Konfigurationsdateien einiger Pakete durch die neue Version ersetzt werden. Da Sie möglicherweise einige der Dateien im aktuellen System bearbeitet haben, erstellt der Paket-Manager normalerweise Sicherungskopien der ersetzten Dateien. Mit diesem Dialogfeld können Sie den Umfang dieser Sicherungen bestimmen.

WICHTIG: Umfang der Sicherung

Diese Sicherung beinhaltet nicht die Software. Sie enthält nur die Konfigurationsdateien.

Sprache

Die primäre Sprache und andere aktuell installierte Sprachen im System werden hier aufgeführt. Ändern Sie diese Werte durch Klicken auf *Sprache* in der ausgewählten Konfiguration oder mithilfe von *Ändern* → *Sprache*. Sie können die Tastaturbelegung und die Zeitzone an die Region anpassen, in der die primäre Sprache gesprochen wird (optional). Weitere Informationen zur Sprachauswahl finden Sie in [Abschnitt 7.5.16, „Sprachauswahl“](#) (S. 184).

Wichtige Informationen zu Aktualisierungen

Die Systemaktualisierung ist ein sehr komplexes Verfahren. Für jedes Programmpaket muss YaST zuerst prüfen, welche Version auf dem Computer installiert ist, und dann ermitteln, welche Vorgänge ausgeführt werden müssen, um die alte Version korrekt durch die neue Version zu ersetzen. YaST versucht außerdem, alle persönlichen Einstellungen der installierten Pakete zu übernehmen.

In den meisten Fällen ersetzt YaST problemlos alte Versionen durch neue Versionen. Vor der Aktualisierung sollte jedoch eine Sicherungskopie des bestehenden Systems erstellt werden, um sicherzustellen, dass die bestehenden Konfigurationen bei der Aktualisierung nicht verloren gehen. Auf diese Weise können Konflikte nach Abschluss der Aktualisierung manuell behoben werden.

7.3.8 Installation in ein Verzeichnis

Mit diesem YaST-Modul können Sie Pakete in einem von Ihnen festgelegten Verzeichnis installieren. Sie können entscheiden, wo das Root-Verzeichnis liegen soll, wie Verzeichnisse benannt werden sollen und welche Art von System und Software installiert werden soll. Nach der Auswahl dieses Moduls ermittelt YaST die Systemeinstellungen und listet das Standardverzeichnis, die Installationsanweisungen und die zu installierende Software auf. Sie können diese Einstellungen durch Klicken auf *Ändern* bearbeiten. Alle Änderungen müssen durch Klicken auf *Übernehmen* bestätigt werden. Wenn Sie Änderungen vorgenommen haben, klicken Sie auf *Weiter*, bis Sie die Meldung erhalten, dass die Installation abgeschlossen ist. Beenden Sie das Dialogfeld mit *Beenden*.

7.3.9 Installation in ein Verzeichnis für Xen

Installieren Sie die Pakete in einem Verzeichnis für Xen mithilfe von *Software* → *Installation in einem Verzeichnis (Xen)*. Xen ist ein Virtual Machine Monitor (VMM) für x86-kompatible Computer, mit dem die Ausführung mehrerer Virtual Machines, jede mit eigenem Betriebssystem, auf einem einzelnen physischen System mit exzellenter Leistung möglich ist. Nach Start dieses Moduls ermittelt YaST die Systemeinstellungen und listet das Standardverzeichnis, die Installationsanweisungen und die zu installierende Software auf. Sie können die Standardwerte durch Klicken auf *Ändern* bearbeiten. Bestätigen Sie alle Änderungen durch Klicken auf *Übernehmen*. Wenn Sie alle gewünschten Änderungen vorgenommen haben, klicken Sie auf *Weiter*, bis Sie die Meldung erhalten, dass die Installation abgeschlossen ist. Beenden Sie das Dialogfeld mit *Beenden*. Detaillierte Informationen zu Xen finden Sie in [Kapitel 23, Virtual Machine Server](#) (S. 473).

7.3.10 Überprüfen von Medien

Wenn Probleme bei der Verwendung von SUSE Linux Enterprise-Installationsdatenträgern auftreten, können Sie die CDs bzw. DVDs mithilfe von *Software* → *Media-*

Überprüfung überprüfen. Medienprobleme treten mit höherer Wahrscheinlichkeit bei selbst gebrannten Medien auf. Um zu überprüfen, ob eine SUSE Linux Enterprise-CD oder -DVD fehlerfrei ist, legen Sie das Medium in das Laufwerk ein und führen Sie dieses Modul aus. Wenn Sie auf *Starten* klicken, überprüft YaST die MD5-Prüfsumme des Mediums. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen. Wenn Fehler gefunden werden, sollten Sie dieses Medium nicht für die Installation verwenden.

7.3.11 Registrieren von SUSE Linux Enterprise

Die Registrierung und Aktivierung Ihres Produkts ist eine Voraussetzung für den Erhalt von technischem Support und Produkt-Updates. Wenn Sie die Registrierung bei der Installation überprungen haben, können Sie sich später mithilfe des Moduls *Produktregistrierung* unter *Software* registrieren. Wenn Sie mit der Registrierung beginnen, müssen Sie Ihre Kontakt-E-Mail und den Registrierungsschlüssel bereithalten.

Wählen Sie unter *Für besseren Service aufnehmen*, ob Sie einen Teil der erforderlichen Informationen von Ihrem System beziehen möchten. Dies vereinfacht die Registrierung. Wenn Sie sehen möchten, was zur Registrierung Ihres Systems nötig ist oder mit Ihren Daten geschieht, verwenden Sie *Details*.

Zur Registrierung kann auch das Kommandozeilenwerkzeug `suse_register` verwendet werden. Eine Anleitung hierfür finden Sie unter `suse_register --help`.

Zur Registrierung Ihres Systems ohne Internetzugang von einem anderen Computer aus müssen Sie zuerst eine Registrierungs-URL abrufen. Zum Abrufen der URL führen Sie `suse_register` ohne Optionen in Ihrem neuen System aus. Kopieren Sie die URL in der Ausgabe von `suse_register` und geben Sie sie in das URL-Feld eines Browsers auf einem anderen Computer ein.

TIPP: Technischer Support

Weitere Informationen zum technischen Support finden Sie unter <http://www.novell.com/support/products/linuxenterpriseserver/>.

7.4 Hardware

Neue Hardware muss zunächst gemäß den Angaben des Herstellers installiert bzw. angeschlossen werden. Schalten Sie die externen Geräte ein und starten Sie das entsprechende YaST-Modul. Die meisten Geräte werden von YaST automatisch erkannt und die technischen Daten werden angezeigt. Wenn die automatische Erkennung nicht funktioniert, bietet YaST eine Liste mit Geräten (Modell, Hersteller usw.), aus der Sie das geeignete Gerät auswählen können. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Hardware.

WICHTIG: Modellbezeichnungen

Wenn Ihr Modell nicht in der Liste enthalten ist, versuchen Sie ein Modell mit einer ähnlichen Bezeichnung. In einigen Fällen muss das Modell jedoch genau übereinstimmen, da ähnliche Bezeichnungen nicht automatisch Kompatibilität bedeuten.

7.4.1 Infrarot-Gerät

Infrarotgeräte können mithilfe von *Hardware* → *Infrarot-Gerät* konfiguriert werden. Klicken Sie auf *IrDA starten*, um die Konfiguration zu starten. Hier können Sie *Port* und *Limit Baud Rate* (Baudratenlimit) konfigurieren.

7.4.2 Grafikkarte und Monitor

Grafikkarten und Monitore können Sie mithilfe von *Hardware* → *Grafikkarte und Monitor* konfigurieren. Dabei wird die SaX2-Schnittstelle (in [Abschnitt 7.13](#), „SaX2“ (S. 209) beschrieben) verwendet.

7.4.3 Drucker

Konfigurieren eines Druckers mithilfe von *Hardware* → *Drucker*. Wenn ein Drucker ordnungsgemäß an das System angeschlossen ist, sollte er automatisch erkannt werden. Detaillierte Anweisungen zum Konfigurieren von Druckern mithilfe von YaST finden Sie in [Abschnitt 24.4](#), „Konfigurieren des Druckers“ (S. 493).

7.4.4 Festplatten-Controller

Normalerweise wird der Festplatten-Controller Ihres Systems während der Installation konfiguriert. Wenn Sie Controller hinzufügen, müssen Sie diese mithilfe von *Hardware* → *Festplatten-Controller* in das System integrieren. Außerdem können Sie die bestehende Konfiguration bearbeiten. Dies ist jedoch in der Regel nicht notwendig.

Das Dialogfeld gibt eine Liste der erkannten Festplatten-Controller an und aktiviert die Zuweisung des geeigneten Kernel-Moduls mit bestimmten Parametern. Mit *Laden des Moduls testen* können Sie überprüfen, ob die aktuellen Einstellungen funktionieren, bevor sie dauerhaft im System gespeichert werden.

WARNUNG: Konfiguration des Festplatten-Controllers

Es empfiehlt sich, die Einstellungen vor der dauerhaften Übernahme in das System zu testen. Falsche Einstellungen können verhindern, dass das System gebootet wird.

7.4.5 Hardware-Informationen

Die ermittelte Hardware und technische Daten können Sie mithilfe von *Hardware* → *Hardware-Information* anzeigen. Klicken Sie auf einen beliebigen Knoten im Baum, um weitere Informationen zu einem Gerät zu erhalten. Dieses Modul ist beispielsweise dann besonders nützlich, wenn Sie eine Supportanforderung übermitteln, für die Angaben zur verwendeten Hardware erforderlich sind.

Die angezeigten Hardware-Informationen können Sie mithilfe von *In Datei speichern* in eine Datei speichern. Wählen Sie das gewünschte Verzeichnis und den gewünschten Dateinamen aus und klicken Sie auf *Speichern*, um die Datei zu erstellen.

7.4.6 IDE DMA-Modus

Mithilfe von *Hardware* → *IDE DMA-Modus* können Sie den DMA-Modus für Ihre IDE-Festplatten und die IDE-CD- und DVD-Laufwerke im installierten System aktivieren bzw. deaktivieren. Dieses Modul wirkt sich nicht auf SCSI-Laufwerke aus. Durch DMA-Modi kann die Leistungsfähigkeit und die Datenübertragungsgeschwindigkeit in Ihrem System enorm erhöht werden.

Während der Installation aktiviert der aktuelle SUSE Linux Enterprise-Kernel automatisch DMA für Festplatten, nicht jedoch für CD-Laufwerke, da eine standardmäßige DMA-Aktivierung für alle Laufwerke häufig zu Problemen mit den CD-Laufwerken führt. Mit dem DMA-Modul können Sie DMA für Ihre Laufwerke aktivieren. Wenn der Treiber den DMA-Modus ohne Probleme unterstützt, lässt sich die Datenübertragungsrate des Laufwerks durch Aktivieren von DMA erhöhen.

ANMERKUNG

DMA (Direct Memory Access, direkter Speicherzugriff) bedeutet, dass die Daten unter Umgehung der Prozessorsteuerung direkt in den RAM-Speicher übertragen werden können.

7.4.7 Joystick

Mithilfe von *Hardware* → *Joystick* können Sie einen an die Soundkarte angeschlossenen Joystick konfigurieren. Wählen Sie in der angegebenen Liste den gewünschten Joysticktyp aus. Wenn Ihr Joystick nicht aufgeführt ist, wählen Sie *Generischer analoger Joystick*. Überprüfen Sie nach der Auswahl Ihres Joysticks, ob dieser angeschlossen ist, und klicken Sie dann auf *Test*, um die Funktionsfähigkeit zu testen. Klicken Sie auf *Weiter* und YaST installiert die erforderlichen Dateien. Wenn das Fenster *Joystick-Test* angezeigt wird, testen Sie den Joystick, indem Sie ihn in alle Richtungen bewegen und auf alle Knöpfe drücken. Jede Bewegung sollte im Fenster angezeigt werden. Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie auf *OK*, um zum Modul zurückzukehren, und auf *Beenden*, um die Konfiguration abzuschließen.

Bei Verwendung eines USB-Geräts ist diese Konfiguration nicht erforderlich. Sie können den Joystick einfach einstecken und sofort verwenden.

7.4.8 Tastaturbelegung

Um die Tastatur für die Konsole zu konfigurieren, führen Sie YaST im Textmodus aus und verwenden Sie anschließend *Hardware* → *Tastaturbelegung*. Nach dem Klicken auf das Modul wird das aktuelle Layout angezeigt. Wenn Sie eine andere Tastaturbelegung wünschen, wählen Sie die gewünschte Belegung aus der angegebenen Liste aus. Sie können die Belegung unter *Test* überprüfen, indem Sie auf der Tastatur auf verschiedene Tasten drücken.

Eine Feineinstellung ist durch Klicken auf *Einstellungen für Experten* möglich. Sie können die Tastenwiederholungsrate und die Anschlagverzögerung anpassen und den Startzustand konfigurieren, indem Sie die gewünschten Einstellungen unter *Zustände bei Start* vornehmen. Geben Sie unter *Geräte für Sperre* eine durch Leerzeichen getrennte Liste der Geräte ein, für die die Einstellungen für `Scroll Lock`, `Num Lock` und `Caps Lock` gelten sollen. Schließen Sie die Feineinstellung durch Klicken auf *OK*, um die Feineinstellung abzuschließen. Wenn Sie alle gewünschten Einstellungen ausgewählt haben, klicken Sie auf *Übernehmen*, um Ihre Änderungen wirksam werden zu lassen.

Um die Tastatur für die grafische Umgebung einzurichten, führen Sie die grafische Version von YaST aus und wählen Sie anschließend *Tastaturbelegung*. Informationen zur grafischen Konfiguration finden Sie in [Abschnitt 7.13.3, „Tastatureigenschaften“](#) (S. 215).

7.4.9 Mausmodell

Wenn Sie die Maus für die grafische Umgebung konfigurieren, können Sie durch Klicken auf *Mausmodell* auf die SaX2-Mauskonfiguration zugreifen. Einzelheiten finden Sie unter [Abschnitt 7.13.2, „Mauseigenschaften“](#) (S. 214).

Wenn Sie die Maus für die Textumgebung konfigurieren möchten, verwenden Sie YaST im Textmodus. Nach Eingabe des Textmodus und Auswahl von *Hardware* → *Mausmodell* können Sie mit den Pfeiltasten der Tastatur die verwendete Maus aus der angegebenen Liste auswählen. Klicken Sie anschließend auf *Übernehmen*, um die Einstellungen zu speichern und das Modul zu beenden.

7.4.10 Audio

Mit *Hardware* → *Sound* können Sie eine Soundkarte konfigurieren. Die meisten Soundkarten werden automatisch erkannt und aufgelistet. Wählen Sie die zu konfigurierenden bzw. zu ändernde Soundkarte aus und klicken Sie auf *Bearbeiten*. Mit *Löschen* können Sie eine Soundkarte entfernen. Dadurch werden bestehende Einträge konfigurierter Soundkarten in `/etc/modprobe.d/sound` deaktiviert.

Klicken Sie auf *Andere*, um ein Dialogfeld zu öffnen, in dem Sie die Optionen des Soundmoduls manuell anpassen können. Mithilfe von *Hinzufügen* können Sie weitere Soundkarten konfigurieren. Wenn YaST eine weitere Soundkarte erkennt, wählen Sie sie aus und fahren Sie mit *Bearbeiten* fort.

Lautstärke und Konfiguration aller installierten Soundkarten werden beim Klicken auf *Beenden* gespeichert. Die Mixer-Einstellungen werden in der Datei `/etc/asound.conf` gespeichert und die ALSA-Konfigurationsdaten werden am Ende der Dateien `/etc/modprobe.d/sound` und `/etc/sysconfig/hardware` angehängt.

Wenn YaST Ihre Soundkarte nicht automatisch erkennt, gehen Sie folgendermaßen vor:

- 1** Klicken Sie auf *Hinzufügen*, um ein Dialogfeld zu öffnen, in dem Sie Hersteller und Modell der Soundkarte auswählen können. Die erforderlichen Informationen finden Sie in der Dokumentation zu Ihrer Soundkarte. Eine Referenzliste der von ALSA unterstützten Soundkarten mit ihren zugehörigen Soundmodulen finden Sie in der Datei `/usr/share/doc/packages/alsa/cards.txt` und unter <http://www.alsa-project.org/~goemon/>. Treffen Sie Ihre Auswahl und klicken Sie dann auf *Weiter*.
- 2** Wählen Sie im *Setup-Dialogfeld* die Konfigurationsstufe im ersten Setup-Bildschirm aus. Bei *Schnelles automatisches Setup* müssen Sie keine weiteren Konfigurationsschritte ausführen. Außerdem findet kein Soundtest statt. Die Soundkarte wird automatisch konfiguriert. Mit *Normales Setup* können Sie die Ausgabelautstärke anpassen und einen Testklang abspielen. Mit *Erweitertes Setup mit der Möglichkeit, Optionen zu ändern* können Sie die Soundkartenoptionen manuell anpassen.

In diesem Dialogfeld finden Sie auch eine Verknüpfung zur Joystick-Konfiguration. Klicken Sie darauf und wählen Sie im folgenden Dialogfeld den Joysticktyp aus. Klicken Sie auf *Weiter*.

- 3** Unter *Soundkartenlautstärke* können Sie die Soundkonfiguration testen und die Lautstärke anpassen. Sie sollten bei ungefähr 10 Prozent beginnen, um eine Beschädigung der Lautsprecher und Hörschäden zu vermeiden. Beim Klicken *Test* sollte ein Testklang hörbar sein. Wenn Sie nichts hören können, erhöhen Sie die Lautstärke. Schließen Sie die Soundkonfiguration mit *Fortsetzen* ab. Die Lautstärkeeinstellung wird gespeichert.

Bei Verwendung einer Soundkarte vom Typ `Creative Soundblaster Live` oder `AWE` können Sie mit *Soundfonts installieren* SF2-Soundfonts von der Original-CD-ROM des Soundblaster-Treibers auf Ihre Festplatte kopieren. Die Soundfonts werden im Verzeichnis `/usr/share/sfbank/creative/` gespeichert.

Für die Wiedergabe von MIDI-Dateien aktivieren Sie *Sequencer starten*. Auf diese Weise werden die Module für die Sequenzerunterstützung zusammen mit den Soundmodulen geladen.

7.4.11 IBM-System z: DASD-Geräte

Es gibt zwei Möglichkeiten zum Hinzufügen einer DASD-Festplatte zum installierten System:

YaST

Verwenden Sie das YaST DASD-Modul (*Hardware* → *DASD*), um einem installierten System eine DASD-Festplatte hinzuzufügen. Wählen Sie im ersten Bildschirm die Festplatten aus, die für Ihre Linux-Installation verfügbar gemacht werden sollen, und klicken Sie auf *Aktion ausführen*. Wählen Sie *Aktivieren* und verlassen Sie dann das Dialogfeld mit *Weiter*.

Befehlszeile

Führen Sie den folgenden Befehl aus:

```
dasd_configure 0.0.0150 1 0
```

Ersetzen Sie *0.0.0150* durch die tatsächliche Nummer des Kanals, an den die DASD-Festplatte angeschlossen ist. Die letzte Null in der Kommandozeile sollte in eine 1 geändert werden, wenn der Zugriff auf die DASD-Festplatte im DIAG-Modus erfolgen soll.

ANMERKUNG

In beiden Fällen müssen Sie die Befehle

```
mkinitrd  
zipl
```

ausführen, um die Änderungen dauerhaft vorzunehmen.

7.4.12 IBM-System z: ZFCP

Verwenden Sie das YaST ZFCP-Modul (*Hardware* → *ZFCP*), um dem installierten System weitere per FCP angeschlossene SCSI-Geräte hinzuzufügen. Wählen Sie *Hinzufügen*, um ein weiteres Gerät hinzuzufügen. Wählen Sie die *Kanalnummer* (Adapter)

aus der Liste und geben Sie *WWPN* und *FCP-LUN* an. Schließen Sie die Einrichtung ab, indem Sie auf *Weiter* und *Schließen* klicken. Vergewissern Sie sich, dass das Gerät hinzugefügt wurde, indem Sie die Ausgabe des Befehls `cat /proc/scsi/scsi` prüfen.

ANMERKUNG

Führen Sie die folgenden Befehle aus, um die Änderungen durch einen Reboot dauerhaft vorzunehmen:

```
mkinitrd
zipl
```

7.5 System

Diese Gruppe von Modulen soll Sie bei der Verwaltung Ihres Systems unterstützen. Alle Module in dieser Gruppe sind systembezogen und tragen als wertvolle Werkzeuge dazu bei, dass das System ordnungsgemäß ausgeführt wird und die Daten effizient verwaltet werden.

TIPP: IBM-System z: Fortsetzung

Für IBM-System z fahren Sie mit [Abschnitt 7.5.4, „Konfiguration des Bootloaders“](#) (S. 175) fort.

7.5.1 Sicherung

Erstellen Sie mithilfe von *System* → *Sicherungskopie der Systembereiche* eine Sicherungskopie sowohl von Ihrem System als auch von Ihren Dateien. Die vom Modul erstellte Sicherung schließt jedoch nicht das gesamte System ein. Das System wird durch Speichern wichtiger Speicherbereiche auf der Festplatte gesichert, denen bei der Wiederherstellung eine entscheidende Bedeutung zukommt, beispielsweise Partitionstabelle oder MBR (Master Boot Record). Außerdem kann es die XML-Konfiguration beinhalten, die aus der Installation des für AutoYaST verwendeten Systems gewonnen wird. Die Sicherung der Daten erfolgt durch Speichern geänderter Dateien von Paketen, die auf Installationsdatenträgern zugänglich sind, von ganzen Paketen, auf die kein Zugriff möglich ist (z. B. Online-Updates) und von Dateien, die

nicht zu Paketen gehören, wie viele der Konfigurationsdateien in `/etc` oder die Verzeichnisse unter `/home`.

7.5.2 Wiederherstellung

Mit `System` → `System wiederherstellen` können Sie Ihr System aus einem mithilfe von `Sicherungskopie der Systembereiche` erstellten Backup-Archiv wiederherstellen. Geben Sie zunächst an, wo sich die Archive befinden (Wechselmedien, lokale Festplatten oder Netzwerkdateisysteme). Klicken Sie auf `Weiter`, um die Beschreibung und die Inhalte der einzelnen Archive anzuzeigen und auszuwählen, welche Elemente aus den Archiven wiederhergestellt werden sollen.

Außerdem können Sie Pakete deinstallieren, die seit der letzten Sicherung hinzugefügt wurden, und Pakete erneut installieren, die seit der letzten Sicherung gelöscht wurden. Mit diesen beiden Schritten können Sie genau den Zustand zum Zeitpunkt der letzten Sicherung wiederherstellen.

WARNUNG: Systemwiederherstellung

Da mit diesem Modul in der Regel viele Pakete und Dateien installiert, ersetzt oder deinstalliert werden, sollten Sie es nur verwenden, wenn Sie Erfahrungen mit Sicherungen haben. Anderenfalls kann Datenverlust auftreten.

7.5.3 Boot- und Rettungsdisketten

TIPP: IBM-System z: Systemreparatur

Das im folgenden Abschnitt beschriebene Verfahren gilt nicht für IBM System z-Plattformen.

Mithilfe von `System` → `Boot or Rescue Floppy` (Boot- oder Rettungsdiskette) können Boot- und Rettungsdisketten erstellt werden. Diese Disketten leisten gute Dienste, wenn die Bootkonfiguration Ihres Systems beschädigt ist. Die Rettungsdiskette ist besonders dann wichtig, wenn das Dateisystem der Rootpartition beschädigt ist.

Die folgenden Optionen stehen zur Verfügung:

Standard-Bootdiskette

Mit dieser Option können Sie die Standardbootdisketten erstellen, mit denen ein installiertes System gebootet wird. Je nach Architektur kann die tatsächliche Anzahl der Bootdisketten variieren, Sie sollten jedoch alle Bootdisketten erstellen, die im Dialogfeld angegeben werden, da alle diese Disketten für den Bootvorgang erforderlich sind. Außerdem werden sie zum Starten des Rettungssystems benötigt.

Rettungsdiskette

Diese Diskette enthält eine besondere Umgebung, mit der Sie Wartungsaufgaben im installierten System durchführen können, beispielsweise Überprüfen und Reparieren des Dateisystems und Aktualisieren des Bootloaders. Zum Starten des Rettungssystems booten Sie mit den Standard-Bootdisketten und wählen Sie dann *Manuelle Installation* → *Installation / System starten* → *Rettungssystem*. Legen Sie die Rettungsdiskette ein, wenn Sie dazu aufgefordert werden.

Benutzerdefinierte Diskette

Verwenden Sie diese Option, um ein beliebiges Disketten-Image von der Festplatte auf Diskette zu schreiben.

Disketten-Image herunterladen

Mit dieser Option können Sie eine URL sowie Authentifizierungsdaten zum Herunterladen eines Disketten-Image aus dem Internet eingeben.

Um eine dieser Disketten zu erstellen, wählen Sie die entsprechende Option aus und klicken Sie auf *Weiter*. Legen Sie auf Aufforderung eine Diskette ein. Klicken Sie erneut auf *Weiter*, um die Diskette zu erstellen.

7.5.4 Konfiguration des Bootloaders

Verwenden Sie zum Konfigurieren des Bootvorgangs für Systeme, die auf Ihrem Computer installiert sind, das Modul *System* → *Bootloader*. Eine ausführliche Beschreibung der Bootloader-Konfiguration mit YaST finden Sie in [Abschnitt 21.3](#), „[Konfigurieren des Bootloaders mit YaST](#)“ (S. 448).

7.5.5 Clustering

Informationen zur Heartbeat- und Hochverfügbarkeitskonfiguration mit YaST finden Sie in [Kapitel 13, Installieren eines Heartbeat 2-Clusters mithilfe von YaST](#) (S. 305) und [Kapitel 12, Hohe Verfügbarkeit \(High Availability\) unter Linux](#) (S. 295).

7.5.6 LVM

LVM (Logical Volume Manager) ist ein Werkzeug zur benutzerdefinierten Partitionierung von Festplatten mit logischen Laufwerken. Informationen zu LVM finden Sie in [Abschnitt 6.1, „LVM-Konfiguration“](#) (S. 133).

7.5.7 EVMS

Das *Enterprise Volume Management System* (EVMS) ist wie LVM ein Werkzeug zur benutzerdefinierten Partitionierung und Gruppierung von Festplatten in virtuelle Volumes. Es ist flexibel, erweiterbar und kann mithilfe eines Plugin-Modells an die einzelnen Anforderungen der verschiedenen Volume-Verwaltungssysteme angepasst werden.

EVMS ist mit den vorhandenen Arbeitsspeicher- und Volume-Verwaltungssystemen, wie DOS, Linux LVM, GPT (GUID-Partitionstabelle), IBM System z, Macintosh und BSD-Partitionen, kompatibel. Weitere Informationen hierzu finden Sie unter <http://evms.sourceforge.net/>.

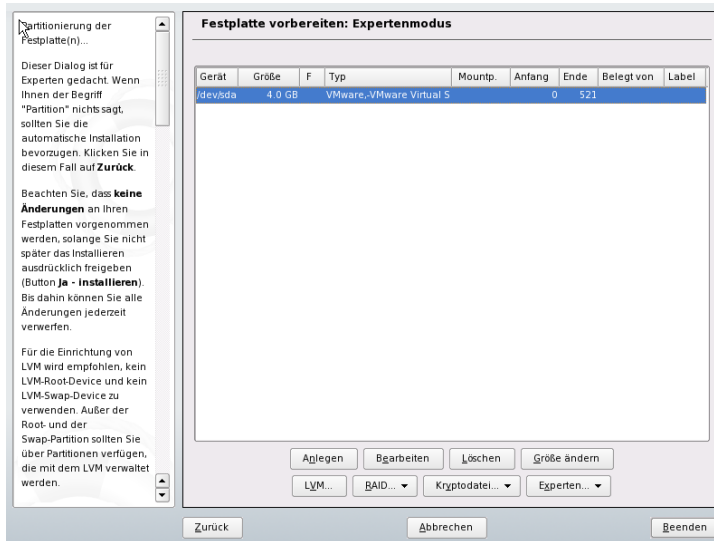
7.5.8 Partitionierung

Das in [Abbildung 7.4, „Das YaST-Partitionierungsprogramm“](#) (S. 177) gezeigte Experten-Dialogfeld 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 RAID-, EVMS- und LVM-Konfiguration zugreifen.

WARNUNG

Eine Änderung der Partitionen im installierten System ist zwar möglich, sollte jedoch nur von Experten vorgenommen werden. Andernfalls ist das Risiko, einen Fehler zu machen, der zu Datenverlust führt, sehr hoch. Wenn Sie eine in Verwendung befindliche Festplatte neu partitionieren, müssen Sie das System unmittelbar danach neu booten. Es ist sicherer, das Rettungssystem zu verwenden als das System während der Ausführung neu zu partitionieren.

Abbildung 7.4 Das YaST-Partitionierungsprogramm



TIPP: IBM-System z: Gerätenamen

IBMSystem z erkennt ausschließlich DASD- und SCSI-Festplatten. IDE-Festplatten werden nicht unterstützt. Aus diesem Grund werden die Geräte in der Partitionstabelle für das erste erkannte Gerät als `dasda` oder `sda` angezeigt.

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/hda` oder `/dev/sda` (bzw. `/dev/dasda`). Partitionen werden als Teile dieser Geräte aufgelistet, beispielsweise `/dev/hda1` oder `/dev/sda1` (bzw.

/dev/dasda1). Größe, Typ, Dateisystem und Einhängpunkt der Festplatten und ihrer Partitionen werden ebenfalls angezeigt. Der Einhängpunkt gibt an, wo sich die Partition im Linux-Dateisystembaum befindet.

Wenn Sie das Experten-Dialogfeld während der Installation ausführen, wird auch sämtlicher freier Speicherplatz aufgeführt und automatisch ausgewählt. Um weiteren Speicherplatz für SUSE Linux Enterprise Server zur Verfügung zu stellen, müssen Sie den benötigten Speicherplatz von unten nach oben in der Liste freigeben. (Sie beginnen also mit der letzten Partition der Festplatte und arbeiten sich bis zu ersten vor.) Wenn Sie beispielsweise über drei Partitionen verfügen, können Sie nicht die zweite ausschließlich für SUSE Linux Enterprise Server und die dritte und erste für andere Betriebssysteme verwenden.

Erstellen von Partitionen

Wählen Sie *Erstellen* aus. Wenn mehrere Festplatten angeschlossen sind, wird ein Auswahldialogfeld angezeigt, in dem Sie eine Festplatte für die neue Partition auswählen können. Geben Sie anschließend 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 „[Partitionstypen](#)“ (S. 47)).

Wählen Sie das zu verwendende Dateisystem und einen Einhängpunkt aus, falls erforderlich. YaST schlägt für jede erstellte Partition einen Einhängpunkt vor. Details der Parameter finden Sie im nächsten Abschnitt. Mit *OK* können Sie Ihre Änderungen übernehmen. Anschließend wird die neue Partition in der Partitionstabelle aufgeführt. Beim Klicken auf *Weiter* werden die aktuellen Werte übernommen. Während der Installation wird der Vorschlag-Bildschirm erneut aufgerufen.

Partitionierungsparameter

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. Manuelle Einstellungen können Sie folgendermaßen vornehmen:

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 Partition zu diesem Zeitpunkt nicht formatieren möchten, sollten Sie ihr eine Dateisystem-ID zuweisen, um sicherzustellen, dass sie richtig registriert wird. Mögliche Werte sind *Linux*, *Linux swap*, *Linux LVM*, *Linux EVMS* und *Linux RAID*. Einzelheiten zu LVM und RAID finden Sie unter [Abschnitt 6.1, „LVM-Konfiguration“](#) (S. 133) und [Abschnitt 6.2, „Soft-RAID-Konfiguration“](#) (S. 142).

Dateisystem

Um die Partition sofort im Rahmen der Installation zu formatieren, müssen Sie eines der folgenden Dateisysteme für die Partition angeben: *Swap*, *Ext2*, *Ext3*, *ReiserFS* oder *JFS*. Einzelheiten zu den verschiedenen Dateisystemen finden Sie in [Kapitel 26, *Dateisysteme in Linux*](#) (S. 523).

Optionen für das Dateisystem

Hier können Sie verschiedene Parameter für das ausgewählte Dateisystem festlegen.

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 48, *Verschlüsseln von Partitionen und Dateien*](#) (S. 949).

Fstab-Options

Geben Sie hier verschiedene Parameter für die Verwaltungsdatei der Dateisysteme an (*/etc/fstab*). Ändern Sie beispielsweise die Dateisystem-ID vom Gerätenamen (Standard) in ein Volume-Label. Im Volume-Label können Sie alle Zeichen mit Ausnahme von "/" und des Leerzeichens verwenden.

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. Aktivieren Sie die Partition mit *Weiter*.

Bei einer manuellen Partitionierung müssen Sie eine Swap-Partition mit mindestens 256 MB erstellen. Die Swap-Partition dient dazu, um den Hauptspeicher von Daten freizugeben, die zurzeit nicht verwendet werden. Dadurch bleibt der Hauptspeicher frei für die am häufigsten verwendeten Daten.

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.

Weitere Partitionierungstipps

Wenn die Partitionierung von YaST durchgeführt wird und andere Partitionen im System erkannt werden, werden diese Partitionen ebenfalls in die Datei `/etc/fstab` eingegeben, um einen leichten Zugriff auf die Daten zu ermöglichen. Diese Datei enthält alle Partitionen im System sowie deren Eigenschaften, beispielsweise Dateisystem, Einhängepunkt und Benutzerberechtigungen.

Beispiel 7.1 */etc/fstab: Partition Data*

```
/dev/sda1 /data1 auto noauto,user 0 0
/dev/sda5 /data2 auto noauto,user 0 0
/dev/sda6 /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 schlechten Interpreter oder verweigerter Berechtigungen, erhalten.

Partitionierung und LVM

Von der Expertenpartitionierung aus können Sie mit *LVM* die LVM-Konfiguration aufrufen (siehe [Abschnitt 6.1, „LVM-Konfiguration“](#) (S. 133)). 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.

7.5.9 PCI-Gerätetreiber

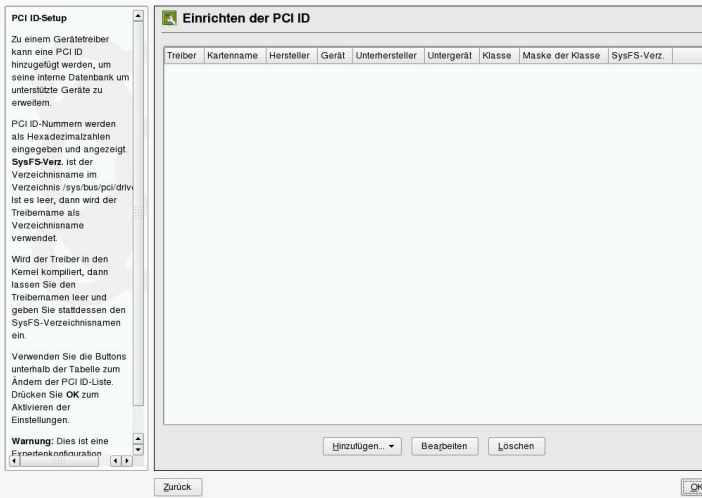
TIPP: IBM-System z: Fortsetzung

Für IBM-System z fahren Sie mit [Abschnitt 7.5.13, „Systemdienste \(Runlevel\)“](#) (S. 183) fort.

Jeder Kernel-Treiber umfasst eine Liste mit den Geräte-IDs aller unterstützten Geräte. Wenn sich ein neues Gerät nicht in der Datenbank eines Treibers befindet, wird das

Gerät so behandelt, als ob es nicht unterstützt wird, selbst wenn es mit einem vorhandenen Treiber verwendet werden kann. Mit diesem YaST-Modul aus dem Bereich *System* können Sie PCI-IDs hinzufügen. Dieses YaST-Modul sollte nur von erfahrenen Benutzern verwendet werden.

Abbildung 7.5 *Hinzufügen einer PCI-ID*



Klicken Sie zum Hinzufügen einer ID auf *Hinzufügen* und wählen Sie die Zuweisungsmethode aus: die Auswahl eines PCI-Geräts aus einer Liste oder die manuelle Eingabe von PCI-Werten. Bei Verwendung der ersten Methode wählen Sie das PCI-Gerät aus der verfügbaren Liste aus und geben Sie dann den Treiber- oder Verzeichnisnamen ein. Wenn das Verzeichnis leer ist, wird der Treibername als Verzeichnisname verwendet. Bei der manuellen Zuweisung von PCI-ID-Werten geben Sie die erforderlichen Daten zur Einrichtung einer PCI-ID ein. Klicken Sie anschließend auf *OK*, um die Änderungen zu speichern.

Zum Bearbeiten einer PCI-CD wählen Sie den Gerätetreiber aus der Liste und klicken Sie auf *Bearbeiten*. Bearbeiten Sie die Informationen und klicken Sie auf *OK*, um die Änderungen zu speichern. Zum Löschen einer ID wählen Sie den Treiber aus und klicken Sie auf *Löschen*. Die ID wird sofort aus der Liste entfernt. Klicken Sie zum Abschluss auf *OK*.

7.5.10 Energieverwaltung

Das Modul *System* → *Energieverwaltung* unterstützt Sie bei der Arbeit mit Energiespartechnologien. Es ist besonders wichtig bei Laptops, um deren Betriebszeit zu verlängern. Detaillierte Informationen zur Verwendung dieses Moduls finden Sie in [Abschnitt 29.6](#), „Das YaST-Energieverwaltungsmodul“ (S. 586).

7.5.11 Konfiguration von Powertweak

Powertweak ist ein Dienstprogramm von SUSE Linux zur Systemoptimierung: Durch Feinabstimmung einiger Kernel- und Hardwarekonfigurationen soll größtmögliche Leistungsfähigkeit erzielt werden. Dieses Programm sollte nur von erfahrenen Benutzern verwendet werden. Nachdem das Programm mit *System* → *Powertweak* gestartet wurde, erkennt es Ihre Systemeinstellungen und listet sie in Baumform im linken Rahmen des Moduls auf. Außerdem können Sie über die Schaltfläche *Suchen* eine Konfigurationsvariable suchen. Wählen Sie die Option zur Systemoptimierung, um sie zusammen mit dem zugehörigen Verzeichnis und den entsprechenden Einstellungen auf dem Bildschirm anzuzeigen. Klicken Sie zum Speichern der Einstellungen auf *Beenden* und bestätigen Sie den Vorgang durch Klicken auf *OK*.

7.5.12 Profil-Manager

Mit *System* → *Profilverwaltung*, dem YaST-Modul zur Verwaltung der Systemkonfigurationsprofile (System Configuration Profile Management, SCPM) können Sie Systemkonfigurationen erstellen, verwalten und zwischen ihnen wechseln. Dies ist besonders für mobile Computer nützlich, die an verschiedenen Standorten (in verschiedenen Netzwerken) und von verschiedenen Benutzern verwendet werden. Dennoch ist diese Funktion auch für stationäre Computer sinnvoll, da sie die Verwendung verschiedener Hardware-Komponenten und Testkonfigurationen erlaubt.

7.5.13 Systemdienste (Runlevel)

Runlevels und die Dienste, die darin starten, können Sie unter *System* → *Runlevel-Editor* konfigurieren. Weitere Informationen zu den Runlevels in SUSE Linux Enterprise und eine Beschreibung des YaST-Runlevel-Editors finden Sie in [Abschnitt 20.2.3](#), „Konfigurieren von Systemdiensten (Runlevel) mit YaST“ (S. 431).

7.5.14 /etc/sysconfig-Editor

Das Verzeichnis `/etc/sysconfig` enthält die Dateien mit den wichtigsten Einstellungen für SUSE Linux Enterprise. Mithilfe von *System* → */etc/sysconfig-Editor* können Sie die Werte bearbeiten und sie in den einzelnen Konfigurationsdateien speichern. In der Regel ist eine manuelle Bearbeitung nicht erforderlich, da die Dateien automatisch angepasst werden, wenn ein Paket installiert oder ein Dienst konfiguriert wird. Weitere Informationen zu `/etc/sysconfig` und dem `sysconfig`-Editor von YaST finden Sie in [Abschnitt 20.3.1, „Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"“](#) (S. 434).

7.5.15 Konfiguration von Zeit und Datum

Die Zeitzone wird ursprünglich während der Installation festgelegt, Sie können sie jedoch unter *System* → *Datum und Uhrzeit* ändern. Außerdem können Sie mit dieser Funktion das aktuelle Datum und die aktuelle Uhrzeit für das System ändern.

Zum Ändern der Zeitzone wählen Sie in der linken Spalte die Region und in der rechten Spalte den Ort bzw. die Zeitzone aus. Legen Sie mithilfe von *Rechneruhr eingestellt auf* fest, ob die Systemuhr *Lokale Zeit* oder *UTC* (Universal Time Coordinated, koordinierte Weltzeit) verwenden soll. In Linux-Systemen wird häufig *UTC* verwendet. Computer mit zusätzlichen Betriebssystemen, wie Microsoft Windows, verwenden meist die Ortszeit.

Mit *Ändern* können Sie die aktuelle Systemzeit und das aktuelle Datum festlegen. Ändern Sie in dem sich öffnenden Dialogfeld *Uhrzeit und Datum*, indem Sie neue Werte eingeben oder Sie mithilfe der Pfeilschaltflächen anpassen. Klicken Sie auf *Übernehmen*, um die Änderungen zu speichern.

7.5.16 Sprachauswahl

Die primäre Sprache und die sekundären Sprachen für Ihr System werden während der Installation festgelegt. Sie können jedoch jederzeit mithilfe von *System* → *Sprache* geändert werden. Die in YaST festgelegte primäre Sprache gilt für das gesamte System, einschließlich YaST und der Desktop-Umgebung. Wählen Sie hierfür die Sprache aus, die Sie voraussichtlich die meiste Zeit verwenden. Sekundäre Sprachen sind Sprachen,

7.6.1 DSL, ISDN, Modem oder Netzwerkkarte

Wählen Sie zur Konfiguration einer DSL-, ISDN- oder Netzwerkschnittstelle bzw. eines Modems das entsprechende Modul aus dem Abschnitt *Netzwerkgeräte*. Wenn das Gerät automatisch erkannt wurde, wählen Sie es in der Liste aus und klicken Sie auf *Bearbeiten*. Wenn Ihr Gerät nicht erkannt wurde, klicken Sie auf *Hinzufügen* und wählen Sie es manuell aus. Um ein vorhandenes Gerät zu bearbeiten, wählen Sie es aus und klicken Sie dann auf *Bearbeiten*. Detailliertere Informationen hierzu finden Sie in [Abschnitt 31.4, „Konfigurieren von Netzwerkverbindungen mit YaST“](#) (S. 623). Informationen zu Schnittstellen für drahtlose Netzwerke finden Sie in [Kapitel 30, *Drahtlose Kommunikation*](#) (S. 591).

TIPP: CDMA- und GPRS-Modems

Sie können unterstützte CDMA- und GPRS-Modems als reguläre Modems im YaST-Modem-Modul konfigurieren.

7.7 Netzwerkdienste

Diese Gruppe enthält Werkzeuge zur Konfiguration verschiedener Arten von Diensten im Netzwerk. Dazu gehören Namensauflösung, Benutzerauthentifizierung und Dateidienste.

7.7.1 Mail Transfer Agent

In *Netzwerkdienste* → *Mail Transfer Agent* können Sie Ihre Mail-Einstellungen konfigurieren, sofern Sie Ihre E-Mails über sendmail, postfix oder den SMTP-Server des Providers versenden. Sie können Mail über das Programm fetchmail abrufen, für das Sie auch die Details des POP3- oder IMAP-Servers Ihres Providers eingeben können. Alternativ können Sie ein beliebiges anderes E-Mail-Programm, wie KMail oder Evolution, zum Festlegen der Zugangsdaten verwenden. In diesem Fall wird dieses Modul nicht benötigt.

Um Ihre Mail mit YaST zu konfigurieren, geben Sie im ersten Dialogfeld den Typ Ihrer Internetverbindung an. Es stehen folgende Optionen zur Auswahl:

Permanent

Wählen Sie diese Option, wenn Sie über eine dedizierte Leitung für das Internet verfügen. Ihr Computer ist permanent online, sodass keine Einwahl erforderlich ist. Wenn Ihr System Teil eines logischen Netzwerks mit zentralem Email-Server ist, können Sie mit dieser Option einen permanenten Zugriff auf Ihre Email-Nachrichten sicherstellen.

Einwahl

Dieser Eintrag ist für Benutzer relevant, die einen Computer zu Hause verwenden, nicht in ein Netzwerk eingebunden sind und gelegentlich eine Verbindung zum Internet herstellen.

Keine Verbindung

Wenn Sie keinen Zugang zum Internet haben und Ihr Computer nicht in ein Netzwerk eingebunden ist, können Sie keine Emails senden oder empfangen.

Durch Auswahl der entsprechenden Option können Sie die Virenprüfung mit AMaViS für eingehende und ausgehende E-Mails aktivieren. Das Paket wird automatisch installiert, sobald Sie den Email-Filter aktivieren. In den folgenden Dialogfeldern müssen Sie den Ausgangsmailserver (normalerweise der SMTP-Server Ihres Anbieters) und die Parameter für eingehende Emails angeben. Richten Sie die verschiedenen POP- bzw. IMAP-Server für den Mail-Empfang durch verschiedene Benutzer ein. In diesem Dialogfeld können Sie außerdem Aliasse zuweisen, Masquerading verwenden oder virtuelle Domänen einrichten. Beenden Sie die Mail-Konfiguration mit *Beenden*.

7.7.2 Mailserver

WICHTIG: LDAP-basierte Mailserver-Konfiguration

Das Mailserver-Modul von SUSE Linux Enterprise Server funktioniert nur, wenn die Benutzer, Gruppen sowie DNS- und DHCP-Dienste mit LDAP verwaltet werden.

Das Mailserver-Modul ermöglicht die Konfiguration von SUSE Linux Enterprise Server als Mailserver. YaST unterstützt Sie bei den folgenden Schritten des Konfigurationsvorgangs:

Globale Einstellungen

Konfiguriert die Identifikation des lokalen Mailservers und die Höchstgröße für ein- und ausgehende Nachrichten sowie den Typ des Mailtransports.

Lokale Zustellung

Konfiguriert den Typ der lokalen Mailzustellung.

Mailtransport

Konfiguriert die speziellen Transportrouten für Mail entsprechend der Zieladresse.

SPAM-Schutz

Konfiguriert die SPAM-Schutzeinstellungen des Mailservers. Das Werkzeug AMaViS wird aktiviert. Legen Sie Typ und Stufe der SPAM-Prüfung fest.

Mailserver-Weiterleitung

Bestimmt, aus welchen Netzwerken der Mailserver nicht zum Senden von nichtlokaler Mail verwendet werden kann.

Abrufen von Mail

Konfiguriert das Abrufen von Mail aus externen Mailkonten über verschiedene Protokolle.

Mailserver-Domänen

Hier wird bestimmt, für welche Domänen der Mailserver verantwortlich sein soll. Es muss mindestens eine Master-Domäne konfiguriert sein, wenn der Server nicht als Null-Client ausgeführt werden soll, der ausschließlich zum Senden von Mail verwendet wird (kein Empfang).

Es wird zwischen drei Domänentypen unterschieden:

main

Haupt- oder Master-Domäne des lokalen Mailservers

local

Alle Benutzer, die in einer Master-Domäne Mail empfangen können, können dies auch in einer lokalen Domäne. Bei Nachrichten innerhalb der lokalen Domäne wird nur der Teil vor dem @ ausgewertet.

virtual

Nur Benutzer mit einer expliziten Adresse innerhalb einer virtuellen Domäne können Mail empfangen. Virtuelle Mailadressen werden im Benutzerverwaltungsmodule von YaST eingerichtet.

7.7.3 Weitere verfügbare Dienste

In YaST *Netzwerkdienste* stehen zahlreiche weitere Netzwerkmodule zur Verfügung.

DHCP-Server

Hiermit können Sie in wenigen Schritten einen benutzerdefinierten DHCP-Server einrichten. In [Kapitel 35, DHCP](#) (S. 707) finden Sie grundlegende Informationen zu diesem Thema und eine Einzelschrittbeschreibung des Konfigurationsvorgangs.

DNS-Server

Für größere Netzwerke wird die Konfiguration eines DNS-Servers, der für die Namensauflösung zuständig ist, empfohlen. Sie können hierfür *DNS-Server* verwenden, wie in [Abschnitt 34.2, „Konfiguration mit YaST“](#) (S. 682) beschrieben. [Kapitel 34, Domain Name System \(DNS\)](#) (S. 681) bietet Hintergrundinformationen zu DNS.

DNS und Hostname

Mit diesem Modul können Sie den Hostnamen und DNS konfigurieren, wenn diese Einstellungen nicht bereits während der Konfiguration der Netzwerkgeräte vorgenommen wurden. Außerdem dient es zum Ändern des Hostnamens und des Domänennamens. Wenn der Anbieter für DSL-, Modem- bzw. ISDN-Zugriff korrekt konfiguriert wurde, enthält die Liste der Namensserver die Einträge, die automatisch aus den Anbieterdaten extrahiert wurden. Wenn der Rechner in ein lokales Netzwerk eingebunden ist, erhalten Sie den Hostnamen möglicherweise über DHCP. In diesem Fall sollte der Name nicht geändert werden.

HTTP-Server

Um Ihren eigenen Webserver auszuführen, konfigurieren Sie Apache in *HTTP-Server*. Weitere Informationen finden Sie in [Kapitel 41, Der HTTP-Server Apache](#) (S. 811).

Hostnamen

Beim Booten in kleinen Netzwerken können Sie anstatt *DBS Hostnamen* für die Auflösung der Hostnamen verwenden. Die Einträge in diesem Modul entsprechen

den Daten der Datei `/etc/hosts`. Weitere Informationen finden Sie in „`/etc/hosts`“ (S. 654).

Kerberos-Client

Verwenden Sie *Kerberos-Client*, wenn Sie in Ihrem Netzwerk einen Kerberos-Server zur Netzwerkauthentifizierung einsetzen. Eine ausführliche Beschreibung der Client-Konfiguration mit YaST finden Sie in [Abschnitt 47.6, „Konfigurieren eines Kerberos-Clients mit YaST“](#) (S. 936).

LDAP-Client

Bei Verwendung von LDAP für die Benutzerauthentifizierung im Netzwerk müssen Sie den Client in *LDAP-Client* konfigurieren. Informationen zu LDAP und eine detaillierte Beschreibung der Client-Konfiguration mit YaST finden Sie in [Abschnitt 37.6, „Konfigurieren eines LDAP-Clients mit YaST“](#) (S. 754).

LDAP-Server

Der LDAP-Server kann zahlreiche Daten in einem zentralen Verzeichnis speichern und sie an alle Clients in Ihrem Netzwerk verteilen. Der LDAP-Server wird vorwiegend zur Speicherung gemeinsamer Kontaktinformationen verwendet, ist jedoch nicht darauf beschränkt. Ein LDAP-Server kann auch zur Authentifizierung eingesetzt werden. Informationen zu LDAP und eine detaillierte Beschreibung der Serverkonfiguration mit YaST finden Sie in [Kapitel 37, *LDAP – Ein Verzeichnisdienst*](#) (S. 735).

NFS-Client

Bei Verwendung des NFS-Client sollten Sie vom NFS-Server bereitgestellte Verzeichnisse in Ihren eigenen Dateibäumen einhängen. Verwenden Sie *NFS-Client*, um Ihr System für den Zugriff auf einen NFS-Server im Netzwerk zu konfigurieren. Eine Beschreibung des YaST-Moduls sowie Hintergrundinformationen zu NFS finden Sie in [Kapitel 39, *Verteilte Nutzung von Dateisystemen mit NFS*](#) (S. 785).

NFS-Server

Führen Sie mit NFS einen Dateiserver aus, auf den alle Mitglieder des Netzwerks zugreifen können. Dieser Dateiserver kann verwendet werden, um bestimmte Anwendungen, Dateien und Speicherplatz für die Benutzer zur Verfügung zu stellen. Unter *NFS-Server* können Sie den Host als NFS-Server konfigurieren und die Verzeichnisse bestimmen, die für die allgemeine Verwendung durch die Netzwerkbenutzer exportiert werden sollen. Alle Benutzer mit den entsprechenden Berechtigungen können diese Verzeichnisse in ihren eigenen Dateibäumen einhängen. Eine Beschreibung des YaST-Moduls sowie Hintergrundinformationen

zu NFS finden Sie in [Kapitel 39, Verteilte Nutzung von Dateisystemen mit NFS](#) (S. 785).

NIS-Client

Wenn Sie einen NIS-Server zur Verwaltung von Benutzerdaten an einem zentralen Ort und zur Verteilung an die Clients einsetzen, konfigurieren Sie den Client hier. Detaillierte Informationen zum NIS-Client und zur Konfiguration mit YaST finden Sie in [Abschnitt 36.2, „Konfigurieren von NIS-Clients“](#) (S. 732).

NIS-Server

Bei Ausführung mehrerer Systeme ist eine lokale Benutzerverwaltung (mit den Dateien `/etc/passwd` und `/etc/shadow`) unpraktisch und erfordert hohen Wartungsaufwand. In diesem Fall sollten die Benutzerdaten auf einem zentralen Server verwaltet und von dort an die Clients verteilt werden. NIS stellt eine Möglichkeit dazu dar. Detaillierte Informationen zu NIS und zur Konfiguration mit YaST finden Sie in [Abschnitt 36.1.1, „Konfigurieren eines NIS-Master-Servers“](#) (S. 726).

NTP-Client

NTP (Network Time Protocol) ist ein Protokoll zur Synchronisierung der Hardware-Uhren über ein Netzwerk. Informationen zu NTP und Anweisungen für die Konfiguration mit YaST finden Sie in [Kapitel 33, Zeitsynchronisierung mit NTP](#) (S. 675).

Netzwerkdienste (xinetd)

Konfigurieren Sie die Netzwerkdienste (z. B. `finger`, `talk` und `ftp`), die beim Booten von SUSE Linux Enterprise gestartet werden sollen, mithilfe von *Netzwerkdienste*. Mit diesen Diensten können externe Hosts eine Verbindung zu Ihrem Computer herstellen. Für jeden Dienst können verschiedene Parameter konfiguriert werden. Standardmäßig wird der Masterdienst, der die einzelnen Dienste verwaltet (`inetd` bzw. `xinetd`), nicht gestartet.

Wählen Sie beim Start dieses Moduls aus, ob `inetd` oder `xinetd` gestartet werden soll. Der ausgewählte Daemon kann mit einer Standardauswahl an Diensten gestartet werden. Alternativ können Sie mit *Hinzufügen*, *Löschen* und *Bearbeiten* Ihre eigene Auswahl an Diensten zusammenstellen.

WARNUNG: Konfigurieren von Netzwerkdiensten (xinetd)

Die Zusammenstellung und Anpassung von Netzwerkdiensten in einem System ist ein komplexer Vorgang, für den ein umfassendes Verständnis des Konzepts der Linux-Dienste erforderlich ist. Die Standardeinstellungen sind für die meisten Fälle ausreichend.

Proxy

Die Client-Einstellungen für den Internet-Proxy können Sie unter *Proxy* konfigurieren. Klicken Sie auf *Proxy aktivieren* und geben Sie anschließend die gewünschten Proxy-Einstellungen ein. Sie können diese Einstellungen durch Klicken auf *Proxy-Einstellungen testen* überprüfen. In einem kleinen Fenster wird angezeigt, ob Ihre Proxy-Einstellungen ordnungsgemäß arbeiten. Nachdem Sie die Einstellungen eingegeben und getestet haben, speichern Sie sie durch Klicken auf *Übernehmen*.

Verwaltung über einen entfernten Rechner

Wenn Sie Ihren Computer über entfernten Zugriff von einem anderen Computer aus verwalten möchten, verwenden Sie *Remote Administration* (Verwaltung via entfernten Rechner (remote)). Um eine entfernte Wartung des Systems durchzuführen, verwenden Sie einen VNC-Client, wie *krdc*, oder einen Java-fähigen Browser. Eine entfernte Verwaltung mit VNC ist zwar einfach und schnell, jedoch wesentlich weniger sicher als bei Verwendung von SSH. Dieser Tatsache sollten Sie sich stets bewusst sein, wenn Sie einen VNC-Server verwenden. Detaillierte Informationen zur Installation mit einem VNC-Client finden Sie in [Abschnitt 4.1.1, „Einfache Installation mit entferntem Zugriff über VNC – Statische Netzwerkkonfiguration“](#) (S. 76).

Sie können entfernte Verwaltung durch Auswahl von *Verwaltung via entfernten Rechner (remote) erlauben* unter *Einstellungen für Verwaltung von entfernten Rechnern aus (remote)* gestatten. Durch Auswahl von *Verwaltung von entferntem Rechner (remote) nicht zulassen* wird diese Funktion deaktiviert. Klicken Sie auf *Firewall-Port öffnen*, um den Zugriff auf den Computer zu gestatten. Durch Klicken auf *Firewall-Details* werden Netzwerkschnittstellen mit offenen Ports in der Firewall angezeigt. Wählen Sie die gewünschte Schnittstelle aus und klicken Sie auf *OK*, um zum Hauptdialogfeld zurückzukehren. Klicken Sie zum Beenden der Konfiguration auf *Übernehmen*.

Das YaST-Modul *Verwaltung via entfernten Rechner (remote)* wird nachdrücklich zur Konfiguration von VNC auf dem Computer empfohlen. Die Eigenschaften für

den entfernten Zugriff können zwar auch mit der SaX2-Schnittstelle festgelegt werden, diese ist jedoch kein Ersatz für YaST. Sie erlaubt lediglich die Konfiguration des X-Servers als Host für VNC-Sitzungen. Weitere Informationen finden Sie in [Abschnitt 7.13.6, „Eigenschaften für den entfernten Zugriff“](#) (S. 216).

Routing

Mit *Routing* können Sie konfigurieren, welche Wege die Daten im Netzwerk durchlaufen. In den meisten Fällen sollten Sie lediglich unter *Standard-Gateway* die IP-Adresse des Systems eingeben, durch das alle Daten gesendet werden sollen. Kompliziertere Konfigurationen können Sie unter *Expertenkonfiguration* erstellen.

Samba-Server

In einem heterogenen Netzwerk mit Linux- und Windows-Hosts steuert Samba die Kommunikation zwischen den beiden Systemen. Informationen zu Samba und zur Konfiguration von Servern finden Sie in [Kapitel 38, Samba](#) (S. 767).

SLP-Server

Mit dem *Service Location Protocol* (SLP) können Sie Clients in Ihrem Netzwerk konfigurieren, ohne die Servernamen und Dienste zu kennen, die diese Server bereitstellen. Detaillierte Informationen zu SLP-Servern und zur Konfiguration mit YaST finden Sie in [Kapitel 32, SLP-Dienste im Netzwerk](#) (S. 669).

TFTP-Server

Ein TFTP-Server ist kein FTP-Server. Während ein FTP-Server das File Transfer Protocol (FTP) verwendet, setzt ein TFTP-Server das viel einfachere Trivial File Transfer Protocol (TFTP) ohne Sicherheitsfunktionen ein. TFTP-Server werden in der Regel zum Booten von Arbeitsstationen, X-Terminals und Routern ohne Festplatte verwendet. Detaillierte Informationen zu TFTP-Servern und zur Konfiguration mit YaST finden Sie in [Abschnitt 4.3.2, „Einrichten eines TFTP-Servers“](#) (S. 97).

WOL

WOL (Wake on LAN) bezieht sich auf die Möglichkeit, einen Computer über das Netzwerk mit speziellen Paketen aus dem Stand-by-Modus zu „erwecken“. WOL funktioniert nur bei Motherboards, deren BIOS diese Funktionalität unterstützt. Die WOL-Konfiguration mit YaST wird in [Abschnitt 4.3.7, „Wake-on-LAN“](#) (S. 105) beschrieben.

Windows-Domänenmitgliedschaft

In einem heterogenen Netzwerk mit Linux- und Windows-Hosts steuert Samba die Kommunikation zwischen den beiden Systemen. Mit dem Modul *Samba-Client* können Sie Ihren Computer als Mitglied einer Windows-Domäne konfigurieren. Informationen zu Samba und zur Konfiguration von Clients finden Sie in [Kapitel 38, Samba](#) (S. 767).

7.8 AppArmor

Novell AppArmor bietet benutzerfreundliche Anwendungssicherheit für Server und Arbeitsstationen. Novell AppArmor ist ein System zur Zugriffssteuerung, in dem Sie für jedes einzelne Programm angeben können, welche Dateien es lesen, schreiben und ausführen darf. Um Novell AppArmor auf Ihrem System zu aktivieren oder zu deaktivieren, verwenden Sie die *AppArmor-Kontrollleiste*. Informationen zu Novell AppArmor und eine detaillierte Beschreibung der Konfiguration mit YaST finden Sie in *Novell AppArmor 2.0 Administration Guide* (↑Novell AppArmor 2.0 Administration Guide).

7.9 Sicherheit und Benutzer

Ein grundlegender Aspekt von Linux ist seine Mehrbenutzerfähigkeit. Somit können verschiedene Benutzer unabhängig voneinander auf demselben Linux-System arbeiten. Jeder Benutzer verfügt über ein Benutzerkonto, das durch einen Anmeldenamen und ein persönliches Passwort für die Anmeldung beim System gekennzeichnet ist. Alle Benutzer verfügen über eigene Home-Verzeichnisse, in denen persönliche Dateien und Konfigurationen gespeichert sind.

7.9.1 Benutzerverwaltung

Verwenden Sie *Sicherheit und Benutzer* → *Benutzer-Verwaltung* zum Erstellen und Bearbeiten von Benutzern. Diese Funktion bietet einen Überblick über die Benutzer im System, einschließlich NIS-, LDAP-, Samba- und Kerberos-Benutzern, sofern angefordert. Wenn Ihr Computer Teil eines umfangreichen Netzwerks ist, klicken Sie auf *Filter festlegen*, um alle Benutzer nach Kategorien aufzulisten (beispielsweise

root- oder NIS-Benutzer). Außerdem können Sie die Filtereinstellungen durch Klicken auf *Benutzerdefinierte Filtereinstellung* anpassen.

Um neue Benutzer hinzuzufügen, klicken Sie auf *Hinzufügen* und geben Sie die entsprechenden Daten ein. Schließen Sie die Hinzufügung durch Klicken auf *Übernehmen* ab. Der neue Benutzer kann sich sofort mit dem neu erstellten Anmeldenamen und dem Passwort anmelden.

Deaktivieren Sie die Benutzeranmeldung mit der entsprechenden Option. Die Feineinstellung der Benutzerprofile ist unter *Details* möglich. Hier können Sie Benutzer-ID, Heimverzeichnis und Standard-Anmelde-Shell manuell festlegen und den neuen Benutzer bestimmten Gruppen zuweisen. Konfigurieren Sie die Gültigkeit des Passworts unter *Passworteinstellungen*. Durch Klicken auf *Übernehmen* werden alle Änderungen gespeichert.

Um einen Benutzer zu löschen, wählen Sie ihn in der Liste aus und klicken Sie auf *Löschen*. Markieren Sie anschließend, ob das Heimverzeichnis gelöscht werden soll, und klicken Sie zur Bestätigung auf *Ja*.

Wenn Sie eine erweiterte Benutzerverwaltung wünschen, können Sie unter *Optionen für Experten* die Standardeinstellungen zum Erstellen neuer Benutzer festlegen. Wählen Sie die Methode für die Benutzerauthentifizierung (z. B. NIS, LDAP, Kerberos oder Samba), die Anmeldeeinstellungen (nur bei KDM oder GDM) sowie den Algorithmus für die Passwortverschlüsselung aus. *Standardeinstellungen für neue Benutzer* und *Passwortverschlüsselung* gelten nur für lokale Benutzer. Unter *Authentifizierung und Benutzerquellen* finden Sie einen Konfigurationsüberblick und die Möglichkeit, den Client zu konfigurieren. Außerdem kann auch die Client-Konfiguration mit diesem Modul durchgeführt werden. Kehren Sie nach der Übernahme der Konfiguration zum ursprünglichen Konfigurationsüberblick zurück. Klicken Sie auf *Änderungen nun schreiben*, um alle Änderungen zu speichern, ohne das Konfigurationsmodul zu beenden.

7.9.2 Gruppenverwaltung

Wählen Sie zum Erstellen bzw. Bearbeiten von Gruppen die Option *Sicherheit und Benutzer* → *Gruppenverwaltung* aus oder klicken Sie im Modul zur Benutzerverwaltung auf *Gruppen*. Beide Dialoge bieten dieselben Funktionen: Sie können Gruppen erstellen, bearbeiten und löschen.

Das Modul bietet einen Überblick über alle Gruppen. Wie beim Dialogfeld für die Benutzerverwaltung können die Filtereinstellungen durch Klicken auf *Filter festlegen* geändert werden.

Um eine Gruppe hinzuzufügen, klicken Sie auf *Hinzufügen* und geben Sie die entsprechenden Daten ein. Wählen Sie die Gruppenmitglieder aus der Liste aus, indem Sie das entsprechende Kontrollkästchen markieren. Klicken Sie auf *Übernehmen*, um die Gruppe zu erstellen. Um eine Gruppe zu bearbeiten, wählen Sie die gewünschte Gruppe aus der Liste aus und klicken Sie auf *Bearbeiten*. Nehmen Sie alle erforderlichen Änderungen vor und speichern Sie sie mit *Übernehmen*. Um eine Gruppe zu löschen, wählen Sie sie einfach in der Liste aus und klicken Sie auf *Löschen*.

Unter *Optionen für Experten* ist eine erweiterte Gruppenverwaltung möglich. Weitere Informationen zu diesen Optionen finden Sie in [Abschnitt 7.9.1, „Benutzerverwaltung“](#) (S. 194).

7.9.3 Lokale Sicherheit

Mit *Sicherheit und Benutzer* → *Lokale Sicherheit* können Sie eine Gruppe von Sicherheitseinstellungen auf Ihr gesamtes System anwenden. Diese Einstellungen umfassen Sicherheit für das Booten, Anmeldung, Passwörter, Benutzererstellung und Dateiberechtigungen. SUSE Linux Enterprise bietet drei vorkonfigurierte Sicherheitssets: *Heim-Arbeitsstation*, *Vernetzte Arbeitsstation* und *Vernetzter Server*. Bearbeiten Sie die Standardwerte mit *Details*. Mithilfe von *Benutzerdefinierte Einstellungen* können Sie Ihr eigenes Schema erstellen.

Zu den detaillierten bzw. benutzerdefinierten Einstellungen gehören folgende Elemente:

Passworteinstellungen

Um neue Passwörter vor der Annahme vom System auf Sicherheit überprüfen zu lassen, klicken Sie auf *Neue Passwörter überprüfen* und *Test auf komplizierte Passwörter*. Legen Sie die Passwort-Mindestlänge für neu erstellte Benutzer fest. Definieren Sie den Zeitraum, für den die Passwörter gelten sollen, und wie viele Tage im Voraus eine Ablaufwarnung ausgegeben werden soll, wenn sich der Benutzer bei der Textkonsole anmeldet.

Einstellungen für den Systemstart

Legen Sie durch Auswahl der gewünschten Aktion fest, wie die Tastenkombination + + interpretiert werden soll. Normalerweise führt diese Kombination

in der Textkonsole dazu, dass das System neu gebootet wird. Bearbeiten Sie diese Einstellung nur, wenn Ihr Computer oder Server öffentlich zugänglich ist und Sie befürchten, dass jemand diesen Vorgang ohne Berechtigung ausführen könnte. Bei Auswahl von *Anhalten* führt diese Tastenkombination zum Herunterfahren des Systems. Mit *Ignorieren* wird die Tastenkombination ignoriert.

Bei Verwendung des KDE-Anmeldemanagers (KDM) können Sie die Berechtigungen für das Herunterfahren des Systems unter *Einstellung für das Herunterfahren unter KDM* festlegen. Sie können folgenden Personengruppen die Berechtigung erteilen: *Nur root* (Systemadministrator), *Alle Benutzer*, *Niemand* oder *Lokale Benutzer*. Bei Auswahl von *Niemand* kann das System nur über die Textkonsole heruntergefahren werden.

Einstellungen für das Anmelden

Üblicherweise ist nach einem gescheiterten Anmeldeversuch eine Wartezeit von mehreren Sekunden erforderlich, bevor eine weitere Anmeldung möglich ist. Dies erschwert Passwortschnüfflern die Anmeldung. Optional können Sie *Aufzeichnung erfolgreicher Anmeldeversuche* und *Grafische Anmeldung von Remote erlauben* aktivieren. Wenn Sie den Verdacht haben, dass jemand versucht, Ihr Passwort zu ermitteln, überprüfen Sie die Einträge in den Systemprotokolldateien in `/var/log`. Um anderen Benutzern Zugriff auf Ihren grafischen Anmeldebildschirm über das Netzwerk zu gestatten, müssen Sie *Grafische Anmeldung von Remote erlauben* aktivieren. Da diese Zugriffsmöglichkeit ein potenzielles Sicherheitsrisiko darstellt, ist sie standardmäßig nicht aktiviert.

Hinzufügen von Benutzern

Jeder Benutzer besitzt eine numerische und eine alphabetische Benutzer-ID. Die Korrelation zwischen diesen beiden IDs erfolgt über die Datei `/etc/passwd` und sollte so eindeutig wie möglich sein. Mit den Daten in diesem Bildschirm legen Sie den Zahlenbereich fest, der beim Hinzufügen eines neuen Benutzers dem numerischen Teil der Benutzer-ID zugewiesen wird. Ein Mindestwert von 500 ist für die Benutzer geeignet. Automatisch generierte Systembenutzer beginnen bei 1000. Verfahren Sie ebenso mit den Gruppen-ID-Einstellungen.

Verschiedene Einstellungen

Zur Verwendung der vordefinierten Dateiberechtigungseinstellungen wählen Sie *Easy (Einfach)*, *Sicher* oder *Paranoid* aus. *Easy (Einfach)* sollte für die meisten Benutzer ausreichen. Die Einstellung *Paranoid* ist sehr restriktiv und kann als grundlegende Betriebsstufe für benutzerdefinierte Einstellungen dienen. Bei Auswahl von *Paranoid* sollten Sie bedenken, dass einige Programme eventuell nicht

mehr oder nicht mehr ordnungsgemäß arbeiten, da die Benutzer keinen Zugriff mehr auf bestimmte Dateien haben.

Legen Sie außerdem fest, welcher Benutzer das Programm `updatedb` starten soll, sofern es installiert ist. Dieses Programm, das automatisch jeden Tag oder nach dem Booten ausgeführt wird, erstellt eine Datenbank (`locatedb`), in der der Speicherort jeder Datei auf dem Computer gespeichert wird. Bei Auswahl von *Niemand* können alle Benutzer nur die Pfade in der Datenbank finden, die von jedem anderen Benutzer ohne besondere Berechtigungen gesehen werden können. Bei Auswahl von `root` werden alle lokalen Dateien indiziert, da der Benutzer `root` als Superuser auf alle Verzeichnisse zugreifen kann. Vergewissern Sie sich, dass die Optionen *Aktuelles Verzeichnis im Pfad des Benutzers root* und *Das aktuelle Verzeichnis im Pfad regulärer Benutzer* deaktiviert sind. Nur fortgeschrittene Benutzer sollten in Erwägung ziehen, diese Optionen zu verwenden, da diese Einstellungen ein erhebliches Sicherheitsrisiko darstellen können, wenn sie falsch eingesetzt werden. Um selbst bei einem Systemabsturz noch einen gewissen Grad an Kontrolle über das System zu haben, klicken Sie auf *}Magic SysRq Keys aktivieren*.

Klicken Sie zum Abschließen der Sicherheitskonfiguration auf *Beenden*.

7.9.4 Zertifikatsverwaltung

Zertifikate werden für die Kommunikation verwendet und können beispielsweise auch auf ID-Karten in Unternehmen eingesetzt werden. Verwenden Sie zum Verwalten oder Importieren eines gemeinsamen Server-Zertifikats das Modul *Sicherheit und Benutzer* → *CA Management*. Detaillierte Informationen zu Zertifikaten, ihren Technologien und ihrer Verwaltung mit YaST finden Sie in [Kapitel 43, Verwalten der X.509-Zertifizierung](#) (S. 881).

7.9.5 Firewall

SuSEfirewall2 kann Ihren Rechner vor Angriffen aus dem Internet schützen. Konfigurieren Sie sie mit *Sicherheit und Benutzer* → *Firewall*. Detaillierte Informationen zu SuSEfirewall2 finden Sie in [Kapitel 44, Masquerading und Firewalls](#) (S. 899).

TIPP: Automatische Aktivierung der Firewall

YaST startet automatisch eine Firewall mit geeigneten Einstellungen auf jeder konfigurierten Netzwerkschnittstelle. Starten Sie dieses Modul nur, wenn Sie die Firewall deaktivieren oder mit benutzerdefinierten Einstellungen neu konfigurieren möchten.

7.10 Andere

Das YaST-Kontrollzentrum verfügt über mehrere Module, die sich nicht ohne weiteres in die ersten sechs Modulgruppen einordnen lassen. Diese dienen beispielsweise zum Anzeigen von Protokolldateien und zur Installation von Treibern von einer Hersteller-CD.

7.10.1 Erstellen benutzerdefinierter Installations-CDs

Mit *Verschiedenes* → *CD Creator* (CD-Erstellung) können Sie eine benutzerdefinierte Installations-CD erstellen. Klicken Sie zum Starten der CD-Erstellung auf *Hinzufügen*. Verwenden Sie den Paket-Manager, um die Pakete auszuwählen, oder eine AutoYaST-Steuerdatei, um ein vorkonfiguriertes AutoYaST-Profil für die Erstellung einzusetzen.

7.10.2 Installationsserverkonfiguration.

Für die Netzwerkinstallation ist ein Installationsserver erforderlich. Verwenden Sie zum Konfigurieren eines solchen Servers das Modul *Verschiedenes* → *Installationsserver*. Weitere Informationen zur Konfiguration eines Installationservers mit YaST finden Sie in [Abschnitt 4.2.1, „Einrichten eines Installationservers mithilfe von YaST“](#) (S. 86).

7.10.3 iSCSI-Konfiguration

Die iSCSI-Technologie bietet eine einfache und günstige Lösung für die Verbindung von Linux-Computern mit zentralen Speichersystemen. Verwenden Sie zum Konfigu-

rieren der Serverseite das Modul *Verschiedenes* → *iSCSI-Ziel*. Zum Konfigurieren einer Verbindung zum zentralen Speicher verwenden Sie *Verschiedenes* → *iSCSI-Initiator*. Weitere Informationen zur Konfiguration von iSCSI mit YaST finden Sie in [Kapitel 11, Massenspeicher über IP-Netzwerke – iSCSI](#) (S. 285).

7.10.4 Automatische Installation

Dieser Teil von SUSE Linux Enterprise ist das AutoYaST-Werkzeug für die automatisierte Installation. Bereiten Sie unter *Verschiedenes* → *Autoinstallation* Profile für dieses Werkzeug vor. Detaillierte Informationen zur automatisierten Installation mit AutoYaST finden Sie in [Kapitel 5, Automatisierte Installation](#) (S. 115). Informationen zur Verwendung des Moduls *Autoinstallation* finden Sie in [Abschnitt 5.1.1, „Erstellen eines AutoYaST-Profiles“](#) (S. 116).

7.10.5 Support-Anfrage

Das Modul *Verschiedenes* → *Support-Anfrage* bietet Ihnen eine Möglichkeit zum Sammeln aller Systeminformationen, die das Support-Team zur Lösung Ihres aktuellen Problems benötigt. Auf diese Weise können Sie so schneller Hilfe erhalten. Wählen Sie die Problemkategorie, die Ihrem Problem entspricht, im folgenden Fenster aus. Wenn alle Informationen gesammelt wurden, können Sie diese an Ihre Support-Anfrage anhängen.

7.10.6 Versionshinweise

Die Versionshinweise sind eine wichtige Quelle zu Installation, Aktualisierung, Konfiguration und technischen Problemen. Die Versionshinweise werden fortlaufend aktualisiert und mittels Online-Update veröffentlicht. Verwenden Sie das Modul *Verschiedenes* → *Versionshinweise*, um die Versionshinweise anzuzeigen.

7.10.7 Startprotokoll

Informationen zum Start des Computers finden Sie im Modul *Verschiedenes* → *Startprotokoll*. Dieses Protokoll ist eine der ersten Informationsquellen bei Problemen mit dem System oder bei der Fehlersuche. Es enthält das Bootprotokoll `/var/log/boot.msg`, das die beim Starten des Computers angezeigten Bildschirmmeldungen

enthält. Durch Prüfen des Protokolls können Sie ermitteln, ob der Computer ordnungsgemäß gestartet wurde und ob alle Dienste und Funktionen korrekt gestartet wurden.

7.10.8 Systemprotokoll

Mithilfe von *Verschiedenes* → *Systemprotokoll* können Sie das Systemprotokoll anzeigen, in dem die Vorgänge des Computers unter `var/log/messages` aufgezeichnet werden. Auch Kernel-Meldungen werden hier, nach Datum und Uhrzeit sortiert, aufgezeichnet. Mithilfe des Felds ganz oben können Sie den Status bestimmter Systemkomponenten anzeigen. In den Modulen "Systemprotokoll" und "Bootprotokoll" stehen folgende Optionen zur Verfügung:

`/var/log/messages`

Dies ist die allgemeine Systemprotokolldatei. Hier können Sie Kernel-Meldungen, die als `root` angemeldeten Benutzer und andere nützliche Informationen anzeigen.

`/proc/cpuinfo`

Hier werden Prozessorinformationen wie Typ, Fabrikat, Modell und Leistung angezeigt.

`/proc/dma`

Hier werden die aktuell verwendeten DMA-Kanäle angezeigt.

`/proc/interrupts`

Hier finden Sie Informationen darüber, welche Interrupts verwendet werden und wie viele bisher verwendet wurden.

`/proc/iomem`

Hier wird der Status des Eingangs-/Ausgangsspeichers angezeigt.

`/proc/ioports`

Hier wird angezeigt, welche E/A-Ports zurzeit verwendet werden.

`/proc/meminfo`

Zeigt den Status des Arbeitsspeichers an.

`/proc/modules`

Zeigt die einzelnen Module an.

`/proc/mounts`
Zeigt die zurzeit eingehängten Geräte an.

`/proc/partitions`
Zeigt die Partitionierung aller Festplatten an.

`/proc/version`
Zeigt die aktuelle Linux-Version an.

`/var/log/YaST2/y2log`
Hier werden alle YaST-Protokollmeldungen angezeigt.

`/var/log/boot.msg`
Zeigt Informationen zum Start des Systems an.

`/var/log/faillog`
Hier werden Anmeldefehler angezeigt.

`/var/log/warn`
Zeigt alle Systemwarnungen an.

7.10.9 Treiber-CD des Herstellers

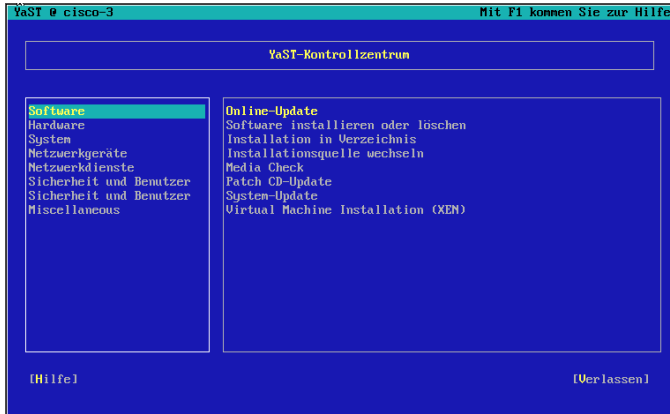
Mithilfe von *Verschiedenes* → *Treiber-CD des Herstellers* können Sie Gerätetreiber von einer Linux-Treiber-CD installieren, die Treiber für SUSE Linux Enterprise enthält. Wenn Sie eine vollständige Neuinstallation von SUSE Linux Enterprise durchführen, können Sie mit diesem YaST-Modul nach der Installation die erforderlichen Treiber von der Hersteller-CD laden.

7.11 YaST im Textmodus

Beim Start von YAST im Textmodus wird zuerst das YaST-Kontrollzentrum angezeigt. Siehe [Abbildung 7.7](#), „Hauptfenster von YaST im Textmodus“ (S. 203). 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 7.7 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 auf `→`. Die Modulauswahl ist nun mit einem dicken Rahmen umgeben. Mit `↓` und `↑` können Sie die Kategorie ändern. 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. Beenden Sie das YaST-Kontrollzentrum durch Drücken von *Verlassen* oder durch Auswahl von *Verlassen* in der Kategorieübersicht und Drücken der `Eingabetaste`.

7.11.1 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 7.11.2](#), „Einsch-

ränkung der Tastenkombinationen“ (S. 205) 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 (**↑** und **↓**) 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** + **→** bzw. **Umschalt** + **←** horizontal nach links und rechts blättern. Alternativ können Sie **Strg** + **E** oder **Strg** + **A** verwenden. Diese Kombination kann auch verwendet werden, wenn **→** bzw. **←** zu einem Wechsel des aktiven Rahmens oder der aktuellen Auswahlliste führen würde, wie dies im Kontrollzentrum der Fall ist.

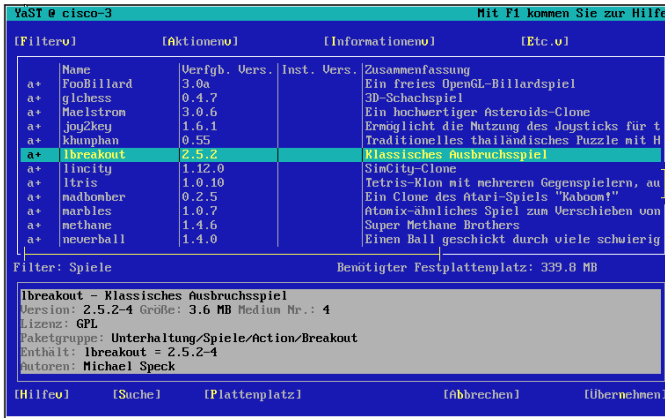
Schaltflächen, Optionsschaltfläche und Kontrollkästchen

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 7.8 Das Software-Installationsmodul



7.11.2 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]**.

Navigation vor und zurück mit **[Strg] + [F]** und **[Strg] + [B]**

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

Einschränkung der Funktionstasten

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

7.11.3 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` bzw. `yast --list` anzeigen. Das Netzwerkmodul beispielsweise wird mit `yast lan` gestartet.

7.12 Aktualisierung über die Kommandozeile

SUSE Linux Enterprise wird mit einem neuen Kommandozeilenwerkzeug (`rug`) für die Installation und Aktualisierung von Paketen geliefert. Mithilfe des `rcd`-Daemons wird Software gemäß den angegebenen Befehlen installiert, aktualisiert und entfernt. Das Kommandozeilenwerkzeug kann Software aus lokalen Dateien oder von Servern installieren. Sie können einen oder mehrere entfernte Server, so genannte Dienste, verwenden. Unterstützte Dienste sind beispielsweise `mount` für lokale Dateien sowie `yum` oder `ZENworks` für Server.

Das Kommandozeilenwerkzeug `rug` teilt Software in Kataloge (auch als Kanäle bezeichnet), Gruppen oder ähnliche Software ein. Ein Katalog kann beispielsweise Software von einem Aktualisierungsserver enthalten, wohingegen ein anderer Katalog Software von einem Drittanbieter aufweist. Abonnieren Sie einzelne Kataloge, um die Anzeige der verfügbaren Pakete zu steuern und zu vermeiden, dass unerwünschte Software versehentlich installiert wird. Es werden normalerweise nur Vorgänge im Zusammenhang mit Software aus Katalogen, die Sie abonniert haben, durchgeführt.

Der am häufigsten verwendete Befehl ist `rug update`. Hiermit werden Patches aus Katalogen heruntergeladen und installiert, die Sie abonniert haben. Wenn Sie nur Software aktualisieren möchten, ist dies der einzige Befehl, den Sie benötigen. Wenn Sie eine Liste aller Pakete aus einem Katalog abrufen möchten, verwenden Sie `rug pa katalogname`. Ersetzen Sie `katalogname` durch den Namen Ihres Katalogs. Um alle verfügbaren Dienste aufzuführen, verwenden Sie `rug sl`. Einige andere sinnvolle `rug`-Befehle und ihre Funktionen erhalten Sie in [Tabelle 7.1, „rug-Befehle“](#) (S. 207).

Tabelle 7.1 *rug-Befehle*

Befehl	Funktion
ca	Kataloge auflisten
sa	Dienst hinzufügen
reg	Dienst registrieren
sub	Abonnieren eines Katalogs
refresh	Liste der Patches aktualisieren

7.12.1 Benutzerverwaltung mit rug

Einer der größten Vorteile von rug ist die Benutzerverwaltung. Normalerweise kann nur der Benutzer `root` neue Pakete aktualisieren oder installieren. Mithilfe von rug können Sie anderen Benutzern beispielsweise das Recht zur Aktualisierung des Systems erteilen und gleichzeitig das Recht zum Entfernen der Software beschränken. Folgende Berechtigungen können erteilt werden:

`install`

Der Benutzer kann neue Software installieren.

`lock`

Der Benutzer kann Paketsperren festlegen.

`remove`

Der Benutzer kann Software entfernen.

`subscribe`

Der Benutzer kann Kanalabonnements ändern.

`trusted`

Der Benutzer gilt als verbürgt und kann daher Pakete ohne Paketsignaturen installieren.

upgrade

Der Benutzer kann Softwarepakete aktualisieren.

view

Der Benutzer kann anzeigen, welche Software auf dem Computer installiert und welche Software über Kanäle verfügbar ist. Diese Option ist nur für entfernte Benutzer relevant; lokale Benutzer sind in der Regel berechtigt, die installierten und verfügbaren Pakete anzuzeigen.

superuser

Erlaubt dem Benutzer die Verwendung aller `rug`-Befehle, mit Ausnahme der Benutzerverwaltung und der Einstellungen, die lokal vorgenommen werden müssen.

Verwenden Sie den Befehl `rug ua benutzername upgrade`, um einem Benutzer die Berechtigung zur Aktualisierung des Systems zu erteilen. Ersetzen Sie *benutzername* durch den Namen des Benutzers. Zum Widerrufen der Berechtigungen eines Benutzers verwenden Sie den Befehl `rug ud benutzername`. Um die Benutzer zusammen mit ihren Rechten aufzuführen, verwenden Sie `rug ul`.

Zum Ändern der aktuellen Berechtigungen eines Benutzers verwenden Sie den Befehl `rug ude benutzername`. Ersetzen Sie *benutzername* durch den Namen des gewünschten Benutzers. Der Bearbeitungsbefehl ist interaktiv. Er listet die Berechtigungen des ausgewählten Benutzers auf und zeigt dann eine Eingabeaufforderung an. Geben Sie ein Plus- (+) oder Minuszeichen (-) sowie den Namen der Berechtigung ein und drücken Sie dann die Eingabetaste. Um einem Benutzer beispielsweise das Löschen von Software zu gestatten, geben Sie `+remove` ein. Zum Speichern und Beenden drücken Sie die Eingabetaste in einer leeren Zeile.

7.12.2 Planen von Aktualisierungen

Mithilfe von `rug` ist eine automatische Aktualisierung des Systems, beispielsweise mit Skripts, möglich. Das einfachste Beispiel ist die vollautomatische Aktualisierung. Um diesen Vorgang als `root` auszuführen, konfigurieren Sie einen Cronjob, der `rug up -y` ausführt. Mithilfe der Option `up -y` werden die Patches aus Ihren Katalogen ohne Bestätigung heruntergeladen und installiert.

Sie möchten jedoch möglicherweise nicht, dass die Patches automatisch installiert werden. Stattdessen möchten Sie die Patches lieber abrufen und die zu installierenden Patches zu einem späteren Zeitpunkt auswählen. Um die Patches lediglich herunterzu-

laden, verwenden Sie den Befehl `rug up -dy`. Die Option `up -dy` lädt die Patches aus Ihren Katalogen ohne Bestätigung herunter und speichert Sie im rug-Cache. Der Standardspeicherort des rug-Cache ist `/var/cache/redcarpet`.

7.12.3 Konfigurieren von rug

rug wird mit vielen Einstellungen geliefert, um die Aktualisierungsfunktionalität in verschiedenen Netzwerkkonfigurationen zu ermöglichen. Um die Einstellungen aufzulisten, die festgelegt werden können, verwenden Sie `rug get`. Um eine Einstellungsvariable festzulegen, geben Sie `rug set` ein. Passen Sie beispielsweise die Einstellungen an, wenn Sie Ihr System aktualisieren möchten, der Computer sich jedoch hinter einem Proxyserver befindet. Senden Sie, bevor Sie Aktualisierungen herunterladen, Ihren Benutzernamen und Ihr Passwort an den Proxyserver. Verwenden Sie hierfür folgende Befehle:

```
rug set proxy-url url_path
rug set proxy-username name
rug set proxy-password password
```

Ersetzen Sie `url_path` durch den Namen des Proxyservers. Ersetzen Sie `name` durch Ihren Benutzernamen. Ersetzen Sie `password` durch Ihr Passwort.

7.12.4 Weitere Informationen

Weitere Informationen zur Aktualisierung über die Kommandozeile erhalten Sie durch die Eingabe von `rug --help` oder ziehen Sie die Manualpage `rug(1)` zurate. Die Option `--help` ist zudem für alle rug-Befehle verfügbar. Wenn Sie beispielsweise Hilfe zu `rug update` benötigen, geben Sie `rug update --help` ein.

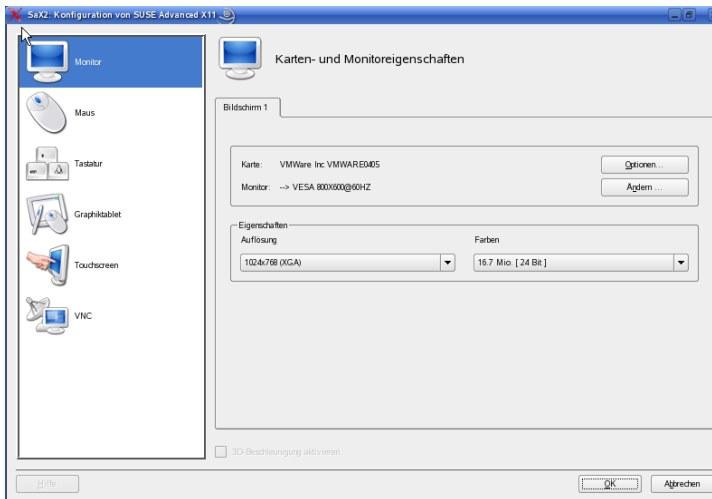
7.13 SaX2

Sie können die grafische Umgebung Ihres Systems mithilfe von *Hardware* → *Grafikkarte und Monitor* konfigurieren. Dadurch wird die Konfigurationsschnittstelle SUSE Advanced X11 (SaX2) geöffnet, mit der Sie Geräte, wie Maus, Tastatur oder Anzeigegeräte, konfigurieren können. Die Schnittstelle kann auch über das Hauptmenü aufgerufen werden. Klicken Sie dazu auf *System* → *Konfiguration* → *SaX2*.

7.13.1 Karten- und Monitoreigenschaften

Sie können die Einstellungen für Ihre Grafikkarte und Ihr Anzeigegerät unter *Karten- und Monitoreigenschaften* anpassen. Wenn mehrere Grafikkarten installiert sind, werden die einzelnen Geräte in separaten Dialogfeldern angezeigt, die über einen Dateireiter aufgerufen werden können. Oben im Dialogfeld werden die aktuellen Einstellungen für die ausgewählte Grafikkarte und den Monitor angezeigt, der daran angeschlossen ist. Falls mehrere Bildschirme an die Karte angeschlossen werden können (Dual Head), wird der Monitor an der primären Ausgabe angezeigt. Normalerweise werden Karte und Anzeigegerät automatisch während der Installation vom System erkannt. Die Feineinstellung für viele Parameter kann jedoch auch manuell vorgenommen werden. Sogar ein vollständiger Austausch des Anzeigegeräts ist möglich.

Abbildung 7.9 Karten- und Monitoreigenschaften



TIPP: Automatische Erkennung neuer Anzeige-Hardware.

Wenn Sie die Anzeige-Hardware nach der Installation ändern, können Sie durch Eingabe von `sax2 -r` in der Kommandozeile erreichen, dass SaX2 die Hardware erkennt. Sie müssen über `root`-Berechtigungen verfügen, um SaX2 über die Kommandozeile ausführen zu können.

Grafikkarte

Es ist nicht möglich, die Grafikkarte zu ändern, da nur bekannte Modelle unterstützt werden und diese automatisch erkannt werden. Sie können jedoch viele Optionen ändern, die sich auf das Verhalten der Karte auswirken. Normalerweise sollte dies nicht erforderlich sein, da das System sie bereits bei der Installation in geeigneter Weise eingerichtet hat. Wenn Sie ein Experte sind und einige der Optionen optimieren möchten, klicken Sie auf *Optionen* neben der Grafikkarte und wählen Sie die zu ändernde Option aus. Um einer bestimmten Option einen benötigten Wert zuzuweisen, geben Sie diesen Wert in das Dialogfeld ein, das nach der Auswahl dieser Option angezeigt wird. Klicken Sie auf *OK*, um das Dialogfeld mit den Optionen zu schließen.

Monitor

Wenn Sie die aktuellen Einstellungen für den Monitor ändern möchten, klicken Sie neben dem Monitor auf *Ändern*. Ein neues Dialogfeld wird geöffnet, in dem Sie verschiedene monitorspezifische Einstellungen anpassen können. Dieses Dialogfeld verfügt über verschiedene Dateireiter für die verschiedenen Aspekte des Monitorbetriebs. Wählen Sie den ersten Dateireiter, um den Hersteller und das Modell des Anzeigergeräts in zwei Listen auszuwählen. Falls Ihr Monitor nicht aufgeführt ist, können Sie nach Bedarf einen der VESA- oder LCD-Modi wählen oder klicken Sie, sofern Sie über eine Treiberdiskette oder -CD des Herstellers verfügen, auf *Diskette* und befolgen Sie die Anweisungen auf dem Bildschirm, um diese zu verwenden. Aktivieren Sie das Kontrollkästchen *DPMS aktivieren*, um die Signalisierung mithilfe der Power-Management-Anzeige zu verwenden. *Anzeigegröße* mit den geometrischen Eigenschaften des Monitors und *Synchronisationsfrequenzen* mit den Bereichen für die horizontalen und vertikalen Synchronisierungsfrequenzen Ihres Monitors werden normalerweise korrekt vom System eingerichtet, Sie können diese Werte jedoch manuell bearbeiten. Klicken Sie nach den Anpassungen auf *OK*, um dieses Dialogfeld zu schließen.

WARNUNG: Ändern der Monitorfrequenzen

Obwohl es Sicherheitsmechanismen gibt, sollten Sie nach wie vor mit Bedacht vorgehen, wenn Sie die zulässigen Monitorfrequenzen manuell ändern. Falsche Werte können zur Zerstörung Ihres Monitors führen. Sie sollten grundsätzlich das Handbuch des Monitors zurate ziehen, bevor Sie die Frequenzen ändern.

Auflösung und Farbtiefe

Die Auflösung und Farbtiefe können direkt über zwei Listen in der Mitte des Dialogfelds ausgewählt werden. Die Auflösung, die Sie hier auswählen, ist die höchste zu verwendende Auflösung. Alle gängigen Auflösungen bis hin zu 640x480 werden ebenfalls automatisch zur Konfiguration hinzugefügt. Je nach dem verwendeten grafischen Desktop können Sie später in diese Auflösungen wechseln, ohne eine erneute Konfiguration durchführen zu müssen.

Dual Head

Wenn auf Ihrem Computer eine Grafikkarte mit zwei Ausgaben installiert ist, können Sie zwei Bildschirme am System installieren. Zwei Bildschirme, die an dieselbe Grafikkarte angeschlossen sind, werden als *Dual Head* bezeichnet. SaX2 erkennt automatisch mehrere Anzeigegeräte auf dem System und bereitet die Konfiguration entsprechend vor. Um den Dual Head-Modus einer Grafikkarte zu verwenden, aktivieren Sie die Option *Dual Head-Modus aktivieren* unten im Dialogfeld und klicken Sie auf *Konfigurieren*, um die Dual Head-Optionen festzulegen und die Anordnung der Bildschirme im Dual Head-Dialogfeld festzulegen.

Die Registerkarten in der Zeile oben im Dialogfeld entsprechen jeweils einer Grafikkarte in Ihrem System. Wählen Sie die zu konfigurierende Karte aus und legen Sie ihre Multihead-Optionen im Dialogfeld fest. Klicken Sie oben im Multihead-Dialogfeld auf *Ändern*, um den zusätzlichen Bildschirm zu konfigurieren. Die möglichen Optionen entsprechen denen für den ersten Bildschirm. Wählen Sie die für diesen Bildschirm zu verwendende Auflösung aus der Liste aus. Wählen Sie eine der drei möglichen Multihead-Modi.

Traditionelles Multihead

Jeder Monitor stellt eine individuelle Einheit dar. Der Mauszeiger kann zwischen den Bildschirmen wechseln.

Cloned Multihead

In diesem Modus zeigen alle Monitore dieselben Inhalte an. Die Maus ist nur auf dem Hauptbildschirm sichtbar.

Xinerama Multihead

Alle Bildschirme werden zu einem einzigen großen Bildschirm zusammengefasst. Programmfenster können frei auf allen Bildschirmen positioniert oder auf eine Größe skaliert werden, die mehrere Monitore ausfüllt.

ANMERKUNG

Linux bietet zurzeit keine 3D-Unterstützung für Xinerama Multihead-Umgebungen an. In diesem Fall deaktiviert SaX2 die 3D-Unterstützung.

Die Anordnung der Dual Head-Umgebung beschreibt die Abfolge der einzelnen Bildschirme. Standardmäßig konfiguriert SaX2 ein Standardlayout, das die Abfolge der erkannten Bildschirme befolgt und alle Bildschirme in einer Reihe von links nach rechts anordnet. Legen Sie im Bereich *Anordnung* des Dialogfelds fest, wie die Monitore angeordnet werden sollen, indem Sie eine der Abfolgeschaltflächen wählen. Klicken Sie auf *OK*, um das Dialogfeld zu schließen.

TIPP: Verwenden eines Beamers mit Notebook-Computern

Um einen Beamer an einen Notebook-Computer anzuschließen, aktivieren Sie den Dual Head-Modus. In diesem Fall konfiguriert SaX2 die externe Ausgabe mit einer Auflösung von 1024x768 und einer Aktualisierungsrate von 60 Hz. Diese Werte sind für die meisten Beamer sehr gut geeignet.

Multihead

Falls auf Ihrem Computer mehrere Grafikkarten installiert sind, können Sie mehrere Bildschirme an Ihr System anschließen. Zwei oder mehr Bildschirme, die an verschiedene Grafikkarten angeschlossen sind, werden als *Multihead* bezeichnet. SaX2 erkennt automatisch mehrere Grafikkarten auf dem System und bereitet die Konfiguration entsprechend vor. Standardmäßig konfiguriert SaX2 ein Standardlayout, das die Abfolge der erkannten Grafikkarten befolgt und alle Bildschirme in einer Reihe von links nach rechts anordnet. Der zusätzliche Dateireiter *Anordnung* ermöglicht das manuelle Ändern dieses Layouts. Ziehen Sie die Symbole, die für die einzelnen Bildschirme stehen, auf das Raster und klicken Sie auf *OK*, um das Dialogfeld zu schließen.

Testen der Konfiguration

Klicken Sie im Hauptfenster auf *OK*, nachdem Sie die Einstellungen für den Monitor und die Grafikkarte vorgenommen haben, und testen Sie anschließend die Einstellungen. Auf diese Weise stellen Sie sicher, dass die vorliegende Konfiguration sich für Ihre Geräte eignet. Falls Sie kein stabiles Bild erhalten, brechen Sie den Test sofort ab, indem Sie `[Strg]+[Alt]+[Leertaste]` drücken und reduzieren Sie die Aktualisierungsrate oder die Auflösung und die Farbtiefe.

ANMERKUNG

Unabhängig davon, ob Sie einen Test durchführen, werden sämtliche Änderungen nur aktiviert, wenn Sie den X-Server neu starten.

7.13.2 Mauseigenschaften

Die Einstellungen für Ihre Maus können Sie unter *Mauseigenschaften* anpassen. Wenn Mäuse mit verschiedenen Treibern installiert sind, werden die einzelnen Treiber auf separaten Dateireitern angezeigt. Mehrere Geräte, die über denselben Treiber betrieben werden, werden als eine einzige Maus angezeigt. Sie können die aktuell ausgewählte Maus mithilfe des Kontrollkästchens oben im Dialogfeld aktivieren bzw. deaktivieren. Unter dem Kontrollkästchen werden die aktuellen Einstellungen für die entsprechende Maus angezeigt. Normalerweise wird die Maus automatisch erkannt, Sie können sie jedoch automatisch ändern, falls ein Fehler mit der automatischen Erkennung auftritt. Ziehen Sie die Dokumentation für Ihre Maus zurate, um eine Beschreibung des Modells zu erhalten. Klicken Sie auf *Ändern*, um den Hersteller und das Modell aus zwei Listen auszuwählen, und klicken Sie dann auf *OK*, um Ihre Auswahl zu bestätigen. Legen Sie im Optionsbereich des Dialogfelds verschiedene Optionen für den Betrieb Ihrer Maus fest.

3-Tasten-Emulation aktivieren

Falls Ihre Maus nur zwei Tasten hat, wird eine dritte Taste emuliert, wenn Sie gleichzeitig beide Tasten drücken.

Mausrad aktivieren

Aktivieren Sie dieses Kontrollkästchen, um das Mousrad zu verwenden.

Rad mit Maustaste emulieren

Falls Ihre Maus kein Mausrad hat, Sie aber eine ähnliche Funktion verwenden möchten, können Sie hierfür eine zusätzliche Taste zuweisen. Wählen Sie die zu verwendende Taste aus. Während Sie diese Taste gedrückt halten, werden alle Bewegungen der Maus in Mausradbefehle übersetzt. Diese Funktion eignet sich besonders für Trackballs.

Wenn Sie mit Ihren Einstellungen zufrieden sind, klicken Sie auf *OK*, um die Änderungen zu bestätigen.

ANMERKUNG

Sämtliche Änderungen, die Sie vornehmen, werden erst wirksam, nachdem Sie den X-Server neu gestartet haben.

7.13.3 Tastatureigenschaften

Mithilfe dieses Dialogfelds können Sie die Einstellungen für den Betrieb Ihrer Tastatur in der grafischen Umgebung anpassen. Wählen Sie oben im Dialogfeld Typ, Sprache und Variante aus. Verwenden Sie das Testfeld unten im Dialogfeld, um zu überprüfen, ob Sonderzeichen richtig angezeigt werden. Wählen Sie zusätzliche Layouts und Varianten, die Sie verwenden möchten, in der mittleren Liste aus. Je nach dem Typ Ihres Desktops können diese im ausgeführten System gewechselt werden, ohne dass eine erneute Konfiguration erfolgen muss. Wenn Sie auf *OK* klicken, werden die Änderungen sofort übernommen.

7.13.4 Tablet-Eigenschaften

In diesem Dialogfeld können Sie ein an Ihr System angeschlossenes Grafik-Tablet konfigurieren. Klicken Sie auf die Registerkarte *Grafik-Tablet*, um Hersteller und Modell aus den Listen auszuwählen. Derzeit unterstützt SUSE® Linux Enterprise nur eine begrenzte Anzahl von Grafik-Tablets. Um das Tablet zu aktivieren, markieren Sie oben im Dialogfeld die Option *Dieses Tablet aktivieren*.

Im Dialogfeld *Port und Modus* konfigurieren Sie die Verbindung zum Tablet. Mit SaX2 können Sie Grafik-Tablets konfigurieren, die mit dem USB-Port oder dem seriellen Port verbunden sind. Wenn Ihr Tablet mit dem seriellen Port verbunden ist, müssen Sie den Port überprüfen. `/dev/ttyS0` bezieht sich auf den ersten seriellen Anschluss.

`/dev/ttyS1` bezieht sich auf den zweiten seriellen Anschluss. Für weitere Anschlüsse wird eine ähnliche Notation verwendet. Wählen Sie geeignete *Optionen* in der Liste aus und wählen Sie unter *Primärer Tablet-Modus* den für Ihre Bedürfnisse geeigneten Modus aus.

Wenn Ihr Grafik-Tablet elektronische Stifte unterstützt, können Sie diese unter *Elektronische Stifte* konfigurieren. Fügen Sie einen Radiergummi und einen Stift hinzu und legen Sie deren Eigenschaften fest, nachdem Sie auf *Eigenschaften* geklickt haben.

Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie auf *OK*, um die Änderungen zu bestätigen.

7.13.5 Touchscreen-Eigenschaften

In diesem Dialogfeld können Sie einen an Ihr System angeschlossenen Touchscreen konfigurieren. Wenn mehrere Touchscreens installiert sind, werden die einzelnen Geräte in separaten Dialogfeldern angezeigt, die über einen Dateireiter aufgerufen werden können. Um den aktuell ausgewählten Touchscreen zu aktivieren, wählen Sie oben im Dialogfeld *Touchscreen für Anzeige zuweisen* aus. Wählen Sie Hersteller und Modell in den Listen unten aus und legen Sie am unteren Bildschirmrand einen geeigneten *Anschlussport* fest. Sie können Touchscreens konfigurieren, die über den USB-Anschluss oder den seriellen Anschluss verbunden sind. Wenn Ihr Touchscreen mit dem seriellen Port verbunden ist, müssen Sie den Port überprüfen. `/dev/ttyS0` bezieht sich auf den ersten seriellen Anschluss. `/dev/ttyS1` bezieht sich auf den zweiten seriellen Anschluss. Für weitere Anschlüsse wird eine ähnliche Notation verwendet. Wenn Sie mit Ihren Einstellungen zufrieden sind, klicken Sie auf *OK*, um die Änderungen zu bestätigen.

7.13.6 Eigenschaften für den entfernten Zugriff

VNC (*Virtual Network Computing*) ist eine Client-Server-Lösung, mit der der Zugriff auf einen entfernten X-Server über einen schlanken, leicht zu bedienenden Client möglich ist. Dieser Client ist für eine Vielzahl von Betriebssystemen verfügbar, darunter Microsoft Windows, MacOS von Apple und Linux. Weitere Informationen zu VNC finden Sie unter <http://www.realvnc.com/>.

Mit diesem Dialogfeld können Sie den X-Server als Host für VNC-Sitzungen konfigurieren. Wenn VNC-Clients eine Verbindung mit Ihrem X-Server herstellen sollen, müssen Sie *Zugriff auf die Anzeige über das VNC-Protokoll zulassen* aktivieren. Legen Sie ein Passwort fest, um den Zugriff auf den VNC-aktivierten X-Server zu beschränken. Aktivieren Sie *Mehrere VNC-Verbindungen zulassen*, wenn mehrere VNC-Clients gleichzeitig eine Verbindung zum X-Server herstellen sollen. HTTP-Zugriff können Sie zulassen, indem Sie die Option *HTTP-Zugriff aktivieren* aktivieren und unter *HTTP-Port* den zu verwendenden Port festlegen.

Wenn Sie mit Ihren Einstellungen zufrieden sind, klicken Sie auf *OK*, um die Änderungen zu speichern.

7.14 Fehlerbehebung

Alle Fehler- und Alarmmeldungen werden im Verzeichnis `/var/log/YaST2` protokolliert. Die wichtigste Datei für das Aufspüren von YaST-Problemen ist `y2log`.

7.15 Weitere Informationen

Weitere Informationen zu YaST finden Sie auf den folgenden Websites und in folgenden Verzeichnissen:

- `/usr/share/doc/packages/yast2` – Lokale YaST-Entwicklungsdokumentation
- http://www.opensuse.org/YaST_Development – YaST-Projektseite in der openSUSE-Wiki
- <http://forge.novell.com/modules/xfmod/project/?yast> – Eine weitere YaST-Projektseite

Aktualisieren von SUSE Linux Enterprise

8

SUSE® Linux Enterprise bietet die Möglichkeit, ein vorhandenes System ohne komplette Neuinstallation auf die neue Version zu aktualisieren. Es ist keine neue Installation erforderlich. Alte Daten, wie Home-Verzeichnisse und Systemkonfigurationen, bleiben erhalten. Während der Lebensdauer des Produkts können Sie Service Packs installieren, um die Systemsicherheit zu gewährleisten und Softwarefehler zu beheben.

8.1 Aktualisieren von SUSE Linux Enterprise

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 vor der Aktualisierung und partitionieren Sie Ihr System neu. Es gibt keine Faustregel hinsichtlich des Speicherplatzes einzelner Partitionen. Die Platzanforderungen hängen von Ihrem bestimmten Partitionsprofil und von der ausgewählten Software ab.

8.1.1 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 8.1, „Über `df -h` angezeigte Liste“](#) (S. 220) ist `/dev/hda3` die Root-Partition, die Sie sich notieren sollten (eingehängt als `/`).

Beispiel 8.1 Über `df -h` angezeigte Liste

```
Filesystem Size  Used Avail Use% Mounted on
/dev/hda3    74G   22G   53G  29% /
tmpfs        506M    0  506M   0% /dev/shm
/dev/hda5    116G   5.8G  111G   5% /home
/dev/hda1    39G   1.6G   37G   4% /windows/C
/dev/hda2    4.6G   2.6G   2.1G  57% /windows/D
```

8.1.2 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. Überprüfen Sie die folgenden Aspekte, bevor Sie das Systemupdate starten.

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.

8.1.3 Aktualisieren mit YaST

Im Anschluss an die in [Abschnitt 8.1.1, „Vorbereitung“](#) (S. 219) erläuterte Vorbereitung kann Ihr System nun aktualisiert werden:

- 1** Bereiten Sie einen optionalen Installationsserver vor. Weitere Informationen finden Sie unter [Abschnitt 4.2.1, „Einrichten eines Installationsservers mithilfe von YaST“](#) (S. 86).
- 2** Booten Sie das System wie zu Installationszwecken (siehe Beschreibung in [Abschnitt 3.2, „Systemstart für die Installation“](#) (S. 38)). Wählen Sie in YaST eine Sprache aus und klicken Sie im Dialogfeld *Installationsmodus* auf *Aktualisieren*. Wählen Sie nicht die Option *Neuinstallation*.
- 3** 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 8.1.1, „Vorbereitung“](#) (S. 219) wurde `/dev/hda3` ausgewählt). YaST liest die alte `fstab` auf dieser Partition, um die hier aufgeführten Dateisysteme zu analysieren und einzuhängen.
- 4** 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.

- 5** Geben Sie im daraufhin angezeigten Dialogfeld an, dass nur die bereits installierte Software aktualisiert werden soll oder dass dem System neue Software-Komponenten hinzugefügt werden sollen (Aufrüstungsmodus). Sie sollten die vorgeschlagene Option akzeptieren. Anpassungen sind zu einem späteren Zeitpunkt mit YaST möglich.

8.2 Installieren von Service Packs

Mit Service Packs können Sie eine SUSE Linux Enterprise-Installation aktualisieren. Es gibt verschiedene Möglichkeiten zur Anwendung eines Service Pack. Entweder Sie aktualisieren die vorhandene Installation oder Sie starten eine völlig neue Installation mit den Service Pack-Medien. Mögliche Szenarios zum Aktualisieren des Systems und zum Einrichten einer zentralen Netzwerkinstallationsquelle werden im Folgenden beschrieben.

TIPP

Lesen Sie die Installationsanweisungen auf den Service Pack-Medien auf weitere Änderungen durch.

8.2.1 Einrichten einer Netzwerkinstallationsquelle für Service Pack-Medien

Wie bei der anfänglichen Installation von SUSE Linux Enterprise ist eine zentrale Installationsquelle auf Ihrem Netzwerk, auf die alle Clients zugreifen, wesentlich effizienter als die Installation auf jedem einzelnen Client mithilfe tatsächlicher Installationsmedien.

Konfigurieren einer Netzwerkinstallationsquelle unter SUSE Linux Enterprise mithilfe von YaST

Folgen Sie der Methode in [Abschnitt 4.2.1, „Einrichten eines Installationsservers mithilfe von YaST“](#) (S. 86). Fügen Sie lediglich eine andere Installationsquelle mit dem Namen `SLE-10-SP-x-arch`, `SLES-10-SP-x-arch` oder `SLED-10-SP-x-arch` (wobei *x* die Nummer des Service Pack und *arch* der Name Ihrer Hardware-Architektur ist) hinzu und machen Sie sie über NFS, HTTP oder FTP verfügbar.

Manuelles Einrichten einer Netzwerkinstallationsquelle

Die Vorgehensweise für das manuelle Einrichten einer Netzwerkinstallationsquelle ist ähnlich wie die unter [Abschnitt 4.2.2, „Manuelles Einrichten einer NFS-Installationsquelle“](#) (S. 88) beschriebene. Sie müssen lediglich ein paar kleinere Änderungen vornehmen, um Installationsquellen für FTP, HTTP und SMB einzurichten.

Beim Kopieren der Installationsmedien gehen Sie wie folgt vor:

- 1 Melden Sie sich als `root`-Benutzer an.
- 2 Wechseln Sie in das Verzeichnis, das die Originalinstallationsmedien enthält (in diesem Beispiel ins Verzeichnis `/install/sle` als `SLE-10-arch/CD1`), indem Sie Folgendes eingeben:

```
cd /install/sle
```

- 3 Erstellen Sie ein neues Unterverzeichnis, z. B. `SLE-10-SP-x-arch` (ersetzen Sie `x` durch die Nummer des SP und `arch` durch den Namen der Hardware-Architektur), indem Sie Folgendes eingeben:

```
mkdir SLE-10-SP-x-arch
```

- 4 Kopieren Sie den Inhalt jedes SP-Installationsmediums in sein eigenes Unterverzeichnis. Sobald Sie damit fertig sind, sieht die Verzeichnisstruktur wie folgt aus:

```
/install/sle/SLE-10-arch/CD1
                        /CD2
                        /CD3
                        /CD4
/install/sle/SLE-10-SP-x-arch/CD1
                        /CD2
                        /CD3
```

- 5 In `SLE-10-arch/CD1` erstellen Sie eine Datei mit dem Namen `Zusatzprodukte`. Der Inhalt von `Zusatzprodukte` legt fest, welcher Service Pack Ihrem SUSE Linux Enterprise 10 hinzugefügt wird. Das Dateiformat ist wie folgt:

```
media_url [path_on_media [product_1 [product_2 [...]]]
```

Wenn Sie den SP beispielsweise über NFS von `sun.example.com` anbieten möchten, machen Sie folgenden Eintrag in `Zusatzprodukte` (die Angabe eines Medienpfads, `produkt_1` etc. ist für Service Packs nicht erforderlich):

```
nfs://sun.example.com/install/sle/SLE-10-SP-x-arch/CD1
```

Ersetzen Sie `x` durch die tatsächliche Service Pack-Nummer und `arch` durch den Namen Ihrer Architektur.

- 6 Stellen Sie die Quellen über NFS, FTP oder HTTP zur Verfügung, wie unter [Abschnitt 4.2, „Einrichten des Servers, auf dem sich die Installationsquellen befinden“](#) (S. 85) beschrieben.

8.2.2 Installieren eines Service Packs

ANMERKUNG

Siehe [Abschnitt 8.2.3, „Aktualisieren auf einen Service Pack“](#) (S. 228) zum Aktualisieren eines vorhandenen SUSE Linux Enterprise 10-Systems auf ein SUSE Linux Enterprise 10 Service Pack (SP).

Das Installieren eines SUSE Linux Enterprise Service Packs funktioniert ähnlich wie die Installation der SUSE Linux Enterprise-Originalmedien. Wie bei der ursprünglichen Installation können Sie auswählen, ob Sie von einer lokalen CD oder DVD installieren oder von einem Netzwerkserver. Weitere Informationen zu diesen beiden Möglichkeiten finden Sie unter [Abschnitt 3.2.2, „Auswählen der Quelle der Installationsdaten“](#) (S. 39).

Installieren von einem lokalen CD- oder DVD-Laufwerk

Vergewissern Sie sich vor einer neuen Installation eines SUSE Linux Enterprise-SP, dass die folgenden Elemente verfügbar sind:

- Die Original-SUSE Linux Enterprise-Installationsdatenträger (CDs oder DVD)
- Alle Service Pack-Installationsmedien (CDs oder DVDs)

Es gibt zwei Möglichkeiten zur völlig neuen Installation eines SUSE Linux Enterprise-SP-Systems: Booten Sie entweder vom Original-Installationsmedium und registrieren

Sie den Service Pack als Zusatzprodukt, wie unter [Booten vom Original-Installationsmedium](#) (S. 225) beschrieben, oder booten Sie vom SP-Medium und legen Sie die Originalmedien ein, sobald Sie von YaST dazu aufgefordert werden (siehe [Booten vom Service Pack-Medium](#) (S. 225)).

Prozedur 8.1 *Booten vom Original-Installationsmedium*

- 1** Geben Sie das SUSE Linux Enterprise 10-Original-Bootmedium ein und booten Sie Ihre Maschine. Weitere Informationen finden Sie unter [Abschnitt 3.2](#), „Systemstart für die Installation“ (S. 38).
- 2** Im YaST-Dialogfeld *Installationsmodus* wählen Sie *Neue Installation* und aktivieren *Include Add-On Products from Separate Media* (Zusatzprodukte von separaten Medien eingeschlossen).
- 3** YaST fordert Sie auf, das SP-Medium als Zusatzprodukt zu registrieren. Sobald Sie damit fertig sind, führen Sie die gewöhnliche Installation, wie unter [Kapitel 3](#), *Installation mit YaST* (S. 37) beschrieben, aus.

Prozedur 8.2 *Booten vom Service Pack-Medium*

- 1** Legen Sie das erste SUSE Linux Enterprise-SP-Medium (CD oder DVD Nr. 1) ein und booten Sie Ihren Computer. Ein ähnlicher Startbildschirm wie bei der ursprünglichen Installation von SUSE Linux Enterprise 10 wird angezeigt.
- 2** Wählen Sie *Installation*, um den SP-Kernel zu booten. Der Kernel wird geladen. Warten Sie, bis Sie aufgefordert werden, die CD1 des Produkts einzulegen.
- 3** Legen Sie das SUSE Linux Enterprise 10-Original-Installationsmedium Nr. 1 ein und klicken Sie dann auf *OK*, um die reguläre Installation auszuführen.
- 4** Akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann eine Sprache, ein Standard-Desktop und andere Installationseinstellungen.
- 5** Klicken Sie auf *Ja, installieren*, um mit der Installation zu beginnen.
- 6** Legen Sie bei jeder Aufforderung das entsprechende Medium ein. Sowohl die SP-Medien als auch die Original-Produktmedien sind erforderlich, je nach der installierten Software.

- 7 Fahren Sie wie gewohnt mit der Installation fort (geben Sie ein Passwort für `root` ein, schließen Sie die Netzwerkkonfiguration ab, testen Sie die Internet-Verbindung, aktivieren Sie den ZENworks® Online Update Service, wählen Sie die Benutzerauthentifizierungsmethode und geben Sie einen Benutzernamen und ein Passwort ein).

Netzwerkinstallation

Vergewissern Sie sich vor der Netzwerkinstallation eines SUSE Linux Enterprise SP, dass die folgenden Voraussetzungen gegeben sind:

- Eine Netzwerkinstallationsquelle, wie unter [Abschnitt 8.2.1, „Einrichten einer Netzwerkinstallationsquelle für Service Pack-Medien“](#) (S. 222), ist eingerichtet.
- Eine funktionierende Netzwerkverbindung auf dem Installationsserver und dem Zielcomputer, der einen Namensdienst, DHCP (optional, aber erforderlich für den PXE-Boot) und OpenSLP (optional) enthält.
- Die SUSE Linux Enterprise-SP-CD oder -DVD Nr. 1 zum Starten des Zielsystems *oder* ein Zielsystem für PXE-Boot, gemäß [Abschnitt 4.3.5, „Vorbereiten des Zielsystems für PXE-Boot“](#) (S. 105).

Netzwerkinstallation – Booten von CD oder DVD

Gehen Sie zum Ausführen einer Netzwerkinstallation mit der SP-CD oder -DVD als Bootmedium wie folgt vor:

- 1 Legen Sie das erste SUSE Linux Enterprise-SP-Medium (CD oder DVD Nr. 1) ein und booten Sie Ihren Computer. Ein ähnlicher Startbildschirm wie bei der ursprünglichen Installation von SUSE Linux Enterprise 10 wird angezeigt.
- 2 Wählen Sie *Installation*, um den SP-Kernel zu booten, und drücken Sie dann die `F3-Taste`, um einen Typ für die Netzwerkinstallationsquelle auszuwählen (FTP, HTTP, NFS oder SMB).
- 3 Geben Sie die entsprechenden Pfadinformationen ein oder wählen Sie *SLP* als Installationsquelle.
- 4 Wählen Sie den entsprechenden Installationsserver aus den angebotenen aus oder geben Sie den Typ der Installationsquelle und deren Standort bei der Aufforderung

der Bootoptionen an, wie unter „[Installation von einem Netzwerkservers](#)“ (S. 40) beschrieben. YaST wird gestartet.

- 5 Akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann eine Sprache, ein Standard-Desktop und andere Installationseinstellungen.
- 6 Klicken Sie auf *Ja, installieren*, um mit der Installation zu beginnen.
- 7 Fahren Sie wie gewohnt mit der Installation fort (geben Sie ein Passwort für `root` ein, schließen Sie die Netzwerkkonfiguration ab, testen Sie die Internet-Verbindung, aktivieren Sie den Online Update Service, wählen Sie die Benutzerauthentifizierungsmethode und geben Sie einen Benutzernamen und ein Passwort ein).

Weitere Informationen zur Installation von SUSE Linux Enterprise finden Sie unter [Kapitel 3, Installation mit YaST](#) (S. 37).

Netzwerkinstallation – PXE-Boot

Gehen Sie zum Ausführen einer Netzwerkinstallation eines SUSE Linux Enterprise-Service Pack über das Netzwerk wie folgt vor:

- 1 Passen Sie den Setup Ihres DHCP-Servers an, um die für den PXE-Boot erforderlichen Adresseninformationen anzugeben, gemäß [Abschnitt 4.3.5, „Vorbereiten des Zielsystems für PXE-Boot“](#) (S. 105).
- 2 Richten Sie einen TFTP-Server ein, der das Boot-Image für den PXE-Boot beinhaltet.

Verwenden Sie die erste CD oder DVD Ihres SUSE Linux Enterprise-Service Pack dafür und folgen Sie sonst den Anleitungen in [Abschnitt 4.3.2, „Einrichten eines TFTP-Servers“](#) (S. 97).

- 3 Bereiten Sie den PXE-Boot und Wake-on-LAN auf dem Zielcomputer vor.
- 4 Starten Sie den Boot des Zielsystems und verwenden Sie VNC, um sich entfernt mit der auf diesem Computer ausgeführten Installationsroutine zu verbinden. Weitere Informationen hierzu finden Sie unter [Abschnitt 4.5.1, „VNC-Installation“](#) (S. 111).

- 5 Akzeptieren Sie die Lizenzvereinbarung und wählen Sie dann eine Sprache, ein Standard-Desktop und andere Installationseinstellungen.
- 6 Klicken Sie auf *Ja, installieren*, um mit der Installation zu beginnen.
- 7 Fahren Sie wie gewohnt mit der Installation fort (geben Sie ein Passwort für `root` ein, schließen Sie die Netzwerkkonfiguration ab, testen Sie die Internet-Verbindung, aktivieren Sie den Online Update Service, wählen Sie die Benutzerauthentifizierungsmethode und geben Sie einen Benutzernamen und ein Passwort ein).

Weitere Informationen zur Installation von SUSE Linux Enterprise finden Sie unter [Kapitel 3, *Installation mit YaST*](#) (S. 37).

8.2.3 Aktualisieren auf einen Service Pack

Sie brauchen die SUSE Linux Enterprise 10 Original-CDs oder -DVD, um das Update abzuschließen.

- 1 Legen Sie bei laufendem SUSE Linux Enterprise-System die SUSE Linux Enterprise-SP-CD oder -DVD Nr. 1 in Ihr CD-Laufwerk ein und klicken Sie auf *Ja*, wenn der Hinweis zur Hardwareerkennung erscheint.

Wird das Bootmedium nicht automatisch erkannt, versuchen Sie es neu einzulegen. Wenn die automatische Erkennung weiterhin fehlschlägt, wählen Sie *System* → *Administratoreinstellungen* → *Software* → *Patch CD-Update*.

- 2 Wenn Sie nicht als `root` angemeldet sind, geben Sie das `root` Passwort ein, sobald Sie dazu aufgefordert werden. Das Dialogfeld *Online Update* wird geöffnet.
- 3 Klicken Sie auf *Weiter*, um mit dem Update-Vorgang zu beginnen. Im *Download and Installation Log* (Protokoll zum herunterladen und installieren) wird der Update-Vorgang verfolgt.
- 4 Wenn Sie aufgefordert werden, die *Patch CD-CD2* einzulegen, legen Sie die *SUSE Linux Enterprise-SP-CD2* ein und klicken Sie auf *OK*. Diese Aufforderung wird nicht angezeigt, wenn Sie von einer DVD aktualisieren.
- 5 Klicken Sie auf *Beenden* wenn am Ende des Vorgangsprotokolls *Installation Finished* (Installation beendet) angezeigt wird.

8.3 Software-Änderungen von Version 9 zu Version 10

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.

8.3.1 Mehrere Kernel

Es können mehrere Kernel gleichzeitig installiert werden. Diese Funktion soll es Administratoren ermöglichen, die Aufrüstung von einem Kernel auf einen anderen durch Installieren des neuen Kernel vorzunehmen; anschließend muss die ordnungsgemäße Funktion des neuen Kernel überprüft und der alte Kernel deinstalliert werden. Obwohl YaST diese Funktion noch nicht unterstützt, ist die Installation und Deinstallation von der Shell aus mithilfe von `rpm -i Paket.rpm` problemlos möglich.

Die standardmäßigen Bootloader-Menüs enthalten nur einen Kernel-Eintrag. Vor dem Installieren mehrerer Kernel empfiehlt es sich, einen Eintrag für die zusätzlichen Kernel hinzuzufügen, um die problemlose Auswahl zu ermöglichen. Der Zugriff auf den Kernel, der vor der Installation des neuen Kernel aktiv war, ist über `vmlinuz.previous` und `initrd.previous` möglich. Wenn ein Bootloader-Eintrag erstellt wird, der dem Standardeintrag ähnelt, und dieser Eintrag auf `vmlinuz.previous` und `initrd.previous` verweist, nicht auf `vmlinuz` und `initrd`, kann auf den zuvor aktiven Kernel zugegriffen werden. Alternativ unterstützen GRUB und LILO Platzhalter für Bootloader-Einträge. Details finden Sie auf den GRUB-Infoseiten (`info grub`) und der Manualpage `lilo.conf` (5).

8.3.2 Änderungen an den Kernel-Modulen

Die folgenden Kernel-Module sind nicht mehr verfügbar:

- `km_fcdsl`: AVM Fritz!Card-DSL
- `km_fritzcapi`: AVM FRITZ! ISDN-Adapter

Die folgenden Kernel-Modulpakete wurden intern geändert:

- `km_wlan`: Verschiedene Treiber für drahtlose LAN-Karten. Der `madwifi`-Treiber für Atheros WLAN-Karten von `km_wlan` wurde entfernt.

Aus technischen Gründen musste die Unterstützung für Ralink WLAN-Karten aufgegeben werden. Die folgenden Module sind nicht in der Distribution enthalten und werden auch in Zukunft nicht hinzugefügt:

- `ati-fglrx`: ATI FireGL-Grafikkarten
- `nvidia-gfx`: NVIDIA gfx-Treiber
- `km_smartlink-softmodem`: Smart Link Soft-Modem

8.3.3 Änderung der Konsolenummer und serielle Geräte

Ab 2.6.10 sind serielle ia64-Geräte namensbasiert. Die Namen richten sich nach der Reihenfolge der ACPI- und PCI-Aufzählung. Das erste Gerät im ACPI-Namespace (sofern vorhanden) erhält die Bezeichnung `/dev/ttyS0`, das zweite die Bezeichnung `/dev/ttyS1` usw. PCI-Geräte werden sequenziell im Anschluss an die ACPI-Geräte benannt.

Auf HP-Systemen muss die EFI-Konsole umkonfiguriert werden. Danach kann der Konsolenparameter im Kernel-Boot-Befehl gelöscht werden. Wenn Sie die Neukonfiguration vermeiden möchten, können Sie statt `console=ttyS0...` auch den Boot-Parameter `console=ttyS1...` verwenden.

Ausführliche Informationen hierzu finden Sie im Softwarepaket `kernel-source` in der Datei `/usr/src/linux/Documentation/ia64/serial.txt`.

8.3.4 Umgebungsvariable LD_ASSUME_KERNEL

Die Umgebungsvariable `LD_ASSUME_KERNEL` sollten Sie nicht mehr verwenden. Bislang konnten Sie über diese Variable die LinuxThreads-Unterstützung erzwingen. Diese Unterstützung gibt es nicht mehr. Wenn Sie in SUSE Linux Enterprise 10 die Einstellung `LD_ASSUME_KERNEL=2.4.x` vornehmen, funktioniert das gesamte System nicht mehr, da `ld.so` das Programm `glibc` und ähnliche Tools in einem Pfad sucht, der entfernt wurde.

8.3.5 Strengere tar-Syntax

Die `tar`-Verwendungssyntax ist nun strenger. Die `tar`-Optionen müssen den Datei- oder Verzeichnisspezifikationen vorangestellt werden. Das Anfügen von Optionen, wie `--atime-preserve` oder `--numeric-owner`, nach der Datei- oder Verzeichnisspezifikation führt dazu, dass bei `tar` ein Problem auftritt. Überprüfen Sie Ihre Sicherungsskripts. Befehle dieser Art funktionieren nicht mehr:

