Administrationshandbuch

SUSE Linux Enterprise Server 12 SP5

Administrationshandbuch

SUSE Linux Enterprise Server 12 SP5

Es behandelt Systemverwaltungsaufgaben wie Wartung, Überwachung und Anpassung eines neu installierten Systems.

Veröffentlicht: 04. November 2019

SUSE LLC
10 Canal Park Drive
Suite 200
Cambridge MA 02141
USA
https://www.suse.com/documentation

Copyright © 2006– 2019 SUSE LLC und Mitwirkende. Alle Rechte vorbehalten.

Es wird die Genehmigung erteilt, dieses Dokument unter den Bedingungen der GNU Free Documentation License, Version 1.2 oder (optional) Version 1.3 zu vervielfältigen, zu verbreiten und/oder zu verändern; die unveränderlichen Abschnitte hierbei sind der Urheberrechtshinweis und die Lizenzbedingungen. Eine Kopie dieser Lizenz (Version 1.2) finden Sie im Abschnitt „GNU Free Documentation License“.

Die SUSE-Marken finden Sie unter http://www.suse.com/company/legal/. Alle anderen Marken von Drittanbietern sind Besitz ihrer jeweiligen Eigentümer. Markensymbole (®, ™ usw.) kennzeichnen Marken von SUSE und der Tochtergesellschaften. Sternchen (*) kennzeichnen Marken von Drittanbietern.

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

Inhaltsverzeichnis

Allgemeines zu diesem Handbuch xxii

I HÄUFIGE TASKS 1

1 Bash-Shell und Bash-Skripte 2

1.1 Was ist „die Shell“? 2

Die Bash-Konfigurationsdateien 2 • Die Verzeichnisstruktur 4

1.2 Schreiben von Shell-Skripten 8

1.3 Umlenken von Kommandoereignissen 9

1.4 Verwenden von Aliassen 11

1.5 Verwenden von Variablen in der Bash-Shell 11

Verwenden von Argumentvariablen 12 • Verwenden der Variablenersetzung 13

1.6 Gruppieren und Kombinieren von Kommandos 14

1.7 Arbeiten mit häufigen Ablaufkonstrukten 15

Das Steuerungskommando „if“ 15 • Erstellen von Schleifen mit dem Kommando **`for`** 16

1.8 Weiterführende Informationen 16

2 sudo 17

2.1 Grundlegende Verwendung von **`sudo`** 17

Ausführung eines einzelnen Kommandos 17 • Starten einer Shell 19 • Umgebungsvariablen 19

2.2 Konfigurieren von **`sudo`** 20

Bearbeiten der Konfigurationsdateien 20 • Basiskonfigurationssyntax von sudoers 21 • Regeln in sudoers 23

2.3 Häufige Einsatzmöglichkeiten 24
Verwenden von **sudo** ohne `root`-Passwort 24 • Verwenden von **sudo** mit X.Org-Anwendungen 26

2.4 Weitere Informationen 26

3 YaST-Online-Aktualisierung 27

3.1 Das Dialogfeld „Online-Aktualisierung“ 28

3.2 Installieren von Patches 29

3.3 Automatische Online-Updates 30

4 YaST 33

4.1 Erweiterte Tastenkombinationen 33

5 YaST im Textmodus 35

5.1 Navigation in Modulen 36

5.2 Erweiterte Tastenkombinationen 38

5.3 Einschränkung der Tastenkombinationen 39

5.4 YaST-Kommandozeilenoptionen 39
Starten der einzelnen Module 39 • Installation von Paketen über die Kommandozeile 40 • Kommandozeilenparameter der YaST-Module 40

6 Verwalten von Software mit Kommandozeilen-Tools 41

6.1 Verwenden von zypper 41
Allgemeine Verwendung 41 • Installieren und Entfernen von Software mit zypper 43 • Aktualisieren von Software mit zypper 48 • Ermitteln von Prozessen und Diensten, die gelöschte Dateien verwenden 52 • Verwalten von Repositorys mit Zypper 54 • Abfragen von Repositorys und Paketen mit Zypper 56 • Konfigurieren von Zypper 58 • Fehlersuche 59 • Zypper-Rollback-Funktion im Btrfs-Dateisystem 59 • Weiterführende Informationen 59

6.2 RPM - der Paket-Manager 60

Prüfen der Authentizität eines Pakets 60 • Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren 61 • Delta-RPM-Pakete 62 • RPM Abfragen 63 • Installieren und Kompilieren von Quellpaketen 66 • Kompilieren von RPM-Pakten mit „build“ 68 • Werkzeuge für RPM-Archive und die RPM-Datenbank 69

7 Systemwiederherstellung und Snapshot-Verwaltung mit Snapper 70

7.1 Standardeinrichtung 71

Typen von Snapshots 72 • Verzeichnisse, die aus Snapshots ausgenommen sind 73 • Anpassen der Einrichtung 74

7.2 Rückgängigmachen von Änderungen mit Snapper 78

Rückgängigmachen von Änderungen durch YaST oder Zypper 79 • Wiederherstellen von Dateien mit Snapper 84

7.3 System-Rollback durch Booten aus Snapshots 86

Snapshots nach dem Rollback 89 • Abrufen und Erkennen von Snapshot-Booteinträgen 90 • Einschränkungen 91

7.4 Erstellen und Bearbeiten von Snapper-Konfigurationen 93

Verwalten vorhandener Konfigurationen 95

7.5 Manuelles Erstellen und Verwalten von Snapshots 98

Snapshot-Metadaten 99 • Erstellen von Snapshots 101 • Bearbeiten von Snapshot-Metadaten 102 • Löschen von Snapshots 102

7.6 Automatisches Bereinigen von Snapshots 104

Bereinigen von nummerierten Snapshots 104 • Bereinigen von Zeitleisten-Snapshots 106 • Bereinigen von Snapshot-Paaren, die sich nicht unterscheiden 107 • Bereinigen manuell erstellter Snapshots 108 • Hinzufügen von Festplattenquotenunterstützung 108

7.7 Häufig gestellte Fragen 110

8 Fernzugriff mit VNC 112

8.1 Der **vncviewer**-Client 112

Verbinden mithilfe der vncviewer-CLI 112 • Verbinden mithilfe der vncviewer-GUI 113 • Benachrichtigungen zu unverschlüsselten Verbindungen 113

8.2 Remmina: Remote-Desktop-Client 114

Installation 114 • Hauptfenster 114 • Hinzufügen von Remote-Sitzungen 114 • Starten von Remote-Sitzungen 116 • Bearbeiten, Kopieren und Löschen gespeicherter Sitzungen 117 • Ausführen von Remote-Sitzungen über die Befehlszeile 118

8.3 Einmalige VNC-Sitzungen 118

Verfügbare Konfigurationen 120 • Initiieren einer einmaligen VNC-Sitzung 121 • Konfigurieren einmaliger VNC-Sitzungen 121

8.4 Permanente VNC-Sitzungen 122

Mit `vncserver` initiierte VNC-Sitzung 122 • Mit `vncmanager` initiierte VNC-Sitzung 124

8.5 Verschlüsselte VNC-Kommunikation 127

9 Kopieren von Dateien mit RSync 130

9.1 Konzeptüberblick 130

9.2 Einfache Syntax 131

9.3 Lokales Kopieren von Dateien und Verzeichnissen 131

9.4 Remote-Kopieren von Dateien und Verzeichnissen 132

9.5 Konfigurieren und Verwenden eines Rsync-Servers 133

9.6 Weiterführende Informationen 136

II BOOTEN EINES LINUX-SYSTEMS 137

10 Einführung in den Bootvorgang 138

10.1 Terminologie 138

10.2 Der Linux-Bootvorgang 139
Initialisierungs- und Bootloader-Phase 139 • Die Kernel-Phase 141 • Die Phase init auf initramfs 144 • Die systemd-Phase 146

11 UEFI (Unified Extensible Firmware Interface) 147

11.1 Secure Boot 147
Implementierung auf SUSE Linux Enterprise Server 148 • MOK (Machine Owner Key) 151 • Booten eines benutzerdefinierten Kernels 152 • Verwenden von Nicht-Inbox-Treibern 154 • Funktionen und Einschränkungen 155

11.2 Weiterführende Informationen 156

12 Der Bootloader GRUB 2 157

12.1 Hauptunterschiede zwischen GRUB Legacy und GRUB 2 157

12.2 Konfigurationsdateistruktur 158
Die Datei `/boot/grub2/grub.cfg` 159 • Die Datei `/etc/default/grub` 159 • Skripte in `/etc/grub.d` 163 • Zuordnung von BIOS-Laufwerken und Linux-Geräten 164 • Ändern von Menüeinträgen während des Bootvorgangs 165 • Festlegen eines Bootpassworts 167

12.3 Konfigurieren des Bootloaders mit YaST 168
Speicherort des Bootloaders und Boot-Code-Optionen 170 • Anpassen der Festplattenreihenfolge 172 • Konfigurieren der erweiterten Optionen 172

12.4 Unterschiede bei der Terminalnutzung auf z Systems 175
Einschränkungen 175 • Tastenkombinationen 175

12.5 Nützliche Kommandos in GRUB 2 178

12.6 Weitere Informationen 179

13 Der Daemon `systemd` 180

13.1 Das Konzept von &systemd 180
Grundlagen von systemd 180 • Unit-Datei 181

13.2 Grundlegende Verwendung 182
Verwalten von Diensten auf einem laufenden System 182 • Dienste dauerhaft aktivieren/deaktivieren 184

13.3 Systemstart und Zielverwaltung 186
Ziele im Vergleich zu Runlevels 186 • Fehlersuche beim Systemstart 190 • System V-Kompatibilität 193

13.4 Verwalten von Services mit YaST 194

13.5 Anpassen von `systemd` 195
Anpassen von Dienstdateien 196 • Erstellen von „Drop-in-Dateien“ 196 • Erstellen von benutzerdefinierten Zielen 197

13.6 Erweiterte Nutzung 197
Bereinigen von temporären Verzeichnissen 197 • Systemprotokoll 198 • Aufnahmen 199 • Laden der Kernelmodule 199 • Ausführen von Aktionen vor dem Laden eines Dienstes 200 • Kernel-Steuergruppen (cgroups) 201 • Beenden von Diensten (Senden von Signalen) 202 • Fehlersuche für Dienste 203

13.7 Weitere Informationen 204

III SYSTEM 205

14 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung 206

14.1 Laufzeitunterstützung 206

14.2 Kernel-Spezifikationen 207

15 `journalctl`: Abfragen des `systemd`-Journals 209

15.1 Festlegen des Journals als persistent 209

15.2 Nützliche Schalter in **`journalctl`** 210

15.3 Filtern der Journalausgabe 211
Filtern nach Bootnummer 211 • Filtern nach Zeitraum 212 • Filtern nach Feldern 212

15.4 Untersuchen von `systemd`-Fehlern 213

15.5 Konfiguration von journald 215

Ändern der Größenbeschränkung für das Journal 215 • Weiterleiten des Journals an `/dev/ttyX` 215 • Weiterleiten des Journals an die Syslog-Funktion 215

15.6 Filtern des `systemd`-Journals mit YaST 216

16 Grundlegendes zu Netzwerken 217

16.1 IP-Adressen und Routing 220

IP-Adressen 221 • Netzmasken und Routing 221

16.2 IPv6 – Das Internet der nächsten Generation 223

Vorteile 224 • Adresstypen und -struktur 226 • Koexistenz von IPv4 und IPv6 231 • IPv6 konfigurieren 232 • Weiterführende Informationen 232

16.3 Namensauflösung 233

16.4 Konfigurieren von Netzwerkverbindungen mit YaST 235

Konfigurieren der Netzwerkkarte mit YaST 235 • IBM z Systems: Konfigurieren von Netzwerkgeräten 249

16.5 Manuelle Netzwerkkonfiguration 251

Die **`wicked`**-Netzwerkkonfiguration 251 • Konfigurationsdateien 259 • Testen der Konfiguration 271 • Unit-Dateien und Startskripte 275

16.6 Grundlegende Routereinrichtung 276

16.7 Einrichten von Bonding-Geräten 277

Hot-Plugging von Bonding-Slaves 280

16.8 Einrichten von Team-Geräten für Netzwerk-Teaming 282

Anwendungsfall: Lastenausgleich mit Netzwerk-Teaming 286 • Anwendungsfall: Failover mit Netzwerk-Teaming 287 • Anwendungsfall: VLAN gegenüber Teamgerät 288

16.9 Softwaredefiniertes Networking mit Open vSwitch 290

Vorteile von Open vSwitch 291 • Installieren von Open vSwitch 291 • Überblick über Open vSwitch-Daemons und -

Dienstprogramme 292 • Erstellen einer Bridge mit Open vSwitch 293 • Verwenden von Open vSwitch direkt mit KVM 294 • Verwenden von Open vSwitch mit `libvirt` 296 • Weitere Informationen 297

17 Druckerbetrieb 298

17.1 Der CUPS-Workflow 299

17.2 Methoden und Protokolle zum Anschließen von Druckern 300

17.3 Installation der Software 301

17.4 Netzwerkdrucker 301

17.5 Konfigurieren von CUPS mit Kommandozeilenwerkzeugen 303

17.6 Drucken über die Kommandozeile 304

17.7 Besondere Funktionen in SUSE Linux Enterprise Server 305
CUPS und Firewall 305 • Durchsuchen nach Netzwerkdruckern 305 • PPD-Dateien in unterschiedlichen Paketen 306

17.8 Fehlersuche 307
Drucker ohne Unterstützung für eine Standard-Druckersprache 307 • Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar 308 • Netzwerkdrucker-Verbindungen 308 • Fehlerhafte Ausdrucke ohne Fehlermeldung 311 • Deaktivierte Warteschlangen 311 • CUPS-Browsing: Löschen von Druckaufträgen 312 • Fehlerhafte Druckaufträge und Fehler bei der Datenübertragung 312 • Fehlersuche für CUPS 313 • Weiterführende Informationen 313

18 Das X Window-System 314

18.1 Installation und Konfiguration von Schriften 314
Anzeigen der installierten Schriften 316 • Anzeigen von Schriften 316 • Abfragen von Schriften 317 • Installieren von Schriften 318 • Konfigurieren der Darstellung von Schriften 318

18.2 Weiterführende Informationen 328

19 Zugriff auf Dateisysteme mit FUSE 329

19.1 Konfigurieren von FUSE 329

19.2 Einhängen einer NTFS-Partition 329

19.3 Weiterführende Informationen 330

20 Verwalten von Kernelmodulen 331

20.1 Auflisten der geladenen Module mit lsmod und modinfo 331

20.2 Einfügen und Entfernen von Kernelmodulen 332
Automatisches Laden von Kernelmodulen beim Booten 332 • Eintragen von Kernelmodulen in schwarze Listen mit modprobe 333

21 Gerätemanagement über dynamischen Kernel mithilfe von udev 335

21.1 Das /dev-Verzeichnis 335

21.2 Kernel-uevents und udev 335

21.3 Treiber, Kernel-Module und Geräte 336

21.4 Booten und erstes Einrichten des Geräts 337

21.5 Überwachen des aktiven udev-Daemons 337

21.6 Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von udev-Regeln 339
Verwenden von Operatoren in udev-Regeln 341 • Verwenden von Ersetzungen in udev-Regeln 342 • Verwenden von udev-Übereinstimmungsschlüsseln 343 • Verwenden von udev-Zuweisungsschlüsseln 344

21.7 Permanente Gerätebenennung 346

21.8 Von udev verwendete Dateien 347

21.9 Weiterführende Informationen 348

22 Live-Patching des Linux-Kernels mithilfe von kGraft 349

22.1 Vorteile von kGraft 349

22.2 Low-Level-Funktion von kGraft 350

22.3 Installieren von kGraft-Patches 351
Aktivierung von SLE Live Patching 351 • Aktualisieren des Systems 352

22.4 Patch-Lebenszyklus 353

22.5 Entfernen eines kGraft-Patches 353

22.6 Hängengebliebene Kernel-Ausführungsthreads 354

22.7 Das Werkzeug **kgr** 354

22.8 Umfang der kGraft-Technologie 354

22.9 Umfang von SLE Live Patching 355

22.10 Interaktion mit den Supportprozessen 355

23 Spezielle Systemfunktionen 356

23.1 Informationen zu speziellen Softwarepaketen 356
Das Paket `bash` und `/etc/profile` 356 • Das cron-Paket 357 • Stoppen der Cron-Statusmeldungen 358 • Protokolldateien: Paket logrotate 358 • Der Befehl „locate“ 359 • Der Befehl „ulimit“ 359 • Der Befehl „free“ 360 • man-Seiten und Info-Seiten 361 • Auswählen von man-Seiten über das Kommando **man** 361 • Einstellungen für GNU Emacs 362

23.2 Virtuelle Konsolen 363

23.3 Tastaturzuordnung 363

23.4 Sprach- und länderspezifische Einstellungen 364
Beispiele 365 • Locale-Einstellungen in `~/.i18n` 366 • Einstellungen für die Sprachunterstützung 367 • Weiterführende Informationen 367

IV SERVICES 369

24 Zeitsynchronisierung mit NTP 370

24.1 Konfigurieren eines NTP-Client mit YaST 370
Grundlegende Konfiguration 370 • Ändern der Basiskonfiguration 371

24.2 Manuelle Konfiguration von NTP im Netzwerk 374

24.3 Dynamische Zeitsynchronisierung während der Laufzeit 375

24.4 Einrichten einer lokalen Referenzuhr 375

24.5 Uhrensynchronisierung mit einer externen Zeitreferenz (ETR) 376

25 Domain Name System (DNS) 377

25.1 DNS-Terminologie 377

25.2 Installation 378

25.3 Konfiguration mit YaST 378
Assistentenkonfiguration 379 • Konfiguration für Experten 382

25.4 Starten des BIND-Nameservers 390

25.5 Die Konfigurationsdatei /etc/named.conf 392
Wichtige
Konfigurationsoptionen 393 • Protokollierung 395 • Zoneneinträge 395

25.6 Zonendateien 396

25.7 Dynamische Aktualisierung von Zonendaten 401

25.8 Sichere Transaktionen 401

25.9 DNS-Sicherheit 403

25.10 Weiterführende Informationen 403

26 DHCP 404

26.1 Konfigurieren eines DHCP-Servers mit YaST 405
Anfängliche Konfiguration (Assistent) 406 • DHCP-Server-Konfiguration (Experten) 410

26.2 DHCP-Softwarepakete 416

26.3 Der DHCP-Server dhcpd 417

Clients mit statischen IP-Adressen 419 • Die SUSE Linux Enterprise Server-Version 420

26.4 Weiterführende Informationen 420

27 Verteilte Nutzung von Dateisystemen mit NFS 421

27.1 Überblick 421

27.2 Installieren des NFS-Servers 422

27.3 Konfigurieren des NFS-Servers 423

Exportieren von Dateisystemen mit YaST 423 • Manuelles Exportieren von Dateisystemen 425 • NFS mit Kerberos 428

27.4 Konfigurieren der Clients 428

Importieren von Dateisystemen mit YaST 429 • Manuelles Importieren von Dateisystemen 430 • pNFS (paralleles NFS) 431

27.5 Weiterführende Informationen 433

28 Samba 434

28.1 Terminologie 434

28.2 Installieren eines Samba-Servers 436

28.3 Starten und Stoppen von Samba 436

28.4 Konfigurieren eines Samba-Servers 436

Konfigurieren eines Samba-Servers mit YaST 436 • Manuelles Konfigurieren des Servers 439

28.5 Konfigurieren der Clients 444

Konfigurieren eines Samba-Clients mit YaST 444

28.6 Samba als Anmeldeserver 444

28.7 Samba-Server im Netzwerk mit Active Directory 445

28.8 Weitere Themen 447
Transparente Dateikomprimierung mit Btrfs 447 • Aufnahmen 448
28.9 Weiterführende Informationen 456
29 Bedarfsweises Einhängen mit autofs 457
29.1 Installation 457
29.2 Konfiguration 457
Die Master-Zuordnungsdatei 457 • Zuordnungsdateien 460
29.3 Funktionsweise und Fehlersuche 461
Steuern des `autofs`-Dienstes 461 • Fehlersuche bei Automounter-Problemen 462
29.4 Automatisches Einhängen als NFS-Freigabe 462
29.5 Weitere Themen 464
`/net`-Einhängepunkt 464 • Verwenden von Platzhalterzeichen beim automatischen Einhängen von Unterverzeichnissen 464 • Automatisches Einhängen des CIFS-Dateisystems 465
30 SLP 466
30.1 Das SLP-Frontend **`slptool`** 466
30.2 Bereitstellen von Diensten über SLP 467
Einrichten eines SLP-Installationsservers 469
30.3 Weiterführende Informationen 469
31 Der HTTP-Server Apache 470
31.1 Kurzanleitung 470
Anforderungen 470 • Installation 471 • Start 471
31.2 Konfigurieren von Apache 472
Apache-Konfigurationsdateien 472 • Manuelle Konfiguration von Apache 476 • Konfigurieren von Apache mit YaST 481
31.3 Starten und Beenden von Apache 488

31.4 Installieren, Aktivieren und Konfigurieren von Modulen 490
Installieren von Modulen 491 • Aktivieren und Deaktivieren von Modulen 491 • Basis- und Erweiterungsmodule 492 • Multiprocessing-Module 495 • Externe Module 496 • Kompilieren von Modulen 498

31.5 Aktivieren von CGI-Skripten 498
Konfiguration in Apache 499 • Ausführen eines Beispielskripten 500 • CGI-Fehlerbehebung 500

31.6 Einrichten eines sicheren Webservers mit SSL 501
Erstellen eines SSL-Zertifikats 502 • Konfigurieren von Apache mit SSL 506

31.7 Ausführen mehrerer Apache-Instanzen auf demselben Server 508

31.8 Vermeiden von Sicherheitsproblemen 511
Stets aktuelle Software 512 • DocumentRoot-Berechtigungen 512 • Zugriff auf das Dateisystem 512 • CGI-Skripten 513 • Benutzerverzeichnisse 513

31.9 Fehlerbehebung 514

31.10 Weiterführende Informationen 515
Apache 2.4 515 • Apache Module 515 • Entwicklung 516 • Verschiedene Informationsquellen 516

32 Einrichten eines FTP-Servers mit YaST 517

32.1 Starten des FTP-Servers 518

32.2 Allgemeine FTP-Einstellungen 518

32.3 FTP-Leistungseinstellungen 519

32.4 Authentifizierung 520

32.5 Einstellungen für Experten 520

32.6 Weiterführende Informationen 521

33 Der Proxyserver Squid 522

33.1 Einige Tatsachen zu Proxy-Caches 523
Squid und Sicherheit 523 • Mehrere Caches 523 • Caching von Internetobjekten 524

33.2 Systemanforderungen 525
RAM 525 • Prozessor 525 • Größe des Festplatten-Cache 526 • Festplatten-/SSD-Architektur 526

33.3 Grundlegende Verwendung von Squid 527
Starten von Squid 527 • Überprüfen, ob Squid ausgeführt wird 527 • Stoppen, Neuladen und Neustarten von Squid 529 • Entfernen von Squid 530 • Lokaler DNS-Server 530

33.4 Das YaST-Squid-Modul 532

33.5 Die Squid-Konfigurationsdatei 532
Allgemeine Konfigurationsoptionen 533 • Optionen für die Zugriffssteuerung 536

33.6 Konfigurieren eines transparenten Proxy 540

33.7 Verwenden der Cache-Manager-CGI von Squid (`cachemgr.cgi`) 543

33.8 squidGuard 545

33.9 Erstellung von Cache-Berichten mit Calamaris 547

33.10 Weiterführende Informationen 548

34 Web Based Enterprise Management mit SFCB 549

34.1 Einführung und grundlegendes Konzept 549

34.2 Einrichten des SFCB 551
Installieren zusätzlicher Anbieter 552 • Starten und Stoppen von SFCB und Überprüfen des SFCB-Status 553 • Absichern des Zugriffs 554

34.3 SFCB CIMOM-Konfiguration 557
Umgebungsvariablen 557 • Befehlszeilenoptionen 558 • SFCB-Konfigurationsdatei 559

34.4 Erweiterte SFCB-Tasks 571
Installieren von CMPI-Anbietern 572 • Testen von SFCB 576 • CIM-Kommandozeilenclient: wbemcli 578

34.5 Weiterführende Informationen 580

V MOBILE COMPUTER 581

35 Mobile Computernutzung mit Linux 582

35.1 Notebooks 582
Energieeinsparung 582 • Integration in unterschiedlichen Betriebsumgebungen 583 • Software-Optionen 586 • Datensicherheit 592

35.2 Mobile Hardware 593

35.3 Mobiltelefone und PDAs 594

35.4 Weiterführende Informationen 594

36 Verwendung von NetworkManager 595

36.1 Anwendungsbeispiele für den NetworkManager 595

36.2 Aktivieren oder Deaktivieren von NetworkManager 595

36.3 Konfigurieren von Netzwerkverbindungen 596
Verwalten von kabelgebundenen Netzwerkverbindungen 598 • Verwalten von drahtlosen Netzwerkverbindungen 598 • Konfigurieren der WLAN-/Bluetooth-Karte als Zugriffspunkt 599 • NetworkManager und VPN 600

36.4 NetworkManager und Sicherheit 601
Benutzer- und Systemverbindungen 602 • Speichern von Passwörtern und Berechtigungsnachweisen 603

36.5 Häufig gestellte Fragen 603

36.6 Fehlersuche 605

36.7 Weiterführende Informationen 606

37 Energieverwaltung 607

37.1 Energiesparfunktionen 607

37.2 Advanced Configuration & Power Interface (ACPI) 608
Steuern der CPU-Leistung 609 • Fehlersuche 610

37.3 Ruhezustand für Festplatte 611

37.4 Fehlersuche 613
CPU-Frequenzsteuerung funktioniert nicht 613

37.5 Weiterführende Informationen 613

VI FEHLERSUCHE 614

38 Hilfe und Dokumentation 615

38.1 Dokumentationsverzeichnis 615
SUSE-Handbücher 616 • Dokumentation zu den einzelnen Paketen 616

38.2 man-Seiten 617

38.3 Infoseiten 619

38.4 Online-Ressourcen 619

39 Erfassen der Systeminformationen für den Support 621

39.1 Anzeigen aktueller Systeminformationen 621

39.2 Erfassen von Systeminformationen mit supportconfig 622
Erstellen einer Serviceanforderungsnummer 622 • Upload-Ziele 623 • Erstellen eines supportconfig-Archivs mit YaST 623 • Erstellen eines supportconfig-Archivs über die Kommandozeile 625 • Allgemeine Optionen für Supportconfig 626

39.3 Übertragen von Informationen an den globalen technischen Support 627

39.4 Analysieren von Systeminformationen 629
SCA-Kommandozeilenwerkzeug 630 • SCA-Appliance 631 • Entwickeln von benutzerdefinierten Analyseschemata 644

39.5 Sammeln von Informationen bei der Installation 644

39.6 Unterstützung für Kernelmodule 645
Technischer Hintergrund 645 • Arbeiten mit nicht unterstützten Modulen 646

39.7 Weiterführende Informationen 647

40 Häufige Probleme und deren Lösung 648

40.1 Suchen und Sammeln von Informationen 648

40.2 Probleme bei der Installation 651
Überprüfen von Medien 651 • Kein bootfähiges DVD-Laufwerk verfügbar 652 • Vom Installationsmedium kann nicht gebootet werden 653 • Computer kann nicht gebootet werden 655 • Grafisches Installationsprogramm lässt sich nicht starten 657 • Nur ein minimalistischer Bootbildschirm wird eingeblendet 659 • Protokolldateien 660

40.3 Probleme beim Booten 660
GRUB 2-Bootloader wird nicht geladen 660 • Keine grafische Anmeldung 661 • Einhängen der Root-Btrfs-Partition nicht möglich 661 • Erzwingen der Prüfung von Root-Partitionen 662

40.4 Probleme bei der Anmeldung 662
Fehler trotz gültiger Kombination aus Benutzername und Passwort 662 • Keine Annahme einer gültigen Kombination aus Benutzername und Passwort 664 • Anmeldung bei verschlüsselter Home-Partition fehlgeschlagen 666 • Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop 667

40.5 Probleme mit dem Netzwerk 668
Probleme mit NetworkManager 673

40.6 Probleme mit Daten 673
Verwalten von Partitions-Images 674 • Verwenden des Rettungssystems 674

40.7 IBM z Systems: Verwenden von initrd als Rettungssystem 682

A Aktualisierungen der Dokumentation 685

A.1 September 2018 (Wartungsaktualisierung der Dokumentation für SUSE Linux Enterprise Server 12 SP3) 685

A.2 Juni 2018 (Wartungsaktualisierung der Dokumentation für SUSE Linux Enterprise Server 12 SP3) 686

A.3 Dezember 2017 (Wartungsversion von SUSE Linux Enterprise Server 12 SP3) 687

A.4 September 2017 (ursprüngliche Version von SUSE Linux Enterprise Server 12 SP3) 688

A.5 November 2016 (ursprüngliche Freigabe von SUSE Linux Enterprise Server 12 SP2) 691

A.6 März 2016 (Wartungsversion von SUSE Linux Enterprise Server 12 SP1) 693

A.7 Dezember 2015 (ursprüngliche Freigabe von SUSE Linux Enterprise Server 12 SP1) 694

A.8 Februar 2015 (Wartungsaktualisierung der Dokumentation) 698

A.9 Oktober 2014 (ursprüngliche Version von SUSE Linux Enterprise Server 12) 699

B Ein Beispielnetzwerk 706

C GNU-Lizenzen 707

C.1 GNU Free Documentation License 707

Allgemeines zu diesem Handbuch

Dieses Handbuch ist für professionelle Netzwerk- und Systemadministratoren 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 für eine solche Überprüfung angefordert wurde.

Dieses Handbuch enthält Folgendes:

Support und übliche Aufgaben

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

In diesem Abschnitt wird das zugrunde liegende Betriebssystem umfassend erläutert. SUSE Linux Enterprise unterstützt mehrere Hardware-Architekturen, mit denen Sie Ihre eigenen Anwendungen anpassen können, die auf SUSE Linux Enterprise ausgeführt werden sollen. Der Bootloader und die Informationen zum Bootvorgang unterstützen Sie dabei zu verstehen, wie Ihr Linux-System arbeitet und wie sich Ihre eigenen Skripten und Anwendungen integrieren lassen.

Services

SUSE Linux Enterprise ist als Netzwerk-Betriebssystem konzipiert. Hier finden Sie eine breite Palette an Netzwerkdiensten, beispielsweise DNS-, DHCP-, Web-, Proxy- und Authentifizierungsdienste. Es lässt sich auch gut in heterogene Umgebungen mit MS Windows-Clients und -Servern integrieren.

Mobile Computer

Laptops und die Kommunikation zwischen mobilen Geräten wie PDAs oder Mobiltelefonen und SUSE Linux Enterprise benötigen eine gewisse Aufmerksamkeit. Achten Sie auf geringen Energieverbrauch und sorgen Sie für die Integration verschiedener Geräte in einer sich ändernden Netzwerkumgebung. Machen Sie sich auch mit den Hintergrundtechnologien vertraut, die die erforderliche Funktionalität liefern.

Fehlerbehebung

Hier erhalten Sie einen Überblick über die Suche nach Hilfetexten und zusätzlicher Dokumentation, wenn Sie weitere Informationen benötigen oder bestimmte Aufgaben durchführen möchten. Außerdem finden Sie hier eine Liste der häufigsten Probleme mit Hinweisen zu ihrer Behebung.

1 Verfügbare Dokumentation

Anmerkung: Online-Dokumentation und neueste Aktualisierungen

Die Dokumentation für unsere Produkte steht unter http://www.suse.com/documentation/ bereit. Hier finden Sie außerdem die neuesten Aktualisierungen und Sie können die Dokumentation durchsuchen oder in verschiedenen Formaten herunterladen.

Darüber hinaus befindet sich die Dokumentation in der Regel auf dem installierten System im Verzeichnis `/usr/share/doc/manual`.

Die folgende Dokumentation ist für dieses Produkt verfügbar:

***Artikel* „Schnelleinführung zur Installation"**

Die Systemanforderungen werden aufgelistet, und Sie werden schrittweise durch die Installation von SUSE Linux Enterprise Server von DVD oder einem ISO-Abbild geführt.

***Buch* „Bereitstellungshandbuch"**

Erfahren Sie, wie Sie einzelne oder mehrere Systeme installieren und die Produktfunktionen für eine Bereitstellungsinfrastruktur nutzen. Wählen Sie aus verschiedenen Ansätzen. Von der lokalen Installation über einen Netzwerkinstallationsserver bis zu einer Masseninstallation über eine entfernt gesteuerte, hochgradig angepasste und automatisierte Installationsmethode ist alles möglich.

Administrationshandbuch

Es behandelt Systemverwaltungsaufgaben wie Wartung, Überwachung und Anpassung eines neu installierten Systems.

Buch „Virtualization Guide"

Hier wird die Virtualisierungstechnologie im Allgemeinen beschrieben, die vereinheitlichte Schnittstelle libvirt für die Virtualisierung wird vorgestellt und Sie finden ausführliche Informationen zu bestimmten Hypervisoren.

Buch „Storage Administration Guide"

Hier finden Sie Informationen zum Verwalten von Speichergeräten auf einem SUSE Linux Enterprise-Server.

Buch „AutoYaST"

AutoYaST ist ein System für die unbeaufsichtigte Massenbereitstellung von SUSE Linux Enterprise Server-Systemen über ein AutoYaST-Profil, in dem sich Installations- und Konfigurationsdaten befinden. Das Handbuch führt Sie durch die grundlegenden Schritte der automatischen Installation: Vorbereitung, Installation und Konfiguration.

Buch „Security Guide"

Zudem werden grundlegende Konzepte der Systemsicherheit vorgestellt, die sowohl lokale als auch netzwerkbezogene Aspekte abdecken. Es wird erläutert, wie Sie die in das Produkt eingegliederte Sicherheitssoftware wie AppArmor oder das Prüfsystem nutzen, mit dem zuverlässig Informationen zu allen sicherheitsspezifischen Ereignissen gesammelt werden.

Buch „Security and Hardening Guide"

Hier finden Sie detaillierte Informationen zum Installieren und Einrichten eines sicheren SUSE Linux Enterprise-Servers sowie zu weiteren Verfahren, die nach dem Installieren anfallen und die Sicherheit und Stabilität der Installation erhöhen. Der Administrator wird bei sicherheitsrelevanten Auswahlmöglichkeiten und Entscheidungen unterstützt.

Buch „System Analysis and Tuning Guide"

Ein Administratorhandbuch zur Problemsuche, Fehlerbehebung und Optimierung. Erfahren Sie, wie Sie Ihr System mithilfe von Überwachungswerkzeugen prüfen und optimieren können und wie Sie Ihre Ressourcen effizient verwalten. Es enthält zudem einen Überblick über häufige Probleme und Lösungen sowie weitere Hilfequellen und Dokumentationsressourcen.

Buch „Subscription Management Tool for SLES 12 SP5"

Ein Administratorhandbuch zum Subscription Management Tool. Dabei handelt es sich um ein Proxy-System für das SUSE Customer Center mit Repository und Registrierungszielen. Erfahren Sie, wie Sie einen lokalen SMT-Server installieren und konfigurieren, Repositorys spiegeln und verwalten, Client-Computer verwalten und Clients für die Verwendung von SMT konfigurieren.

Buch „GNOME-Benutzerhandbuch"

Einführung in den GNOME-Desktop von SUSE Linux Enterprise Server. Das Handbuch begleitet Sie bei der Verwendung und Konfiguration des Desktops und hilft Ihnen, wichtige Aufgaben zu erledigen. Dies richtet sich in erster Linie an Endbenutzer, die GNOME als ihren Standard-Desktop nutzen möchten.

2 Rückmeldungen

Für Rückmeldungen stehen mehrere Kanäle zur Verfügung:

Fehler und Verbesserungsanforderungen

Informationen zu Diensten und Support-Optionen, die für Ihr Produkt verfügbar sind, finden Sie unter http://www.suse.com/support/.

Die Community bietet Hilfe für openSUSE. Weitere Informationen finden Sie unter https://en.opensuse.org/Portal:Support.

Zum Melden von Fehlern in einer Produktkomponente gehen Sie zu https://scc.suse.com/support/requests, melden Sie sich an und klicken Sie auf *Neu erstellen*.

Anregungen und Kritik unserer Leser

Wir freuen uns über Ihre Kommentare und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation dieses Produkts. Verwenden Sie die Funktion „Benutzerkommentare" unten auf den einzelnen Seiten der Online-Dokumentation oder geben Sie Ihre Kommentare auf der Seite http://www.suse.com/documentation/feedback.html ein.

Mail

Für Feedback zur Dokumentation dieses Produkts können Sie auch eine Email an `doc-team@suse.de` senden. Geben Sie auf jeden Fall auch den Titel der Dokumentation, die Produktversion und das Datum der Veröffentlichung der Dokumentation an. Geben Sie eine genaue Beschreibung des Problems an und beziehen Sie sich auf die entsprechende Abschnittsnummer und Seite (oder URL), wenn Sie Fehler melden oder Verbesserungen vorschlagen.

3 Konventionen in der Dokumentation

In der vorliegenden Dokumentation werden die folgenden Hinweise und typografischen Konventionen verwendet:

- `/etc/passwd`: Verzeichnis- und Dateinamen
- *`PLATZHALTER`*: Ersetzen Sie *`PLATZHALTER`* durch den tatsächlichen Wert.
- `PATH`: die Umgebungsvariable PATH
- **`ls`**, `--help`: Kommandos, Optionen und Parameter
- `Benutzer`: Benutzer oder Gruppen
- `Paketname` : Name eines Pakets
- `Alt`, `Alt`–`F1`: Eine Taste oder Tastenkombination. Tastennamen werden wie auf der Tastatur in Großbuchstaben dargestellt.
- *Datei*, *Datei* › *Speichern unter*: Menüelemente, Schaltflächen
- `x86_64` Dieser Absatz ist nur für die AMD64-/Intel-64-Architektur relevant. Die Pfeile kennzeichnen den Anfang und das Ende des Textblocks.
  `System z, POWER` Dieser Absatz ist nur für die Architekturen `z Systems` und `POWER` relevant. Die Pfeile kennzeichnen den Anfang und das Ende des Textblocks.
- *Tanzende Pinguine* (Kapitel *Pinguine*, ↑Zusätzliches Handbuch): Dies ist ein Verweis auf ein Kapitel in einem anderen Handbuch.
- Kommandos, die mit `root`-Privilegien ausgeführt werden müssen. Diesen Befehlen kann zur Ausführung als nicht privilegierter Benutzer auch häufig das Präfix **`sudo`** vorangestellt sein.

```
root # command
tux > sudo command
```

- Kommandos, die von Benutzern ohne Privilegien ausgeführt werden können.

```
tux > command
```

- Hinweise

Warnung: Warnhinweis

Wichtige Informationen, die Sie kennen müssen, bevor Sie fortfahren. Warnt vor Sicherheitsrisiken, potenziellen Datenverlusten, Beschädigung der Hardware oder physischen Gefahren.

Wichtig: Wichtiger Hinweis

Wichtige Informationen, die Sie beachten sollten, bevor Sie den Vorgang fortsetzen.

Anmerkung: Anmerkung

Ergänzende Informationen, beispielsweise zu unterschiedlichen Softwareversionen.

Tipp: Tipp

Hilfreiche Informationen, etwa als Richtlinie oder praktische Empfehlung.

4 Informationen über die Herstellung dieser Dokumentation

Diese Dokumentation wurde in Novdoc, einem Teilsatz von DocBook 5 (http://www.docbook.org) geschrieben. Die XML-Quelldateien wurden mit **`jing`** (siehe https://code.google.com/p/jing-trang/) überprüft, mit **`xsltproc`** verarbeitet und mit einer benutzerdefinierten Version der Stylesheets von Norman Walsh in XSL-FO konvertiert. Die endgültige PDF-Datei wurde mit FOP von der Apache Software Foundation (https://xmlgraphics.apache.org/fop) formatiert. Die Open-Source-Tools und die Umgebung, mit denen diese Dokumentation aufgebaut wurde, wurden von der DocBook Authoring and Publishing Suite (DAPS) bereitgestellt. Die Startseite des Projekts finden Sie unter https://github.com/openSUSE/daps.

Den XML-Quellcode dieser Dokumentation finden Sie unter https://github.com/SUSE/doc-sle.

I Häufige Tasks

1 Bash-Shell und Bash-Skripte 2

2 sudo 17

3 YaST-Online-Aktualisierung 27

4 YaST 33

5 YaST im Textmodus 35

6 Verwalten von Software mit Kommandozeilen-Tools 41

7 Systemwiederherstellung und Snapshot-Verwaltung mit Snapper 70

8 Fernzugriff mit VNC 112

9 Kopieren von Dateien mit RSync 130

1 Bash-Shell und Bash-Skripte

Heutzutage werden zunehmend Computer mit einer grafischen Bedienoberfläche (GUI) wie GNOME verwendet. Diese bieten zwar viele Funktionen, jedoch ist ihre Verwendung beschränkt, was automatisierte Aufgaben angeht. Shells sind eine gute Ergänzung für GUIs, und dieses Kapitel gibt Ihnen einen Überblick über einige Aspekte von Shells, in diesem Fall die Bash-Shell.

1.1 Was ist „die Shell“?

Traditionell handelt es sich bei *der* Shell um Bash (Bourne again Shell). Wenn in diesem Kapitel die Rede von „der Shell“ ist, ist die Bash-Shell gemeint. Außer Bash sind noch weitere Shells verfügbar (ash, csh, ksh, zsh und viele mehr), von denen jede unterschiedliche Funktionen und Merkmale aufweist. Wenn Sie weitere Informationen über andere Shells wünschen, suchen Sie in YaST nach *shell*.