```
tar czf etc.tar.gz /etc --atime-preserve
```

Weitere Informationen finden Sie auf den `tar`-Infoseiten.

8.3.6 Apache 2 durch Apache 2.2 ersetzt

Der Apache-Webserver (Version 2) wurde durch Version 2.2 ersetzt. Für Apache Version 2.2 wurde [Kapitel 41, Der HTTP-Server Apache](#) (S. 811) 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.

8.3.7 Kerberos für die Authentifizierung im Netzwerk

Kerberos ist anstelle von heimdal der Standard für die Netzwerkauthentifizierung. Die automatische Konvertierung einer bestehenden heimdal-Konfiguration ist nicht möglich. Bei einer Systemaktualisierung werden Sicherungskopien von Konfigurationsdateien erstellt, wie in [Tabelle 8.1](#), „Sicherungsdateien“ (S. 232) dargestellt.

Tabelle 8.1 *Sicherungsdateien*

Alte Datei	Sicherungsdatei
/etc/krb5.conf	/etc/krb5.conf.heimdal
/etc/krb5.keytab	/etc/krb5.keytab.heimdal

Die Client-Konfiguration (/etc/krb5.conf) ist mit der von heimdal weitgehend identisch. Wenn keine besondere Konfiguration vorgenommen wurde, muss lediglich der Parameter `kpasswd_server` durch `admin_server` ersetzt werden.

Die serverbezogenen Daten (`kdc` und `kadmin`) können nicht kopiert werden. Nach der Systemaktualisierung steht die alte heimdal-Datenbank weiterhin unter `/var/heimdal` zur Verfügung. MIT-Kerberos verwaltet die Datenbank unter `/var/lib/kerberos/krb5kdc`. Weitere Informationen finden Sie in [Kapitel 46, Netzwerkauthentifizierung – Kerberos](#) (S. 919) und [Kapitel 47, Installation und Administration von Kerberos](#) (S. 927).

8.3.8 Über den udev-Daemon verarbeitete Hotplug-Ereignisse

Hotplug-Ereignisse werden jetzt vollständig über den udev-Daemon (`udev`) verarbeitet. Das Ereignis-Multiplexer-System in `/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.

8.3.9 Firewall-Aktivierung während der Installation

Für erhöhte Sicherheit wird die integrierte Firewall-Lösung SUSEFirewall2 am Ende der Installation im Vorschlags-Dialogfeld aktiviert. Dies bedeutet, dass sämtliche Ports anfänglich geschlossen sind und im Bedarfsfall über das Vorschlags-Dialogfeld geöffnet werden können. Standardmäßig ist die Anmeldung bei entfernten Systemen nicht möglich. Zudem werden das Suchen im Netzwerk sowie Multicast-Anwendungen, beispielsweise SLP, Samba ("Netzwerkumgebung"), sowie einige Spiele beeinträchtigt. Mit YaST können Sie die Firewall-Einstellungen präzisieren.

Wenn beim Installieren oder Konfigurieren eines Diensts auf das Netzwerk zugegriffen werden muss, öffnet das entsprechende YaST-Modul die benötigten TCP (Transmission Control Protocol)- und UDP (User Datagram Protocol)-Ports sämtlicher interner und externer Schnittstellen. Wenn dies nicht erwünscht ist, schließen Sie die Ports im YaST-Modul oder nehmen Sie andere detaillierte Firewall-Einstellungen vor.

8.3.10 KDE und IPv6-Unterstützung

Standardmäßig ist die IPv6-Unterstützung für KDE (K Desktop Environment) nicht aktiviert. Sie kann mithilfe des `/etc/sysconfig`-Editors von YaST aktiviert werden. Die Funktion wurde deaktiviert, da IPv6-Adressen nicht von allen Internetdiensteanbietern (ISP) unterstützt werden und beim Surfen im Web Fehlermeldungen ausgegeben werden oder bei der Anzeige von Webseiten Verzögerungen auftreten.

8.3.11 Online-Update und Delta-Pakete

Das Online-Update unterstützt nun eine besondere Art von RPM-Paket, in dem nur die binäre Abweichung von einem bestimmten Basispaket gespeichert wird. Diese Technik führt zu einer deutlich geringeren Paketgröße und weniger Zeitaufwand beim Herunterladen, bei der Neuzusammenstellung des endgültigen Pakets kommt es jedoch zu einer höheren CPU-Auslastung. Technische Details finden Sie in `/usr/share/doc/packages/deltarpm/README`.

8.3.12 Konfiguration des Drucksystems

Am Ende der Installation (Vorschlags-Dialogfeld) müssen die für das Drucksystem benötigten Ports in der Firewall-Konfiguration geöffnet sein. Port 631/TCP und Port 631/UDP werden für CUPS (Common Unix Printing System) benötigt und sollten für den normalen Betrieb nicht geschlossen werden. Port 515/TCP (für das alte LPD-(Line Printer Daemon-)Protokoll und die von Samba genutzten Ports müssen für das Drucken über LPD bzw. SMB (Server Message Block) ebenfalls geöffnet sein.

8.3.13 Umstellung auf X.Org

Die Umstellung von XFree86 auf X.Org wird über Kompatibilitätslinks ermöglicht, die den Zugriff auf wichtige Dateien und Befehle mit den alten Namen ermöglichen.

Tabelle 8.2 *Befehle*

XFree86	X.Org
XFree86	Xorg
xf86config	xorgconfig
xf86cfg	xorgcfg

Tabelle 8.3 *Protokolldateien in /var/log*

XFree86	X.Org
XFree86.0.log	Xorg.0.log
XFree86.0.log.old	Xorg.0.log.old

Bei der Umstellung auf X.Org wurden die Pakete von XFree86* in xorg-x11* umbenannt.

8.3.14 X.Org-Konfigurationsdatei

Vom SaX2-Konfigurationswerkzeug werden die X.Org-Konfigurationseinstellungen in `/etc/X11/xorg.conf` geschrieben. Bei einer kompletten Neuinstallation wird kein Kompatibilitätslink zwischen `XF86Config` und `xorg.conf` erstellt

8.3.15 Keine XView- und OpenLook-Unterstützung mehr

Die Pakete `xview`, `xview-devel`, `xview-devel-examples`, `olvwm` und `xtoolpl` wurden verworfen. In der Vergangenheit wurde lediglich das XView- (OpenLook-)Basissystem bereitgestellt. Die XView-Bibliotheken stehen nach der Systemaktualisierung nicht mehr zur Verfügung. Ein noch wichtigerer Punkt: OLVWM (OpenLook Virtual Window Manager) ist ebenfalls nicht mehr verfügbar.

8.3.16 Terminalemulatoren für X11

Einige Terminalemulatoren wurden entfernt, da sie entweder nicht mehr unterstützt werden oder in der Standardumgebung nicht funktionieren, insbesondere, da sie UTF-8 nicht unterstützen. SUSE Linux Enterprise Server stellt Standardterminals bereit, beispielsweise `xterm`, die KDE- und GNOME-Terminals und `mlterm` (Multilingual Terminal Emulator für X), die möglicherweise als Ersatz für `aterm` und `eterm` dienen.

8.3.17 OpenOffice.org (OOo)

Verzeichnisse

OOo wird nun in `/usr/lib/ooo-2.0` anstelle von `/opt/OpenOffice.org` installiert. `~/lib/ooo-2.0` ist nun anstelle von `~/OpenOffice.org1.1` das Standardverzeichnis für Benutzereinstellungen.

Packer

Es gibt einige neue Packer für das Aufrufen der OOo-Komponenten. Die neuen Namen sind aus [Tabelle 8.4](#), „Packer“ (S. 236) ersichtlich.

Tabelle 8.4 *Packer*

Alt	Neu
<code>/usr/X11R6/bin/OOo-calc</code>	<code>/usr/bin/ocalc</code>
<code>/usr/X11R6/bin/OOo-draw</code>	<code>/usr/bin/oodraw</code>
<code>/usr/X11R6/bin/OOo-impress</code>	<code>/usr/bin/ooimpress</code>
<code>/usr/X11R6/bin/OOo-math</code>	<code>/usr/bin/oomath</code>
<code>/usr/X11R6/bin/OOo-padmin</code>	<code>/usr/sbin/oopadmin</code>
<code>/usr/X11R6/bin/OOo-setup</code>	–
<code>/usr/X11R6/bin/OOo-template</code>	<code>/usr/bin/oofromtemplate</code>
<code>/usr/X11R6/bin/OOo-web</code>	<code>/usr/bin/ooweb</code>
<code>/usr/X11R6/bin/OOo-writer</code>	<code>/usr/bin/oowriter</code>
<code>/usr/X11R6/bin/OOo</code>	<code>/usr/bin/ooffice</code>
<code>/usr/X11R6/bin/OOo-wrapper</code>	<code>/usr/bin/ooo-wrapper</code>

Der Packer unterstützt nun die Option `--icons-set` für das Umschalten zwischen KDE- und GNOME-(GNU Network Objekt Model Environment-)Symbolen.

Folgende Optionen werden nicht mehr unterstützt:

`--default-configuration`, `--gui`, `--java-path`, `--skip-check`,
`--lang` (die Sprache wird nun anhand von Locales bestimmt),
`--messages-in-window` und `--quiet`.

KDE- und GNOME-Unterstützung

KDE- und GNOME-Erweiterungen stehen in den Paketen

`OpenOffice_org-kde` und `OpenOffice_org-gnome` zur Verfügung.

8.3.18 kmix-Soundmixer

Der kmix-Soundmixer ist standardmäßig voreingestellt. Für High-End-Hardware stehen andere Mixer zur Verfügung, beispielsweise QAMix, KAMix, envy24control (nur ICE1712) oder hdspmixer (nur RME Hammerfall).

8.3.19 Brennen von DVDs

In der Vergangenheit wurde ein Patch aus dem `cdrecord`-Paket auf die Binärdatei `cdrecord` angewendet, um die Unterstützung für das Brennen von DVDs bereitzustellen. Nun wird eine neue Binärdatei, `cdrecord-dvd`, installiert, die über diesen Patch verfügt.

Mit dem `growisofs`-Programm aus dem `dvd+rw-tools`-Paket können nun sämtliche DVD-Medien (DVD+R, DVD-R, DVD+RW, DVD-RW, DVD+RL) gebrannt werden. Verwenden Sie dieses Programm anstelle von `cdrecord-dvd` mit dem Patch.

8.3.20 Starten der manuellen Installation an der Kernel-Eingabeaufforderung

Der Modus *Manuelle Installation* steht im Bootloader-Bildschirm nicht mehr zur Verfügung. Mit `manual=1` an der Boot-Eingabeaufforderung kann `linuxrc` weiterhin in den manuellen Modus versetzt werden. Dies ist normalerweise nicht erforderlich, da die Installationsoptionen direkt an der Kernel-Eingabeaufforderung festgelegt werden können, beispielsweise `textmode=1`; es kann auch eine URL als Installationsquelle angegeben werden.

8.3.21 JFS: Nicht mehr unterstützt

Aufgrund technischer Probleme wird JFS nicht mehr unterstützt. Der Kernel-Dateisystemtreiber ist weiterhin vorhanden, die Partitionierung mit JFS wird jedoch von YaST nicht angeboten.

8.3.22 AIDE als Tripwire-Ersatz

Verwenden Sie als System zur Unbefugterkennung AIDE (Paketname `aide`); die Veröffentlichung erfolgt gemäß GPL (GNU Public License). Tripwire ist unter SUSE Linux nicht mehr verfügbar.

8.3.23 PAM-Konfiguration

Neue Konfigurationsdateien (mit Kommentaren für mehr Information)

`common-auth`

Standardmäßige PAM-Konfiguration für auth-Abschnitt

`common-account`

Standardmäßige PAM-Konfiguration für account-Abschnitt

`common-password`

Standardmäßige PAM-Konfiguration für password-Abschnitt

`common-session`

Standardmäßige PAM-Konfiguration für Sitzungsverwaltung

Sie sollten diese standardmäßigen Konfigurationsdateien aus Ihrer anwendungsspezifischen Konfigurationsdatei aufnehmen, da es einfacher ist, anstelle der etwa vierzig Dateien, die zuvor auf dem System vorhanden waren, eine einzige Datei zu ändern und zu verwalten. Einer zu einem späteren Zeitpunkt installierten Anwendung werden die bereits angewendeten Änderungen vererbt und der Administrator muss nicht daran denken, die Konfiguration anzupassen.

Die Änderungen sind einfach. Wenn Sie über folgende Konfigurationsdatei verfügen (sollte bei den meisten Anwendungen der Standard sein):

```
##PAM-1.0
auth    required      pam_unix2.so
account required      pam_unix2.so
password required     pam_pwcheck.so
password required     pam_unix2.so         use_first_pass use_authtok
#password required    pam_make.so          /var/yp
session required      pam_unix2.so
```

können Sie sie folgendermaßen ändern:

```

#%PAM-1.0
auth    include      common-auth
account include      common-account
password include     common-password
session include      common-session

```

8.3.24 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.

8.3.25 Änderungen im powersave-Paket

Die Konfigurationsdateien in `/etc/sysconfig/powersave` wurden geändert.

Tabelle 8.5 Aufgeteilte Konfigurationsdateien in `/etc/sysconfig/powersave`

Alt	Jetzt aufgeteilt in
<code>/etc/sysconfig/powersave/ common</code>	<code>common</code>
	<code>cpufreq</code>
	<code>events</code>
	<code>battery</code>
	<code>sleep</code>
	<code>thermal</code>

`/etc/powersave.conf` ist inzwischen veraltet. Bestehende Variablen wurden in die in [Tabelle 8.5](#), „Aufgeteilte Konfigurationsdateien in `/etc/sysconfig/powersave`“ (S. 239) aufgeführten Tabellen verschoben. Wenn Sie die „event“-Variablen in `/etc/`

`powersave.conf` geändert haben, muss deren Anpassung nun in `/etc/sysconfig/powersave/events` erfolgen.

Die Namen der sleep-Statusangaben wurden wie nachfolgend angegeben geändert.
Von:

- `suspend` (ACPI S4, APM `suspend`)
- `standby` (ACPI S3, APM `standby`)

In:

- `suspend to disk` (ACPI S4, APM `suspend`)
- `suspend to ram` (ACPI S3, APM `suspend`)
- `standby` (ACPI S1, APM `standby`)

8.3.26 powersave-Konfigurationsvariablen

Namen der powersave-Konfigurationsvariablen wurden aus Konsistenzgründen geändert, die `sysconfig`-Dateien sind unverändert. Weitere Informationen finden Sie in [Abschnitt 29.5.1, „Konfigurieren des powersave-Pakets“](#) (S. 577).

8.3.27 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 `pcmcia`-Startskript wurde entfernt und `cardctl` wird durch `pccardctl` ersetzt. Weitere Informationen finden Sie in `/usr/share/doc/packages/pcmciautils/README.SUSE`.

8.3.28 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.

8.3.29 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`

8.3.30 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, wird `gamin` bevorzugt (Begründung: Inotify wird nur von `gamin` unterstützt und ist für lokale Dateisysteme effizienter).
- Wenn der FAM-Daemon ausgeführt wird, wird FAM bevorzugt (Begründung: Wenn FAM ausgeführt wird, möchten Sie wahrscheinlich entfernte Benachrichtigungen erhalten, die nur von FAM unterstützt werden).

8.3.31 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.

8.3.32 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.

Teil 2. Administration

OpenWBEM

Novell® begrüßt die Strategien für den offenen Standard des Web-Based Enterprise Management (WBEM) der Distributed Management Task Force (DMTF) [<http://www.dmtf.org/home>] und wendet sie aus Überzeugung an. Durch die Implementierung dieser Strategien vereinfacht sich die Verwaltung unterschiedlicher Systeme in einem Netzwerk erheblich.

Nachfolgend werden eine Reihe der in den DTMF-Standards vorgeschlagenen Komponenten beschrieben. Wenn Sie verstehen, worum es sich hierbei handelt und wie die Komponenten zusammenwirken, verstehen Sie OpenWBEM besser und können es in Ihrem Netzwerk effektiver einsetzen.

- Web-Based Enterprise Management (WBEM) fasst eine Reihe von Verwaltungs- und Internet-Standardtechnologien zusammen, die in der Absicht entwickelt wurden, die Verwaltung der Computerumgebungen in Unternehmen zu vereinheitlichen. WBEM bietet die Möglichkeit, einen gut integrierten Satz mit standardisierten Verwaltungstools bereitzustellen, die auf den neuesten Webtechnologien aufsetzen. Die DMTF hat für WBEM einen Kernsatz mit Standards entwickelt:
- Datenmodell: der CIM-Standard (Common Information Model)
- Verschlüsselungsspezifikation: CIM-XML-Verschlüsselungsspezifikation
- Übertragungsmechanismus: CIM verwendet HTTP
- Das Common Information Model (CIM) ist ein konzeptuelles Informationsmodell, das die Verwaltung definiert, aber an keine bestimmte Implementierung gebunden ist. Dies ermöglicht den Austausch von Verwaltungsinformationen zwischen ver-

schiedenen Verwaltungssystemen und Anwendungen. Möglich sind Agent-zu-Manager oder Manager-zu-Manager-Kommunikationen, die eine verteilte Systemverwaltung bereitstellen. CIM besteht aus zwei Komponenten: der CIM-Spezifikation und dem CIM-Schema.

Die CIM-Spezifikation beschreibt die Sprache, die Namenskonventionen und das Metaschema. Das Metaschema legt die formelle Definition des Modells fest. Es definiert die Begriffe zur Beschreibung des Modells, sowie deren Verwendung und Semantik. Die Elemente des Metaschemas sind "Klassen", "Eigenschaften" und "Methoden". Als Klassen unterstützt das Metaschema auch Ereignisklassen und Assoziationen, als Eigenschaften auch Referenzen.

Das CIM-Schema enthält die eigentlichen Modellbeschreibungen. Es legt einen Klassensatz mit Eigenschaften und Assoziationen fest, die ein gut verstandenes, konzeptuelles Rahmenwerk bilden, innerhalb dem die verfügbaren Informationen zur verwalteten Umgebung organisiert werden können.

- Der Common Information Model Object Manager (CIMOM) ist ein CIM-Objektmanager bzw. eine Anwendung, die Objekte entsprechend den CIM-Standards verwaltet.
- CIMOM-Anbieter sind Programme, die bestimmte, von den Clientanwendungen angeforderte Aufgaben innerhalb des CIMOM ausführen. Jeder Anbieter stellt ein oder mehrere Aspekte des CIMOM-Schemas bereit.

SUSE® Linux Enterprise Server enthält den Open Source-CIMOM des OpenWBEM-Projekts [<http://openwbem.org>].

Die Softwareauswahl des Web-Based Enterprise Management (WBEM) umfasst einen Paketsatz, der grundlegende Novell-Anbieter einschließlich einiger Beispielanbieter enthält, sowie einen grundlegenden Satz begleitender Novell-Schemen.

Im Zuge der Weiterentwicklung von OpenWBEM und der Entwicklung spezieller Anbieter wird Novell auch Tools mit den folgenden wichtigen Funktionen bereitstellen:

- Effiziente Überwachung der Netzwerksysteme
- Aufzeichnung von Änderungen innerhalb bestehender Verwaltungskonfigurationen
- Hardware-Bestandsaufnahme und Anlagenverwaltung

Wenn Sie verstehen, wie OpenWBEM CIMOM aufgebaut ist und wie es konfiguriert wird, wird Ihnen die Überwachung und Verwaltung unterschiedlicher Systeme in Ihrem Netzwerk wesentlich leichter fallen.

9.1 Einrichten von OpenWBEM

OpenWBEM können Sie während der Installation von SUSE Linux Enterprise Server in YaST auswählen oder nachträglich auf einem Server installieren, auf dem SUSE Linux Enterprise Server bereits läuft. Wählen Sie dazu die Softwareauswahl Web-Based Enterprise Management aus. Diese Softwareauswahl enthält die folgenden Pakete:

- **cim-schema, Common Information Model-Schema (CIM):** Dieses Paket enthält das Common Information Model (CIM). CIM ist ein Modell für die Beschreibung der globalen Verwaltungsinformationen in einer Netzwerk- oder Unternehmensumgebung. CIM besteht aus einer Spezifikation und einem Schema. Die Spezifikation legt die Einzelheiten für die Integration mit anderen Verwaltungsmodellen fest. Das Schema stellt die eigentlichen Modellbeschreibungen bereit.
- **openwbem, Web Based Enterprise Management-Implementierung (WBEM):** Dieses Paket enthält die Implementierung von OpenWBEM. OpenWBEM besteht aus einem Satz Softwarekomponenten, die die Bereitstellung des DMTF CIM und der WBEM-Technologien erleichtern. Informationen über die DMTF (Distributed Management Task Force) und deren Technologien finden Sie auf der DMTF-Website [<http://www.dmtf.org>].
- **openwbem-base-providers:** Dieses Paket enthält einen Novell Linux-Satz der grundlegenden Betriebssystemkomponenten wie Computer, System, Betriebssystem und Prozesse für den OpenWBEM CIMOM.
- **openwbem-smash-providers:** Dieses Paket enthält einen Novell Linux-Satz der SMASH-Anbieter (Systems Management Architecture for Server Hardware) für den OpenWBEM CIMOM.
- **yast2-cim, YaST2-CIM-Bindungen:** Dieses Paket fügt YaST2 CIM-Bindungen hinzu (YaST2 ist die grafische Benutzerschnittstelle des SUSE System Tools Manager). Diese Bindungen stellen eine Client-Schnittstelle für den Common Information Model Object Manager (CIMOM) bereit.

Dieser Abschnitt enthält folgende Themen:

- [Abschnitt 9.1.1, „Starten, Beenden und Überprüfen des Status von owcimomd“](#) (S. 250)
- [Abschnitt 9.1.2, „Absichern des Zugriffs“](#) (S. 250)
- [Abschnitt 9.1.3, „Einrichten der Protokollierung“](#) (S. 253)

9.1.1 Starten, Beenden und Überprüfen des Status von owcimomd

Wenn die Web-Based Enterprise Management-Software installiert ist, wird der Daemon owcimomd automatisch gestartet. In folgender Tabelle wird beschrieben, wie der Daemon gestartet, beendet und wie sein Status überprüft wird.

Tabelle 9.1 *Befehle zur Verwaltung von owcimomd*

Aufgabe	Linux-Befehl
Starten von owcimomd	Geben Sie in einer Konsolen-Shell als root-Benutzer den Befehl <code>rcowcimomd start</code> ein.
Beenden von owcimomd	Geben Sie in einer Konsolen-Shell als root-Benutzer den Befehl <code>rcowcimomd stop</code> ein.
Überprüfen des Status von owcimomd	Geben Sie in einer Konsolen-Shell als root-Benutzer den Befehl <code>rcowcimomd status</code> ein.

9.1.2 Absichern des Zugriffs

Die Standardkonfiguration von OpenWBEM ist ziemlich sicher. Wenn jedoch für Ihr Unternehmen besondere Sicherheitsanforderungen gelten, können Sie den Zugriff auf die OpenWBEM-Komponenten zusätzlich absichern.

- [„Zertifikate“](#) (S. 251)

- [„Ports“](#) (S. 251)
- [„Authentifizierung“](#) (S. 253)

Zertifikate

Für eine sichere Kommunikation via SSL (Secure Socket Layers) ist ein Zertifikat erforderlich. Bei der Installation von OES generiert OpenWBEM ein selbst signiertes Zertifikat für die Komponente.

Den Pfad dieses Standardzertifikats können Sie durch den Pfad eines kommerziell erworbenen Zertifikats oder eines anderen Zertifikats ersetzen, das Sie in der Datei `openwbem.conf` in der Einstellung `http_server.SSL_cert = pfad_dateiname` angeben.

Das Standardzertifikat befindet sich in folgender Datei:

```
/etc/openwbem/servercert.pem
```

Mit dem folgenden Befehl können Sie ein neues Zertifikat erstellen. Da das aktuelle Zertifikat bei diesem Vorgang ersetzt wird, empfiehlt Novell vor der Generierung des neuen Zertifikats die Erstellung einer Kopie des alten Zertifikats.

Geben Sie in einer Konsolen-Shell als root-Benutzer den Befehl `sh/etc/openwbem/owgencert` ein.

Wenn Sie das von OpenWBEM verwendete Zertifikat ändern möchten, lesen Sie [Abschnitt 9.2.2, „Ändern der Zertifikatkonfiguration“](#) (S. 262).

Ports

OpenWBEM ist standardmäßig so konfiguriert, dass die gesamte Kommunikation am sicheren Port 5989 eingeht. Die Einrichtung der Portkommunikation und die empfohlene Konfiguration entnehmen Sie bitte folgender Tabelle.

Tabelle 9.2 *Einrichtung der Portkommunikation und empfohlene Konfiguration*

Port	Typ	Hinweise und Empfehlungen
5989	Secure	<p>Der sichere Port, den OpenWBEM für die Kommunikation via HTTPS-Diensten verwendet.</p> <p>Dies ist die Standardkonfiguration.</p> <p>Bei dieser Einstellung wird die gesamte Kommunikation zwischen dem CIMOM und den Clientanwendungen für die Internet-Übertragung zwischen Servern und Arbeitsstationen verschlüsselt. Zur Anzeige dieser Informationen müssen sich die Benutzer über die Clientanwendung authentifizieren.</p> <p>Novell empfiehlt die Beibehaltung dieser Einstellung in der Konfigurationsdatei.</p> <p>In Routern und Firewalls (sofern zwischen Clientanwendung und überwachten Knoten eingeschaltet) muss dieser Port offen sein, damit der OpenWBEM CIMOM mit den erforderlichen Anwendungen kommunizieren kann.</p>
5988	Unsecure	<p>Der unsichere Port, den OpenWBEM für die Kommunikation via HTTP-Diensten verwendet.</p> <p>Diese Einstellung ist standardmäßig deaktiviert.</p> <p>Bei dieser Einstellung steht die gesamte Kommunikation zwischen dem CIMOM und den Clientanwendungen während der Internet-Übertragung zwischen Servern und Arbeitsstationen jeder Person ohne Authentifizierung offen.</p> <p>Novell empfiehlt diese Einstellung nur für das Debuggen von Problemen mit dem CIMOM. Nach der Behebung des Problems sollten Sie diese Portoption sofort wieder deaktivieren.</p> <p>In Routern und Firewalls (sofern zwischen Clientanwendung und überwachten Knoten eingeschaltet) muss dieser Port offen sein,</p>

Port	Typ	Hinweise und Empfehlungen
		damit der OpenWBEM CIMOM mit Anwendungen, für die der nicht sichere Zugriff erforderlich ist, kommunizieren kann.

Informationen zur Änderung der Standard-Portzuweisungen finden Sie in [Abschnitt 9.2.3, „Ändern der Portkonfiguration“](#) (S. 263).

Authentifizierung

In SUSE Linux Enterprise Server sind für OpenWBEM standardmäßig die folgenden Authentifizierungseinstellungen eingerichtet und aktiviert.

Sie können jede dieser Standardeinstellungen ändern. Siehe [Abschnitt 9.2.1, „Ändern der Authentifizierungskonfiguration“](#) (S. 255).

- `http_server.allow_local_authentication = true`
- `http_server.ssl_client_verification = disabled`
- `http_server.use_digest = false`
- `owcimmd.allow_anonymous = false`
- `owcimmd.allowed_users = root`
- `owcimmd.authentication_module = /usr/lib/openwbem/authentication/libpamauthentication.so`

Der OpenWBEM CIMOM ist standardmäßig PAM-fähig. Die Authentifizierung beim OpenWBEM CIMOM kann daher mit den Anmeldeinformationen des lokalen root-Benutzers erfolgen.

9.1.3 Einrichten der Protokollierung

Sie können jede dieser Standardeinstellungen ändern. Weitere Informationen finden Sie in [Abschnitt 9.2.4, „Ändern der Standardprotokollkonfiguration“](#) (S. 264).

Standardmäßig ist die Protokollierung für OpenWBEM wie folgt eingerichtet.

- `log.main.components = *`
- `log.main.level = ERROR`
- `log.main.type = syslog`

Das `owcimomd`-Protokoll wird also in der Datei `/var/log/messages` bzw. je nach Konfiguration von `syslogd` in anderen Dateien gespeichert. In der Standardeinstellung protokolliert `owcimomd` sämtliche Fehler aller OpenWBEM-Komponenten.

9.2 Ändern der OpenWBEM CIMOM-Konfiguration

Beim Start von OpenWBEM CIMOM (`owcimomd`) liest der Daemon seine Laufzeitkonfiguration aus der Datei `openwbem.conf` ein. Die Datei `openwbem.conf` befindet sich im Verzeichnis `/etc/openwbem`.

Jede Einstellung in dieser Datei, deren Optionen durch einen Strichpunkt (;) oder ein Gatter (#) auskommentiert sind, verwendet die Standardeinstellung.

Diese Datei können Sie in jedem Texteditor bearbeiten, der die Datei in einem der Plattform entsprechenden Format speichert.

Sie können alle Einstellungen der Datei `openwbem.conf` ändern. In diesem Abschnitt werden die folgenden Konfigurationseinstellungen besprochen:

- [Abschnitt 9.2.1, „Ändern der Authentifizierungskonfiguration“](#) (S. 255)
- [Abschnitt 9.2.2, „Ändern der Zertifikatkonfiguration“](#) (S. 262)
- [Abschnitt 9.2.3, „Ändern der Portkonfiguration“](#) (S. 263)
- [Abschnitt 9.2.4, „Ändern der Standardprotokollkonfiguration“](#) (S. 264)
- [Abschnitt 9.2.5, „Konfigurieren der Debug-Protokollierung“](#) (S. 273)
- [Abschnitt 9.2.6, „Konfigurieren weiterer Protokolle“](#) (S. 274)

9.2.1 Ändern der Authentifizierungskonfiguration

Im Zusammenhang mit der Authentifizierung können Sie folgende Aspekte beeinflussen:

- Wer hat Zugriff auf den CIMOM?
- Welches Authentifizierungsmodul wird verwendet?

Sehen Sie sich hierzu die folgenden Einstellungen an:

- „[http_server.allow_local_authentication](#)“ (S. 255)
- „[http_server.digest_password_file](#)“ (S. 256)
- „[http_server.ssl_client_verification](#)“ (S. 257)
- „[http_server.ssl_trust_store](#)“ (S. 258)
- „[http_server.use_digest](#)“ (S. 258)
- „[owcimomd.ACL_superuser](#)“ (S. 259)
- „[owcimomd.allow_anonymous](#)“ (S. 259)
- „[owcimomd.allowed_users](#)“ (S. 260)
- „[owcimomd.authentication_module](#)“ (S. 261)
- „[simple_auth.password_file](#)“ (S. 262)

http_server.allow_local_authentication

Zweck

Weist den `http_server` an, die lokale Authentifizierung ohne Eingabe eines Passworts zuzulassen, also die Dateiberechtigungen des lokalen Systems zu übernehmen.

Diese Einstellung kann mit der Basis- und der Digestauthentifizierung verwendet werden.

Syntax

```
http_server.allow_local_authentication = option
```

Option	Beschreibung
true	Aktiviert die lokale Authentifizierung. Dies ist die Standardeinstellung.
false	Deaktiviert die lokale Authentifizierung.

Beispiel

```
http_server.allow_local_authentication = true
```

http_server.digest_password_file

Zweck

Gibt den Speicherort der Passwortdatei an. Die Angabe des Speicherorts ist erforderlich, wenn die Einstellung "http_server.use_digest" aktiviert ist.

Syntax

```
http_server.digest_password_file = pfad_dateiname
```

Der Standardpfad und -dateiname der Digest-Passwortdatei lautet:

```
/etc/openwbem/digest_auth.passwd
```

Beispiel

```
http_server.digest_password_file =  
/etc/openwbem/digest_auth.passwd
```

http_server.ssl_client_verification

Zweck

Bestimmt, ob der Server die Clients mittels der SSL-Client-Zertifikatüberprüfung authentifizieren soll.

Diese Einstellung ist standardmäßig deaktiviert.

Syntax

```
http_server.ssl_client_verification = option
```

Option	Beschreibung
autoupdate	Legt die gleiche Funktionalität fest, wie die Option <i>Optional</i> . Allerdings werden bislang unbekannte Client-Zertifikate, die die HTTP-Authentifizierung bestehen, einem verbürgten Speicher hinzugefügt. Nachfolgende Client-Verbindungen mit den gleichen Zertifikaten müssen die HTTP-Authentifizierung daher nicht erneut durchlaufen.
disabled	Deaktiviert die Client-Zertifikatüberprüfung. Dies ist die Standardeinstellung.
optional	Lässt die Authentifizierung eines verbürgten Zertifikats zu (die HTTP-Authentifizierung ist nicht mehr erforderlich). Außerdem besteht ein nicht verbürgtes Zertifikat das SSL-Handshake, wenn der Client die HTTP-Authentifizierung besteht.
required	Für ein erfolgreiches SSL-Handshake ist ein verbürgtes Zertifikat erforderlich.

Beispiel

```
http_server.ssl_client_verification = disabled
```

http_server.ssl_trust_store

Zweck

Gibt das Verzeichnis für den verbürgten OpenSSL-Speicher an.

Syntax

```
http_server.ssl_trust_store = pfad
```

Der Standardpfad der verbürgten Speicherdatei lautet:

```
/etc/openwbem/truststore
```

Beispiel

```
http_server.ssl_trust_store = /etc/openwbem/truststore
```

http_server.use_digest

Zweck

Weist den HTTP-Server an, die Digest-Authentifizierung zu verwenden, die den Mechanismus der Basisauthentifizierung umgeht. Für diese Art der Authentifizierung muss unter `owdigestgenpass` die Digest-Passwortdatei eingerichtet sein.

Digest verwendet nicht das unter `owcimomd.authentication_module` angegebene Authentifizierungsmodul.

Syntax

```
http_server.use_digest = option
```

Option	Beschreibung
false	Aktiviert die Basisauthentifizierung. Dies ist die Standardeinstellung.

Option	Beschreibung
true	Aktiviert die Digest-Authentifizierung.

Beispiel

```
http_server.use_digest = false
```

owcimomd.ACL_superuser

Zweck

Gibt den Benutzernamen des Benutzers an, der auf alle Daten des Common Information Model (CIM) in allen von owcimomd verwalteten Namespaces zugreifen darf. Dieser Benutzer kann als Administrator des Namespace `/root/security` eingesetzt werden, in dem sämtliche ACL-Benutzerrechte gespeichert sind.

Die ACL-Verarbeitung wird allerdings erst durch den Import der Datei `OpenWBEM_Acl1.0.mof` aktiviert.

Syntax

```
owcimomd.ACL_superuser = benutzername
```

Beispiel

```
owcimomd.ACL_superuser = root
```

owcimomd.allow_anonymous

Zweck

Aktiviert bzw. deaktiviert anonyme Anmeldungen bei owcimomd.

Syntax

```
owcimomd.allow_anonymous = option
```

Option	Beschreibung
false	Für den Zugriff auf owcimomd-Daten ist die Anmeldung über Benutzername und Passwort erforderlich. Dies ist die Standardeinstellung (empfohlen).
true	Ermöglicht den Zugriff auf owcimomd über die anonyme Anmeldung. Die Authentifizierung wird dadurch deaktiviert. Für den Zugriff auf owcimomd-Daten ist weder Benutzername noch Passwort erforderlich.

Beispiel

```
owcimomd.allowed_anonymous = false
```

owcimomd.allowed_users

Zweck

Legt die Liste der Benutzer fest, die auf owcimomd-Daten zugreifen dürfen.

Syntax

```
owcimomd.allowed_users = option
```

Option	Beschreibung
<i>benutzername</i>	Gibt einen oder mehrere Benutzer an, die auf die owcimomd-Daten zugreifen dürfen. Die einzelnen Benutzernamen müssen durch eine Leerstelle getrennt werden.
*	Ermöglicht allen Benutzern die Authentifizierung (stattdessen kann der Zugriff zum Beispiel über ACLs gesteuert werden).

Option	Beschreibung
	Diese Option wird bei allen Authentifizierungsmethoden durchgesetzt, es sei denn <code>owcimomd.allow_anonymous = true</code> .
	Dies ist die Standardeinstellung.

Beispiel

```
owcimomd.allowed_users = bcwhitely jkcarey jlanderson
```

owcimomd.authentication_module

Zweck

Bestimmt das von owcimom verwendete Authentifizierungsmodul. Diese Einstellung sollte den absoluten Pfad der freigegebenen Bibliothek angeben, die das Authentifizierungsmodul enthält.

Syntax

```
owcimomd.authentication_module = pfad_dateiname
```

Der Standardpfad und -dateiname der Bibliothek mit den Authentifizierungsmodulen lautet:

```
/usr/lib/openwbem/authentication/libpamauthentication.so
```

Beispiel

```
owcimomd.authentication_module =  
/usr/lib/openwbem/authentication/libpamauthentication.so
```

simple_auth.password_file

Zweck

Gibt den Pfad der Passwortdatei an, die für das einfache Authentifizierungsmodul erforderlich ist.

Diese Einstellung ist standardmäßig deaktiviert.

Syntax

```
simple_auth.password_file = pfad_dateiname
```

Beispiel

```
simple_auth.password_file =  
/etc/openwbem/simple_auth.passwd
```

9.2.2 Ändern der Zertifikatkonfiguration

Die Einstellungen `http_server.SSL_key` und `http_server.SSL_cert` legen den Speicherort der Dateien fest, die den privaten Schlüssel des Host und das von OpenSSL für die HTTPS-Kommunikation verwendete Zertifikat enthalten.

Standardmäßig befinden sich die `.pem`-Dateien in folgenden Verzeichnissen:

```
/etc/openwbem/servercert.pem
```

```
/etc/openwbem/serverkey.pem
```

9.2.2 Syntax

```
http_server.SSL_cert = pfad_dateiname
```

Oder:

```
http_server.SSL_key = pfad_dateiname
```

ANMERKUNG

Schlüssel und Zertifikat können auch in der gleichen Datei gespeichert werden. In diesem Fall wären die Werte von `http_server.SSL_key` und `http_server.SSL_cert` identisch.

9.2.2 Beispiele

```
http_server.SSL_cert = /etc/openwbem/servercert.pem
```

```
http_server.SSL_key = /etc/openwbem/servercert.pem
```

```
http_server.SSL_key = /etc/openwbem/serverkey.pem
```

9.2.3 Ändern der Portkonfiguration

Die Einstellungen `http_server.http_port` und `server.https_port` legen die Portnummern fest, die `owcimomd` bei der HTTP- bzw. HTTPS-Kommunikation überwacht.

9.2.3 Syntax

```
http_server.http_port = option
```

Oder:

```
http_server.https_port = option
```

Option	Beschreibung
<i>bestimmte_portnummer</i>	Legt eine bestimmte Portnummer für die HTTP- bzw. HTTPS-Kommunikation fest. Der Standardport für HTTP ist Port 5988. Der Standardport für HTTPS ist Port 5989.

Option	Beschreibung
-1	Deaktiviert HTTP- bzw. HTTPS-Verbindungen (Sie können zum Beispiel HTTP deaktivieren, wenn Sie nur HTTPS-Verbindungen zulassen möchten).
0	Weist die Portnummer dynamisch während der Laufzeit zu.

9.2.3 Beispiel

Die nachfolgenden Einstellungen deaktivieren den HTTP-Port und aktivieren Port 5989 für HTTPS-Verbindungen:

```
http_server.http_port = -1
```

```
http_server.https_port = 5989
```

9.2.4 Ändern der Standardprotokollkonfiguration

Mit den folgenden Protokolleinstellungen in der Datei `owcimomd.conf` legen Sie das Ausmaß der Protokollierung, den Typ der protokollierten Fehler, die Protokollgröße, den Pfad und Dateinamen des Protokolls sowie das Protokollformat fest:

- „[log.main.categories](#)“ (S. 265)
- „[log.main.components](#)“ (S. 266)
- „[log.main.format](#)“ (S. 267)
- „[log.main.level](#)“ (S. 269)
- „[log.main.location](#)“ (S. 270)
- „[log.main.max_backup_index](#)“ (S. 271)
- „[log.main.max_file_size](#)“ (S. 271)

- „log.main.type“ (S. 272)

Informationen zur Einrichtung der Debug-Protokollierung finden Sie in [Abschnitt 9.2.5](#), „Konfigurieren der Debug-Protokollierung“ (S. 273).

Informationen zur Einrichtung weiterer Protokolle finden Sie in [Abschnitt 9.2.6](#), „Konfigurieren weiterer Protokolle“ (S. 274).

log.main.categories

Zweck

Legt die protokollierten Fehlerkategorien fest.

Syntax

```
log.main.categories = option
```

Option	Beschreibung
--------	--------------

<i>kategorie_name</i>	Legt die protokollierten Fehlerkategorien fest. Geben Sie die einzelnen Kategorien jeweils getrennt durch ein Leerzeichen ein.
-----------------------	--

In owcimomd werden folgende Fehlerkategorien verwendet:

- DEBUG
- ERROR
- FATAL
- INFO

Weitere Informationen über diese Optionen erhalten Sie in [„log.main.level“](#) (S. 269).

Sofern mit dieser Option angegeben, werden die vordefinierten Kategorien nicht als Ebenen, sondern als unabhängige Kategorien behandelt. Für diesen Parameter gibt es keine

Option	Beschreibung
	Standardeinstellung. Wenn keine Kategorie festgelegt ist, also keine Kategorien protokolliert werden, wird die Einstellung <code>log.main.level</code> verwendet.
*	Alle Kategorien werden protokolliert.
	Dies ist die Standardeinstellung.

Beispiel

```
log.main.categories = FATAL ERROR INFO
```

log.main.components

Zweck

Legt die Komponenten fest, über die ein Protokoll geführt wird.

Syntax

```
log.main.components = option
```

Option	Beschreibung
<i>komponenten_name</i>	Legt die protokollierten Komponenten fest (z. B. owci-momd). Geben Sie die einzelnen Komponenten jeweils getrennt durch ein Leerzeichen ein.
	Anbieter können ihre eigenen Komponenten verwenden.
*	Alle Komponenten werden protokolliert.
	Dies ist die Standardeinstellung.

Beispiel

```
log.main.components = owcimomd nssd
```

log.main.format

Zweck

Legt das Format der Protokollmeldungen fest (Text gemischt mit printf()-Konvertierungsangaben).

Syntax

```
log.main.format = konvertierungs_angabe
```

Option	Angabe
%%	%
%c	Komponente (z. B. owcimomd)
%d	Datum Danach ist eine Datumsformatangabe in eckigen Klammern möglich. Zum Beispiel: %d{%H:%M:%S} oder %d{%d %b %Y %H:%M:%S}. Wenn die Datumsformatangabe fehlt, wird das ISO 8601-Format verwendet. Der einzige mögliche Zusatz ist %Q (Anzahl der Millisekunden). Weitere Informationen zu Datumsformatangaben finden Sie in der Beschreibung der Funktion strftime(), die im <ctime>-Header vorkommt.
%e	Meldung im Format XML CDATA; dieses Format umfasst “<![CDATA[“ und Endung “]]>”
%F	Dateiname

Option	Angabe
%l	Dateiname und Zeilennummer; zum Beispiel: datei.cpp(100)
%L	Zeilennummer
%M	Name der Methode, von der die Protokollanforderung ausgegeben wurde (funktioniert nur auf C++-Compilern, die <code>__PRETTY_FUNCTION__</code> oder C99's <code>__func__</code> unterstützen)
%m	Meldung
%n	Plattform-abhängige(s) Zeilenumbruchzeichen (<code>\n</code> oder <code>\r\n</code>)
%p	Kategorie, auch als Ebene oder Priorität bezeichnet
%r	Zeit in Millisekunden zwischen dem Start der Anwendung und der Erstellung des Protokollereignisses
%t	Thread-ID
\n	Neue Zeile
\t	Tabulator
\r	Zeilenumbruch
\\	\
\x<hexDigits>	Zeichen in Hexadezimalformat

Außerdem kann die minimale und maximale Feldbreite sowie die Ausrichtung geändert werden. Der optionale Format-Modifier wird zwischen dem Prozentzeichen (%) und dem Konvertierungszeichen eingefügt. Der erste optionale Format-Modifier ist die Flag für Linksausrichtung, ein Minuszeichen (-). Darauf folgt der optionale Format-Modifier für die minimale Feldbreite, eine Ganzzahl, die die Mindestanzahl der auszugebenden Zeichen angibt. Falls für das Datumselement weniger Zeichen erforderlich sind, wird das Feld abhängig vom Ausrichtungsflag links oder rechts mit Leerzeichen aufgefüllt.

Sind mehr Zeichen erforderlich, als die minimale Feldbreite vorgibt, wird das Feld entsprechend vergrößert.

Der Format-Modifizier für die maximale Feldbreite ist ein Punkt (.) gefolgt von einer Dezimalkonstante. Falls das Datumelement länger als die maximale Feldbreite ist, wird standardmäßig am Anfang des Elements bzw. bei Auswahl der Linksausrichtung am Ende des Elements die entsprechende Anzahl an Zeichen abgeschnitten.

Beispiele

Log4j TTCC-Layout:

```
"%r [%t] %-5p %c - %m"
```

Ähnlich wie TTCC, allerdings mit einigen Feldern mit fester Größe:

```
"%-6r [%15.15t] %-5p %30.30c - %m"
```

log4j.dtd 1.2-konforme XML-Ausgabe, die von Chainsaw verarbeitet werden kann (normalerweise ohne Zeilenumbruch; zur besseren Lesbarkeit ist die Ausgabe hier jedoch auf mehrere Zeilen aufgeteilt):

```
"<log4j:event logger=\"%c\" timestamp=\"%d{%s%Q}\" level=\"%p\"  
thread=\"%t\"> <log4j:message>%e</log4j:message>  
<log4j:locationInfo class=\"\" method=\"\" file=\"%F\"  
line=\"%L\"/></log4j:event>"
```

Die Standardeinstellung lautet:

```
log.main.format = [%t]%m
```

log.main.level

Zweck

Legt die protokollierte Ebene fest. Wenn eingestellt, gibt das Protokoll alle vordefinierten Kategorien ab der angegebenen Ebene aus.

Syntax

```
log.main.level = option
```

Option	Beschreibung
DEBUG	Das Protokoll gibt alle Debug-, Info-, Error- und Fatal-Fehlermeldungen aus.
ERROR	Das Protokoll gibt alle Error- und Fatal-Fehlermeldungen aus. Dies ist die Standardeinstellung.
FATAL	Das Protokoll gibt nur Fatal-Fehlermeldungen aus.
INFO	Das Protokoll gibt alle Info, Error- und Fatal-Fehlermeldungen aus.

Beispiel

```
log.main.level = ERROR
```

log.main.location

Zweck

Gibt den Speicherort der von owcimomd verwendeten Protokolldatei an, wenn in der Einstellung `log.main.type` festgelegt ist, dass das Protokoll in eine Datei ausgegeben wird.

Syntax

```
log.main.location = pfad_dateiname
```

Beispiel

```
log.main.location = /system/cimom/var/owcimomd.log
```

log.main.max_backup_index

Zweck

Gibt an, wie viele Sicherungsprotokolle aufbewahrt werden, bevor das älteste Protokoll gelöscht wird.

Syntax

```
log.main.backup_index = option
```

Option	Beschreibung
<i>ganzzahl_über_0_ohne_vorzeichen</i>	Gibt die Anzahl der aufzubewahrenden Sicherungsprotokolle an. Die Standardeinstellung ist 1.
0	Es werden keine Sicherungsprotokolle erstellt. Sobald das Protokoll seine maximale Dateigröße erreicht, werden die Einträge am Anfang gelöscht.

Beispiel

```
log.main.max_backup_index = 1
```

log.main.max_file_size

Zweck

Gibt die maximal zulässige Dateigröße (in KB) des owcimomd-Protokolls an.

Syntax

```
log.main.max_file_size = option
```

Option	Beschreibung
<i>ganzzahl_ohne_vorzeichen_in_KB</i>	Legt die maximale Größe des Protokolls in KB fest.
0	Für das Protokoll gibt es keine Größeneinschränkung. Dies ist die Standardeinstellung.

Beispiel

```
log.main.max_file_size = 0
```

log.main.type

Zweck

Legt den Typ des von `owcimomd` verwendeten Hauptprotokolls fest.

Syntax

```
log.main.type = option
```

Option	Beschreibung
file	Gibt alle Meldungen in die von <code>log.main.location</code> festgelegte Datei aus.
null	Deaktiviert die Protokollierung.
syslog	Gibt alle Meldungen an die syslog-Schnittstelle aus. Dies ist die Standardeinstellung.

Beispiel

```
log.main.type = syslog
```

9.2.5 Konfigurieren der Debug-Protokollierung

Wenn `owcimond` im Debug-Modus ausgeführt wird, werden sämtliche Meldungen in das Debug-Protokoll ausgegeben. Das Debug-Protokoll hat folgende Einstellungen:

- `log.debug.categories = *`
- `log.debug.components = *`
- `log.debug.format = [%t] %m`
- `log.debug.level = *`
- `log.debug.type = stderr`

Farbiges Debug-Protokoll

Mit den folgenden ASCII-Escape-Codes können Sie das Debug-Protokoll farbig anzeigen:

```
log.debug.format =  
\x1b[1;37;40m[\x1b[1;31;40m%- .6t\x1b[1;37;40m]\x1b[1;32;40m  
%m\x1b[0;37;40m
```

Wenn Sie weitere Farben verwenden möchten, geben Sie im Befehl `log.debug.format` die folgenden Codes an:

Tabelle 9.3 Weitere Farbcodes für den Befehl `log.debug.format`

Farbe	Code
Rot	<code>\x1b[1;31;40m</code>

Farbe	Code
Dunkelrot	\x1b[0;31;40m
Grün	\x1b[1;32;40m
Dunkelgrün	\x1b[0;32;40m
Gelb	\x1b[1;33;40m
Dunkelgelb	\x1b[0;33;40m
Blau	\x1b[1;34;40m
Dunkelblau	\x1b[0;34;40m
Violett	\x1b[1;35;40m
Dunkelviolett	\x1b[0;35;40m
Zyan	\x1b[1;36;40m
Dunkelzyan	\x1b[0;36;40m
Weiß	\x1b[1;37;40m
Dunkles weiß	\x1b[0;37;40m
Grau	\x1b[0;37;40m
Farbe zurücksetzen	\x1b[0;37;40m

9.2.6 Konfigurieren weiterer Protokolle

Wenn Sie weitere Protokolle erstellen möchten, geben Sie deren Namen unter folgender Einstellung an:

```
owcimond.additional_logs = protokoll_name
```

Die Protokollnamen müssen jeweils durch ein Leerzeichen getrennt sein.

9.2.6 Syntax

```
owcimomd.additional_logs = protokoll_name
```

Für jedes Protokoll gelten die folgenden Einstellungen:

- `log.protokoll_name.categories`
- `log.protokoll_name.components`
- `log.protokoll_name.format`
- `log.protokoll_name.level`
- `log.protokoll_name.location`
- `log.protokoll_name.max_backup_index`
- `log.protokoll_name.max_file_size`

9.2.6 Beispiel

```
owcimomd.additional_logs = fehlerprotokoll1  
fehlerprotokoll2 fehlerprotokoll3
```

9.3 Weitere Informationen

Hier finden Sie weitere Informationen zu OpenWBEM:

- Dokumente in `usr/share/doc/packages/openwbem` auf dem Dateisystem des lokalen Servers:
 - `Readme`
 - `Openwbem-faq.html`

- Novell Cool Solutions-Artikel: An Introduction to WBEM and OpenWBEM in SUSE Linux [<http://www.novell.com/cool solutions/feature/14625.html>]
- OpenWBEM-Website [<http://www.openwbem.org>]
- DMTF-Website [<http://www.dmtf.org>]

Multipath-E/A

Linux-Multipathing bietet E/A-Failover und verteilte Pfadauslastung für Block-Geräte mit mehreren Pfaden. Die Multipath-E/A-Unterstützung in SUSE® Linux Enterprise Server basiert auf dem Multipath-Modul Device-Mapper (Gerätezuordnung) des Linux-Kernels und dem userspace-Paket `multipath-tools`.

Die Gerätezuordnung über MultiPath-E/A ermöglicht die automatische Konfiguration von Subsystemen in zahlreichen Implementierungen. Aktiv/Passiv- oder Aktiv/Aktiv- (mit Round-Robin-Lastverteilung) Konfigurationen mit bis zu acht Pfaden zu jedem Gerät werden unterstützt.

`multipath-tools` kümmert sich um die automatische Pfadermittlung und -gruppierung sowie automatisierte Wiederholungen von Pfadprüfungen, damit ein zuvor ausgefallener Pfad automatisch wieder eingesetzt wird, sobald er ordnungsgemäß funktioniert. Damit wird der Bedarf an Administratoreingriffen in einer Produktionsumgebung minimiert.

Gerätezuordnung mit Multipath-E/A unterstützt Partitionen (mit Einschränkungen) und LVM2. Software-RAID wird ebenfalls unterstützt, aber automatische Ermittlung ist nicht verfügbar. Damit Software-RAID mit `mdadm` genutzt werden kann, muss `/etc/mdadm.conf` korrekt eingerichtet sein. Weitere Informationen hierzu finden Sie unter [Abschnitt 10.4, „Verwenden der Geräte“](#) (S. 283).

Momentan ist die Gerätezuordnung mit Multipath-E/A nicht für die Boot-Partition verfügbar, da der Bootloader Multipath-E/A nicht unterstützt. Daher wird empfohlen, bei der Verwendung von Multipath-E/A eine separate Boot-Partition einzurichten.

10.1 Unterstützte Hardware

Multipath-E/A ist auf allen Plattformen verfügbar, die von SUSE Linux Enterprise Server unterstützt werden. Die folgenden Speichersubsysteme werden automatisch ermittelt:

- 3Pardata VV
- Compaq HSV110 / MSA1000
- DDN SAN MultiDirector
- DEC HSG80
- EMC CLARiiON CX
- FSC CentricStor
- HP HSV110 / A6189A / Open-
- Hitachi DF400 / DF500 / DF600
- IBM 3542 / ProFibre 4000R / F20 / SVC / DS6000 / DS8000
- NETAPP
- SGI TP9100 / TP9300 / TP9400 / TP9500
- STK OPENstorage DS280
- SUN StorEdge 3510 / T4

Die meisten anderen Speichersubsysteme sollten ebenfalls funktionieren, erfordern aber eine manuelle Konfiguration in `/etc/multipath.conf`.

Für Speichersubsysteme, die spezielle Befehle beim Failover von einem Pfad auf den anderen oder spezielle Nicht-Standard-Fehlerbehandlung erfordern, ist eventuell umfangreicherer Support nötig. Daher bietet das DM-Framework Einsprungpunkte für Hardware-Steuerprogramme und ein solches Steuerprogramm für die Array-Serie EMC CLARiiON CX wird bereits zur Verfügung gestellt.

10.2 Systemkonfiguration

Das System muss manuell konfiguriert werden, um automatisch die Gerätetreiber für die Controller zu laden, mit denen die Multipath-E/A-Geräte im `INITRD` verbunden sind. Fügen Sie daher das erforderliche Treibermodul der Variablen `INITRD_MODULES` in der Datei `/etc/sysconfig/kernel` hinzu.

Wenn Ihr System beispielsweise einen RAID-Controller enthält, auf den der Treiber `cciss` zugreift, und Multipath-E/A-Geräte mit einem Qlogic-Controller verbunden sind, auf den der Treiber `qla2xxx` zugreift, würde der Eintrag wie folgt aussehen:

```
INITRD_MODULES="cciss"
```

Da der Qlogic-Treiber nicht automatisch beim Start geladen wird, fügen Sie ihn hier hinzu:

```
INITRD_MODULES="cciss qla2xxx"
```

Erstellen Sie nach dem Ändern von `/etc/sysconfig/kernel` das `INITRD` auf Ihrem System mit dem Befehl `mkinitrd`.

Wenn Sie LILO als Boot-Manager einsetzen, installieren Sie es erneut mit dem Befehl `/sbin/lilo`. Wenn Sie GRUB verwenden, ist keine weitere Aktion erforderlich.

10.3 Software-Konfiguration

10.3.1 Konfigurieren von `multipath-tools`

Wenn Sie ein automatisch erkanntes Speichersubsystem verwenden (siehe [Abschnitt 10.1, „Unterstützte Hardware“](#) (S. 278)), ist keine weitere Konfiguration der `multipath-tools` erforderlich. Erstellen Sie anderenfalls `/etc/multipath.conf` und fügen Sie den entsprechenden Geräteeintrag für Ihr Speichersubsystem hinzu. Unter `/usr/share/doc/packages/multipath-tools/multipath.conf.annotated` finden Sie eine Vorlage mit ausführlichen Kommentaren.

Nachdem Sie die Konfiguration eingerichtet haben, können Sie einen „Probelauf“ mit `multipath -v2 -d` ausführen, bei dem lediglich die Geräte gescannt werden und anschließend ausgedruckt wird, wie die Einrichtung aussehen würde. Die Ausgabe sieht in etwa folgendermaßen aus:

```
3600601607cf30e00184589a37a31d911 ❶  
[size=127 GB] ❷[features="0"] ❸[hwhandler="1  
  emc"] ❹  
\_ round-robin 0 [first] ❺  
  \_ 1:0:1:2 sdav 66:240 [ready ]  
  \_ 0:0:1:2 sdr  65:16  [ready ]  
\_ round-robin 0 ❻  
  \_ 1:0:0:2 sdag 66:0   [ready ]  
  \_ 0:0:0:2 sdc  8:32  [ready ]
```

- ❶ Name des Geräts
- ❷ Größe des Geräts
- ❸ Funktionen des Geräts
- ❹ Zugehörige Hardware-Steuerprogramme
- ❺ Prioritätsgruppe 1
- ❻ Prioritätsgruppe 2

Pfade werden in Prioritätsgruppen zusammengefasst. Es ist immer nur jeweils eine Prioritätsgruppe in aktivem Gebrauch. Um eine Aktiv/Aktiv-Konfiguration zu modellieren, landen alle Pfade in derselben Gruppe. Um Aktiv/Passiv zu modellieren, sollten die Pfade, die nicht gleichzeitig aktiv sein dürfen, in mehreren distinkten Prioritätsgruppen platziert werden. Dies geschieht in der Regel bei der Ermittlung eines Geräts völlig automatisch.

Die Ausgabe zeigt die Reihenfolge, in der die verwendete Planungsstrategie die E/A innerhalb der Gruppe ausgeglichen hat, sowie die Pfade für jede Prioritätsgruppe an. Für jeden Pfad werden die physische Adresse (`host:bus:target:lun`), der Name des Geräteknotens, die "major:minor"-Nummer und der Status angezeigt.

10.3.2 Aktivieren der Komponenten

Um die Multipath-E/A-Dienste zu starten, führen Sie die folgenden Befehle aus:

```
/etc/init.d/boot.multipath start
/etc/init.d/multipathd start
```

Die Multipath-Geräte sollten nun automatisch unter `/dev/disk/by-name/` aufgeführt werden. Der Standardname ist der WWN (World Wide Name) der logischen Einheit, den Sie auch mithilfe von `/var/lib/multipath/bindings` überschreiben können, indem Sie `user_friendly_names` in `/etc/multipath.conf` auf `yes` setzen.

Um Multipath-E/A-Dienste permanent zur Boot-Sequenz hinzuzufügen, führen Sie den folgenden Befehl aus:

```
insserv boot.multipath multipathd
```

10.3.3 Abfragen des Status

Bei einer Abfrage des Multipath-E/A-Status wird der aktuelle Status der Multipath-Zuordnungen ausgegeben. Um den aktuellen MPIO-Status abzufragen, führen Sie `multipath -l` aus.

Die Ausgabe ist ähnlich der bereits in [Abschnitt 10.2, „Systemkonfiguration“](#) (S. 279) beschriebenen, aber sie enthält zusätzliche Informationen zum Status jeder Prioritätsgruppe und jedes Pfads:

```
3600601607cf30e00184589a37a31d911
[size=127 GB][features="0"][hwhandler="1 emc"]
\_ round-robin 0 [active][first]
  \_ 1:0:1:2 sdav 66:240 [ready ][active]
  \_ 0:0:1:2 sdr 65:16 [ready ][active]
\_ round-robin 0 [enabled]
  \_ 1:0:0:2 sdag 66:0 [ready ][active]
  \_ 0:0:0:2 sdc 8:32 [ready ][active]
```

10.3.4 Einstellen des Failover mit spezifischen Hostbus-Adaptern

Zeitüberschreitungen von Hostbus-Adaptern werden in der Regel für Umgebungen ohne Multipath-E/A eingerichtet, da die einzige Alternative wäre, die E/A mit Fehlerstatus abzubrechen und den Fehler an die Anwendung weiterzugeben. Mit Multipath-E/A sollten einige Fehler (wie Kabelausfälle) so schnell wie möglich nach oben wei-

tergereicht werden, damit die Multipath-E/A-Schicht rasch Maßnahmen ergreifen und die E/A auf einen anderen, fehlerfreien Pfad lenken kann.

Um die Zeitüberschreitungen für Ihren Hostbus-Adapter zu konfigurieren, fügen Sie die entsprechenden Optionen zu `/etc/modprobe.conf.local` hinzu. Für die QLogic 2xxx-Serie von Hostbus-Adaptoren beispielsweise werden die folgenden Einstellungen empfohlen:

```
options qla2xxx qlport_down_retry=1 ql2xfailover=0 ql2xretrycount=5
```

10.3.5 Verwaltung von E/A in Fehlersituationen

In bestimmten Situationen, in denen Treiber-, Hostbus-Adapter- oder Infrastruktur-Fehler auftreten, die zu einem Verlust aller Pfade führen, sollte sämtliche E/A in eine Warteschlange gestellt anstatt nach oben propagiert werden.

Dies kann mit der folgenden Einstellung in `/etc/multipath.conf` erreicht werden.

```
defaults {
    default_features "1 queue_if_no_path"
}
```

Da dies dazu führt, dass die E/A ununterbrochen in einer Warteschlange steht, sofern kein Pfad neu aktiviert wird, stellen Sie sicher, dass Multipathd ausgeführt wird und für Ihre Situation gilt. Anderenfalls kann die E/A ständig auf dem betroffenen MPIO-Gerät beeinflusst sein, bis zu einem Neuboot oder bis Sie manuell den folgenden Befehl ausgeben:

```
dmsetup message <NAME> 0 fail_if_no_path
```

Dadurch schlägt automatisch sämtliche in der Warteschlange anstehende E/A fehl. (Ersetzen Sie `<NAME>` durch den korrekten Zuordnungsnamen). Sie können die Warteschlange erneut aktivieren, indem Sie den folgenden Befehl ausgeben:

```
dmsetup message <NAME> 0 queue_if_no_path
```

Sie können auch diese beiden Befehle verwenden, um zwischen den Testmodi umzuschalten, bevor der Befehl an `/etc/multipath.conf` übermittelt wird.

10.4 Verwenden der Geräte

MPIO-Geräte können direkt benutzt werden: mit LVM und mit mdadm.

10.4.1 Direkte Verwendung der Geräte

Wenn Sie die gesamten LUNs direkt verwenden möchten (beispielsweise beim Partitionieren Ihres Speichers mithilfe von SAN-Funktionen), können Sie einfach die `/dev/disk/by-name/xxx`-Namen direkt für `mkfs`, `fstab`, Ihre Anwendung usw. benutzen.

10.4.2 Verwenden von LVM2

Damit LVM2 die MPIO-Geräte als mögliche physische Volumes erkennt, müssen Sie `/etc/lvm/lvm.conf` modifizieren. Es ist wichtig, die Änderung so auszuführen, dass LVM2 die physischen Pfade nicht scannt und verwendet, sondern nur durch die Multipath-E/A-Schicht auf den Multipath-E/A-Speicher zugreift. Ändern Sie dafür die Einträge `filter` und `types` in `/etc/lvm/lvm.conf` wie folgt:

```
filter = [ "a|/dev/disk/by-name/.*", "r|.*)" ]
types = [ "device-mapper", 253 ]
```

Damit kann LVM2 nur die namentlich aufgeführten Pfade scannen und weist alle anderen zurück. Wenn Sie LVM2 auch auf Nicht-Multipath-E/A-Geräten verwenden, nehmen Sie die erforderlichen Anpassungen für Ihre Einrichtung vor.

10.4.3 Verwenden von mdadm

Für `mdadm` gilt dasselbe wie für LVM2: Auf die Geräte muss über ihren Namen zugegriffen werden, nicht über den physischen Pfad. Daher muss der Eintrag `DEVICE` in `/etc/mdadm.conf` geändert werden:

```
DEVICE /dev/disk/by-name/*
```

10.4.4 Partitionen

Derzeit ist es nicht möglich, Multipath-E/A-Geräte zu partitionieren. Wenn das zugrunde liegende physische Gerät bereits partitioniert ist, reflektiert das Multipath-E/A-Gerät

diese Partitionen und die Schicht bietet `/dev/disk/by-name/>name<p1 . . .`
pN-Geräte an, damit Sie über die Multipath-E/A-Schicht auf die Partitionen zugreifen
können.

Daher müssen die Geräte vor der Aktivierung von Multipath-E/A partitioniert werden.
Wenn Sie die Partitionierung im laufenden System ändern, erkennt und reflektiert
Multipath-E/A diese Änderungen nicht automatisch. Es muss neu initialisiert werden,
was gewöhnlich einen Neuboot erfordert.

Massenspeicher über IP-Netzwerke – iSCSI

11

Eine zentrale Aufgabe in Rechenzentren und beim Betreiben von Servern ist die Bereitstellung von Festplattenkapazität für Serversysteme. Im Mainframe-Sektor wird dafür häufig Fiber-Channel verwendet. Bisher sind UNIX-Computer und die überwiegende Zahl der Server nicht mit zentralen Speicherlösungen verbunden.

linux-iSCSI bietet eine einfache und ziemlich preiswerte Lösung für den Anschluss von Linux-Computern an zentrale Speichersysteme. Im Prinzip repräsentiert iSCSI eine Übertragung von SCSI-Befehlen auf IP-Ebene. Wenn ein Programm eine Anfrage an ein solches Gerät startet, generiert das Betriebssystem die erforderlichen SCSI-Befehle. Diese werden dann in IP-Pakete eingebettet und durch Software verschlüsselt, die als *iSCSI-Initiator* bezeichnet wird. Die Pakete werden dann an die entsprechende entfernte iSCSI-Station, auch *iSCSI-Ziel* genannt, übertragen.

Viele Speicherlösungen bieten Zugriff über iSCSI, jedoch ist es auch möglich, einen Linux-Server zu betreiben, der ein iSCSI-Ziel bereitstellt. In diesem Fall ist es wichtig, dass der Linux-Server für Dateisystemdienste optimiert ist. Das iSCSI-Ziel greift nur auf Block-Geräte in Linux zu. Daher ist es möglich, RAID-Lösungen zur Vergrößerung des Festplattenspeichers sowie viel Arbeitsspeicher zum besseren Daten-Caching zu verwenden. Weitere Informationen zu RAID erhalten Sie auch unter [Abschnitt 6.2](#), „Soft-RAID-Konfiguration“ (S. 142).

11.1 Einrichten eines iSCSI-Ziels

SUSE® Linux Enterprise Server wird mit einer Open-Source-Lösung eines iSCSI-Ziels geliefert, die sich aus dem Ardis iSCSI-Ziel entwickelt hat. Eine grundlegende

Konfiguration kann mit YaST erfolgen, aber um alle Vorteile von iSCSI zu nutzen, ist eine manuelle Einrichtung erforderlich.

11.1.1 Erstellen von iSCSI-Zielen mit YaST

Die iSCSI-Zielkonfiguration exportiert bestehende Block-Geräte oder Dateisystem-Images an iSCSI-Initiatoren. Erstellen Sie zunächst die erforderlichen Block-Geräte mit YaST oder erstellen Sie Dateisystem-Images. Einen Überblick über Partitionierung erhalten Sie in [Abschnitt 7.5.8, „Partitionierung“](#) (S. 176). Dateisystem-Images müssen manuell erstellt werden. Beispiel: Wenn Sie das Image `/var/lib/xen/images/xen-0` mit der Größe 4 GB erstellen möchten, stellen Sie zunächst sicher, dass das Verzeichnis vorhanden ist, und legen Sie dann das eigentliche Image an:

```
mkdir -p /var/lib/xen/images
dd if=/dev/zero of=/var/lib/xen/images/xen-0 seek=1M bs=4096 count=1
```

Um das iSCSI-Ziel zu konfigurieren, führen Sie das Modul *iSCSI-Ziel* in YaST aus. Die Konfiguration ist in drei Registerkarten gegliedert. Wählen Sie in der Registerkarte *Service* den Startmodus und die Firewall-Einstellungen. Wenn Sie von einem entfernten Computer auf das iSCSI-Ziel zugreifen möchten, wählen Sie *Firewall-Port öffnen*.

Die Registerkarte *Global* bietet Einstellungen für den iSCSI-Server. Die hier eingestellte Authentifizierung wird zur Erkennung von Diensten, nicht für den Zugriff auf die Ziele verwendet. Wenn Sie den Zugriff auf die Erkennung nicht beschränken möchten, wählen Sie *Keine Authentifizierung*.

Wenn Authentifizierung erforderlich ist, gibt es zwei Möglichkeiten. Bei der einen Möglichkeit muss ein Initiator beweisen, dass er berechtigt ist, eine Erkennung auf dem iSCSI-Ziel auszuführen. Dies geschieht mit *Eingehende Authentifizierung*. Bei der anderen Möglichkeit muss das iSCSI-Ziel dem Initiator beweisen, dass es das erwartete Ziel ist. Daher kann das iSCSI-Ziel auch einen Benutzernamen und ein Passwort angeben. Dies geschieht mit *Ausgehende Authentifizierung*. Weitere Informationen zur Authentifizierung finden Sie in RFC 3720 (siehe <http://www.ietf.org/rfc/rfc3720.txt>).

Die Ziele werden in der Registerkarte *Ziele* definiert. Mit *Hinzufügen* erstellen Sie ein neues iSCSI-Ziel. Im ersten Dialogfeld werden Informationen zu dem zu exportierenden Gerät angefordert.

Ziel

Die Zeile *Ziel* hat eine feste Syntax und sieht etwa wie folgt aus:

```
iqn.yyyy-mm.<reversed domain name>
```

Sie beginnt stets mit `iqn. jfff-mm` ist das Format des Datums, an dem dieses Ziel aktiviert wird. Weitere Informationen zu Namenskonventionen finden Sie in RFC 3722 (siehe <http://www.ietf.org/rfc/rfc3722.txt>).

Bezeichner

Der *Bezeichner* ist frei wählbar. Er sollte einem Schema folgen, um das ganze System besser zu strukturieren.

LUN

Es ist möglich, einem Ziel mehrere LUNs zuzuweisen. Dies wird jedoch mit YaST nicht unterstützt. Daher sollte dies immer auf den Wert 0 eingestellt sein.

Pfad

Fügen Sie diesen Pfad dem Block-Gerät oder Dateisystem-Image hinzu, das exportiert werden soll.

Das nächste Menü konfiguriert die Zugriffsbeschränkungen des Ziels. Die Konfiguration ist sehr ähnlich der Konfiguration der Erkennungsauthentifizierung. In diesem Fall sollte mindestens eine eingehende Authentifizierung eingerichtet werden.

Weiter beendet die Konfiguration des neuen Ziels und bringt Sie zurück zur Übersichtseite der Registerkarte *Ziel*. Aktivieren Sie Ihre Änderungen, indem Sie auf *Beenden* klicken.

11.1.2 Manuelle Konfiguration eines iSCSI-Ziels

Konfigurieren Sie ein iSCSI-Ziel in `/etc/ietd.conf`. Alle Parameter in dieser Datei vor der ersten *Target*-Deklaration sind für die Datei global. Authentifizierungsinformationen in diesem Bereich haben eine besondere Bedeutung: Sie sind nicht global, werden aber für die Erkennung des iSCSI-Ziels verwendet.

Sämtliche iSCSI-Authentifizierungen sind in zwei Richtungen möglich. Das iSCSI-Ziel kann verlangen, dass sich der iSCSI-Initiator mit dem `IncomingUser` authentifiziert, der mehrmals hinzugefügt werden kann. Der iSCSI-Initiator kann auch verlangen,

dass sich das iSCSI-Ziel authentifiziert. Verwenden Sie dafür `OutgoingUser`. Beide haben dieselbe Syntax:

```
IncomingUser <username> <password>
OutgoingUser <username> <password>
```

Auf die Authentifizierung folgen eine oder mehrere Zieldefinitionen. Fügen Sie für jedes Ziel einen Abschnitt `Target` hinzu. Dieser Abschnitt beginnt immer mit dem Bezeichner `Target`, auf die Definitionen von logischen Einheitennummern (LUNs) folgen:

```
Target iqn.yyyy-mm.<reversed domain name>[:identifizier]
    Lun 0 Path=/dev/mapper/system-v3
    Lun 1 Path=/dev/hda4
    Lun 2 Path=/var/lib/xen/images/xen-1,Type=fileio
```

In der Zeile `Target` gibt `yyyy-mm` das Datum an, an dem dieses Ziel aktiviert wird, und der Bezeichner ist frei wählbar. Weitere Informationen zu Namenskonventionen finden Sie in RFC 3722 (siehe <http://www.ietf.org/rfc/rfc3722.txt>). Drei verschiedene Block-Geräte werden in diesem Beispiel exportiert. Das erste ist ein logisches Volume (siehe auch [Abschnitt 6.1, „LVM-Konfiguration“](#) (S. 133)), das zweite ist eine IDE-Partition und das dritte ist ein Image, das im lokalen Dateisystem verfügbar ist. Für einen iSCSI-Initiator sehen alle wie Block-Geräte aus.

Bevor Sie das iSCSI-Ziel aktivieren, fügen Sie mindestens einen `IncomingUser` nach den `Lun`-Definitionen hinzu. Damit wird die Authentifizierung für die Verwendung dieses Ziels festgelegt.

Um alle Änderungen zu aktivieren, starten Sie den `iscsitarget`-Daemon neu mit `rciscsi restart`. Prüfen Sie Ihre Konfiguration im Dateisystem `/proc`:

```
cat /proc/net/iet/volume
tid:1 name:iqn.2006-02.com.example.iserv:systems
    lun:0 state:0 iotype:fileio path:/dev/mapper/system-v3
    lun:1 state:0 iotype:fileio path:/dev/hda4
    lun:2 state:0 iotype:fileio path:/var/lib/xen/images/xen-1
```

Es gibt noch viele weitere Optionen, die das Verhalten des iSCSI-Ziels steuern. Informationen dazu finden Sie auf der Manualpage von `ietd.conf`.

Aktive Sitzungen werden ebenfalls im Dateisystem `/proc` angezeigt. Für jeden Initiator wird ein zusätzlicher Eintrag zu `/proc/net/iet/session` hinzugefügt:

```
cat /proc/net/iet/session
tid:1 name:iqn.2006-02.com.example.iserv:system-v3
    sid:562949957419520
```

```
initiator:iqn.2005-11.de.suse:cn=rome.example.com,01.9ff842f5645
  cid:0 ip:192.168.178.42 state:active hd:none dd:none
sid:281474980708864 initiator:iqn.2006-02.de.suse:01.6f7259c88b70
  cid:0 ip:192.168.178.72 state:active hd:none dd:none
```

11.1.3 Konfigurieren von Online-Zielen mit ietadm

Wenn Änderungen an der iSCSI-Zielkonfiguration erforderlich sind, müssen Sie immer das Ziel neu starten, um die Änderungen zu aktivieren, die in der Konfigurationsdatei vorgenommen wurden. Leider werden alle aktiven Sitzungen durch diesen Vorgang unterbrochen. Um einen ungestörten Betrieb zu wahren, sollten die Änderungen in der Hauptkonfigurationsdatei `/etc/ietd.conf` erfolgen, aber auch manuell in der aktuellen Konfiguration mit dem Administrationsdienstprogramm `ietadm` vorgenommen werden.

Um ein neues iSCSI-Ziel mit einer LUN zu erstellen, aktualisieren Sie zunächst Ihre Konfigurationsdatei. Der zusätzliche Eintrag könnte folgendermaßen aussehen:

```
Target iqn.2006-02.com.example.iserv:system2
  Lun 0 Path=/dev/mapper/system-swap2
  IncomingUser joe secret
```

So richten Sie diese Konfiguration manuell ein:

- 1 Erstellen Sie ein neues Ziel mit dem Befehl `ietadm --op new --tid=2 --params Name=iqn.2006-02.com.example.iserv:system2`.
- 2 Fügen Sie eine logische Einheit hinzu mit `ietadm --op new --tid=2 --lun=0 --params Path=/dev/mapper/system-swap2`.
- 3 Definieren Sie die Kombination aus Benutzername und Passwort für dieses Ziel mit `ietadm --op new --tid=2 --user --params=IncomingUser=joe,Password=secret`.
- 4 Prüfen Sie die Konfiguration mit `cat /proc/net/iet/volume`.

Sie können auch aktive Verbindungen löschen. Prüfen Sie zunächst alle aktiven Verbindungen mit dem Befehl `cat /proc/net/iet/session`. Das kann wie folgt aussehen:

```
cat /proc/net/iet/session
tid:1 name:ign.2006-03.com.example.iserv:system
      sid:281474980708864 initiator:ign.1996-04.com.example:01.82725735af5
      cid:0 ip:192.168.178.72 state:active hd:none dd:none
```

Um die Sitzung mit der Sitzungs-ID 281474980708864 zu löschen, verwenden Sie den Befehl `ietadm --op delete --tid=1 --sid=281474980708864 --cid=0`. Beachten Sie, dass das Gerät dadurch auf dem Clientsystem unzugänglich wird und sich Prozesse, die auf dieses Gerät zugreifen, wahrscheinlich aufhängen.

`ietadm` kann auch zum Ändern verschiedener Konfigurationsparameter verwendet werden. Beziehen Sie eine Liste der globalen Variablen mit `ietadm --op show --tid=1 --sid=0`. Die Ausgabe sieht wie folgt aus:

```
InitialR2T=Yes
ImmediateData=Yes
MaxConnections=1
MaxRecvDataSegmentLength=8192
MaxXmitDataSegmentLength=8192
MaxBurstLength=262144
FirstBurstLength=65536
DefaultTime2Wait=2
DefaultTime2Retain=20
MaxOutstandingR2T=1
DataPDUInOrder=Yes
DataSequenceInOrder=Yes
ErrorRecoveryLevel=0
HeaderDigest=None
DataDigest=None
OFMarker=No
IFMarker=No
OFMarkInt=Reject
IFMarkInt=Reject
```

All diese Parameter lassen sich auf einfache Weise ändern. Wenn Sie beispielsweise die maximale Anzahl der Verbindungen auf zwei ändern möchten, verwenden Sie `ietadm --op update --tid=1 --params=MaxConnections=2`. In der Datei `/etc/ietd.conf` sollte die zugehörige Leitung aussehen wie `MaxConnections 2`.

WARNUNG: Aktualisieren von `ietd.conf` gemäß den Änderungen mithilfe von `ietadm`

Die Änderungen, die Sie mit dem Befehl `ietadm` vornehmen, sind für das System nicht permanent. Diese Änderungen gehen beim nächsten Neubooten verloren, wenn sie nicht in die Konfigurationsdatei `/etc/ietd.conf`

aufgenommen werden. Abhängig von der Nutzung von iSCSI in Ihrem Netzwerk kann dies zu ernststen Problemen führen.

Es gibt etliche weitere Optionen für den Befehl `ietadm`. Einen Überblick erhalten Sie mit `ietadm -h`. Die Abkürzungen sind dort die Ziel-ID (`tid`), Sitzungs-ID (`sid`) und Verbindungs-ID (`cid`). Diese können auch in `/proc/net/iet/session` gefunden werden.

11.2 Konfigurieren eines iSCSI-Initiators

Ein iSCSI-Initiator, auch Client genannt, kann zur Verbindung zu einem beliebigen iSCSI-Ziel verwendet werden. Dies ist nicht auf die oben erläuterte iSCSI-Ziellösung beschränkt. Die Konfiguration des iSCSI-Initiators umfasst zwei wesentliche Schritte: die Erkennung von verfügbaren iSCSI-Zielen und das Einrichten einer iSCSI-Sitzung. Beides kann mit YaST erledigt werden.

11.2.1 Verwendung von YaST für die iSCSI-Initiator-Konfiguration

Die Konfiguration ist in drei Registerkarten gegliedert. Über die Registerkarte *Dienst* kann der iSCSI-Initiator beim Booten aktiviert werden. Die Registerkarte *Verbundene Ziele* gibt einen Überblick über die aktuell verbundenen iSCSI-Ziele. Wie die Registerkarte *Ermittelte Ziele* bietet sie eine Option für das Hinzufügen neuer Ziele zum System. *Ermittelte Ziele* ist die Registerkarte, mit der begonnen wird. Sie bietet die Möglichkeit, iSCSI-Ziele im Netzwerk zu ermitteln.

- 1 Wählen Sie *Ermittlung*, um das entsprechende Dialogfeld zu öffnen.
- 2 Geben Sie die IP-Adresse ein und ändern Sie den Port, falls erforderlich.
- 3 Fügen Sie bei Bedarf die *Eingehende* oder *Ausgehende* Authentifizierung hinzu.
- 4 Starten Sie die Ermittlung, indem Sie auf *Weiter* klicken.

Verwenden Sie nach einer erfolgreichen Ermittlung *Anmeldung*, um das Ziel zu aktivieren. Sie werden aufgefordert, Authentifizierungsinformationen für die Verwendung des ausgewählten iSCSI-Ziels einzugeben. *Weiter* beendet die Konfiguration. Wenn alles korrekt ausgeführt wurde, wird das Ziel nun in *Verbundene Ziele* angezeigt.

Das virtuelle iSCSI-Gerät ist nun verfügbar. Finden Sie das tatsächliche Gerät mit `lsscsi`:

```
lsscsi
[1:0:0:0] disk IET VIRTUAL-DISK 0 /dev/sda
```

11.2.2 Manuelles Einrichten des iSCSI-Initiators

Sowohl die Ermittlung als auch die Konfiguration von iSCSI-Verbindungen erfordert ein laufendes `iscsid`. Beim ersten Ausführen der Ermittlung wird die interne Datenbank des iSCSI-Initiators im Verzeichnis `/var/lib/open-iscsi` angelegt.

Wenn Ihre Ermittlung durch ein Passwort geschützt ist, geben Sie die Authentifizierungsinformation für `iscsid` an. Da die interne Datenbank bei der ersten Ermittlung nicht existiert, kann sie zu diesem Zeitpunkt nicht benutzt werden. Stattdessen muss die Konfigurationsdatei `/etc/iscsid.conf` so bearbeitet werden, dass die Information geliefert wird. Um Ihre Passwortinformation für die Ermittlung anzugeben, fügen Sie die folgenden Zeilen an das Ende von `/etc/iscsid.conf`:

```
discovery.sendtargets.auth.authmethod = CHAP
discovery.sendtargets.auth.username = <username>
discovery.sendtargets.auth.password = <password>
```

Die Ermittlung speichert alle empfangenen Werte in einer internen persistenten Datenbank. Zusätzlich zeigt sie alle ermittelten Ziele an. Führen Sie diese Ermittlung aus mit `iscsiadm -m discovery --type=st --portal=<targetip>`. Die Ausgabe sollte wie folgt aussehen:

```
[bd0ac2] 149.44.171.99:3260,1 iqn.2006-02.com.example.iserv:systems
```

Für jedes Ziel, das auf dem iSCSI-Ziel definiert ist, wird eine Zeile angezeigt. Im vorherigen Beispiel lautet die ID des Ziels `bd0ac2`. Diese ID wird verwendet, um auf das Ziel zuzugreifen. Weitere Informationen zu den gespeicherten Daten erhalten Sie in [Abschnitt 11.2.3, „Die iSCSI-Client-Datenbanken“](#) (S. 293). Ändern Sie im Moment nur die Authentifizierungsdaten in dieser Datenbank, damit Sie auf das Ziel `bd0ac2`

zugreifen können. Nehmen Sie an, dass Sie mit *incoming user*<username> (Eingehender Benutzer <Benutzername>) und *password* <password> (Passwort <Passwort>) auf ein Ziel zugreifen:

```
iscsiadm -m node --record=bd0ac2 --op=update \  
    --name=node.session.auth.authmethod --value=CHAP  
iscsiadm -m node --record=bd0ac2 --op=update \  
    --name=node.session.auth.username --value=<username>  
iscsiadm -m node --record=bd0ac2 --op=update \  
    --name=node.session.auth.password --value=<password>
```

Nun ist der Initiator für seine Aktivierung vorbereitet. Die Spezialoption `--login` von `iscsiadm` erstellt alle erforderlichen Geräte:

```
iscsiadm -m node --record=bd0ac2 --login
```

Die neu generierten Geräte werden in der Ausgabe von `lsscsi` aufgeführt und per "mount" (Einhängen) kann auf sie zugegriffen werden.

11.2.3 Die iSCSI-Client-Datenbanken

Sämtliche Informationen, die vom iSCSI-Initiator ermittelt wurden, werden in zwei Datenbankdateien gespeichert, die sich in `/var/lib/open-iscsi` befinden. Es gibt eine Datenbank für die Ermittlung von Zielen und eine für die ermittelten Knoten. Beim Zugriff auf eine Datenbank müssen Sie zuerst wählen, ob Sie Ihre Daten aus der Ermittlungs- oder der Knoten-Datenbank beziehen möchten. Das erledigen Sie mit den Parametern `-m discovery` und `-m node` von `iscsiadm`. Wenn Sie `iscsiadm` mit nur einem dieser Parameter verwenden, erhalten Sie eine Übersicht über die gespeicherten Datensätze:

```
iscsiadm -m discovery  
[bd0ac2] 149.44.171.99:3260,1 iqn.2006-02.com.example.iserv:systems
```

Die Datensatz-ID in diesem Beispiel lautet `bd0ac2`. Diese ID ist für sämtliche Aktionen erforderlich, die sich auf diesen Datensatz beziehen. Verwenden Sie den folgenden Befehl, um den Inhalt des Datensatzes mit der ID `bd0c2` zu prüfen:

```
iscsiadm -m node --record=bd0ac2  
node.name = iqn.2006-02.com.example.iserv:systems  
node.transport_name = tcp  
node.tpgt = 1  
node.active_conn = 1  
node.startup = manual  
node.session.initial_cmdsnsn = 0  
node.session.reopen_max = 32
```

```
node.session.auth.authmethod = CHAP
node.session.auth.username = joe
node.session.auth.password = *****
node.session.auth.username_in = <empty>
node.session.auth.password_in = <empty>
node.session.timeo.replacement_timeout = 0
node.session.err_timeo.abort_timeout = 10
node.session.err_timeo.reset_timeout = 30
node.session.iscsi.InitialR2T = No
node.session.iscsi.ImmediateData = Yes
....
```

Um den Wert einer dieser Variablen zu bearbeiten, verwenden Sie den Befehl `iscsiadm` mit der Option `update`. Wenn `iscsid` sich beispielsweise bei seiner Initialisierung beim iSCSI-Ziel anmelden soll, setzen Sie die Variable `node.startup` auf den Wert `automatic`:

```
iscsiadm -m node --record=bd0ac2 --op=update --name=node.startup
--value=automatic
```

Entfernen Sie veraltete Datensätze mit der Operation `delete`. Wenn der Datensatz `bd0ac2` nicht mehr gültig ist, löschen Sie ihn mit dem Befehl `iscsiadm -m node --record=bd0ac2 --op=delete`. Verwenden Sie diesen Befehl mit Vorsicht, da er den Datensatz ohne zusätzliche Bestätigung löscht.

11.2.4 Weitere Informationen

Das iSCSI-Protokoll ist schon mehrere Jahre verfügbar. Es gibt viele Reviews und zusätzliche Dokumentation, die iSCSI mit SAN-Lösungen vergleicht, Leistungs-Benchmarks testet oder einfach Hardwarelösungen beschreibt. Wichtige Seiten für weitere Information zu `open-iscsi`:

- <http://www.open-iscsi.org/>
- <http://www.open-iscsi.org/cgi-bin/wiki.pl>
- <http://www.novell.com/coolsolutions/appnote/15394.html>

Es steht auch einige Online-Dokumentation zur Verfügung. Siehe die Manualpages von `iscsiadm`, `iscsid`, `ietd.conf` und `ietd` sowie die Beispiel-Konfigurationsdatei `/etc/iscsid.conf`.

Hohe Verfügbarkeit (High Availability) unter Linux

12

In diesem Kapitel erhalten Sie eine kurze Übersicht über die grundlegenden Konzepte und Werkzeuge für eine hohe Verfügbarkeit unter Linux. Außerdem erhalten Sie zu allen erläuterten Themen Hinweise zu weiteren Publikationen.

Hohe Verfügbarkeit bedeutet, dass Systeme bestimmte Fehlfunktionen überwinden können. Damit sind vor allem Ausfälle einzelner Computer gemeint. Der Dienst steht nach nur kurzer Ausfallzeit wieder für den Benutzer zur Verfügung. Hardware und Software sind sorgfältig aufeinander abgestimmt und in Bezug auf Redundanz optimiert. So ist bei einem Ausfall ein automatischer Wechsel zu anderen Komponenten möglich. Die Bezeichnung „Hohe Verfügbarkeit“ unterscheidet sich von der „Fehlertoleranz“, da der Dienst kurzfristig für die Zeit des Umschaltens nicht verfügbar ist. Das macht sich in Verzögerungen oder kurzen Verbindungsverlusten bemerkbar.

Ein System mit hoher Verfügbarkeit bedeutet, dass die Gesamtverfügbarkeit des Dienstes zwischen 99,999 Prozent und 99,99999 liegt. Das entspricht einer Ausfallzeit von drei Sekunden bis fünf Minuten in einem ganzen Jahr. Der wichtigste Faktor ist nicht nur die Software und Hardware, sondern vor allem eine gut geplante Systemadministration mit gut dokumentierten und verständlichen Prozessen zur Fehlerbeschränkung. Dabei müssen Risiken und Kosten stets abgewägt werden. Verschiedene Anforderungen und Lösungen sind eventuell erforderlich, je nach dem Anwendungsszenario. Ihr Novell-Partner berät Sie gerne.

12.1 Wichtige Begriffe

Im Folgenden sehen Sie einige wichtige Begriffe zur hohen Verfügbarkeit:

SPOF

Single Point of Failure: Systemkomponente, deren Ausfall die Funktion des ganzen Systems behindert.

Failover

Eine ähnliche Systemkomponente übernimmt automatisch die Funktion der ausgefallenen Komponente.

Cold-Standby

Die alternative Hardware befindet sich im Cold-Standby-Modus. Der Failover muss manuell durchgeführt werden. So wird der Fehler deutlich bemerkbar.

Warm-Standby

Das Backup-System wird im Hintergrund ausgeführt. Der Wechsel findet automatisch statt. Die Daten beider Systeme werden automatisch synchronisiert. Für den Benutzer wird der Failover als sehr schneller automatischer Neustart eines Diensts sichtbar. Der aktuelle Vorgang wird jedoch eventuell abgebrochen, weil eine Synchronisierung der Daten vor dem Fehler nicht möglich war.

Hot-Standby

Beide Systeme werden ständig parallel ausgeführt. Die Daten auf beiden Systemen sind hundertprozentig synchronisiert. Der Benutzer bemerkt keinen Ausfall. Diese Stufe kann gewöhnlich nicht erreicht werden, ohne eine entsprechende Änderung am Client vorzunehmen. Sollen beide Systeme komplett synchron ausgeführt werden, müssen die Verbindungen mit dem Client hundertprozentig gespiegelt werden. Das erfordert meist, dass die Clients mit zwei oder mehr Servern gleichzeitig verbunden sind und mit allen kommunizieren. Ein gewöhnlicher Webbrowser genügt hierfür nicht.

Belastungsausgleich

Die Verteilung der Belastung in einem Cluster von Computern. Der *Belastungsausgleich* wird beispielsweise in einem LVS-Szenario (*Linux Virtual-Server*) verwendet (siehe [Abschnitt 12.5.2, „Linux Virtual Server“](#) (S. 301)).

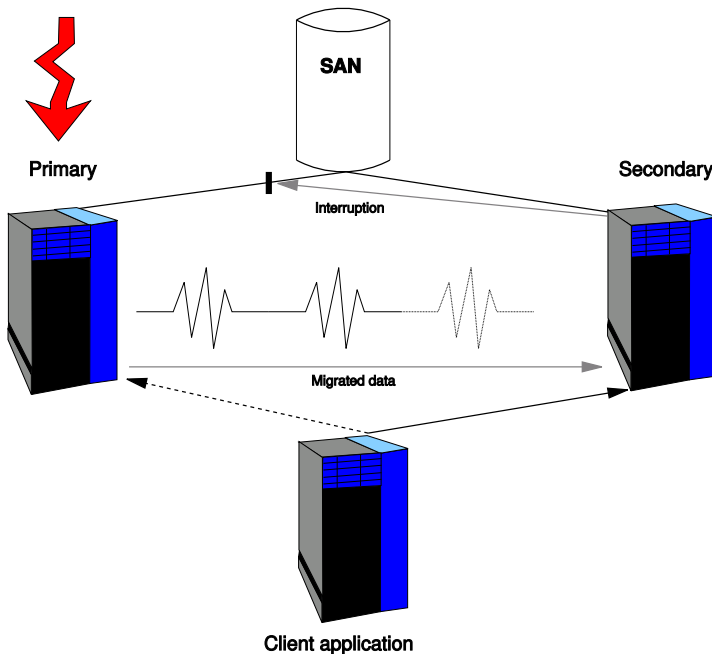
STONITH

Shot the other node in the head: Spezielle Hard- und Software, die sicherstellt, dass ein fehlerhafter Knoten keinen Schreibzugriff auf verteilte Medien in einem Cluster hat und so die Datenkonsistenz im gesamten Cluster gefährdet. Das bedeutet, dass das System einfach von der Stromversorgung getrennt wird.

12.2 Ein Mindestszenario als Beispiel

Die Vorgänge in einem Zwei-Knoten-Cluster, wenn ein Knoten ausfällt und die verschiedenen Standby-Systeme, die gegebenenfalls übernehmen können, sind unten aufgeführt (siehe [Abbildung 12.1](#), „Ein einfacher Cluster mit hoher Verfügbarkeit“ (S. 297)).

Abbildung 12.1 Ein einfacher Cluster mit hoher Verfügbarkeit



Die beiden Server (primärer und Backup-Server) sind beide mit einem SAN (Storage Area Network) verbunden. Je nach dem Modus wird auf das Netzwerk nur über den aktiven Knoten zugegriffen. Die Server kommunizieren miteinander, indem Sie regelmäßig ein „Lebenszeichen“ (Heartbeat) von sich geben. Die Kommunikationskanäle (oder *Heartbeat-Links*) sind auch redundant ausgelegt. Daher können über verschiedene Netzwerkkarten und Kabelkanäle unabhängige Kanäle verwendet werden. Fällt einer der Links aus, berichten die Backup-Links korrekt, dass der entsprechende Server immer noch „lebt“. Falls das Hauptsystem keine Lebenszeichen mehr von sich gibt, wird das Standby-System aktiviert. Es übernimmt die Dienste des ausgefallenen Partners und entfernt ihn komplett aus dem Netzwerk (STONITH)

12.3 Komponenten einer Lösung mit hoher Verfügbarkeit

Eine Lösung mit hoher Verfügbarkeit besteht aus verschiedenen Komponenten:

Allgemeine Infrastruktur

Bei der Planung einer Lösung mit hoher Verfügbarkeit sollten Sie nicht vergessen, dass sogar die Installation aller Schlüsselservers an einem einzigen Standort ein potenzieller SPOF sein kann, falls dieser Standort von einer Katastrophe oder einem Stromausfall heimgesucht wird. Die Umgebungsbedingungen der Server sollten ebenfalls beachtet werden: (redundante) Klimaanlage sind unbedingt erforderlich.

Hardware

Sogar die anspruchsvollste Software kann kein System mit hoher Verfügbarkeit garantieren, wenn Hardware-seitig nicht die bestmögliche Ausfallsicherheit garantiert wird. Die grundlegenden Hardwarekomponenten, die in Betracht gezogen und mit größtmöglicher Redundanz geplant werden sollten, lauten:

Stromversorgung

Sichern Sie Ihre Server, falls möglich mit einer unterbrechungsfreien Stromversorgung (UPS), um sicherzustellen, dass ein kurzer Stromausfall überbrückt wird und die Systeme korrekt heruntergefahren werden können, falls ein längerer Ausfall droht. Die Stromversorgung sollte auch für die Redundanz konfiguriert werden.

Netzwerkschnittstellen

Vergewissern Sie sich, dass jedes Ihrer Systeme über mehrere Netzwerkschnittstellen verfügt. Falls eine Schnittstelle ausfällt, muss automatisch eine andere die Adresse und Aufgabe der ausgefallenen Komponente übernehmen. Die Redundanz bezieht sich auf beide Schnittstellenrichtungen. Es kann nicht schaden, wenn Sie eine aktive und eine Backup-Schnittstelle für die internen und externen Schnittstellen planen.

Festplatten

Weisen Sie Ihrem System mehrere Festplatten zu und organisieren Sie die Datensicherung (z. B. mit RAID oder drbd) so, dass im Falle eines Festplattenverlusts die anderen vollständige Datensätze enthalten. Es muss möglich sein, eine fehlerhafte Festplatte durch eine andere auszutauschen, ohne das System anzuhalten.

Anwendungen

Alle wichtigen Daten und Anwendungen, die das Äußere Ihres Systems ausmachen, müssen so angeordnet werden, dass sie keinen Neustart verhindern. Wenn eine Anwendung nach einem Systemabsturz die Sperre nicht freigibt, kann der entsprechende Prozess nicht neu gestartet werden. Das bedeutet, dass die Anwendung sich nicht für eine Umgebung mit hoher Verfügbarkeit eignet. Der „Gesundheitszustand“ bestimmter Anwendungen, Betriebssystemprozesse und Netzwerkverbindungen sollte am besten mit einem passenden Überwachungstool überwacht werden.

Daten

Nach einem Systemausfall müssen alle relevanten Daten für das Failover-System komplett und intakt verfügbar sein. Diese Art der hohen Verfügbarkeit wird erreicht durch die Verteilung gespeicherter Daten auf einige Systeme und Festplatten. Dafür wird der Inhalt einer Platte regelmäßig auf eine andere Platte (oder mehrere) gespiegelt. Diese haben bei einem Systemausfall die intakten Datensätze verfügbar. Verwenden Sie ein Journaling-Dateisystem, um sicherzustellen, dass ein Dateisystem nach einem Systemabsturz vollständig startet.

Netzwerk

Die gesamte Netzwerkinfrastruktur sollte in Bezug auf Redundanz konfiguriert werden, vom Router und der Switch-Infrastruktur bis zum einfachsten Netzwerkkabel.

12.4 Software-Anforderungen bei hoher Verfügbarkeit

Im Folgenden werden die grundlegenden Software-Aspekte einer Lösung mit hoher Verfügbarkeit beschrieben.

12.4.1 heartbeat

heartbeat ist ein Softwarepaket zur Überwachung aller Knoten im Cluster. *heartbeat* sendet „Herztöne“ an den Netzwerkschnittstellen der Cluster-Mitglieder, um herauszufinden, welche Knoten im Cluster aktiv sind. Wenn ein Knoten ausfällt, gibt er kein Signal aus. In diesem Fall stellt *heartbeat* sicher, dass ein anderer Knoten die

entsprechenden Aufgaben und die Identität übernimmt und gibt den Failover im Netzwerk bekannt. Das bedeutet, der Cluster bleibt konsistent. Weitere Informationen hierzu finden Sie in [Kapitel 13, *Installieren eines Heartbeat 2-Clusters mithilfe von YaST*](#) (S. 305).

12.4.2 RAID

RAID (die redundante Anordnung unabhängiger Festplatten) kombiniert mehrere Festplattenpartitionen, um eine große *virtuelle* Festplatte zu bilden. RAID kann zur Leistungsoptimierung und zur Datensicherung Ihres Systems verwendet werden. RAID-Stufen 1 bis 5 bieten Schutz gegen den Ausfall einer Festplatte, weil die Daten auf mehreren Platten gleichzeitig gespeichert werden. Dadurch wird sichergestellt, dass der komplette Datensatz immer auf anderen Festplatten im System verfügbar ist, falls eine ausfällt. Weitere Informationen zum Einsatz von RAID mit SUSE® Linux Enterprise Server finden Sie in [Abschnitt 6.2, „Soft-RAID-Konfiguration“](#) (S. 142).

12.4.3 rsync

rsync kann zum Synchronisieren großer Datenmengen zwischen einem Server und seinem Backup verwendet werden. rsync verfügt über anspruchsvolle Mechanismen zur ausschließlichen Übertragung der Änderungen in den Dateien. Dies betrifft nicht nur Textdateien, sondern auch binäre Dateien. Um die Unterschiede zwischen den Dateien zu ermitteln, teilt rsync die Dateien in Blöcke und berechnet Prüfsummen für diese Blöcke. Weitere Informationen zu rsync finden Sie in [Abschnitt 40.6, „Einführung in rsync“](#) (S. 805).

12.4.4 DRBD

Distributed replicated block device (drbd) spiegelt (RAID1) Partitionen und logische Volumes (Datenbereiche), indem ein normales Netzwerk auf Basis von TCP/IP gespiegelt wird. Jeder Knoten verfügt über eine bestimmte aktive drbd-Ressource und alle Änderungen werden als sichere Transaktionen gespiegelt.

drbd hat zusätzliche Funktionen im Vergleich zu RAID1 für lokale Festplatten, die die Resynchronisierungszeit minimieren nachdem die beiden Knoten kurz unterbrochen wurden und eine gründliche Überprüfung nach verschiedenen Fehlfunktionen ermöglichen, um herauszufinden, welche Seite über die neusten, konsistenten Daten verfügt.

12.5 Clustering

12.5.1 Cluster-Alias

Der Cluster-Alias ist eine Technologie mit der mehrere Knoten mit einer gemeinsamen IP-Adresse konfiguriert werden können. Dabei werden auch TCP/IP-Verbindungen mit dieser Adresse erlaubt. Eingehende TCP/IP-Verbindungen werden automatisch verteilt.

Anders als bei Linux Virtual Server ist kein dedizierter Lastenausgleich erforderlich. Aufgrund der Installationsart ist der Cluster-Alias jedoch weniger effizient, wenn es eine große Anzahl von Knoten gibt. Im Fall des Cluster-Alias werden alle IP-Pakete an alle Knoten verteilt, die dann die für sie bestimmten Pakete herausfiltern. Im Fall des LVS wird diese Entscheidung nur vom Lastenausgleich getroffen. Genauere Informationen zur Konfiguration dieser Funktion finden Sie auf der Manualpage `iptables`.

12.5.2 Linux Virtual Server

Linux Virtual Server basiert auf einem echten Cluster mit mehreren Servern, die über einen Lastenausgleich verbunden sind. Dieser verteilt die Lastung auf die verschiedenen Mitglieder des Clusters. Von außen sieht ein solcher Cluster wie ein einzelner virtueller Server aus. Der Lastenausgleich sollte also auf Redundanz konfiguriert und mithilfe von `heartbeat` gesichert werden. Das Ziel einer LVS-Konfiguration ist die bestmögliche Nutzung der vorhandenen Ressourcen und eine gute Skalierbarkeit. Der `heartbeat-lldirectord`-Daemon wird in diesen Fällen zur Überwachung des „Gesundheitszustands“ der verschiedenen echten Server verwendet.

12.5.3 Cluster für hohe Verfügbarkeit

Cluster für hohe Verfügbarkeit sind so ausgelegt, dass alle verfügbaren Dienste jederzeit nutzbar sind, unabhängig von Hard- oder Softwareausfällen. Wenn ein Knoten im Cluster ausfällt, übernimmt sofort ein anderer. Dieser Knoten (*sekundär*) ist ein gespiegeltes Image des ausgefallenen Knotens (*primär*) und übernimmt die Identität des ausgefallenen Knotens während des Failovers. So bleibt die Cluster-Umgebung äußerlich konsistent.

12.6 Weitere Informationen

12.6.1 Hohe Verfügbarkeit im Allgemeinen und heartbeat

Die hauptsächliche Informationsquelle zur hohen Verfügbarkeit unter Linux ist die Homepage des Projekts *Linux-HA* (<http://linux-ha.org>). Hier finden Sie viele Tipps und Links zu Dokumentationen, Berichten und Szenarien.

Weitere Informationen in Buchform zur hohen Verfügbarkeit erhalten Sie unter *Blueprints in High Availability*:

Marcus, Evan & Stern, Hal: *Blueprints in High Availability*. John Wiley & Sons Inc., 2000. (ISBN 0-471-35601-8)

► **zseries:** Es gibt ein sehr ausführliches Redpaper für Linux auf IBM-System z mit einer Vielzahl an Beispielszenarien und Konfigurationen unter <http://publib-b.boulder.ibm.com/Redbooks.nsf/RedpaperAbstracts/redp0220.html>. ◀

Einen Wiki in Bezug auf Hohe Verfügbarkeit und heartbeat finden Sie unter <http://wiki.trick.ca/linux-ha/PressRoom> und <http://wiki.trick.ca/linux-ha/HeartbeatTutorials>

12.6.2 DRBD

Die Homepage für das DRBD-Projekt lautet <http://www.drbd.org/>. Einen nützlichen Artikel des Linux-Magazins finden Sie unter http://www.linux-mag.com/2003-11/drbd_01.html.

12.6.3 RAID

Eine genaue Link-Sammlung zum Thema RAID: <http://linas.org/linux/raid.html>

12.6.4 Clustering

Die Homepage *Linux Clustering Information Center* bietet weitere Informationen zum Clustering unter <http://www.lcic.org/>. Die Homepage für das Projekt *Linux Virtual Server* lautet <http://www.linuxvirtualserver.org/>.

Einzelheiten zum *Oracle-Cluster-Dateisystem* erhalten Sie auf der Projekt-Homepage unter <http://oss.oracle.com/projects/ocfs/> und genaue Dokumentation unter <http://oss.oracle.com/projects/ocfs/documentation/>.

Installieren eines Heartbeat 2-Clusters mithilfe von YaST

13

Heartbeat 2 ist nun Teil von SUSE® Linux Enterprise 10. Ein Heartbeat 2-Cluster kann mithilfe des YaST-Einrichtungswerkzeugs installiert und konfiguriert werden. Während der Installation von Heartbeat 2 werden Sie zur Eingabe von Informationen aufgefordert, die für die korrekte Funktionsweise von Heartbeat 2 erforderlich sind. Dieser Abschnitt enthält Informationen, die Sie bei der Installation und Konfiguration eines Heartbeat 2-Clusters unterstützen.

Dieses Cluster-Installationsprogramm kopiert nicht das Heartbeat-Softwarepaket auf Cluster-Knoten. Vor Ausführung dieses Installationsprogramms muss das Heartbeat-Softwarepaket auf allen Knoten installiert werden, die Ihrem Cluster angehören sollen. Dies ist während der Installation von SUSE Linux Enterprise 10 oder später möglich.

Dieses Installationsprogramm ermöglicht Ihnen die Erstellung eines neuen Clusters oder das Hinzufügen von Knoten zu einem bestehenden Cluster. Wenn Sie einem bestehenden Cluster neue Knoten hinzufügen möchten, müssen Sie dieses Installationsprogramm von einem Knoten ausführen, der bereits im Cluster enthalten ist, nicht auf einem Knoten, den Sie in den Cluster aufnehmen möchten.

13.1 Hardware-Anforderungen

Die folgende Liste führt die Hardware-Anforderungen für ein Heartbeat 2-Cluster auf. Diese Anforderungen stellen die Hardware-Minimalkonfiguration dar. Abhängig vom beabsichtigten Einsatz Ihres Heartbeat 2-Clusters kann zusätzliche Hardware erforderlich sein.

- Mindestens zwei Linux-Server

Die Server benötigen keine identische Hardware (Arbeitsspeicher, Festplattengröße usw.)

- Mindestens ein Kommunikationsmedium (Ethernet usw.), das die Kommunikation zwischen Cluster-Knoten ermöglicht

13.2 Software-Anforderungen

Stellen Sie sicher, dass die folgenden Software-Anforderungen erfüllt sind:

- SUSE Linux Enterprise 10 ist auf allen Knoten installiert, die dem Heartbeat 2-Cluster angehören sollen.
- Das Heartbeat 2-Softwarepaket ist auf allen Knoten installiert, die dem Heartbeat-Cluster angehören sollen.

13.3 Voraussetzungen für ein freigegebenes Festplattensystem

Ein freigegebenes Festplattensystem (Storage Area Network bzw. SAN) ist für Ihr Cluster erforderlich, um eine hohe Verfügbarkeit Ihrer Daten zu erzielen. Wenn ein freigegebenes Festplattensubsystem benutzt wird, stellen Sie Folgendes sicher:

- Das freigegebene Festplattensystem wurde gemäß den Anweisungen des Herstellers installiert und funktioniert ordnungsgemäß.
- Novell empfiehlt, dass die im freigegebenen Festplattensystem enthaltenen Festplatten so konfiguriert sind, dass sie Spiegelung oder RAID verwenden, um das freigegebene Festplattensystem mit Fehlertoleranz zu versehen.
- Wenn Sie über iSCSI auf das freigegebene Plattensystem zugreifen, stellen Sie sicher, dass die iSCSI-Initiatoren und -Ziele korrekt konfiguriert sind.

13.4 Installieren von Heartbeat 2

- 1 Geben Sie an der Linux-Serverkonsole eines Servers `yast2 heartbeat` ein, um das Heartbeat 2-Installationsprogramm zu starten.

Sie müssen als `root` angemeldet sein, um auf den Cluster-Konfigurationsbildschirm zuzugreifen.

- 2 Fügen Sie dem Cluster im Fenster "Node Configuration" einen Knoten hinzu, indem Sie den Namen des gewünschten Knotens eingeben und auf *Add* klicken. Wiederholen Sie diesen Vorgang für jeden Knoten, den Sie dem Cluster hinzufügen möchten, und klicken Sie dann auf *Next*.

Sie können Knotennamen für Server finden, indem Sie auf jedem Knoten `uname -n` eingeben.

Wenn Sie nach dem Hinzufügen eines Knotens zum Cluster den Namen dieses Knotens ändern müssen, doppelklicken Sie auf den entsprechenden Knoten, ändern Sie seinen Namen und klicken Sie dann auf "Edit".

- 3 Geben Sie im Fenster "Authentication Keys" die Authentifizierungsmethode für die Kommunikation zwischen Cluster-Knoten sowie bei Bedarf einen Authentifizierungsschlüssel (ein Passwort) an. Klicken Sie anschließend auf *Weiter*.

Für die MD5- und SHA1-Methode ist ein gemeinsam genutzter geheimer Schlüssel erforderlich, anhand dessen Nachrichten geschützt und authentifiziert werden. Die CRC-Methode führt keine Nachrichtenauthentifizierung durch und schützt nur vor Beschädigung, nicht vor Angriffen.

Die SHA1-Methode wird empfohlen, da sie das stärkste Authentifizierungsschema bietet, das verfügbar ist. Der angegebene Authentifizierungsschlüssel (Passwort) wird für alle Knoten im Cluster verwendet.

- 4 Geben Sie im Fenster "Medienkonfiguration" die Methode an, die Heartbeat 2 zur internen Kommunikation zwischen Cluster-Knoten verwenden soll.

Auf diese Weise können Cluster-Knoten anderen Knoten im Cluster signalisieren, dass sie aktiv sind. Für korrekte Redundanz sollten Sie nach Möglichkeit mindestens zwei Heartbeat-Medien angeben.

Wählen Sie mindestens ein Heartbeat-Medium, falls möglich mehrere.

Wenn Sie "Broadcast" wählen, wählen Sie eines der verfügbaren Netzwerkgeräte in der Geräteliste aus.

Wählen Sie für Multicast ein Netzwerkgerät, die beizutretende Multicast-Gruppe (Klasse D Multicast-Adresse 224.0.0.0 - 239.255.255.255) und geben Sie den ttl-Wert (1-255) an.

"UDP Port" legt den UDP-Port fest, der für die Broadcast-Medien verwendet wird. Belassen Sie dessen Einstellung auf dem Standardwert (694), außer Sie betreiben mehrere Heartbeat-Cluster auf demselben Netzwerksegment. In diesem Fall müssen Sie jedes Cluster auf einer unterschiedlichen Portnummer ausführen.

- 5** Klicken Sie nach der Angabe eines Heartbeat-Mediums auf "Add", um Heartbeat diesen Medientyp hinzuzufügen.
- 6** Geben Sie im Fenster "STONITH Configuration" den Namen des Knotens in das Feld *Host from* ein bzw. wählen Sie den Knoten aus, wählen Sie den STONITH-Typ, geben Sie die erforderlichen Parameter an und klicken Sie auf "Add". Wiederholen Sie diesen Vorgang für jeden gewünschten Knoten.

STONITH muss konfiguriert werden, um freigegebene Daten zu schützen. Heartbeat kann eine Reihe von seriellen und Netzwerkstromschaltern steuern und verhindern, dass ein potenziell fehlerhafter Knoten freigegebene Daten beschädigt, indem es die Stromzufuhr zu diesem Knoten unterbricht.

Die im Feld "Host from" angegebenen Knotennamen sind die Knoten, die auf den Stromschalter des Netzwerks zugreifen können. Für einen seriellen Stromschalter ist dies ein bestimmter Knotenname. Für einen Netzwerknetzschalter sollten Sie in der Regel ein Sternchen * eingeben, um zu kennzeichnen, dass er von allen Knoten aus zugänglich ist.

Der STONITH-Typ ist der Name des Moduls, mit dem der Stromschalter gesteuert wird. Parameter sind spezifisch für das angegebene Modul. Siehe das Kommandozeilen-Werkzeug `stonith -h`, um eine Liste der unterstützten Module und der jeweils akzeptierten Parameter zu erhalten.

- 7** Wählen Sie im Fenster "Start-up Configuration", ob die Heartbeat-Software auf diesem Cluster-Server bei jedem Booten starten soll.

Wenn Sie *Off* wählen, müssen Sie Heartbeat bei jedem Booten des Cluster-Servers manuell starten. Sie können den Heartbeat-Server manuell mit dem Befehl `/etc/init.d/heartbeat start` starten.

Um den Heartbeat-Server sofort zu starten, wählen Sie *Start Heartbeat Server Now*.

Um Heartbeat auf den anderen Servern zu starten, wenn diese gebootet werden, geben Sie `chkconfig heartbeat on` an der Serverkonsole jedes entsprechenden Servers ein. Sie können auch `chkconfig heartbeat off` an der Serverkonsole eingeben, damit Heartbeat beim Neubooten des Servers nicht automatisch startet.

13.5 Zusätzliche Informationen

Zusätzliche Informationen über hohe Verfügbarkeit auf Linux und Heartbeat sowie das Konfigurieren von Cluster-Ressourcen und Verwalten und Anpassen von Heartbeat-Clustern finden Sie in The High-Availability Linux Project [<http://www.linux-ha.org>] (Das Linux-Projekt für hohe Verfügbarkeit).

Oracle Cluster File System 2

- [Abschnitt 14.1, „Überblick über OCFS2“](#) (S. 311)
- [Abschnitt 14.2, „Erstellen eines OCFS2-Volumes“](#) (S. 318)
- [Abschnitt 14.3, „Einhängen eines OCFS2-Volumes“](#) (S. 324)
- [Abschnitt 14.4, „Zusätzliche Informationen“](#) (S. 325)

14.1 Überblick über OCFS2

Oracle Cluster File System 2 (OCFS2) ist ein allgemeines Journaling-Dateisystem, das vollständig in den Linux 2.6-Kernel und spätere Versionen integriert ist. OCFS2 ermöglicht das Speichern von binären Anwendungsdateien, Datendateien und Datenbanken auf Geräten in einem SAN. Alle Knoten in einem Cluster haben gleichzeitig Lese- und Schreibzugriff auf das Dateisystem. Ein verteilter Sperrenmanager sorgt dafür, dass es zu keinen Dateizugriffskonflikten kommt. OCFS2 unterstützt bis zu 32.000 Unterverzeichnisse und Millionen von Dateien in jedem Verzeichnis. Zur Verwaltung des Clusters läuft auf jedem Knoten der O2CB-Cluster-Dienst (ein Treiber).

14.1.1 Funktionen und Vorteile

OCFS2 wurde SUSE Linux Enterprise Server 9 im August 2005 hinzugefügt, um Oracle Real Application Cluster (RAC)-Datenbanken und Oracle Home (die Anwendungs-

dateien von Oracle) zu unterstützen. Ab SUSE Linux Enterprise Server 10 kann OCFS2 für jede der folgenden Speicherlösungen verwendet werden:

- Oracle RAC und andere Datenbanken
- Allgemeine Anwendungen und Auslastungen
- XEN-Image-Speicher in einem Cluster

Virtuelle XEN-Computer und virtuelle Server können auf OCFS2-Volumes gespeichert werden, die von Cluster-Servern eingehängt werden, um eine schnelle und einfache Portabilität der virtuellen XEN-Computer zwischen den Servern zu gewährleisten.

- LAMP-Stacks (Linux, Apache, MySQL und PHP | Pearl | Python)

OCFS2 ist zudem vollständig in Heartbeat 2 integriert.

Als leistungsstarkes, symmetrisches, paralleles Cluster-Dateisystem unterstützt OCFS2 die folgenden Funktionen:

- Die Dateien einer Anwendung stehen allen Knoten des Clusters zur Verfügung. Die Anwendung wird nur einmal auf einem OCFS2-Volume im Cluster installiert.
- Alle Knoten haben gleichzeitig über die Standard-Dateisystemschnittstelle Lese- und Schreibzugriff auf den Speicher; dies vereinfacht die Verwaltung der clusterweit ausgeführten Anwendungen.
- Der Dateizugriff wird vom Distributed Lock Manager (DLM) koordiniert.

Die Steuerung über den DLM ist in den meisten Fällen zweckmäßig; das Anwendungsdesign kann jedoch die Skalierbarkeit beeinträchtigen, wenn die Anwendung mit dem DLM um die Koordination des Dateizugriffs konkurriert.

- Speichersicherungsfunktionen stehen auf allen Backend-Speichern zur Verfügung. Problemlos lässt sich ein Image der freigegebenen Anwendungsdateien erstellen, das bei einem Notfall eine schnelle Wiederherstellung ermöglicht.

OCFS2 bietet darüber hinaus folgende Funktionen:

- Metadaten-Caching

- Metadaten-Journaling
- Knotenübergreifende Dateidatenkonsistenz
- Eine GTK GUI-basierte Verwaltung über das Dienstprogramm `ocfs2console`
- Betrieb als freigegebenes Stammdateisystem
- Unterstützung für verschiedene Blockgrößen (jedes Volume kann eine andere Blockgröße haben) bis zu 4 KB bei einer maximalen Volume-Größe von 16 TB
- Unterstützung für bis zu 255 Cluster-Knoten
- Unterstützung für kontextabhängige symbolische Links (CDSL) bei knotenspezifischen lokalen Dateien
- Asynchrone und direkte E/A-Unterstützung für Datenbankdateien zur Verbesserung der Datenbankanleistung

14.1.2 O2CB-Cluster-Dienst

Der O2CB-Cluster-Dienst umfasst verschiedene Module sowie arbeitsspeicherinterne Dateisysteme, die zur Verwaltung der OCFS2-Dienste und -Volumes erforderlich sind. Sie können festlegen, dass diese Module beim Systemstart geladen und eingehängt werden. Anleitungen hierzu erhalten Sie in [Abschnitt 14.2.2, „Konfigurieren der OCFS2-Dienste“](#) (S. 319).

Tabelle 14.1 *O2CB-Cluster-Dienststapel*

Dienst	Beschreibung
Node Manager (NM)	Zeichnet alle Knoten in der Datei <code>/etc/ocfs2/cluster.conf</code> auf.
Heartbeat (HB)	Gibt Benachrichtigungen nach oben oder unten aus, wenn Knoten zum Cluster hinzukommen oder den Cluster verlassen.

Dienst	Beschreibung
TCP	Ermöglicht die Kommunikation zwischen den Knoten über das TCP-Protokoll.
Distributed Lock Manager (DLM)	Zeichnet sämtliche Sperren sowie deren Eigentümer und Status auf.
CONFIGFS	Dateisystem für die Konfiguration des Benutzerspeicherplatzes. Weitere Informationen finden Sie in Abschnitt 14.1.4, „Arbeitsspeicherinterne Dateisysteme“ (S. 315).
DLMFS	Schnittstelle zwischen Benutzerspeicherplatz und DLM des Kernel-Speicherplatzes. Weitere Informationen finden Sie in Abschnitt 14.1.4, „Arbeitsspeicherinterne Dateisysteme“ (S. 315).

14.1.3 Disk Heartbeat

Für OCFS2 müssen die Knoten im Netzwerk "alive" (betriebsbereit und online) sein. Um sicherzustellen, dass dies auch der Fall ist, sendet der O2CB-Cluster-Dienst in regelmäßigen Abständen so genannte Keepalive-Pakete. Der Cluster-Dienst verwendet dazu statt des LAN eine private Verbindung zwischen den Knoten, um zu verhindern, dass eventuelle Netzwerkverzögerungen als verschwundener Knoten interpretiert werden, was einer Selbstabriegelung des Knotens gleichkommen würde.

Der OC2B-Cluster-Dienst kommuniziert den Knotenstatus über ein Disk Heartbeat. Die Heartbeat-Systemdatei befindet sich auf dem SAN, wo sie allen Knoten des Clusters zur Verfügung steht. Die Blockzuweisungen der Datei entsprechen der Reihenfolge nach den Steckplatz-Zuweisungen der einzelnen Knoten.

Jeder Knoten liest die Datei in Zwei-Sekunden-Intervallen und schreibt in den ihm zugewiesenen Block. Änderungen am Zeitstempel eines Knotens sind ein Hinweis darauf, dass der Knoten betriebsbereit ist. Als "tot" wird ein Knoten bezeichnet, wenn er über eine bestimmte Anzahl an Intervallen (dem Heartbeat-Schwellenwert) nicht mehr in die Heartbeat-Datei schreibt. Selbst wenn nur ein einziger Knoten "alive" ist,

muss der O2CB-Cluster-Dienst diese Überprüfung durchführen, da jederzeit ein anderer Knoten dynamisch hinzugefügt werden kann.

Den Disk Heartbeat-Schwellenwert können Sie in der Datei `/etc/sysconfig/o2cb` mit dem Parameter `O2CB_HEARTBEAT_THRESHOLD` ändern. Die Wartezeit berechnet sich wie folgt:

```
(O2CB_HEARTBEAT_THRESHOLD value - 1) * 2 = threshold in seconds
```

Wenn beispielsweise für `O2CB_HEARTBEAT_THRESHOLD` der Standardwert 7 eingestellt ist, beträgt die Wartezeit 12 Sekunden $((7 - 1) * 2 = 12)$.

14.1.4 Arbeitsspeicherinterne Dateisysteme

OCFS2 verwendet zur Kommunikation zwei arbeitsspeicherinterne Dateisysteme:

Tabelle 14.2 Von OCFS2 verwendete, arbeitsspeicherinterne Dateisysteme

Arbeitsspeicher-internes Dateisystem	Beschreibung	Einhängepunkt
<code>configs</code>	Kommuniziert die Liste der Cluster-Knoten an den Node Manager im Kernel und meldet die für das Heartbeat verwendete Ressource an den Heartbeat-Thread im Kernel.	<code>/config</code>
<code>ocfs2_dlmfs</code>	Kommuniziert die Aktivierung und Deaktivierung clusterweiter Ressourcensperren an den Distributed Lock Manager im Kernel, der sämtliche Sperren sowie deren Eigentümer und den jeweiligen Status überwacht.	<code>/dlm</code>

14.1.5 Verwaltungsprogramme und -befehle

OCFS2 speichert spezifische Parameterdateien für die Cluster-Knoten. Die Cluster-Konfigurationsdatei (`/etc/ocfs2/cluster.conf`) befindet sich auf jedem dem Cluster zugewiesenen Knoten.

Das Dienstprogramm `ocfs2console` ist eine GTK GUI-basierte Schnittstelle für die Konfigurationsverwaltung der OCFS2-Dienste im Cluster. Mit diesem Programm können Sie die Datei `/etc/ocfs2/cluster.conf` einrichten und auf allen Mitgliedsknoten des Clusters speichern. Darüber hinaus können Sie mit diesem Programm OCFS2-Volumes formatieren und einstellen sowie ein- und aushängen.

Weitere OCFS2-Dienstprogramme werden in der folgenden Tabelle beschrieben. Eine Beschreibung der Syntax dieser Befehle finden Sie auf den jeweiligen Manualpages.

Tabelle 14.3 *OCFS2-Dienstprogramme*

OCFS2-Dienstprogramm	Beschreibung
<code>debugfs.ocfs2</code>	Untersucht den Status des OCFS2-Dateisystems (zum Debuggen).
<code>fsck.ocfs2</code>	Untersucht das Dateisystem auf Fehler und kann diese optional auch korrigieren.
<code>mkfs.ocfs2</code>	Erstellt ein OCFS2-Dateisystem auf einem Gerät (normalerweise auf einer Partition einer freigegebenen physikalischen oder logischen Festplatte). Zur Ausführung dieses Dienstprogramms muss der O2CB-Cluster-Dienst laufen.
<code>mounted.ocfs2</code>	Ermittelt alle OCFS2-Volumes eines Cluster-Systems und zeigt diese an. Listet alle OCFS2-Geräte bzw. alle Knoten des Systems auf, auf denen ein OCFS2-Gerät eingehängt ist.
<code>ocfs2cdsl</code>	Erstellt für einen Knoten einen kontextabhängigen symbolischen Link (CDSL) für den angegebenen Dateinamen (Datei oder Verzeichnis). Ein CDSL-Dateiname verfügt für einen bestimmten Knoten über ein eigenes Image, in OCFS2 jedoch über einen Common Name (allgemeinen Namen).
<code>tune.ocfs2</code>	Stellt die OCFS2-Dateisystemparameter ein, unter anderem das Volume-Label, die Anzahl der Knotensteckplätze, die Journal-Größe aller Knotensteckplätze und die Volume-Größe.

Zur Verwaltung der O2CB-Dienste verwenden Sie die folgenden Befehle. Eine Beschreibung der Befehlssyntax von `o2cb` finden Sie auf der Manualpage dieses Befehls.

Tabelle 14.4 *O2CB-Befehle*

Befehl	Beschreibung
<code>/etc/init.d/o2cb status</code>	Meldet, ob die o2cb-Dienste geladen und eingehängt sind.
<code>/etc/init.d/o2cb load</code>	Lädt die O2CB-Module und arbeitsspeicherinternen Dateisysteme.
<code>/etc/init.d/o2cb online</code> <code>ocfs2</code>	Stellt den Cluster mit der Bezeichnung "ocfs2" online. Dazu muss mindestens ein Knoten des Clusters aktiv sein.
<code>/etc/init.d/o2cb offline</code> <code>ocfs2</code>	Schaltet den Cluster mit der Bezeichnung "ocfs2" offline.
<code>/etc/init.d/o2cb unload</code>	Entlädt die O2CB-Module und arbeitsspeicherinternen Dateisysteme.
<code>/etc/init.d/o2cb start</code> <code>ocfs2</code>	Wenn der Cluster mit der Bezeichnung "ocfs2" so eingerichtet ist, dass es beim Systemstart geladen wird, wird es durch diesen Befehl gestartet, indem <code>o2cb</code> geladen und der Cluster online gestellt wird. Dazu muss mindestens ein Knoten des Clusters aktiv sein.
<code>/etc/init.d/o2cb stop</code> <code>ocfs2</code>	Wenn der Cluster mit der Bezeichnung "ocfs2" so eingerichtet ist, dass es beim Systemstart geladen wird, wird es durch diesen Befehl beendet, indem der Cluster offline geschaltet wird und die O2CB-Module und arbeitsspeicherinternen Dateisysteme entladen werden.

14.1.6 OCFS2-Pakete

Ab SUSE Linux Enterprise Server 10 wird das OCFS2-Kernelmodul (`ocfs2`) automatisch installiert. Allerdings müssen Sie, wenn Sie OCFS2 verwenden möchten, noch die Pakete `ocfs2-tools` und `ocfs2console` auf den einzelnen Cluster-Knoten installieren. Dazu können Sie YaST oder die Kommandozeile verwenden.

- 1 Melden Sie sich als `root`-Benutzer (bzw. als Benutzer mit gleichwertigen Berechtigungen) an und öffnen Sie das YaST-Kontrollzentrum.
- 2 Wählen Sie *Software* → *Software installieren oder löschen*.
- 3 Geben Sie unter *Suche* Folgendes ein:

```
ocfs2
```

Auf der rechten Seite sollten nun die Softwarepakete `ocfs2-tools` und `ocfs2console` angezeigt werden. Sind sie bereits markiert, so sind sie schon installiert.

- 4 Wenn die Pakete noch installiert werden müssen, markieren Sie sie, klicken Sie auf *Installieren* und befolgen Sie die Anweisungen auf dem Bildschirm.

14.2 Erstellen eines OCFS2-Volumes

Dieser Abschnitt zeigt Ihnen, wie Sie Ihr System für OCFS2 konfigurieren und OCFS2-Volumes erstellen.

14.2.1 Voraussetzungen

Führen Sie vor der Konfiguration die folgenden Schritte aus:

- Initialisieren bzw. konfigurieren Sie nach Bedarf RAIDs auf den SAN-Festplatten, um die Geräte vorzubereiten, die Sie für Ihre OCFS2-Volumes verwenden möchten. Belassen Sie die Geräte als freien Speicher.

Generell empfiehlt es sich, Anwendungs- und Datendateien auf verschiedenen OCFS2-Volumes zu speichern. Zwingend erforderlich ist dies allerdings nur, wenn

für die Anwendungs- und Daten-Volumes unterschiedliche Einhängeanforderungen gelten. Für das Oracle RAC-Datenbank-Volume sind beispielsweise die Einhängeoptionen `datavolume` und `nointr` erforderlich, für das Oracle Home-Volume dürfen diese hingegen auf gar keinen Fall verwendet werden.

- Vergewissern Sie sich, dass die Pakete `ocfs2console` und `ocfs2-tools` installiert sind. Diese Pakete können Sie bei Bedarf mit YaST oder über die Kommandozeile installieren. Anleitungen zur Installation mit YaST erhalten Sie in [Abschnitt 14.1.6, „OCFS2-Pakete“](#) (S. 318).

14.2.2 Konfigurieren der OCFS2-Dienste

Vor der Erstellung von OCFS2-Volumes müssen Sie die OCFS2-Dienste konfigurieren. Im folgenden Verfahren erstellen Sie die Datei `/etc/ocfs2/cluster.conf` und speichern diese Datei auf allen Knoten. Danach erstellen und starten Sie den O2CB-Cluster-Dienst (`o2cb`).

Die Anleitung in diesem Abschnitt ist für jeden Cluster-Knoten gesondert durchzuführen.

- 1 Öffnen Sie ein Terminalfenster und melden Sie sich als `root`-Benutzer (bzw. als Benutzer mit gleichwertigen Berechtigungen) an.
- 2 Wenn der `o2cb`-Cluster-Dienst noch nicht aktiviert ist, geben Sie Folgendes ein:

```
chkconfig --add o2cb
```

Beim Hinzufügen eines neuen Diensts stellt der Befehl `chkconfig` sicher, dass der Dienst in jeder Ausführungsebene entweder über einen "start"- oder einen "kill"-Eintrag verfügt.

- 3 Wenn der `ocfs2`-Dienst noch nicht aktiviert ist, geben Sie Folgendes ein:

```
chkconfig --add ocfs2
```

- 4 Konfigurieren Sie den `o2cb`-Cluster-Diensttreiber so, dass er beim Systemstart geladen wird.

- a Geben Sie Folgendes ein:

```
/etc/init.d/o2cb configure
```

- b** Geben Sie an der Eingabeaufforderung `Load O2CB driver on boot` (`y/n`) [`n`] (`O2CB-Treiber beim Systemstart laden (j/n) [n]`) Folgendes ein:

`y`

(yes) to enable load on boot. ((Ja), damit der Treiber beim Systemstart geladen wird.)

- c** Geben Sie an der Eingabeaufforderung `Cluster to start on boot` (Enter "`none`" to clear) [`ocfs2`] (Beim Systemstart zu startendes Cluster (zum Löschen "Keines" eingeben) [`ocfs2`]) Folgendes ein:

`none`

Nehmen Sie diesen Eintrag nur vor, wenn Sie OCFS2 zum ersten Mal einrichten bzw. den Dienst zurücksetzen wollen. Im nächsten Schritt bei der Einrichtung der Datei `/etc/ocfs2/cluster.conf` geben Sie den Cluster-Namen an.

- 5** Mit dem Dienstprogramm `ocfs2console` können Sie die Datei `/etc/ocfs2/cluster.conf` einrichten und auf allen Mitgliedsknoten des Clusters speichern.

Diese Datei sollte auf allen Knoten im Cluster identisch sein. Führen Sie die folgenden Schritte aus, um den ersten Knoten einzurichten. Danach können Sie dem Cluster mit `ocfs2console` dynamisch weitere Knoten hinzufügen und die Datei `cluster.conf` auf alle Knoten übertragen.

Wenn Sie jedoch andere Einstellungen ändern, beispielsweise den Cluster-Namen oder die IP-Adresse, müssen Sie den Cluster neu starten, damit die Änderungen wirksam werden (siehe [Schritt 6](#) (S. 321)).

- a** Öffnen Sie die Bedienoberfläche von `ocfs2console` durch folgende Eingabe:

`ocfs2console`

- b** Wählen Sie in `ocfs2console` die Option `Cluster` → `Cluster-Knoten` aus.

Wenn noch keine `cluster.conf` vorhanden ist, wird die Datei nun mit dem Standard-Cluster-Namen `ocfs2` erstellt. Den Cluster-Namen können Sie nach Belieben ändern.

- c Klicken Sie im Dialogfeld "Knotenkonfiguration" auf *Hinzufügen*, um das Dialogfeld "Knoten hinzufügen" zu öffnen.
- d Geben Sie im Dialogfeld "Knoten hinzufügen" einen einmaligen Namen für den Primärknoten, eine eindeutige IP-Adresse (z. B. `192.168.1.1`) und die Portnummer (optional, Standard ist 7777) ein und klicken Sie anschließend auf *OK*.

`ocfs2console` weist den Knoten nun der Reihe nach Steckplätze von 0 bis 254 zu.

- e Klicken Sie im Dialogfeld "Knotenkonfiguration" auf *Anwenden* und danach auf *Schließen*, um das Dialogfeld zu schließen.
- f Klicken Sie auf *Cluster* → *Propagate Configuration* (Konfiguration übertragen), um die Datei `cluster.conf` auf alle Knoten zu übertragen.

- 6** Wenn Sie das OCFS2-Cluster neu starten müssen, damit Änderungen wirksam werden, geben Sie die folgenden Zeilen ein. Warten Sie nach jeder Zeile kurz auf das *OK* des Prozesses.

```
/etc/init.d/o2cb stop  
/etc/init.d/o2cb start
```

14.2.3 Erstellen eines OCFS2-Volumes

Zum Erstellen eines OCFS2-Dateisystems und zum Hinzufügen neuer Cluster-Knoten sollten Sie nur einen der Knoten im Cluster verwenden.

- 1** Öffnen Sie ein Terminalfenster und melden Sie sich als `root`-Benutzer (bzw. als Benutzer mit gleichwertigen Berechtigungen) an.
- 2** Wenn der O2CB-Cluster-Dienst offline ist, starten Sie ihn durch Eingabe des folgenden Befehls und warten Sie auf das *OK* des Prozesses.