1.1.1 Die Bash-Konfigurationsdateien

Eine Shell lässt sich aufrufen als:

1. **Interaktive Login-Shell.** Diese wird zum Anmelden bei einem Computer durch den Aufruf von Bash mit der Option `--login` verwendet oder beim Anmelden an einem entfernten Computer mit SSH.

2. **„Gewöhnliche“ interaktive Shell.** Dies ist normalerweise beim Starten von xterm, konsole, gnome-terminal oder ähnlichen Tools der Fall.

3. **Nicht interaktive Shell.** Dies wird beim Aufrufen eines Shell-Skripts in der Kommandozeile verwendet.

Abhängig vom verwendeten Shell-Typ werden unterschiedliche Konfigurationsdateien gelesen. Die folgenden Tabellen zeigen die Login- und Nicht-Login-Shell-Konfigurationsdateien.

TABELLE 1.1 BASH-KONFIGURATIONSDATEIEN FÜR LOGIN-SHELLS

Datei	Beschreibung
`/etc/profile`	Bearbeiten Sie diese Datei nicht, andernfalls können Ihre Änderungen bei Ihrem nächsten Update zerstört werden.
`/etc/profile.local`	Verwenden Sie diese Datei, wenn Sie `/etc/profile` erweitern.
`/etc/profile.d/`	Enthält systemweite Konfigurationsdateien für bestimmte Programme
`~/.profile`	Fügen Sie hier benutzerspezifische Konfigurationsdaten für Login-Shells ein.

Die Login-Shell greift außerdem auf die unter *Tabelle 1.2, „Bash-Konfigurationsdateien für Nicht-Login-Shells“* aufgeführten Konfigurationsdateien zu.

TABELLE 1.2 BASH-KONFIGURATIONSDATEIEN FÜR NICHT-LOGIN-SHELLS

`/etc/bash.bashrc`	Bearbeiten Sie diese Datei nicht, andernfalls können Ihre Änderungen bei Ihrem nächsten Update zerstört werden.
`/etc/bash.bashrc.local`	Verwenden Sie diese Datei, um Ihre systemweiten Änderungen nur für die Bash-Shell einzufügen.
`~/.bashrc`	Fügen Sie hier benutzerspezifische Konfigurationsdaten ein.

Daneben verwendet die Bash-Shell einige weitere Dateien:

TABELLE 1.3 BESONDERE DATEIEN FÜR DIE BASH-SHELL

Datei	Beschreibung
`~/.bash_history`	Enthält eine Liste aller Kommandos, die Sie eingegeben haben.

Datei	Beschreibung
`~/.bash_logout`	Wird beim Abmelden ausgeführt.
`~/.alias`	Benutzerdefinierte Aliase für häufig verwendete Kommandos. Weitere Informationen zum Definieren von Aliasen finden Sie unter **`man 1 alias`**.

1.1.2 Die Verzeichnisstruktur

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

TABELLE 1.4 ÜBERBLICK ÜBER EINE STANDARDVERZEICHNISSTRUKTUR

Verzeichnis	Inhalt
`/`	Root-Verzeichnis – Startpunkt der Verzeichnisstruktur.
`/bin`	Grundlegende binäre Dateien, z. B. Kommandos, die der Systemadministrator und normale Benutzer brauchen. Enthält gewöhnlich auch die Shells, z. B. Bash.
`/boot`	Statische Dateien des Bootloaders.
`/dev`	Erforderliche Dateien für den Zugriff auf Host-spezifische Geräte.
`/etc`	Host-spezifische Systemkonfigurationsdateien.
`/home`	Enthält die Home-Verzeichnisse aller Benutzer mit einem Konto im System. Das Home-Verzeichnis von `root` befindet sich jedoch nicht unter `/home`, sondern unter `/root`.
`/lib`	Grundlegende freigegebene Bibliotheken und Kernel-Module.
`/media`	Einhängepunkte für Wechselmedien.
`/mnt`	Einhängepunkt für das temporäre Einhängen eines Dateisystems.

Verzeichnis	Inhalt
`/opt`	Add-On-Anwendungssoftwarepakete.
`/Root`	Home-Verzeichnis für den Superuser `root`.
`/sbin`	Grundlegende Systembinärdateien.
`/srv`	Daten für Dienste, die das System bereitstellt.
`/tmp`	Temporäre Dateien.
`/usr`	Sekundäre Hierarchie mit Nur-Lese-Daten.
`/var`	Variable Daten wie Protokolldateien.
`/Fenster`	Nur verfügbar, wenn sowohl Microsoft Windows* als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten.

Die folgende Liste bietet detailliertere Informationen und einige Beispiele für die Dateien und Unterverzeichnisse, die in den Verzeichnissen verfügbar sind:

`/bin`

Enthält die grundlegenden Shell-Befehle, die `root` und andere Benutzer verwenden können. Zu diesen Kommandos gehören **`ls`**, **`mkdir`**, **`cp`**, **`mv`**, **`rm`** und **`rmdir`**. `/bin` umfasst außerdem Bash, die Standard-Shell in SUSE Linux Enterprise Server.

`/boot`

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

`/dev`

Enthält Gerätedateien, die Hardware-Komponenten darstellen.

`/etc`

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

`/home/BENUTZERNAME`

Enthält die privaten Daten aller Benutzer, die ein Konto auf dem System haben. Die Dateien, die hier gespeichert sind, können nur durch den Besitzer oder den Systemadministrator geändert werden. Standardmäßig befinden sich hier Ihr Email-Verzeichnis und Ihre persönliche Desktopkonfiguration in Form von verborgenen Dateien und Verzeichnissen, z. B. `.gconf/` und `.config`.

Anmerkung: Home-Verzeichnis in einer Netzwerkumgebung

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

`/lib`

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

`/media`

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

`/mnt`

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

`/opt`

Reserviert für die Installation von Drittanbieter-Software. Hier finden Sie optionale Softwareprogramme und größere Add-On-Programmpakete.

`/root`

Home-Verzeichnis für den Benutzer `root`. Hier befinden sich die persönlichen Daten von `root`.

`/run`

Ein tmpfs-Verzeichnis, das von `systemd` und verschiedenen Komponenten genutzt wird. `/var/run` stellt einen symbolischen Link zu `/run` dar.

`/sbin`

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

`/srv`

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

`/tmp`

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

Wichtig: Bereinigen des temporären Verzeichnisses `/tmp` bei Systemstart

Im Verzeichnis `/tmp` gespeicherte Daten werden nicht zwingend bei einem Neustart des Systems beibehalten. Dies ist beispielsweise von den Einstellungen in `/etc/tmpfiles.d/tmp.conf` abhängig.

`/usr`

`/usr` hat nichts mit Benutzern („user“) zu tun, sondern ist das Akronym für UNIX-Systemressourcen. Die Daten in `/usr` sind statische, schreibgeschützte Daten, die auf verschiedenen Hosts freigegeben sein können, die den `Filesystem Hierarchy Standard` (FHS) einhalten. Dieses Verzeichnis enthält alle Anwendungsprogramme (auch die grafischen Desktops wie GNOME) und bildet eine zweite Hierarchie im Dateisystem. `/usr` enthält mehrere Unterverzeichnisse, z. B. `/usr/bin`, `/usr/sbin`, `/usr/local` und `/usr/share/doc`.

`/usr/bin`

Enthält Programme, die für den allgemeinen Zugriff verfügbar sind.

`/usr/sbin`

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

`/usr/local`

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

`/usr/share/doc`

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

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

Wenn HOWTOs (Verfahrensbeschreibungen) auf Ihrem System installiert sind, enhält `/usr/share/doc` auch das Unterverzeichnis `howto` mit zusätzlicher Dokumentation zu vielen Aufgaben im Zusammenhang mit der Einrichtung und Ausführung von Linux-Software.

`/var`

Während `/usr` statische, schreibgeschützte Daten enthält, ist `/var` für Daten, die während des Systembetriebs geschrieben werden und daher variabel sind, z. B. Protokolldateien oder Spooling-Daten. Eine Übersicht über die wichtigsten Protokolldateien finden Sie unter `/var/log/`. Weitere Informationen stehen unter *Tabelle 40.1, „Protokolldateien“* zur Verfügung.

1.2 Schreiben von Shell-Skripten

Shell-Skripte bieten eine bequeme Möglichkeit, die verschiedensten Aufgaben zu erledigen: Erfassen von Daten, Suche nach einem Wort oder Begriff in einem Text und andere nützliche Dinge. Das folgende Beispiel zeigt ein kleines Shell-Skript, das einen Text druckt:

BEISPIEL 1.1 EIN SHELL-SKRIPT, DAS EINEN TEXT DRUCKT

```
#!/bin/sh ❶
# Output the following line: ❷
echo "Hello World" ❸
```

❶ Die erste Zeile beginnt mit dem *Shebang*-Zeichen (`#!`), das darauf hinweist, dass es sich bei dieser Datei um ein Skript handelt. Das Skript wird mit dem Interpreter ausgeführt, der nach dem Shebang angegeben ist, in diesem Fall mit `/bin/sh`.

❷ Die zweite Zeile ist ein Kommentar, der mit dem Hash-Zeichen beginnt. Es wird empfohlen, schwierige Zeilen zu kommentieren, damit ihre Bedeutung auch später klar ist.

❸ Die dritte Zeile verwendet das integrierte Kommando **`echo`**, um den entsprechenden Text zu drucken.

Bevor Sie dieses Skript ausführen können, müssen einige Voraussetzungen erfüllt sein:

1. Jedes Skript muss eine Shebang-Zeile enthalten (wie im obigen Beispiel.) Falls die Zeile fehlt, müssen Sie den Interpreter manuell aufrufen.
2. Sie können das Skript an beliebiger Stelle speichern. Jedoch empfiehlt es sich, es in einem Verzeichnis zu speichern, in dem die Shell es finden kann. Der Suchpfad in einer Shell wird durch die Umgebungsvariable `PATH` bestimmt. In der Regel verfügt ein normaler Benutzer über keinen Schreibzugriff auf `/usr/bin`. Daher sollten Sie Ihre Skripten im Benutzerverzeichnis `~/bin/` speichern. Das obige Beispiel erhält den Namen `hello.sh`.
3. Das Skript muss zum Ausführen von Dateien berechtigt sein. Stellen Sie die Berechtigungen mit dem folgenden Kommando ein:

```
chmod +x ~/bin/hello.sh
```

Wenn Sie alle oben genannten Voraussetzungen erfüllt haben, können Sie das Skript mithilfe der folgenden Methoden ausführen:

1. **Als absoluten Pfad.** Das Skript kann mit einem absoluten Pfad ausgeführt werden. In unserem Fall lautet er **`~/bin/hello.sh`**.
2. **Überall.** Wenn die Umgebungsvariable `PATH` das Verzeichnis enthält, in dem sich das Skript befindet, können Sie das Skript mit **`hello.sh`** ausführen.

1.3 Umlenken von Kommandoereignissen

Jedes Kommando kann drei Kanäle für Eingabe oder Ausgabe verwenden:

- **Standardausgabe.** Dies ist der Standardausgabe-Kanal. Immer wenn ein Kommando eine Ausgabe erzeugt, verwendet es den Standardausgabe-Kanal.
- **Standardeingabe.** Wenn ein Kommando Eingaben von Benutzern oder anderen Kommandos benötigt, verwendet es diesen Kanal.
- **Standardfehler.** Kommandos verwenden diesen Kanal zum Melden von Fehlern.

Zum Umlenken dieser Kanäle bestehen folgende Möglichkeiten:

`Kommando > Datei`

Speichert die Ausgabe des Kommandos in eine Datei; eine etwaige bestehende Datei wird gelöscht. Beispielsweise schreibt das Kommando **`ls`** seine Ausgabe in die Datei `listing.txt`:

```
ls > listing.txt
```

`Kommando >> Datei`

Hängt die Ausgabe des Kommandos an eine Datei an. Beispielsweise hängt das Kommando **`ls`** seine Ausgabe an die Datei `listing.txt` an:

```
ls >> listing.txt
```

`Kommando < Datei`

Liest die Datei als Eingabe für das angegebene Kommando. Beispielsweise liest das Kommando **`read`** den Inhalt der Datei in die Variable ein:

```
read a < foo
```

`Kommando1 | Kommando2`

Leitet die Ausgabe des linken Kommandos als Eingabe für das rechte Kommando um. Beispiel: Das Kommando **`cat`** gibt den Inhalt der Datei `/proc/cpuinfo` aus. Diese Ausgabe wird von **`grep`** verwendet, um nur diejenigen Zeilen herauszufiltern, die `cpu` enthalten:

```
cat /proc/cpuinfo | grep cpu
```

Jeder Kanal verfügt über einen *Dateideskriptor*: 0 (Null) für Standardeingabe, 1 für Standardausgabe und 2 für Standardfehler. Es ist zulässig, diesen Dateideskriptor vor einem `<`- oder `>`-Zeichen einzufügen. Beispielsweise sucht die folgende Zeile nach einer Datei, die mit `foo` beginnt, aber seine Fehlermeldungen durch Umlenkung zu `/dev/null` unterdrückt:

```
find / -name "foo*" 2>/dev/null
```

1.4 Verwenden von Aliassen

Ein Alias ist ein Definitionskürzel für einen oder mehrere Kommandos. Die Syntax für einen Alias lautet:

```
alias NAME=DEFINITION
```

Beispielsweise definiert die folgende Zeile den Alias **lt**, der eine lange Liste ausgibt (Option `-l`), sie nach Änderungszeit sortiert (`-t`) und sie in umgekehrter Reihenfolge sortiert ausgibt (`-r`):

```
alias lt='ls -ltr'
```

Zur Anzeige aller Aliasdefinitionen verwenden Sie **alias**. Entfernen Sie den Alias mit **Alias entfernen** und dem entsprechenden Aliasnamen.

1.5 Verwenden von Variablen in der Bash-Shell

Eine Shell-Variable kann global oder lokal sein. Auf globale Variablen, z. B. Umgebungsvariablen, kann in allen Shells zugegriffen werden. Lokale Variablen sind hingegen nur in der aktuellen Shell sichtbar.

Verwenden Sie zur Anzeige von allen Umgebungsvariablen das Kommando **printenv**. Wenn Sie den Wert einer Variable kennen müssen, fügen Sie den Namen Ihrer Variablen als ein Argument ein:

```
printenv PATH
```

Eine Variable (global oder lokal) kann auch mit **echo** angezeigt werden:

```
echo $PATH
```

Verwenden Sie zum Festlegen einer lokalen Variablen einen Variablennamen, gefolgt vom Gleichheitszeichen und dem Wert für den Namen:

```
PROJECT="SLED"
```

Geben Sie keine Leerzeichen um das Gleichheitszeichen ein, sonst erhalten Sie einen Fehler. Verwenden Sie zum Setzen einer Umgebungsvariablen **export**:

```
export NAME="tux"
```

Zum Entfernen einer Variable verwenden Sie **unset**:

```
unset NAME
```

Die folgende Tabelle enthält einige häufige Umgebungsvariablen, die Sie in Ihren Shell-Skripten verwenden können:

TABELLE 1.5 NÜTZLICHE UMGEBUNGSVARIABLEN

HOME	Home-Verzeichnis des aktuellen Benutzers
HOST	Aktueller Hostname
LANG	Wenn ein Werkzeug lokalisiert wird, verwendet es die Sprache aus dieser Umgebungsvariablen. Englisch kann auch auf C gesetzt werden
PFAD	Suchpfad der Shell, eine Liste von Verzeichnissen, die durch Doppelpunkte getrennt sind
PS1	Gibt die normale Eingabeaufforderung an, die vor jedem Kommando angezeigt wird
PS2	Gibt die sekundäre Eingabeaufforderung an, die beim Ausführen eines mehrzeiligen Kommandos angezeigt wird
PWD	Aktuelles Arbeitsverzeichnis
USER	Aktueller Benutzer

1.5.1 Verwenden von Argumentvariablen

Wenn Sie beispielsweise über das Skript **foo.sh** verfügen, können Sie es wie folgt ausführen:

```
foo.sh "Tux Penguin" 2000
```

Für den Zugriff auf alle Argumente, die an Ihr Skript übergeben werden, benötigen Sie Positionsparameter. Diese sind $1 für das erste Argument, $2 für das zweite usw. Sie können bis zu neun Parameter verwenden. Verwenden Sie $0 zum Abrufen des Skriptnamens.

Das folgende Skript **foo.sh** gibt alle Argumente von 1 bis 4 aus:

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

Wenn Sie das Skript mit den obigen Argumenten ausführen, erhalten Sie Folgendes:

```
"Tux Penguin" "2000" "" ""
```

1.5.2 Verwenden der Variablenersetzung

Variablenersetzungen wenden beginnend von links oder rechts ein Schema auf den Inhalt einer Variable an. Die folgende Liste enthält die möglichen Syntaxformen:

`${VAR#schema}`

entfernt die kürzeste mögliche Übereinstimmung von links:

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##schema}`

entfernt die längste mögliche Übereinstimmung von links:

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

`${VAR%schema}`

entfernt die kürzeste mögliche Übereinstimmung von rechts:

```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%schema}`

entfernt die längste mögliche Übereinstimmung von rechts:

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

`${VAR/pattern_1/pattern_2}`

ersetzt den Inhalt von *VAR* von *PATTERN_1* durch *PATTERN_2*:

```
file=/home/tux/book/book.tar.bz2
echo ${file/tux/wilber}
/home/wilber/book/book.tar.bz2
```

1.6 Gruppieren und Kombinieren von Kommandos

In Shells können Sie Kommandos für die bedingte Ausführung verketten und gruppieren. Jedes Kommando übergibt einen Endcode, der den Erfolg oder Misserfolg seiner Ausführung bestimmt. Wenn er 0 (Null) lautet, war das Kommando erfolgreich, alle anderen Codes bezeichnen einen Fehler, der spezifisch für das Kommando ist.

Die folgende Liste zeigt, wie sich Kommandos gruppieren lassen:

`Kommando1 ; Kommando2`

führt die Kommandos in sequenzieller Reihenfolge aus. Der Endcode wird nicht geprüft. Die folgende Zeile zeigt den Inhalt der Datei mit **`cat`** an und gibt deren Dateieigenschaften unabhängig von deren Endcodes mit **`ls`** aus:

```
cat filelist.txt ; ls -l filelist.txt
```

`Kommando1 && Kommando2`

führt das rechte Kommando aus, wenn das linke Kommando erfolgreich war (logisches UND). Die folgende Zeile zeigt den Inahlt der Datei an und gibt deren Dateieigenschaften nur aus, wenn das vorherige Kommando erfolgreich war (vgl. mit dem vorherigen Eintrag in dieser Liste):

```
cat filelist.txt && ls -l filelist.txt
```

`Kommando1 || Kommando2`

führt das rechte Kommando aus, wenn das linke Kommando fehlgeschlagen ist (logisches ODER). Die folgende Zeile legt nur ein Verzeichnis in `/home/wilber/bar` an, wenn die Erstellung des Verzeichnisses in `/home/tux/foo` fehlgeschlagen ist:

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

`funcname(){ ... }`

erstellt eine Shell-Funktion. Sie können mithilfe der Positionsparameter auf ihre Argumente zugreifen. Die folgende Zeile definiert die Funktion `hello` für die Ausgabe einer kurzen Meldung:

```
hello() { echo "Hello $1"; }
```

Sie können diese Funktion wie folgt aufrufen:

```
hello Tux
```

Die Ausgabe sieht wie folgt aus:

```
Hello Tux
```

1.7 Arbeiten mit häufigen Ablaufkonstrukten

Zur Steuerung des Ablaufs Ihres Skripts verfügt eine Shell über **`while`**-, **`if`**-, **`for`**- und **`case`**-Konstrukte.

1.7.1 Das Steuerungskommando „if“

Das Kommando **`if`** wird verwendet, um Ausdrücke zu prüfen. Beispielsweise testet der folgende Code, ob es sich beim aktuellen Benutzer um Tux handelt:

```
if test $USER = "tux"; then
  echo "Hello Tux."
else
  echo "You are not Tux."
fi
```

Der Testausdruck kann so komplex oder einfach wie möglich sein. Der folgende Ausdruck prüft, ob die Datei `foo.txt` existiert:

```
if test -e /tmp/foo.txt ; then
  echo "Found foo.txt"
fi
```

Der Testausdruck kann auch in eckigen Klammern abgekürzt werden:

```
if [ -e /tmp/foo.txt ] ; then
```

```
  echo "Found foo.txt"
fi
```

Weitere nützliche Ausdrücke finden Sie unter http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lsst/ch03sec02.html.

1.7.2 Erstellen von Schleifen mit dem Kommando `for`

Mithilfe der `for`-Schleife können Sie Kommandos an einer Liste von Einträgen ausführen. Beispielsweise gibt der folgende Code einige Informationen über PNG-Dateien im aktuellen Verzeichnis aus:

```
for i in *.png; do
 ls -l $i
done
```

1.8 Weiterführende Informationen

Wichtige Informationen über die Bash-Shell finden Sie auf den man-Seiten zu `man bash`. Für weitere Informationen zu diesem Thema siehe die folgende Liste:

- http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html – Bash Guide for Beginners (Bash-Anleitungen für Anfänger)
- http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html – BASH Programming - Introduction HOW-TO (BASH-Programmierung – Einführende schrittweise Anleitungen)
- http://tldp.org/LDP/abs/html/index.html – Advanced Bash-Scripting Guide (Anleitung für erweiterte Bash-Skripts)
- http://www.grymoire.com/Unix/Sh.html – Sh - the Bourne Shell (Sh – die Bourne-Shell)

2 sudo

Viele Kommandos und Systemdienstprogramme müssen als `root` ausgeführt werden, um Dateien zu bearbeiten und/oder Tasks auszuführen, für die nur der Superuser berechtigt ist. Aus Sicherheitsgründen und um das unbeabsichtigte Ausführen gefährlicher Kommandos zu vermeiden, ist es allgemein ratsam, sich nicht direkt als `root` anzumelden. Stattdessen wird empfohlen, als normaler, nicht privilegierter Benutzer zu arbeiten und das **`sudo`**-Kommando zum Ausführen von Kommandos mit erhöhten Berechtigungen zu verwenden.

Auf SUSE Linux Enterprise Server ist **`sudo`** standardmäßig auf eine ähnliche Funktionsweise wie „su“ konfiguriert. Jedoch bietet **`sudo`** die Möglichkeit, Benutzern das Ausführen von Kommandos mit Berechtigungen jedes anderen Benutzers mit umfassenden Konfigurationsmöglichkeiten zu erlauben. Dies kann dazu genutzt werden, Rollen mit bestimmten Berechtigungen bestimmten Benutzern und Gruppen zuzuweisen. Es ist beispielsweise möglich, Mitgliedern der Gruppe `users` das Ausführen eines Kommandos mit den Berechtigungen von `wilber` zu erlauben. Der Zugriff auf das Kommando kann zusätzlich eingeschränkt werden, indem beispielsweise das Angeben jeglicher Kommandooptionen verboten wird. Während „su“ immer das `root`-Passwort für die Authentifizierung mit PAM erfordert, kann **`sudo`** für die Authentifizierung mit Ihren eigenen Berechtigungsnachweisen konfiguriert werden. Dies erhöht die Sicherheit, da das `root`-Passwort nicht freigegeben werden muss. Sie können Mitgliedern der Gruppe `users` beispielsweise erlauben, ein **`frobnicate`**-Kommando als `wilber` auszuführen, mit der Einschränkung, dass keine Argumente angegeben werden. Dies kann dazu genutzt werden, Rollen mit bestimmten Funktionen bestimmten Benutzern und Gruppen zuzuweisen.

2.1 Grundlegende Verwendung von **sudo**

`sudo` ist einfach zu verwenden und dabei sehr funktionsreich.

2.1.1 Ausführung eines einzelnen Kommandos

Wenn Sie als normaler Benutzer angemeldet sind, können Sie alle Befehle als `root` ausführen, indem Sie **`sudo`** vor den Befehl setzen. Eine Eingabeaufforderung für das root-Passwort erscheint und bei erfolgreicher Authentifizierung wird das Kommando als `root` ausgeführt:

```
tux > id -un❶
tux
```

```
tux > sudo id -un
root's password: ❷
root
tux > id -un
tux ❸
tux > sudo id -un
❹
root
```

❶ Das Kommando **`id -un`** druckt den Anmeldenamen des aktuellen Benutzers.

❷ Das Passwort wird bei der Eingabe weder als Klartext noch durch Punkte angezeigt.

❸ Nur Kommandos, die mit **`sudo`** beginnen, werden mit erhöhten Berechtigungen ausgeführt. Wenn Sie dasselbe Kommando ohne das Präfix **`sudo`** ausführen, wird es wieder mit den Berechtigungen des aktuellen Benutzers ausgeführt.

❹ Für einen begrenzten Zeitraum müssen Sie das `root`-Passwort nicht erneut eingeben.

Tipp: E/A-Umleitung

Die E/A-Umleitung funktioniert nicht so, wie Sie es wahrscheinlich erwarten:

```
tux >  sudo echo s > /proc/sysrq-trigger
bash: /proc/sysrq-trigger: Permission denied
tux >  sudo cat < /proc/1/maps
bash: /proc/1/maps: Permission denied
```

Nur die **`echo`**-/**`cat`**-Binärdatei wird mit erhöhten Berechtigungen ausgeführt. Die Umleitung erfolgt über die Shell des Benutzers mit Benutzerberechtigungen. Sie können entweder eine Shell starten, wie in *Abschnitt 2.1.2, „Starten einer Shell“* beschrieben, oder stattdessen das Dienstprogramm **`dd`** verwenden:

```
echo s | sudo dd of=/proc/sysrq-trigger
sudo dd if=/proc/1/maps | cat
```

2.1.2 Starten einer Shell

Es kann mühselig sein, jedem Befehl **sudo** voranstellen zu müssen. Sie könnten eine Shell als **sudo bash**-Kommando angeben. Es wird jedoch empfohlen, einen der integrierten Mechanismen zum Starten einer Shell zu verwenden:

`sudo -s (<Kommando>)`

Startet eine von der Umgebungsvariablen `SHELL` angegebene Shell oder die Standard-Shell des Zielbenutzers. Wird ein Kommando angegeben, wird es an die Shell übergeben (mit der Option `-c`), sonst wird die Shell im interaktiven Modus ausgeführt.

```
tux:~ > sudo -i
root's password:
root:/home/tux # exit
tux:~ >
```

`sudo -i (<Kommando>)`

Wie `-s`, startet die Shell jedoch als Login-Shell. Dies bedeutet, dass die Startdateien der Shell (`.profile` usw.) verarbeitet werden und das aktuelle Home-Verzeichnis als Basisverzeichnis des Zielbenutzers festgelegt wird.

```
tux:~ > sudo -i
root's password:
root:~ # exit
tux:~ >
```

2.1.3 Umgebungsvariablen

Standardmäßig gibt **sudo** keine Umgebungsvariablen weiter:

```
tux > ENVVAR=test env | grep ENVVAR
ENVVAR=test
tux > ENVVAR=test sudo env | grep ENVVAR
root's password:
❶
tux >
```

❶ Die leere Ausgabe zeigt, dass die Umgebungsvariable `ENVVAR` im Kontext des Kommandos, das mit **sudo** ausgeführt wurde, nicht vorhanden war.

Dieses Verhalten kann mit der Option `env_reset` geändert werden. Siehe *Tabelle 2.1, „Hilfreiche Flags und Optionen“*.

2.2 Konfigurieren von **sudo**

sudo ist ein sehr flexibles Werkzeug mit umfassenden Konfigurationsmöglichkeiten.

Anmerkung: Versehentliches Aussperren aus sudo

Wenn Sie sich versehentlich aus **sudo** ausgesperrt haben, öffnen Sie mit **su -** und dem `root`-Passwort eine Root-Shell. Beheben Sie den Fehler mit **visudo**.

2.2.1 Bearbeiten der Konfigurationsdateien

Die Hauptkonfigurationsdatei mit den Richtlinien für **sudo** ist `/etc/sudoers`. Da es möglich ist, sich selbst aus dem System auszusperren, wenn in dieser Datei Fehler enthalten sind, wird dringend empfohlen, **visudo** zum Bearbeiten zu verwenden. Gleichzeitige Änderungen an der geöffneten Datei werden so verhindert und es wird vor dem Speichern der Änderungen auf Syntaxfehler geprüft.

Trotz des Namens können Sie andere Editoren als „vi“ verwenden, indem Sie die Umgebungsvariable `EDITOR` festlegen. Beispiel:

```
sudo EDITOR=/usr/bin/nano visudo
```

Die Datei `/etc/sudoers` selbst hingegen wird von den Systempaketen bereitgestellt und Änderungen können bei Aktualisierungen verloren gehen. Daher wird empfohlen, benutzerdefinierte Konfigurationen in Dateien im Verzeichnis `/etc/sudoers.d/` abzulegen. Jede Datei in diesem Verzeichnis ist automatisch eingeschlossen. Um eine Datei in diesem Unterverzeichnis zu erstellen oder zu bearbeiten, führen Sie das folgende Kommando aus:

```
sudo visudo -f /etc/sudoers.d/NAME
```

Alternativ mit einem anderen Editor (beispielsweise **nano**):

```
sudo EDITOR=/usr/bin/nano visudo -f /etc/sudoers.d/NAME
```

Anmerkung: Ignorierte Dateien in `/etc/sudoers.d`

Das Kommando `#includedir` in `/etc/sudoers`, das für `/etc/sudoers.d` verwendet wird, ignoriert Dateien, die mit einer Tilde (`~`) enden oder einen Punkt (`.`) enthalten.

Führen Sie `man 8 visudo` aus, um weitere Informationen zum Kommando `visudo` zu erhalten.

2.2.2 Basiskonfigurationssyntax von sudoers

In den sudoers-Konfigurationsdateien gibt es zwei Optionstypen: Strings und Flags. Strings können beliebige Werte enthalten, Flags hingegen können nur aktiviert (ON) oder deaktiviert (OFF) werden. Die wichtigsten Syntaxkonstrukte für sudoers-Konfigurationsdateien sind:

```
# Everything on a line after a # gets ignored ❶
Defaults !insults # Disable the insults flag ❷
Defaults env_keep += "DISPLAY HOME" # Add DISPLAY and HOME to env_keep
tux ALL = NOPASSWD: /usr/bin/frobnicate, PASSWD: /usr/bin/journalctl ❸
```

❶ Es gibt zwei Ausnahmen: `#include` und `#includedir` sind normale Kommandos. Gefolgt von Zahlen, gibt es eine UID an.

❷ Entfernen Sie das Ausrufezeichen (`!`), um für das angegebene Flag ON festzulegen.

❸ Siehe *Abschnitt 2.2.3, „Regeln in sudoers“*.

TABELLE 2.1 HILFREICHE FLAGS UND OPTIONEN

Optionsname	Beschreibung	Beispiel
`targetpw`	Dieses Flag steuert, ob der aufrufende Benutzer das Passwort des Zielbenutzers (ON) (beispielsweise `root`) oder des aufrufenden Benutzers (OFF) eingeben muss.	`Defaults targetpw # Turn targetpw flag ON`
`rootpw`	Ist diese Option festgelegt, fordert `sudo` die Eingabe des `root`-Passworts und nicht des Passworts des Zielbenutzers oder des aufrufenden Benutzers. Standardmäßig ist OFF festgelegt.	`Defaults !rootpw # Turn rootpw flag OFF`

Optionsname	Beschreibung	Beispiel
`env_reset`	Ist diese Option festgelegt, richtet **`sudo`** eine Minimalumgebung ein, in der nur `TERM`, `PATH`, `HOME`, `MAIL`, `SHELL`, `LOGNAME`, `USER`, `USERNAME` und `SUDO_*` festgelegt sind. Zusätzlich werden Variablen aus der aufrufenden Umgebung importiert, die in `env_keep` aufgelistet sind. Standardmäßig ist ON festgelegt.	`Defaults env_reset # Turn env_reset flag ON`

`env_keep`	Eine Liste der Umgebungsvariablen, die beizubehalten sind, wenn für das Flag `env_reset` ON festgelegt ist.	`# Set env_keep to contain EDITOR and PROMPT`
		`Defaults env_keep = "EDITOR PROMPT"`
		`Defaults env_keep += "JRE_HOME" # Add JRE_HOME`
		`Defaults env_keep -= "JRE_HOME" # Remove JRE_HOME`

`env_delete`	Eine Liste der Umgebungsvariablen, die zu löschen sind, wenn für das Flag `env_reset` OFF festgelegt ist.	`# Set env_delete to contain EDITOR and PROMPT`
		`Defaults env_delete = "EDITOR PROMPT"`
		`Defaults env_delete += "JRE_HOME" # Add JRE_HOME`
		`Defaults env_delete -= "JRE_HOME" # Remove JRE_HOME`

Das Token `Defaults` kann auch zum Erstellen von Aliassen für eine Sammlung von Benutzern, Hosts oder Kommandos verwendet werden. Außerdem ist es möglich, eine Option anzuwenden, die nur für eine bestimmte Reihe von Benutzern gültig ist.

Genauere Informationen zur Konfigurationsdatei `/etc/sudoers` erhalten Sie mit dem Kommando **`man 5 sudoers`**.

2.2.3 Regeln in sudoers

Die Regeln in der sudoers-Konfiguration können sehr komplex sein. In diesem Abschnitt werden daher nur die Grundlagen abgedeckt. Jede Regel befolgt ein Basisschema (`[]` markiert optionale Teile):

```
#Who      Where         As whom      Tag                What
User_List Host_List = [(User_List)] [NOPASSWD:|PASSWD:] Cmnd_List
```

SYNTAX FÜR SUDOERS-REGELN

`User_List`

Eine oder mehrere Kennungen (getrennt durch `,`): Entweder ein Benutzername, eine Gruppe im Format `%GROUPNAME` oder eine Benutzer-ID im Format `#UID` . Eine Negation erzielen Sie mit dem Präfix `!`

`Host_List`

Eine oder mehrere Kennungen (getrennt durch `,`): Entweder ein (vollständig qualifizierter) Hostname oder eine IP-Adresse. Eine Negation erzielen Sie mit dem Präfix `!` `ALL` ist die übliche Option für `Host_List` .

`NOPASSWD:|PASSWD:`

Der Benutzer wird nicht aufgefordert, ein Passwort einzugeben, wenn Kommandos ausgeführt werden, die `CMDSPEC` nach `NOPASSWD:` entsprechen.
`PASSWD` ist der Standardwert. Er muss nur angegeben werden, wenn beide Werte in der gleichen Zeile sind:

```
tux ALL = PASSWD: /usr/bin/foo, NOPASSWD: /usr/bin/bar
```

`Cmnd_List`

Eine oder mehrere Kennungen (getrennt durch `,`): Ein Pfad zu einer ausführbaren Datei, gefolgt von erlaubten Argumenten oder keinen weiteren Angaben.

```
/usr/bin/foo     # Anything allowed
/usr/bin/foo bar # Only "/usr/bin/foo bar" allowed
/usr/bin/foo ""  # No arguments allowed
```

`ALL` kann als `User_List` , `Host_List` und `Cmnd_List` verwendet werden.

Eine Regel, die es `tux` erlaubt, alle Kommandos als „root“ ohne Eingabe des Passworts auszuführen:

```
tux ALL = NOPASSWD: ALL
```

Eine Regel, die es `tux` erlaubt, **`systemctl restart apache2`** auszuführen:

```
tux ALL = /usr/bin/systemctl restart apache2
```

Eine Regel, die es `tux` erlaubt, **`wall`** als `admin` ohne Argumente auszuführen:

```
tux ALL = (admin) /usr/bin/wall ""
```

Warnung: Gefährliche Konstrukte

Konstrukte des Typs

```
ALL ALL = ALL
```

dürfen nicht ohne `Defaults targetpw` verwendet werden, sonst kann jeder Kommandos als `root` ausführen.

2.3 Häufige Einsatzmöglichkeiten

Obwohl die Standardkonfiguration oft für einfache Konfigurationen und Desktopumgebungen ausreicht, können benutzerdefinierte Konfigurationen sehr hilfreich sein.

2.3.1 Verwenden von **sudo** ohne `root`-Passwort

In Anwendungsfällen mit besonderen Einschränkungen („Benutzer X kann Kommando Y nur als `root`“ ausführen) ist dies nicht möglich. In anderen Fällen ist es weiterhin vorteilhaft, eine Art Trennung zu haben. Grundsätzlich können Mitglieder der Gruppe `wheel` alle Kommandos mit **`sudo`** als „root“ ausführen.

1. Fügen Sie sich selbst zur Gruppe `wheel` hinzu.
   Ist Ihr Benutzerkonto nicht bereits Mitglied der Gruppe `wheel`, fügen Sie es hinzu, indem Sie **`sudo usermod -a -G wheel`** *BENUTZERNAME* ausführen und sich ab- und wieder anmelden. Überprüfen Sie, ob die Änderung erfolgreich war, indem Sie **`groups`** *BENUTZERNAME* ausführen.
2. Legen Sie die Authentifizierung mit dem Passwort des aufrufenden Benutzers als Standard fest.

Erstellen Sie die Datei `/etc/sudoers.d/userpw` mit **`visudo`** (siehe *Abschnitt 2.2.1, „Bearbeiten der Konfigurationsdateien“*) und fügen Sie Folgendes hinzu:

```
Defaults !targetpw
```

3. Wählen Sie eine neue Standardregel aus.
   Je nachdem, ob Sie möchten, dass Benutzer ihre Passwörter erneut eingeben oder nicht, entfernen Sie das Kommentarzeichen in der entsprechenden Zeile in `/etc/sudoers` und kommentieren Sie die Standardregel aus.

```
## Uncomment to allow members of group wheel to execute any command
# %wheel ALL=(ALL) ALL

## Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL
```

4. Gestalten Sie die Standardregel restriktiver.
   Kommentieren Sie die Regel, die alles erlaubt, in `/etc/sudoers` aus oder löschen Sie sie:

```
ALL     ALL=(ALL) ALL   # WARNING! Only use this together with 'Defaults targetpw'!
```

Warnung: Gefährliche Regel in sudoers

Vergessen Sie diesen Schritt nicht, sonst kann *jeder* Benutzer *alle* Kommandos als `root` ausführen!

5. Testen Sie die Konfiguration.
   Versuchen Sie, **`sudo`** als Mitglied und Nicht-Mitglied von `wheel` auszuführen.

```
tux:~ > groups
users wheel
tux:~ > sudo id -un
tux's password:
root
wilber:~ > groups
users
wilber:~ > sudo id -un
wilber is not in the sudoers file.  This incident will be reported.
```

2.3.2 Verwenden von **sudo** mit X.Org-Anwendungen

Wenn Sie Grafikanwendungen mit **sudo** starten, stoßen Sie auf den folgenden Fehler:

```
tux > sudo xterm
xterm: Xt error: Can't open display: %s
xterm: DISPLAY is not set
```

YaST wählt die ncurses-Schnittstelle und nicht die grafische Schnittstelle.

Um X.Org in Anwendungen zu verwenden, die mit **sudo** gestartet werden, müssen die Umgebungsvariablen `DISPLAY` und `XAUTHORITY` übertragen werden. Um dies zu konfigurieren, erstellen Sie die Datei `/etc/sudoers.d/xorg` (siehe *Abschnitt 2.2.1, „Bearbeiten der Konfigurationsdateien“*) und fügen Sie die folgende Zeile hinzu:

```
Defaults env_keep += "DISPLAY XAUTHORITY"
```

Wenn die Variable `XAUTHORITY` nicht bereits entsprechend festgelegt ist, legen Sie sie wie folgt fest:

```
export XAUTHORITY=~/.Xauthority
```

Jetzt können X.Org-Anwendungen wie üblich ausgeführt werden:

```
sudo yast2
```

2.4 Weitere Informationen

Einen kurzen Überblick über die verfügbaren Kommandozeilenschalter können Sie mit **sudo --help** abrufen. Eine Erklärung und andere wichtige Informationen finden Sie auf der man-Seite: **man 8 sudo**. Die Konfiguration ist auf der man-Seite **man 5 sudoers** dokumentiert.

3 YaST-Online-Aktualisierung

SUSE stellt fortlaufend Sicherheitsaktualisierungen für Ihr Softwareprodukt bereit. Standardmäßig stellt das Miniprogramm für die Aktualisierung sicher, dass Ihr System stets auf dem neuesten Stand ist. Weitere Informationen zu diesem Miniprogramm finden Sie im *Buch „*Bereitstellungshandbuch*", Kapitel 13 „Installieren bzw. Entfernen von Software", Abschnitt 13.5 „Halten Sie Ihr System auf dem neuesten Stand"*. Dieses Kapitel behandelt das alternative Tool für die Aktualisierung von Software-Paketen: die YaST-Online-Aktualisierung.

Die aktuellen Patches für SUSE® Linux Enterprise Server sind über ein Software-Aktualisierungs-Repository verfügbar. Wenn Sie Ihr Produkt während der Installation registriert haben, ist das Aktualisierungs-Repository bereits konfiguriert. Falls Sie SUSE Linux Enterprise Server noch nicht registriert haben, starten Sie die *Produktkonfiguration* in YaST. Alternativ können Sie ein Aktualisierungs-Repository manuell von einer verbürgten Quelle hinzufügen. Starten Sie zum Hinzufügen oder Entfernen von Repositorys den Repository-Manager über *Software › Software-Repositorys* in YaST. Weitere Informationen zum Repository Manager finden Sie in *Buch „*Bereitstellungshandbuch*", Kapitel 13 „Installieren bzw. Entfernen von Software", Abschnitt 13.4 „Verwalten von Software-Repositorys und -Diensten"*.

Anmerkung: Fehler beim Zugriff auf den Aktualisierungskatalog

Wenn Sie keinen Zugriff auf den Aktualisierungskatalog erhalten, liegt das eventuell daran, dass Ihr Abo abgelaufen ist. In der Regel umfasst SUSE Linux Enterprise Server ein einjähriges oder dreijähriges Abo, mit dem Sie Zugriff auf den Aktualisierungskatalog erhalten. Dieser Zugriff wird verweigert, sobald das Abo beendet ist.

Falls der Zugriff zum Aktualisierungskatalog verweigert wird, wird eine Warnmeldung angezeigt, mit der Sie aufgefordert werden, das SUSE Customer Center aufzurufen und Ihr Abo zu überprüfen. Das SUSE Customer Center erreichen Sie unter https://scc.suse.com// .

SUSE bietet Aktualisierungen mit verschiedenen Relevanzstufen:

Sicherheits-Updates

Beseitigen ernsthafte Sicherheitsrisiken und sollten stets installiert werden.

Empfohlene Updates

Beseitigen Probleme, die Ihrem Rechner schaden können.

Optionale Updates

Beseitigen nicht sicherheitsrelevante Probleme oder bieten Verbesserungen.

3.1 Das Dialogfeld „Online-Aktualisierung“

Zum Öffnen des Dialogfelds *Online-Aktualisierung* starten Sie YaST, und wählen Sie *Software* › *Online-Aktualisierung*. Stattdessen können Sie es auch von der Kommandozeile aus mit dem Kommando **`yast2 online_update`** starten.

Das Fenster *Online-Update* ist in vier Abschnitte unterteilt.

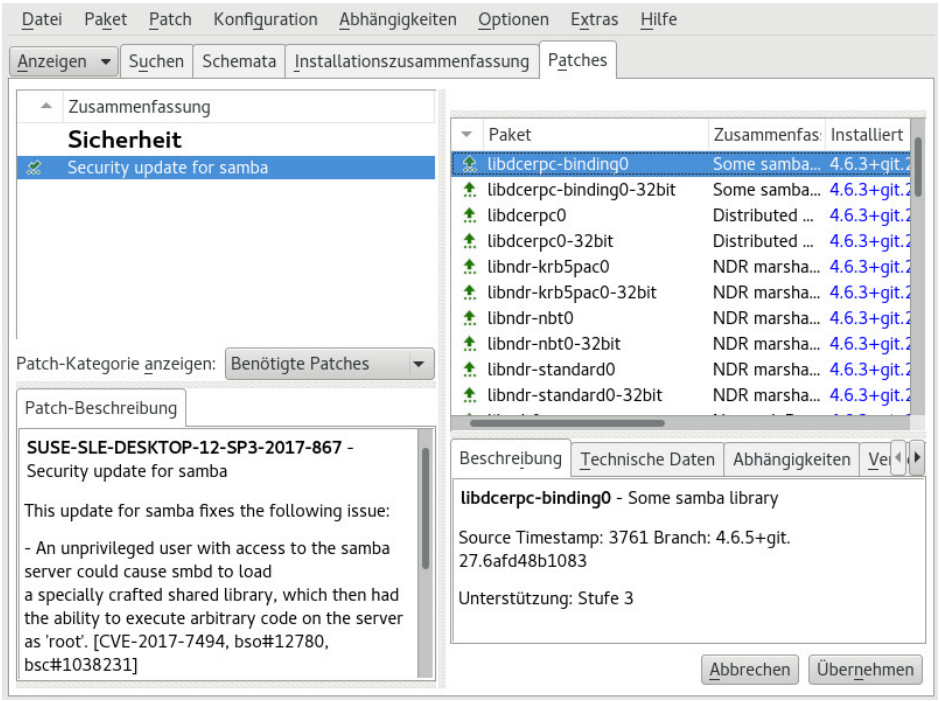


ABBILDUNG 3.1 YAST-ONLINE-AKTUALISIERUNG

Unter *Zusammenfassung* im linken Bereich werden die verfügbaren Patches für SUSE Linux Enterprise Server aufgeführt. Die Patches werden nach Sicherheitsrelevanz (`Sicherheit`, `Empfohlen` und `Optional`) sortiert. Sie können die Ansicht des Abschnitts *Zusammenfassung* ändern, indem Sie eine der folgenden Optionen unter *Patch-Kategorie anzeigen* auswählen:

Erforderliche Patches **(Standardansicht)**

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

Nicht erforderliche Patches

Patches für Pakete, die nicht auf Ihrem System installiert sind, oder Patches, die nicht mehr erforderlich sind (weil die relevanten Pakete bereits von einer anderen Quelle aktualisiert wurden).

Alle Patches

Alle verfügbaren Patches für SUSE Linux Enterprise Server.

Jeder Listeneintrag im Abschnitt *Zusammenfassung* besteht aus einem Symbol und dem Patch-Namen. Eine Übersicht der möglichen Symbole und deren Bedeutung erhalten Sie, wenn Sie die Taste Umschalttaste–F1 drücken. Die erforderlichen Aktionen für Patches der Kategorie `Sicherheit` und `Empfohlen` sind automatisch voreingestellt. Möglich sind die Aktionen *Automatisch installieren*, *Automatisch aktualisieren* und *Automatisch löschen*.

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

Wählen Sie einen Eintrag im Abschnitt *Zusammenfassung* aus, um eine kurze *Patch-Beschreibung* unten links im Dialogfeld anzuzeigen. Im Abschnitt oben rechts werden die Pakete aufgeführt, die im ausgewählten Patch enthalten sind (ein Patch kann aus mehreren Paketen bestehen). Klicken Sie im Abschnitt oben rechts auf einen Eintrag, um Details zu dem entsprechenden Paket, das im Patch enthalten ist, anzuzeigen.

3.2 Installieren von Patches

Im Dialogfeld der YaST-Online-Aktualisierung können Sie wahlweise alle verfügbaren Patches gleichzeitig installieren oder die gewünschten Patches manuell auswählen. Außerdem können Sie Patches, die auf das System angewendet wurden, zurücksetzen.

Standardmäßig sind alle neuen Patches (außer den `optionalen`), die derzeit für Ihr System verfügbar sind, bereits zur Installation markiert. Sie werden automatisch angewendet, sobald Sie auf *Übernehmen* oder *Anwenden* klicken. Falls das System bei einem oder mehreren Patches neu gebootet werden muss, werden Sie hierüber informiert, bevor die Patch-Installation beginnt. Sie können dann die Installation der ausgewählten Patches fortsetzen, die Installation aller Patches, für die das System neu gebootet werden muss, überspringen und die restlichen Patches installieren oder auch zur manuellen Patch-Auswahl zurückkehren.

PROZEDUR 3.1 ANWENDEN VON PATCHES MIT DER YAST-ONLINE-AKTUALISIERUNG

1. Starten Sie YaST, und wählen Sie *Software* › *Online-Aktualisierung*.
2. Sollen alle neuen Patches (ausgenommen die `optionalen` Patches), die derzeit für Ihr System verfügbar sind, automatisch angewendet werden, wählen Sie *Anwenden* oder *Übernehmen* aus.
3. Ändern Sie zunächst die Auswahl der Patches, die Sie anwenden möchten:
   a. Verwenden Sie die verfügbaren Filter und Ansichten der Schnittstelle. Detaillierte Informationen finden Sie in *Abschnitt 3.1, „Das Dialogfeld „Online-Aktualisierung““*.
   b. Wählen Sie die Patches gemäß Ihren Anforderungen aus (bzw. heben Sie die Auswahl der Patches wieder auf), und wählen Sie die entsprechende Aktion im Kontextmenü.

      Wichtig: Anwenden von Sicherheits-Updates ohne Ausnahme

      Heben Sie die Auswahl der `sicherheitsrelevanten` Patches nicht ohne stichhaltigen Grund auf. Diese Patches beseitigen ernsthafte Sicherheitsrisiken und schützen Ihr System vor Angriffen.

   c. Die meisten Patches umfassen Aktualisierungen für mehrere Pakete. Wenn Sie Aktionen für einzelne Pakete ändern möchten, klicken Sie mit der rechten Maustaste auf eine Paketansicht und wählen Sie eine Aktion.
   d. Bestätigen Sie Ihre Auswahl, und wenden Sie die ausgewählten Patches mit *Anwenden* oder *Übernehmen* an.
4. Klicken Sie nach abgeschlossener Installation auf *Beenden*, um das YaST-Dialogfeld *Online-Aktualisierung* zu verlassen. Ihr System ist nun auf dem neuesten Stand.

3.3 Automatische Online-Updates

YaST bietet außerdem die Möglichkeit, eine automatische Aktualisierung mit täglichem, wöchentlichem oder monatlichem Zeitplan einzurichten. Um das entsprechende Modul zu verwenden, müssen Sie zunächst das Paket `yast2-online-update-configuration` installieren.

Standardmäßig werden die Aktualisierungen als Delta-RPMs heruntergeladen. Das Neuaufbauen von RPM-Paketen aus Delta-RPMs bewirkt eine hohe Belastung des Arbeitsspeichers und des Prozessors. Aus Leistungsgründen müssen Sie daher bei bestimmten Einrichtungen oder Hardware-Konfigurationen die Verwendung von Delta-RPMs deaktivieren.

Einige Patches, z. B. Kernel-Updates oder Pakete mit Lizenzvereinbarungen, erfordern Benutzerinteraktion, wodurch der automatische Aktualisierungsprozess angehalten würde. Sie können festlegen, dass Patches, für die ein Eingreifen des Benutzers erforderlich ist, übersprungen werden sollen.

PROZEDUR 3.2 KONFIGURIEREN DES AUTOMATISCHEN ONLINE-UPDATES

1. Nach der Installation starten Sie YaST, und wählen Sie *Software* › *Einrichtung der Online-Aktualisierung*.
   Sie können das Modul auch mit dem Kommando **`yast2 online_update_configuration`** von der Kommandozeile aus starten.
2. Aktivieren Sie die Option *Automatische Online-Aktualisierung*.
3. Legen Sie das Aktualisierungsintervall fest: *Täglich*, *Wöchentlich* oder *Monatlich*.
4. Damit Lizenzvereinbarungen automatisch akzeptiert werden, aktivieren Sie die Option *Lizenzen zustimmen*.
5. Wählen Sie aus, ob Sie *Interaktive Patches überspringen* möchten, für den Fall, dass der Aktualisierungsprozess vollständig automatisch fortgesetzt werden soll.

   ### Wichtig: Überspringen von Patches

   Wenn Sie Pakete, die Benutzerinteraktion erfordern, überspringen, führen Sie gelegentlich eine manuelle *Online-Aktualisierung* aus, um diese Patches ebenfalls zu installieren. Andernfalls entgehen Ihnen möglicherweise wichtige Patches.
6. Sollen alle Pakete automatisch installiert werden, die durch die aktualisierten Pakete empfohlen werden, aktivieren Sie *Empfohlene Pakete einbeziehen*.
7. Soll die Verwendung von Delta-RPMs deaktiviert werden (aus Leistungsgründen), deaktivieren Sie *Delta-RPMs verwenden*.

8. Sollen die Patches nach Kategorie gefiltert werden (z. B. Sicherheits-Patches oder empfohlene Patches), aktivieren Sie *Nach Kategorie filtern*, und fügen Sie die entsprechenden Patch-Kategorien aus der Liste ein. Es werden nur Patches aus den ausgewählten Kategorien installiert. Andere werden übersprungen.

9. Bestätigen Sie die Konfiguration mit *OK*.

Die automatische Online-Aktualisierung startet das System im Anschluss nicht automatisch neu. Sind Paketaktualisierungen vorhanden, die einen System-Reboot erfordern, müssen Sie dies manuell durchführen.

4 YaST

YaST ist das Installations- und Konfigurationswerkzeug für SUSE Linux Enterprise Server. Mit der grafischen Benutzeroberfläche können Sie das System während und nach der Installation schnell und einfach an Ihre Bedürfnisse anpassen. Damit können Sie die Hardware einrichten, das Netzwerk und die Systemdienste konfigurieren und auch die Sicherheitseinstellungen verfeinern.

4.1 Erweiterte Tastenkombinationen

YaST umfasst einen Satz erweiterter Tastenkombinationen.

`Bildschirminhalt drucken`

Erstellt und speichert ein Bildschirmfoto. In einigen Desktop-Umgebungen mit YaST eventuell nicht verfügbar.

`Umschalttaste`–`F4`

Aktiviert/deaktiviert die optimierte Farbpalette für Benutzer mit beeinträchtigtem Sehvermögen.

`Umschalttaste`–`F7`

Aktiviert/Deaktiviert die Protokollierung von Fehlermeldungen (Debugging).

`Umschalttaste`–`F8`

Öffnet einen Dateidialog, über den Sie die Protokolldateien in einem nicht standardmäßigen Speicherort speichern können.

`Strg`–`Umschalttaste`–`Alt`–`D`

Sendet ein Fehlerereignis (Debugging). YaST-Module können darauf mit der Ausführung spezieller Debugging-Aktionen reagieren. Das Ergebnis ist abhängig vom jeweiligen YaST-Modul.

`Strg`–`Umschalttaste`–`Alt`–`M`

Startet/Stoppt den Makro-Rekorder.

`Strg`–`Umschalttaste`–`Alt`–`P`

Gibt ein Makro wieder.

`Strg`–`Umschalttaste`–`Alt`–`S`

Öffnet den Layoutdatei-Editor.

Strg–Umschalttaste–Alt–T

Speichert den Miniprogramm-Baum in der Protokolldatei.

Strg–Umschalttaste–Alt–X

Öffnet ein Konsolenfenster (xterm). Nützlich für VNC-Installationen.

Strg–Umschalttaste–Alt–Y

Öffnet den Miniprogramm-Baum-Browser.

5 YaST im Textmodus

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

YaST verwendet im Textmodus die ncurses-Bibliothek, um eine bequeme pseudografische Bedienoberfläche zu bieten. Die ncurses-Bibliothek wird standardmäßig installiert. Die minimale unterstützte Größe des Terminal-Emulators, in dem Sie YaST ausführen, beträgt 80 x 25 Zeichen.

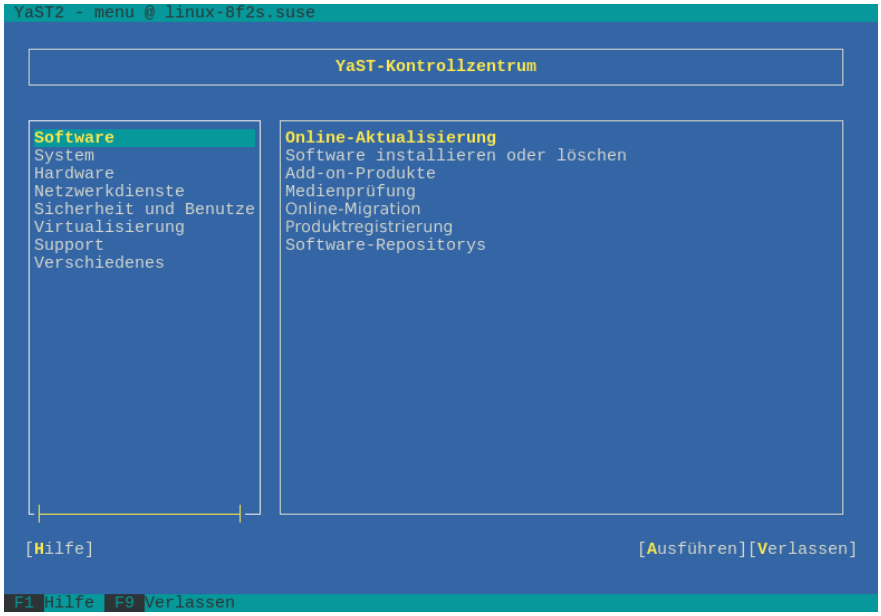


ABBILDUNG 5.1 HAUPTFENSTER VON YAST IM TEXTMODUS

Wenn Sie YaST im Textmodus starten, wird das YaST-Kontrollzentrum angezeigt (siehe *Abbildung 5.1*). Das Hauptfenster besteht aus drei Bereichen. Der linke Bereich zeigt die Kategorien, denen die verschiedenen Module angehören. Dieser Bereich ist beim Start von YaST aktiv und wird daher durch eine breite weiße Umrandung gekennzeichnet. Die aktive Kategorie ist ausgewählt. Der linke Bereich bietet einen Überblick über die Module, die in der aktiven Kategorie zur Verfügung stehen. Der untere Bereich enthält die Schaltflächen für *Hilfe* und *Verlassen*.

Wenn Sie das YaST-Kontrollzentrum starten, wird automatisch die Kategorie *Software* ausgewählt. Mit ↓ und ↑ können Sie die Kategorie ändern. Um ein Modul aus der Kategorie auszuwählen, aktivieren Sie den rechten Bereich mit →, und wählen Sie dann das Modul mithilfe

von ↓ und ↑ aus. Halten Sie die Pfeiltasten gedrückt, um durch die Liste der verfügbaren Module zu blättern. Der ausgewählte Eintrag wird ausgewählt. Drücken Sie Eingabetaste, um das aktive Modul zu starten.

Zahlreiche Schaltflächen oder Auswahlfelder im Modul enthalten einen markierten Buchstaben (standardmäßig gelb) Mit Alt–markierter_Buchstabe können Sie eine Schaltfläche direkt auswählen, müssen also nicht mit →| zur Schaltfläche wechseln. Zum Verlassen des YaST-Kontrollzentrums drücken Sie Alt–Q, oder wählen Sie *Verlassen*, und drücken Sie Eingabetaste.

Tipp: Neuladen von YaST-Dialogfeldern

Wenn ein YaST-Dialogfeld verzerrt oder unleserlich wird (z. B. beim Ändern der Fenstergröße), drücken Sie Strg–L. Damit wird das Fenster aktualisiert, und der Fensterinhalt wird wiederhergestellt.

5.1 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 5.3, „Einschränkung der Tastenkombinationen“* finden Sie Informationen zu möglichen Ausnahmen.

Navigation zwischen Schaltflächen und Auswahllisten

Verwenden Sie →|, um zwischen den Schaltflächen und Einzelbildern mit den Auswahllisten zu navigieren. Zum Navigieren in umgekehrter Reihenfolge verwenden Sie die Tastenkombinationen Alt–→| oder Umschalttaste–→| .

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 Umschalttaste–→ oder Umschalttaste–← horizontal nach rechts bzw. links blättern. Alternativ können Sie Strg–E oder Strg–A verwenden. Diese Kombination kann auch verwendet werden, wenn → oder ← zu einem Wechsel des aktiven Rahmens oder der aktuellen Auswahlliste führt, 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 Leertaste oder Eingabetaste. Alternativ können Optionsschaltflächen und Kontrollkästchen unmittelbar mit Alt–markierter_Buchstabe ausgewählt werden. In diesem Fall brauchen Sie die Auswahl nicht mit Eingabetaste zu bestätigen. Wenn Sie mit →| zu einem Element wechseln, können Sie mit Eingabetaste die ausgewählte Aktion ausführen bzw. das betreffende Menüelement aktivieren.

Funktionstasten

Die Funktionstasten (F1 bis F12) bieten schnellen Zugriff auf die verschiedenen Schaltflächen. In der untersten Zeile im YaST-Bildschirm werden verfügbare Tastenkombinationen (F*x*) angezeigt. Welche Funktionstasten welchen Schaltflächen zugeordnet sind, hängt vom aktiven YaST-Modul ab, da die verschiedenen Module unterschiedliche Schaltflächen aufweisen (*Details*, *Info*, *Hinzufügen*, *Löschen* usw.). F10 wird für *Übernehmen*, *OK*, *Weiter* und *Beenden* verwendet. Drücken Sie F1 , um Zugriff auf die YaST-Hilfe zu erhalten.

Verwenden der Navigationsstruktur im ncurses-Modus

Einige YaST-Module bieten im linken Fensterbereich eine Navigationsstruktur, in der Konfigurationsdialogfenster ausgewählt werden können. Verwenden Sie die Pfeiltasten (↑ und ↓), um in der Baumstruktur zu navigieren. Drücken Sie Leertaste , um Elemente der Struktur zu öffnen oder zu schließen. Im ncurses-Modus muss nach der Auswahl in der Navigationsstruktur die Taste Eingabetaste gedrückt werden, um das ausgewählte Dialogfeld anzuzeigen. Dieses beabsichtigte Verhalten erspart zeitraubende Bildaufbauvorgänge beim Blättern durch die Navigationsstruktur.

Auswählen von Software im Software-Installationsmodul

Mit den Filtern im linken Bereich begrenzen Sie die Anzahl der angezeigten Pakete. Installierte Pakete sind mit dem Buchstaben i gekennzeichnet. Mit der Leertaste oder der Eingabetaste ändern Sie den Status eines Pakets. Alternativ wählen Sie den gewünschten neuen Modus (Installieren, Löschen, Aktualisieren, Tabu oder Sperre) über das Menü *Aktionen*.

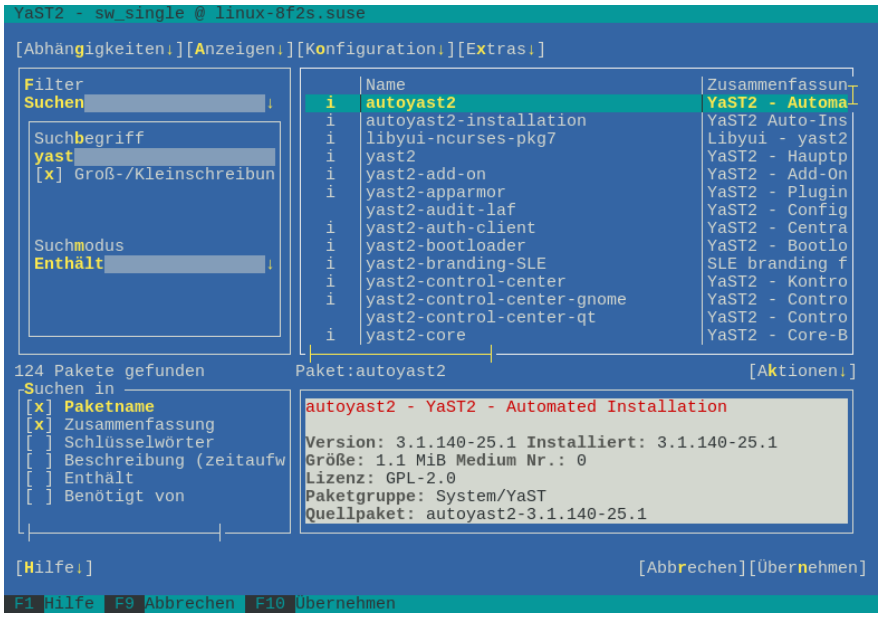


ABBILDUNG 5.2 DAS SOFTWARE-INSTALLATIONSMODUL

5.2 Erweiterte Tastenkombinationen

YaST bietet im Textmodus eine Reihe erweiterter Tastenkombinationen.

`Umschalttaste`–`F1`

Zeigt eine Liste der erweiterten Tastenkombinationen.

`Umschalttaste`–`F4`

Ändert das Farbschema.

`Strg`–`\`

Beendet die Anwendung.

`Strg`–`L`

Aktualisiert den Bildschirm.

`Strg`–`D` `F1`

Zeigt eine Liste der erweiterten Tastenkombinationen.

`Strg`–`D` `Umschalttaste`–`D`

Speichert das Dialogfeld als Bildschirmfoto in der Protokolldatei.

`Strg`–`D` `Umschalttaste`–`Y`

Öffnet YDialogSpy mit der Widget-Hierarchie.

5.3 Einschränkung der Tastenkombinationen

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

Ersetzen der Alt-Taste durch die Esc-Taste

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

Navigation vor und zurück mit Strg–F und Strg–B

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

Einschränkung der Funktionstasten

Die Funktionstasten (F1 bis F12) werden auch für Funktionen herangezogen. 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.

5.4 YaST-Kommandozeilenoptionen

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

```
yast -h
```

5.4.1 Starten der einzelnen Module

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

```
yast <module_name>
```

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

5.4.2 Installation von Paketen über die Kommandozeile

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

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

oder

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

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

Wenn Sie ein kommandozeilenbasiertes Softwareverwaltungs-Dienstprogramm mit Funktionen benötigen, die über die von YaST hinausgehen, sollten Sie möglicherweise Zypper verwenden. Dieses Dienstprogramm verwendet die Softwareverwaltungsbibliothek, die auch die Grundlage des YaST-Paket-Managers bildet. Die grundlegende Verwendung von Zypper wird in *Abschnitt 6.1, „Verwenden von zypper“* erläutert.

5.4.3 Kommandozeilenparameter der YaST-Module

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

```
yast <module_name> help
```

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

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

6 Verwalten von Software mit Kommandozeilen-Tools

Dieses Kapitel behandelt zypper und RPM, zwei Kommandozeilen-Tools zum Verwalten von Software. Eine Definition der in diesem Kontext verwendeten Terminologie (beispielsweise `Repository`, `Patch` oder `Update`) finden Sie unter *Buch „Bereitstellungshandbuch", Kapitel 13 „Installieren bzw. Entfernen von Software", Abschnitt 13.1 „Definition der Begriffe"*.

6.1 Verwenden von zypper

Zypper ist ein Kommandozeilen-Paketmanager für Installation, Aktualisierung und Löschung von Paketen sowie zum Verwalten von Repositorys. Damit können Sie Software per Fernzugriff oder mithilfe von Shell-Skripten verwalten.

6.1.1 Allgemeine Verwendung

Die allgemeine Syntax von Zypper sieht wie folgt aus:

```
zypper [--global-options] COMMAND  [--command-options] [arguments]
```

Die Komponenten in Klammern sind nicht erforderlich. Eine Liste der allgemeinen Optionen und aller Befehle erhalten Sie mit **`zypper help`**. Wenn Sie Hilfe zu einem bestimmten Befehl abrufen möchten, geben Sie **`zypper help`** *BEFEHL* ein.

Zypper-Kommandos

Am einfachsten führen Sie Zypper aus, indem Sie seinen Namen gefolgt von einem Kommando eingeben. Geben Sie z. B. für das Anwenden aller erforderlichen Patches auf das System Folgendes ein:

```
tux > sudo zypper patch
```

Globale Optionen

Zusätzlich können Sie aus einer oder mehreren globalen Optionen wählen, indem Sie sie direkt vor dem Kommando eingeben:

```
tux > sudo zypper --non-interactive patch
```

Im Beispiel oben bedeutet die Option `--non-interactive`, dass das Kommando ausgeführt wird, ohne nach Informationen zu fragen (die Standardantworten werden automatisch angewendet).

Kommandospezifische Optionen

Um die spezifischen Optionen für ein bestimmtes Kommando zu verwenden, geben Sie sie direkt nach dem Kommando ein.

```
tux > sudo zypper patch --auto-agree-with-licenses
```

Im Beispiel oben wird `--auto-agree-with-licenses` verwendet, um alle erforderlichen Patches auf ein System anzuwenden, ohne dass Sie aufgefordert werden, Lizenzen zu bestätigen. Stattdessen wird die Lizenz automatisch akzeptiert.

Argumente

Einige Kommandos erfordern ein oder mehrere Argumente. Wird beispielsweise das Kommando **`install`** verwendet, müssen Sie angeben, welches Paket oder welche Pakete Sie *installieren* möchten:

```
tux > sudo zypper install mplayer
```

Manche Optionen erfordern auch ein einzelnes Argument. Das folgende Kommando listet alle bekannten Muster auf:

```
tux > zypper search -t pattern
```

Sie können alle obigen Optionen kombinieren. Beispielsweise werden durch das folgende Kommando die Pakete `aspell-de` und `aspell-fr` aus dem `factory`-Repository im Verbose-Modus installiert:

```
tux > sudo zypper -v install --from factory aspell-de aspell-fr
```

Mit der Option `--from` bleiben alle Repositorys aktiviert (damit alle Abhängigkeiten aufgelöst werden können), wenn das Paket aus dem angegebenen Repository abrufen wird.

Die meisten Zypper-Kommandos besitzen eine `dry-run`-Option, die eine Simulation des angegebenen Kommandos ausführt. Sie kann für Tests verwendet werden.

```
tux > sudo zypper remove --dry-run MozillaFirefox
```

Zypper unterstützt die globale Option `--userdata ZEICHENKETTE`. Bei dieser Option können Sie eine Zeichenkette angeben, die dann in die Protokolle und Plugins von Zypper geschrieben wird (z. B. in das Btrfs-Plugin). Hiermit können Sie Transaktionen in Protokolldateien kennzeichnen.

```
tux > sudo zypper --userdata STRING patch
```

6.1.2 Installieren und Entfernen von Software mit zypper

Verwenden Sie zur Installation oder Löschung von Paketen die folgenden Kommandos:

```
tux > sudo zypper install PACKAGE_NAME
sudo zypper remove PACKAGE_NAME
```

Warnung: Entfernen Sie keine obligatorischen Systempakete

Entfernen Sie keine obligatorischen Systempakete, wie `glibc`, `zypper`, `kernel`. Werden diese Pakete entfernt, kann das System instabil werden oder aufhören zu funktionieren.

6.1.2.1 Auswählen, welche Pakete zu installieren oder zu entfernen sind

Es gibt verschiedene Methoden, Pakete mit den Kommandos **`zypper install`** und **`zypper remove`** zu adressieren.

Nach dem exakten Paketnamen

```
tux > sudo zypper install MozillaFirefox
```

Nach dem genauen Namen und der Versionsnummer des Pakets

```
tux > sudo zypper install MozillaFirefox-52.2
```

Nach dem Repository-Alias und Paketnamen

```
tux > sudo zypper install mozilla:MozillaFirefox
```

Dabei ist `mozilla` der Alias des Repositorys, aus dem installiert werden soll.

Nach dem Paketnamen mit Platzhaltern

Sie können alle Pakete mit Namen auswählen, die mit einer bestimmten Zeichenfolge anfangen oder enden. Verwenden Sie Platzhalter mit äußerster Umsicht, vor allem beim Entfernen von Paketen. Das folgende Kommando installiert alle Pakete, deren Name mit „Moz“ beginnt:

```
tux > sudo zypper install 'Moz*'
```

Tipp: Entfernen aller `-debuginfo` -Pakete

Beim Debuggen eines Problems müssen Sie unter Umständen zahlreiche `-debuginfo` -Pakete temporär installieren, mit denen Sie weitere Informationen zu den ausgeführten Prozessen erhalten. Nach Abschluss der Debugging-Sitzung bereinigen Sie die Umgebung wie folgt:

```
tux > sudo zypper remove '*-debuginfo'
```

Nach Funktion

Wenn Sie beispielsweise ein Perl-Modul installieren möchten, ohne den Namen des Pakets zu kennen, sind Funktionen praktisch:

```
tux > sudo zypper install firefox
```

Nach Funktion, Hardware-Architektur oder Version

Zusammen mit einer Funktion können Sie eine Hardware-Architektur und eine Version angeben:

- Der Name der gewünschten Hardware-Architektur wird nach einem Punkt an die Funktion angefügt. Um beispielsweise die AMD64-/Intel-64-Architekturen anzugeben (die in Zypper `x86_64` heißen), verwenden Sie Folgendes:

  ```
  tux > sudo zypper install 'firefox.x86_64'
  ```

- Versionen müssen am Ende der Zeile angefügt werden und ein Operator muss vorangestellt sein: `<` (kleiner als), `<=` (kleiner oder gleich), `=` (gleich), `>=` (größer oder gleich), `>` (größer als).

```
tux > sudo zypper install 'firefox>=52.2'
```

- Sie können auch eine Hardware-Architektur und eine Versionsanforderung kombinieren:

```
tux > sudo zypper install 'firefox.x86_64>=52.2'
```

Nach dem Pfad der RPM-Datei

Sie können einen lokalen oder entfernten Pfad zu einem Paket angeben:

```
tux > sudo zypper install /tmp/install/MozillaFirefox.rpm
tux > sudo zypper install http://download.example.com/MozillaFirefox.rpm
```

6.1.2.2 Kombinieren der Installation und der Entfernung von Paketen

Zum gleichzeitigen Installieren und Entfernen von Paketen verwenden Sie die Modifikatoren `+/-`. Um `emacs` zu installieren und gleichzeitig `vim` zu entfernen, verwenden Sie Folgendes:

```
tux > sudo zypper install emacs -vim
```

Um `emacs` zu entfernen und gleichzeitig `vim` zu installieren, verwenden Sie Folgendes:

```
tux > sudo zypper remove emacs +vim
```

Um zu vermeiden, dass der mit `-` beginnende Paketname als Kommandooption interpretiert wird, verwenden Sie ihn stets als das zweite Argument. Falls dies nicht möglich ist, stellen Sie ihm `--` voran:

```
tux > sudo zypper install -emacs +vim       # Wrong
tux > sudo zypper install vim -emacs        # Correct
tux > sudo zypper install -- -emacs +vim    # Correct
tux > sudo zypper remove emacs +vim         # Correct
```

6.1.2.3 Bereinigen von Abhängigkeiten entfernter Pakete

Wenn (zusammen mit einem bestimmten Paket) automatisch alle Pakete entfernt werden sollen, die nach dem Entfernen dieses Pakets nicht mehr erforderlich sind, verwenden Sie die Option `--clean-deps`:

```
tux > sudo zypper rm PACKAGE_NAME --clean-deps
```

6.1.2.4 Verwenden von Zypper in Skripten

Standardmäßig verlangt Zypper eine Bestätigung, bevor ein ausgewähltes Paket installiert oder entfernt wird oder wenn ein Problem auftritt. Mit der Option `--non-interactive` können Sie dieses Verhalten deaktivieren. Die Option muss jedoch vor dem tatsächlich auszuführenden Kommando (**`install`**, **`remove`** oder **`patch`**) angegeben werden, wie im Folgenden erkennbar:

```
tux > sudo zypper --non-interactive install PACKAGE_NAME
```

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

6.1.2.5 Installieren und Herunterladen von Quellpaketen

Wenn Sie das entsprechende Quellpaket eines Pakets installieren möchten, verwenden Sie:

```
tux > zypper source-install PACKAGE_NAME
```

Wird das Kommando als `root` ausgeführt, ist der Standardspeicherort der Quellpakete `/usr/src/packages/` und `~/rpmbuild`, wenn es als Benutzer ausgeführt wird. Diese Werte können in Ihrer lokalen **`rpm`**-Konfiguration geändert werden.

Dieses Kommando installiert auch die Build-Abhängigkeiten des angegebenen Pakets. Wenn Sie dies nicht wünschen, fügen Sie den Schalter `-D` hinzu:

```
tux > sudo zypper source-install -D PACKAGE_NAME
```

Um nur die Build-Abhängigkeiten zu installieren, verwenden Sie `-d`.

```
tux > sudo zypper source-install -d PACKAGE_NAME
```

Natürlich gelingt dies nur, wenn das Repository mit den Quellpaketen in Ihrer Repository-Liste aktiviert ist (es wird standardmäßig hinzugefügt, aber nicht aktiviert). Details zur Repository-Verwaltung finden Sie unter *Abschnitt 6.1.5, „Verwalten von Repositorys mit Zypper“*.

Eine Liste aller Quellpakete, die in Ihren Repositorys verfügbar sind, können Sie wie folgt abrufen:

```
tux > zypper search -t srcpackage
```

Wenn Sie möchten, können Sie die Quellpakete für alle installierten Pakete in ein lokales Verzeichnis herunterladen. Zum Herunterladen von Quellpaketen verwenden Sie:

```
tux > zypper source-download
```

Das Standardverzeichnis für heruntergeladene Dateien lautet `/var/cache/zypper/source-download`. Mit der Option `--directory` können Sie dieses Verzeichnis ändern. Sollen nur fehlende oder überzählige Pakete angezeigt werden, ohne Pakete herunterzuladen oder zu löschen, verwenden Sie die Option `--status`. Zum Löschen überzähliger Pakete verwenden Sie die Option `--delete`. Soll das Löschen deaktiviert werden, verwenden Sie die Option `--no-delete`.

6.1.2.6 Installieren von Paketen aus deaktivierten Repositorys

In der Regel können Sie nur Pakete aus aktivierten Repositorys installieren oder aktualisieren. Mit der Option `--plus-content` *`TAG`* können Sie bestimmte Repositorys aktualisieren, temporär während der aktuellen Zypper-Sitzung aktivieren und nach Abschluss der Sitzung wieder deaktivieren.

Sollen beispielsweise Repositorys mit zusätzlichen `-debuginfo`- oder `-debugsource`-Paketen aktiviert werden, geben Sie `--plus-content debug` ein. Diese Option kann mehrfach angegeben werden.

Sollen diese „Debug“-Repositorys vorübergehend aktiviert werden, damit Sie ein bestimmtes `--debuginfo`-Paket installieren können, geben Sie die Option wie folgt an:

```
tux > sudo zypper --plus-content debug \
   install "debuginfo(build-id)=eb844a5c20c70a59fc693cd1061f851fb7d046f4"
```

Die Zeichenkette `build-id` wird von **`gdb`** für fehlende debuginfo-Pakete zurückgegeben.

6.1.2.7 Dienstprogramme

Wenn Sie prüfen möchten, ob alle Abhängigkeiten noch erfüllt sind, und fehlende Abhängigkeiten reparieren möchten, verwenden Sie:

```
tux > zypper verify
```

Zusätzlich zu Abhängigkeiten, die erfüllt sein müssen, „empfehlen“ einige Pakete andere Pakete. Diese empfohlenen Pakete werden installiert, wenn sie aktuell verfügbar und installierbar sind. Falls empfohlene Pakete erst nach der Installation des empfehlenden Pakets (durch Hinzufügen zusätzlicher Pakete oder zusätzlicher Hardware) zur Verfügung steht, verwenden Sie das folgende Kommando:

```
tux > sudo zypper install-new-recommends
```

Dieses Kommando ist nach dem Anschließen einer Webcam oder eines WLAN-Geräts äußerst nützlich. Hiermit werden Treiber für das Gerät und die zugehörige Software installiert, sofern verfügbar. Die Treiber und die zugehörige Software sind nur dann installierbar, wenn bestimmte Hardware-Abhängigkeiten erfüllt sind.

6.1.3 Aktualisieren von Software mit zypper

Es gibt drei verschiedene Möglichkeiten, Software mithilfe von Zypper zu installieren: durch Installation von Patches, durch Installation einer neuen Version eines Pakets oder durch Aktualisieren der kompletten Distribution. Letzteres wird mit **`zypper dist-upgrade`** erreicht. Durchführen von Upgrades von SUSE Linux Enterprise Server wird im *Buch „Bereitstellungshandbuch“, Kapitel 19 „Aufrüsten von SUSE Linux Enterprise“* erläutert.

6.1.3.1 Installieren aller erforderlichen Patches

Um alle offiziell herausgegebenen Patches für Ihr System zu installieren, führen Sie Folgendes aus:

```
tux > sudo zypper patch
```

Alle verfügbaren Patches aus den auf Ihrem Computer konfigurierten Repositorys werden auf Relevanz für Ihre Installation überprüft. Sind sie relevant (und nicht als `optional` oder `feature` klassifiziert), werden sie sofort installiert. Beachten Sie, dass das offizielle Aktualisierungs-Repository erst verfügbar ist, nachdem Sie Ihre SUSE Linux Enterprise Server-Installation registriert haben.

Umfasst ein zu installierendes Patch Änderungen, die einen System-Reboot erfordern, werden Sie zuvor benachrichtigt.

Mit dem einfachen Befehl **`zypper patch`** werden keine Patches aus Drittanbieter-Repositorys angewendet. Sollen auch die Drittanbieter-Repositorys aktualisiert werden, geben Sie die Befehlsoption `with-update` wie folgt an:

```
tux > sudo zypper patch --with update
```

Um auch optionale Patches zu installieren, verwenden Sie Folgendes:

```
tux > sudo zypper patch --with-optional
```

Um alle Patches zu installieren, die zu einem bestimmten Bugzilla-Problem gehören, verwenden Sie Folgendes:

```
tux > sudo zypper patch --bugzilla=NUMBER
```

Um alle Patches zu installieren, die zu einem bestimmten CVE-Datenbankeintrag gehören, verwenden Sie Folgendes:

```
tux > sudo zypper patch --cve=NUMBER
```

Zum Installieren eines Sicherheits-Patches mit der CVE-Nummer `CVE-2010-2713` führen Sie beispielsweise Folgendes aus:

```
tux > sudo zypper patch --cve=CVE-2010-2713
```

Um nur Patches zu installieren, die Auswirkungen auf Zypper und die Paketverwaltung an sich haben, verwenden Sie Folgendes:

```
tux > sudo zypper patch --updatestack-only
```

Denken Sie daran, dass andere Befehlsoptionen, mit denen auch andere Repositorys aktualisiert würden, außer Acht gelassen werden, wenn Sie die Befehlsoption `updatestack-only` angeben.

6.1.3.2 Auflisten von Patches

Um herauszufinden, ob Patches verfügbar sind, erlaubt Zypper das Anzeigen der folgenden Informationen:

Anzahl der erforderlichen Patches

Um die Anzahl der erforderlichen Patches aufzulisten (Patches, die für Ihr System gelten, aber noch nicht installiert sind), verwenden Sie **`patch-check`**:

```
tux > zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

Dieses Kommando kann mit der Option `--updatestack-only` kombiniert werden, um nur Patches aufzulisten, die Auswirkungen auf Zypper und die Paketverwaltung an sich haben.