```
/etc/init.d/o2cb online ocfs2
```

Ersetzen Sie `ocfs2` durch den Cluster-Namen Ihres OCFS2-Clusters.

Das OCFS2-Cluster muss online sein, da vor der Formatierung sichergestellt werden muss, dass das Volume noch nicht auf einem Knoten des Clusters eingehängt ist.

3 Erstellen und formatieren Sie das Volume mit einer der folgenden Methoden:

- Gehen Sie in EVMSGUI zur Seite "Volumes", wählen Sie *Dateisystem erstellen* → *OCFS2* aus und legen Sie die Konfiguration fest.
- Verwenden Sie das Dienstprogramm `mkfs.ocfs2`. Eine Beschreibung der Syntax dieses Befehls finden Sie auf der zugehörigen Manualpage.
- Klicken Sie in `ocfs2console` auf *Tasks* → *Formatieren*, wählen Sie in der Liste der verfügbaren Geräte das Gerät aus, auf dem Sie das OCFS2-Volume erstellen möchten, legen Sie die Konfiguration des Volumes fest und klicken Sie auf *OK*, um das Volume zu formatieren.

Die empfohlenen Einstellungen entnehmen Sie bitte der folgenden Tabelle.

OCFS2-Parameter	Beschreibung und Empfehlung
Volume-Label	Eine beschreibende Bezeichnung für das Volume, die das Volume eindeutig identifiziert, selbst wenn es auf unterschiedlichen Knoten eingehängt ist. Mit dem Dienstprogramm <code>tunefs.ocfs2</code> können Sie das Label jederzeit ändern.
Cluster-Größe	Die kleinste Speicherplatzeinheit, die einer Datei für die Aufnahme von Daten zugewiesen ist. Zur Auswahl stehen 4, 8, 16, 32, 64, 128, 256, 512 und 1024 KB. Die Cluster-Größe kann nach der Formatierung des Volumes nicht mehr geändert werden.

**OCFS2-
Parameter****Beschreibung und Empfehlung**

	<p>Für Datenbank-Volumes empfiehlt Oracle eine Cluster-Größe von mindestens 128 KB. Für Oracle Home empfiehlt Oracle eine Cluster-Größe von 32 oder 64 KB.</p>
Anzahl der Knotensteckplätze	<p>Die maximale Anzahl an Knoten, auf denen ein Volume gleichzeitig eingehängt sein kann. Beim Einhängen erstellt OCFS2 für jeden Knoten separate Systemdateien (z. B. die Journals). Bei den Knoten, die auf das Volume zugreifen, kann es sich um eine Kombination aus Little-Endian-Architekturen (wie x86, x86-64 und ia64) und Big-Endian-Architekturen (wie ppc64 und s390x) handeln.</p> <p>Knotenspezifische Dateien werden als lokale Dateien bezeichnet. Jede lokale Datei zeichnet sich durch die angehängte Knoten-Steckplatznummer aus. Beispiel: <code>journal:0000</code> gehört zu dem Knoten, der Steckplatznummer 0 zugewiesen ist.</p> <p>Stellen Sie die maximale Anzahl der Knotensteckplätze bei der Erstellung eines Volumes auf die Anzahl an Knoten ein, auf denen das Volume voraussichtlich gleichzeitig eingehängt wird. Mit dem Dienstprogramm <code>tunefs.ocfs2</code> können Sie die Anzahl der Knotensteckplätze nachträglich erhöhen, jedoch nicht herabsetzen.</p>
Blockgröße	<p>Die kleinste adressierbare Speicherplatzeinheit im Dateisystem. Die Blockgröße wird bei der Erstellung des Volumes festgelegt.</p> <p>Zur Auswahl stehen 512 Byte (nicht empfehlenswert), 1 KB, 2 KB oder 4 KB (für die meisten Volumes empfehlenswert). Die Blockgröße kann nach der Formatierung des Volumes nicht mehr geändert werden.</p>

14.3 Einhängen eines OCFS2-Volumes

- 1 Öffnen Sie ein Terminalfenster und melden Sie sich als `root`-Benutzer (bzw. als Benutzer mit gleichwertigen Berechtigungen) an.
- 2 Wenn der O2CB-Cluster-Dienst offline ist, starten Sie ihn durch Eingabe des folgenden Befehls und warten Sie auf das *OK* des Prozesses.

```
/etc/init.d/o2cb online ocfs2
```

Ersetzen Sie `ocfs2` durch den Cluster-Namen Ihres OCFS2-Clusters.

Das OCFS2-Cluster muss online sein, da vor der Formatierung sichergestellt werden muss, dass das Volume noch nicht auf einem Knoten des Clusters eingehängt ist.

- 3 Hängen Sie das Volume mit einer der folgenden Methoden ein:
 - Wählen Sie in `ocfs2console` aus der Liste der verfügbaren Geräte ein Gerät aus, klicken Sie auf *Einhängen*, geben Sie den Einhängpunkt des Verzeichnisses sowie optional die Einhängparameter an und klicken Sie auf *OK*.
 - Hängen Sie das Volume mit dem Befehl `mount` über die Kommandozeile ein.
 - Hängen Sie das Volume beim Systemstart über die Datei `/etc/fstab` ein.

Das Einhängen eines OCFS2-Volumes dauert je nachdem, wie lange der Heartbeat-Thread zur Stabilisierung benötigt, etwa 5 Sekunden. Wenn das Volume erfolgreich eingehängt wurde, zeigt die Geräteliste in `ocfs2console` den Einhängpunkt mit dem Gerät an.

Weitere Informationen zum Einhängen eines OCFS2-Volumes mit diesen Methoden finden Sie im *OCFS2-Benutzerhandbuch* [<http://oss.oracle.com/projects/ocfs2/documentation/>] zum OCFS2-Projekt von Oracle [<http://oss.oracle.com/projects/ocfs2/>].

Verwenden Sie unter Oracle RAC für OCFS2-Volumen, die die Voting Diskfile (CRS), die Cluster-Registrierung (OCR) sowie Datendateien, Redo-Protokolle, Archivprotokolle und Steuerdateien enthalten, unbedingt die Einhängoptionen

`datavolume` und `nointr`. Beim Einhängen des Oracle Home-Volumens sollten Sie diese Optionen hingegen nicht auswählen.

Option	Beschreibung
<code>datavolume</code>	Stellt sicher, dass die Oracle-Prozesse Dateien mit der <code>o_direct</code> -Flag öffnen.
<code>nointr</code>	Ohne Unterbrechungen. Stellt sicher, dass die Ein-/Ausgabe nicht durch Signale unterbrochen wird.

14.4 Zusätzliche Informationen

Weitere Informationen zur Verwendung von OCFS2 finden Sie im *OCFS2-Benutzerhandbuch* [<http://oss.oracle.com/projects/ocfs2/documentation/>] zum OCFS2-Projekt von Oracle [<http://oss.oracle.com/projects/ocfs2/>].

Zugriffssteuerungslisten unter Linux

15

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.

15.1 Traditionelle Dateiberechtigungen

Die Grundlagen der traditionellen Linux-Dateiberechtigungen werden in [Abschnitt 18.2](#), „Benutzer und Zugriffsberechtigungen“ (S. 389) erläutert. Erweiterte Funktionen sind das `setuid`-, das `setgid`- und das `sticky`-Bit.

15.1.1 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 sind beispielsweise im Regelfall `root`-Berechtigungen für den Zugriff auf `/etc/passwd` erforderlich. Diese Datei enthält wichtige Informationen, beispielsweise die Home-Verzeichnisse von Benutzern sowie Benutzer- und Gruppen-IDs. Folglich ist es einem normalen Benutzer im Regelfall nicht möglich, `passwd` zu ändern, da es zu gefährlich wäre, allen Benutzern den direkten Zugriff auf diese Datei zu gewähren. Eine mögliche Lösung dieses Problems stellt der *setuid*-Mechanismus dar. `setuid` (set user ID (Benutzer-ID festlegen)) ist ein spezielles Dateiattribut, das das System zum Ausführen entsprechend markierter Programme unter einer bestimmten Benutzer-ID veranlasst. Betrachten wir einmal den `passwd`-Befehl:

```
-rwsr-xr-x 1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

Sie sehen das `s`, das angibt, dass das `setuid`-Bit für die Benutzerberechtigung festgelegt ist. Durch das `setuid`-Bit führen alle Benutzer, die den `passwd`-Befehl aufrufen, den entsprechenden Vorgang als `root` aus.

15.1.2 setgid-Bit

Das `setuid`-Bit hat für Benutzer Gültigkeit. Es gibt jedoch eine entsprechende Eigenschaft für Gruppen: das *setgid*-Bit. Ein Programm, für das dieses Bit festgelegt wurde, wird unter der Gruppen-ID ausgeführt, unter der es gespeichert wurde, unabhängig davon, von welchem Benutzer es gestartet wird. Folglich werden in einem Verzeichnis mit dem `setgid`-Bit alle neu erstellten Dateien und Unterverzeichnisse der Gruppe zugewiesen, der das Verzeichnis zugehörig ist. Betrachten wir einmal folgendes Beispielverzeichnis:

```
drwxrws--- 2 tux archive 48 Nov 19 17:12 backup
```

Sie sehen das `s`, das angibt, dass das `setgid`-Bit für die Gruppenberechtigung festgelegt ist. Der Eigentümer des Verzeichnisses sowie Mitglieder der Gruppe `archive` dürfen auf dieses Verzeichnis zugreifen. Benutzer, die nicht Mitglied dieser Gruppe sind, werden der entsprechenden Gruppe „zugeordnet“. `archive` ist die Gruppen-ID für alle geschriebenen Dateien. Ein mit der Gruppen-ID `archive` ausgeführtes Sicherungsprogramm kann auch ohne `root`-Berechtigungen auf dieses Verzeichnis zugreifen.

15.1.3 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
```

15.2 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.

15.3 Definitionen

Benutzerklasse

Das traditionelle POSIX-Berechtigungskonzept verwendet drei *Klassen* von Benutzern für das Zuweisen von Berechtigungen im Dateisystem: den Eigentümer (*owner*), die Eigentümergruppe (*owning group*) und andere Benutzer (*other*). Pro Benutzerklasse können jeweils die drei Berechtigungsbits zum Lesen (*r*), Schreiben (*w*) und Ausführen (*x*) gesetzt werden.

Zugriffs-ACL

Die Zugriffsberechtigungen für Benutzer 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.

15.4 Arbeiten mit ACLs

[Tabelle 15.1, „Typen von ACL-Einträgen“](#) (S. 331) fasst die sechs möglichen Typen von ACL-Einträgen zusammen und beschreibt die für einen Benutzer oder eine Gruppe von Benutzern verfügbaren Berechtigungen. Der Eintrag *owner* definiert die Berechtigungen des Benutzers, der Eigentümer der Datei oder des Verzeichnisses ist. Der Eintrag *owning group* definiert die Berechtigungen der Gruppe, die Eigentümer der Datei ist. Der Superuser kann den Eigentümer (*owner*) oder die Eigentümergruppe

(owning group) mit `chown` oder `chgrp` ändern, in welchem Fall die Einträge "owner" und "owning group" sich auf den neuen Eigentümer bzw. die neue Eigentümergruppe beziehen. Die Einträge des Typs *named user* definieren die Berechtigungen des Benutzers, der im Bezeichnerfeld des Eintrags angegeben ist. Die Einträge des Typs *named group* definieren die Berechtigungen der im Bezeichnerfeld des Eintrags angegebenen Gruppe. Nur die Einträge des Typs "named user" und "named group" verfügen über ein Bezeichnerfeld, das nicht leer ist. Der Eintrag *other* definiert die Berechtigungen aller anderen Benutzer.

Der Eintrag *mask* schränkt die durch die Einträge "named user", "named group" und "owning group" gewährten Berechtigungen ein, indem durch ihn festgelegt werden kann, welche der Berechtigungen in diesen Einträgen wirksam und welche maskiert sind. Sind Berechtigungen sowohl in einem der oben genannten Einträge als auch in der Maske vorhanden, werden sie wirksam. Berechtigungen, die nur in der Maske oder nur im eigentlichen Eintrag vorhanden sind, sind nicht wirksam, d. h. die Berechtigungen werden nicht gewährt. Die in den Einträgen "owner" und "owning group" gewährten Berechtigungen sind immer wirksam. Dieser Mechanismus wird mit dem Beispiel in [Tabelle 15.2, „Maskierung von Zugriffsberechtigungen“](#) (S. 332) 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 traditionellen 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 15.1 Typen von ACL-Einträgen

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

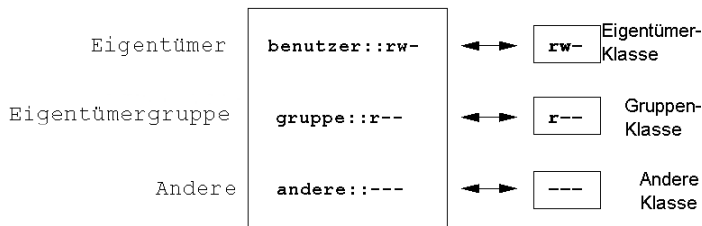
Tabelle 15.2 Maskierung von Zugriffsberechtigungen

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

15.4.1 ACL-Einträge und Dateimodus-Berechtigungsbits

Abbildung 15.1, „Minimale ACL: ACL-Einträge vs. Berechtigungsbits“ (S. 332) und Abbildung 15.2, „Erweiterte ACL: ACL-Einträge vs. Berechtigungsbits“ (S. 333) zeigen eine minimale und eine erweiterte ACL. Die Abbildungen sind in drei Blöcke gegliedert - der linke Block zeigt die Typspezifikationen der ACL-Einträge, der mittlere Block zeigt ein Beispiel einer ACL und der rechte Block zeigt die entsprechenden Berechtigungsbits gemäß dem herkömmlichen Berechtigungskonzept, wie sie beispielsweise auch `ls -l` anzeigt. 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.

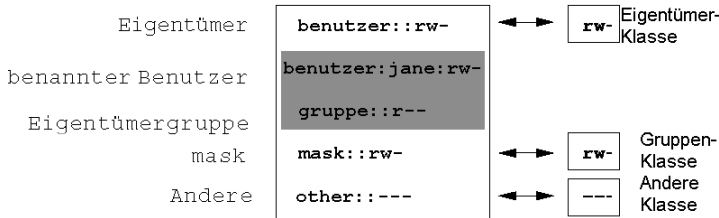
Abbildung 15.1 Minimale ACL: ACL-Einträge vs. Berechtigungsbits



Im Fall einer minimalen ACL – ohne "mask" – werden die "group class"-Berechtigungen dem ACL-Eintrag "owning group" zugeordnet. Dies ist in [Abbildung 15.1, „Minimale ACL: ACL-Einträge vs. Berechtigungsbits“](#) (S. 332) dargestellt. Im Fall einer erweiterten ACL – mit "mask" – werden die "group class"-Berechtigungen dem "mask"-Eintrag

zugeordnet. Dies ist in [Abbildung 15.2](#), „Erweiterte ACL: ACL-Einträge vs. Berechtigungsbits“ (S. 333) dargestellt.

Abbildung 15.2 *Erweiterte ACL: ACL-Einträge vs. 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.

15.4.2 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, wobei er dem Eigentümer sämtliche Berechtigungen (0) gewährt, der Gruppe den Schreibzugriff (2) verweigert und allen anderen Benutzern überhaupt keine Berechtigungen erteilt (7). Die entsprechenden Berechtigungsbits werden von `umask` maskiert oder deaktiviert. Weitere Informationen hierzu finden Sie auf der Manualpage `umask`.

`mkdir mydir` erstellt das Verzeichnis `mydir` mit den durch `umask` festgelegten Standardberechtigungen. Mit dem Befehl `ls -dl mydir` können Sie prüfen, ob alle Berechtigungen ordnungsgemäß zugewiesen wurden. Die Ausgabe für dieses Beispiel sieht wie folgt aus:

```
drwxr-x--- ... tux project3 ... mydir
```

Mit dem Befehl `getfacl mydir` prüfen Sie den anfänglichen Status der ACL. Es werden ähnliche Informationen wie im folgenden Beispiel zurückgegeben:

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

Die ersten drei Zeilen der Ausgabe nennen Namen, Eigentümer und Eigentümergruppe des Verzeichnisses. Die drei nächsten Zeilen enthalten die drei ACL-Einträge "owner", "owning group" und "other". Insgesamt liefert Ihnen der Befehl `getfacl` im Fall dieser minimalen ACL keine Informationen, die Sie mit `ls` nicht auch erhalten hätten.

Ändern Sie die ACL so, dass Sie dem zusätzlichen Benutzer `geeko` und der zusätzlichen Gruppe `mascots` Lese-, Schreib- und Ausführberechtigungen gewähren, indem Sie folgenden Befehl eingeben:

```
setfacl -m user:geeko:rwx,group:mascots:rwx mydir
```

Mit der Option `-m` kann per `setfacl` die vorhandene ACL geändert werden. Das nachfolgende Argument gibt an, welche ACL-Einträge geändert werden (mehrere Einträge werden durch Kommas voneinander getrennt). Im letzten Teil geben Sie den Namen des Verzeichnisses an, für das diese Änderungen gelten sollen. Mit dem Befehl `getfacl` können Sie sich die resultierende ACL ansehen.

```
# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other::---
```

Zusätzlich zu den von Ihnen erstellten Einträgen für den Benutzer `geeko` und die Gruppe `mascots` wurde ein "mask"-Eintrag generiert. Der mask-Eintrag wird automatisch gesetzt, sodass alle Berechtigungen wirksam sind. Außerdem passt `setfacl` vorhandene mask-Einträge automatisch an die geänderten Einstellungen an, es sei denn, Sie deaktivieren diese Funktion mit `-n`. "mask" legt die maximal wirksamen Zugriffsberechtigungen für alle Einträge innerhalb der "group class" fest. Dazu gehören "named user", "named group" und "owning group". Die Berechtigungsbits des Typs "group class", die mit `ls -dl mydir` ausgegeben werden, entsprechen jetzt dem mask-Eintrag.

```
drwxrwx---+ ... tux project3 ... mydir
```

Die erste Spalte der Ausgabe enthält ein zusätzliches +, um darauf hinzuweisen, dass für dieses Objekt eine *erweiterte* ACL vorhanden ist.

Gemäß der Ausgabe des Befehls `ls` beinhalten die Berechtigungen für den mask-Eintrag auch Schreibzugriff. Solche Berechtigungsbits würden normalerweise bedeuten, dass die "owning group" (hier `project3`) ebenfalls Schreibzugriff auf das Verzeichnis `mydir` hätte. Allerdings sind die wirklich wirksamen Zugriffsberechtigungen für die "owning group" als die Schnittmenge aus den für "owning group" und den für "mask" gesetzten Berechtigungen definiert, in unserem Beispiel also `r-x` (siehe [Tabelle 15.2](#), „Maskierung von Zugriffsberechtigungen“ (S. 332)). 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 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 mit dem Befehl `chmod` den Schreibzugriff über die "group class"-Bits deaktiviert haben, liefert Ihnen bereits die Ausgabe des Befehls `ls` den Hinweis darauf, dass die mask-Bits entsprechend angepasst wurden: Die Schreibberechtigung ist wieder 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.

15.4.3 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 dann Folgendes zurück:

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

Die Ausgabe von `getfacl mydir/myfile` lautet wie folgt:

```
# 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. 336)). 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.

15.4.4 Der ACL-Auswertungsalgorithmus

Bevor ein Prozess oder eine Anwendung Zugriff auf ein durch eine ACL geschütztes Dateisystemobjekt erhält, wird ein Auswertungsalgorithmus angewendet. Die ACL-Einträge werden grundsätzlich in der folgenden Reihenfolge untersucht: "owner", "named user", "owning group" oder "named group" und "other". 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. Für das Endresultat „Zugriff gewährt“ ist es natürlich unerheblich, welcher dieser Einträge den Ausschlag gegeben hat. 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.

15.5 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.

15.6 Weitere Informationen

Ausführliche Informationen zu ACLs finden Sie unter <http://acl.bestbits.at/>. Weitere Informationen finden Sie außerdem auf den Manualpages für `getfacl(1)`, `acl(5)` und `setfacl(1)`.

RPM - der Paket-Manager

In SUSE® Linux wird RPM (RPM Package Manager) 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: Softwarepakete installieren, de-installieren oder aktualisieren, die RPM-Datenbank neu aufbauen, Anfragen an die RPM-Datenbank bzw. an einzelne RPM-Archive richten, Pakete auf Integrität überprüfen und Pakete signieren. `rpmbuild` dient dazu, installierbare Pakete aus den unverfälschten Quellen herzustellen.

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`.

16.1 Prüfen der Authentizität eines Pakets

RPM-Pakete von SUSE Linux Enterprise 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 so feststellen, ob es wirklich von SUSE Linux oder einer anderen vertrauenswürdigen Stelle 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.

16.2 Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren

Im Normalfall ist das Installieren eines RPM-Archivs ganz simpel: `rpm -i paket.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 wacht die RPM-Datenbank darüber, dass keine Konflikte entstehen: Eine 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 aufgelösten 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 in einem Ausnahmefall ein solcher Löschvorgang nicht möglich ist, obwohl *keine* Abhängigkeiten mehr bestehen, kann es nützlich sein, die RPM-Datenbank mit der Option `--rebuilddb` neu aufzubauen.

16.3 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 -qpP1 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 Patches, die im System installiert sind, 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 Manualpages von `rpm` und `rpmbuild` zur Verfügung.

16.4 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`.

16.5 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. Siehe [Tabelle 16.1](#), „Die wichtigsten RPM-Abfrageoptionen“ (S. 346).

Tabelle 16.1 *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>--scripts</code>	Installationsskripts (preinstall, postinstall, uninstall)

Beispielsweise gibt der Befehl `rpm -q -i wget` die in [Beispiel 16.1](#), „rpm -q -i wget“ (S. 347) gezeigte Information aus.

Beispiel 16.1 `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 16.2](#), „Skript für die Suche nach Paketen“ (S. 348) gezeigt. Übergeben Sie den partiellen Dateinamen als Parameter beim Aufruf des Skripts.

Beispiel 16.2 *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. Leiten Sie die Überprüfungen mit `-V`, `-y` oder `--verify` ein. 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 16.2 *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 als erwartet ist, 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_RPMDDB_BACKUPS` (Standard: 5) in `/etc/sysconfig/backup` gesteuert. Die Größe einer einzelnen Sicherungskopie beträgt ungefähr 1 MB für 1 GB in `/usr`.

16.6 Installieren und Kompilieren von Quellpaketen

Alle Quellpakete von SUSE Linux Enterprise 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/rpmsrc`, 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 erforderlichen Komponenten in `/usr/src/packages` installiert: die Quellen und Anpassungen in `SOURCES` und die relevante `.spec`-Datei 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 wie 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.

16.7 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 unter `/var/tmp/build-root` eine minimale Umgebung in `/var/tmp/build-root` 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`.

16.8 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 Frontend für `rpm` an. Ein Paket-Manager mit allen Funktionen ist als YaST-Modul verfügbar (siehe [Abschnitt 7.3.1, „Installieren und Entfernen von Software“](#) (S. 152)).

Dienstprogramme zur Systemüberwachung

17

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.

17.1 Fehlersuche

17.1.1 Erforderliche Bibliothek angeben: `ldd`

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

```
tester@linux:~> 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.

```
tester@linux:~> ldd /bin/sash
not a dynamic executable
tester@linux:~> 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
```

17.1.2 Bibliotheksaufrufe eines aktiven Programms: `ltrace`

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

```
tester@linux:~> 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
  1.18     0.231189       27     8531  strcpy
  1.17     0.230765       27     8358  memcpy
[...]
```

0.00	0.000036	36	1 textdomain

100.00	19.662715		105717 total

17.1.3 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:

```
tester@linux:~> strace ls
execve("/bin/ls", ["ls"], [/* 61 vars */]) = 0
uname({sys="Linux", node="linux", ...}) = 0
brk(0) = 0x805c000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or \
directory)
open("/etc/ld.so.cache", O_RDONLY) = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=89696, ...}) = 0
mmap2(NULL, 89696, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb7ef2000
close(3) = 0
open("/lib/librt.so.1", O_RDONLY) = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\0\3\0\3\0\1\0\0\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:

```
tester@linux:~> 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`.

17.2 Dateien und Dateisysteme

17.2.1 Bestimmen Sie den Dateityp: `file`

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

```
tester@linux:~> 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:

```
tester@linux:~> file /usr/share/man/man1/file.1.gz
usr/share/man/man1/file.1.gz: gzip compressed data, from Unix, max compression
tester@linux:~> 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)
```

17.2.2 Dateisysteme und ihre Nutzung: `mount`, `df` und `du`

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

```
tester@linux:~> mount
/dev/hda3 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/hda1 on /boot type ext2 (rw,acl,user_xattr)
/dev/hda4 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.

```
tester@linux:~> df -h
Filesystem Size  Used Avail Use% Mounted on
/dev/hda3   11G  3.2G  6.9G  32% /
udev       252M  104K  252M   1% /dev
/dev/hda1   16M   6.6M   7.8M  46% /boot
/dev/hda4   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:

```
tester@linux:~> du -sh /local
1.7M    /local
```

17.2.3 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:

```
tester@linux:~> readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 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
```

17.2.4 Dateieigenschaften: stat

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

```
tester@linux:~> stat /etc/profile
Datei: `etc/profile'
  Size      : 7930 Blocks: 16          IO Block: 4096   regular file
Ger t: 303h/771d      Inode: 40657       Links: 1
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2006-01-06 16:45:43.000000000 +0100
Modify: 2005-11-21 14:54:35.000000000 +0100
Change: 2005-12-19 09:51:04.000000000 +0100
```

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

```
tester@linux:~> stat /etc/profile --filesystem
Datei: "/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
```

17.3 Hardware-Informationen

17.3.1 PCI-Ressourcen: lspci

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

```
linux:~ # 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.0 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:

```

linux:~ # 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.

17.3.2 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. Folgendes ist die Ausgabe von `lsusb` mit den folgenden angeschlossenen USB-Geräten: Hub, Speicherstick, Festplatte und Maus.

```

linux:/ # 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

```

17.3.3 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.

```
linux:/ # 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
```

Die Option `-d` gibt eine Defektliste aus, die zwei Tabellen mit fehlerhaften Blöcken einer Festplatte enthält: die erste stammt vom Hersteller (manufacturer table), die zweite ist die Liste der fehlerhaften Blöcke, die während des Betriebs aufgetreten sind (grown table). Wenn die Anzahl der Einträge in der während des Betriebs generierten Tabelle (grown table) zunimmt, empfiehlt es sich, die Festplatte zu ersetzen.

17.4 Netzwerke

17.4.1 Netzwerkstatus anzeigen: netstat

Mit `netstat` werden Netzwerkverbindungen, Routing-Tabellen (`-r`), Schnittstellen (`-i`), Masquerade-Verbindungen (`-M`), Multicast-Mitgliedschaften (`-g`) und Statistiken (`-s`) angezeigt.

```
tester@linux:~> netstat -r
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
192.168.22.0     *                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          192.168.22.254  0.0.0.0        UG      0 0        0 eth0
```

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

Beim Anzeigen von Netzwerkverbindungen oder Statistiken können Sie den gewünschten Socket-Typ angeben: TCP (`-t`), UDP (`-u`) oder roh (`-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.

```
linux:~ # netstat -t -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address State      PID/Pro
tcp    0      0 linux:33513    www.novell.com:www-http ESTABLISHED 6862/fi
tcp    0      352 linux:ssh      linux2.:trc-netpoll ESTABLISHED 19422/s
tcp    0      0 localhost:ssh  localhost:17828    ESTABLISHED -
```

Nachfolgend werden die Statistiken für das TCP-Protokoll angezeigt:

```
tester@linux:~> 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
```

17.5 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:

```
tester@linux:~> 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:

```
tester@linux:~> 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:

```
tester@linux:~> ls -l /proc/self
lrwxrwxrwx 1 root root 64 2006-01-09 13:03 /proc/self -> 5356
tester@linux:~> ls -l /proc/self/
total 0
dr-xr-xr-x 2 tester users 0 2006-01-09 17:04 attr
-r----- 1 tester users 0 2006-01-09 17:04 auxv
-r--r--r-- 1 tester users 0 2006-01-09 17:04 cmdline
lrwxrwxrwx 1 tester users 0 2006-01-09 17:04 cwd -> /home/tester
-r----- 1 tester users 0 2006-01-09 17:04 environ
lrwxrwxrwx 1 tester users 0 2006-01-09 17:04 exe -> /bin/ls
dr-x----- 2 tester users 0 2006-01-09 17:04 fd
-rw-r--r-- 1 tester users 0 2006-01-09 17:04 loginuid
-r--r--r-- 1 tester users 0 2006-01-09 17:04 maps
-rw----- 1 tester users 0 2006-01-09 17:04 mem
-r--r--r-- 1 tester users 0 2006-01-09 17:04 mounts
-rw-r--r-- 1 tester users 0 2006-01-09 17:04 oom_adj
-r--r--r-- 1 tester users 0 2006-01-09 17:04 oom_score
lrwxrwxrwx 1 tester users 0 2006-01-09 17:04 root -> /
-rw----- 1 tester users 0 2006-01-09 17:04 seccomp
-r--r--r-- 1 tester users 0 2006-01-09 17:04 smaps
-r--r--r-- 1 tester users 0 2006-01-09 17:04 stat
-r--r--r-- 1 tester users 0 2006-01-09 17:04 statm
-r--r--r-- 1 tester users 0 2006-01-09 17:04 status
```

```
dr-xr-xr-x 3 tester users 0 2006-01-09 17:04 task
-r-----r-- 1 tester users 0 2006-01-09 17:04 wchan
```

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

```
tester@linux:~> 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]
```

17.5.1 procinfo

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

```
tester@linux:~> procinfo
Linux 2.6.15-rc5-git3-2-default (geeko@buildhost) (gcc 4.1.0 20051129) #1 Wed
```

Memory:	Total	Used	Free	Shared	Buffers
Mem:	515584	509472	6112	0	73024
Swap:	658656	0	658656		

```
Bootup: Mon Jan 9 12:59:08 2006 Load average: 0.10 0.04 0.05 1/86 5406
```

user :	0:02:07.98	0.8%	page in :	442638	disk 1:	20125r 134
nice :	00:02:20.91	0,9%	page out:	134950		
system:	0:00:42.93	0.3%	page act:	70577		
IOWait:	0:01:25.40	0.6%	page dea:	11696		
hw irq:	0:00:08.94	0.1%	page flt:	1423622		
sw irq:	00:00:01.29	0.0%	swap in :	0		
idle :	04:06:30.54	97,3%	swap out:	0		
uptime:	4:13:20.72		context :	3813145		

```
irq 0: 3799268 timer irq 8: 2 rtc
```



```

irq 1:      130 i8042 irq 9:      1 acpi, uhci_hcd:usb
irq 2:      0 cascade [4]      irq 10:      0 uhci_hcd:usb3
irq 3:      8                  irq 11:      75905 uhci_hcd:usb2, eth
irq 4:      8                  irq 12:      101150 i8042
irq 5:      564535 Intel 82801DB-ICH4 irq 14:      33733 ide0
irq 6:      9                  irq 15:      157045 ide1
irq 7:      1 parport0 [3]

```

Verwenden Sie den Parameter `-a`, wenn Sie alle Informationen sehen 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:

17.6 Prozesse

17.6.1 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  tester    600        393216     2          dest
0x00000000  58294273  tester    600        196608     2          dest
0x00000000  83886083  tester    666        43264     2
0x00000000  83951622  tester    666        192000     2
0x00000000  83984391  tester    666        282464     2
0x00000000  84738056  root      644        151552     2          dest

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

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

```

17.6.2 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`:

```
tester@linux:~> 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
[...]
tester   4047  0.0   6,0 158548 31400 ?        Ssl  13:02    0:06 mono-best
tester   4057  0.0   0,7  9036  3684 ?        Sl   13:02    0:00 /opt/gnome
tester   4067  0.0   0,1  2204   636 ?        S    13:02    0:00 /opt/gnome
tester   4072  0.0   1,0 15996  5160 ?        Ss   13:02    0:00 gnome-scre
tester   4114  0.0   3.7 130988 19172 ?        SLl  13:06    0:04 sound-juic
tester   4818  0.0   0.3  4192  1812 pts/0    Ss   15:59    0:00 -bash
tester   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.

```
tester@linux:~> 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: tester [priv]
 4817 ?        R       0:00 sshd: tester@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:

```
tester@linux:~> 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

```

17.6.3 Prozessbaum: pstree

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

```

tester@linux:~> 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`:

17.6.4 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. Das Programm wird mit der Taste `q` beendet. 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`:

```
tester@linux:~> 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   0:000.00  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  udevd
 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.

17.7 Systeminformationen

17.7.1 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.

17.7.2 Speichernutzung: **free**

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

```
tester@linux:~> 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.

17.7.3 Liste der Benutzer bzw. Prozesse, die auf Dateien zugreifen: `fuser`

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

```
tester@linux:~> fuser -v /mnt/*

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

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

17.7.4 Kernel Ring Buffer: `dmesg`

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

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

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

17.7.5 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:

```
tester@linux:~> lsof -p $$
COMMAND PID  USER  FD  TYPE DEVICE        SIZE  NODE NAME
bash    5552 tester cwd   DIR   3,3    1512 117619 /home/tester
bash    5552 tester rtd   DIR   3,3     584    2 /
bash    5552 tester txt   REG   3,3  498816  13047 /bin/bash
bash    5552 tester mem   REG   0,0         0 [heap] (stat: No such
bash    5552 tester mem   REG   3,3  217016 115687 /var/run/nscd/passwd
bash    5552 tester mem   REG   3,3  208464 11867 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  882134 11868 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3 1386997  8837 /lib/libc-2.3.6.so
bash    5552 tester mem   REG   3,3  13836  8843 /lib/libdl-2.3.6.so
bash    5552 tester mem   REG   3,3  290856 12204 /lib/libncurses.so.5.5
bash    5552 tester mem   REG   3,3  26936 13004 /lib/libhistory.so.5.1
bash    5552 tester mem   REG   3,3 190200 13006 /lib/libreadline.so.5.
bash    5552 tester mem   REG   3,3  54 11842 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  2375 11663 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  290 11736 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  52 11831 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  34 11862 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  62 11839 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3 127 11664 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  56 11735 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  23 11866 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  21544  9109 /usr/lib/gconv/gconv-m
bash    5552 tester mem   REG   3,3  366  9720 /usr/lib/locale/en_GB.
bash    5552 tester mem   REG   3,3  97165  8828 /lib/ld-2.3.6.so
bash    5552 tester 0u   CHR 136,5         7 /dev/pts/5
bash    5552 tester 1u   CHR 136,5         7 /dev/pts/5
bash    5552 tester 2u   CHR 136,5         7 /dev/pts/5
bash    5552 tester 255u CHR 136,5         7 /dev/pts/5
```

Es wurde die spezielle Shell-Variablen `$$` 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:

```
tester@linux:~> lsof | grep CHR
bash    3838 tester 0u   CHR 136,0         2 /dev/pts/0
```

```

bash    3838 tester    1u   CHR 136,0      2 /dev/pts/0
bash    3838 tester    2u   CHR 136,0      2 /dev/pts/0
bash    3838 tester   255u  CHR 136,0      2 /dev/pts/0
bash    5552 tester    0u   CHR 136,5      7 /dev/pts/5
bash    5552 tester    1u   CHR 136,5      7 /dev/pts/5
bash    5552 tester    2u   CHR 136,5      7 /dev/pts/5
bash    5552 tester   255u  CHR 136,5      7 /dev/pts/5
X       5646      root   mem          CHR   1,1          1006 /dev/mem
lsof    5673      tester 0u          CHR 136,5          7 /dev/pts/5
lsof    5673      tester 2u          CHR 136,5          7 /dev/pts/5
grep    5674      tester 1u          CHR 136,5          7 /dev/pts/5
grep    5674      tester 2u          CHR 136,5          7 /dev/pts/5

```

17.7.6 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
UDEVE [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UDEVE [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEVE [1138806687] add@/class/scsi_host/host4
UDEVE [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
UDEVE [1138806693] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEVE [1138806693] add@/class/scsi_generic/sg1
UDEVE [1138806693] add@/class/scsi_device/4:0:0:0
UDEVE [1138806693] add@/block/sdb
UEVENT[1138806694] add@/block/sdb/sdb1
UDEVE [1138806694] add@/block/sdb/sdb1
UEVENT[1138806694] mount@/block/sdb/sdb1
UEVENT[1138806697] umount@/block/sdb/sdb1

```


17.7.7 Von X11-Clients verwendete Serverressourcen: xrestop

Mit `xrestop` werden Statistiken für die serverseitigen Ressourcen der einzelnen angeschlossenen X11-Clients angegeben. Die Ausgabe ähnelt [Abschnitt 17.6.4, „Prozesse: top“](#) (S. 368).

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

res-base	Wins	GCs	Fnts	Pxms	Misc	Pxm mem	Other	Total	PID	Identifier
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	2.816K	4K	2.820K	?	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	1.772K	3K	1.775K	?	Root - Kon
4800000	37	24	1	34	49	1.772K	3K	1.775K	?	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

17.8 Benutzerinformationen

17.8.1 Wer macht was: w

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

```
tester@linux:~> w
 16:33:03 up  3:33,  2 users,  load average: 0.14, 0.06, 0.02
USER      TTY      LOGIN@  IDLE   JCPU   PCPU WHAT
tester    :0       16:33   ?xdm?  9.42s  0.15s /bin/sh /opt/kde3/bin/startk
tester    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.

17.9 Zeit und Datum

17.9.1 Zeitmessung mit `time`

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

```
tester@linux:~> time find . > /dev/null

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

Arbeiten mit der Shell

Beim Start des Linux-Systems wird in der Regel eine grafische Bedienoberfläche geöffnet, die Sie durch die Anmeldung und die darauf folgenden Interaktionen mit dem System führt. Obwohl grafische Bedienoberflächen zunehmend wichtiger und benutzerfreundlicher geworden sind, sind sie nicht die einzige Kommunikationsmöglichkeit mit Ihrem System. Sie können auch eine rein text-orientierte Kommunikationsmethode wählen, wie einen Kommandozeilen-Interpreter (auch Shell genannt), in den Sie Ihre Befehle eingeben. Da Ihnen Linux die Möglichkeit bietet, Shell-Fenster direkt aus der grafischen Bedienoberfläche zu starten, können Sie beide Methoden bequem nebeneinander verwenden.

Gerade bei der Administration spielen Shell-basierte Anwendungen eine besonders große Rolle, wenn Sie zum Beispiel Computer über langsame Netzwerkverbindungen steuern müssen oder Aufgaben als `root` von der Kommandozeile ausführen möchten. Wenn Sie bislang noch nicht mit Linux gearbeitet haben, mag Ihnen die Eingabe von Befehlen in einer Shell vielleicht ungewöhnlich vorkommen. Sie werden aber bald feststellen, dass die Shell nicht nur für Administratoren geeignet ist, sondern häufig auch der schnellste und einfachste Weg ist, Ihre täglichen Aufgaben auszuführen.

Für UNIX bzw. Linux gibt es mehrere Shells. Die Standard-Shell in SUSE® Linux Enterprise ist Bash (GNU Bourne-Again Shell).

Dieses Kapitel befasst sich mit einigen Grundlagen, die Sie für die Arbeit mit der Shell kennen sollten. Hierzu zählen unter anderem die folgenden Themen: die Eingabe von Befehlen, die Verzeichnisstruktur von Linux, die Verwendung von Dateien und Verzeichnissen, einige der grundlegenden Funktionen der Shell, das Benutzer- und Berechtigungskonzept von Linux, eine Übersicht über die wichtigsten Shell-Befehle

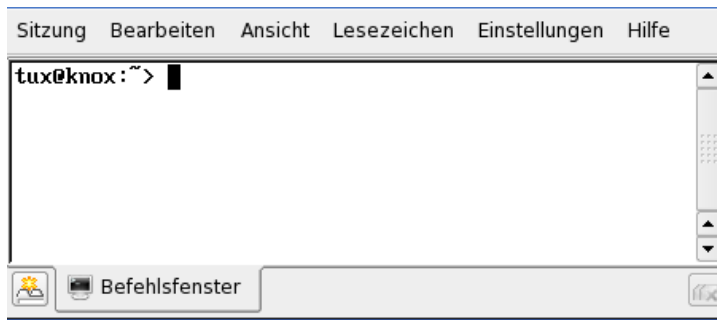
sowie eine kurze Einführung in den Editor vi, einem Standardeditor, der auf UNIX- und Linux-Systemen immer zur Verfügung steht.

18.1 Einführung in die Bash-Shell

Unter Linux können Sie die Kommandozeile parallel zur grafischen Bedienoberfläche verwenden und einfach zwischen den beiden wechseln. Um ein Terminalfenster über die grafische Bedienoberfläche in KDE zu starten, klicken Sie in der Kontrollleiste auf das Symbol für "Konsole". Klicken Sie in GNOME auf das Symbol "GNOME-Terminal" in der Kontrollleiste.

Das Konsole-Fenster bzw. das GNOME-Terminalfenster wird geöffnet. Dabei erscheint die Eingabeaufforderung (Prompt) in der ersten Zeile, wie in [Abbildung 18.1](#), „[Beispiel eines Bash-Terminalfensters](#)“ (S. 376). Die Eingabeaufforderung zeigt normalerweise folgende Informationen an: Ihren Anmeldenamen (in diesem Fall `tux`), den Hostnamen Ihres Computers (hier `knox`) und den aktuellen Pfad (in diesem Fall Ihr Home-Verzeichnis, gekennzeichnet durch die Tilde, `~`) an. 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 18.1 *Beispiel eines Bash-Terminalfensters*



18.1.1 Eingeben von Befehlen

Ein Befehl besteht aus mehreren Elementen. Das erste Element ist stets der tatsächliche Befehl, gefolgt von Parametern oder Optionen. Sie können einen Befehl eintippen und

ihn nachfolgend mithilfe von `←`, `→`, `⇐`, `Entf` und `Leertaste` ändern. Sie können außerdem Optionen hinzufügen oder Tippfehler korrigieren. Befehle werden erst ausgeführt, wenn Sie `Eingabetaste` drücken.

WICHTIG: Keine Nachricht ist eine gute Nachricht.

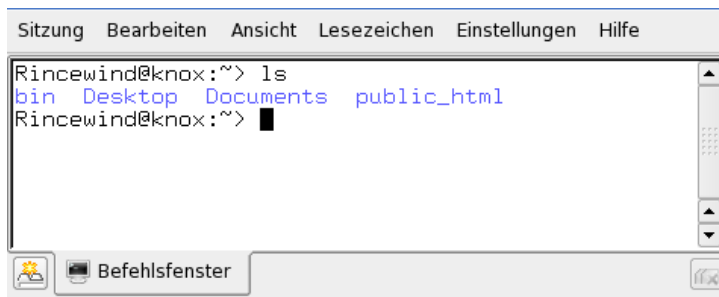
Die Shell gibt nicht viele Meldungen aus: Im Gegensatz zu einigen grafischen Bedienoberflächen erhalten Sie normalerweise keine Bestätigungsmeldungen, wenn Befehle ausgeführt wurden. Meldungen erscheinen nur bei Problemen oder Fehlern ausgegeben.

Beachten Sie dies auch bei Befehlen zum Löschen von Objekten. Bevor Sie einen Befehl zum Entfernen einer Datei eingeben, wie beispielsweise `rm`, sollten Sie sich sicher sein, dass Sie das betreffende Objekt wirklich löschen möchten: Es wird ohne Nachfrage unwiederbringlich gelöscht.

Verwenden von Befehlen ohne Optionen

Betrachten wir die Struktur von Befehlen anhand eines einfachen Beispiels: anhand des Befehls `ls`, der verwendet wird, um den Inhalt eines Verzeichnisses aufzulisten. Der Befehl kann mit oder ohne Optionen verwendet werden. Durch Eingabe des Befehls `ls` ohne Zusatz wird der Inhalt des aktuellen Verzeichnisses angezeigt:

Abbildung 18.2 *Der Befehl ls*



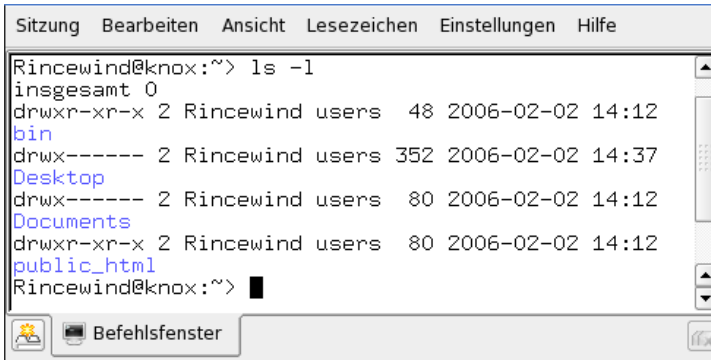
The image shows a terminal window titled 'Befehlsfenster'. The menu bar at the top includes 'Sitzung', 'Bearbeiten', 'Ansicht', 'Lesezeichen', 'Einstellungen', and 'Hilfe'. The terminal content shows the prompt 'Rincewind@knox:~>' followed by the command 'ls'. The output is 'bin Desktop Documents public_html'. The prompt 'Rincewind@knox:~>' is followed by a cursor. The terminal window has a scrollbar on the right and a taskbar at the bottom with a 'Befehlsfenster' tab and a close button.

Anders als bei anderen Betriebssystemen können Dateien in Linux eine Dateinamenserweiterung, wie `.txt`, aufweisen, müssen jedoch nicht. Daher ist es in dieser Ausgabe von `ls` schwierig, Dateien von Ordnern zu unterscheiden. Standardmäßig können Sie sich an den Farben orientieren: Verzeichnisse werden normalerweise in blauer, Dateien in schwarzer Farbe angezeigt.

Verwenden von Befehlen mit Optionen

Eine bessere Methode, weitere Details zum Inhalt eines Verzeichnisses zu erhalten, besteht darin, den Befehl `ls` mit einer Reihe von Optionen zu verwenden. Durch Optionen wird die Funktionsweise eines Befehls verändert, so dass Sie damit spezielle Aufgaben ausführen können. Optionen werden vom Befehl durch ein Leerzeichen getrennt und ihnen ist ein Bindestrich vorangestellt. Der Befehl `ls -l` z. B. zeigt den Inhalt desselben Verzeichnisses mit allen Details an (long listing format).

Abbildung 18.3 Der Befehl `ls -l`



```
Rincewind@knox:~> ls -l
insgesamt 0
drwxr-xr-x 2 Rincewind users 48 2006-02-02 14:12
bin
drwx----- 2 Rincewind users 352 2006-02-02 14:37
Desktop
drwx----- 2 Rincewind users 80 2006-02-02 14:12
Documents
drwxr-xr-x 2 Rincewind users 80 2006-02-02 14:12
public_html
Rincewind@knox:~>
```

Links neben den einzelnen Objektnamen werden in mehreren Spalten Informationen zum Objekt angezeigt. Die wichtigsten Informationen sind folgende: Die erste Spalte zeigt den Dateityp des Objekts (im vorliegenden Beispiel: `d` für Verzeichnisse ("directory") oder `-` für Dateien). In den nächsten neun Spalten werden die Benutzerberechtigungen für das Objekt angezeigt. Die Spalten 11 und 12 zeigen den Namen des Dateieigentümers und der Gruppe an (in diesem Fall: `tux` und `users`). Informationen zu Benutzerberechtigungen und dem Benutzerkonzept von Linux finden Sie in [Abschnitt 18.2, „Benutzer und Zugriffsberechtigungen“](#) (S. 389). In der nächsten Spalte wird die Dateigröße in Byte angezeigt, danach Datum und Uhrzeit der letzten Änderung. Die letzte Spalte zeigt den Namen des Objekts an.

Wenn Sie noch weitere Informationen anzeigen möchten, können Sie zwei Optionen für den Befehl `ls` kombinieren und `ls -la` eingeben. Die Shell zeigt nun auch verborgene Dateien im Verzeichnis an. Diese werden durch einen vorangestellten Punkt gekennzeichnet. (z. B. `.verborgenedatei`).

Aufrufen der Hilfe

Sie müssen sich nicht alle Optionen für alle Befehle merken. Wenn Sie den Namen eines Befehls wissen, sich jedoch hinsichtlich der Optionen nicht sicher sind, können Sie den Befehl mit nachfolgendem Leerzeichen und `--help` eingeben. Die Option `--help` ist für viele Befehle verfügbar. Durch Eingabe von `ls --help` werden alle Optionen für den Befehl `ls` angezeigt.

18.1.2 Linux-Verzeichnisstruktur

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-Systemen besitzen. Sie können sich Verzeichnisse als elektronische Ordner vorstellen, in denen Dateien, Programme und Unterverzeichnisse gespeichert sind. Die oberste Ebene in der Hierarchie bildet das `root`-Verzeichnis, auch `/` genannt. Von hier aus können Sie auf alle anderen Verzeichnisse zugreifen.

[Abbildung 18.4](#) zeigt den Standard-Verzeichnisbaum in Linux mit den Home-Verzeichnissen der Beispielbenutzer `xyz`, `linux` und `tux` an. Das Verzeichnis `/home` enthält die Verzeichnisse, in denen die einzelnen Benutzer ihre persönlichen Dateien speichern können.

ANMERKUNG: Home-Verzeichnis in einer Netzwerkumgebung

Wenn Sie in einer Netzwerkumgebung arbeiten, trägt Ihr Home-Verzeichnis möglicherweise nicht den Namen `/home`. Es kann jedem beliebigen Verzeichnis im Dateisystem zugeordnet sein.

Die folgende Liste enthält eine kurze Beschreibung der Standardverzeichnisse in Linux.

Abbildung 18.4 Auszug aus einer Standardverzeichnisstruktur

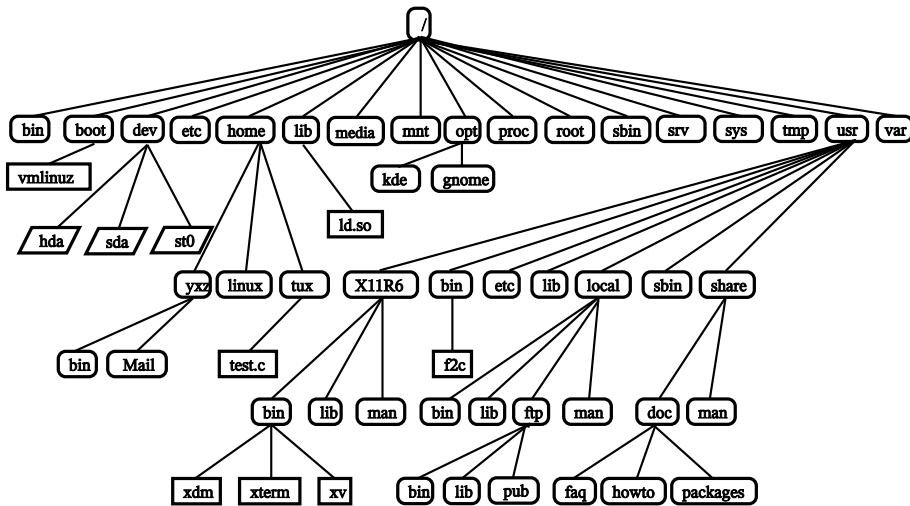


Tabelle 18.1 Überblick über eine Standardverzeichnisstruktur

/	Root-Verzeichnis, Startpunkt der Verzeichnisstruktur
/home	Persönliche Verzeichnisse von Benutzern
/dev	Geräte Dateien, die Hardware-Komponenten darstellen
/etc	Wichtige Dateien für die Systemkonfiguration
/etc/init.d	Startskripts
/bin, /sbin	Programme, die am Anfang des Startvorgangs (/bin) und für den Administrator (/sbin) benötigt werden
/usr, /usr/local	Alle Anwendungsprogramme und lokalen, verteilungsunabhängigen Erweiterungen (/usr/local)
/usr/bin, /usr/sbin	Programme, die für den allgemeinen Zugriff verfügbar (/usr/bin) und für den Systemadministrator reserviert sind (/usr/sbin)

<code>/usr/share/doc</code>	Verschiedene Dokumentationsdateien
<code>/tmp, /var/tmp</code>	Temporäre Dateien (speichern Sie keine Dateien in diesem Verzeichnis, es sei denn, diese werden nicht benötigt)
<code>/opt</code>	Optionale Software, größere Add-On-Programmpakete (wie KDE, GNOME und Netscape)
<code>/proc</code>	Prozessdateisystem
<code>/sys</code>	Systemdateisystem, in dem alle Gerätedaten für das Kernel gesammelt werden.
<code>/var/log</code>	Systemprotokolldateien

18.1.3 Arbeiten mit Verzeichnissen und Dateien

Um eine bestimmte Datei bzw. ein bestimmtes Verzeichnis anzusprechen, müssen Sie den Pfad angeben, der zu dem betreffenden Verzeichnis bzw. der betreffenden Datei führt. Es gibt zwei Möglichkeiten, einen Pfad anzugeben:

- Der vollständige Pfad vom root-Verzeichnis zur jeweiligen Datei (absoluter Pfad)
- Der Pfad, der vom aktuellen Verzeichnis ausgeht (relativer Pfad)

Absolute Pfade beginnen immer mit einem Schrägstrich. Relativen Pfaden ist kein Schrägstrich vorangestellt.

ANMERKUNG: Bei Linux muss die Groß- und Kleinschreibung berücksichtigt werden

Linux unterscheidet im Dateisystem zwischen Groß- und Kleinbuchstaben. So ist es für Linux ein Unterschied, ob Sie `test.txt` oder `Test.txt` eingeben. Beachten Sie dies bei der Eingabe von Dateinamen und Pfaden.

Mit dem Befehl `cd` können Sie das Verzeichnis wechseln.

- Geben Sie `cd` ein, um zu Ihrem Home-Verzeichnis zu wechseln.
- Das aktuelle Verzeichnis wird mit einem Punkt (`.`) angegeben. Dies ist hauptsächlich für andere Befehle (`cp`, `mv`, ...) sinnvoll.
- Die nächsthöhere Ebene in der Struktur wird durch zwei Punkte dargestellt (`..`). Um beispielsweise zum übergeordneten Verzeichnis des aktuellen Verzeichnisses zu wechseln, geben Sie `cd ..` ein.

Beispiele, wie Sie Dateien ansprechen können

In [Abschnitt 18.1.3, „Arbeiten mit Verzeichnissen und Dateien“](#) (S. 381) wurden relative Pfade bei der Eingabe von `cd` verwendet. Sie können auch absolute Pfade verwenden. Angenommen, Sie möchten eine Datei aus Ihrem Home-Verzeichnis in ein Unterverzeichnis von `/tmp` kopieren:

- 1 Erstellen Sie ausgehend von Ihrem Home-Verzeichnis ein Unterverzeichnis in `/tmp`:
 - a Wenn das aktuelle Verzeichnis nicht Ihr Home-Verzeichnis ist, geben Sie `cd ~` ein, um zum Home-Verzeichnis zu wechseln. Sie können von jeder Stelle im Dateisystem zu Ihrem Home-Verzeichnis wechseln, indem Sie `cd ~` eingeben.
 - b Geben Sie in Ihrem Home-Verzeichnis `mkdir /tmp/test` ein. `mkdir` steht für „make directory“. Mit diesem Befehl erstellen Sie ein neues Verzeichnis mit dem Namen `test` im Verzeichnis `/tmp`. In diesem Fall verwenden Sie einen absoluten Pfad, um das Verzeichnis zu erstellen.
 - c Geben Sie nun `ls -l /tmp` ein, um zu überprüfen, was geschehen ist. Das neue Verzeichnis `test` sollte nun in der Inhaltsliste des Verzeichnisses `/tmp` angezeigt werden.
- 2 Erstellen Sie nun eine neue Datei in Ihrem Home-Verzeichnis und kopieren Sie sie mithilfe eines relativen Pfads in das Verzeichnis `/tmp/test`.
 - a Geben Sie den Befehl `touch myfile.txt` ein. Durch den Befehl `touch` mit der Option `myfile.txt` wird eine neue, leere Datei mit dem Namen `myfile.txt` in Ihrem aktuellen Verzeichnis erstellt.

- b** Prüfen Sie dies, indem Sie `ls -l` eingeben. Die neue Datei sollte in der Inhaltsliste angezeigt werden.
- c** Geben Sie `cp myfile.txt ../tmp/test` ein. Dadurch wird `myfile.txt` in das Verzeichnis `/tmp/test` kopiert, ohne den Namen der Datei zu ändern.
- d** Prüfen Sie dies, indem Sie `ls -l /tmp/test` eingeben. Die Datei `myfile.txt` sollte nun in der Inhaltsliste für `/tmp/test` angezeigt werden.

Um die Inhalte von Home-Verzeichnissen anderer Benutzer aufzulisten, geben Sie `ls ~benutzername` ein. Im Beispielsverzeichnisbaum in [Abbildung 18.4](#), „Auszug aus einer Standardverzeichnisstruktur“ (S. 380) ist einer der Beispielbenutzer `tux`. In diesem Fall würde `ls ~tux` den Inhalt des Home-Verzeichnisses von `tux` auflisten.

ANMERKUNG: Leerzeichen in Datei- oder Verzeichnisnamen

Wenn ein Dateiname ein Leerzeichen enthält, geben Sie entweder vor dem Leerzeichen ein Escape-Zeichen (umgekehrter Schrägstrich `\`) ein oder schließen Sie den Dateinamen in einfache oder doppelte Anführungszeichen ein. Anderenfalls interpretiert Bash einen Dateinamen wie `Eigene Dokumente` als den Namen von zwei Dateien oder Verzeichnissen. Der Unterschied zwischen einfachen und doppelten Anführungszeichen ist, dass bei doppelten Anführungszeichen eine Variablenerweiterung stattfindet. Einfache Anführungszeichen gewährleisten, dass die Zeichenfolge von der Shell buchstäblich interpretiert wird.

18.1.4 Nützliche Funktionen der Shell

Befehle in Bash einzugeben, kann mit höherem Tippaufwand verbunden sein. Im Folgenden lernen Sie einige Funktionen von Bash kennen, die Ihre Arbeit erleichtern und Ihnen viel Tippaufwand ersparen können.

History und Ergänzung

Standardmäßig „merkt“ sich Bash die Befehle, die Sie eingeben. Diese Funktion wird *History* genannt. Um einen Befehl zu wiederholen, der bereits eingegeben wurde, drücken Sie `↑`, bis die Eingabeaufforderung den vorherigen Befehl anzeigt. Drücken Sie `↓`, um sich vorwärts durch die Liste der zuvor eingegebenen Befehle zu bewegen. Verwenden Sie `Strg + R`, um die History zu durchsuchen.

Sie können den ausgewählten Befehl ändern, indem Sie beispielsweise den Namen einer Datei ändern, bevor Sie den Befehl durch Drücken von `Eingabetaste` ausführen. Um die Kommandozeile zu bearbeiten, verschieben Sie den Cursor mit den Pfeiltasten an die gewünschte Position und beginnen die Eingabe.

Die Ergänzung eines Datei- oder Verzeichnisnamens nach der Eingabe der ersten Buchstaben ist eine weitere hilfreiche Funktion von Bash. Geben Sie hierzu die ersten Buchstaben einer vorhandenen Datei oder eines vorhandenen Verzeichnisses ein und drücken Sie die `→|`. Wenn der Dateiname bzw. Pfad eindeutig identifiziert werden kann, wird er sofort ergänzt und der Cursor springt zum Ende des Dateinamens. Anschließend können Sie die nächste Option des Befehls eingeben, falls erforderlich. Wenn der Dateiname oder Pfad nicht eindeutig identifiziert werden kann (da mehrere Dateinamen mit denselben Buchstaben beginnen), wird der Dateiname nur so weit ergänzt, bis mehrere Varianten möglich sind. Eine Auflistung dieser Varianten erhalten Sie, indem Sie ein zweites Mal die Taste `→|` drücken. Anschließend können Sie die nächsten Buchstaben der Datei bzw. des Pfads eingeben und erneut die Ergänzungsfunktion durch Drücken von `→|` aktivieren. Wenn Sie Dateinamen und Pfade mithilfe von `→|` ergänzen, können Sie gleichzeitig überprüfen, ob die Datei bzw. der Pfad, den Sie eingeben möchten, tatsächlich vorhanden ist (und Sie können sicher sein, dass er richtig geschrieben ist).

Platzhalter

Eine weitere Komfortfunktion der Shell sind Platzhalter, die Sie verwenden können, um Dateinamen zu erweitern. Platzhalter sind Zeichen, die für andere Zeichen stehen. Bash kennt drei verschiedene Arten von Platzhaltern:

?

Stimmt genau mit einem zufälligen Zeichen überein

*

Stimmt mit einer beliebigen Zahl an Zeichen überein

[*set*]

Stimmt mit einem Zeichen aus der Gruppe überein, die in den eckigen Klammern angegeben wurde und hier durch die Zeichenfolge *set* dargestellt wird. Als Teil von *set* können Sie auch Zeichenklassen mit der Syntax [*class*:] festlegen, wobei *class* zu *alnum*, *alpha*, *ascii* usw. gehört.

Wenn Sie **!** oder **^** am Beginn der Gruppe verwenden (**[!set]**), wird eine Übereinstimmung mit einem Zeichen gesucht, das keinem der Zeichen entspricht, die durch *set* festgelegt wurden.

Angenommen, das Verzeichnis `test` enthält die Dateien `Testfile`, `Testfile1`, `Testfile2` und `datafile`.

- Der Befehl `ls Testfile?` führt die Dateien `Testfile1` und `Testfile2` auf.
- Der Befehl `ls Testfile*` führt die Dateien `Testfile1` und `Testfile2` auf.
- Bei Verwendung des Befehls `ls Test*` umfasst die Liste auch `Testfile`.
- Der Befehl `ls *fil*` führt alle Beispieldateien auf.
- Verwenden Sie den Platzhalter `set`, um alle Beispieldateien zu adressieren, deren letztes Zeichen eine Ziffer ist: `ls Testfile[1-9]` oder, wenn Sie Klassen verwenden `ls Testfile[[:digit:]]`.

Von den vier Platzhaltertypen beinhaltet das Sternchen die meisten Zeichen. Es kann verwendet werden, um alle im Verzeichnis enthaltenen Dateien in ein anderes zu kopieren oder um alle Dateien mit einem Befehl zu löschen. Der Befehl `rm *fil*` würde z. B. alle Dateien im aktuellen Verzeichnis löschen, deren Namen die Zeichenfolge *fil* umfassen.

Anzeigen von Dateien mit **Less and More**

Linux umfasst zwei kleine Programme zum Anzeigen von Textdateien direkt in der Shell: `less` und `more`. Anstatt einen Editor zu starten, um eine Datei zu lesen wie

`Readme.txt`, geben Sie einfach `less Readme.txt` ein, um den Text im Konsolenfenster anzuzeigen. Verwenden Sie die `[Leertaste]`, um die Seiten durchzublättern. Verwenden Sie `[Pfeil-Aufwärts]` und `[Pfeil-Abwärts]`, um sich im Text nach vorne oder hinten zu bewegen. Um "less" zu beenden, drücken Sie `[Q]`.

Statt "less" können Sie auch das ältere Programm "more" verwenden. Dies ist jedoch weniger praktisch, da Sie nicht zurückblättern können.

Das Programm "less" hat seinen Namen von dem Konzept *less is more* (*weniger ist mehr*) und kann auch verwendet werden, um die Ausgabe von Befehlen auf bequeme Art zu gestalten. Wenn Sie wissen möchten, wie dies funktioniert, lesen Sie „Umleitung und Pipes“ (S. 386).

Umleitung und Pipes

Normalerweise ist die Standardausgabe in der Shell der Bildschirm oder das Konsolenfenster und die Standardeingabe erfolgt über die Tastatur. Allerdings bietet die Shell Funktionen, mit denen Sie die Eingabe bzw. Ausgabe an ein anderes Objekt, beispielsweise eine Datei oder einen anderen Befehl, umleiten können. Mithilfe der Symbole `>` und `<` beispielsweise können Sie die Ausgabe eines Befehls in eine Datei weiterleiten (Ausgabeumleitung) oder eine Datei als Eingabe für einen Befehl verwenden (Eingabeumleitung). Wenn Sie also die Ausgabe eines Befehls, wie beispielsweise `ls` in eine Datei schreiben möchten, geben Sie `ls -l > file.txt` ein. Dadurch wird eine Datei mit dem Namen `file.txt` erstellt, die eine Inhaltsliste des aktuellen Verzeichnisses enthält, welche Sie durch den Befehl `ls` erzeugt haben. Wenn jedoch bereits eine Datei mit dem Namen `file.txt` vorhanden ist, wird mit diesem Befehl die bestehende Datei überschrieben. Sie können diese mit `>>` verhindern. Durch Eingabe von `ls -l >> file.txt` wird die Ausgabe des Befehls `ls` einfach an eine bereits bestehende Datei `file.txt` angehängt. Wenn die Datei noch nicht vorhanden ist, wird sie erstellt.

Manchmal ist es auch sinnvoll, eine Datei als Eingabe für einen Befehl zu verwenden. So können Sie beispielsweise mit dem Befehl `tr` Zeichen ersetzen, die aus einer Datei umgeleitet wurden, und das Ergebnis in die Standardausgabe, den Bildschirm, schreiben. Angenommen, Sie möchten alle Zeichen `t` in der Datei `file.txt` aus dem obigen Beispiel durch `x` ersetzen und das Ergebnis auf dem Bildschirm ausgeben. Geben Sie dazu `tr t x < file.txt` ein.

Wie die Standardausgabe wird die Standardfehlerausgabe zur Konsole gesendet. Um eine Standardfehlerausgabe an eine Datei mit dem Namen `fehler` zu senden, hängen Sie `2> fehler` an den entsprechenden Befehl an. Sowohl Standardausgabe als auch Standardfehler werden in einer Datei mit dem Namen `gesamtausgabe` gespeichert, wenn Sie `>& Gesamtausgabe` anhängen.

Die Verwendung von *Pipelines* bzw. *Pipes* ist ebenfalls eine Art von Umleitung. Allerdings ist die Verwendung der Pipe nicht auf Dateien beschränkt. Mit einer Pipe (`|`) können Sie mehrere Befehle kombinieren, indem Sie die Ausgabe eines Befehls als Eingabe für den nächsten Befehl verwenden. Um beispielsweise den Inhalt Ihres aktuellen Verzeichnisses in `less` anzuzeigen, geben Sie `ls | less` ein. Dies ist nur sinnvoll, wenn die normale Ausgabe mit `ls` zu lang wäre. Wenn Sie z. B. den Inhalt des Verzeichnisses `dev` mit `ls /dev` anzeigen, können Sie nur einen kleinen Teil des Fensters sehen. Die gesamte Liste können Sie mit `ls /dev | less` anzeigen.

18.1.5 Archive und Datenkomprimierung

Da Sie nun bereits eine Reihe von Dateien und Verzeichnissen erstellt haben, möchten Sie vielleicht Archive erstellen und die Daten komprimieren. Angenommen, Sie möchten das gesamte Verzeichnis `test` in eine Datei packen, die Sie auf einem USB-Stick als Sicherungskopie speichern oder per eine E-Mail versenden können. Verwenden Sie hierzu den Befehl `tar` (für *tape archiver* (*Bandarchivierung*)). Durch Eingabe von `tar --help` können Sie alle Optionen für den Befehl `tar` anzeigen. Die wichtigste dieser Optionen wird hier erklärt:

- c
(für create, erstellen) Ein neues Archiv erstellen.
- t
(für table, Tabelle) Inhalt eines Archivs anzeigen.
- x
(für extract, extrahieren) Das Archiv entpacken.
- v
(für verbose, ausführlich) Alle Dateien auf dem Bildschirm anzeigen, während das Archiv erstellt wird.

-f

(für file, Datei) Wählen Sie einen Dateinamen für die Archivdatei. Beim Erstellen eines Archivs muss diese Option stets zuletzt gegeben sein.

Gehen Sie wie folgt vor, um das Verzeichnis `test` mit allen Dateien und Unterverzeichnissen in ein Archiv mit dem Namen `testarchiv.tar` zu packen:

- 1 Öffnen Sie eine Shell.
- 2 Verwenden Sie `cd`, um zu Ihrem Home-Verzeichnis zu wechseln, in dem sich das Verzeichnis `test` befindet.
- 3 Geben Sie `tar -cvf testarchive.tar test` ein. Die Option `-c` erstellt das Archiv, `-f` macht es zu einer Datei. Die Option `-v` listet die Dateien bei der Verarbeitung auf.
- 4 Zeigen Sie den Inhalt der Archivdatei mit `tar -tf testarchiv.tar` an.

Das Verzeichnis `test` mit all seinen Dateien und Verzeichnissen befindet sich immer noch unverändert auf der Festplatte. Um das Archiv zu entpacken, geben Sie `tar -xvf testarchiv.tar` ein, aber versuchen Sie dies jetzt noch nicht.

Für die Dateikomprimierung ist die offensichtliche Wahl `gzip` oder `bzip2` für ein verbessertes Komprimierungsverhältnis. Geben Sie einfach `gzip testarchiv.tar` (oder `bzip2 testarchiv.tar`; in diesem Beispiel wird jedoch `gzip` verwendet). Mit `ls` sehen Sie, dass die Datei `testarchiv.tar` nicht mehr vorhanden ist und dass die Datei `testarchiv.tar.gz` stattdessen erstellt wurde. Diese Datei ist viel kleiner und daher besser geeignet für die Übertragung durch E-Mail oder für die Speicherung auf einem USB-Stick.

Entpacken Sie jetzt die Datei im zuvor erstellten `test2`-Verzeichnis. Geben Sie hierzu `cp testarchiv.tar.gz test2` ein, um die Datei in dieses Verzeichnis zu kopieren. Wechseln Sie in das Verzeichnis mit `cd test2`. Ein komprimiertes Archiv mit der Erweiterung `.tar.gz` kann entzippt werden mit dem Befehl `gunzip`. Geben Sie `gunzip testarchive.tar.gz` ein. Dadurch wird die Datei `testarchiv.tar` erstellt, die mit `tar -xvf testarchiv.tar` extrahiert oder "*untarred*" werden muss. Sie können ein komprimiertes Archiv auch in einem Schritt entzippen und extrahieren mit `tar -xvf testarchiv.tar.gz` (das Hinzufügen der Option `-z` ist nicht mehr erforderlich). Mit `ls` können Sie sehen, dass ein neues Verzeichnis

`test` mit demselben Inhalt erstellt wurde wie das Verzeichnis `test` im Home-Verzeichnis.

18.1.6 Löschen

Nach diesem Schnellkurs sind Sie mit den Grundlagen der Linux-Shell oder der Kommandozeile vertraut. Sie können das Home-Verzeichnis bereinigen, indem Sie die verschiedenen Testdateien und Verzeichnisse mit den Befehlen `rm` und `rmdir` löschen. Unter [Abschnitt 18.3, „Wichtige Linux-Befehle“](#) (S. 393) finden Sie eine Liste der wichtigsten Befehle und eine kurze Beschreibung ihrer Funktionen.

18.2 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.

18.2.1 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. So kann eine Gruppe, die an einem bestimmten Projekt arbeitet, den Namen `project3` erhalten. 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 18.1](#), „[Beispielausgabe mit Dateiberechtigungen](#)“ (S. 390) aus.

Beispiel 18.1 *Beispielausgabe mit Dateiberechtigungen*

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

Wie aus der dritten Spalte hervorgeht, ist diese Datei Benutzer `tux` zugehörig. 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 (-) besagt, 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. Aus den ersten drei Zeichen geht hervor, 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 (-) bedeutet, dass nicht in die Datei geschrieben werden kann. 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 weisen den Typ d auf. Für Verzeichnisse weicht die Bedeutung der einzelnen Berechtigungen geringfügig voneinander ab.

Beispiel 18.2 *Beispielausgabe mit Verzeichnisberechtigungen*

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

In [Beispiel 18.2](#), „[Beispielausgabe mit Verzeichnisberechtigungen](#)“ (S. 391) sind der Eigentümer (tux) und die Eigentümergruppe (project3) des Verzeichnisses ProjectData leicht zu identifizieren. Im Gegensatz zu den Dateizugriffsberechtigungen unter [Dateizugriff](#) (S. 390) 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).

18.2.2 Bearbeiten von Dateiberechtigungen

Ändern von Zugriffsberechtigungen

Die Zugriffsberechtigungen für eine Datei und ein Verzeichnis können vom Eigentümer und natürlich von `root` mithilfe des Befehls `chmod` geändert werden, gefolgt von den Parametern, mit denen die Berechtigungen geändert werden, und einem oder mehreren Dateinamen. 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 (weitere)*) – zusätzliche Benutzer (wenn kein Parameter angegeben ist, gelten die Änderungen für alle Kategorien)
2. Ein Zeichen für das Löschen (-), Festlegen (=) oder Einfügen (+)
3. Die Abkürzungen
 - `r` – *read (Lesen)*
 - `w` – *write (Schreiben)*
 - `x` – *execute (Ausführen)*
4. Dateiname oder durch Leerzeichen voneinander getrennte Dateinamen

Wenn der Benutzer `tux` in [Beispiel 18.2, „Beispielausgabe mit Verzeichnisberechtigungen“](#) (S. 391) 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 Schreibberechtigungen erteilen möchte, kann er hierzu den Befehl `chmod go-w ProjectData` eingeben. Um allen Benutzern das Hinzufügen einer neuen Datei zu 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 18.2, „Beispielausgabe mit Verzeichnisberechtigungen“](#) (S. 391) 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 18.1, „Beispielausgabe mit Dateiberechtigungen“](#) (S. 390) die Eigentümerschaft der Datei `ProjectData` in `project4` ändern (mithilfe des Befehls `chgrp project4 ProjectData`), wenn er Mitglied dieser neuen Gruppe ist.

18.3 Wichtige Linux-Befehle

Dieser Abschnitt gibt Ihnen einen Überblick über die wichtigsten Befehle des SUSE® Linux Enterprise-Systems. 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 Manualpages, die Sie mit dem Befehl `man` gefolgt von dem Namen des jeweiligen Befehls öffnen (z. B. `man ls`).

In den Manualpages 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 Manualpages. 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 durch die Schrift `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.

18.3.1 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 nur 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`
Lesen

`w`
Schreiben

`x`
Ausführen (Ausführen der Dateien oder Wechseln in das Verzeichnis)

`s`
Setuid-Bit – Die Anwendung bzw. das Programm wird so gestartet, 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`. Anwendungsbeispiele finden Sie in [Abschnitt 18.1.5, „Archive und Datenkomprimierung“](#) (S. 387).

`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 Platzhalter 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. Allerdings hat diese Vorgehensweise auch einen erheblichen Nachteil: `locate` findet keine Dateien, die nach der letzten Aktualisierung dieser Datenbank erstellt wurden. Die Datenbank wird mit `updatedb` aktualisiert. Dazu benötigen Sie allerdings `Root`-Berechtigungen.

`updatedb` [Optionen]

Dieser Befehl aktualisiert die von `locate` verwendete Datenbank. 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

`file` [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` [Optionen] Dateien

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 Einhängepunkt]`

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 \(1\)](#).

```
aush ngen [Optionen] Einh ngepunkt
```

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.

Anderenfalls besteht die Gefahr eines Datenverlustes! Normalerweise können die Befehle `einhangen` und `aushangen` 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.

18.3.2 Systembefehle

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

Systeminformationen

```
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 menschenlesbarer 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 hierzu finden Sie unter [Abschnitt 22.1.6](#), „Der Befehl `free`“ (S. 464).

-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]`

Ohne Angabe von Optionen zeigt dieser Befehl eine Tabelle der von Ihnen gestarteten Programme und Prozesse 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`).

Andere

`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 den Befehl ohne Benutzername 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]

Führt 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.

18.3.3 Weitere 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.

18.4 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.

18.4.1 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.

In vi werden drei grundlegende Betriebsmodi verwendet: *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. *Beenden ohne 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* **[Umsch-alttaste]** + **[Z]** **[Umschalttaste]** + **[Z]**. Zum Beenden des Programms und zum Speichern

aller Änderungen im *erweiterten* Modus geben Sie `:`–`W`–`Q` ein. Im *erweiterten* Modus steht `w` für Schreiben und `q` für Beenden.

18.4.2 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 18.2, „Einfache Befehle im vi-Editor“](#) (S. 407) aufgeführt. Diese Liste ist nicht vollständig. Umfangreichere Listen finden Sie in der Dokumentation in [Abschnitt 18.4.3, „Weitere Informationen“](#) (S. 409).

Tabelle 18.2 *Einfache Befehle im vi-Editor*

<code>Esc</code>	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 + R	Rückgängig gemachte Änderung erneut ausführen
Umschalttaste + J	Folgende Zeile an die aktuelle Zeile anfügen
.	Letzten Befehl wiederholen

18.4.3 Weitere 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 SUSE® Linux Enterprise ist vim (vi improved), eine verbesserte Version von vi, enthalten. 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>, <http://www.linuxgazette.com/node/view/9039> 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 3. System

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

19

SUSE® Linux Enterprise ist für verschiedene 64-Bit-Plattformen verfügbar. Das bedeutet jedoch nicht unbedingt, dass alle enthaltenen Anwendungen bereits auf 64-Bit-Plattformen portiert wurden. SUSE Linux Enterprise unterstützt die Verwendung von 32-Bit-Anwendungen in einer 64-Bit-Systemumgebung. Dieses Kapitel bietet einen kurzen Überblick darüber, wie diese Unterstützung auf SUSE Linux Enterprise-64-Bit-Plattformen implementiert ist. 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.

ANMERKUNG: 31-Bit-Anwendungen auf IBM-System z:

s390 auf IBM-System z nutzt eine 31-Bit-Umgebung. Verweise auf 32-Bit-Anwendungen gelten im Folgenden auch für 31-Bit-Anwendungen.

SUSE Linux Enterprise für die 64-Bit-Plattformen ia64, ppc64, s390x und x86_64 ist so konzipiert, dass bestehende 32-Bit-Anwendungen sofort in der 64-Bit-Umgebung ausgeführt werden können. Die entsprechenden 32-Bit-Plattformen sind x86 für ia64, ppc für ppc64, s390 für s390x und x86 für x86_64. 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. Das aktuelle ppc64-System führt die meisten Anwendungen im 32-Bit-Modus aus, es können aber auch 64-Bit-Anwendungen ausgeführt werden.

19.1 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.

Derselbe Ansatz gilt für die 64-Bit-Plattformen `ppc64`, `s390x` und `x86_64`: Um die Kompatibilität mit der 32-Bit-Version aufrechtzuerhalten, werden die Bibliotheken am selben Ort im System gespeichert wie in der 32-Bit-Umgebung. Die 32-Bit-Version von `libc.so.6` befindet sich sowohl in der 32-Bit- als auch in der 64-Bit-Umgebung unter `/lib/libc.so.6`.

Alle 64-Bit-Bibliotheken und Objektdateien befinden sich in Verzeichnissen mit dem Namen `lib64`. Die 64-Bit-Objektdateien, die sich normalerweise unter `/lib`, `/usr/lib` und `/usr/X11R6/lib` befinden, werden nun unter `/lib64`, `/usr/lib64` bzw. `/usr/X11R6/lib64` gespeichert. Unter `/lib`, `/usr/lib` und `/usr/X11R6/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. Beispielsweise befinden sich die X11-Schriftarten noch immer am gewohnten Ort unter `/usr/X11R6/lib/X11/fonts`. Das Schema entspricht LSB (Linux Standards Base) und FHS (File System Hierarchy Standard).

► **ipf:** Die 64-Bit-Bibliotheken für `ia64` befinden sich in den standardmäßigen `lib`-Verzeichnissen. In solchen Fällen gibt es weder das Verzeichnis `lib64` noch das Verzeichnis `lib32`. `ia64` führt den 32-Bit-`x86`-Code unter einer Emulation aus. Eine Reihe von Basisbibliotheken wird unter `/emul/ia32-linux/lib` und `/emul/ia32-linux/usr/X11R6/lib` installiert. ◀

19.2 Software-Entwicklung

Alle 64-Bit-Architekturen unterstützen die Entwicklung von 64-Bit-Objekten. Der Grad der Unterstützung für die 32-Bit-Kompilierung ist von der Architektur abhängig. Dies sind die verschiedenen Implementierungsoptionen für die Toolkette von GCC (GNU Compiler-Sammlung) und Binutils, die den Assembler `as` und den Linker `ld` umfassen:

Doppelarchitektur-Compiler

Mit einer Doppelarchitektur-Entwicklungstoolkette können sowohl 32-Bit- als auch 64-Bit-Objekte erstellt werden. Das Kompilieren von 64-Bit-Objekten gehört bei fast allen Plattformen zum Standard. 32-Bit-Objekte können erstellt werden, wenn spezielle Flags verwendet werden. Diese spezielle Flag ist `-m32` für GCC (`-m32` zum Generieren von s390x-Binärdateien). Die Flags für die Binutils sind architekturabhängig, aber GCC überträgt die richtigen Flags an die Linker und Assembler. Zurzeit ist eine Doppelarchitektur-Entwicklungstoolkette für amd64 (unterstützt die Entwicklung von x86- und amd64-Anweisungen), s390x und ppc64 vorhanden. 32-Bit-Objekte werden in der Regel auf der ppc64-Plattform erstellt. Zur Erstellung von 64-Bit-Objekten muss das Flag `-m64` verwendet werden.

Keine Unterstützung

SUSE Linux Enterprise bietet keine Unterstützung für die direkte Entwicklung von 32-Bit-Software auf allen Plattformen. Zur Entwicklung von Anwendungen für x86 unter ia64 müssen Sie die entsprechende 32-Bit-Version von SUSE Linux Enterprise verwenden.

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

19.3 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` oder

`rpmname-x86` (für `ia64`), wenn die zweite Architektur eine 32-Bit-Architektur ist, oder `rpmname-64bit`, wenn die zweite Architektur eine 64-Bit-Architektur ist. Außerdem benötigen Sie die entsprechenden Header und Bibliotheken aus den `rpmname-devel`-Paketen und die Entwicklungsbibliotheken für die zweite Architektur aus `rpmname-devel-32bit` oder `rpmname-devel-64bit`.

Zum Kompilieren eines Programms, das `libaio` auf einem System verwendet, dessen zweite Architektur eine 32-Bit-Architektur ist (`x86_64` oder `s390x`), benötigen Sie beispielsweise die folgenden RPMs:

`libaio-32bit`
32-Bit-Laufzeitpaket

`libaio-devel-32bit`
Header und Bibliotheken für die 32-Bit-Entwicklung

`libaio`
64-Bit-Laufzeitpaket

`libaio-devel`
Header und Bibliotheken für die 64-Bit-Entwicklung

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. Beispiele für `s390x` mit `s390` als zweiter Architektur oder `ppc64` mit `ppc` als zweiter Architektur würden ähnlich aussehen. Dieses Beispiel gilt nicht für `ia64`-Systeme, wo Sie keine 32-Bit-Pakete erstellen.

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/X11R6/lib/
```

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

Ein Beispiel für einen `configure`-Aufruf zur Kompilierung einer nativen 32-Bit-Anwendung auf `x86_64`, `ppc64` oder `s390x` könnte wie folgt aussehen:

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

19.4 Kernel-Spezifikationen

Die 64-Bit-Kernel für `x86_64`, `ppc64` und `s390x` 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 müssen einige wenige Anwendungen, wie beispielsweise `lspci`, auf Nicht-ppc64-Plattformen als 64-Bit-Programme kompiliert werden, damit sie ordnungsgemäß funktionieren. Bei IBM-Systemen sind nicht alle `ioctl`s in der 32-Bit-Kernel-ABI verfügbar.

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

20

Das Booten eines Linux-Systems umfasst mehrere unterschiedliche Komponenten. In diesem Kapitel werden die zugrunde liegenden Prinzipien erläutert und die beteiligten Komponenten vorgestellt. Außerdem werden in diesem Kapitel das Konzept der Runlevel sowie die Systemkonfiguration von SUSE mit `sysconfig` vorgestellt.

20.1 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 Systemsteuerung vom BIOS an den Bootloader über. Wenn das BIOS Netzwerk-Bootting unterstützt, ist es auch möglich, einen Boot-Server zu konfigurieren, der den Bootloader bereitstellt. Auf x86-Systemen ist PXE-Boot erforderlich. Andere Architekturen verwenden meist das BOOTP-Protokoll, um den Bootloader abzurufen.
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 21, *Der Bootloader*](#) (S. 437). Bei einem Netzwerk-Boot fungiert das BIOS als Bootloader. Es erhält das Image für den Start vom Boot-Server und starten dann das System. Dieser Vorgang ist vollständig unabhängig von den lokalen Festplatten.

3. **Kernel und "initramfs"** Um die Systemsteuerung zu übergeben, lädt der Bootloader sowohl den Kernel als auch ein initiales RAM-basiertes Dateisystem (das *initramfs*) in den Arbeitsspeicher. Die Inhalte der Datei *initramfs* können direkt vom Kernel verwendet werden. *initramfs* enthält eine kleine ausführbare Datei namens "init", die das Einhängen des root-Dateisystems übernimmt. In früheren Versionen von SUSE® Linux wurden diese Tasks von "initrd" bzw. "linuxrc" durchgeführt. Weitere Informationen zu *initramfs* finden Sie unter [Abschnitt 20.1.1, „initramfs“](#) (S. 421). Wenn das System über keine lokale Festplatte verfügt, muss *initramfs* das Root-Dateisystem für den Kernel bereitstellen. Dies kann mithilfe eines Netzwerkblockgeräts, wie iSCSI oder SAN, bewerkstelligt werden, es kann aber auch NFS als Root-Gerät eingesetzt werden.
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 20.1.2, „init on initramfs“](#) (S. 422). Weitere Informationen zu *udev* finden Sie in [Kapitel 25, *Gerätemanagement über dynamischen Kernel mithilfe von udev*](#) (S. 515).
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 20.2, „Der init-Vorgang“](#) (S. 424).

20.1.1 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 wird von init durchgeführt.

Wenn in einem installierten System Hardwarekomponenten (Festplatten) ausgetauscht werden müssen und diese Hardware zur Boot-Zeit andere Treiber im Kernel erfordert, müssen Sie das initramfs aktualisieren. Dies erfolgt auf dieselbe Weise wie die Aktualisierung des Vorgängers, initrd, nämlich durch den Aufruf von `mkinitrd`. Durch das Aufrufen von `mkinitrd` ohne Argumente wird ein initramfs erstellt. Durch das Aufrufen von `mkinitrd -R` wird ein initrd erstellt. In SUSE® Linux Enterprise werden die zu ladenden Module durch die Variable `INITRD_MODULES` in `/etc/sysconfig/kernel` angegeben. Diese Variable wird nach der Installation automatisch auf den richtigen Wert gesetzt. Die Module werden genau in der Reihenfolge geladen, in der sie in `INITRD_MODULES` erscheinen. 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.

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.

20.1.2 `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 spezieller Block-Dateien

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 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 6.2, „Soft-RAID-Konfiguration“](#) (S. 142). Informationen zu LVM finden Sie in [Abschnitt 6.1, „LVM-Konfiguration“](#) (S. 133).

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 sich das Dateisystem auf einem Netzwerkblockgerät, wie iSCSI oder SAN, befindet, wird die Verbindung zum Speicherserver ebenfalls vom `initramfs` eingerichtet.

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 20.1.1, „initramfs“](#) (S. 421) 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 Namen der Module, die für den Boot-Vorgang benötigt werden, werden in `INITRD_MODULES` im 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.

20.2 Der init-Vorgang

Das Programm `init` ist der Prozess mit der ID 1. Er ist verantwortlich für die erforderliche Initialisierung des Systems. `init` wird direkt durch den Kernel gestartet und ist nicht anfällig für "Signal 9", das Prozesse normalerweise 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 20.2.1, „Runlevel“](#) (S. 424)). Diese Datei legt auch fest, welche Dienste und Daemons in den einzelnen Levels verfügbar sind. Je nach den Einträgen in `/etc/inittab` werden von `init` mehrere Skripts ausgeführt. Diese Skripts, die der Deutlichkeit halber als *init-Skripts* bezeichnet werden, befinden sich alle im Verzeichnis `/etc/init.d` (siehe [Abschnitt 20.2.2, „Init-Skripts“](#) (S. 427)).

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.

20.2.1 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. Siehe [Tabelle 20.1, „Verfügbare Runlevel“](#) (S. 424). 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.

Tabelle 20.1 *Verfügbare Runlevel*

Runlevel	Beschreibung
0	Systemstopp

Runlevel	Beschreibung
S	Einzelbenutzer-Modus; über die Boot-Eingabeaufforderung, nur mit der amerikanischen Tastaturbelegung verfügbar
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 der standardmäßige Runlevel bei allen SUSE Linux Enterprise-Standardinstallationen. Die Benutzer werden aufgefordert, sich mit einer grafischen Oberfläche anzumelden, oder der Standardbenutzer wird automatisch angemeldet. Wenn 3 der standardmäßige Runlevel ist, muss das X Window System wie unter [Kapitel 27, Das X Window-System](#) (S. 535) 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 den standardmäßigen 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 Computer neu starten.

Beim Ändern der Runlevel geschehen in der Regel zwei Dinge. Zunächst werden Stopp-Skripts des aktuellen Runlevel gestartet, die einige der für den aktuellen Runlevel wichtigen Programme schließen. Anschließend werden die Start-Skripts 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-Skripts des aktuellen Runlevel auf, für die es im neuen Runlevel keine Start-Skripts gibt. In diesem Beispiel sind dies alle Skripts, 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-Skripts 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.

20.2.2 Init-Skripts

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

Skripts, 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 ein Benutzer drückt `[Strg] + [Alt] + [Entf]`). Bei IBM-System z-Systemen ist dies nur während des Boot-Vorgangs der Fall oder wenn das sofortige Herunterfahren des Systems initiiert wird (Stromausfall oder „Signalstilllegung“). Die Ausführung dieser Skripts ist in `/etc/inittab` definiert.

Skripts, die indirekt von `init` ausgeführt werden

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

Sämtliche Skripts befinden sich im Verzeichnis `/etc/init.d`. Skripts, die während des Bootens ausgeführt werden, werden über symbolische Links aus `/etc/init.d/boot.d` aufgerufen. Skripts zum Ändern des Runlevel 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 Skripts, wenn diese in unterschiedlichen Runleveln verwendet werden. Da jedes Skript sowohl als Start- als auch als Stopp-Skript ausgeführt werden kann, müssen diese Skripts die Parameter `start` und `stop` verstehen. Die Skripts erkennen außerdem die Optionen `restart`, `reload`, `force-reload` und `status`. Diese unterschiedlichen Optionen werden in [Tabelle 20.2](#), „Mögliche `init`-Skript-Optionen“ (S. 428) erläutert. Die von `init` direkt ausgeführten Skripts verfügen nicht über diese Links. Sie werden unabhängig vom Runlevel bei Bedarf ausgeführt.

Tabelle 20.2 *Mögliche `init`-Skript-Optionen*

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

Mithilfe von Links in den einzelnen Runlevel-spezifischen Unterverzeichnissen können Skripts 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-Skripts sowie eine Erläuterung des Steuerskripts.

`boot`

wird 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 `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 Bildschirmdaten, 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 Skripts 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-Skripts des aktuellen Runlevel und die Start-Skripts des neu gewählten Runlevel auf.

Sie können Ihre eigenen Skripts erstellen und diese problemlos in das oben beschriebene Schema integrieren. Anweisungen zum Formatieren, Benennen und Organisieren benutzerdefinierter Skripts finden Sie in den Spezifikationen von LSB und auf den Manualpages von `init`, `init.d`, `chkconfig` und `insserv`. Weitere Informationen finden Sie zudem auf den Manualpages zu `startproc` und `killproc`.

WARNUNG: Fehlerhafte init-Skripts können das System stoppen

Bei fehlerhaften `init`-Skripts kann es dazu kommen, dass der Computer hängt. Diese Skripts sollten mit großer Vorsicht bearbeitet werden und, wenn möglich, gründlich in der Mehrbenutzer-Umgebung getestet werden. Einige hilfreiche Informationen zu `init`-Skripts finden Sie in [Abschnitt 20.2.1, „Runlevel“](#) (S. 424).

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. Siehe [Beispiel 20.1, „Ein minimaler INIT INFO-Block“](#) (S. 430).

Beispiel 20.1 *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 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 Skripts 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-Skripts 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 zum Erstellen der Links ein grafisches Werkzeug bevorzugen, verwenden Sie den von YaST zur Verfügung gestellten Runlevel-Editor wie in [Abschnitt 20.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 431) 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.

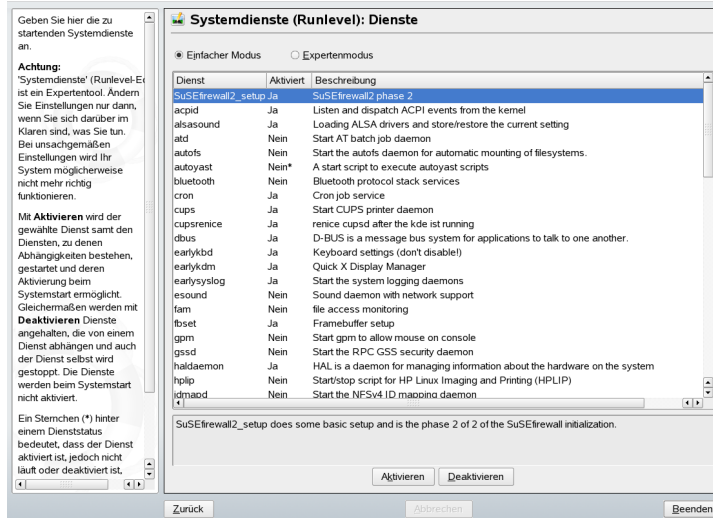
Diese Links dürfen nicht manuell festgelegt werden. Wenn der `INFO`-Block Fehler enthält, treten Probleme auf, wenn `insserv` zu einem späteren Zeitpunkt für einen anderen Dienst ausgeführt wird. Der manuell hinzugefügte Dienst wird bei der nächsten Ausführung von `insserv` entfernt.

20.2.3 Konfigurieren von Systemdiensten (Runlevel) mit YaST

Nach dem Starten 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 20.1 *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. Der standardmäßige Runlevel eines SUSE Linux Enterprise-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 einen Runlevel (wie unter [Tabelle 20.1](#), „[Verfügbare Runlevel](#)“ (S. 424) 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 *Beenden* 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.

20.3 Systemkonfiguration über `/etc/sysconfig`

Die Hauptkonfiguration von SUSE Linux Enterprise wird über die Konfigurationsdateien in `/etc/sysconfig` gesteuert. Die einzelnen Dateien in `/etc/sysconfig` werden nur von den Skripts gelesen, für die sie relevant sind. Dadurch wird gewährleistet, dass Netzwerkeinstellungen beispielsweise nur von netzwerkbezogenen Skripts analysiert werden. Viele andere Systemkonfigurationsdateien werden gemäß den Einstellungen in `/etc/sysconfig` generiert. Diese Task wird von `SuSEconfig` ausgeführt. Wenn Sie beispielsweise die Netzwerkkonfiguration ändern, nimmt `SuSEconfig` ggf. auch Änderungen an der Datei `/etc/host.conf` vor, da sie eine der für die Netzwerkkonfiguration relevanten Dateien ist. Dieses Konzept ermöglicht es, dass die meisten Konfigurationsarbeiten an einem zentralen Ort und nicht in verschiedenen Konfigurationsdateien an unterschiedlichen Stellen des Betriebssystems vorgenommen werden können.

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

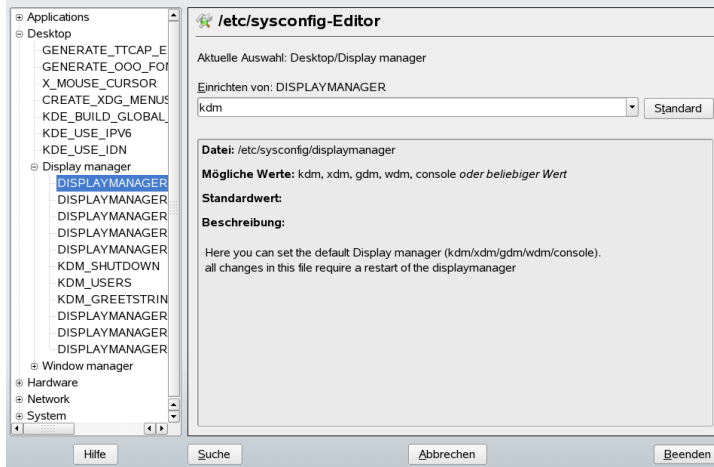
20.3.1 Ändern der Systemkonfiguration mithilfe des YaST-Editors "sysconfig"

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 20.2 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 Konfigurationsskripts nach dem Ändern der Variable ausgeführt und welche neuen Dienste als Folge dieser Änderung gestartet werden. YaST fordert Sie zur Bestätigung der Änderungen auf und zeigt an, welche Skripts ausgeführt werden, wenn Sie *Beenden* wählen. Außerdem können Sie die Dienste und Skripts 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.

20.3.2 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 `init 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 Befehl wie `init 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 SUSE® Linux Enterprise 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 20, *Booten und Konfigurieren eines Linux-Systems*](#) (S. 419). Ein Bootloader stellt die Schnittstelle zwischen Computer (BIOS) und dem Betriebssystem (SUSE Linux Enterprise) dar. 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 festgelegt. 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 „[Partitionstypen](#)“ (S. 47)). Die Partitionstabelle enthält Informationen zur Partitionierung der Festplatte und zu Dateisystemtypen. Das Betriebssystem benötigt diese Tabelle für die Verwaltung der Festplatte. Beim konventionellen generischen Code in MBR muss genau eine Partition als *aktiv* markiert sein. Die letzten zwei 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 Dateisystems anfänglich leer (mit Ausnahme des Dateisystems XFS). 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).

21.1 Auswählen eines Bootloaders

In SUSE Linux Enterprise 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 SUSE Linux Enterprise-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`.

21.2 Booten mit GRUB

GRUB (Grand Unified Bootloader) besteht aus zwei Stufen. Stufe 1 (stage1) besteht aus 512 Byte und 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 JFS, 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-Disk-Devices (vom BIOS erkannte Disketten, Festplatten, CD- oder DVD-Laufwerke) zugreifen. Daher erfordern Änderungen an der GRUB-Konfigurationsdatei (`menu.lst`) keine Neuinstallation des Boot-Managers mehr. Beim Booten des Systems liest GRUB die Menüdatei samt der aktuellen Pfade und Partitionsdaten zur 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 sämtliche Informationen zu Partitionen oder Betriebssystemen, die mit GRUB gebootet werden können. Wenn diese Angaben nicht zur Verfügung stehen, wird der Benutzer in der GRUB-Kommandozeile danach gefragt (siehe [„Ändern von Menü-Einträgen während des Bootvorgangs“](#) (S. 444)).

```
/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 über eine Art Eingabeaufforderung (siehe [„Ändern von Menü-Einträgen während des Bootvorgangs“](#) (S. 444)) Bootbefehle interaktiv

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

GRUB liegt in zwei Versionen vor: als Bootloader und als normales Linux-Programm im Verzeichnis `/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 eine 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.

21.2.1 Das GRUB-Bootmenü

Hinter dem grafischen Eröffnungsbildschirm mit dem Bootmenü steht die GRUB-Konfigurationsdatei `/boot/grub/menu.lst`, die alle Informationen zu allen Partitionen oder Betriebssystemen enthält, die über das Menü gebootet werden können.

GRUB liest bei jedem Systemstart 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 21.3](#), „Konfigurieren des Bootloaders mit YaST“ (S. 448) 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. 441) 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 neueres Linux-System mit erweiterten Hotplug-Funktionen verwendet wird, muss `initrd` mit einem separaten GRUB-Befehl angegeben werden, dessen einziges Argument der Pfad zu der 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. 442).

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/hda1.

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 21.2.2](#), „Die Datei `device.map`“ (S. 445).

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/hda5, eine Root-Partition unter /dev/hda7 und eine Windows-Installation unter /dev/hda1.

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
```

```

title linux
    kernel (hd0,4)/vmlinuz root=/dev/hda7 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/hda7 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/hda5`.

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` setzen, 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 verantwortlich SUSE Linux Enterprise. 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/hda7/`), 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`). Mittels `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 permanent editieren und dauerhaft speichern. Alternativ können Sie temporäre Änderungen interaktiv über die Bearbeitungsfunktion von GRUB vornehmen. Siehe „[Ändern von Menü-Einträgen während des Bootvorgangs](#)“ (S. 444).

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 Boot-Eingabeaufforderung zusätzliche Bootparameter eingeben. Um einzelne Menüeinträge direkt zu bearbeiten, drücken Sie die `[Esc]`-Taste, um den Eröffnungsbildschirm zu schließen und das textbasierte GRUB-Menü anzuzeigen, und 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 52.1, „US-Tastaturbelegung“](#) (S. 1003).

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/hda3 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.

21.2.2 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/hda
(hd1) /dev/sda
```

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. Ist das Linux-System erst gebootet, können Sie die Änderungen in der Datei `device.map` mithilfe des YaST Bootloader-Moduls oder eines Editors Ihrer Wahl dauerhaft übernehmen.

WICHTIG: SATA-Festplatten

Je nach Controller werden SATA-Festplatten als IDE-Geräte (`/dev/hd x`) oder SCSI-Geräte (`/dev/sd x`) erkannt.

Installieren Sie nach dem manuellen Bearbeiten von `device.map` GRUB mithilfe des folgenden Befehls `neu`. 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
```

21.2.3 Die Datei `"/etc/grub.conf"`

Die drittwichtigste Konfigurationsdatei von GRUB nach `menu.lst` und `device.map` ist `/etc/grub.conf`. 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

Der Befehl `grub` sollte mit dem Parameter `install` ausgeführt werden. `stage1` des Bootloaders sollte im erweiterten Partitionscontainer (`/grub/stage1 (hd0, 3)`) installiert werden. Dabei handelt es sich um eine etwas "esoterische" Lösung, aber in vielen Fällen funktioniert sie. `stage2` sollte in die Speicheradresse `0x8000 (/grub/stage2 0x8000)` geladen werden. Der letzte Eintrag (`(hd0, 4)/grub/menu.lst`) weist GRUB an, wo die Menüdatei zu finden ist.

21.2.4 Festlegen eines Bootpassworts

GRUB unterstützt schon vor dem Booten des Betriebssystems den Zugriff auf Dateisysteme. Dies bedeutet, dass Benutzer ohne `root`-Berechtigungen auf Dateien des Linux-Systems zugreifen können, auf die sie nach dem Booten keinen Zugriff haben. Um diese Zugriffe oder das Booten bestimmter Betriebssysteme zu verhindern, können Sie ein Bootpasswort festlegen.

WICHTIG: Bootpasswort und Eröffnungsbildschirm

Wenn Sie für GRUB ein Bootpasswort verwenden, wird der übliche Eröffnungsbildschirm nicht angezeigt.

Legen Sie als Benutzer `root` das Bootpasswort wie folgt fest:

- 1 Verschlüsseln Sie an der `root`-Eingabeaufforderung das Passwort mit Hilfe von `grub-md5-crypt`:

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

- 2 Fügen Sie die verschlüsselte Zeichenkette in den globalen Abschnitt der Datei `menu.lst` ein:

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$1S2dv/$JOYcdxIn7CJk9xShzzJVw/
```

Jetzt können GRUB-Befehle in der Boot-Eingabeaufforderung nur nach Drücken der Taste **P** und der Eingabe des Passworts ausgeführt werden. 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/hda7 vga=791
    initrd (hd0,4)/initrd
    lock
```

Nach dem Neubooten des Systems und der Auswahl des Linux-Eintrags im Bootmenü erscheint zunächst folgende Fehlermeldung:

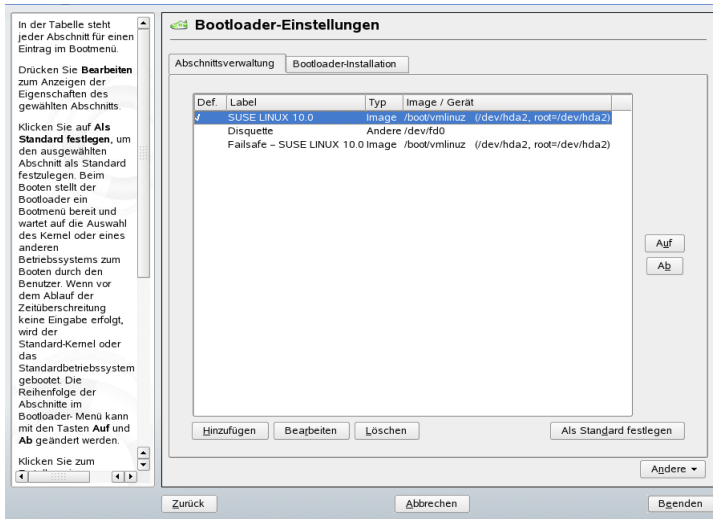
```
Error 32: Must be authenticated
```

Drücken Sie die **Eingabetaste**, um das Menü zu öffnen. Drücken Sie anschließend die Taste **P**, um die Eingabeaufforderung für das Passwort zu öffnen. Wenn Sie das Passwort eingegeben und die **Eingabetaste** gedrückt haben, sollte das ausgewählte Betriebssystem (in diesem Fall Linux) gebootet werden.

21.3 Konfigurieren des Bootloaders mit YaST

Mit dem YaST-Modul ist die Konfiguration des Bootloaders auf Ihrem SUSE Linux Enterprise-System am einfachsten. Wählen Sie im YaST-Kontrollzentrum *System* → *Konfiguration des Bootloaders*. Wie in [Abbildung 21.1](#), „[Konfigurieren des Bootloaders mit YaST](#)“ (S. 449) zeigt dies die aktuelle Bootloader-Konfiguration des Systems und ermöglicht Ihnen, Änderungen vorzunehmen.

Abbildung 21.1 Konfigurieren des Bootloaders mit YaST



Auf der Registerkarte *Abschnittsverwaltung* können Sie die Bootloader-Abschnitte für die einzelnen Betriebssysteme bearbeiten, ändern und löschen. Klicken Sie zum Hinzufügen einer Option auf *Hinzufügen*. Wenn Sie den Wert einer bestehenden Option ändern möchten, wählen Sie ihn mit der Maus aus und klicken Sie auf *Bearbeiten*. Wenn Sie eine bestehende Option überhaupt nicht verwenden möchten, wählen Sie sie aus und klicken Sie auf *Löschen*. Wenn Sie nicht mit den Bootloader-Optionen vertraut sind, lesen Sie zunächst [Abschnitt 21.2, „Booten mit GRUB“](#) (S. 438).

Verwenden Sie die Registerkarte *Bootloader-Installation*, um die Einstellungen in Bezug auf Typ, Speicherort und erweiterte Bootloader-Einstellungen anzuzeigen und zu ändern.

21.3.1 Bootloader-Typ

Den Bootloader-Typ können Sie unter *Bootloader-Installation* festlegen. In SUSE Linux Enterprise wird standardmäßig der Bootloader GRUB verwendet. Gehen Sie wie folgt vor, wenn Sie LILO verwenden möchten:

Prozedur 21.1 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 SUSE Linux Enterprise nicht verfügbar.
 - Auf Festplatte gespeicherte Konfiguration einlesen
Lädt Ihre eigene Datei `/etc/lilo.conf`. Diese Aktion ist während der Installation von SUSE Linux Enterprise nicht verfügbar.
- 4 Klicken Sie auf *OK*, um die Änderungen zu speichern.
- 5 Klicken Sie im Hauptdialogfeld auf *Beenden*, 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.

21.3.2 Speicherort des Bootloaders

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

Prozedur 21.2 *Speicherort des Bootloaders ändern*

- 1 Wählen Sie die Registerkarte *Bootloader-Installation* und anschließend eine der folgenden Optionen für *Speicherort des Bootloaders*:

Master Boot Record von /dev/hdX

Dadurch wird der Bootloader im MBR einer Festplatte installiert. X gibt die Festplatte an, beispielsweise a, b, c oder d:

```
hda => ide0 master
hdb => ide0 slave
hdc => ide1 master
hdd => ide1 slave
```

Bootsektor der Boot-Partition /dev/hdXY

Der Bootsektor der Partition /boot. Dies ist der Standard für die Option, wenn Sie auf Ihrer Festplatte mehrere Betriebssysteme installiert haben. Das Y steht für die Partition (1, 2, 3, 4, 5 usw.), wie in:

```
/dev/hda1
```

Bootsektor der Root-Partition /dev/hdXY

Der Bootsektor der / (root)-Partition. Solange keine /boot-Partition erforderlich ist oder der MBR verwendet werden muss, ist dies der bevorzugte Standardwert.

Andere

Mit dieser Option können Sie den Speicherort des Bootloaders manuell angeben.

- 2 Klicken Sie zum Anwenden der Einstellungen auf *Beenden*.

21.3.3 Standardsystem

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

Prozedur 21.3 *Standardsystem einrichten*

- 1 Öffnen Sie die Registerkarte *Abschnittsverwaltung*.
- 2 Wählen Sie das gewünschte System in der Liste aus.

- 3 Klicken Sie auf *Als Standard festlegen*.
- 4 Klicken Sie auf *Beenden*, um die Änderungen zu aktivieren.

21.3.4 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 21.4 *Ändern des Bootloader-Zeitlimits*

- 1 Öffnen Sie die Registerkarte *Bootloader-Installation*.
- 2 Klicken Sie auf *Bootloader-Optionen*.
- 3 Aktivieren Sie *Boot-Modus*.
- 4 Ändern Sie unter *Boot-Modus* den Wert für *Beim Systemstart*, indem Sie einen neuen Wert eingeben, mit der Maus auf den entsprechenden Pfeil klicken oder die Pfeiltasten der Tastatur verwenden.
- 5 Klicken Sie auf *OK*.
- 6 Klicken Sie auf *Beenden*, um die Änderungen zu speichern.

Das Bootmenü sollte dauerhaft ohne Zeitlimit angezeigt werden, wenn *Bootvorgang nach Zeitüberschreitung fortsetzen* deaktiviert ist.

21.3.5 Sicherheitseinstellungen

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

Prozedur 21.5 *Festlegen eines Bootloader-Passworts*

- 1 Öffnen Sie die Registerkarte *Bootloader-Installation*.

- 2 Klicken Sie auf *Bootloader-Optionen*.
- 3 Aktivieren Sie unter *Passwortschutz* die Option *Bootloader durch Passwort schützen* und geben Sie ein Passwort an.
- 4 Klicken Sie auf *OK*.
- 5 Klicken Sie auf *Beenden*, um die Änderungen zu speichern.

21.3.6 Festplattenreihenfolge

Wenn Ihr Computer mehrere Festplatten hat, können Sie die Bootsequenz der Festplatten so festlegen, dass sie dem BIOS-Setup des Computers entsprechen (siehe [Abschnitt 21.2.2, „Die Datei "device.map"“](#) (S. 445)). Gehen Sie hierfür wie folgt vor:

Prozedur 21.6 *Festlegen der Festplattenreihenfolge*

- 1 Öffnen Sie die Registerkarte *Bootloader-Installation*.
- 2 Klicken Sie auf *Details zur Bootloader-Installation*.
- 3 Ändern Sie bei mehreren aufgeführten Festplatten deren Reihenfolge mit einem Klick auf *Auf* oder *Ab*.
- 4 Klicken Sie auf *OK*, um die Änderungen zu speichern.
- 5 Klicken Sie auf *Beenden*, um die Änderungen zu speichern.

Mithilfe dieses Moduls können Sie auch den Master Boot Record durch generischen Code ersetzen, mit dem die aktive Partition gebootet wird. Klicken Sie unter *Aktualisierung der Festplattenbereiche* auf *MBR durch generischen Code ersetzen*. Wählen Sie *Bootloader-Partition aktivieren*, um die Partition zu aktivieren, die den Bootloader enthält. Klicken Sie auf *Beenden*, um die Änderungen zu speichern.

21.4 Deinstallieren des Linux-Bootloaders

Mit YaST können Sie den Linux-Bootloader deinstallieren und den Zustand des MBR wiederherstellen, der vor der Installation von Linux vorlag. 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* → *Konfiguration des Bootloaders*). Wählen Sie im ersten Dialogfeld *Zurücksetzen* → *MBR von Festplatte wiederherstellen* und schließen Sie das Dialogfeld mit *Beenden*.

21.5 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 eines bootfähigen CD-ROM mit GRUB ist lediglich eine spezielle Form von *stage2* namens *stage2_eltorito* erforderlich sowie, optional, eine benutzerdefinierte Datei *menu.lst*. Die klassischen Dateien *stage1* und *stage2* sind nicht erforderlich.

Prozedur 21.7 Erstellen von Boot-CDs

- 1 Erstellen Sie ein Verzeichnis, in dem das ISO-Image erstellt werden soll, beispielsweise:

```
cd /tmp
mkdir iso
```

- 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 `/boot/message` nach `iso/boot/`:

```
cp /boot/vmlinuz iso/boot/  
cp /boot/initrd iso/boot/  
cp /boot/message iso/boot/  
cp /boot/grub/menu.lst iso/boot/grub
```

- 4** Passen Sie die Pfadeinträge in `iso/boot/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 `(hd*)` aufgeführt sind, mit dem Gerätenamen des CD-ROM-Laufwerks, das mit `(cd)` angegeben wird:

```
gfxmenu (cd)/boot/message  
timeout 8  
default 0  
  
title Linux  
    kernel (cd)/boot/vmlinuz root=/dev/hda5 vga=794 resume=/dev/hda1 \  
    splash=verbose showopts  
    initrd (cd)/boot/initrd
```

- 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 iso
```

- 6** Schreiben Sie die so erstellte Datei namens `grub.iso` unter Verwendung Ihres bevorzugten Dienstprogramms auf eine CD.

21.6 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 den Kernel-Parameter `splash=0` zur Konfiguration des Bootloaders hinzu. Weitere Informationen hierzu finden Sie in [Kapitel 21, Der Bootloader](#) (S. 437). 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.

21.7 Fehlerbehebung

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://portal.suse.de/sdb/en/index.html> beschrieben. Sollte Ihr spezifisches Problem nicht in dieser Liste enthalten sein, empfehlen wir, in der Suchmaske der Support-Datenbank unter <https://portal.suse.com/PM/page/search.pm> nach den Stichworten *GRUB*, *Booten* 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 und JFS

Obwohl technisch möglich, ist eine Kombination von GRUB mit JFS problematisch. Erstellen Sie in solchen Fällen eine separate Bootpartition (`/boot`) und formatieren Sie sie mit Ext2. Installieren Sie anschließend GRUB auf dieser Partition.

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 in solchen Fällen aus, wenn Linux auf einer zusätzlichen Festplatte im System installiert wurde, diese aber nicht im BIOS registriert wurde. Der erste Teil des Bootloaders *stage1* wird korrekt gefunden und geladen, aber die zweite Stufe *stage2* wird 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 nimmt GRUB beispielsweise `/dev/hda` als `hd0` und `/dev/sda` als `hd1` an, wobei aber 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. Anschließend überprüfen Sie 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. Dazu 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.

21.8 Weitere 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 „GRUB“ als Suchwort in der Supportdatenbank unter <http://portal.suse.de/sdb/en/index.html> eingeben.

Sonderfunktionen in SUSE Linux Enterprise

22

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 landes-spezifischen Einstellungen (I18N und L10N).

22.1 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. Manualpages und info-Seiten sind hilfreiche Informationsquellen zu Befehlen, sind jedoch nicht immer verfügbar. GNU Emacs ist ein beliebter konfigurierbarer Texteditor.

22.1.1 Das Paket `bash` und `/etc/profile`

Bash ist die Standard-Shell in SUSE® Linux Enterprise. 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`

In `~/.profile` oder in `~/.bashrc` können benutzerdefinierte Einstellungen vorgenommen werden. Um die richtige Verarbeitung der Dateien zu gewährleisten, müssen die Grundeinstellungen aus `/etc/skel/.profile` oder `/etc/skel/.bashrc` in das Home-Verzeichnis des Benutzers kopiert werden. Es empfiehlt sich, die Einstellungen aus `/etc/skel` nach einer Aktualisierung zu kopieren. Führen Sie die folgenden Shell-Befehle aus, um den Verlust persönlicher Einstellungen zu vermeiden:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Kopieren Sie anschließend die persönlichen Einstellungen erneut aus den `*.old`-Dateien.

22.1.2 Das cron-Paket

Wenn Sie Befehle regelmäßig und automatisch im Hintergrund zu bestimmten Zeitpunkten ausführen möchten, verwenden Sie in der Regel das Werkzeug `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 22.1](#), „Eintrag in `/etc/crontab`“ (S. 460), 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 22.1 Eintrag in `/etc/crontab`

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```


`/etc/crontab` kann nicht durch Aufrufen des Befehls `crontab -e` bearbeitet werden. Die Datei muss direkt in einem Editor geladen, geändert und dann gespeichert werden.

Einige Pakete installieren Shell-Skripts 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 von der Haupttabelle (`/etc/crontab`) alle 15 Minuten ausgeführt. Hiermit wird gewährleistet, dass vernachlässigte Prozesse zum richtigen Zeitpunkt ausgeführt werden können.

Zum Ausführen der Skripts `hourly`, `daily` oder von anderen Skripts für regelmäßige Wartungsarbeiten zu benutzerdefinierten Zeitpunkten entfernen Sie regelmäßig die Verwendung der Zeitstempeldateien mithilfe von `/etc/crontab`-Einträgen (siehe [Beispiel 22.2](#), „`/etc/crontab`: Entfernen von Zeitstempeldateien“ (S. 461), wodurch `hourly` vor jeder vollen Stunde und `daily` einmal täglich um 2.14 Uhr entfernt wird usw.).

Beispiel 22.2 `/etc/crontab`: Entfernen von 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
```

Die täglichen Systemwartungsaufträge wurden 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`.

22.1.3 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`. Mit der Spezifikation `include` werden die zusätzlich zu lesenden Dateien hauptsächlich konfiguriert. Mit SUSE® Linux Enterprise wird sichergestellt, dass Programme, die Protokolldateien erstellen, einzelne Konfigurationsdateien in `/etc/logrotate.d` installieren. Solche Programme sind beispielsweise im Lieferumfang der Pakete `apache2` (`/etc/logrotate.d/apache2`) und `syslogd` (`/etc/logrotate.d/syslog`) enthalten.

Beispiel 22.3 *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.

22.1.4 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 `find-locate`. Der Prozess `updatedb` wird jeden Abend etwa 15 Minuten nach dem Booten des Systems gestartet.

22.1.5 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 22.1, „ulimit: Festlegen von Ressourcen für Benutzer“](#) (S. 463) aufgeführten Optionen.

Tabelle 22.1 *ulimit: Festlegen 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 22.4 *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`.

WICHTIG

`ulimit`-Direktiven werden nicht von allen Shells unterstützt. PAM (beispielsweise `pam_limits`) bietet umfassende Anpassungsmöglichkeiten, wenn Sie Einstellungen für diese Beschränkungen vornehmen müssen.

22.1.6 Der Befehl "free"

Der Befehl `free` ist leicht irreführend, wenn Sie herausfinden möchten, wie viel Arbeitsspeicher zurzeit verwendet wird. Die entsprechenden Informationen finden Sie in `/proc/meminfo`. Heute müssen sich Benutzer, die ein modernes Betriebssystem wie Linux verwenden, in der Regel kaum Gedanken über den Arbeitsspeicher machen. Das Konzept des *verfügbaren Arbeitsspeichers* geht auf Zeiten vor der einheitlichen Speicherverwaltung zurück. Bei Linux gilt der Grundsatz *freier Arbeitsspeicher ist schlechter Arbeitsspeicher*. Daher wurde bei Linux immer darauf geachtet, die Caches auszugleichen, ohne freien oder nicht verwendeten Arbeitsspeicher zuzulassen.

Der Kernel verfügt nicht direkt über Anwendungs- oder Benutzerdaten. Stattdessen verwaltet er Anwendungen und Benutzerdaten in einem *Seiten-Cache*. Falls nicht mehr genügend Arbeitsspeicher vorhanden ist, werden Teile auf der Swap-Partition oder in Dateien gespeichert, von wo aus sie mithilfe des Befehls `mmap` abgerufen werden können. (siehe `man mmap`).

Der Kernel enthält zusätzlich andere Caches, wie beispielsweise den *slab-Cache*, in dem die für den Netzwerkzugriff verwendeten Caches gespeichert werden. Hiermit können die Unterschiede zwischen den Zählern in `/proc/meminfo` erklärt werden. Die meisten, jedoch nicht alle dieser Zähler können über `/proc/slabinfo` aufgerufen werden.

22.1.7 Die Datei `/etc/resolv.conf`

Die Auflösung von Domännennamen erfolgt über die Datei `/etc/resolv.conf`. Informationen hierzu erhalten Sie in [Kapitel 34, Domain Name System \(DNS\)](#) (S. 681).

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.

22.1.8 Manualpages und Info-Seiten

Für einige GNU-Anwendungen (wie beispielsweise `tar`) sind keine Manualpages 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 durch Eingabe von `info info`. Info-Seiten können durch Eingabe von `emacs -f info` mit Emacs oder mit `info` direkt in einer Konsole angezeigt werden. Sie können auch `tkinfo`, `xinfo` oder das Hilfesystem von SUSE zum Anzeigen von info-Seiten verwenden.

22.1.9 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.

In `.gnu-emacs` wird die Datei `~/ .gnu-emacs-custom` als `custom-file` definiert. Wenn Benutzer in Emacs Einstellungen mit den `customize`-Optionen vornehmen, werden die Einstellungen in `~/ .gnu-emacs-custom` gespeichert.

Bei SUSE® Linux Enterprise 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-Unterstützung.
- `emacs-nox`: das Programm *ohne* X11-Unterstützung.
- `emacs-info`: Onlinedokumentation im Info-Format.
- `emacs-el`: Die nicht kompilierten Bibliotheksdateien in Emacs Lisp. Sie sind während der Laufzeit nicht erforderlich.
- Falls erforderlich, können mehrere Zusatzpakete installiert werden:
`emacs-auctex` (für LaTeX), `psgml` (für SGML und XML), `gnuserv` (für den Client- und Serverbetrieb) und andere.

22.2 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 Tasten `[Alt] + [F1]`

bis **Alt** + **F6** können Sie zwischen diesen 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 Tasten **Strg** + **Alt** + **F1** bis **Strg** + **Alt** + **F6**. Mit **Alt** + **F7** kehren Sie zu X zurück.

22.3 Tastaturzuordnung

Um die Tastaturzuordnung der Programme zu standardisieren, wurden Änderungen an folgenden Dateien vorgenommen:

```
/etc/inputrc
/usr/X11R6/lib/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/X11R6/lib/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 von SUSE® Linux Enterprise enthalten sind, sollten an diese Standards angepasst werden.

Unter X kann auf die Compose-Taste (Multikey) über **Strg** + **Umschalt** (rechts) zugegriffen werden. Siehe auch den entsprechenden Eintrag in `/usr/X11R6/lib/X11/Xmodmap`.

Weitere Einstellungen sind möglich mit der X-Tastaturerweiterung (XKB) Diese Erweiterung wird auch von den Desktop-Umgebungen GNOME (gswitchit) und KDE (kxkb) verwendet.

TIPP: Weitere Informationen

Informationen zu XKB finden Sie in `/etc/X11/xkb/README` und den dort aufgeführten Dokumenten.

Detaillierte Informationen zur Eingabe von Chinese, Japanisch und Koreanisch (CJK) finden Sie auf der Seite von Mike Fabian: <http://www.suse.de/~mfabian/suse-cjk/input.html>.

22.4 Sprach- und länderspezifische Einstellungen

SUSE® Linux Enterprise wurde zu einem großen Teil internationalisiert und kann flexibel an lokale Gegebenheiten angepasst werden. Anders ausgedrückt: Die Internationalisierung (*I18N*) ermöglicht spezielle Lokalisierungen (*L10N*). Die Abkürzungen *I18N* und *L10N* wurden von den ersten und letzten Buchstaben der englischsprachigen Begriffe und der Anzahl der dazwischen stehenden ausgelassenen Wörter abgeleitet.

Die Einstellungen werden mit `LC_`-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dies bezieht sich nicht nur auf die *native Sprachunterstützung*, sondern auch auf die Kategorien *Meldungen* (Sprache) *Zeichensatz*, *Sortierreihenfolge*, *Uhrzeit und Datum*, *Zahlen* und *Währung*. Diese Kategorien können direkt über eine eigene Variable oder indirekt mit einer Master-Variable in der Datei `language` festgelegt werden (weitere Informationen erhalten Sie auf der Manualpage zu `locale`).

```
RC_LC_MESSAGES, RC_LC_CTYPE, RC_LC_COLLATE, RC_LC_TIME,  
RC_LC_NUMERIC, RC_LC_MONETARY
```

Diese Variablen werden ohne das Präfix `RC_` an die Shell weitergegeben und stehen für die aufgelisteten Kategorien. Die betreffenden Shell-Profile werden unten aufgeführt. Die aktuelle Einstellung lässt sich mit dem Befehl `locale` anzeigen.

```
RC_LC_ALL
```

Sofern diese Variable festgelegt ist, setzt Sie die Werte der bereits erwähnten Variablen außer Kraft.