Liste der erforderlichen Patches

Um alle erforderlichen Patches aufzulisten (Patches, die für Ihr System gelten, aber noch nicht installiert sind), verwenden Sie **`list-patches`**:

```
tux > zypper list-patches
Loading repository data...
Reading installed packages...

Repository     | Name        | Version | Category | Status  | Summary
---------------+-------------+---------+----------+---------+---------
SLES12-Updates | SUSE-2014-8 | 1       | security | needed  | openssl: Update for OpenSSL
```

Liste aller Patches

Um alle für SUSE Linux Enterprise Server verfügbaren Patches aufzulisten, unabhängig davon, ob sie bereits installiert sind oder für Ihre Installation gelten, verwenden Sie **`zypper patches`**.

Sie können auch Patches für bestimmte Probleme auflisten und installieren. Dazu geben Sie das Kommando **`zypper list-patches`** mit den folgenden Optionen ein:

Nach Bugzilla-Problemen

Um alle Patches mit Bezug zu Bugzilla-Problemen aufzulisten, verwenden Sie die Option `--bugzilla`.

Um Patches für einen bestimmten Fehler aufzulisten, können Sie auch eine Fehlernummer angeben: `--bugzilla=NUMMER`. Fügen Sie Kommas zwischen den Fehlernummern hinzu, um nach Patches mit Bezug zu mehreren Bugzilla-Problemen zu suchen, z. B.:

```
tux > zypper list-patches --bugzilla=972197,956917
```

Nach CVE-Nummer

Um alle erforderlichen Patches aufzulisten, die Bezug zu einem Eintrag in der CVE-Datenbank (Common Vulnerabilities and Exposures) haben, verwenden Sie die Option `--cve`. Um Patches für einen bestimmten CVE-Datenbankeintrag aufzulisten, können Sie auch eine CVE-Nummer angeben: `--cve=NUMMER`. Fügen Sie Kommas zwischen den CVE-Nummern hinzu, um nach Patches mit Bezug zu mehreren CVE-Datenbankeinträgen zu suchen, z. B.:

```
tux > zypper list-patches --bugzilla=CVE-2016-2315,CVE-2016-2324
```

Um alle Patches aufzulisten, unabhängig davon, ob sie erforderlich sind, verwenden Sie zusätzlich die Option `--all`. Um beispielsweise alle Patches aufzulisten, denen eine CVE-Nummer zugewiesen ist, verwenden Sie Folgendes:

```
tux > zypper list-patches --all --cve
Issue | No.           | Patch              | Category    | Severity  | Status
------+---------------+--------------------+-------------+-----------+----------
cve   | CVE-2015-0287 | SUSE-SLE-Module.. | recommended | moderate  | needed
cve   | CVE-2014-3566 | SUSE-SLE-SERVER.. | recommended | moderate  | not needed
[...]
```

6.1.3.3 Installieren neuer Paketversionen

Wenn ein Repository neue Pakete enthält, aber keine Patches zur Verfügung stellt, zeigt **`zypper patch`** keinerlei Wirkung. Zum Aktualisieren aller installierten Pakete mit verfügbaren neuen Versionen (unter Beibehaltung der Systemintegrität) verwenden Sie Folgendes:

```
tux > sudo zypper update
```

Zum Aktualisieren einzelner Pakete geben Sie das Paket mit dem Aktualisierungs- oder Aktualisierungskommando an:

```
tux > sudo zypper update PACKAGE_NAME
sudo zypper install PACKAGE_NAME
```

Mit dem Kommando kann eine Liste mit allen neuen installierbaren Paketen abgerufen werden.

```
tux > zypper list-updates
```

Dieses Kommando listet ausschließlich Pakete auf, die die folgenden Kriterien erfüllen:

- stammt von demselben Hersteller wie das bereits installierte Paket,
- umfasst Repositorys mit mindestens derselben Priorität wie das bereits installierte Paket,
- ist installierbar (alle Abhängigkeiten wurden erfüllt).

Eine Liste *aller* neuen verfügbaren Pakete (unabhängig davon, ob diese Pakete installierbar sind oder nicht) erhalten Sie mit Folgendem:

```
tux > sudo zypper list-updates --all
```

Um festzustellen, warum ein neues Paket nicht installiert werden kann, verwenden Sie das Kommando **`zypper install`** oder **`zypper update`**, wie oben beschrieben.

6.1.3.4 Ermitteln verwaister Pakete

Immer, wenn Sie ein Repository aus Zypper entfernen oder Ihr System aktualisieren, erhalten manche Pakete den Status „Verwaist“. Diese *verwaisten* Pakete gehören zu keinem aktiven Repository mehr. Mit dem folgenden Kommando erhalten Sie eine entsprechende Liste:

```
tux > sudo zypper packages --orphaned
```

Anhand dieser Liste können Sie entscheiden, ob ein Paket noch benötigt wird oder sicher entfernt werden kann.

6.1.4 Ermitteln von Prozessen und Diensten, die gelöschte Dateien verwenden

Beim Anwenden von Patches, beim Aktualisieren oder beim Entfernen von Paketen können auf dem System Prozesse aktiv sein, die weiterhin Dateien verwenden, die durch die Aktualisierung oder das Entfernen gelöscht wurden. Verwenden Sie **`zypper ps`**, um Prozesse aufzulisten, die gelöschte Dateien verwenden. Falls der Prozess zu einem bekannten Dienst gehört, wird der Dienstname aufgelistet und der Dienst kann leicht neu gestartet werden. Standardmäßig zeigt **`zypper ps`** eine Tabelle an:

```
tux > zypper ps
```

```
PID   | PPID | UID | User  | Command      | Service      | Files
------+------+-----+-------+--------------+--------------+------------------
814   | 1    | 481 | avahi | avahi-daemon | avahi-daemon | /lib64/ld-2.19.s->
      |      |     |       |              |              | /lib64/libdl-2.1->
      |      |     |       |              |              | /lib64/libpthrea->
      |      |     |       |              |              | /lib64/libc-2.19->
[...]
```

PID: ID des Prozesses

PPID: ID des übergeordneten Prozesses

UID: ID des Benutzers, der den Prozess ausführt

Login: Anmeldename des Benutzers, der den Prozess ausführt

Command: Kommando, das zum Ausführen des Prozesses verwendet wird

Service: Dienstname (nur, wenn das Kommando einem Systemdienst zugewiesen ist)

Files: Liste der gelöschten Dateien

Das Ausgabeformat von **zypper ps** kann wie folgt gesteuert werden:

zypper ps -s

Kurze Tabelle ohne gelöschte Dateien erstellen.

```
tux > zypper ps -s
PID   | PPID | UID  | User    | Command      | Service
------+------+------+---------+--------------+--------------
814   | 1    | 481  | avahi   | avahi-daemon | avahi-daemon
817   | 1    | 0    | root    | irqbalance   | irqbalance
1567  | 1    | 0    | root    | sshd         | sshd
1761  | 1    | 0    | root    | master       | postfix
1764  | 1761 | 51   | postfix | pickup       | postfix
1765  | 1761 | 51   | postfix | qmgr         | postfix
2031  | 2027 | 1000 | tux     | bash         |
```

zypper ps -ss

Nur Prozesse anzeigen, die einem Systemdienst zugewiesen sind.

```
PID   | PPID | UID  | User    | Command      | Service
------+------+------+---------+--------------+--------------
814   | 1    | 481  | avahi   | avahi-daemon | avahi-daemon
817   | 1    | 0    | root    | irqbalance   | irqbalance
1567  | 1    | 0    | root    | sshd         | sshd
1761  | 1    | 0    | root    | master       | postfix
1764  | 1761 | 51   | postfix | pickup       | postfix
1765  | 1761 | 51   | postfix | qmgr         | postfix
```

zypper ps -sss

Nur Systemdienste anzeigen, die gelöschte Dateien verwenden.

```
avahi-daemon
irqbalance
postfix
sshd
```

zypper ps --print "systemctl status %s"

Kommandos zum Abrufen von Statusinformationen für Dienste anzeigen, die einen Neustart erfordern könnten.

```
systemctl status avahi-daemon
systemctl status irqbalance
systemctl status postfix
systemctl status sshd
```

Weitere Informationen zum Handhaben von Diensten finden Sie unter *Kapitel 13, Der Daemon* `systemd`.

6.1.5 Verwalten von Repositorys mit Zypper

Sämtliche Installations- und Patch-Kommandos von Zypper sind von der Liste der bekannten Repositorys abhängig. Um alle dem System bekannten Repositorys aufzulisten, verwenden Sie das Kommando:

```
tux > zypper repos
```

Das Ergebnis ist der folgenden Ausgabe ähnlich:

BEISPIEL 6.1 ZYPPER – LISTE DER BEKANNTEN REPOSITORYS

```
tux > zypper repos
# | Alias        | Name          | Enabled | Refresh
--+--------------+---------------+---------+--------
1 | SLEHA-12-GEO | SLEHA-12-GEO  | Yes     | No
2 | SLEHA-12     | SLEHA-12      | Yes     | No
3 | SLES12       | SLES12        | Yes     | No
```

Bei der Angabe von Repositorys kann in verschiedenen Kommandos ein Alias, URI oder eine Repository-Nummber aus der Ausgabe des Kommandos **zypper repos** verwendet werden. Ein Repository-Alias ist eine Kurzform des Repository-Namens, der in Repository-Kommandos verwendet wird. Beachten Sie dabei, dass sich die Repository-Nummern nach dem Bearbeiten der Repository-Liste ändern können. Der Alias ändert sich nie von alleine.

Standardmäßig werden Details wie URI oder Priorität des Repositorys nicht angezeigt. Verwenden Sie das folgende Kommando, um alle Details aufzulisten:

```
tux > zypper repos -d
```

6.1.5.1 Hinzufügen von Repositorys

Zum Hinzufügen eines Repository, führen Sie Folgendes aus:

```
tux > sudo zypper addrepo URI ALIAS
```

URI kann ein Internet-Repository, eine Netzwerkressource, ein Verzeichnis oder eine CD oder DVD sein (für Details siehe http://en.opensuse.org/openSUSE:Libzypp_URIs). Der *ALIAS* ist ein Kürzel und eine eindeutige Kennung für das Repository. Sie können ihn frei wählen, vorausgesetzt, er ist eindeutig. Zypper gibt eine Warnung aus, wenn Sie einen Alias angeben, der bereits verwendet wird.

6.1.5.2 Aktualisieren von Repositorys

Mit **zypper** können Sie Änderungen in Paketen aus konfigurierten Repositorys abrufen. Rufen Sie die Änderungen wie folgt ab:

```
tux > sudo zypper refresh
```

Anmerkung: Standardverhalten von zypper

Standardmäßig führen bestimmte Befehle **refresh** automatisch aus, sodass dieser Befehl nicht explizit aufgerufen werden muss.

Mit der Option `--plus-content` für **refresh** können Sie Änderungen auch in deaktivierten Repositorys abrufen:

```
tux > sudo zypper --plus-content refresh
```

Diese Option ruft Änderungen in Repositorys ab und behält dabei den Zustand der deaktivierten Repositorys unverändert bei – also deaktiviert.

6.1.5.3 Entfernen von Repositorys

Wenn ein Repository von der Liste entfernt werden soll, verwenden Sie das Kommando **`zypper removerepo`** zusammen mit dem Alias oder der Nummer des zu löschenden Repositorys. Um beispielsweise das Repository `SLEHA-12-GEO` aus *Beispiel 6.1, „Zypper – Liste der bekannten Repositorys“* zu entfernen, verwenden Sie eines der folgenden Kommandos:

```
tux > sudo zypper removerepo 1
tux > sudo zypper removerepo "SLEHA-12-GEO"
```

6.1.5.4 Ändern von Repositorys

Aktivieren oder deaktivieren von Repositorys mit **`zypper modifyrepo`**. Mit diesem Kommando können Sie auch die Eigenschaften des Repositorys (z. B. Aktualisierungsverhalten, Name oder Priorität) ändern. Das folgende Kommando aktiviert das Repository mit dem Namen `updates`, aktiviert die automatische Aktualisierung und stellt seine Priorität auf 20 ein:

```
tux > sudo zypper modifyrepo -er -p 20 'updates'
```

Das Ändern von Repositorys ist nicht auf ein einziges Repository beschränkt – Sie können auch Gruppen bearbeiten:

`-a`: alle Repositorys
`-l`: lokale Repositorys
`-t`: entfernte Repositorys
`-m` *`TYPE`*: Repositorys eines bestimmten Typs (wobei *`TYPE`* eines der folgenden sein kann: `http`, `https`, `ftp`, `cd`, `dvd`, `dir`, `file`, `cifs`, `smb`, `nfs`, `hd`, `iso`)

Zum Umbenennen eines Repository-Alias verwenden Sie das Kommando `renamerepo`. Das folgende Beispiel ändert den Alias von `Mozilla Firefox` in `firefox`:

```
tux > sudo zypper renamerepo 'Mozilla Firefox' firefox
```

6.1.6 Abfragen von Repositorys und Paketen mit Zypper

Zypper bietet zahlreiche Methoden zur Abfrage von Repositorys oder Paketen. Verwenden Sie die folgenden Kommandos, um eine Liste aller verfügbaren Produkte, Muster, Pakete oder Patches zu erhalten:

```
tux > zypper products
```

```
tux > zypper patterns
tux > zypper packages
tux > zypper patches
```

Zur Abfrage aller Repositorys auf bestimmte Pakete verwenden Sie `search`. Mit dem Befehl `info` erhalten Sie Informationen zu bestimmten Paketen.

6.1.6.1 Verwendung von `zypper search`

Der Befehl **`zypper search`** lässt sich auf Paketnamen oder optional auf Paketzusammenfassungen und -beschreibungen anwenden. Zeichenketten, die mit `/` umschlossen sind, werden als reguläre Ausdrücke behandelt. Standardmäßig unterscheidet der Suchvorgang keine Groß- und Kleinschreibung.

Einfache Suche nach einem Paketnamen mit dem Namensbestandteil `fire`

```
tux > zypper search "fire"
```

Einfache Suche nach dem genauen Paketnamen `MozillaFirefox`

```
tux > zypper search --match-exact "MozillaFirefox"
```

Suche auf Paketbeschreibungen und -zusammenfassungen ausdehnen

```
tux > zypper search -d fire
```

Nur Pakete anzeigen, die nicht bereits installiert sind

```
tux > zypper search -u fire
```

Pakete anzeigen, die die Zeichenkette `fir` enthalten, nicht gefolgt von `e`

```
tux > zypper se "/fir[^e]/"
```

6.1.6.2 Verwendung von `zypper what-provides`

Verwenden Sie zur Suche nach Paketen, die eine spezielle Funktion bieten, das Kommando `what-provides`. Wenn Sie beispielsweise wissen möchten, welches Paket das Perl-Modul `SVN::Core` bereitstellt, verwenden Sie das folgende Kommando:

```
tux > zypper what-provides 'perl(SVN::Core)'
```

`what-provides -PAKETNAME` ähnelt dem Befehl **`rpm -q --whatprovides`** *`PAKETNAME`*; RPM kann jedoch nur Abfragen für die RPM-Datenbank (Datenbank mit allen installierten Paketen) durchführen. zypper informiert Sie auf der anderen Seite über Anbieter der Möglichkeit von einem beliebigen Repository, nicht nur von denen, die installiert sind.

6.1.6.3 Verwendung von **`zypper info`**

Um einzelne Pakete abzufragen, verwenden Sie **`info`** mit einem exakten Paketnamen als Argument. Hiermit werden detaillierte Informationen zu einem Paket angezeigt. Falls der Paketname nicht mit einem Paketnamen aus den Repositorys übereinstimmt, gibt der Befehl ausführliche Informationen zu den fehlenden Pakettreffern aus. Wenn Sie einen bestimmten Typ festlegen (mit der Option `-t`) und dieser Typ nicht vorhanden ist, gibt der Befehl andere verfügbare Treffer aus, jedoch ohne ausführliche Informationen.

Wenn Sie ein Quellpaket angeben, zeigt der Befehl die aus dem Quellpaket aufgebauten Binärpakete. Wenn Sie ein Binärpaket angeben, gibt der Befehl die Quellpakete aus, aus denen das Binärpaket aufgebaut wurde.

Um auch die Elemente abzurufen, die für das Paket erforderlich/empfohlen sind, verwenden Sie die Optionen `--requires` und `--recommends`:

```
tux > zypper info --requires MozillaFirefox
```

6.1.7 Konfigurieren von Zypper

Zypper ist nunmehr mit einer Konfigurationsdatei ausgestattet, in der Sie die Arbeitsweise von Zypper dauerhaft verändern können (wahlweise systemweit oder benutzerspezifisch). Für systemweite Änderungen bearbeiten Sie `/etc/zypp/zypper.conf`. Für benutzerspezifische Änderungen bearbeiten Sie `~/.zypper.conf`. Falls `~/.zypper.conf` noch nicht vorhanden ist, können Sie `/etc/zypp/zypper.conf` als Schablone verwenden. Kopieren Sie diese Datei in `~/.zypper.conf`, und passen Sie sie nach Ihren Anforderungen an. Weitere Informationen zu den verfügbaren Optionen finden Sie in den Kommentaren in der Datei.

6.1.8 Fehlersuche

Falls Sie aus konfigurierten Repositorys heraus nicht problemlos auf Pakete zugreifen können (Zypper kann beispielsweise ein bestimmtes Paket nicht finden, obwohl Sie wissen, dass sich dieses Paket in einem der Repositorys befindet), aktualisieren Sie probeweise die Repositorys:

```
tux > sudo zypper refresh
```

Falls das nicht wirkt, probieren Sie Folgendes:

```
tux > sudo zypper refresh -fdb
```

Damit wird eine vollständige Aktualisierung und ein kompletter Neuaufbau der Datenbank erzwungen, außerdem ein erzwungener Download von Roh-Metadaten.

6.1.9 Zypper-Rollback-Funktion im Btrfs-Dateisystem

Wenn das Btrfs-Dateisystem in der Stammpartition verwendet wird und `_` installiert ist, ruft Zypper automatisch **`Snapper`** auf, wenn an das Dateisystem Änderungen übermittelt werden, um entsprechende Dateisystem-Snapshots zu erstellen. Diese Snapshots können verwendet werden, um alle durch Zypper vorgenommenen Änderungen rückgängig zu machen. Weitere Informationen finden Sie in *Kapitel 7, Systemwiederherstellung und Snapshot-Verwaltung mit Snapper*.

6.1.10 Weiterführende Informationen

Wenn Sie weitere Informationen zur Verwaltung von Software benötigen, geben Sie den Befehl **`zypper help`**, **`zypper help`** *BEFEHL* in die Befehlszeile ein oder rufen Sie die man-Seite **`zypper(8)`** auf. Eine ausführliche Kommandoreferenz mit `Tricks` zu den wichtigsten Kommandos sowie Informationen zur Verwendung von Zypper in Skripten und Anwendungen finden Sie unter http://en.opensuse.org/SDB:Zypper_usage. Eine Liste der Software-Änderungen in der aktuellen SUSE Linux Enterprise Server-Version finden Sie unter http://en.opensuse.org/openSUSE:Zypper versions.

6.2 RPM - der Paket-Manager

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

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

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

Tipp: Pakete zur Software-Entwicklung

Für mehrere Pakete wurden die erforderlichen Komponenten für die Software-Entwicklung (Bibliotheken, Header, Include-Dateien usw.) in separate Pakete verpackt. Diese Entwicklungspakete werden nur benötigt, wenn Sie Software selbst kompilieren möchten (beispielsweise die neuesten GNOME-Pakete). Solche Pakete sind am Namenszusatz `-` zu erkennen, z. B. die Pakete `alsa-devel` und `gimp-devel`.

6.2.1 Prüfen der Authentizität eines Pakets

RPM-Pakete sind mit GPG signiert. Verwenden Sie zum Verifizieren der Signatur eines RPM-Pakets das Kommando **`rpm --checksig`** *PACKAGE*-1.2.3.rpm. So können Sie feststellen, ob das Paket von SUSE oder einer anderen verbürgten Einrichtung stammt. Dies ist insbesondere bei Update-Paketen aus dem Internet zu empfehlen.

Zum Beheben von Problemen im Betriebssystem müssen Sie ggf. einen PTF (Problem Temporary Fix, temporäre Fehlerbehebung) in einem Produktionssystem installieren. Die Pakete von SUSE sind mit einem besonderen PTF-Schlüssel signiert. Im Gegensatz zu SUSE Linux Enterprise 11 wird dieser Schlüssel jedoch nicht standardmäßig von SUSE Linux Enterprise 12-Systemen importiert. Importieren Sie den Schlüssel mit dem folgenden Befehl:

```
tux > sudo rpm --import \
/usr/share/doc/packages/suse-build-key/suse_ptf_key.asc
```

Nach dem Importieren des Schlüssels können Sie PTF-Pakete auf dem System installieren.

6.2.2 Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren

In der Regel kann ein RPM-Archiv einfach installiert werden: **`rpm -i`** *PACKAGE*.rpm. Mit diesem Kommando 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.
- Wenn der Systemadministrator eine Konfigurationsdatei vor der Aktualisierung geändert hatte, speichert **`rpm`** die geänderte Datei mit der Dateinamenerweiterung `.rpmorig` oder `.rpmsave` (Sicherungsdatei) und installiert die Version des neuen Pakets. Dies gilt nur

dann, wenn die ursprünglich installierte Datei und die neuere Version nicht identisch sind. 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 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/rpm-configcheck` 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.

Zum Entfernen eines Pakets geben Sie **`rpm -e`** *`PAKET`* ein. Dieses Kommando löscht das Paket nur, wenn keine ungelösten 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 (selbst wenn *keine* Abhängigkeiten mehr bestehen), kann es nützlich sein, die RPM-Datenbank mit der Option `--rebuilddb` neu aufzubauen.

6.2.3 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 ein ganz neues 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 **makedeltarpm** und **applydelta** 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:

```
tux > sudo makedeltarpm old.rpm new.rpm new.delta.rpm
```

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

```
tux > sudo applydeltarpm new.delta.rpm new.rpm
```

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

```
tux > sudo applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

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

6.2.4 RPM Abfragen

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

TABELLE 6.1 DIE WICHTIGSTEN RPM-ABFRAGEOPTIONEN

`-i`	Paketinformation
`-l`	Dateiliste
`-f FILE`	Abfrage nach Paket, das die Datei *`FILE`* enthält. (*`FILE`* muss mit dem vollständigen Pfad angegeben werden.)
`-s`	Dateiliste mit Statusinformation (impliziert `-l`)

`-d`	Nur Dokumentationsdateien auflisten (impliziert `-l`)
`-c`	Nur Konfigurationsdateien auflisten (impliziert `-l`)
`--dump`	Dateiliste mit vollständigen Details (mit `-l`, `-c` oder `-d` benutzen)
`--provides`	Funktionen des Pakets auflisten, die ein anderes Paket mit `--requires` anfordern kann
`--requires`, `-R`	Fähigkeiten, die das Paket benötigt
`--Skripten`	Installationsskripten (preinstall, postinstall, uninstall)

Beispielsweise gibt der Befehl **`rpm -q -i wget`** die in *Beispiel 6.2, „`rpm -q -i wget`“* gezeigte Information aus.

BEISPIEL 6.2 `rpm -q -i wget`

```
Name        : wget
Version     : 1.14
Release     : 17.1
Architecture: x86_64
Install Date: Mon 30 Jan 2017 14:01:29 CET
Group       : Productivity/Networking/Web/Utilities
Size        : 2046483
License     : GPL-3.0+
Signature   : RSA/SHA256, Thu 08 Dec 2016 07:48:44 CET, Key ID 70af9e8139db7c82
Source RPM  : wget-1.14-17.1.src.rpm
Build Date  : Thu 08 Dec 2016 07:48:34 CET
Build Host  : sheep09
Relocations : (not relocatable)
Packager    : https://www.suse.com/
Vendor      : SUSE LLC <https://www.suse.com/>
URL         : http://www.gnu.org/software/wget/
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.
Distribution: SUSE Linux Enterprise 12
```

Die Option `-f` funktioniert nur, wenn Sie den kompletten Dateinamen mit dem vollständigen Pfad angeben. Sie können beliebig viele Dateinamen angeben. Beispiel:

```
tux > rpm -q -f /bin/rpm /usr/bin/wget
rpm-4.11.2-15.1.x86_64
wget-1.14-17.1.x86_64
```

Wenn nur ein Teil des Dateinamens bekannt ist, verwenden Sie ein Shell-Skript, wie in *Beispiel 6.3, „Skript für die Suche nach Paketen“* gezeigt. Übergeben Sie den partiellen Dateinamen als Parameter beim Aufruf des Skripts.

BEISPIEL 6.3 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`** *PAKET* zeigt eine detaillierte Liste der Änderungsinformation zu einem bestimmten Paket nach Datum sortiert.

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

TABELLE 6.2 RPM-ÜBERPRÜFUNGSOPTIONEN

`5`	MD5-Prüfsumme
`S`	Dateigröße
`L`	Symbolischer Link
`T`	Änderungszeit
`D`	Major- und Minor-Gerätenummern
`U`	Eigentümer
`G`	Gruppe
`M`	Modus (Berechtigungen und Dateityp)

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

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

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

6.2.5 Installieren und Kompilieren von Quellpaketen

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

Anmerkung: Installierte Quellpakete

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/rpmrc`, 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: Systemintegrität

Experimentieren Sie nicht mit Systemkomponenten (`glibc`, `rpm` usw.), da Sie damit die Stabilität Ihres Systems riskieren.

Das folgende Beispiel verwendet das `wget.src.rpm`-Paket. Nach der Installation des Quellpakets sollten Dateien wie in der folgenden Liste vorhanden sein:

```
/usr/src/packages/SOURCES/wget-1.11.4.tar.bz2
/usr/src/packages/SOURCES/wgetrc.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.

Denken Sie daran, dass die `BuildRoot`-Direktive in der spec-Datei seit SUSE Linux Enterprise Server 12 nicht mehr verwendet wird. Benötigen Sie die Funktion weiterhin, verwenden Sie die Option `--buildroot` als Alternative.Weitere Hintergrundinformationen finden Sie in der Support-Datenbank unter https://www.suse.com/support/kb/doc?id=7017104.

6.2.6 Kompilieren von RPM-Pakten 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 das Kommando **`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 Kommandos:

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

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

Das Skript **build** bietet mehrere zusätzliche Optionen. Beispielsweise können Sie das Skript veranlassen, Ihre eigenen RPMs bevorzugt zu verwenden, die Initialisierung der build-Umgebung auszulassen oder das Kommando **rpm** auf eine der oben erwähnten Stufen zu beschränken. Weitere Informationen erhalten Sie über **build** `--help` oder die man-Seite **build**.

6.2.7 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 Cursortasten und der Eingabetaste an. Kopieren Sie Archivkomponenten mit F5.

Ein Paket-Manager mit allen Funktionen ist als YaST-Modul verfügbar. Weitere Informationen finden Sie unter *Buch „Bereitstellungshandbuch", Kapitel 13 „Installieren bzw. Entfernen von Software"*.

7 Systemwiederherstellung und Snapshot-Verwaltung mit Snapper

Viele Benutzer fragten bereits nach einer Funktion, mit der sie Snapshots des Dateisystems anfertigen könnten, um so Rollbacks für Linux auszuführen. Dank Snapper mit dem `Btrfs`-Dateisystem oder mit Thin Provisioned LVM-Volumes ist diese Lücke nunmehr geschlossen.

Das neue Copy-on-Write-Dateisystem `Btrfs` für Linux unterstützt Dateisystem-Snapshots (Kopie des Zustands eines Subvolume zu einem bestimmten Zeitpunkt) von Subvolumes (ein oder mehrere separat einhängbare Dateisysteme auf den einzelnen physischen Partitionen). Snapshots werden auch auf LVM-Volumes mit Thin-Provisioning unterstützt, die mit XFS, Ext4 oder Ext3 formatiert sind. Mit Snapper erstellen und verwalten Sie diese Snapshots. Snapper ist mit einer Kommandozeile und einer YaST-Oberfläche ausgestattet. Ab SUSE Linux Enterprise Server 12 können Sie außerdem aus `Btrfs`-Snapshots booten. Weitere Informationen finden Sie in *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots“*.

Snapper ermöglicht Folgendes:

- Systemänderungen rückgängig machen, die von **`zypper`** und YaST vorgenommen wurden. Weitere Informationen finden Sie in *Abschnitt 7.2, „Rückgängigmachen von Änderungen mit Snapper“*.
- Dateien aus früheren Snapshots wiederherstellen. Weitere Informationen finden Sie in *Abschnitt 7.2.2, „Wiederherstellen von Dateien mit Snapper“*.
- System-Rollback durch Booten aus einem Snapshot vornehmen. Weitere Informationen finden Sie in *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots“*.
- Snapshots interaktiv manuell erstellen und vorhandene Snapshots verwalten. Weitere Informationen finden Sie in *Abschnitt 7.5, „Manuelles Erstellen und Verwalten von Snapshots“*.

7.1 Standardeinrichtung

Snapper unter SUSE Linux Enterprise Server wird als „Werkzeug zum Rückgängigmachen und Wiederherstellen“ von Systemänderungen eingerichtet. Standardmäßig ist die Root-Partition (`/`) von SUSE Linux Enterprise Server mit `Btrfs` formatiert. Das Anfertigen von Snapshots wird automatisch aktiviert, wenn die Root-Partition (`/`) groß genug ist (ungefähr mehr als 16 GB). Das Anfertigen von Snapshots auf anderen Partitionen (abgesehen von `/`) ist standardmäßig nicht aktiviert.

Tipp: Aktivieren von Snapper im installierten System

Wenn Sie Snapper während der Installation deaktiviert haben, können Sie dieses Werkzeug später jederzeit wieder aktivieren. Erstellen Sie hierzu eine Snapper-Standardkonfiguration für das Root-Dateisystem mit

```
tux > sudo snapper -c root create-config /
```

Aktivieren Sie dann die verschiedenen Snapshot-Typen gemäß den Anweisungen unter *Abschnitt 7.1.3.1, „Deaktivieren/Aktivieren von Snapshots“*.

Denken Sie daran, dass für Snapshots ein Btrfs-Root-Dateisystem erforderlich ist, dessen Subvolumes gemäß den Vorschlägen des Installationsprogramms und mit einer Partitionsgröße von mindestens 16 GB eingerichtet werden müssen.

Beim Erstellen eines Snapshots verweisen sowohl der Snapshot als auch das Original auf dieselben Blöcke im Dateisystem. Zunächst belegt ein Snapshot also keinen zusätzlichen Speicherplatz auf der Festplatte. Werden Daten im Original-Dateisystem bearbeitet, so werden die geänderten Datenblöcke kopiert, und die alten Datenblöcke werden im Snapshot beibehalten. Der Snapshot belegt daher dieselbe Speicherplatzmenge wie die geänderten Daten. Im Lauf der Zeit wächst der Speicherplatzbedarf eines Snapshots somit an. Wenn Sie also Dateien aus einem `Btrfs`-Dateisystem löschen, auf dem sich Snapshots befinden, wird unter Umständen *kein* Speicherplatz freigegeben!

Anmerkung: Position der Snapshots

Snapshots befinden sich stets auf der Partition oder dem Subvolume, auf dem der Snapshot aufgenommen wurde. Es ist nicht möglich, einen Snapshot auf einer anderen Partition oder einem anderen Subvolume zu speichern.

Partitionen mit Snapshots müssen daher größer sein als „normale“ Partitionen. Die Speichermenge ist dabei abhängig von der Anzahl der Snapshots und vom Umfang der Änderungen an den Daten. In der Regel sollten Sie etwa den doppelten Speicherplatz bereitstellen. Um zu verhindern, dass es zu wenig Speicherplatz gibt, werden alte Snapshots automatisch bereinigt. Weitere Informationen finden Sie unter *Abschnitt 7.1.3.4, „Steuern der Snapshot-Archivierung“*.

7.1.1 Typen von Snapshots

Die Snapshots an sich unterscheiden sich streng genommen nicht voneinander, werden allerdings dennoch gemäß den Ereignissen, die sie ausgelöst haben, in drei Snapshot-Typen gegliedert:

Zeitleisten-Snapshots

In Abständen von einer Stunde wird ein einzelner Snapshot erstellt. Alte Snapshots werden automatisch gelöscht. Standardmäßig wird der erste Snapshot der letzten zehn Tage, Monate und Jahre beibehalten. Zeitleisten-Snapshots sind standardmäßig deaktiviert.

Installations-Snapshots

Wenn Sie ein oder mehrere Pakete mit YaST oder zypper installieren, wird ein Snapshot-Paar erstellt: ein Snapshot vor Beginn der Installation („Pre“) und ein zweiter Snapshot nach Abschluss der Installation („Post“). Wird eine wichtige Systemkomponente installiert (z. B. der Kernel), wird das Snapshot-Paar als wichtig gekennzeichnet (`important=yes`). Alte Snapshots werden automatisch gelöscht. Standardmäßig werden die letzten zehn wichtigen Snapshots und die letzten zehn „normalen“ Snapshots (auch Verwaltungs-Snapshots) beibehalten. Installations-Snapshots sind standardmäßig aktiviert.

Verwaltungs-Snapshots

Wenn Sie die Verwaltung eines Systems mit YaST vornehmen, wird ein Snapshot-Paar erstellt: ein Snapshot beim Starten eines YaST-Moduls („Pre“) und ein zweiter Snapshot beim Schließen des Moduls („Post“). Alte Snapshots werden automatisch gelöscht. Standardmäßig werden die letzten zehn wichtigen Snapshots und die letzten zehn „normalen“ Snapshots (auch Installations-Snapshots) beibehalten. Verwaltungs-Snapshots sind standardmäßig aktiviert.

7.1.2 Verzeichnisse, die aus Snapshots ausgenommen sind

Bestimmte Verzeichnisse müssen aus verschiedenen Gründen aus den Snapshots ausgenommen werden. Die folgende Liste zeigt alle ausgeschlossenen Verzeichnisse:

`/boot/grub2/i386-pc`, `/boot/grub2/x86_64-efi`, `/boot/grub2/powerpc-ieee1275`, `/boot/grub2/s390x-emu`

Ein Rollback der Bootloader-Konfiguration wird nicht unterstützt. Die obigen Verzeichnisse sind abhängig von der Architektur. Die ersten beiden Verzeichnisse gelten für AMD64-/Intel-64-Computer und die letzten beiden Verzeichnisse für IBM POWER bzw. für IBM z Systems.

`/home`

Wenn `/home` sich nicht auf einer separaten Partition befindet, wird dieses Verzeichnis ausgeschlossen, damit bei einem Rollback kein Datenverlust eintritt.

`/opt`, `/var/opt`

Produkte von Drittanbietern werden in der Regel in `/opt` installiert. Dieses Verzeichnis wird ausgeschlossen, damit die betreffenden Anwendungen bei einem Rollback nicht deinstalliert werden.

`/srv`

Enthält Daten für Web- und FTP-Server. Ausgeschlossen, damit bei einem Rollback kein Datenverlust eintritt.

`/tmp`, `/var/tmp`, `/var/cache`, `/var/crash`

Alle Verzeichnisse, die temporäre Dateien und Caches enthalten, werden aus den Snapshots ausgeschlossen.

`/usr/local`

Dieses Verzeichnis wird bei der manuellen Installation von Software verwendet. Dieses Verzeichnis wird ausgeschlossen, damit die betreffenden Installationen bei einem Rollback nicht deinstalliert werden.

`/var/lib/libvirt/images`

Die Standardposition für Images von virtuellen Rechnern, die mit libvirt verwaltet werden Dieses Verzeichnis wird ausgeschlossen, damit bei einem Rollback keine Images von virtuellen Rechnern durch ältere Versionen ersetzt werden. Standardmäßig wird dieses Subvolume mit der Option `no copy on write` (keine Kopie beim Schreibvorgang) erstellt.

`/var/lib/mailman`, `/var/spool`

Verzeichnisse, die Emails oder Email-Warteschlangen enthalten, werden ausgeschlossen, damit kein Email-Verlust nach einem Rollback eintritt.

`/var/lib/named`

Enthält Zonendaten für den DNS-Server. Aus den Snapshots ausgeschlossen, damit ein Nameserver auch nach einem Rollback noch funktionsfähig ist.

`/var/lib/mariadb`, `/var/lib/mysql`, `/var/lib/pgqsl`

Diese Verzeichnisse enthalten Datenbankdaten. Standardmäßig werden diese Subvolumes mit der Option `no copy on write` (keine Kopie beim Schreibvorgang) erstellt.

`/var/log`

Standort der Protokolldatei. Aus den Snapshots ausgeschlossen, damit die Protokolldateien auch nach dem Rollback eines fehlerhaften Systems noch analysiert werden können.

7.1.3 Anpassen der Einrichtung

Die Standardeinrichtung von SUSE Linux Enterprise Server deckt die meisten Anwendungsfälle ab. Sie haben jedoch die Möglichkeit, alle Aspekte beim Anfertigen und Beibehalten der Snapshots ganz nach Ihren Anforderungen zu konfigurieren.

7.1.3.1 Deaktivieren/Aktivieren von Snapshots

Die drei Snapshot-Typen (Zeitleiste, Installation, Administration) können unabhängig voneinander einzeln aktiviert oder deaktiviert werden.

Deaktivieren/Aktivieren von Zeitleisten-Snapshots

Aktivieren. `snapper -c root set-config "TIMELINE_CREATE=yes"`

Deaktivieren. `snapper -c root set-config "TIMELINE_CREATE=no"`

Mit Ausnahme der Root-Partition sind Zeitleisten-Snapshots standardmäßig aktiviert.

Deaktivieren/Aktivieren von Installations-Snapshots

Aktivieren: Installieren Sie das Paket `snapper-zypp-plugin`.

Deaktivieren: Deinstallieren Sie das Paket `snapper-zypp-plugin`

Installations-Snapshots sind standardmäßig aktiviert.

Deaktivieren/Aktivieren von Administrations-Snapshots

Aktivieren: Stellen Sie `USE_SNAPPER` in `/etc/sysconfig/yast2` auf `yes` ein.

Deaktivieren: Stellen Sie `USE_SNAPPER` in `/etc/sysconfig/yast2` auf `no` ein. Administrations-Snapshots sind standardmäßig aktiviert.

7.1.3.2 Steuern von Installations-Snapshots

Das Anfertigen von Snapshot-Paaren beim Installieren von Paketen mit YaST oder Zypper erfolgt mit `snapper-zypp-plugin`. Die XML-Konfigurationsdatei `/etc/snapper/zypp-plugin.conf` definiert den Zeitpunkt, an dem die Snapshots erstellt werden sollen. Standardmäßig sieht die Datei folgendermaßen aus:

```
 1 <?xml version="1.0" encoding="utf-8"?>
 2 <snapper-zypp-plugin-conf>
 3  <solvables>
 4   <solvable match="w"❶ important="true"❷>kernel-*❸</solvable>
 5   <solvable match="w" important="true">dracut</solvable>
 6   <solvable match="w" important="true">glibc</solvable>
 7   <solvable match="w" important="true">systemd*</solvable>
 8   <solvable match="w" important="true">udev</solvable>
 9   <solvable match="w">*</solvable>❹
10  </solvables>
11 </snapper-zypp-plugin-conf>
```

❶ Das Übereinstimmungsattribut definiert, ob das Schema eine Wildcard im Unix-Shell-Format (`w`) oder ein regulärer Python-Ausdruck (`re`) ist.

❷ Wenn für das angegebene Schema eine Übereinstimmung vorliegt und das entsprechende Paket als wichtig gekennzeichnet ist (z. B. Kernel-Pakete), wird der Snapshot ebenfalls als wichtig gekennzeichnet.

❸ Schema, das mit einem Paketnamen abgeglichen werden soll. Gemäß der Einstellung für das Attribut `match` werden Sonderzeichen entweder als Shell-Wildcards oder als reguläre Ausdrücke interpretiert. Dieses Schema stimmt mit allen Paketnamen überein, die mit `kernel-` beginnen.

❹ Mit dieser Zeile werden alle Pakete als übereinstimmend eingestuft.

Bei dieser Konfiguration werden Snapshot-Paare angefertigt, sobald ein Paket installiert wird (Zeile 9). Wenn Kernel-, dracut-, glibc-, systemd- oder udev-Pakete installiert werden, die als wichtig gekennzeichnet sind, wird auch das Snapshot-Paar als wichtig gekennzeichnet (Zeile 4 bis 8). Alle Regeln werden ausgewertet.

Zum Deaktivieren einer Regel können Sie die betreffende Regel löschen oder mithilfe von XML-Kommentaren deaktivieren. Wenn das System beispielsweise keine Snapshot-Paare für alle Paketinstallationen anfertigen soll, kommentieren Sie Zeile 9 aus:

```
 1 <?xml version="1.0" encoding="utf-8"?>
 2 <snapper-zypp-plugin-conf>
 3  <solvables>
 4   <solvable match="w" important="true">kernel-*</solvable>
 5   <solvable match="w" important="true">dracut</solvable>
 6   <solvable match="w" important="true">glibc</solvable>
 7   <solvable match="w" important="true">systemd*</solvable>
 8   <solvable match="w" important="true">udev</solvable>
 9   <!-- <solvable match="w">*</solvable> -->
10  </solvables>
11 </snapper-zypp-plugin-conf>
```

7.1.3.3 Erstellen und Einhängen neuer Subvolumes

Das Erstellen eines neuen Subvolumes unter der `/`-Hierarchie und das dauerhafte Einhängen dieses Subvolumes werden unterstützt. Ein solches Subvolume wird in den Snapshots nicht berücksichtigt. Das Subvolume darf nicht in einem vorhandenen Snapshot angelegt werden, da Sie dann nach einem Rollback keine Snapshots mehr löschen könnten.

SUSE Linux Enterprise Server ist mit dem Subvolume `/@/` konfiguriert, das als unabhängiger Root für dauerhafte Subvolumes wie `/opt`, `/srv` oder `/home` fungiert. Alle erstellten und dauerhaft eingehängten Subvolumes müssen in diesem anfänglichen Root-Dateisystem erstellt werden.

Führen Sie hierzu die nachfolgenden Befehle aus. In diesem Beispiel wird das neue Subvolume `/usr/important` aus `/dev/sda2` erstellt.

```
tux > sudo mount /dev/sda2 -o subvol=@ /mnt
tux > sudo btrfs subvolume create /mnt/usr/important
tux > sudo umount /mnt
```

Der zugehörige Eintrag in `/etc/fstab` muss dabei wie folgt lauten (Beispiel):

```
/dev/sda2 /usr/important btrfs subvol=@/usr/important 0 0
```

Tipp: Deaktivieren des Copy-on-Write-Verfahrens (COW)

Ein Subvolume kann Dateien enthalten, die sich fortwährend ändern, z. B. virtualisierte Festplatten-Images, Datenbankdateien oder Protokolldateien. Wenn dies der Fall ist, sollten Sie die Copy-on-Write-Funktion für dieses Volume deaktivieren, damit die Festplattenblöcke nicht dupliziert werden. Geben Sie hierzu die Einhängeoption `nodatacow` in `/etc/fstab` an:

```
/dev/sda2 /usr/important btrfs nodatacow,subvol=@/usr/important 0 0
```

Mit dem Befehl **`chattr +C`** *PATH* können Sie das Copy-on-Write-Verfahren alternativ für einzelne Dateien oder Verzeichnisse deaktivieren.

7.1.3.4 Steuern der Snapshot-Archivierung

Snapshots belegen Speicherplatz auf der Festplatte. Damit keine Systemfehler wegen mangelnden Festplattenspeichers auftreten, werden alte Snapshots automatisch gelöscht. Standardmäßig werden zehn wichtige Installations- und Verwaltungs-Snapshots und bis zu zehn normale Installations- und Verwaltungs-Snapshots beibehalten. Wenn diese Snapshots mehr als 50 % des Root-Dateisystems einnehmen, werden zusätzliche Snapshots gelöscht. Mindestens vier wichtige und zwei normale Snapshots werden immer beibehalten.

Anweisungen zum Ändern dieser Werte finden Sie in *Abschnitt 7.4.1, „Verwalten vorhandener Konfigurationen“*.

7.1.3.5 Verwenden von Snapper auf Thin Provisioned LVM-Volumes

Neben Snapshots auf `Btrfs`-Dateisystemen unterstützt Snapper auch das Anfertigen von Snapshots auf LVM-Volumes mit Thin-Provisioning (Snapshots auf normalen LVM-Volumes werden *nicht* unterstützt), die mit XFS, Ext4 oder Ext3 formatiert sind. Weitere Informationen zu LVM-Volumes sowie Anweisungen zum Einrichten dieser Volumes finden Sie im *Buch „*Bereitstellungshandbuch*“, Kapitel 12 „Fortgeschrittene Festplattenkonfiguration“, Abschnitt 12.2 „LVM-Konfiguration“*.

Um Snapper auf einem Thin Provisioned LVM-Volume zu nutzen, müssen Sie eine Snapper-Konfiguration für dieses Volume erstellen. Auf LVM muss das Dateisystem mit `--fstype=lvm(FILESYSTEM)` angegeben werden. Zulässige Werte für *FILESYSTEM* sind `ext3`, `etx4` und `xfs`. Beispiel:

```
tux > sudo snapper -c lvm create-config --fstype="lvm(xfs)" /thin_lvm
```

Sie können diese Konfiguration gemäß den Anweisungen unter *Abschnitt 7.4.1, „Verwalten vorhandener Konfigurationen“* an Ihre Anforderungen anpassen.

7.2 Rückgängigmachen von Änderungen mit Snapper

Snapper unter SUSE Linux Enterprise Server ist als Werkzeug vorkonfiguriert, mit dem Sie die Änderungen rückgängig machen, die von **`zypper`** und YaST vorgenommen werden. Hierzu ist Snapper so konfiguriert, dass vor und nach jeder Ausführung von **`zypper`** bzw. YaST ein Snapshot-Paar erstellt wird. Mit Snapper können Sie außerdem Systemdateien wiederherstellen, die versehentlich gelöscht oder geändert wurden. Zeitleisten-Snapshots für die Root-Partition müssen für diesen Zweck aktiviert werden. Weitere Detailinformationen finden Sie unter *Abschnitt 7.1.3.1, „Deaktivieren/Aktivieren von Snapshots“*.

Standardmäßig werden automatische Snapshots (wie oben beschrieben) für die Root-Partition und deren Subvolumes konfiguriert. Sollen Snapshots auch für andere Partitionen zur Verfügung stehen, beispielsweise für `/home`, können Sie benutzerdefinierte Konfigurationen anlegen.

Wichtig: Rückgängigmachen von Änderungen im Vergleich zu Rollback

Beim Wiederherstellen von Daten mithilfe von Snapshots ist zu beachten, dass Snapper zwei grundlegend verschiedene Szenarien bearbeiten kann:

Rückgängigmachen von Änderungen

Beim Rückgängigmachen von Änderungen gemäß den nachfolgenden Anweisungen werden zwei Snapshots miteinander verglichen, und die Änderungen zwischen diesen beiden Snapshots werden rückgängig gemacht. Bei diesem Verfahren können Sie zudem die wiederherzustellenden Dateien explizit auswählen.

Rollback

Beim Rollback gemäß den Anweisungen in *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots“* wird das System in den Zustand zurückversetzt, der beim Anfertigen des Snapshots vorlag.

Beim Rückgängigmachen von Änderungen können Sie außerdem einen Snapshot mit dem aktuellen System vergleichen. Das Wiederherstellen *aller* Dateien aus einem solchen Vergleich liefert dasselbe Ergebnis wie ein Rollback. Für ein Rollback ist jedoch das in *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots“* beschriebene Verfahren vorzuziehen, da es schneller ist und Sie das System vor dem Ausführen des Rollbacks prüfen können.

Warnung: Datenkonsistenz

Es gibt keinen Mechanismus, mit dem die Datenkonsistenz beim Erstellen von Snapshots gewährleistet werden kann. Wenn eine Datei (z. B. eine Datenbank) zur selben Zeit geschrieben wird, während der Snapshot erstellt wird, so wird diese Datei beschädigt oder nur teilweise geschrieben. Beim Wiederherstellen dieser Datei treten Probleme auf. Darüber hinaus dürfen bestimmte Systemdateien wie `/etc/mtab` unter keinen Umständen wiederhergestellt werden. Es wird daher dringend empfohlen, die Liste der geänderten Dateien und ihrer Unterschiede (Diffs) *in jedem Fall* sorgfältig zu prüfen. Stellen Sie nur solche Dateien wieder her, die tatsächlich zu der zurückzunehmenden Aktion gehören.

7.2.1 Rückgängigmachen von Änderungen durch YaST oder Zypper

Wenn Sie die Stammpartition während der Installation mit `Btrfs` einrichten, wird Snapper (für Rollbacks von Änderungen durch YaST oder Zypper vorkonfiguriert) automatisch installiert. Bei jedem Starten eines YaST-Moduls und bei jeder Zypper-Transaktion werden zwei Snapshots erstellt: ein „Pre-Snapshot“ mit dem Zustand des Dateisystems vor dem Start des Moduls und ein „Post-Snapshot“ nach Beendigung des Moduls.

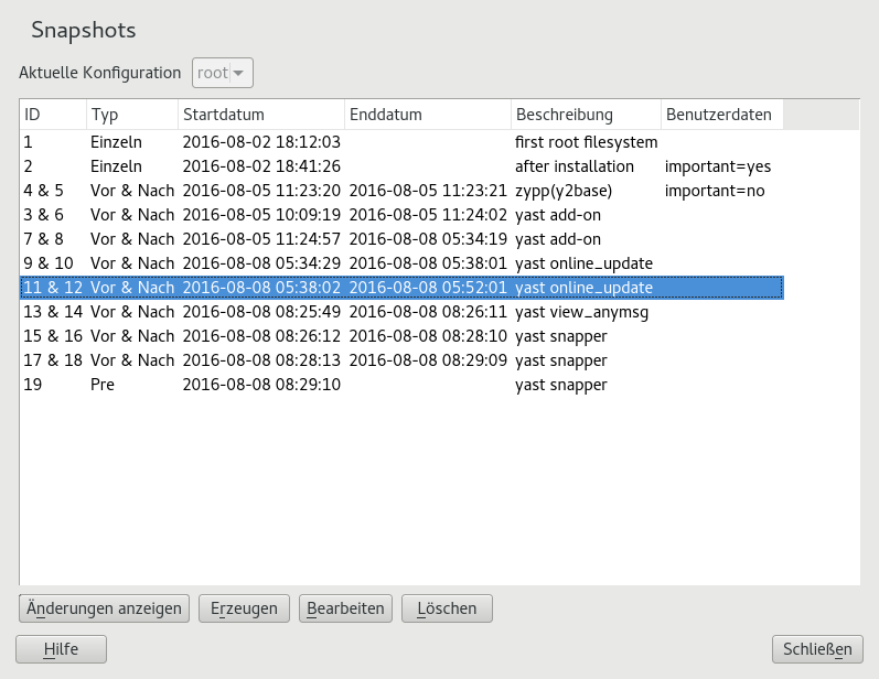
Mit dem YaST-Snapper-Modul oder mit dem **`snapper`**-Kommandozeilenwerkzeug können Sie Dateien aus dem „Pre-Snapshot“ wiederherstellen und so die Änderungen durch YaST/Zypper rückgängig machen. Durch den Vergleich der beiden Snapshots mit diesen Werkzeugen erkennen Sie außerdem, welche Dateien geändert wurden. Darüber hinaus können Sie die Unterschiede (Diff) zwischen zwei Versionen einer Datei abrufen.

PROZEDUR 7.1 RÜCKGÄNGIGMACHEN VON ÄNDERUNGEN MIT DEM *SNAPPER*-MODUL IN YAST

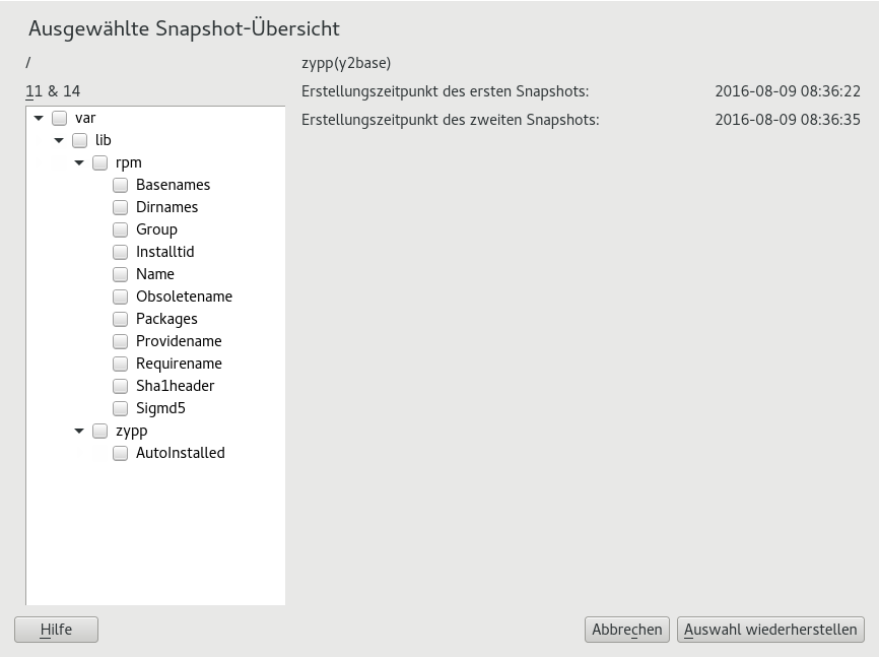
1. Starten Sie das *Snapper*-Modul im Abschnitt *Verschiedenes* in YaST, oder geben Sie **`yast2 snapper`** ein.

2. Unter *Aktuelle Konfiguration* muss die Option *root* eingestellt sein. Dies ist im Prinzip immer der Fall, sofern Sie nicht eigene Snapper-Konfigurationen manuell hinzugefügt haben.

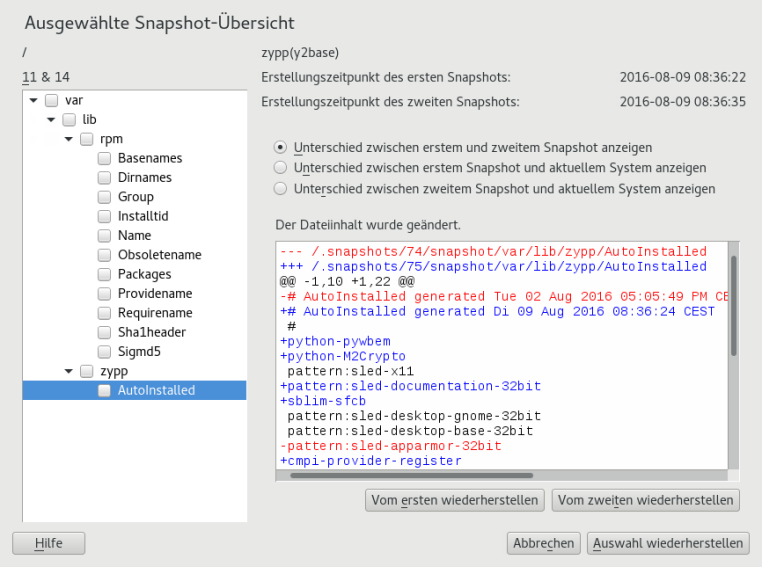
3. Wählen Sie ein Pre-/Post-Snapshot-Paar aus der Liste aus. Sowohl die YaST als auch die Zypper-Snapshot-Paare sind vom Typ *Pre & Post*. Für YaST-Snapshots wird die Bezeichnung `zyyp(y2base)` in der *Spalte „Beschreibung“* angezeigt, für zypper-Snapshots die Bezeichnung `zypp(zypper)`.



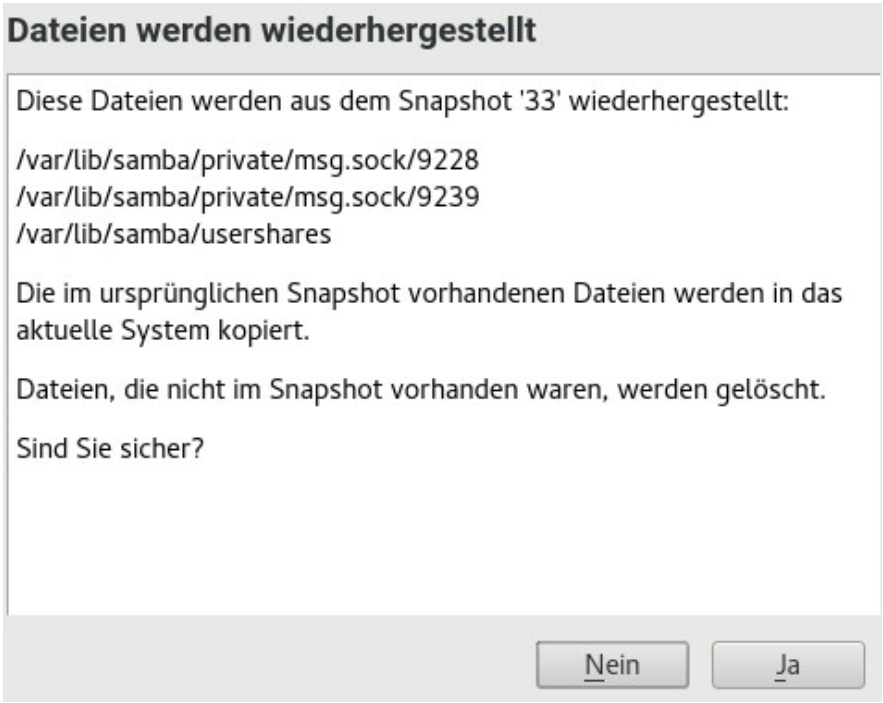
4. Klicken Sie auf *Änderungen anzeigen*. Die Liste der Dateien, bei denen Unterschiede zwischen den beiden Snapshots bestehen, wird geöffnet.



5. Prüfen Sie die Dateiliste. Zum Anzeigen der Unterschiede („Diff“) zwischen der Pre- und der Post-Version einer Datei wählen Sie die Datei aus der Liste aus.



6. Zum Wiederherstellen von einer oder mehreren Dateien aktivieren Sie das entsprechende Kontrollkästchen für die gewünschten Dateien oder Verzeichnisse. Klicken Sie auf *Auswahl wiederherstellen*, und bestätigen Sie den Vorgang mit *Ja*.



Zum Wiederherstellen einer einzelnen Datei klicken Sie auf den Namen dieser Datei. Die Diff-Ansicht der Datei wird aktiviert. Klicken Sie auf *Vom ersten wiederherstellen*, und bestätigen Sie mit *Ja*.

PROZEDUR 7.2 RÜCKGÄNGIGMACHEN VON ÄNDERUNGEN MIT DEM KOMMANDO `snapper`

1. Mit dem Kommando **`snapper list -t pre-post`** erhalten Sie eine Liste der YaST- und Zypper-Snapshots. Für YaST-Snapshots wird die Bezeichnung `yast` *`MODULNAME`* in der *Spalte „Beschreibung“* angezeigt, für zypper-Snapshots die Bezeichnung `zypp(zypper)`.

```
tux > sudo snapper list -t pre-post
Pre # | Post # | Pre Date                     | Post Date                    | Description
------+--------+------------------------------+------------------------------+-------------
311   | 312    | Tue 06 May 2014 14:05:46 CEST | Tue 06 May 2014 14:05:52 CEST | zypp(y2base)
340   | 341    | Wed 07 May 2014 16:15:10 CEST | Wed 07 May 2014 16:15:16 CEST | zypp(zypper)
342   | 343    | Wed 07 May 2014 16:20:38 CEST | Wed 07 May 2014 16:20:42 CEST | zypp(y2base)
344   | 345    | Wed 07 May 2014 16:21:23 CEST | Wed 07 May 2014 16:21:24 CEST | zypp(zypper)
346   | 347    | Wed 07 May 2014 16:41:06 CEST | Wed 07 May 2014 16:41:10 CEST | zypp(y2base)
348   | 349    | Wed 07 May 2014 16:44:50 CEST | Wed 07 May 2014 16:44:53 CEST | zypp(y2base)
350   | 351    | Wed 07 May 2014 16:46:27 CEST | Wed 07 May 2014 16:46:38 CEST | zypp(y2base)
```

2. Mit dem Kommando **`snapper status`** *`PRE`* erhalten Sie eine Liste der geänderten Dateien für ein Snapshot-Paar. *`POST`*. Dateien, deren Inhalt geändert wurde, sind mit *c* gekennzeichnet, hinzugefügte Dateien mit + und gelöschte Dateien mit -.

```
tux > sudo snapper status 350..351
```

```
+..... /usr/share/doc/packages/mikachan-fonts
+..... /usr/share/doc/packages/mikachan-fonts/COPYING
+..... /usr/share/doc/packages/mikachan-fonts/dl.html
c..... /usr/share/fonts/truetype/fonts.dir
c..... /usr/share/fonts/truetype/fonts.scale
+..... /usr/share/fonts/truetype/#####-p.ttf
+..... /usr/share/fonts/truetype/#####-pb.ttf
+..... /usr/share/fonts/truetype/#####-ps.ttf
+..... /usr/share/fonts/truetype/#####.ttf
c..... /var/cache/fontconfig/7ef2298fde41cc6eeb7af42e48b7d293-x86_64.cache-4
c..... /var/lib/rpm/Basenames
c..... /var/lib/rpm/Dirnames
c..... /var/lib/rpm/Group
c..... /var/lib/rpm/Installtid
c..... /var/lib/rpm/Name
c..... /var/lib/rpm/Packages
c..... /var/lib/rpm/Providename
c..... /var/lib/rpm/Requirename
c..... /var/lib/rpm/Sha1header
c..... /var/lib/rpm/Sigmd5
```

3. Zum Anzeigen der Unterschiede (Diff) für eine bestimmte Datei führen Sie **`snapper diff`** *PRE* aus. *POST* *FILENAME*. Wenn Sie *FILENAME* nicht angeben, wird die Diff-Ansicht für alle Dateien angezeigt.

```
tux > sudo snapper diff 350..351 /usr/share/fonts/truetype/fonts.scale
--- /.snapshots/350/snapshot/usr/share/fonts/truetype/fonts.scale       2014-04-23
 15:58:57.000000000 +0200
+++ /.snapshots/351/snapshot/usr/share/fonts/truetype/fonts.scale       2014-05-07
 16:46:31.000000000 +0200
@@ -1,4 +1,4 @@
-1174
+1486
 ds=y:ai=0.2:luximr.ttf -b&h-luxi mono-bold-i-normal--0-0-0-0-c-0-iso10646-1
 ds=y:ai=0.2:luximr.ttf -b&h-luxi mono-bold-i-normal--0-0-0-0-c-0-iso8859-1
[...]
```

4. Zum Wiederherstellen einer oder mehrerer Dateien führen Sie **`snapper -v undochange`** *PRE* aus. *POST* *FILENAMES*. Wenn Sie *FILENAMES* nicht angeben, werden alle geänderten Dateien wiederhergestellt.

```
tux > sudo snapper -v undochange 350..351
     create:0 modify:13 delete:7
     undoing change...
     deleting /usr/share/doc/packages/mikachan-fonts
     deleting /usr/share/doc/packages/mikachan-fonts/COPYING
```

```
    deleting /usr/share/doc/packages/mikachan-fonts/dl.html
    deleting /usr/share/fonts/truetype/#####-p.ttf
    deleting /usr/share/fonts/truetype/#####-pb.ttf
    deleting /usr/share/fonts/truetype/#####-ps.ttf
    deleting /usr/share/fonts/truetype/#####.ttf
    modifying /usr/share/fonts/truetype/fonts.dir
    modifying /usr/share/fonts/truetype/fonts.scale
    modifying /var/cache/fontconfig/7ef2298fde41cc6eeb7af42e48b7d293-x86_64.cache-4
    modifying /var/lib/rpm/Basenames
    modifying /var/lib/rpm/Dirnames
    modifying /var/lib/rpm/Group
    modifying /var/lib/rpm/Installtid
    modifying /var/lib/rpm/Name
    modifying /var/lib/rpm/Packages
    modifying /var/lib/rpm/Providename
    modifying /var/lib/rpm/Requirename
    modifying /var/lib/rpm/Sha1header
    modifying /var/lib/rpm/Sigmd5
    undoing change done
```

Warnung: Rückgängigmachen des Hinzufügens von Benutzern

Es wird nicht empfohlen, das Hinzufügen von Benutzern durch Rückgängigmachen von Änderungen zurückzunehmen. Einige Dateien, die zu diesen Benutzern gehören, verbleiben im System, da bestimmte Verzeichnisse von den Snapshots ausgeschlossen sind. Wenn ein Benutzer mit derselben Benutzer-ID wie ein gelöschter Benutzer erstellt wird, würde dieser neue Benutzer die zurückgebliebenen Dateien erben. Für das Entfernen von Benutzern wird daher dringend das YaST-Werkzeug *Benutzer- und Gruppenverwaltung* empfohlen.

7.2.2 Wiederherstellen von Dateien mit Snapper

Neben den Installations- und Verwaltungs-Snapshots werden auch Zeitleisten-Snapshots in Snapper angefertigt. Mithilfe dieser Sicherungs-Snapshots können Sie Dateien wiederherstellen, die versehentlich gelöscht wurden, oder eine frühere Version einer Datei wiederherstellen. Mit der Diff-Funktion in Snapper können Sie außerdem feststellen, welche Änderungen zu einem bestimmten Zeitpunkt vorgenommen wurden.

Das Wiederherstellen von Daten ist besonders für Daten interessant, die sich in Subvolumes oder Partitionen befinden, für die standardmäßig keine Snapshots erstellt werden. Damit Sie beispielsweise Dateien aus einem home-Verzeichnis wiederherstellen können, legen Sie eine

separate Snapper-Konfiguration für `/home` an, mit der automatische Zeitleisten-Snapshots angefertigt werden. Eine Anleitung dazu finden Sie in *Abschnitt 7.4, „Erstellen und Bearbeiten von Snapper-Konfigurationen“*.

Warnung: Wiederherstellen von Dateien im Vergleich zu Rollback

Anhand der Snapshots für das Root-Dateisystem (in der Root-Konfiguration von Snapper definiert) können Sie ein Rollback des Systems vornehmen. Hierzu wird empfohlen, aus dem Snapshot zu booten und dann das Rollback auszuführen. Weitere Informationen finden Sie in *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots“*.

Zum Ausführen eines Rollbacks können Sie alternativ alle Dateien aus einem Root-Dateisystem gemäß den nachfolgenden Anweisungen wiederherstellen. Diese Methode wird jedoch nicht empfohlen. Sie können durchaus einzelne Dateien wiederherstellen, beispielsweise eine Konfigurationsdatei im Verzeichnis `/etc`, nicht jedoch die gesamte Liste aller Dateien im Snapshot.

Diese Beschränkung gilt nur für Snapshots, die für das Root-Dateisystem angefertigt wurden.

PROZEDUR 7.3 WIEDERHERSTELLEN VON DATEIEN MIT DEM *SNAPPER*-MODUL IN YAST

1. Starten Sie das *Snapper*-Modul im Abschnitt *Verschiedenes* in YaST, oder geben Sie **`yast2 snapper`** ein.
2. Wählen Sie die *Aktuelle Konfiguration* aus, von der ein Snapshot ausgewählt werden soll.
3. Wählen Sie einen Zeitleisten-Snapshot aus, aus dem eine Datei wiederhergestellt werden soll, und wählen Sie *Änderungen anzeigen*. Zeitleisten-Snapshots weisen den Typ *Einzeln* und den Beschreibungswert *timeline* (Zeitachse) auf.
4. Wählen Sie eine Datei im Textfeld aus; klicken Sie hierzu auf den Dateinamen. Die Unterschiede zwischen der Snapshot-Version und dem aktuellen System werden angezeigt. Aktivieren Sie das Kontrollkästchen für die wiederherzustellende Datei. Wiederholen Sie dies für alle wiederherzustellenden Dateien.
5. Klicken Sie auf *Auswahl wiederherstellen*, und bestätigen Sie den Vorgang mit *Ja*.

PROZEDUR 7.4 WIEDERHERSTELLEN VON DATEIEN MIT DEM KOMMANDO snapper

1. Mit dem folgenden Kommando erhalten Sie eine Liste der Zeitleisten-Snapshots für eine bestimmte Konfiguration:

   ```
   tux > sudo snapper -c CONFIG list -t single | grep timeline
   ```

   Ersetzen Sie *CONFIG* durch eine vorhandene Snapper-Konfiguration. Mit **snapper list-configs** rufen Sie eine Liste ab.

2. Mit dem folgenden Kommando erhalten Sie eine Liste der geänderten Dateien in einem bestimmten Snapshot:

   ```
   tux > sudo snapper -c CONFIG status SNAPSHOT_ID..0
   ```

   Ersetzen Sie *SNAPSHOT_ID* durch die ID des Snapshots, aus dem die Datei(en) wiederhergestellt werden sollen.

3. Rufen Sie optional mit dem folgenden Kommando eine Liste der Unterschiede zwischen der aktuellen Dateiversion und der Dateiversion im Snapshot ab:

   ```
   tux > sudo snapper -c CONFIG diff SNAPSHOT_ID..0 FILE NAME
   ```

   Wenn Sie keinen Dateinamen (*<FILE NAME>*) angeben, werden die Unterschiede für alle Dateien angezeigt.

4. Zum Wiederherstellen einer oder mehrerer Dateien führen Sie Folgendes aus:

   ```
   tux > sudo snapper -c CONFIG -v undochange SNAPSHOT_ID..0 FILENAME1 FILENAME2
   ```

   Wenn Sie keine Dateinamen angeben, werden alle geänderten Dateien wiederhergestellt.

7.3 System-Rollback durch Booten aus Snapshots

Mit der GRUB 2-Version in SUSE Linux Enterprise Server können Sie aus Btrfs-Snapshots booten. Zusammen mit der Rollback-Funktion in Snapper sind Sie so in der Lage, ein falsch konfiguriertes System wiederherzustellen. Nur Snapshots, die für die Snapper-Standardkonfiguration (`root`) erstellt wurden, sind bootfähig.

Wichtig: Unterstützte Konfiguration

Ab SUSE Linux Enterprise Server 12 SP5 werden System-Rollbacks nur unterstützt, wenn die Konfiguration des Standard-Subvolumes der Root-Partition nicht geändert wurde.

Beim Booten eines Snapshots werden die Teile des Dateisystems, die sich im Snapshot befinden, schreibgeschützt eingehängt. Alle anderen Dateisysteme und Teile, die aus Snapshots ausgeschlossen sind, werden schreibfähig eingehängt und können bearbeitet werden.

Wichtig: Rückgängigmachen von Änderungen im Vergleich zu Rollback

Beim Wiederherstellen von Daten mithilfe von Snapshots ist zu beachten, dass Snapper zwei grundlegend verschiedene Szenarien bearbeiten kann:

Rückgängigmachen von Änderungen

Beim Rückgängigmachen von Änderungen gemäß den Anweisungen in *Abschnitt 7.2, „Rückgängigmachen von Änderungen mit Snapper“* werden zwei Snapshots miteinander verglichen, und die Änderungen zwischen diesen beiden Snapshots werden rückgängig gemacht. Bei diesem Verfahren können Sie zudem die Dateien, die von der Wiederherstellung ausgeschlossen werden sollen, explizit auswählen.

Rollback

Beim Rollback gemäß den folgenden Anweisungen wird das System in den Zustand zurückversetzt, der beim Anfertigen des Snapshots vorlag.

Zum Ausführen eines Rollbacks aus einem bootfähigen Snapshot müssen die nachfolgenden Anforderungen erfüllt sein. Bei einer Standardinstallation wird das System entsprechend eingerichtet.

ANFORDERUNGEN FÜR EIN ROLLBACK AUS EINEM BOOTFÄHIGEN SNAPSHOT

- Das Root-Dateisystem muss Btrfs sein. Das Booten aus Snapshots für LVM-Volumes wird nicht unterstützt.

- Das Root-Dateisystem muss sich auf einem einzelnen Gerät, in einer einzelnen Partition und auf einem einzelnen Subvolume befinden. Verzeichnisse, die aus Snapshots ausgeschlossen sind, beispielsweise `/srv` (vollständige Liste siehe *Abschnitt 7.1.2, „Verzeichnisse, die aus Snapshots ausgenommen sind“*), können sich auf separaten Partitionen befinden.

- Das System muss über den installierten Bootlader bootfähig sein.

So führen Sie ein Rollback aus einem bootfähigen Snapshot aus:

1. Booten Sie das System. Wählen Sie im Bootmenü den Eintrag *Bootable snapshots* (Bootfähige Snapshots), und wählen Sie den zu bootenden Snapshot aus. Die Snapshots sind nach Datum geordnet, wobei der jüngste Snapshot an oberster Stelle steht.

2. Melden Sie sich beim System an. Prüfen Sie sorgfältig, ob alle Funktionen wie erwartet arbeiten. Beachten Sie, dass Sie in kein Verzeichnis schreiben können, das Teil des Snapshots ist. Daten, die Sie in andere Verzeichnisse schreiben, gehen *nicht* verloren, unabhängig von Ihrem nächsten Schritt.

3. Wählen Sie den nächsten Schritt abhängig davon aus, ob das Rollback ausgeführt werden soll oder nicht:

   a. Wenn sich das System in einem Status befindet, in dem kein Rollback ausgeführt werden soll, booten Sie erneut in den aktuellen Systemstatus. Sie können dann einen anderen Snapshot auswählen oder das Rettungssystem starten.

   b. Zum Ausführen des Rollbacks führen Sie Folgendes aus:

   ```
   tux > sudo snapper rollback
   ```

   Führen Sie anschließend einen Reboot aus. Wählen Sie im Bootbildschirm den Standard-Booteintrag. Das neu eingesetzte System wird erneut gebootet. Ein Snapshot mit dem Zustand des Dateisystems, bevor das Rollback erstellt wird. Das Standard-Subvolume für Root wird durch einen frischen Schreib-Lese-Snapshot ersetzt. Weitere Informationen finden Sie im *Abschnitt 7.3.1, „Snapshots nach dem Rollback“*.
   Mit der Option `-d` geben Sie eine Beschreibung für den Snapshot an. Beispiel:

   ```
   New file system root since rollback on DATE TIME
   ```

Tipp: Rollback zu einem bestimmten Installationszustand

Wenn die Snapshots bei der Installation nicht deaktiviert werden, wird am Ende der ursprünglichen Systeminstallation ein anfänglicher bootfähiger Snapshot angelegt. Diesen Zustand können Sie jederzeit wiederherstellen; booten Sie hierzu diesen Snapshot. Der Snapshot ist an der Beschreibung `Nach der Installation` erkennbar.

Auch beim Starten einer Systemaufrüstung auf ein Service Pack oder eine neue Hauptversion wird ein bootfähiger Snapshot erstellt (sofern die Snapshots nicht deaktiviert sind).

7.3.1 Snapshots nach dem Rollback

Vor dem Ausführen eines Rollbacks wird ein Snapshot des laufenden Dateisystems erstellt. Die Beschreibung verweist auf die ID des Snapshots, der mit dem Rollback wiederhergestellt wurde.

Die mit Rollbacks erstellten Snapshots erhalten den Wert `number` für das Attribut `Cleanup`. Die Rollback-Snapshots werden daher automatisch gelöscht, sobald die angegebene Anzahl von Snapshots erreicht ist. Weitere Informationen hierzu erhalten Sie unter *Abschnitt 7.6, „Automatisches Bereinigen von Snapshots“*. Wenn der Snapshot wichtige Daten enthält, extrahieren Sie die Daten aus dem Snapshot, bevor er entfernt wird.

7.3.1.1 Beispiel für einen Rollback-Snapshot

Nach einer Neuinstallation liegen beispielsweise die folgenden Snapshots auf dem System vor:

```
root # snapper --iso list
Type   | # |     | Cleanup | Description           | Userdata
-------+---+ ... +---------+-----------------------+--------------
single | 0 |     |         | current               |
single | 1 |     |         | first root filesystem |
single | 2 |     | number  | after installation    | important=yes
```

Nach dem Ausführen von **`sudo snapper rollback`** wird der Snapshot `3` erstellt. Dieser Snapshot enthält den Zustand des Systems vor Beginn des Rollbacks. Snapshot `4` ist das neue Btrfs-Standard-Subvolume und damit das neue System nach dem Neustart.

```
root # snapper --iso list
Type   | # |     | Cleanup | Description           | Userdata
-------+---+ ... +---------+-----------------------+--------------
single | 0 |     |         | current               |
```

```
single | 1 |     | number  | first root filesystem |
single | 2 |     | number  | after installation    | important=yes
single | 3 |     | number  | rollback backup of #1 | important=yes
single | 4 |     |         |                       |
```

7.3.2 Abrufen und Erkennen von Snapshot-Booteinträgen

Zum Booten aus einem Snapshot booten Sie den Computer neu und wählen Sie *Start Bootloader from a read-only snapshot* (Bootloader aus einem schreibgeschützten Snapshot starten). Ein Bildschirm mit allen bootfähigen Snapshots wird geöffnet. Der jüngste Snapshot steht an erster Stelle in der Liste, der älteste entsprechend an letzter Stelle. Navigieren Sie mit den Tasten ↓ und ↑ zum gewünschten Snapshot und aktivieren Sie ihn mit Eingabetaste. Wenn Sie einen Snapshot aus dem Bootmenü heraus aktivieren, wird der Computer nicht sofort neu gestartet; stattdessen wird der Bootloader des ausgewählten Snapshots geöffnet.

ABBILDUNG 7.1 BOOTLOADER: SNAPSHOTS

Die einzelnen Snapshot-Einträge im Bootloader sind an ihrem Namensschema leicht erkennbar:

```
[*] ❶ OS ❷ (KERNEL ❸ ,DATE ❹ TTIME ❺ ,DESCRIPTION ❻ )
```

❶ Wenn der Snapshot als `wichtig` markiert wurde, ist der Eintrag mit einem Sternchen (`*`) gekennzeichnet.

2. Bezeichnung des Betriebssystems.
4. Datum im Format `JJJJ-MM-TT`.
5. Uhrzeit im Format `HH:MM`.
6. Dieses Feld enthält eine Beschreibung des Snapshots. Bei einem manuell erstellten Snapshot ist dies die Zeichenkette, die mit der Option `--description` erstellt wurde, oder eine benutzerdefinierte Zeichenkette (siehe *Tipp: Festlegen einer benutzerdefinierten Beschreibung für Snapshot-Einträge im Bootloader*). Bei einem automatisch erstellten Snapshot ist dies das aufgerufene Werkzeug, beispielsweise `zypp(zypper)` oder `yast_sw_single`. Wenn der Platz im Boot-Bildschirm nicht ausreicht, werden zu lange Beschreibungen ggf. gekürzt.

Tipp: Festlegen einer benutzerdefinierten Beschreibung für Snapshot-Einträge im Bootloader

Sie können die standardmäßige Zeichenkette im Beschreibungsfeld eines Snapshots durch eine benutzerdefinierte Zeichenkette ersetzen. Dies empfiehlt sich beispielsweise, wenn eine automatisch erstellte Beschreibung nicht ausreicht oder eine benutzerdefinierte Beschreibung zu lang ist. Mit dem folgenden Befehl legen Sie eine benutzerdefinierte Zeichenkette *`STRING`* für den Snapshot *`NUMBER`* fest:

```
tux > sudo snapper modify --userdata "bootloader=STRING" NUMBER
```

Die Beschreibung sollte nicht mehr als 25 Zeichen haben. Längere Beschreibungen sind auf dem Bootbildschirm nicht lesbar.

7.3.3 Einschränkungen

Ein *vollständiges* System-Rollback, bei dem der exakte Zustand des gesamten Systems zum Zeitpunkt eines Snapshots wiederhergestellt wird, ist nicht möglich.

7.3.3.1 Verzeichnisse, die aus Snapshots ausgenommen sind

Snapshots des Root-Dateisystems enthalten nicht alle Verzeichnisse. Weitere Informationen und Begründungen finden Sie unter *Abschnitt 7.1.2, „Verzeichnisse, die aus Snapshots ausgenommen sind“*. Als allgemeine Folge werden Daten in diesen Verzeichnissen nicht wiederhergestellt, was zu den nachfolgenden Beschränkungen führt.

Add-ons und Software von Drittanbietern sind nach einem Rollback u. U. nicht nutzbar

Anwendungen und Add-ons, mit denen Daten in Subvolumes installiert werden, die vom Snapshot ausgeschlossen sind (z. B. `/opt`), sind nach einem Rollback möglicherweise nicht funktionsfähig, wenn andere Teile der Anwendungsdaten auf Subvolumes installiert wurden, die im Snapshot berücksichtigt wurden. Zum Beheben dieses Problems installieren Sie die Anwendung oder das Add-on neu.

Probleme beim Dateizugriff

Wenn bei einer Anwendung die Berechtigungen und/oder das Eigentum für Dateien zwischen dem Anfertigen des Snapshots und dem aktuellen Zustand des Systems geändert wurden, kann diese Anwendung möglicherweise nicht mehr auf diese Dateien zugreifen. Setzen Sie die Berechtigungen und/oder das Eigentum für die betreffenden Dateien nach dem Rollback zurück.

Inkompatible Datenformate

Wenn ein Service oder eine Anwendung ein neues Datenformat zwischen dem Anfertigen des Snapshots und dem aktuellen Zustand des Systems festgelegt hat, kann die Anwendung die betreffenden Datendateien nach einem Rollback möglicherweise nicht mehr lesen.

Subvolumes mit einer Mischung aus Code und Daten

Subvolumes wie `/srv` können eine Mischung aus Code und Daten enthalten. Bei einem Rollback entsteht dabei möglicherweise nicht funktionsfähiger Code. Ein Downgrade der PHP-Version kann beispielsweise zu fehlerhaften PHP-Skripten für den Webserver führen.

Benutzerdaten

Wenn bei einem Rollback bestimmte Benutzer aus dem System entfernt werden, so werden die Daten im Eigentum dieser Benutzer in Verzeichnissen, die vom Snapshot ausgeschlossen sind, nicht entfernt. Wenn ein Benutzer mit derselben Benutzer-ID erstellt wird, würde dieser neue Benutzer die Dateien erben. Suchen und entfernen Sie bezuglose (verwaiste) Dateien mit einem Werkzeug wie **`find`**.

7.3.3.2 Kein Rollback der Bootloader-Daten

Ein Rollback des Bootloaders ist nicht möglich, da alle „Stufen“ des Bootloaders zusammenpassen müssen. Dies kann bei einem Rollback von `/boot` nicht gewährleistet werden.

7.4 Erstellen und Bearbeiten von Snapper-Konfigurationen

Das Verhalten von Snapper ist in je einer Konfigurationsdatei pro Partition und `Btrfs`-Subvolume definiert. Diese Konfigurationsdateien sind unter `/etc/snapper/configs/` gespeichert.

Falls das Root-Dateisystem groß genug ist (etwa 12 GB), werden bei der Installation Snapshots automatisch für das Root-Dateisystem `/` aktiviert. Die entsprechende Standardkonfiguration hat den Namen `root`. Mit ihr werden die YaST- und Zypper-Snapshots erstellt und verwaltet. Eine Liste der Standardwerte finden Sie im *Abschnitt 7.4.1.1, „Konfigurationsdaten“*.