RC_LANG

Falls keine der zuvor genannten Variablen festgelegt ist, ist dies das Fallback. Standardmäßig ist in SUSE Linux 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 20.3.1](#), „Ändern der Systemkonfiguration mithilfe des YaST-Editors `sysconfig`“ (S. 434)) 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>]
```

22.4.1 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> and <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.

22.4.2 Locale-Einstellungen in `~/ .i18n`

Wenn Sie nicht mit den Systemeinstellungen für Locale zufrieden sind, ändern Sie die Einstellungen in `~/ .i18n`. 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`.

22.4.3 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 tritt auf, wenn `LANG` auf einen aus zwei Buchstaben bestehenden Sprachcode wie `de`, gesetzt ist, in der 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.

22.4.4 Weitere 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`.

Virtual Machine Server

SUSE Linux umfasst eine Virtual Machine Technologie, die einem einzelnen Computer die Ausführung als *Virtual Machine Server* (VM-Server) ermöglicht. Ein VM-Server kann als Host für ein oder mehrere *virtuelle Computer* (VMs) fungieren.

ANMERKUNG

Dieser Abschnitt enthält einführende Informationen sowie grundlegende Anleitungen für die Einrichtung eines Virtual Machine Servers. Aktuelle und umfassende Informationen zur Virtual Machine Technologie finden Sie unter Novell VM-Server-Technologie [http://www.novell.com/documentation/technology/vm_server].

Inhalt dieses Abschnitts:

- [Abschnitt 23.1, „Systemvoraussetzungen“](#) (S. 474)
- [Abschnitt 23.2, „Vorteile von virtuellen Computern“](#) (S. 476)
- [Abschnitt 23.3, „Terminologie“](#) (S. 476)
- [Abschnitt 23.4, „Virtual Machine Modi“](#) (S. 477)
- [Abschnitt 23.5, „Virtual Machine Server“](#) (S. 478)
- [Abschnitt 23.6, „Einrichten des Virtual Machine Servers“](#) (S. 481)
- [Abschnitt 23.7, „Erstellen virtueller Computer“](#) (S. 484)

- [Abschnitt 23.8, „Verwalten virtueller Computer“](#) (S. 485)

23.1 Systemvoraussetzungen

VM-Server-Komponente	Voraussetzung
Softwarepakete	<p>VM-Server erfordert die folgenden Softwarepakete und deren Abhängigkeiten.</p> <ul style="list-style-type: none"> • kernel-xen • xen • xen-tools • xen-tools-ioemu (Dieses Paket wird für den Hardware-gestützten Vollvirtualisierungsmodus benötigt.) • kernel-xenpae (Bei Verwendung anstelle von kernel-xen ermöglicht dieses Paket 32-Bit-Computern den Einsatz physischer Adresserweiterungen für den Zugriff auf Arbeitsspeicherbereichen über 4 GB.)
Computertyp und CPU	<p>VM-Server kann VM-fähige Betriebssysteme auf Computern mit x86 32-Bit- oder 64-Bit-Architekturen ausführen.</p> <p>VM-Server kann VMs im vollständig virtualisierten Modus nur auf Computern ausführen, die die hardwaregestützte Virtualisierung unterstützen, wie beispielsweise Intel VT oder AMD Virtualization.</p>
Erforderlicher Arbeitsspeicher	<p>Fügen Sie dem Arbeitsspeicher, der für SUSE Linux benötigt wird, den erforderlichen Arbeitsspeicher für alle geplanten virtuellen Computer hinzu.</p>

VM-Server-Komponente	Voraussetzung
Erforderlicher Festplattenspeicher	Je nach Anforderung der einzelnen VMs kann zusätzlich zum erforderlichen Speicherplatz für SUSE Linux weiterer Festplattenspeicher erforderlich sein.
Betriebssysteme für VMs	<p>VM-Server können für die folgenden VM-fähigen Betriebssysteme im paravirtualisierten Modus als Host fungieren:</p> <ul style="list-style-type: none"> • SUSE Linux 10.1 • SUSE Linux Enterprise Server 10 • SUSE Linux Enterprise Desktop 10 <p>Durch die hardwaregestützte Virtualisierung stellt der VM-Server eine vollständig virtualisierte Umgebung bereit, die als Host für die am häufigsten verwendeten Betriebssysteme fungieren kann.</p> <p>Wenn der VM-Server kernel-xenpae für den Zugriff auf Arbeitsspeicherbereiche über 4 GB ausführt, muss das VM-Betriebssystem ebenfalls für PAE aktiviert werden.</p>
Gerätetreiber für die VM-Umgebung	<p>Auf Hardware-gestützten virtuellen Computern werden die folgenden Geräte emuliert; sie erfordern systemeigene BS-Treiber:</p> <ul style="list-style-type: none"> • Netzwerkkarte: AMD PCNet, NE2000 • Laufwerk: IDE • Grafikkarte: VESA-konformer VGA, Cirrus Logic GD5446 • Eingabegerät: PS/2-Maus und -Tastatur • Audio: Creative Sound Blaster 16, ENSONIQ ES1370

23.2 Vorteile von virtuellen Computern

Die aktuellen Verbesserungen auf dem Gebiet der Virtualisierungstechnologie fördern die Implementierung von virtuellen Computern in Datencenter- und Filialbüroumgebungen. Einsatzmöglichkeiten für virtuelle Computer:

- Konsolidierung der Server im Datencenter.

Server, die im Datencenter ausgeführt werden, sind häufig nicht ausgelastet. Eine Studie hat ergeben, dass die genutzte Prozessorzeit bei Datencentern im Schnitt nur 12 Prozent der Kapazität entspricht. Durch die Konsolidierung mehrerer physischer Server zu VMs, die auf einem Virtual Machine Server ausgeführt werden, können Datencenter die Kosten für Hardware, Wartung und Stromversorgung senken.

- Konsolidierung und Hosting von veralteten Anwendungen.
- Isolierung von Anwendungen auf demselben physischen Server.
- Gleichmäßige Verteilung der Datenlast auf die Datencenter-Ressourcen.
- Anwendungsportabilität und -flexibilität über verschiedene Hardwareplattformen hinweg.

23.3 Terminologie

Die folgenden Erläuterungen sollen Ihnen dabei helfen, dieses Dokument und die Virtualisierungstechnologie zu verstehen.

- Der Begriff *Virtual Machine* (VM, virtueller Computer) bezeichnet eine Instanz einer virtuellen Hardware-Umgebung sowie das Betriebssystem, das auf dieser virtuellen Hardware-Instanz ausgeführt wird. Ein virtueller Computer kann jede Art von Software ausführen, beispielsweise einen Server, Client oder Desktop. Er wird häufig auch als Gast, Domäne U, domU oder unprivilegierte Domäne bezeichnet.

- Der Begriff *Virtual Machine Server* oder *VM-Server* bezeichnet einen physischen Computer und Software, die zusammen für das Hosting, die Erstellung und die Steuerung virtueller Computer eingesetzt werden. Er wird manchmal auch als Host, Domäne 0 oder privilegierte Domäne bezeichnet.
- Der Begriff *Virtual Machine Monitor* (VMM) bezeichnet die Softwareschicht, die SUSE Linux das Hosting virtueller Computer ermöglicht. Er wird manchmal auch als Hypervisor bezeichnet. Der VMM umfasst Software, die von der Xen Open-Source-Community entwickelt und verwaltet wird. Der VMM wird für eine vollständige Hardware-Emulation durch die QEMU-Software erweitert.
- Der Begriff *VM-fähig* bezieht sich auf ein Betriebssystem, das für die VM-Umgebung optimiert ist. Ein solches Betriebssystem wird häufig auch als paravirtualisierter, Xen-fähiger, modifizierter oder optimierter Gast bezeichnet.
- Betriebssysteme, die nicht für die VM-Umgebung optimiert sind, werden häufig als eingeschweißter, unmodifizierter oder vollständig virtualisierter Gast bzw. als Gast "von der Stange" bezeichnet.

23.4 Virtual Machine Modi

Der VM-Server hostet virtuelle Computer mit Betriebssystemen in zwei verschiedenen Modi: *vollständig virtualisiert* oder *paravirtualisiert*.

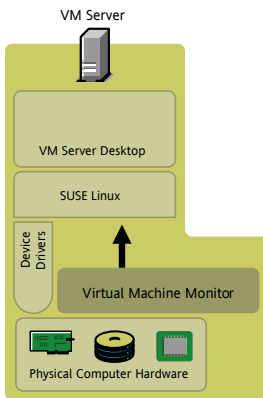
- **Vollständig virtualisiert:** Vollständige Emulation aller Hardwaregeräte. Obwohl hierfür spezielle Computerhardware erforderlich ist, können die meisten Betriebssysteme im vollständig virtualisierten Modus ausgeführt werden, da der VMM alle Computergeräte emuliert, um das Betriebssystem glauben zu lassen, dass es über exklusiven Zugriff auf einen vollständigen Computer verfügt. Diese vollständige Emulation der Computerhardware beansprucht mehr CPU-Ressourcen des VM-Servers. Daher läuft ein Betriebssystem im vollständig virtualisierten Modus langsamer.
- **Paravirtualisiert:** Selektive Emulation von Hardwaregeräten. Ein Betriebssystem, das für den VMM optimiert ist, wird als *VM-fähig* bezeichnet und kann im paravirtualisierten Modus ausgeführt werden. Der paravirtualisierte Modus erfordert keine vollständige Emulation und bedeutet daher weniger Verwaltungsaufwand. VM-fähige Betriebssysteme erfordern beispielsweise keine emulierte Grafikkarte, sodass der VM-Server keine Videodaten emulieren muss. Folglich benötigt ein Betriebs-

system im paravirtualisierten Modus weniger CPU-Ressourcen und verfügt über eine bessere Leistung. Darüber hinaus wird keine spezielle Computerhardware benötigt.

23.5 Virtual Machine Server

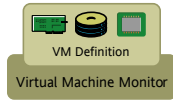
Der Virtual Machine Monitor (VMM) wird zwischen der Serverhardware und dem Betriebssystem-Kernel von SUSE Linux ausgeführt. Wenn der Computer bootet, wird zuerst der VMM geladen und dann der VM-Server im *privilegierten Modus* gestartet. Dies bewirkt, dass der VM-Server virtuelle Computer erstellen und steuern kann sowie über direkten Zugriff auf die Computerhardware verfügt. Der VM-Server wird mit systemeigenen Gerätetreibern konfiguriert, die mit den tatsächlichen Geräten des Computers übereinstimmen. Wenn der Computer beispielsweise über eine physische e1000-Netzwerkkarte verfügt, wird der VM-Server für das Laden und Ausführen des SUSE Linux-Gerätetreibers für die e1000-Karte konfiguriert.

Abbildung 23.1 Virtual Machine Server und Gerätetreiber



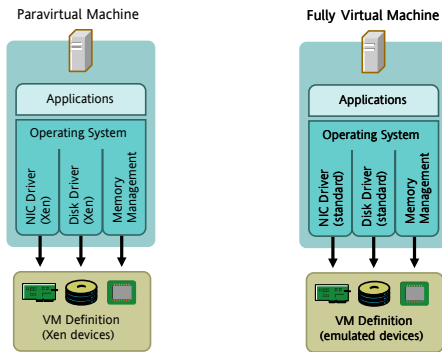
Virtuelle Computer werden auf dem VM-Server definiert und gespeichert. Die Definitionen (*VM-Definitionen* genannt) werden in einer Konfigurationsdatei im Verzeichnis `/etc/xen/vm/VM-Name` gespeichert. Die Konfigurationsdatei definiert die virtuellen Ressourcen, wie CPU, Arbeitsspeicher, Netzwerkkarte und Block-Geräte, die das Betriebssystem sieht, wenn es auf dem virtuellen Computer installiert und gebootet wird.

Abbildung 23.2 Virtual Machine Definitionen und Virtual Machine Monitor



Sowohl im vollständig virtualisierten als auch im paravirtualisierten Modus verwendet das Betriebssystem eines virtuellen Computers Gerätetreiber für die Interaktion mit dem VMM. Im vollständig virtualisierten Modus verwendet das Betriebssystem systemeigene BS-Gerätetreiber für einen Standardsatz emulierter Geräte, wie beispielsweise eine AMD PCNet- oder NE2000-Netzwerkkarte, ein IDE-Laufwerk und eine VGA-Grafikkarte. Im paravirtualisierten Modus verfügen die VM-fähigen Betriebssysteme über spezielle Gerätetreiber (*Xen-Treiber* genannt) für die Kommunikation mit den physischen Geräten des Computers über den VMM und den VM-Server.

Abbildung 23.3 VM-Gerätetreiber

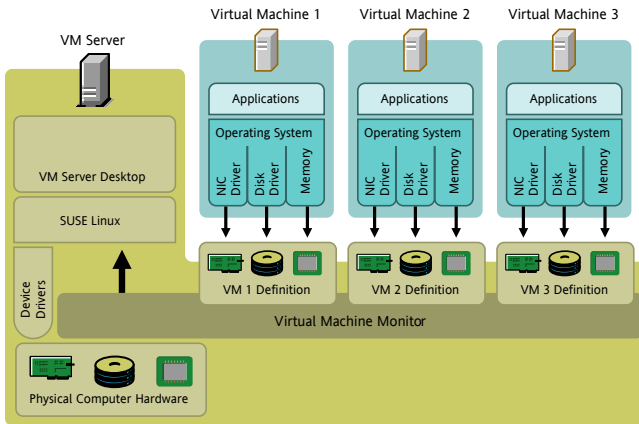


Wenn beispielsweise das Betriebssystem eines virtuellen Computers, das im vollständig virtualisierten Modus ausgeführt wird, eine Datei auf seiner virtuellen 20-GB-Festplatte speichern soll, übergibt das Betriebssystem die Anforderung über den Gerätetreiber an den VMM. Der VMM versteht, auf welchen Teil der physischen 500-GB-Festplatte der virtuelle Computer Zugriff hat und übergibt entsprechende Anweisungen an den VM-Server. Der VM-Server greift auf das Festplattenlaufwerk zu und schreibt die Datei an der vordefinierten Position auf die 500-GB-Festplatte.

Abhängig von Ihren Anforderungen an das Computersystem und von den verfügbaren Computerressourcen kann eine beliebige Anzahl virtueller Computer erstellt und gleichzeitig auf dem VM-Server ausgeführt werden. Das Betriebssystem jedes virtuellen Computers interagiert unabhängig von den anderen mit dem VMM und der VM-Ser-

verplattform, um die virtuelle oder emulierte CPU, den Arbeitsspeicher, das Block-Gerät und die Netzwerkressourcen zu nutzen.

Abbildung 23.4 VM-Server und virtuelle Computer



Die virtuellen Computer können über die Arbeitsoberfläche des VM-Servers angezeigt und verwaltet werden.

Abbildung 23.5 Arbeitsoberfläche des VM-Servers und drei virtuelle Computer



23.6 Einrichten des Virtual Machine Servers

Dieser Abschnitt führt Sie durch die Schritte zur Einrichtung und Ausführung eines VM-Servers.

- [Abschnitt 23.6.1, „Installation der Softwarepakete“](#) (S. 481)
- [Abschnitt 23.6.2, „Prüfung, ob der GRUB-Bootloader den VM-Server bootet“](#) (S. 482)
- [Abschnitt 23.6.3, „Booten des Virtual Machine Servers“](#) (S. 483)

23.6.1 Installation der Softwarepakete

Die Softwarepakete können während der SUSE Linux-Installation oder auf einem Computer, auf dem SUSE Linux bereits ausgeführt wird, installiert werden. Eine Liste der erforderlichen Softwarepakete finden Sie unter [Abschnitt 23.1, „Systemvoraussetzungen“](#) (S. 474).

23.6.1 Während der SUSE Linux-Installation

- 1 Beginnen Sie mit der Installation von SUSE Linux.
- 2 Klicken Sie im Bildschirm *Installationseinstellungen* auf *Ändern > Software*.
- 3 Aktivieren Sie das Kontrollkästchen neben der Auswahl für *Hostserver für Xen Virtual Machine*.
- 4 Befolgen Sie die Anweisungen zur Durchführung der SUSE Linux-Installation.

Fahren Sie nach der Installation mit [Abschnitt 23.6.2, „Prüfung, ob der GRUB-Bootloader den VM-Server bootet“](#) (S. 482) fort.

23.6.1 SUSE Linux wird bereits ausgeführt

- 1 Starten Sie YaST über das Startmenü.
- 2 Klicken Sie auf *System > Software installieren oder löschen*.
- 3 Aktivieren Sie das Kontrollkästchen neben der Auswahl für *Hostserver für Xen Virtual Machine*.
- 4 Klicken Sie auf *Übernehmen* und führen Sie die Schritte zur Installation der Pakete aus.

Fahren Sie nach der Installation der Pakete mit [Abschnitt 23.6.2, „Prüfung, ob der GRUB-Bootloader den VM-Server bootet“](#) (S. 482) fort.

23.6.2 Prüfung, ob der GRUB-Bootloader den VM-Server bootet

Bei der Installation der Xen-Softwarepakete wird der GRUB-Bootloader automatisch aktualisiert, sodass der VM-Server als Boot-Option angegeben wird. Die Konfigurationsdatei des GRUB-Bootloader ist in der Regel unter `/boot/grub/menu.lst` gespeichert.

Sie können Ihre GRUB-Bootloader-Konfigurationsdatei mit dem Beispiel unten vergleichen, um zu bestätigen, dass die Datei zum Booten des VM-Servers aktualisiert wurde. Das erste Beispiel zeigt eine typische GRUB-Bootloader-Datei, die zum Laden der Xen-Software aktualisiert wurde. Die zweite Datei zeigt eine GRUB-Bootloader-Datei, die einen PAE-fähigen Kernel lädt, der 32-Bit-Computern den Zugriff auf Arbeitsspeicherbereiche über 4 GB ermöglicht.

23.6.2 Beispiel für eine GRUB-Bootloader-Datei (typisch)

```
title XEN
  root (hd0,5)
  kernel /boot/xen.gz hype_parameter
  module /boot/vmlinuz-xen kernel_parameter
  module /boot/initrd-xen
```

23.6.2 Beispiel für eine GRUB-Bootloader-Datei (PAE)

```
title XEN
  root (hd0,5)
  kernel /boot/xen-pae.gz hype_parameter
  module /boot/vmlinuz-xenpae kernel_parameter
  module /boot/initrd-xenpae
```

Die Zeile `title` gibt den Namen des GRUB-Moduls an. Ändern Sie diese Zeile nicht, da YaST nach dem Wort *Xen* sucht, um zu bestätigen, dass die Pakete installiert sind.

Die Zeile `root` gibt an, in welcher Partition die Boot-Partition und das Verzeichnis `/boot` gespeichert sind. Ersetzen Sie `(hd0,5)` durch die richtige Partition. Wenn beispielsweise `hd1` das Verzeichnis `/boot` enthält, sollte der Eintrag `(hd0,0)` lauten.

Die Zeile `kernel` gibt das Verzeichnis und den Dateinamen der Hypervisor-Software an. Ersetzen Sie *Hype-Parameter* durch die Parameter, die an den Hypervisor übergeben werden sollen. Ein häufig verwendeter Parameter ist `dom0_mem=Speichermenge`. Er gibt an, wieviel Arbeitsspeicher dem VM-Server zugeordnet werden soll. Die Speichermenge wird in KB oder in Einheiten, beispielsweise 128M, angegeben. Wenn keine Menge angegeben wird, belegt der VM-Server den größtmöglichen Arbeitsspeicher. Weitere Informationen zu den Hypervisor-Parametern finden Sie auf der XenSource-Website [<http://www.xensource.com/>].

Die erste Zeile `module` gibt das Verzeichnis und den Dateinamen des zu ladenden Linux-Kernel an. Ersetzen Sie *Kernel-Parameter* durch die Parameter, die an den Kernel übergeben werden sollen. Diese Parameter sind mit jenen identisch, die auf physischer Computerhardware an einen Standard-Linux-Kernel übergeben werden.

Die zweite Zeile `module` gibt das Verzeichnis und den Dateinamen des RAM-Datenträgers an, der zum Booten des VM-Servers verwendet wird.

Wenn der Computer bootet, sollte der GRUB-Bootloader nun den VM-Server als Boot-Option anzeigen.

23.6.3 Booten des Virtual Machine Servers

- 1 Wenn der Computer bootet, wählen Sie im Bildschirm des GRUB-Bootloader die Option *VM-Server (Xen)*.
- 2 Melden Sie sich beim Computer als Benutzer `root` an.

- 3 Vergewissern Sie sich, dass der Computer als VM-Server ausgeführt wird, indem Sie `xm list` in ein Terminalfenster eingeben.

Der VM-Server wird ausgeführt, wenn der Befehl `xm list` funktioniert.

Der Computer sollte nun als VM-Server ausgeführt werden. Befolgen Sie die Schritte unter [Abschnitt 23.7, „Erstellen virtueller Computer“](#) (S. 484), um virtuelle Computer für die Ausführung auf dem VM-Server zu erstellen.

VM-Server-Fehlersuche

Die folgenden Informationen können hilfreich sein, wenn der Computer nicht ordnungsgemäß als VM-Server gebootet wird.

- Vergewissern Sie sich, dass der Computer die Hardware-Mindestanforderungen erfüllt.
- Geben Sie den Befehl `rpm -qa | grep xen` ein und vergewissern Sie sich, dass die Softwarepakete installiert sind, die unter [Abschnitt 23.1, „Systemvoraussetzungen“](#) (S. 474) aufgelistet sind.
- Stellen Sie sicher, dass die Parameter in der GRUB-Bootloader-Konfigurationsdatei korrekt sind. Vergleichen Sie Ihre Datei mit dem Beispiel unter [Abschnitt 23.6.2, „Beispiel für eine GRUB-Bootloader-Datei \(typisch\)“](#) (S. 482).

23.7 Erstellen virtueller Computer

Nach der Installation der Xen-Softwarepakete und dem Booten des Computers als VM-Server können virtuelle Computer für die Ausführung auf dem VM-Server erstellt werden. Ein virtueller Computer wird durch seinen Modus, seine Festplattenlaufwerke, Netzwerkkarten und anderen virtuellen Ressourcen definiert, die das Betriebssystem während der Installation und beim Booten erkennt.

- 1 Booten Sie den VM-Server.
- 2 Klicken Sie in der Arbeitsoberfläche des VM-Servers auf *System > Installation der Virtual Machine (XEN)*.

- 3 Klicken Sie auf *Ändern*, um die VM-Definitionen zu bearbeiten.
- 4 Klicken Sie auf *Virtualisierungsmodus*, um zu definieren, in welchem Modus der virtuelle Computer ausgeführt wird.
- 5 Klicken Sie auf *Optionen*, um den virtuellen Arbeitsspeicher, die Boot-Parameter und andere Optionen zu definieren.
- 6 Klicken Sie auf *Festplatten*, um Anzahl und Größe der virtuellen Festplatten zu definieren.
- 7 Klicken Sie auf *Netzwerk*, um die virtuelle Netzwerkkarte zu definieren.
- 8 Klicken Sie auf *Betriebssystem* und geben Sie dann das Verzeichnis an, in dem sich das Installationsprogramm des Betriebssystems oder ein bereits installierter Kernel befindet.
- 9 Befolgen Sie die Anweisungen auf dem Bildschirm, um die VM-Definitionen in einer Konfigurationsdatei zu speichern.

Die Definitionen werden automatisch in der Konfigurationsdatei `/etc/xen/vm/VM-Name` gespeichert.

- 10 (Optional) Zur Anpassung oder zur Prüfung, ob die Definitionen korrekt aufgezeichnet und gespeichert wurden, vergleichen Sie die Definitionen mit jenen in den Beispieldateien unter `/etc/xen/examples`.
- 11 (Bedingt) Je nach ausgewählter Installationsmethode wird möglicherweise das Installationsprogramm des Betriebssystems gestartet. Führen Sie in diesem Fall die Anweisungen des Installationsprogramms aus.

Der virtuelle Computer ist nun definiert und das Betriebssystem installiert. Fahren Sie mit [Abschnitt 23.8, „Verwalten virtueller Computer“](#) (S. 485) fort, um Anweisungen zum Starten und Verwalten virtueller Computer zu erhalten.

23.8 Verwalten virtueller Computer

Virtuelle Computer werden über die Arbeitsoberfläche des VM-Servers mithilfe des Befehls `xm` in einem Terminalfenster verwaltet. Der Zugriff auf VMs, die im vollstän-

dig virtualisierten Modus ausgeführt werden, kann auch über VNC- und SDL-Viewer erfolgen.

Tabelle 23.1 *Aufgaben und Befehle zur Verwaltung virtueller Computer*

Aufgabe	Befehl
So zeigen Sie eine Liste der verfügbaren Parameter für den Befehl <code>xm an</code>	<code>xm help</code>
So zeigen Sie eine Liste aller ausgeführten virtuellen Computer an	<code>xm list</code>
So starten und zeigen Sie einen virtuellen Computer an (paravirtualisiert)	<code>xm create /etc/xen/vm/VM-Name -c</code>
(Der virtuelle Computer wird gestartet und im Terminalfenster angezeigt.)	
So starten und zeigen Sie einen virtuellen Computer an (vollständig virtualisiert)	<code>xm create /etc/xen/vm/VM-Name</code>
(Der virtuelle Computer wird gestartet und in einem separaten SDL-Viewer-Fenster angezeigt.)	
So zeigen Sie die Konsole eines ausgeführten virtuellen Computers an (paravirtualisiert)	<code>xm console VM-Name</code>
So ändern Sie den verfügbaren Arbeitsspeicher für einen virtuellen Computer (paravirtualisiert)	<code>xm mem-set VM-Name MB_Arbeitsspeicher</code>
So fahren Sie das VM-Betriebssystem normal herunter (paravirtualisiert)	<code>xm shutdown VM-Name</code>
So fahren Sie das VM-Betriebssystem normal herunter (vollständig virtualisiert)	Öffnen Sie die Konsole des Betriebssystems. Führen Sie die erforderlichen Schritte zum Herunterfahren des Systems aus.

Aufgabe	Befehl
So beenden Sie einen virtuellen Computer sofort (paravirtualisiert)	<code>xm destroy VM-Name</code>
So beenden Sie einen virtuellen Computer sofort (vollständig virtualisiert)	Schließen Sie das SDL-Viewer-Fenster.

SDL ist der Standard-Viewer für die Anzeige virtueller VMs. Sie können jedoch auch zu VNC wechseln. Während SDL beim Anzeigen von Arbeitsoberflächen auf demselben Computer schneller ist, ist VNC beim Anzeigen von Arbeitsoberflächen über das Netzwerk schneller.

Tabelle 23.2 *Ändern der Viewer-Einstellungen*

Aufgabe	Befehl
So legen Sie VNC als Standard-Viewer fest anstatt SDL (vollständig virtualisiert)	Bearbeiten Sie die Datei <code>/etc/xen/vm/VM-Name</code> . Fügen Sie Zeilen hinzu oder nehmen Sie Änderungen daran vor: <code>vnc=1 vncviewer=1 sdl=0</code>
So verwenden Sie VNC zum Anzeigen der Konsole eines bereits ausgeführten virtuellen Computers (paravirtualisiert)	<code>vncviewer VM-Server_IP-Adresse: VM_ID</code>
So legen Sie SDL wieder als Standard-Viewer fest (vollständig virtualisiert)	Bearbeiten Sie die Datei <code>/etc/xen/vm/VM-Name</code> . Fügen Sie Zeilen hinzu oder nehmen Sie Änderungen daran vor: <code>vnc=0 vncviewer=0 sdl=1</code>

ANMERKUNG

Durch Schließen des VNC-Viewer-Fensters wird der virtuelle Computer nicht beendet.

Druckerbetrieb

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

Drucker können nach Schnittstelle, z. B. USB oder Netzwerk, und nach Druckersprache unterschieden werden. Stellen Sie beim Kauf eines Druckers sicher, dass dieser über eine von der Hardware unterstützte Schnittstelle und über 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 diese Linux-Distributoren unter einer Open-Source-Lizenz zur Verfügung stellt. Die meisten dieser Drucker finden sich im mittleren Preisbereich.

Proprietäre Drucker (in der Regel GDI-Drucker)

Für proprietäre Drucker sind in der Regel nur ein oder mehrere Windows-Treiber verfügbar. Diese Drucker unterstützen die gängigen Druckersprachen nicht und die von ihnen verwendeten Druckersprachen unterliegen Änderungen, wenn neue Versionen eines Modells auf den Markt gebracht werden. Weitere Informationen hierzu finden Sie unter [Abschnitt 24.7.1, „Drucker ohne Unterstützung für eine Standard-Druckersprache“](#) (S. 507).

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-Webseite
- `/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. Demnach ist es möglich, dass ein Drucker, der aktuell als „vollständig unterstützt“ eingestuft wird, diesen Status bei der Veröffentlichung der neuesten SUSE® Linux Enterprise-Version nicht aufgewiesen hat. Die Datenbank gibt daher nicht notwendigerweise den richtigen Status, sondern nur eine Annäherung an diesen an.

24.1 Workflow des Drucksystems

Der Benutzer erstellt einen Druckauftrag. Der Druckauftrag besteht aus den zu druckenden 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.

Für jeden Drucker ist eine dedizierte Druckwarteschlange verfügbar. 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 zu druckenden Daten (ASCII, PostScript, PDF, JPEG usw.) in die druckerspezifischen 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 Backend empfängt die druckerspezifischen Daten vom Filter und leitet diese an den Drucker weiter.

24.2 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.

► **zseries:** Von der z/VM bereitgestellte Drucker und ähnliche Geräte, die Sie lokal an IBM-System z-Mainframes anschließen können, werden von CUPS und LPRng nicht unterstützt. Auf diesen Plattformen ist das Drucken nur über das Netzwerk möglich. Die Kabel für Netzwerkdrucker müssen gemäß den Anleitungen des Druckerherstellers angeschlossen werden. ◀

WARNUNG: Kabelverbindung zum Computer

Vergessen Sie beim Anschließen des Druckers an den Computer nicht, dass während des Betriebs nur USB-Geräte angeschlossen werden können. Vor dem Anschließen anderer Verbindungstypen muss das System heruntergefahren werden.

24.3 Installieren 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 SUSE Linux Enterprise 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. Siehe [Abschnitt 24.6.3, „PPD-Dateien in unterschiedlichen Paketen“](#) (S. 504) und [Abschnitt 24.7.2, „Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar“](#) (S. 508).

Neue PPD-Dateien können im Verzeichnis `/usr/share/cups/model/` gespeichert oder dem Drucksystem mithilfe von YaST hinzugefügt werden (siehe [„Manuelle Konfiguration“](#) (S. 494)). 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 würde erstens dazu führen, dass Sie die Unterstützung von SUSE Linux Enterprise verlieren, und zweitens können Druckbefehle anders funktionieren und das System ist möglicherweise nicht mehr in der Lage, Geräte anderer Hersteller anzusprechen. Aus diesem Grund wird das Installieren von Herstellersoftware nicht empfohlen.

24.4 Konfigurieren des Druckers

Wenn Sie den Drucker an den Computer angeschlossen und die Software installiert haben, installieren Sie den Drucker im System. Dies sollte mit den von SUSE Linux Enterprise zur Verfügung gestellten Werkzeugen ausgeführt werden. Da SUSE Linux Enterprise großen Wert auf Sicherheit legt, haben Fremdhersteller-Werkzeuge häufig Schwierigkeiten mit den Sicherheitseinschränkungen und verursachen mehr Komplikationen als sie Vorteile bieten. Informationen zur Fehlerbehebung finden Sie in [Abschnitt 24.6.1, „CUPS-Server und Firewall“](#) (S. 501) und [Abschnitt 24.6.2, „Änderungen am CUPS-Druckdienst“](#) (S. 502).

24.4.1 Lokale Drucker

Wenn Sie sich anmelden und ein nicht konfigurierter Drucker erkannt wird, beginnt YaST mit dessen Konfiguration. Hierbei werden dieselben Dialogfelder wie in der folgenden Konfigurationsbeschreibung verwendet.

Um den Drucker zu konfigurieren, wählen Sie im YaST-Kontrollzentrum *Hardware* → *Drucker*. Dadurch wird das Hauptfenster für die Druckerkonfiguration geöffnet, in dem im oberen Teil die erkannten Geräte aufgelistet sind. Im unteren Teil werden alle bislang konfigurierten Warteschlangen aufgelistet. Wenn Ihr Drucker nicht erkannt wurde, müssen Sie ihn manuell konfigurieren.

WICHTIG

Wenn der Eintrag *Drucker* im YaST-Kontrollzentrum nicht verfügbar ist, ist das Paket `yast2-printer` wahrscheinlich nicht installiert. Um dieses Problem zu beheben, installieren Sie das Paket `yast2-printer` und starten Sie YaST neu.

Automatische Konfiguration

YaST kann den Drucker automatisch konfigurieren, wenn der Parallel- oder USB-Anschluss automatisch eingerichtet werden kann und der angeschlossene Drucker erkannt wird. Die Druckerdatenbank muss zudem die ID-Zeichenkette des Druckers enthalten, den YaST während der automatischen Hardware-Erkennung ermittelt. Wenn sich die Hardware-ID von der Modellbezeichnung unterscheidet, wählen Sie das Modell manuell aus.

Um sicherzustellen, dass alles ordnungsgemäß funktioniert, sollte jede Konfiguration mit der YaST-Funktion zum Drucken einer Testseite geprüft werden. Die Testseite bietet zudem wichtige Informationen zur getesteten Konfiguration.

Manuelle Konfiguration

Wenn die Anforderungen für eine automatische Konfiguration nicht erfüllt sind oder Sie eine benutzerdefinierte Konfiguration vorziehen, müssen Sie den Drucker manuell konfigurieren. Je nachdem, wie erfolgreich die automatische Erkennung ist und wie viele Informationen zum Druckermodell in der Datenbank gefunden werden, kann YaST die richtigen Einstellungen automatisch erkennen oder mindestens eine angemessene Vorauswahl treffen.

Die folgenden Parameter müssen konfiguriert werden:

Hardwareverbindung (Anschluss)

Die Konfiguration des Hardware-Anschlusses ist davon abhängig, ob YaST während der automatischen Hardware-Erkennung den Drucker finden konnte. Wenn YaST das Druckermodell automatisch erkennen kann, ist davon auszugehen, dass der Drucker auf Hardware-Ebene funktioniert und in dieser Hinsicht keine Einstellungen geändert werden müssen. Wenn YaST das Druckermodell nicht automatisch erkennen kann, liegt auf Hardware-Ebene möglicherweise ein Problem mit der Verbindung vor. In diesem Fall muss die Verbindung manuell konfiguriert werden.

Klicken Sie im Dialogfeld *Druckerkonfiguration* auf *Hinzufügen*, um die manuelle Konfiguration zu starten. Wählen Sie den *Druckertyp* (z. B. *Drucker am USB-Anschluss*). Klicken Sie auf *Weiter*, um das Dialogfeld *Druckeranschluss* zu öffnen, und wählen Sie das gewünschte Gerät aus.

Name der Warteschlange

Der Name der Warteschlange wird bei der Eingabe von Druckbefehlen verwendet. Der Name sollte relativ kurz sein und nur Kleinbuchstaben und Zahlen enthalten. Geben Sie den *Name für den Druck* im nächsten Dialogfeld (*Name der Warteschlange*) ein.

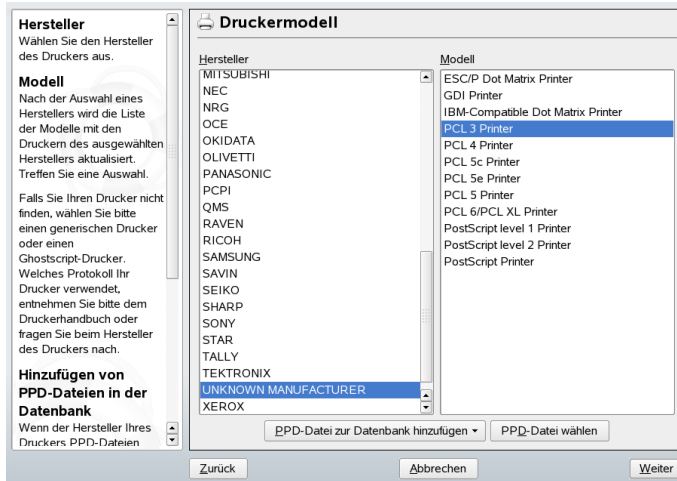
Druckermodell und PPD-Datei

Sämtliche druckerspezifischen Parameter, z. B. der zu verwendende Ghostscript-Treiber sowie die Druckerfilter-Parameter für den Treiber, sind in einer PPD-Datei gespeichert. Weitere Informationen zu PPD-Dateien finden Sie in [Abschnitt 24.3](#), „[Installieren der Software](#)“ (S. 492).

Für viele Druckermodelle sind mehrere PPD-Dateien verfügbar, beispielsweise, wenn mehrere Ghostscript-Treiber mit dem entsprechenden Modell funktionieren. Wenn Sie im nächsten Dialogfeld (*Druckermodell*) einen Hersteller und ein Modell auswählen, wählt YaST die entsprechende PPD-Datei für den Drucker aus. Wenn für das Modell mehrere PPD-Dateien verfügbar sind, wählt YaST standardmäßig eine dieser Dateien aus (normalerweise die als *empfohlen* markierte Datei). Sie können die ausgewählte PPD-Datei im nächsten Dialogfeld mit der Option *Bearbeiten* ändern.

Für Nicht-PostScript-Modelle werden alle druckerspezifischen Daten vom Ghostscript-Treiber generiert. Aus diesem Grund ist die Treiberkonfiguration der wichtigste Faktor beim Festlegen der Ausgabequalität. Die Qualität des Ausdrucks ist sowohl vom Typ des ausgewählten Ghostscript-Treibers (PPD-Datei) als auch von den für diesen angegebenen Optionen abhängig. Falls erforderlich, können Sie weitere (durch die PPD-Datei zur Verfügung gestellte) Optionen nach Auswahl von *Bearbeiten* ändern.

Abbildung 24.1 Auswählen des Druckermodells



Sie sollten die vorgenommenen Einstellungen immer prüfen, indem Sie die Testseite drucken. Wenn die Ausgabe nicht akzeptabel ist und beispielsweise mehrere Seiten fast leer sind, sollten Sie zunächst den Drucker anhalten, indem Sie das gesamte Papier entfernen und anschließend den Test über YaST stoppen.

Wenn die Druckerdatenbank keinen Eintrag für Ihr Modell enthält, können Sie entweder eine neue PPD-Datei hinzufügen, indem Sie *PPD-Datei zur Datenbank hinzufügen* wählen oder eine Sammlung generischer PPD-Dateien verwenden, damit der Drucker mit einer der Standard-Druckersprachen druckt. Wählen Sie hierzu *UNKNOWN MANUFACTURER* als Druckerhersteller.

Erweiterte Einstellungen

Die hier angegebenen Einstellungen müssen in der Regel nicht geändert werden.

24.4.2 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.

CUPS unterstützt die Protokolle `socket`, `LPD`, `IPP` und `smb`. Im Folgenden finden Sie einige ausführlichere Informationen zu diesen Protokollen:

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. Ein Beispiel für einen Geräte-URI ist `socket://host-printer: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://host-printer/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://host-printer/ps` und `ipp://host-cupserver/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://Benutzer:Passwort@Arbeitsgruppe/Server/Drucker`,
`smb://Benutzer:Passwort@Host/Drucker` und
`smb://Server/Drucker`.

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
```

Konfigurieren von CUPS im Netzwerk unter Verwendung von YaST

Netzwerkdrucker sollten mit YaST konfiguriert werden. YaST vereinfacht die Konfiguration und ist bestens ausgestattet, um die Sicherheitseinschränkungen in CUPS handzuhaben (siehe [Abschnitt 24.6.2, „Änderungen am CUPS-Druckdienst“](#) (S. 502)). Weitere Informationen und Richtlinien zur Installation von CUPS im Netzwerk finden Sie im Beitrag *CUPS in aller Kürze* in der Support-Datenbank unter http://en.opensuse.org/SDB:CUPS_in_a_Nutshell.

Starten Sie die Druckerkonfiguration und klicken Sie auf *Hinzufügen*. Falls Sie keine anderen Anweisungen von Ihrem Netzwerkadministrator erhalten haben, probieren Sie die Option *Direkt auf Netzwerkdrucker drucken* aus und fahren Sie gemäß den lokalen Anforderungen fort.

Konfigurieren mit Kommandozeilenoptionen

CUPS kann alternativ auch mit Kommandozeilenoptionen wie `lpadmin` und `lpoptions` konfiguriert werden. Sie benötigen einen Geräte-URI (Uniform Resource Identifier), der aus einem Backend, 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. Fügen Sie eine Druckwarteschlange unter Verwendung der folgenden Syntax hinzu:

```
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://192.168.1.0:9100/ -P \  
/usr/share/cups/model/Postscript-levell.ppd.gz -E
```

Weitere Informationen hierzu sowie weitere Optionen für `lpadmin` finden Sie auf der Manualpage für den Befehl `lpadmin(1)`.

Während der Druckerkonfiguration werden bestimmte Optionen standardmäßig gesetzt. Diese Optionen können (je nach verwendetem 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
```

Example:

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

Die aktivierte Standardoption wird durch das vorangehende Sternchen (*) gekennzeichnet.

2 Ändern Sie die Option mit `lpadmin`:

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

3 Prüfen Sie die neue Einstellung:

```
lptions -p queue -l
```

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

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

24.5 Konfiguration für Anwendungen

Anwendungen verwenden die vorhandenen Druckwarteschlangen auf dieselbe Weise wie Kommandozeilenwerkzeuge. Es ist nicht erforderlich, den Drucker für eine bestimmte Anwendung neu zu konfigurieren, da Sie unter Verwendung der verfügbaren Warteschlangen aus der Anwendung heraus drucken können sollten.

Um den Druckvorgang über die Kommandozeile zu starten, geben Sie `lp -d Name_der_Warteschlange Dateiname` 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`. Damit dies in KDE-Programmen funktioniert, aktivieren Sie die Option *Über externes Programm drucken*. Andernfalls können Sie den Druckbefehl nicht eingeben.

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` als Standardschnittstelle zum Drucken von Nicht-KDE-Anwendungen verwenden, indem Sie `kprinter` oder `kprinter --stdin` als Druckbefehl in den Druckdialogfeldern dieser Anwendungen angeben. Welcher der beiden Befehle gewählt wird, wird vom Verhalten der Anwendung selbst festgelegt. Wenn die Anwendung ordnungsgemäß koniguriert ist, sollte sie bei jeder Ausgabe eines Druckauftrags das Dialogfeld "kprinter" öffnen, in dem Sie in diesem Dialogfeld eine Warteschlange wählen und andere Druckoptionen festlegen können. Dies erfordert,

dass zwischen den anwendungsspezifischen Druckereinstellungen und denen von kprinter keine Konflikte auftreten und dass die Druckoptionen nur über kprinter geändert werden, nachdem es aktiviert wurde.

24.6 Spezielle Funktionen in SUSE Linux Enterprise

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

24.6.1 CUPS-Server und Firewall

Es gibt mehrere Möglichkeiten, CUPS als Client eines Netzwerkservers zu konfigurieren.

1. Sie können für jede Warteschlange auf dem Netzwerkserver eine lokale Warteschlange konfigurieren, über die alle Druckaufträge an den entsprechenden Netzwerkserver weitergeleitet werden (diese Warteschlange bezeichnet man auch als Weiterleitungswarteschlange). Dieser Ansatz wird in der Regel jedoch nicht empfohlen, da alle Client-Computer neu konfiguriert werden müssen, wenn sich die Konfiguration des Netzwerkservers ändert.
2. Druckaufträge können auch direkt an einen Netzwerkserver weitergeleitet werden. Für diesen Konfigurationstyp wird kein lokaler CUPS-Daemon ausgeführt. `lp` oder entsprechende Bibliotheksaufrufe anderer Programme können die Druckaufträge direkt an den Netzwerkserver senden. Diese Konfiguration funktioniert jedoch nicht, wenn Sie gleichzeitig auf einem lokalen Drucker drucken möchten.
3. Der CUPS-Daemon kann auf IPP-Broadcast-Pakete lauschen, die andere Netzwerkserver senden, um die verfügbaren Warteschlangen bekannt zu geben.

Dies ist die beste CUPS-Konfiguration für das Drucken über entfernte CUPS-Server. Es besteht jedoch das Risiko, dass ein Angreifer IPP-Broadcast-Pakete mit Warteschlangen sendet und der lokale Daemon auf eine gefälschte Warteschlange zugreift. Wenn die Warteschlange dann mit demselben Namen wie die andere Warteschlange auf dem lokalen Server angezeigt wird, glaubt der Eigentümer des Auftrags möglicherweise, dass der Auftrag an einen lokalen

Server gesendet wird, während er in Wirklichkeit an den Server des Angreifers geleitet wird.

YaST kann CUPS-Server mit zwei Methoden ermitteln: Durch Durchsuchen der lokalen Netzwerk-Hosts, um festzustellen, ob diese den IPP-Dienst anbieten, oder durch Lauschen auf IPP-Broadcast-Pakete. Dies setzt jedoch voraus, dass die Firewall für eingehende Pakete an Port 631/UDP (IPP-Client) durchlässig ist. Diese Voraussetzung ist automatisch erfüllt, wenn Sie Ihren Computer in der internen Firewall-Zone konfiguriert haben. Das Öffnen eines Ports zum Konfigurieren des Zugriffs auf entfernte Warteschlangen in der externen Zone kann ein Sicherheitsrisiko darstellen, da ein Angreifer einen Server anbieten kann, der dann möglicherweise von den Benutzern angenommen wird. Standardmäßig werden IPP-Broadcasts daher in der externen Zone verweigert. Weitere Informationen zur Firewall-Konfiguration finden Sie in [Abschnitt 44.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 906).

Alternativ kann der Benutzer CUPS-Server erkennen, indem er die lokalen Netzwerk-Hosts aktiv durchsucht oder alle Warteschlangen manuell konfiguriert. Aufgrund der am Anfang dieses Abschnitts erwähnten Gründe wird diese Methode nicht empfohlen.

24.6.2 Änderungen am CUPS-Druckdienst

Diese Änderungen wurden ursprünglich in SUSE Linux 9.1 vorgenommen.

cupsd wird als Benutzer lp ausgeführt

Beim Start ändert sich `cupsd` vom Benutzer `root` in den Benutzer `lp`. Dies bietet einen viel höheren Grad an Sicherheit, da der CUPS-Druckdienst nicht mit uneingeschränkten Berechtigungen, sondern nur mit den für den Druckdienst erforderlichen Berechtigungen ausgeführt wird.

Die Authentifizierung (die Passwortüberprüfung) kann nicht über `/etc/shadow` ausgeführt werden, da `lp` keinen Zugriff auf `/etc/shadow` hat. Stattdessen muss die CUPS-spezifische Authentifizierung über `/etc/cups/passwd.md5` verwendet werden. Zu diesem Zweck muss ein CUPS-Administrator mit der CUPS-Administrationsgruppe `sys` und einem CUPS-Passwort in `/etc/cups/passwd.md5` eingegeben werden. Geben Sie hierzu als `root` Folgendes ein:

```
lppasswd -g sys -a CUPS-admin-name
```

Diese Einstellung ist außerdem wichtig, wenn Sie das Web-Administrations-Frontend von CUPS oder das Werkzeug für die Druckeradministration von KDE verwenden möchten.

Wenn `cupsd` als `lp` ausgeführt wird, kann `/etc/printcap` nicht generiert werden, da `lp` nicht berechtigt ist, Dateien in `/etc/` zu erstellen. Daher generiert `cupsd` die Datei `/etc/cups/printcap`. Um sicherzustellen, dass Anwendungen, die Warteschlangennamen in `/etc/printcap` nur lesen können, weiter ordnungsgemäß funktionieren, ist `/etc/printcap` ein symbolischer Link, der auf `/etc/cups/printcap` verweist.

Wenn `cupsd` als `lp` ausgeführt wird, kann Port 631 nicht geöffnet werden. Daher kann `cupsd` mit dem Befehl `rcups reload` nicht neu geladen werden. Verwenden Sie stattdessen `rcups restart`.

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 „[cupsd wird als Benutzer lp ausgeführt](#)“ (S. 502) und „[Allgemeinere Funktionalität für BrowseAllow und BrowseDeny](#)“ (S. 503) sind wichtige Voraussetzungen für diese Funktion, da andernfalls die Sicherheit für eine automatische Aktivierung von `cupsd` nicht ausreichend wäre.

24.6.3 PPD-Dateien in unterschiedlichen Paketen

Die YaST-Druckerkonfiguration richtet die Warteschlangen für CUPS auf dem System nur unter Verwendung der 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/` enthalten 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/` nach Bedarf 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. Die PPD-Dateien für die PostScript-Drucker können 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. Die entsprechenden 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)` dem Druckermodell entspricht und das Paket `manufacturer-PPDs` 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 im Paket `manufacturer-PPDs` ist die einzige geeignete PPD-Datei für das Druckermodell oder es ist eine Foomatic-PPD-Datei mit dem Eintrag `*NickName: ... Foomatic/Postscript (recommended)` vorhanden, die dem Druckermodell ebenfalls entspricht.

YaST verwendet demzufolge 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 genannten Gründen aber nicht konfigurieren kann, müssen Sie das entsprechende Druckermodell manuell in YaST auswählen.

24.7 Fehlerbehebung

In den folgenden Abschnitten werden einige der am häufigsten auftretenden Probleme mit der Druckerhardware und -software sowie deren Lösungen oder Umgehungen beschrieben.

24.7.1 Drucker ohne Unterstützung für eine Standard-Druckersprache

Drucker, die keine der geläufigen Druckersprachen unterstützen und nur mit speziellen Steuersequenzen adressiert werden können, werden als *GDI-Drucker* bezeichnet. Diese Drucker funktionieren nur mit den Betriebssystemversionen, für die der Hersteller einen Treiber zur Verfügung stellt. *GDI* ist eine von Microsoft für Grafikgeräte entwickelte Programmierschnittstelle. Das eigentliche Problem ist nicht die Programmierschnittstelle, sondern die Tatsache, dass GDI-Drucker nur mit der proprietären Druckersprache des jeweiligen Druckermodells adressiert werden können.

Der Betrieb einiger Drucker kann sowohl im GDI-Modus als auch in einer der Standard-Druckersprachen ausgeführt werden. Einige Hersteller stellen für ihre GDI-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.

24.7.2 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 anschließend mit dem Dienstprogramm `cupstestppd`, ob die PPD-Datei der „Adobe PostScript-PDF-Format-Spezifikation, Version 4.3“, entspricht. Wenn das Dienstprogramm „FAIL“ zurückgibt, sind die Fehler in den PPD-Dateien schwerwiegend und verursachen wahrscheinlich größere Probleme. Die von `cupstestppd` protokollierten Problempunkte müssen behoben werden. Fordern Sie beim Druckerhersteller ggf. eine geeignete PPD-Datei an.

24.7.3 Parallelanschlüsse

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

- I/O address: 378 (hexadezimal)
- Interrupt: irrelevant
- Mode: Normal, SPP oder Output Only
- DMA: disabled

Wenn der Drucker trotz dieser Einstellungen über den Parallelanschluss nicht angesprochen werden kann, geben Sie die E/A-Adresse explizit in Übereinstimmung mit der Einstellung im BIOS in Form von `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 24.1](#), „`/etc/modprobe.conf`: Interrupt-Modus für den ersten Parallelanschluss“ (S. 509) 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 24.1 `/etc/modprobe.conf`: Interrupt-Modus für den ersten Parallelanschluss

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

24.7.4 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.

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 24.2](#), „Fehlermeldung vom `lpd`“ (S. 510) erhalten, wird das Problem durch den entfernten `lpd` verursacht.

Beispiel 24.2 Fehlermeldung vom `lpd`

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

Entfernten `cupsd` prüfen

Der CUPS-Netzwerkserver sollte Informationen über seine Warteschlangen standardmäßig alle 30 Sekunden an UDP-Port 631 via Broadcast senden. 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 24.3](#), „Broadcast vom CUPS-Netzwerkserver“ (S. 510) dargestellt.

Beispiel 24.3 Broadcast vom CUPS-Netzwerkserver

```
ipp://host.domain:631/printers/queue
```

► **zseries:** Berücksichtigen Sie, dass IBM System z-Ethernetgeräte standardmäßig keine Broadcasts empfangen. ◀

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 aber 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. Siehe [Abschnitt 24.4.2](#), „Netzwerkdrucker“ (S. 496).

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 angeschlossenen 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 hierzu finden Sie auf der Manualpage für den Befehl `nmap`.

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.

24.7.5 Fehlerhafte Ausdrücke ohne Fehlermeldung

Für das Drucksystem ist der Druckauftrag abgeschlossen, wenn das CUPS-Backend 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.

24.7.6 Deaktivierte Warteschlangen

Wenn die Datenübertragung zum Empfänger auch nach mehreren Versuchen nicht erfolgt, meldet das CUPS-Backend, 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.

24.7.7 Durchsuchen von CUPS: Löschen von Druckaufträgen

Wenn ein CUPS-Netzwerkserver seine Warteschlangen den Client-Hosts via Brwosing 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 einen Befehl wie `lpstat -h Print-Server -o` ein, um die Auftragsnummer auf dem Server zu ermitteln, vorausgesetzt, der Server hat den Druckauftrag nicht bereits abgeschlossen (d. h. ihn an den Drucker gesendet). Mithilfe dieser Auftragsnummer kann der Druckauftrag auf dem Server gelöscht werden:

```
cancel -h print-server queue-jobnumber
```

24.7.8 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 Print-Server -o` ein, um zu prüfen, über welche Warteschlange aktuell gedruckt wird. Löschen Sie den Druckauftrag mit `cancel Warteschlange-Auftragsnummer` oder mit `cancel -h Print-Server 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 Pro-

zesse zu beenden, die aktuell noch auf den Drucker zugreifen (präziser: auf den Parallelanschluss).

- 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.

24.7.9 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.

Gerätemanagement über dynamischen Kernel mithilfe von udev

25

Seit Version 2.6 kann der Kernel nahezu jedes Gerät im 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 Skripts hinzufügen, die als Teil der Kernel-Gerätebehandlung ausgeführt werden, oder indem Sie zusätzliche Daten zur Auswertung bei der Gerätebehandlung anfordern und importieren.

25.1 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`.

25.2 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.

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.

25.3 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.

25.4 Booten und erstes Einrichten des Geräts

Alle Geräteereignisse, die während des Boot-Vorgangs 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. Um diesen Verlust auszugleichen, stellt der Kernel eine `uevent`-Datei für jedes Gerät im `sysfs`-Dateisystem zur Verfügung. Durch das Schreiben von `add` in die entsprechende Datei sendet der Kernel dasselbe Ereignis, das während des Boot-Vorgangs 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 Boot-Vorgangs vorhanden ist, nicht durch die frühe Boot-Logik 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.

25.5 Fehlersuche bei udev-Ereignissen

Das Programm `udevmonitor` kann verwendet werden, um die Treiber-Core-Ereignisse und das Timing der udev-Ereignisprozesse zu visualisieren.

```
UEVENT[1132632714.285362] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UEVENT[1132632714.288166] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UEVENT[1132632714.309485] add@/class/input/input6
UEVENT[1132632714.309511] add@/class/input/input6/mouse2
UEVENT[1132632714.309524] add@/class/usb_device/usbdev2.12
UDEV [1132632714.348966] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UDEV [1132632714.420947] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UDEV [1132632714.427298] add@/class/input/input6
UDEV [1132632714.434223] add@/class/usb_device/usbdev2.12
UDEV [1132632714.439934] add@/class/input/input6/mouse2
```

Die `UEVENT`-Zeilen zeigen die Ereignisse an, die der Kernel an Netlink gesendet hat. Die `UDEV`-Zeilen zeigen die fertig gestellten udev-Ereignisbehandlungsroutinen an. Das Timing wird in Mikrosekunden angegeben. Die Zeit zwischen `UEVENT` und `UDEV` ist die Zeit, die udev benötigt hat, um dieses Ereignis zu verarbeiten oder der udev-Daemon hat eine Verzögerung bei der Ausführung der Synchronisierung dieses Ereignisses mit zugehörigen und bereits ausgeführten Ereignissen erfahren. Beispielsweise warten Ereignisse für Festplattenpartitionen immer, bis das Ereignis für den primären Datenträger fertig gestellt ist, da die Partitionereignisse möglicherweise auf die Daten angewiesen sind, die das Ereignis für den primären Datenträger von der Hardware angefordert hat.

`udevmonitor --env` zeigt die vollständige Ereignisumgebung:

```
UDEV [1132633002.937243] add@/class/input/input7
UDEV_LOG=3
ACTION=add
DEVPATH=/class/input/input7
SUBSYSTEM=input
SEQNUM=1043
PHYSDEVPATH=/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
PHYSDEVBUS=usb
PHYSDEVDRIVER=usbhid
PRODUCT=3/46d/c03e/2000
NAME="Logitech USB-PS/2 Optical Mouse"
```

```
PHYS="usb-0000:00:1d.1-2/input0"  
UNIQ=""  
EV=7  
KEY=70000 0 0 0 0 0 0 0  
REL=103
```

udev sendet auch Meldungen an syslog. Die standardmäßige syslog-Priorität, die steuert, welche Meldungen an syslog gesendet werden, wird in der udev-Konfigurationsdatei `/etc/udev/udev.conf` angegeben. Die Protokollpriorität des ausgeführten Daemons kann mit `udevcontrol log_priority=level/number` geändert werden.

25.6 Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von udev-Regeln

Eine udev-Regel kann mit einer beliebigen Eigenschaft abgeglichen werden, die der Kernel der Ereignisliste hinzufügt oder mit beliebigen Informationen, die der Kernel in `sysfs` exportiert. Die Regel kann auch zusätzliche Informationen aus externen Programmen anfordern. Jedes Ereignis wird gegen alle angegebenen Regeln abgeglichen. Alle Regeln befinden sich im Verzeichnis `/etc/udev/rules.d/`.

Jede Zeile in der Regeldatei enthält mindestens ein Schlüsselwertepaar. Es gibt zwei Arten von Schlüsseln: die Übereinstimmungsschlüssel und Zuweisungsschlüssel. Wenn alle Übereinstimmungsschlüssel mit ihren Werten übereinstimmen, wird diese Regel angewendet und der angegebene Wert wird den Zuweisungsschlüsseln zugewiesen. Eine übereinstimmende Regel kann den Namen des Geräteknotens angeben, auf den Knoten verweisende Symlinks hinzufügen oder ein bestimmtes Programm als Teil der Ereignisbehandlung ausführen. Falls keine übereinstimmende Regel gefunden wird, wird der standardmäßige Geräteknotenname verwendet, um den Geräteknoten zu erstellen. Die Regelsyntax und die angegebenen Schlüssel zum Abgleichen oder Importieren von Daten werden auf der Manualpage für udev beschrieben.

25.7 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 Block-Gerät, das der Kernel erstellt, wird von Werkzeugen mit speziellem Wissen 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
```

25.8 Das ersetzte hotplug-Paket

Das ehemals verwendete hotplug-Paket wird gänzlich durch udev und die udev-bezogene Kernel-Infrastruktur ersetzt. Die folgenden Teile der ehemaligen hotplug-Infrastruktur sind inzwischen überflüssig bzw. ihre Funktionalität wurde von udev übernommen:

```
/etc/hotplug/*.agent
```

Nicht mehr erforderlich oder in `/lib/udev` verschoben

`/etc/hotplug/*.rc`

Durch den `/sys/*/uevent`-Auslöser ersetzt

`/etc/hotplug/blacklist`

Durch die `blacklist`-Option in `modprobe.conf` ersetzt

`/etc/dev.d/*`

Durch die `udev`-Regel im `RUN`-Schlüssel ersetzt

`/etc/hotplug.d/*`

Durch die `udev`-Regel im `RUN`-Schlüssel ersetzt

`/sbin/hotplug`

Durch das Lauschen auf Netlink durch `udev` ersetzt; nur im anfänglichen RAM-Dateisystem verwendet, bis das Root-Dateisystem eingehängt werden kann; wird anschließend deaktiviert

`/dev/*`

Ersetzt durch dynamisches `udev` und statischen Inhalt in `/lib/udev/devices/*`

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

25.9 Weitere 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

Linux unterstützt eine Reihe von unterschiedlichen Dateisystemen. Dieses Kapitel gibt einen kurzen Überblick über die gängigsten Linux-Dateisysteme, erläutert deren Designkonzepte, Vorzüge und Anwendungsgebiete. Daneben erhalten Sie einige Zusatzinformation zu LFS (Large File Support) in Linux.

26.1 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.

26.2 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 nicht anders angegeben, können alle Schritte für das Einrichten oder Ändern von Partitionen und Dateisystemen mit YaST ausgeführt werden.

26.2.1 ReiserFS

Offiziell eine der Hauptfunktionen der Kernel-Version 2.4, stand ReiserFS als Kernel-Patch für 2.2.x SUSE-Kernels seit Version 6.4 zur Verfügung. ReiserFS wurde von Hans Reiser und dem Namesys-Entwicklungsteam entwickelt. Es hat sich als leistungsstarke Alternative zu Ext2 bewährt. Seine Vorzüge sind eine bessere 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. Zusätzlich 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 26.2.3, „Ext3“](#) (S. 526), umrissen werden. Der Standardmodus ist `data=ordered`, was die Integrität von Daten und Metadaten sicherstellt, aber Journaling nur für Metadaten nutzt.

26.2.2 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 dabei helfen kann, zu verstehen, 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.

26.2.3 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

26.2.4 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 `ext3` und `jbd` der Variablen `INITRD_MODULES` hinzufügen. Führen Sie nach dem Speichern der Änderungen den Befehl `mkinitrd` aus. Damit wird eine neue `initrd` aufgebaut und zur Verwendung vorbereitet.

26.2.5 Reiser4

Direkt nach der Veröffentlichung von Kernel 2.6 bekam die Familie der Journaling File Systeme Zuwachs durch ein weiteres Mitglied: Reiser4. Reiser4 unterscheidet sich grundlegend von seinem Vorgänger ReiserFS (Version 3.6). Es optimiert die Dateisystemfunktionalität durch Plugins und bietet ein engmaschigeres Sicherheitskonzept.

Engmaschiges Sicherheitskonzept

Bei Reiser4 legten die Entwickler besonderen Wert auf die Implementierung von Sicherheitsfunktionen. Reiser4 wird daher mit einem Satz an speziellen Sicherheits-Plugins geliefert. Das wichtigste führt das Konzept von Datei-„Items“ ein. Derzeit wird die Dateizugriffskontrolle pro Datei definiert. Wenn eine umfangreiche Datei relevante Informationen für mehrere Benutzer, Gruppen oder Anwendungen enthält, mussten die Zugriffsrechte ziemlich unpräzise sein, um alle betroffenen Parteien zu berücksichtigen. In Reiser4 können Sie diese Dateien in kleinere Teile (die „Items“) zerlegen. Zugriffsrechte lassen sich dann für jedes Element und jeden Benutzer separat festlegen, was eine viel präzisere Verwaltung der Dateisicherheit erlaubt. Ein perfektes Beispiel ist `/etc/passwd`. Bisher konnte nur `root` die Datei lesen und bearbeiten, während Nicht-`root`-Benutzer nur Lesezugriff auf

diese Datei erhielten. Mithilfe des Item-Konzepts von Reiser4 können Sie diese Datei in mehrere Elemente zerlegen (ein Item pro Benutzer) und Benutzern oder Anwendungen erlauben, ihre eigenen Daten zu ändern, aber nicht auf die Daten anderer Benutzer zuzugreifen. Dieses Konzept erhöht sowohl die Sicherheit als auch die Flexibilität.

Erweiterbarkeit durch Plugins

Viele Dateisystemfunktionen und externe Funktionen, die ein Dateisystem gewöhnlich nutzt, werden in Reiser4 als Plugins implementiert. Diese Plugins lassen sich bequem dem Basissystem hinzufügen. Sie brauchen den Kernel nicht mehr neu zu kompilieren oder die Festplatte neu zu formatieren, um Ihrem Dateisystem neue Funktionen hinzuzufügen.

Besseres Dateisystemlayout durch "Delayed Allocation"

Wie XFS unterstützt Reiser4 "Delayed Allocation" (verzögerte Speicherzuweisung). Siehe [Abschnitt 26.2.6, „XFS“](#) (S. 529). Der Einsatz dieser Technik sogar für Metadaten kann zu einem besseren Gesamlayout führen.

26.2.6 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* (Allocation Groups) 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.

26.3 Weitere unterstützte Dateisysteme

In [Tabelle 26.1, „Dateisystemarten unter Linux“](#) (S. 531) 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 26.1 Dateisystemarten unter Linux

cramfs	<i>Compressed ROM file system</i> : Ein komprimiertes Dateisystem mit Lesezugriff für ROMs.
hpfs	<i>High Performance File System</i> : Das OS/2-Standarddateisystem – nur im Nur-Lese-Modus unterstützt.
iso9660	Standarddateisystem auf CD-ROMs.
minix	Dieses Dateisystem wurde ursprünglich für Forschungsprojekte zu Betriebssystemen entwickelt und war das erste unter Linux verwendete Dateisystem. Heute wird es noch für Disketten eingesetzt.
msdos	<i>fat</i> , das von DOS stammende Dateisystem, wird heute noch von verschiedenen Betriebssystemen verwendet.
ncpfs	Dateisystem zum Einhängen von Novell-Volumes über Netzwerke.
nfs	<i>Network File System</i> : Hier können Daten auf einem beliebigen vernetzten Rechner gespeichert werden und der Zugriff kann über ein Netzwerk erfolgen.
smbfs	<i>Server Message Block</i> wird von Produkten wie Windows für den Dateizugriff über ein Netzwerk verwendet.
sysv	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 on MSDOS</i> : Aufgesetzt auf einem normalen <i>fat</i> -Dateisystem. Erhält UNIX-Funktionalität (Rechte, Links, lange Dateinamen) durch die Erstellung spezieller Dateien.
vfat	<i>Virtual FAT</i> : Erweiterung des <i>fat</i> -Dateisystems (unterstützt lange Dateinamen).

26.4 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 26.2, „Maximale Größe von Dateisystemen \(Festplattenformat\)“](#) (S. 532) bietet einen Überblick über die derzeitigen Beschränkungen für Linux-Dateien und -Dateisysteme.

Tabelle 26.2 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)
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)

Dateisystem	Dateigröße (Byte)	Dateisystemgröße (Byte)
NFSv3 (Client-seitig)	2^{63} (8 EB)	2^{63} (8 EB)

WICHTIG: Linux-Kernel-Beschränkungen

Tabelle 26.2, „Maximale Größe von Dateisystemen (Festplattenformat)“ (S. 532) 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. Dabei handelt es sich um folgende:

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.

26.5 Weitere 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://www.ibm.com/developerworks/linux/library/l-jfs.html>
- <http://oss.sgi.com/projects/xfs/>

Ein umfassendes mehrteiliges Tutorial zu Linux-Dateisystemen findet sich unter *IBM developerWorks*: <http://www-106.ibm.com/developerworks/library/l-fs.html>. Einen Vergleich der verschiedenen Journaling File Systeme

unter Linux befindet sich im Beitrag von Juan I. Santos Florido unter *Linuxgazette*:
<http://www.linuxgazette.com/issue55/florido.html>. Eine ausführliche Arbeit zu LFS unter Linux erhalten Sie auf Andreas Jaegers LFS-Site: http://www.suse.de/~aj/linux_lfs.html.

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 zu der Verwendung von Schriften unter SUSE® Linux Enterprise und erfahren, wie OpenGL und 3D konfiguriert werden.

Der folgende Text enthält mehrere Verweise auf Dokumentation, die sich unter `/usr/share/doc/packages/Xorg` und `/usr/share/doc/howto/en` befindet. Dieses Material ist mit den zugehörigen Manualpages nur verfügbar, wenn die entsprechenden Dokumentationspakete installiert sind (`xorg-x11-doc`, `xorg-x11-man` und `howtoenh`).

TIPP: IBM-System z: Konfigurieren der grafischen Bedienoberfläche

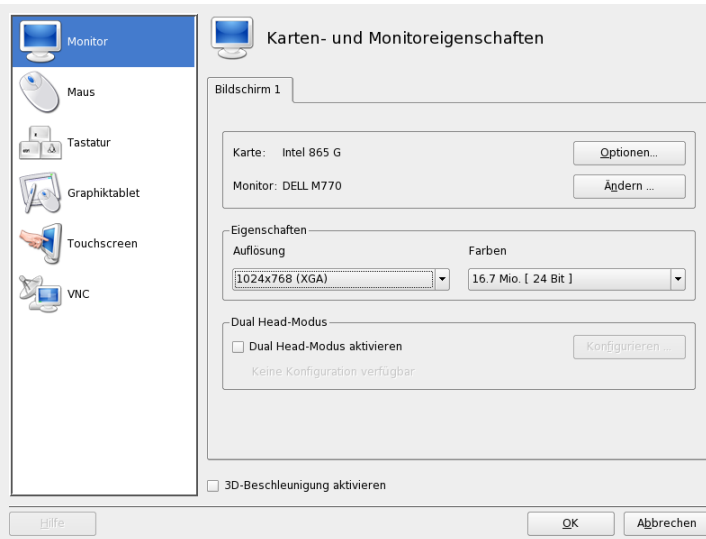
IBM-System z verfügt nicht über Eingabe- oder Ausgabegeräte, die von X.Org unterstützt werden, daher gelten keine der in diesem Abschnitt beschriebenen Vorgehensweisen für diese Systeme. Weitere relevante Informationen für IBM-System z finden Sie in [Abschnitt 7.6, „Netzwerkgeräte“](#) (S. 185).

27.1 X11-Konfiguration mit SaX2

Die grafische Bedienoberfläche, d. h. der X-Server, ist für die Kommunikation zwischen Hardware und Software verantwortlich. Desktops wie KDE und GNOME sowie die

zahlreichen Fenstermanager verwenden den X-Server für die Interaktion mit dem Benutzer. Die grafische Bedienoberfläche wird anfänglich während der Installation konfiguriert. Um die Einstellungen zu einem späteren Zeitpunkt zu ändern, verwenden Sie das entsprechende Modul aus dem YaST-Kontrollzentrum oder starten Sie SaX2 manuell über die Kommandozeile mit dem Befehl `sax2`. Das SaX2-Hauptfenster bietet eine gemeinsame Schnittstelle für die einzelnen Module aus dem YaST-Kontrollzentrum.

Abbildung 27.1 Das Hauptfenster von SaX2



In der linken Navigationsleiste befinden sich sechs Elemente, die den entsprechenden Konfigurationsdialogfeldern aus dem YaST-Kontrollzentrum entsprechen. Die im Folgenden erwähnten Abschnitte werden in [Kapitel 7, Systemkonfiguration mit YaST](#) (S. 149) beschrieben.

Monitor

Eine Beschreibung der Konfiguration des Monitors und der Grafikkarte finden Sie in [Abschnitt 7.13.1, „Karten- und Monitoreigenschaften“](#) (S. 210).

Maus

Eine Beschreibung der Mauskonfiguration in der grafischen Umgebung finden Sie in [Abschnitt 7.13.2, „Mauseigenschaften“](#) (S. 214).

Tastatur

Eine Beschreibung der Tastaturkonfiguration in der grafischen Umgebung finden Sie in [Abschnitt 7.13.3, „Tastatureigenschaften“](#) (S. 215).

Graphiktablett

Eine Beschreibung der Konfiguration des Graphiktablets finden Sie in [Abschnitt 7.13.4, „Tablet-Eigenschaften“](#) (S. 215).

Touchscreen

Eine Beschreibung der Konfiguration des Touchscreens finden Sie in [Abschnitt 7.13.5, „Touchscreen-Eigenschaften“](#) (S. 216).

VNC

Eine Beschreibung der VNC-Konfiguration finden Sie in [Abschnitt 7.13.6, „Eigenschaften für den entfernten Zugriff“](#) (S. 216).

27.2 Optimierung der X-Konfiguration

X.Org ist eine Open-Source-Implementierung des X Window-Systems. Es wird von der X.Org Foundation weiterentwickelt, die auch für die Entwicklung neuer Technologien und Standards für das X Window-System verantwortlich ist.

Die Konfiguration kann manuell angepasst werden, um eine bestmögliche Nutzung der verfügbaren Hardware wie Maus, Grafikkarte, Monitor und Tastatur zu gewährleisten. Einige Aspekte dieser Optimierung werden im Folgenden erläutert. Detaillierte Informationen zur Konfiguration des X Window-Systems finden Sie in den verschiedenen Dateien im Verzeichnis `/usr/share/doc/packages/Xorg` und erhalten Sie durch Eingabe von `man xorg.conf`.

WARNUNG

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 SUSE Linux 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.

Die Programme SaX2 und xorgconfig erstellen die Datei `xorg.conf` standardmäßig unter `/etc/X11`. Dabei handelt es sich um die primäre Konfigurationsdatei für das 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 Abschnitte haben folgende Form:

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

Die verfügbaren Abschnittstypen finden Sie in [Tabelle 27.1](#), „Abschnitte in `/etc/X11/xorg.conf`“ (S. 538).

Tabelle 27.1 Abschnitte in `/etc/X11/xorg.conf`

Typ	Bedeutung
<code>Files</code>	In diesem Abschnitt werden die Pfade definiert, die für Schriften und die RGB-Farbtabelle verwendet werden.
<code>ServerFlags</code>	Hier werden allgemeine Parameter festgelegt.
<code>InputDevice</code>	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> .
<code>Monitor</code>	Beschreibt den verwendeten Monitor. Die einzelnen Elemente dieses Abschnitts sind der Name, auf den später in der Definition von <code>Screen</code> verwiesen wird, die Bandbreite (<code>bandwidth</code>) und die Grenzwerte für die Synchronisierungsfrequenz

Typ	Bedeutung
	(<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.
<code>Modes</code>	Hier werden Modeline-Parameter für die einzelnen Bildschirmauflösungen gespeichert. Diese Parameter können von SaX2 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/XFree86-Video-Timings-HOWTO</code> .
<code>Ge r t</code>	In diesem Abschnitt wird eine bestimmte Grafikkarte definiert. Sie wird mit ihrem beschreibenden Namen angeführt.
<code>Screen</code>	Hier wird eine Verbindung zwischen einem <code>Monitor</code> und einer Grafikkarte (<code>Device</code>) hergestellt, um alle erforderlichen Einstellungen für <code>X.Org</code> bereitzustellen. Im Unterabschnitt <code>Display</code> können Sie die Größe des virtuellen Bildschirms (<code>Virtual</code>), den <code>ViewPort</code> und die <code>Modes</code> für diesen Bildschirm festlegen.
<code>ServerLayout</code>	In diesem Abschnitt wird das Layout einer Single- oder Multihead-Konfiguration beschrieben. In diesem Abschnitt werden Kombinationen aus Eingabegeräten (<code>InputDevice</code>) und Anzeigegeräten (<code>Screen</code>) festgelegt.

`Monitor`, `Device` und `Screen` werden im Folgenden noch genauer erläutert. Weitere Informationen zu den anderen Abschnitten finden Sie auf den Manualpages 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`.

In diesem Fall gibt der darauf folgende Abschnitt `ServerLayout` an, welcher dieser Abschnitte genutzt wird.

27.2.1 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 27.1](#), „Abschnitt "Screen" der Datei `/etc/X11/xorg.conf`“ (S. 540) aussehen.

Beispiel 27.1 *Abschnitt "Screen" der Datei `/etc/X11/xorg.conf`*

```
Section "Screen"
    DefaultDepth 16
    SubSection "Display"
        Depth 16
        Modes "1152x864" "1024x768" "800x600"
        Virtual 1152x864
    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]"
    Monitor "Monitor[0]"
EndSection
```

In der Zeile `Identifier` (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.

Wählen Sie mit der Einstellung `DefaultDepth` die Farbtiefe aus, die der Server verwenden soll, wenn er nicht mit einer bestimmten Farbtiefe gestartet wird. Für jede Farbtiefe gibt es einen Unterabschnitt `Display`. Das Schlüsselwort `Depth` weist die für diesen Unterabschnitt gültige Farbtiefe zu. Mögliche Werte für `Depth` sind 8, 15, 16 und 24. Nicht alle X-Servermodule unterstützen diese Werte.

Unterhalb der Farbtiefe wird eine Liste der Auflösungen im Abschnitt `Modes` festgelegt. 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 nach links wechseln. So lässt sich die Auflösung ändern, während X ausgeführt wird.

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. 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 dieser Speicher auf der Karte auch für diverse Schrift- und Grafik-Caches genutzt wird.

27.2.2 Abschnitt "Device"

Im Abschnitt "Device" wird eine bestimmte Grafikkarte beschrieben. Es kann eine beliebige Anzahl von Grafikkarteneinträgen in `xorg.conf` vorhanden sein, solange deren Namen sich unterscheiden, d. h. solange ein eindeutiger Name mithilfe des Schlüsselworts `Identifier` festgelegt ist. Als generelle Regel gilt, dass bei der Installation mehrerer Grafikkarten die Abschnitte einfach der Reihe nach nummeriert werden. Die erste wird als `Device [0]`, die zweite als `Device [1]` usw. eingetragen.

Folgendes ist ein Auszug aus dem Abschnitt `Device` eines Computers mit einer Matrox Millennium-PCI-Grafikkarte:

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

Wenn Sie SaX2 für die Konfiguration einsetzen, sollte der Abschnitt "Device" in etwa wie in diesem Beispiel aussehen. Die Einträge unter `Driver` und `BusID` sind von der Hardware Ihres Computer abhängig und werden automatisch von SaX2 erkannt. Der Wert unter `BusID` steht für den PCI- oder AGP-Steckplatz, in dem die Grafikkarte installiert ist. Dieser entspricht der ID, die bei Eingabe des Befehls "lspci" angezeigt wird. Der X-Server benötigt Details im Dezimalformat, lspci zeigt diese jedoch im Hexadezimalformat an.

Über den Parameter `Driver` geben Sie den Treiber an, der für diese Grafikkarte verwendet werden soll. 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/X11R6/lib/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. Abhängig vom Treibermodul können verschiedene Optionen verfügbar sein. Diese finden Sie in den Beschreibungsdateien der Treibermodule im Verzeichnis `/usr/X11R6/lib/X11/doc`. Allgemein gültige Optionen finden Sie außerdem in den entsprechenden Manualpages (`man xorg.conf` und `man X.Org`).

27.2.3 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. 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

Wenn Sie nicht über fundierte Kenntnisse zu Monitor- und Grafikkartenfunktionen verfügen, sollten Sie an den Modelines keine Änderungen vornehmen, weil dies Ihren Monitor schwer beschädigen kann.

Falls Sie Ihre eigenen Monitorbeschreibungen entwickeln möchten, sollten Sie sich genauestens mit der Dokumentation unter `/usr/X11/lib/X11/doc` vertraut machen. In diesem Zusammenhang soll besonders auf den Abschnitt zu den Grafikmodi hingewiesen werden. In ihm wird detailliert beschrieben, wie die Hardware funktioniert und wie Modelines zu erstellen sind.

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 praktisch allen Kombinationen aus Grafikkarte und Monitor.

27.3 Installation und Konfiguration von Schriften

Die Installation zusätzlicher Schriften unter SUSE Linux Enterprise ist sehr einfach. Kopieren Sie einfach die Schriften in ein beliebiges Verzeichnis im X11-Pfad für Schriften (siehe [Abschnitt 27.3.1](#), „X11 Core-Schriften“ (S. 544)). Damit die Schriften verwendet werden können, sollte das Installationsverzeichnis ein Unterverzeichnis der

Verzeichnisse sein, die in `/etc/fonts/fonts.conf` konfiguriert sind (siehe [Abschnitt 27.3.2, „Xft“](#) (S. 546)).

Die Schriftdateien können manuell (vom `root`) in ein geeignetes Verzeichnis, beispielsweise `/usr/X11R6/lib/X11/fonts/truetype`, kopiert werden. 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 Skript `/usr/sbin/fonts-config`, das sich um die Konfiguration der Schriften kümmert. Weitere Informationen zur Arbeitsweise dieses Skripts finden Sie auf der Manualpage des Skripts (`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. Nur für CID-keyed-Schriften ist eine geringfügig unterschiedliche Vorgehensweise erforderlich. Weitere Informationen hierzu finden Sie in [Abschnitt 27.3.3, „CID-keyed-Schriften“](#) (S. 549).

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

27.3.1 X11 Core-Schriften

Heute unterstützt das X11 Core-Schriftsystem nicht nur Bitmap-Schriften, sondern auch skalierbare Schriften wie Type1-, TrueType- und OpenType-Schriften sowie CID-keyed-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 mithilfe von `xset +fp <Pfad>` hinzugefügt. Unerwünschte Pfade lassen sich mit `xset -fp <Pfad>` löschen.

Wenn der X-Server bereits aktiv ist, können Sie neu installierte Schriften in gemounteten Verzeichnissen mit dem Befehl `xset fp rehash` verfügbar machen. Dieser Befehl wird von `SuSEconfig --module fonts` ausgeführt. Da zur Ausführung des Befehls `xset` 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 lässt sich dies mit `root`-Berechtigungen erreichen. Geben Sie hierzu `su` und das `root`-Passwort ein. `su` überträgt die Zugriffsberechtigungen des Benutzers, der den X-Server gestartet hat, an 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 SUSE Linux Enterprise 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. Praktisch alle Unicode-Schriften, die unter SUSE Linux Enterprise zur Verfügung stehen, umfassen zumindest die für europäische Sprachen erforderlichen Schriftzeichen (früher als `iso-8859-*` kodiert).

27.3.2 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 SUSE Linux Enterprise 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 27.2 *Parameter zur Verwendung mit fc-list*

Parameter	Bedeutung und zulässige Werte
<code>family</code>	Der Name der Schriftfamilie, z. B. <code>FreeSans</code> .
<code>foundry</code>	Der Hersteller der Schrift, z. B. <code>urw</code> .
<code>style</code>	Der Schriftschnitt, z. B. <code>Medium</code> , <code>Regular</code> , <code>Bold</code> , <code>Italic</code> oder <code>Heavy</code> .

Parameter	Bedeutung und zulässige Werte
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.
file	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.

27.3.3 CID-keyed-Schriften

Im Gegensatz zu den anderen Schrifttypen können Sie CID-keyed-Schriften nicht einfach in einem beliebigen Verzeichnis installieren. CID-keyed-Schriften müssen in `/usr/share/ghostscript/Resource/CIDFont` installiert werden. Dies gilt nicht für Xft/fontconfig, ist jedoch für Ghostscript und das X11 Core-Schriftsystem erforderlich.

TIPP

Weitere Informationen zu Schriften unter X11 finden Sie unter <http://www.xfree86.org/current/fonts.html>.

27.4 OpenGL – 3D-Konfiguration

27.4.1 Hardware-Unterstützung

SUSE® Linux Enterprise beinhaltet mehrere OpenGL-Treiber zur Unterstützung von 3D-Hardware. [Tabelle 27.3](#), „Unterstützte 3D-Hardware“ (S. 550) bietet eine Übersicht.

Tabelle 27.3 *Unterstützte 3D-Hardware*

OpenGL-Treiber	Unterstützte Hardware
NVIDIA*	NVIDIA*-Chips: alle außer einigen veralteten Chipsätzen (GeForce2 und älter)
DRI	Intel* i810/i815/i830M, Intel* 845G/852GM/855GM/865G/915G,915GM/945G Matrox* G200/G400/G450/G550, ATI* Rage 128(Pro)/Radeon (bis 9250)

Wenn Sie das erste Mal mit YaST installieren, kann bei der Installation 3D-Beschleunigung aktiviert werden, sofern YaST 3D-Unterstützung erkennt. Für nVidia-Grafikchips muss zuvor der nVidia-Treiber installiert werden. Wählen Sie dafür den nVidia-Treiber-Patch in YOU (YaST Online Update) aus. Aus Lizenzgründen ist der nVidia-Treiber in diesem Paket nicht inbegriffen.

Wenn Sie stattdessen Ihr System aktualisieren, ist die Prozedur für das Konfigurieren der 3D-Hardware-Unterstützung eine andere. Sie hängt vom verwendeten OpenGL-Treiber ab. Weitere Einzelheiten erhalten Sie im folgenden Abschnitt.

27.4.2 OpenGL-Treiber

Die OpenGL-Treiber nVidia und DRI lassen sich einfach mit SaX2 konfigurieren. Für nVidia-Adapter muss zuvor der nVidia-Treiber installiert werden. Geben Sie den Befehl `3Ddiag` ein, um zu prüfen, ob die Konfiguration für nVidia oder DRI korrekt ist.

Aus Sicherheitsgründen dürfen nur Benutzer, die der Gruppe `video` angehören, auf die 3D-Hardware zugreifen. Stellen Sie daher sicher, dass alle lokalen Benutzer Mitglieder dieser Gruppe sind. Andernfalls wird die langsame *Software-Rendering-Ausweichlösung* des OpenGL-Treibers für OpenGL-Anwendungen benutzt. Verwenden Sie den Befehl `id`, um zu prüfen, ob der aktuelle Benutzer der Gruppe `video` angehört. Wenn dies nicht der Fall ist, nehmen Sie den Benutzer mithilfe von YaST in die Gruppe auf.

27.4.3 Das Diagnosewerkzeug 3Ddiag

Das Diagnosewerkzeug `3Ddiag` ermöglicht die Überprüfung der 3D-Konfiguration in SUSE Linux. Dabei handelt es sich um ein Kommandozeilenwerkzeug, das in einem Terminalfenster gestartet werden muss. Geben Sie `3Ddiag -h` ein, um mögliche Optionen für `3Ddiag` aufzulisten.

Um die X.Org-Konfiguration zu verifizieren, prüft das Werkzeug, ob die für 3D-Unterstützung erforderlichen Pakete installiert sind und die korrekte OpenGL-Bibliothek und GLX-Erweiterung verwendet werden. Befolgen Sie die Anweisungen von `3Ddiag`, wenn Sie Fehlermeldungen erhalten. Wenn alles korrekt ist, sehen Sie am Bildschirm nur Meldungen mit "done" (fertig).

27.4.4 OpenGL-Test-Dienstprogramme

Für das Testen von OpenGL können das Programm `glxgears` und Spiele wie `tuxracer` und `armagetron` (Pakete haben denselben Namen) nützlich sein. Wenn 3D-Unterstützung aktiviert wurde, sollte es möglich sein, diese drei reibungslos auf einem relativ neuen Computer auszuführen. Ohne 3D-Unterstützung würden diese Spiele sehr langsam ablaufen (Diashow-Effekt). Verwenden Sie den Befehl `glxinfo`, um zu prüfen, ob 3D aktiv ist. Wenn ja, enthält die Ausgabe eine Zeile mit `direct rendering: Yes` (Direktes Rendering: Ja).

27.4.5 Fehlerbehebung

Wenn die OpenGL-3D-Testergebnisse negativ sind (die Spiele laufen nicht reibungslos), verwenden Sie `3Ddiag`, um sicherzustellen, dass die Konfiguration keine Fehler enthält (Fehlermeldungen). Wenn die Korrektur nicht hilft oder keine Fehlermeldungen aufgetaucht sind, sehen Sie die X.Org-Protokolldateien an.

Häufig finden Sie in der X.Org-Datei `/var/log/Xorg.0.log` die Zeile `DRI is disabled` (DRI ist deaktiviert). Die genaue Ursache lässt sich nur durch genaue Prüfung der Protokolldatei erkennen – eine Aufgabe, die einige Erfahrung voraussetzt.

In solchen Fällen liegt kein Konfigurationsfehler vor, da diesen bereits 3Ddiag erkannt hätte. Daher besteht an dieser Stelle nur die Möglichkeit, die Software-Rendering-Ausweidlösung des DRI-Treibers zu verwenden, die keine 3D-Hardwareunterstützung bietet. Sie sollten auch bei Auftreten von OpenGL-Darstellungsfehlern oder Instabilität ohne 3D-Unterstützung arbeiten. Verwenden Sie SaX2, um 3D-Unterstützung vollständig zu deaktivieren.

27.4.6 Installationssupport

Abgesehen von der Software-Rendering-Ausweidlösung des DRI-Treibers befinden sich einige OpenGL-Treiber in Linux noch in der Entwicklungsphase und werden daher als experimentell betrachtet. Diese Treiber sind wegen der hohen Anforderung für 3D-Hardwarebeschleunigung in Linux im Paket enthalten. In Anbetracht des experimentellen Status von einigen OpenGL-Treibern kann SUSE keinen Installationssupport für die Konfiguration von 3D-Hardwarebeschleunigung geben oder bei zugehörigen Problemen weiteren Beistand leisten. Die Basiskonfiguration der grafischen Bedienoberfläche (X Window System) umfasst keine Konfiguration für 3D-Hardwarebeschleunigung. Wenn Sie Probleme mit der 3D-Hardwarebeschleunigung feststellen, wird empfohlen, die 3D-Unterstützung vollständig zu deaktivieren.

27.4.7 Weitere Informationen

Informationen erhalten Sie in den README-Dateien unter `/usr/X11R6/lib/X11/doc`. Weitere Informationen zur nVidia-Treiberinstallation finden Sie unter <http://www.suse.de/~sndirsch/nvidia-installer-HOWTO.html>.

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 oder SAMBA, 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 die meisten PAM-Module gespeichert, in denen die genaue Verhaltensweise der Module definiert ist (Beispiele: `pam_env.conf`, `pam_pwcheck.conf`, `pam_unix2.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.

28.1 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.

`account`

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 (wie Mailkonten, Home-Verzeichnis, Systemgrenzen usw.) zu konfigurieren.

Die zweite Spalte enthält Steuerflaggen, mit denen das Verhalten der gestarteten Module beeinflusst wird:

`required`

Ein Modul mit dieser Flagge muss erfolgreich verarbeitet werden, damit die Authentifizierung fortgesetzt werden kann. Wenn ein Modul mit der Flagge `required` ausfällt, werden alle anderen Module mit derselben Flagge verarbeitet, bevor der Benutzer eine Meldung bezüglich des Fehlers beim Authentifizierungsversuch erhält.

`requisite`

Module mit dieser Flagge müssen ebenfalls erfolgreich verarbeitet werden, ähnlich wie Module mit der Flagge `required`. Falls jedoch ein Modul mit dieser Flagge ausfällt, erhält der Benutzer sofort eine entsprechende Rückmeldung und es werden keine weiteren Module verarbeitet. Bei einem erfolgreichen Vorgang werden die anderen Module nachfolgend verarbeitet genau wie alle Module mit der Flagge `required`. Die Flagge `requisite` kann als Basisfilter verwendet werden, um zu überprüfen, ob bestimmte Bedingungen erfüllt sind, die für die richtige Authentifizierung erforderlich sind.

`sufficient`

Wenn ein Modul mit dieser Flagge erfolgreich verarbeitet wurde, erhält die anfordernde Anwendung sofort eine Nachricht bezüglich des erfolgreichen Vorgangs und keine weiteren Module werden verarbeitet, vorausgesetzt, es ist zuvor kein Fehler bei einem Modul mit der Flagge `required` aufgetreten. Ein Fehler eines Moduls mit der Flagge `sufficient` hat keine direkten Auswirkungen auf die Verarbeitung oder die Verarbeitungsreihenfolge nachfolgender Module.

`optional`

Ein Fehler oder die erfolgreiche Verarbeitung hat bei diesem Modul keine direkten Folgen. Dies kann für Module sinnvoll sein, die nur der Anzeige einer Meldung (beispielsweise um dem Benutzer mitzuteilen, dass er eine E-Mail erhalten hat) dienen, ohne weitere Aktionen auszuführen.

`include`

Wenn diese Flagge festgelegt ist, wird die als Argument angegebene Datei an dieser Stelle eingefügt.

Der Modulpfad muss nicht explizit angegeben werden, solange das Modul sich im Standardverzeichnis `/lib/security` befindet (für alle von SUSE® Linux Enterprise

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).

28.2 PAM-Konfiguration von sshd

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

Beispiel 28.1 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 `include`-Anweisungen, die auf die Konfigurationsdateien von vier Modultypen verweisen: `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.

Mit der ersten `include`-Datei (`common-auth`) werden zwei Module vom Typ `auth` aufgerufen: `pam_env` und `pam_unix2`. Siehe [Beispiel 28.2](#), „Standardkonfiguration für den Abschnitt `auth`“ (S. 557).

Beispiel 28.2 *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- 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 28.3](#), „Standardkonfiguration für den Abschnitt `account`“ (S. 557). 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 28.4](#), „Standardkonfiguration für den Abschnitt `password`“ (S. 557) dargestellt.

Beispiel 28.3 *Standardkonfiguration für den Abschnitt account*

```
account required    pam_unix2.so
```

Beispiel 28.4 *Standardkonfiguration für den Abschnitt password*

```
password required    pam_pwcheck.so    nullok
password required    pam_unix2.so      nullok use_first_pass use_authok
#password required    pam_make.so        /var/yp
```

Auch hier beinhaltet die PAM-Konfiguration von `sshd` nur eine `include`-Anweisung, die auf die Standardkonfiguration für `password`-Module in der Datei

`common-password` verweist. 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 28.5 *Standardkonfiguration für den Abschnitt `session`*

```
session required      pam_limits.so
session required      pam_unix2.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. `pam_unix2` wird zwar erneut verarbeitet, hat jedoch aufgrund der Option `none`, die in der entsprechenden Konfigurationsdatei des Moduls `pam_unix2.conf` angegeben ist, keine praktischen Konsequenzen. Mit dem Modul `pam_limits` wird die Datei `/etc/security/limits.conf` geladen, mit der Nutzungseinschränkungen für bestimmte Systemressourcen definiert werden können. Die `session`-Module werden beim Abmelden des Benutzers ein zweites Mal aufgerufen.

28.3 Konfiguration von PAM-Modulen

Einige PAM-Module können konfiguriert werden. Die entsprechenden Konfigurationsdateien sind im Verzeichnis `/etc/security` gespeichert. In diesem Abschnitt werden die für das `sshd`-Beispiel relevanten Konfigurationsdateien, `pam_unix2.conf`, `pam_env.conf`, `pam_pwcheck.conf` und `limits.conf`, kurz beschrieben.

28.3.1 pam_unix2.conf

Die herkömmliche passwortbasierte Authentifizierungsmethode wird durch das PAM-Modul `pam_unix2` gesteuert. Hiermit können die erforderlichen Daten aus `/etc/passwd`, `/etc/shadow`, NIS-Zuordnungen, NIS+-Tabellen oder aus einer LDAP-Datenbank gelesen werden. Das Verhalten des Moduls kann durch die Konfiguration der PAM-Optionen der einzelnen Anwendung selbst oder global durch Bearbeiten der Datei `/etc/security/pam_unix2.conf` beeinflusst werden. Eine ganz grundlegende Konfigurationsdatei für das Modul wird in [Beispiel 28.6](#), „`pam_unix2.conf`“ (S. 559) dargestellt.

Beispiel 28.6 *pam_unix2.conf*

```
auth:    nullok
account:
password:    nullok
session:    none
```

Mit der Option `nullok` für die Modultypen `auth` und `password` wird angegeben, dass leere Passwörter für den entsprechenden Kontotyp zulässig sind. Die Benutzer sind zudem berechtigt, die Passwörter für ihre Konten zu ändern. Die Option `none` für den Modultyp `session` gibt an, dass für dieses Modul keine Meldungen protokolliert werden sollen (dies ist die Standardeinstellung). Informationen zu zusätzlichen Konfigurationsoptionen erhalten Sie in den Kommentaren in der Datei selbst und auf der Handbuchseite `pam_unix2(8)`.

28.3.2 pam_env.conf

Diese Datei kann verwendet werden, um eine standardisierte Umgebung für Benutzer zu definieren, die beim Aufrufen des `pam_env`-Moduls festgelegt wird. Hiermit legen Sie Umgebungsvariablen mit folgender Syntax fest:

```
VARIABLE [DEFAULT=[value]] [OVERRIDE=[value]]
```

```
VARIABLE
```

Name der festzulegenden Umgebungsvariablen.

```
[DEFAULT=[value]]
```

Der Standardwert, den der Administrator festlegen möchte.

```
[OVERRIDE=[value]]
```

Werte, die von `pam_env` abgefragt und festgelegt werden können und die den Standardwert außer Kraft setzen.

Ein typisches Beispiel für eine Verwendungsmöglichkeit von `pam_env` ist die Anpassung der Variable `DISPLAY`, die immer dann geändert wird, wenn eine entfernte Anmeldung stattfindet. Dies ist in [Beispiel 28.7](#), „`pam_env.conf`“ (S. 560) dargestellt.

Beispiel 28.7 `pam_env.conf`

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

In der ersten Zeile wird der Wert der Variable `REMOTEHOST` auf `localhost` gesetzt, der immer dann verwendet wird, wenn mit `pam_env` kein anderer Wert bestimmt werden kann. Die Variable `DISPLAY` hingegen enthält den Wert `REMOTEHOST`. Weitere Informationen hierzu finden Sie in den Kommentaren der Datei `/etc/security/pam_env.conf`.

28.3.3 `pam_pwcheck.conf`

Diese Konfigurationsdatei ist für das Modul `pam_pwcheck` bestimmt, das daraus Optionen für alle Module vom Typ `password` abliest. Die in dieser Datei gespeicherten Einstellungen haben Vorrang vor den PAM-Einstellungen der einzelnen Anwendungen. Wenn keine anwendungsspezifischen Einstellungen definiert wurden, verwendet die Anwendung die globalen Einstellungen. Über [Beispiel 28.8](#), „`pam_pwcheck.conf`“ (S. 560) erhält `pam_pwcheck` die Anweisung, leere Passwörter und die Änderung von Passwörtern zuzulassen. Weitere Optionen für das Modul werden der Datei `/etc/security/pam_pwcheck.conf` beschrieben.

Beispiel 28.8 `pam_pwcheck.conf`

```
password: nullok
```

28.3.4 `limits.conf`

Systemgrenzen können auf Benutzer- oder Gruppenbasis in der Datei `limits.conf` festgelegt werden, die vom Modul `pam_limits` gelesen wird. In der Datei können Sie Festgrenzen, die niemals überschritten werden dürfen, und Softgrenzen festlegen,

die vorübergehend überschritten werden können. Informationen zur Syntax und zu den verfügbaren Optionen erhalten Sie in den in der Datei enthaltenen Kommentaren.

28.4 Weitere 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.

Thorsten Kukuk hat mehrere PAM-Module entwickelt und unter <http://www.suse.de/~kukuk/pam/> einige Informationen zu diesen Modulen zur Verfügung gestellt.

Energieverwaltung

Die Energieverwaltung ist insbesondere bei Notebook-Computern von großer Wichtigkeit, sie ist jedoch auch für andere Systeme sinnvoll. Es sind zwei Technologien verfügbar: APM (Advanced Power Management, erweiterte Energieverwaltung) und ACPI (Advanced Configuration and Power Interface, erweiterte Konfigurations- und Energieschnittstelle). Daneben ist es außerdem möglich, die CPU-Frequenzskalierung zu steuern, um Energie zu sparen oder den Geräuschpegel zu senken. Diese Optionen können manuell oder über ein spezielles YaST-Modul konfiguriert werden.

Die in diesem Kapitel beschriebenen Funktionen und Hardwareelemente sind auf IBM-Systemen nicht vorhanden. Das Kapitel ist für diese Plattformen daher irrelevant.

Anders als bei APM, das früher nur auf Notebooks zur Energieverwaltung eingesetzt wurde, steht das Hardware-Informations- und -Konfigurationswerkzeug ACPI auf allen modernen Computern (Notebooks, Desktops und Servern) zur Verfügung. Für alle Energieverwaltungstechnologien sind geeignete Hardware- und BIOS-Routinen erforderlich. Die meisten Notebooks und modernen Desktops und Server erfüllen diese Anforderungen.

APM wurde bei vielen älteren Computern verwendet. Da APM größtenteils aus einem Funktionsset besteht, das im BIOS integriert ist, kann der Grad der APM-Unterstützung je nach Hardware variieren. Dies gilt noch mehr für ACPI, einem noch komplexeren Werkzeug. Daher ist es praktisch unmöglich, eines der beiden Tools gegenüber dem anderen zu empfehlen. Testen Sie einfach die verschiedenen Verfahren auf Ihrer Hardware und wählen Sie dann die Technologie, die von der Hardware am besten unterstützt wird.

WICHTIG: Energieverwaltung für AMD64-Prozessoren

AMD64-Prozessoren mit 64-Bit-Kernel unterstützen nur ACPI.

29.1 Energiesparfunktionen

Energiesparfunktionen sind nicht nur für die mobile Verwendung von Notebooks von Bedeutung, sondern auch für Desktop-Systeme. Die Hauptfunktionen und ihre Verwendung bei den Energieverwaltungssystemen APM und ACPI sind folgende:

Standby

Bei diesem Betriebsmodus wird der Bildschirm ausgeschaltet. Bei einigen Computern wird die Prozessorleistung gedrosselt. Diese Funktion ist nicht bei allen APM-Implementierungen verfügbar. Diese Funktion entspricht ACPI-Zustand S1 bzw. S2.

Suspend (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. Geräte, die APM verwenden, können normalerweise durch Schließen des Deckels in den Suspend-Modus versetzt und durch Öffnen des Deckels wieder aktiviert werden. 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 APM und ACPI unabhängig sind.

Akku-Überwachung

ACPI und APM überprüfen den Ladezustand des Akkus und geben die entsprechenden Informationen an. Außerdem koordinieren beide Systeme die bei Erreichen eines kritischen Ladezustands durchzuführenden Aktionen.

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 Zusammenhang mit der CPU sind drei verschiedene Arten der Energieeinsparung möglich: Frequenz- und Spannungsskalierung (auch als PowerNow! oder Speedstep bekannt), Drosselung und Versetzen des Prozessors in den Ruhezustand (C-Zustände). Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden.

29.2 APM

Einige der Stromsparfunktionen werden vom APM-BIOS selbst ausgeführt. Auf vielen Notebooks können Stand-by- und Suspend-Zustände ohne besondere Betriebssystemfunktion durch Tastenkombinationen oder Schließen des Deckels aktiviert werden. Um diese Modi über einen Befehl zu aktivieren, müssen allerdings bestimmte Aktionen ausgelöst werden, bevor das System in den Suspend-Modus versetzt wird. Zur Anzeige des Akku-Ladezustands benötigen Sie spezielle Programmpakete und einen geeigneten Kernel.

SUSE® Linux Enterprise-Kernels verfügen über integrierte APM-Unterstützung. APM wird jedoch nur aktiviert, wenn ACPI nicht im BIOS implementiert ist und ein APM-BIOS ermittelt wird. Zur Aktivierung der APM-Unterstützung muss ACPI an der Boot-Eingabeaufforderung mit `acpi=off` deaktiviert werden. Geben Sie `cat /proc/apm` ein, um zu überprüfen, ob APM aktiv ist. Eine Ausgabe, die aus verschiedenen Nummern besteht, deutet darauf hin, dass alles in Ordnung ist. Es sollte nun möglich sein, den Computer mit dem Befehl `shutdown -h` herunterzufahren.

BIOS-Implementationen, die nicht vollständig standardkompatibel sind, können Probleme mit APM verursachen. Einige Probleme lassen sich durch spezielle Boot-Parameter umgehen. Alle Parameter werden an der Boot-Eingabeaufforderung in folgender Form eingegeben: `apm=parameter.parameter` ist entweder

`on` bzw. `off`

Aktiviert bzw. deaktiviert die APM-Unterstützung.

`(no-)allow-ints`

Lässt Interrupts während der Ausführung von BIOS-Funktionen zu.

`(no-)broken-psr`

Die BIOS-Funktion „GetPowerStatus“ funktioniert nicht ordnungsgemäß.

`(no-)realmode-power-off`

Setzt den Prozessor vor dem Herunterfahren auf den Real-Modus zurück.

`(no-)debug`

Protokolliert APM-Ereignisse im Systemprotokoll.

`(no-)power-off`

Schaltet Systemenergie nach dem Herunterfahren aus.

`bounce-interval=n`

Zeit in hundertstel Sekunden nach einem Suspend-Ereignis, während die weiteren Suspend-Ereignisse ignoriert werden.

`idle-threshold=n`

Prozentsatz der Systeminaktivität, bei dem die BIOS-Funktion `idle` ausgeführt wird (0 = immer, 100 = nie).

`idle-period=n`

Zeit in hunderstel Sekunden, nach der die Systemaktivität gemessen wird.

Der APM-Daemon (apmd) wird nicht mehr verwendet. Seine Funktionen werden vom neuen "powersaved" übernommen, der auch ACPI unterstützt und viele andere Funktionen bietet.

29.3 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 29.3.4, „Fehlerbehebung“](#) (S. 573).

29.3.1 ACPI in Aktion

Wenn der Kernel beim Booten des Systems ein ACPI BIOS entdeckt, wird ACPI automatisch aktiviert und APM deaktiviert. Bei einigen älteren Computern kann der Bootparameter `acpi=force` erforderlich sein. Der Computer muss ACPI 2.0 oder höher unterstützen. Überprüfen Sie anhand der Boot-Meldungen unter `/var/log/boot.msg`, ob ACPI aktiviert wurde.

Anschließend muss eine Reihe von Modulen geladen werden. Dies erfolgt über das Startskript des `acpid`-Skripts. Wenn eines dieser Module Probleme verursacht, kann das betreffende Modul unter `/etc/sysconfig/powersave/common` aus dem Lade- bzw. Entladevorgang ausgeschlossen werden. Das Systemprotokoll (`/var/log/messages`) enthält die Meldungen der Module, denen Sie entnehmen können, welche Komponenten erkannt wurden.

`/proc/acpi` enthält nun eine Nummer der Dateien, die Informationen zum Systemzustand bieten oder zum Ändern einiger Zustände verwendet werden können. Einige Funktionen funktionieren noch nicht, da sie sich noch in der Entwicklungsphase befinden, und die Unterstützung einiger Funktionen hängt weitgehend von der Implementierung durch den Hersteller ab.

Alle Dateien (mit Ausnahme von `dsdt` und `fadt`) können mit `cat` gelesen werden. In einigen Dateien können die Einstellungen mit `echo` geändert werden, beispielsweise `echo X > file` zur Angabe geeigneter Werte für `X`. Eine Möglichkeit für den einfachen Zugriff auf diese Werte ist der `powersave`-Befehl, der als Frontend für den Powersave-Daemon dient. Im Folgenden werden die wichtigsten Dateien beschrieben:

`/proc/acpi/info`

Allgemeine Informationen zu ACPI.

`/proc/acpi/alarm`

Hier können Sie angeben, wann das System aus einem Ruhezustand wieder aktiviert werden soll. Zurzeit wird diese Funktion nicht vollständig unterstützt.

`/proc/acpi/sleep`

Bietet Informationen zu möglichen Ruhezuständen.

`/proc/acpi/event`

Hier werden alle Ereignisse gemeldet und vom Powersave-Daemon (`powersaved`) verarbeitet. Wenn kein Daemon auf diese Datei zugreift, können Ereignisse, wie ein kurzes Antippen des Netzschalters oder das Schließen des Deckels mit `cat /proc/acpi/event` gelesen werden (Beenden mit `Strg` + `C`).

`/proc/acpi/dsdt` und `/proc/acpi/fadt`

Diese Dateien enthalten die ACPI-Tabellen DSDT (Differentiated System Description Table) und FADT (Fixed ACPI Description Table). Diese 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 durch einen Vergleich zwischen `last full capacity` (letzte volle Kapazität) aus `info` (Info) und `remaining capacity` (verbleibende Kapazität) aus `state` (Zustand) ermittelt. Bequemer lässt sich der Ladezustand mit einem speziellen Programm ermitteln, das in [Abschnitt 29.3.3](#), „ACPI-Werkzeuge“ (S. 573) beschrieben werden. 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 passiver bzw. aktiver Kühlung, Suspend-Modus (beim Zustand *hot* (heiß)) oder Herunterfahren (beim Zustand *critical* kritisch)). Die möglichen Aktionen sind in der DSDT definiert (geräteabhängig). Folgende Schwellenwerte werden in der ACPI-Spezifikation 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. Siehe [Abschnitt 29.3.3](#), „ACPI-Werkzeuge“ (S. 573).

29.3.2 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

Bei AMD und Intel läuft diese Technologie unter dem Namen PowerNow! bzw. 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 APM oder ACPI. Es gibt zwei Hauptverfahren für die Skalierung der CPU-Frequenz, über den Kernel an sich 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 festgelegt wird, steuert der Kernel die CPU-Frequenz durch die Skalierung auf eine userspace-Anwendung (normalerweise ein Daemon). In SUSE Linux Enterprise-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 ondemand-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 System-schnittstelle 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 Zustände: 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 ondemand 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 SUSE Linux Enterprise werden diese Technologien vom Powersave-Daemon gesteuert. Die Konfiguration wird in [Abschnitt 29.5](#), „Das powersave-Paket“ (S. 577) erläutert.

29.3.3 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, klapptopdaemon, 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 `pmttools`).

29.3.4 Fehlerbehebung

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 Boot-Parameter Abhilfe schaffen:

`pci=noacpi`

ACPI nicht zum Konfigurieren der PCI-Geräte verwenden.

`acpi=oldboot`

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 Boot-Meldungen des Systems mit dem Befehl `dmesg | grep -2i acpi` (oder 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 29.5.4, „Fehlerbehebung“](#) (S. 583) erläutert.

In der Kernel-Konfiguration gibt es einen Schalter zur Aktivierung der ACPI-Fehlermeldungen. 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.

Weitere 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)

29.4 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. Die meisten Funktionen lassen sich mit `powerd` und dem YaST-Energieverwaltungsmodul steuern. Letzteres wird in [Abschnitt 29.6](#), „Das YaST-Energieverwaltungsmodul“ (S. 586) genauer behandelt.

Mit der Anwendung `hdparm` können verschiedene Festplatteneinstellungen bearbeitet werden. Die Option `-y` schaltet die Festplatte sofort in den Stand-by-Modus. `-Y` versetzt sie in den Ruhezustand. `hdparm -S x` führt dazu, dass die Festplatte nach einem bestimmten Inaktivitätszeitraum abgeschaltet wird. Ersetzen Sie `x` wie folgt: 0 deaktiviert diesen Mechanismus, was zu einem Dauerbetrieb der Festplatte führt. Werte von 1 bis 240 werden mit 5 Sekunden multipliziert. Werte von 241 bis 251 entsprechen 1- bis 11-mal 30 Minuten.

Die internen Energiesparoptionen der Festplatte lassen sich über die Option `-B` steuern. Wählen Sie einen Wert 0 (maximale Energieeinsparung) bis 255 (maximaler Durchsatz). Das Ergebnis hängt von der verwendeten Festplatte ab und ist schwer einzuschätzen.

Die Geräuschentwicklung einer Festplatte können Sie mit der Option `-M` reduzieren. Wählen Sie einen Wert von 128 (ruhig) bis 254 (schnell).

Häufig ist es nicht so einfach, die Festplatte in den Ruhezustand zu versetzen. Bei Linux führen zahlreiche Prozesse Schreibvorgänge auf der Festplatte durch, wodurch diese wiederholt aus dem Ruhezustand reaktiviert wird. Daher sollten Sie unbedingt verstehen, wie Linux mit Daten umgeht, die auf die Festplatte geschrieben werden müssen. Zunächst werden alle Daten im RAM-Puffer gespeichert. Dieser Puffer wird vom 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.

29.5 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, APM, 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 (mit Ausnahme von `acpid`, der als Multiplexer für ACPI-Ereignisse fungiert) sollten nicht gleichzeitig mit dem `powersave`-Daemon ausgeführt werden.

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.

29.5.1 Konfigurieren des powersave-Pakets

Die Konfiguration von `powersave` wird an 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
- do_suspend_to_disk
- do_suspend_to_ram
- do_standby
- notify
- screen_saver
- reread_cpu_capabilities

`throttle` verlangsamt den Prozessor um den in `MAX_THROTTLING` festgelegten Wert. Dieser Wert hängt vom aktuellen Schema ab. `dethrottle` setzt den Prozessor auf volle Leistung. `suspend_to_disk`, `suspend_to_ram` und `standby` lösen das Systemereignis für einen Energiesparmodus aus. Diese drei Aktionen sind in der Regel für die Auslösung des Energiesparmodus zuständig, sie sollten jedoch stets mit bestimmten Systemereignissen verknüpft sein.

Das Verzeichnis `/usr/lib/powersave/scripts` enthält Skripts 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.

`set_disk_settings`

Führt die in `/etc/sysconfig/powersave/disk` vorgenommenen Datenträgereinstellungen aus.

Bei Festlegung der Variablen

`EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk do_suspend_to_disk"` beispielsweise werden die beiden Skripts bzw. 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 bestimmt, 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/sleep`

In dieser Datei können Sie die Energiesparmodi aktivieren und festlegen, welche kritischen Module vor einem Suspend- oder Stand-by-Ereignis entladen und welche Dienste angehalten werden sollen. Wenn der Betrieb des Systems wieder aufgenommen wird, werden diese Module erneut geladen und die Dienste werden

neu gestartet. Es ist sogar möglich, einen ausgelösten Energiesparmodus zu verzögern, beispielsweise um Dateien zu speichern. Die Standardeinstellungen betreffen vor allem USB- und PCMCIA-Module. Fehler bei Suspend oder Stand-by werden normalerweise von bestimmten Modulen verursacht. Weitere Informationen zur Ermittlung des Fehlers finden Sie in [Abschnitt 29.5.4, „Fehlerbehebung“](#) (S. 583).

```
/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/disk
```

Diese Konfigurationsdatei steuert die Aktionen und Einstellungen, die in Bezug auf die Festplatte vorgenommen werden sollen.

```
/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.

29.5.2 Konfigurieren von APM und ACPI

Suspend und Stand-by

Es gibt drei grundlegende ACPI-Energiesparmodi und zwei APM-Energiesparmodi:

Suspend to Disk (ACPI S4, APM suspend)

Speichert den gesamten Inhalt des Arbeitsspeichers auf die Festplatte. Der Computer wird vollständig ausgeschaltet und verbraucht keinerlei Energie. Dieser Energiesparmodus ist standardmäßig aktiviert und sollte auf allen System funktionieren.

Suspend to RAM (ACPI S3, APM suspend)

Speichert die Zustände aller Geräte im Hauptspeicher. Nur der Hauptspeicher verbraucht weiterhin Energie. Dieser Energiesparmodus ist standardmäßig deaktiviert, da er nach wie vor Probleme auf einigen Systemen verursacht. Die Unterstützung wurde jedoch enorm erweitert.

Standby (ACPI S1, APM standby)

Schaltet einige Geräte aus (herstellerabhängig).

Stellen Sie sicher, dass folgende Standardoptionen in der Datei `/etc/sysconfig/powersave/events` festgelegt sind, um die ordnungsgemäße Verarbeitung von Suspend, Stand-by und Resume zu gewährleisten (Standardeinstellungen nach der Installation von SUSE Linux Enterprise):

```
EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk screen_saver do_suspend_to_disk"
EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram screen_saver do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
    "prepare_standby screen_saver do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

Benutzerdefinierte Akku-Ladezustände

In der Datei `/etc/sysconfig/powersave/battery` können Sie drei Akku-Ladezustände (in Prozent) definieren, bei deren Erreichen Systemwarnungen oder bestimmte Aktionen ausgelöst werden.

```
BATTERY_WARNING=12
BATTERY_LOW=7
BATTERY_CRITICAL=2
```

Die Aktionen bzw. Skripts, die ausgeführt werden sollen, wenn der Ladezustand unter die angegebenen Grenzwerte fällt, werden in der Konfigurationsdatei `/etc/sysconfig/powersave/events` festgelegt. Die Standardaktionen für Schaltflächen können wie in [Abschnitt 29.5.1, „Konfigurieren des powersave-Pakets“](#) (S. 577) beschrieben geändert werden.

```
EVENT_BATTERY_NORMAL="ignore"
EVENT_BATTERY_WARNING="notify"
EVENT_BATTERY_LOW="notify"
EVENT_BATTERY_CRITICAL="wm_shutdown"
```

Anpassen des Energieverbrauchs an unterschiedliche Bedingungen

Das Systemverhalten kann an die Art der Stromversorgung angepasst werden. Der Energieverbrauch des Systems sollte reduziert werden, wenn das System vom Stromnetz getrennt und mit dem Akku betrieben wird. Ebenso sollte die Leistung automatisch zunehmen, sobald das System an das Stromnetz angeschlossen wird. Die CPU-Frequenz, die Energiesparfunktion von IDE und eine Reihe anderer Parameter können geändert werden.

Die Aktionen, die ausgeführt werden sollen, wenn der Computer vom Stromnetz getrennt bzw. wieder daran angeschlossen wird, werden in `/etc/sysconfig/powersave/events` festgelegt. Die zu verwendenden Schemata können in `/etc/sysconfig/powersave/common` ausgewählt werden:

```
AC_SCHEME="performance"
BATTERY_SCHEME="powersave"
```

Die Schemata werden in Dateien im Verzeichnis `/etc/sysconfig/powersave` gespeichert. Für die Dateinamen wird das Formatschema `_name-des-schemas` verwendet. Das Beispiel bezieht sich auf zwei Schemata: `scheme_performance` und `scheme_powersave`. `performance`, `powersave`, `presentation` und `acoustic` sind vorkonfiguriert. Mithilfe des in [Abschnitt 29.6](#), „Das YaST-Energieverwaltungsmodul“ (S. 586) beschriebenen YaST-Modul für die Energieverwaltung können bestehende Schemata bearbeitet, erstellt, gelöscht oder mit verschiedenen Energieversorgungszuständen verknüpft werden.

29.5.3 Weitere ACPI-Funktionen

Bei Verwendung von ACPI können Sie festlegen, 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.

```
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 Computern.

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.

29.5.4 Fehlerbehebung

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 folgenden Abschnitten werden die häufigsten Probleme mit powersave 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/tables> 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/*`. Wenn ein spezielles Modul bzw. eine spezielle Modulooption erforderlich ist, konfigurieren Sie diese(s) in der Datei `/etc/sysconfig/powersave/cpufreq` mithilfe der Variablen `CPUFREQD_MODULE` und `CPUFREQD_MODULE_OPTS`.

Suspend und Stand-by funktionieren nicht

Es gibt mehrere Kernel-bezogene Probleme, die die Verwendung der Suspend- und Stand-by-Ereignisse auf ACPI-Systemen verhindern:

- Zurzeit unterstützen Systeme mit mehr als 1 GB RAM keine Suspend-Ereignisse.
- Zurzeit unterstützen Multiprozessorsysteme und Systeme mit einem P4-Prozessor (mit Hyperthreading) keine Suspend-Ereignisse.

Der Fehler kann auch durch eine fehlerhafte DSDT-Implementierung (BIOS) verursacht worden sein. In diesem Fall müssen Sie eine neue DSDT installieren.

Bei ACPI- und APM-Systemen gilt Folgendes: 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 vom `powersave`-Daemon in `/var/log/suspend2ram.log` und `/var/log/suspend2disk.log` erstellten Protokolldateien stellen hierfür eine große Hilfe dar. Wenn der Computer nicht in den Energiesparmodus eintritt, liegt die Ursache im zuletzt entladenen Modul. Bearbeiten Sie die folgenden Einstellungen in `/etc/sysconfig/powersave/sleep`, um problematische Module vor einem Suspend- oder Stand-by-Ereignis zu entladen.