Anmerkung: Erforderliche Mindestgröße des Root-Dateisystems für Snapshots

Wie unter *Abschnitt 7.1, „Standardeinrichtung“* erläutert, belegen Snapshots zusätzlichen freien Speicherplatz im Root-Dateisystem. Die tatsächliche Menge ist abhängig von der Anzahl der installierten Pakete und der Anzahl der Änderungen am Volume, das in den Snapshots berücksichtigt wird. Auch die Snapshot-Häufigkeit und die Anzahl der archivierten Snapshots spielen eine Rolle.

Es ist eine bestimmte Mindestgröße des Dateisystems erforderlich, damit Snapshots während der Installation automatisch aktiviert werden können. Die Größe beträgt etwa 12 GB. Dieser Wert kann sich in Zukunft durchaus ändern, je nach der Architektur und der Größe des Basissystems. Dieser Wert ist abhängig vom Wert der folgenden Tags in der Datei `/control.xml` auf den Installationsmedien:

```
<root_base_size>
<btrfs_increase_percentage>
```

Die Berechnung erfolgt nach der folgenden Formel: *`ROOT_BASISGRÖSSE`* * (1 + *`PROZENTSATZ_FÜR_BTRFS_ZUWACHS`*/100)

Denken Sie daran, dass dieser Wert lediglich die Mindestgröße angibt. Stellen Sie ggf. mehr Speicherplatz für das Root-Dateisystem bereit. Als Faustregel sollten Sie die Größe, die ohne aktivierte Snapshots gelten würde, verdoppeln.

Sie können eigene Konfigurationen für andere, mit `Btrfs` formatierte Partitionen sowie für vorhandene Subvolumes auf einer `Btrfs`-Partition erstellen. Im nachfolgenden Beispiel wird eine Snapper-Konfiguration zum Sichern der Webserverdaten eingerichtet, die sich auf einer separaten, mit `Btrfs` formatierten, unter `/srv/www` eingehängten Partition befinden.

Nach dem Erstellen einer Konfiguration können Sie Dateien aus diesen Snapshots wahlweise mit **`snapper`** selbst oder mit dem *Snapper*-Modul in YaST wiederherstellen. In YaST wählen Sie die *Aktuelle Konfiguration* aus, wobei Sie die Konfiguration für **`snapper`** mit dem globalen Schalter `-c` angeben (z. B. **`snapper -c myconfig list`**).

Zum Erstellen einer neuen Snapper-Konfiguration führen Sie **`snapper create-config`** aus:

```
tux > sudo snapper -c www-data❶ create-config /srv/www❷
```

❶ Der Name der Konfigurationsdatei.

❷ Einhängepunkt der Partition oder des `Btrfs`-Subvolumes, für das die Snapshots angefertigt werden sollen.

Mit diesem Kommando erstellen Sie eine neue Konfigurationdsdatei `/etc/snapper/configs/www-data` mit geeigneten Standardwerten (aus `/etc/snapper/config-templates/default` übernommen). Anweisungen zum Anpassen dieser Standardwerte finden Sie in *Abschnitt 7.4.1, „Verwalten vorhandener Konfigurationen“*.

Tipp: Standardwerte für die Konfiguration

Die Standardwerte für eine neue Konfiguration werden aus `/etc/snapper/config-templates/default` übernommen. Sollen eigene Standardwerte verwendet werden, erstellen Sie eine Kopie dieser Datei in demselben Verzeichnis, und passen Sie diese Kopie gemäß Ihren Anforderungen an. Geben Sie dann die Option `-t` option für das Kommando create-config an:

```
tux > sudo snapper -c www-data create-config -t MY_DEFAULTS /srv/www
```

7.4.1 Verwalten vorhandener Konfigurationen

Das Kommando **snapper** bietet verschiedene Subkommandos für die Verwaltung von vorhandenen Konfigurationen. Sie können sie auflisten, anzeigen, löschen und bearbeiten:

Auflisten von Konfigurationen

Mit dem Kommando **snapper list-configs** rufen Sie alle vorhandenen Konfigurationen ab:

```
tux > sudo snapper list-configs
Config | Subvolume
-------+----------
root   | /
usr    | /usr
local  | /local
```

Anzeigen einer Konfiguration

Mit dem Subkommando **snapper -c** *KONFIG* **get-config** zeigen Sie die angegebene Konfiguration an. Ersetzen Sie *KONFIG* dabei durch den Namen einer Konfiguration, die mit **snapper list-configs** aufgeführt wird. Weitere Informationen zu den Konfigurationsoptionen finden Sie in *Abschnitt 7.4.1.1, „Konfigurationsdaten“*.

Zum Anzeigen der Standardkonfiguration führen Sie das folgende Kommando aus:

```
tux > sudo snapper -c root get-config
```

Bearbeiten einer Konfiguration

Mit dem Subkommando **snapper -c** *KONFIG* **set-config** *OPTION=WERT* bearbeiten Sie eine Option in der angegebenen Konfiguration. Ersetzen Sie *KONFIG* dabei durch den Namen einer Konfiguration, die mit **snapper list-configs** aufgeführt wird. Eine Liste der möglichen Werte für *OPTION* and *WERT* finden Sie in *Abschnitt 7.4.1.1, „Konfigurationsdaten“*.

Löschen einer Konfiguration

Mit dem Subkommando **snapper -c** *KONFIG* delete-config löschen Sie eine Konfiguration. Ersetzen Sie *KONFIG* dabei durch den Namen einer Konfiguration, die mit **snapper list-configs** aufgeführt wird.

7.4.1.1 Konfigurationsdaten

Jede Konfiguration enthält eine Liste von Optionen, die über die Kommandozeile bearbeitet werden können. Die folgende Liste zeigt weitere Details zu den einzelnen Optionen. Um einen Wert zu ändern, führen Sie das Kommando **`snapper -c`** *KONFIG* **`set-config "`***SCHLÜSSEL=WERT***`"`** aus.

`ALLOW_GROUPS`, `ALLOW_USERS`

Erteilt regulären Benutzern die erforderlichen Berechtigungen zum Verwenden von Snapshots. Weitere Informationen finden Sie in *Abschnitt 7.4.1.2, „Verwenden von Snapper als normaler Benutzer“*.

Der Standardwert ist `""`.

`BACKGROUND_COMPARISON`

Legt fest, ob Pre- und Post-Snapshots nach dem Erstellen im Hintergrund miteinander verglichen werden sollen.

Der Standardwert lautet `"yes"`.

`EMPTY_*`

Definiert den Bereinigungsalgorithmus für Snapshot-Paare mit identischen Pre- und Post-Snapshots. Weitere Informationen finden Sie im *Abschnitt 7.6.3, „Bereinigen von Snapshot-Paaren, die sich nicht unterscheiden“*.

`FSTYPE`

Dateisystemtyp der Partition. Bearbeiten Sie diese Datei nicht.

Der Standardwert lautet `„btrfs“`.

NUMBER_*

Definiert den Bereinigungsalgorithmus für Installations- und Verwaltungs-Snapshots. Weitere Informationen finden Sie im *Abschnitt 7.6.1, „Bereinigen von nummerierten Snapshots“*.

`QGROUP` / `SPACE_LIMIT`

Fügt Quotenunterstützung zu Bereinigungs-Algorithmen hinzu. Weitere Informationen finden Sie im *Abschnitt 7.6.5, „Hinzufügen von Festplattenquotenunterstützung“*.

`SUBVOLUME`

Einhängepunkt für die Partition oder das Subvolume am Snapshot. Bearbeiten Sie diese Datei nicht.

Der Standardwert ist `"/"`.

`SYNC_ACL`

Wenn Snapper von regulären Benutzern verwendet wird (siehe *Abschnitt 7.4.1.2, „Verwenden von Snapper als normaler Benutzer“*), müssen die Benutzer auf die Verzeichnisse `.snapshot` zugreifen und Dateien in diesen Verzeichnissen lesen können. Wenn SYNC_ACL auf `yes` (ja) gesetzt ist, macht Snapper die betreffenden Verzeichnisse automatisch mithilfe von ACLs für die Benutzer und Gruppen zugänglich, die in den Einträgen ALLOW_USERS oder ALLOW_GROUPS angegeben sind.

Der Standardwert lautet `„no“` (nein).

`TIMELINE_CREATE`

Bei `yes` (ja) werden stündliche Snapshots erstellt. Gültige Werte: `yes`, `no`.

Der Standardwert lautet `„no“` (nein).

`TIMELINE_CLEANUP` / `TIMELINE_LIMIT_*`

Definiert den Bereinigungsalgorithmus für Zeitleisten-Snapshots. Weitere Informationen finden Sie im *Abschnitt 7.6.2, „Bereinigen von Zeitleisten-Snapshots“*.

7.4.1.2 Verwenden von Snapper als normaler Benutzer

Standardmäßig kann Snapper nur von `root` verwendet werden. Unter Umständen müssen jedoch bestimmte Gruppen oder Benutzer in der Lage sein, Snapshots zu erstellen oder Änderungen durch Wiederherstellen eines Snapshots rückgängig zu machen:

- Website-Administratoren, die Snapshots von `/srv/www` anfertigen möchten
- Benutzer, die einen Snapshot von ihrem Home-Verzeichnis anfertigen möchten

Für diese Zwecke können Sie Snapper-Konfigurationen erstellen, in denen Benutzern und/oder Gruppen Berechtigungen gewährt werden. Die Benutzer müssen in der Lage sein, das zugehörige Verzeichnis `.snapshots` zu lesen und darauf zuzugreifen. Am einfachsten erreichen Sie dies, wenn Sie die Option SYNC_ACL auf `yes` (ja) einstellen.

PROZEDUR 7.5 ERMÖGLICHEN DER VERWENDUNG VON SNAPPER FÜR NORMALE BENUTZER

Beachten Sie, dass alle Schritte in diesem Verfahren von `root` ausgeführt werden müssen.

1. Erstellen Sie eine Snapper-Konfiguration für die Partition oder das Subvolume, auf dem der Benutzer Snapper verwenden soll (falls noch nicht vorhanden). Weitere Anweisungen finden Sie unter *Abschnitt 7.4, „Erstellen und Bearbeiten von Snapper-Konfigurationen“*. Beispiel:

   ```
   tux > sudo snapper --config web_data create /srv/www
   ```

2. Die Konfigurationsdatei wird unter `/etc/snapper/configs/CONFIG` angelegt, wobei CONFIG dem Wert entspricht, den Sie im vorherigen Schritt mit `-c/--config` angegeben haben (beispielsweise `/etc/snapper/configs/webdaten`). Nehmen Sie die gewünschten Anpassungen vor (Details finden Sie unter *Abschnitt 7.4.1, „Verwalten vorhandener Konfigurationen“*).

3. Legen Sie Werte für `ALLOW_USERS` und/oder `ALLOW_GROUPS` fest. Damit gewähren Sie bestimmten Benutzern bzw. Gruppen die Berechtigungen. Mehrere Einträge müssen mit `Leertaste` getrennt werden. Um beispielsweise dem Benutzer `www_admin` Berechtigungen zu gewähren, führen Sie Folgendes aus:

```
tux > sudo snapper -c web_data set-config "ALLOW_USERS=www_admin" SYNC_ACL="yes"
```

4. Die vorhandene Snapper-Konfiguration kann nunmehr durch den oder die angegebenen Benutzer und/oder Gruppen verwendet werden. Testen Sie dies beispielsweise mit dem Kommando `list`:

```
www_admin:~ > snapper -c web_data list
```

7.5 Manuelles Erstellen und Verwalten von Snapshots

Snapper ist nicht auf das automatische Erstellen und Verwalten von Snapshots über eine Konfiguration beschränkt. Mit dem Kommandozeilenwerkzeug oder dem YaST-Modul können Sie auch selbst Snapshot-Paare („vorher/nachher“) oder einzelne Snapshots manuell erstellen.

Alle Snapper-Vorgänge werden für eine vorhandene Konfiguration ausgeführt (weitere Details finden Sie unter *Abschnitt 7.4, „Erstellen und Bearbeiten von Snapper-Konfigurationen“*). Sie können Snapshots nur für Partitionen oder Volumes erstellen, für die eine Konfiguration vorhanden ist. Standardmäßig wird die Systemkonfiguration (`root`) verwendet. Wenn Sie Snapshots für Ihre eigene Konfiguration erstellen oder verwalten möchten, müssen Sie diese Konfiguration explizit auswählen. Verwenden Sie das Dropdown-Feld *Aktuelle Konfiguration* in YaST oder geben Sie den Schalter `-c` in der Kommandozeile an (**`snapper -c`** *`MEINE_KONF KOMMANDO`*).

7.5.1 Snapshot-Metadaten

Ein Snapshot besteht jeweils aus dem Snapshot selbst und aus einigen Metadaten. Beim Erstellen eines Snapshots müssen Sie auch die Metadaten angeben. Wenn Sie einen Snapshot bearbeiten, so ändern Sie die Metadaten – der Inhalt selbst kann nicht bearbeitet werden. Verwenden Sie das Kommando **`snapper list`**, um die vorhandenen Snapshots und ihre Metadaten anzuzeigen:

`snapper --config home list`
: Listet Snapshots für die Konfiguration `home` auf. Um Snapshots für die Standardkonfiguration (root) aufzulisten, verwenden Sie **`snapper -c root list`** oder **`snapper list`**.

`snapper list -a`
: Listet Snapshots für alle vorhandenen Konfigurationen auf.

`snapper list -t pre-post`
: Listet alle Pre- und Post-Snapshot-Paare für die Standardkonfiguration (`root`) auf.

`snapper list -t single`
: Listet alle Snapshots des Typs `single` für die Standardkonfiguration (`root`) auf.

Die folgenden Metadaten sind für jeden Snapshot verfügbar:

- **Typ**: Snapshot-Typ; Details siehe *Abschnitt 7.5.1.1, „Snapshot-Typen“*. Diese Daten können nicht geändert werden.
- **Nummer:** Eindeutige Nummer des Snapshots. Diese Daten können nicht geändert werden.
- **Pre Number (Pre-Nummer):** Nummer des zugehörigen Pre-Snapshots. Nur für Snapshots vom Post-Typ. Diese Daten können nicht geändert werden.
- **Beschreibung:** Beschreibung des Snapshots.
- **Benutzerdaten:** Erweiterte Beschreibung, in der Sie benutzerdefinierte Daten als kommagetrennte Liste im Format Schlüssel=Wert angeben können, beispielsweise `reason=testing, project=foo`. Mit diesem Feld wird außerdem ein Snapshot als wichtig gekennzeichnet (`important=yes`), und der Benutzer, der den Snapshot erstellt hat, wird hier aufgeführt (user=tux).
- **Bereinigungsalgorithmus**: Bereinigungsalgorithmus für den Snapshot; Details siehe *Abschnitt 7.6, „Automatisches Bereinigen von Snapshots“*.

7.5.1.1 Snapshot-Typen

In Snapper gibt es drei Typen von Snapshots: pre, post und einzeln. Physisch unterscheiden sie sich nicht, sie werden jedoch in Snapper unterschiedlich behandelt.

`Pre`

Snapshot eines Dateisystems *vor* einer Änderung. Zu jedem `Pre`-Snapshot gibt es einen zugehörigen `Post`-Snapshot. Verwendung z. B. für die automatischen YaST-/Zypper-Snapshots.

`Post`

Snapshot eines Dateisystems *nach* einer Änderung. Zu jedem `Post`-Snapshot gibt es einen zugehörigen `Pre`-Snapshot. Verwendung z. B. für die automatischen YaST-/Zypper-Snapshots.

`Einzeln`

Eigenständiger Snapshot. Verwendung z. B. für die automatischen stündlichen Snapshots. Dies ist der Standardtyp beim Erstellen von Snapshots.

7.5.1.2 Bereinigungsalgorithmen

Snapper bietet drei Algorithmen zum Bereinigen alter Snapshots. Die Algorithmen werden im Rahmen eines täglichen CRON-Auftrags ausgeführt. Sie können die Anzahl der verschiedenen Typen von Snapshots definieren, die in der Snapper-Konfiguration aufbewahrt werden sollen (siehe *Abschnitt 7.4.1, „Verwalten vorhandener Konfigurationen“*).

Zahl

Löscht alte Snapshots, sobald eine bestimmte Anzahl von Snapshots erreicht wird.

timeline (Zeitleiste)

Löscht Snapshots, die ein bestimmtes Alter erreicht haben; hierbei werden allerdings mehrere stündliche, tägliche, monatliche und jährliche Snapshots beibehalten.

empty-pre-post (Leer-Pre-Post)

Löscht Pre-/Post-Snapshot-Paare, zwischen denen keine Unterschiede (Diffs) bestehen.

7.5.2 Erstellen von Snapshots

Zum Erstellen eines Snapshots führen Sie `snapper create` aus, oder klicken Sie im *Snapper*-Modul in YaST auf *Erstellen*. In den nachfolgenden Beispielen wird erläutert, wie Sie Snapshots über die Kommandozeile erstellen. Die Anpassung ist über die YaST-Oberfläche ganz einfach.

Tipp: Snapshot-Beschreibung

Geben Sie stets eine aussagekräftige Beschreibung an, mit der der Zweck des Snapshots auch später noch eindeutig erkennbar ist. Über die Option für die Benutzerdaten können Sie noch mehr Informationen festlegen.

`snapper create --description "Snapshot für Woche 2 2014"`

Erstellt einen eigenständigen Snapshot (Einzeltyp) für die Standardkonfiguration (`root`) mit einer Beschreibung. Da kein Bereinigungsalgorithmus angegeben ist, wird der Snapshot nicht automatisch gelöscht.

`snapper --config home create --description "Bereinigung in ~tux"`

Erstellt einen eigenständigen Snapshot (Einzeltyp) für die benutzerdefinierte Konfiguration (`home`) mit einer Beschreibung. Da kein Bereinigungsalgorithmus angegeben ist, wird der Snapshot nicht automatisch gelöscht.

`snapper --config home create --description "Tägliche Datensicherung" --cleanup-algorithm timeline`>

Erstellt einen eigenständigen Snapshot (Einzeltyp) für die benutzerdefinierte Konfiguration (`home`) mit einer Beschreibung. Die Datei wird automatisch gelöscht, sobald die Kriterien für den Zeitleisten-Bereinigungsalgorithmus in der Konfiguration erfüllt sind.

`snapper create --type pre--print-number--description "Vor Apache-Konfigurationsbereinigung"--userdata "important=yes"`

Erstellt einen Snapshot vom `Pre`-Typ und gibt die Snapshot-Nummer aus. Erstes Kommando zum Erstellen eines Snapshot-Paars, mit dem der „Vorher“-/„Nachher“-Zustand festgehalten wird. Der Snapshot wird als wichtig gekennzeichnet.

`snapper create --type post--pre-number 30--description "Nach der Apache-Konfigurationsbereinigung"--userdata "important=yes"`

Erstellt einen Snapshot vom `Post`-Typ, gepaart mit der `Pre`-Snapshot-Nummer `30`. Zweites Kommando zum Erstellen eines Snapshot-Paars, mit dem der „Vorher“-/„Nachher“-Zustand festgehalten wird. Der Snapshot wird als wichtig gekennzeichnet.

snapper create --command *KOMMANDO* **--description "Vor und nach KOMMANDO"**

Erstellt automatisch ein Snapshot-Paar vor und nach dem Ausführen von *KOMMANDO*. Diese Option ist nur verfügbar, wenn Snapper in der Kommandozeile verwendet wird.

7.5.3 Bearbeiten von Snapshot-Metadaten

Bei Snapper können Sie die Beschreibung, den Bereinigungsalgorithmus und die Benutzerdaten eines Snapshots bearbeiten. Alle anderen Metadaten können nicht geändert werden. In den nachfolgenden Beispielen wird erläutert, wie Sie Snapshots über die Kommandozeile bearbeiten. Die Anpassung ist über die YaST-Oberfläche ganz einfach.

Um einen Snapshot in der Kommandozeile zu bearbeiten, müssen Sie seine Nummer kennen. Mit **snapper list** rufen Sie alle Snapshots mit den dazugehörigen Nummern ab.

Im *Snapper*-Modul in YaST werden bereits alle Snapshots aufgelistet. Wählen Sie einen Eintrag in der Liste, und klicken Sie auf *Bearbeiten*.

snapper modify --cleanup-algorithm "timeline" 10

Bearbeitet die Metadaten von Snapshot 10 für die Standardkonfiguration (`root`). Der Bereinigungsalgorithmus ist mit `Zeitleiste` festgelegt.

snapper --config home modify --description "Tägliche Sicherung" -cleanup-algorithm "timeline" 120

Bearbeitet die Metadaten von Snapshot 120 für die benutzerdefinierte Konfiguration `home`. Eine neue Beschreibung wird festgelegt, und der Bereinigungsalgorithmus wird aufgehoben.

7.5.4 Löschen von Snapshots

Zum Löschen eines Snapshots mit dem *Snapper*-Modul in YaST wählen Sie den gewünschten Snapshot in der Liste aus, und klicken Sie auf *Löschen*.

Um einen Snapshot mit dem Kommandozeilenwerkzeug zu löschen, müssen Sie seine Nummer kennen. Führen Sie hierzu **snapper list** aus. Zum Löschen eines Snapshots führen Sie **snapper delete** *NUMBER* aus.

Der Snapshot des aktuellen Standard-Subvolumes darf nicht gelöscht werden.

Wenn Sie Snapshots mit Snapper löschen, wird der freigegebene Speicherplatz von einem Btrfs-Prozess in Anspruch genommen, der im Hintergrund ausgeführt wird. Der freie Speicherplatz wird daher erst mit Verzögerung sichtbar und verfügbar. Wenn der Speicherplatz, der durch Löschen eines Snapshots freigegeben wurde, sofort zur Verfügung stehen soll, ergänzen Sie den Löschbefehl mit der Option `--sync`.

Tipp: Löschen von Snapshot-Paaren

Wenn Sie einen `Pre`-Snapshot löschen, müssen Sie auch den zugehörigen `Post`-Snapshot löschen (und umgekehrt).

`snapper delete 65`

Löscht Snapshot 65 für die Standardkonfiguration (`root`).

`snapper -c home delete 89 90`

Löscht Snapshots 89 und 90 für die benutzerdefinierte Konfiguration `home`.

`snapper delete --sync 23`

Löscht Snapshot 23 für die Standardkonfiguration (`root`) und stellt den freigegebenen Speicherplatz sofort zur Verfügung.

Tipp: Löschen nicht referenzierter Snapshots

In bestimmten Fällen ist zwar der Btrfs-Snapshot vorhanden, die XML-Datei mit den Metadaten für Snapper fehlt jedoch. Der Snapshot ist daher nicht für Snapper sichtbar, muss also manuell gelöscht werden:

```
btrfs subvolume delete /.snapshots/SNAPSHOTNUMBER/snapshot
rm -rf /.snapshots/SNAPSHOTNUMBER
```

Tipp: Alte Snapshots belegen mehr Speicherplatz

Wenn Sie Snapshots löschen, um Speicherplatz auf der Festplatte freizugeben, löschen Sie zuerst die älteren Snapshots. Je älter ein Snapshot ist, desto mehr Speicherplatz belegt er.

Snapshots werden außerdem im Rahmen eines täglichen CRON-Auftrags automatisch gelöscht. Weitere Informationen finden Sie unter *Abschnitt 7.5.1.2, „Bereinigungsalgorithmen“*.

7.6 Automatisches Bereinigen von Snapshots

Snapshots belegen Speicherplatz und mit der Zeit kann der von Snapshots belegte Speicherplatz groß werden. Damit Festplatten nicht zu wenig Speicherplatz haben, bietet Snapper einen Algorithmus, mit dem alte Snapshots automatisch gelöscht werden. Diese Algorithmen unterscheiden zwischen Zeitleisten-Snapshots und nummerierten Snapshots (Verwaltungs- plus Installations-Snapshot-Paare). Sie können die Anzahl der Snapshots angeben, die für jeden Typ beibehalten werden soll.

Zusätzlich dazu können Sie optional eine Speicherplatzquote angeben, mit der die maximale Größe des Speicherplatzes festgelegt wird, die Snapshots belegen können. Es ist auch möglich, Pre- und Post-Snapshot-Paare, die sich nicht unterscheiden, automatisch zu löschen.

Ein Bereinigungsalgorithmus ist immer an eine einzelne Snapper-Konfiguration gebunden, daher müssen Sie Algorithmen für jede Konfiguration festlegen. Weitere Informationen, wie das versehentliche Löschen bestimmter Snapshots verhindert wird, finden Sie unter *F:*.

Die Standardeinrichtung (`root`) ist so konfiguriert, dass nummerierte Snapshots und leere Pre- und Post-Snapshot-Paare bereinigt werden. Die Quotenunterstützung ist aktiviert. Snapshots dürfen nicht mehr als 50 % des verfügbaren Speicherplatzes der Root-Partition belegen. Zeitleisten-Snapshots sind standardmäßig deaktiviert. Daher ist der Bereinigungsalgorithmus auch deaktiviert.

7.6.1 Bereinigen von nummerierten Snapshots

Das Bereinigen nummerierter Snapshots – Verwaltungs- plus Installations-Snapshot-Paare – wird von den nachfolgenden Parametern einer Snapper-Konfiguration gesteuert.

`NUMBER_CLEANUP`

Aktiviert oder deaktiviert die Bereinigung von Installations- und Verwaltungs-Snapshot-Paaren. Ist die Option aktiviert, werden Snapshot-Paare gelöscht, wenn die Gesamtzahl der Snapshots eine Zahl überschreitet, die mit `NUMBER_LIMIT` und/oder `NUMBER_LIMIT_IMPORTANT` *festgelegt ist, und* wenn sie ein Alter überschreiten, das mit `NUMBER_MIN_AGE` definiert ist. Gültige Werte: `yes` (aktivieren), `no` (deaktivieren).

Der Standardwert lautet `"yes"`.

Beispielkommando zum Ändern oder Festlegen:

```
tux > sudo snapper -c CONFIG set-config "NUMBER_CLEANUP=no"
```

`NUMBER_LIMIT` / `NUMBER_LIMIT_IMPORTANT`

Definiert, wie viele normale und/oder wichtige Installations- und Administrations-Snapshot-Paare beibehalten werden sollen. Nur die jeweils jüngsten Snapshots werden beibehalten. Wird ignoriert, wenn für `NUMBER_CLEANUP` der Wert `"no"` festgelegt ist.

Der Standardwert ist `"2-10"` für `NUMBER_LIMIT` und `"4-10"` für `NUMBER_LIMIT_IMPORTANT`.

Beispielkommando zum Ändern oder Festlegen:

```
tux > sudo snapper -c CONFIG set-config "NUMBER_LIMIT=10"
```

Wichtig: Bereichswerte im Vergleich zu Fixwerten

Falls die Quotenunterstützung aktiviert ist (siehe *Abschnitt 7.6.5, „Hinzufügen von Festplattenquotenunterstützung“*), muss der Grenzwert als Minimum-Maximum-Bereich angegeben sein, z. B. `2-10`. Wenn die Quotenunterstützung deaktiviert ist, muss ein Fixwert, z. B. `10`, angegeben werden, sonst schlägt das Bereinigen fehl.

`NUMBER_MIN_AGE`

Definiert das Mindestalter in Sekunden, das ein Snapshot aufweisen soll, bevor er automatisch gelöscht werden kann. Snapshots, die jünger als der hier angegebene Wert sind, werden, unabhängig davon, wie viele vorhanden sind, nicht gelöscht.

Der Standardwert lautet `"1800"`.

Beispielkommando zum Ändern oder Festlegen:

```
tux > sudo snapper -c CONFIG set-config "NUMBER_MIN_AGE=864000"
```

Anmerkung: Grenzwert und Alter

`NUMBER_LIMIT`, `NUMBER_LIMIT_IMPORTANT` und `NUMBER_MIN_AGE` werden stets ausgewertet. Die Snapshots werden nur dann gelöscht, wenn *alle* Bedingungen erfüllt sind.

Wenn Sie immer die mit `NUMBER_LIMIT*` festgelegte Anzahl an Snapshots beibehalten möchten, unabhängig von ihrem Alter, legen Sie für `NUMBER_MIN_AGE` den Wert `0` fest.

Das folgende Beispiel zeigt eine Konfiguration, mit der die letzten zehn wichtigen und regulären Snapshots unabhängig vom Alter beibehalten werden:

```
NUMBER_CLEANUP=yes
NUMBER_LIMIT_IMPORTANT=10
NUMBER_LIMIT=10
```

```
NUMBER_MIN_AGE=0
```

Wenn Sie andererseits keine Snapshots beibehalten möchten, die ein bestimmtes Alter überschreiten, legen Sie für `NUMBER_LIMIT*` den Wert `0` fest und geben Sie das Alter mit `NUMBER_MIN_AGE` an.

Das folgende Beispiel zeigt eine Konfiguration, in der lediglich Snapshots beibehalten werden, die jünger als zehn Tage sind:

```
NUMBER_CLEANUP=yes
NUMBER_LIMIT_IMPORTANT=0
NUMBER_LIMIT=0
NUMBER_MIN_AGE=864000
```

7.6.2 Bereinigen von Zeitleisten-Snapshots

Das Bereinigen von Zeitleisten-Snapshots wird von den nachfolgenden Parametern einer Snapper-Konfiguration gesteuert.

`TIMELINE_CLEANUP`

Aktiviert oder deaktiviert die Bereinigung von Zeitleisten-Snapshots. Ist der Parameter aktiviert, werden Snapshots gelöscht, wenn die Gesamtanzahl der Snapshots eine mit `TIMELINE_LIMIT_*` *angegebene Zahl und* ein mit `TIMELINE_MIN_AGE` angegebenes Alter überschreiten. Gültige Werte: `yes`, `no`.

Der Standardwert lautet `"yes"`.

Beispielkommando zum Ändern oder Festlegen:

```
tux > sudo snapper -c CONFIG set-config "TIMELINE_CLEANUP=yes"
```

`TIMELINE_LIMIT_DAILY`, `TIMELINE_LIMIT_HOURLY`, `TIMELINE_LIMIT_MONTHLY`, `TIMELINE_LIMIT_WEEKLY`, `TIMELINE_LIMIT_YEARLY`

Anzahl der Snapshots, die pro Stunde, Tag, Monat, Woche und Jahr beibehalten werden sollen.

Der Standardwert für jeden Eintrag ist `"10"`, außer für `TIMELINE_LIMIT_WEEKLY`, hier ist der Standardwert `"0"`.

`TIMELINE_MIN_AGE`

Definiert das Mindestalter in Sekunden, das ein Snapshot aufweisen soll, bevor er automatisch gelöscht werden kann.

Der Standardwert lautet „1800“.

BEISPIEL 7.1 BEISPIEL FÜR EINE ZEITLEISTEN-KONFIGURATION

```
TIMELINE_CLEANUP="yes"
TIMELINE_CREATE="yes"
TIMELINE_LIMIT_DAILY="7"
TIMELINE_LIMIT_HOURLY="24"
TIMELINE_LIMIT_MONTHLY="12"
TIMELINE_LIMIT_WEEKLY="4"
TIMELINE_LIMIT_YEARLY="2"
TIMELINE_MIN_AGE="1800"
```

In dieser Beispielkonfiguration werden stündliche Snapshots vorgenommen, die automatisch bereinigt werden. `TIMELINE_MIN_AGE` und `TIMELINE_LIMIT_*` werden stets gemeinsam ausgewertet. In diesem Beispiel ist das Mindestalter eines Snapshots, ab dem er gelöscht werden kann, auf 30 Minuten (1800 Sekunden) eingestellt. Durch die stündliche Erstellung der Snapshots werden nur die jeweils neuesten Snapshots beibehalten. Wenn `TIMELINE_LIMIT_DAILY` auf einen Wert ungleich null gesetzt ist, wid auch der erste Snapshot des Tages beibehalten.

BEIZUBEHALTENDE SNAPSHOTS

- Stündlich: Die letzten 24 angefertigten Snapshots.
- Täglich: Jeweils der erste Snapshot, der zu Tagesbeginn angefertigt wurde, für die letzten sieben Tage.
- Monatlich: Jeweils der erste Snapshot, der am letzten Tag des Monats angefertigt wurde, für die letzten zwölf Monate.
- Wöchentlich: Jeweils der erste Snapshot, der am letzten Tag der Woche angefertigt wurde, für die letzten vier Wochen.
- Jährlich: Jeweils der erste Snapshot, der am letzten Tag des Jahres angefertigt wurde, für die letzten zwei Jahre.

7.6.3 Bereinigen von Snapshot-Paaren, die sich nicht unterscheiden

Wie in *Abschnitt 7.1.1, „Typen von Snapshots“* erklärt, wird immer beim Ausführen eines YaST-Moduls oder beim Ausführen von Zypper ein Pre-Snapshot beim Starten erstellt und ein Post-Snapshot beim Beenden. Falls Sie keine Änderungen vorgenommen haben, gibt es zwischen

dem Pre- und Post-Snapshot keinen Unterschied. Solche „leeren“ Snapshot-Paare können automatisch gelöscht werden, indem die folgenden Parameter in einer Snapper-Konfiguration festgelegt werden:

`EMPTY_PRE_POST_CLEANUP`

Bei `yes` (ja) werden Snapshot-Paare mit identischem Pre- und Post-Snapshot gelöscht. Der Standardwert lautet `„yes“` (ja).

`EMPTY_PRE_POST_MIN_AGE`

Definiert das Mindestalter in Sekunden, das ein Snapshot-Paar mit identischem Pre- und Post-Snapshot aufweisen soll, bevor es automatisch gelöscht werden kann. Der Standardwert lautet `„1800“`.

7.6.4 Bereinigen manuell erstellter Snapshots

Snapper bietet keine benutzerdefinierten Bereinigungsalgorithmen für manuell erstellte Snapshots. Sie können jedoch den Nummern- oder Zeitleisten-Bereinigungsalgorithmus einem manuell erstellten Snapshot zuweisen. Wenn Sie dies tun, reiht sich der Snapshot in der „Bereinigungswarteschlange“ für den angegebenen Algorithmus ein. Sie können einen Bereinigungsalgorithmus angeben, wenn Sie einen Snapshot erstellen oder indem Sie einen vorhandenen Snapshot bearbeiten:

`snapper create --description "Test" --cleanup-algorithm number`

Erstellt einen eigenständigen Snapshot (Typ: „single“) für die Standardkonfiguration (root) und weist den Bereinigungsalgorithmus `number` zu.

`snapper modify --cleanup-algorithm "timeline" 25`

Ändert den Snapshot mit der Nummer 25 und weist den Bereinigungsalgorithmus `timeline` zu.

7.6.5 Hinzufügen von Festplattenquotenunterstützung

Zusätzlich zu den oben beschriebenen Nummern- und/oder Zeitleisten-Bereinigungsalgorithmen unterstützt Snapper Quoten. Sie können festlegen, welchen prozentualen Anteil des verfügbaren Speicherplatzes Snapshots belegen dürfen. Dieser Prozentwert gilt immer für das Btrfs-Subvolume, das in der entsprechenden Snapper-Konfiguration definiert ist.

Wenn Snapper bei der Installation aktiviert wurde, wird die Quotenunterstützung automatisch aktiviert. Falls Sie Snapper zu einem späteren Zeitpunkt manuell aktivieren, können Sie die Quotenunterstützung aktivieren, indem Sie **`snapper setup-quota`** ausführen. Dies erfordert eine gültige Konfiguration (weitere Informationen finden Sie in *Abschnitt 7.4, „Erstellen und Bearbeiten von Snapper-Konfigurationen“*).

Die Quotenunterstützung wird von den folgenden Parametern der Snapper-Konfiguration gesteuert.

`QGROUP`

Die Btrfs-Quotengruppe, die von Snapper verwendet wird. Ist dies nicht festgelegt, führen Sie **`snapper setup-quota`** aus. Ist dies bereits festgelegt, nehmen Sie nur Änderungen vor, wenn Sie die man-Seite **`man 8 btrfs-qgroup`** kennen. Dieser Wert wird mit **`snapper setup-quota`** festgelegt und sollte nicht geändert werden.

`SPACE_LIMIT`

Grenzwert für den Speicherplatz, den Snapshots belegen dürfen, in Bruchteilen von 1 (1 = 100 %). Gültig sind Werte zwischen 0 und 1 (0.1 = 10 %, 0.2 = 20 % ...).

Es gelten die folgenden Einschränkungen und Richtlinien:

- Quoten werden nur *zusätzlich* zu einem vorhandenen Nummern- und/oder Zeitleisten-Bereinigungsalgorithmus aktiviert. Ist kein Bereinigungsalgorithmus aktiviert, werden keine Quoteneinschränkungen angewendet.
- Ist die Quotenunterstützung aktiviert, führt Snapper bei Bedarf zwei Bereinigungsläufe durch. Im ersten Lauf werden die Regeln angewendet, die für Nummern- und Zeitleisten-Snapshots angegeben sind. Nur, wenn die Quote nach diesem Lauf überschritten wird, werden die quotenspezifischen Regeln in einem zweiten Lauf angewendet.
- Selbst wenn die Quotenunterstützung aktiviert ist, wird die Anzahl der Snapshots, die mit den Werten `NUMBER_LIMIT*` und `TIMELINE_LIMIT*` angegeben ist, von Snapper beibehalten, auch wenn die Quote überschritten wird. Daher wird empfohlen, die Bereichswerte (*`MIN.-MAX.`*) für `NUMBER_LIMIT*` und `TIMELINE_LIMIT*` anzugeben, um sicherzustellen, dass die Quote angewendet werden kann.
  Wenn beispielsweise `NUMBER_LIMIT=5-20` festgelegt ist, führt Snapper einen ersten Bereinigungslauf durch und reduziert die Anzahl normaler Nummern-Snapshots auf 20. Falls diese 20 Snapshots die Quote überschreiten, löscht Snapper die ältesten Snapshots in einem zweiten Lauf, bis die Quote eingehalten wird. Mindestens fünf Snapshots werden immer beibehalten, unabhängig davon, wie viel Speicherplatz sie belegen.

7.7 Häufig gestellte Fragen

F: *Warum zeigt Snapper keine Änderungen in `/var/log`, `/tmp` und anderen Verzeichnissen an?*

A: Einige Verzeichnisse werden aus Snapshots ausgeschlossen. Weitere Informationen und Begründungen finden Sie unter *Abschnitt 7.1.2, „Verzeichnisse, die aus Snapshots ausgenommen sind“*. Sollen für einen Pfad keine Snapshots angefertigt werden, legen Sie ein Subvolume für diesen Pfad an.

F: *Wie viel Speicherplatz belegen die Snapshots? Wie kann ich Speicherplatz freigeben?*

A: Die `Btrfs`-Werkzeuge unterstützen zurzeit noch nicht die Anzeige des Speicherplatzes, der von einem Snapshot belegt wird. Wenn die Quote jedoch aktiviert ist, ist es möglich zu bestimmen, wie viel Speicherplatz frei werden würde, wenn *alle* Snapshots gelöscht würden:

1. Rufen Sie die Quotengruppen-ID ab (`1/0` im folgenden Beispiel):

```
tux > sudo snapper -c root get-config | grep QGROUP
QGROUP                 | 1/0
```

2. Führen Sie erneut einen Scan für die Subvolume-Quoten durch:

```
tux > sudo btrfs quota rescan -w /
```

3. Zeigen Sie die Daten der Quotengruppe an (`1/0` im folgenden Beispiel):

```
tux > sudo btrfs qgroup show / | grep "1/0"
1/0           4.80GiB    108.82MiB
```

   In der dritten Spalte wird der Speicherplatz angezeigt, der frei werden würde, wenn alle Snapshots gelöscht würden (`108.82MiB`).

Um Speicherplatz auf einer `Btrfs`-Partition mit Snapshots freizugeben, müssen Sie keine Dateien löschen, sondern die nicht mehr benötigten Snapshots. Ältere Snapshots belegen mehr Speicherplatz als neuere Snapshots. Weitere Informationen finden Sie in *Abschnitt 7.1.3.4, „Steuern der Snapshot-Archivierung“*.

Wenn Sie eine Aufrüstung von einem Service Pack auf ein höheres Service Pack vornehmen, belegen die entstehenden Snapshots einen großen Teil des Festplattenspeichers auf den System-Subvolumes, da große Mengen an Daten geändert werden (Aktualisierungen

der Pakete). Es wird daher empfohlen, diese Snapshots manuell zu löschen, sobald Sie sie nicht mehr benötigen. Weitere Informationen finden Sie in *Abschnitt 7.5.4, „Löschen von Snapshots“*.

F: *Kann ich einen Snapshot über den Bootloader booten?*

A: Ja. Weitere Informationen finden Sie in *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots“*.

F: *Wie kann ein Snapshot dauerhaft beibehalten werden?*

A: Derzeit bietet Snapper keine Möglichkeit, zu verhindern, dass ein Snapshot manuell gelöscht wird. Jedoch können Sie verhindern, dass Snapshots automatisch durch Bereinigungsalgorithmen gelöscht werden. Manuell erstellten Snapshots (siehe *Abschnitt 7.5.2, „Erstellen von Snapshots“*) ist kein Bereinigungsalgorithmus zugewiesen, es sei denn, Sie geben einen mit `--cleanup-algorithm` an. Automatisch erstellten Snapshots ist immer entweder der `number`- oder `timeline`-Algorithmus zugewiesen. Um auf diese Weise eine Zuweisung für einen oder mehrere Snapshots zu entfernen, gehen Sie wie folgt vor:

1. Auflisten aller verfügbaren Snapshots:

   ```
   tux > sudo snapper list -a
   ```

2. Merken Sie sich die Zahl der Snapshots, deren Löschung Sie verhindern möchten.

3. Führen Sie das folgende Kommando aus und ersetzen Sie die Zahlenplatzhalter durch die Zahl(en), die Sie sich gemerkt haben:

   ```
   tux > sudo snapper modify --cleanup-algorithm "" #1 #2 #n
   ```

4. Überprüfen Sie das Ergebnis, indem Sie erneut **`snapper list -a`** ausführen. Der Eintrag in der Spalte `Cleanup` sollte nun für die bearbeiteten Snapshots leer sein.

F: *Wo finde ich weitere Informationen zu Snapper?*

A: Besuchen Sie die Snapper-Homepage unter http://snapper.io/.

8 Fernzugriff mit VNC

Mit Virtual Network Computing (VNC) können Sie einen Remote-Computer über einen grafischen Desktop steuern (anders als bei einem Remote-Shell-Zugriff). VNC ist plattformunabhängig und ermöglicht Ihnen den Zugriff auf den Remote-Rechner über ein beliebiges Betriebssystem.

SUSE Linux Enterprise Server unterstützt zwei verschiedene Arten von VNC-Sitzungen: einmalige Sitzungen, die so lange „aktiv“ sind, wie die VNC-Verbindung zum Client besteht, und permanente Sitzungen, die so lange „aktiv“ sind, bis sie explizit beendet werden.

Anmerkung: Sitzungstypen

Ein Rechner kann beide Sitzungen gleichzeitig auf verschiedenen Ports bieten, eine geöffnete Sitzung kann jedoch nicht von einem Typ in den anderen konvertiert werden.

8.1 Der **vncviewer**-Client

Um eine Verbindung zu einem VNC-Dienst herzustellen, der von einem Server bereitgestellt wird, ist ein Client erforderlich. Der Standard-Client in SUSE Linux Enterprise Server ist **vncviewer**, der im Paket `tigervnc` bereitgestellt wird.

8.1.1 Verbinden mithilfe der vncviewer-CLI

Mit folgendem Kommando können Sie den VNC-Viewer starten und eine Sitzung mit dem Server initiieren:

```
tux > vncviewer jupiter.example.com:1
```

Anstelle der VNC-Anmeldenummer können Sie auch die Portnummer mit zwei Doppelpunkten angeben:

```
tux > vncviewer jupiter.example.com::5901
```

Anmerkung: Anzeige- und Portnummer

Die im VNC-Client angegebene Anzeige- oder Portnummer muss mit der Anzeige- oder Portnummer übereinstimmen, die durch den Befehl **`vncserver`** auf dem Zielcomputer ausgewählt wird. Weitere Informationen finden Sie unter *Abschnitt 8.4, „Permanente VNC-Sitzungen“*.

8.1.2 Verbinden mithilfe der vncviewer-GUI

Wenn **`vncviewer`** ausgeführt wird, ohne **`--listen`** oder einen Host für die Verbindung anzugeben, wird ein Fenster zur Eingabe von Verbindungsinformationen angezeigt. Geben Sie den Host in das Feld *VNC server* (VNC-Server) wie in *Abschnitt 8.1.1, „Verbinden mithilfe der vncviewer-CLI“* ein und klicken Sie auf *Connect* (Verbinden).

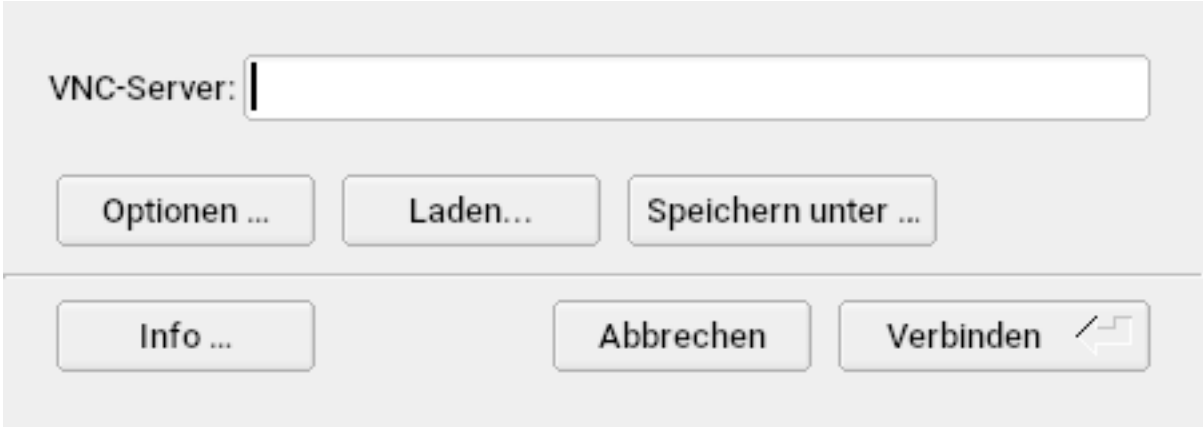


ABBILDUNG 8.1 VNCVIEWER

8.1.3 Benachrichtigungen zu unverschlüsselten Verbindungen

Das VNC-Protokoll unterstützt verschiedene Arten von verschlüsselten Verbindungen, nicht zu verwechseln mit Passwortauthentifizierung. Wenn eine Verbindung kein TLS verwendet, wird der Text „(Connection not encrypted!)“ (Verbindung nicht verschlüsselt!) im Fenstertitel des VNC-Viewers angezeigt.

8.2 Remmina: Remote-Desktop-Client

Der moderne Remote-Desktop-Client Remmina bietet einen großen Funktionsumfang. Es werden mehrere Zugriffsmethoden unterstützt, z. B. VNC, SSH, RDP oder Spice.

8.2.1 Installation

Wenn Sie mit Remmina arbeiten möchten, prüfen Sie, ob das Paket `remmina` auf dem System installiert ist, und holen Sie die Installation ggf. nach. Denken Sie daran, auch das VNC-Plugin für Remmina zu installieren:

```
root # zypper in remmina remmina-plugin-vnc
```

8.2.2 Hauptfenster

Starten Sie Remmina mit dem Befehl **`remmina`**.

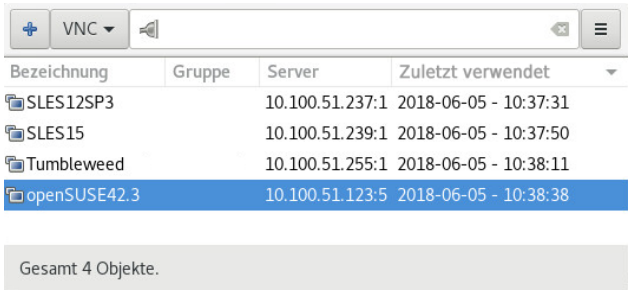


ABBILDUNG 8.2 HAUPTFENSTER VON REMMINA

Das Hauptanwendungsfenster enthält eine Liste der gespeicherten Remote-Sitzungen. Hier können Sie eine neue Remote-Sitzung hinzufügen und speichern, eine neue Sitzung per Schnellstart beginnen (also ohne zu speichern), eine zuvor gespeicherte Sitzung starten oder die globalen Einstellungen für Remmina festlegen.

8.2.3 Hinzufügen von Remote-Sitzungen

Mit oben links im Hauptfenster können Sie eine neue Remote-Sitzung hinzufügen und speichern. Das Fenster *Remote Desktop Preference* wird geöffnet.

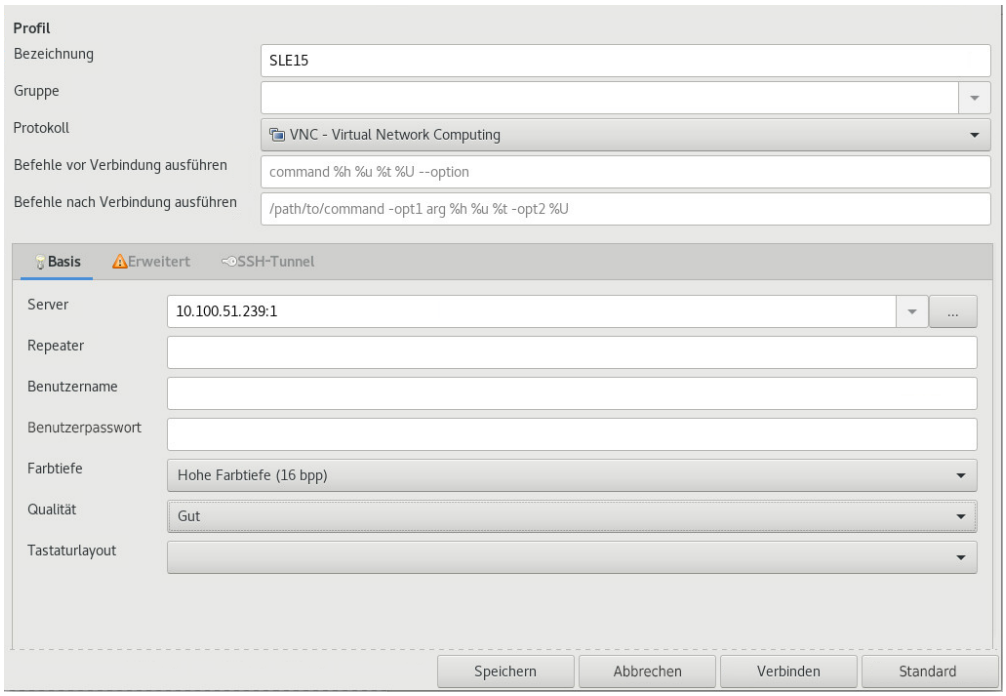


ABBILDUNG 8.3 REMOTE DESKTOP PREFERENCE

Füllen Sie die Felder für das soeben hinzugefügte Remote-Sitzungsprofil aus. Die wichtigsten sind:

Name

Name des Profils. Wird im Hauptfenster angezeigt.

Protokoll

Protokoll für die Verbindung zur Remote-Sitzung, z. B. VNC

Server

IP- oder DNS-Adresse und Anzeigenummer des Remote-Servers.

Benutzername, Benutzerpasswort

Berechtigungsnachweis für die Remote-Authentifizierung. Soll keine Authentifizierung erfolgen, geben Sie hier nichts ein.

Farbtiefe, Qualität

Wählen Sie die optimalen Optionen für Ihre Verbindungsgeschwindigkeit und -qualität.

Auf der Registerkarte *Advanced* finden Sie weitere Einstellungen.

Tipp: Verschlüsselung deaktivieren

Wenn die Kommunikation zwischen dem Client und dem Remote-Server nicht verschlüsselt ist, aktivieren Sie die Option *Disable encryption*. Ansonsten kommt es zu Verbindungsfehlern.

Auf der Registerkarte *SSH* finden Sie erweiterte Optionen für SSH-Tunneling und Authentifizierung.

Bestätigen Sie die Eingabe mit *Speichern*. Das neue Profil wird im Hauptfenster angezeigt.

8.2.4 Starten von Remote-Sitzungen

Sie können entweder eine zuvor gespeicherte Sitzung starten oder eine Remote-Sitzung per Schnellstart beginnen (also ohne die Verbindungsdetails zu speichern).

8.2.4.1 Schnellstart von Remote-Sitzungen

Mit der Dropdown-Box und dem Textfeld oben im Hauptfenster können Sie eine Remote-Sitzung per Schnellstart beginnen, ohne die Verbindungsdetails anzugeben und zu speichern.

ABBILDUNG 8.4 SCHNELLSTART

Wählen Sie das Kommunikationsprotokoll im Dropdown-Feld aus (z. B. „VNC“). Geben Sie dann die DNS-oder IP-Adresse des VNC-Servers ein, gefolgt von einem Doppelpunkt und einer Anzeigenummer, und bestätigen Sie mit `Eingabetaste`.

8.2.4.2 Öffnen von gespeicherten Remote-Sitzungen

Zum Öffnen einer bestimmten Remote-Sitzung doppelklicken Sie in der Sitzungsliste auf diese Sitzung.

8.2.4.3 Fenster der Remote-Sitzungen

Die Remote-Sitzungen werden in Registerkarten eines separaten Fensters geöffnet. Jede Registerkarte enthält eine Sitzung. Über die Symbolleiste links im Fenster können Sie die Fenster/Sitzungen verwalten, zum Beispiel den Vollbildmodus aktivieren/deaktivieren, die Fenstergröße an die Anzeigegröße der Sitzung anpassen, bestimmte Tastatureingaben an die Sitzung senden, Bildschirmfotos der Sitzung aufnehmen oder die Bildqualität festlegen.

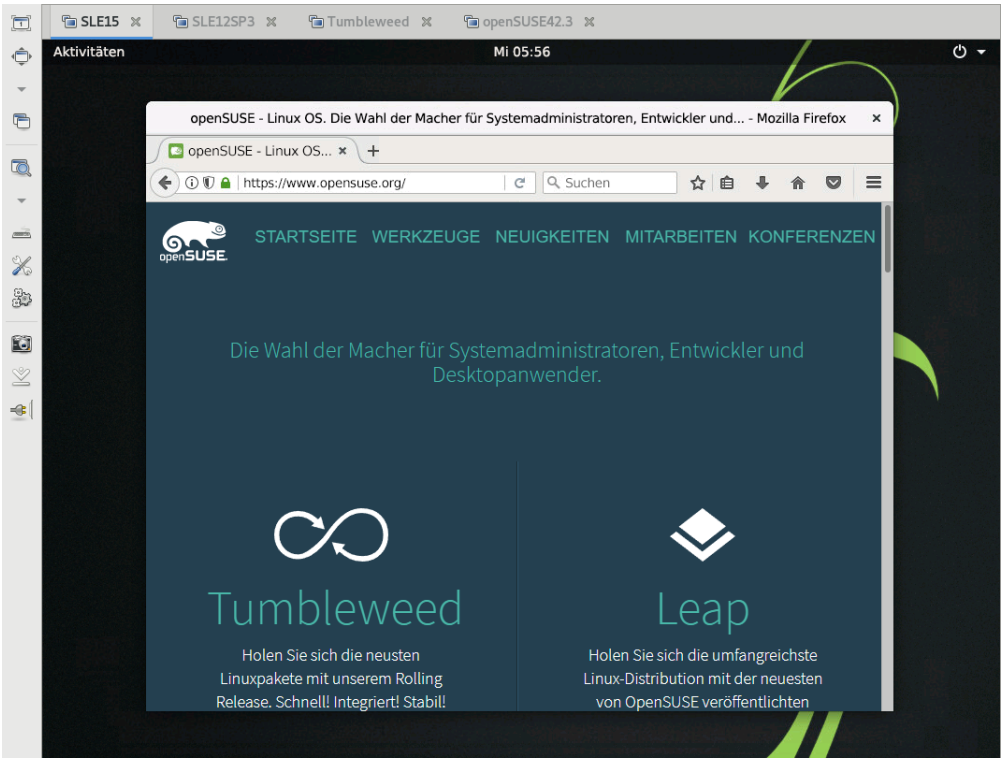


ABBILDUNG 8.5 REMMINA-REMOTE-SITZUNG MIT ANZEIGE VON SLES 15

8.2.5 Bearbeiten, Kopieren und Löschen gespeicherter Sitzungen

Zum *Bearbeiten* einer gespeicherten Remote-Sitzung klicken Sie mit der rechten Maustaste im Hauptfenster von Remmina auf den Namen der Sitzung und wählen Sie *Edit*. Eine Beschreibung der relevanten Felder finden Sie unter *Abschnitt 8.2.3, „Hinzufügen von Remote-Sitzungen“*.

Zum *Kopieren* einer gespeicherten Remote-Sitzung klicken Sie mit der rechten Maustaste im Hauptfenster von Remmina auf den Namen der Sitzung und wählen Sie *Copy*. Ändern Sie im Fenster *Remote Desktop Preference* den Name des Profils, passen Sie optional die relevanten Optionen an und bestätigen Sie mit *Save*.

Zum *Löschen* einer gespeicherten Remote-Sitzung klicken Sie mit der rechten Maustaste im Hauptfenster von Remmina auf den Namen der Sitzung und wählen Sie *Delete*. Bestätigen Sie das nächste Dialogfeld mit *Yes*.

8.2.6 Ausführen von Remote-Sitzungen über die Befehlszeile

Mit der folgenden Syntax öffnen Sie eine Remote-Sitzung über die Befehlszeile oder aus einer Stapeldatei heraus, ohne zunächst das Hauptanwendungsfenster zu öffnen:

```
tux > remmina -c profile_name.remmina
```

Die Profildateien von Remmina werden im Verzeichnis `.local/share/remmina/` in Ihrem Benutzerverzeichnis gespeichert. Zum Ermitteln der Profildatei für die zu öffnende Sitzung starten Sie Remmina und klicken Sie im Hauptfenster auf den Sitzungsnamen. Der Pfad zur Profildatei wird in der Statuszeile unten im Fenster angezeigt.

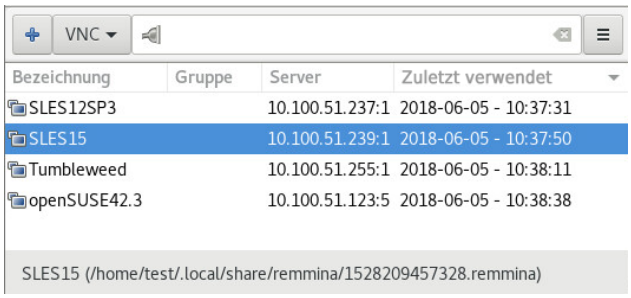


ABBILDUNG 8.6 PFAD ZUR PROFILDATEI

Wenn Remmina nicht ausgeführt wird, können Sie den Namen der Profildatei durch einen aussagekräftigeren Dateinamen ersetzen (z. B. `sle15.remmina`). Sie können sogar die Profildatei in Ihr Benutzerverzeichnis kopieren und mit dem Befehl **`remmina -c`** direkt aus diesem Verzeichnis heraus ausführen.

8.3 Einmalige VNC-Sitzungen

Eine einmalige Sitzung wird vom Remote-Client initiiert. Sie startet einen grafischen Anmeldebildschirm auf dem Server. Auf diese Weise können Sie den Benutzer auswählen, der die Sitzung starten soll sowie, sofern vom Anmeldungsmanager unterstützt, die Desktop-Umgebung. Wenn

Sie die Client-Verbindung, beispielsweise eine VNC-Sitzung, beenden, werden auch alle während der Sitzung gestarteten Anwendungen beendet. Einmalige VNC-Sitzungen können nicht freigegeben werden, Sie können jedoch mehrere Sitzungen gleichzeitig auf demselben Host ausführen.

PROZEDUR 8.1 AKTIVIEREN VON EINMALIGEN VNC-SITZUNGEN

1. Starten Sie *YaST* › *Netzwerkdienste* › *Verwaltung von entfernten Rechnern aus (remote) (VNC)*.
2. Aktivieren Sie die Option *Allow Remote Administration Without Session Management* (Verwaltung von entfernten Rechnern aus (remote) ohne Sitzungsverwaltung zulassen).
3. Aktivieren Sie die Option *Enable access using a web browser* (Zugriff über Webbrowser aktivieren), wenn der Zugriff auf die VNC-Sitzung über einen Webbrowser-Fenster erfolgen soll.
4. Aktivieren Sie bei Bedarf *Firewall-Port öffnen* (wenn Ihre Netzwerkschnittstelle z. B. so konfiguriert ist, dass sie in der externen Zone liegt). Wenn Sie mehrere Netzwerkschnittstellen haben, beschränken Sie das Öffnen der Firewall-Ports über *Firewall-Details* auf eine bestimmte Schnittstelle.
5. Bestätigen Sie die Einstellungen mit *Weiter*.
6. Falls zu dem Zeitpunkt noch nicht alle erforderlichen Pakete verfügbar sind, müssen Sie der Installation der fehlenden Pakete zustimmen.

Tipp: Neustart des Anzeigemanagers

YaST nimmt Änderungen an den Einstellungen des Anzeigemanagers vor. Diese Änderungen treten erst dann in Kraft, wenn Sie sich aus der aktuellen grafischen Sitzung abmelden und den Anzeigemanager neu starten.

ABBILDUNG 8.7 FERNVERWALTUNG

8.3.1 Verfügbare Konfigurationen

Die Standardkonfiguration von SUSE Linux Enterprise Server stellt Sitzungen mit einer Auflösung von 1024 x 768 Pixeln und einer Farbtiefe von 16 Bit bereit. Die Sitzungen sind an Port `5901` für „reguläre“ VNC-Viewer (entspricht VNC-Display `1`) und an Port `5801` für Webbrowser verfügbar.

Weitere Konfigurationen können an anderen Ports verfügbar gemacht werden, siehe *Abschnitt 8.3.3, „Konfigurieren einmaliger VNC-Sitzungen“*

VNC-Anzeigenummern und X-Anzeigenummern sind bei einmaligen Sitzungen unabhängig. Eine VNC-Anzeigenummer wird manuell jeder Konfiguration zugewiesen, die vom Server unterstützt wird (:1 im obigen Beispiel). Immer, wenn eine VNC-Sitzung mit einer der Konfigurationen initiiert wird, erhält sie automatisch eine freie X-Display-Nummer.

Standardmäßig versuchen sowohl der VNC-Client als auch der Server, über ein selbstsigniertes SSL-Zertifikat sicher zu kommunizieren, das nach der Installation erzeugt wird. Verwenden Sie wahlweise das Standardzertifikat oder ersetzen Sie es durch Ihr eigenes Zertifikat. Bei Nutzung eines selbstsignierten Zertifikats müssen Sie vor der ersten Verbindung dessen Signatur bestätigen.

8.3.2 Initiieren einer einmaligen VNC-Sitzung

Um eine Verbindung zu einer einmaligen VNC-Sitzung herzustellen, muss ein VNC-Viewer installiert sein, lesen Sie hierzu auch *Abschnitt 8.1, „Der* **vncviewer***-Client“*.

8.3.3 Konfigurieren einmaliger VNC-Sitzungen

Sie können diesen Abschnitt überspringen, wenn Sie die Standardkonfiguration nicht ändern müssen bzw. möchten.

Einmalige VNC-Sitzungen werden über den `systemd`-Socket `xvnc.socket` gestartet. Standardmäßig bietet sie sechs Konfigurationsblöcke: drei für VNC-Viewer (`vnc1` bis `vnc3`) und drei für Java-Applets (`vnchttpd1` bis `vnchttpd3`). Standardmäßig sind nur `vnc1` und `vnchttpd1` aktiv.

Mit dem folgenden Befehl aktivieren Sie den VNC-Server-Socket beim Booten:

```
sudo systemctl enable xvnc.socket
```

Mit dem folgenden Befehl starten Sie den Socket sofort:

```
sudo systemctl start xvnc.socket
```

Der **`Xvnc`**-Server kann mit der Option `server_args` konfiguriert werden. Eine Liste der Optionen finden Sie unter **`Xvnc --help`**.

Achten Sie beim Hinzufügen benutzerdefinierter Konfigurationen darauf, keine Ports zu verwenden, die bereits von anderen Konfigurationen, anderen Services oder bestehenden permanenten VNC-Sitzungen auf demselben Host verwendet werden.

Aktivieren Sie Konfigurationsänderungen mit folgendem Kommando:

```
tux > sudo systemctl reload xvnc.socket
```

Wichtig: Firewall und VNC-Ports

Wenn Sie die entfernte Verwaltung wie in *Prozedur 8.1, „Aktivieren von einmaligen VNC-Sitzungen“* beschrieben aktivieren, werden die Ports `5801` und `5901` in der Firewall geöffnet. Wenn die Netzwerkschnittstelle, über die die VNC-Sitzung bereitgestellt wird, durch eine Firewall geschützt wird, müssen Sie die entsprechenden Ports manuell öffnen, wenn Sie zusätzliche Ports für VNC-Sitzungen aktivieren. Eine Anleitung dazu finden Sie in *Buch „Security Guide“, Kapitel 15 „Masquerading and Firewalls“*.

8.4 Permanente VNC-Sitzungen

Auf eine permanente Sitzung kann gleichzeitig von mehreren Clients zugegriffen werden. Dies eignet sich ideal für Demozwecke, bei denen ein Client den vollen Zugriff und alle anderen einen reinen Anzeigezugriff haben. Weiter eignet sich dies für Schulungen, bei denen der Schulungsleiter einen Zugriff auf den Desktop des Teilnehmers benötigt.

Tipp: Verbindung zu einer permanenten VNC-Sitzung herstellen

Um eine Verbindung zu einer permanenten VNC-Sitzung herzustellen, muss ein VNC-Viewer installiert sein. Weitere Informationen finden Sie in *Abschnitt 8.1, „Der* **vncviewer**-*Client“*.

Es gibt zwei Arten von permanenten VNC-Sitzungen:

- *Mit* `vncserver` *initiierte VNC-Sitzung*
- *Mit* `vncmanager` *initiierte VNC-Sitzung*

8.4.1 Mit `vncserver` initiierte VNC-Sitzung

Diese Art einer permanenten VNC-Sitzung wird auf dem Server initiiert. Die Sitzung und sämtliche in dieser Sitzungsausführung gestarteten Anwendungen werden ungeachtet der Client-Verbindungen so lange ausgeführt, bis die Sitzung beendet wird. Der Zugriff auf permanente Sitzungen wird durch zwei mögliche Arten von Passwörtern geschützt:

- ein reguläres Passwort, das den vollen Zugriff ermöglicht, oder
- ein optionales Passwort, das keinen interaktiven Zugriff ermöglicht und nur eine Anzeige liefert.

Eine Sitzung kann mehrere Client-Verbindungen beider Arten gleichzeitig haben.

PROZEDUR 8.2 STARTEN EINER PERMANENTEN VNC-SITZUNG MIT `vncserver`

1. Öffnen Sie eine Shell uns stellen Sie sicher, dass Sie als der Benutzer angemeldet sind, der Eigentümer der VNC-Sitzung sein soll.

2. Wenn die Netzwerkschnittstelle, über die die VNC-Sitzung bereitgestellt wird, durch eine Firewall geschützt wird, müssen Sie die von Ihrer Sitzung verwendeten Ports manuell in der Firewall öffnen. Wenn Sie mehrere Sitzungen starten, können ie alternativ einen Portbereich öffnen. Details zur Konfiguration der Firewall finden Sie unter *Buch „Security Guide", Kapitel 15 „Masquerading and Firewalls"*.
   `vncserver` verwendet die Port `5901` für Display `:1`, `5902` für Display `:2` usw. Bei permanenten Sitzungen haben das VNC-Display und das X-Display normalerweise dieselbe Nummer.

3. Geben Sie folgendes Kommando ein, um eine Sitzung mit einer Auflösung von 1024x769 Pixel und einer Farbtiefe von 16 Bit zu starten:

   ```
   vncserver -alwaysshared -geometry 1024x768 -depth 16
   ```

   Das Kommando **`vncserver`** verwendet, sofern keine Display-Nummer angegeben ist, eine freie Display-Nummer und gibt seine Auswahl aus. Weitere Optionen finden Sie mit **`man 1 vncserver`**.

Bei der erstmaligen Ausführung von **`vncserver`** wird nach einem Passwort für den vollständigen Zugriff auf die Sitzung gefragt. Geben Sie gegebenenfalls auch ein Passwort für den reinen Anzeigezugriff auf die Sitzung ein.

Die hier angegebenen Passwörter werden auch für zukünftige Sitzungen verwendet, die durch denselben Benutzer gestartet werden. Sie können mit dem Kommando **`vncpasswd`** geändert werden.

Wichtig: Sicherheitsüberlegungen

Achten Sie darauf, dass Ihre Passwörter sicher und ausreichend lang sind (mindestens acht Zeichen). Teilen Sie diese Passwörter niemandem mit.

Beenden Sie, um die Sitzung zu beenden, die Desktopumgebung, die innerhalb der VNC-Sitzung ausgeführt wird über den VNC-Viewer so, wie Sie eine normale lokale X-Sitzung beenden würden.

Wenn Sie eine Sitzung lieber manuell beenden, öffnen Sie eine Shell auf dem VNC-Server und vergewissern Sie sich, dass Sie als der Benutzer angemeldet ist, der der Eigentümer der zu beendenden VNC-Sitzung ist. Führen Sie das folgende Kommando aus, um die Sitzung zu beenden, die auf Display `:1`: **`vncserver -kill :1`** ausgeführt wird.

8.4.1.1 Konfigurieren von permanenten VNC-Sitzungen

Permanente VNC-Sitzungen können durch Bearbeiten von `$HOME/.vnc/xstartup` konfiguriert werden. Standardmäßig startet dieses Shell-Skript dieselbe GUI bzw. denselben Fenstermanager, aus dem es gestartet wurde. In SUSE Linux Enterprise Server ist dies entweder GNOME oder IceWM. Wenn Sie beim Starten Ihrer Sitzung einen bestimmten Fenstermanager verwenden möchten, legen Sie die Variable `WINDOWMANAGER` fest:

```
WINDOWMANAGER=gnome vncserver -geometry 1024x768
WINDOWMANAGER=icewm vncserver -geometry 1024x768
```

Anmerkung: Eine Konfiguration pro Benutzer

Permanente VNC-Sitzungen werden jeweils nur einmal pro Benutzer konfiguriert. Mehrere von demselben Benutzer gestartete Sitzungen verwenden alle dieselben Start- und Passwortdateien.

8.4.2 Mit `vncmanager` initiierte VNC-Sitzung

PROZEDUR 8.3 AKTIVIEREN VON PERMANENTEN VNC-SITZUNGEN

1. Starten Sie *YaST* › *Netzwerkdienste* › *Verwaltung von entfernten Rechnern aus (remote) (VNC)*.
2. Aktivieren Sie die Option *Allow Remote Administration With Session Management* (Verwaltung von entfernten Rechnern aus (remote) mit Sitzungsverwaltung zulassen).
3. Aktivieren Sie die Option *Enable access using a web browser* (Zugriff über Webbrowser aktivieren), wenn der Zugriff auf die VNC-Sitzung über ein Webbrowser-Fenster erfolgen soll.
4. Aktivieren Sie bei Bedarf *Firewall-Port öffnen* (wenn Ihre Netzwerkschnittstelle z. B. so konfiguriert ist, dass sie in der externen Zone liegt). Wenn Sie mehrere Netzwerkschnittstellen haben, beschränken Sie das Öffnen der Firewall-Ports über *Firewall-Details* auf eine bestimmte Schnittstelle.
5. Bestätigen Sie die Einstellungen mit *Weiter*.
6. Falls zu dem Zeitpunkt noch nicht alle erforderlichen Pakete verfügbar sind, müssen Sie der Installation der fehlenden Pakete zustimmen.

Tipp: Neustart des Anzeigemanagers

YaST nimmt Änderungen an den Einstellungen des Anzeigemanagers vor. Diese Änderungen treten erst dann in Kraft, wenn Sie sich aus der aktuellen grafischen Sitzung abmelden und den Anzeigemanager neu starten.

8.4.2.1 Konfigurieren von permanenten VNC-Sitzungen

Sobald Sie die VNC-Sitzungsverwaltung gemäß *Prozedur 8.3, „Aktivieren von permanenten VNC-Sitzungen“* aktiviert haben, können Sie wie gewohnt eine Verbindung zur Remote-Sitzung über den VNC-Viewer herstellen, z. B. **`vncviewer`** oder Remmina. Der Anmeldebildschirm wird geöffnet. Nach erfolgter Anmeldung wird das VNC-Symbol in der Taskleiste der Desktop-Umgebung angezeigt. Zum Öffnen des Fensters *VNC-Sitzung* klicken Sie auf das Symbol. Falls das Fenster nicht geöffnet wird oder Ihre Desktop-Umgebung keine Symbole in der Task-Leiste unterstützt, führen Sie **`vncmanager-controller`** manuell aus.

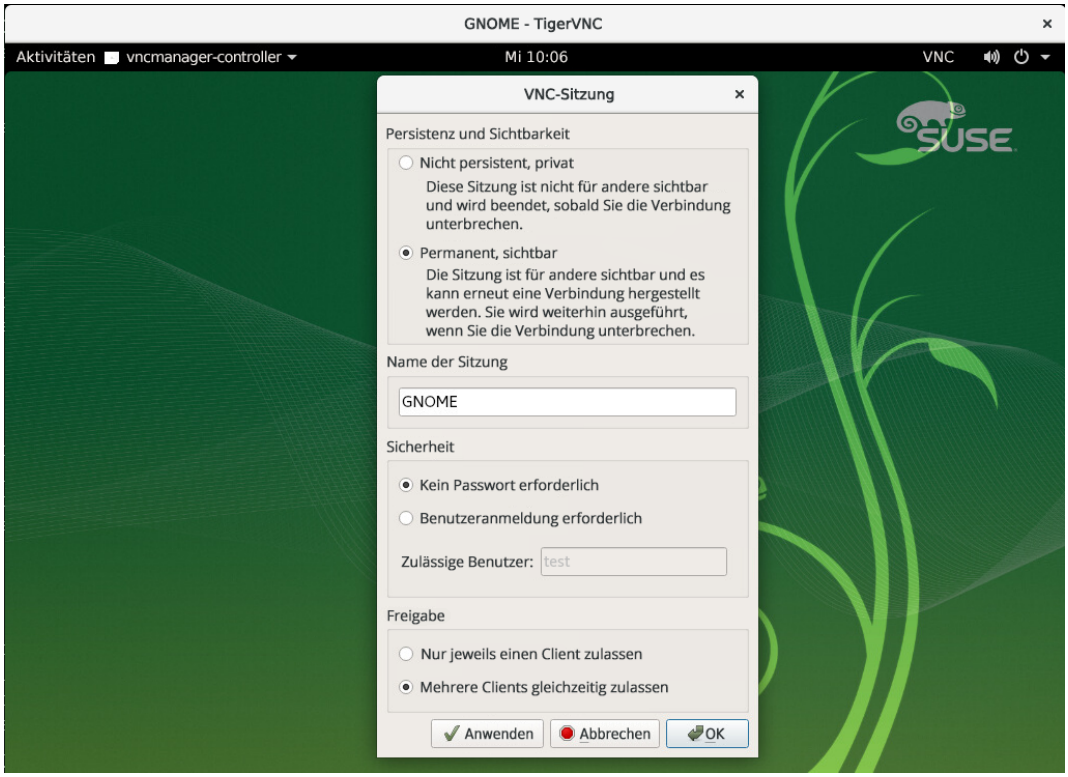


ABBILDUNG 8.8 VNC-SITZUNGSEINSTELLUNGEN

Verschiedene Einstellungen beeinflussen das Verhalten der VNC-Sitzung:

Nicht persistent, privat

Dies entspricht einer einmaligen Sitzung. Diese Sitzung ist für andere nicht sichtbar und wird beendet, sobald Sie die Verbindung zur Sitzung trennen. Weitere Informationen finden Sie unter *Abschnitt 8.3, „Einmalige VNC-Sitzungen“*.

Permanent, sichtbar

Die Sitzung ist für andere Benutzer sichtbar und wird weiter ausgeführt, auch wenn Sie die Verbindung zur Sitzung trennen.

Name der Sitzung

Geben Sie den Namen der permanenten Sitzung an, sodass sie beim Wiederherstellen der Verbindung eindeutig erkennbar ist.

Kein Passwort erforderlich

Die Sitzung ist frei zugänglich, ohne dass die Benutzer sich mit ihrem Berechtigungsnachweis anmelden müssen.

Benutzeranmeldung erforderlich

Zum Zugriff auf die Sitzung müssen Sie sich mit einem gültigen Benutzernamen und Passwort anmelden. Führen Sie die gültigen Benutzernamen im Textfeld *Zulässige Benutzer* auf.

Nur jeweils einen Client zulassen

Es können nicht mehrere Benutzer gleichzeitig der Sitzung beitreten.

Mehrere Clients gleichzeitig zulassen

Mehrere Benutzer können gleichzeitig der permanenten Sitzung beitreten. Eignet sich beispielsweise für Remote-Präsentationen und -Schulungen.

Bestätigen Sie Ihre Auswahl mit *OK*.

8.4.2.2 Beitreten zu permanenten VNC-Sitzungen

Sobald Sie eine permanente VPC-Sitzung gemäß *Abschnitt 8.4.2.1, „Konfigurieren von permanenten VNC-Sitzungen“* eingerichtet haben, können Sie dieser Sitzung über den VNC-Viewer beitreten. Nachdem Ihr VNC-Client eine Verbindung zum Server aufgebaut hat, werden Sie gefragt, ob Sie eine neue Sitzung erstellen oder der bestehenden Sitzung beitreten möchten:

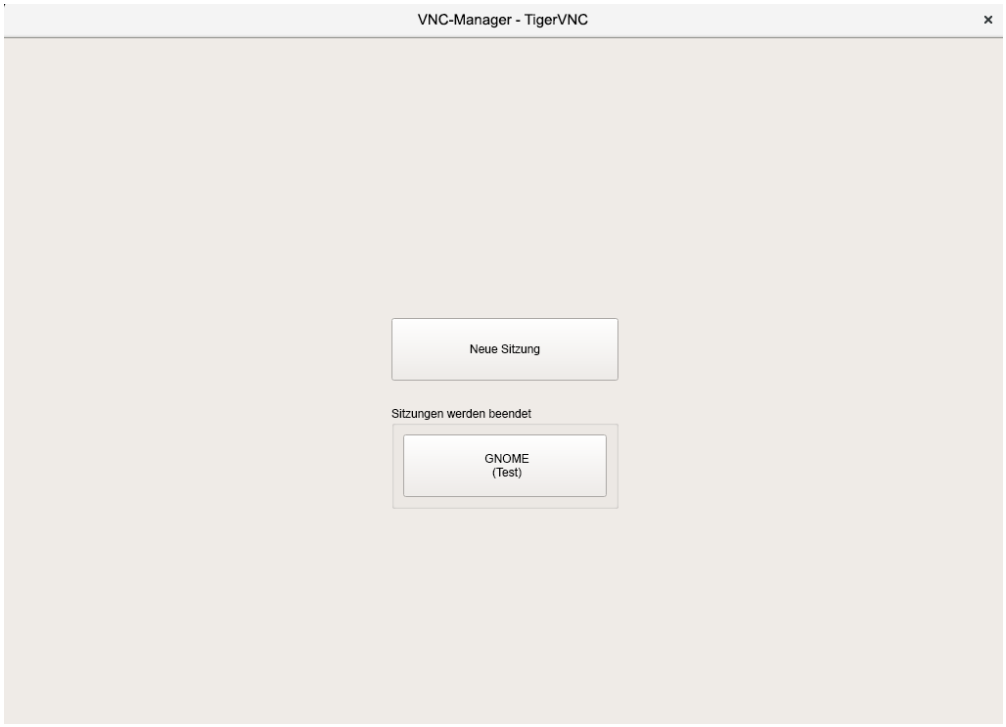


ABBILDUNG 8.9 BEITRETEN ZU EINER PERMANENTEN VNC-SITZUNG

Wenn Sie auf den Namen der bestehenden Sitzung klicken, werden Sie ggf. aufgefordert, Ihren Berechtigungsnachweis anzugeben, abhängig von den Einstellungen für die dauerhafte Sitzung.

8.5 Verschlüsselte VNC-Kommunikation

Wenn der VNC-Server ordnungsgemäß eingerichtet ist, wird die gesamte Kommunikation zwischen dem VNC-Server und dem Client verschlüsselt. Die Authentifizierung wird zu Beginn der Sitzung vorgenommen, die eigentliche Datenübertragung beginnt erst danach.

Die Sicherheitsoptionen für einmalige und für permanente VNC-Sitzungen werden mit dem Parameter `-securitytypes` des Befehls **`/usr/bin/Xvnc`** in der Zeile `server_args` konfiguriert. Der Parameter `-securitytypes` bestimmt sowohl die Authentifizierungsmethode als auch die Verschlüsselung. Hier stehen die folgenden Optionen zur Auswahl:

AUTHENTIFIZIERUNGEN

None, TLSNone, X509None
: Keine Authentifizierung.

VncAuth, TLSVnc, X509Vnc
: Authentifizierung mit benutzerdefiniertem Passwort.

Plain, TLSPlain, X509Plain
: Authentifizierung mit Überprüfung des Benutzerpassworts mit PAM.

VERSCHLÜSSELUNGEN

None, VncAuth, Plain
: Keine Verschlüsselung.

TLSNone, TLSVnc, TLSPlain
: Anonyme TLS-Verschlüsselung. Alle Angaben werden verschlüsselt; auf dem Remote-Host erfolgt jedoch keine Überprüfung. Damit sind Sie gegen passive Angreifer geschützt, nicht jedoch gegen Man-in-the-Middle-Angreifer.

X509None, X509Vnc, X509Plain
: TLS-Verschlüsselung mit Zertifikat. Wenn Sie ein selbstsigniertes Zertifikat heranziehen, werden Sie bei der ersten Verbindung aufgefordert, dieses Zertifikat zu bestätigen. Bei weiteren Verbindungen erhalten Sie nur dann eine Warnung, wenn das Zertifikat geändert wurde. So sind Sie gegen alle Angreifer geschützt, ausgenommen Man-in-the-Middle-Angreifer bei der ersten Verbindung (ähnlich wie bei der typischen SSH-Verwendung). Wenn Sie ein Zertifikat heranziehen, das von einer Zertifizierungsstelle signiert wurde und das mit dem Computernamen übereinstimmt, erzielen Sie praktisch uneingeschränkte Sicherheit (ähnlich wie bei der typischen HTTPS-Verwendung).

Tipp: Pfad zum Zertifikat und zum Schlüssel

Bei der X509-gestützten Verschlüsselung müssen Sie den Pfad zum X509-Zertifikat/-Schlüssel mit den Optionen `-X509Cert` und `-X509Key` angeben.