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES=""
```

Wenn Sie Suspend- oder Stand-by-Ereignisse in veränderlichen Netzwerkkumgebungen oder in Verbindung mit entfernt eingehängten Dateisystemen, wie Samba und NIS, verwenden, sollten Sie diese mithilfe von `automounter` einhängen oder die entsprechenden Dienste, beispielsweise `smbfs` oder `nfs` in der oben angegebenen Variablen ergänzen. Wenn eine Anwendung vor einem Suspend- oder Stand-by-Ereignis auf das entfernt eingehängte Dateisystem zugreift, kann der Dienst nicht richtig gestoppt und kein ordnungsgemäßes Aushängen des Dateisystems durchgeführt werden. Wenn der Betrieb des Systems wieder aufgenommen wird, kann das Dateisystem beschädigt und ein erneutes Einhängen erforderlich sein.

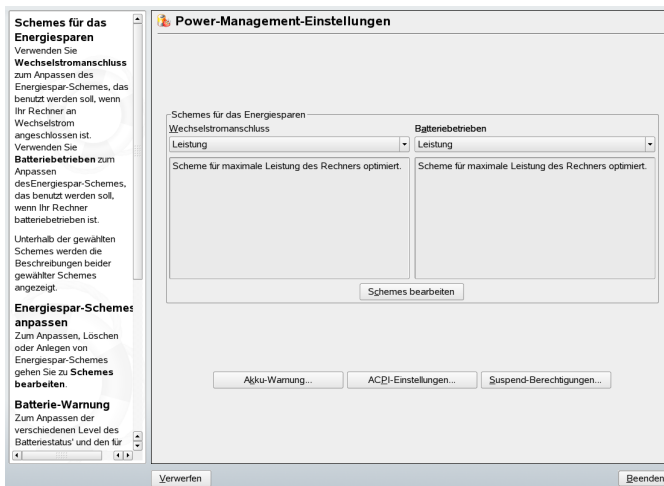
29.5.5 Weitere Informationen

- </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

29.6 Das YaST-Energieverwaltungsmodul

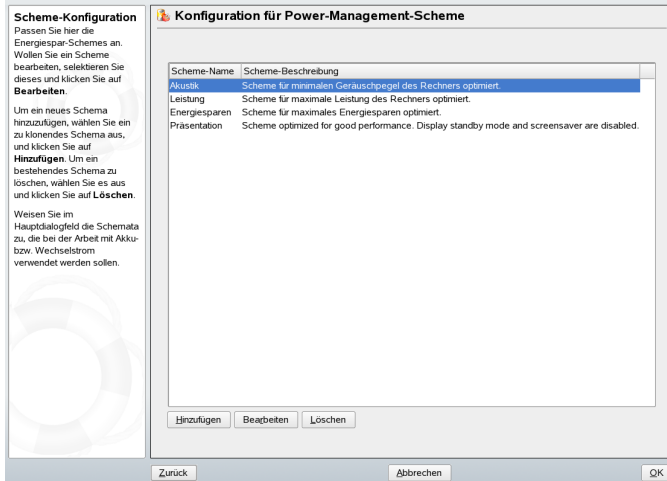
Das YaST-Energieverwaltungsmodul kann alle bereits beschriebenen Energieverwaltungseinstellungen konfigurieren. Beim Start über das YaST-Kontrollzentrum mithilfe von *System* → *Power-Management* wird das erste Dialogfeld des Moduls geöffnet (siehe [Abbildung 29.1](#), „Schemaauswahl“ (S. 586)).

Abbildung 29.1 Schemaauswahl



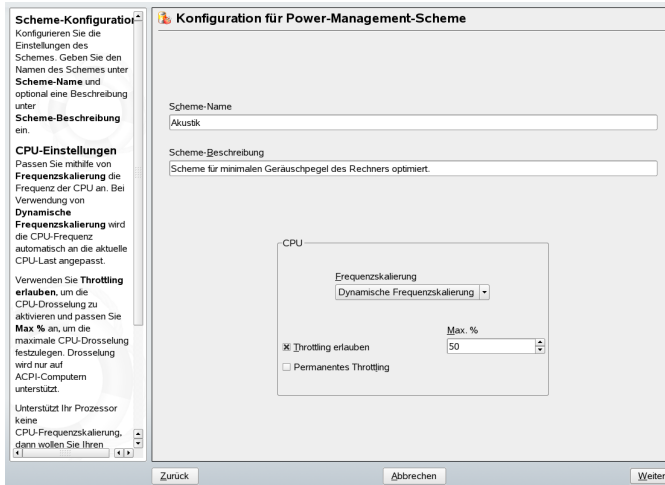
Dieses Dialogfeld dient zur Auswahl der Schemata für Akku- und Netzbetrieb. Um die Schemata zu ergänzen oder zu ändern, klicken Sie auf *Schemes bearbeiten*. Dadurch wird ein Überblick über die vorhandenen Schemata geöffnet, ähnlich wie in [Abbildung 29.2](#), „Überblick über vorhandene Schemata“ (S. 587) gezeigt.

Abbildung 29.2 Überblick über vorhandene Schemata



Wählen Sie in der Übersicht das zu ändernde Schema aus und klicken Sie auf *Bearbeiten*. Um ein neues Schema zu erstellen, klicken Sie auf *Hinzufügen*. In beiden Fällen öffnet sich das in [Abbildung 29.3](#), „Konfigurieren von Schemata“ (S. 588) gezeigte Dialogfeld.

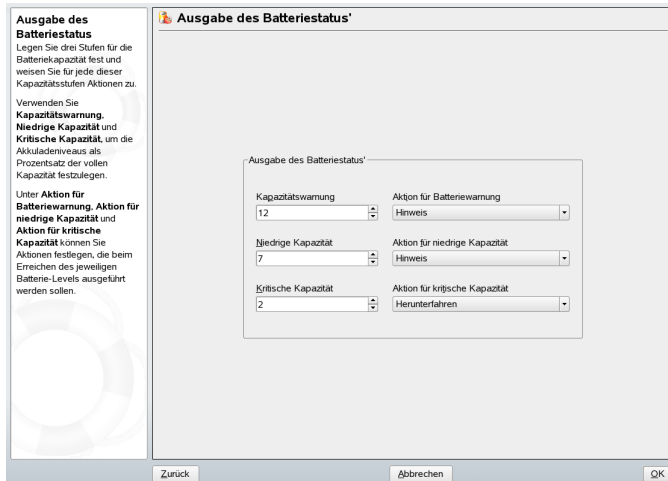
Abbildung 29.3 Konfigurieren von Schemata



Geben Sie zunächst einen geeigneten Namen und eine Beschreibung für das neue bzw. bearbeitete Schema ein. Bestimmen Sie, ob und wie die CPU-Leistung für dieses Schema gesteuert werden soll. Legen Sie fest, ob und in welchem Umfang Frequenzskalierung und Drosselung eingesetzt werden sollen und ob Prozesse mit niedriger Priorität bei der Anpassung der CPU-Frequenz ignoriert werden sollen. Legen Sie im anschließend angezeigten Dialogfeld für die Festplatte eine *Stand-by-Strategie* für höchstmögliche Leistung bzw. zum Energiesparen fest. Die *Akustik-Strategie* steuert den Geräuschpegel der Festplatte (nur von wenigen Festplatten unterstützt). Mithilfe der *Kühlstrategie* wird die zu verwendende Kühlmethode bestimmt. Leider wird diese Art von Wärmesteuerung selten vom BIOS unterstützt. Lesen Sie `/usr/share/doc/packages/powersave/powersave_manual.html#Thermal`, um zu erfahren, wie Sie den Ventilator und passive Kühlmethoden einsetzen können.

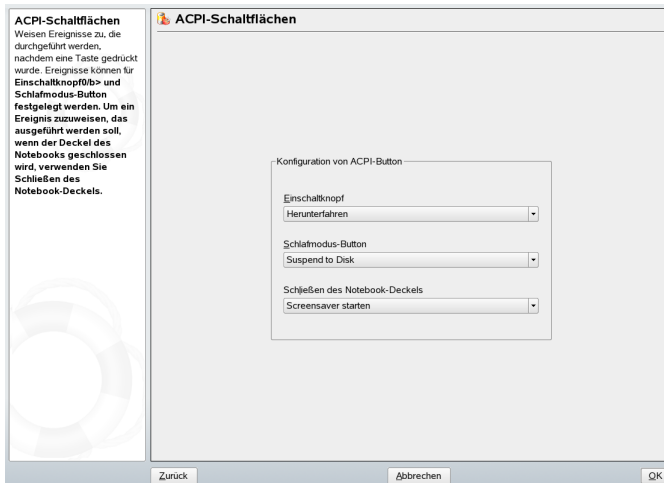
Globale Energieverwaltungseinstellungen können außerdem über das Anfangsdialogfeld festgelegt werden. Verwenden Sie dazu die Optionen *Akku-Warnung*, *ACPI-Einstellungen* oder *Suspend-Berechtigungen*. Diese Steuerelemente öffnen Sie über *Andere Einstellungen* und Auswahl des entsprechenden Menüeintrags. Klicken Sie auf *Akku-Warnung*, um das Dialogfeld für den Akku-Ladezustand aufzurufen, das Sie in [Abbildung 29.4](#), „Batteriestatus“ (S. 589) sehen können.

Abbildung 29.4 Batteriestatus



Das BIOS des Systems benachrichtigt das Betriebssystem jeweils, wenn der Ladezustand unter bestimmte, festlegbare Grenzwerte fällt. In diesem Dialogfeld können Sie drei Grenzwerte festlegen: *Kapazitätswarnung*, *Niedrige Kapazität* und *Kritische Kapazität*. Wenn der Ladezustand unter diese Grenzwerte fällt, werden bestimmte Aktionen ausgelöst. In der Regel lösen die ersten beiden Zustände lediglich eine Benachrichtigung an den Benutzer aus. Beim dritten, kritischen Ladezustand, wird das Herunterfahren ausgelöst, da die verbleibende Energie nicht für eine Fortsetzung des Systembetriebs ausreicht. Wählen Sie geeignete Ladezustände und die gewünschten Aktionen aus und klicken Sie dann auf *OK*, um zum Startdialogfeld zurückzukehren.

Abbildung 29.5 ACPI-Schaltflächen



Rufen Sie das Dialogfeld zur Konfiguration der ACPI-Schalter mithilfe von *ACPI-Einstellungen* auf. Browsen. Die Einstellungen für die ACPI-Schalter legen fest, wie das System auf bestimmte Schalter reagieren soll. Konfigurieren Sie die Systemreaktion auf das Drücken des Netzschalters, des Energiespar-Schalters und das Schließen des Notebookdeckels. Klicken Sie auf *OK*, um die Konfiguration abzuschließen und zum Startdialogfeld zurückzukehren.

Klicken Sie auf *Suspend aktivieren*, um ein Dialogfeld aufzurufen, in dem Sie festlegen können, ob und wie die Benutzer dieses Systems die Suspend- bzw. Stand-by-Funktion verwenden dürfen. Durch Klicken auf *OK* gelangen Sie zurück in das Hauptdialogfeld. Klicken Sie erneut auf *OK*, um das Modul zu beenden und die festgelegten Energieverwaltungseinstellungen zu bestätigen.

Drahtlose Kommunikation

Über Wireless LAN kann die Kommunikation zwischen SUSE® Linux Enterprise-Computern hergestellt werden. Dieses Kapitel enthält eine Einführung in die Grundlagen kabelloser Netzwerke und deren grundlegende Konfiguration.

30.1 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 30.1 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

Name	Band (GHz)	Maximale Übertragungsrate (MBit/s)	Hinweis
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.

30.1.1 Hardware

802.11-Karten werden von SUSE® Linux Enterprise 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:

- Aironet 4500, 4800
- Atheros 5210, 5211, 5212
- Atmel at76c502, at76c503, at76c504, at76c506
- Intel PRO/Wireless 2100, 2200BG, 2915ABG
- Intersil Prism2/2.5/3
- Intersil PrismGT
- Lucent/Agere Hermes
- Ralink RT2400, RT2500
- 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 umfassende Liste mit WLAN-Karten und den von ihnen verwendeten Chips sind auf der Website von *AbsoluteValue Systems* unter http://www.linux-wlan.org/docs/wlan_adapters.html.gz verfügbar. <http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz> bietet einen Überblick über die verschiedenen WLAN-Chips.

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 SUSE Linux Enterprise 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`.

30.1.2 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 weisen ein Verwaltungselement auf: 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. 601)), 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.

Offen

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. 596)) 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 Verfahren zur Verbindungsherstellung und Authentifizierung beim Server: 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.

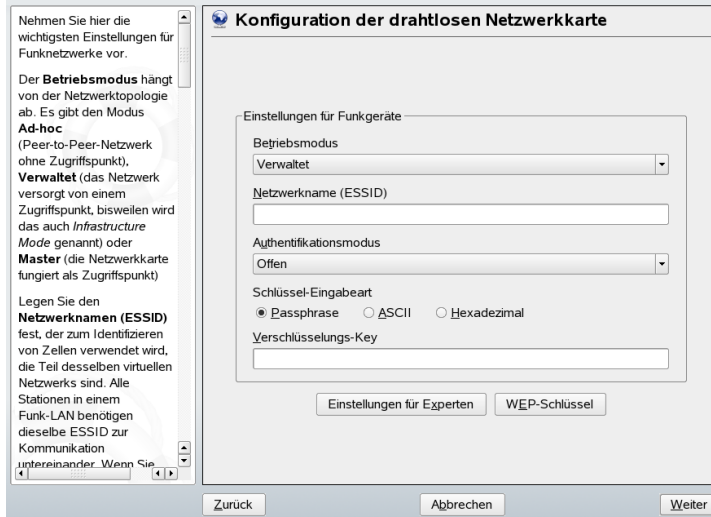
CCMP (in IEEE 802.11i definiert)

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.

30.1.3 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 30.1, „YaST: Konfigurieren der WLAN-Karte“](#) (S. 597)) die Grundeinstellungen für den WLAN-Betrieb vor:

Abbildung 30.1 YaST: Konfigurieren der WLAN-Karte



Betriebsmodus

Eine Station kann in drei verschiedenen Modi in ein WLAN integriert werden. Der geeignete Modus hängt von der Art des Netzwerks ab, in dem die Kommunikation erfolgen soll: *Ad-hoc* (Peer-to-Peer-Netzwerk ohne Zugriffspunkt), *Verwaltet* (Netzwerk wird über einen Zugriffspunkt verwaltet) oder *Master* (Ihre Netzwerkkarte sollte 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.

Authentifikationsmodus

Wählen Sie eine geeignete Authentifizierungsmethode für Ihr Netzwerk aus: *Offen*, *Gemeinsamer Schlüssel*, *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. 596) und „[Sicherheit](#)“ (S. 601).

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 Listenbereich unten im Dialogfeld können bis zu vier verschiedene Schlüssel angegeben werden, die Ihre Station für die Verschlüsselung verwenden soll. Wählen Sie *Als Standard festlegen*, um einen davon als Standardschlüssel festzulegen. Wenn Sie hier keine Auswahl treffen, verwendet YaST den als erstes eingegebenen Schlüssel als Standardschlüssel. Wenn der Standardschlüssel gelöscht wird, muss einer der anderen Schlüssel manuell als Standardschlüssel gekennzeichnet werden. Klicken Sie auf *Bearbeiten*, um bestehende Listeneinträge zu bearbeiten oder neue Schlüssel zu erstellen. In diesem Fall werden Sie über ein Popup-Fenster dazu aufgefordert, einen Eingabetyp auszuwählen (*Passwortsatz*, *ASCII* oder *Hexadezimal*). Geben Sie bei Verwendung von *Passwortsatz* ein Wort oder eine Zeichenkette ein, aus der ein Schlüssel mit der zuvor festgelegten Länge erstellt wird. *ASCII* erfordert die Eingabe von 5 Zeichen für einen 64-Bit-Schlüssel

und von 13 Zeichen für einen 128-Bit-Schlüssel. Bei *Hexadezimal* geben Sie 10 Zeichen für einen 64-Bit-Schlüssel bzw. 26 Zeichen für einen 128-Bit-Schlüssel in Hexadezimalnotation ein.

WPA-PSK

Für die Eingabe eines Schlüssels für WPA-PSK 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 diese Dateien auf `0600` (Lesen und Schreiben nur für Eigentümer).

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, geben Sie *any*, *MD5*, *GTC*, *CHAP*, *PAP*, *MSCHAPv1* oder *MSCHAPv2* an. Wenn Sie PEAP ausgewählt haben, geben Sie *any*, *MD5*, *GTC* oder *MSCHAPv2* an. *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:

Kanal

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.

30.1.4 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.

30.1.5 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 mithilfe des Dienstprogramms `iwconfig` auf der Kommandozeile (Feld `Link-Qualit t`) oder mithilfe von `KInternet`

in KDE überprüfen. Bei Problemen mit der Signalqualität sollten Sie versuchen, die Geräte an einer anderen Position einzurichten oder die Antennen der Zugriffspunkte neu zu positionieren. Hilfsantennen, die den Empfang erheblich verbessern sind für eine Reihe von PCMCIA-WLAN-Karten erhältlich. Die vom Hersteller angegebene Rate, beispielsweise 54 MBit/s, ist ein Nennwert, der für das theoretische Maximum steht. IN der Praxis beträgt der maximale Datendurchsatz nicht mehr als die Hälfte dieses Werts.

Sicherheit

Wenn Sie ein drahtloses Netzwerk einrichten möchten, sollten Sie bedenken, dass jeder, der sich innerhalb der Übertragungreichweite befindet, problemlos auf das Netzwerk zugreifen kann, sofern keine Sicherheitsmaßnahmen implementiert sind. Daher sollten Sie auf jeden Fall eine Verschlüsselungsmethode aktivieren. Alle WLAN-Karten und Zugriffspunkte unterstützen WEP-Verschlüsselung. Dieses Verfahren bietet zwar keine absolute Sicherheit, es stellt jedoch durchaus ein Hindernis für mögliche Angreifer dar. WEP ist für den privaten Gebrauch in der Regel ausreichend. WPA-PSK bietet noch größere Sicherheit, es ist jedoch in älteren Zugriffspunkten und Routern mit WLAN-Funktionen nicht implementiert. Auf einigen Geräten kann WPA mithilfe einer Firmware-Aktualisierung implementiert werden. Außerdem unterstützt Linux WPA nicht auf allen Hardware-Komponenten. Zum Zeitpunkt der Erstellung dieser Dokumentation funktionierte WPA nur bei Karten mit folgenden Arten von Chips: Atheros, Intel PRO/Wireless oder Prism2/2.5/3. Bei Prism2/2.5/3 funktioniert WPA nur bei Verwendung des hostap-Treibers (siehe „[Probleme mit Prism2-Karten](#)“ (S. 602)). 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.

30.1.6 Fehlerbehebung

Wenn Ihre WLAN-Karte nicht reagiert, überprüfen Sie, ob Sie die benötigte Firmware heruntergeladen haben. Informationen finden Sie in [Abschnitt 30.1.1](#), „[Hardware](#)“ (S. 592). 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`.

WPA

WPA-Unterstützung ist bei SUSE Linux Enterprise relativ neu und befindet sich noch in der Entwicklungsphase. Daher unterstützt YaST nicht die Konfiguration aller WPA-Authentifizierungsmethoden. Nicht alle WLAN-Karten und -Treiber unterstützen WPA. Bei einigen Karten ist zur Aktivierung von WPA eine Firmware-Aktualisierung erforderlich. Wenn Sie WPA verwenden möchten, lesen Sie `/usr/share/doc/packages/wireless-tools/README.wpa`.

30.1.7 Weitere 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. Siehe http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html.

Teil 4. Dienste

Grundlegendes zu Netzwerken

31

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 31.1](#), „[Verschiedene Protokolle aus der TCP/IP-Familie](#)“ (S. 606) 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.

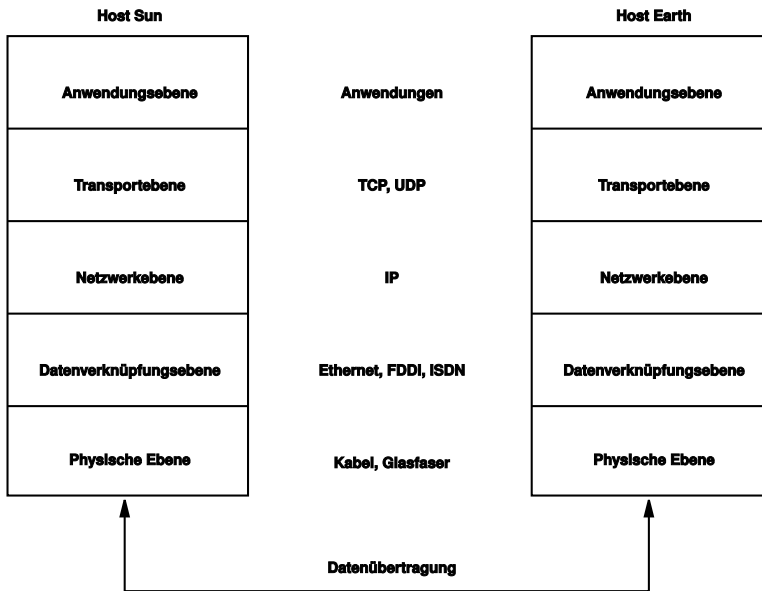
RFC ist das Akronym für *Request for Comments*. RFCs sind Dokumente, die unterschiedliche Internetprotokolle und Implementierungsverfahren für das Betriebssystem und seine Anwendungen beschreiben. Die RFC-Dokumente beschreiben das Einrichten der Internetprotokolle. Weitere Informationen zu diesen Protokollen finden Sie in den entsprechenden RFC-Dokumenten. Diese sind online unter <http://www.ietf.org/rfc.html> verfügbar.

Tabelle 31.1 *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, unsicheres 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 steuert das Verhalten des Computers bei der Implementierung von IP-Multicast.

Der Datenaustausch findet wie in [Abbildung 31.1](#), „Vereinfachtes Schichtmodell für TCP/IP“ (S. 607) 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 31.1 Vereinfachtes Schichtmodell für TCP/IP



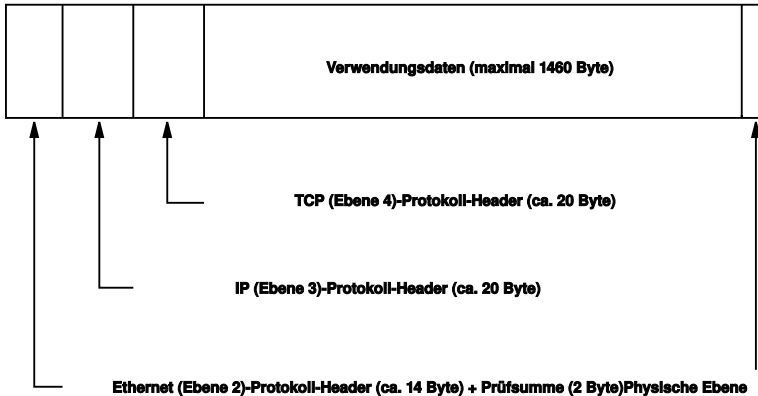
Dieses Diagramm bietet für jede Schicht ein oder zwei Beispiele. Die Schichten sind nach *Abstraktionsstufen* sortiert. Die unterste Schicht ist sehr Hardware-nah. Die oberste Schicht ist beinahe vollständig von der Hardware losgelöst. Jede Schicht hat ihre eigene spezielle Funktion. Die speziellen Funktionen 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 31.2](#), „TCP/IP-Ethernet-Paket“ (S. 608) dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

Abbildung 31.2 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.

31.1 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 31.2](#), „IPv6 – Das Internet der nächsten Generation“ (S. 612).

31.1.1 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 31.1](#), „IP-Adressen schreiben“ (S. 609) dargestellt geschrieben.

Beispiel 31.1 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.

31.1.2 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 31.2](#), „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 610). 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 31.2](#), „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 610) könnte das erste Netz mit 24 Bit auch als 192.168.0.0/24 geschrieben werden.

Beispiel 31.2 *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 der Zugriff auf sie erfolgt direkt. 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 erreichen oder ihre TTL-Zeit (Time to Live) abgelaufen ist.

Tabelle 31.2 *Spezifische Adressen*

Adresstyp	Beschreibung
Netzwerkbasiss-adresse	Dies ist die Netzmaske, die durch UND mit einer Netzwerkadresse verknüpft ist, wie in Beispiel 31.2 , „Verknüpfung von IP-Adressen mit der Netzmaske“ (S. 610) unter <code>Ergebnis</code> 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 Ergebnis im obigen Beispiel würde 192.168.0.255 lauten. Diese Adresse kann keinem Host zugewiesen 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 31.3, „Private IP-Adressdomänen“](#) (S. 611) aufgelistet.

Tabelle 31.3 *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

31.2 IPv6 – Das Internet der nächsten Generation

WICHTIG: IBM-System z: IPv6-Unterstützung

IPv6 wird von den CTC- und IUCV-Netzwerkverbindungen der IBM-System z-Hardware nicht unterstützt.

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. Es gehen auch einige IP-Adressen verloren, die aufgrund der Art, wie Netzwerke organisiert werden, 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 erforderlich sind: die Broadcast- und die Netzwerkbasisisadresse.

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.

31.2.1 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 Billionen 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 31.2.2, „Adresstypen und -struktur“](#) (S. 614).

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. Dadurch können Benutzer problemlos auf mehrere Netzwerke zugreifen, was beispielsweise mit den von Mobilfunkunternehmen angebotenen internationalen Roaming-Diensten vergleichbar ist. Wenn Sie Ihr Mobiltelefon mit ins Ausland nehmen, meldet sich das Telefon automatisch bei dem fremden Dienst an, sobald Sie dessen Bereich betreten, sodass Sie überall unter Ihrer Rufnummer erreichbar sind und Anrufe genauso wie in Ihrem Heimatland tätigen können.

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. Siehe [Abschnitt 31.2.3](#), „Koexistenz von IPv4 und IPv6“ (S. 619). 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 erlaubt einen sehr viel feineren Ansatz, indem es Servern ermöglicht, Hosts über *Multicasting* anzusprechen, d. h., sie sprechen mehrere Hosts als Teile einer Gruppe an. Dies unterscheidet sich von der 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.

31.2.2 Adresstypen und -struktur

Wie bereits erwähnt weist das aktuelle IP-Protokoll zwei wichtige Aspekte nicht auf: Es gibt einen zunehmenden Mangel an IP-Adressen und das Konfigurieren des Netzwerks sowie die Verwaltung der Routing-Tabellen wird immer komplexer und arbeitsintensiver. IPv6 löst das erste Problem durch die Erweiterung des Adressraums auf 128 Bit. Das zweite Problem wird durch die Einführung einer hierarchischen Adressstruktur behoben, die mit weiteren hoch entwickelten Techniken zum Zuordnen von Netzwerkadressen sowie mit dem *Multihoming* (der Fähigkeit, einem Gerät mehrere Adressen zuzuordnen und so den Zugriff auf mehrere Netzwerke zu ermöglichen) kombiniert wird.

Bei der Arbeit mit IPv6 ist es hilfreich, die drei unterschiedlichen Adresstypen zu kennen:

Unicast

Adressen dieses Typs werden genau einer Netzwerkschnittstelle zugeordnet. Pakete mit derartigen Adressen werden nur einem Ziel zugestellt. Unicast-Adressen werden dementsprechend zum Übertragen von Paketen an einzelne Hosts im lokalen Netzwerk oder im Internet verwendet.

Multicast

Adressen dieses Typs beziehen sich auf eine Gruppe von Netzwerkschnittstellen. Pakete mit derartigen Adressen werden an alle Ziele zugestellt, die dieser Gruppe angehören. Multicast-Adressen werden hauptsächlich von bestimmten Netzwerkdiensten für die Kommunikation mit bestimmten Hostgruppen verwendet, wobei diese gezielt adressiert werden.

Anycast

Adressen dieses Typs beziehen sich auf eine Gruppe von Schnittstellen. Pakete mit einer derartigen Adresse werden gemäß den Prinzipien des zugrunde liegenden Routing-Protokolls dem Mitglied der Gruppe gesendet, das dem Absender am nächsten ist. Anycast-Adressen werden verwendet, damit Hosts Informationen zu Servern schneller abrufen können, die im angegebenen Netzwerkbereich bestimmte Dienste anbieten. Sämtliche Server desselben Typs verfügen über dieselbe Anycast-Adresse. Wann immer ein Host einen Dienst anfordert, erhält er eine Antwort von dem vom Routing-Protokoll ermittelten nächstgelegenen Server. Wenn dieser Server aus irgendeinem Grund nicht erreichbar ist, wählt das Protokoll automatisch den zweitnächsten Server, dann den dritten usw. aus.

Eine IPv6-Adresse besteht aus acht vierstelligen Feldern, wobei jedes 16 Bit repräsentiert, und wird in hexadezimaler Notation geschrieben. Die Felder werden ebenfalls durch Doppelpunkte (:) getrennt. Alle führenden Null-Byte innerhalb eines bestimmten Felds können ausgelassen werden, alle anderen Nullen jedoch nicht. Eine weitere Konvention ist, dass mehr als vier aufeinander folgenden Null-Byte mit einem doppelten Doppelpunkt zusammengefasst werden können. Pro Adresse ist jedoch nur ein :: zulässig. ***DELETE***. Diese Art der Kurznotation wird in [Beispiel 31.3](#), „[Beispiel einer IPv6-Adresse](#)“ (S. 616) dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

Beispiel 31.3 *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 31.4](#), „IPv6-Adressen mit Angabe der Präfix-Länge“ (S. 616) 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 31.4 *IPv6-Adressen mit Angabe der Präfix-Länge*

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige von diesen sind in [Tabelle 31.4](#), „Unterschiedliche IPv6-Präfixe“ (S. 616) aufgeführt.

Tabelle 31.4 *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 gibt es folgende Adressräume: 2001::/16 (Production Quality Address Space) und 2002::/16 (6to4 Address Space).

Präfix (hexadezimal)	Definition
<code>fe80::/10</code>	Link-local-Adressen. Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.
<code>fec0::/10</code>	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 <code>10.x.x.x</code>).
<code>ff</code>	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)

Diese Adresse verwendet ein Host 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 31.2.3](#), „Koexistenz von IPv4 und IPv6“ (S. 619)). 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 ($fe80::/10$) und die Schnittstellen-ID der Netzwerkkarte aus. Der Mittelteil der Adresse besteht aus Null-Bytes. Diese Art Adresse wird von den Autokonfigurationsmethoden verwendet, um Hosts im selben Subnetz anzusprechen.

site-local

Pakete mit diesem Adresstyp werden an andere Subnetze weitergeleitet, müssen jedoch innerhalb des firmeneigenen Netzwerks verbleiben. Solche Adressen werden für Intranets eingesetzt und sind ein Äquivalent zu den privaten IPv4-Adressen. Neben einem definierten Präfix ($fec0::/10$) 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 davon kann mithilfe der

MAC-Adresse und einem bekannten Präfix vollautomatisch konfiguriert werden, sodass gleich nach 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.

31.2.3 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 31.2.2, „Adresstypen und -struktur“](#) (S. 614)) sind hier die besten Lösungen.

Einzelne IPv6-Hosts im (weltweiten) IPv4-Netz tauschen ihre Daten über Tunnel aus. Beim Tunneling werden IPv6-Pakete in IPv4-Pakete verpackt, um sie über ein IPv4-Netzwerk transportieren zu können. 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.

WICHTIG: Die 6Bone-Initiative

Mitten im „altmodischen“ Internet existiert ein weltweit verteiltes Netzwerk von IPv6-Subnetzen, die über Tunnel miteinander verbunden sind. Dies ist das 6Bone-Netzwerk (<http://www.6bone.net>), eine IPv6-Testumgebung, die von Programmierern und ISPs genutzt werden kann, die IPv6-basierte Dienste entwickeln und anbieten möchten, um Erfahrungen mit dem neuen Protokoll zu sammeln. Weitere Informationen finden Sie auf den Projektseiten von 6Bone im Internet.

31.2.4 IPv6 konfigurieren

Um IPv6 zu konfigurieren, müssen Sie auf den einzelnen Arbeitsstationen in der Regel keine Änderungen vornehmen. Dazu muss jedoch die IPv6-Unterstützung geladen werden. Geben Sie hierzu den Befehl `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)`".

31.2.5 Weitere 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.ngnet.it/e/cosa-ipv6.php>

Eine Artikelserie mit einer gut geschriebenen Einführung in das IPv6-Konzept. Eine gute Grundlage für das Thema.

<http://www.bieringer.de/linux/IPv6/>

Hier finden Sie den Beitrag "Linux IPv6 HOWTO" und viele verwandte Links zum Thema.

<http://www.6bone.net/>

Besuchen Sie diese Site, wenn Sie eine Verbindung zu einem getunnelten IPv6-Netzwerk benötigen.

<http://www.ipv6.org/>

Alles rund um IPv6.

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).

31.3 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.

Schauen wir uns einmal einen vollständigen Namen an, z. B. `earth.example.com`, geschrieben im Format `hostname.domain`. 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 annimmt, der so genannte *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 SUSE® Linux Enterprise ist in [Kapitel 34, *Domain Name System \(DNS\)*](#) (S. 681) 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.

31.4 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 31.6, „Manuelle Netzwerkkonfiguration“](#) (S. 647).

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 SUSE Linux Enterprise unterstützten Netzwerkverbindungen beschrieben.

TIPP: IBM-System z: Hotplug-fähige Netzwerkkarten

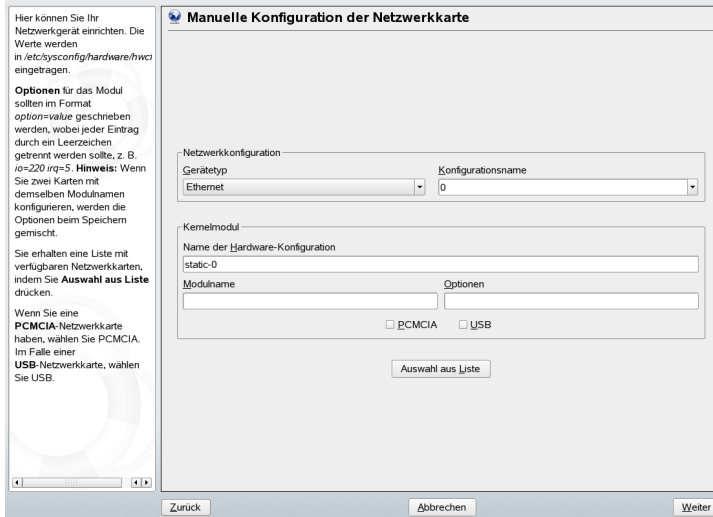
Auf den IBM-System z-Plattformen werden Hotplug-fähige Netzwerkkarten unterstützt, aber nicht deren automatische Netzwerkkonfiguration über DHCP (wie beim PC). Nach der Erkennung muss die Schnittstelle manuell konfiguriert werden.

31.4.1 Konfigurieren der Netzwerkkarte mit YaST

Zum Konfigurieren der verkabelten sowie der drahtlosen Netzwerkkarte in YaST wählen Sie *Netzwerkgeräte* → *Netzwerkkarte*. Nach dem Starten des YaST-Moduls gelangen Sie in eine allgemeine Übersicht zur Netzwerkkonfiguration. Entscheiden Sie, ob YaST oder der NetworkManager für die Verwaltung all Ihrer Netzwerkgeräte verwendet werden soll. Wenn Sie Ihr Netzwerk auf traditionelle Weise mit YaST konfigurieren möchten, aktivieren Sie *Traditionelle Methode mit ifup* und klicken Sie auf *Weiter*. Um den NetworkManager zu verwenden, aktivieren Sie *Benutzergesteuert mithilfe von NetworkManager* und klicken Sie auf *Weiter*. Detaillierte Informationen zum NetworkManager finden Sie in [Abschnitt 31.5, „Verwalten der Netzwerkverbindungen mit dem NetworkManager“](#) (S. 644).

Im oberen Bereich des nächsten Dialogfelds wird eine Liste mit allen für die Konfiguration verfügbaren Netzwerkkarten angezeigt. Alle ordnungsgemäß erkannten Karten werden mit ihren Namen aufgeführt. Wenn Sie die Konfiguration des ausgewählten Geräts ändern möchten, klicken Sie auf *Bearbeiten*. Nicht erkannte Geräte können über *Hinzufügen*, wie in [„Konfigurieren einer unerkannten Netzwerkkarte“](#) (S. 632) beschrieben, konfiguriert werden.

Abbildung 31.3 Konfigurieren einer Netzwerkkarte



Ändern der Konfiguration einer Netzwerkkarte

Wenn Sie die Konfiguration einer Netzwerkkarte ändern möchten, wählen Sie die Karte aus der Liste der erkannten Karten im YaST-Konfigurationsmodul für Netzwerkkarten aus und klicken Sie auf *Bearbeiten*. Das Dialogfeld *Konfiguration der Netzwerkkarte* wird angezeigt. Hier können Sie die Kartenkonfiguration auf den Registerkarten *Adresse* und *Allgemein* anpassen. Genauere Informationen zur drahtlosen Kartenkonfiguration finden Sie unter [Abschnitt 30.1.3, „Konfiguration mit YaST“](#) (S. 596).

Über die Registerkarte *Adresse* können Sie folgende Aspekte Ihrer Netzwerkkartenkonfiguration anpassen.

Konfiguration des Adresstyps und IP-Adresseninformationen

Je nach dem Zweck Ihrer SUSE Linux Enterprise-Maschine sollten Sie sich entscheiden, ob eine statische oder eine dynamische Adresse verwendet wird. Die meisten Client-Konfigurationen in Unternehmens- oder Heimnetzwerken funktionieren gut mit der dynamischen Einrichtung über DHCP. Server oder Router sollten jedoch statische IP-Adressen verwenden. Detaillierte Informationen finden Sie in [„Konfigurieren der IP-Adressen“](#) (S. 627).

Hostname und DNS

Damit Ihre SUSE Linux Enterprise-Maschine sich in ein Netzwerk integrieren lässt, müssen Sie den Hostnamen und den Namensdienst angeben. Wird DHCP für die Netzwerkeinrichtung gewählt, werden diese Einstellungen automatisch vorgenommen. Detaillierte Informationen finden Sie in „[Konfigurieren des Hostnamens und DNS](#)“ (S. 628).

Routing

Sie stellen sicher, dass der Netzwerkverkehr von Ihrer Maschine den richtigen Weg nimmt, indem Sie ein Standard-Gateway und gegebenenfalls eine Route festlegen. Wird DHCP verwendet, werden diese Einstellungen automatisch vorgenommen. Detaillierte Informationen finden Sie in „[Konfigurieren des Routing](#)“ (S. 629).

Erweiterte Optionen

Bei manchen Hardwaregeräten sind zur korrekten Funktion zusätzliche Optionen für den Kernel erforderlich. Diese Optionen geben Sie in einem Dialogfeld an. Wählen Sie dazu *Hardwaredetails*. Einzelheiten finden Sie unter „[Hinzufügen spezieller Hardware-Optionen](#)“ (S. 630).

Die standardmäßig ausgeführte DHCP-Konfiguration eignet sich für die meisten Fälle. Wenn Sie die DHCP-Konfiguration genauer abstimmen möchten, verwenden Sie *DHCP-Optionen*. Einzelheiten finden Sie unter „[Konfigurieren der IP-Adressen](#)“ (S. 627).

Verfügt Ihre Maschine über mehrere IP-Adressen, sollten Sie diese mithilfe von *Zusätzliche Adressen* festlegen. Siehe „[Konfigurieren der IP-Adressen](#)“ (S. 627).

Auf der Registerkarte *Allgemein* passen Sie folgende Elemente an:

Firewall-Zone

Entscheiden Sie, ob Ihre Netzwerkschnittstelle von einer Firewall geschützt werden soll. Detaillierte Informationen finden Sie in „[Konfigurieren der Firewall](#)“ (S. 631).

Geräte-Aktivierung

Je nach den verwendeten Anwendungen oder Skripten zur Steuerung Ihrer Netzwerkkomponenten sollten Sie den entsprechenden Startmodus einstellen. Detaillierte Informationen finden Sie in „[Starten des Geräts](#)“ (S. 630).

MTU

Legen Sie die maximale Übertragungsrate (MTU) für Ihre Schnittstelle fest. Normalerweise können Sie diese Einstellung beruhigt leer lassen und die Standardein-

stellung übernehmen. Ändern Sie diesen Wert nur, wenn es Ihre Einrichtung speziell erfordert.

Konfigurieren der IP-Adressen

Wenn möglich, werden die verkabelten Netzwerkkarten während der Installation automatisch konfiguriert, um die automatische Adresseneinrichtung, DHCP, zu verwenden.

ANMERKUNG: IBM-System z und DHCP

Auf IBM System z-Plattformen wird die DHCP-basierte Adressenkonfiguration nur mit Netzwerkkarten unterstützt, die über eine MAC-Adresse verfügen. Das ist nur der Fall bei OSA- und OSA Express-Karten.

DHCP sollten Sie auch verwenden, wenn Sie eine DSL-Leitung verwenden, Ihr ISP Ihnen aber keine statische IP-Adresse zugewiesen hat. Wenn Sie DHCP nutzen möchten, konfigurieren Sie die Details in *Optionen für DHCP-Client*. Wählen Sie dafür in der Registerkarte *Adresse* die Option *Erweitert → DHCP-Optionen*. Legen Sie fest, ob der DHCP-Server immer auf Broadcast-Anforderungen antworten soll. Außerdem können Sie optional eine Kennung angeben. In einer virtuellen Hostumgebung, in der unterschiedliche Hosts über dieselbe Schnittstelle kommunizieren, werden diese anhand einer Kennung unterschieden.

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 eine Karte aus der Liste der erkannten Karten im YaST-Konfigurationsmodul für Netzwerkkarten aus und klicken Sie auf *Bearbeiten*.
- 2 Wählen Sie in der Registerkarte *Adresse* die Option *Konfiguration der statischen Adresse*.
- 3 Geben Sie die *IP-Adresse* und die *Subnetzmaske* ein.
- 4 Klicken Sie auf *Weiter*.
- 5 Klicken Sie zum Aktivieren der Konfiguration noch einmal auf *Weiter*.

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 eine Karte aus der Liste der erkannten Karten im YaST-Konfigurationsmodul für Netzwerkkarten aus und klicken Sie auf *Bearbeiten*.
- 2 Wählen Sie in der Registerkarte *Adresse* die Option *Erweitert → Konfiguration der statischen Adresse*.
- 3 Klicken Sie auf *Hinzufügen*.
- 4 Geben Sie den *Aliasnamen*, die *IP-Adresse* und die *Netzmaske* ein.
- 5 Klicken Sie auf *OK*.
- 6 Klicken Sie noch einmal auf *OK*.
- 7 Klicken Sie auf *Weiter*.
- 8 Klicken Sie zum Aktivieren der Konfiguration noch einmal auf *Weiter*.

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 Wählen Sie eine Karte aus der Liste der erkannten Karten im YaST-Konfigurationsmodul für Netzwerkkarten aus und klicken Sie auf *Bearbeiten*.
- 2 Klicken Sie in der Registerkarte *Adresse* auf *Hostname und Namensserver*.

- 3 Zum Deaktivieren der DHCP-gesteuerten Hostnamenkonfiguration deaktivieren Sie die Option *Hostnamen über DHCP ändern*.
- 4 Geben Sie den *Hostnamen* und gegebenenfalls den *Domänennamen* an.
- 5 Wenn Sie die DHCP-gesteuerten Updates der Namenserverliste deaktivieren möchten, deaktivieren Sie die Option *Namenserver und Suchliste über DHCP aktualisieren*.
- 6 Geben Sie die Namenserver und Domänensuchlisten an.
- 7 Klicken Sie auf *OK*.
- 8 Klicken Sie auf *Weiter*.
- 9 Klicken Sie zum Aktivieren der Konfiguration noch einmal auf *Weiter*.

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 Wählen Sie eine Karte aus der Liste der erkannten Karten im YaST-Konfigurationsmodul für Netzwerkkarten aus und klicken Sie auf *Bearbeiten*.
- 2 Klicken Sie in der Registerkarte *Adresse* auf *Routing*.
- 3 Geben Sie die IP des *Standard-Gateways* ein.
- 4 Klicken Sie auf *OK*.
- 5 Klicken Sie auf *Weiter*.
- 6 Klicken Sie zum Aktivieren der Konfiguration noch einmal auf *Weiter*.

Hinzufügen spezieller Hardware-Optionen

Manchmal sind zur korrekten Funktion eines Netzwerkkartenmoduls spezielle Parameter erforderlich. Mit YaST legen Sie diese wie folgt fest:

- 1 Wählen Sie eine Karte aus der Liste der erkannten Karten im YaST-Konfigurationsmodul für Netzwerkkarten aus und klicken Sie auf *Bearbeiten*.
- 2 Wählen Sie in der Registerkarte *Adresse* die Option *Erweitert* → *Hardware-Details*.
- 3 Unter *Optionen* geben Sie die Parameter für Ihre Netzwerkkarte ein. Wenn zwei Karten konfiguriert werden, die dasselbe Modul verwenden, gelten die Parameter für beide.
- 4 Klicken Sie auf *OK*.
- 5 Klicken Sie auf *Weiter*.
- 6 Klicken Sie zum Aktivieren der Konfiguration noch einmal auf *Weiter*.

Starten des Geräts

Sie können 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 eine Karte aus der Liste der erkannten Karten im YaST-Konfigurationsmodul für Netzwerkkarten aus und klicken Sie auf *Bearbeiten*.
- 2 In der Registerkarte *Allgemein* wählen Sie den gewünschten Eintrag unter *Geräte-Aktivierung*.
- 3 Klicken Sie auf *Weiter*.
- 4 Klicken Sie zum Aktivieren der Konfiguration noch einmal auf *Weiter*.

Konfigurieren der Firewall

Sie müssen nicht die genaue Firewall-Konfiguration durchführen, wie unter [Abschnitt 44.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 906) 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 eine Karte aus der Liste der erkannten Karten im YaST-Konfigurationsmodul für Netzwerkkarten aus und klicken Sie auf *Bearbeiten*.
- 2 Öffnen Sie die Registerkarte *Allgemein* des Dialogfelds zur Netzwerkkonfiguration.
- 3 Legen Sie die Firewall-Zone fest, der Ihre Schnittstelle zugewiesen werden soll. Die folgenden Optionen stehen zur Verfügung:

Firewall deaktiviert

Die Firewall wird nicht ausgeführt. Verwenden Sie diese Option nur, wenn Ihre Maschine 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. Das ist die Standardoption.

- 4 Klicken Sie auf *Weiter*.
- 5 Aktivieren Sie die Konfiguration, indem Sie auf *Weiter* klicken.

Konfigurieren einer unerkannten Netzwerkkarte

Eventuell wird Ihre Karte nicht korrekt 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 *Hinzufügen*.
- 2 Wählen Sie für den *Gerätetyp* der Schnittstelle die Optionen *Konfigurationsname* und *Modulname*. 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 anderenfalls über die Option *Auswahl aus Liste* das Modell Ihrer Netzwerkkarte aus. YaST wählt dann automatisch das geeignete Kernelmodul für die Karte aus.

Name der Hardwarekonfiguration gibt den Namen der Datei `/etc/sysconfig/hardware/hwcfg-*` an, in der die Hardware-Einstellungen der Netzwerkkarte enthalten sind. Dazu gehören der Name des Kernelmoduls sowie die zum Initialisieren der Hardware erforderlichen Optionen.

- 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 *Konfiguration der statischen Adresse*. Dann geben Sie die *IP-Adresse* und *Subnetzmaske* ein. Hier können Sie auch den Hostnamen, Namensserver und die Routing-Details angeben (siehe „[Konfigurieren des Hostnamens und DNS](#)“ (S. 628) und „[Konfigurieren des Routing](#)“ (S. 629)).

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 30.1, „Wireless LAN“](#) (S. 591).

- 5 In der Registerkarte *Allgemein* legen Sie die *Firewall-Zone* und die *Geräte-Aktivierung* fest. Mit der Option *Benutzergesteuert* gewähren Sie gewöhnlichen Benutzern eine Verbindungskontrolle.
- 6 Klicken Sie auf *Weiter*.

7 Klicken Sie zum Aktivieren der neuen Netzwerkkonfiguration noch einmal auf *Weiter*.

Informationen zu den Konventionen für Konfigurationsnamen finden Sie auf der Manualpage `getcfg(8)`.

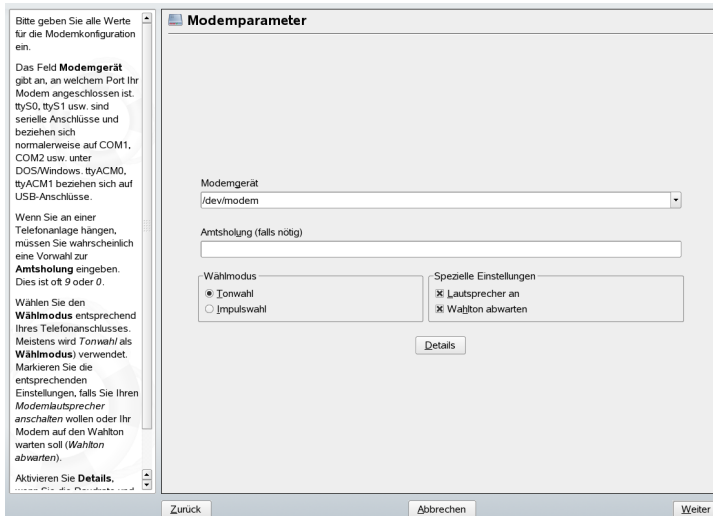
31.4.2 Modem

TIPP: IBM-System z: Modem

Die Konfiguration dieses Hardwaretyps wird auf den IBM System z-Plattformen nicht unterstützt.

Im YaST-Kontrollzentrum finden Sie unter *Netzwerkgeräte* die Modem-Konfiguration. Falls die automatische Erkennung fehlschlägt, öffnen Sie das Dialogfeld für die manuelle Konfiguration. Geben Sie in diesem Dialogfeld unter *Modem* die Schnittstelle an, mit der das Modem verbunden ist.

Abbildung 31.4 *Modemparameter*



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*. Um die Steuerung des Modems an den normalen Benutzer ohne root-Berechtigungen zu delegieren, aktivieren Sie *Benutzergesteuert*. 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 folgenden 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.

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.

Ignoranz-Modus

Diese Option ist standardmäßig aktiviert. Eingabeaufforderungen vom ISP-Server werden ignoriert, um den Verbindungsaufbau zu erleichtern.

Externe Firewall-Schnittstelle und Firewall neu starten

Mit diesen Optionen aktivieren Sie SUSEfirewall2 und sind für die Dauer der 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 *Beenden*.

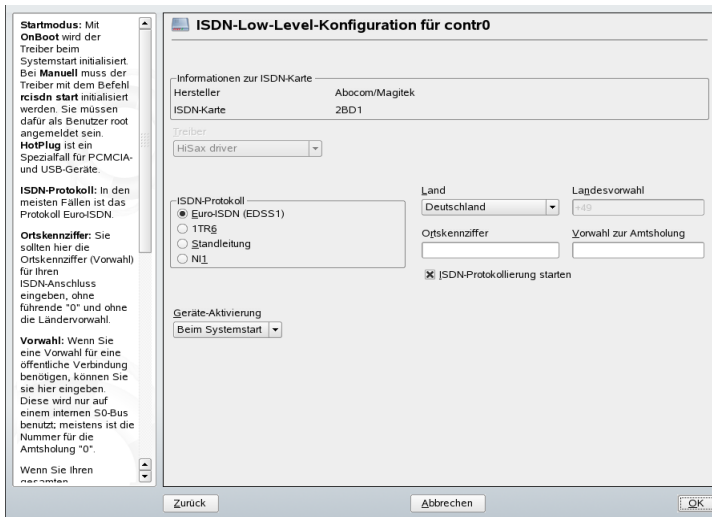
31.4.3 ISDN

TIPP: IBM-System z: ISDN

Die Konfiguration dieses Hardwaretyps wird auf den IBM System z-Plattformen nicht unterstützt.

Dieses Modul ermöglicht die Konfiguration einer oder mehrerer ISDN-Karten in Ihrem System. Wenn YaST Ihre ISDN-Karte nicht erkennt, wählen Sie sie 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 31.5 ISDN-Konfiguration

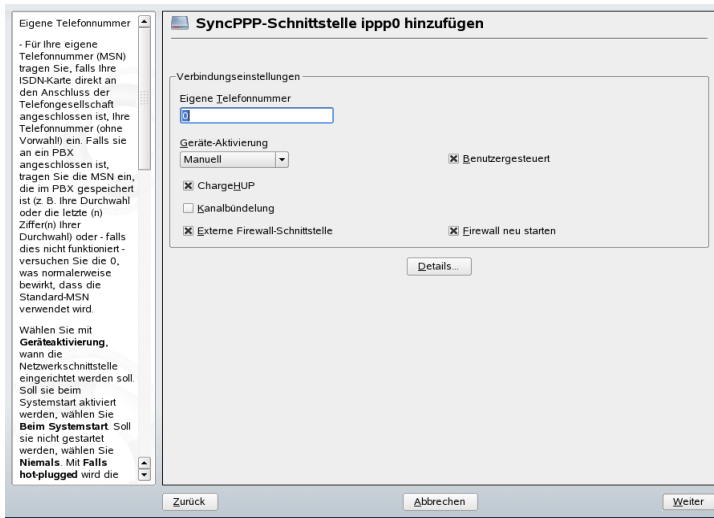


Wählen Sie im nächsten Dialogfeld, das in [Abbildung 31.5](#), „ISDN-Konfiguration“ (S. 636) dargestellt ist, das zu verwendende Protokoll. Der Standard ist *Euro-ISDN (EDSS1)*, aber für ältere oder größere Telefonanlagen wählen Sie *1TR6*. Für die USA gilt *NI1*. Wählen Sie das Land in dem dafür vorgesehenen Feld aus. Die entsprechende Landeskenntung wird im Feld daneben angezeigt. Geben Sie dann noch die *Ortsnetz-kennzahl* und ggf. die *Vorwahl zur Amtsholung* ein.

Startmodus legt fest, wie die ISDN-Schnittstelle gestartet werden soll: *Bei Systemstart* bewirkt, dass der ISDN-Treiber bei jedem Systemstart initialisiert wird. *Manuell* erfordert, dass Sie den ISDN-Treiber als `root` mit dem Befehl `rcisdn start` laden. *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 31.6 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 Ortsnetzkennzahl. 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. Um dem normalen Benutzer ohne Administratorberechtigung das Aktivieren oder Deaktivieren der Schnittstelle zu ermöglichen, wählen Sie *Benutzergesteuert*.

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 einer Einzelplatz-Arbeitsstation *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 Namenservers übergeben. Bei einer Einzelplatz-Arbeitsstation 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 Namenserver 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. Wählen Sie zum Aktivieren dieser Einstellungen *Beenden*.

31.4.4 Kabelmodem

TIPP: IBM-System z: Kabelmodem

Die Konfiguration dieses Hardwaretyps wird auf den IBM System z-Plattformen nicht unterstützt.

In einigen Ländern, z. B. in Österreich und in den USA, ist es nicht ungewöhnlich, dass der Zugriff auf das Internet über TV-Kabelnetzwerke erfolgt. 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.

Wählen Sie beim Konfigurieren der Netzwerkkarte je nach Anweisungen Ihres ISPs entweder *Automatische Adressenkonfiguration (mit DHCP)* oder *Konfiguration der statischen Adresse*. 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.

31.4.5 DSL

TIPP: IBM-System z: DSL

Die Konfiguration dieses Hardwaretyps wird auf den IBM System z-Plattformen nicht unterstützt.

Wählen Sie zum Konfigurieren des DSL-Geräts das YaST-Modul *DSL* unter *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

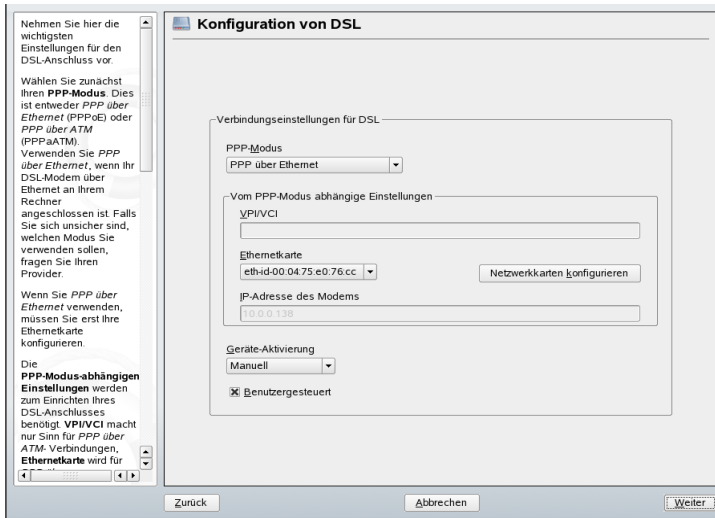
Beachten Sie bitte, dass die Konfiguration Ihres DSL-Zugangs mit PPPoE und PPTP eine korrekte Konfiguration der Netzwerkkarte voraussetzt. Falls dies nicht schon geschehen ist, konfigurieren Sie zunächst die Karte, indem Sie *Netzwerkkarten konfigurieren* (siehe [Abschnitt 31.4.1](#), „Konfigurieren der Netzwerkkarte mit YaST“ (S. 624)) auswählen. Die automatische IP-Adressvergabe erfolgt bei DSL zwar automatisch, aber nicht mit dem DHCP-Protokoll. Deshalb dürfen Sie auch nicht die Option *Automatische Adressenkonfiguration (mit DHCP)* 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 31.7 DSL-Konfiguration



Zu Beginn der DSL-Konfiguration (siehe [Abbildung 31.7](#), „DSL-Konfiguration“ (S. 641)) wählen Sie zunächst 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. Klicken Sie auf *Benutzergesteuert*, um dem normalen Benutzer ohne root-Berechtigungen das Aktivieren und Deaktivieren der Schnittstelle mit KIn-ternet zu ermöglichen. In diesem Dialogfeld können Sie außerdem Ihr Land und einen der dort ansässigen ISPs 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 einer Einzelplatz-Arbeitsstation *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 einer Einzelplatz-Arbeitsstation 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 erfolgt ähnlich wie die DSL-Konfiguration. Durch Auswahl von *T-Online* als Provider gelangen Sie in das YaST-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.

31.4.6 IBM-System z: Konfigurieren von Netzwerkgeräten

SUSE Linux Enterprise Server für IBM-System z unterstützt mehrere verschiedene Netzwerkschnittstellen. YaST kann zur Konfiguration dieser Schnittstellen verwendet werden.

Das qeth-hsi-Gerät

Wenn Sie dem installierten System eine `qeth-hsi` (IBM Hipersocket)-Schnittstelle hinzufügen möchten, starten Sie das YaST-Netzwerkkartenmodul (*Netzwerkgeräte* → *Netzwerkkarte*). Wählen Sie eines der Geräte mit der Bezeichnung *IBM Hipersocket* aus, um es als READ-Geräteadresse zu verwenden, und klicken Sie auf *Konfigurieren*. Im Dialogfeld *Konfiguration der Netzwerkadresse* geben Sie die IP-Adresse und die Netzmaske für die neue Schnittstelle an und verlassen Sie die Netzwerkkonfiguration, indem Sie auf *Weiter* und *Fertig stellen* klicken.

Das qeth-ethernet-Gerät

Wenn Sie dem installierten System eine `qeth-ethernet` (IBM OSA Express Ethernet Card)-Schnittstelle hinzufügen möchten, starten Sie das YaST-Netzwerkkartenmodul (*Netzwerkgeräte* → *Netzwerkkarte*). Wählen Sie eines der Geräte mit der Bezeichnung *IBM OSA Express Ethernet Card* aus, um es als READ-Geräteadresse zu verwenden, und klicken Sie auf *Konfigurieren*. Geben Sie den erforderlichen Port-Namen, einige zusätzliche Optionen (siehe *Linux für IBM-System z: Handbücher für Gerätetreiber*,

Funktionen und Befehle, <http://www.ibm.com/developerworks/linux/linux390/index.html>), Ihre IP-Adresse und eine entsprechende Netzmaske ein. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *Fertig stellen*.

Das ctc-Gerät

Wenn Sie dem installierten System eine `ctc` (IBM parallel CTC Adapter)-Schnittstelle hinzufügen möchten, starten Sie das YaST-Netzwerkkartenmodul (*Netzwerkgeräte* → *Netzwerkkarte*). Wählen Sie eines der Geräte mit der Bezeichnung *IBM parallel CTC Adapter* aus, um es als READ-Kanal zu verwenden, und klicken Sie auf *Konfigurieren*. Wählen Sie die *Geräteeinstellungen* für Ihre Geräte (gewöhnlich ist das *Kompatibilitätsmodus*). Geben Sie Ihre IP-Adresse und die IP-Adresse des entfernten Partners ein. Passen Sie gegebenenfalls die MTU-Größe mit *Erweitert* → *Besondere Einstellungen* an. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *Fertig stellen*.

WARNUNG

Die Nutzung dieser Schnittstelle ist veraltet. Diese Schnittstelle wird in künftigen Versionen von SUSE Linux Enterprise Server nicht unterstützt.

Das lcs-Gerät

Wenn Sie dem installierten System eine `lcs` (IBM OSA-2 Adapter)-Schnittstelle hinzufügen möchten, starten Sie das YaST-Netzwerkkartenmodul (*Netzwerkgeräte* → *Netzwerkkarte*). Wählen Sie eines der Geräte mit der Bezeichnung *IBM OSA-2 Adapter* und klicken Sie auf *Konfigurieren*. Geben Sie die erforderliche Portnummer, einige zusätzliche Optionen (siehe *Linux für IBM-System z: Handbücher für Gerätetreiber, Funktionen und Befehle*, <http://www.ibm.com/developerworks/linux/linux390/index.html>), Ihre IP-Adresse und eine entsprechende Netzmaske ein. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *Fertig stellen*.

Das IUCV-Gerät

Wenn Sie dem installierten System eine `iucv` (IUCV)-Schnittstelle hinzufügen möchten, starten Sie das YaST-Netzwerkkartenmodul (*Netzwerkgeräte* → *Netzwerkkarte*). Wählen Sie eines der Geräte mit der Bezeichnung *IUCV* und klicken Sie auf *Konfigurieren*. YaST fordert Sie auf, den Namen Ihres IUCV-Partners einzugeben. Geben Sie den Namen ein (beachten Sie die Groß-/Kleinschreibung) und wählen Sie

Weiter. Geben Sie Ihre IP-Adresse und die IP-Adresse des Partners ein. Passen Sie gegebenenfalls die MTU-Größe mit *Erweitert* → *Besondere Einstellungen* an. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *Fertig stellen*.

WARNUNG

Die Nutzung dieser Schnittstelle ist veraltet. Diese Schnittstelle wird in künftigen Versionen von SUSE Linux Enterprise Server nicht unterstützt.

31.5 Verwalten der Netzwerkverbindungen mit dem NetworkManager

Der NetworkManager ist die ideale Lösung für eine mobile Arbeitsstation. Wenn Sie viel unterwegs sind und den NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen Netzwerken zu verschwenden. Der NetworkManager stellt automatisch Verbindungen mit den ihm bekannten WLAN-Netzwerken her. Bei zwei oder gar mehreren Verbindungsmöglichkeiten stellt der NetworkManager die Verbindung zum schnelleren Netzwerk her.

ANMERKUNG: Der NetworkManager und SCPM

Verwenden Sie den NetworkManager nicht gemeinsam mit SCPM, wenn die Netzwerkeinstellungen durch SCPM-Profile geändert werden. Möchten Sie SCPM und den NetworkManager zur gleichen Zeit verwenden, müssen Sie die Netzwerkressource in der SCPM-Konfiguration deaktivieren.

In den folgenden Fällen ist der NetworkManager ungeeignet:

- Sie möchten für eine Schnittstelle mehrere Einwahlanbieter verwenden
- Ihr Computer ist ein Netzwerk-Router
- Ihr Computer stellt Netzwerkdienste für andere Computer in Ihrem Netzwerk bereit (es handelt sich zum Beispiel um einen DHCP- oder DNS-Server)

ANMERKUNG: Der NetworkManager und mit YaST konfigurierte Netzwerkgeräte

Wenn Sie Ihr System bislang mit YaST konfiguriert haben und nun zum NetworkManager übergehen, werden die Konfigurationen aus YaST übernommen.

31.5.1 Steuern des NetworkManagers

Den NetworkManager aktivieren Sie im YaST-Modul Ihres Netzwerkgeräts. Da für den NetworkManager keine Standardnetzwerkkonfiguration erforderlich ist, wird die YaST-Konfiguration deaktiviert. Der NetworkManager wählt automatisch das beste verfügbare Netzwerk aus, kann aber nur automatisch eine Verbindung zu einem bekannten Netzwerk herstellen. Für die erste Verbindung mit einem Netzwerk müssen Sie daher das NetworkManager-Applet verwenden. Vom Netzwerk angeforderte Informationen, wie der Name, das Passwort oder der Verschlüsselungsschlüssel, werden vom NetworkManager automatisch abgefragt.

Sowohl KDE also auch GNOME verfügen über eigene Applets für den NetworkManager. Ein passendes Applet sollte automatisch mit der Desktop-Umgebung gestartet werden. Das Applet wird dann als Symbol in der Kontrollleiste angezeigt. Die Funktionen beider Applets sind ähnlich, aber ihre Schnittstellen sind verschieden. Sie können auch in anderen grafischen Umgebungen verwendet werden, die die standardmäßige Kontrollleiste unterstützen.

Das KNetworkManager-Applet

KNetworkManager ist ein KDE-Applet für die Steuerung des NetworkManagers. Falls es nicht ausgeführt wird, starten Sie es mit dem Befehl `knetworkmanager`. Wenn es ausgeführt wird, wird ein blaues Globussymbol in der Kontrollleiste angezeigt. Wenn Sie mit der rechten Maustaste auf das Symbol klicken, wird das KNetworkManager-Menü mit verschiedenen Befehlen für die Verwaltung der Netzwerkverbindungen geöffnet.

Das Menü enthält die verfügbaren Netzwerkverbindungen, sowohl für verkabelte als auch für drahtlose Geräte. Wenn Sie mit dem Cursor auf diese zeigen, werden Details angezeigt. Die zurzeit verwendete Verbindung ist im Menü aktiviert. Die Signalstärke der drahtlosen Netzwerke wird ebenfalls im Menü angezeigt. Verschlüsselte drahtlose

Netzwerke sind mit einem blauen Schlosssymbol gekennzeichnet. Um eine Verbindung mit einem verschlüsselten Netzwerk herzustellen, wählen Sie es im Menü aus. Wählen Sie im nun geöffneten Dialogfeld den Typ der *Verschlüsselung*, den das Netzwerk verwendet und geben Sie den passenden *Passwortsatz* oder *Schlüssel* ein.

Um eine Verbindung mit einem Netzwerk herzustellen, das seinen ESSID (Service Set Identifier) nicht sendet und demzufolge nicht automatisch erkannt werden kann, wählen Sie *Verbindung zu anderem drahtlosen Netzwerk herstellen*. Geben Sie in dem daraufhin angezeigten Dialogfeld den ESSID ein und legen Sie gegebenenfalls die Verschlüsselungsparameter fest.

Um auf Einwahlverbindungen zuzugreifen, wählen Sie *Einwahlverbindungen*. Wenn bereits Einwahlverbindungen definiert wurden, starten Sie die Verbindung durch Klicken auf die zu verwendende Verbindung. *Einwahlverbindungen konfigurieren* öffnet YaST. Hier können Sie eine neue Einwahlverbindung definieren.

Um eine aktive Netzwerkverbindung zu deaktivieren, wählen Sie *Optionen → In Offline-Modus wechseln* im KNetworkManager-Menü aus. Um die Verbindung wieder zu aktivieren, wählen Sie *Optionen → In Online-Modus wechseln*. Um drahtlose Netzwerkverbindungen zu deaktivieren, wählen Sie *Optionen → Drahtlose Netzwerke deaktivieren* im KNetworkManager-Menü. Um drahtlose Verbindungen erneut zu aktivieren, wählen Sie *Optionen → Drahtlose Netzwerke aktivieren*. Das Aktivieren der Netzwerke nimmt einige Sekunden in Anspruch.

Das GNOME-NetworkManager-Applet

GNOME verfügt zudem über sein eigenes Applet für den NetworkManager. Falls es nicht ausgeführt wird, starten Sie es mit dem Befehl `nm-applet`. Wenn es ausgeführt wird, wird ein Symbol in der Kontrollleiste angezeigt. Wie das Symbol aussieht, hängt vom Status der Netzwerkverbindung ab. Wenn Sie nicht sicher sind, was das Symbol bedeutet, zeigen Sie mit dem Cursor darauf, bis eine Erklärung angezeigt wird.

Klicken Sie mit der linken Maustaste auf das Applet-Symbol, um ein Menü mit verfügbaren Netzwerken anzuzeigen. Die zurzeit verwendete Verbindung ist im Menü aktiviert. Die Signalstärke der drahtlosen Netzwerke wird ebenfalls im Menü angezeigt. Verschlüsselte drahtlose Netzwerke sind mit einem blauen Schildsymbol gekennzeichnet. Um eine Verbindung mit einem verschlüsselten Netzwerk herzustellen, wählen Sie es im Menü aus. Wählen Sie im nun geöffneten Dialogfeld den Typ der *Verschlüsselung*, den das Netzwerk verwendet und geben Sie den passenden *Passwortsatz* oder *Schlüssel* ein.

Um eine Verbindung mit einem Netzwerk herzustellen, das seinen ESSID (Service Set Identifier) nicht sendet und demzufolge nicht automatisch erkannt werden kann, klicken Sie mit der linken Maustaste auf das Symbol und wählen Sie *Verbindung zu anderem drahtlosen Netzwerk herstellen*. Geben Sie in dem daraufhin angezeigten Dialogfeld den ESSID ein und legen Sie gegebenenfalls die Verschlüsselungsparameter fest.

Um Netzwerkverbindungen zu deaktivieren, klicken Sie mit der rechten Maustaste auf das Applet-Symbol und deaktivieren Sie die Option *Enable Networking* (Netzwerk aktivieren). Um drahtlose Netzwerkverbindungen zu deaktivieren, klicken Sie mit der rechten Maustaste auf das Applet-Symbol und deaktivieren Sie die Option *Drahtlose Netzwerke aktivieren*.

Um Informationen zur aktuellen Verbindung (z. B. verwendete Schnittstelle, IP-Adresse und Hardwareadresse) abzurufen, klicken Sie mit der rechten Maustaste auf das Applet-Symbol und wählen Sie *Verbindungsinformationen* im Menü aus.

31.5.2 Weitere Informationen

Weitere Informationen zum NetworkManager und d-bus erhalten Sie auf den folgenden Websites bzw. in den folgenden Verzeichnissen:

- <http://www.gnome.org/projects/NetworkManager/> (Projektseite des NetworkManagers)
- <http://www.freedesktop.org/Software/dbus> (Projektseite von d-bus)
- `/usr/share/doc/packages/NetworkManager`

31.6 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte immer die letzte Alternative sein. Wir empfehlen, YaST zu benutzen. Die folgenden Hintergrundinformationen zur Netzwerkkonfiguration können Ihnen jedoch auch bei der Arbeit mit YaST behilflich sein.

Alle integrierten Netzwerkkarten und Hotplug-Netzwerkkarten (PCMCIA, USB und einige PCI-Karten) werden über Hotplug erkannt und konfiguriert. Das System erkennt

eine Netzwerkkarte auf zwei unterschiedliche Weisen: erstens als physisches Gerät und zweitens als Schnittstelle. Das Einstecken eines Geräts löst ein Hotplug-Ereignis aus. Dieses Hotplug-Ereignis löst dann die Initialisierung des Geräts mithilfe des Skripts `hwup` aus. Wenn die Netzwerkkarte als neue Netzwerkschnittstelle initialisiert wird, generiert der Kernel ein weiteres Hotplug-Ereignis, das das Einrichten der Schnittstelle mit `ifup` auslöst.

Der Kernel nummeriert die Schnittstellennamen gemäß der zeitlichen Reihenfolge ihrer Registrierung. Die Initialisierungsreihenfolge ist für die Zuordnung der Namen entscheidend. Falls eine von mehreren Netzwerkkarten ausfallen sollte, wird die Nummerierung aller danach initialisierten Karten verschoben. Für echte Hotplug-fähige Karten ist die Reihenfolge, in der die Geräte angeschlossen werden, wichtig.

Um eine flexible Konfiguration zu ermöglichen, wurde die Konfiguration der Geräte (Hardware) und der Schnittstellen voneinander getrennt und die Zuordnung der Konfigurationen zu Geräten und Schnittstellen erfolgt nicht mehr auf Basis der Schnittstellennamen. Die Gerätekonfigurationen befinden sich im Verzeichnis `/etc/sysconfig/hardware/hwcfg-*`. Die Schnittstellenkonfigurationen befinden sich im Verzeichnis `/etc/sysconfig/network/ifcfg-*`. Die Namen der Konfigurationen werden so zugewiesen, dass sie die Geräte und die damit verknüpften Schnittstellen beschreiben. Da bei der früheren Zuordnung von Treibern zu Schnittstellennamen statische Schnittstellennamen erforderlich waren, kann diese Zuordnung nicht mehr in der Datei `/etc/modprobe.conf` erfolgen. Im neuen Konzept würden die Aliaseinträge in dieser Datei Probleme verursachen.

Die Konfigurationsnamen – d. h., die Einträge hinter `hwcfg-` oder `ifcfg-` – beschreiben die Geräte anhand des Steckplatzes, der gerätespezifischen ID oder des Schnittstellennamens. Der Konfigurationsname für eine PCI-Karte kann beispielsweise `bus-pci-0000:02:01.0` (PCI-Steckplatz) oder `vpid-0x8086-0x1014-0x0549` (Hersteller- und Produkt-ID) lauten. Der Name der zugeordneten Schnittstelle kann `bus-pci-0000:02:01.0` oder `wlan-id-00:05:4e:42:31:7a` (MAC-Adresse) lauten.

Um eine bestimmte Netzwerkkonfiguration einer Karte eines bestimmten Typs zuzuordnen (von der immer nur jeweils eine eingesetzt ist), wählen Sie anstelle einer bestimmten Karte weniger spezifische Konfigurationsnamen. So würde `bus-pcmcia` beispielsweise für alle PCMCIA-Karten verwendet werden. Die Namen können andererseits auch durch einen vorangestellten Schnittstellentyp eingeschränkt werden. So würde `wlan-bus-usb` beispielsweise WLAN-Karten zugeordnet werden, die an einen USB-Anschluss angeschlossen sind.

Das System verwendet immer die Konfiguration, die eine Schnittstelle oder das Gerät, das die Schnittstelle zur Verfügung stellt, am besten beschreibt. Die Suche nach der am besten geeigneten Konfiguration erfolgt mit dem Befehl `getcfg`. Die Ausgabe von `getcfg` enthält alle Informationen, die für die Beschreibung eines Geräts verwendet werden können. Weitere Informationen zur Spezifikation von Konfigurationsnamen finden Sie auf der Manualpage für den Befehl `getcfg`.

Mit der beschriebenen Methode wird eine Netzwerkschnittstelle auch dann mit der richtigen Konfiguration eingestellt, wenn die Netzwerkgeräte nicht immer in derselben Reihenfolge initialisiert werden. Der Name der Schnittstelle ist jedoch weiter von der Initialisierungsreihenfolge abhängig. Es gibt zwei Möglichkeiten, den zuverlässigen Zugriff auf die Schnittstelle einer bestimmten Netzwerkkarte sicherzustellen:

- `getcfg-interface Konfigurationsname` gibt den Namen der zugeordneten Netzwerkschnittstelle zurück. Daher kann in einigen Konfigurationsdateien der Konfigurationsname, z. B. Firewall, DHCPD, Routing oder eine virtuelle Netzwerkschnittstelle (Tunnel), anstelle des Schnittstellennamens eingegeben werden, da Letzterer nicht persistent ist.
- Persistente Schnittstellennamen werden automatisch jeder Schnittstelle zugewiesen. Sie können diese Ihren Anforderungen anpassen. Gehen Sie zum Erstellen von Schnittstellennamen vor wie in `/etc/udev/rules.d/30-net_persistent_names.rules` beschrieben. Der persistente Name `pname` muss sich jedoch von dem Namen unterscheiden, den der Kernel automatisch zuweisen würde. Aus diesem Grund sind `eth*`, `tr*`, `wlan*`, `qeth*`, `iucv*` usw. nicht zulässig. Verwenden Sie stattdessen `net*` oder beschreibende Namen wie `extern`, `intern` oder `dmz`. Stellen Sie sicher, dass jeder Schnittstellename nur einmal benutzt wird. Erlaubte Zeichen in Schnittstellennamen sind auf `[a-zA-Z0-9]` beschränkt. Ein persistenter Name kann einer Schnittstelle nur direkt nach deren Registrierung zugewiesen werden, d. h., der Treiber der Netzwerkkarte muss neu geladen oder `hwup Gerätebeschreibung` muss ausgeführt werden. Der Befehl `rcnetwork restart` reicht für diesen Zweck nicht aus.

WICHTIG: Verwendung persistenter Schnittstellennamen

Die Verwendung persistenter Schnittstellennamen wurde noch nicht für alle Bereiche getestet. Daher sind einige Anwendungen möglicherweise nicht in der Lage, frei ausgewählte Schnittstellennamen handzuhaben.

`ifup` erfordert eine vorhandene Schnittstelle, da es die Hardware nicht initialisiert. Die Initialisierung der Hardware erfolgt über den Befehl `hwup` (wird von `hotplug` oder `coldplug` ausgeführt). Bei der Initialisierung eines Geräts wird `ifup` automatisch für die neue Schnittstelle über `hotplug` ausgeführt und die Schnittstelle wird eingerichtet, wenn der Startmodus `onboot`, `hotplug` oder `auto` ist und der Dienst `network` gestartet wurde. Früher wurde die Hardware-Initialisierung durch den Befehl `ifup Schnittstellename` ausgelöst. Jetzt ist die Vorgehensweise genau umgekehrt. Zuerst wird eine Hardwarekomponente initialisiert und anschließend werden alle anderen Aktionen ausgeführt. Auf diese Weise kann eine variierende Anzahl an Geräten mit einem vorhandenen Satz an Konfigurationen immer bestmöglich konfiguriert werden.

Tabelle 31.5, „Skripts für die manuelle Netzwerkkonfiguration“ (S. 650) zeigt die wichtigsten an der Netzwerkkonfiguration beteiligten Skripts. Die Skripts werden, wann immer möglich, nach Hardware und Schnittstelle unterschieden.

Tabelle 31.5 *Skripts für die manuelle Netzwerkkonfiguration*

Konfigurationsphase	Befehl	Funktion
Hardware	<code>hw{up, down, status}</code>	Die <code>hw*</code> -Skripts werden vom Hotplug-Subsystem ausgeführt, um ein Gerät zu initialisieren, die Initialisierung rückgängig zu machen oder den Status eines Geräts abzufragen. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl <code>hwup</code> .
Schnittstelle	<code>getcfg</code>	<code>getcfg</code> kann zum Abfragen des Namens der Schnittstelle verwendet werden, die mit einem Konfigurationsnamen oder einer Hardwarebeschreibung verknüpft ist. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl <code>getcfg</code> .

Konfigurationsphase	Befehl	Funktion
Schnittstelle	<code>if{up,down,status}</code>	Die <code>if*</code> -Skripts 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> .

Weitere Informationen zu Hotplug und persistenten Gerätenamen finden Sie in [Kapitel 25, Geräteverwaltung über dynamischen Kernel mithilfe von udev](#) (S. 515).

31.6.1 Konfigurationsdateien

Dieser Abschnitt bietet einen Überblick über die Netzwerkkonfigurationsdateien und erklärt ihren Zweck sowie das verwendete Format.

`/etc/sysconfig/hardware/hwcfg-*`

Diese Dateien enthalten die Hardwarekonfigurationen der Netzwerkkarten und weiterer Geräte. Sie enthalten die erforderlichen Parameter, z. B. das Kernelmodul, den Startmodus und Skriptverknüpfungen. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `hwup`. Die `hwcfg-static-*`-Konfigurationen werden unabhängig von der Hardware angewendet, wenn `coldplug` gestartet wird.

`/etc/sysconfig/network/ifcfg-*`

Diese Dateien enthalten die Konfigurationsdaten, die spezifisch für eine Netzwerkschnittstelle sind. Sie enthalten Informationen wie den Startmodus und die IP-Adresse. Mögliche Parameter sind auf der Manualpage 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.

► **zseries:** IBM-System z unterstützt USB nicht. Die Namen der Schnittstellendateien und Netzwerkaliasse enthalten System z-spezifische Elemente, wie `qeth`. ◀

`/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. Sämtliche statische Routen, die für die unterschiedlichen System-Tasks erforderlich sind, können in die Datei `/etc/sysconfig/network/routes` eingegeben werden: Routen zu einem Host, Routen zu einem Host über ein Gateway sowie Routen zu einem Netzwerk. Definieren Sie für jede Schnittstelle, für die ein separates Routing erforderlich ist, eine zusätzliche Konfigurationsdatei: `/etc/sysconfig/network/ifroute-*`. Ersetzen Sie `*` durch den Namen der Schnittstelle. Die Einträge in der Routing-Konfigurationsdatei sehen wie folgt aus:

# 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 Gerätename eingegeben werden.

In einer (optionalen) fünften Spalte kann der Typ einer Route angegeben werden. Nicht benötigte Spalten sollten ein Minuszeichen – enthalten, um sicherzustellen, dass der Parser den Befehl korrekt interpretiert. Weitere Informationen hierzu finden Sie auf der Manualpage für den Befehl `routes(5)`.

/etc/resolv.conf

In dieser Datei wird die Domäne angegeben, zu der der Host gehört (Schlüsselwort `search`). Ebenfalls aufgeführt ist der Status des Namenservers, auf den der Zugriff erfolgt (Schlüsselwort `nameserver`). Es können mehrere Domännennamen angegeben werden. Bei der Auflösung eines Namens, der nicht voll qualifiziert ist, wird versucht, einen solchen zu generieren, indem die einzelnen `search`-Einträge angehängt werden. Wenn Sie mehrere Namenserver verwenden, geben Sie mehrere Zeilen ein, wobei jede Zeile mit `nameserver` beginnt. Stellen Sie Kommentaren ein `#`-Zeichen voran. YaST trägt den angegebenen Namenserver in diese Datei ein. [Beispiel 31.5](#), „`/etc/resolv.conf`“ (S. 653) zeigt, wie `/etc/resolv.conf` aussehen könnte.

Beispiel 31.5 `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

Einige Dienste, z. B. `pppd` (`wvdial`), `ippd` (`isdn`), `dhcp` (`dhcpcd` und `dhclient`), `pcmcia` und `hotplug` ändern die Datei `/etc/resolv.conf` mit dem 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`, `pcmcia` und `hotplug`.

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` über 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 31.6](#), „`/etc/hosts`“ (S. 654) 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 31.6 `/etc/hosts`

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.0 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. Siehe [Beispiel 31.7](#), „`/etc/networks`“ (S. 654).

Beispiel 31.7 `/etc/networks`

```
loopback      127.0.0.0
localnet      192.168.0.0
```

`/etc/host.conf`

Das Auflösen von Namen, d. h. das Übersetzen von Host- bzw. Netzwerknamen über die *resolver*-Bibliothek, wird durch diese Datei gesteuert. 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 31.6](#), „Parameter für `/etc/host.conf`“ (S. 655) aufgeführt. Ein Beispiel für `/etc/host.conf` wird in [Beispiel 31.8](#), „`/etc/host.conf`“ (S. 656) gezeigt.

Tabelle 31.6 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): <code>hosts</code> : Durchsuchen der Datei <code>/etc/hosts</code> <code>bind</code> : Greift auf einen Namensserver zu <code>nis</code> : Über 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</code> <i>Domänenname</i>	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 31.8 */etc/host.conf*

```
# We have named running
order hosts bind
# Allow multiple addrs
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 31.9](#), „`/etc/nsswitch.conf`“ (S. 656) dargestellt. Kommentare werden durch ein #-Zeichen eingeleitet. Der Eintrag unter der `hosts`-Datenbank bedeutet, dass Anfragen über DNS an `/etc/hosts(files)` gehen (siehe [Kapitel 34, Domain Name System \(DNS\)](#) (S. 681)).

Beispiel 31.9 */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 31.7](#), „Über `/etc/nsswitch.conf` verfügbare Datenbanken“ (S. 656) aufgelistet. Zusätzlich sind in Zukunft zudem `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten. Die Konfigurationsoptionen für NSS-Datenbanken sind in [Tabelle 31.8](#), „Konfigurationsoptionen für NSS-„Datenbanken““ (S. 657) aufgelistet.

Tabelle 31.7 *Über `/etc/nsswitch.conf` verfügbare Datenbanken*

<code>aliases</code>	Mail-Aliasse, die von <code>sendmail</code> implementiert werden. Siehe <code>man 5 aliases</code> .
----------------------	--

<code>ethers</code>	Ethernet-Adressen
<code>group</code>	Für Benutzergruppen, die von <code>getgrent</code> verwendet werden. Weitere Informationen hierzu finden Sie auch auf der Manualpage für den Befehl <code>group</code> .
<code>hosts</code>	Für Hostnamen und IP-Adressen, die von <code>gethostbyname</code> und ähnlichen Funktionen verwendet werden.
<code>netgroup</code>	Im Netzwerk gültige Host- und Benutzerlisten zum Steuern von Zugriffsrechten. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>netgroup(5)</code> .
<code>networks</code>	Netzwerknamen und -adressen, die von <code>getnetent</code> verwendet werden.
<code>passwd</code>	Benutzerpasswörter, die von <code>getpwent</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage <code>passwd(5)</code> .
<code>protocols</code>	Netzwerkprotokolle, die von <code>getprotoent</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>protocols(5)</code> .
<code>rpc</code>	Remote Procedure Call-Namen und -Adressen, die von <code>getrpcbyname</code> und ähnlichen Funktionen verwendet werden.
<code>services</code>	Netzwerkdienste, die von <code>getservent</code> verwendet werden.
<code>shadow</code>	Shadow-Passwörter der Benutzer, die von <code>getspnam</code> verwendet werden. Weitere Informationen hierzu finden Sie auf der Manualpage für <code>shadow(5)</code> .

Tabelle 31.8 Konfigurationsoptionen für NSS-„Datenbanken“

<code>files</code>	Direkter Dateizugriff, z. B. <code>/etc/aliases</code>
<code>db</code>	Zugriff über eine Datenbank

<code>nis, nisplus</code>	NIS, siehe auch Kapitel 36, Arbeiten mit NIS (S. 725)
<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`

Mithilfe dieser Datei wird `nscd` (Name Service Cache Daemon) konfiguriert. Weitere Informationen hierzu finden Sie auf den [Manualpages `nscd\(8\)` und `nscd.conf\(5\)`](#). Standardmäßig werden die Systemeinträge von `passwd` und `groups` von `nscd` gecacht. Dies ist wichtig für die Leistung der Verzeichnisdienste, z. B. NIS und LDAP, da anderenfalls die Netzwerkverbindung für jeden Zugriff auf Namen oder Gruppen verwendet werden muss. `hosts` wird standardmäßig nicht gecacht, da der Mechanismus in `nscd` dazu führen würde, dass das lokale System keine Trust-Forward- und Reverse-Lookup-Tests mehr ausführen kann. Statt `nscd` das Cachen der Namen zu übertragen, sollten Sie einen DNS-Server für das Cachen einrichten.

Wenn das Caching für `passwd` aktiviert wird, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten von `nscd` mit dem Befehl `rcnscd restart` kann diese Wartezeit verkürzt werden.

`/etc/HOSTNAME`

Hier steht der Name des Computers, also nur der Hostname ohne den Domännennamen. Diese Datei wird von verschiedenen Skripten beim Booten des Computers gelesen. Sie darf nur eine Zeile enthalten, in der der Hostname steht.

31.6.2 Testen der Konfiguration

Bevor Sie Ihre Konfiguration in den Konfigurationsdateien speichern, können Sie sie testen. Zum Einrichten einer Testkonfiguration verwenden Sie den Befehl `ip`. Zum Testen der Verbindung verwenden Sie den Befehl `ping`. Ältere Konfigurationswerkzeuge, `ifconfig` und `route`, sind ebenfalls verfügbar.

Die Befehle `ip`, `ifconfig` und `route` ändern die Netzwerkkonfiguration direkt, ohne sie in der Konfigurationsdatei zu speichern. Wenn Sie die Konfiguration nicht in die korrekten Konfigurationsdateien eingeben, geht die geänderte Netzwerkkonfiguration nach dem Neustart verloren.

Konfigurieren einer Netzwerkschnittstelle mit `ip`

`ip` ist ein Werkzeug zum Anzeigen und Konfigurieren von Routing, Netzwerkgeräten, Richtlinien-Routing und Tunneln. Er wurde als Ersatz für die älteren Werkzeuge `ifconfig` und `route` gedacht.

`ip` ist ein sehr komplexes Werkzeug. Seine allgemeine Syntax lautet `ip options object command`. Sie können mit folgenden Objekten arbeiten:

`link`

Dieses Objekt stellt ein Netzwerkgerät dar.

`address`

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.

`rule`

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. Zum Festlegen der IP-Adresse verwenden Sie `ip addr add ip_address + dev device_name`. Wenn Sie beispielsweise die Adresse der Schnittstelle `eth0` auf `192.168.12.154/30` setzen möchten mit dem standardmäßigen Broadcast (Option `brd`), 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. Zum Einstellen des Gateways für Ihr System, geben Sie `ip route get gateway_ip_address` ein. Zum Übersetzen einer IP-Adresse in eine andere verwenden Sie `nat: ip route add nat ip_address via other_ip_address`.

Zum Anzeigen aller Geräte verwenden Sie `ip link ls`. Zum Anzeigen nur der aktiven Schnittstellen verwenden Sie `ip link ls up`. Zum Drucken von Schnittstellenstatistiken für ein Gerät geben Sie `ip -s link ls device_name` ein. Zum Anzeigen von Adressen Ihrer Geräte 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`.

Genauere Informationen zur Verwendung von `ip` erhalten Sie, indem Sie `ip help` eingeben oder auf der Manualpage `ip(8)`. Die Option `help` ist zudem für alle `ip`-Objekte verfügbar. Wenn Sie beispielsweise Hilfe zu `ip addr` benötigen, geben Sie `ip addr 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 kann aber noch mehr, als nur die Funktion der Verbindung zwischen zwei Computern zu testen: Der Befehl bietet grundlegende Informationen zur Qualität der Verbindung. In [Beispiel 31.10](#), „Ausgabe des ping-Befehls“ (S. 661) sehen Sie ein Beispiel der ping-Ausgabe. Die vorletzte Zeile enthält Informationen zur Anzahl der übertragenen Pakete, der verlorenen Pakete und der Gesamtlaufzeit von ping.

Als Ziel können Sie einen Hostnamen oder eine IP-Adresse verwenden, z. B. `ping example.com` oder `ping 130.57.5.75`. 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 3 192.168.0` ein.

Beispiel 31.10 *Ausgabe des ping-Befehls*

```
ping -c 3 example.com
  PING example.com (130.57.5.75) 56(84) bytes of data:
  64 bytes from example.com (130.57.5.75): icmp_seq=1 ttl=49 time=188
ms
  64 bytes from example.com (130.57.5.75): icmp_seq=2 ttl=49 time=184
ms
  64 bytes from example.com (130.57.5.75): icmp_seq=3 ttl=49 time=183
ms

--- example.com ping statistics ---
 3 packets transmitted, 3 received, 0% packet loss, time 2007ms
 rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

Das Standardintervall zwischen zwei Paketen beträgt eine Sekunde. Zum Ändern des Intervalls bietet der ping-Befehl die Option `-i`. Wenn Sie beispielsweise das Ping-Intervall auf zehn Sekunden erhöhen möchten, geben Sie `ping -i 10 192.168.0` ein.

In einem System mit mehreren Netzwerkgeräten ist es manchmal nützlich, wenn der ping-Befehl über eine spezifische Schnittstellenadresse gesendet wird. Das legen Sie mit der `-I`-Option und dem Namen des ausgewählten Geräts fest. Beispiel: `ping -I wlan1 192.168.0`.

Genauere Optionen und Informationen zur Verwendung von ping erhalten Sie, indem Sie `ping -h` eingeben oder auf der Manualpage `ping (8)`.

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 31.11](#), „Ausgabe des `ifconfig`-Befehls“ (S. 662) 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 31.11 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)
```

Genauere Optionen und Informationen zur Verwendung von `ifconfig`, erhalten Sie, indem Sie `ifconfig -h` eingeben oder auf der Manualpage `ifconfig` (8).

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 31.12 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
```

Genauere Optionen und Informationen zur Verwendung von `route`, erhalten Sie, indem Sie `v -h` eingeben oder auf der Manualpage `route` (8).

31.6.3 Startup-Skripts

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripts, die beim Booten des Computers die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Mehrbenutzer-Runlevel* wechselt. Einige der Skripts sind in [Tabelle 31.9, „Einige Start-Skripts für Netzwerkprogramme“](#) (S. 664) beschrieben.

Tabelle 31.9 *Einige Start-Skripts für Netzwerkprogramme*

<code>/etc/init.d/ network</code>	Dieses Skript übernimmt die Konfiguration der Netzwerkschnittstellen. Die Hardware muss bereits von <code>/etc/init.d/coldplug</code> (über Hotplug) initialisiert worden sein. Wenn der Dienst <code>network</code> nicht gestartet wurde, werden keine Netzwerkschnittstellen beim Einstecken über Hotplug implementiert.
<code>/etc/init.d/inetd</code>	Startet <code>xinetd</code> . <code>xinetd</code> kann verwendet werden, um bei Bedarf Serverdienste auf dem System zur Verfügung zu stellen. Beispielsweise kann er <code>vsftpd</code> starten, sobald eine FTP-Verbindung initiiert wird.
<code>/etc/init.d/ portmap</code>	Startet den Portmapper, der für einen RPC-Server benötigt wird, z. B. für einen NFS-Server.
<code>/etc/init.d/ nfsserver</code>	Startet den NFS-Server.
<code>/etc/init.d/ sendmail</code>	Steuert den <code>sendmail</code> -Prozess.
<code>/etc/init.d/ypserv</code>	Startet den NIS-Server.
<code>/etc/init.d/ypbind</code>	Startet den NIS-Client.

31.7 smpppd als Einwählhelfer

Die meisten 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 Einwählverbindung über ein KDE-Applet oder eine Kommandozeilen-Schnittstelle steuern.

Wenn das Internet-Gateway nicht der eigentliche Arbeitscomputer ist, besteht die Möglichkeit, die Einwählverbindung über einen Host im Netzwerk zu steuern.

An dieser Stelle kommt `smpppd` ins Spiel. Der Dienst bietet den Hilfsprogrammen eine einheitliche Schnittstelle, die in zwei Richtungen funktioniert. Zum einen programmiert er den jeweils erforderlichen `pppd` oder `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.

31.7.1 Konfigurieren von `smpppd`

Die von `smpppd` bereitgestellten Verbindungen werden automatisch von YaST konfiguriert. Die eigentlichen Einwählprogramme `KInternet` und `cinternet` werden ebenfalls vorkonfiguriert. Manuelle Einstellungen sind nur notwendig, wenn Sie zusätzliche Funktionen von `smpppd`, z. B. die Fernsteuerung, einrichten möchten.

Die Konfigurationsdatei von `smpppd` ist `/etc/smpppd.conf`. Sie ist so eingestellt, dass standardmäßig keine Fernsteuerung möglich ist. Die wichtigsten Optionen dieser Konfigurationsdatei sind:

`open-inet-socket = yes/no`

Wenn `smpppd` über das Netzwerk gesteuert werden soll, muss diese Option auf `yes` (ja) gesetzt 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`

Wenn ein Host mehrere IP-Adressen hat, können Sie mit dieser Einstellung festlegen, über welche IP-Adresse `smpppd` Verbindungen akzeptiert.

`host-range = Anfangs-IP End-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 Manualpages zu `smpppd(8)` und `smpppd.conf(5)`.

31.7.2 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.

Sofern der smpppd-Dienst aktiv ist, können Sie jetzt versuchen, auf ihn zuzugreifen, z. B. mit dem Befehl `cinternet --verbose --interface-list`. Sollten Sie an dieser Stelle Schwierigkeiten haben, finden Sie weitere Informationen in den Manualpages 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.

WICHTIG: SLP-Unterstützung in SUSE Linux Enterprise Server

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.)

SUSE® Linux Enterprise unterstützt die Installation von per SLP bekannt gegebenen 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 SUSE Linux Enterprise zur Verfügung zu stellen.

32.1 Installation über SLP

Wenn Sie einen Installationsserver mit SUSE Linux Enterprise-Installationsmedien in Ihrem Netzwerk anbieten, kann dieser mit SLP registriert werden. Weitere Informationen

finden Sie in [Abschnitt 4.2.1](#), „Einrichten eines Installationservers mithilfe von YaST“ (S. 86). 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.

32.2 Registrieren eigener Dienste

Viele Anwendungen unter SUSE Linux Enterprise verfügen durch die `libslp`-Bibliothek bereits über eine integrierte SLP-Unterstützung. Falls ein Dienst ohne SLP-Unterstützung kompiliert wurde, können Sie ihn mit einer der folgenden Methoden per SLP verfügbar machen:

Statische Registrierung über `/etc/slp.reg.d`

Legen Sie für jeden neuen Dienst eine separate Registrierungsdatei an. Dies ist ein Beispiel einer solchen Datei für die Registrierung eines Scannerdiensts:

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
watch-port-tcp=6566
description=SANE scanner daemon
```

Die wichtigste Zeile dieser Datei ist die *Dienst-URL*, die mit `service:` beginnt. Sie enthält den Dienstyp (`scanner.sane`) und die Adresse, unter der der Dienst auf dem Server verfügbar ist. `$HOSTNAME` wird automatisch durch den vollständigen Hostnamen ersetzt. Abgetrennt durch einen Doppelpunkt folgt nun der Name des TCP-Ports, auf dem der entsprechende Dienst gefunden werden kann. Geben Sie nun die Sprache an, in der der Dienst angekündigt werden soll, und die 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-tcp-port` und `description`. `watch-tcp-port` koppelt die SLP-Dienstankündigung daran, ob der entsprechende Dienst aktiv ist, indem `slpd` den Status des Dienstes

überprüft. Die zweite Variable enthält eine genauere Beschreibung des Diensts, die in den entsprechenden Browsern angezeigt wird.

TIPP: YaST und SLP

Einige von YaST bereitgestellte Dienste, wie ein Installationsserver oder You-Server, führen diese Registrierung für Sie automatisch durch, wenn Sie SLP in den Modul-Dialogfeldern aktivieren. Dann erstellt YaST Registrierungsdateien für diese Dienste.

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 Skripts das Kommandozeilen-Frontend `slptool`.

32.3 SLP-Frontends in SUSE Linux Enterprise

SUSE Linux Enterprise enthält mehrere Frontends, um SLP-Informationen über ein Netzwerk zu überprüfen und zu verwenden:

`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 Skripts heraus aufgerufen werden, die SLP-Informationen verarbeiten.

SLP-Browser von YaST

YaST enthält unter *Netzwerkdienste* → *SLP-Browser* einen separaten SLP-Browser, der alle im lokalen Netzwerk über SLP bekannt gegebenen Dienste in einer Baumansicht darstellt.

Konqueror

Wird Konqueror als Netzwerkbrowser eingesetzt und mit `slp:/` aufgerufen, werden alle im lokalen Netz verfügbaren SLP-Dienste angezeigt. 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.

32.4 SLP aktivieren

`slpd` muss auf Ihrem System laufen, wenn Sie Dienste anbieten möchten. Für das bloße Abfragen von Diensten ist ein Start dieses Daemons nicht erforderlich. Wie die meisten Systemdienste unter SUSE Linux Enterprise wird der `slpd`-Daemon 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 as root` aus, um ihn zu starten. Mit dem Befehl `rcslpd stop` können Sie ihn stoppen. Mit `restart` oder `status` lösen Sie einen Neustart bzw. eine Statusabfrage aus. Soll `slpd` standardmäßig aktiv sein, 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.

32.5 Weitere 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.com>

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 SUSE Linux Enterprise, 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.

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. Es gibt zwei Ziele – das Aufrechterhalten der absoluten Zeit und das Synchronisieren der Systemzeit aller Computer im Netzwerk.

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. In einem Netzwerk muss in der Regel die Systemzeit aller Computer synchronisiert werden, von der manuellen Zeitanpassung wird jedoch dringend abgeraten. `xntp` stellt einen Mechanismus zur Lösung dieser Probleme bereit. Er passt die Systemzeit ständig anhand zuverlässiger Zeitserver im Netzwerk an. Zudem ermöglicht er die Verwaltung lokaler Referenzuhren, beispielsweise funkgesteuerter Uhren.

33.1 Konfigurieren eines NTP-Client mit YaST

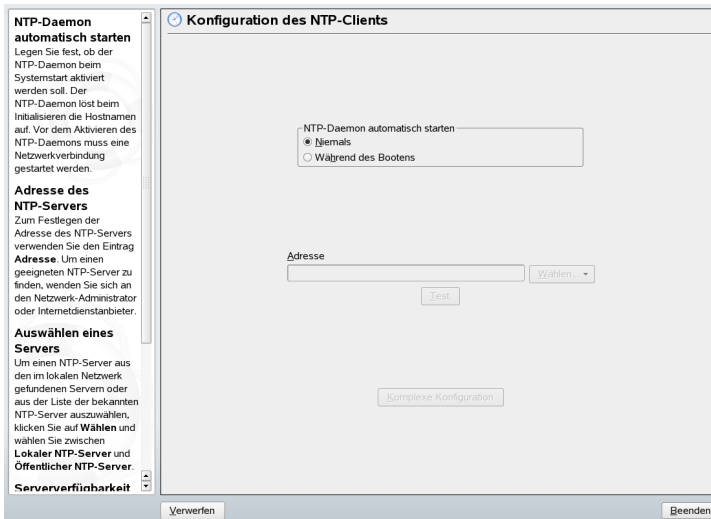
`xntp` ist so voreingestellt, dass die lokale Computeruhr als Zeitreferenz verwendet wird. Das Verwenden der (BIOS-) Uhr ist jedoch nur eine Ausweidlösung, wenn keine genauere Zeitquelle verfügbar ist. SUSE® Linux Enterprise ermöglicht die

Konfiguration eines NTP-Client mit YaST. Für Clients, die SuSEfirewall ausführen, haben Sie die Wahl zwischen der Schnellkonfiguration und der komplexen Konfiguration, da diese Teil eines geschützten Intranets sind. Beide Konfigurationstypen werden nachfolgend erläutert.

33.1.1 Schnelle NTP-Client-Konfiguration

Die schnelle NTP-Client-Konfiguration (*Netzwerkdienste* → *NTP-Client*) umfasst 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 dann 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 33.1 YaST: Konfigurieren eines NTP-Client



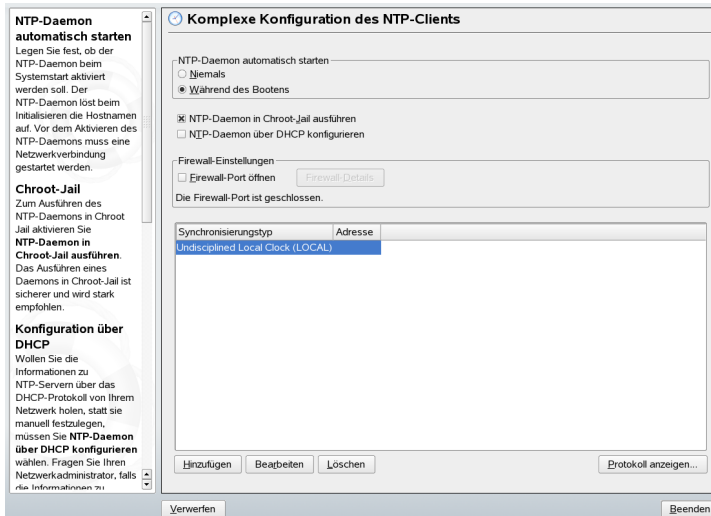
Geben Sie im Dialogfeld für die detaillierte Serverauswahl an, ob die Zeitsynchronisierung anhand eines Zeitservers in Ihrem lokalen Netzwerk (*Lokaler NTP-Server*) oder eines Zeitservers im Internet erfolgen soll, der Ihre Zeitzone verwaltet (*Öffentlicher NTP-Server*). Bei einem lokalen Zeitserver klicken Sie auf *Lookup*, um eine SLP-Abfrage für verfügbare Zeitserver in Ihrem Netzwerk zu starten. Wählen Sie den am

besten geeigneten Zeitserver in der Liste der Suchergebnisse aus und schließen Sie das Dialogfeld mit *OK*. Bei einem öffentlichen Zeitserver wählen Sie in der Liste unter *Öffentlicher NTP-Server* Ihr Land (Ihre Zeitzone) sowie einen geeigneten Server aus und schließen das Dialogfeld dann mit *OK*. Im Hauptdialogfeld testen Sie die Verfügbarkeit des ausgewählten Servers mit *Test* und schließen das Dialogfeld mit *Beenden*.

33.1.2 Komplexe NTP-Client-Konfiguration

Der Zugriff auf die komplexe Konfiguration eines NTP-Client ist unter *Komplexe Konfiguration* im Hauptdialogfeld des Moduls *NTP-Client* möglich (siehe [Abbildung 33.1](#), „*YaST: Konfigurieren eines NTP-Client*“ (S. 676)); zunächst muss jedoch wie in der schnellen Konfiguration beschrieben ein Start-Modus ausgewählt werden.

Abbildung 33.2 *YaST: Komplexe NTP-Client-Konfiguration*



Legen Sie unter *Komplexe Konfiguration des NTP-Clients* fest, ob *xntpd* in *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. 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. Die folgenden Optionen stehen zur Verfügung:

Server

In einem anderen Dialogfeld können Sie einen NTP-Server auswählen (siehe Beschreibung unter [Abschnitt 33.1.1, „Schnelle NTP-Client-Konfiguration“](#) (S. 676)). Aktivieren Sie *Für initiale Synchronisierung verwenden*, um die Synchronisierung der Zeitinformationen zwischen dem Server und dem Client auszulösen, wenn das System gebootet wird. In einem Eingabefeld können Sie zusätzliche Optionen für `xntpd` angeben. 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 wie 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/html/refclock.htm`.

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.

33.2 Konfigurieren von xntp im Netzwerk

Die einfachste Art der Verwendung eines Zeitservers im Netzwerk besteht darin, Serverparameter festzulegen. Wenn beispielsweise ein Zeitserver mit der Bezeichnung `ntp.example.com` vom Netzwerk aus erreichbar ist, ergänzen Sie die Datei `/etc/ntp.conf` um seinen Namen, indem Sie die Zeile `server ntp.example.com` hinzufügen. Wenn Sie weitere Zeitserver hinzufügen möchten, fügen Sie zusätzliche Zeilen mit dem Schlüsselwort `server` hinzu. Nach der Initialisierung von `xntpd` mit dem Befehl `rcntp start` 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.

Der NTP-Mechanismus kann auf zwei unterschiedliche Arten als Client verwendet werden: Erstens kann der Client die Zeit in regelmäßigen Intervallen 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 der 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.

33.3 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/html/refclock.htm` zur Verfügung. Jeder Treiber ist mit einer Nummer verknüpft. In `xntp` erfolgt die eigentliche Konfiguration mithilfe von Pseudo-IPs. 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 bestimmt, welcher Treiber verwendet wird; `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/html/driverNN.htm` (NN steht für die Anzahl der Treiber) bietet Informationen zu dem bestimmten 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. Im Anschluss an die Installation des `xntp-doc`-Pakets steht die Dokumentation für `xntp` im Verzeichnis `/usr/share/doc/packages/xntp-doc/html` zur Verfügung. Die Datei `/usr/share/doc/packages/xntp-doc/html/refclock.htm` enthält Links zu den Treiberseiten, auf denen die Treiberparameter beschrieben werden.

Domain Name System (DNS)

34

DNS (Domain Name System) ist zur Auflösung der Domänen- und Hostnamen in IP-Adressen erforderlich. So wird die IP-Adresse 192.168.0.0 beispielsweise dem Hostnamen `earth` zugewiesen. Bevor Sie Ihren eigenen Namensserver einrichten, sollten Sie die allgemeinen Informationen zu DNS in [Abschnitt 31.3](#), „Namensauflösung“ (S. 622) lesen. Die folgenden Konfigurationsbeispiele beziehen sich auf BIND.

34.1 DNS-Terminologie

Zone

Der Domänen-Namespace wird in Regionen, so genannte Zonen, unterteilt. So ist beispielsweise `opensuse.org` der Bereich bzw. die Zone `opensuse` der Domäne `org`.

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 Masterserver. 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.

Eintrag

Der Eintrag besteht aus Informationen zu Namen und IP-Adresse. Die unterstützten Einträge und ihre Syntax sind in der BIND-Dokumentation beschrieben. Einige spezielle Einträge sind beispielsweise:

NS-Eintrag

Ein NS-Eintrag informiert die Namenserver darüber, welche Computer für eine bestimmte Domänenzone zuständig sind.

MX-Eintrag

Die MX (Mailaustausch)-Einträge beschreiben die Computer, die für die Weiterleitung von Mail über das Internet kontaktiert werden sollen.

SOA-Eintrag

Der SOA (Start of Authority)-Eintrag ist der erste Eintrag in einer Zonendatei. Der SOA-Eintrag wird bei der Synchronisierung von Daten zwischen mehreren Computern über DNS verwendet.

34.2 Konfiguration mit YaST

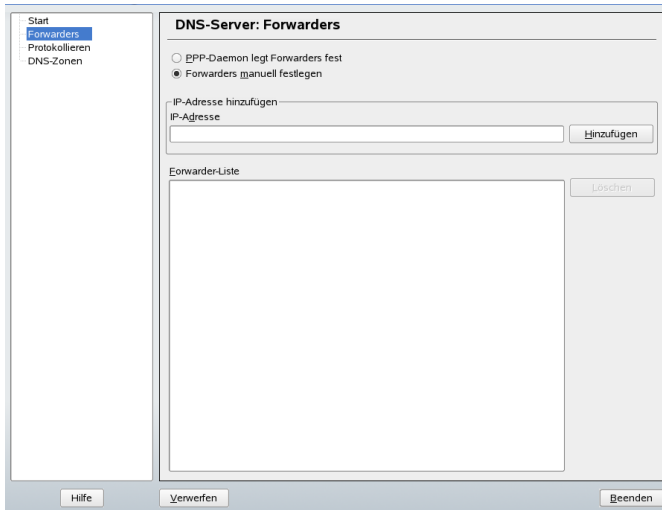
Mit dem DNS-Modul von YaST können Sie einen DNS-Server für Ihr lokales Netzwerk konfigurieren. Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Nach Abschluss der anfänglichen Konfiguration ist eine grundlegende Serverkonfiguration verfügbar, die für einfache Szenarien ausreichend ist. Der Expertenmodus kann für erweiterte Konfigurationsaufgaben verwendet werden, beispielsweise zum Einrichten von ACLs, für Protokollaufgaben, TSIG-Schlüssel und andere Optionen.

34.2.1 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 34.1](#), „DNS-Server-Installation: Forwarder-Einstellungen“ (S. 683)) 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*).

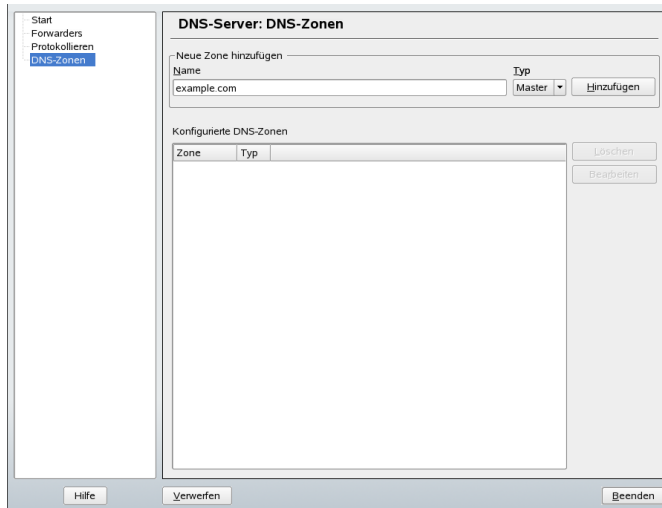
Abbildung 34.1 DNS-Server-Installation: Forwarder-Einstellungen



- 2 Das Dialogfeld *DNS-Zonen* besteht aus mehreren Teilen und ist für die Verwaltung von Zonendateien zuständig, wie in [Abschnitt 34.5](#), „Zonendateien“ (S. 699) 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. Siehe [Abbildung 34.2](#), „DNS-Server-Installation: DNS-Zonen“ (S. 684). Klicken Sie auf *Zone bearbeiten*, um andere Einstellungen für eine

bestehende Zone zu konfigurieren. Zum Entfernen einer Zone klicken Sie auf *Zone löschen*.

Abbildung 34.2 DNS-Server-Installation: DNS-Zonen



- 3 Im letzten Dialogfeld können Sie den DNS-Port in der Firewall öffnen, indem Sie auf *Firewall-Port öffnen* klicken. Legen Sie dann fest, ob der DNS-Server gestartet werden soll (*Ein* oder *Aus*). Außerdem können Sie die LDAP-Unterstützung aktivieren. Siehe [Abbildung 34.3](#), „DNS-Server-Installation: Wizard beenden“ (S. 685).

Abbildung 34.3 DNS-Server-Installation: Wizard beenden



34.2.2 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 *Systemstart* fest, ob der DNS-Server beim Booten des Systems oder manuell gestartet werden soll. Um den DNS-Server sofort zu starten, wählen Sie *DNS-Server nun starten*. Um den DNS-Server anzuhalten, wählen Sie *DNS-Server nun anhalten*. Zum Speichern der aktuellen Einstellungen wählen Sie *Einstellungen speichern und DNS-Server nun neu starten*. Sie können den DNS-Anschluss in der Firewall mit *Firewall-Port öffnen* öffnen und die Firewall-Einstellungen mit *Firewall-Details* bearbeiten.

Wenn Sie *LDAP-Unterstützung aktiv* wählen, werden die Zone-Dateien von einer LDAP-Datenbank verwaltet. Alle Änderungen an Zonendaten, die in der LDAP-Datenbank gespeichert werden, werden vom DNS-Server gleich nach dem Neustart erfasst oder er wird aufgefordert, seine Konfiguration neu zu laden.

DNS-Server: Grundlegende Optionen

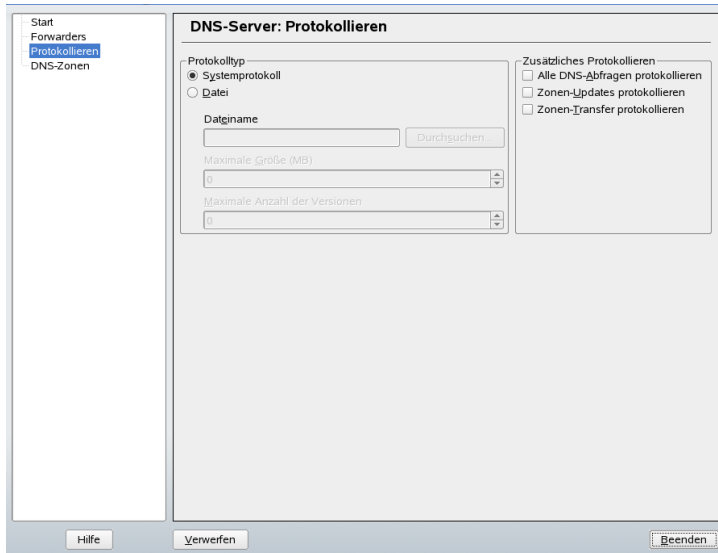
In diesem Abschnitt werden grundlegende Serveroptionen festgelegt. Wählen Sie im Menü *Option* das gewünschte Element und geben Sie dann den Wert im entsprechenden Eintragsfeld an. Nehmen Sie den neuen Eintrag auf, indem Sie auf *Hinzufügen* klicken.

Protokollieren

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` durch Auswahl von *In Systemprotokoll protokollieren* oder geben Sie durch Auswahl von *In Datei protokollieren* eine andere Datei an. In letzterem Fall müssen Sie außerdem die maximale Dateigröße in Megabyte und die Anzahl der zu speichernden 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*. Siehe [Abbildung 34.4](#), „DNS-Server: Protokollieren“ (S. 687).

Abbildung 34.4 DNS-Server: Protokollieren



Verwenden von ACLs

In diesem Fenster legen Sie ACLs (Access Control Lists = Zugriffssteuerungslisten) fest, mit denen Sie den Zugriff einschränken. Nach der Eingabe eines eindeutigen Namens unter *Name* geben Sie unter *Wert* eine IP-Adresse (mit oder ohne Netzmaske) wie folgt an:

```
{ 10.10/16; }
```

Die Syntax der Konfigurationsdatei erfordert, dass die Adresse mit einem Strichpunkt endet und in geschwungenen Klammern steht.

TSIG-Schlüssel

Der Hauptzweck von TSIG-Schlüsseln (Transaction Signatures = Transaktions-signaturen) ist die Sicherung der Kommunikation zwischen DHCP- und DNS-Servern. Diese werden in [Abschnitt 34.7](#), „Sichere Transaktionen“ (S. 704) beschrieben.

Zum Erstellen eines TSIG-Schlüssels geben Sie einen eindeutigen Namen im Feld mit der Beschriftung *Schlüssel-ID* ein und geben die Datei an, in der der Schlüssel gespeichert werden soll (*Dateiname*). Bestätigen Sie Ihre Einstellung mit *Hinzufügen*.

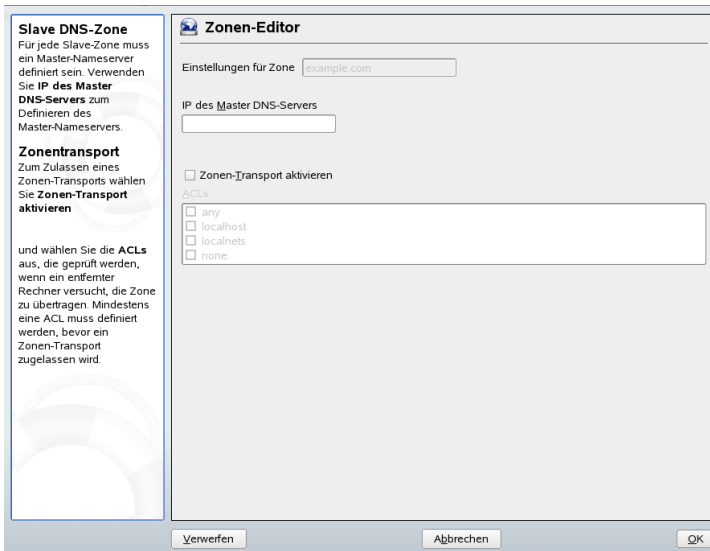
Wenn Sie einen vorher erstellten Schlüssel verwenden möchten, lassen Sie das Feld *Schlüssel-ID* leer und wählen die Datei, in der der gewünschten Schlüssel gespeichert wurde unter *Dateiname*. Dann bestätigen Sie die Auswahl mit *Hinzufügen*.

Hinzufügen einer Slave-Zone

Wenn Sie eine Slave-Zone hinzufügen möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Slave* aus und klicken Sie auf *Hinzufügen*.

Geben Sie im *Zonen-Editor* unter *Master DNS Server* (Master-DNS-Server), 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. Siehe [Abbildung 34.5](#), „DNS-Server: Zonen-Editor des Slave“ (S. 688).

Abbildung 34.5 DNS-Server: Zonen-Editor des Slave



Hinzufügen einer Masterzone

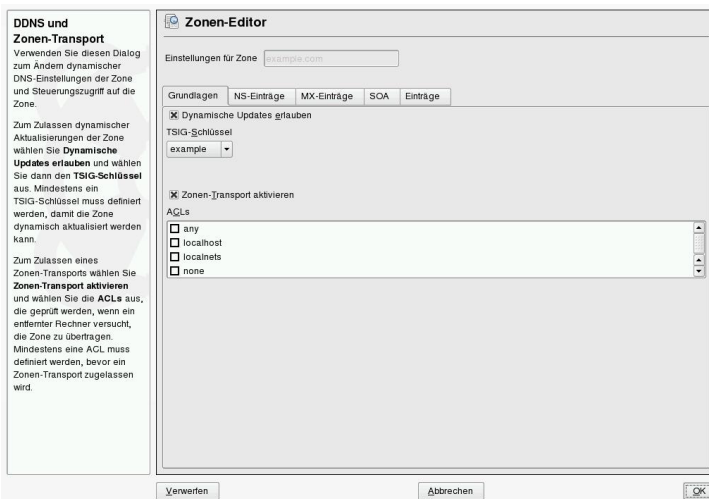
Wenn Sie eine Masterzone hinzufügen möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Master* aus, geben Sie den Namen der neuen Zone ein und klicken Sie auf *Hinzufügen*.

Bearbeiten einer Masterzone

Wenn Sie eine Masterzone bearbeiten möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Master* aus, wählen Sie die Masterzone in der Tabelle aus und klicken Sie auf *Bearbeiten*. Das Dialogfeld besteht aus mehreren Seiten: *Basic* (Grundlagen) (die zuerst geöffnete Seite), *NS-Einträge*, *MX-Einträge*, *SOA* und *Einträge*.

Im grundlegenden Dialogfeld in [Abbildung 34.6](#), „DNS-Server: Zonen-Editor (Standard)“ (S. 689) können Sie die Einstellungen für das dynamische DNS festlegen und auf Optionen für Zonentransfers an Clients und Slave-Namensserver zugreifen. Zum Zulassen dynamischer Aktualisierungen der Zonen wählen Sie *Dynamische Updates erlauben* und wählen Sie dann den entsprechenden TSIG-Schlüssel aus. Der Schlüssel muss definiert werden, bevor die Aktualisierung startet. Zum Aktivieren der Zonentransfers wählen Sie die entsprechenden ACLs. ACLs müssen bereits definiert sein.

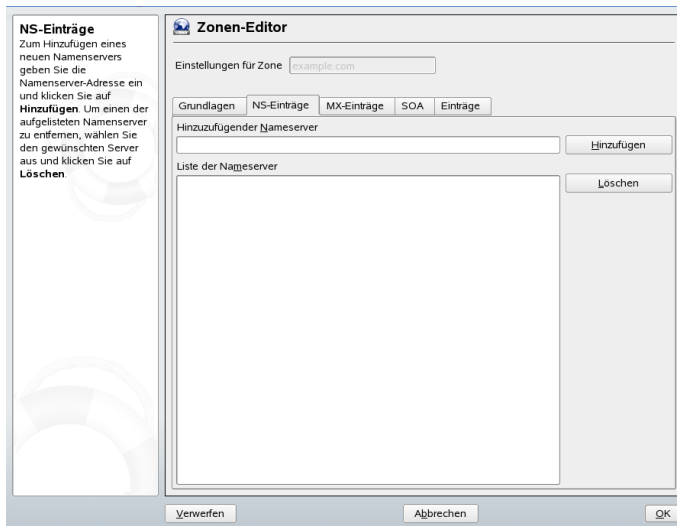
Abbildung 34.6 DNS-Server: Zonen-Editor (Standard)



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 Namenserver* ein und bestätigen Sie den Vorgang anschließend mit *Hinzufügen*. Siehe [Abbildung 34.7, „DNS-Server: Zonen-Editor \(NS-Einträge\)“](#) (S. 690).

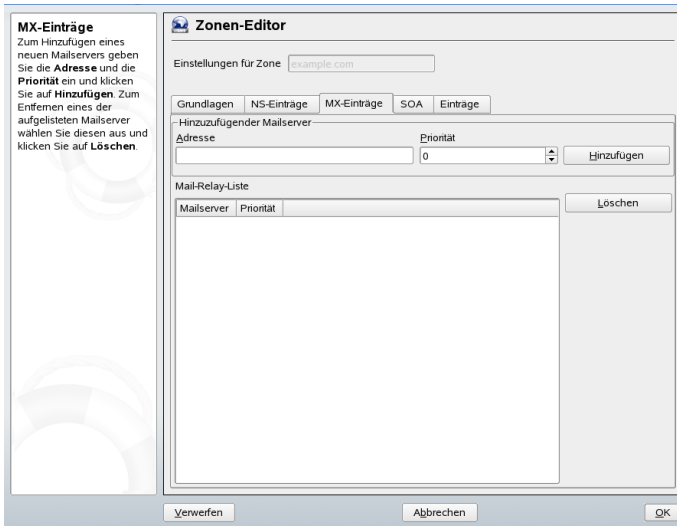
Abbildung 34.7 DNS-Server: Zonen-Editor (NS-Einträge)



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*. Siehe [Abbildung 34.8, „DNS-Server: Zonen-Editor \(MX-Einträge\)“](#) (S. 691).

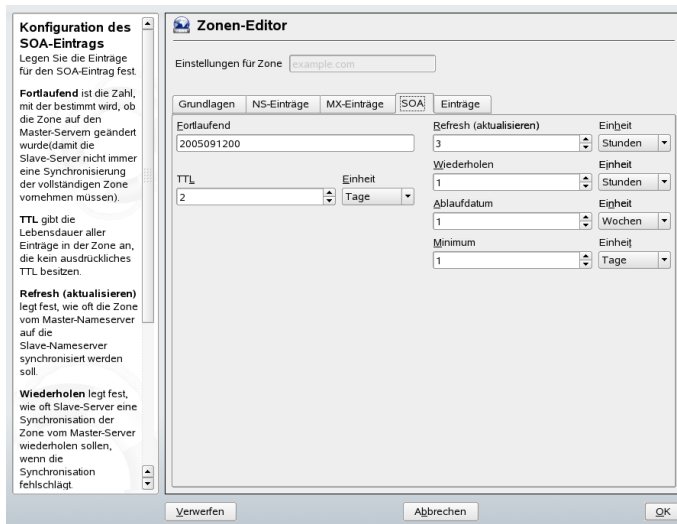
Abbildung 34.8 DNS-Server: Zonen-Editor (MX-Einträge)



Zonen-Editor (SOA)

Auf dieser Seite können Sie SOA (Start of Authority)-Einträge erstellen. Eine Erklärung der einzelnen Optionen finden Sie in [Beispiel 34.6](#), „Datei `/var/lib/named/world.zone`“ (S. 699). Das Ändern von SOA-Datensätzen wird für dynamischen Zonen, die über LDAP verwaltet werden, nicht unterstützt.

Abbildung 34.9 DNS-Server: Zonen-Editor (SOA)



Zonen-Editor (Einträge)

In diesem Dialogfeld wird die Namensauflösung verwaltet. Geben Sie unter *Eintragschlüssel* 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.

34.3 Starten des Namenservers BIND

Bei SUSE® Linux Enterprise-Systemen ist der Namenserver BIND (*Berkeley Internet Name Domain*) vorkonfiguriert, sodass er problemlos unmittelbar nach der Installation gestartet werden kann. Wenn Sie bereits über eine funktionierende Internetverbindung verfügen und 127.0.0.1 als Namenserveradresse für localhost in /etc/resolv.conf eingegeben haben, verfügen Sie normalerweise bereits über eine funktionierende Namensauflösung, ohne dass Ihnen der DNS des Anbieters bekannt sein muss. BIND führt die Namensauflösung über den Root-Namenserver durch. Dies ist ein wesentlich langsamerer Prozess. Normalerweise sollte der DNS des Anbieters zusammen mit der

zugehörigen IP-Adresse in die Konfigurationsdatei `/etc/named.conf` unter `forwarders` eingegeben werden, um eine effektive und sichere Namensauflösung zu gewährleisten. Wenn dies so weit funktioniert, wird der Namenserver als reiner *Nur-Cache*-Namenserver ausgeführt. Nur wenn Sie seine eigenen Zonen konfigurieren, wird er ein richtiger DNS. Ein einfaches Beispiel hierfür ist in der Dokumentation unter `/usr/share/doc/packages/bind/sample-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 `rcnamed start` als `root` ein. Falls rechts in grüner Schrift „done“ angezeigt wird, wurde `named`, wie der Namenserverprozess hier genannt wird, erfolgreich gestartet. Testen Sie den Namenserver umgehend auf dem lokalen System mit den Programmen `host` bzw. `dig`. Diese sollten `localhost` als Standardserver mit der Adresse `127.0.0.1` zurückgeben. Ist dies nicht der Fall, enthält `/etc/resolv.conf` vermutlich einen falschen Namenservereintrag oder die Datei ist überhaupt nicht vorhanden. Beim ersten Test geben Sie `host 127.0.0.1` ein. Dies sollte immer funktionieren. Wenn Sie eine Fehlermeldung erhalten, sollten Sie mit `rcnamed status` überprüfen, ob der Server tatsächlich ausgeführt wird. Wenn der Namenserver sich nicht starten lässt oder unerwartetes Verhalten zeigt, finden Sie die Ursache normalerweise in der Protokolldatei `/var/log/messages`.

Um den Namenserver des Anbieters oder einen bereits in Ihrem Netzwerk ausgeführten Server als Forwarder zu verwenden, geben Sie die entsprechende IP-Adresse(n) im Abschnitt `options` unter `forwarders` ein. Bei den Adressen in [Beispiel 34.1](#), „Weiterleitungsoptionen in `named.conf`“ (S. 694) handelt es sich lediglich um Beispiele. Passen Sie diese Einträge an Ihr eigenes Setup an.

Beispiel 34.1 Weiterleitungsoptionen in *named.conf*

```
options {
    directory "/var/lib/named";
    forwarders { 10.11.12.13; 10.11.12.14; };
    listen-on { 127.0.0.1; 192.168.0.99; };
    allow-query { 127/8; 192.168.0/24; };
    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. Nach dem Ändern der Konfigurationsdatei `/etc/named.conf` oder der Zonendateien müssen Sie BIND anweisen, diese erneut zu lesen. Dies geschieht mit dem Befehl `rndnamed reload`. Dieselbe Wirkung erzielen Sie, wenn Sie den Namensserver mit `rndnamed restart` anhalten und erneut starten. Sie können den Server jederzeit durch Eingabe von `rndnamed stop` anhalten.

34.4 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 34.2](#), „Eine Grundversion von `/etc/named.conf`“ (S. 695).

Beispiel 34.2 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";
};
```

34.4.1 Wichtige Konfigurationsoptionen

`directory "Dateiname";`

Gibt das Verzeichnis an, in dem BIND die Dateien mit den Zonendaten finden kann. In der Regel ist dies `/var/lib/named`.

`forwarders { ip-adresse; };`

Gibt die Namenserver (zumeist des Anbieters) an, an die DNS-Anforderungen weitergeleitet werden sollen, wenn sie nicht direkt aufgelöst werden können.

Ersetzen Sie *ip-adresse* durch eine IP-Adresse wie `10.0.0.1`.

`forward first;`

Führt dazu, dass DNS-Anforderungen weitergeleitet werden, bevor versucht wird, sie über die Root-Namenserver aufzulösen. Anstatt `forward first` kann `forward only` verwendet werden. Damit werden alle Anforderungen weitergeleitet, ohne dass sie an die Root-Namenserver gesendet werden. Dies ist bei Firewall-Konfigurationen sinnvoll.

`listen-on port 53 { 127.0.0.1; ip-adresse; };`

Informiert BIND darüber, an welchen Netzwerkschnittstellen und Ports Client-Abfragen akzeptiert werden sollen. `port 53` muss nicht explizit angegeben wer-

den, da 53 der Standardport ist. Geben Sie `127.0.0.1` ein, um Anforderungen vom lokalen Host zuzulassen. Wenn Sie diesen Eintrag ganz auslassen, werden standardmäßig alle Schnittstellen verwendet.

`listen-on-v6 port 53 {any;};`

Informiert BIND darüber, welcher Port auf IPv6-Client-Anforderungen überwacht werden soll. Die einzige Alternative zu `any` ist `none`. Bei IPv6 akzeptiert der Server nur Wildcard-Adressen.

`query-source address * port 53;`

Dieser Eintrag ist erforderlich, wenn eine Firewall ausgehende DNS-Anforderungen blockiert. Dadurch wird BIND angewiesen, Anforderungen extern von Port 53 und nicht von einem der Ports mit den hohen Nummern über 1024 aufzugeben.

`query-source-v6 address * port 53;`

Informiert BIND darüber, welcher Port für IPv6-Abfragen verwendet werden soll.

`allow-query { 127.0.0.1; netz;};`

Definiert die Netzwerke, von denen aus Clients DNS-Anforderungen aufgeben können. Ersetzen Sie `netz` durch Adressinformationen wie `192.168.1/24`. Der Wert `/24` am Ende ist ein abgekürzter Ausdruck für die Netzmaske, hier `255.255.255.0`.

`allow-transfer ! *;;`

Legt fest, welche Hosts Zonentransfers anfordern können. Im vorliegenden Beispiel werden solche Anforderungen durch `! *` vollständig verweigert. Ohne diesen Eintrag können Zonentransfers ohne Einschränkungen von jedem beliebigen Ort aus angefordert werden.

`statistics-interval 0;`

Ohne diesen Eintrag generiert BIND in der Datei `/var/log/messages` mehrere Zeilen mit statistischen Informationen pro Stunde. Setzen Sie diesen Wert auf `"0"`, um diese Statistiken vollständig zu unterdrücken, oder legen Sie ein Zeitintervall in Minuten fest.

`cleaning-interval 720;`

Diese Option legt fest, in welchen Zeitabständen BIND den Cache leert. Jedes Mal, wenn dies geschieht, wird ein Eintrag in `/var/log/messages` ausgelöst. Die verwendete Einheit für die Zeitangabe ist Minuten. Der Standardwert ist 60 Minuten.

`interface-interval 0;`

BIND durchsucht die Netzwerkschnittstellen regelmäßig nach neuen oder nicht vorhandenen Schnittstellen. Wenn dieser Wert auf 0 gesetzt ist, wird dieser Vorgang nicht durchgeführt und BIND überwacht nur die beim Start erkannten Schnittstellen. Anderenfalls wird das Zeitintervall in Minuten angegeben. Der Standardwert ist 60 Minuten.

`notify no;`

`no` verhindert, dass anderen Namenserver informiert werden, wenn Änderungen an den Zonendaten vorgenommen werden oder wenn der Namenserver neu gestartet wird.

34.4.2 Protokollieren

Der Umfang, die Art und Weise und der Ort der Protokollierung kann in BIND extensiv konfiguriert werden. Normalerweise sollten die Standardeinstellungen ausreichen. In [Beispiel 34.3](#), „Eintrag zur Deaktivierung der Protokollierung“ (S. 697) sehen Sie die einfachste Form eines solchen Eintrags, bei dem jegliche Protokollierung unterdrückt wird.

Beispiel 34.3 Eintrag zur Deaktivierung der Protokollierung

```
logging {  
    category default { null; };  
};
```

34.4.3 Zoneneinträge

Beispiel 34.4 Zoneneintrag für *meine-domaene.de*

```
zone "my-domain.de" in {  
    type master;  
    file "my-domain.zone";  
    notify no;  
};
```

Geben Sie nach `zone` den Namen der zu verwaltenden Domäne (`meine-domaene.de`) an, gefolgt von `in` und einem Block relevanter Optionen in geschweiften Klammern, wie in [Beispiel 34.4](#), „Zoneneintrag für *meine-domaene.de*“ (S. 697) gezeigt. Um eine *Slave-Zone* zu definieren, ändern Sie den Wert von `type` in `slave` und geben Sie einen Namenserver an, der diese Zone als `master` verwaltet

(dieser kann wiederum ein Slave eines anderen Masters sein), wie in [Beispiel 34.5](#), „Zoneneintrag für andere-domaene.de“ (S. 698) gezeigt.

Beispiel 34.5 *Zoneneintrag für andere-domaene.de*

```
zone "other-domain.de" in {
    type slave;
    file "slave/other-domain.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 zur Festlegung der Root-Namensserver verwendet. Diese Zonendefinition kann unverändert beibehalten werden.

`file meine-domaene.zone` oder `file „slave/andere-domaene.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 gestatten würde. Dies ist in der Regel aus Sicherheitsgründen nicht erstrebenswert. Ohne diesen Eintrag sind überhaupt keine Zonenaktuali-

sierungen zulässig. Der oben stehende Eintrag hat dieselbe Wirkung, da ! * solche Aktivitäten effektiv unterbindet.

34.5 Zonendateien

Zwei Arten von Zonendateien sind erforderlich. Eine weist den Hostnamen IP-Adressen zu und die andere macht genau das Gegenteil: Sie stellt einen Hostnamen für eine IP-Adresse bereit.

TIPP: Verwenden des Punktes in Zonendateien

Der Punkt (.) ist in den Zonendateien von entscheidender Bedeutung. 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 `world.zone`, die für die Domäne `world.cosmos` zuständig ist (siehe [Beispiel 34.6](#), „Datei `/var/lib/named/world.zone`“ (S. 699)).

Beispiel 34.6 Datei `/var/lib/named/world.zone`

```
$TTL 2D world.cosmos. IN SOA      gateway root.world.cosmos. ( 2003072441
; serial 1D          ; refresh 2H          ; retry 1W          ; expiry 2D )
; minimum

      IN NS      gateway IN MX      10 sun

gateway      IN A      192.168.0.1 IN A      192.168.1.1 sun      IN A
      192.168.0.2 moon      IN A      192.168.0.3 earth      IN A
      192.168.1.2 mars      IN A      192.168.1.3 www      IN CNAME
moon
```

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 `world.cosmos` 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 `gateway` zu `gateway.world.cosmos` 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. Statt `root@world.cosmos` muss der Eintrag `root.world.cosmos.` lauten. Der Punkt (`.`) am Ende muss stehen, damit nicht die Zone angefügt 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`) 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 – die Zeitdauer, die Ergebnisse nicht aufgelöster DNS-Abfragen von anderen Servern im Cache gespeichert werden können.

Zeile 9:

IN NS gibt den für diese Domäne verantwortlichen Namensserver an. `gateway` wird zu `gateway.world.cosmos` erweitert, da es nicht mit `.` endet. Es kann mehrere solche Zeilen geben – eine für den primären und jeweils eine für jeden 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 `world.cosmos` annimmt, verarbeitet und weiterleitet. In diesem Beispiel ist dies der Host `sun.world.cosmos`. 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 12-17:

Dies sind die eigentlichen Adresseinträge, in denen den Hostnamen eine oder mehrere IP-Adressen zugewiesen werden. Die Namen sind hier ohne `.` aufgeführt, da sie ihre Domäne nicht enthalten. Daher werden sie alle um `world.cosmos` ergänzt. Dem Host-Gateway (`gateway`) werden zwei IP-Adressen zugewiesen, weil er zwei Netzwerkkarten aufweist. Bei jeder traditionellen Hostadresse (IPv4) wird der Eintrag mit `A` gekennzeichnet. Wenn es sich um einer IPv6-Adresse handelt, wird der Eintrag mit `A6` gekennzeichnet. Das frühere Token für IPv6-Adressen war `AAAA`. Dieses ist inzwischen veraltet.

ANMERKUNG: A6-Syntax

Der `A6`-Eintrag weicht in seiner Syntax ein wenig vom `AAAA`-Eintrag ab. 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. Beispiel: Ein alter AAAA-Datensatz mit folgender Syntax:

```
pluto IN          AAAA 2345:00C1:CA11:0001:1234:5678:9ABC:DEF0
pluto IN          AAAA 2345:00D2:DA11:0001:1234:5678:9ABC:DEF0
```

Hier müssen Sie im A6-Format Informationen zu fehlenden Bits hinzufügen. Da das obige Beispiel vollständig ist (es fehlen keine Bits), lautet das A6-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. Wenn ein Host eine IPv4-Adresse aufweist, verwendet er einen A- und keinen A6-Eintrag.

Zeile 18:

Der Alias `www` kann zur Adressierung von `mond` (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. `192.168.1` wird also in `1.168.192.in-addr.arpa` aufgelöst. Siehe [Beispiel 34.7](#), „Reverse-Lookup“ (S. 702).

Beispiel 34.7 *Reverse-Lookup*

```
$TTL 2D 1.168.192.in-addr.arpa. IN SOA gateway.world.cosmos. root.world.cosmos.
( 2003072441 ; serial 1D ; refresh 2H ; retry
1W ; expiry 2D ) ; minimum

IN NS gateway.world.cosmos.

1 IN PTR gateway.world.cosmos. 2
IN PTR earth.world.cosmos. 3 IN PTR
mars.world.cosmos.
```

Zeile 1:

\$TTL definiert die Standard-TTL, die für alle Einträge hier gilt.

Zeile 2:

Die Konfigurationsdatei sollte Reverse-Lookup für das Netzwerk `192.168.1.0` aktivieren. Angenommen, die Zone heißt `1.168.192.in-addr.arpa`, sollte sie nicht zu den Hostnamen hinzugefügt werden. Daher werden alle Hostnamen in ihrer vollständigen Form eingegeben – mit ihrer Domäne und mit einem Punkt (.) am Ende. Die restlichen Einträge entsprechen den im vorherigen Beispiel (`world.cosmos`) beschriebenen Einträgen.

Zeilen 3-7:

Siehe vorheriges Beispiel für `world.cosmos`.

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.

34.6 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 Manual Page für `nsupdate` (`man 8 nsupdate`) entnehmen. Aus Sicherheitsgründen sollten solche Aktualis-

ierungen mithilfe von TSIG-Schlüsseln durchgeführt werden, wie in [Abschnitt 34.7](#), „Sichere Transaktionen“ (S. 704) beschrieben.

34.7 Sichere Transaktionen

Sichere Transaktionen können mithilfe von Transaktionssignaturen (TSIGs) durchgeführt werden, die auf gemeinsam genutzten geheimen Schlüsseln (auch TSIG-Schlüssel genannt) 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 einen TSIG-Schlüssel mit folgendem Befehl (Einzelheiten finden Sie unter `man dnssec-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` aufgenommen wird. 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 `192.168.2.3`), muss die Datei `/etc/named.conf` des Servers folgende Regel enthalten:

```
server 192.168.2.3 {  
    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.

34.8 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.

34.9 Weitere 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 Manualpages. `/usr/share/doc/packages/bind/README.SuSE` enthält aktuelle Informationen zu BIND in SUSE Linux Enterprise.

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.

TIPP: IBM-System z: DHCP-Unterstützung

Auf IBM-System z-Plattformen funktioniert DHCP nur bei Schnittstellen, die die OSA- und OSA Express-Netzwerkkarten verwenden. Diese Karten sind die einzigen mit einer MAC-Adresse, die für die Autokonfigurationsfunktionen von DHCP erforderlich ist.

Zum einen kann ein DHCP-Server so konfiguriert werden, dass er jeden Client anhand der Hardware-Adresse seiner Netzwerkkarte (die in den meisten Fällen unveränderlich ist) 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 entsprechenden Netzwerkeinstellungen von einem DHCP-Server ist auch besonders interessant für Notebooks, die regelmäßig in unterschiedlichen Netzwerken verwendet werden.

Neben IP-Adresse und Netzmaske werden dem Client nicht nur der Computer- und Domänenname, sondern auch das zu verwendende Gateway und die Adressen der Namenserver mitgeteilt. Im Übrigen können auch etliche andere Parameter zentral konfiguriert werden, z. B. ein Zeitserver, von dem die Clients die aktuelle Uhrzeit abrufen können, oder ein Druckserver.

35.1 Konfigurieren eines DHCP-Servers mit YaST

WICHTIG: LDAP-Unterstützung

In dieser Version von SUSE® Linux Enterprise kann das YaST DHCP-Modul 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.

Das YaST DHCP-Modul ermöglicht die Einrichtung Ihres eigenen DHCP-Servers für das lokale Netzwerk. Das Modul kann im einfachen oder im Expertenmodus ausgeführt werden.

35.1.1 Anfängliche Konfiguration (Assistent)

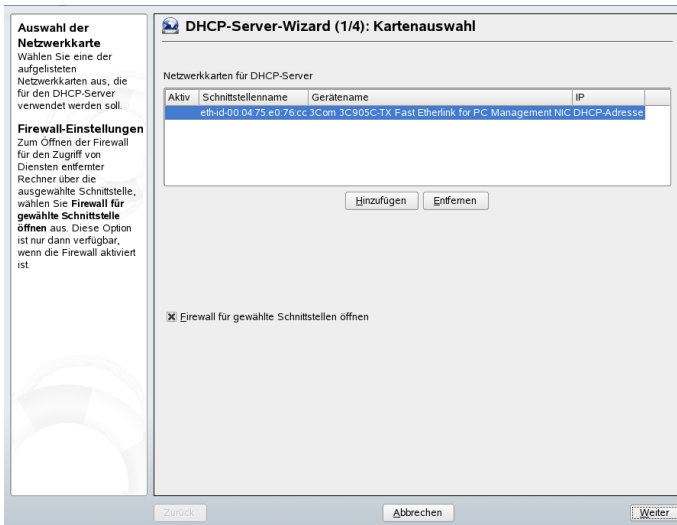
Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Nach Abschluss der anfänglichen Konfiguration ist eine grundlegende Serverkonfiguration

verfügbar, die für einfache Szenarien ausreichend ist. Komplexere Konfigurationsaufgaben 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. Siehe [Abbildung 35.1](#), „DHCP-Server: Kartenauswahl“ (S. 709).

Abbildung 35.1 DHCP-Server: Kartenauswahl



Globale Einstellungen

Geben Sie anhand des Kontrollkästchens an, ob Ihre DHCP-Einstellungen automatisch von einem LDAP-Server gespeichert werden sollen. In den Eingabefeldern legen Sie die Netzwerkinformationen fest, die jeder von diesem DHCP-Server verwaltete Client erhalten soll. Diese sind: Domänenname, Adresse eines Zeitservers, Adressen der primären und sekundären Namensserver, Adressen eines Druck- und WINS-Servers (für gemischte Netzwerkumgebungen mit Windows- und Linux-Clients), Gateway-Adressen und Leasing-Zeit. Siehe [Abbildung 35.2](#), „DHCP-Server: Globale Einstellungen“ (S. 710).

Abbildung 35.2 DHCP-Server: Globale Einstellungen

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.
Mit **IP des primären Nameservers** and **IP des sekundären Nameservers** werden diese Namensserver den DHCP-Clients bereitgestellt. Diese Werte müssen IP-Adressen sein.
Mit **Standard-Gateway** wird dieser Wert als Standardroute in die Routing-Tabelle der Clients eingefügt.
Über **Zeitserver** erhalten Clients die Anweisung, diesen Server für die Zeitsynchronisierung zu verwenden.
Druckserver bietet diesen Server als Standarddruckserver an.

DHCP-Server-Wizard (2/4): Globale Einstellungen

Domainname	example.com	NTP-Zeitserver	ntp.example.com
IP des primären Nameservers	10.20.0.2	Druckserver	
IP des sekundären Nameservers		WINS-Server	
Standardgateway (Router)	10.20.0.1	Standard-Leasing-Zeit	4 Stunden

Zurück Abbrechen Weiter

Dynamisches DHCP

In diesem Schritt konfigurieren Sie die Vergabe der dynamischen IP-Adressen an Clients. Hierzu legen Sie einen Bereich von IP-Adressen fest, in dem die zu vergebenden Adressen der DHCP-Clients liegen dürfen. Alle zu vergebenden Adressen müssen unter eine gemeinsame Netzmaske fallen. Legen Sie abschließend die Leasing-Zeit fest, für die ein Client seine IP-Adresse behalten darf, ohne eine Verlängerung der Leasing-Zeit beantragen zu müssen. Legen Sie optional auch die maximale Leasing-Zeit fest, für die eine bestimmte IP-Adresse auf dem Server für einen bestimmten Client reserviert bleibt. Siehe [Abbildung 35.3](#), „DHCP-Server: Dynamisches DHCP“ (S. 711).

Abbildung 35.3 DHCP-Server: Dynamisches DHCP

The screenshot shows the 'DHCP-Server-Wizard (3/4): Dynamisches DHCP' window. On the left, there is a sidebar with two sections: 'IP-Adressbereich' and 'Leasing-Zeit'. The main area contains the following fields and controls:

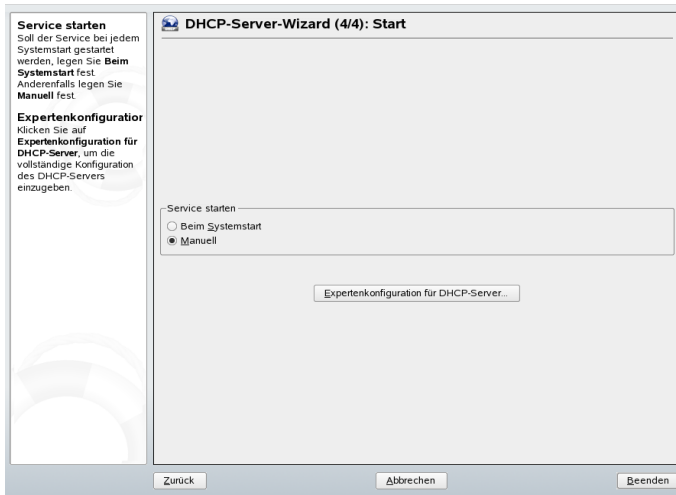
- IP-Adressbereich:**
 - Aktuelles Netzwerk: 172.22.0.0
 - Aktuelle Netzmaske: 255.255.0.0
 - Erste IP-Adresse: 10.20.0.5
 - Letzte IP-Adresse: 10.20.0.255
- Leasing-Zeit:**
 - Standard: 4 (Stunden)
 - Maximum: 2 (Tage)

At the bottom of the window, there are three buttons: 'Zurück', 'Abbrechen', and 'Weiter'.

Fertigstellen der Konfiguration und Auswahl des Startmodus

Nachdem Sie den dritten Teil des Konfigurationsassistenten abgeschlossen haben, gelangen Sie in ein letztes Dialogfeld, das sich mit den Startoptionen des DHCP-Servers befasst. Hier können Sie festlegen, ob der DHCP-Server automatisch beim Booten des Systems oder bei Bedarf manuell (z. B. zu Testzwecken) gestartet werden soll. Klicken Sie auf *Beenden*, um die Konfiguration des Servers abzuschließen. Siehe [Abbildung 35.4](#), „DHCP-Server: Start“ (S. 712). Alternativ können Sie *Host-Verwaltung* links aus der Baumstruktur auswählen, um zusätzlich zur grundlegenden Konfiguration bestimmte Host-Verwaltungsfunktionen zu konfigurieren (siehe [Abbildung 35.5](#), „DHCP-Server: Host-Verwaltung“ (S. 713)).

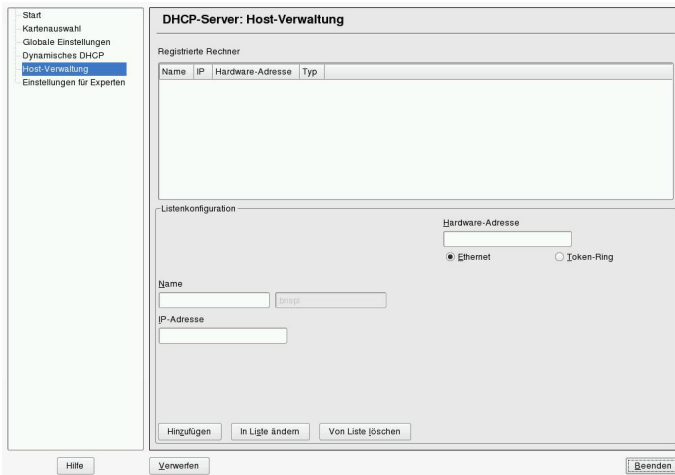
Abbildung 35.4 DHCP-Server: Start



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*. Siehe [Abbildung 35.5](#), „DHCP-Server: Host-Verwaltung“ (S. 713).

Abbildung 35.5 DHCP-Server: Host-Verwaltung



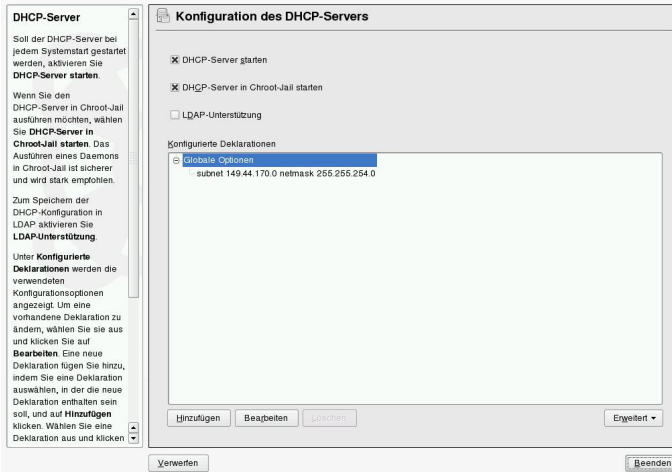
35.1.2 Konfiguration für Experten

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. Siehe [Abbildung 35.6](#), „*DHCP-Server: Chroot-Jail und Deklarationen*“ (S. 714). 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.

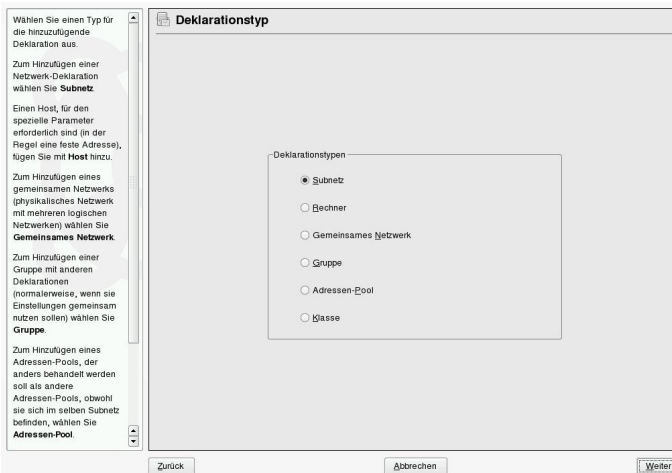
Abbildung 35.6 DHCP-Server: Chroot-Jail und Deklarationen



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 35.7](#), „DHCP-Server: Auswählen eines Deklarationstyps“ (S. 714)).

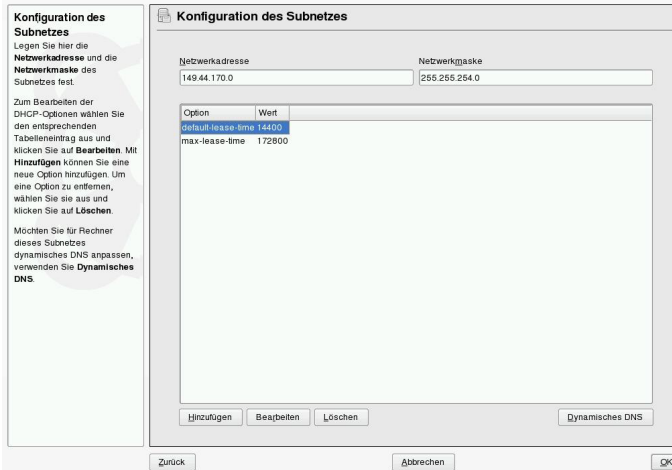
Abbildung 35.7 DHCP-Server: Auswählen eines Deklarationstyps



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*.

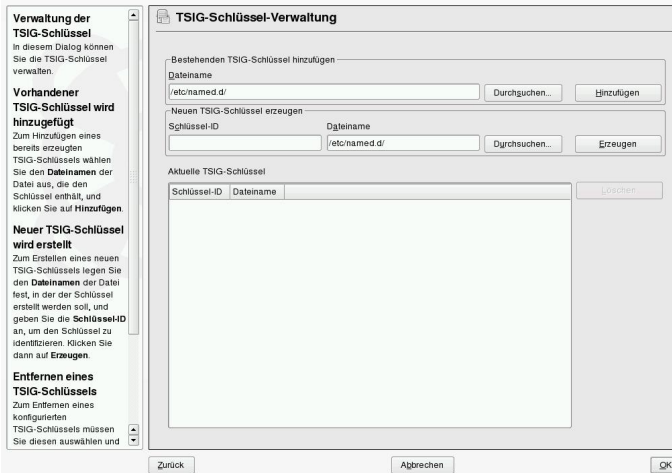
Abbildung 35.8 DHCP-Server: Konfigurieren von Subnetzen



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 35.10](#), „DHCP-Server: Schnittstellenkonfiguration für das dynamische DNS“ (S. 717)).

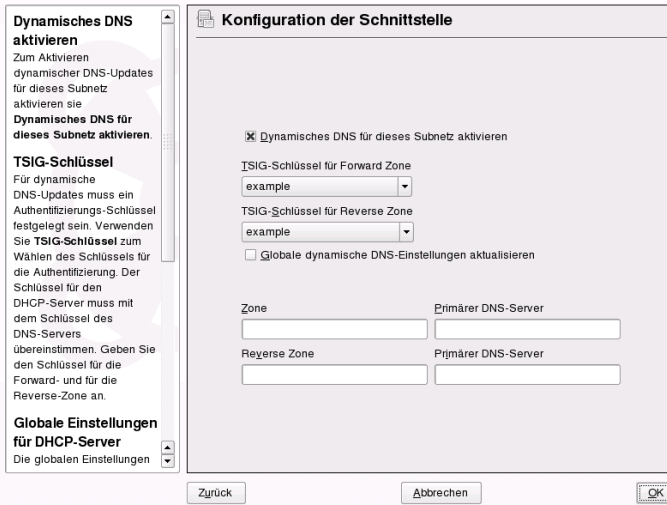
Abbildung 35.9 DHCP-Server: TSIG-Konfiguration



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 35.8](#), „DHCP-Server: Konfigurieren von Subnetzen“ (S. 715)). Wenn Sie noch einmal auf *OK* klicken, gelangen Sie wieder zum ursprünglichen Dialogfeld für die Expertenkonfiguration.

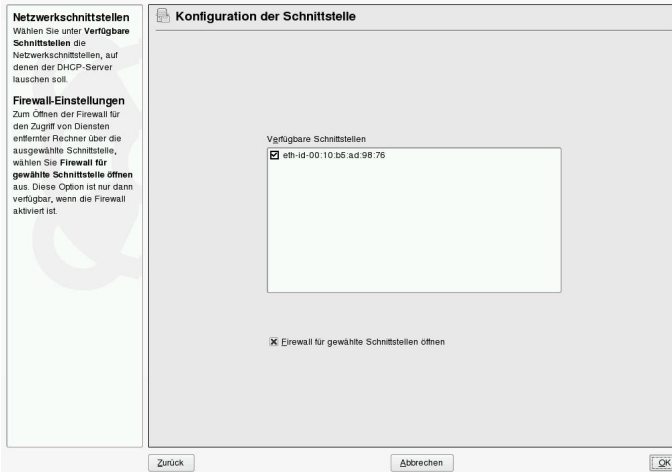
Abbildung 35.10 *DHCP-Server: Schnittstellenkonfiguration für das dynamische DNS*



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 35.11](#), „DHCP-Server: Netzwerkschnittstelle und Firewall“ (S. 718)). Jetzt können Sie zum ursprünglichen Dialogfeld zurückkehren, indem Sie auf *OK* klicken.

Abbildung 35.11 DHCP-Server: Netzwerkschnittstelle und Firewall



Nach Abschluss aller Konfigurationsschritte schließen Sie das Dialogfeld mit *OK*. Der Server wird jetzt mit seiner neuen Konfiguration gestartet.

35.2 DHCP-Softwarepakete

Für SUSE Linux Enterprise stehen sowohl ein DHCP-Server als auch -Clients bereit. Der vom Internet Software Consortium (ISC) herausgegebene DHCP-Server `dhcpd` stellt die Serverfunktionalität zur Verfügung. Client-seitig können Sie zwischen zwei unterschiedlichen DHCP-Clientprogrammen wählen: `dhclient` (ebenfalls vom ISC) und der DHCP Client Daemon im Paket `dhcpd`.

SUSE Linux Enterprise installiert standardmäßig `dhcpd`. 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. Für komplexere Situationen greifen Sie auf `dhclient` von ISC zurück, das sich über die Konfigurationsdatei `/etc/dhclient.conf` steuern lässt.

35.3 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 35.1](#), „Die Konfigurationsdatei `"/etc/dhcpd.conf"`“ (S. 719) an.

Beispiel 35.1 Die Konfigurationsdatei `"/etc/dhcpd.conf"`

```
default-lease-time 600;           # 10 minutes
max-lease-time 7200;             # 2 hours

option domain-name "cosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;

subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.10 192.168.1.20;
    range 192.168.1.100 192.168.1.200;
}
```

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 34, Domain Name System \(DNS\)](#) (S. 681).
- 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 35.1, „Die Konfigurationsdatei `/etc/dhcpd.conf`“](#) (S. 719) können Clients Adressen zwischen `192.168.1.10` und `192.168.1.20` sowie `192.168.1.100` und `192.168.1.200` zugewiesen werden.

Nach dem Bearbeiten dieser wenigen Zeilen sollten Sie bereits in der Lage sein, den DHCP-Daemon mit dem Befehl `rcdhcpd start` zu aktivieren. Der DHCP-Daemon ist sofort einsatzbereit. Mit dem Befehl `rcdhcpd check-syntax` können Sie eine kurze Überprüfung der Konfigurationsdatei vornehmen lassen. Sollte wider Erwarten ein Problem mit der Konfiguration auftreten (z. B. der Server schlägt fehl oder beim Starten `done` nicht zurückgibt), finden Sie in der zentralen Systemprotokolldatei `/var/log/messages` meist ebenso Informationen dazu wie auf Konsole 10 (`Strg` + `Alt` + `F10`).

Auf einem SUSE Linux Enterprise-Standardsystem wird der DHCP-Daemon aus Sicherheitsgründen in einer chroot-Umgebung gestartet. Damit der Daemon die Konfigurationsdateien finden kann, müssen diese in die chroot-Umgebung kopiert

werden. In der Regel müssen Sie dazu nur den Befehl `rcdhcpd start` eingeben, um die Dateien automatisch zu kopieren.

35.3.1 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. `00:00:45:12:EE:F4`. Werden die entsprechenden Zeilen, wie z. B. in [Beispiel 35.2](#), „Ergänzungen zur Konfigurationsdatei“ (S. 721) zur Konfigurationsdatei von [Beispiel 35.1](#), „Die Konfigurationsdatei `/etc/dhcpd.conf`“ (S. 719) hinzugefügt, weist der DHCP-Daemon dem entsprechenden Client immer dieselben Daten zu.

Beispiel 35.2 *Ergänzungen zur Konfigurationsdatei*

```
host earth {
hardware ethernet 00:00:45:12:EE:F4;
fixed-address 192.168.1.21;
}
```

Der Name des entsprechenden Clients (`host Hostname`, hier `earth`) 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 `ip link show` gefolgt vom Netzwerkgerät (z. B. `eth0`) ermittelt werden. Die Ausgabe sollte in etwa wie folgt aussehen:

```
link/ether 00:00:45:12:EE:F4
```

Im vorherigen Beispiel wird also dem Client, dessen Netzwerkkarte die MAC-Adresse `00:00:45:12:EE:F4` hat, automatisch die IP-Adresse `192.168.1.21` und der Hostname "earth" 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.

35.3.2 Die SUSE Linux Enterprise-Version

Aus Sicherheitsgründen enthält bei SUSE Linux der DHCP-Server von ISC den non-root/chroot-Patch von Ari Edelkind. Damit kann `dhcpd` unter 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. Diese Dateien müssen aktualisiert gehalten 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`.

35.4 Weitere Informationen

Weitere Informationen zu DHCP finden Sie auf der Website des *Internet Software Consortium* (<http://www.isc.org/products/DHCP/>). Weitere Informationen finden Sie zudem auf den Manualpages `dhcpcd`, `dhcpcd.conf`, `dhcpcd.leases` und `dhcpcd-options`.

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 soll für die Benutzer transparent sein: Sie sollten unabhängig vom verwendeten Computer immer die gleiche Umgebung vorfinden. Möglich wird dies durch die NIS- und NFS-Dienste. NFS dient der Verteilung von Dateisystemen im Netzwerk und wird in [Kapitel 39, Verteilte Nutzung von Dateisystemen mit NFS](#) (S. 785) 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.

36.1 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 36.1.1, „Konfigurieren eines NIS-Master-Servers“](#) (S. 726) fort.
- Wenn Ihr NIS-Master-Server seine Daten an Slave-Server exportieren soll, richten Sie den Master-Server ein, wie unter [Abschnitt 36.1.1, „Konfigurieren eines NIS-Master-Servers“](#) (S. 726) beschrieben, und richten Sie die Slave-Server in den Subnetzen ein, wie unter [Abschnitt 36.1.2, „Konfigurieren eines NIS-Slave-Servers“](#) (S. 731) beschrieben.

36.1.1 Konfigurieren eines NIS-Master-Servers

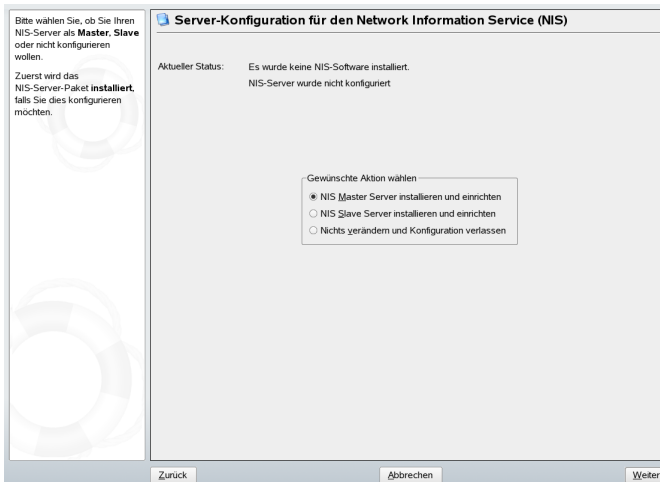
Gehen Sie wie folgt vor, um einen NIS-Master-Server für Ihr Netzwerk zu konfigurieren:

- 1 Starten Sie *YaST* → *Netzwerkdienste* → *NIS-Server*.
- 2 Falls Sie nur einen NIS-Server in Ihrem Netzwerk benötigen oder dieser Server als Master für NIS-Slave-Server fungieren soll, wählen Sie *NIS Master Server installieren und einrichten*. YaST installiert die erforderlichen Pakete.

TIPP

Wenn bereits NIS-Serversoftware auf Ihrem Computer installiert ist, klicken Sie auf *NIS Master Server einrichten*, um die Erstellung eines NIS-Master-Servers zu initiieren.

Abbildung 36.1 NIS-Serverkonfiguration



3 Legen Sie die grundlegenden Optionen für das NIS-Setup fest:

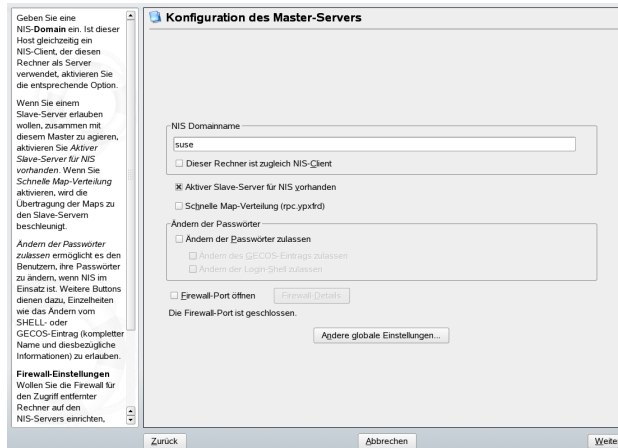
- a** Geben Sie den NIS-Domännennamen ein.
- b** Definieren Sie, ob der Host auch ein NIS-Client sein soll, an dem sich Benutzer anmelden und auf Daten vom NIS-Server zugreifen können, indem Sie *Dieser Rechner ist zugleich NIS-Client* auswählen.

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.

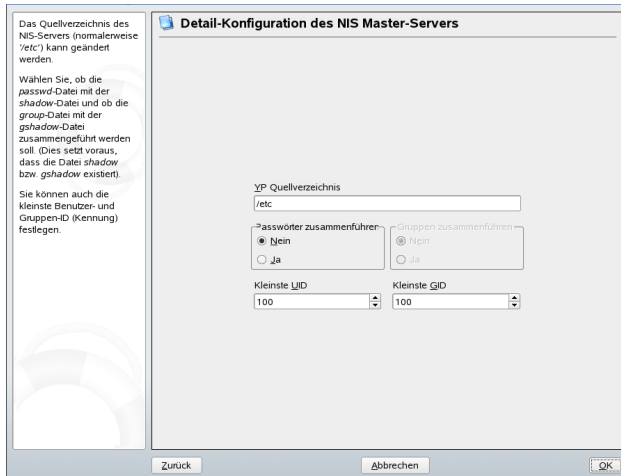
- c Wenn Ihr NIS-Server als Master-Server für NIS-Slave-Server in anderen Subnetzen fungieren soll, wählen Sie *Aktiver Slave-Server für NIS vorhanden*.
- d Wählen Sie *Firewall-Ports öffnen*, damit YaST die Firewall-Einstellungen für den NIS-Server anpasst.

Abbildung 36.2 Konfiguration des Master-Servers



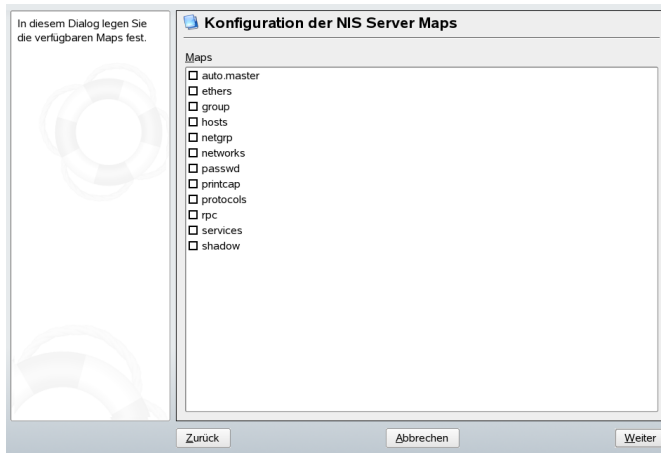
- e Schließen Sie dieses Dialogfeld mit *Weiter* oder klicken Sie auf *Andere globale Einstellungen*, um zusätzliche Einstellungen vorzunehmen. *Andere globale Einstellungen* umfassen das Ändern des Quellverzeichnis für den NIS-Server (standardmäßig `/etc`). Außerdem können hier Passwörter zusammengeführt 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 36.3 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 36.4 Konfiguration der NIS Server Maps

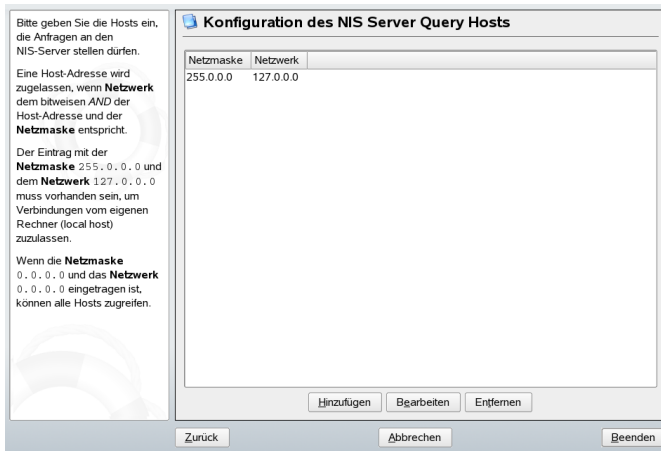


- 7** Geben Sie die Hosts ein, die den NIS-Server abfragen dürfen. Mithilfe der entsprechenden Schaltflächen können Sie Hosts hinzufügen, bearbeiten oder entfernen. Legen Sie fest, aus welchen Netzwerken Anforderungen an den NIS-Server gesendet werden dürfen. Dies ist in der Regel nur das interne Netzwerk. 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 36.5 Einrichten von Anforderungsberechtigungen für einen NIS-Server



- 8 Klicken Sie auf *Beenden*, um die Änderungen zu speichern und das Setup abzuschließen.

36.1.2 Konfigurieren eines NIS-Slave-Servers

Gehen Sie wie folgt vor, um zusätzliche *NIS-Slave-Server* in Ihrem Netzwerk zu konfigurieren:

- 1 Starten Sie *YaST* → *Netzwerkdienste* → *NIS-Server*.
- 2 Wählen Sie *NIS Slave Server installieren und einrichten* und klicken Sie auf *Weiter*.

TIPP

Wenn bereits NIS-Serversoftware auf Ihrem Computer installiert ist, klicken Sie auf *NIS Slave Server einrichten*, um die Erstellung eines NIS-Slave-Servers zu initiieren.

- 3 Vervollständigen Sie das grundlegende Setup Ihres NIS-Slave-Servers:
 - a Geben Sie die NIS-Domäne ein.

- b** Geben Sie den Hostnamen oder die IP-Adresse des Master-Servers ein.
 - c** Aktivieren Sie *Dieser Rechner ist zugleich NIS-Client*, wenn Sie Benutzeranmeldungen auf diesem Server ermöglichen möchten.
 - d** Passen Sie die Firewall-Einstellungen mit *Ports in Firewall öffnen* an.
 - e** 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 *Beenden*, um die Änderungen zu speichern und das Setup abzuschließen.

36.2 Konfigurieren von NIS-Clients

Verwenden Sie das 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 35, DHCP](#) (S. 707). Falls eine statische IP-Adresse verwendet wird, geben Sie die NIS-Domäne und den NIS-Server manuell an. Siehe [Abbildung 36.6, „Festlegen der Domäne und Adresse eines NIS-Servers“](#) (S. 733). *Suchen* weist YaST an, in Ihrem ganzen 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.

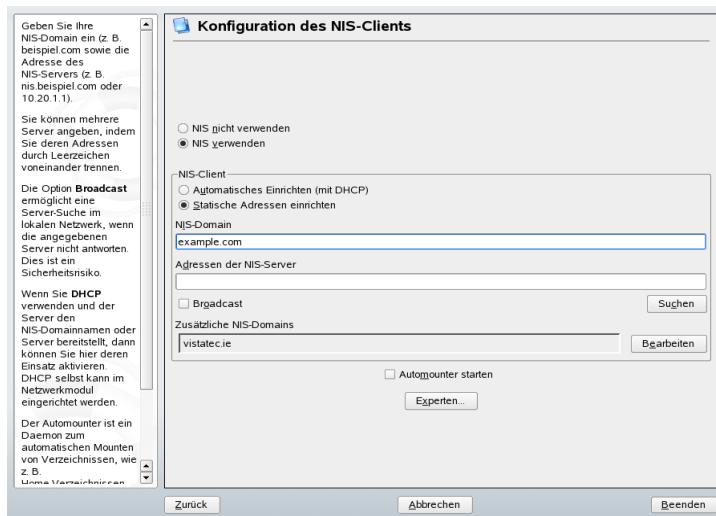
Sie können auch mehrere Server angeben, indem Sie ihre Adressen durch Leerzeichen getrennt unter *Adressen der NIS-Server* angeben.

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 Manualpage `man ypbind`.

Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf *Beenden*, um sie zu speichern und zum YaST-Kontrollzentrum zurückzukehren.

Abbildung 36.6 Festlegen der Domäne und Adresse eines NIS-Servers



LDAP – Ein Verzeichnisdienst

37

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. So ist es nicht erforderlich, für jedes einzelne Kalenderwerkzeug und jeden Email-Client eine eigene Datenbank zu speichern, da stattdessen 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.

37.1 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.

37.2 Struktur eines LDAP-Verzeichnisbaums

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* (DIT, Directory Information Tree) 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`

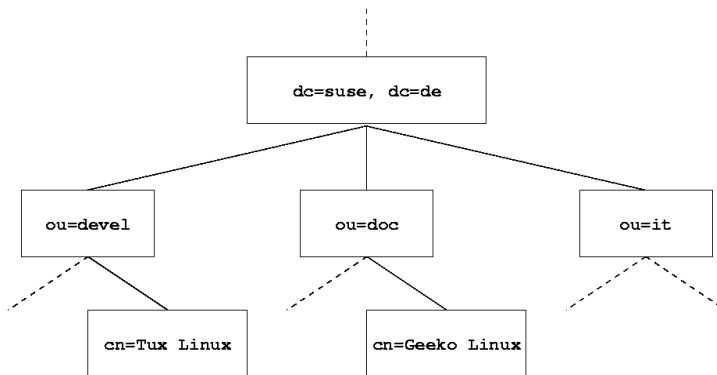
(Domänenkomponente). Dieses Modell ist mit Verzeichnissen (Ordern) in einem Dateisystem vergleichbar.

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 37.1](#), „Struktur eines LDAP-Verzeichnisses“ (S. 738) gezeigt wird.

Abbildung 37.1 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 SUSE-Mitarbeiter Geeko Linux lautet in diesem Fall `cn=Geeko Linux, ou=doc, dc=suse, dc=de`. Er wird zusammengesetzt, indem dem RDN `cn=Geeko Linux` der DN des vorhergehenden Eintrags `ou=doc, dc=suse, dc=de` 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 Objektclassen 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 37.1](#), „Häufig verwendete Objektklassen und Attribute“ (S. 739) 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 Attributwerte.

Tabelle 37.1 Häufig verwendete Objektklassen und Attribute

Objektklasse	Bedeutung	Beispieleintrag	Erforderliche Attribute
dcObject	<i>domainComponent</i> (Name der Domänenkomponenten)	suse	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 37.1](#), „Ausschnitt aus `schema.core`“ (S. 740) wird ein Ausschnitt einer Schemadirektive mit entsprechenden Erklärungen dargestellt (die Zeilen sind für Erklärungszwecke nummeriert).

Beispiel 37.1 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
    $ internationaliSDNNNumber $ 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.

37.3 Serverkonfiguration mit slapd.conf

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.

37.3.1 Globale Direktiven in slapd.conf

Beispiel 37.2 *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 37.2](#), „[slapd.conf: Include-Direktive für Schemata](#)“ (S. 741) dargestellte Direktive in `slapd.conf` gibt das Schema an, anhand dessen das LDAP-Verzeichnis organisiert wird. Der Eintrag `core.schema` ist erforderlich. Dieser Direktive werden zusätzliche erforderliche Schemata angefügt. Weitere Informationen erhalten Sie in der im Lieferumfang enthaltenen OpenLDAP-Dokumentation.

Beispiel 37.3 *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 37.4 *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 37.4**, „*slapd.conf*: Zugriffssteuerung“ (S. 742) 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 und alle folgenden Einträge werden ignoriert.
- Mit *who* wird festgelegt, wer Zugriff auf die mit *what* angegebenen Bereich 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 37.2, „Benutzergruppen und ihre Zugriffsberechtigungen“ (S. 743) dargestellten Einträge sind möglich.

Tabelle 37.2 *Benutzergruppen und ihre Zugriffsberechtigungen*

Tag	Umfang
*	Alle Benutzer ohne Ausnahme
anonymous	Nicht authentifizierte („anonyme“) Benutzer
users	Authentifizierte Benutzer
self	Mit dem Zielobjekt verbundene Benutzer
dn.regex=<regex>	Alle Benutzer, die mit dem regulären Ausdruck übereinstimmen

- Mit *access* wird der Zugriffstyp angegeben. Verwenden Sie die in [Tabelle 37.3](#), „Zugriffstypen“ (S. 743) angegebenen Optionen.

Tabelle 37.3 *Zugriffstypen*

Tag	Umfang des Zugriffs
none	Kein Zugriff
auth	Für die Verbindung zum Server
compare	Für Objekt für Vergleichszugriff
search	Für den Einsatz von Suchfiltern
read	Lesezugriff
write	Schreibzugriff

slapd vergleicht das vom Client angeforderte Zugriffsrecht mit den in `slapd.conf` gewährten Rechten. Dem Client wird Zugriff gewährt, wenn in den Regeln ein höheres als das angeforderte Recht oder gleichwertiges Recht festgelegt ist. Wenn der Client ein höheres Recht als die in den Regeln deklarierten Rechte anfordert, wird ihm der Zugriff verweigert.

In [Beispiel 37.5](#), „`slapd.conf`: Beispiel für die Zugriffssteuerung“ (S. 744) ist ein Beispiel einer einfachen Zugriffssteuerung dargestellt, die mithilfe von regulären Ausdrücken beliebig entwickelt werden kann.

Beispiel 37.5 *slapd.conf: Beispiel für die Zugriffssteuerung*

```
access to dn.regex="ou=([\^,]+),dc=suse,dc=de"  
by dn.regex="cn=administrator,ou=$1,dc=suse,dc=de" 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 Zugriffsteuerung 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>.

37.3.2 Datenbankspezifische Direktiven in slapd.conf

Beispiel 37.6 *slapd.conf: Datenbankspezifische Direktiven*

```
database bdb
checkpoint      1024      5
cachesize       10000
suffix "dc=suse,dc=de"
rootdn "cn=admin,dc=suse,dc=de"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw secret
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd/tools. Mode 700 recommended.
directory /var/lib/ldap
# Indices to maintain
index objectClass eq
```

Der Datenbanktyp, in diesem Fall eine Berkeley-Datenbank, wird in der ersten Zeile dieses Abschnitts festgelegt (siehe [Beispiel 37.6](#), „[slapd.conf: Datenbankspezifische Direktiven](#)“ (S. 745)). Mit `checkpoint` wird die Datenmenge (in KB) festgelegt, die im Transaktionsprotokoll gespeichert wird, bevor die Daten in die tatsächliche Datenbank geschrieben werden. Hiermit wird auch die Zeit (in Minuten) bestimmt, die zwischen zwei Schreibvorgängen vergeht. Mit `cachesize` wird die Anzahl der im Zwischenspeicher der Datenbank gespeicherten Objekte festgelegt. Mit `suffix` wird angegeben, für welchen Teil des LDAP-Baums dieser Server verantwortlich sein soll. 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. Das Administratorpasswort wird mit `rootpw` festgelegt. Anstelle von `secret` kann hier auch der mit `slappasswd` erstellte Hash-Wert des Administratorpassworts eingegeben werden. Die `directory`-Direktive gibt das Verzeichnis im Dateisystem an, in dem die Datenbankverzeichnisse auf dem Server gespeichert sind. 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. Die an dieser Stelle für die Datenbank festgelegten benutzerdefinierten Regeln für Access können anstelle der globalen Access-Regeln verwendet werden.

37.3.3 Starten und Anhalten der Server

Nachdem der LDAP-Server vollständig konfiguriert und alle gewünschten Einträge gemäß dem in [Abschnitt 37.4, „Datenbehandlung im LDAP-Verzeichnis“](#) (S. 746) beschriebenen Schema vorgenommen wurden, starten Sie den LDAP-Server als `root`, indem Sie den Befehl `rcldap start` eingeben. Durch Eingabe des Befehls `rcldap stop` können Sie den Server manuell anhalten. Den Status des laufenden LDAP-Servers fragen Sie mit `rcldap status` ab.

Mit dem in [Abschnitt 20.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 431) beschriebenen Runlevel-Editor von YaST kann der Server automatisch beim Booten und Anhalten des Systems gestartet bzw. angehalten werden. Darüber hinaus besteht die Möglichkeit, wie in [Abschnitt 20.2.2, „Init-Skripts“](#) (S. 427) beschrieben, die entsprechenden Verknüpfungen zu den Start- und Anhaltsskripten mit dem Befehl `insserv` über die Kommandozeile zu erstellen.

37.4 Datenbehandlung im LDAP-Verzeichnis

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 kurz beschrieben.

37.4.1 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 37.1](#), „Struktur eines LDAP-Verzeichnisses“ (S. 738) würde der Datei in [Beispiel 37.7](#), „Beispiel für eine LDIF-Datei“ (S. 747) ähneln.

Beispiel 37.7 *Beispiel für eine LDIF-Datei*

```
# The SUSE Organization
dn: dc=suse,dc=de
objectClass: dcObject
objectClass: organization
o: SUSE AG dc: suse

# The organizational unit development (devel)
dn: ou=devel,dc=suse,dc=de
objectClass: organizationalUnit
ou: devel

# The organizational unit documentation (doc)
dn: ou=doc,dc=suse,dc=de
objectClass: organizationalUnit
ou: doc

# The organizational unit internal IT (it)
dn: ou=it,dc=suse,dc=de
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 er `cn=admin,dc=suse,dc=de`. Mit `-W` wird die Passwordeingabe in der Kommandozeile (unverschlüsselt) umgangen und eine separate Passwordeingabeaufforderung aktiviert. Das Passwort wurde zuvor in `slapd.conf` mit `rootpw` festgelegt. Mit `-f`

wird der Dateiname weitergegeben. Detaillierte Informationen zum Ausführen von `ldapadd` erhalten Sie in [Beispiel 37.8](#), „`ldapadd` mit `example.ldif`“ (S. 748).

Beispiel 37.8 *ldapadd mit example.ldif*

```
ldapadd -x -D cn=admin,dc=suse,dc=de -W -f example.ldif
```

```
Enter LDAP password:
adding new entry "dc=suse,dc=de"
adding new entry "ou=devel,dc=suse,dc=de"
adding new entry "ou=doc,dc=suse,dc=de"
adding new entry "ou=it,dc=suse,dc=de"
```

Die Benutzerdaten einzelner Personen können in separaten LDIF-Dateien vorbereitet werden. In [Beispiel 37.9](#), „LDIF-Daten für Tux“ (S. 748) wird dem neuen LDAP-Verzeichnis Tux hinzugefügt.

Beispiel 37.9 *LDIF-Daten für Tux*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
objectClass: inetOrgPerson
cn: Tux Linux
givenName: Tux
sn: Linux
mail: tux@suse.de
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.

37.4.2 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 37.10](#), „Geänderte LDIF-Datei tux.ldif“ (S. 749) angegeben.

Beispiel 37.10 *Geänderte LDIF-Datei tux.ldif*

```
# coworker Tux
dn: cn=Tux Linux,ou=devel,dc=suse,dc=de
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=admin,dc=suse,dc=de -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=admin,dc=suse,dc=de -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=suse,dc=de
changetype: modify
replace: telephoneNumber
telephoneNumber: +49 1234 567-10
```

Detaillierte Informationen zu `ldapmodify` und der zugehörigen Syntax finden Sie auf der Manualpage `ldapmodify`.

37.4.3 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=suse,dc=de "(objectClass=*)"
```

Mit der Option `-b` wird die Suchbasis festgelegt – der Abschnitt des Baums, in dem die Suche durchgeführt werden soll. Im aktuellen Fall lautet er `dc=suse,dc=de`. 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)`).

37.4.4 Löschen von Daten in einem LDAP-Verzeichnis

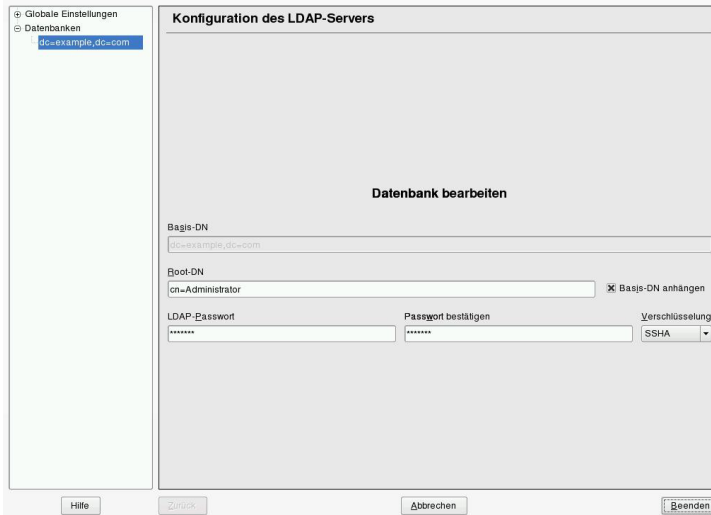
Mit `ldapdelete` werden unerwünschte Einträge gelöscht. Die Syntax ist ähnlich wie die der anderen Befehle. Wenn Sie beispielsweise den vollständigen Eintrag für `Tux Linux` löschen möchten, erteilen Sie folgenden Befehl:

```
ldapdelete -x -D cn=admin,dc=suse,dc=de -W cn=Tux \
Linux,ou=devel,dc=suse,dc=de
```

37.5 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 37.2 *YaST-LDAP-Server-Konfiguration*



Zum Einrichten eines LDAP-Servers für Benutzerkontodaten gehen Sie wie folgt vor:

- 1 Melden Sie sich als `root`-Benutzer 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. Wählen Sie dabei aus:

`bind_v2`

Diese Option aktiviert Verbindungsanforderungen (Bind-Anforderungen) von Clients mit der vorigen Version des Protokolls (LDAPv2).

`bind_anon_cred`

Für gewöhnlich 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`

Wenn Sie diese Option aktivieren, sind nicht authentifizierte (anonyme) Update-Vorgänge möglich. Der Zugriff ist gemäß ACLs und anderen Regeln beschränkt (siehe [Abschnitt 37.3.1](#), „Globale Direktiven in `slapd.conf`“ (S. 741)).

- 4 Zum Konfigurieren der sicheren Kommunikation von Client und Server fahren Sie mit *TLS-Einstellungen* fort:
 - a Setzen Sie *TLS Active* auf *Yes*, um die TLS und SSL-Verschlüsselung der Client/Server-Kommunikation zu aktivieren.
 - b Klicken Sie auf *Zertifikat auswählen* und bestimmen Sie, wie ein gültiges Zertifikat erhalten wird. Wählen Sie *Zertifikat importieren* (Import eines Zertifikats von externer Quelle) oder *Gemeinsames Serverzertifikat verwenden* (Verwenden des bei der Installation von SUSE® Linux Enterprise Server erstellten Zertifikats).

- Wenn Sie ein Zertifikat importieren möchten, werden Sie von YaST aufgefordert, den genauen Pfad zum Standort anzugeben.
- Wenn Sie sich für das gemeinsame Serverzertifikat entschieden haben und dieses während der Installation nicht erstellt wurde, wird es anschließend erstellt.

Gehen Sie zum Konfigurieren der Datenbanken Ihres LDAP-Servers wie folgt vor:

- 1 Wählen Sie die Option *Datenbanken* links im Dialogfeld.
- 2 Klicken Sie auf *Datenbanken hinzufügen*, um die neue Datenbank hinzuzufügen.
- 3 Geben Sie die erforderlichen Daten ein:

Basis-DN

Geben Sie den Basis-DN Ihres LDAP-Servers an.

Root-DN

Geben Sie den DN des verantwortlichen Server-Administrators an. Wenn Sie die Option *Basis-DN anhängen* aktivieren, müssen Sie nur den `cn` des Administrators eingeben. Das System macht die restlichen Angaben automatisch.

LDAP-Passwort

Geben Sie das Passwort für den Datenbankadministrator ein.

Verschlüsselung

Legen Sie den Verschlüsselungsalgorithmus zum Sichern des Passworts für den Root-DN fest. Wählen Sie *crypt*, *sm5*, *sha* oder *sha*. Im Dialogfeld ist auch die Option *plain* verfügbar, um die Verwendung von reinen Textpasswörtern zu ermöglichen. Aus Sicherheitsgründen wird diese Option jedoch nicht empfohlen. Wählen Sie *OK* zum Bestätigen Ihrer Einstellungen und um zum vorigen Dialogfeld zurückzukehren.

Zum Bearbeiten einer vorher erstellten Datenbank wählen Sie Ihren Basis-DN links im Baum aus. Im rechten Teil des Fensters zeigt YaST ein ähnliches Dialogfeld, das dem zum Erstellen einer neuen Datenbank ähnelt. Dabei ist der hauptsächliche Unterschied, dass der DN-Eintrag grau dargestellt ist und nicht verändert werden kann.

Nach dem Beenden der LDAP-Serverkonfiguration mit *Fertig stellen* 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.

37.6 Konfigurieren eines LDAP-Clients 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 durch Auswahl von *Netzwerkdienste* → *LDAP-Client*. YaST aktiviert alle PAM- und NSS-bezogenen Änderungen, die für LDAP erforderlich sind, und installiert die benötigten Dateien.

37.6.1 Standardverfahren

Hintergrundwissen über die Prozesse, die auf einem Client-Computer im Hintergrund ausgeführt werden, erleichtert Ihnen das Verständnis der Funktionsweise des YaST-Moduls LDAP-Client. Wenn LDAP für die Netzwerkauthentifizierung aktiviert oder das YaST-Modul aufgerufen wird, werden die Pakete `pam_ldap` und `nss_ldap` installiert und die beiden entsprechenden Konfigurationsdateien angepasst. `pam_ldap` ist das PAM-Modul, das für die Verhandlung zwischen den Anmeldeprozessen und dem LDAP-Verzeichnis als Quelle der Authentifizierungsdaten verantwortlich ist. Das dedizierte Modul `pam_ldap.so` wird installiert und die PAM-Konfiguration entsprechend angepasst (siehe [Beispiel 37.11](#), „An LDAP angepasste Datei `pam_unix2.conf`“ (S. 754)).

Beispiel 37.11 *An LDAP angepasste Datei `pam_unix2.conf`*

```
auth:         use_ldap
account:      use_ldap
password:     use_ldap
session:      none
```

Bei der manuellen Konfiguration zusätzlicher Dienste für die Verwendung von LDAP nehmen Sie das PAM-LDAP-Modul in die entsprechende PAM-Konfigurationsdatei für den Dienst in `/etc/pam.d` auf. Konfigurationsdateien, die bereits für einzelne

Dienste angepasst sind, finden Sie unter `/usr/share/doc/packages/pam_ldap/pam.d/`. Kopieren Sie die entsprechenden Dateien in `/etc/pam.d`.

Die `glibc`-Namenauflösung über den `nsswitch`-Mechanismus wird an den Einsatz von LDAP mit `nss_ldap` angepasst. Bei der Installation dieses Pakets wird eine neue angepasste Datei `nsswitch.conf` in `/etc/` erstellt. Weitere Informationen zur Funktionsweise von `nsswitch.conf` erhalten Sie unter [Abschnitt 31.6.1](#), „[Konfigurationsdateien](#)“ (S. 651). In der Datei `nsswitch.conf` müssen für die Benutzerverwaltung und -authentifizierung mit LDAP folgende Zeilen vorhanden sein: Siehe [Beispiel 37.12](#), „[Anpassungen in nsswitch.conf](#)“ (S. 755).

Beispiel 37.12 *Anpassungen in nsswitch.conf*

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

Mit diesen Zeilen wird die Resolver-Bibliothek von `glibc` so angeordnet, dass zuerst die entsprechenden Dateien in `/etc` bewertet und zusätzlich der LDAP-Server aufgerufen wird, die als Quellen für Authentifizierungs- und Benutzerdaten dienen. Diesen Mechanismus können Sie testen, indem Sie beispielsweise die Inhalte der Benutzerdatenbank mit dem Befehl `getent passwd` abrufen. Der zurückgegebene Datensatz enthält eine Übersicht über die lokalen Benutzer des Systems und über alle auf dem LDAP-Server gespeicherten Benutzer.

Um zu verhindern, dass sich reguläre über LDAP verwaltete Benutzer mit `ssh` oder `login` beim Server anmelden, müssen die Dateien `/etc/passwd` und `/etc/group` eine zusätzliche Zeile enthalten. Hierbei handelt es sich um die Zeile `+:::/:sbin/nologin` in `/etc/passwd` und `+:::` in `/etc/group`.

37.6.2 Konfigurieren des LDAP-Client

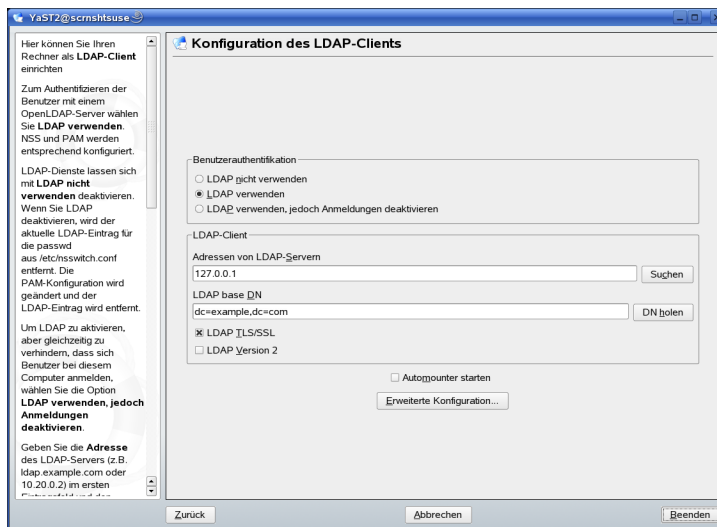
Nachdem YaST die ersten Anpassungen von `nss_ldap`, `pam_ldap`, `/etc/passwd` und `/etc/group` vorgenommen hat, können Sie einfach eine Verbindung zwischen dem Client und dem Server herstellen und die Benutzer von YaST über LDAP verwalten lassen. Das grundlegende Setup wird in „[Grundlegende Konfiguration](#)“ (S. 756) 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 „[Konfigurieren der YaST-Gruppe und der Benutzerverwaltungsmodule](#)“ (S. 759) beschrieben.

Grundlegende Konfiguration

Das Dialogfeld für die grundlegende Konfiguration des LDAP-Client ([Abbildung 37.3](#), „[YaST: Konfiguration des LDAP-Client](#)“ (S. 756)) wird während der Installation geöffnet, wenn Sie die LDAP-Benutzerverwaltung oder *Netzwerkdienste* → *LDAP-Client* im YaST-Kontrollzentrum des installierten Systems auswählen.

Abbildung 37.3 *YaST: Konfiguration des LDAP-Client*



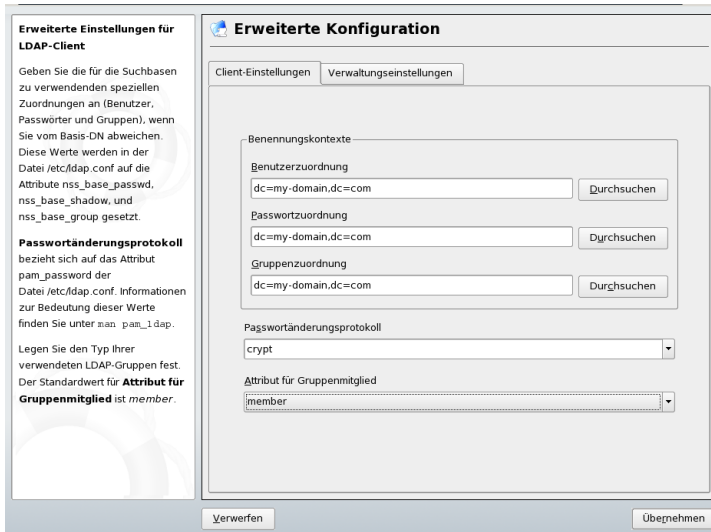
Gehen Sie wie folgt vor, um die Benutzer Ihres Computers bei einem OpenLDAP-Server zu authentifizieren und die Benutzerverwaltung über OpenLDAP zu aktivieren:

- 1 Klicken Sie zum Aktivieren von LDAP auf *LDAP verwenden*. Wählen Sie *LDAP verwenden, jedoch Anmeldungen deaktivieren* aus, wenn LDAP für die Authen-

tifizierung 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** Klicken Sie zum Anwenden der Einstellungen auf *Beenden*.

Abbildung 37.4 YaST: Erweiterte Konfiguration



Wenn Sie als Administrator Daten auf einem Server ändern möchten, klicken Sie auf *Erweiterte Konfiguration*. Das folgende Dialogfeld verfügt über zwei Registerkarten. Siehe [Abbildung 37.4](#), „YaST: Erweiterte Konfiguration“ (S. 758).

- 1** Passen Sie auf der Registerkarte *Client-Einstellungen* die folgenden Einstellungen je nach Bedarf an:
 - a** 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.
 - b** 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 Manualseite `pam_ldap`.
 - c** 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:

- a** Legen Sie die Basis zum Speichern der Benutzerverwaltungsdaten mit *Konfigurations-Base DN* fest.
- b** 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=admin,dc=suse,dc=de`) oder aktivieren Sie *Basis-DN anhängen*, damit der Basis-DN automatisch angehängt wird, wenn Sie `cn=admin` eingeben.
- c** Aktivieren Sie die Option *Standardkonfigurationsobjekte erzeugen*, um die Standardkonfigurationsobjekte auf dem Server zu erstellen und so die Benutzerverwaltung über LDAP zu ermöglichen.
- d** Wenn der Client-Computer als Dateiserver für die Home-Verzeichnisse in Ihrem Netzwerk fungieren soll, aktivieren Sie *Home-Verzeichnisse auf diesem Computer*.
- e** Klicken Sie zum Verlassen der *Erweiterten Konfiguration* auf *Übernehmen* und anschließend zum Zuweisen der Einstellungen auf *Beenden*.

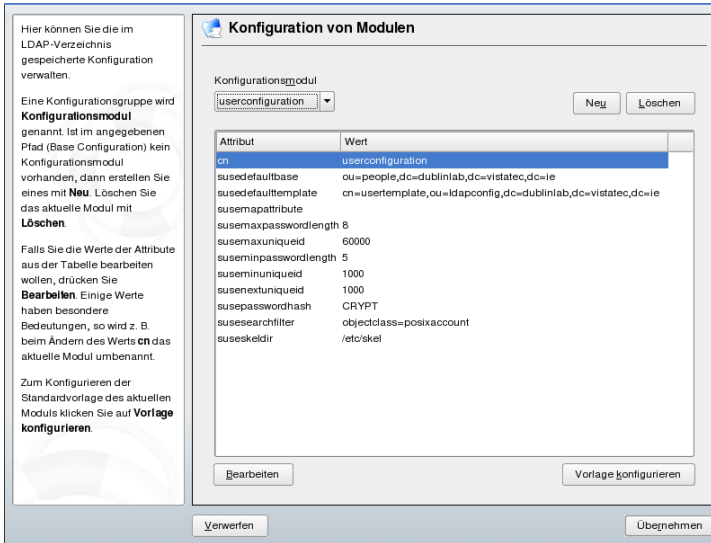
Mit *Einstellungen für die Benutzerverwaltung konfigurieren* bearbeiten Sie Einträge auf dem LDAP-Server. Der Zugriff auf die Konfigurationsmodule auf dem Server wird anschließend entsprechend den auf dem Server gespeicherten ACLs und ACIs gewährt. Befolgen Sie die in [„Konfigurieren der YaST-Gruppe und der Benutzerverwaltungsmodule“](#) (S. 759) beschriebenen Schritte.

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 37.5 YaST: Modulkonfiguration



Im Dialogfeld für die Modulkonfiguration ([Abbildung 37.5](#), „YaST: Modulkonfiguration“ (S. 760)) 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,

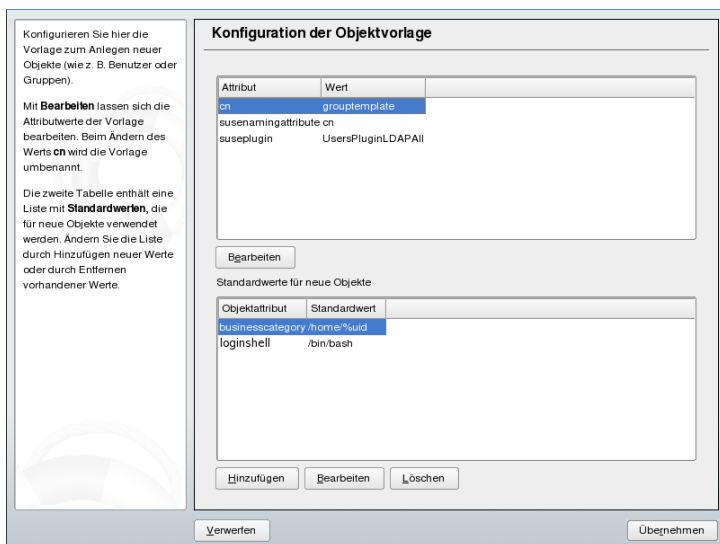
indem Sie *Bearbeiten* wählen und den neuen Wert eingeben. Ein Modul können Sie umbenennen, indem Sie einfach das Attribut `cn` des Moduls ändern. Durch Klicken auf *Löschen* wird das ausgewählte Modul gelöscht.

4 Mit *Übernehmen* fügen Sie das neue Modul dem Auswahlménú 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 37.6 YaST: Konfiguration einer Objektvorlage



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 Vorlage richtig konfiguriert wurden und zum Ausführen bereit sind, können neue Gruppen und Benutzer wie gewohnt mit YaST registriert werden.

37.7 Konfigurieren von LDAP-Benutzern und -Gruppen in YaST

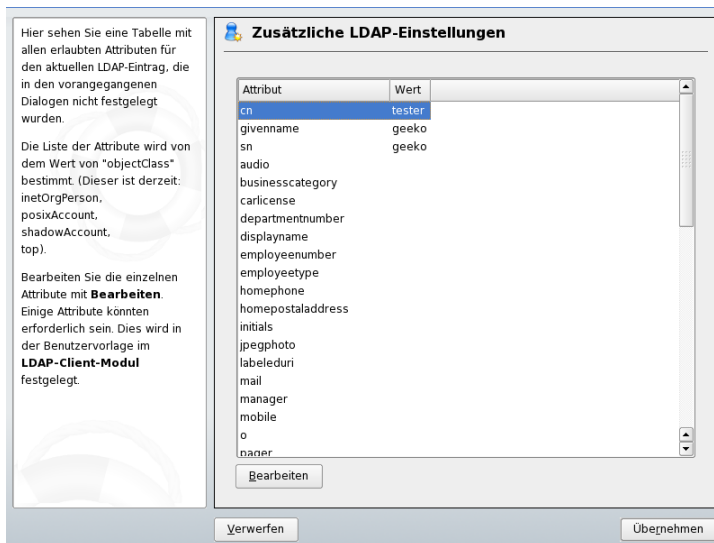
Die tatsächliche Registrierung der Benutzer- und Gruppendaten weicht nur geringfügig von dem Vorgang ohne Verwendung von LDAP ab. Die folgenden kurzen Anweisungen betreffen die Benutzerverwaltung. Das Verfahren für die Gruppenverwaltung entspricht dieser Vorgehensweise.

- 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:
 - a Geben Sie auf der Registerkarte *Benutzerdaten* den Benutzernamen, die Anmeldeinformationen und das Passwort an.

- b 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 „[Konfigurieren der YaST-Gruppe und der Benutzerwartungsmodule](#)“ (S. 759) beschriebenen Schritten definiert werden.
- c Ändern oder akzeptieren Sie die standardmäßigen *Passworteinstellungen*.
- d 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 37.7](#), „[YaST: Zusätzliche LDAP-Einstellungen](#)“ (S. 763)).

4 Klicken Sie zum Zuweisen der Einstellungen und zum Beenden der Benutzerkonfiguration auf *Übernehmen*.

Abbildung 37.7 *YaST: Zusätzliche LDAP-Einstellungen*



Im ersten Eingabeformular der Benutzerverwaltung stehen *LDAP-Optionen* zur Verfügung. Hier haben Sie die Möglichkeit, LDAP-Suchfilter auf die Gruppe der verfügbaren Benutzer anzuwenden oder das Modul zur Konfiguration von LDAP-Benutzern

und -Gruppen durch die Auswahl von *Verwaltung von Benutzern und Gruppen* aufzurufen.

37.8 Weitere 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* (Verweise siehe unten).

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. Sie 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.

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.

38.1 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-Domänennetzwerk einrichten konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das TCP/IP-Protokoll installiert sein.

TIPP: IBM-System z: NetBIOS-Unterstützung

IBM-System z unterstützt nur SMB über TCP/IP. NetBIOS-Unterstützung ist auf diesen Systemen nicht verfügbar.

CIFS-Protokoll

Das CIFS-Protokoll (Common Internet File System) ist ein weiteres Protokoll, das von Samba unterstützt wird. 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 nah an der Netzwerkhardware arbeitet, nennt sich NetBEUI, wird aber 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 Daemons 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 Verzeichnisses entsprechen. Ebenso wird einem Drucker ein Name zugeordnet. Unter diesem Namen können die Clients auf den Drucker zugreifen.

38.2 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 38.3.1, „Konfigurieren eines Samba-Servers mit YaST“](#) (S. 769) beschrieben ist.

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`.

38.3 Konfigurieren eines Samba-Servers

Ein Samba-Server in SUSE® Linux Enterprise kann auf zwei Arten konfiguriert werden: mit YaST oder manuell. Bei der manuellen Konfiguration können Sie mehr Details einstellen, allerdings müssen Sie ohne den Komfort der Bedienoberfläche von YaST zurechtkommen.

38.3.1 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 *Fertig stellen*, 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 38.2, „Starten und Stoppen von Samba“](#) (S. 769).

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 der Registerkarte *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, beispielsweise LDAP, können Sie festlegen, wenn Sie auf *Erweiterte Einstellungen* klicken.

Benutzer anderer Domänen

Sie ermöglichen Benutzern anderer Domänen den Zugriff auf Ihre Domäne, indem Sie die entsprechenden Einstellungen in der Registerkarte *Verbürgte Domänen* vornehmen. Klicken Sie zum Hinzufügen einer neuen Domäne auf *Hinzufügen*. Zum Entfernen der ausgewählten Domäne klicken Sie auf *Löschen*.

Verwenden von LDAP

In der Registerkarte *LDAP-Einstellungen* können Sie den LDAP-Server für die Authentifizierung festlegen. Um die Verbindung mit Ihrem LDAP-Server zu testen, klicken Sie auf *Verbindung testen*. LDAP-Einstellungen für Experten oder die Verwendung von Standardwerten können Sie festlegen, wenn Sie auf *Erweiterte Einstellungen* klicken.

Weitere Informationen zu IrDA finden Sie in [Kapitel 37, LDAP – Ein Verzeichnisdienst](#) (S. 735).

38.3.2 Web-Administration mit SWAT

Ein alternatives Werkzeug für die Administrationsaufgaben von Samba-Server ist SWAT (Samba Web Administration Tool). 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. Öffnen Sie zur Aktivierung in YaST *Netzwerkdienste* → *Netzwerkdienste (xinetd)*, aktivieren Sie die Konfiguration der Netzwerkdienste, wählen Sie *swat* aus der Tabelle und klicken Sie auf *Status wechseln (Ein oder Aus)*.

38.3.3 Manuelles Konfigurieren des Servers

Wenn Sie Samba als Server einsetzen 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. Sollte der Name bereits vergeben sein, 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 38.1 *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 38.2 *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 Freigabennamen 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 Freigabenamen 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 Benutzerzeichnisses 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 `writeable = 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`.

38.4 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.

38.4.1 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 *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 *Beenden*, um die Konfiguration abzuschließen.

38.4.2 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.

38.5 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 38.3](#), „[Abschnitt "global" in smb.conf](#)“ (S. 777) beschrieben.

Beispiel 38.3 *Abschnitt "global" in smb.conf*

```
[global]
    workgroup = TUX-NET
    domain logons = Yes
    domain master = Yes
```

Werden zur Verifizierung verschlüsselte Passwörter genutzt (Standard bei gepflegten MS Windows 9x-Installationen, MS Windows NT 4.0 ab Service Pack 3 und allen

späteren Produkten), muss der Samba-Server damit umgehen 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. Dies erfolgt mit dem 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 38.4 *Einrichten eines Computerkontos*

```
useradd hostname\$\n\nsmbpasswd -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 Beispielkonfiguration (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) sind Einstellungen enthalten, die diese Arbeiten automatisieren.

Beispiel 38.5 *Automatisiertes Einrichten eines Computerkontos*

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \n\n-s /bin/false %m\$\n
```

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`).

38.6 Samba-Server im Netzwerk mit Active Directory

Wenn Sie Linux- und Windows-Server gemeinsam ausführen, können Sie zwei unabhängige Authentifizierungssysteme und -netzwerke aufbauen oder die Server mit

einem Netzwerk verbinden, das über ein zentrales Authentifizierungssystem verfügt. Da Samba mit einer Active Directory-Domäne zusammenarbeitet, können Sie Ihr SUSE Linux Enterprise Server mit Active Directory (AD) anbinden.

Binden Sie eine vorhandene AD-Domäne während der Installation an oder indem Sie später die SMB-Benutzerauthentifizierung mit YaST im installierten System aktivieren. Genauere Informationen zur Domänenanbindung während der Installation finden Sie unter „Konfigurieren des Host als Mitglied der Windows-Domäne“ (S. 72).

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 die zu verbindende Domäne unter *Domäne oder Arbeitsgruppe* im Dialogfeld *Windows-Domänenmitgliedschaft* an. Sie können auch den Befehl *Durchsuchen* verwenden, um eine Liste aller verfügbarer Domänen zu erhalten und eine auszuwählen.

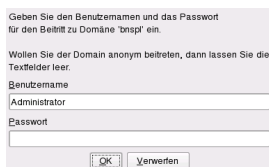
Abbildung 38.1 Festlegen der Windows-Domänenmitgliedschaft



- 4 Aktivieren Sie *Zusätzlich SMB-Informationen für Linux-Authentifizierung verwenden*, um die SMB-Quelle für die Linux-Authentifizierung unter SUSE Linux Enterprise Server zu nutzen.

- 5 Klicken Sie auf *Fertig stellen* und bestätigen Sie nach Aufforderung die Domänenverbindung.
- 6 Geben Sie das Passwort für den Windows-Administrator auf dem AD-Server an und klicken Sie auf *OK*.

Abbildung 38.2 *Angeben von Administratorberechtigungen*



Ihr Server ist jetzt so eingerichtet, dass alle Authentifizierungsdaten vom Active Directory-Domänencontroller abgerufen werden.

38.7 Migrieren eines Windows NT-Servers auf Samba

Abgesehen von der Samba- und der LDAP-Konfiguration besteht die Migration eines Windows NT-Server auf einen SUSE Linux Enterprise Server Samba-Server aus zwei grundlegenden Schritten. Zuerst müssen die Profile, dann die Konten migriert werden.

38.7.1 Vorbereiten des LDAP-Servers

Der erste Schritt bei der Migration ist die Konfiguration des LDAP-Servers. Sie müssen grundlegende DN-Informationen und Einträge für Konten Ihrer Software-Clients mit Passwörtern hinzufügen. Ausführliche Informationen zur LDAP-Konfiguration erhalten Sie unter [Kapitel 37, LDAP – Ein Verzeichnisdienst](#) (S. 735).

Eine manuelle Konfiguration ist nicht erforderlich. Sie können Skripts von `smbldap-tools` verwenden. Diese Skripts sind Teil des Pakets `samba-doc` und befinden sich nach der Installation des Pakets in `/usr/share/doc/packages/samba/examples/LDAP`.

ANMERKUNG: LDAP und Sicherheit

Der LDAP-Administrations-DN sollte ein anderes Konto als der Root-DN sein. Damit das Netzwerk sicherer wird, können Sie außerdem eine sichere Verbindung mit TLS nutzen.

38.7.2 Vorbereiten des Samba-Servers

Vor der Migration müssen Sie Ihren Samba-Server konfigurieren. Die Konfiguration der Freigaben `profile`, `netlogon` und `home` finden Sie auf der Registerkarte *Freigaben* des YaST-Moduls *Samba-Server*. Um den Standardwert zu ändern, wählen Sie die Freigabe aus und klicken Sie auf *Bearbeiten*.

Um die LDAP-Konfiguration für Ihren Samba-Server und die Berechtigungen des LDAP-Administrators hinzuzufügen, verwenden Sie die Registerkarte *LDAP-Einstellungen* des YaST-Moduls *Samba-Server*. Der LDAP-Administrations-DN (Kennung *Administrations-DN*) und das Passwort sind zum Hinzufügen oder Ändern von Konten im LDAP-Verzeichnis unbedingt erforderlich.

38.7.3 Migrieren der Windows-Profile

Führen Sie für jedes zu migrierende Profil folgende Schritte aus:

Prozedur 38.1 *Migrieren eines Profils*

- 1 Klicken Sie auf Ihrem NT4-Domänencontroller mit der rechten Maustaste auf *Arbeitsplatz* und wählen Sie *Eigenschaften*. Wählen Sie die Registerkarte *Benutzerprofile*.
- 2 Wählen Sie ein Benutzerprofil, das Sie migrieren möchten und klicken Sie darauf.
- 3 Klicken Sie auf *Kopieren nach*.
- 4 Unter *Profil kopieren nach* geben Sie den neuen Pfad ein, z. B. `c:\temp\profiles`.
- 5 Klicken Sie in *Zugelassen* auf *Ändern*.

- 6 Klicken Sie auf *Jeder*. Zum Schließen des Felds klicken Sie auf *OK*.
- 7 Zum abschließenden Speichern des Profils klicken Sie auf *OK*.
- 8 Kopieren Sie die gespeicherten Profile in die entsprechenden Profilverzeichnisse auf Ihrem Samba-Server.

38.7.4 Migrieren der Windows-Konten

Prozedur 38.2 Der Migrationsvorgang für Konten

- 1 Erstellen Sie ein BDC-Konto in der alten NT4-Domäne für den Samba-Server mit NT-Server-Manager. Samba muss nicht ausgeführt werden.

```
net rpc join -S NT4PDC -w DOMNAME -U Administrator%passwd net rpc vampire
-S NT4PDC -U administrator%passwd pbedit -L
```

- 2 Weisen Sie jede der UNIX-Gruppen den NT-Gruppen zu:

Beispiel 38.6 Beispiel-Skript initGroups.sh

```
#!/bin/bash ##### Keep this as a shell script for future re-use #
Known domain global groups net groupmap modify ntgroup="Domain
Admins"
unixgroup=root net groupmap modify ntgroup="Domain Users"
unixgroup=users net groupmap modify ntgroup="Domain Guests"
unixgroup=nobody # Our domain global groups net groupmap add
ntgroup="Operation" unixgroup=operation type=d net groupmap add
ntgroup="Shipping" unixgroup=shipping type=d
```

- 3 Überprüfen Sie, dass alle Gruppen erkannt werden:

```
net groupmap list
```

38.8 Weitere 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 Manualpages aufzurufen. Alternativ dazu finden Sie im Verzeichnis `/usr/`

`share/doc/packages/samba` weitere Online-Dokumentationen und Beispiele. Eine kommentierte Beispielkonfiguration (`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.

Verteilte Nutzung von Dateisystemen mit NFS

39

Wie bereits in [Kapitel 36, Arbeiten mit NIS](#) (S. 725) erwähnt, dient NFS neben NIS dazu, ein Netzwerk für den Benutzer transparent zu machen. Durch NFS lassen sich Dateisysteme im Netzwerk verteilen. Unabhängig davon, an welchem Terminal die Anwender angemeldet sind, finden sie 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).

WICHTIG: DNS-Bedarf

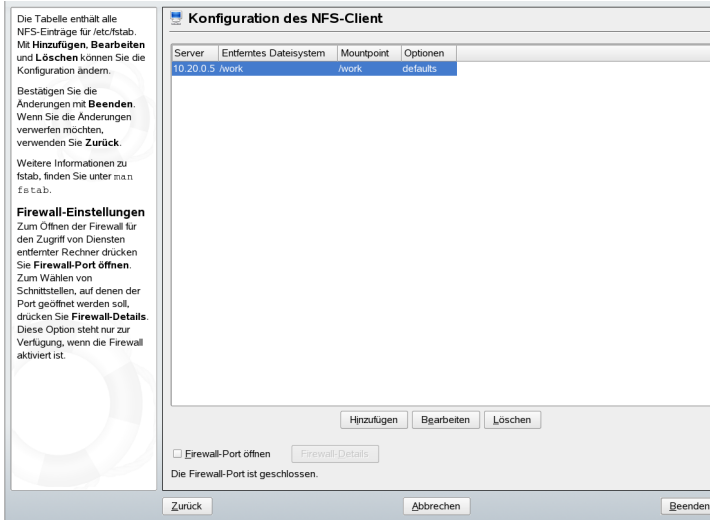
Im Prinzip können alle Exporte allein mit IP-Adressen vorgenommen werden. Es ist jedoch ratsam, über ein funktionierendes DNS-System zu verfügen, um Zeitüberschreitungen zu vermeiden. Dies ist zumindest für die Protokollierung erforderlich, weil der `moumntd`-Daemon Reverse-Lookups ausführt.

39.1 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 Einhängungspunkt an, an dem das Verzeichnis lokal eingehängt werden soll. Diese Eingaben werden im ersten Dialogfeld nach einem Klick auf *Hinzufügen*

eingetragen. Klicken Sie auf *Firewall-Port öffnen*, um die Firewall zu öffnen und entfernten Computern den Zugriff auf den Dienst zu gewähren. Der Status der Firewall wird neben dem Kontrollkästchen angezeigt. Mit einem Klick auf *OK* werden Ihre Änderungen gespeichert. Siehe [Abbildung 39.1](#), „Konfiguration des NFS-Clients mit YaST“ (S. 786).

Abbildung 39.1 Konfiguration des NFS-Clients mit YaST



39.2 Manuelles Importieren von Dateisystemen

Das manuelle Importieren von Dateisystemen von einem NFS-Server ist sehr einfach. Die einzige Voraussetzung ist, dass ein RPC-Portmapper läuft, der durch die Eingabe des Befehls `rpcportmap start` vom `root` gestartet werden kann. Sobald diese Voraussetzung erfüllt ist, können auf den entsprechenden Computer exportierte entfernte Dateisysteme analog zu lokalen Festplatten über den Befehl `einhängen` im Dateisystem eingehängt werden. Die Syntax ist wie folgt:

```
mount host:entfernter_pfadlokaler_pfad
```

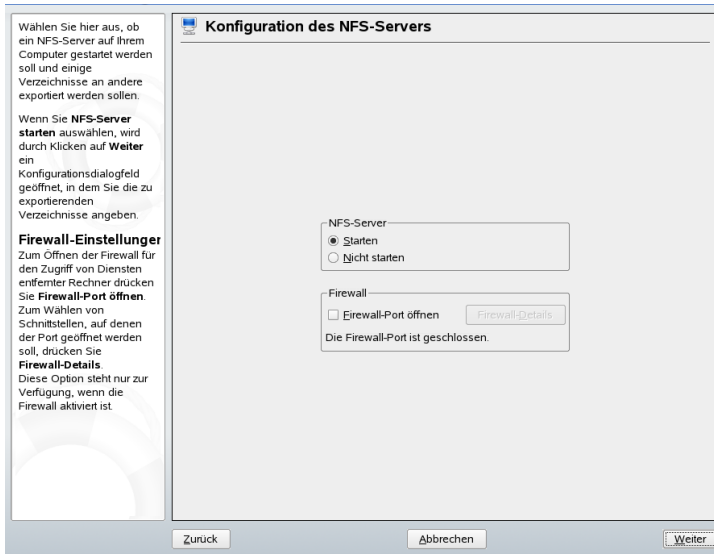
Wenn beispielsweise Benutzerverzeichnisse vom Rechner `sun` importiert werden sollen, lautet der Befehl:

mount sun:/home /home

39.3 Exportieren von Dateisystemen mit YaST

Mit YaST können Sie einen Rechner Ihres Netzwerks zu einem NFS-Server machen. 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 YaST zum Installieren eines solchen Servers und wählen Sie *Netzwerkdienste* → *NFS-Server*. Es erscheint ein Dialogfeld wie in [Abbildung 39.2](#), „*Konfiguration des NFS-Servers*“ (S. 787).

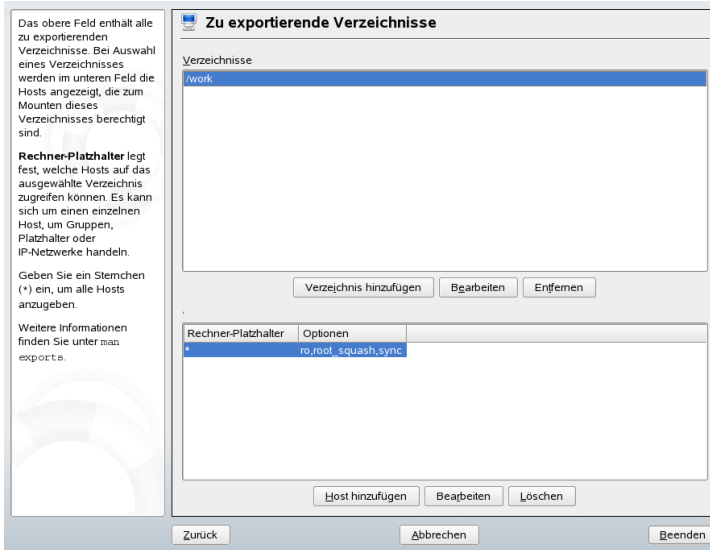
Abbildung 39.2 Konfiguration des NFS-Servers



Aktivieren Sie im nächsten Schritt *NFS-Server starten* und klicken Sie auf *Weiter*. Geben Sie im oberen Textfeld die zu exportierenden Verzeichnisse an. Legen Sie darunter Hosts fest, die darauf Zugriff erhalten sollen. Dieses Dialogfeld ist in [Abbildung 39.3](#), „*Konfigurieren eines NFS-Servers mit YaST*“ (S. 788) abgebildet. Für jeden Host können vier Optionen eingestellt werden: `single host`, `netgroups`,

wildcards und IP networks. Nähere Erklärungen zu diesen Optionen erhalten Sie durch Eingabe von `man exports`. *Beenden* schließt die Konfiguration ab.

Abbildung 39.3 Konfigurieren eines NFS-Servers mit YaST



WICHTIG: Automatische Firewall-Konfiguration

Wenn auf Ihrem System eine Firewall aktiviert ist (SuSEfirewall2), passt YaST deren Konfiguration für den NFS-Server an, indem der `nfs`-Dienst aktiviert wird, wenn *Firewall-Ports öffnen* ausgewählt ist.

39.4 Weitere Informationen

Informationen zum Konfigurieren eines NFS-Servers finden Sie in `/usr/share/doc/packages/nfs-utils/README` und den dort aufgeführten Dokumenten. Die ausführliche technische Dokumentation steht online unter <http://nfs.sourceforge.net/> zur Verfügung.

Dateisynchronisierung

Viele Menschen benutzen heutzutage mehrere Computer: einen Computer zu Hause, einen oder mehrere Computer am Arbeitsplatz und eventuell noch ein Notebook oder einen PDA für unterwegs. Viele Dateien werden auf allen diesen Computern benötigt. Da Sie mit allen Computern arbeiten und die Dateien ändern möchten, sollten alle Daten überall in aktueller Version zur Verfügung stehen.

40.1 Verfügbare Software zur Datensynchronisierung

Auf Computern, die ständig miteinander über ein schnelles Netzwerk in Verbindung stehen, ist die Datensynchronisierung kein Problem. In diesem Fall wählen Sie ein Netzwerkdateisystem, wie zum Beispiel NFS, und speichern die Dateien auf einem Server. Alle Rechner greifen dabei über das Netzwerk auf ein und dieselben Daten zu. Dieser Ansatz ist unmöglich, wenn die Netzverbindung schlecht oder teilweise gar nicht vorhanden ist. Wer mit einem Laptop unterwegs ist, ist darauf angewiesen, von allen benötigten Dateien Kopien auf der lokalen Festplatte zu haben. Wenn Dateien bearbeitet werden, stellt sich aber schnell das Problem der Synchronisierung. Wenn Sie eine Datei auf einem Computer ändern, stellen Sie sicher, dass die Kopie der Datei auf allen anderen Computern aktualisiert wird. Dies kann bei gelegentlichen Kopiervorgängen manuell mithilfe von `scp` oder `rsync` erledigt werden. Bei vielen Dateien wird das jedoch schnell aufwändig und erfordert hohe Aufmerksamkeit vom Benutzer, um Fehler, wie etwa das Überschreiben einer neuen mit einer alten Datei, zu vermeiden.

WARNUNG: Risiko des Datenverlusts

Bevor Sie Ihre Daten mit einem Synchronisierungssystem verwalten, sollten Sie mit dem verwendeten Programm vertraut sein und dessen Funktionalität testen. Für wichtige Dateien ist das Anlegen einer Sicherungskopie unerlässlich.

Zur Vermeidung der zeitraubenden und fehlerträchtigen manuellen Arbeit bei der Datensynchronisierung gibt es Programme, die diese Aufgabe mit verschiedenen Ansätzen automatisieren. Die folgenden Zusammenfassungen sollen dem Benutzer eine Vorstellung davon liefern, wie diese Programme funktionieren und genutzt werden können. Vor dem tatsächlichen Einsatz sollten Sie die Programmdokumentation sorgfältig lesen.

40.1.1 Unison

Unison ist kein Netzwerkdateisystem. Die Dateien werden einfach lokal gespeichert und bearbeitet. Das Programm Unison kann manuell aufgerufen werden, um Dateien zu synchronisieren. Bei der ersten Synchronisierung wird auf den beteiligten beiden Hosts eine Datenbank angelegt, in der Prüfsummen, Zeitstempel und Berechtigungen der ausgewählten Dateien gespeichert sind. Beim nächsten Aufruf kann Unison erkennen, welche Dateien geändert wurden und die Übertragung vom oder zum anderen Host vorschlagen. Für gewöhnlich können Sie alle Vorschläge annehmen.

40.1.2 CVS

CVS, das meistens zur Versionsverwaltung von Quelltexten von Programmen benutzt wird, bietet die Möglichkeit, Kopien der Dateien auf mehreren Computern zu führen. Damit eignet es sich auch für die Datensynchronisierung. CVS führt ein zentrales Repository auf dem Server, das nicht nur die Dateien, sondern auch die Änderungen an ihnen speichert. Lokal erfolgte Änderungen werden an das Repository übermittelt und können von anderen Computern durch ein Update abgerufen werden. Beide Prozeduren müssen vom Benutzer initiiert werden.

Dabei ist CVS bei gleichzeitigen Änderungen einer Datei auf mehreren Computern sehr fehlertolerant. Die Änderungen werden zusammengeführt und nur, wenn in gleichen Zeilen Änderungen stattfanden, gibt es einen Konflikt. Die Datenbank bleibt im Kon-

fliktfall in einem konsistenten Zustand. Der Konflikt ist nur am Client-Host sichtbar und muss dort gelöst werden.

40.1.3 Subversion

Im Gegensatz zu CVS, das sich im Laufe der Zeit „entwickelt“ hat, ist Subversion ein durchgängig konzipiertes Projekt. Subversion wurde als technisch verbesserter Nachfolger von CVS entwickelt.

Subversion wurde gegenüber seinem Vorgänger in vielen Bereichen deutlich verbessert. CVS verwaltet aufgrund seiner Geschichte nur Dateien und "weiß" nichts von Verzeichnissen. In Subversion dagegen besitzen auch Verzeichnisse eine Versions-History und können wie Dateien kopiert und umbenannt werden. Des Weiteren können jeder Datei und jedem Verzeichnis Metadaten hinzugefügt werden. Diese Metadaten können ebenfalls der Versionsverwaltung unterliegen. Im Gegensatz zu CVS bietet Subversion transparenten Netzwerkzugriff über einige Protokolle, wie zum Beispiel WebDAV (Web-based Distributed Authoring and Versioning). WebDAV erweitert das HTTP-Protokoll für verteiltes Arbeiten an Dateien auf entfernten Webservern.

Subversion wurde weitgehend auf der Grundlage von existierenden Programmpaketen zusammengestellt. Daher wird zum Einsatz von Subversion immer auch der Webserver Apache mit der Erweiterung WebDAV verwendet.

40.1.4 mailsync

Im Unterschied zu den bisher erwähnten Synchronisierungswerkzeugen dient mailsync einzig und allein der Synchronisierung von E-Mails zwischen verschiedenen Mailboxen. Es kann sich sowohl um lokale Mailbox-Dateien als auch um Mailboxen handeln, die auf einem IMAP-Server untergebracht sind.

Dabei wird für jede Nachricht aufgrund der im E-Mail-Header enthaltenen Message-ID einzeln entschieden, ob sie synchronisiert bzw. gelöscht werden muss. Synchronisierung ist sowohl zwischen einzelnen Mailboxen als auch zwischen Hierarchien von Mailboxen möglich.

40.1.5 rsync

Wenn Sie keine Versionskontrolle benötigen, aber große Dateistrukturen über langsame Netzwerkverbindungen synchronisieren möchten, bietet das Tool rsync ausgefeilte Mechanismen an, um ausschließlich Änderungen an Dateien zu übertragen. Dies betrifft nicht nur Textdateien sondern auch binäre Dateien. Um die Unterschiede zwischen Dateien zu erkennen, teilt rsync die Dateien in Blöcke auf und berechnet Prüfsummen zu diesen Blöcken.

Der Aufwand beim Erkennen der Änderungen hat seinen Preis. Für den Einsatz von rsync sollten die Computer, die synchronisiert werden sollen, großzügig dimensioniert sein. RAM ist besonders wichtig.

40.1.6 Novell iFolder

Mit Novell iFolder können Sie jederzeit von überall auf Ihre Dateien zugreifen. Wenn Sie Ihre Dateien in Ihrem iFolder-Verzeichnis ablegen, wird dieses sofort auf dem Server synchronisiert. Mit dieser Methode können Sie überall arbeiten.

Novell iFolder erlaubt Ihnen auch, offline zu arbeiten. Das ist praktisch, wenn Sie z. B. bei der Arbeit an einem Notebook unterwegs keine Internet-Verbindung haben. Nach einer erfolgreichen Verbindung mit dem Internet werden die Änderungen an Ihrer Arbeit an den Server übertragen.

Das Arbeiten mit iFolder umfasst die folgenden Schritte:

1. Melden Sie sich an, bevor Sie mit iFolder arbeiten.
2. Ändern Sie Ihre Einstellungen für die gewünschte Häufigkeit der Synchronisierung.
3. Synchronisieren Sie Ihre Dateien und beobachten Sie die Aktivität zwischen Ihrem Client und dem iFolder-Server.
4. Lösen Sie alle etwaigen Konflikte, die bei der Synchronisierung auftreten. Konflikte treten auf, wenn Sie dieselbe Datei auf zwei verschiedenen Computern ändern. iFolder speichert Konfliktdateien in einem separaten Verzeichnis, um Datenverlust zu vermeiden.

Weitere Informationen zu iFolder erhalten Sie unter <http://www.novell.com/en-en/documentation/>. Tipps und Tricks zu iFolder siehe unter <http://www.novell.com/cool solutions/ifmag/>.

40.2 Kriterien für die Auswahl eines Programms

Bei der Entscheidung für ein Programm müssen einige wichtige Kriterien berücksichtigt werden.

40.2.1 Client-Server oder Peer-to-Peer

Zur Verteilung von Daten sind zwei verschiedene Modelle verbreitet. Im ersten Modell gleichen alle Clients ihre Dateien mit einem zentralen Server ab. Der Server muss zumindest zeitweise von allen Clients erreichbar sein. Dieses Modell wird von Subversion, CVS und WebDAV verwendet.

Die andere Möglichkeit ist, dass alle Hosts gleichberechtigt (als Peers) vernetzt sind und ihre Daten gegenseitig abgleichen. Diesen Ansatz verfolgt Unison. rsync arbeitet eigentlich im Client-Modus, jedoch kann jeder Client auch als Server fungieren.

40.2.2 Portabilität

Subversion, CVS und Unison sind auch für viele andere Betriebssysteme, wie verschiedene Unix- und Windows-Systeme, erhältlich.

40.2.3 Interaktiv oder automatisch

In Subversion, CVS, WebDAV und Unison startet der Benutzer die Datensynchronisierung manuell. Dies erlaubt die genaue Kontrolle über die abzugleichenden Dateien und einen einfachen Umgang mit Konflikten. Andererseits können sich durch zu lange Synchronisierungsintervalle die Chancen für Konflikte erhöhen.

40.2.4 Konflikte: Auftreten und Lösung

Konflikte treten bei Subversion oder CVS nur selten auf, selbst wenn mehrere Leute an einem umfangreichen Programmprojekt arbeiten. Das liegt daran, dass die Dokumente zeilenweise zusammengeführt werden. Wenn ein Konflikt auftritt, ist davon immer nur ein Client betroffen. In der Regel lassen sich Konflikte in Subversion oder CVS einfach lösen.

Unison meldet Konflikte und Sie können dann die betroffenen Dateien einfach von der Synchronisierung ausschließen. Jedoch lassen sich Änderungen nicht so einfach zusammenführen wie bei Subversion oder CVS.

Während in Subversion oder CVS im Konfliktfall Änderungen auch teilweise übernommen werden können, wird bei WebDAV ein Checkin nur dann vollzogen, wenn die gesamte Änderung erfolgreich ist.

In rsync gibt es keine Konfliktbehandlung. Der Benutzer muss selbst darauf achten, dass er nicht versehentlich Dateien überschreibt, und alle etwaigen Konflikte manuell lösen. Zur Sicherheit können Sie zusätzlich ein Versionierungssystem, wie RCS, verwenden.

40.2.5 Auswählen und Hinzufügen von Dateien

In seiner Standardkonfiguration synchronisiert Unison eine ganze Verzeichnisstruktur. Neue Dateien in der Struktur werden automatisch in die Synchronisierung einbezogen.

Bei Subversion oder CVS müssen neue Verzeichnisse und Dateien explizit über den Befehl `svn add` bzw. `cvs add` hinzugefügt werden. Daraus resultiert eine genauere Kontrolle über die zu synchronisierenden Dateien. Andererseits werden neue Dateien häufig übersehen, vor allem, wenn aufgrund einer großen Anzahl von Dateien die Fragezeichen in der Ausgabe von `svn update` und `svn status` oder `cvs update` ignoriert werden.

40.2.6 History

Subversion und CVS bieten eine Rekonstruktion alter Dateiversionen als zusätzliche Funktion. Bei jeder Änderung kann ein kurzer Bearbeitungsvermerk hinzugefügt werden. Damit lässt sich später die Entwicklung der Dateien aufgrund des Inhalts und der Vermerke gut nachvollziehen. Für Diplomarbeiten und Programmtexte ist dies eine wertvolle Hilfe.

40.2.7 Datenmenge und Speicherbedarf

Auf jedem der beteiligten Computer ist für alle verteilten Daten genügend Speicherplatz auf der Festplatte erforderlich. Bei Subversion bzw. CVS fällt zusätzlich der Platzbedarf für die Repository-Datenbank auf dem Server an. Da auf dem Server auch die Datei-History gespeichert wird, ist dort deutlich mehr Speicherplatz nötig. Bei Dateien im Textformat müssen nur geänderte Zeilen neu gespeichert werden. Bei binären Dateien wächst hingegen der Platzbedarf bei jeder Änderung um die Größe der Datei.

40.2.8 GUI

Unison bietet eine grafische Bedienoberfläche (GUI), die anzeigt, welche Synchronisierungsvorgänge Unison ausführen möchte. Nehmen Sie den Vorschlag an oder schließen Sie einzelne Dateien aus der Synchronisierung aus. Im Textmodus bestätigen Sie die einzelnen Vorgänge interaktiv.

Erfahrene Benutzer führen Subversion bzw. CVS gewöhnlich über die Kommandozeile aus. Es gibt jedoch grafische Bedienoberflächen für Linux (z. B. cervisia) und für andere Betriebssysteme (z. B. wincvs). Viele Entwicklungswerkzeuge (z. B. kdevelop) und Texteditoren (z. B. emacs) unterstützen CVS oder Subversion. Die Behebung von Konflikten wird mit diesen Frontends oft sehr vereinfacht.

40.2.9 Benutzerfreundlichkeit

Unison und rsync sind ziemlich einfach zu benutzen und bieten sich auch für Anfänger an. CVS und Subversion sind etwas schwieriger zu bedienen. Benutzer sollten zu deren Verwendung das Zusammenspiel zwischen Repository und lokalen Daten verstehen. Änderungen der Daten sollten zunächst immer lokal mit dem Repository zusam-

mengeführt werden. Dies erfolgt gewöhnlich mit dem Befehl `cv`s `update` bzw. `svn update`. Anschließend müssen die Daten über den Befehl `cv`s `commit` bzw. `svn commit` wieder in das Repository zurückgeschickt werden. Wenn dieser Vorgang verstanden wurde, ist CVS bzw. Subversion auch für Anfänger leicht zu benutzen.

40.2.10 Sicherheit vor Angriffen

Idealerweise sollten die Daten bei der Übertragung vor Abhören oder Änderungen geschützt sein. Unison, CVS, rsync und Subversion lassen sich einfach über SSH (Secure Shell) benutzen und sind dann gut gegen derartige Angriffe gesichert. Es sollte vermieden werden, CVS oder Unison über rsh (Remote Shell) einzusetzen. Zugriffe auf CVS mit dem Mechanismus *pserver* sind in ungeschützten Netzwerken ebenfalls nicht empfehlenswert. Subversion stellt bereits durch die Verwendung von Apache die benötigten Sicherheitsmechanismen zur Verfügung.

40.2.11 Schutz vor Datenverlust

CVS wird schon sehr lange von vielen Entwicklern zur Verwaltung ihrer Programmprojekte benutzt und ist äußerst stabil. Durch das Speichern der Entwicklungsgeschichte bietet CVS sogar Schutz vor bestimmten Benutzerfehlern, wie irrtümliches Löschen einer Datei. Obwohl Subversion im Vergleich zu CVS noch nicht sehr weit verbreitet ist, wird es bereits im produktiven Einsatz verwendet (z. B. vom Subversion-Projekt selbst).

Unison ist noch relativ neu, weist aber eine hohe Stabilität auf. Es ist jedoch empfindlicher gegen Benutzerfehler. Wenn die Synchronisierung eines Löschvorgangs bei einer Datei einmal bestätigt wurde, ist die Datei nicht mehr zu retten.

Tabelle 40.1 Funktionen der Werkzeuge zur Datensynchronisierung: -- = sehr schlecht, - = schlecht bzw. nicht verfügbar, o = mittelmäßig, + = gut, ++ = ausgezeichnet, x = verfügbar

	Unison	CVS/SVN	rsync	mailsync
Client/Server	gleich	C-S/C-S	C-S	gleich
Portabilität	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x,Win	Lin,Un*x

	Unison	CVS/SVN	rsync	mailsync
Interaktivität	x	x/x	x	-
Geschwindigkeit	-	o/+	+	+
Konflikte	o	++/++	o	+
Dateiauswahl	Verz.	Ausw./Datei, Verz.	Verz.	Mailbox
History	-	x/x	-	-
Speicherbedarf	o	--	o	+
GUI	+	o/o	-	-
Schwierigkeit	+	o/o	+	o
Angriffe	+(ssh)	+/(ssh)	+(ssh)	+(SSL)
Datenverlust	+	++/++	+	+

40.3 Einführung in Unison

Unison eignet sich hervorragend für Synchronisierung und Transfer ganzer Verzeichnisstrukturen. Die Synchronisierung erfolgt in beide Richtungen und lässt sich intuitiv über eine grafische Oberfläche steuern. Eine Konsolenversion kann ebenfalls verwendet werden. Die Synchronisierung lässt sich auch automatisieren, damit keine Interaktion mit dem Benutzer anfällt. Dazu ist jedoch einige Erfahrung nötig.

40.3.1 Voraussetzungen

Unison muss sowohl auf dem Client als auch auf dem Server installiert sein. Hier ist mit *Server* ein zweiter, entfernter Host gemeint (im Unterschied zu CVS, siehe [Abschnitt 40.1.2](#), „CVS“ (S. 790)).

Im folgenden Abschnitt wird Unison zusammen mit ssh verwendet. In diesem Fall muss ein SSH-Client auf dem Client und ein SSH-Server auf dem Server installiert sein.

40.3.2 Verwendung von Unison

Das Grundprinzip bei Unison ist, zwei Verzeichnisse (so genannte *roots*) aneinander zu binden. Diese Bindung ist symbolisch – es handelt sich nicht um eine Online-Verbindung. In diesem Beispiel ist das Verzeichnis-Layout wie folgt:

Client:	/home/tux/dir1
Server:	/home/geeko/dir2

Diese beiden Verzeichnisse sollen synchronisiert werden. Auf dem Client ist der Benutzer als tux bekannt, auf dem Server dagegen als geeko. Als Erstes soll getestet werden, ob die Kommunikation zwischen Client und Server funktioniert:

```
unison -testserver /home/tux/dir1 ssh://geeko@server//homes/geeko/dir2
```

Die häufigsten Probleme, die hierbei auftreten können:

- Die auf dem Client und Server eingesetzten Versionen von Unison sind nicht kompatibel.
- Der Server lässt keine SSH-Verbindung zu.
- Keiner der angegebenen beiden Pfade existiert.

Wenn alles funktioniert, lassen Sie die Option `-testserver` weg. Bei der ersten Synchronisierung kennt Unison die Beziehung zwischen den beiden Verzeichnissen noch nicht und macht von daher Vorschläge für die Übertragungsrichtung der einzelnen Dateien und Verzeichnisse. Die Pfeile in der Spalte *Action* geben die Übertragungsrichtung an. Ein Fragezeichen bedeutet, dass Unison keinen Vorschlag zur Übertragungsrichtung machen kann, da beide Versionen in der Zwischenzeit geändert wurden bzw. neu sind.

Mit den Pfeiltasten können Sie die Übertragungsrichtung für jeden Eintrag einstellen. Stimmen die Übertragungsrichtungen für alle angezeigten Einträge, dann klicken Sie einfach auf *Go*.

Das Verhalten von Unison (z. B., ob in eindeutigen Fällen die Synchronisierung automatisch durchgeführt werden soll) lässt sich beim Programmstart mithilfe von Kommandozeilenparametern steuern. Eine komplette Liste aller Parameter liefert `unison --help`.

Beispiel 40.1 *Die Datei `~/unison/example.prefs`*

```
root=/home/tux/dir1
root=ssh://wilber@server//homes/wilber/dir2
batch=true
```

Für jede Bindung wird im Benutzerverzeichnis `~/unison` ein Synchronisierungsprotokoll geführt. Konfigurationssets, wie `~/unison/example.prefs`, können ebenfalls in diesem Verzeichnis gespeichert werden. Um die Synchronisierung zu starten, geben Sie diese Datei als Kommandozeilenparameter an, wie in `unison example.prefs`.

40.3.3 Weitere Informationen

Die offizielle Dokumentation zu Unison ist äußerst nützlich. Daher gibt dieser Abschnitt nur eine kurze Einführung. Das vollständige Handbuch steht unter <http://www.cis.upenn.edu/~bcpierce/unison/> und mit dem SUSE-Paket `unison` zur Verfügung.

40.4 Einführung in CVS

CVS bietet sich zur Synchronisierung an, wenn einzelne Dateien häufig bearbeitet werden und in einem Dateiformat vorliegen, wie ASCII-Text oder Programm Quelltext. Die Verwendung von CVS für die Synchronisierung von Daten in anderen Formaten, wie z. B. JPEG-Dateien, ist zwar möglich, führt aber schnell zu großen Datenmengen, da jede Variante einer Datei dauerhaft auf dem CVS-Server gespeichert wird. Zudem bleiben in solchen Fällen die meisten Möglichkeiten von CVS ungenutzt. Die Verwendung von CVS zur Dateisynchronisierung ist nur möglich, wenn alle Arbeitsstationen auf denselben Server zugreifen können.

40.4.1 Konfigurieren eines CVS-Servers

Der *Server* ist der Ort, an dem sich alle gültigen Dateien befinden, einschließlich der neuesten Version jeder Datei. Jede stationäre Arbeitsstation kann als Server benutzt werden. Wünschenswert ist, dass die Daten des CVS-Repository in regelmäßige Backups einbezogen werden.

Beim Konfigurieren eines CVS-Servers ist es sinnvoll, Benutzern über SSH Zugang zum Server zu gestatten. Ist auf diesem Server der Benutzer als `tux` bekannt und sowohl auf dem Server als auch auf dem Client die CVS-Software installiert, müssen auf der Client-Seite die folgenden Umgebungsvariablen gesetzt sein:

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

Mit dem Befehl `cvs init` lässt sich der CVS-Server von der Client-Seite aus initialisieren. Das ist nur einmal erforderlich.

Abschließend muss ein Name für die Synchronisierung festgelegt werden. Wählen oder erzeugen Sie auf dem Client ein Verzeichnis, das ausschließlich Dateien enthält, die von CVS verwaltet werden sollen (es darf auch leer sein). Der Name des Verzeichnisses ist auch der Name der Synchronisierung. In diesem Beispiel wird das Verzeichnis `synchome` genannt. Wechseln Sie in dieses Verzeichnis. Um den Synchronisationsnamen auf `synchome` zu setzen, geben Sie Folgendes ein:

```
cvs import synchome tux wilber
```

Viele Befehle von CVS erfordern einen Kommentar. Zu diesem Zweck startet CVS einen Editor (den in der Umgebungsvariable `$EDITOR` definierten, ansonsten `vi`). Den Aufruf des Editors können Sie umgehen, indem Sie den Kommentar bereits in der Kommandozeile eingeben, wie in folgendem Beispiel:

```
cvs import -m 'Das ist ein Test' synchome tux wilber
```

40.4.2 Verwenden von CSV

Das Synchronisierungsrepository kann jetzt mit `cvs co synchome` von allen Hosts gespeichert ("ausgecheckt") werden. Dadurch wird auf dem Client das neue Unterverzeichnis `synchome` angelegt. Um Ihre Änderungen an den Server zu übermitteln, wechseln Sie in das Verzeichnis `synchome` (oder eines seiner Unterverzeichnisse) und geben Sie `cvs commit` ein.

Standardmäßig werden alle Dateien (einschließlich Unterverzeichnisse) an den Server übermittelt. Um nur einzelne Dateien oder Verzeichnisse zu übermitteln, geben Sie diese folgendermaßen an: `cvs commit datei1 verzeichnis1`. Neue Dateien und Verzeichnisse müssen dem Repository mit einem Befehl, wie `cvs add datei1 verzeichnis1`, hinzugefügt werden, bevor sie an den Server übermittelt werden. Übermitteln Sie anschließend die neu hinzugefügten Dateien und Verzeichnisse mit `cvs commit datei1 verzeichnis1`.

Wenn Sie zu einer anderen Arbeitsstation wechseln, speichern Sie das Synchronisierungsrepository, falls dies nicht in einer früheren Sitzung an derselben Arbeitsstation erfolgt ist (siehe oben).

Starten Sie die Synchronisierung mit dem Server über `cvs update`. Aktualisieren Sie einzelne Dateien oder Verzeichnisse, wie in `cvs update datei1 verzeichnis1`. Den Unterschied zwischen den aktuellen Dateien und den auf dem Server gespeicherten Versionen sehen Sie mithilfe des Befehls `cvs diff` oder `cvs diff datei1 verzeichnis1`. Verwenden Sie `cvs -nq update`, um zu sehen, welche Dateien von einer Aktualisierung betroffen sind.

Hier sind einige der Statussymbole, die während einer Aktualisierung angezeigt werden:

U

Die lokale Version wurde aktualisiert. Dies betrifft alle Dateien, die vom Server bereitgestellt werden und auf dem lokalen System fehlen.

M

Die lokale Version wurde geändert. Falls Änderungen am Server erfolgt sind, war es möglich, die Unterschiede mit der lokalen Kopie zusammenzuführen.

P

Die lokale Version wurde durch einen Patch der Server-Version aktualisiert.

C

Die lokale Datei hat einen Konflikt mit der aktuellen Version im Repository.

?

Die Datei existiert nicht in CVS.

Der Status M kennzeichnet eine lokal geänderte Datei. Entweder übermitteln Sie die lokale Kopie an den Server oder Sie entfernen die lokale Datei und führen die Aktualisierung erneut durch. In diesem Fall wird die fehlende Datei vom Server

abgerufen. Wenn von verschiedenen Benutzern die gleiche Datei in derselben Zeile editiert und dann übermittelt wurde, entsteht ein Konflikt, der mit `C` gekennzeichnet wird.

Beachten Sie in diesem Fall die Konfliktmarkierungen (`>>`) und (`<<`) in der Datei und entscheiden Sie sich für eine der beiden Versionen. Da dies eine ziemlich unangenehme Aufgabe sein kann, könnten Sie sich entscheiden, Ihre Änderungen zu verwerfen, die lokale Datei zu löschen und dann mit der Eingabe `cvsv up` die aktuelle Version vom Server abzurufen.

40.4.3 Weitere Informationen

Dieser Abschnitt gibt nur eine kurze Einführung in die vielen Möglichkeiten von CVS. Ausführliche Dokumentation steht unter den folgenden URLs zur Verfügung:

<http://www.cvshome.org/>
<http://www.gnu.org/manual/>

40.5 Einführung in Subversion

Subversion ist ein freies Open Source-System zur Versionskontrolle und wird häufig als Nachfolger von CVS betrachtet, d. h. bereits vorgestellte Eigenschaften von CVS treffen auch zum großen Teil auf Subversion zu. Es bietet sich vor allem an, wenn Sie die Vorteile von CVS genießen möchten, ohne dessen Nachteile in Kauf nehmen zu müssen. Viele dieser Eigenschaften wurden bereits ansatzweise in [Abschnitt 40.1.3](#), „Subversion“ (S. 791) erwähnt.

40.5.1 Installieren eines Subversion-Servers

Die Installation einer Repository-Datenbank auf einem Server ist eine relativ einfache Prozedur. Subversion bietet dafür ein einfaches Administrationswerkzeug. Geben Sie zum Anlegen eines neuen Repositories den folgenden Befehl ein:

```
svnadmin create /path/to/repository
```

Weitere Optionen erhalten Sie mit `svnadmin help`. Im Unterschied zu CVS verwendet Subversion nicht RCS als Basis, sondern andere Arten von Repository. Für gewöhnlich wird die Berkeley-Datenbank oder FSFS (ein Repository, welches das Dateisystem

direkt verwendet) verwendet. Legen Sie ein Repository nicht auf entfernten Dateisystemen, wie NFS, AFS oder Windows SMB, an. Die Datenbank benötigt POSIX-Sperremechanismen, die diese Dateisysteme nicht unterstützen.

Der Befehl `svnlook` bietet Informationen zu einem bestehenden Repository.

```
svnlook info /path/to/repository
```

Ein Server muss konfiguriert werden, um verschiedenen Benutzern den Zugriff auf das Repository zu erlauben. Verwenden Sie dafür entweder den Apache-Webserver mit WebDAV oder `svnserve`, der Server, der mit Subversion geliefert wird. Sobald `svnserve` eingerichtet ist und läuft, kann über eine URL mit `svn://` oder `svn+ssh://` auf das Repository zugegriffen werden. Benutzer, die sich beim Aufruf von `svn` authentifizieren sollten, können in `/etc/svnserve.conf` eingerichtet werden.

Die Entscheidung für Apache oder `svnserve` hängt von vielen Faktoren ab. Sie sollten das Subversion-Handbuch studieren. Weitere Informationen dazu finden Sie in [Abschnitt 40.5.3, „Weitere Informationen“](#) (S. 805).

40.5.2 Benutzung und Betrieb

Verwenden Sie den Befehl `svn` (ähnlich wie `cvs`) für den Zugriff auf ein Subversion-Repository. Mit `svn help` erhalten Sie die Beschreibung von Befehlsparametern:

```
checkout (co): Speichern einer Arbeitskopie aus einem Repository auf dem Client.  
Syntax: checkout URL[@REV]... [PATH]
```

Sofern angegeben, bestimmt `REV`, in welcher Revision die URL zuerst nachgeschlagen wird.

Wenn `PATH` weggelassen wird, wird der URL-Basisname als Ziel verwendet. Wenn mehrere URLs angegeben sind, werden Sie einzeln in ein Unterverzeichnis von `PATH` ausgecheckt, wobei der Name des Unterverzeichnisses der URL-Basisname ist.

...

Auf den Inhalt, den ein korrekt konfigurierter Server mit einem entsprechenden Repository liefert, kann jeder Client mit einem der folgenden Befehle zugreifen:

```
svn list http://svn.example.com/path/to/project
```

Oder:

```
svn list svn://svn.example.com/path/to/project
```

Speichern Sie ein bestehendes Projekt im aktuellen Verzeichnis mit dem Befehl

`svn checkout:`

```
svn checkout http://svn.example.com/path/to/project nameofproject
```

Dadurch wird auf dem Client das neue Unterverzeichnis `nameofproject` angelegt. Anschließend können Operationen (Hinzufügen, Kopieren, Umbenennen, Löschen) daran ausgeführt werden:

```
svn add file
svn copy oldfile newfile
svn move oldfile newfile
svn delete file
```

Diese Befehle können auch auf Verzeichnisse angewendet werden. Subversion kann zusätzlich Eigenschaften einer Datei oder eines Verzeichnisses aufzeichnen:

```
svn propset license GPL foo.txt
```

Das vorangehende Beispiel setzt den Wert `GPL` für die Eigenschaft `license`. Zeigen Sie Eigenschaften an mit `svn proplist`:

```
svn proplist --verbose foo.txt
Properties on 'foo.txt':
license : GPL
```

Speichern Sie die Änderungen mit `svn commit` auf dem Server. Ein anderer Benutzer kann Ihre Änderungen in sein Arbeitsverzeichnis übernehmen, indem er mithilfe von `svn update` eine Synchronisierung mit dem Server ausführt.

Im Unterschied zu CVS kann der Status eines Arbeitsverzeichnisses in Subversion *ohne* Zugriff auf das Repository über den Befehl `svn status` angezeigt werden. Lokale Änderungen werden in fünf Spalten angezeigt. Die erste Spalte ist dabei die wichtigste:

''

Keine Änderungen.

'A'

Objekt ist zum Hinzufügen markiert.

'D'

Objekt ist zum Löschen markiert.

'M'

Objekt wurde geändert.

'C'

Objekt ist in einem Konflikt.

'I'

Objekt wurde ignoriert.

'?'

Objekt unterliegt nicht der Versionskontrolle.

'!'

Objekt wird vermisst. Diese Markierung erscheint, wenn das Objekt ohne den Befehl `svn` gelöscht oder verschoben wurde.

'~'

Objekt wurde als Datei verwaltet, wurde jedoch mittlerweile durch ein Verzeichnis ersetzt, oder umgekehrt.

Die zweite Spalte zeigt den Status der Eigenschaften. Die Bedeutung aller übrigen Spalten kann im Subversion-Handbuch nachgeschlagen werden.

40.5.3 Weitere Informationen

Erste Quelle ist die Homepage von Subversion unter <http://subversion.tigris.org/>. Ein sehr empfehlenswertes, komplett englischsprachiges Buch finden Sie nach der Installation des Pakets `subversion-doc` im Verzeichnis `file:///usr/share/doc/packages/subversion/html/book.html`. Es ist auch unter <http://svnbook.red-bean.com/svnbook/index.html> verfügbar.

40.6 Einführung in rsync

`rsync` bietet sich immer dann an, wenn große Datenmengen, die sich nicht wesentlich ändern, regelmäßig übertragen werden müssen. Dies ist z. B. bei der Erstellung von Sicherungskopien häufig der Fall. Ein weiteres Einsatzgebiet sind so genannte Staging-Server. Dabei handelt es sich um Server, auf denen komplette Verzeichnisstrukturen von Webservern gespeichert werden, die regelmäßig auf den eigentlichen Webserver in einer "DMZ" gespiegelt werden.

40.6.1 Konfiguration und Betrieb

rsync lässt sich in zwei verschiedenen Modi benutzen. Zum einen kann rsync zum Archivieren oder Kopieren von Daten verwendet werden. Dazu ist auf dem Zielsystem nur eine Remote-Shell, wie z. B. SSH, erforderlich. Jedoch kann rsync auch als Daemon verwendet werden und Verzeichnisse im Netz zur Verfügung stellen.

Die grundlegende Verwendung von rsync erfordert keine besondere Konfiguration. Mit rsync ist es direkt möglich, komplette Verzeichnisse auf ein anderes System zu spiegeln. Beispielsweise kann mit folgendem Befehl ein Backup des Home-Verzeichnisses von "tux" auf einem Backupserver "sun" angelegt werden:

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

Mit dem folgenden Befehl wird das Verzeichnis zurückgespielt:

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

Bis hierher unterscheidet sich die Benutzung kaum von einem normalen Kopierprogramm, wie scp.

Damit rsync seine Funktionen voll ausnutzen kann, sollte das Programm im „rsync“-Modus betrieben werden. Dazu wird auf einem der Systeme der Daemon rsyncd gestartet. Konfigurieren Sie rsync in der Datei `/etc/rsyncd.conf`. Wenn beispielsweise das Verzeichnis `/srv/ftp` über rsync zugänglich sein soll, verwenden Sie die folgende Konfiguration:

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log
```

```
[FTP]
    path = /srv/ftp
    comment = An Example
```

Starten Sie dann rsyncd mit `rcrsyncd start`. rsyncd kann auch automatisch beim Bootvorgang gestartet werden. Hierzu muss entweder dieser Dienst in YaST im Runlevel-Editor aktiviert oder manuell der Befehl `insserv rsyncd` eingegeben werden. Alternativ kann rsyncd auch von xinetd gestartet werden. Dies empfiehlt sich aber nur bei Servern, auf denen rsyncd nicht allzu oft verwendet wird.

Im obigen Beispiel wird auch eine Protokolldatei über alle Verbindungen angelegt. Diese Datei wird unter `/var/log/rsyncd.log` abgelegt.

Dann kann die Übertragung von einem Clientsystem aus getestet werden. Das geschieht mit folgendem Befehl:

```
rsync -avz sun::FTP
```

Dieser Befehl listet alle Dateien auf, die auf dem Server im Verzeichnis `/srv/ftp` liegen. Diese Anfrage wird auch in der Protokolldatei unter `/var/log/rsyncd.log` aufgezeichnet. Um die Übertragung tatsächlich zu starten, geben Sie ein Zielverzeichnis an. Verwenden Sie `.` für das aktuelle Verzeichnis. Beispiel:

```
rsync -avz sun::FTP .
```

Standardmäßig werden bei der Synchronisierung mit `rsync` keine Dateien gelöscht. Wenn dies erzwungen werden soll, muss zusätzlich die Option `--delete` angegeben werden. Um sicherzustellen, dass keine neueren Dateien überschrieben werden, kann stattdessen die Option `--update` angegeben werden. Dadurch entstehende Konflikte müssen manuell aufgelöst werden.

40.6.2 Weitere Informationen

Wichtige Informationen zu `rsync` finden Sie in den Manualpages `man rsync` und `man rsyncd.conf`. Eine technische Dokumentation zur Vorgehensweise von `rsync` finden Sie unter `/usr/share/doc/packages/rsync/tech_report.ps`. Aktuelles zu `rsync` finden Sie auf der Projekt-Website unter <http://rsync.samba.org/>.

40.7 Einführung in mailsync

`mailsync` eignet sich vor allem für die folgenden drei Aufgaben:

- Synchronisierung von lokal gespeicherten E-Mails mit E-Mails, die auf einem Server gespeichert sind
- Migration von Mailboxen in ein anderes Format bzw. auf einen anderen Server
- Integritätsprüfung einer Mailbox bzw. Suche nach Duplikaten

40.7.1 Konfiguration und Verwendung

mailsync unterscheidet zwischen der Mailbox an sich (einem so genannten *Store*) und der Verknüpfung zwischen zwei Mailboxen (einem so genannten *Channel*). Die Definitionen der Stores und Channels sind in der `~/ .mailsync` abgelegt. Die folgenden Abschnitte geben einige Beispiele für Stores.

Eine einfache Definition kann wie folgt aussehen:

```
store saved-messages {
    pat Mail/saved-messages
    prefix Mail/
}
```

`Mail/` ist ein Unterverzeichnis im Home-Verzeichnis des Benutzers, das Ordner mit E-Mails enthält, unter anderem den Ordner `saved-messages`. Wird nun mailsync mit dem Befehl `mailsync -m saved-messages` gestartet, wird ein Index aller Nachrichten in `saved-messages` aufgelistet. Für die folgende Definition:

```
store localdir {
    pat Mail/*
    prefix Mail/
}
```

listet der Befehl `mailsync -m localdir` alle Nachrichten auf, die unter `Mail/` gespeichert sind. Der Befehl `mailsync localdir` listet dagegen die Ordnernamen auf. Die Spezifikation eines Store auf einem IMAP-Server sieht wie folgt aus:

```
store imapinbox {
    server {mail.edu.harvard.com/user=gulliver}
    ref {mail.edu.harvard.com}
    pat INBOX
}
```

Das obige Beispiel adressiert nur den Hauptordner auf dem IMAP-Server. Ein Store für die Unterordner würde wie folgt aussehen:

```
store imapdir {
    server {mail.edu.harvard.com/user=gulliver}
    ref {mail.edu.harvard.com}
    pat INBOX.*
    prefix INBOX.
}
```

Unterstützt der IMAP-Server verschlüsselte Verbindungen, sollte die Server-Spezifikation wie folgt geändert werden:

```
server {mail.edu.harvard.com/ssl/user=gulliver}
```

oder, falls das Server-Zertifikat nicht bekannt ist, wie folgt:

```
server {mail.edu.harvard.com/ssl/novalidate-cert/user=gulliver}
```

Das Präfix wird später erklärt.

Nun sollen die Ordner unter `Mail/` mit den Unterverzeichnissen auf dem IMAP-Server verbunden werden:

```
channel folder localdir imapdir {  
  msinfo .mailsync.info  
}
```

`mailsync` verfolgt mithilfe der Datei `msinfo`, welche Nachrichten bereits synchronisiert wurden.

Der Befehl `mailsync folder` bewirkt Folgendes:

- Auf beiden Seiten wird das Mailbox-Schema erweitert.
- Von den resultierenden Ordnernamen wird jeweils das Präfix entfernt.
- Die Ordner werden paarweise synchronisiert (bzw. angelegt, falls noch nicht vorhanden).

Der Ordner `INBOX.sent-mail` auf dem IMAP-Server wird also mit dem lokalen Ordner `Mail/sent-mail` synchronisiert (obige Definitionen vorausgesetzt). Die Synchronisierung zwischen den einzelnen Ordnern wird wie folgt durchgeführt:

- Existiert eine Nachricht schon auf beiden Seiten, geschieht nichts.
- Fehlt die Nachricht auf einer Seite und ist neu (d. h. nicht in der Datei `msinfo` protokolliert), wird sie dorthin übertragen.
- Existiert die Nachricht nur auf einer Seite und ist alt (d. h. bereits in der Datei `msinfo` protokolliert), wird sie dort gelöscht (da sie offenbar auf der anderen Seite existiert hatte und dort gelöscht wurde).

Um im Voraus ein Bild davon zu erhalten, welche Nachrichten bei einer Synchronisierung übertragen und welche gelöscht werden, starten Sie `mailsync` mit einem Channel *und* einem Store gleichzeitig: `mailsync folder localdir`. Dadurch erhalten Sie eine Liste aller Nachrichten, die auf dem lokalen Host neu sind, sowie eine Liste

aller Nachrichten, die bei einer Synchronisierung auf der IMAP-Seite gelöscht werden würden. Ähnlich erhalten Sie mit `mailsync folder imapdir` sowohl eine Liste aller Nachrichten, die auf der IMAP-Seite neu sind, als auch eine Liste aller Nachrichten, die bei einer Synchronisierung auf dem lokalen Host gelöscht werden würden.

40.7.2 Potenzielle Probleme

Im Fall eines Datenverlusts ist es das sicherste Vorgehen, die zugehörige Channel-Protokolldatei `msinfo` zu löschen. Dadurch gelten alle Nachrichten, die nur auf jeweils einer Seite existieren, als neu und werden bei der nächsten Synchronisierung übertragen.

Nur Nachrichten mit einer Message-ID werden in die Synchronisierung einbezogen. Nachrichten ohne Message-ID werden einfach ignoriert, d. h. sie werden weder übertragen noch gelöscht. Das Fehlen einer Message-ID wird in der Regel durch fehlerhafte Programme beim Senden oder Schreiben einer Nachricht verursacht.

Auf bestimmten IMAP-Servern werden der Hauptordner mit `INBOX` und Unterordner mit einem beliebigen Namen angesprochen (im Gegensatz zu `INBOX` und `INBOX.name`). Dadurch ist es bei solchen IMAP-Servern nicht möglich, ein Schema ausschließlich für die Unterordner anzugeben.

Die von `mailsync` benutzten Mailbox-Treiber (`c-client`) setzen nach der erfolgreichen Übertragung der Nachrichten an einen IMAP-Server ein spezielles Status-Flag. Daher können einige E-Mail-Programme, wie z. B. `mutt`, diese Nachrichten nicht als neu erkennen. Sie können das Setzen dieses speziellen Status-Flags mithilfe der Option `-n` verhindern.

40.7.3 Weitere Informationen

Die im Paket `mailsync` enthaltene `README`-Datei unter `/usr/share/doc/packages/mailsync/` bietet weitere Informationen. Von besonderem Interesse ist in diesem Zusammenhang auch RFC 2076 „Common Internet Message Headers“.

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 November 2005 der weltweit am häufigsten eingesetzte Webserver. Der von Apache Software Foundation (<http://www.apache.org/>), entwickelte Apache-Server läuft auf fast allen Betriebssystemen. SUSE® Linux Enterprise Server enthält 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.

41.1 Schnellstart

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.

41.1.1 Voraussetzungen

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 31, Grundlegendes zu Netzwerken](#) (S. 605).

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 33, Zeitsynchronisierung mit NTP](#) (S. 675).
3. Die neuesten Sicherheitsaktualisierungen sind installiert. Falls Sie sich nicht sicher sind, führen Sie YaST-Online-Update aus.
4. In der Firewall ist der Standardport des Webservers (Port 80) geöffnet. Lassen Sie dazu in SUSEFirewall2 den Service *HTTP-Server* in der externen Zone zu. Diese Konfiguration können Sie in YaST vornehmen. Weitere Informationen erhalten Sie unter [Abschnitt 44.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 906).

41.1.2 Installation

Apache ist in der Standardinstallation von SUSE Linux Enterprise Server nicht enthalten. Zur Installation starten Sie YaST und wählen Sie *Software* → *Software-Management* aus. Wählen Sie dann *Filter* → *Schemata* und schließlich *Web- and LAMP-Server* aus. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

Apache wird mit einer voreingestellten Standardkonfiguration installiert. Hierzu zählt sowohl das Multiprocessing-Modul (MPM) `apache2-prefork` als auch das Modul `PHP5`. Weitere Informationen zu Modulen erhalten Sie unter [Abschnitt 41.4, „Installieren, Aktivieren und Konfigurieren von Modulen“](#) (S. 831).

41.1.3 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 *Beenden* speichern, wird Apache beim Systemstart automatisch in Runlevel 3 und 5 gestartet. Weitere Informationen zu den Runlevels in SUSE Linux Enterprise Server und eine Beschreibung des YaST-Runlevel-Editors finden Sie in [Abschnitt 20.2.3, „Konfigurieren von Systemdiensten \(Runlevel\) mit YaST“](#) (S. 431).

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 41.8, „Fehlerbehebung“](#) (S. 852).

Nachdem der Webserver nun läuft, können Sie eigene Dokumente hinzufügen, die Konfiguration an Ihre Anforderungen anpassen und weitere Module mit den benötigten Funktionen installieren.

41.2 Konfigurieren von Apache

In SUSE Linux Enterprise Server kann Apache auf zweierlei Weisen konfiguriert werden: 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 Computer automatisch neu gestartet. Der manuelle Neustart wird unter [Abschnitt 41.3, „Starten und Beenden von Apache“](#) (S. 829) beschrieben. Für die meisten Konfigurationsänderungen ist allerdings nur eine Aktualisierung mit `rcapache2 reload` erforderlich.

41.2.1 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.

WICHTIG: Kein SuSEconfig-Modul für Apache

Das SuSEconfig-Modul für Apache wurde aus SUSE Linux Enterprise Server entfernt. SuSEconfig muss nach einer Änderung von `/etc/sysconfig/apache2` nicht mehr ausgeführt werden.

`/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-global.conf
|- ssl.*
|- 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. 818)).

`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. Einzelheiten finden Sie unter [Abschnitt 41.4, „Installieren, Aktivieren und Konfigurieren von Modulen“](#) (S. 831). Die Konfigurationsdateien optionaler Module befinden sich im Verzeichnis `conf.d`.

`server-tuning.conf`

Diese Datei enthält Konfigurationsdirektiven für verschiedene MPMs (siehe [Abschnitt 41.4.4, „Multiprocessing-Module“](#) (S. 836)) und allgemeine Konfigurationsoptionen, die sich auf die Leistung von Apache auswirken. Sie können diese Datei bearbeiten, sollten den Webserver anschließend aber gründlich testen.

`ssl-global.conf` und `ssl.*`

Diese Dateien enthalten die globale SSL-Konfiguration und die SSL-Zertifikatdaten. Einzelheiten finden Sie unter [Abschnitt 41.6, „Einrichten eines sicheren Webservers mit SSL“](#) (S. 843).

`sysconfig.d/*.conf`

Diese Konfigurationsdateien werden automatisch aus `/etc/sysconfig/apache2` konfiguriert. 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. Einzelheiten finden Sie unter „[Virtuelle Hostkonfiguration](#)“ (S. 817).

Virtuelle Hostkonfiguration

Virtueller Host bezieht sich auf die Fähigkeit von Apache, mehrere URIs (Universal Resource Identifiers) vom gleichen physischen Computer aus bedienen zu können. In anderen Worten: Mehrere Domänen wie `www.beispiel.com` und `www.beispiel.net` können von einem einzigen Webserver auf einem physischen Computer ausgeführt werden.

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. 825)) oder manuell durch Bearbeitung einer Konfigurationsdatei konfiguriert werden. In SUSE Linux Enterprise Server 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/2.0/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 41.1 *Beispiele für namensbasierte VirtualHost-Einträge*

```
# NameVirtualHost ip-adresse[:port]
NameVirtualHost 192.168.1.100:80
NameVirtualHost 192.168.1.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:164::]: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 41.2 *Namensbasierte VirtualHost-Direktiven*

```
<VirtualHost 192.168.1.100:80>
...
</VirtualHost>

<VirtualHost 192.168.1.100>
...
</VirtualHost>

<VirtualHost *:80>
...
</VirtualHost>

<VirtualHost *>
...
</VirtualHost>

<VirtualHost [2002:c0a8:164::]>
...
</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 192.168.0.10, auf dem sich zwei Domänen mit den zusätzlichen IPs 192.168.0.20 und 192.168.0.30 befinden. Für jeden virtuellen Server wird ein eigener VirtualHost-Block benötigt.

Beispiel 41.3 *IP-basierte VirtualHost-Direktiven*

```
<VirtualHost 192.168.0.20>
...
</VirtualHost>

<VirtualHost 192.168.0.30>
...
</VirtualHost>
```

In diesem Beispiel sind nur für die beiden zusätzlichen IP-Adressen (also nicht für 192.168.0.10) VirtualHost-Direktiven angegeben. Sollte für 192.168.0.10 auch eine Listen-Direktive konfiguriert sein, müsste ein eigener IP-basierter Host für die HTTP-Anforderungen an diese Schnittstelle eingerichtet werden. Anderenfalls fänden die Direktiven aus der Standardserverkonfiguration (`/etc/apache2/default-server.conf`) Anwendung.

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. Daher müssen Sie das `DocumentRoot`-Verzeichnis, in dem Sie die von Apache zu bedienenden Dateien abgelegt haben, explizit entsperren:

```
<Directory "/srv/www/example.com_htdocs">
  Order allow,deny
  Allow from all
</Directory>
```

Die vollständige Basiskonfiguration eines virtuellen Hosts sieht wie folgt aus:

Beispiel 41.4 *Basiskonfiguration eines virtuellen Hosts*

```
<VirtualHost 192.168.0.10>
  ServerName www.example.com
  DocumentRoot /srv/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/example.com">
    Order allow,deny
    Allow from all
  </Directory>
</VirtualHost>
```

41.2.2 Konfigurieren von Apache mit YaST

Zur Konfiguration des Webservers mit YaST starten Sie YaST und wählen Sie *Netzwerkdienste* → *HTTP-Server* aus. 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. 827) 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

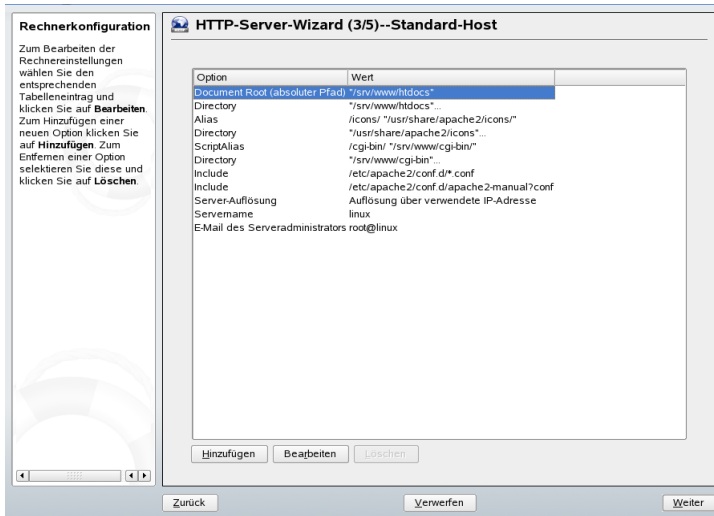
Mit dieser Konfigurationsoption aktivieren bzw. deaktivieren Sie die vom Webserver unterstützten Skriptsprachen. Informationen zur Aktivierung bzw. Deaktivierung anderer Module erhalten Sie unter „[Servermodule](#)“ (S. 828). Klicken Sie auf *Weiter*, um das nächste Dialogfeld zu öffnen.

Standardhost

Diese Option betrifft den Standard-Webserver. Wie in „[Virtuelle Hostkonfiguration](#)“ (S. 817) 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 41.1 HTTP-Server-Wizard: Standard-Host



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 SUSE Linux Enterprise Server `Alias` für die in der Verzeichnis-index-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-Skripts festlegt.

`Verzeichnis`

Unter dieser Einstellung können Sie mehrere Konfigurationsoptionen zusammenfassen, die nur für das angegebene Verzeichnis gelten.

Hier werden auch die Zugriffs- und Anzeigooptionen für die Verzeichnisse `/usr/share/apache2/icons` und `/srv/www/cgi-bin` konfiguriert. Eine Änderung dieser Standardeinstellungen sollte nicht erforderlich sein.

`Include`

Hier können weitere Konfigurationsdateien hinzugefügt werden. Im Verzeichnis `/etc/apache2/conf.d/` befinden sich z. B. die Konfigurationsdateien der externen Module. Standardmäßig sind alle Dateien in diesem Verzeichnis (`*.conf`) eingeschlossen. Das Verzeichnis `/etc/apache2/conf.d/apache2-manual?conf` enthält hingegen alle `apache2-manual`-Konfigurationsdateien.

`Servername`

Hier wird die Standard-URL festgelegt, über die Clients den Webserver kontaktieren. Verwenden Sie einen qualifizierten Domänennamen (FQDN), um den Webserver unter `http://FQDN/` zu erreichen. Alternativ können Sie auch die IP-Adresse verwenden. Geben Sie hier keinen willkürlichen Namen ein – 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.

Server-Auflösung

Diese Option bezieht sich auf „[Virtuelle Hostkonfiguration](#)“ (S. 817). Wenn *Anfrage-Server durch HTTP-Header bestimmen* aktiviert ist, kann ein virtueller Host die an seinen Servernamen gerichteten Anforderungen beantworten (siehe „[Namensbasierte virtuelle Hosts](#)“ (S. 818)). Wenn *Anfrage-Server durch Server-IP-Adresse bestimmen* aktiviert ist, wählt Apache den angeforderten Host entsprechend der vom Client gesendeten HTTP-Header-Informationen aus. Weitere Informationen über IP-basierte virtuelle Hosts erhalten Sie in „[IP-basierte virtuelle Hosts](#)“ (S. 819).

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. 817)). Falls Sie vor Ausführung des HTTP-Assistenten keine manuellen Konfigurationsänderungen vorgenommen haben, wird nur ein virtueller Host angezeigt. Dieser ist identisch mit dem im vorangegangenen Schritt konfigurierten Standardhost. Durch einen Stern neben seinem Servernamen ist er als Standard gekennzeichnet.

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). Diese Optionen werden in „[Standardhost](#)“ (S. 823) näher erläutert.

Klicken Sie auf *Weiter*, um mit dem zweiten Teil der virtuellen Hostkonfiguration fortzufahren.

Im zweiten Teil der virtuellen Hostkonfiguration legen Sie fest, ob CGI-Skripts zugelassen sind und welches Verzeichnis für diese Skripts 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 41.6.2](#), „[Konfigurieren von Apache mit SSL](#)“ (S. 849). 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 *Enable Public HTML* (Öffentliches HTML aktivieren) stellen Sie den Inhalt der öffentlichen Benutzerverzeichnisse (`~user/public_html/`) auf dem Server unter `http://www.beispiel.com/~user` bereit.

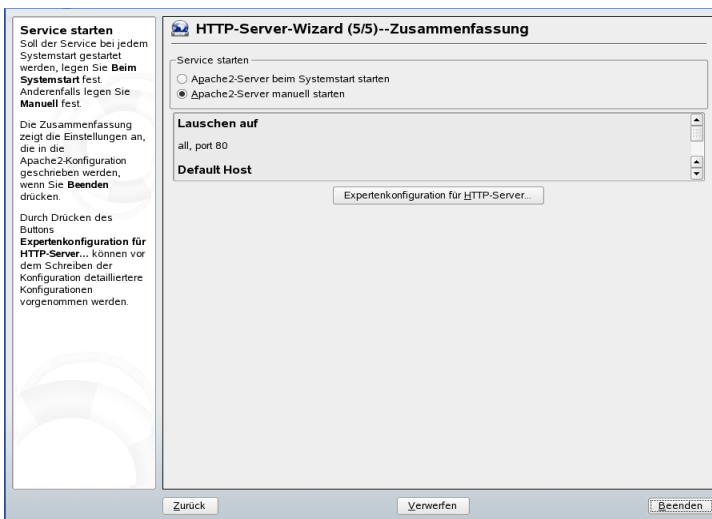
WICHTIG: Erstellen virtueller Hosts

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. Hier können Sie festlegen, wie und wann der Apache-Server gestartet werden soll: beim Systemstart 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 *Beenden* 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. 827) beschriebene Dialogfeld öffnen.

Abbildung 41.2 *HTTP-Server-Wizard: Zusammenfassung*



HTTP-Server-Konfiguration

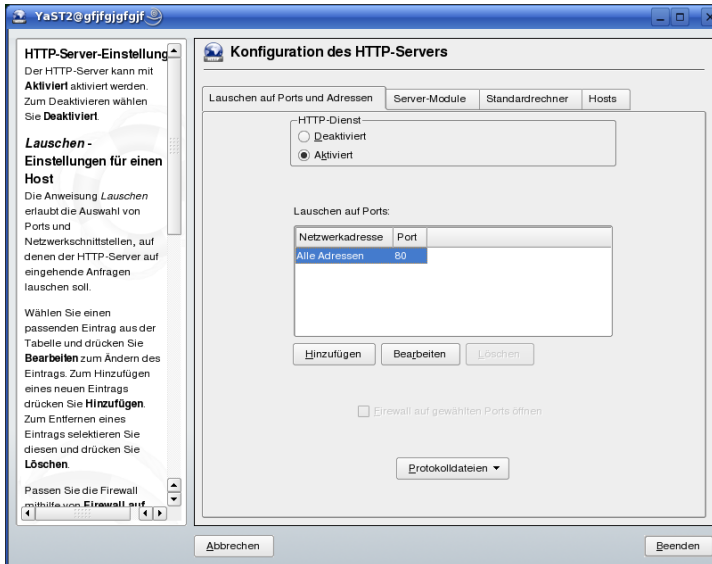
Im Dialogfeld *HTTP-Server-Konfiguration* können Sie weitaus mehr Einstellungen vornehmen als im Assistenten (dieser wird ohnehin nur bei der Anfangskonfiguration des Webservers ausgeführt). Das Dialogfeld enthält vier Registerkarten, die nachfolgend beschrieben werden. Keine der in diesem Dialogfeld vorgenommenen Konfigurationsänderungen wird sofort wirksam. Dies geschieht erst, wenn Sie das Dialogfeld mit *Beenden* 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 41.3](#), „[Starten und Beenden von Apache](#)“ (S. 829)). Diese Befehle werden sofort ausgeführt.

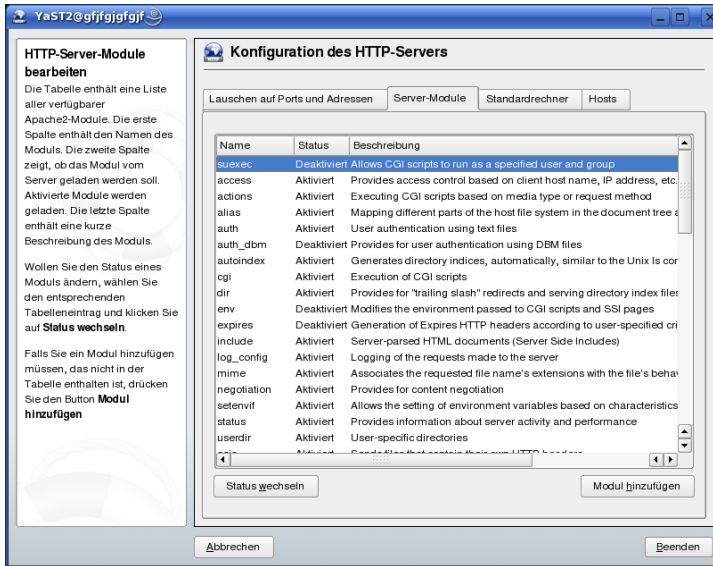
Abbildung 41.3 *HTTP-Server-Konfiguration: Listen Ports and Addresses (Überwachte Ports und Adressen)*



Servermodule

Über *Toggle Status* (Status ändern) 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 41.4](#), „[Installieren, Aktivieren und Konfigurieren von Modulen](#)“ (S. 831).

Abbildung 41.4 HTTP-Server-Konfiguration: Server-Module



"Standardhost" und "Hosts"

Diese Registerkarten sind identisch mit den in „Standardhost“ (S. 823) und „Virtuelle Hosts“ (S. 825) beschriebenen Dialogfeldern.

41.3 Starten und Beenden von Apache

Wenn Apache in YaST konfiguriert wurde (siehe [Abschnitt 41.2.2, „Konfigurieren von Apache mit YaST“](#) (S. 822)), 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 20.2.2, „Init-Skripts“](#) (S. 427)). 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 41.6, „Einrichten eines sicheren Webservers mit SSL“](#) (S. 843).

`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 `rcapach2`-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 `rcapach2` angeben, werden direkt an den Webserver weitergeleitet.

41.4 Installieren, Aktivieren und Konfigurieren von Modulen

Die Apache-Software ist modular aufgebaut. Sämtliche Funktionen mit Ausnahme der wichtigsten Aufgaben werden in Modulen zur Verfügung gestellt. 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 41.4.2, „Aktivieren und Deaktivieren von Modulen“](#) (S. 832).

Apache-Module lassen sich in vier Kategorien einteilen:

Basismodule

Basismodule sind standardmäßig in Apache enthalten. In Apache von SUSE Linux sind nur die Basismodule `mod_so` und `http_core` kompiliert. Alle anderen Basismodule stehen als gemeinsame Objekte zur Verfügung: Sie sind zwar nicht im Server-Binary enthalten, können jedoch während der Laufzeit hinzugefügt werden.

Erweiterungsmodule

Im Allgemeinen sind Erweiterungsmodule im Apache-Softwarepaket enthalten, jedoch nicht statisch im Server kompiliert. In SUSE Linux 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. SUSE Linux 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.

41.4.1 Installieren von Modulen

Wenn Sie das Standardinstallationsverfahren für Apache durchgeführt haben (siehe [Abschnitt 41.1.2, „Installation“](#) (S. 812)), wird Apache mit allen Basis- und Erweiterungsmodulen sowie dem Multiprocessing-Modul Prefork und dem externen Modul PHP5 installiert.

In YaST können Sie weitere externe Module installieren. Starten Sie dazu YaST und wählen Sie *Software* → *Software-Management*. Wählen Sie danach *Filter* → *Suche* und suchen Sie nach *apache*. Die Ergebnisliste zeigt nun neben anderen Paketen alle verfügbaren externen Apache-Module an.

41.4.2 Aktivieren und Deaktivieren von Modulen

Die Skriptsprachenmodule PHP5, Perl, Python und Ruby können Sie in YaST mit der im [Abschnitt „HTTP-Server-Wizard“](#) (S. 822) beschriebenen Modulkonfiguration aktivieren oder deaktivieren. Alle anderen Module werden, wie im [Abschnitt „Servermodule“](#) (S. 828) beschrieben, aktiviert oder deaktiviert.

Manuell können Sie die Module mit dem Befehl `a2enmod mod_foo` bzw. `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`.

41.4.3 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_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 stellen zwei Authentifizierungsmethoden bereit: Die Standardauthentifizierung mit `mod_auth_basic` und die 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` funktionieren nur gemeinsam mit dem Authentifizierungsanbietermodul `mod_authn_*` (z. B. `mod_authn_file` für die Authentifizierung auf Basis einer Textdatei) und mit dem Autorisierungsmodul `mod_authz_*` (z. B. `mod_authz_user` für die Benutzerautorisierung).

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. Allerdings sind Verzeichnislisten 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_expires

Mit `mod_expires` legen Sie fest, wie häufig Ihre Dokumente über Proxy- und Browser-Caches durch Zustellung eines `Expires`-Header aktualisiert werden. Dieses Modul ist standardmäßig aktiviert.

mod_include

`mod_include` ermöglicht die Verwendung von serverseitigen Includes (SSI), die die grundlegende Funktionalität für die dynamische Generierung von HTML-Seiten bereitstellen. Dieses Modul ist standardmäßig aktiviert.

mod_info

Dieses Modul stellt unter `http://localhost/server-info/` eine umfassende Übersicht über die Serverkonfiguration bereit. Aus Sicherheitsgründen sollte der Zugriff auf diese URL generell eingeschränkt sein. Standardmäßig erhält nur `localhost` Zugriff auf diese URL. `mod_info` wird in der Datei `/etc/apache2/mod_info.conf` konfiguriert.

mod_log_config

Mit diesem Modul konfigurieren Sie den Aufbau der Apache-Protokolldateien. Dieses Modul ist standardmäßig aktiviert.

mod_mime

Dieses Modul sorgt dafür, dass eine Datei auf Basis seiner Dateinamenerweiterung mit dem korrekten MIME-Header bereitgestellt wird (z. B. `text/html` für HTML-Dokumente). Dieses Modul ist standardmäßig aktiviert.

mod_negotiation

Dieses Modul ist für die Inhaltsverhandlung erforderlich. Weitere Informationen erhalten Sie unter <http://httpd.apache.org/docs/2.2/content-negotiation.html>. Dieses Modul ist standardmäßig aktiviert.

mod_rewrite

Dieses Modul stellt die gleiche Funktionalität wie `mod_alias` bereit, bietet aber mehr Funktionen und ist somit flexibler. Mit `mod_rewrite` können Sie URLs auf Basis verschiedener Regeln umleiten, Header anfordern und einiges mehr.

mod_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 Einzelheiten finden Sie unter [Abschnitt 41.6, „Einrichten eines sicheren Webservers mit SSL“](#) (S. 843). 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-Skripts 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.

41.4.4 Multiprocessing-Module

SUSE Linux Enterprise Server bietet zwei Multiprocessing-Module (MPMs) für Apache.

Prefork-MPM

Das Prefork-MPM implementiert einen Prefork-Webserver, der keine Threads verwendet. Mit diesem Modul verhält sich der Webserver, was die Handhabung von Anforderungen betrifft, ähnlich wie Apache Version 1.x: Er isoliert jede einzelne Anforderung und verarbeitet sie in einem separaten untergeordneten Prozess (Forking). Eine Beeinträchtigung aller Anforderungen durch wenige problematische Anforderungen und somit eine Sperre des Webserver lassen sich dadurch vermeiden.

Die prozessbasierte Vorgehensweise des Prefork-MPM bietet zwar Stabilität, konsumiert aber mehr Systemressourcen wie das Worker-MPM. Für UNIX-basierte Betriebssysteme gilt das Prefork-MPM als Standard-MPM.

WICHTIG: MPMs in diesem Dokument

In diesem Dokument wird davon ausgegangen, dass Apache mit dem Prefork-MPM verwendet wird.

Worker-MPM

Das Worker-MPM implementiert einen Multithread-Webserver. Ein Thread ist die „Lightweight-Version“ eines Prozesses. Der Vorteil von Threads gegenüber Prozessen ist deren geringerer Ressourcenkonsum. Anstatt lediglich untergeordnete Prozesse zu erstellen (Forking), verarbeitet das Worker-MPM Anforderungen durch Threads mit Serverprozessen. Die untergeordneten Prefork-Prozesse sind auf mehrere Threads aufgeteilt (Multithreading). Diese Ansatzweise macht den Apache-Server durch den geringeren Ressourcenkonsum leistungsfähiger als mit dem Prefork-MPM.

Ein gravierender Nachteil ist allerdings die geringere Stabilität des Worker-MPM: Ein beschädigter Thread kann sich auf alle Threads des 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.

41.4.5 Externe Module

Nachfolgend finden Sie eine Liste aller externen Module, die mit SUSE Linux Enterprise Server ausgeliefert werden. Die Dokumentation zu den einzelnen Modulen finden Sie in den jeweils genannten Verzeichnissen.

FastCGI

FastCGI ist eine sprachunabhängige, skalierbare Erweiterung zu CGI, die erstklassige Leistung ohne die Einschränkungen serverspezifischer APIs bietet. FastCGI-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_fastcgi`

Konfigurationsdatei: `/etc/apache2/conf.d/mod_fastcgi.conf`

Weitere Informationen: `/usr/share/doc/packages/apache2-mod_fastcgi`

`mod_perl`

`mod_perl` ermöglicht die Ausführung von Perl-Skripts in einem eingebetteten Interpreter. Durch den persistenten, 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_ruby`

`mod_ruby` bettet den Ruby-Interpreter in den Apache-Webserver ein. Dadurch können Ruby CGI-Skripts in Originalversion ausgeführt werden. Diese Skripts werden mit `mod_ruby` wesentlich schneller ausgeführt.

Paketname: `apache2-mod_ruby`
Weitere Informationen: `/usr/share/doc/packages/apache2-mod_ruby`

`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`

41.4.6 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. Die Module werden im Verzeichnis `/usr/lib/apache2-prefork` installiert.
- `/usr/sbin/apxs2-worker`: Für die Entwicklung von Worker-MPM-Modulen.

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.

41.5 Aktivieren von CGI-Skripts

Die Common Gateway Interface (CGI) von Apache ermöglicht die dynamische Erstellung von Inhalten mit Programmen bzw. so genannten CGI-Skripts. CGI-Skripts

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-Skripts 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 41.4.2, „Aktivieren und Deaktivieren von Modulen“](#) (S. 832).

WARNUNG: CGI-Sicherheit

Die Zulassung der CGI-Skriptausführung auf dem Server ist ein Sicherheitsrisiko. Weitere Informationen hierzu erhalten Sie unter [Abschnitt 41.7, „Vermeiden von Sicherheitsproblemen“](#) (S. 850).

41.5.1 Konfiguration in Apache

In SUSE Linux Enterprise Server ist die Ausführung von CGI-Skripts nur im Verzeichnis `/srv/www/cgi-bin/` erlaubt. Dieses Verzeichnis ist bereits für die Ausführung von CGI-Skripts konfiguriert. Wenn Sie eine virtuelle Hostkonfiguration erstellt haben (siehe [„Virtuelle Hostkonfiguration“](#) (S. 817)) und Ihre CGI-Skripts in einem Host-spezifischen Verzeichnis ablegen möchten, müssen Sie das betreffende Verzeichnis entsperren und für CGI-Skripts konfigurieren.

Beispiel 41.5 CGI-Konfiguration für virtuelle Hosts

```
ScriptAlias /cgi-bin/ "/srv/www/example.com_cgi-bin/"❶
```

```
<Directory "/srv/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-Skripts zu behandeln
- ❷ Aktiviert die Ausführung von CGI-Skripts
- ❸ Fordert den Server auf, Dateien mit den Erweiterungen .pl und .cgi als CGI-Skripts zu behandeln; passen Sie diese Anweisung entsprechend Ihren Anforderungen an
- ❹ Die Order- und Allow-Direktiven legen den Standardzugriffsstatus sowie die Reihenfolge fest, in der Allow- und Deny-Direktiven ausgewertet werden; in diesem Beispiel werden „deny“-Anweisungen vor „allow“-Anweisungen ausgewertet und der Zugriff ist von jedem Ort aus möglich.

41.5.2 Ausführen eines Beispielskripts

Die CGI-Programmierung unterscheidet sich von der herkömmlichen Programmierung insoweit, als CGI-Programmen und -Skripts ein MIME-Typ-Header wie `Content-type: text/html` vorangestellt sein 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 – dies ist in den meisten Fällen HTML, 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/beispiel.com_cgi-bin/`) und benennen Sie es in `test.cgi` um.

Über den Webserver zugängliche Dateien sollten dem `root`-Benutzer gehören (siehe auch [Abschnitt 41.7, „Vermeiden von Sicherheitsproblemen“](#) (S. 850)). Da der Webserver unter einem anderen Benutzer ausgeführt wird, müssen CGI-Skripts 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://example.com/cgi-bin/test.cgi` auf. Nun sollte der „CGI/1.0-Testskriptbericht“ angezeigt werden.

41.5.3 Fehlerbehebung

Wenn Sie nach der Ausführung des CGI-Testskripts 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.

41.6 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/TSL 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/TSL-Protokolle nicht selbst, sondern fungiert als Schnittstelle zwischen Apache und einer SSL-Bibliothek. In SUSE Linux Enterprise Server 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://`).

41.6.1 Erstellen eines SSL-Zertifikats

Wenn Sie SSL/TSL mit dem Webserver einsetzen möchten, müssen Sie ein SSL-Zertifikat erstellen. Dieses Zertifikat ist für die Autorisierung zwischen Webserver und Client erforderlich, damit beide Endpunkte jeweils die Identität des anderen Endpunkts überprüfen können. Zum Nachweis der Zertifikatintegrität muss das Zertifikat von einer Organisation signiert sein, der jeder der beteiligten Benutzer vertraut.

Sie können drei verschiedene Zertifikattypen erstellen: ein „Dummy“-Zertifikat, das allein zum Testen 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: Weitere 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. Sie brauchen dazu lediglich das Skript `/usr/bin/gensslcert` aufzurufen. 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 41.1 *Erstellen eines selbst signierten Zertifikats mit `mkcert.sh`*

- 1** Decide the signature algorithm used for certificates
(Signaturalgorithmus für Zertifikat auswählen)

Wählen Sie RSA aus (, 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. Unter „Common Name“ (allgemeiner Name) müssen Sie den Namen der Zertifizierungsstelle eingeben. Geben Sie hier einen aussagekräftigen Namen ein, beispielsweise „Zertifizierungsstelle von *My company*“.

- 4 Generating X.509 certificate for CA signed by itself
(Von CA selbst signiertes X.509-Zertifikat für CA erstellen)

Wählen Sie Zertifikatversion aus (die Standardeinstellung).

- 5 Generating RSA private key for SERVER (1024 bit)
(Privaten RSA-Schlüssel für SERVER (1024 Bit) erstellen)

Keine Eingabe erforderlich.

- 6 Generating X.509 certificate signing request for SERVER
(X.509-Zertifikatsignierungsanforderung für SERVER erstellen)

Hier erstellen Sie den DN für den Serverschlüssel. Es werden nahezu die gleichen Fragen gestellt wie für den DN der Zertifizierungsstelle. Ihre Antworten betreffen jedoch den Webserver und müssen nicht unbedingt identisch mit den für die Zertifizierungsstelle eingegebenen Daten sein (der Server kann sich z. B. an einem anderen Standort befinden).

WICHTIG: Auswahl eines Common Name

Als Common Name (allgemeiner Name) müssen Sie hier den vollständig qualifizierten Hostnamen des sicheren Servers eingeben (z. B. `www.beispiel.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 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 aus und geben Sie ein Passwort ein.

- 9 Encrypting RSA private key of SERVER with a pass phrase for security (Privaten RSA-Schlüssel des SERVERS aus Sicherheitsgründen mit einem Passwort verschlüsseln)

Wenn Sie den Serverschlüssel mit einem Passwort verschlüsseln, müssen Sie dieses Passwort bei jedem Start des Webservers eingeben. Dies macht den automatischen Start des Webservers beim Hochfahren des Computers oder einen Neustart des Webservers nahezu unmöglich. Aus diesem Grund sollten Sie diese Frage mit 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 sich dennoch entscheiden, den Serverschlüssel mit einem Passwort zu verschlüsseln, sollten Sie den `APACHE_TIMEOUT`-Wert in `/etc/sysconfig/apache2` heraufsetzen. Anderenfalls bleibt Ihnen unter Umständen nicht genügend Zeit für die Eingabe des Passworts, bevor der Startversuch des Servers wegen Zeitüberschreitung abgebrochen wird.

Die Ergebnisseite des Skripts enthält eine Liste der generierten Zertifikate und Schlüssel. Die Dateien wurden allerdings nicht, wie im Skript angegeben, im lokalen Verzeichnis `conf` erstellt, sondern in den passenden Verzeichnissen unter `/etc/apache2/`.

Der letzte Schritt besteht darin, die Zertifikatdatei der Zertifizierungsstelle aus dem Verzeichnis `/etc/apache2/ssl.crt/ca.crt` in ein Verzeichnis zu kopieren, in dem die Benutzer auf die Datei zugreifen können. Aus diesem Verzeichnis können die Benutzer die Zertifizierungsstelle in ihren Webbrowsern der Liste der bekannten und vertrauenswürdigen Zertifizierungsstellen hinzufügen. Wäre die Zertifizierungsstelle nicht in dieser Liste enthalten, würde der Browser melden, dass das Zertifikat von einer unbekanntem Zertifizierungsstelle ausgegeben wurde. Das neu erstellte Zertifikat ist ein Jahr lang gültig.

WICHTIG: Selbst signierte 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 (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.

Zur Anforderung eines offiziell signierten Zertifikats senden Sie kein unsigniertes 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. Schließlich wird alles, was Sie hier eingeben, 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. Unter „Common Name“ (allgemeiner Name) müssen Sie den Namen der Zertifizierungsstelle eingeben. Geben Sie hier einen aussagekräftigen Namen ein, beispielsweise „Zertifizierungsstelle von *My company*“. 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`.

41.6.2 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 44.4.1](#), „Konfigurieren der Firewall mit YaST“ (S. 906)).

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. 817).

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.

41.7 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.

41.7.1 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.suse.com/us/private/support/online_help/maillinglists/
- **Mailingliste** http://www.suse.com/us/private/support/online_help/maillinglists/

- **RSS-Newsticker** http://www.novell.com/linux/security/suse_security.xml

41.7.2 DocumentRoot-Berechtigungen

In SUSE Linux Enterprise Server sind das `DocumentRoot`-Verzeichnis `/srv/www/htdocs` (absoluter Pfad) 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.

41.7.3 Zugriff auf das Dateisystem

`/etc/apache2/httpd.conf` verweigert standardmäßig den Zugriff auf das gesamte Dateisystem. Diese Direktiven sollten Sie nicht überschreiben. Stattdessen sollten Sie explizit den Zugriff auf die Verzeichnisse aktivieren, die Apache lesen muss (siehe „[Basiskonfiguration eines virtuellen Hosts](#)“ (S. 820)). Achten Sie dabei darauf, dass keine unbefugten Personen auf kritische Dateien wie Passwort- oder Systemkonfigurationsdateien zugreifen können.

41.7.4 CGI-Skripts

Interaktive Skripts in Perl, PHP, SSI oder anderen Programmiersprachen können im Prinzip jeden beliebigen Befehl ausführen und stellen damit generell ein Sicherheitsrisiko dar. Skripts, die vom Server ausgeführt werden, sollten nur aus Quellen stammen, denen der Serveradministrator vertraut. Keine gute Idee ist es, den Benutzern die Ausführung ihrer eigenen Skripts zu erlauben. Zusätzlich empfiehlt es sich, die Sicherheit aller Skripts zu überprüfen.

Es ist durchaus üblich, sich die Skriptverwaltung durch eine Einschränkung der Skriptausführung zu vereinfachen. Dabei wird die Ausführung von CGI-Skripts auf bestimmte Verzeichnisse eingeschränkt, statt sie global zuzulassen. Die Direktiven `ScriptAlias` und `Option ExecCGI` werden zur Konfiguration verwendet. In der Standardkonfiguration von SUSE Linux Enterprise Server ist es generell nicht gestattet, CGI-Skripts von jedem beliebigen Ort aus auszuführen.

Alle CGI-Skripts werden unter dem gleichen Benutzer ausgeführt. Es kann daher zu Konflikten zwischen verschiedenen Skripts kommen. Abhilfe schafft hier das Modul `suEXEC`, das die Ausführung von CGI-Skripts unter einem anderen Benutzer oder einer anderen Gruppe ermöglicht.

41.7.5 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 SUSE Linux Enterprise Server sind `.htaccess`-Dateien standardmäßig aktiviert. Den Benutzern ist es allerdings nicht erlaubt, mit `mod_userdir` Option-Direktiven zu überschreiben (sehen Sie sich hierzu die Konfigurationsdatei `/etc/apache2/mod_userdir.conf` an).

41.8 Fehlerbehebung

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 41.3, „Starten und Beenden von Apache“](#) (S. 829)) 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 Webservers 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

Die Apache-Protokollmeldungen können Sie mit dem Befehl `tail -F /var/log/apache2/my_error_log` überwachen. Führen Sie danach 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 41.2.2, „Konfigurieren von Apache mit YaST“](#) (S. 822)). 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-Benutzercommunity wenden, die Sie via Mailingliste unter <http://httpd.apache.org/userslist.html> erreichen. Des Weiteren empfehlen wir die Newsgroup comp.infosystems.www.servers.unix.

41.9 Weitere 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.*`.

41.9.1 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>.

41.9.2 Apache-Module

Weitere Informationen zu der in [Abschnitt 41.4.5](#), „Externe Module“ (S. 837) beschriebenen, externen Apache-Module finden Sie unter folgenden Adressen:

FastCGI

<http://www.fastcgi.com/>

mod_perl

<http://perl.apache.org/>

mod_php5

<http://www.php.net/manual/en/install.unix.apache2.php>

mod_python

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

mod_ruby

<http://www.modruby.net/>

41.9.3 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/>

41.9.4 Verschiedene Informationsquellen

Wenn Sie in SUSE Linux Enterprise Server Probleme mit Apache haben, werfen Sie einen Blick auf die SUSE-Support-Datenbank unter <http://en.opensuse.org/SDB:SDB>. 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.

Der Proxyserver Squid

Squid ist ein häufig verwendeter Proxy-Cache für Linux- und UNIX-Plattformen. Das bedeutet, dass er angeforderte Internetobjekte, wie beispielsweise Daten auf einem Web- oder FTP-Server, auf einem Computer speichert, der sich näher an der Arbeitsstation befindet, die die Anforderung ausgegeben hat, als der Server. Er kann in mehreren Hierarchien eingerichtet werden. So werden optimale Reaktionszeiten und die Nutzung einer niedrigen Bandbreite garantiert – auch bei Modi, die für den Endbenutzer transparent sind. Zusätzliche Software, wie squidGuard, kann zum Filtern der Webinhalte verwendet werden.

Squid dient als Proxy-Cache. Er leitet Objktanforderungen von Clients (in diesem Fall: von Webbrowsern) an den Server weiter. Wenn die angeforderten Objekte vom Server eintreffen, stellt er die Objekte dem Client zu und behält eine Kopie davon im Festplatten-Cache. Einer der Vorteile des Cachings besteht darin, dass mehrere Clients, die dasselbe Objekt anfordern, aus dem Festplatten-Cache versorgt werden können. Dadurch können die Clients die Daten wesentlich schneller erhalten als aus dem Internet. Durch dieses Verfahren wird außerdem der Datenverkehr im Netzwerk reduziert.

Neben dem eigentlichen Caching bietet Squid eine breite Palette von Funktionen, wie die Verteilung der Last auf mehrere miteinander kommunizierende Hierarchien von Proxyservern, die Definition strenger Zugriffssteuerungslisten für alle Clients, die auf den Proxy zugreifen, das Zulassen oder Verweigern des Zugriffs auf bestimmte Webseiten mithilfe anderer Anwendungen und das Erstellen von Statistiken zu häufig besuchten Webseiten zur Bewertung der Internetgewohnheiten des Benutzers. Squid ist kein generischer Proxy. Er fungiert normalerweise nur bei HTTP-Verbindungen als Proxy. Außerdem unterstützt er die Protokolle FTP, Gopher, SSL und WAIS, nicht jedoch andere Internetprotokolle, wie Real Audio, News oder Video-Konferenzen. Da Squid nur das UDP-Protokoll für die Bereitstellung von Kommunikation zwischen

verschiedenen Caches unterstützt, werden zahlreiche andere Multimedia-Programme nicht unterstützt.

42.1 Einige Tatsachen zu Proxy-Caches

Als Proxy-Cache kann Squid auf verschiedene Weise verwendet werden. In Kombination mit einer Firewall kann er die Sicherheit unterstützen. Mehrere Proxies können gemeinsam verwendet werden. Außerdem kann er ermitteln, welche Objekttypen für wie lange im Cache gespeichert werden sollen.

42.1.1 Squid und Sicherheit

Squid kann zusammen mit einer Firewall verwendet werden, um interne Netzwerke mithilfe eines Proxy-Caches gegen Zugriffe von außen zu schützen. Die Firewall verweigert allen Clients Zugriff auf externe Dienste mit Ausnahme von Squid. Alle Webverbindungen müssen vom Proxy erstellt werden. Bei dieser Konfiguration steuert Squid den gesamten Webzugriff.

Wenn zur Firewall-Konfiguration eine DMZ gehört, sollte der Proxy in dieser Zone betrieben werden. In [Abschnitt 42.5](#), „[Konfigurieren eines transparenten Proxy](#)“ (S. 870) wird die Implementierung eines *transparenten* Proxy beschrieben. Dadurch wird die Konfiguration der Clients erleichtert, da sie in diesem Fall keine Informationen zum Proxy benötigen.

42.1.2 Mehrere Caches

Mehrere Instanzen von Squid können für den Austausch von Objekten konfiguriert werden. Dadurch verringert sich die Gesamtlast im System und die Wahrscheinlichkeit, ein Objekt zu finden, das bereits im lokalen Netzwerk vorhanden ist, erhöht sich. Außerdem können Cache-Hierarchien konfiguriert werden, sodass ein Cache Objektanforderungen an gleichgeordnete Caches oder einen übergeordneten Cache weiterleiten kann, sodass er Objekte aus einem anderen Cache im lokalen Netzwerk oder direkt von der Quelle erhält.

Die Auswahl einer geeigneten Topologie für die Cache-Hierarchie ist von entscheidender Bedeutung, da es nicht erstrebenswert ist, das Gesamtaufkommen an Datenverkehr im Netzwerk zu erhöhen. Bei sehr großen Netzwerken ist es sinnvoll, einen Proxyserver für jedes Subnetzwerk zu konfigurieren und mit einem übergeordneten Proxy zu verbinden, der wiederum mit dem Proxy-Cache des ISP verbunden ist.

Diese gesamte Kommunikation wird über das ICP (Internet Cache Protocol) abgewickelt, das über dem UDP-Protokoll ausgeführt wird. Die Übertragungen zwischen den Caches erfolgen über HTTP (Hypertext Transmission Protocol) auf der Grundlage von TCP.

Um den geeignetsten Server zum Abrufen der Objekte zu finden, sendet ein Cache eine ICP-Anforderung an alle gleichgeordneten Proxies. Diese beantworten die Anforderungen über ICP-Antworten mit einem HIT-Code, wenn das Objekt erkannt wurde bzw. mit einem MISS-Code, wenn es nicht erkannt wurde. Wenn mehrere HIT-Antworten gefunden wurden, legt der Proxyserver fest, von welchem Server heruntergeladen werden soll. Diese Entscheidung ist unter anderem davon abhängig, welcher Cache die schnellste Antwort gesendet hat bzw. welcher näher ist. Wenn keine zufriedenstellenden Antworten eingehen, wird die Anforderung an den übergeordneten Cache gesendet.

TIPP

Um eine Verdopplung der Objekte in verschiedenen Caches im Netzwerk zu vermeiden, werden andere ICP-Protokolle verwendet, wie beispielsweise CARP (Cache Array Routing Protocol) oder HTCP (Hypertext Cache Protocol). Je mehr Objekte sich im Netzwerk befinden, desto größer ist die Wahrscheinlichkeit, das gewünschte zu finden.

42.1.3 Caching von Internetobjekten

Nicht alle im Netzwerk verfügbaren Objekte sind statisch. Es gibt eine Vielzahl dynamisch erstellter CGI-Seiten, Besucherzähler und verschlüsselter SSL-Inhaltsdokumente. Derartige Objekte werden nicht im Cache gespeichert, da sie sich bei jedem Zugriff ändern.

Es bleibt die Frage, wie lange alle anderen im Cache gespeicherten Objekte dort verbleiben sollten. Um dies zu ermitteln, wird allen Objekten im Cache einer von mehreren möglichen Zuständen zugewiesen. Web- und Proxyserver ermitteln den Status eines Objekts, indem sie Header zu diesen Objekten hinzufügen, beispielsweise "Zuletzt

geändert" oder "Läuft ab", und das entsprechende Datum. Andere Header, die angeben, dass Objekte nicht im Cache gespeichert werden dürfen, werden ebenfalls verwendet.

Objekte im Cache werden normalerweise aufgrund mangelnden Festplattenspeichers ersetzt. Dazu werden Algorithmen, wie beispielsweise LRU (last recently used), verwendet. Dies bedeutet im Wesentlichen, dass der Proxy die Objekte löscht, die am längsten nicht mehr angefordert wurden.

42.2 Systemvoraussetzungen

Die wichtigste Aufgabe besteht darin, die maximale Netzwerkklast zu ermitteln, die das System tragen muss. Daher muss besonders auf die Belastungsspitzen geachtet werden, die mehr als das Vierfache des Tagesdurchschnitts betragen können. Im Zweifelsfall ist es vorzuziehen, die Systemanforderungen zu hoch einzuschätzen, da es zu erheblichen Einbußen in der Qualität des Diensts führen kann, wenn Squid an der Grenze seiner Leistungsfähigkeit arbeitet. Die folgenden Abschnitte widmen sich den einzelnen Systemfaktoren in der Reihenfolge ihrer Wichtigkeit.

42.2.1 Festplatten

Da Geschwindigkeit beim Caching eine wichtige Rolle spielt, muss diesem Faktor besondere Aufmerksamkeit gewidmet werden. Bei Festplatten wird dieser Parameter als *random seek time* (Zufallszugriffszeit, gemessen in Millisekunden) beschrieben. Da die Datenblöcke, die Squid von der Festplatte liest oder auf die Festplatte schreibt, eher klein zu sein scheinen, ist die Zugriffszeit der Festplatte entscheidender als ihr Datendurchsatz. Für die Zwecke von Proxies sind Festplatten mit hoher Rotationsgeschwindigkeit wohl die bessere Wahl, da bei diesen der Lese-Schreib-Kopf schneller an die gewünschte Stelle gebracht werden kann. Eine Möglichkeit zur Systembeschleunigung besteht in der gleichzeitigen Verwendung mehrerer Festplatten oder im Einsatz von Striping-RAID-Arrays.

42.2.2 Größe des Festplatten-Cache

Bei einem kleinen Cache ist die Wahrscheinlichkeit eines HIT (Auffinden des angeforderten Objekts, das sich bereits dort befindet) gering, da der Cache schnell voll ist und die weniger häufig angeforderten Objekte durch neuere ersetzt werden. Wenn

beispielsweise 1 GB für den Cache zur Verfügung steht und die Benutzer nur Datenverkehr im Umfang von 10 MB pro Tag in Anspruch nehmen, dauert es mehrere hundert Tage, um den Cache zu füllen.

Die einfachste Methode zur Ermittlung der benötigten Cache-Größe geht von der maximalen Übertragungsrate der Verbindung aus. Bei einer Verbindung mit 1 Mbit/s beträgt die maximale Übertragungsrate 125 KB/s. Wenn dieser Datenverkehr vollständig im Cache gespeichert wird, ergeben sich in einer Stunde 450 MB. Dadurch würden bei 8 Arbeitsstunden 3,6 GB an einem einzigen Tag erreicht. Da normalerweise nicht das gesamte Volumen der Verbindung ausgeschöpft wird, kann angenommen werden, dass das Gesamtdatenvolumen, das auf den Cache zukommt, bei etwa 2 GB liegt. Daher sind bei diesem Beispiel 2 GB Festplattenspeicher erforderlich, damit Squid die durchsuchten Daten eines Tags im Cache speichern kann.

42.2.3 RAM

Der von Squid benötigte Arbeitsspeicher (RAM) steht in direktem Verhältnis zur Anzahl der Objekte im Cache. Außerdem speichert Squid Cache-Objekt-Bezüge und häufig angeforderte Objekte im Hauptspeicher, um das Abrufen dieser Daten zu beschleunigen. RAM ist wesentlich schneller als eine Festplatte.

Außerdem gibt es andere Daten, die Squid im Arbeitsspeicher benötigt, beispielsweise eine Tabelle mit allen IP-Adressen, einen exakten Domännennamen-Cache, die am häufigsten angeforderten Objekte, Zugriffssteuerungslisten, Puffer usw.

Es ist sehr wichtig, dass genügend Arbeitsspeicher für den Squid-Vorgang zur Verfügung steht, da die Systemleistung erheblich eingeschränkt ist, wenn ein Wechsel auf die Festplatte erforderlich ist. Das Werkzeug `cachemgr.cgi` kann für die Arbeitsspeicherverwaltung des Cache verwendet werden. Dieses Werkzeug wird in [Abschnitt 42.6](#), „`cachemgr.cgi`“ (S. 873) behandelt. Bei Sites mit extrem hohem Netzwerkverkehr sollte die Verwendung eines AMD64- oder Intel EM64T-Systems mit mehr als 4 GB Arbeitsspeicher in Erwägung gezogen werden.

42.2.4 CPU

Die Verwendung von Squid bringt keine intensive CPU-Auslastung mit sich. Die Prozessorlast wird nur erhöht, während die Inhalte des Cache geladen oder überprüft werden. Durch die Verwendung eines Computers mit mehreren Prozessoren wird die System-

leistung nicht erhöht. Um die Effizienz zu steigern, sollten vielmehr schnellere Festplatten oder ein größerer Arbeitsspeicher verwendet werden.

42.3 Starten von Squid

Squid ist in SUSE® Linux Enterprise Server bereits vorkonfiguriert. Sie können das Programm unmittelbar nach der Installation starten. Um einen reibungslosen Start zu gewährleisten, sollte das Netzwerk so konfiguriert werden, dass mindestens ein Namensserver und das Internet erreicht werden können. Es können Probleme auftreten, wenn eine Einwahlverbindung zusammen mit einer dynamischen DNS-Konfiguration verwendet wird. In diesem Fall sollte zumindest der Namensserver eingegeben werden, da Squid nicht startet, wenn kein DNS-Server in `/etc/resolv.conf` gefunden wird.

42.3.1 Befehle zum Starten und Stoppen von Squid

Geben Sie zum Starten von Squid als `root` in der Kommandozeile den Befehl `rcsquid start` ein. Beim ersten Start muss zunächst die Verzeichnisstruktur des Cache in `/var/cache/squid` definiert werden. Dies geschieht automatisch über das Startskript `/etc/init.d/squid` und kann einige Sekunden oder sogar Minuten in Anspruch nehmen. Wenn rechts in grüner Schrift `done` angezeigt wird, wurde Squid erfolgreich geladen. Um die Funktionsfähigkeit von Squid im lokalen System zu testen, geben Sie `localhost` als Proxy und `3128` als Port im Browser an.

Um Benutzern aus dem lokalen System und anderen Systemen den Zugriff auf Squid und das Internet zu ermöglichen, müssen Sie den Eintrag in den Konfigurationsdateien `/etc/squid/squid.conf` von `http_access deny all` in `http_access allow all` ändern. Beachten Sie dabei jedoch, dass dadurch jedem der vollständige Zugriff auf Squid ermöglicht wird. Daher sollten Sie ACLs definieren, die den Zugriff auf den Proxy steuern. Weitere Informationen hierzu finden Sie in [Abschnitt 42.4.2](#), „Optionen für die Zugriffssteuerung“ (S. 868).

Nach der Bearbeitung der Konfigurationsdatei `/etc/squid/squid.conf` muss Squid die Konfigurationsdatei erneut laden. Verwenden Sie hierfür `rcsquid reload`.

Alternativ können Sie mit `rcsquid restart` einen vollständigen Neustart von Squid durchführen.

Mit dem Befehl `rcsquid status` kann überprüft werden, ob der Proxy ausgeführt wird. Mit dem Befehl `rcsquid stop` wird Squid heruntergefahren. Dieser Vorgang kann einige Zeit in Anspruch nehmen, da Squid bis zu einer halben Minute (Option `shutdown_lifetime` in `/etc/squid/squid.conf`) wartet, bevor es die Verbindungen zu den Clients trennt und seine Daten auf die Festplatte schreibt.

WARNUNG: Beenden von Squid

Das Beenden von Squid mit `kill` oder `killall` kann zur Beschädigung des Cache führen. Damit Squid neu gestartet werden kann, muss der beschädigte Cache gelöscht werden.

Wenn Squid nach kurzer Zeit nicht mehr funktioniert, obwohl das Programm erfolgreich gestartet wurde, überprüfen Sie, ob ein fehlerhafter Namenservereintrag vorliegt oder ob die Datei `/etc/resolv.conf` fehlt. Squid protokolliert die Ursache eines Startfehlers in der Datei `/var/log/squid/cache.log`. Wenn Squid beim Booten des Systems automatisch geladen werden soll, müssen Sie Squid mithilfe des YaST-Runlevel-Editors für die gewünschten Runlevels aktivieren. Siehe [Abschnitt 7.5.13](#), „Systemdienste (Runlevel)“ (S. 183).

Durch eine Deinstallation von Squid werden weder die Cache-Hierarchie noch die Protokolldateien entfernt. Um diese zu entfernen, müssen Sie das Verzeichnis `/var/cache/squid` manuell löschen.

42.3.2 Lokaler DNS-Server

Die Einrichtung eines lokalen DNS-Servers ist sinnvoll, selbst wenn er nicht seine eigene Domäne verwaltet. Er fungiert dann einfach als Nur-Cache-Namenserver und kann außerdem DNS-Anforderungen über die Root-Namenserver auflösen, ohne dass irgendeine spezielle Konfiguration erforderlich ist (siehe [Abschnitt 34.3](#), „Starten des Namensservers BIND“ (S. 692)). Wie dies durchgeführt werden kann, hängt davon ab, ob Sie bei der Konfiguration der Internetverbindung dynamisches DNS auswählen.

Dynamisches DNS

Normalerweise wird bei dynamischem DNS der DNS-Server während des Aufbaus der Internetverbindung vom Anbieter festgelegt und die lokale Datei `/etc/`

`resolv.conf` wird automatisch angepasst. Dieses Verhalten wird in der Datei `/etc/sysconfig/network/config` mit der `sysconfig`-Variablen `MODIFY_RESOLV_CONF_DYNAMICALLY` gesteuert, die auf `"yes"` gesetzt ist. Setzen Sie diese Variable mit dem `sysconfig`-Editor von YaST auf `"no"` (siehe [Abschnitt 20.3.1](#), „Ändern der Systemkonfiguration mithilfe des YaST-Editors `"sysconfig"`“ (S. 434)). Geben Sie anschließend den lokalen DNS-Server in die Datei `/etc/resolv.conf` ein. Verwenden Sie die IP-Adresse `127.0.0.1` für `localhost`. Auf diese Weise kann Squid immer den lokalen Namensserver finden, wenn er gestartet wird.

Um den Zugriff auf den Namensserver des Anbieters zu ermöglichen, geben Sie ihn zusammen mit seiner IP-Adresse in die Konfigurationsdatei `/etc/named.conf` unter `forwarders` ein. Mit dynamischem DNS kann dies automatisch während des Verbindungsaufbaus erreicht werden, indem die `sysconfig`-Variable `MODIFY_NAMED_CONF_DYNAMICALLY` auf `YES` gesetzt wird.

Statisches DNS

Beim statischen DNS finden beim Verbindungsaufbau keine automatischen DNS-Anpassungen statt, sodass auch keine `sysconfig`-Variablen geändert werden müssen. Sie müssen jedoch den lokalen DNS-Server in die Datei `/etc/resolv.conf` eingeben, wie oben beschrieben. Außerdem muss der statische Namensserver des Anbieters zusammen mit seiner IP-Adresse manuell in die Datei `/etc/named.conf` unter `forwarders` eingegeben werden.

TIPP: DNS und Firewall

Wenn eine Firewall ausgeführt wird, müssen Sie sicherstellen, dass DNS-Anforderungen durchgelassen werden.

42.4 Die Konfigurationsdatei `/etc/squid/squid.conf`

Alle Einstellungen für den Squid-Proxyserver werden in der Datei `/etc/squid/squid.conf` vorgenommen. Beim ersten Start von Squid sind keine Änderungen in dieser Datei erforderlich, externen Clients wird jedoch ursprünglich der Zugriff verweigert. Der Proxy ist für `localhost` verfügbar. Der Standardport ist 3128. Die vorinstallierte Konfigurationsdatei `/etc/squid/squid.conf` bietet detaillierte

Informationen zu den Optionen sowie zahlreiche Beispiele. Fast alle Einträge beginnen mit # (kommentierte Zeilen) und die relevanten Spezifikationen befinden sich am Ende der Zeile. Die angegebenen Werte korrelieren fast immer mit den Standardwerten, sodass das Entfernen der Kommentarzeichen ohne Ändern der Parameter in den meisten Fällen kaum Auswirkungen hat. Lassen Sie die Beispiele nach Möglichkeit unverändert und geben Sie die Optionen zusammen mit den geänderten Parametern in der Zeile darunter ein. Auf diese Weise können die Standardwerte problemlos wiederhergestellt und mit den Änderungen verglichen werden.

TIPP: Anpassen der Konfigurationsdatei nach einer Aktualisierung

Wenn Sie eine Aktualisierung einer früheren Squid-Version durchgeführt haben, sollten Sie die neue Datei `/etc/squid/squid.conf` bearbeiten und nur die in der vorherigen Datei vorgenommenen Änderungen übernehmen. Wenn Sie versuchen, die alte `squid.conf` zu verwenden, besteht das Risiko, dass die Konfiguration nicht mehr funktioniert, da die Optionen manchmal bearbeitet und neue Änderungen hinzugefügt werden.

42.4.1 Allgemeine Konfigurationsoptionen (Auswahl)

`http_port 3128`

Dies ist der Port, den Squid auf Client-Anforderungen überwacht. Der Standardport ist 3128, 8080 wird jedoch ebenfalls häufig verwendet. Sie können auch mehrere Portnummern durch Leerzeichen getrennt eingeben.

`cache_peer hostname type proxy-port icp-port`

Geben Sie hier einen übergeordneten Proxy ein, beispielsweise wenn Sie den Proxy Ihres ISP verwenden möchten. Geben Sie als `hostname` den Namen und die IP-Adresse des zu verwendenden Proxy und als `type parent` ein. Geben Sie als `proxy-port` die Portnummer ein, die ebenfalls vom Operator des Parent für die Verwendung im Browser angegeben wurde, in der Regel 8080. Setzen Sie `icp-port` auf 7 oder 0, wenn der ICP-Port des übergeordneten Proxy nicht bekannt ist und seine Verwendung für den Anbieter nicht wichtig ist. Außerdem können `default` und `no-query` nach den Portnummern angegeben werden, um die Verwendung des ICP-Protokolls zu verhindern. Squid verhält sich dann in Bezug auf den Proxy des Anbieters wie ein normaler Browser.

`cache_mem 8 MB`

Dieser Eintrag legt fest, wie viel Arbeitsspeicher Squid für besonders beliebte Antworten verwenden kann. Der Standardwert ist 8 MB. Dieser Wert gibt nicht die Arbeitsspeichernutzung von Squid an und kann überschritten werden.

`cache_dir ufs /var/cache/squid/ 100 16 256`

Der Eintrag `cache_dir` legt das Verzeichnis fest, in dem alle Objekte auf dem Datenträger gespeichert werden. Die Zahlen am Ende geben den maximal zu verwendenden Festplattenspeicher in MB und die Anzahl der Verzeichnisse auf der ersten und zweiten Ebene an. Der Parameter `ufs` sollte nicht geändert werden. Standardmäßig werden 100 MB Speicherplatz im Verzeichnis `/var/cache/squid` belegt und 16 Unterverzeichnisse erstellt, die wiederum jeweils 256 Unterverzeichnisse aufweisen. Achten Sie bei der Angabe des zu verwendenden Speicherplatzes darauf, genügend Reserve einzuplanen. Werte von mindestens 50 bis maximal 80 % des verfügbaren Speicherplatzes erscheinen hier am sinnvollsten. Die letzten beiden Werte für die Verzeichnisse sollten nur nach reiflicher Überlegung erhöht werden, da zu viele Verzeichnisse ebenfalls zu Leistungsproblemen führen können. Wenn der Cache von mehreren Datenträgern gemeinsam verwendet wird, müssen Sie mehrere `cache_dir`-Zeilen eingeben.

`cache_access_log /var/log/squid/access.log, cache_log /var/log/squid/cache.log,`
`cache_store_log /var/log/squid/store.log`

Diese drei Einträge geben die Pfade an, unter denen Squid alle Aktionen protokolliert. Normalerweise werden hier keine Änderungen vorgenommen. Bei hoher Auslastung von Squid kann es sinnvoll sein, Cache und Protokolldateien auf mehrere Datenträger zu verteilen.

`emulate_htpdd_log off`

Wenn der Eintrag auf `on` gesetzt ist, erhalten Sie lesbare Protokolldateien. Einige Evaluierungsprogramme können solche Dateien jedoch nicht interpretieren.

`client_netmask 255.255.255.255`

Mit diesem Eintrag werden die IP-Adressen von Clients in den Protokolldateien maskiert. Die letzte Ziffer der IP-Adresse wird auf 0 gesetzt, wenn Sie hier `255.255.255.0` eingeben. Auf diese Weise können Sie den Datenschutz für die Clients gewährleisten.

`ftp_user Squid@`

Mit dieser Option wird das Passwort festgelegt, das Squid für die anonyme FTP-Anmeldung verwenden soll. Es kann sinnvoll sein, hier eine gültige E-Mail-Adresse anzugeben, da einige FTP-Server die Adressen auf Gültigkeit prüfen.

`cache_mgr webmaster`

Eine E-Mail-Adresse, an die Squid eine Meldung sendet, wenn es plötzlich abstürzt. Der Standardwert ist *webmaster*.

`logfile_rotate 0`

Bei Ausführung von `squid -k rotate` kann Squid ein Rotationssystem für gesicherte Protokolldateien einführen. Bei diesem Prozess werden die Dateien nummeriert und nach dem Erreichen des angegebenen Werts wird die älteste Datei überschrieben. Der Standardwert ist 0, da das Archivieren und Löschen von Protokolldateien in SUSE Linux Enterprise Server von einem in der Konfigurationsdatei `/etc/logrotate/squid` festgelegten Cronjob durchgeführt wird.

`append_domain <Domaene>`

Mit *append_domain* können Sie angeben, welche Domäne automatisch angefügt wird, wenn keine angegeben wurde. Normalerweise wird hier die eigene Domäne angegeben, sodass bei der Eingabe von *www* im Browser ein Zugriff auf Ihren eigenen Webserver erfolgt.

`forwarded_for on`

Wenn Sie den Eintrag auf *off* setzen, entfernt Squid die IP-Adresse und den Systemnamen des Client aus den HTTP-Anforderungen. Anderenfalls wird eine Zeile zum Header hinzugefügt, beispielsweise:

```
X-Forwarded-For: 192.168.0.0
```

`negative_ttl 5 minutes; negative_dns_ttl 5 minutes`

Die hier angegebenen Werte müssen in der Regel nicht geändert werden. Bei einer Einwahlverbindung kann das Internet jedoch zeitweise nicht verfügbar sein. Squid protokolliert die nicht erfolgreichen Anforderungen und lässt dann keine weiteren zu, auch wenn die Internetverbindung zwischenzeitlich wieder hergestellt wurde. In solchen Fällen sollten Sie *minutes* in *seconds* ändern. Danach sollte nach dem Klicken auf *Neu laden* im Browser der Einwahlvorgang nach wenigen Sekunden wieder aktiviert werden.

`never_direct allow ACL-Name`

Um zu verhindern, dass Squid Anforderungen direkt aus dem Internet entgegennimmt, müssen Sie mit dem oben stehenden Befehl die Verbindung mit einem anderen Proxy erzwingen. Dieser muss zuvor unter *cache_peer* eingegeben worden sein. Wenn als *ACL-Name* `all` angegeben wird, werden alle Anforderungen zwangsweise direkt an den übergeordneten Proxy (*parent*) weitergeleitet. Dies kann beispielsweise dann erforderlich sein, wenn Sie einen Anbieter verwenden, der die Verwendung der eigenen Proxies strikt vorschreibt oder der durch seine Firewall direkten Internetzugriff verweigert.

42.4.2 Optionen für die Zugriffssteuerung

Squid bietet ein detailliertes System für die Steuerung des Zugriffs auf den Proxy. Durch die Implementierung von ACLs kann es problemlos und umfassend konfiguriert werden. Dazu gehören Listen mit Regeln, die nacheinander verarbeitet werden. Die ACLs müssen zuerst definiert werden, bevor sie verwendet werden können. Einige Standard-ACLs, wie beispielsweise *all* und *localhost*, sind bereits vorhanden. Die bloße Definition einer ACL bedeutet jedoch noch nicht, dass sie tatsächlich angewendet wird. Dies geschieht nur in Verbindung mit *http_access*-Regeln.

`acl <ACL-Name> <Typ> <Daten>`

Für die Definition einer ACL sind mindestens drei Spezifikationen erforderlich. Der Name *<ACL-Name>* kann frei gewählt werden. Als *<Typ>* können Sie aus einer Vielzahl verschiedener Optionen wählen, die Sie im Abschnitt *ACCESS CONTROLS* in der Datei `/etc/squid/squid.conf` finden. Die Spezifikation für *<Daten>* hängt vom einzelnen ACL-Typ ab und kann auch aus einer Datei gelesen werden, beispielsweise über Hostnamen, IP-Adressen oder URLs. Im Folgenden finden Sie einige einfache Beispiele:

```
acl mysurfers srcdomain .my-domain.com
acl teachers src 192.168.1.0/255.255.255.0
acl students src 192.168.7.0-192.168.9.0/255.255.255.0
acl lunch time MTWHF 12:00-15:00
```

`http_access allow <ACL-Name>`

http_access legt fest, wer den Proxy verwenden kann und wer auf welche Seiten im Internet zugreifen kann. Hierfür müssen ACLs angegeben werden. *localhost* und *all* wurden bereits oben definiert. Diese Optionen können den Zugriff über *deny* bzw. *allow* verweigern bzw. zulassen. Es können Listen mit einer beliebigen Anzahl von *http_access*-Einträgen erstellt und von oben nach unten verarbeitet

werden. Je nachdem, was zuerst vorkommt, wird der Zugriff auf die betreffende URL gestattet oder verweigert. Der letzte Eintrag sollte immer *http_access deny all* lauten. Im folgenden Beispiel hat *localhost* freien Zugriff auf alle Elemente, während allen anderen Hosts der Zugriff vollständig verweigert wird.

```
http_access allow localhost
http_access deny all
```

In einem anderen Beispiel, bei dem diese Regeln verwendet werden, hat die Gruppe *teachers* immer Zugriff auf das Internet. Die Gruppe *students* erhält nur montags bis freitags während der Mittagspause Zugriff.

```
http_access deny localhost
http_access allow teachers
http_access allow students lunch time
http_access deny all
```

Die Liste mit den *http_access*-Einträgen sollte um der besseren Lesbarkeit willen nur an der angegebenen Position in der Datei `/etc/squid/squid.conf` eingegeben werden. Also zwischen dem Text

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

und dem letzten

```
http_access deny all
```

`redirect_program /usr/bin/squidGuard`

Mit dieser Option können Sie eine Umleitungsfunktion, wie beispielsweise *squidGuard*, angeben, die das Blockieren unerwünschter URLs ermöglicht. Der Internetzugang kann mithilfe der Proxy-Authentifizierung und der entsprechenden ACLs individuell für verschiedene Benutzergruppen gesteuert werden. *squidGuard* ist ein gesondertes Paket, das installiert und konfiguriert werden kann.

`auth_param basic program /usr/sbin/pam_auth`

Wenn die Benutzer auf dem Proxy authentifiziert werden müssen, geben Sie ein entsprechendes Programm an, beispielsweise *pam_auth*. Beim ersten Zugriff auf *pam_auth* wird dem Benutzer ein Anmeldefenster angezeigt, in das er den Benutzernamen und das Passwort eingeben muss. Außerdem ist noch immer eine ACL erforderlich, sodass nur Clients mit einer gültigen Anmeldung das Internet benutzen können.

```
acl password proxy_auth REQUIRED
```

```
http_access allow password
http_access deny all
```

Das *REQUIRED* nach *proxy_auth* kann durch eine Liste der zulässigen Benutzernamen oder durch den Pfad zu einer solchen Liste ersetzt werden.

```
ident_lookup_access allow <ACL-Name>
```

Lassen Sie damit eine ident-Anforderung für alle ACL-definierten Clients ausführen, um die Identität der einzelnen Benutzer zu ermitteln. Wenn Sie *all* auf *<ACL-Name>* anwenden, gilt dies für alle Clients. Außerdem muss ein ident-Daemon auf allen Clients ausgeführt werden. Bei Linux installieren Sie für diesen Zweck das Paket "pidentd". Für Microsoft Windows steht kostenlose Software zum Herunterladen aus dem Internet zur Verfügung. Um sicherzustellen, dass nur Clients mit einem erfolgreichen ident-Lookup zulässig sind, definieren Sie hier eine entsprechende ACL:

```
acl idenhosts ident REQUIRED

http_access allow idenhosts
http_access deny all
```

Ersetzen Sie auch hier *REQUIRED* durch eine Liste der zulässigen Benutzernamen. Durch die Verwendung von *ident* kann die Zugriffszeit erheblich reduziert werden, da die ident-Lookups für jede Anforderung wiederholt werden.

42.5 Konfigurieren eines transparenten Proxy

Normalerweise läuft die Arbeit mit Proxyservern folgendermaßen ab: Der Webbrowser sendet Anforderungen an einen bestimmten Port im Proxyserver und der Proxy stellt die angeforderten Objekte bereit, unabhängig davon, ob sie sich in seinem Cache befinden oder nicht. Bei der Arbeit in einem Netzwerk können verschiedene Situationen entstehen:

- Aus Sicherheitsgründen sollten alle Clients einen Proxy für den Zugriff auf das Internet verwenden.
- Alle Clients müssen einen Proxy verwenden, unabhängig davon, ob sie sich dessen bewusst sind.

- Der Proxy in einem Netzwerk wird verschoben, die vorhandenen Clients sollten jedoch ihre alte Konfiguration beibehalten.

In all diesen Fällen kann ein transparenter Proxy verwendet werden. Das Prinzip ist extrem einfach: Der Proxy fängt die Anforderungen des Webbrowsers ab und beantwortet sie, sodass der Webbrowser die angeforderten Seiten erhält, ohne dass bekannt ist, woher sie kommen. Wie der Name schon andeutet, verläuft der gesamte Prozess transparent.

42.5.1 Konfigurationsoptionen in `/etc/squid/squid.conf`

Folgende Optionen müssen in der Datei `/etc/squid/squid.conf` aktiviert werden, um den transparenten Proxy in Betrieb zu nehmen:

- `httpd_accel_host virtual`
- `httpd_accel_port 80`

Die Portnummer des eigentlichen HTTP-Servers

- `httpd_accel_with_proxy on`
- `httpd_accel_uses_host_header on`

42.5.2 Firewall-Konfiguration mit SuSEfirewall2

Leiten Sie nun alle eingehenden Anforderungen über die Firewall mithilfe einer Port-Weiterleitungsregel an den Squid-Port um. Verwenden Sie dazu das eingeschlossene Werkzeug `SuSEfirewall2` (in [Abschnitt 44.4.1](#), „Konfigurieren der Firewall mit YaST“ (S. 906) beschrieben). Die Konfigurationsdatei dieses Programms finden Sie in `/etc/sysconfig/SuSEfirewall2`. Die Konfigurationsdatei besteht aus gut dokumentierten Einträgen. Um einen transparenten Proxy festzulegen, müssen Sie mehrere Firewall-Optionen konfigurieren:

- Gerät, das auf das Internet verweist: `FW_DEV_EXT="eth1"`

- Gerät, das auf das Netzwerk verweist: `FW_DEV_INT="eth0"`

Ports und Dienste (siehe `/etc/services`) auf der Firewall definieren, auf die ein Zugriff von nicht verbürgten (externen) Netzwerken, wie beispielsweise dem Internet, erfolgt. In diesem Beispiel werden nur Webdienste für den Außenbereich angeboten:

```
FW_SERVICES_EXT_TCP="www"
```

Definieren Sie Ports und Dienste (siehe `/etc/services`) auf der Firewall, auf die vom sicheren (internen) Netzwerk aus zugegriffen wird (sowohl über TCP als auch über UDP):

```
FW_SERVICES_INT_TCP="domain www 3128"
FW_SERVICES_INT_UDP="domain"
```

Dies ermöglicht den Zugriff auf Webdienste und Squid (Standardport: 3128). Der Dienst "domain" steht für DNS (Domain Name Service, Domännennamen-Dienst). Dieser Dienst wird häufig verwendet. Andernfalls nehmen Sie einfach die oben stehenden Einträge heraus und setzen Sie die folgende Option auf `no`:

```
FW_SERVICE_DNS="yes"
```

Die wichtigste Option ist Option Nummer 15:

Beispiel 42.1 *Firewall-Konfiguration: Option 15*

```
# 15.)
# Which accesses to services should be redirected to a local port
# on the firewall machine?
#
# This can be used to force all internal users to surf via your
# Squid proxy, or transparently redirect incoming Web traffic to
# a secure Web server.
#
# Choice: leave empty or use the following explained syntax of
# redirecting rules, separated with spaces.
# A redirecting rule consists of 1) source IP/net,
# 2) destination IP/net, 3) original destination port and
# 4) local port to redirect the traffic to, separated by a colon,
# e.g. "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
```

Die oben angegebenen Kommentare geben die zu verwendende Syntax an. Geben Sie zuerst die IP-Adresse und die Netzmaske der internen Netzwerke ein, die auf die Proxy-Firewall zugreifen. Geben Sie als Zweites die IP-Adresse und die Netzmaske ein, an die diese Clients ihre Anforderungen senden. Geben Sie bei Webbrowsern die Netzwerke `0/0` an. Dieser Platzhalter bedeutet "überallhin". Geben Sie anschließend den ursprünglichen Port ein, an den diese Anforderungen gesendet werden, und schließlich

den Port, an den alle diese Anforderungen umgeleitet werden. Da Squid andere Protokolle als HTTP unterstützt, müssen Anforderungen von anderen Ports an den Proxy umgeleitet werden, beispielsweise FTP (Port 21), HTTPS oder SSL (Port 443). In diesem Beispiel werden Webdienste (Port 80) an den Proxy-Port (Port 3128) umgeleitet. Wenn mehrere Netzwerke bzw. Dienste hinzugefügt werden sollen, müssen diese im entsprechenden Eintrag durch ein Leerzeichen getrennt sein.

```
FW_REDIRECT_TCP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"  
FW_REDIRECT_UDP="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"
```

Um die Firewall mit der neuen Konfiguration zu starten, müssen Sie einen Eintrag in der Datei `/etc/sysconfig/SuSEfirewall2` ändern. Der Eintrag `START_FW` muss auf `"yes"` gesetzt werden.

Starten Sie Squid, wie in [Abschnitt 42.3, „Starten von Squid“](#) (S. 862) gezeigt. Um zu überprüfen, ob alles ordnungsgemäß funktioniert, müssen Sie die Squid-Protokolle in `/var/log/squid/access.log` überprüfen. Um sicherzustellen, dass alle Ports korrekt konfiguriert sind, müssen Sie eine Portabsuche auf dem Computer von einem beliebigen Computer außerhalb Ihres Netzwerks aus durchführen. Nur die Webdienste (Port 80) sollten verfügbar sein. Die Befehlssyntax für das Absuchen der Ports mit `nmap` lautet `nmap -O IP_address`.

42.6 cachemgr.cgi

Der Cache-Manager (`cachemgr.cgi`) ist ein CGI-Dienstprogramm für die Anzeige der Statistiken zur Arbeitsspeichernutzung eines laufenden Squid-Prozesses. Außerdem bietet er eine bequemere Methode zur Verwaltung des Cache und zur Anzeige der Statistiken ohne Anmeldung beim Server.

42.6.1 Setup

Zunächst muss ein Webserver in Ihrem System ausgeführt werden. Konfigurieren Sie Apache, wie in [Kapitel 41, *Der HTTP-Server Apache*](#) (S. 811) beschrieben. Um zu überprüfen, ob Apache bereits ausgeführt wird, geben Sie als `root` den Befehl `rcapache status` ein. Wenn eine Meldung der folgenden Art angezeigt wird:

```
Checking for service httpd: OK  
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

wird Apache auf dem Rechner angezeigt. Andernfalls geben Sie `rcapache start` ein, um Apache mit den Standardeinstellungen von SUSE Linux Enterprise Server zu starten. Der letzte Schritt besteht darin, die Datei `cachemgr.cgi` in das Apache-Verzeichnis `cgi-bin` zu kopieren:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi /srv/www/cgi-bin/
```

42.6.2 Cache-Manager-ACLs in `/etc/squid/squid.conf`

Es gibt einige Standardeinstellungen in der Originaldatei, die für den Cache-Manager erforderlich sind. Zuerst werden zwei ACLs definiert. Anschließend verwenden die `http_access`-Optionen diese ACLs, um Zugriff vom CGI-Script auf Squid zu gewähren. Die erste ACL ist die wichtigste, da der Cache-Manager versucht, über das `cache_object`-Protokoll mit Squid zu kommunizieren.

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Folgende Regeln gewähren Apache Zugriffsrechte auf Squid:

```
http_access allow manager localhost
http_access deny manager
```

Diese Regeln setzen voraus, dass der Webserver und Squid auf demselben Computer ausgeführt werden. Wenn die Kommunikation zwischen Cache-Manager und Squid von dem Webserver auf einem anderen Computer ihren Ausgang nimmt, müssen Sie eine zusätzliche ACL aufnehmen, wie in [Beispiel 42.2](#), „Zugriffsregeln“ (S. 874) beschrieben.

Beispiel 42.2 *Zugriffsregeln*

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # webserver IP
```

Fügen Sie dann die Regeln in [Beispiel 42.3](#), „Zugriffsregeln“ (S. 874) hinzu, um den Zugriff vom Webserver zu gestatten.

Beispiel 42.3 *Zugriffsregeln*

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Konfigurieren Sie ein Passwort für den Manager für den Zugriff auf weitere Optionen, wie das Schließen des Cache über entfernten Zugriff oder die Anzeige weiterer Informationen zum Cache. Konfigurieren Sie hierfür den Eintrag `cachemgr_passwd` mit einem Passwort für den Manager und der Liste der anzuzeigenden Optionen. Diese Liste wird als Teil des Eintragskommentars in `/etc/squid/squid.conf` angezeigt.

Starten Sie Squid nach jeder Änderung der Konfigurationsdatei neu. Verwenden Sie hierfür einfach `rcsquid reload`.

42.6.3 Anzeige der Statistiken

Rufen Sie die entsprechende Website auf: <http://webserver.example.org/cgi-bin/cachemgr.cgi>. Drücken Sie *continue* (Fortsetzen) und blättern Sie durch die verschiedenen Statistiken. Weitere Details für die einzelnen, vom Cache-Manager angezeigten Einträge finden Sie in den Squid FAQ unter <http://www.squid-cache.org/Doc/FAQ/FAQ-9.html>.

42.7 squidGuard

Dieser Abschnitt dient nicht zur Erläuterung einer umfassenden Konfiguration von squidGuard. Er soll lediglich eine Einführung und einige Hinweise für die Verwendung bieten: Eine Behandlung tiefer gehender Konfigurationsfragen finden Sie auf der squidGuard-Website unter <http://www.squidguard.org>.

squidGuard ist ein kostenloses (GPL), flexibles und schnelles Filter-, Umleitungs- und Zugriffssteuerungs-Plugin für Squid. Damit können Sie mehrere Zugriffsregeln mit verschiedenen Einschränkungen für verschiedene Benutzergruppen in einem Squid-Cache erstellen. squidGuard verwendet die Standard-Umleitungsschnittstelle von Squid und bietet folgende Möglichkeiten:

- Einschränken des Webzugriffs für einige Benutzer auf eine Liste akzeptierter oder gut bekannter Webserver bzw. URLs.
- Blockieren des Zugriffs auf einige gelistete oder in einer Blacklist stehende Webserver bzw. URLs für einige Benutzer.
- Blockieren des Zugriffs bestimmter Benutzer auf URLs, die reguläre Ausdrücke oder Wörter aus einer entsprechenden Liste enthalten.

- Umleiten blockierter URLs an eine "intelligente" CGI-basierte Informationsseite.
- Umleiten nicht registrierter Benutzer zu einem Registrierungsformular.
- Umleiten von Bannern in eine leere GIF-Datei.
- Verwenden verschiedener Zugriffsregeln je nach Tageszeit, Wochentag, Datum usw.
- Verwenden verschiedener Regeln für verschiedene Benutzergruppen.

squidGuard und Squid können nicht zu folgenden Zwecken eingesetzt werden:

- Bearbeiten, Filtern oder Zensieren von Text in Dokumenten.
- Bearbeiten, Filtern oder Zensieren von in HTML eingebetteten Skriptsprachen, wie JavaScript oder VBscript.

Vor der Verwendung muss squidGuard zunächst installiert werden. Geben Sie eine Datei mit der Minimalkonfiguration als `/etc/squidguard.conf` an. Konfigurationsbeispiele finden Sie unter <http://www.squidguard.org/config/>. Später können Sie mit komplizierteren Konfigurationseinstellungen experimentieren.

Erstellen Sie als Nächstes eine Dummy-Seite mit "Zugriff verweigert" oder eine mehr oder weniger komplexe CGI-Seite, um Squid umzuleiten, wenn der Client eine Website anfordert, die auf der schwarzen Liste steht. Die Verwendung von Apache wird dringend empfohlen.

Konfigurieren Sie nun Squid für die Verwendung von squidGuard. Verwenden Sie folgenden Eintrag in der Datei `/etc/squid/squid.conf`:

```
redirect_program /usr/bin/squidGuard
```

Eine weitere Option, `redirect_children`, dient zur Konfiguration der Anzahl der "Umleitungs"-Prozesse (in diesem Fall squidGuard-Prozesse), die auf dem Computer ausgeführt werden. squidGuard ist schnell genug, um mit einer großen Anzahl von Anforderungen umgehen zu können: Bei einem Pentium-Prozessor mit 500 MHz, 5.900 Domänen und 7.880 URLs (insgesamt 13.780) können 100.000 Anforderungen innerhalb von 10 Sekunden verarbeitet werden. Daher wird nicht empfohlen, mehr als vier Prozesse festzulegen, da die Zuordnung dieser Prozesse übermäßig viel Speicher verbrauchen würde.

```
redirect_children 4
```


Lassen Sie Squid abschließend die neue Konfiguration laden, indem Sie `rcsquid reload` ausführen. Testen Sie nun Ihre Einstellungen mit einem Browser.

42.8 Erstellung von Cache-Berichten mit Calamaris

Calamaris ist ein Perl-Skript, mit dem Berichte über die Cache-Aktivität im ASCII- oder HTML-Format erstellt werden können. Es arbeitet mit nativen Squid-Zugriffsprotokolldateien. Die Calamaris-Homepage befindet sich unter <http://Calamaris.Cord.de/>. Das Programm ist recht benutzerfreundlich.

Melden Sie sich als `root` an und geben Sie `cat access.log.files | calamaris Optionen > reportfile` ein. Beim Piping mehrerer Protokolldateien ist darauf zu achten, dass die Protokolldateien chronologisch (die ältesten Dateien zuerst) geordnet sind. Im Folgenden finden Sie einige Optionen des Programms:

- a
Ausgabe aller verfügbaren Berichte
- w
Ausgabe als HTML-Bericht
- l
Einschließen einer Meldung oder eines Logos in den Berichtsheader

Weitere Informationen zu den verschiedenen Optionen finden Sie auf der Manualpage des Programms (`man calamaris`).

Typisches Beispiel:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \  
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

Dadurch wird der Bericht im Verzeichnis des Webservers gespeichert. Zur Anzeige des Berichts ist Apache erforderlich.

Ein weiteres leistungsstarkes Werkzeug zum Erstellen von Berichten ist SARG (Squid Analysis Report Generator). Weitere Informationen hierzu finden Sie unter: <http://sarg.sourceforge.net/>.

42.9 Weitere Informationen

Besuchen Sie die Squid-Homepage unter <http://www.squid-cache.org/>. Hier finden Sie das Squid-Benutzerhandbuch und eine umfassende Sammlung mit FAQ zu Squid.

Nach der Installation ist eine kleine HOWTO-Datei zu transparenten Proxies in `howtoenh` verfügbar: `/usr/share/doc/howto/en/txt/TransparentProxy.gz`. Außerdem sind Sie unter squid-users@squid-cache.org Mailinglisten zu Squid verfügbar. Das zugehörige Archiv finden Sie unter <http://www.squid-cache.org/mail-archive/squid-users/>.

Teil 5. Sicherheit

Verwalten der X.509-Zertifizierung

43

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 SUSE® Linux Enterprise Server stehen zwei YaST-Module für die Zertifizierung zur Verfügung, die grundlegende Verwaltungsfunktionen für digitale X.509-Zertifikate bieten. 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>.

43.1 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, auch *Schlüssel* genannt, verschlüsselt. Der Schlüssel wird in einem mathematischen Prozess auf die Benutzerd-

aten 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:

Privater Schlüssel

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.

43.1.1 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.

43.1.2 X.509-Zertifikate

Bei einem X.509-Zertifikat handelt es sich um eine Datenstruktur mit mehreren festen Feldern und optionalen zusätzlichen Erweiterungen. In den Textfeldern sind hauptsächlich der Name des Schlüsseleigentümers, der öffentliche Schlüssel und die Daten zur ausstellenden Zertifizierungsstelle (Name und Signatur) enthalten. 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 eine Erweiterung nur dann einstufen 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.

In [Tabelle 43.1](#) werden die Felder eines grundlegenden X.509-Zertifikats der Version 3 dargestellt.

Tabelle 43.1 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)
Erweiterungen	Optionale zusätzliche Informationen, wie „KeyUsage“ oder „BasicConstraints“.

43.1.3 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 43.2, „X.509-Zertifikatswiderrufsliste \(CRL\)“](#) (S. 885) werden die grundlegenden Bestandteile einer X.509-CRL dargestellt.

Tabelle 43.2 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 Veröfentlichers der CRL (in der Regel die ausstellende Zertifizierungsstelle)
This Update (Diese Aktualisierung)	Der Zeitpunkt der Veröffentlichung dieser CRL (Datum und Uhrzeit)
Next Update (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)
Erweiterungen	Optionale CRL-Erweiterungen

43.1.4 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 37, LDAP – Ein Verzeichnisdienst](#) (S. 735). [Kapitel 41, Der HTTP-Server Apache](#) (S. 811) enthält Informationen zu HTTP-Servern.

43.1.5 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 entsprechenden 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.

43.2 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.

43.2.1 Erstellen einer Stammzertifizierungsstelle

Der erste Schritt bei der Einrichtung einer PKI ist die Erstellung einer Stammzertifizierungsstelle. Gehen Sie in diesem Fall wie folgt vor:

- 1 Starten Sie YaST und wählen Sie *Sicherheit und Benutzer* → *CA Management* aus.
- 2 Klicken Sie auf *Root-CA erstellen*.
- 3 Geben Sie die Grunddaten für die Zertifizierungsstelle im ersten in [Abbildung 43.1](#), „YaST-CA-Modul – Grunddaten für eine Stammzertifizierungsstelle“ (S. 887) dargestellten Dialogfeld ein. Die Textfelder haben folgende Bedeutungen:

Abbildung 43.1 YaST-CA-Modul – Grunddaten für eine Stammzertifizierungsstelle

Zum Erzeugen einer neuen CA werden einige Einträge benötigt:

Dies hängt von der in der Konfigurationsdatei festgelegten Politik ab.

CA-Name ist der Name eines CA-Zertifikats. Verwenden Sie nur ASCII-Zeichen, "-" 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.

Erzeugen eines/r neuen Root CA (Schritt 1/3)

CA-Name: example-cert

Allgemeiner Name: example-ca

E-Mail-Adressen: cool@example.com

Eirma/Organisation: example organization

Abteilung: example

Ort:

Bundesland:

Land: Deutschland

Zurück Abbrechen Weiter

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.

Allgemeiner Name

Geben Sie den Namen ein, der für Verweise auf die Zertifizierungsstelle verwendet werden soll.

E-Mail-Adressen

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.

Firma/Organisation, Abteilung, Ort, Status

Optionale Werte

- 4 Klicken Sie auf *Weiter*.
- 5 Geben Sie im zweiten Dialogfeld ein Passwort ein. Das Passwort ist bei jeder Verwendung der Zertifizierungsstelle zum Erstellen einer untergeordneten Zertifizierungsstelle oder zum Generieren von Zertifikaten erforderlich. 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 3650 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 43.4](#), „*YaST-CA-Modul – Erweiterte Einstellungen*“ (S. 893)). 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.

43.2.2 Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle

Eine untergeordnete Zertifizierungsstelle wird auf dieselbe Weise erstellt wie eine Stammzertifizierungsstelle. Gehen Sie in diesem Fall 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*.

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. Die wichtigsten Informationen zur Zertifizierungsstelle werden in YaST auf der Registerkarte *Beschreibung* angezeigt (siehe [Abbildung 43.2](#)).

Abbildung 43.2 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 43.2.1, „Erstellen einer Stammzertifizierungsstelle“](#) (S. 886) fort.
- 6 Wählen Sie die Registerkarte *Zertifikate* aus. 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 43.2.5, „Erstellen von CRLs“](#) (S. 894) beschrieben.
- 7 Klicken Sie abschließend auf *OK*.

43.2.3 Erstellen oder Widerrufen von Benutzerzertifikaten

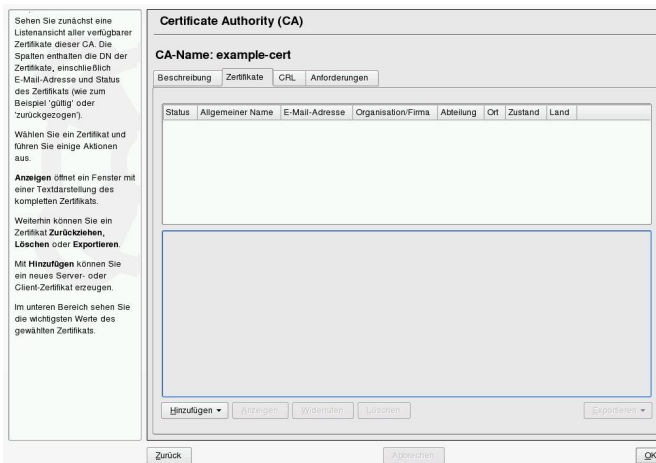
Die Erstellung von Client- und Server-Zertifikaten ähnelt der Erstellung des Zertifikats zum Erstellen von Zertifizierungsstellen in [Abschnitt 43.2.1, „Erstellen einer Stamm-](#)

zertifizierungsstelle“ (S. 886). 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. Die wichtigsten Informationen zur Zertifizierungsstelle werden in YaST auf der Registerkarte *Beschreibung* angezeigt.
- 4 Klicken Sie auf *Zertifikate* (siehe [Abbildung 43.3](#), „Zertifikate einer Zertifizierungsstelle“ (S. 891)).

Abbildung 43.3 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. Die wichtigsten Informationen zur Zertifizierungsstelle werden in YaST auf der Registerkarte *Beschreibung* angezeigt.
- 4 Klicken Sie auf *Zertifikate* (siehe [Abschnitt 43.2.2](#), „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“ (S. 889)).
- 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

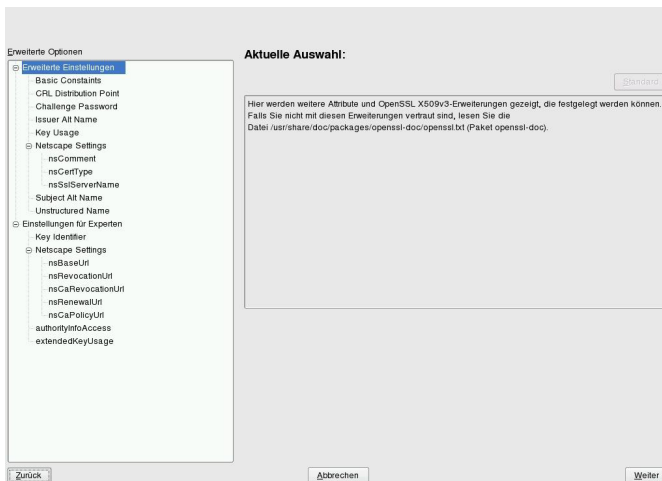
Ein Widerruf allein reicht zur Deaktivierung eines Zertifikats nicht aus. Widerrufene Zertifikate müssen zudem in einer CRL veröffentlicht werden. In [Abschnitt 43.2.5](#), „Erstellen von CRLs“ (S. 894) wird die Erstellung von CRLs erläutert. Nach der Veröffentlichung in einer CRL können widerrufene Zertifikate vollständig mit *Löschen* entfernt werden.

43.2.4 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 43.2.2](#), „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“ (S. 889) 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 43.4](#), „YaST-CA-Modul – Erweiterte Einstellungen“ (S. 893) gezeigte Dialogfeld zum Ändern der Standardeinstellungen geöffnet.

Abbildung 43.4 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.

43.2.5 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 43.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“](#) (S. 889) (für untergeordnete Zertifizierungsstellen) und in [Abschnitt 43.2.3, „Erstellen oder Widerrufen von Benutzerzertifikaten“](#) (S. 890) (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 43.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“](#) (S. 889) 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.

43.2.6 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 43.3](#), „Passwörter beim LDAP-Export“ (S. 895)).

Tabelle 43.3 *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 Zertifizierungsstelle zum Exportieren gemäß der Beschreibung in [Abschnitt 43.2.2, „Erstellen oder Widerrufen einer untergeordneten Zertifizierungsstelle“](#) (S. 889) ein. Wählen Sie im folgenden Dialogfeld die Optionsfolge *Erweitert* → *Nach LDAP exportieren* aus, 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 gegebenenfalls 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.

43.2.7 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.

Zertifikate, Zertifizierungsstellen und CRLs werden, wie in [Abschnitt 43.2.6, „Exportieren von Zertifizierungsstellenobjekten in LDAP“](#) (S. 895) beschrieben, auf dieselbe Weise als Datei exportiert wie in LDAP, mit der Ausnahme, dass Sie anstelle von *Nach LDAP exportieren* die Option *Als Datei exportieren* auswählen. 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.

43.2.8 Importieren von Common Server Certificates

Wenn Sie ein Server-Zertifikat über YaST auf Ihren Datenträger auf einem isolierten Zertifizierungsstellen-Verwaltungscomputer exportiert haben, können Sie das betreffende Zertifikat als *Common Server Certificate* auf einem 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 *Fertig stellen*.

Masquerading und Firewalls

Wann immer Linux in einer Netzwerkumgebung eingesetzt wird, können Sie die Kernel-Funktionen verwenden, mit denen Netzwerkpakete so bearbeitet werden können, dass zwischen internen und externen Netzwerkbereichen unterschieden wird. Das Linux-Netfilter-Framework ermöglicht die Einrichtung einer wirksamen Firewall, die die verschiedenen Netzwerke voneinander trennt. Mithilfe von iptables – einer generischen Tabellenstruktur für die Definition von Regelsätzen – können Sie präzise steuern, welche Pakete eine Netzwerkschnittstelle passieren dürfen. Ein derartiger Paketfilter kann schnell und einfach mithilfe von SuSEfirewall2 und dem entsprechenden YaST-Modul eingerichtet werden.

44.1 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.

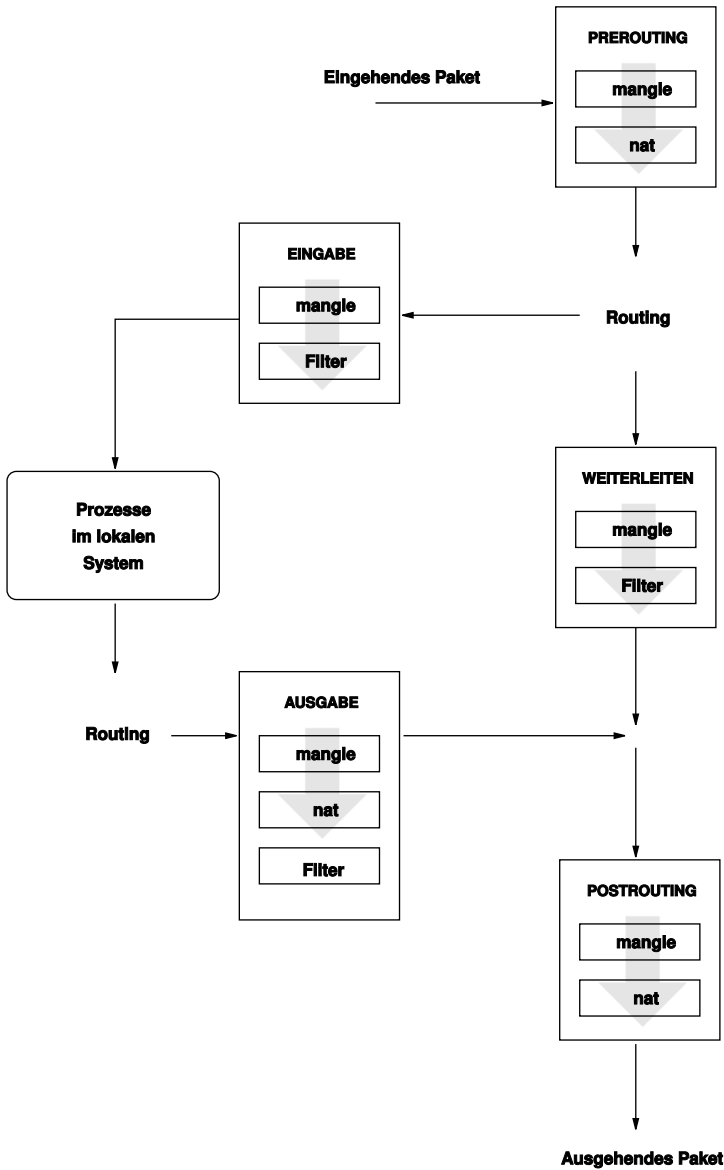
nat

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 44.1 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 44.1](#), „[iptables: Die möglichen Wege eines Pakets](#)“ (S. 901) 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.

44.2 Grundlegendes zum Masquerading

Masquerading ist der Linux-Spezialfall von NAT (Network Address Translation), der Übersetzung von Netzwerkadressen. Es kann verwendet werden, um ein kleines LAN (in dem die Hosts IP-Adressen aus dem privaten Bereich verwenden – siehe [Abschnitt 31.1.2](#), „[Netzmasken und Routing](#)“ (S. 609)) mit dem Internet (in dem offizielle IP-Adressen verwendet werden) 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 separate Schnittstelle für die 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 SUSE® Linux Enterprise ist diese Funktion in einer Standardinstallation 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 davon können bei einigen Anwendungsprotokollen, z. B. ICQ, `cucme`, IRC (DCC, CTCP) und FTP (im PORT-Modus) Probleme auftreten. Netscape, 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.

44.3 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 SUSE Linux Enterprise 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 Befehl `less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz`.

44.4 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 31.1.2, „Netzmasken und Routing“](#) (S. 609)) 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 44.4.1, „Konfigurieren der Firewall mit YaST“](#) (S. 906)). 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.

44.4.1 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*.

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 die Dienste nach Auswahl der gewünschten Zone in *Erlaubte Dienste für gewählte Zone*.

Masquerading

Mit der Masquerading-Funktionalität verbergen Sie das interne Netzwerk vor externen Netzwerken, z. B. dem Internet, und ermöglichen den Hosts im internen Netzwerk gleichzeitig den transparenten Zugriff auf das externe Netzwerk. Anforderungen vom externen an das interne Netzwerk werden blockiert. Anforderungen aus dem internen Netzwerk werden scheinbar vom Masquerading-Server ausgegeben, der extern sichtbar ist. Wenn dem externen Netzwerk spezielle Dienste eines internen Computers zur Verfügung gestellt werden sollen, fügen Sie für den Dienst eine spezielle Umadressierungsregel hinzu.

Broadcast

In diesem Dialogfeld konfigurieren Sie die UDP-Ports, die Broadcasts zulassen sollen. Fügen Sie die erforderlichen Nummern der Ports oder Dienste getrennt durch Leerzeichen für die entsprechende Zone hinzu. Weitere Informationen hierzu finden Sie in der Datei `/etc/services`.

Hier können Sie auch das Protokollieren von Broadcasts aktivieren, die nicht akzeptiert werden. Dies kann problematisch sein, da sich Windows-Hosts über Broadcasts miteinander bekannt machen und daher viele Pakete generieren, die nicht akzeptiert werden.

IPsec-Unterstützung

In diesem Dialogfeld konfigurieren Sie, ob dem externen Netzwerk der IPsec-Dienst zur Verfügung stehen soll. Unter *Details* konfigurieren Sie, welche Pakete als verbürgt angesehen werden sollen.

Protokollierungs-Level

Für die Protokollierung gibt es zwei Regeln: eine für akzeptierte und eine für 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.

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.

44.4.2 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 Ihren Runlevel (wahrscheinlich 3 oder 5). Dadurch werden symbolische Links für die SuSEfirewall2_*-Skripts 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. Geben Sie für eine ISDN-Verbindung `ipp0` ein. Für DSL-Verbindungen geben Sie `dsl0` ein. 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 zugewiesene IP-Adressen haben. 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 im Anschluss an die Konfiguration die Firewall. Die Firewall-Regeln 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-DEFAULT 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.

44.5 Weitere 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: Sicherer Netzwerkbetrieb

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. SUSE Linux Enterprise bietet SSH-Funktionen mit dem Paket `OpenSSH` an.

45.1 Das Paket OpenSSH

SUSE Linux Enterprise installiert das Paket OpenSSH standardmäßig. Daher stehen Ihnen die Programme `ssh`, `scp` und `sftp` als Alternative für `telnet`, `rlogin`, `rsh`, `rcp` und `ftp` zur Verfügung. In der Standardkonfiguration ist der Zugriff auf ein SUSE Linux Enterprise-System nur mit den OpenSSH-Dienstprogrammen möglich, und nur wenn dies die Firewall erlaubt.

45.2 Das ssh-Programm

Mit `ssh` können Sie Verbindung zu einem entfernten System aufnehmen und dort interaktiv arbeiten. Es ersetzt somit gleichermaßen `telnet` und `rlogin`. Das Programm `slogin` ist lediglich ein symbolischer Link, der auf `ssh` weist. Sie können sich z. B. mit dem Befehl `ssh sun` auf dem Rechner `sun` anmelden. Der Host fordert Sie dann zur Eingabe des Passworts am System `sun` auf.

Nach erfolgreicher Authentifizierung können Sie dort in der Kommandozeile oder interaktiv, z. B. mit YaST, arbeiten. Sollten sich der lokale Benutzername und der auf dem entfernten System unterscheiden, können Sie einen abweichenden Namen angeben, z. B. `ssh -l augustine sun` oder `ssh augustine@sun`.

Darüber hinaus bietet `ssh` die von `rsh` bekannte Möglichkeit, Befehle auf einem entfernten System auszuführen. Im folgenden Beispiel wird der Befehl `uptime` auf dem Host `sun` ausgeführt und ein Verzeichnis mit dem Namen `tmp` angelegt. Die Programmausgabe erfolgt auf dem lokalen Terminal des Hosts `earth`.

```
ssh otherplanet "uptime; mkdir tmp"
Password:
1:21pm up 2:17, 9 users, load average: 0.15, 0.04, 0.02
```

Anführungszeichen sind hier zum Zusammenfassen der beiden Anweisungen in einem Befehl erforderlich. Nur so wird auch der zweite Befehl auf dem Host `sun` ausgeführt.

45.3 scp – sicheres Kopieren

`scp` kopiert Dateien auf einen entfernten Computer. Es ist ein sicherer und verschlüsselter Ersatz für `rcp`. Beispielsweise `scp MyLetter.tex sun:` kopiert die Datei

MyLetter.tex vom Host earth auf den Host sun. Wenn sich die Benutzernamen auf earth und sun unterscheiden, geben Sie den letzteren im Format `benutzername@host` an. Eine Option `-l` existiert für diesen Befehl nicht.

Nachdem das Passwort eingegeben wurde, beginnt `scp` mit der Datenübertragung und zeigt dabei den Fortschritt durch einen von links nach rechts anwachsenden Balken aus Sternen an. Zudem wird am rechten Rand die geschätzte Restübertragungszeit (bis zum Erreichen des rechten Balkenendes) angezeigt. Jegliche Ausgabe kann durch die Option `-q` unterdrückt werden.

`scp` bietet auch ein rekursives Kopierverfahren für ganze Verzeichnisse. Der Befehl `scp -r src/ sun:backup/` kopiert den kompletten Inhalt des Verzeichnisses `src` einschließlich aller Unterverzeichnisse in das Unterverzeichnis `backup` auf dem Host sun. Das Unterverzeichnis wird automatisch angelegt, wenn es noch nicht existiert.

Die Option `-p` weist `scp` an, den Zeitstempel von Dateien unverändert zu belassen. `-C` sorgt für komprimierte Datenübertragung. Dadurch wird das zu übertragende Datenvolumen minimiert, aber der Prozessor stärker belastet.

45.4 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.

45.5 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. Somit kann allein der kontaktierte SSH-Daemon mit seinen privaten Schlüsseln den Sitzungsschlüssel 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. So können so genannte

"man-in-the-middle"-Angriffe unterbunden werden, d. h. Versuche von fremden SSH-Servern, Name und IP-Adresse eines anderen vorzutauschen. 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.

45.6 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 Schlüsselpaars, das vom Benutzer erzeugt wird. Dazu liefert das SSH-Paket ein Hilfsprogramm: `ssh-keygen`. Nach der Eingabe von `ssh-keygen -t rsa` oder `ssh-keygen -t dsa` 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 alte 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.

45.7 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 `DISPLAY`-Variable gesetzt und alle X-Ausgaben werden durch die bestehende SSH-Verbindung an den entfernten Computer exportiert. Gleichzeitig unterbindet dies die bisher bestehenden Abhörmöglichkeiten bei entfernt aufgerufenen und lokal betrachteten X-Anwendungen.

Durch Hinzufügen der Option `-A` wird der Authentifizierungsmechanismus von `ssh-agent` auf den nächsten Computer mit übernommen. So können Sie an unterschiedlichen Computern arbeiten, ohne ein Passwort eingeben zu müssen. Allerdings ist das nur möglich, wenn Sie zuvor Ihren öffentlichen Schlüssel auf die beteiligten Zielhosts verteilt und dort korrekt gespeichert haben.

Beide Mechanismen sind in der Voreinstellung deaktiviert, können jedoch in der systemweiten Konfigurationsdatei `/etc/ssh/sshd_config` oder der benutzereigenen Datei `~/.ssh/config` permanent aktiviert werden.

ssh kann auch zur Umleitung von TCP/IP-Verbindungen benutzt werden. In den folgenden Beispielen wird SSH angewiesen, den SMTP- bzw. POP3-Port umzuleiten:

```
ssh -L 25:sun:25 earth
```

Mit diesem Befehl wird jede Verbindung zu Port 25 (SMTP) von earth auf den SMTP-Port von sun über den verschlüsselten Kanal weitergeleitet. Dies ist insbesondere für Benutzer von SMTP-Servern ohne SMTP-AUTH oder POP-before-SMTP-Funktionen von Nutzen. E-Mail kann so von jedem beliebigen Ort mit Netzanschluss zur Auslieferung durch den „home“-Mailserver übertragen werden. Analog können mit folgendem Befehl alle POP3-Anfragen (Port 110) an earth auf den POP3-Port von sun weitergeleitet werden:

```
ssh -L 110:sun:110 earth
```

Beide Befehle müssen Sie als Benutzer `root` ausführen, da die Verbindung zu privilegierten, lokalen Ports erfolgt. Bei bestehender SSH-Verbindung wird E-Mail wie gewohnt als normaler Benutzer verschickt und abgerufen. Der SMTP- und POP3-Host muss für diese Aufgabe auf `localhost` konfiguriert werden. Zusätzliche Informationen entnehmen Sie den Manualpages für die einzelnen Programme und den Dateien unter `/usr/share/doc/packages/openssh`.

Netzwerkauthentifizierung – Kerberos

46

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.

46.1 Kerberos-Terminologie

Im folgenden Glossar wird die Kerberos-Terminologie erläutert.

Berechtigung

Benutzer oder Clients müssen bestimmte Berechtigungen vorweisen, die Sie zur Anforderung von Diensten autorisieren. Bei Kerberos gibt es zwei Arten von Berechtigungen – Ticket und Authentifikator

Ticket

Ein Ticket ist eine Berechtigung pro Server, die von einem Client verwendet wird, um sich bei einem Server, von dem er einen Dienst anfordert, zu authentifizieren. 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 beweist ein Authentifikator, dass der Client, der das Ticket vorlegt, wirklich der ist, der er zu sein behauptet. 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) für den ein Ticket zugewiesen werden kann. Ein Prinzipal besteht aus folgenden Komponenten:

- **Primär** – der erste Teil des Prinzipals, der im Falle eines Benutzer dem Benutzernamen entsprechen kann.
- **Instanz** – einige zusätzliche Informationen zur genaueren Bestimmung des Primär. 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*.

46.2 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 nicht einmal sshd aus.

46.2.1 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 Ticket ausstellenden Diensts 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 folgende Informationen, die alle mit einem Sitzungsschlüssel verschlüsselt sind, der nur dem Authentifizierungsserver und dem Ticket ausstellenden Server bekannt ist:

- 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.

46.2.2 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.

46.2.3 Gegenseitige 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.

46.2.4 Ticket-Ausstellung – Kontakt mit allen Servern

Tickets sind jeweils nur für die Verwendung durch einen Server gedacht. 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.

46.2.5 Kompatibilität mit Windows 2000

Windows 2000 enthält eine Microsoft-Version von Kerberos 5. Da SUSE® Linux Enterprise Server die MIT-Implementierung von Kerberos 5 verwendet, erhalten Sie nützliche Informationen in der MIT-Dokumentation. Siehe [Abschnitt 46.4, „Weitere Informationen“](#) (S. 926).

46.3 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 Arbeitsstationen 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.

46.4 Weitere 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

47

In diesem Abschnitt werden die Installation der MIT Kerberos-Implementierung sowie einige administrative Aspekte erläutert. Es wird davon ausgegangen, dass Sie mit den grundlegenden Kerberos-Konzepten vertraut sind (siehe auch [Kapitel 46, Netzwerkauthentifizierung – Kerberos](#) (S. 919)).

47.1 Auswählen der Kerberos-Bereiche

Die Domäne einer Kerberos-Installation wird als Bereich bezeichnet und mit einem Namen identifiziert, z. B. `FOOBAR.COM` oder einfach `BUCHHALTUNG`. Kerberos unterstützt die Groß-/Kleinschreibung, daher ist `foobar.com` ein anderer Bereich als `FOOBAR.COM`. Verwenden Sie nach Ihrem Belieben Groß- oder Kleinschreibung. Gewöhnlich verwendet man jedoch Bereichsnamen in Großbuchstaben.

Daher ist eine gute Wahl Ihr DNS Domain Name (oder eine Unterdomäne, wie `ACCOUNTING.FOOBAR.COM`). 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. Sie können keinen Bereich namens `FOOBAR.COM` einrichten, zwei „Unterbereiche“ namens `ENTWICKLUNG` und `BUCHHALTUNG` darunter einrichten und erwarten, dass die beiden untergeordneten Bereiche die Prinzipale von `FOOBAR.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.

47.2 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 – wenn jemand einbricht, sind alle Benutzerkonten und Ihre gesamte, von Kerberos geschützte Infrastruktur beeinträchtigt. 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. Damit sind auch Server und Clients gemeint. 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` zur Verwendung ausschließlich lokaler Dateien für Benutzer- und Gruppensuche. Ändern Sie die Zeilen für `passwd` und `group`, damit sie wie folgt aussehen:

```
passwd:      files
group:       files
```

Bearbeiten Sie die Dateien `passwd`, `group`, `shadow` und `gshadow` unter `/etc` und entfernen Sie die Zeilen, die mit einem `+`-Zeichen beginnen (diese sind für NIS-Suchen).

- 6 Deaktivieren Sie alle Benutzerkonten außer das `root`-Konto, indem Sie die Datei `/etc/shadow` bearbeiten und die Rautezeichen für Passwörter durch `*`- oder `!`-Zeichen ersetzen.

47.3 Uhrensynchronisation

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. Dafür können Sie entweder einen NTP-Daemon im Client-Modus auf diesen Maschinen ausführen oder Sie führen einmal pro Tag `ntpdate` von allen Clients aus. (Letztere Lösung eignet sich eher 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 33.1](#), „Konfigurieren eines NTP-Client mit YaST“ (S. 675) 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 [Abschnitt 47.5.3](#), „Anpassen der Zeitdifferenz“ (S. 935) beschrieben.

47.4 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. Weitere Einzelheiten finden Sie unter [Abschnitt 47.4.1](#), „Installieren der RPMs“ (S. 931).
- 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.
- 4 Anpassen der ACL-Dateien: Administratoren hinzufügen** Die Kerberos-Datenbank des KDC kann entfernt verwaltet werden. Damit der Zugriff auf die Datenbank durch unberechtigte Prinzipale verhindert wird, verwendet Kerberos Zugriffskontrolllisten (ACLs). Sie müssen den entfernten Zugriff für den Administrator-Prinzipal zum Verwalten der Datenbank explizit erlauben.
- 5 Erstellen der Kerberos-Datenbank: Administratoren hinzufügen** Sie benötigen zum Ausführen und Verwalten von Kerberos mindestens einen Administrator-Prinzipal. Dieser Prinzipal muss hinzugefügt werden, bevor das KDC gestartet wird.

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.

7 Erstellen eines Prinzipals für Sie selbst

47.4.1 Installieren der RPMs

Vor dem Start installieren Sie die Kerberos-Software. Installieren Sie die Pakete `krb5`, `krb5-server` und `krb5-client` auf dem KDC.

47.4.2 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 aufbewahren. 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.

47.4.3 Erstellen eines Prinzipals

Als Nächstes erstellen Sie zwei Kerberos-Prinzipale für sich selbst: einen gewöhnlichen Prinzipal für die Arbeit und einen für die Verwaltungsaufgaben von Kerberos. 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>
```

Als Nächstes erstellen Sie einen weiteren Prinzipal mit dem Namen `newbie/admin`, indem Sie `ank newbie/admin` beim `kadmin`-Prompt 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.

47.4.4 Starten des KDC

Starten Sie den KDC-Daemon und den `kadmin`-Daemon. Sie starten die Daemons manuell, indem Sie `rc krb5kdc start` und `rc kadmin start` eingeben. Vergewissern Sie sich außerdem, dass KDC und `kadmin` standardmäßig beim Neustart der Servermaschine mit den Befehlen `insserv krb5kdc` und `insserv kadmin` gestartet werden.

47.5 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 dem 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 über DNS verursacht ein geringes Sicherheitsproblem. Ein Angreifer kann Ihre Infrastruktur über Ihr 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.

47.5.1 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.

47.5.2 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 Lastausgleich 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"
```

47.5.3 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 meist 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:

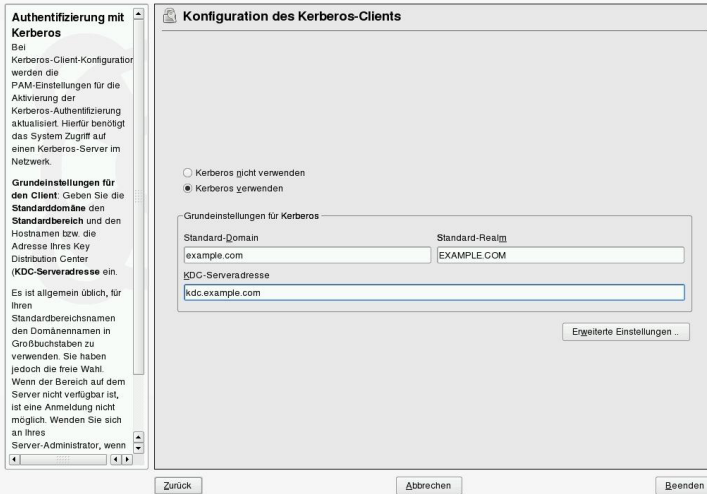
```
[libdefaults]  
    clockskew = 120
```

47.6 Konfigurieren eines Kerberos-Clients mit YaST

Als Alternative zu der oben beschriebenen manuellen Konfiguration können Sie einen Kerberos-Client mit YaST konfigurieren. Führen Sie dazu die folgenden Schritte aus:

- 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:
 - a** Bestätigen Sie die angezeigten *Kerberos-Grundeinstellungen*.
 - b** 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:
 - a** Legen Sie die *Standarddomäne*, den *Standardbereich* und die *KDC-Serveradresse* fest, sodass sie zu Ihrer Installation passen.
 - b** Klicken Sie auf *Erweiterte Einstellungen*, um die Einzelheiten in Bezug auf Tickets, Unterstützung von OpenSSH und Zeitsynchronisation zu konfigurieren.

Abbildung 47.1 *YaST: Grundlegende Konfiguration eines Kerberos-Client*



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. Dadurch wird das NTP-Client-Dialogfeld von YaST geöffnet. Es wird unter [Abschnitt 33.1](#), „[Konfigurieren eines NTP-Client mit YaST](#)“ (S. 675) genauer beschrieben. Nach Abschluss der Konfiguration führt YaST alle erforderlichen Änderungen durch und der Kerberos-Client kann nun eingesetzt werden.

Abbildung 47.2 YaST: Erweiterte Konfiguration eines Kerberos-Client

Die Werte für Standardlebensdauer, Standardwert für erneuerbare Lebensdauer und Zeitdifferenz werden standardmäßig in Sekunden angegeben. Geben Sie alternativ die Zeiteinheit (s für Minuten, h für Stunden oder d für Tage) an und verwenden Sie sie als Wertsuffix, wie bei 1 d bzw. 24h für einen Tag.

Weiterleitbar ermöglicht die Weiterleitung Ihrer vollständigen Identität (TGT) auf einen anderen Computer.

Weitervermittelbar ermöglicht nur die Übertragung bestimmter Tickets.

Wenn Beibehalten aktiviert wurde, behält ein PAM-Modul die Tickets nach dem Schließen der Sitzung.

Um Kerberos-Unterstützung für den OpenSSH-Client zu aktivieren, wählen Sie Kerberos-Unterstützung für OpenSSH-Client aus. In einem solchen Fall werden Kerberos-Tickets für die

Erweiterte Konfiguration des Kerberos-Clients

Ticket-Attribute

Standardlebensdauer: 1d

Standardwert für erneuerbare Lebensdauer: 1d

Weiterleitbar
 Weitervermittelbar
 Beibehalten

Kerberos-Unterstützung für OpenSSH-Client

Kleinste UID: 0

Zeitdifferenz: 300

47.7 Entfernte Kerberos-Administration

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. Tun Sie das, indem Sie die Datei `/var/lib/kerberos/krb5kdc/kadm5.ac1` bearbeiten. Die ACL (Zugriffskontrollliste)-Datei ermöglicht die Angabe von Berechtigungen mit einer guten Kontrolle. Genauere Einzelheiten finden Sie auf der Manualpage `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.

47.7.1 Verwenden von `kadmin` für die entfernte Administration

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/sha1, 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 Manualpage `man 8 kadmin`.

47.8 Erstellen der Kerberos-Host-Prinzipals

Jede Maschine im Netzwerk muss einem bestimmten Kerberos-Bereich angehören und muss wissen, welches KDC kontaktiert werden muss. Erstellen Sie außerdem einen *Host-Prinzipal* dafür. Bis jetzt wurden nur Benutzerberechtigungen erläutert. Kerberos-kompatible Dienste müssen sich jedoch selbst beim Client-Benutzer authentifizieren. Daher müssen spezielle Host-Prinzipale in der Kerberos-Datenbank für jeden Host im Bereich vorhanden sein.

Die Namenkonvention für Host-Prinzipale lautet `host/<hostname>@<REALM>`, wobei der `hostname` der vollständig qualifizierte Hostname ist. Host-Prinzipale ähneln Benutzer-Prinzipalen, aber es gibt wesentliche Unterschiede. Der hauptsächliche Unterschied zwischen einem Benutzer-Prinzipal und einem Host-Prinzipal ist, dass der

Schlüssel des ersteren durch ein Passwort geschützt ist. Wenn ein Benutzer ein Ticket ausstellendes Ticket vom KDC erhält, muss er das 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 wird der Schlüssel zur Entschlüsselung des anfänglichen Tickets für den Host-Prinzipal vom Administrator über das KDC einmal extrahiert und in einer lokalen Datei namens *keytab* gespeichert. 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 Host-Prinzipals für `test.example.com` geben Sie die folgenden Befehle 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/test.example.com
WARNING: no policy specified for host/test.example.com@EXAMPLE.COM;
defaulting
to no policy
Principal "host/test.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/test.example.com
Entry for principal host/test.example.com with kvno 3, encryption type Triple
DES cbc mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/test.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.

47.9 Aktivieren der PAM-Unterstützung für Kerberos

SUSE® Linux Enterprise wird mit einem PAM-Modul namens `pam_krb5` geliefert, 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.

Das `pam_unix2`-Modul unterstützt ebenfalls die Kerberos-Authentifizierung und die Passwort-Aktualisierung. Zum Aktivieren der Kerberos-Unterstützung von `pam_unix2`, müssen Sie der Datei `/etc/security/pam_unix2.conf` folgende Zeilen hinzufügen:

```
auth:          use_krb5 nullok
account:       use_krb5
password:      use_krb5 nullok
session:       none
```

Danach verwenden alle Programme, die auf die Einträge in dieser Datei zugreifen, Kerberos als Benutzerauthentifizierung. Bei einem Benutzer, der über keinen Kerberos-Prinzipal verfügt, verwendet `pam_unix2` wieder die normale Passwort-Authentifizierung. Alle Benutzer mit einem Prinzipal können nun ihre Kerberos-Passwörter transparent ändern, indem sie den Befehl `passwd` verwenden.

Wenn Sie Feineinstellungen für die Verwendung der Datei `pam_krb5` vornehmen möchten, bearbeiten Sie die Datei `/etc/krb5.conf` und fügen Sie `pam` die Standardanwendungen hinzu. Genauere Einzelheiten finden Sie auf der Manualpage `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.

47.10 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 zu kaschieren (bei Kerberos, einem Authentifizierungssystem mit öffentlichem Schlüssel, wie SPKM oder anderen). 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 neu mit dem Befehl `rcsshd restart`.

Wenn Sie die Kerberos-Authentifizierung mit der Protokollversion 2 verwenden möchten, aktivieren Sie sie auch auf der Client-Seite. Tun Sie das entweder in der systemweiten Konfigurationsdatei `/etc/ssh/ssh_config` oder für jeden Benutzer einzeln, indem Sie die Datei `~/.ssh/config` bearbeiten. 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: Zusätzliche Informationen

Die Datei `/usr/share/doc/packages/openssh/README.kerberos` erläutert die Interaktion von OpenSSH und Kerberos genauer.

47.11 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. Daher können Sie 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` gesetzt wurde (das 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"
```

Dann starten Sie den LDAP-Server neu, indem Sie `rcldap restart` verwenden.

47.11.1 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. Das wurde wahrscheinlich gewählt, weil diese Anzahl von 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.

47.11.2 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 Stück im Puzzle. Wie kann der LDAP-Server herausfinden, 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
```

Wenn Sie wissen möchten, wie das funktioniert, müssen Sie zuerst 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

48

Vertrauliche Daten, die kein unberechtigter Dritter einsehen sollte, hat jeder Benutzer. Je vernetzter und mobiler Sie arbeiten, desto sorgfältiger sollten Sie im Umgang mit Ihren Daten sein. Die Verschlüsselung von Dateien oder von ganzen Partitionen macht immer dann Sinn, wenn Dritte entweder über eine Netzwerkverbindung oder direkt Zugriff auf das System haben. Bei Laptops oder Wechseldatenträgern, wie externen Festplatten oder USB-Sticks, die leicht verloren gehen oder gestohlen werden können, ist es ebenso sehr sinnvoll, Partitionen (oder Teile des Dateisystems) mit vertraulichen Daten zu 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. Details finden Sie unter [Abschnitt 48.1.1, „Anlegen einer verschlüsselten Partition während der Installation“](#) (S. 951) und [Abschnitt 48.1.2, „Einrichten einer verschlüsselten Partition im laufenden System“](#) (S. 952). Diese Option kann auch für Wechseldatenträger, wie externe Festplatten, verwendet werden (siehe [Abschnitt 48.1.4, „Verschlüsseln des Inhalts von Wechselmedien“](#) (S. 953)).

Erstellen einer verschlüsselten Datei als Container

Mit YaST können Sie jederzeit auf Ihrer Festplatte oder auf einem Wechseldatenträger eine verschlüsselte Datei erstellen. Die verschlüsselte Datei kann dann verwendet werden, um darin andere Dateien oder Ordner zu *verwahren*. Weitere Informationen finden Sie in [Abschnitt 48.1.3, „Erstellen einer verschlüsselten Datei als Container“](#) (S. 952).

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 hierzu finden Sie unter [Abschnitt 48.2, „Verschlüsselung einzelner Dateien mit vi“](#) (S. 953).

WARNUNG: Das Verschlüsseln von Medien bietet nur eingeschränkten Schutz

Beachten Sie, dass die in diesem Kapitel beschriebenen Methoden nicht Ihr laufendes System vor Manipulation schützen können. Nachdem die verschlüsselten Medien erfolgreich eingehängt wurden, können alle Benutzer mit den entsprechenden Berechtigungen darauf zugreifen. Die Verwendung verschlüsselter Medien ist jedoch von Vorteil, wenn Ihr Computer einmal verloren geht oder gestohlen wird oder um zu verhindern, dass unbefugte Personen Ihre vertraulichen Daten lesen.

48.1 Einrichten eines verschlüsselten Dateisystems 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.

48.1.1 Anlegen einer verschlüsselten Partition während der Installation

WARNUNG: Passwordeingabe

Beachten Sie bei der Passwordeingabe die Warnungen zur Passwortsicherheit und merken Sie sich das Passwort gut. Ohne das Passwort können Sie die verschlüsselten Daten weder öffnen noch wiederherstellen.

Das in [Abschnitt 7.5.8, „Partitionierung“](#) (S. 176) beschriebene YaST-Expertendialogfeld für die Partitionierung bietet die Möglichkeit zum Anlegen einer verschlüsselten Partition. Klicken Sie zum Erstellen einer neuen verschlüsselten Partition auf *Create* (Erstellen). Es wird ein Dialogfeld geöffnet, in dem Sie die Partitionierungsparameter für die neue Partition, z. B. die gewünschte Formatierung und den Einhängepunkt, festlegen können. Schließen Sie den Prozess ab, indem Sie auf *Dateisystem verschlüsseln* klicken. Geben Sie im folgenden Dialogfeld das Passwort zweimal ein. Die neue verschlüsselte Partition wird erstellt, wenn Sie das Dialogfeld durch Klicken auf *OK* schließen. Beim Booten des Systems werden Sie vor dem Einhängen der Partition zur Eingabe des Passworts aufgefordert.

Wenn die verschlüsselte Partition nicht während des Boot-Vorgangs eingehängt werden soll, drücken Sie die [Eingabetaste], wenn Sie zur Eingabe des Passworts aufgefordert werden. 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. Nach dem Einhängen steht die Partition allen Benutzern zur Verfügung.

Wenn das verschlüsselte Dateisystem nur bei Bedarf eingehängt werden soll, aktivieren Sie die Option *Nicht beim Systemstart einhängen* im Dialogfeld *Optionen für Fstab*. Die betreffende Partition wird beim Booten des Systems nicht eingehängt. Um sie anschließend verfügbar zu machen, hängen Sie sie manuell ein mit `einhängen Name_der_Partition Einhängepunkt`. Geben Sie das Passwort ein, wenn Sie dazu aufgefordert werden. Wenn Sie die Partition nicht mehr benötigen, hängen Sie sie aus mit `einhängen Name_der_Partition`, um zu verhindern, dass andere Benutzer auf sie zugreifen.

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 48.1.2, „Einrichten einer verschlüsselten Partition im laufenden System“](#) (S. 952) und bedenken Sie, dass durch diese Aktion alle Daten in der bestehenden Partition, die Sie verschlüsseln möchten, gelöscht werden.

48.1.2 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. Klicken Sie nicht wie oben beschrieben auf *Anlegen*, sondern wählen Sie *Bearbeiten*. Führen Sie alle verbleibenden Schritte wie in [Abschnitt 48.1.1, „Anlegen einer verschlüsselten Partition während der Installation“](#) (S. 951) beschrieben aus.

48.1.3 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. Diese Containerdateien werden im selben YaST-Dialogfeld erstellt. Wählen Sie *Kryptodatei* und geben Sie den Pfad zu der zu erstellenden Datei sowie den Platzbedarf der Datei an. Übernehmen Sie die Voreinstellungen für die Formatierung und den Dateisystemtyp. Geben Sie anschließend den Einhängepunkt an und legen Sie fest, ob das verschlüsselte Dateisystem beim Booten des Systems eingehängt werden soll.

Der Vorteil verschlüsselter Containerdateien 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.

48.1.4 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. Geben Sie allerdings nicht an, dass diese Medien beim Booten des Systems eingehängt werden sollen, da sie in der Regel nur an das laufende System angeschlossen werden.

48.2 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 -x Dateiname` 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

49

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, indem er ein Sicherheits*profil* für diese Anwendung entwickelt — 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.

Die Erstellung von AppArmor-Profilen zur Einschränkung einer Anwendung ist sehr bequem und einfach. AppArmor wird mit mehreren Werkzeugen geliefert, 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 bietet verständliche Werkzeuge für Profilaktualisierungen oder -änderungen.

Benutzer sollten AppArmor gar nicht bemerken. 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 2.0-Administrationshandbuch*.

49.1 Installation von Novell AppArmor

Novell AppArmor wird bei jeder Installation von SUSE® Linux Enterprise 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`

49.2 Aktivieren und Deaktivieren von Novell AppArmor

Novell AppArmor ist für die standardmäßige Ausführung auf jeder neuen Installation von SUSE Linux Enterprise 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.

Mithilfe 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 Skripts 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 *AppArmor aktivieren* → *Konfigurieren*.
- 4 Klicken Sie auf *Aktivieren* und *OK*, um AppArmor zu aktivieren, oder auf *Deaktivieren* und *OK*, um AppArmor zu deaktivieren.
- 5 Beenden Sie die AppArmor-Kontrollleiste mit *Fertig*.

49.3 Einführung in die Erstellung von Anwendungsprofilen

Bereiten Sie einen erfolgreichen Einsatz von Novell AppArmor auf Ihrem System vor, indem Sie die folgenden Punkte genau beachten:

- 1 Ermitteln Sie die Anwendungen, die ein Profil brauchen. Weitere Informationen dazu finden Sie unter [Abschnitt 49.3.1, „Wählen der Anwendungen, die ein Profil erhalten sollen“](#) (S. 959).
- 2 Erstellen Sie die erforderlichen Profile wie in [Abschnitt 49.3.2, „Erstellen und Ändern von Profilen“](#) (S. 960) 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. Informationen finden Sie in [Abschnitt 49.3.3, „Konfigurieren von Novell AppArmor-Ereignisbenachrichtigung und -Berichten“](#) (S. 963).
- 4 Aktualisieren Sie Ihre Profile, wenn sich Ihre Umgebung ändert. Andernfalls müssen Sie auf Sicherheitsereignisse reagieren, die das AppArmor-Berichtwerk-

zeug protokolliert. Informationen finden Sie in [Abschnitt 49.3.4](#), „Aktualisieren Ihrer Profile“ (S. 964).

49.3.1 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) haben offene Netzwerkports und Netzwerkagenten sind Serverprogramme, die auf diese Netzwerkports reagieren. Benutzerclients, wie Mail-Clients und Webbrowser, haben ebenfalls offene Netzwerkports und vermitteln Berechtigungen. Bei jedem Angriff auf den Webbrowser oder E-Mail-Client eines Benutzers kann der Angreifer private Daten des Benutzers stehlen. Darüber hinaus kann der Angreifer den durch den Angriff erhaltenen Zugriff nutzen, um weitere Berechtigungen im System zu erhalten.

Webanwendungen

CGI-Skripts in Perl, PHP-Seiten und komplexere Webanwendungen können durch einen Webbrowser gestartet werden.

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 49.1 *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: Weitere Informationen

Weitere Informationen zur Auswahl der richtigen Anwendungen für die Profilerstellung finden Sie unter Kapitel *Auswählen von Programmen, die immunisiert werden sollen* (↑Novell AppArmor 2.0 Administration Guide).

49.3.2 Erstellen und Ändern von Profilen

Novell AppArmor unter SUSE Linux Enterprise wird mit einem vorkonfigurierten Satz an 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 besteht in der Verwendung des grafischen Frontend der YaST Novell AppArmor-Module, bei der anderen werden die Kommandozeilenwerkzeuge genutzt, die in der AppArmor-Suite zur Verfügung stehen. Beide Methoden arbeiten grundsätzlich auf dieselbe Weise.

Die Ausführung von `aa-unconfined` (wie in [Abschnitt 49.3.1](#), „Wählen der Anwendungen, die ein Profil erhalten sollen“ (S. 959) 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 ein grundlegendes Profil, indem Sie den *YaST → Novell AppArmor → -Assistenten 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. 961) generiert wurden, indem Sie `[5]` in `aa-genprof` eingeben.

Oder:

Analysieren Sie die Protokolle, indem Sie im *Assistenten zum Hinzufügen von Profilen* auf *Scan system log for AppArmor events* (Systemprotokoll auf AppArmor-Ereignisse prüfen) klicken und den Anweisungen des Assistenten folgen, bis das Profil fertig gestellt ist.

AppArmor prüft die Protokolle, die während der Ausführung der Anwendung aufgezeichnet wurden, und fordert Sie auf, für jedes protokollierte Ereignis die Zugriffsberechtigungen festzulegen. Legen Sie die Zugriffsberechtigungen für jede Datei fest oder verwenden Sie Platzhalterzeichen.

- 4 Sobald alle Berechtigungen festgelegt sind, wird Ihr Profil in den Erzwingen-Modus gesetzt. Das Profil wird angewendet und AppArmor beschränkt die Anwendung entsprechend dem soeben erstellten Profil.

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`—Eingabe des Meldungs- oder Lernmodus“ (Kapitel 3, *Erstellen von Novell AppArmor-Profilen*, ↑Novell AppArmor 2.0 Administration Guide) und „`aa-enforce`—Eingeben des Erzwingen-Modus“ (Kapitel 3, *Erstellen von Novell AppArmor-Profilen*, ↑Novell AppArmor 2.0 Administration Guide).

Testen Sie Ihre Profileinstellungen, indem Sie jede benötigte Aufgabe mit der soeben eingeschränkten Anwendung ausführen. Normalerweise läuft das eingeschränkte Programm reibungslos und Sie bemerken überhaupt keine AppArmor-Aktivitäten. 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.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. 961) beschrieben, um das Profil anzupassen. Bestimmen Sie die Zugriffsberechtigungen oder Einschränkungen, wenn Sie dazu aufgefordert werden.

TIPP: Weitere Informationen

Weitere Informationen zum Erstellen und Ändern von Profilen finden Sie in Kapitel *Erstellen von Novell AppArmor-Profilen* (↑Novell AppArmor 2.0 Administration Guide).

49.3.3 Konfigurieren von Novell AppArmor-Ereignisbenachrichtigung und -Berichten

Richten Sie Ereignisbenachrichtigung in Novell AppArmor ein, damit Sie Sicherheitsereignisse überprüfen können. Ereignisbenachrichtigung ist eine Novell AppArmor-Funktion, die einen angegebenen E-Mail-Empfänger benachrichtigt, wenn im System eine Novell AppArmor-Aktivität unter der gewählten Sicherheitsebene auftritt. Diese Funktion steht derzeit in der 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 anschließend *Novell AppArmor* → *AppArmor-Kontrollleiste*.
- 3 Wählen Sie unter *Sicherheitsereignisbenachrichtigung aktivieren* die Option *Konfigurieren*.
- 4 Stellen Sie für jeden Eintragstyp (*Knapp*, *Zusammenfassung* und *Ausführlich*) eine Berichthäufigkeit ein, geben Sie die E-Mail-Adresse ein, an welche die Berichte gesendet werden, und legen Sie den Schweregrad der aufzuzeichnenden Ereignisse fest. Zur Aufnahme von unbekanntem Ereignissen in die Ereignisberichte aktivieren Sie *Ereignisse mit unbekanntem Schweregrad aufnehmen*.

ANMERKUNG: Auswählen zu protokollierender 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* → *Beenden*, 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: Weitere Informationen

Weitere Informationen zur Konfiguration der Ereignisbenachrichtigung in Novell AppArmor finden Sie unter Abschnitt „Einrichten der Ereignisbenachrichtigung“ (Kapitel 4, *Verwalten von Anwendungen mit Profilen*, ↑Novell AppArmor 2.0 Administration Guide). Weitere Informationen zur Berichtkonfiguration finden Sie in Abschnitt „Berichte“ (Kapitel 4, *Verwalten von Anwendungen mit Profilen*, ↑Novell AppArmor 2.0 Administration Guide).

49.3.4 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 Ihnen, Ihren Profilsatz entsprechend anzupassen. Jedes Anwedungsverhalten, 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 den *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: Weitere Informationen

Weitere Informationen zur Aktualisierung Ihrer Profile über die Systemprotokolle finden Sie in Abschnitt „Updating Profiles from Log Entries“ (Kapitel 3, *Erstellen von Novell AppArmor-Profilen*, ↑*Novell AppArmor 2.0 Administration Guide*).

Sicherheit und Vertraulichkeit

50

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 dieses Backup der Daten wird es nicht nur im Fall eines Hardwaredefekts schwierig sein, weiterhin auf die Daten zuzugreifen, sondern insbesondere auch dann, wenn nur der Verdacht besteht, dass jemand sich unbefugterweise an den Daten zu schaffen gemacht hat.

50.1 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 dagegen, indem Sie Passwörter für das BIOS und den Bootloader festlegen.

Oft werden noch 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 dabei der einfachste Angriffspunkt: Wenn ein alter Drucker daran angeschlossen ist, kann die Kommunikation einfach aufgezeichnet werden. 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.

50.1.1 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.

50.1.2 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. Daraus gewinnen Sie ein sicheres Passwort: „DNdRvUE9“. Im Gegensatz dazu können Passwörter wie „Saufkumpan“ oder „Jasmin76“ schon von jemandem erraten werden, der Sie oberflächlich gut kennt.

50.1.3 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 21, Der Bootloader](#) (S. 437)). 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.

50.1.4 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 einzelnen Berechtigungen der weit über 200.000 Dateien einer SUSE-Distribution sind sorgfältig vergeben. 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 SUSE® Linux Enterprise 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.

Die Auswahl der Dateien, die für Konfigurationsprogramme von SUSE zur Vergabe der Rechte benutzt werden sollen, können Sie auch komfortabel mit YaST unter dem Menüpunkt *Sicherheit* treffen. Weitere Informationen zu diesem Thema finden Sie in

den Kommentaren in `/etc/permissions` oder auf der Manualpage für den Befehl `chmod` (`man chmod`).

50.1.5 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 50.1.4, „Dateiberechtigungen“](#) (S. 971)).

Format-String-Programmfehler funktionieren etwas anders, auch hierbei kann über die Benutzereingabe das Programm von seinem eigentlichen Weg abgebracht werden. Diese Programmierfehler werden normalerweise bei 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 50.1.4, „Dateiberechtigungen“](#) (S. 971)).

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.

50.1.6 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. SUSE-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.

50.1.7 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 den beiden Sicherheitsaspekten differenziert werden: bis zur erfolgten Authentifizierung geht es um Netzwerksicherheit, nach der Anmeldung um lokale Sicherheit.

50.1.8 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. Es könnte beispielsweise noch ein zweiter Benutzer auf dem Host mit dem Client-Programm arbeiten und dieser hätte dann genau wie jemand, der die IP-Adresse stiehlt, Zugriff auf den X-Server. Deswegen wird auf diese Authentifizierungsmethode auch 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 Kekse. 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. Weitere Informationen zur Sicherheit von X Window-Systemen finden Sie auf der Manualpage für den Befehl `Xsecurity` (`man Xsecurity`).

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 45, SSH: Sicherer Netzbetrieb](#) (S. 911).

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.

50.1.9 Pufferüberläufe und Format-String-Programmfehler

Wie in [Abschnitt 50.1.5, „Pufferüberläufe und Format-String-Programmfehler“](#) (S. 972) 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 frisch gefundenen 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. Da bei freier Software der Quellcode für jedermann erhältlich ist (SUSE Linux Enterprise liefert alle verfügbaren Quellen mit), kann jemand, der eine Sicherheitslücke mitsamt Exploit-Code findet, auch gleichzeitig noch einen Patch für das Problem anbieten.

50.1.10 DoS – Denial of Service

Ziel von DoS-Angriffen ist das Blockieren eines Serverprogramms oder sogar des ganzen Systems. Dies kann auf verschiedenste Arten passieren: durch Überlasten des Servers, indem er mit unsinnigen Paketen beschäftigt wird, oder durch Ausnutzen von entfernten Pufferüberläufen. 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.

50.1.11 Man in the Middle: Sniffing, Hijacking, Spoofing

Im Allgemeinen gilt: Ein entfernter Angriff, bei dem der Angreifer eine Position zwischen zwei kommunizierenden Hosts einnimmt, wird 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 eines Man-in-the-middle-Angriffs wird als *Sniffer* bezeichnet. Bei diesen belauscht der Angreifer einfach nur die Netzverbindungen, die an ihm vorüber geführt werden. 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. Die meisten aktiven Angriffsvarianten verlangen das Verschicken von gefälschten Paketen, was unter Unix/Linux übrigens nur der Superuser (`root`) kann.

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.

50.1.12 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 Namenserver 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.

50.1.13 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.

50.2 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. Die SUSE-Sicherheitsmitteilungen (Security Announcements) werden über eine Mailingliste verbreitet, in die Sie sich unter der Adresse <http://www.novell.com/linux/security/securitysupport.html> eintragen können. Die Liste suse-security-announce@suse.de, die u.a. von Mitgliedern des SUSE-Sicherheitsteams erstellt wird, ist die erste Informationsquelle für Update-Pakete.

Diese Mailingliste suse-security@suse.de 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:

- Vermeiden Sie es, als `root` zu arbeiten, entsprechend dem Prinzip, die geringstnötigen Privilegien für eine Aufgabe zu verwenden. 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, sendmail, 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`).

- Zur zuverlässigen Integritätsprüfung der Dateien in Ihrem System sollten Sie das Programm AIDE (Advanced Intrusion Detection Environment) verwenden, das unter SUSE Linux Enterprise 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, ob die Prüfsumme und die Signatur eines (nicht installierten) Pakets stimmen. 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 Manualpages zu `tcpd` und `hosts_access` (`man 8 tcpd`, `man hosts_access`).
- Als zusätzlichen Schutz zu `tcpd` (`tcp_wrapper`) könnten Sie `SuSEfirewall` verwenden.
- Richten Sie die Sicherheitsmaßnahmen redundant ein: Eine Meldung, die zweimal gelesen wird, ist besser als eine, die Sie nie sehen.

50.3 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>.

Teil 6. Fehlerbehebung

Hilfe und Dokumentation

51

SUSE® Linux Enterprise beinhaltet verschiedene Informationsquellen und Dokumentationen. Der zentrale Ort der Information ist die SUSE-Hilfe, in der Sie die wichtigsten Dokumentationsressourcen des Systems öffnen und durchsuchen können. Verfügbar sind Online-Hilfen für alle installierten Anwendungen, Manualpages, Infoseiten, Datenbanken zu Hardware- und Software-Themen sowie alle mit dem Produkt ausgelieferten Handbücher.

51.1 Verwenden der SUSE-Hilfe

Wenn Sie die SUSE-Hilfe zum ersten Mal aus dem Hauptmenü mit der Option *SUSE-Hilfe* oder von der Shell mit dem Befehl `susehelp` starten, wird das in [Abbildung 51.1](#), „Das Hauptfenster der SUSE-Hilfe“ (S. 986) gezeigte Fenster geöffnet. Dieses Fenster enthält drei Hauptbereiche:

Menüleiste und Werkzeugleiste

Die Menüleiste bietet die wichtigsten Optionen zum Bearbeiten, Navigieren und Konfigurieren. Das Menü *Datei* enthält eine Option zum Drucken des aktuell angezeigten Inhalts. Unter *Bearbeiten* rufen Sie die Suchfunktion auf. *Gehe zu* bietet sämtliche Navigationsmöglichkeiten: *Inhalt* (Startseite der Hilfe), *Zurück*, *Weiter* und *Letztes Suchergebnis*. Mit *Einstellungen* → *Suchindex erstellen* generieren Sie einen Suchindex für alle ausgewählten Informationsquellen. Die Werkzeugleiste enthält drei Navigationssymbole (Weiter, Zurück, Startseite der Hilfe) sowie ein Druckersymbol zum Drucken des aktuellen Inhalts.

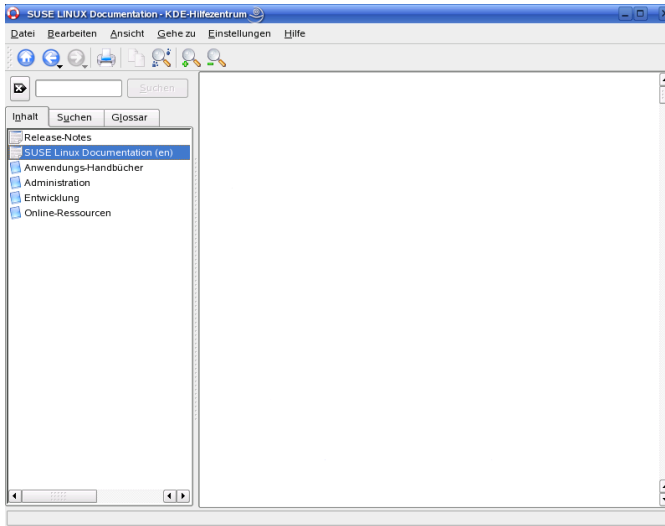
Navigationsbereich mit Registerkarten

Der Navigationsbereich auf der linken Seite des Fensters enthält ein Eingabefeld für die Schnellsuche in ausgewählten Informationsquellen. Detaillierte Informationen zur Suche und zur Konfiguration der Suchfunktion auf der Registerkarte *Suchen* finden Sie in [Abschnitt 51.1.2, „Die Suchfunktion“](#) (S. 987). Die Registerkarte *Inhalt* enthält eine Baumansicht aller verfügbaren und aktuell installierten Informationsquellen. Klicken Sie auf die Buchsymbole, um die einzelnen Kategorien zu öffnen und zu durchsuchen.

Ansichtsfenster

Im Ansichtsfenster werden die aktuell ausgewählten Inhalte wie Online-Handbücher, Suchergebnisse oder Webseiten angezeigt.

Abbildung 51.1 *Das Hauptfenster der SUSE-Hilfe*



ANMERKUNG: Ansicht für Sprachauswahl

Die im SUSE-Hilfzentrum verfügbare Dokumentation hängt von der aktuellen Sprache ab. Durch den Wechsel der Sprache ändert sich auch die Baumansicht.

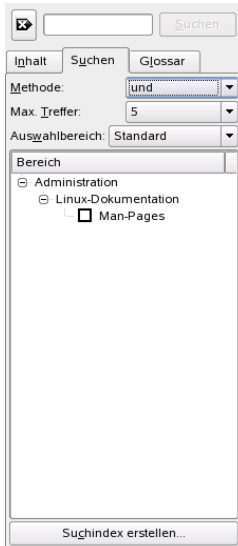
51.1.1 Inhalt

Die SUSE-Hilfe bündelt nützliche Informationen aus verschiedenen Quellen. Sie enthält spezielle Dokumentationen für SUSE Linux Enterprise (*Start* und *Referenz*), sämtliche verfügbaren Informationsquellen für Ihre Workstation-Umgebung, Online-Hilfen für die installierten Programme und Hilfetexte für andere Anwendungen. Darüber hinaus bietet die SUSE-Hilfe Zugriff auf die Online-Datenbanken von SUSE, die sich mit speziellen Hardware- und Software-Themen zu SUSE Linux Enterprise befassen. Alle diese Informationsquellen lassen sich problemlos durchsuchen, sobald der Suchindex generiert ist.

51.1.2 Die Suchfunktion

Um alle installierten Informationsquellen von SUSE Linux Enterprise zu durchsuchen, müssen Sie einen Suchindex generieren und einige Suchparameter festlegen. Öffnen Sie dazu die Registerkarte *Suchen* (siehe [Abbildung 51.2](#), „*Konfigurieren der Suchfunktion*“ (S. 987)).

Abbildung 51.2 Konfigurieren der Suchfunktion



Wenn noch kein Suchindex generiert wurde, werden Sie vom System automatisch dazu aufgefordert, sobald Sie die Registerkarte *Suchen* öffnen oder eine Suchzeichenfolge eingeben und auf *Suchen* klicken. Wählen Sie im Dialogfeld zur Generierung des Suchindex (siehe [Abbildung 51.3](#), „Generieren des Suchindex“ (S. 988)) die Kontrollkästchen derjenigen Informationsquellen aus, die indiziert werden sollen. Der Index wird generiert, sobald Sie das Dialogfeld mit *Index erstellen* schließen.

Abbildung 51.3 Generieren des Suchindex



Den Suchbereich und die Trefferliste sollten Sie möglichst präzise eingrenzen. Bestimmen Sie dazu über die drei Dropdown-Menüs die zu durchsuchenden Quellen sowie die Anzahl der angezeigten Treffer. Zur Bestimmung des Suchbereichs stehen die folgenden Optionen zur Verfügung:

Standard

Eine vordefinierte Auswahl an Quellen wird durchsucht.

Alle

Alle Quellen werden durchsucht.

Keine

Für die Suche werden keine Quellen ausgewählt.

Benutzerdefiniert

Die mit den Kontrollkästchen ausgewählten Quellen werden durchsucht.

Klicken Sie auf *Suchen*, nachdem Sie die Suchparameter festgelegt haben. Die gefundenen Elemente werden im Ansichtsfenster angezeigt und können per Mausklick geöffnet werden.

51.2 Manualpages

Manualpages sind ein wichtiger Teil des Linux-Hilfesystems. Sie erklären die Verwendung der einzelnen Befehle und deren Optionen und Parameter. Manualpages sind in Kategorien unterteilt, wie in [Tabelle 51.1](#), „[Manualpages – Kategorien und Beschreibungen](#)“ (S. 989) gezeigt (diese Einteilung wurde direkt von der Manualpage für den Befehl "man" übernommen).

Tabelle 51.1 *Manualpages – Kategorien und Beschreibungen*

Ziffer	Beschreibung
1	Ausführbare Programme oder Shell-Befehle
2	Systemaufrufe (vom Kernel bereitgestellte Funktionen)
3	Bibliotheksaufrufe (Funktionen in Programmbibliotheken)
4	Spezielle Dateien (gewöhnlich in /dev)
5	Dateiformate und Konventionen (/etc/fstab)
6	Spiele
7	Sonstiges (wie Makropakete und Konventionen), zum Beispiel man(7) oder groff(7)
8	Systemverwaltungsbefehle (in der Regel nur für "root")
9	Nicht standardgemäße Kernel-Routinen

Manualpages werden in der Regel durch den zugehörigen Befehl geöffnet. Sie können in der SUSE-Hilfe oder direkt in einer Shell durchsucht werden. Im letzteren Fall verwenden Sie den Befehl `man`. Um zum Beispiel die Manualpage des Befehls `ls` zu

öffnen, geben Sie `man ls` ein. Jede Manualpage besteht aus den Abschnitten *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* und *AUTHOR*. Je nach Befehlstyp stehen möglicherweise auch weitere Abschnitte zur Verfügung. Mit `Q` schließen Sie eine Manualpage.

Manualpages können auch in Konqueror angezeigt werden. Geben Sie dazu in Konqueror den betreffenden Befehl ein, zum Beispiel `man : /ls`. Falls der Befehl in mehreren Kategorien beschrieben ist, werden die entsprechenden Links angezeigt.

51.3 Infoseiten

Eine weitere wichtige Informationsquelle sind Infoseiten. Diese sind im Allgemeinen ausführlicher als Manualpages. Infoseiten werden in einem Info-Betrachter angezeigt, der die verschiedenen Abschnitte über so genannte „Knoten“ bereitstellt. Zum Öffnen von Infoseiten verwenden Sie den Befehl `info`. Wenn Sie beispielsweise die Infoseite für den Befehl `info` anzeigen möchten, geben Sie in der Shell `info info` ein.

Einfacher ist die Navigation auf den Infoseiten, wenn Sie die SUSE-Hilfe oder Konqueror verwenden. Starten Sie dazu Konqueror und geben Sie `info: /` ein, um die oberste Ebene der Infoseiten anzuzeigen. Um zum Beispiel die Infoseite für den Befehl `grep` anzuzeigen, geben Sie `info: /grep` ein.

51.4 Das Linux-Dokumentationsprojekt

Das Linux-Dokumentationsprojekt (TLDP) ist eine auf freiwilliger Mitarbeit beruhende Gemeinschaftsinitiative zur Erarbeitung von Linux-Dokumentationen und Veröffentlichungen zu verwandten Themen (siehe <http://www.tldp.org>). Sie finden dort durchaus Anleitungen, die auch für Anfänger geeignet sind, doch hauptsächlich richten sich die Dokumente an erfahrene Benutzer, zum Beispiel an professionelle Systemadministratoren. Das Projekt veröffentlicht HOWTOs (Verfahrensbeschreibungen), FAQs (Antworten zu häufigen Fragen) sowie ausführliche Handbücher und stellt diese unter einer kostenlosen Lizenz zur Verfügung.

51.4.1 HOWTOs

HOWTOs (Verfahrensbeschreibungen) beinhalten meist eine kurze, schrittweise Anleitung zur Ausführung einer bestimmten Aufgabe, die im Allgemeinen von Fachleuten eines bestimmten Gebiets für weniger erfahrene Benutzer geschrieben wird. Ein HOWTO kann sich zum Beispiel mit der Einrichtung eines DHCP-Servers befassen. HOWTOs befinden sich im Paket `howto` und werden unter `/usr/share/doc/howto` installiert.

51.4.2 FAQs

FAQs (Antworten zu häufigen Fragen) beinhalten bestimmte Fragestellungen und deren Antworten. FAQs wurden ursprünglich in Usenet Newsgroups eingeführt, um zu vermeiden, dass immer wieder die gleichen grundlegenden Fragen gestellt werden.

51.5 Wikipedia: die kostenlose Online-Enzyklopädie

Wikipedia ist eine „mehrsprachige Enzyklopädie, die jeder nutzen und zu der jeder beitragen kann“ (siehe <http://en.wikipedia.org>). Die Inhalte von Wikipedia werden von den Benutzern der Enzyklopädie selbst geschrieben und stehen unter einer kostenlosen Lizenz (der GDFL) zur Verfügung. Da jeder Besucher die Artikel bearbeiten kann, ist deren Wahrheitsgehalt nicht immer gegeben, aber dadurch sollten Sie sich nicht von der Nutzung dieser umfangreichen Wissensquelle abschrecken lassen. In den über vierhunderttausend Artikeln finden Sie Informationen über nahezu alle Wissensgebiete.

51.6 Handbücher und andere Literatur

Über Linux wurden zahlreiche Handbücher und Leitfäden veröffentlicht.

51.6.1 Handbücher von SUSE

SUSE stellt ausführliche und informative Handbücher in verschiedenen Sprachen in den Formaten HTML und PDF zur Verfügung. Die PDF-Datei befindet sich auf der DVD im Verzeichnis `docu`. Die HTML-Version befindet sich im Paket `suselinux-manual_SPRACHE` (wobei *SPRACHE* für die Sprache des jeweiligen Pakets steht). Nach deren Installation steht die HTML-Version in der SUSE-Hilfe zur Verfügung.

51.6.2 Weitere Handbücher

Über die SUSE-Hilfe stehen Ihnen Handbücher und Leitfäden zu verschiedenen Themen und Programmen zur Verfügung. Weitere Handbücher sind unter <http://www.tldp.org/guides.html> veröffentlicht. Dort finden Sie Handbücher von einem *Bash Guide for Beginners* (Schnelleinstieg für Anfänger) und der *Linux Filesystem Hierarchy* (Linux-Dateisystemhierarchie) bis hin zum *Linux Administrator's Security Guide* (Sicherheitshandbuch für Linux-Administratoren). Im Allgemeinen sind Handbücher ausführlicher und umfassender als HOWTOs oder FAQs und werden von Fachleuten für erfahrene Benutzer geschrieben. Einige dieser Bücher sind älteren Datums, dürften jedoch immer noch gültig sein. Diese Handbücher und Anleitungen installieren Sie mit YaST.

51.7 Dokumentation zu den einzelnen Paketen

Bei der Installation eines Pakets wird auf Ihrem System ein neues Verzeichnis namens `/usr/share/doc/packages/Paketname` erstellt. Dort finden Sie informative Dateien vom Hersteller des Pakets wie auch Informationen von SUSE. Gelegentlich enthält dieses Verzeichnis auch Beispiele, Konfigurationsdateien, zusätzliche Skripts und Ähnliches. Für dieses Verzeichnis sind die folgenden Dateien vorgesehen, von denen jedoch die eine oder andere auch fehlen kann.

AUTHORS

Die Liste der wichtigsten Entwickler dieses Pakets und gewöhnlich deren Aufgaben.

BUGS

Bekannte Bugs und Fehler in diesem Paket. In der Regel auch ein Link zur Bugzilla-Webseite, auf der alle Bugs aufgeführt sind.

CHANGES, ChangeLog

Diese Datei enthält eine Übersicht der in den einzelnen Versionen vorgenommenen Änderungen. Die Datei dürfte nur für Entwickler interessant sein, da sie sehr detailliert ist.

COPYING, LICENSE

Lizenzinformationen.

FAQ

Mailing-Listen und Newsgroups entnommene Fragen und Antworten.

INSTALL

Anleitungen zur Installation des Pakets. Sie brauchen diese Datei normalerweise nicht zu lesen, da das Paket bereits auf Ihrem System installiert ist.

README, README.*

Allgemeine Informationen u. a. zur Funktion und Verwendung des Pakets.

TODO

Diese Datei beschreibt Funktionen, die in diesem Paket noch nicht implementiert, jedoch für spätere Versionen vorgesehen sind.

MANIFEST

Diese Datei enthält eine Übersicht über die im Paket enthaltenen Dateien.

NEWS

Beschreibung der Neuerungen in dieser Version.

51.8 Usenet

Das Usenet entstand bereits 1979, also noch vor dem Aufstieg des Internet, und ist damit eines der ältesten noch aktiven Computernetzwerke. Das Format und die Übertragung der Artikel in den dortigen Newsgroups ist vergleichbar mit der Handhabung von E-Mail-Nachrichten, nur dass hier die Diskussion unter mehreren Teilnehmern im Vordergrund steht.

Das Usenet ist in sieben thematische Bereiche gegliedert: `comp.*` für die Diskussion von Computer-Themen, `misc.*` für verschiedene Themen, `news.*` für Diskussionen über die Usenet Newsgroups selbst, `rec.*` für Freizeit und Unterhaltung, `sci.*` für wissenschaftliche Diskussionen, `soc.*` für gesellschaftliche Themen und `talk.*` für verschiedene kontroverse Themen. Diese Bereiche enthalten wiederum verschiedene Unterbereiche. So ist zum Beispiel `comp.os.linux.hardware` eine Newsgroup für Linux-spezifische Hardware-Fragen.

Bevor Sie einen Artikel in einer Newsgroup veröffentlichen können, müssen Sie sich mittels eines News-Clients mit einem News-Server verbinden und die gewünschte Newsgroup abonnieren. Als News-Client können Sie zum Beispiel Knode oder Evolution verwenden. Jeder News-Server steht mit anderen News-Servern in Verbindung und tauscht mit diesen Artikel aus. Allerdings stellt nicht jeder News-Server alle Newsgroups zur Verfügung.

Interessante Linux-Newsgroups sind unter anderem `comp.os.linux.apps`, `comp.os.linux.questions` und `comp.os.linux.hardware`. Wenn Sie eine bestimmte Newsgroup suchen, informieren Sie sich unter <http://www.linux.org/docs/usenetlinux.html>. Bitte beachten Sie die im Usenet üblichen Regeln, wie sie unter <http://www.faqs.org/faqs/usenet/posting-rules/part1/> beschrieben sind.

51.9 Standards und Spezifikationen

Informationen zu Standards und Spezifikationen werden von verschiedenen Organisationen zur Verfügung gestellt.

<http://www.linuxbase.org>

Die Free Standards Group ist eine unabhängige, gemeinnützige Organisation, deren Ziel die Verbreitung von freier und Open Source-Software ist. Dies soll durch die Definition von distributionsübergreifenden Standards erreicht werden. Unter der Führung dieser Organisation werden mehrere Standards gepflegt, unter anderem der für Linux sehr wichtige Standard LSB (Linux Standard Base).

<http://www.w3.org>

Das World Wide Web Consortium (W3C) ist wohl eine der bekanntesten Einrichtungen. Es wurde im Oktober 1994 von Tim Berners-Lee gegründet und konzentriert sich auf die Standardisierung von Webtechnologien. W3C fördert die Verbreitung

von offenen, lizenzfreien und herstellerunabhängigen Spezifikationen, wie HTML, XHTML und XML. Diese Webstandards werden in einem vierstufigen Prozess in *Working Groups* (Arbeitsgruppen) entwickelt und als *W3C Recommendations (REC)* (Empfehlungen des W3C) der Öffentlichkeit vorgestellt.

<http://www.oasis-open.org>

OASIS (Organization for the Advancement of Structured Information Standards) ist ein internationales Konsortium, das sich auf die Entwicklung von Standards zu Websicherheit, E-Business, Geschäftstransaktionen, Logistik und der Interoperabilität zwischen verschiedenen Märkten spezialisiert hat.

<http://www.ietf.org>

Die Internet Engineering Task Force (IETF) ist eine international agierende Gemeinschaft von Forschern, Netzwerkdesignern, Lieferanten und Anwendern. Sie konzentriert sich auf die Entwicklung der Internet-Architektur und den reibungslosen Betrieb des Internets durch Protokolle.

Jeder IETF-Standard wird als RFC (Request for Comments) veröffentlicht und ist gebührenfrei. Es gibt sechs Arten von RFCs: Proposed Standards (vorgeschlagene Standards), Draft Standards (Standardentwürfe), Internet Standards (Internet-Standards), Experimental Protocols (Protokolle in der Testphase), Information Documents (Dokumentation) und Historic Standards (historische Standards). Nur die ersten drei (Proposed, Draft und Internet) sind IETF-Standards im engeren Sinne (siehe hierzu auch die Zusammenfassung unter <http://www.ietf.org/rfc/rfc1796.txt>).

<http://www.ieee.org>

Das Institute of Electrical and Electronics Engineers (IEEE) ist eine Einrichtung, die Standards für die Bereiche Informationstechnologie, Telekommunikation, Medizin/Gesundheitswesen, Transportwesen und andere technische Bereiche entwickelt. IEEE-Standards sind kostenpflichtig.

<http://www.iso.org>

Das ISO-Komitee (International Organization for Standards) ist der weltgrößte Entwickler von Standards und unterhält ein Netzwerk von nationalen Normungsinstituten in über 140 Ländern. ISO-Standards sind kostenpflichtig.

<http://www.din.de>, <http://www.din.com>

Das Deutsche Institut für Normung (DIN) ist ein eingetragener, technisch-wissenschaftlicher Verein, der 1917 gegründet wurde. Laut DIN ist dieses Institut

„die für die Normungsarbeit zuständige Institution in Deutschland und vertritt die deutschen Interessen in den weltweiten und europäischen Normungsorganisationen“.

Der Verein ist ein Zusammenschluss von Herstellern, Verbrauchern, Handwerkern, Dienstleistungsunternehmen, Wissenschaftlern und anderen Personen, die ein Interesse an der Erstellung von Normen haben. Die Normen sind kostenpflichtig und können über die Homepage von DIN bestellt werden.

Häufige Probleme und deren Lösung

52

Dieses Kapitel beschreibt eine Reihe häufiger Probleme, die mit SUSE Linux Enterprise auftreten können; Ziel ist es, so viele verschiedene der potenziellen Probleme wie möglich abzudecken. Auf diese Weise finden Sie hier, auch wenn Ihr genaues Problem nicht aufgeführt ist, möglicherweise ein ganz ähnliches, das Rückschlüsse auf eine Lösung zulässt.

52.1 Ausfindigmachen von Informationen

Die Protokollierung unter Linux ist recht detailliert. Es gibt mehrere Quellen, die Sie bei einem Problem mit einem SUSE Linux Enterprise-System zurate ziehen können. Einige davon beziehen sich auf Linux-Systeme im Allgemeinen, einige sind speziell auf SUSE Linux Enterprise-Systeme ausgerichtet.

Nachfolgend finden Sie eine Liste der am häufigsten überprüften Protokolldateien und was sie normalerweise enthalten.

Protokolldatei	Beschreibung
<code>/var/log/boot.msg</code>	Meldungen vom Kernel beim Bootprozess.
<code>/var/log/mail.*</code>	Meldungen vom E-Mail-System.

Protokolldatei	Beschreibung
<code>/var/log/messages</code>	Ständige Meldungen vom Kernel und dem Systemprotokoll-Daemon während der Ausführung.
<code>/var/log/SaX.log</code>	Hardware-Meldungen von der SaX-Anzeige und dem KVM-System.
<code>/home/benutzer/.xsession-errors</code>	Meldungen von den zurzeit ausgeführten Desktop-Anwendungen. Ersetzen Sie <i>benutzer</i> durch den tatsächlichen Benutzernamen.
<code>/var/log/warn</code>	Alle Meldungen vom Kernel und dem Systemprotokoll-Daemon, denen die Stufe WARNUNG oder höher zugewiesen wurde.
<code>/var/log/wtmp</code>	Binärdatei mit Benutzeranmeldedatensätzen für die aktuelle Computersitzung. Die Anzeige erfolgt mit <code>last</code> .
<code>/var/log/Xorg.*.log</code>	Unterschiedliche Start- und Laufzeitprotokolle des X-Window-Systems. Hilfreich für die Fehlersuche bei Problemen beim Start von X.
<code>/var/log/YaST2/</code>	Verzeichnis, das die Aktionen von YAST und deren Ergebnissen enthält.
<code>/var/log/samba/</code>	Verzeichnis, das Protokollmeldungen vom Samba-Server und -Client enthält.

Linux bietet eine Reihe von Werkzeugen für die Systemanalyse und -überwachung. Unter [Kapitel 17, Dienstprogramme zur Systemüberwachung](#) (S. 353) finden Sie eine Auswahl der wichtigsten, die zur Systemdiagnose eingesetzt werden.

Jedes der nachfolgenden Szenarien beginnt mit einem Header, in dem das Problem beschrieben wird, gefolgt von ein oder zwei Absätzen mit Lösungsvorschlägen, verfü-

baren Referenzen für detailliertere Lösungen sowie Querverweisen auf andere Szenarien, die hiermit möglicherweise in Zusammenhang stehen.

52.2 Probleme bei der Installation

Probleme bei der Installation sind Situationen, wenn die Installation eines Computers nicht möglich ist. Der Vorgang kann entweder gar nicht ausgeführt bzw. das grafische Installationsprogramm kann nicht aufgerufen werden. In diesem Abschnitt wird auf einige typische Probleme eingegangen, die möglicherweise auftreten; außerdem finden Sie hier mögliche Lösungsansätze bzw. Tipps zur Umgehung solcher Fälle.

52.2.1 Kein bootfähiges CD-ROM-Laufwerk verfügbar

Wenn Ihr Computer kein bootfähiges CD- bzw. DVD-ROM-Laufwerk enthält bzw. das von Ihnen verwendete Laufwerk von Linux nicht unterstützt wird, gibt es mehrere Möglichkeiten zur Installation Ihres Computers ohne integriertes CD- bzw. DVD-Laufwerk:

Booten von einer Diskette

Erstellen Sie eine Bootdiskette und booten Sie von Diskette anstatt von CD oder DVD.

Verwenden eines externen Boot-Devices

Wenn es vom BIOS des Computers und dem Installationskernel unterstützt wird, booten Sie zu Installationszwecken von externen CD- oder DVD-Laufwerken.

Netzwerk-Boot über PXE

Wenn ein Computer kein CD- oder DVD-Laufwerk aufweist, jedoch eine funktionierende Ethernet-Verbindung verfügbar ist, führen Sie eine vollständige netzwerkbasierte Installation durch. Details finden Sie unter [Abschnitt 4.1.3](#), „Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN“ (S. 79) und [Abschnitt 4.1.6](#), „Installation auf entfernten Systemen über SSH – PXE-Boot und Wake-on-LAN“ (S. 84).

Booten von einer Diskette (SYSLINUX)

Ältere Computer verfügen möglicherweise über kein bootfähiges CD-ROM-Laufwerk, jedoch über ein Diskettenlaufwerk. Um die Installation auf einem System dieser Art vorzunehmen, erstellen Sie Bootdisketten und booten Sie Ihr System damit. Unter [Abschnitt 7.5.3, „Boot- und Rettungsdisketten“](#) (S. 174) finden Sie Anweisungen zur Erstellung von Bootdisketten mit YaST.

Die Bootdisketten enthalten den SYSLINUX-Loader und das linuxrc-Programm. SYSLINUX ermöglicht während der Bootprozedur die Auswahl eines Kernel sowie die Angabe sämtlicher Parameter, die für die verwendete Hardware erforderlich sind. Das linuxrc-Programm unterstützt das Laden von Kernel-Modulen für Ihre Hardware und startet anschließend die Installation.

Beim Booten von einer Bootdiskette wird die Bootprozedur vom Bootloader SYSLINUX initiiert (Paket `syslinux`). Wenn das System gebootet wird, führt SYSLINUX eine minimale Hardware-Erkennung durch, die hauptsächlich folgende Schritte umfasst:

1. Das Programm überprüft, ob das BIOS VESA 2.0-kompatible Framebuffer-Unterstützung bereitstellt, und bootet den Kernel entsprechend.
2. Die Überwachungsdaten (DDC info) werden gelesen.
3. Der erste Block der ersten Festplatte (MBR) wird gelesen, um bei der Bootloader-Konfiguration den Linux-Gerätenamen BIOS-IDs zuzuordnen. Das Programm versucht, den Block mithilfe der lba32-Funktionen des BIOS zu lesen, um zu ermitteln, ob das BIOS diese Funktionen unterstützt.

Wenn Sie beim Starten von SYSLINUX die Umschalttaste gedrückt halten, werden alle diese Schritte übersprungen. Fügen Sie für die Fehlersuche die Zeile

```
verbose 1
```

in `syslinux.cfg` ein, damit der Bootloader anzeigt, welche Aktion zurzeit ausgeführt wird.

Wenn der Computer nicht von der Diskette bootet, müssen Sie die Bootsequenz im BIOS möglicherweise in A, C, CDROM ändern.

Externe Boot-Devices

Die meisten CD-ROM-Laufwerke werden unterstützt. Wenn es beim Booten vom CD-ROM-Laufwerk zu Problemen kommt, versuchen Sie, anstelle der festgelegten CD von CD 2 zu booten.

Wenn das System kein CD-ROM-Laufwerk bzw. Diskettenlaufwerk aufweist, kann dennoch ein externes CD-ROM-Laufwerk, das übers USB (Universal Serial Bus, universeller serieller Bus) FireWire oder SCSI (Small Computer System Interface, Schnittstelle für Kleinrechnersysteme) verbunden ist, zum Booten des Systems verwendet werden. Dies ist hauptsächlich von der Interaktion zwischen dem BIOS und der verwendeten Hardware abhängig. In einigen Fällen kann bei Problemen eine BIOS-Aktualisierung hilfreich sein.

52.2.2 Vom Installationsmedium kann nicht gebootet werden

Es gibt zwei Gründe dafür, warum ein Computer nicht zu Installationszwecken gebootet werden kann:

CD- bzw. DVD-ROM-Laufwerk kann Boot-Image nicht lesen

Ihr CD-ROM-Laufwerk kann möglicherweise das Boot-Image von CD 1 nicht lesen. Verwenden Sie in diesem Fall CD 2 zum Booten des Systems. CD 2 enthält ein konventionelles Boot-Image mit 2,88 MB, das auch von nicht unterstützten Laufwerken gelesen werden kann und die Installation über das Netzwerk ermöglicht (siehe Beschreibung in [Kapitel 4, *Installation mit entferntem Zugriff*](#) (S. 75)).

Falsche Bootsequenz im BIOS

Für die BIOS-Bootsequenz muss "CD-ROM" als erster Eintrag für das Booten vorhanden sein. Andernfalls versucht der Computer, von einem anderen Medium zu booten, normalerweise von der Festplatte. Anweisungen zum Ändern der BIOS-Bootsequenz finden Sie in der Dokumentation zu Ihrem Motherboard bzw. in den nachfolgenden Abschnitten.

Als BIOS wird die Software bezeichnet, die die absolut grundlegenden Funktionen eines Computers ermöglicht. Motherboard-Hersteller stellen ein speziell für ihre Hardware konzipiertes BIOS bereit. Normalerweise kann nur zu einem bestimmten Zeitpunkt auf das BIOS-Setup zugegriffen werden – wenn der Computer gebootet wird. Während dieser Initialisierungsphase führt der Computer einige Diagnosetests der

Hardware durch. Einer davon ist die Überprüfung des Arbeitsspeichers, auf die durch einen Arbeitsspeicherzähler hingewiesen wird. Wenn der Zähler eingblendet wird, suchen Sie nach der Zeile, in der die Taste für den Zugriff auf das BIOS-Setup angegeben wird (diese Zeile befindet sich normalerweise unterhalb des Zählers oder am unteren Rand). Normalerweise muss die Taste **Entf**, **F1** oder **Esc** gedrückt werden. Halten Sie diese Taste gedrückt, bis der Bildschirm mit dem BIOS-Setup angezeigt wird.

Prozedur 52.1 *Ändern der BIOS-Bootsequenz*

- 1** Drücken Sie die aus den Bootroutinen hervorgehende Taste, um ins BIOS zu gelangen, und warten Sie, bis der BIOS-Bildschirm angezeigt wird.
- 2** Wenn Sie die Bootsequenz in einem AWARD BIOS ändern möchten, suchen Sie nach dem Eintrag *BIOS FEATURES SETUP* (SETUP DER BIOS-FUNKTIONEN). Andere Hersteller verwenden hierfür eine andere Bezeichnung, beispielsweise *ADVANCED CMOS SETUP* (ERWEITERTES CMOS-SETUP). Wenn Sie den Eintrag gefunden haben, wählen Sie ihn aus und bestätigen Sie ihn mit der **Eingabetaste**.
- 3** Suchen Sie im daraufhin angezeigten Bildschirm nach einem Untereintrag namens *BOOT SEQUENCE* (BOOTSEQUENZ). Die Bootsequenz ist häufig auf *C, A* bzw. *A, C* o. *Ä.* eingestellt. Im ersten Fall durchsucht der Computer erst die Festplatte (*C*) und dann das Diskettenlaufwerk (*A*) nach einem bootfähigen Medium. Ändern Sie die Einstellungen mithilfe der Taste **Bild-Auf** bzw. **Bild-Ab**, bis die Sequenz *A, CDROM, C* lautet.
- 4** Drücken Sie **Esc**, um den BIOS-Setup-Bildschirm zu schließen. Zum Speichern der Änderungen wählen Sie *SAVE & EXIT SETUP* (SPEICHERN & SETUP BEENDEN) oder drücken Sie **F10**. Um zu bestätigen, dass Ihre Einstellungen gespeichert werden sollen, drücken Sie **Y**.

Prozedur 52.2 *Ändern der Bootsequenz in einem SCSI-BIOS (Adaptec-Hostadapter)*

- 1** Mit **Strg** + **A** gelangen Sie ins Setup.
- 2** Wählen Sie *Disk Utilities* (Datenträgerprogramme), um die angeschlossenen Hardware-Komponenten anzuzeigen.

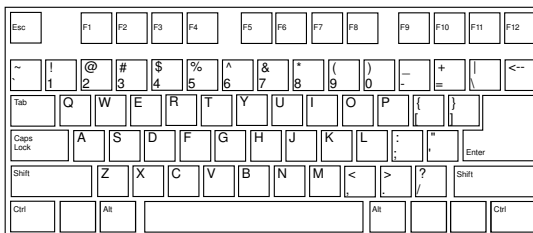
Notieren Sie sich die SCSI-ID Ihres CD-ROM-Laufwerks.

- 3** Verlassen Sie das Menü mit **Esc**.

- 4 Öffnen Sie *Configure Adapter Settings* (Adaptoreinstellungen konfigurieren). Wählen Sie unter *Additional Options* (Zusätzliche Optionen) den Eintrag *Boot Device Options* (Boot-Device-Optionen) aus und drücken Sie die Eingabetaste.
- 5 Geben Sie die ID des CD-ROM-Laufwerks ein und drücken Sie erneut die Eingabetaste.
- 6 Drücken Sie zweimal Esc, um zum Startbildschirm des SCSI-BIOS zurückzukehren.
- 7 Schließen Sie diesen Bildschirm und bestätigen Sie mit *Yes* (Ja), um den Computer zu booten.

Unabhängig von Sprache und Tastaturbelegung Ihrer endgültigen Installation wird in den meisten BIOS-Konfigurationen die US-Tastaturbelegung verwendet (siehe Abbildung):

Abbildung 52.1 US-Tastaturbelegung



52.2.3 Computer kann nicht gebootet werden

Bei bestimmter Hardware, insbesondere bei verhältnismäßig alter bzw. sehr neuer, tritt bei der Installation ein Fehler auf. In vielen Fällen ist dies darauf zurückzuführen, dass dieser Hardwaretyp im Installationskernel nicht unterstützt wird; oft sind auch bestimmte Funktionen dieses Kernel, beispielsweise ACPI (Advanced Configuration and Power Interface), die Ursache, die bei bestimmter Hardware nach wie vor zu Problemen führt.

Wenn Ihr System über den standardmäßigen Modus für die *Installation* (Installation) im ersten Installations-Boot-Bildschirm nicht installiert werden kann, gehen Sie folgendermaßen vor:

- 1 Belassen Sie die erste CD bzw. DVD im CD-ROM-Laufwerk und booten Sie den Computer über die Tastenkombination `Strg` + `Alt` + `Entf` bzw. über den Reset-Knopf der Hardware neu.
- 2 Navigieren Sie im Boot-Bildschirm mithilfe der Pfeiltasten der Tastatur zu *Installation--ACPI Disabled* (Installation – ACPI deaktiviert) und drücken Sie die `Eingabetaste`, um den Boot- und Installationsvorgang zu starten. Mit dieser Option wird die Unterstützung für ACPI-Energieverwaltungstechniken deaktiviert.
- 3 Fahren Sie wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben mit der Installation fort.

Wenn es hierbei zu Problemen kommt, fahren Sie wie oben beschrieben fort, wählen Sie jedoch in diesem Fall *Installation--Safe Settings* (Installation – Sichere Einstellungen) aus. Mit dieser Option wird die Unterstützung für ACPI und DMA (Direct Memory Access) deaktiviert. Mit dieser Option sollte das Booten der meisten Hardware möglich sein.

Wenn bei diesen beiden Optionen Probleme auftauchen, versuchen Sie mithilfe der Bootoptionen-Eingabeaufforderung sämtliche zusätzlichen Parameter, die für die Unterstützung dieses Hardwaretyps erforderlich sind, an den Installationskernel zu übermitteln. Weitere Informationen zu den Parametern, die als Bootoptionen zur Verfügung stehen, finden Sie in der Kernel-Dokumentation unter `/usr/src/linux/Documentation/kernel-parameters.txt`.

TIPP: Aufrufen der Kernel-Dokumentation

Installieren Sie das Paket `kernel-source`. Darin ist die Kernel-Dokumentation enthalten.

Es gibt noch einige andere mit ACPI in Zusammenhang stehende Kernel-Parameter, die vor dem Booten zu Installationszwecken an der Boot-Eingabeaufforderung eingegeben werden können:

`acpi=off`

Mit diesem Parameter wird das vollständige ACPI-Subsystem auf Ihrem Computer deaktiviert. Dies kann hilfreich sein, wenn ACPI von Ihrem Computer nicht unterstützt wird bzw. Sie vermuten, dass ACPI auf Ihrem Computer zu Problemen führt.

`acpi=force`

Aktivieren Sie ACPI in jedem Fall, auch wenn das BIOS Ihres Computers von vor dem Jahre 2000 stammt. Mit diesem Parameter wird ACPI auch aktiviert, wenn die Festlegung zusätzlich zu `acpi=off` erfolgt.

`acpi=noirq`

ACPI nicht für IRQ-Routing verwenden.

`acpi=ht`

Nur genügend ACPI ausführen, um Hyper-Threading zu aktivieren.

`acpi=strict`

Geringere Toleranz von Plattformen, die nicht genau der ACPI-Spezifikation entsprechen.

`pci=noacpi`

Deaktiviert das PCI-IRQ-Routing des neuen ACPI-Systems.

Nachdem Sie die richtige Parameterkombination ermittelt haben, schreibt YaST sie automatisch in die Bootloader-Konfiguration, um sicherzustellen, dass das System beim nächsten Mal vorschriftsmäßig gebootet wird.

Wenn beim Laden des Kernel oder bei der Installation unerwartete Fehler auftreten, wählen Sie im Boot-Menü die Option *Memory Test* (Speichertest), um den Arbeitsspeicher zu überprüfen. Wenn von *Memory Test* (Speichertest) ein Fehler zurückgegeben wird, liegt in der Regel ein Hardware-Fehler vor.

52.2.4 Grafisches Installationsprogramm lässt sich nicht starten

Nachdem Sie die erste CD oder DVD in das Laufwerk eingelegt und den Computer neu gebootet haben, wird der Installationsbildschirm angezeigt, nach der Auswahl von *Installation* wird jedoch das grafische Installationsprogramm nicht aufgerufen.

In diesem Fall haben Sie mehrere Möglichkeiten:

- Wählen Sie eine andere Bildschirmauflösung für die installationsbezogenen Dialogfelder.
- Wählen Sie den *Text Mode* (Expertenmodus) für die Installation aus.
- Führen Sie über VNC und unter Verwendung des grafischen Installationsprogramms eine entfernte Installation durch.

Wenn Sie für die Installation eine andere Bildschirmauflösung verwenden möchten, gehen Sie wie folgt vor:

- 1 Booten Sie zu Installationszwecken.
- 2 Drücken Sie **F3**, um ein Menü zu öffnen, in dem Sie für Installationszwecke eine niedrigere Auflösung auswählen können.
- 3 Wählen Sie *Installation* aus und fahren Sie, wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben, mit der Installation fort.

Zum Durchführen der Installation im Expertenmodus gehen Sie wie folgt vor:

- 1 Booten Sie zu Installationszwecken.
- 2 Drücken Sie **F3** und wählen Sie *Text Mode* (Expertenmodus) aus.
- 3 Wählen Sie *Installation* aus und fahren Sie, wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben, mit der Installation fort.

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

- 1 Booten Sie zu Installationszwecken.
- 2 Geben Sie an der Bootoptionen-Eingabeaufforderung folgenden Text ein:

```
vnc=1 vncpassword=beliebiges_passwort
```

Ersetzen Sie *beliebiges_passwort* durch das für die Installation zu verwendende Passwort.

- 3 Wählen Sie *Installation* (Installation) aus und drücken Sie dann die , um die Installation zu starten.

Anstatt direkt in die Routine für die grafische Installation einzusteigen, wird das System weiterhin im Expertenmodus ausgeführt und dann angehalten; in einer Meldung werden die IP-Adresse und die Portnummer angegeben, unter der über die Browserschnittstelle oder eine VNC-Viewer-Anwendung auf das Installationsprogramm zugegriffen werden kann.

- 4 Wenn Sie über einen Browser auf das Installationsprogramm zugreifen, starten Sie den Browser und geben Sie die Adressinformationen ein, die von den Installationsroutinen auf dem zukünftigen SUSE® Linux Enterprise-Computer bereitgestellt werden, und drücken Sie die :

```
http://ip_adresse_der_maschine:5801
```

Im Browserfenster wird ein Dialogfeld geöffnet, in dem Sie zur Eingabe des VNC-Passworts aufgefordert werden. Geben Sie das Passwort ein und fahren Sie, wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben, mit der Installation fort.

WICHTIG

Die Installation über VNC kann mit jedem Browser und unter jedem beliebigen Betriebssystem vorgenommen werden, vorausgesetzt, die Java-Unterstützung ist aktiviert.

Wenn Sie unter Ihrem bevorzugten Betriebssystem mit einem beliebigen VNC-Viewer arbeiten, geben Sie die IP-Adresse und das Passwort bei entsprechender Aufforderung ein. Daraufhin wird ein Fenster mit den installationsbezogenen Dialogfeldern geöffnet. Fahren Sie wie gewohnt mit der Installation fort.

52.2.5 Nur ein minimalistischer Boot-Bildschirm wird eingeblendet

Sie haben die erste CD oder DVD in das Laufwerk eingelegt, die BIOS-Routinen sind abgeschlossen, das System zeigt jedoch den grafischen Boot-Bildschirm nicht an. Stattdessen wird eine sehr minimalistische textbasierte Oberfläche angezeigt. Dies kann

auf Computern der Fall sein, die für die Darstellung eines grafischen Boot-Bildschirms nicht ausreichend Grafikspeicher aufweisen.

Obwohl der textbasierte Boot-Bildschirm minimalistisch wirkt, bietet er nahezu dieselbe Funktionalität wie der grafische:

Boot-Optionen

Im Gegensatz zur grafischen Oberfläche können die unterschiedlichen Bootoptionen nicht mithilfe der Cursortasten der Tastatur ausgewählt werden. Das Boot-Menü des Expertenmodus-Boot-Bildschirms ermöglicht die Eingabe einiger Schlüsselwörter an der Boot-Eingabeaufforderung. Diese Schlüsselwörter sind den Optionen in der grafischen Version zugeordnet. Treffen Sie Ihre Wahl und drücken Sie die `[Eingabetaste]`, um den Bootprozess zu starten.

Benutzerdefinierte Bootoptionen

Geben Sie nach der Auswahl einer Bootoption das entsprechende Schlüsselwort an der Boot-Eingabeaufforderung ein; Sie können auch einige benutzerdefinierte Boot-Optionen eingeben (siehe Beschreibung in [Abschnitt 52.2.3, „Computer kann nicht gebootet werden“](#) (S. 1003)). Wenn Sie den Installationsvorgang starten möchten, drücken Sie die `[Eingabetaste]`.

Bildschirmauflösungen

Die Bildschirmauflösung für die Installation lässt sich mithilfe der F-Tasten bestimmen. Wenn Sie im Expertenmodus, also im Textmodus, booten müssen, drücken Sie `[F3]`.

52.3 Probleme beim Booten

Probleme beim Booten sind Fälle, in denen Ihr System nicht vorschriftsmäßig gebootet wird, das Booten also nicht mit dem erwarteten Runlevel und Anmeldebildschirm erfolgt.

52.3.1 Probleme beim Laden des GRUB-Bootloaders

Wenn die Hardware vorschriftsmäßig funktioniert, wurde der Bootloader möglicherweise beschädigt und Linux kann auf dem Computer nicht gestartet werden. In diesem Fall

muss der Bootloader neu installiert werden. Gehen Sie zur erneuten Installation des Bootloader wie folgt vor:

- 1** Legen Sie das Installationsmedium in das Laufwerk ein.
- 2** Booten Sie den Computer neu.
- 3** Wählen Sie im Boot-Menü die Option *Installation* (Installation) aus.
- 4** Wählen Sie eine Sprache aus.
- 5** Nehmen Sie die Lizenzvereinbarung an.
- 6** Wählen Sie im Bildschirm *Installationsmodus* die Option *Experten* aus und legen Sie den Installationsmodus auf *Reparatur des installierten Systems* fest.
- 7** Wenn Sie sich im YaST-Modul für die Systemreparatur befinden, wählen Sie zunächst *Expertenwerkzeuge* und dann *Neuen Bootloader installieren* aus.
- 8** Stellen Sie die ursprünglichen Einstellungen wieder her und installieren Sie den Bootloader neu.
- 9** Beenden Sie die YaST-Systemreparatur und booten Sie das System neu.

Die Gründe dafür, dass der Computer nicht gebootet werden kann, stehen möglicherweise in Zusammenhang mit dem BIOS.

BIOS-Einstellungen

Überprüfen Sie Ihr BIOS auf Verweise auf Ihre Festplatte hin. GRUB wird möglicherweise einfach deshalb nicht gestartet, weil die Festplatte bei den aktuellen BIOS-Einstellungen nicht gefunden werden.

BIOS-Bootreihenfolge

Überprüfen Sie, ob die Festplatte in der Bootreihenfolge Ihres Systems enthalten ist. Wenn die Festplatten-Option nicht aktiviert wurde, wird Ihr System möglicherweise vorschriftsmäßig installiert. Das Booten ist jedoch nicht möglich, wenn auf die Festplatte zugegriffen werden muss.

52.3.2 Keine grafische Anmeldung

Wenn der Computer hochfährt, jedoch der grafische Anmelde-Manager nicht gebootet wird, müssen Sie entweder hinsichtlich der Auswahl des standardmäßigen Runlevel oder der Konfiguration des X-Window-Systems mit Problemen rechnen. Wenn Sie die Runlevel-Konfiguration überprüfen möchten, melden Sie sich als `root`-Benutzer an und überprüfen Sie, ob der Computer so konfiguriert ist, dass das Booten in Runlevel 5 erfolgt (grafischer Desktop). Eine schnelle Möglichkeit stellt das Überprüfen des Inhalts von `/etc/inittab` dar, und zwar folgendermaßen:

```
nld-machine:~ # grep "id:" /etc/inittab
id:5:initdefault:
nld-machine:~ #
```

Aus der zurückgegebenen Zeile geht hervor, dass der Standard-Runlevel des Computer (`initdefault`) auf 5 eingestellt ist und dass das Booten in den grafischen Desktop erfolgt. Wenn der Runlevel auf eine andere Nummer eingestellt ist, kann er über den YaST-Runlevel-Editor auf 5 eingestellt werden.

WICHTIG

Bearbeiten Sie die Runlevel-Konfiguration nicht manuell. Andernfalls überschreibt SUSEconfig (durch YaST ausgeführt) diese Änderungen bei der nächsten Ausführung. Wenn Sie hier manuelle Änderungen vornehmen möchten, deaktivieren Sie zukünftige Änderungen, indem Sie `CHECK_INITTAB` in `/etc/sysconfig/suseconfig` auf `no` (Nein) festlegen.

Wenn der Runlevel auf 5 eingestellt ist, kommt es möglicherweise zur Beschädigung des Desktop oder der Software von X Windows. Suchen Sie in den Protokolldateien von `/var/log/Xorg.*.log` nach detaillierten Meldungen vom X-Server beim versuchten Start. Wenn es beim Starten zu einem Problem mit dem Desktop kommt, werden möglicherweise Fehlermeldungen in `/var/log/messages` protokolliert. Wenn diese Fehlermeldungen auf ein Konfigurationsproblem mit dem X-Server hinweisen, versuchen Sie, diese Probleme zu beseitigen. Wenn das grafische System weiterhin nicht aktiviert wird, ziehen Sie die Neuinstallation des grafischen Desktop in Betracht.

Schneller Test: Durch den Befehl `startx` sollte das X-Window-System mit den konfigurierten Standardeinstellungen gestartet werden, wenn der Benutzer zurzeit bei der Konsole angemeldet ist. Wenn dies nicht funktioniert, sollten Fehler auf der Kon-

sole protokolliert werden. Weitere Informationen zur Konfiguration des X-Window-Systems finden Sie in [Kapitel 27, *Das X Window-System*](#) (S. 535).

52.4 Probleme bei der Anmeldung

Probleme bei der Anmeldung sind Fälle, in denen Ihr Computer in den erwarteten Begrüßungsbildschirm bzw. die erwartete Anmelde-Eingabeaufforderung bootet, den Benutzernamen und das Passwort jedoch entweder nicht akzeptiert oder zunächst akzeptiert, sich dann aber nicht erwartungsgemäß verhält (der grafische Desktop wird nicht gestartet, es treten Fehler auf, es wird wieder eine Kommandozeile angezeigt usw.).

52.4.1 Benutzer kann sich trotz gültigem Benutzernamen und Passwort nicht anmelden

Dieser Fall tritt normalerweise ein, wenn das System zur Verwendung von Netzwerkauthentifizierung oder Verzeichnisdiensten konfiguriert wurde und aus unbekanntem Grund keine Ergebnisse von den zugehörigen konfigurierten Servern abrufen kann. Der `root`-Benutzer ist der einzige lokale Benutzer, der sich noch bei diesen Computern anmelden kann. Nachfolgend sind einige der häufigen Ursachen dafür aufgeführt, dass ein Computer zwar funktionstüchtig zu sein scheint, jedoch Anmeldungen nicht ordnungsgemäß verarbeiten kann:

- Es liegt ein Problem mit der Netzwerkfunktion vor. Weitere Anweisungen hierzu finden Sie in [Abschnitt 52.5, „Probleme mit dem Netzwerk“](#) (S. 1018).
- DNS ist zurzeit nicht funktionsfähig (dadurch ist GNOME bzw. KDE nicht funktionsfähig und das System kann keine an sichere Server gerichteten bestätigten Anforderungen durchführen). Ein Hinweis, dass dies zutrifft, ist, dass der Computer auf sämtliche Aktionen ausgesprochen langsam reagiert. Weitere Informationen zu diesem Thema finden Sie in [Abschnitt 52.5, „Probleme mit dem Netzwerk“](#) (S. 1018).
- Wenn das System zur Verwendung von Kerberos konfiguriert wurde, hat die lokale Systemzeit möglicherweise die zulässige Abweichung zur Kerberos-Serverzeit

(üblicherweise 300 Sekunden) überschritten. Wenn NTP (Network Time Protocol) nicht ordnungsgemäß funktioniert bzw. lokale NTP-Server nicht funktionieren, kann auch die Kerberos-Authentifizierung nicht mehr verwendet werden, da sie von der allgemeinen netzwerkübergreifenden Uhrsynchronisierung abhängt.

- Die Authentifizierungskonfiguration des Systems ist fehlerhaft. Prüfen Sie die betroffenen PAM-Konfigurationsdateien auf Tippfehler oder falsche Anordnung von Direktiven hin. Zusätzliche Hintergrundinformationen zu PAM (Password Authentication Module) und der Syntax der betroffenen Konfigurationsdateien finden Sie in [Kapitel 28, Authentifizierung mit PAM](#) (S. 553).

In allen Fällen, in denen keine externen Netzwerkprobleme vorliegen, besteht die Lösung darin, das System erneut im Einzelbenutzermodus zu booten und die Konfigurationsfehler zu beseitigen, bevor Sie erneut in den Betriebsmodus booten und erneut versuchen, sich anzumelden. So booten Sie in den Einzelbenutzerbetrieb:

- 1 Booten Sie das System neu. Daraufhin wird der Boot-Bildschirm mit einer Eingabeaufforderung eingeblendet.
- 2 Geben Sie an der Boot-Eingabeaufforderung 1 ein, damit das System in den Einzelbenutzerbetrieb bootet.
- 3 Geben Sie Benutzername und Passwort für `root` ein.
- 4 Nehmen Sie alle erforderlichen Änderungen vor.
- 5 Booten Sie in den vollen Mehrbenutzer- und Netzwerkbetrieb, indem Sie `telinit 5` an der Kommandozeile eingeben.

52.4.2 Gültiger Benutzername/gültiges Passwort werden nicht akzeptiert

Dies ist das mit Abstand häufigste Problem, auf das Benutzer stoßen, da es hierfür zahlreiche Ursachen gibt. Je nachdem, ob Sie lokale Benutzerverwaltung und Authentifizierung oder Netzwerkauthentifizierung verwenden, treten Anmeldefehler aus verschiedenen Gründen auf.

Fehler bei der lokalen Benutzerverwaltung können aus folgenden Gründen auftreten:

- Der Benutzer hat möglicherweise das falsche Passwort eingegeben.
- Das Home-Verzeichnis des Benutzers, das die Desktopkonfigurationsdateien enthält, ist beschädigt oder schreibgeschützt.
- Möglicherweise bestehen hinsichtlich der Authentifizierung dieses speziellen Benutzers durch das X-Windows-System Probleme, insbesondere, wenn das Home-Verzeichnis des Benutzers vor der Installation der aktuellen Distribution für andere Linux-Distributionen verwendet wurde.

Gehen Sie wie folgt vor, um den Grund für einen Fehler bei der lokalen Anmeldung ausfindig zu machen:

- 1** Überprüfen Sie, ob der Benutzer sein Passwort richtig in Erinnerung hat, bevor Sie mit der Fehlersuche im gesamten Authentifizierungsmechanismus beginnen. Wenn sich der Benutzer eventuell nicht mehr an sein Passwort erinnert, können Sie es mithilfe des YaST-Moduls für die Benutzerverwaltung ändern.
- 2** Melden Sie sich als `root`-Benutzer an und untersuchen Sie `/var/log/messages` auf PAM-Fehlermeldungen und Fehlermeldungen aus dem Anmeldeprozess.
- 3** Versuchen Sie, sich von der Konsole aus anzumelden (mit `Strg` + `Alt` + `F1`). Wenn dies gelingt, liegt der Fehler nicht bei PAM, da die Authentifizierung dieses Benutzers auf diesem Computer möglich ist. Versuchen Sie, mögliche Probleme mit dem X-Window-System oder dem Desktop (GNOME bzw. KDE) ausfindig zu machen. Weitere Informationen finden Sie in [Abschnitt 52.4.3](#), „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“ (S. 1016) und [Abschnitt 52.4.4](#), „Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop“ (S. 1017).
- 4** Wenn das Home-Verzeichnis des Benutzers für eine andere Linux-Distribution verwendet wurde, entfernten Sie die Datei `Xauthority` aus dem Heimverzeichnis des Benutzers. Melden Sie sich mit `Strg` + `Alt` + `F1` bei der Konsole an und führen Sie `rm .Xauthority` als dieser Benutzer aus. Auf diese Weise sollten die X-Authentifizierungsprobleme dieses Benutzers beseitigt werden. Versuchen Sie erneut, sich beim grafischen Desktop anzumelden.
- 5** Wenn die grafikbasierte Anmeldung nicht möglich ist, melden Sie sich mit `Strg` + `Alt` + `F1` bei der Konsole an. Versuchen Sie, eine X-Sitzung in einer anderen Anzeige zu starten; die erste (`:0`) wird bereits verwendet:

```
startx -- :1
```

Daraufhin sollten ein grafikbasierter Bildschirm und Ihr Desktop angezeigt werden. Prüfen Sie andernfalls die Protokolldateien des X-Window-Systems (`/var/log/Xorg.anzeigenummer.log`) bzw. die Protokolldateien Ihrer Desktop-Anwendungen (`.xsession-errors` im Home-Verzeichnis des Benutzers) auf Unregelmäßigkeiten hin.

- 6 Wenn der Desktop aufgrund beschädigter Konfigurationsdateien nicht aufgerufen werden konnte, fahren Sie mit [Abschnitt 52.4.3, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“](#) (S. 1016) oder [Abschnitt 52.4.4, „Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop“](#) (S. 1017) fort.

Nachfolgend sind einige der häufigsten Ursachen dafür aufgeführt, warum es bei der Netzwerkauthentifizierung eines bestimmten Benutzers auf einem bestimmten Computer zu Problemen kommen kann:

- Der Benutzer hat möglicherweise das falsche Passwort eingegeben.
- Der Benutzername ist in den lokalen Authentifizierungsdateien des Computers vorhanden und wird zudem von einem Netzwerkauthentifizierungssystem bereitgestellt, was zu Konflikten führt.
- Das Home-Verzeichnis ist zwar vorhanden, ist jedoch beschädigt oder nicht verfügbar. Es ist möglicherweise schreibgeschützt oder befindet sich auf einem Server, auf den momentan nicht zugegriffen werden kann.
- Der Benutzer ist nicht berechtigt, sich bei diesem Host im Authentifizierungssystem anzumelden.
- Der Hostname des Computers hat sich geändert und der Benutzer ist nicht zur Anmeldung bei diesem Host berechtigt.
- Der Computer kann keine Verbindung mit dem Authentifizierungs- oder Verzeichnisserver herstellen, auf dem die Informationen dieses Benutzers gespeichert sind.
- Möglicherweise bestehen hinsichtlich der Authentifizierung dieses speziellen Benutzers durch das X-Window-System Probleme, insbesondere, wenn das Heimverzeichnis des Benutzers vor der Installation der aktuellen Distribution für andere Linux-Distributionen verwendet wurde.

Gehen Sie wie folgt vor, um die Ursache der Anmeldefehler bei der Netzwerkauthentifizierung zu ermitteln:

- 1** Überprüfen Sie, ob der Benutzer sein Passwort richtig in Erinnerung hat, bevor Sie mit der Fehlersuche im gesamten Authentifizierungsmechanismus beginnen.
- 2** Ermitteln Sie den Verzeichnisserver, den der Computer für die Authentifizierung verwendet, und vergewissern Sie sich, dass dieser ausgeführt wird und ordnungsgemäß mit den anderen Computern kommuniziert.
- 3** Überprüfen Sie, ob der Benutzername und das Passwort des Benutzers auf anderen Computern funktionieren, um sicherzustellen, dass seine Authentifizierungsdaten vorhanden sind und ordnungsgemäß verteilt wurden.
- 4** Finden Sie heraus, ob sich ein anderer Benutzer bei dem problembehafteten Computer anmelden kann. Wenn sich ein anderer Benutzer oder der `root`-Benutzer anmelden kann, melden Sie sich mit dessen Anmeldedaten an und überprüfen Sie die Datei `/var/log/messages`. Suchen Sie nach dem Zeitstempel, der sich auf die Anmeldeversuche bezieht, und finden Sie heraus, ob von PAM Fehlermeldungen generiert wurden.
- 5** Versuchen Sie, sich von der Konsole aus anzumelden (mit `Strg` + `Alt` + `F1`). Wenn dies gelingt, liegt der Fehler nicht bei PAM oder dem Verzeichnisserver mit dem Heimverzeichnis des Benutzers, da die Authentifizierung dieses Benutzers auf diesem Computer möglich ist. Versuchen Sie, mögliche Probleme mit dem X-Window-System oder dem Desktop (GNOME bzw. KDE) ausfindig zu machen. Weitere Informationen finden Sie in [Abschnitt 52.4.3, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“](#) (S. 1016) und [Abschnitt 52.4.4, „Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop“](#) (S. 1017).
- 6** Wenn das Home-Verzeichnis des Benutzers für eine andere Linux-Distribution verwendet wurde, entfernten Sie die Datei `Xauthority` aus dem Heimverzeichnis des Benutzers. Melden Sie sich mit `Strg` + `Alt` + `F1` bei der Konsole an und führen Sie `rm .Xauthority` als dieser Benutzer aus. Auf diese Weise sollten die X-Authentifizierungsprobleme dieses Benutzers beseitigt werden. Versuchen Sie erneut, sich beim grafischen Desktop anzumelden.
- 7** Wenn die grafikbasierte Anmeldung nicht möglich ist, melden Sie sich mit `Strg` + `Alt` + `F1` bei der Konsole an. Versuchen Sie, eine X-Sitzung in einer anderen Anzeige zu starten; die erste (`:0`) wird bereits verwendet:

```
startx -- :1
```

Daraufhin sollten ein grafikbasierter Bildschirm und Ihr Desktop angezeigt werden. Prüfen Sie andernfalls die Protokolldateien des X-Window-Systems (`/var/log/Xorg.anzeigennummer.log`) bzw. die Protokolldateien Ihrer Desktop-Anwendungen (`.xsession-errors` im Home-Verzeichnis des Benutzers) auf Unregelmäßigkeiten hin.

- 8 Wenn der Desktop aufgrund beschädigter Konfigurationsdateien nicht aufgerufen werden konnte, fahren Sie mit [Abschnitt 52.4.3, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“](#) (S. 1016) oder [Abschnitt 52.4.4, „Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop“](#) (S. 1017) fort.

52.4.3 Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop

Wenn dies für einen bestimmten Benutzer zutrifft, wurden die GNOME-Konfigurationsdateien des Benutzers möglicherweise beschädigt. Mögliche Symptome: Die Tastatur funktioniert nicht, die Geometrie des Bildschirms ist verzerrt oder es ist nur noch ein leeres graues Feld zu sehen. Die wichtige Unterscheidung ist hierbei, dass der Computer normal funktioniert, wenn sich ein anderer Benutzer anmeldet. Wenn dies der Fall ist, kann das Problem höchstwahrscheinlich verhältnismäßig schnell behoben werden, indem das GNOME-Konfigurationsverzeichnis des Benutzers an einen neuen Speicherort verschoben wird, da GNOME daraufhin ein neues initialisiert. Obwohl der Benutzer GNOME neu konfigurieren muss, gehen keine Daten verloren.

- 1 Melden Sie sich als `root`-Benutzer an.
- 2 Wechseln Sie mit `cd` zum Home-Verzeichnis des Benutzers.
- 3 Verschieben Sie die GNOME-Konfigurationsverzeichnisse des Benutzers an einen temporären Speicherort:

```
mv ~/.gconf ~/.gconf-ORIG-RECOVER
mv ~/.gnome2 ~/.gnome2-ORIG-RECOVER
```

- 4 Melden Sie sich ab.

- 5 Bitten Sie den Benutzer, sich anzumelden, untersagen Sie ihm jedoch jegliche Ausführung von Anwendungen.
- 6 Stellen Sie die individuellen Anwendungskonfigurationsdaten des Benutzers wieder her (einschließlich der Daten des Evolution-E-mail-Client), indem Sie das Verzeichnis `~/ .gconf-ORIG-RECOVER/apps/` folgendermaßen in das neue Verzeichnis `~/ .gconf` zurückkopieren:

```
cp -a ../.gconf-ORIG-RECOVER/apps ../.gconf/
```

Wenn dies die Ursache für die Anmeldeprobleme ist, versuchen Sie, nur die kritischen Anwendungsdaten herzustellen, und weisen Sie den Benutzer an, die restlichen Anwendungen neu zu konfigurieren.

52.4.4 Anmeldung erfolgreich, jedoch Problem mit KDE-Desktop

Es gibt mehrere Gründe dafür, warum sich Benutzer nicht bei einem KDE-Desktop anmelden können. Beschädigte Cache-Daten sowie beschädigte KDE-Desktop-Konfigurationsdateien können zu Problemen bei der Anmeldung führen.

Cache-Daten werden beim Desktop-Start zur Leistungssteigerung herangezogen. Wenn diese Daten beschädigt sind, wird der Startvorgang nur sehr langsam oder gar nicht ausgeführt. Durch das Entfernen dieser Daten müssen die Desktop-Starttroutinen ganz am Anfang beginnen. Dies nimmt mehr Zeit als ein normaler Startvorgang in Anspruch, die Daten sind jedoch im Anschluss intakt und der Benutzer kann sich anmelden.

Wenn die Cache-Dateien des KDE-Desktop entfernt werden sollen, geben Sie als `root`-Benutzer folgenden Befehl ein:

```
rm -rf /tmp/kde-benutzer /tmp/socket-benutzer
```

Ersetzen Sie *benutzer* durch den tatsächlichen Benutzernamen. Durch das Entfernen dieser beiden Verzeichnisse werden lediglich die beschädigten Cache-Dateien entfernt. Andere Dateien werden durch dieses Verfahren nicht beeinträchtigt.

Beschädigte Desktop-Konfigurationsdateien können stets durch die anfänglichen Konfigurationsdateien ersetzt werden. Wenn die vom Benutzer vorgenommenen Anpassungen wiederhergestellt werden sollen, kopieren Sie sie, nachdem die

Konfiguration mithilfe der standardmäßigen Konfigurationswerte wiederhergestellt wurde, sorgfältig von ihrem temporären Speicherort zurück.

Gehen Sie wie folgt vor, um die beschädigte Desktop-Konfiguration durch die anfänglichen Konfigurationswerte zu ersetzen:

1 Melden Sie sich als `root`-Benutzer an.

2 Begeben Sie sich in das Home-Verzeichnis des Benutzers:

```
cd /home/benutzer
```

3 Verschieben Sie das KDE-Konfigurationsverzeichnis sowie die `.skel`-Dateien an einen temporären Speicherort:

```
mv .kde .kde-ORIG-RECOVER
mv .skel .skel-ORIG-RECOVER
```

4 Melden Sie sich ab.

5 Bitten Sie den Benutzer, sich bei diesem Computer anzumelden.

6 Kopieren Sie nach dem erfolgreichen Aufruf des Desktop die Konfigurationen des Benutzers in das entsprechende Verzeichnis zurück:

```
cp -a .kde-ORIG-RECOVER/share .kde/share
```

WICHTIG

Wenn die vom Benutzer vorgenommenen Anpassungen zu den Anmeldeproblemen geführt haben und dies auch weiterhin tun, wiederholen Sie die oben beschriebenen Prozeduren, unterlassen Sie jedoch das Kopieren des Verzeichnisses `.kde/share`.

52.5 Probleme mit dem Netzwerk

Zahlreiche Probleme Ihres Systems stehen möglicherweise mit dem Netzwerk in Verbindung, obwohl zunächst ein anderer Eindruck entsteht. So kann beispielsweise ein Netzwerkproblem die Ursache sein, wenn sich Benutzer bei einem System nicht

anmelden können. In diesem Abschnitt finden Sie eine einfache Checkliste, anhand der Sie die Ursache jeglicher Netzwerkprobleme ermitteln können.

Gehen Sie zur Überprüfung der Netzwerkverbindung Ihres Computers folgendermaßen vor:

- 1** Wenn Sie eine Ethernet-Verbindung nutzen, überprüfen Sie zunächst die Hardware. Stellen Sie sicher, dass das Netzkabel fest mit dem Computer verbunden ist. Die Kontrolllampchen neben dem Ethernet-Anschluss (falls vorhanden) sollten beide leuchten.

Wenn keine Verbindung hergestellt werden kann, testen Sie, ob Ihr Netzkabel funktionstüchtig ist, wenn es mit einem anderen Computer verbunden wird. Wenn dies der Fall ist, ist das Problem auf Ihre Netzwerkkarte zurückzuführen. Wenn Hubs oder Switches Bestandteil Ihrer Netzwerkeinrichtung sind, können auch sie mögliche Auslöser sein.

- 2** Bei einer drahtlosen Verbindung testen Sie, ob die drahtlose Verbindung von anderen Computern hergestellt werden kann. Wenn dies nicht der Fall ist, wenden Sie sich an den Administrator des drahtlosen Netzwerks.
- 3** Nachdem Sie die grundlegende Netzwerkkonnektivität sichergestellt haben, versuchen Sie zu ermitteln, welcher Dienst nicht reagiert. Tragen Sie die Adressinformationen aller Netzwerkserver zusammen, die Bestandteil Ihrer Einrichtung sind. Suchen Sie sie entweder im entsprechenden YaST-Modul oder wenden Sie sich an Ihren Systemadministrator. In der nachfolgenden Liste sind einige der typischen Netzwerkserver aufgeführt, die Bestandteil einer Einrichtung sind; außerdem finden Sie hier die Symptome eines Ausfalls.

DNS (Namendienst)

Ein Namensdienst, der ausgefallen ist oder Fehlfunktionen aufweist, kann die Funktionsweise des Netzwerks auf vielfältige Weise beeinträchtigen. Wenn der lokale Computer hinsichtlich der Authentifizierung von Netzwerkservern abhängig ist und diese Server aufgrund von Problemen bei der Namensauflösung nicht gefunden werden, können sich die Benutzer nicht einmal anmelden. Computer im Netzwerk, die von einem ausgefallenen Namensserver verwaltet werden, sind füreinander nicht „sichtbar“ und können nicht kommunizieren.

NTP (Zeitdienst)

Ein NTP-Dienst, der ausgefallen ist oder Fehlfunktionen aufweist, kann die Kerberos-Authentifizierung und die X-Server-Funktionalität beeinträchtigen.

NFS (Dateidienst)

Wenn eine Anwendung Daten benötigt, die in einem NFS-eingehängten Verzeichnis gespeichert sind, kann sie nicht aufgerufen werden bzw. weist Fehlfunktionen auf, wenn dieser Dienst ausgefallen oder falsch konfiguriert ist. Im schlimmsten Fall wird die persönliche Desktop-Konfiguration eines Benutzers nicht angezeigt, wenn sein Home-Verzeichnis mit dem `.gconf-` bzw. `.kde-`Unterverzeichnis nicht gefunden wird, da der NFS-Server ausgefallen ist.

Samba (Dateidienst)

Wenn eine Anwendung Daten benötigt, die in einem Verzeichnis auf einem Samba-Server gespeichert sind, kann sie nicht aufgerufen werden bzw. weist Fehlfunktionen auf, wenn dieser Dienst ausgefallen ist.

NIS (Benutzerverwaltung)

Wenn Ihr SUSE Linux Enterprise-System hinsichtlich der Bereitstellung der Benutzerdaten von einem NIS-Server abhängig ist, können sich Benutzer nicht bei diesem Computer anmelden, wenn der NIS-Dienst ausgefallen ist.

LDAP (Benutzerverwaltung)

Wenn Ihr SUSE Linux Enterprise-System hinsichtlich der Bereitstellung der Benutzerdaten von einem LDAP-Server abhängig ist, können sich Benutzer nicht bei diesem Computer anmelden, wenn der LDAP-Dienst ausgefallen ist.

Kerberos (Authentifizierung)

In diesem Fall kann die Authentifizierung nicht vorgenommen werden und die Anmeldung ist bei keinem Computer möglich.

CUPS (Netzwerkdruck)

In diesem Fall können die Benutzer nicht drucken.

- 4 Überprüfen Sie, ob die Netzwerkserver aktiv sind und ob Ihre Netzwerkeinrichtung das Herstellen einer Verbindung ermöglicht:

WICHTIG

Das unten beschriebene Fehlersuchverfahren gilt nur für ein einfaches Setup aus Netzwerkserver/-Client, das kein internes Routing beinhaltet. Es wird davon ausgegangen, dass sowohl Server als auch Client Mitglieder desselben Subnetzes sind, ohne dass die Notwendigkeit für weiteres Routing besteht.

- a** Mit `ping hostname` (ersetzen Sie `hostname` durch den Hostnamen des Servers) können Sie überprüfen, ob die einzelnen Server verfügbar sind und ob vom Netzwerk aus auf sie zugegriffen werden kann. Wenn dieser Befehl erfolgreich ist, besagt dies, dass der von Ihnen gesuchte Host aktiv ist und dass der Namensdienst für Ihr Netzwerk vorschriftsmäßig konfiguriert ist.

Wenn beim Ping-Versuch die Meldung `destination host unreachable` zurückgegeben wird, also nicht auf den Ziel-Host zugegriffen werden kann, ist entweder Ihr System oder der gewünschte Server nicht vorschriftsmäßig konfiguriert oder ausgefallen. Überprüfen Sie, ob Ihr System erreichbar ist, indem Sie `ping ihr_hostname` von einem anderen Computer aus ausführen. Wenn Sie von einem anderen Computer aus auf Ihren Computer zugreifen können, ist der Server nicht aktiv oder nicht vorschriftsmäßig konfiguriert.

Wenn beim Ping-Versuch die Meldung `unknown host` zurückgegeben wird, der Host also nicht bekannt ist, ist der Namensdienst nicht vorschriftsmäßig konfiguriert oder der verwendete Hostname ist falsch. Mit `ping -nipadresse` können Sie versuchen, ohne den Namensdienst eine Verbindung mit diesem Host herzustellen. Wenn dieser Vorgang erfolgreich ist, überprüfen Sie die Schreibweise des Hostnamens und prüfen Sie, ob in Ihrem Netzwerk ein nicht vorschriftsmäßig konfigurierter Namensdienst vorhanden ist. Weitere Prüfungen dieser Art finden Sie unter [Schritt 4.b](#) (S. 1021). Wenn der Ping-Versuch weiterhin erfolglos ist, ist entweder Ihre Netzwerkkarte nicht vorschriftsmäßig konfiguriert bzw. Ihre Netzwerk-Hardware ist fehlerhaft. Informationen hierzu finden Sie unter [Schritt 4.c](#) (S. 1023).

- b** Mit `host hostname` können Sie überprüfen, ob der Hostname des Servers, mit dem Sie eine Verbindung herstellen möchten, vorschriftsmäßig in eine IP-Adresse übersetzt wird (und umgekehrt). Wenn bei diesem Befehl

die IP-Adresse dieses Host zurückgegeben wird, ist der Namensdienst aktiv. Wenn es bei diesem `host`-Befehl zu einem Problem kommt, überprüfen Sie alle Netzwerkkonfigurationsdateien, die für die Namen- und Adressauflösung auf Ihrem Host relevant sind:

```
/etc/resolv.conf
```

Mithilfe dieser Datei wissen Sie stets, welchen Namensserver und welche Domäne Sie zurzeit verwenden. Diese Datei kann manuell bearbeitet oder unter Verwendung von YaST oder DHCP automatisch angepasst werden. Die automatische Anpassung ist empfehlenswert. Stellen Sie jedoch sicher, dass diese Datei die nachfolgend angegebene Struktur aufweist und dass alle Netzwerkadressen und Domännennamen richtig sind:

```
search vollständiger_domänename  
nameserver ipadresse_von_nameserver
```

Diese Datei kann die Adresse eines oder mehrerer Namensserver enthalten, mindestens einer davon muss aber richtig sein, um die Namensauflösung für Ihren Host bereitzustellen. Passen Sie diese Datei im Bedarfsfall unter Verwendung des YaST-Moduls für den DNS- und Hostnamen an.

Wenn Ihre Netzwerkverbindung über DHCP erfolgt, aktivieren Sie DHCP, um die Informationen zum Hostnamen und Namensdienst zu ändern, indem Sie im YaST-Modul für den DNS- und Hostnamen die Optionen *Hostnamen über DHCP ändern* und *Namensserver und Suchliste über DHCP aktualisieren* auswählen.

```
/etc/nsswitch.conf
```

Aus dieser Datei geht hervor, wo Linux nach Namensdienstinformationen suchen soll. Sie sollte folgendes Format aufweisen:

```
...  
hosts: files dns  
networks: files dns  
...
```

Der Eintrag `dns` ist von großer Bedeutung. Hiermit wird Linux angewiesen, einen externen Namensserver zu verwenden. Normalerweise werden diese Einträge von YaST automatisch erstellt, es empfiehlt sich jedoch, dies zu überprüfen.

Wenn alle relevanten Einträge auf dem Host richtig sind, lassen Sie Ihren Systemadministrator die DNS-Serverkonfiguration auf die richtigen Zoneninformationen hin prüfen. Detaillierte Informationen zu DNS finden Sie in [Kapitel 34, Domain Name System \(DNS\)](#) (S. 681). Wenn Sie sichergestellt haben, dass die DNS-Konfiguration auf Ihrem Host und dem DNS-Server richtig ist, überprüfen Sie als Nächstes die Konfiguration Ihres Netzwerks und Netzwerkgeräts.

- c** Wenn von Ihrem System keine Verbindung mit dem Netzwerk hergestellt werden kann und Sie Probleme mit dem Namensdienst mit Sicherheit als Ursache ausschließen können, überprüfen Sie die Konfiguration Ihrer Netzwerkkarte.

Verwenden Sie den Befehl `ifconfig netzwerkgerät` (Ausführung als `root`), um zu überprüfen, ob dieses Gerät vorschriftsmäßig konfiguriert ist. Stellen Sie sicher, dass sowohl die `inet address` (inet-Adresse) als auch die `Mask` (Maske) ordnungsgemäß konfiguriert sind. Wenn die IP-Adresse einen Fehler enthält oder die Netzwerkmaske unvollständig ist, kann Ihre Netzwerkkonfiguration nicht verwendet werden. Führen Sie diese Überprüfung im Bedarfsfall auch auf dem Server durch.

- d** Wenn der Namensdienst und die Netzwerk-Hardware ordnungsgemäß konfiguriert und aktiv/verfügbar sind, bei einigen externen Netzwerkverbindungen jedoch nach wie vor lange Zeitüberschreitungen auftreten bzw. der Verbindungsaufbau überhaupt nicht möglich ist, können Sie mit `traceroute vollständiger_domänename` (Ausführung als `root`) die Netzwerkroute dieser Anforderungen überwachen. Mit diesem Befehl werden sämtliche Gateways (Sprünge) aufgelistet, die eine Anforderung von Ihrem Computer auf ihrem Weg zu ihrem Ziel passiert. Mit ihm wird die Antwortzeit der einzelnen Sprünge (Hops) aufgelistet und es wird ersichtlich, ob dieser Sprung überhaupt erreichbar ist. Verwenden Sie eine Kombination von "traceroute" und "ping", um die Ursache des Problems ausfindig zu machen, und informieren Sie die Administratoren.

Nachdem Sie die Ursache Ihres Netzwerkproblems ermittelt haben, können Sie es selbst beheben (wenn es auf Ihrem Computer vorliegt) oder die Administratoren Ihres Netzwerks entsprechend informieren, damit sie die Dienste neu konfigurieren bzw. die betroffenen Systeme reparieren können.

52.6 Probleme mit Daten

Probleme mit Daten treten auf, wenn der Computer entweder ordnungsgemäß gebootet werden kann oder nicht, in jedem Fall jedoch offensichtlich ist, dass Daten auf dem System beschädigt wurden und das System wiederhergestellt werden muss. In dieser Situation muss eine Sicherung Ihrer kritischen Daten durchgeführt werden, damit Sie wieder zu dem Zustand zurückkehren können, in dem sich Ihr System befand, bevor das Problem auftrat. SUSE Linux Enterprise bietet spezielle YaST-Module für die Systemsicherung und -wiederherstellung sowie ein Rettungssystem, das die externe Wiederherstellung eines beschädigten Systems ermöglicht.

52.6.1 Sichern kritischer Daten

Systemsicherungen können mithilfe des Yast-Moduls für Systemsicherungen problemlos vorgenommen werden.

- 1 Rufen Sie YaST als `root`-Benutzer auf und wählen Sie *System* → *Sicherungskopie der Systembereiche* aus.
- 2 Erstellen Sie ein Sicherungsprofil mit allen für die Sicherung erforderlichen Details, dem Dateinamen der Archivdatei, dem Umfang sowie dem Sicherungstyp:
 - a Wählen Sie *Profilverwaltung* → *Hinzufügen* aus.
 - b Geben Sie einen Namen für das Archiv ein.
 - c Geben Sie den Pfad für den Speicherort der Sicherung ein, wenn Sie lokal über eine Sicherung verfügen möchten. Damit Ihre Sicherung auf einem Netzwerkserver archiviert werden kann (über NFS), geben Sie die IP-Adresse oder den Namen des Servers und des Verzeichnisses für die Speicherung Ihres Archivs an.
 - d Bestimmen Sie den Archivtyp und klicken Sie dann auf *Weiter*.
 - e Bestimmen Sie die zu verwendenden Sicherungsoptionen; geben Sie beispielsweise an, ob Dateien gesichert werden sollen, die keinem Paket zugehörig sind, und ob vor der Erstellung des Archivs eine Liste der Dateien angezeigt werden soll. Legen Sie außerdem fest, ob geänderte

Dateien durch den zeitintensiven MDS-Mechanismus identifiziert werden sollen.

Mit *Erweitert* gelangen Sie in ein Dialogfeld für die Sicherung ganzer Festplattenbereiche. Diese Option hat zurzeit nur für das Ext2-Dateisystem Gültigkeit.

- f** Legen Sie abschließend die Suchoptionen fest, um bestimmte Systembereiche von der Sicherung auszuschließen, die nicht gesichert werden müssen, beispielsweise Lock- oder Cache-Dateien. Fügen Sie Einträge hinzu, bearbeiten oder löschen Sie sie, bis die Liste Ihren Vorstellungen entspricht, und schließen Sie das Dialogfeld mit *OK*.

- 3** Nachdem Sie die Profileinstellungen festgelegt haben, können Sie die Sicherung umgehend mit *Sicherungskopie erstellen* beginnen oder die automatische Sicherung konfigurieren. Sie können auch weitere Profile erstellen, die auf andere Zwecke zugeschnitten sind.

Zum Konfigurieren der automatischen Sicherung für ein bestimmtes Profil gehen Sie wie folgt vor:

- 1** Wählen Sie im Menü *Profilverwaltung* die Option *Automatische Sicherungskopie* aus.
- 2** Wählen Sie *Sicherungskopie automatisch starten* aus.
- 3** Legen Sie die Sicherungshäufigkeit fest. Wählen Sie *Täglich*, *Wöchentlich* oder *Monatlich* aus.
- 4** Legen Sie die Startzeit für die Sicherung fest. Diese Einstellungen werden durch die ausgewählte Sicherungshäufigkeit bestimmt.
- 5** Geben Sie an, ob alte Sicherungen beibehalten werden sollen, und wenn ja, wie viele. Wenn eine automatisch generierte Statusmeldung bezüglich des Sicherungsvorgangs ausgegeben werden soll, aktivieren Sie *Mail mit Zusammenfassung an Benutzer 'root' senden*.
- 6** Klicken Sie auf *OK*, um die Einstellungen zu speichern. Danach wird die erste Sicherung zum angegebenen Zeitpunkt gestartet.

52.6.2 Wiederherstellen einer Systemsicherung

Mithilfe des YaST-Moduls für die Systemwiederherstellung kann die Systemkonfiguration anhand einer Sicherung wiederhergestellt werden. Sie können entweder die gesamte Sicherung wiederherstellen oder bestimmte Komponenten auswählen, die beschädigt wurden und wieder in ihren alten Zustand zurückversetzt werden sollen.

- 1 Wählen Sie die Optionsfolge *YaST* → *System* → *System wiederherstellen*.
- 2 Geben Sie den Speicherort der Sicherungsdatei ein. Hierbei kann es sich um eine lokale Datei, um eine im Netzwerk eingehängte Datei oder eine Datei auf einem Wechselmedium handeln, beispielsweise einer Diskette oder CD. Klicken Sie anschließend auf *Weiter*.

Im nachfolgenden Dialogfeld ist eine Zusammenfassung der Archiveigenschaften zu sehen, beispielsweise Dateinamen, Erstellungsdatum, Sicherungstyp sowie optionale Kommentare.

- 3 Überprüfen Sie den archivierten Inhalt, indem Sie auf *Inhalt des Archivs klicken*. Mit *OK* kehren Sie zum Dialogfeld *Eigenschaften des Archivs* zurück.
- 4 Mit *Optionen für Experten* gelangen Sie in ein Dialogfeld, in dem Sie den Wiederherstellungsvorgang präzisieren können. Kehren Sie zum Dialogfeld *Eigenschaften des Archivs* zurück, indem Sie auf *OK* klicken.
- 5 Klicken Sie auf *Weiter*, um die wiederherzustellenden Pakete anzuzeigen. Mit *Übernehmen* werden alle Dateien im Archiv wiederhergestellt. Mit den Schaltflächen *Alle auswählen*, *Alle abwählen* und *Dateien wählen* können Sie Ihre Auswahl präzisieren. Verwenden Sie die Option *RPM-Datenbank wiederherstellen* nur, wenn die RPM-Datenbank beschädigt oder gelöscht wurde und in der Sicherung enthalten ist.
- 6 Wenn Sie auf *Übernehmen* klicken, wird die Sicherung wiederhergestellt. Wenn der Wiederherstellungsvorgang abgeschlossen ist, schließen Sie das Modul mit *Beenden*.

52.6.3 Wiederherstellen eines beschädigten Systems

Ein System kann aus mehreren Gründen nicht aktiviert und ordnungsgemäß betrieben werden. Zu den häufigsten Gründen zählen ein beschädigtes Dateisystem nach einem Systemabsturz, beschädigte Konfigurationsdateien oder eine beschädigte Bootloader-Konfiguration.

SUSE Linux Enterprise bietet zwei Methoden für den Umgang mit dieser Art von Situation. Sie können entweder die YaST-Systemreparatur verwenden oder das Rettungssystem booten. Die folgenden Abschnitte befassen sich mit beiden Arten der Systemreparatur.

Verwenden der YaST-Systemreparatur

Vor dem Start des YaST-Moduls zur Systemreparatur sollten Sie ermitteln, in welchem Modus das Modul ausgeführt werden sollte, damit es am besten Ihren Bedürfnissen entspricht. Je nach Ihren Fachkenntnissen und Schweregrad und Ursache des Systemausfalls und können Sie zwischen drei verschiedenen Modi wählen.

Automatische Reparatur

Wenn Ihr System aufgrund einer unbekanntenen Ursache ausgefallen ist, und Sie nicht wissen, welcher Teil des Systems für den Ausfall verantwortlich ist, sollten Sie *Automatische Reparatur* verwenden. Eine umfassende automatische Prüfung wird an allen Komponenten des installierten Systems durchgeführt. Eine detaillierte Beschreibung dieses Verfahrens finden Sie in „[Automatische Reparatur](#)“ (S. 1028).

Benutzerdefinierte Reparatur

Wenn Ihr System ausgefallen ist und Sie bereits wissen, an welcher Komponente es liegt, können Sie die langwierige Systemprüfung von *Automatische Reparatur* abkürzen, indem Sie den Bereich der Systemanalyse auf die betreffenden Komponenten beschränken. Wenn die Systemmeldungen vor dem Ausfall beispielsweise auf einen Fehler mit der Paketdatenbank hindeuten, können Sie das Analyse- und Reparaturverfahren so einschränken, dass nur dieser Aspekt des Systems überprüft und wiederhergestellt wird. Eine detaillierte Beschreibung dieses Verfahrens finden Sie in „[Benutzerdefinierte Reparatur](#)“ (S. 1030).

Expertenwerkzeuge

Wenn Sie bereits eine klare Vorstellung davon haben, welche Komponente ausgefallen ist und wie dieser Fehler behoben werden kann, können Sie die Analyseläufe überspringen und die für die Reparatur der betreffenden Komponente erforderlichen Werkzeuge unmittelbar anwenden. Detaillierte Informationen finden Sie in „[Expertenwerkzeuge](#)“ (S. 1031).

Wählen Sie einen der oben beschriebenen Reparaturmodi aus und setzen Sie die Systemreparatur, wie in den folgenden Abschnitten beschrieben, fort.

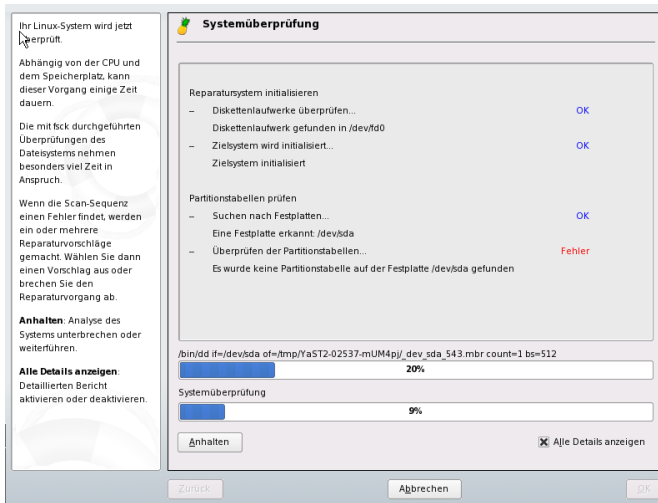
Automatische Reparatur

Um den Modus für automatische Reparatur der YaST-Systemreparatur zu starten, gehen Sie wie folgt vor:

- 1** Booten Sie das System mit dem Original-Installationsmedium, das sie für die ursprüngliche Installation verwendet haben (wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben).
- 2** Wählen Sie unter *Systemanalyse* die Optionsfolge *Andere* → *Reparatur des installierten Systems* aus.
- 3** Wählen Sie *Automatische Reparatur*.

YaST startet nun eine umfassende Analyse des installierten Systems. Der Verlauf des Vorgangs wird unten auf dem Bildschirm mit zwei Verlaufs Balken angezeigt. Der obere Balken zeigt den Verlauf des aktuell ausgeführten Tests. Der untere Balken zeigt den Gesamtverlauf des Analysevorgangs. Im Protokollfenster im oberen Abschnitt werden der aktuell ausgeführte Test und sein Ergebnis aufgezeichnet. Siehe [Abbildung 52.2, „Modus "Automatische Reparatur"“](#) (S. 1029). Die folgenden Haupttestläufe werden bei jeder Ausführung durchgeführt. Sie enthalten jeweils eine Reihe einzelner Untertests.

Abbildung 52.2 Modus "Automatische Reparatur"



Partitionstabellen aller Festplatten

Überprüft Validität und Kohärenz der Partitionstabellen aller erkannten Festplatten.

Swap-Partitionen

Die Swap-Partitionen des installierten Systems werden erkannt, getestet und gegebenenfalls zur Aktivierung angeboten. Das Angebot sollte angenommen werden, um eine höhere Geschwindigkeit für die Systemreparatur zu erreichen.

Dateisysteme

Alle gefundenen Dateisysteme werden einer dateisystem-spezifischen Prüfung unterworfen.

Einträge in der Datei `/etc/fstab`

Die Einträge in der Datei werden auf Vollständigkeit und Konsistenz überprüft. Alle gültigen Partitionen werden eingehängt.

Konfiguration des Bootloaders

Die Bootloader-Konfiguration des installierten Systems (GRUB oder LILO) wird auf Vollständigkeit und Kohärenz überprüft. Boot- und Root-Geräte werden untersucht, und die Verfügbarkeit der `initrd`-Module wird überprüft.

Paketdatenbank

Mit dieser Option wird überprüft, ob alle für den Betrieb einer Minimalinstallation erforderlichen Pakete vorliegen. Es ist zwar möglich, die Basispakete ebenfalls zu analysieren, dies dauert jedoch aufgrund ihrer großen Anzahl sehr lange.

- 4 Immer wenn ein Fehler gefunden wird, wird der Vorgang angehalten und es öffnet sich ein Dialogfeld, in dem die Details und die möglichen Lösungen beschrieben werden.

Lesen Sie die Bildschirmmeldungen genau durch, bevor Sie die vorgeschlagene Reparaturmöglichkeit akzeptieren. Wenn Sie eine vorgeschlagene Lösung ablehnen, werden keine Änderungen am System vorgenommen.

- 5 Klicken Sie nach erfolgreicher Beendigung des Reparaturvorgangs auf *OK* und *Beenden* und entfernen Sie die Installationsmedien. Das System wird automatisch neu gebootet.

Benutzerdefinierte Reparatur

Um den Modus *Benutzerdefinierte Reparatur* zu starten und ausgewählte Komponenten des installierten Systems zu prüfen, gehen Sie wie folgt vor:

- 1 Booten Sie das System mit dem Original-Installationsmedium, das sie für die ursprüngliche Installation verwendet haben (wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben).
- 2 Wählen Sie unter *Systemanalyse* die Optionsfolge *Andere* → *Reparatur des installierten Systems* aus.
- 3 Wählen Sie *Benutzerdefinierte Reparatur*.

Bei Auswahl von *Benutzerdefinierte Reparatur* wird eine Liste der Testläufe angezeigt, die zunächst alle für die Ausführung markiert sind. Der Gesamttestbereich entspricht dem der automatischen Reparatur. Wenn Sie bereits Systembereiche kennen, in denen kein Schaden vorliegt, heben Sie die Markierung der entsprechenden Tests auf. Beim Klicken auf *Weiter* wird ein engeres Testverfahren gestartet, für dessen Ausführung vermutlich wesentlich weniger Zeit erforderlich ist.

Nicht alle Testgruppen können individuell angewendet werden. Die Analyse der fstab-Einträge ist stets an eine Untersuchung der Dateisysteme gebunden, einschließlich bestehender Swap-Partitionen. YaST löst solche Abhängigkeiten automatisch auf, indem es die kleinste Zahl an erforderlichen Testläufen auswählt.

- 4 Immer wenn ein Fehler gefunden wird, wird der Vorgang angehalten und es öffnet sich ein Dialogfeld, in dem die Details und die möglichen Lösungen beschrieben werden.

Lesen Sie die Bildschirmmeldungen genau durch, bevor Sie die vorgeschlagene Reparaturmöglichkeit akzeptieren. Wenn Sie eine vorgeschlagene Lösung ablehnen, werden keine Änderungen am System vorgenommen.

- 5 Klicken Sie nach erfolgreicher Beendigung des Reparaturvorgangs auf *OK* und *Beenden* und entfernen Sie die Installationsmedien. Das System wird automatisch neu gebootet.

Expertenwerkzeuge

Wenn Sie mit SUSE® Linux Enterprise vertraut sind und bereits eine genaue Vorstellung davon haben, welche Komponenten in Ihrem System repariert werden müssen, können Sie die Systemanalyse überspringen und die Werkzeuge direkt anwenden.

Um die Funktion *Expertenwerkzeuge* der YaST-Systemreparatur zu verwenden, fahren Sie wie folgt fort:

- 1 Booten Sie das System mit dem Original-Installationsmedium, das sie für die ursprüngliche Installation verwendet haben (wie in [Kapitel 3, *Installation mit YaST*](#) (S. 37) beschrieben).
- 2 Wählen Sie unter *Systemanalyse* die Optionsfolge *Andere* → *Reparatur des installierten Systems* aus.
- 3 Wählen Sie *Expertenwerkzeuge* und anschließend eine oder mehrere Reparaturoptionen aus.
- 4 Klicken Sie nach erfolgreicher Beendigung des Reparaturvorgangs auf *OK* und *Beenden* und entfernen Sie die Installationsmedien. Das System wird automatisch neu gebootet.

In den Expertenwerkzeugen stehen die folgenden Optionen zum Reparieren des fehlerhaften Systems zur Verfügung:

Neuen Bootloader installieren

Dadurch wird das Konfigurationsmodul für den YaST-Bootloader gestartet. Einzelheiten finden Sie in [Abschnitt 21.3, „Konfigurieren des Bootloaders mit YaST“](#) (S. 448).

Partitionierer starten

Mit dieser Option wird das Expertenwerkzeug für die Partitionierung in YaST gestartet. Einzelheiten finden Sie in [Abschnitt 7.5.8, „Partitionierung“](#) (S. 176).

Reparatur des Dateisystems

Mit dieser Option werden die Dateisysteme Ihrer installierten Systeme überprüft. Ihnen wird zunächst eine Auswahl aller erkannten Partitionen angeboten, aus denen Sie die zu überprüfenden auswählen können.

Verlorene Partitionen wiederherstellen

Sie können versuchen, beschädigte Partitionstabellen zu rekonstruieren. Zunächst wird eine Liste der erkannten Festplatten zur Auswahl angeboten. Durch Klicken auf *OK* wird die Untersuchung gestartet. Je nach Prozessorleistung und Größe der Festplatte kann dieser Vorgang einige Zeit in Anspruch nehmen.

WICHTIG: Rekonstruktion von Partitionstabellen

Die Rekonstruktion einer Partitionstabellen ist ein komplizierter Vorgang. YaST versucht, verloren gegangene Partitionen durch Analyse der Datensektoren der Festplatte wiederherzustellen. Die verlorenen Partitionen werden, wenn sie erkannt werden, zur neu erstellten Partitionstabelle hinzugefügt. Dies ist jedoch nicht in allen vorstellbaren Fällen erfolgreich.

Systemeinstellungen auf Diskette speichern

Mit dieser Option werden wichtige Systemdateien auf eine Diskette gespeichert. Wenn eine dieser Dateien beschädigt wird, kann Sie von der Diskette wiederhergestellt werden.

Installierte Software prüfen

Mit dieser Option werden die Konsistenz der Paketdatenbank und die Verfügbarkeit der wichtigsten Pakete überprüft. Mit diesem Werkzeug können alle beschädigten Installationspakete wiederhergestellt werden.

Verwenden des Rettungssystems

Ihr Linux-System beinhaltet ein Rettungssystem. Das Rettungssystem ist ein kleines Linux-System, das auf einen RAM-Datenträger geladen und als Root-Dateisystem eingehängt werden kann. Es ermöglicht Ihnen so den externen Zugriff auf Ihre Linux-Partitionen. Mithilfe des Rettungssystems kann jeder wichtige Aspekt Ihres Systems wiederhergestellt oder geändert werden:

- Jede Art von Konfigurationsdatei kann bearbeitet werden.
- Das Dateisystem kann auf Fehler hin überprüft und automatische Reparaturvorgänge können gestartet werden.
- Der Zugriff auf das installierte System kann in einer „change-root“-Umgebung erfolgen.
- Die Bootloader-Konfiguration kann überprüft, geändert und neu installiert werden.
- Die Größe von Partitionen kann mithilfe des parted-Befehls verändert werden. Weitere Informationen zu diesem Tool finden Sie auf der Website von GNU Parted (<http://www.gnu.org/software/parted/parted.html>).

Das Rettungssystem kann aus verschiedenen Quellen und von verschiedenen Speicherorten geladen werden. Am einfachsten lässt sich das Rettungssystem von der Original-Installations-CD bzw. -DVD booten:

- 1 Legen Sie das Installationsmedium in das CD- bzw. DVD-Laufwerk ein.
- 2 Booten Sie das System neu.
- 3 Wählen Sie im Boot-Bildschirm die Option *Rescue System* aus.
- 4 Geben Sie an der Eingabeaufforderung `Rescue: root` ein. Ein Passwort ist nicht erforderlich.

Wenn Ihnen kein CD- bzw. DVD-Laufwerk zur Verfügung steht, können Sie das Rettungssystem von einer Netzwerkquelle (einschließlich des SUSE-FTP-Servers) booten. Das nachfolgende Beispiel bezieht sich auf das entfernte Booten – wenn Sie ein anderes Boot-Medium verwenden, beispielsweise eine Diskette, ändern Sie die Datei `info` entsprechend und führen Sie den Boot-Vorgang wie bei einer normalen Installation aus.

- 1 Geben Sie die Konfiguration Ihrer PXE-Boot-Einrichtung ein und ersetzen Sie `install=protokoll://instquelle` durch `rescue=protokoll://instquelle`. Wie bei einer normalen Installation steht `protokoll` für eines der unterstützten Netzwerkprotokolle (NFS, HTTP, FTP usw.) und `instquelle` für den Pfad zur Netzwerkinstallationsquelle.
- 2 Booten Sie das System mit Wake-on-LAN.
- 3 Geben Sie an der Eingabeaufforderung `Rescue: root` ein. Ein Passwort ist nicht erforderlich.

Sobald Sie sich im Rettungssystem befinden, können Sie die virtuellen Konsolen verwenden; der Zugriff erfolgt mit `[Alt] + [F1]` bis `[Alt] + [F6]`.

Eine Shell und viele andere hilfreiche Dienstprogramme, beispielsweise das `mount`-Programm, stehen im Verzeichnis `/bin` zur Verfügung. Das Verzeichnis `sbin` enthält wichtige Datei- und Netzwerkdienstprogramme, mit denen das Dateisystem überprüft und repariert werden kann. In diesem Verzeichnis finden Sie auch die wichtigsten Binärdateien für die Systemwartung, beispielsweise `fdisk`, `mkfs`, `mkswap`, `mount`, `mount`, `init` und `shutdown` sowie `ifconfig`, `ip`, `route` und `netstat` für die Netzwerkwartung. Das Verzeichnis `/usr/bin` enthält den `vi`-Editor, `find`, `less` sowie `ssh`.

Die Systemmeldungen können über den Befehl `dmesg` angezeigt werden; Sie können auch die Datei `/var/log/messages` zurate ziehen.

Überprüfen und Bearbeiten von Konfigurationsdateien

Als Beispiel für eine Konfiguration, die mithilfe des Rettungssystems repariert werden kann, soll eine beschädigte Konfigurationsdatei dienen, die das ordnungsgemäße Booten des Systems verhindert. Dieses Problem kann mit dem Rettungssystem behoben werden.

Gehen Sie zum Bearbeiten einer Konfigurationsdatei folgendermaßen vor:

- 1 Starten Sie das Rettungssystem mithilfe einer der oben erläuterten Methoden.
- 2 Verwenden Sie zum Einhängen eines Root-Dateisystems unter `/dev/sda6` in das Rettungssystem folgenden Befehl:

```
mount /dev/sda6 /mnt
```

Sämtliche Verzeichnisse des Systems befinden sich nun unter `/mnt`

3 Wechseln Sie in das eingehängte Root -Dateisystem:

```
cd /mnt
```

4 Öffnen Sie die fehlerhafte Konfigurationsdatei im vi-Editor. Passen Sie die Konfiguration an und speichern Sie sie.

5 Hängen Sie das Root-Dateisystem aus dem Rettungssystem aus:

```
umount /mnt
```

6 Booten Sie den Computer neu.

Reparieren und Überprüfen von Dateisystemen

Generell ist das Reparieren von Dateisystemen auf einem zurzeit aktiven System nicht möglich. Bei ernsthaften Problemen ist möglicherweise nicht einmal das Einhängen Ihres Root-Dateisystems möglich und das Booten des Systems endet unter Umständen mit einer so genannten `Kernel-Panic`. In diesem Fall ist nur die externe Reparatur des Systems möglich. Für diese Aufgabe wird die Verwendung der YaST-Systemreparatur dringend empfohlen (Details finden Sie hier: „[Verwenden der YaST-Systemreparatur](#)“ (S. 1027)). Wenn Sie jedoch die manuelle Überprüfung bzw. Reparatur des Dateisystems durchführen müssen, booten Sie das Rettungssystem. Es enthält die Dienstprogramme für die Überprüfung und Reparatur der Dateisysteme `ext2`, `ext3`, `reiserfs`, `ufs`, `jfs`, `dosfs` und `vfat`.

Zugriff auf das installierte System

Wenn Sie vom Rettungssystem auf das installierte System zugreifen müssen, um beispielsweise die Bootloader-Konfiguration zu ändern oder ein Dienstprogramm für die Hardwarekonfiguration auszuführen, muss dies in einer „change-root“-Umgebung erfolgen.

Gehen Sie zur Einrichtung einer „change-root“-Umgebung, die auf dem installierten System basiert, folgendermaßen vor:

1 Hängen Sie zunächst die Root-Partition vom installierten System sowie das gerätebezogene Dateisystem ein:

```
mount /dev/sda6 /mnt  
mount --bind /dev /mnt/dev
```

2 Nun können Sie per „change-root“ in die neue Umgebung wechseln:

```
chroot /mnt
```

3 Hängen Sie dann `/proc` und `/sys` ein:

```
mount /proc  
mount /sys
```

4 Abschließend hängen Sie die restlichen Partitionen vom installierten System ein:

```
mount -a
```

5 Nun können Sie auf das installierte System zugreifen. Hängen Sie vor dem Reboot des Systems die Partitionen mit `umount -a` aus und verlassen Sie die „change-root“-Umgebung mit `exit`.

WARNUNG: Beschränkungen

Obwohl Sie über uneingeschränkten Zugriff auf die Dateien und Anwendungen des installierten Systems verfügen, gibt es einige Beschränkungen. Der ausgeführte Kernel ist derjenige, der mithilfe des Rettungssystems gebootet wurde. Er unterstützt nur essenzielle Hardware, und das Hinzufügen von Kernel-Modulen über das installierte System ist nur möglich, wenn die Kernel-Versionen genau übereinstimmen (die Wahrscheinlichkeit hierfür ist sehr gering). Sie können folglich beispielsweise nicht auf eine Soundkarte zugreifen. Der Aufruf einer grafischen Bedienoberfläche ist ebenfalls nicht möglich.

Beachten Sie zudem, dass Sie die „change-root“-Umgebung verlassen, wenn Sie die Konsole mit `[Alt] + [F1]` bis `[Alt] + [F6]` umschalten.

Bearbeiten und erneutes Installieren des Bootloader

In einigen Fällen kann ein System aufgrund einer beschädigten Bootloader-Konfiguration nicht gebootet werden. Die Start-Routinen sind beispielsweise nicht in der Lage, physische Geräte in die tatsächlichen Speicherorte im Linux-Dateisystem zu übersetzen, wenn der Bootloader nicht ordnungsgemäß funktioniert.

Gehen Sie wie folgt vor, um die Bootloader-Konfiguration zu überprüfen und den Bootloader neu zu installieren:

- 1 Führen Sie die unter „Zugriff auf das installierte System“ (S. 1035) erläuterten erforderlichen Schritte für den Zugriff auf das installierte System aus.
- 2 Vergewissern Sie sich, dass die nachfolgend angegebenen Dateien gemäß den in [Kapitel 21, *Der Bootloader*](#) (S. 437) erläuterten GRUB-Konfigurationsgrundlagen ordnungsgemäß konfiguriert sind

- `/etc/grub.conf`
- `/boot/grub/device.map`
- `/boot/grub/menu.lst`

Beseitigen Sie im Bedarfsfall Fehler hinsichtlich der Gerätezuordnung (`device.map`) bzw. des Speicherorts von Root-Partition und Konfigurationsdateien durch Anwendung von Fixes.

- 3 Installieren Sie den Bootloader mit folgender Befehlssequenz neu:

```
grub --batch < /etc/grub.conf
```

- 4 Hängen Sie die Partitionen aus, melden Sie sich von der „change-root“-Umgebung ab und führen Sie den Reboot des Systems durch:

```
umount -a  
exit  
reboot
```

52.7 IBM-System z: initrd als Rettungssystem verwenden

Wenn der Kernel von SUSE® Linux Enterprise Server für IBM-System z aktualisiert oder geändert wird, kann es zu einem versehentlichen Neustart des Systems in einem instabilen Zustand kommen, sodass Fehler bei Standardprozeduren von IPLing im installierten System auftreten. Dies tritt häufig dann auf, wenn ein neuer oder aktualisierter SUSE Linux Enterprise Server-Kernel installiert und das Programm `zipl` nicht ausgeführt wurde, um den IPL-Datensatz zu aktualisieren. Verwenden Sie in diesem Fall das Standardinstallationspaket als Rettungssystem, von dem aus das Programm `zipl` zur Aktualisierung des IPL-Datensatzes ausgeführt werden kann.

52.7.1 Rettungssystem IPLing

WICHTIG: Bereitstellen der Installationsdaten

Damit diese Methode funktioniert, müssen die SUSE Linux Enterprise Server-Installationsdaten für IBM-System z verfügbar sein. Genauere Informationen hierzu erhalten Sie unter Abschnitt „Bereitstellen der Installationsdaten“ (Kapitel 2, *Vorbereitung der Installation*, ↑Architekturspezifische Informationen) in *Architekturspezifische Informationen*. Darüber hinaus benötigen Sie die Kanalnummer des Geräts und die Nummer der Partition innerhalb des Geräts, die das Stammdateisystem der SUSE Linux Enterprise Server-Installation enthält.

Führen Sie zuerst IPL für das SUSE Linux Enterprise Server-Installationssystem von IBM-System z aus, wie im Handbuch *Architecture-Specific Information* beschrieben. Anschließend wird eine Liste der Auswahlmöglichkeiten für den Netzwerkadapter angezeigt.

Wählen Sie *4 Installation oder System starten* und anschließend *3 Start Rescue System* (Rettungssystem starten) aus, um das Rettungssystem zu starten. Je nach Installationsumgebung müssen Sie jetzt die Parameter für den Netzwerkadapter und die Installationsquelle angeben. Das Rettungssystem wird geladen und abschließend wird folgende Anmeldeeingabeaufforderung angezeigt:

```
Skipped services in runlevel 3:  nfs nfsboot
```

```
Rescue login:
```

Nun können Sie sich ohne Passwort als Benutzer `root` anmelden.

52.7.2 Konfigurieren von Festplatten

Zu diesem Zeitpunkt sind noch keine Festplatten konfiguriert. Sie müssen Sie konfigurieren, um fortfahren zu können.

Prozedur 52.3 Konfigurieren von DASDs

- 1 Konfigurieren Sie DASDs mit folgendem Befehl:

```
dasd_configure 0.0.0150 1 0
```

DASD wird an den Kanal 0.0.0150 angeschlossen. Mit 1 wird die Festplatte aktiviert (durch eine 0 an dieser Stelle würde die Festplatte deaktiviert). Die 0 steht für „kein DIAG-Modus“ für den Datenträger (mit einer 1 würde DAIG an dieser Stelle für den Zugriff auf die Festplatte aktiviert).

- 2 Nun ist DASD online (dies kann mit dem Befehl `cat /proc/partitions` überprüft werden) und kann für nachfolgende Befehle verwendet werden.

Prozedur 52.4 *Konfigurieren einer zFCP-Festplatte*

- 1 Für die Konfiguration einer zFCP-Festplatte muss zunächst der zFCP-Adapter konfiguriert werden. Das geschieht mit folgendem Befehl:

```
zfcplib_host_configure 0.0.4000 1
```

0.0.4000 ist der Kanal, an den der Adapter angeschlossen ist. Die 1 steht für "aktivieren" (mit einer 0 an dieser Stelle würde der Adapter deaktiviert).

- 2 Nach dem Aktivieren des Adapters kann die Festplatte konfiguriert werden. Das geschieht mit folgendem Befehl:

```
zfcplib_disk_configure 0.0.4000 1234567887654321 8765432100000000 1
```

0.0.4000 ist die zuvor verwendete Kanal-ID, 1234567887654321 ist die WWPN (World wide Port Number) und 8765432100000000 die LUN (logical unit number). Mit 1 wird die Festplatte aktiviert (durch eine 0 an dieser Stelle würde die Festplatte deaktiviert).

- 3 Nun ist die zFCP-Festplatte online (dies kann mit dem Befehl `cat /proc/partitions` überprüft werden) und kann für nachfolgende Befehle verwendet werden.

52.7.3 Einhängen des Root-Geräts

Wenn alle benötigten Festplatten online sind, kann das Root-Gerät eingehängt werden. Wenn sich das Root-Gerät beispielsweise auf der zweiten Partition des DASD-Geräts (`/dev/dasda2`) befindet, lautet der entsprechende Befehl `mount /dev/dasda2 /mnt`.

WICHTIG: Dateisystemkonsistenz

Wenn das installierte System nicht richtig heruntergefahren wurde, empfiehlt es sich, vor dem Einhängen die Dateisystemkonsistenz zu überprüfen. Dadurch werden unerwünschte Datenverluste vermieden. Geben Sie für dieses Beispiel den Befehl `fsck /dev/dasda2` ein, um sicherzustellen, dass sich das System in einem konsistenten Status befindet.

Mit dem Befehl `mount` können Sie überprüfen, ob das Dateisystem richtig eingehängt werden konnte.

Beispiel 52.1 Ausgabe des Befehls "mount"

```
SuSE Instsys suse:/ # mount
shmfs on /newroot type shm (rw,nr_inodes=10240)
devpts on /dev/pts type devpts (rw)
virtual-proc-file-system on /proc type proc (rw)
/dev/dasda2 on /mnt type reiserfs (rw)
```

52.7.4 Ändern des eingehängten Dateisystems

Ändern Sie das auf dem System installierte Root-Gerät mit dem Befehl `chroot`, damit die Konfigurationsdatei mit dem Befehl `zipl` aus der Konfiguration des installierten Root-Geräts und nicht vom Rettungssystem abgelesen wird:

Beispiel 52.2 Ausführen des Befehls "chroot" für das eingehängte Dateisystem

```
SuSE Instsys suse:/ # cd /mnt
SuSE Instsys suse:/mnt # chroot /mnt
```

52.7.5 Ausführen des Befehls "zipl"

Führen Sie jetzt den Befehl `zipl` aus, um den IPL-Datensatz erneut mit den richtigen Werten zu speichern:

Beispiel 52.3 *Installieren des IPL-Datensatzes mit dem Befehl "zipl"*

```
sh-2.05b# zipl
building bootmap : /boot/zipl/bootmap
adding Kernel Image : /boot/kernel/image located at 0x00010000
adding Ramdisk : /boot/initrd located at 0x00800000
adding Parmline : /boot/zipl/parmfile located at 0x00001000
Bootloader for ECKD type devices with z/OS compatible layout installed.
Syncing disks....
...done
```

52.7.6 Beenden des Rettungssystems

Schließen Sie zum Beenden des Rettungssystems die mit dem Befehl `chroot` geöffnete Shell mit `exit`. Um Datenverluste zu vermeiden, leeren Sie alle nicht gespeicherten Puffer, indem Sie die darin enthaltenen Daten mit dem Befehl `sync` auf der Festplatte speichern. Ändern Sie jetzt das `root`-Verzeichnis des Rettungssystems und hängen Sie das Root-Gerät der SUSE Linux Enterprise Server-Installation für IBM-System z aus.

Beispiel 52.4 *Aushängen des Dateisystems*

```
SuSE Instsys suse:/mnt # cd /
SuSE Instsys suse:/ # umount /mnt
```

Halten Sie das Rettungssystem mit dem Befehl `halt` an. Für das SUSE Linux Enterprise Server-System kann jetzt IPLed ausgeführt werden, wie unter [Abschnitt 3.9.10](#), „IBM-System z: Ausführen von IPL für das installierte System“ (S. 60) beschrieben.

Index

Symbole

- 64-Bit-Linux, 413
 - Kernel-Spezifikationen, 417
 - Laufzeitunterstützung, 414
 - Software-Entwicklung, 415

A

- ACLs, 327–340
 - Auswertungsalgorithmus, 339
 - Auswirkungen, 336
 - Berechtigungsbits, 332
 - Definitionen, 330
 - Masken, 334
 - Standard, 330, 336
 - Struktur, 330
 - Umgang, 330
 - Unterstützung, 339
 - Zugriff, 330, 333
- ACPI
 - Deaktivieren, 41
- Add-On-Produkte, 159
- Adressen
 - IP, 608
- Aktualisieren
 - Online
 - Kommandozeile, 206
- Aktualisierung
 - Online, 161–162
 - passwd und group, 220
 - Patch-CD, 162
 - Probleme, 220
 - Soundmixer, 237
 - YaST, 221
- Apache, 189, 811–855
 - Beenden, 829
 - CGI-Skripts, 839

- Fehlerbehebung, 852
- Installieren, 812
- Konfigurieren, 813
 - Dateien, 814
 - HTTP-Assistent von YaST, 822
 - HTTP-Server-Konfiguration mit YaST, 827
 - Manuell, 813–821
 - Virtuelle Hosts, 817
 - YaST, 822–829
- Module, 831–839
 - Externe Module, 837
 - Installieren, 832
 - Module entwickeln, 838
 - Multiprocessing-Module, 836
 - Verfügbare, 833
- Schnellstart, 811
- Sicherheit, 850
- Squid, 873
- SSL, 843–850
 - Apache mit SSL konfigurieren, 849
 - SSL-Zertifikat erstellen, 843
- Starten, 829
- Weitere Informationen, 853
- Arbeitsspeicher
 - RAM, 464
- aushängen, 401
- Authentifizierung
 - Kerberos, 232
 - PAM, 553–561
- AutoYaST, 200
 - System klonen, 73

B

- Bash, 376–389
 - .bashrc, 460
 - .profile, 460
- Befehle, 376
- Funktionen, 383

- Pipes, 386
- Platzhalter, 384
- Profil, 459
- Befehle, 393–405
 - aushängen, 401
 - bzip2, 388
 - cat, 399
 - cd, 395
 - chgrp, 393, 396
 - chmod, 392, 396
 - chown, 393, 395
 - clear, 405
 - cp, 394
 - date, 402
 - df, 401
 - diff, 400
 - du, 401
 - einhängen, 400
 - file, 399
 - find, 398
 - fonts-config, 544
 - free, 402, 464
 - getfacl, 334
 - grep, 399
 - grub, 438
 - gzip, 388, 397
 - halt, 405
 - help, 379
 - ip, 659
 - kadmin, 931
 - kill, 403
 - killall, 403
 - kinit, 939
 - ktadd, 941
 - ldapadd, 747
 - ldapdelete, 750
 - ldapmodify, 749
 - ldapsearch, 749, 946
 - less, 399
 - ln, 395

- locate, 398
- lp, 500
- ls, 394
- man, 393
- mkdir, 395
- mv, 394
- nslookup, 404
- passwd, 404
- ping, 403, 660
- ps, 402
- reboot, 405
- rm, 395
- rmdir, 395
- rpm, 341
- rpmbuild, 341
- scp, 912
- setfacl, 334
- sftp, 913
- slptool, 671
- smbpasswd, 778
- ssh, 912
- ssh-agent, 916
- ssh-keygen, 915
- su, 404
- Suchen, 398
- tar, 387, 397
- telnet, 404
- top, 402
- updatedb, 398
- Benutzer
 - /etc/passwd, 556, 755
 - Verwaltung mit YaST, 194
- Berechtigungen, 389
 - ACLs, 327–340
 - Anzeigen, 391
 - Dateiberechtigungen, 462
 - Dateien, 390
 - Dateisysteme, 390
 - Verzeichnisse, 391
 - Ändern, 396

- ändern, 392
- Bildschirm
 - Auflösung, 541
- BIND, 692–703
- BIOS
 - Bootsequenz, 1001
- Booten, 419
 - Bootsektoren, 437–438
 - CD, Booten von CD, 1001
 - Disketten, Booten von, 1000
 - Grafisch, 455
 - GRUB, 437–458
 - initramfs, 421
 - initrd, 421
 - Konfiguration, 58
 - Konfigurieren
 - YaST, 448–453
 - Protokoll, 200
- bzip2, 388

C

- cat, 399
- cd, 395
- CDs
 - Booten, 454
 - Booten von, 1001
 - Überprüfen, 165
- chgrp, 393, 396
- chmod, 392, 396
- chown, 393, 395
- CJK, 468
- clear, 405
- Codierung
 - ISO-8859-1, 470
- commands
 - ifconfig, 662
 - route, 663
- Core-Dateien, 463
- cp, 394

- cpuspeed, 577
- cron, 460
- CVS, 790, 799–802

D

- date, 402
- Dateien
 - Anzeigen, 385, 399
 - Archivieren, 387, 397
 - Dekomprimieren, 388
 - Durchsuchen des Inhalts, 399
 - Komprimieren, 387, 397
 - Kopieren, 394
 - Löschen, 395
 - Pfade, 381
 - Suchen, 398
 - suchen, 463
 - Synchronisieren, 789–810
 - CVS, 790, 799–802
 - iFolder, 792
 - mailsync, 791, 807–810
 - rsync, 792
 - Subversion, 791
 - Unison, 790, 797–799
 - Vergleichen, 400
 - Verschieben, 394
 - Verschlüsseln, 952
- Dateiserver, 190
- Dateisysteme, 523–534
 - ACLs, 327–340
 - Auswählen, 524
 - Begriffe, 523
 - Beschränkungen, 532
 - cryptofs, 949
 - Ext2, 525–526
 - Ext3, 526–528
 - FAT, 52
 - LFS, 532
 - NTFS, 52, 54

- Reiser4, 528–529
- ReiserFS, 524–525
- Reparieren, 1035
- unterstützt, 530–532
- Verschlüsseln, 949
- XFS, 529–530
- Datenträger
 - Bootdisketten, 174
 - Erforderlicher Speicherplatz, 48
 - Rettungsdisketten, 174
- Deinstallieren
 - GRUB, 454
 - Linux, 454
- deltarpm, 345
- df, 401
- DHCP, 189, 707–723
 - dhcpd, 719–721
 - Konfigurieren mit YaST, 708
 - Pakete, 718
 - Server, 719–721
 - Zuweisung statischer Adressen, 721
- diff, 400
- Distributed Replicated Block Device (Siehe DRBD)
- DNS, 622
 - BIND, 692–703
 - Domänen, 653
 - Fehlersuche, 693
 - Konfigurieren, 189, 681
 - Mail Exchanger, 623
 - Namensserver, 653
 - NIC, 623
 - Optionen, 695
 - Protokollierung, 697
 - Reverse-Lookup, 702
 - Sicherheit, 977
 - Squid und, 863
 - Starten, 693
 - Terminologie, 681
 - Top Level Domain, 622
 - Weiterleitung, 693
 - Zonen
 - Dateien, 699
- Dokumentation (Siehe Hilfe)
- Domain Name System (Siehe DNS)
- DOS
 - Dateien freigeben, 767
- DRBD, 300
- Drucken, 489, 493–496
 - Anschluss, 494
 - Aus Anwendungen, 500
 - CUPS, 500
 - Drucken im Netzwerk, 509
 - GDI-Drucker, 507
 - Ghostscript-Treiber, 495
 - Kommandozeile, 500
 - Konfigurieren mit YaST, 493
 - kprinter, 500
 - PPD-Datei, 495
 - Samba, 769
 - Testseite, 495
 - Treiber, 495
 - Verbindung, 494
 - Warteschlangen, 495
 - xpp, 500
- du, 401

E

- E-Mail
 - Synchronisieren, 791
 - mailsync, 807–810
- Editoren
 - Emacs, 465–466
 - vi, 405
- einhängen, 400
- Emacs, 465–466
 - .emacs, 465
 - default.el, 466
- Email

- Konfigurieren, 186
- Energieverwaltung, 563–586
 - ACPI, 563, 567–575, 580
 - Akku-Überwachung, 565
 - APM, 563, 565–567, 580
 - cpufreq, 577
 - cpuspeed, 577
 - Ladezustand, 581
 - powersave, 577
 - Stand-by, 564
 - Suspend, 564
 - Tiefschlaf, 564
 - YaST, 586

F

- Fehlermeldungen
 - Berechtigung verweigert, 180
 - schlechter Interpreter, 180
- Festplatten
 - DMA, 168
- file, 399
- find, 398
- Firefox
 - Befehl zum Öffnen von URLs, 242
- Firewalls, 198, 899
 - Paketfilter, 899, 904
 - Squid and, 871
 - SuSEfirewall2, 899, 905
- free, 402

G

- GNOME
 - Shell, 376
- Grafik
 - 3D, 550–552
 - 3Ddiag, 551
 - Diagnose, 551
 - Fehlersuche, 551
 - Installationssupport für, 552

- SaX, 550
 - testen, 551
 - Treiber, 550
 - Unterstützung für, 550
- GLIDE, 550–552
- Karten
 - 3D, 550–552
 - Treiber, 542
- OpenGL, 550–552
 - testen, 551
 - Treiber, 550
- grep, 399
- GRUB, 437–458
 - Befehle, 438–448
 - Booten, 438
 - Bootmenü, 440
 - Bootpasswort, 447
 - Bootsektoren, 438
 - Deinstallieren, 454
 - device.map, 439, 445
 - Einschränkungen, 438
 - Fehlerbehebung, 456
 - Gerätenamen, 441
 - GRUB Geom Error, 457
 - grub.conf, 439, 446
 - JFS und GRUB, 456
 - Master Boot Record (MBR), 437
 - menu.lst, 439–440
 - Menü-Editor, 444
 - Partitionsnamen, 441
- Gruppen
 - Verwaltung, 195
- gunzip, 388
- gzip, 388, 397

H

- halt, 405
- Hardware
 - DASD, 172

- Festplatten-Controller, 168
- Grafikkarten, 167, 209
- Informationen, 168
- Infrarot, 167
- ISDN, 635
- Monitor, 167, 209
- ZFCP, 172
- heartbeat, 299
- Hilfe, 985–989
 - Dokumentation zu Paketen, 992
 - FAQs, 991
 - Handbücher, 991–992
 - HOWTOs, 991
 - info-Seiten, 465
 - Infoseiten, 990
 - Linux-Dokumentationsprojekt (TLDP), 990
 - Literatur, 991
 - Man Pages, 393
 - Manualpages, 465, 989
 - Spezifikationen, 994
 - Standards, 994
 - SUSE-Handbücher, 992
 - SUSE-Hilfe, 985
 - Usenet, 993
 - Wikipedia, 991
 - X, 543
- Hohe Verfügbarkeit, 295–303 (Siehe Hohe Verfügbarkeit)
 - Belastungsausgleich, 296
 - Cluster, 301
 - Cold Standby, 296
 - DRBD, 300
 - Failover, 296
 - heartbeat, 299
 - Hot-Standby, 296
 - Linux Virtual Server, 301
 - RAID, 300
 - rsync, 300
 - SPOF, 296
 - STONITH, 296
 - Warm-Standby-Modus, 296
- Hostnamen, 189

I

- I18N, 468
- iFolder, 792
- inetd, 191
- info-Seiten, 465
- init, 424
 - inittab, 424
 - Skripts, 427–431
 - Skripts hinzufügen, 430
- Installation
 - in ein Verzeichnis, 165
 - Manuell, 237
 - YaST, 37–74
- Installationssupport
 - 3D-Grafikkarten und, 552
- Installieren
 - GRUB, 438
 - Pakete, 342
 - Xen, 165
- Internationalisierung, 468
- Internet
 - cinternet, 666
 - DSL, 640
 - Einwahl, 664–667
 - ISDN, 635
 - KInternet, 666
 - qinternet, 666
 - smpppd, 664–667
 - TDSL, 642
- IP-Adressen
 - Dynamische Zuweisung, 707
 - IPv6, 612
 - Konfigurieren, 621
 - Klassen, 609
 - Masquerading, 902

Privat, 611
iSCSI, 285

J

Joystick
Konfigurieren, 169

K

Karten
Grafik, 542
Netzwerk, 623–624
Soundkarten, 170

KDE
Shell, 376

Kerberos, 919–926
Administration, 927–947
Authentifikator, 920
Berechtigungen, 920
Bereiche, 927
Erstellen, 931

Clients
Konfigurieren, 933–935

Installation, 927–947

KDC, 928–932
Administration, 938
nsswitch.conf, 929
Starten, 932

keytab, 941

Konfigurieren
Clients, 933–935

LDAP und, 944–947

Master-Schlüssel, 931

PAM-Unterstützung, 942

Prinzipale, 920
Erstellen, 932
Host, 940

Sitzungsschlüssel, 921

SSH-Konfiguration, 943

Stapeldatei, 931

Ticket ausstellen, 923

Tickets, 920, 923

Uhrensynchronisation, 929

Zeitdifferenz, 935

Kernels

Beschränkungen, 533

Caches, 464

kill, 403

killall, 403

Konfiguration

PAM, 238

Konfigurationsdateien, 651

.bashrc, 460, 463

.emacs, 465

.mailsync, 808

.profile, 460

.xsession, 916

acpi, 568

asound.conf, 171

Berechtigungen, 979

crontab, 460

csh.cshrc, 470

dhclient.conf, 718

dhcp, 652

dhcpd.conf, 719

Dienste, 771, 872

fstab, 180, 400

group, 220

grub.conf, 446

host.conf, 655

HOSTNAME, 658

Hosts, 189, 622, 654

ifcfg-*, 651

inittab, 424, 426–427, 467

inputrc, 467

Kernel, 421

krb5.conf, 933, 935, 942

krb5.keytab, 941

language, 468, 470

logrotate.conf, 462

- menu.lst, 440
- modprobe.d/sound, 171
- named.conf, 693–703, 863
- Netzwerk, 652
- Netzwerke, 654
- nscd.conf, 658
- nsswitch.conf, 656, 755
- openldap, 945
- pam_unix2.conf, 754, 942
- passwd, 220
- powersave, 567
- powersave.conf, 239
- Profil, 459, 463
- profile, 470
- resolv.conf, 465, 653, 693, 862
- Routen, 652
- Samba, 771
- slapd.conf, 741, 946–947
- smb.conf, 772, 783
- smpppd-c.conf, 666
- smpppd.conf, 665
- squid.conf, 862, 864, 868, 871, 874, 876
- squidguard.conf, 876
- sshd_config, 917, 943
- ssh_config, 943
- suseconfig, 436
- sysconfig, 184, 433–436
- termcap, 467
- wireless, 652
- XF86Config, 235
- xorg.conf, 235, 537
 - Device, 541
 - Monitor, 542
 - Screen, 540
- Konfigurieren, 433
 - Benutzer, 194
 - DASD, 172
 - DNS, 189, 681
 - Drucken, 493–496
 - DSL, 186, 640
 - Email, 186
 - Energieverwaltung, 183
 - Festplatten
 - DMA, 168
 - Festplatten-Controller, 168
 - Firewalls, 198
 - Grafikkarten, 167, 209
 - GRUB, 438, 446
 - Gruppen, 195
 - Hardware, 167–173
 - IPv6, 621
 - ISDN, 186, 635
 - Kabelmodem, 639
 - Mailserver, 187
 - Modems, 186, 633
 - Monitor, 167, 209
 - Netzwerke, 185–194, 624
 - Manuell, 647–664
 - Netzwerkkarten, 186
 - NFS, 190
 - NTP, 191
 - Powertweak, 183
 - Routing, 193, 652
 - Samba, 769–776
 - Clients, 193–194, 776
 - Server, 193
 - Sicherheit, 194–199
 - Software, 152–163
 - Soundkarten, 170
 - Sprachen, 184
 - Squid, 864
 - SSH, 911
 - System, 149–202
 - Systemdienste, 191
 - T-DSL, 642
 - Wireless-Karten, 186
 - Zeitzone, 184
 - ZFCP, 172
- Konsolen

- Grafische, 455
 - umschalten, 466
 - zuweisen, 467
- L**
- L10N, 468
 - Laufwerke
 - Aushängen, 401
 - Einhängen, 400
 - LDAP, 735–765
 - ACLs, 742
 - Benutzer verwalten, 762
 - Gruppen verwalten, 762
 - Hinzufügen von Daten, 746
 - Kerberos und, 944–947
 - Konfigurieren
 - YaST, 750
 - ldapadd, 746
 - ldapdelete, 750
 - ldapmodify, 748
 - ldapsearch, 749
 - Löschen von Daten, 750
 - Server
 - Konfigurieren mit YaST, 750
 - Serverkonfiguration, 741
 - Suchen von Daten, 749
 - Verzeichnisbaum, 737
 - YaST
 - Module, 755
 - Vorlagen, 755
 - YaST LDAP-Client, 754
 - Zugriffssteuerung, 744
 - Ändern von Daten, 748
 - Less, 385
 - less, 399
 - LFS, 532
 - Lightweight Directory Access Protocol (Siehe LDAP)
 - Linux
 - Dateien mit anderen Betriebssystemen gemeinsam nutzen, 767
 - Deinstallieren, 454
 - Netzwerke, 605
 - Linux Virtual Server, 301
 - linuxrc
 - Manuelle Installation, 237
 - Lizenzvereinbarung, 45
 - ln, 395
 - locate, 398, 463
 - Logical Volume Manager (Siehe LVM)
 - logrotate, 461
 - Lokalisierung, 468
 - LPAR-Installation
 - IPL, 60
 - ls, 377, 394
 - LSB
 - Installieren von Paketen, 341
 - LVM
 - YaST, 133
- M**
- Mailserver
 - Konfigurieren, 187
 - Man Pages, 393
 - Manualpages, 465
 - Masquerading, 902
 - Konfigurieren mit SuSEfirewall2, 905
 - Master Boot Record (Siehe MBR)
 - Maus
 - Konfigurieren, 170
 - MBR, 437–438
 - mkdir, 395
 - Modems
 - Kabel, 639
 - YaST, 633
 - More, 385
 - Multipath-E/A, 277–284
 - LVM2, 283

- mdadm, 283
- Software-Konfiguration, 279
- Systemkonfiguration, 279
- Unterstützte Hardware, 278

mv, 394

N

- Namensserver (Siehe DNS)
- NAT (Siehe Masquerading)
- NetBIOS, 768
- Network Information Service (Siehe NIS)
- Netzwerk-Dateisystem (Siehe NFS)
- Netzwerke, 605
 - Authentifizierung
 - Kerberos, 919–926
 - Broadcast-Adresse, 611
 - DHCP, 189, 707
 - DNS, 622
 - Konfigurationsdateien, 651–658
 - Konfigurieren, 185–194, 623–642, 647–664
 - IPv6, 621
 - localhost, 611
 - Netzmasken, 609
 - Netzwerkbasisadresse, 610
 - Routing, 193, 608–609
 - SLP, 669
 - TCP/IP, 605
 - YaST, 624
 - Alias, 628
 - Gateway, 629
 - Hostname, 628
 - IP-Adressen, 627
 - Starten, 630
- NFS, 785
 - Clients, 190, 785
 - Einhängen, 786
 - Importieren, 786
 - Server, 190, 787

- NIS, 725–733
 - Client, 191
 - Clients, 732
 - Master, 725–732
 - Server, 191
 - Slave, 725–732

Notebooks

- Energieverwaltung, 563–576
- Novell iFolder, 792
- nslookup, 404
- NSS, 656
 - Datenbanken, 656
- NTP
 - Client, 191

O

- OpenLDAP (Siehe LDAP)
- OpenSSH (Siehe SSH)
- OS/2
 - Dateien freigeben, 767

P

Pakete

- Deinstallieren, 342
- Installieren, 342
- Kompilieren, 349
- Kompilieren mit build, 351
- LSB, 341
- Paket-Manager, 341
- Prüfen, 342
- RPMS, 341

Paketfilter (Siehe Firewalls)

- PAM, 553–561
 - Konfiguration, 238

Partitionen

- erstellen, 47
- Erstellen, 176, 178
- EVMS, 179
- fstab, 180

- Größe ändern, Windows, 51
- LVM, 179
- Parameter, 178
- Partitionstabelle, 437
- RAID, 179
- Swap, 179
- Typen, 47
- Verschlüsseln, 951
- passwd, 404
- Passwörter
 - Ändern, 404
- PCI-Gerät
 - Treiber, 181
- Pfade, 381
 - absolut, 381
 - relativ, 381
- ping, 403, 660
- Platzhalter, 398
- Pluggable Authentication Modules (Siehe PAM)
- Ports
 - 53, 695
 - Durchsuchen, 873
- PostgreSQL
 - Aktualisierung, 220
- powersave, 577
 - Konfigurieren, 577
- Protokolldateien, 197, 461
 - boot.msg, 200, 567
 - Meldungen, 693, 909
 - Nachrichten, 201
 - Squid, 863, 866, 873
 - Unison, 799
 - XFree86, 552
- Protokolle
 - CIFS, 768
 - IPv6, 612
 - LDAP, 735
 - SLP, 669
 - SMB, 767

- Protokollieren
 - Anmeldeversuche, 197
- Proxies, 192, 857 (Siehe Squid)
 - Caches, 857
 - Transparent, 870
 - Vorteile, 857
- Prozesse, 402
 - Terminieren, 403
 - Überblick, 402
- ps, 402

Q

- Quelle
 - Kompilieren, 349

R

- RAID, 300
 - YaST, 142
- reboot, 405
- Registrieren
 - Kommandozeile, 166
 - YaST, 166
- Registrierung
 - ohne Internet, 166
- Reparieren von Systemen, 1027
- Rettungssystem, 1033, 1037
 - Start von CD, 1033
 - Start von Netzwerkquelle, 1033
- RFCs, 605
- rm, 395
- rmdir, 395
- Routing, 193, 608, 652–653
 - Masquerading, 902
 - Netzmasken, 609
 - Routen, 652
 - Statisches, 652
- RPM, 341–352
 - Abfragen, 346
 - Abhängigkeiten, 342

- Aktualisieren, 343
- Datenbank
 - Neu aufbauen, 344, 349
- Deinstallieren, 344
- deltarpm, 345
- Patches, 344
- Prüfen, 342
- rpmnew, 342
- rpmorig, 342
- rpmsave, 342
- Sicherheit, 979
- SRPMS, 350
- Werkzeuge, 352
- Überprüfen, 348
- rpmbuild, 341
- rsync, 300, 792, 805
- Runlevel, 183, 424–427
 - Bearbeiten in YaST, 431
 - Ändern, 426–427

S

- Samba, 767–783
 - Anmeldung, 777
 - Berechtigungen, 775
 - CIFS, 768
 - Clients, 193–194, 768–769, 776–777
 - Drucken, 777
 - Drucker, 769
 - Freigaben, 769, 773
 - Installieren, 769
 - Konfigurieren, 769–776
 - Namen, 768
 - Server, 193–194, 768–776
 - Sicherheit, 775–776
 - SMB, 767
 - Starten, 769
 - Stoppen, 769
 - swat, 771
 - TCP/IP, 767

- SaX2
 - Anzeige-Einstellungen, 210
 - Anzeigegerät, 211
 - Auflösung und Farbtiefe, 212
 - Dual Head, 212
 - entfernter Zugriff (VNC), 216
 - Grafik-Tablet, 215
 - Grafikkarte, 211
 - Mauseinstellungen, 214
 - Multihead, 213
 - Tastatureinstellungen, 215
 - Touchscreen, 216
- Schriften, 544
 - CID-keyed, 549
 - TrueType, 543
 - X11 Core, 544
 - Xft, 546
- SCPM, 183
- scripts
 - modify_resolvconf, 465
- Service Location Protocol (Siehe SLP)
- Shells, 375–409
 - Bash, 376
 - Befehle, 393–405
 - Pipes, 386
 - Platzhalter, 384
- Sicherheit, 967–981
 - Angriffe, 976–977
 - Berechtigungen, 971–972
 - Booten, 968–971
 - DNS, 977
 - Engineering, 968
 - Firewalls, 198, 899
 - Konfigurieren, 194–199
 - Lokal, 969–973
 - Netzwerk, 973–977
 - Passwörter, 969–970
 - Probleme melden, 980
 - Programmfehler, 972, 975
 - RPM-Signaturen, 979

- Samba, 775
- Serielle Terminals, 968–969
- Squid, 858
- SSH, 911–917
- tcpd, 980
- telnet, 911
- Tipps und Tricks, 978
- Unbefugtererkennung, 238
- Viren, 973
- Würmer, 977
- X und, 974
- Sicherungen, 164
 - Erstellen mit YaST, 173
 - Wiederherstellen, 174
- Skripts
 - init.d, 424, 427–431, 663
 - boot, 429
 - boot.local, 429
 - boot.setup, 429
 - halt, 430
 - Netzwerk, 664
 - nfsserver, 664
 - portmap, 664
 - rc, 427, 430
 - sendmail, 664
 - Squid, 862
 - xinetd, 664
 - ypbind, 664
 - ypserv, 664
 - mkinitrd, 421
 - modify_resolvconf, 653
 - SuSEconfig, 433–436
 - Deaktivieren, 436
- SLP, 669
 - Browser, 671
 - Konqueror, 672
 - Registrieren von Diensten, 670
 - slptool, 671
- SMB (Siehe Samba)
- smpd, 767

- Soft-RAID (Siehe RAID)
- Software
 - Entfernen, 152–159
 - Entwicklung
 - SUSE SDK, 160
 - Installieren, 152–159
 - Kompilieren, 349
 - Treiber, 160
- Sound
 - Konfigurieren in YaST, 170
 - MIDI, 171
 - Mixer, 237
 - Soundfonts, 171
- spm, 349
- Sprache, 164
- Sprachen, 184
- Squid, 857
 - ACLs, 868
 - Apache, 873
 - Berechtigungen, 862, 868
 - Berichte, 877
 - cachemgr.cgi, 873, 875
 - Caches, 857–858
 - Beschädigt, 863
 - Größe, 860
 - Calamaris, 877
 - CPU, 861
 - Deinstallation, 863
 - DNS, 863
 - Fehlersuche, 863
 - Firewalls, 871
 - Funktionen, 857
 - Konfigurieren, 864
 - Objektstatus, 859
 - Protokolldateien, 863, 866, 873
 - RAM, 861
 - Sicherheit, 858
 - squidGuard, 875
 - Starten, 862
 - Statistiken, 873, 875

- Stoppen, 862
- Systemvoraussetzungen, 860
- Transparente Proxies, 870, 873
- Verzeichnisse, 862
- Zugriffssteuerung, 874
- SSH, 911–917
 - Authentifizierungsmechanismen, 915
 - Daemon, 913
 - Schlüsselpaare, 914–915
 - scp, 912
 - sftp, 913
 - ssh, 912
 - ssh-agent, 916
 - ssh-keygen, 915
 - sshd, 913
 - X und, 916
- su, 404
- Subversion, 791, 802
- SUSE SDK, 160
- SUSE-Handbücher, 992
- SVN (Subversion), 791
- System
 - Aktualisierung, 163
 - Beschränken der Ressourcennutzung, 463
 - Dienste, 191
 - Herunterfahren, 405
 - Konfigurieren, 149–202
 - Lokalisierung, 468
 - Neubooten, 405
 - Rettung, 1033
 - Sicherheit, 196
 - Sprachen, 184
- T**
 - tar, 387, 397
 - Tastatur
 - Asiatische Zeichen, 468
 - Konfiguration, 169
 - Layout, 467
 - X-Tastaturerweiterung, 467
 - XKB, 467
 - Zuordnung, 467
 - Compose, 467
 - Multikey, 467
- TCP/IP, 605
 - ICMP, 606
 - IGMP, 606
 - Pakete, 607–608
 - Schichtmodell, 606
 - TCP, 606
 - UDP, 606
- Telefonanlage, 637
- telnet, 404
- TLDP, 990
- top, 402
- Treiber, 160
- Tripwire
 - durch AIDE ersetzt, 238
- U**
 - ulimit, 463
 - Optionen, 463
 - updatedb, 398
- V**
 - Variablen
 - Umgebung, 468
 - Verschlüsseln, 949–953
 - Dateien, 952–953
 - Dateien mit vi, 953
 - Erstellen von Partitionen, 951
 - Partitionen, 950–952
 - Wechselmedien, 953
 - YaST, 950
 - Versionshinweise, 200
 - Verzeichnisse
 - Erstellen, 395

- Löschen, 395
- Pfade, 381
- Struktur, 379
- Ändern, 395
- Virtueller Arbeitsspeicher, 179
- VNC
 - Verwaltung, 192

W

- whois, 623
- Windows
 - Dateien freigeben, 767

X

- X
 - Anzeige-Einstellungen, 210
 - Anzeigegerät, 211
 - Auflösung und Farbtiefe, 212
 - CID-keyed-Schriften, 549
 - Dual Head, 212
 - entfernter Zugriff (VNC), 216
 - Grafik-Tablet, 215
 - Grafikkarte, 211
 - Hilfe, 543
 - Mauseinstellungen, 214
 - Multihead, 213
 - Optimierung, 537–543
 - SaX2, 538
 - Schriften, 543
 - Schriftsysteme, 544
 - Sicherheit, 974
 - SSH und, 916
 - Tastatureinstellungen, 215
 - Touchscreen, 216
 - Treiber, 542
 - TrueType-Schriften, 543
 - Virtueller Bildschirm, 541
 - X11 Core-Schriften, 544
 - xf86config, 538

- xft, 543
- Xft, 546
- Zeichensätze, 543
- X Window-System (Siehe X)
- X-Tastaturerweiterung (Siehe Tastatur, XKB)
- X.509-Zertifizierung
 - Prinzipien, 881
 - Repository, 885–886
 - Widerrufsliste , 884
 - YaST, 881
 - Zertifikate, 883
- X.Org, 537
- Xen
 - Installation im Verzeichnis, 165
- Xft, 546
- xinetd, 191
- XKB (Siehe Tastatur, XKB)
- xorg.conf
 - Depth, 541
 - Device, 541
 - Display, 541
 - Farbtiefe, 541
 - Files, 538
 - InputDevice, 538
 - Modeline, 541
 - Modelines, 539
 - Modes, 541
 - Modi, 539
 - Monitor, 539, 541
 - ServerFlags, 538

Y

- YaST
 - 3D, 550
 - Add-On, 159
 - Aktualisierung, 162–163, 221
 - Automatische Installation, 200
 - Profile, 200

- AutoYaST, 200
- Benutzerverwaltung, 194
- Boot-Konfiguration, 448
 - Sicherheit, 452
 - Standardsystem, 451
 - Zeitlimit, 452
- Boot-Modus, 58
- Bootloader
 - Festplattenreihenfolge, 453
 - Passwort, 452
 - Speicherort, 450
 - Typ, 449
- CA-Management, 198
- Clustering, 176
- DASD, 172
- DHCP, 708
- Diskettenerstellung, 174
- DMA, 168
- DNS, 189
- Drucken, 493–496
- DSL, 640
- Email, 186
- Energieverwaltung, 183, 586
- EVMS, 176
- Festplatten-Controller, 168
- Festplattenspeicher, 48
- Firewall, 198
- Grafikkarten, 167, 209
- GRUB, 449
- Gruppenverwaltung, 195
- Hardware, 167–173
- Hardware-Erkennung, 57
- Hardware-Informationen, 168
- Heartbeat, 176
- Hochverfügbarkeit, 176
- Hostname, 62, 189
- Infrarot, 167
- Installation in ein Verzeichnis, 165
- Installation mit YaST, 37–74
- Installationseinstellungen, 46
- Installationsmodus, 45
- Installationsquellen, 161
- Installationsumfang, 55
- Installationsüberblick, 46
- ISDN, 635
- Joystick, 169
- Kabelmodem, 639
- Kerberos-Client, 190
- Konfigurieren, 149–202
- Kontrollzentrum, 151
- LDAP, 190
- LDAP-Client, 754
- LDAP-Clients, 70
- LDAP-Server, 750
- LILO, 449
- LVM, 133, 176
- Mailserver, 187
- Medienüberprüfung, 165
- Modems, 633
- Monitor, 167, 209
- ncurses, 202
- Netzwerkkarte, 624
- Netzwerkconfiguration, 63, 185–194
- NFS-Clients, 190
- NFS-Server, 190
- NIS-Clients, 71, 732
- Novell AppArmor, 194
- NTP-Client, 191
- Online-Update, 161–162
- Paketabhängigkeiten, 56
- Partitionieren, 176
- Partitionierung, 47
- PCI-Gerätetreiber, 181
- Powertweak, 183
- Profil-Manager, 183
- RAID, 142
- registrieren, 166
- Reparieren von Systemen, 1027
- root-Passwort, 62
- Routing, 193

- Runlevel, 431
- Samba
 - Clients, 193–194, 776
 - Server, 193
- Samba-Clients, 72
- SCPM, 183
- sendmail, 186
- Server-Zertifikat, 198
- Sichere Einstellungen, 41
- Sicherheit, 194–199
- Sicherungen, 164, 173
- SLP, 193
- SLP-Browser, 671
- Software, 152–163
- Software-Updates, 66
- Soundkarten, 170
- Sprache, 164
- Sprachen, 42, 150, 184
- starten, 38
- Starten, 149
- Support-Anfrage, 200
- sysconfig-Editor, 184, 434
- Systemanalyse, 45
- Systemsicherheit, 196
- Systemstart, 38
- T-DSL, 642
- Tastatur, 169
- Tastaturbelegung, 58
- Textmodus, 202–209
 - Module, 206
- Treiber-CDs, 202
- Versionshinweise, 200
- X.509-Zertifizierung, 881
 - Erstellen von CRLs, 894
 - Exportieren von Zertifizierungsstellenobjekten als Datei, 896
 - Exportieren von Zertifizierungsstellenobjekten in LDAP, 895
 - Importieren von Common Server Certificates, 897

- Stammzertifizierungsstelle, 886
- untergeordnete Zertifizierungsstelle, 889
- Zertifikate, 890
 - Ändern von Standardwerten, 893
- Xen, 165
- Zeitzone, 46, 184
- Zertifizierungsstellenmodul, 886
- ZFCP, 172
- YP (Siehe NIS)

Z

- z/VM-Installation
 - IPL, 60
- Zeitzone, 184
- Zugriffsberechtigungen (Siehe Berechtigungen)