Wenn Sie mehrere Sicherheitstypen angeben (jeweils durch Komma getrennt), wird der erste Typ herangezogen, der sowohl vom Client als auch vom Server unterstützt wird. So können Sie die opportunistische Verschlüsselung auf dem Server konfigurieren. Dies ist von Nutzen, wenn VNC-Clients unterstützt werden sollen, die ihrerseits keine Verschlüsselung unterstützen.

Auf dem Client können Sie außerdem die zulässigen Sicherheitstypen angeben, sodass ein Downgrade-Angriff vermieden wird, wenn Sie eine Verbindung zu einem Server herstellen, auf dem bekanntermaßen die Verschlüsselung aktiviert ist. (Der VNC-Viewer zeigt in diesem Fall allerdings die Meldung „Verbindung nicht verschlüsselt!“ an.)

9 Kopieren von Dateien mit RSync

Viele moderne Benutzer arbeiten heutzutage gleich mit mehreren Computern: Computer daheim und am Arbeitsplatz, Laptop, Smartphone oder Tablet. Damit wird die Synchronisierung von Dateien und Dokumenten über mehrere Geräte wichtiger als je zuvor.

Warnung: Risiko des Datenverlusts

Bevor Sie ein Synchronisierungstool starten, machen Sie sich mit dessen Funktionen und Optionen vertraut. Sichern Sie in jedem Fall wichtige Dateien.

9.1 Konzeptüberblick

Sollen große Datenmengen über eine langsame Netzwerkverbindung synchronisiert werden, bietet Rsync eine zuverlässige Methode, mit der ausschließlich die Änderungen in den Dateien übermittelt werden. 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.

Zum Erkennen der Änderungen ist eine gewisse Rechenleistung erforderlich. Die Computer auf beiden Seiten müssen daher ausreichende Ressourcen aufweisen (auch ausreichend RAM).

Rsync ist insbesondere dann von Nutzen, wenn große Datenmengen mit kleinen Änderungen in regelmäßigen Abständen übermittelt werden sollen. Dies ist häufig bei Sicherungskopien der Fall. Rsync eignet sich auch zum Spiegeln von Staging-Servern, mit denen komplette Verzeichnisbaumstrukturen von Webservern auf einem Webserver in einer DMZ gespeichert werden.

Trotz seines Namens ist Rsync kein Synchronisierungswerkzeug. Rsync ist ein Werkzeug, das Daten jeweils nur in eine einzige Richtung kopiert, nicht in beide Richtungen. Etwas anderes ist damit nicht möglich. Wenn Sie ein bidirektionales Werkzeug benötigen, mit dem Quelle und Ziel synchronisiert werden, verwenden Sie Csync.

9.2 Einfache Syntax

Für das Befehlszeilenwerkzeug Rsync gilt die folgende grundlegende Syntax:

```
rsync [OPTION] SOURCE [SOURCE]... DEST
```

Sie können Rsync auf jedem lokalen Computer oder Remote-Computer verwenden, sofern Sie die erforderlichen Zugriffs- und Schreibrechte besitzen. Es können mehrere *SOURCE*-Einträge vorliegen. Die Platzhalter *SOURCE* und *DEST* können durch Pfade und/oder durch URLs ersetzt werden.

Die folgenden Rsync-Optionen werden am häufigsten verwendet:

`-v`
: Gibt einen ausführlicheren Text zurück

`-a`
: Archivmodus; kopiert Dateien rekursiv und behält die Zeitstempel, das Benutzer-/Gruppeneigentum, die Dateiberechtigungen und die symbolischen Links bei.

`-z`
: Komprimiert die übermittelten Daten

Anmerkung: Anzahl der nachgestellten Schrägstriche

Beim Arbeiten mit Rsync sind die nachgestellten Schrägstriche besonders zu beachten. Ein nachgestellter Schrägstrich nach dem Verzeichnis bezeichnet den *Inhalt* des Verzeichnisses. Die Angabe ohne nachgestellten Schrägstrich bezeichnet das *Verzeichnis selbst*.

9.3 Lokales Kopieren von Dateien und Verzeichnissen

In der nachfolgenden Beschreibung wird vorausgesetzt, dass der aktuelle Benutzer Schreibrechte für das Verzeichnis `/var/backup` besitzt. Mit dem folgenden Befehl kopieren Sie eine einzelne Datei aus einem Verzeichnis auf dem Computer in einen anderen Pfad:

```
tux > rsync -avz backup.tar.xz /var/backup/
```

Die Datei `backup.tar.xz` wird in das Verzeichnis `/var/backup/` kopiert; der absolute Pfad lautet `/var/backup/backup.tar.xz`.

Denken Sie daran, den *nachgestellten Schrägstrich* nach dem Verzeichnis `/var/backup/` anzugeben! Wenn Sie den Schrägstrich nicht einfügen, wird die Datei `backup.tar.xz` in `/var/backup` kopiert (also in eine Datei), *nicht* in das Verzeichnis `/var/backup/`!

Verzeichnisse werden auf ähnliche Weise kopiert wie einzelne Dateien. Im folgenden Beispiel wird das Verzeichnis `tux/` mit dessen Inhalt in das Verzeichnis `/var/backup/` kopiert:

```
tux > rsync -avz tux /var/backup/
```

Die Kopie befindet sich im absoluten Pfad `/var/backup/tux/`.

9.4 Remote-Kopieren von Dateien und Verzeichnissen

Das Rsync-Werkzeug muss auf beiden Computern vorhanden sein. Zum Kopieren von Dateien aus Remote-Verzeichnissen oder in diese benötigen Sie eine IP-Adresse oder einen Domänennamen. Ein Benutzername ist optional, wenn die aktuellen Benutzernamen auf dem lokalen Computer und dem Remote-Computer identisch sind.

Mit dem folgenden Befehl kopieren Sie die Datei `file.tar.xz` vom lokalen Host auf den Remote-Host `192.168.1.1` mit identischen Benutzern (lokal und remote):

```
tux > rsync -avz file.tar.xz  tux@192.168.1.1:
```

Alternativ sind auch die folgenden Befehle möglich und äquivalent:

```
tux > rsync -avz file.tar.xz 192.168.1.1:~
tux > rsync -avz file.tar.xz 192.168.1.1:/home/tux
```

In allen Fällen mit Standardkonfiguration werden Sie aufgefordert, den Passwortsatz des Remote-Benutzers einzugeben. Mit diesem Befehl wird `file.tar.xz` in das Benutzerverzeichnis des Benutzers `tux` kopiert (in der Regel `/home/tux`).

Verzeichnisse werden im Remote-Verfahren auf ähnliche Weise kopiert wie lokal. Im folgenden Beispiel wird das Verzeichnis `tux/` mit dessen Inhalt in das Remote-Verzeichnis `/var/backup/` auf dem Host `192.168.1.1` kopiert:

```
tux > rsync -avz tux 192.168.1.1:/var/backup/
```

Unter der Voraussetzung, dass Sie Schreibrechte auf dem Host `192.168.1.1` besitzen, befindet sich die Kopie im absoluten Pfad `/var/backup/tux`.

9.5 Konfigurieren und Verwenden eines Rsync-Servers

Rsync kann als Daemon (`rsyncd`) ausgeführt werden, der den Standardport 873 auf eingehende Verbindungen überwacht. Dieser Daemon kann „Kopierziele“ empfangen.

Mit den nachfolgenden Anweisungen erstellen Sie einen Rsync-Server auf `jupiter` mit einem *backup*-Ziel. In diesem Ziel können Sie Ihre Sicherungskopien speichern. So erstellen Sie einen Rsync-Server:

PROZEDUR 9.1 EINRICHTEN EINES RSYNC-SERVERS

1. Erstellen Sie auf jupiter ein Verzeichnis, in dem alle Sicherungskopien gespeichert werden sollen. In diesem Beispiel wird das Verzeichnis `/var/backup` verwendet:

   ```
   root # mkdir /var/backup
   ```

2. Legen Sie das Eigentum fest. In diesem Fall ist der Benutzer `tux` in der Gruppe `users` der Eigentümer des Verzeichnisses:

   ```
   root # chown tux.users /var/backup
   ```

3. Konfigurieren Sie den rsyncd-Daemon.
   Die Konfigurationsdatei wird in eine Hauptdatei und einige „Module“ aufgeteilt, in denen sich das Sicherungsziel befindet. So können zusätzliche Module später einfacher eingefügt werden. Die globalen Werte können in den Dateien `/etc/rsyncd.d/*.inc` gespeichert werden, die Module dagegen in den Dateien `/etc/rsyncd.d/*.conf`:

   a. Erstellen Sie das Verzeichnis `/etc/rsyncd.d/`:

      ```
      root # mkdir /etc/rsyncd.d/
      ```

   b. Tragen Sie die folgenden Zeilen in die Hauptkonfigurationsdatei `/etc/rsyncd.conf` ein:

      ```
      # rsyncd.conf main configuration file
      log file = /var/log/rsync.log
      pid file = /var/lock/rsync.lock

      &merge /etc/rsyncd.d ❶
      &include /etc/rsyncd.d ❷
      ```

1. Führt die globalen Werte aus den Dateien `/etc/rsyncd.d/*.inc` in der Hauptkonfigurationsdatei zusammen.
2. Lädt die Module (oder Ziele) aus den Dateien `/etc/rsyncd.d/*.conf`. Diese Dateien dürfen keine Verweise auf die globalen Werte enthalten.

c. Legen Sie das Modul (das Sicherungsziel) mit den folgenden Zeilen in der Datei `/etc/rsyncd.d/backup.conf` an:

```
# backup.conf: backup module
[backup] ❶
   uid = tux ❷
   gid = users ❷
   path = /var/backup ❸
   auth users = tux  ❹
   secrets file = /etc/rsyncd.secrets ❺
   comment = Our backup target
```

1. Das *backup*-Ziel. Geben Sie einen beliebigen Namen ein. Benennen Sie das Ziel nach Möglichkeit entsprechend seinem Zweck und verwenden Sie denselben Namen in der `*.conf`-Datei.
2. Gibt den Benutzer- oder Gruppennamen an, der für die Dateiübertragung herangezogen werden soll.
3. Definiert den Pfad, in dem die Sicherungskopien gespeichert werden sollen (aus *Schritt 1*).
4. Gibt eine durch Komma getrennte Liste der zulässigen Benutzer an. In der einfachsten Form enthält diese Liste die Namen der Benutzer, die berechtigt sind, eine Verbindung zu diesem Modul herzustellen. In diesem Fall ist lediglich der Benutzer `tux` zulässig.
5. Gibt den Pfad einer Datei an, die Zeilen mit Benutzernamen und einfachen Passwörtern enthält.

d. Erstellen Sie die Datei `/etc/rsyncd.secrets` mit dem folgenden Inhalt und ersetzen Sie *`PASSPHRASE`*:

```
# user:passwd
tux:PASSPHRASE
```

e. Die Datei darf nur von `root` gelesen werden können:

```
root # chmod 0600 /etc/rsyncd.secrets
```

4. Starten und aktivieren Sie den rsyncd-Daemon:

```
root # systemctl enable rsyncd
root # systemctl start rsyncd
```

5. Testen Sie den Zugriff auf den Rsync-Server:

```
tux > rsync jupiter::
```

Beispiel für eine Antwort:

```
backup          Our backup target
```

Ansonsten prüfen Sie die Konfigurationsdatei-, Firewall- und Netzwerkeinstellungen.

Mit den obigen Schritten wird ein Rsync-Server erstellt, auf dem Sie nun Sicherungskopien speichern können. Im obigen Beispiel wird auch eine Protokolldatei über alle Verbindungen angelegt. Diese Datei wird unter `/var/log/rsyncd.log` abgelegt. Diese Funktion ist besonders beim Debuggen der Datenübertragungen hilfreich.

Mit dem folgenden Befehl listen Sie den Inhalt des Sicherungsziels auf:

```
rsync -avz jupiter::backup
```

Dieser Befehl listet alle Dateien auf, die auf dem Server im Verzeichnis `/var/backup` liegen. Diese Anfrage wird auch in der Protokolldatei unter `/var/log/rsyncd.log` aufgezeichnet. Um die Übertragung tatsächlich zu starten, geben Sie ein Quellverzeichnis an. Verwenden Sie `.` für das aktuelle Verzeichnis. Mit dem folgenden Befehl wird beispielsweise das aktuelle Verzeichnis auf den Rsync-Sicherungsserver kopiert:

```
rsync -avz . jupiter::backup
```

Standardmäßig werden beim Ausführen von Rsync keine Dateien und Verzeichnisse gelöscht. Soll die Löschung aktiviert werden, müssen Sie die zusätzliche Option `--delete` angeben. Um sicherzustellen, dass keine neueren Dateien überschrieben werden, kann stattdessen die Option `--update` angegeben werden. Dadurch entstehende Konflikte müssen manuell aufgelöst werden.

9.6 Weiterführende Informationen

CSync

Bidirektionales Dateisynchronisierungswerkzeug, siehe https://www.csync.org/.

RSnapshot

Erstellt inkrementelle Sicherungen, siehe http://rsnapshot.org.

Unison

Bidirektionales Dateisynchronisierungswerkzeug – ähnlich wie CSync, jedoch mit grafischer Benutzeroberfläche, siehe http://www.seas.upenn.edu/~bcpierce/unison/.

Rear

Disaster Recovery-Framework, siehe *Administrationshandbuch* für die SUSE Linux Enterprise-Hochverfügbarkeitserweiterung https://www.suse.com/documentation/sle-ha-12/.

II Booten eines Linux-Systems

10 Einführung in den Bootvorgang 138

11 UEFI (Unified Extensible Firmware Interface) 147

12 Der Bootloader GRUB 2 157

13 Der Daemon `systemd` 180

10 Einführung in den Bootvorgang

Das Booten eines Linux-Systems umfasst verschiedene Komponenten und Tasks. Nach der Firmware- und Hardware-Initialisierung, die von der Computerarchitektur abhängt, wird der Kernel mithilfe des Bootloaders GRUB 2 gestartet. Anschließend wird der Bootvorgang vollständig vom Betriebssystem gesteuert und über `systemd` abgewickelt. `systemd` bietet eine Reihe von „Zielen“, mit denen Konfigurationen für den normalen Gebrauch, für Wartungsarbeiten oder für Notfälle gebootet werden.

10.1 Terminologie

In diesem Kapitel werden Begriffe verwendet, die unter Umständen nicht eindeutig sind. Aus diesem Grund stellen wir im Folgenden einige Definitionen bereit:

`init`

Derzeit gibt es zwei unterschiedliche Prozesse mit dem Namen „init“:

- den `initramfs`-Vorgang, mit dem das Root-Dateisystem eingehängt wird
- den Betriebssystemprozess, mit dem alle anderen Prozesse gestartet werden und der über das echte Root-Dateisystem ausgeführt wird

In beiden Fällen wird die jeweilige Aufgabe vom Programm `systemd` ausgeführt. Zunächst wird sie aus dem `initramfs` ausgeführt, sodass das Root-Dateisystem eingehängt wird. Wurde dieser Vorgang erfolgreich abgeschlossen, wird der Vorgang als ursprünglicher Prozess erneut ausgeführt, diesmal aus dem Root-Dateisystem. Damit keine Verwirrung entsteht, welcher der beiden `systemd`-Prozesse gemeint ist, bezeichnen wir den ersten als *init auf initramfs* und den zweiten als *systemd*.

`initrd`/`initramfs`

Eine `initrd` (ursprüngliche RAM-Festplatte) ist eine Imagedatei, die ein Image des Root-Dateisystems enthält, das vom Kernel geladen und über `/dev/ram` als temporäres Root-Dateisystem eingehängt wird. Für das Einhängen dieses Dateisystems ist ein Dateisystemtreiber erforderlich.

Ab Kernel 2.6.13 wurde initrd durch `initramfs` (ursprüngliches RAM-Dateisystem) ersetzt, für das kein Einhängen eines Dateisystemtreibers erforderlich ist. SUSE Linux Enterprise Server nutzt ausschließlich `initramfs`. Da `initramfs` jedoch als `/boot/initrd` gespeichert ist, wird es auch häufig als „initrd“ bezeichnet. In diesem Kapitel verwenden wir ausschließlich den Begriff `initramfs`.

10.2 Der Linux-Bootvorgang

Der Linux-Bootvorgang besteht aus mehreren Phasen, von denen jede einer anderen Komponente entspricht:

1. *Abschnitt 10.2.1, „ Initialisierungs- und Bootloader-Phase “*
2. *Abschnitt 10.2.2, „Die Kernel-Phase“*
3. *Abschnitt 10.2.3, „Die Phase init auf initramfs“*
4. *Abschnitt 10.2.4, „Die systemd-Phase“*

10.2.1 Initialisierungs- und Bootloader-Phase

Während der Initialisierungsphase wird die Computerhardware eingerichtet und die Geräte werden vorbereitet. Dieser Prozess verläuft, abhängig von der Hardwarearchitektur, bei jedem Gerät anders.

SUSE Linux Enterprise Server nutzt für alle Architekturen den Bootloader GRUB 2. Abhängig von Architektur und Firmware ist das Starten des Bootloaders GRUB 2 unter Umständen ein Prozess mit mehreren Schritten. Zweck des Bootloaders ist es, den Kernel und das ursprüngliche RAM-basierte Dateisystem (initramfs) zu laden. Weitere Informationen zu GRUB 2 finden Sie in *Kapitel 12, Der Bootloader GRUB 2*.

10.2.1.1 Initialisierungs- und Bootloader-Phase auf AArch64 und AMD64/Intel 64

Nach dem Einschalten des Computers initialisiert das BIOS oder das UEFI den Bildschirm und die Tastatur und testet den Hauptspeicher. Bis zu dieser Phase greift der Computer nicht auf Massenspeichergeräte zu. Anschließend werden Informationen zum aktuellen Datum, zur aktu-

ellen Uhrzeit und zu den wichtigsten Peripheriegeräten aus den CMOS-Werten geladen. Wenn die Boot-Medien und deren Geometrie erkannt wurden, geht die Systemkontrolle vom BIOS/UEFI an den Bootloader über.

Auf einem mit traditionellem BIOS ausgestatteten Computer kann nur Code des ersten physischen 512-Byte-Datensektors (Master-Boot-Datensatz, MBR) der Boot-Festplatte geladen werden. Nur die minimalistische Version von GRUB 2 passt in den MBR. Seine einzige Aufgabe besteht darin, ein Core-Image von GRUB 2 zu laden, das die Dateisystemtreiber aus der Lücke zwischen MBR und erster Partition (MBR-Partitionstabelle) oder der BIOS-Boot-Partition (GPT-Partitionstabelle) enthält. Dieses Image enthält Dateisystemtreiber und ist somit in der Lage, auf `/boot` im Root-Dateisystem zuzugreifen. `/boot` enthält zusätzliche Module für den Core von GRUB 2 sowie den Kernel und das initramfs-Image. Sobald GRUB 2 Zugriff auf diese Partition hat, lädt es den Kernel und das initramfs-Image in den Speicher und übergibt die Steuerung an den Kernel.

Wird ein BIOS-System aus einem verschlüsselten Dateisystem gebootet, das über eine verschlüsselte `/boot`-Partition verfügt, müssen Sie das Entschlüsselungspasswort zweimal eingeben. Zunächst benötigt es GRUB 2, um `/boot` zu entschlüsseln, die zweite Eingabe ermöglicht es `systemd`, die verschlüsselten Volumes einzuhängen.

Auf UEFI-Computern verläuft der Boot-Vorgang sehr viel einfacher als auf Computern mit herkömmlichem BIOS. Die Firmware ist dazu in der Lage, eine FAT-formatierte Systempartition von Festplatten mit GPT-Partitionstabelle zu lesen. Diese EFI-Systempartition (im laufenden System eingehängt als `/boot/efi`) bietet ausreichend Platz für eine komplette GRUB 2-Anwendung, die unmittelbar von der Firmware geladen und ausgeführt wird.

Wenn das BIOS/UEFI Netzwerk-Booting unterstützt, ist es auch möglich, einen Boot-Server zu konfigurieren, der den Bootloader bereitstellt. Das System kann dann über PXE gebootet werden. Das BIOS/UEFI dient als Bootloader. Es erhält das Boot-Image vom Boot-Server und startet das System. Dieser Vorgang ist vollständig unabhängig von den lokalen Festplatten.

10.2.1.2 Initialisierungs- und Bootloader-Phase auf IBM z-Systems

Bei IBM z Systems muss der Boot-Vorgang durch einen Bootloader namens **`zipl`** (ursprüngliches z-Programmladen) initialisiert werden. Obwohl **`zipl`** das Lesen unterschiedlicher Dateisysteme unterstützt, unterstützt es nicht das SLE-Standarddateisystem (Btrfs) oder das Booten aus Snapshots. SUSE Linux Enterprise Server nutzt somit einen zweistufigen Boot-Vorgang, der gewährleistet, dass Btrfs zum Boot-Zeitpunkt vollständig unterstützt wird:

1. **`zipl`** bootet über die ext2-formatierte Partition `/boot/zipl`. Diese Partition enthält einen minimalistischen Kernel sowie ein initramfs, die in den Speicher geladen werden. Das initramfs enthält (unter anderem) einen Btrfs-Treiber und den Bootloader GRUB 2. Der Kernel wird mit dem Parameter `initgrub` gestartet, der ihm befiehlt, GRUB 2 zu starten.
2. Der Kernel hängt das Root-Dateisystem ein, sodass auf `/boot` zugegriffen werden kann. Jetzt wird GRUB 2 über initramfs gestartet. Die Anwendung liest ihre Konfiguration aus `/boot/grub2/grub.cfg` aus und lädt den letzten Kernel und das initramfs aus `/boot`. Der neue Kernel wird nun über Kexec geladen.

10.2.2 Die Kernel-Phase

Sobald der Bootloader die Systemsteuerung übergeben hat, läuft der Boot-Vorgang auf allen Architekturen gleich ab. Der Bootloader lädt sowohl den Kernel als auch ein ursprüngliches RAM-basiertes Dateisystem (`initramfs`) in den Speicher und der Kernel übernimmt die Steuerung.

Nachdem der Kernel die Speicherverwaltung eingerichtet und CPU-Typ und -Eigenschaften erkannt hat, wird die Hardware initialisiert und das temporäre Root-Dateisystem aus dem Speicher eingehängt, der mit `initramfs` geladen wurde.

10.2.2.1 Die `initramfs`-Datei

`initramfs` (ursprüngliches RAM-Dateisystem) ist ein kleines cpio-Archiv, das der Kernel auf einen RAM-Datenträger laden kann. Zu finden ist es unter `/boot/initrd`. Es lässt sich mit einem Tool namens **`dracut`** erstellen – weitere Hinweise finden Sie unter **`man 8 dracut`**.

`initramfs` stellt eine minimale Linux-Umgebung bereit, die das Ausführen von Programmen ermöglicht, bevor das eigentliche Root-Dateisystem eingehängt wird. Diese minimale Linux-Umgebung wird durch eine BIOS- oder UEFI-Routine in den Arbeitsspeicher geladen, wobei

lediglich ausreichend Arbeitsspeicher zur Verfügung stehen muss; ansonsten gelten keine besonderen Anforderungen. Das `initramfs`-Archiv must stets eine ausführbare Datei mit der Bezeichnung `init` umfassen, die den `systemd`-Daemon auf dem Root-Dateisystem ausführt, so dass der Bootvorgang 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 werden mithilfe von `init` oder `initramfs` geladen. 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 geschieht über die `systemd`-Einheit `systemd-udev-trigger.service`.

10.2.2.1.1 Erneutes Generieren von initramfs

Da `initramfs` Treiber enthält, muss es aktualisiert werden, sobald neue Versionen der darin gespeicherten Treiber verfügbar sind. Dies geschieht automatisch bei der Installation des Pakets, das die Treiberaktualisierung enthält. YaST oder zypper informieren Sie über diesen Umstand, indem Sie den Output des Befehls anzeigen, mit dem `initramfs` generiert wird. Es gibt jedoch einige Situationen, in denen Sie `initramfs` manuell neu erzeugen müssen:

- *Hinzufügen von Treibern aufgrund von Änderungen an der Hardware*
- *Verschieben von Systemverzeichnissen auf RAID oder LVM*
- *Hinzufügen von Festplatten zu einer LVM-Gruppe/einem Btrfs-RAID mit Root-Dateisystem*
- *Ändern der Kernel-Variablen*

Hinzufügen von Treibern aufgrund von Änderungen an der Hardware

Wenn Hardwarekomponenten (z. B. Festplatten) ausgetauscht werden müssen und diese Hardware zur Bootzeit andere Treiber im Kernel erfordert, müssen Sie die Datei `initramfs` aktualisieren.

Bearbeiten Sie `/etc/dracut.conf.d/01-dist.conf` (oder erstellen Sie es, falls es noch nicht vorhanden sein sollte) und fügen Sie folgende Zeile hinzu.

```
force_drivers+="DRIVER1"
```

Ersetzen Sie dabei *DRIVER1* durch den Modulnamen des Treibers. Sie können auch mehrere Treiber hinzufügen. In diesem Fall geben Sie eine durch Leerzeichen getrennte Liste der Modulnamen ein:

```
force_drivers+="DRIVER1 DRIVER2"
```

Fahren Sie mit *Prozedur 10.1, „Generieren eines initramfs“* fort.

Verschieben von Systemverzeichnissen auf RAID oder LVM

Wann immer Sie Auslagerungsdateien oder Systemverzeichnisse wie `/usr` in einem laufenden System auf RAID oder ein logisches Volume verschieben, müssen Sie ein `initramfs` erstellen, das Softwaretreiber für RAID oder LVM unterstützt.

Hierzu müssen Sie die entsprechenden Einträge in `/etc/fstab` erstellen und die neuen Einträge (beispielsweise mit **`mount -a`** und/oder **`swapon -a`**) einhängen.

Fahren Sie mit *Prozedur 10.1, „Generieren eines initramfs“* fort.

Hinzufügen von Festplatten zu einer LVM-Gruppe/einem Btrfs-RAID mit Root-Dateisystem

Wann immer Sie eine Festplatte zu einer logischen Volumegruppe oder einem Btrfs-RAID, die oder das das Root-Dateisystem enthält, hinzufügen (oder daraus entfernen), müssen Sie ein `initramfs` erstellen, das das größere Volume unterstützt. Befolgen Sie die Anweisungen unter *Prozedur 10.1, „Generieren eines initramfs“*.

Fahren Sie mit *Prozedur 10.1, „Generieren eines initramfs“* fort.

Ändern der Kernel-Variablen

Wenn Sie die Werte von Kernel-Variablen über die **`sysctl`**-Benutzeroberfläche ändern und dabei die zugehörigen Dateien ändern (`/etc/sysctl.conf` oder `/etc/sysctl.d/*.conf`), geht die Änderung beim nächsten Neubooten des Systems verloren. Die Änderungen werden selbst dann nicht in der `initramfs`-Datei gespeichert, wenn Sie die Werte zur Laufzeit mit **`sysctl --system`** laden. Aktualisieren Sie es, in dem Sie wie in *Prozedur 10.1, „Generieren eines initramfs“* beschrieben vorgehen.

PROZEDUR 10.1 GENERIEREN EINES INITRAMFS

Beachten Sie, dass alle Befehle des folgenden Verfahrens unter dem Benutzer `root` ausgeführt werden müssen.

1. Generieren Sie eine neue `initramfs`-Datei, indem Sie Folgendes ausführen:

   ```
   dracut MY_INITRAMFS
   ```

Ersetzen Sie *MY_INITRAMFS* durch einen Dateinamen Ihrer Wahl. Das neue `initramfs` wird als `/boot/MY_INITRAMFS` erstellt.
Alternativ können Sie **`dracut -f`** ausführen. Somit wird die aktuell verwendete, bereits vorhandene Datei überschrieben.

2. (Überspringen Sie diesen Schritt, wenn Sie im vorangegangenen Schritt **`dracut -f`** ausgeführt haben.) Erstellen Sie einen Link zur `initramfs`-Datei, die Sie im vorangegangenen Schritt erstellt haben:

```
(cd /boot && ln -sf MY_INITRAMFS initrd)
```

3. Unter der Architektur IBM z Systems müssen Sie zudem **`grub2-install`** ausführen.

10.2.3 Die Phase init auf initramfs

Das temporäre Root-Dateisystem, das vom Kernel aus `initramfs` eingehängt wird, enthält die ausführbare Datei `systemd` (die wir im Folgenden als `init` auf `initramfs` bezeichnen, siehe auch *Abschnitt 10.1, „Terminologie“*). Dieses Programm führt alle erforderlichen Aktionen aus, mit denen das eigentliche Root-Dateisystem eingehängt wird. Es bietet Kernel-Funktionen für das benötigte Dateisystem sowie Gerätetreiber für Massenspeicher-Controller mit `udev`.

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

Laden der Kernelmodule

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

Bereitstellen von speziellen Blockdateien

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

Verwalten von RAID- und LVM-Setups

Wenn Ihr System so konfiguriert ist, dass das Root-Dateisystem sich unter RAID oder LVM befindet, richtet `init` unter `initramfs` LVM oder RAID so ein, dass der Zugriff auf das Root-Dateisystem zu einem späteren Zeitpunkt erfolgt.

Verwalten der Netzwerkkonfiguration

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 von `init` unter `initramfs` eingerichtet. SUSE Linux Enterprise Server unterstützt das Booten von einem sekundären iSCSI-Ziel, wenn das primäre Ziel nicht verfügbar ist. Weitere Details zur Konfiguration des Boot-iSCSI-Ziels finden Sie im *Buch „*Storage Administration Guide*", Kapitel 14 „Mass Storage over IP Networks: iSCSI", Abschnitt 14.3.1 „Using YaST for the iSCSI Initiator Configuration"*.

Anmerkung: Umgang mit Einhängefehlern

Wenn beim Einhängen des Root-Dateisystems in der Bootumgebung ein Fehler auftritt, muss es überprüft und repariert werden, bevor das Booten fortgesetzt werden kann. Die Dateisystemprüfung wird für Ext3- und Ext4-Dateisysteme automatisch gestartet. Der Reparaturvorgang findet für XFS- und Btrfs-Dateisysteme nicht automatisch statt und dem Benutzer werden Informationen angezeigt, die die verfügbaren Optionen zur Reparatur des Dateisystems beschreiben. Wenn das Dateisystem erfolgreich repariert wurde, versucht das System nach dem Beenden der Bootumgebung erneut, das Root-Dateisystem einzuhängen. Falls dieser Vorgang erfolgreich ist, wird der Bootvorgang wie gewohnt fortgesetzt.

10.2.3.1 Die Phase init auf initramfs während des Installationsvorgangs

Wenn `init` unter `initramfs` im Rahmen des Installationsvorgangs während des anfänglichen Boot-Vorgangs aufgerufen wird, unterscheiden sich seine Tasks von den oben beschriebenen. Beachten Sie, dass das Installationssystem auch `systemd` aus `initramfs` nicht startet – diese Aufgaben werden von **`linuxrc`** übernommen.

Suchen des Installationsmediums

Beim Starten des Installationsvorgangs lädt der Rechner einen Installations-Kernel und eine besondere `init` mit dem YaST-Installationsprogramm. Das YaST-Installationsprogramm wird in einem RAM-Dateisystem ausgeführt und 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 bereits in *Abschnitt 10.2.2.1, „Die `initramfs`-Datei“* erwähnt, beginnt der Boot-Vorgang mit einem Mindestsatz an Treibern, die für die meisten Hardware-Konfigurationen verwendet werden können. Bei Computern mit AArch64, POWER und AMD64/Intel 64 löst **`linuxrc`** zunächst einen Hardware-Scanvorgang aus, der die Treiber bestimmt, die sich für Ihre Hardwarekonfiguration eignen. Unter IBM z Systems muss beispielsweise über linuxrc oder parmfile eine Liste der Treiber und ihrer Parameter bereitgestellt werden.

Diese Treiber werden zur Erstellung der zum Booten des Systems benötigten, benutzerdefinierten `initramfs`-Datei verwendet. Falls die Module nicht für "boot", sondern für "coldplug" benötigt werden, können sie mit `systemd` geladen werden. Weitere Informationen finden Sie unter *Abschnitt 13.6.4, „Laden der Kernelmodule“*.

Laden des Installationssystems

Wenn die Hardware ordnungsgemäß erkannt wurde, werden die entsprechenden Treiber geladen. Das `udev`-Programm erstellt die speziellen Gerätedateien und **`linuxrc`** startet das Installationssystem mit dem YaST-Installationsprogramm.

Starten von YaST

`linuxrc` startet schließlich YaST, das wiederum die Paketinstallation und die Systemkonfiguration startet.

10.2.4 Die systemd-Phase

Nachdem das „echte“ Root-Dateisystem gefunden wurde, wird es auf Fehler geprüft und eingehängt. Wenn dieser Vorgang erfolgreich ist, wird das `initramfs` bereinigt, und der `systemd`-Daemon wird für das Root-Dateisystem ausgeführt. `systemd` ist das System von Linux sowie dessen Servicemanager. Es handelt sich dabei um den übergeordneten Prozess, der als PID 1 gestartet wird und wie ein init-System agiert, das die Benutzerraumdienste startet und betreibt. Weitere Informationen finden Sie in *Kapitel 13, Der Daemon `systemd`*.

11 UEFI (Unified Extensible Firmware Interface)

Die UEFI (Unified Extensible Firmware Interface) bildet die Schnittstelle zwischen der Firmware, die sich auf der Systemhardware befindet, allen Hardware-Komponenten des Systems und dem Betriebssystem.

UEFI wird auf PC-Systemen immer stärker verbreitet und ersetzt allmählich das bisherige PC-BIOS. UEFI bietet beispielsweise echte Unterstützung für 64-Bit-Systeme und ermöglicht das sichere Booten („Secure Boot“, Firmware-Version 2.3.1c oder höher erforderlich), eine der zentralen Funktionen dieser Schnittstelle. Nicht zuletzt stellt UEFI auf allen x86-Plattformen eine Standard-Firmware bereit.

UEFI eröffnet außerdem die folgenden Vorteile:

- Booten von großen Festplatten (mehr als 2 TiB) mithilfe einer GUID-Partitionstabelle (GPT).
- CPU-unabhängige Architektur und Treiber.
- Flexible Vor-OS-Umgebung mit Netzwerkfunktionen.
- CSM (Compatibility Support Module) zur Unterstützung des Bootens älterer Betriebssysteme über eine PC-BIOS-ähnliche Emulation.

Weitere Informationen finden Sie unter http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface. Die nachfolgenden Abschnitte sollen keinen allgemeinen Überblick über UEFI liefern, sondern sie weisen lediglich darauf hin, wie bestimmte Funktionen in SUSE Linux Enterprise Server implementiert sind.

11.1 Secure Boot

Bei UEFI bedeutet die Absicherung des Bootstrapping-Prozesses, dass eine Vertrauenskette aufgebaut wird. Die „Plattform“ ist die Grundlage dieser Vertrauenskette; im SUSE Linux Enterprise Server-Kontext bilden die Hauptplatine und die On-Board-Firmware diese „Plattform“. Anders gesagt ist dies der Hardware-Hersteller, und die Vertrauenskette erstreckt sich von diesem Hardware-Hersteller zu den Komponentenherstellern, den Betriebssystemherstellern usw.

Das Vertrauen wird durch die Verschlüsselung mit öffentlichen Schlüsseln ausgedrückt. Der Hardware-Hersteller integriert einen sogenannten Plattformschlüssel (Platform Key, PK) in die Firmware, der die Grundlage für das Vertrauen legt. Das Vertrauensverhältnis zu Betriebssystemherstellern und anderen Dritten wird dadurch dokumentiert, dass ihre Schlüssel mit dem PK signiert werden.

Zum Gewährleisten der Sicherheit wird schließlich verlangt, dass die Firmware erst dann einen Code ausführt, wenn dieser Code mit einem dieser „verbürgten“ Schlüssel signiert ist – ein OS-Bootloader, ein Treiber im Flash-Speicher einer PCI-Express-Karte oder auf der Festplatte oder auch eine Aktualisierung der Firmware selbst.

Um Secure Boot nutzen zu können, muss der OS-Loader also mit einem Schlüssel signiert sein, der für die Firmware als verbürgt gilt, und der OS-Loader muss überprüfen, ob der zu ladende Kernel ebenfalls verbürgt ist.

In die UEFI-Schlüsseldatenbank können KEKs (Key Exchange Keys) aufgenommen werden. Auf diese Weise können Sie auch andere Zertifikate nutzen, sofern diese mit dem privaten Teil des PK signiert sind.

11.1.1 Implementierung auf SUSE Linux Enterprise Server

Standardmäßig wird der KEK (Key Exchange Key) von Microsoft installiert.

Anmerkung: GUID-Partitionstabelle (GPT) erforderlich

Die Secure Boot-Funktion ist in UEFI/x86_64-Installationen standardmäßig aktiviert. Die Option *Secure Boot-Unterstützung aktivieren* finden Sie auf der Registerkarte *Bootcode-Optionen* im Dialogfeld *Bootloader-Einstellungen*. Diese Option unterstützt das Booten, wenn Secure Boot in der Firmware aktiviert ist, wobei Sie auch dann booten können, wenn diese Funktion deaktiviert ist.

ABBILDUNG 11.1 SECURE BOOT-UNTERSTÜTZUNG

Für die Secure Boot-Funktion ist eine GUID-Partitionstabelle (GPT) erforderlich, die die bisherige Partitionierung per MBR (Master Boot Record) ersetzt. Wenn YaST während der Installation den EFI-Modus feststellt, wird versucht, eine GPT-Partition zu erstellen. UEFI erwartet die EFI-Programme auf einer FAT-formatierten ESP (EFI-Systempartition).

Zur Unterstützung von UEFI Secure Boot ist im Wesentlichen ein Bootloader mit einer digitalen Signatur erforderlich, den die Firmware als verbürgten Schlüssel erkennt. Die Firmware vertraut diesem Schlüssel a priori und ohne manuelle Intervention.

Hierzu gibt es zwei Möglichkeiten. Die erste Möglichkeit ist die Zusammenarbeit mit Hardware-Herstellern, sodass diese einen SUSE-Schlüssel zulassen, mit dem dann der Bootloader signiert wird. Die zweite Möglichkeit besteht darin, das Windows Logo Certification-Programm von Microsoft zu durchlaufen, damit der Bootloader zertifiziert wird und Microsoft den SUSE-Signierschlüssel anerkennt (also mit dem KEK von Microsoft signiert). Bislang wurde der Loader für SUSE vom UEFI Signing Service (in diesem Fall von Microsoft) signiert.

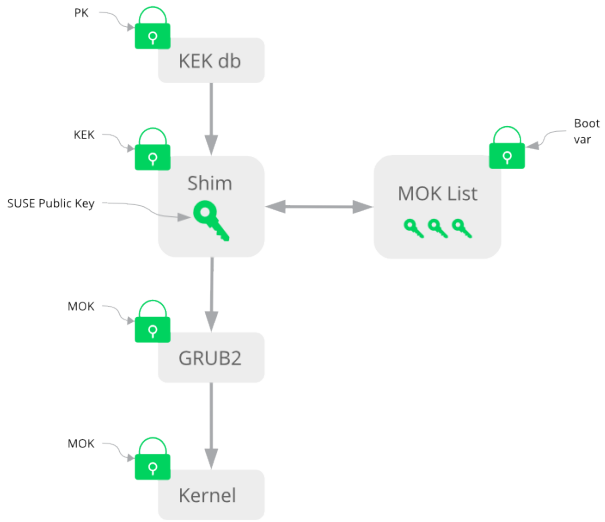


ABBILDUNG 11.2 UEFI: SECURE BOOT-VORGANG

Auf der Implementierungsschicht nutzt SUSE den `shim`-Loader, der standardmäßig installiert wird. Durch diese elegante Lösung werden rechtliche Probleme vermieden und der Zertifizierungs- und Signierungsschritt wird erheblich vereinfacht. Der `shim`-Loader lädt einen Bootloader wie GRUB 2 und überprüft diesen Loader; der Bootloader wiederum lädt ausschließlich Kernels, die mit einem SUSE-Schlüssel signiert sind. SUSE bietet diese Funktion ab SLE11 SP3 in Neuinstallationen, in denen UEFI Secure Boot aktiviert ist.

Es gibt zwei Typen von verbürgten Benutzern.

- Erstens: Benutzer, die die Schlüssel besitzen. Der PK (Platform Key) ermöglicht nahezu alle Aktionen. Der KEK (Key Exchange Key) ermöglicht dieselben Aktionen wie ein PK, mit der Ausnahme, dass der PK hiermit nicht geändert werden kann.

- Zweitens: Benutzer mit physischem Zugang zum Computer. Ein Benutzer mit physischem Zugang kann den Computer neu booten und UEFI konfigurieren.

UEFI bietet zwei Arten von Variablen für die Anforderungen dieser Benutzer:

- Der erste Variablentyp sind die sogenannten „authentifizierten Variablen“, die sowohl aus dem Bootprozess (der sogenannten Boot-Dienstumgebung) und dem laufenden Betriebssystem heraus aktualisiert werden können. Dies ist nur dann möglich, wenn der neue Wert

der Variable mit demselben Schlüssel signiert ist wie der bisherige Wert der Variable. Zudem können diese Variablen nur an einen Wert mit einer höheren Seriennummer angehängt oder in einen Wert mit einer höheren Seriennummer geändert werden.

- Die zweiten Variablen sind die sogenannten „Boot Services Only Variables“ (Variablen für Boot-Services). Diese Variablen stehen jedem Code zur Verfügung, der während des Bootvorgangs ausgeführt wird. Nach Abschluss des Bootvorgangs und vor dem Starten des Betriebssystems muss der Bootloader den Aufruf `ExitBootServices` auslösen. Anschließend sind diese Variablen nicht mehr zugänglich, und das Betriebssystem kann nicht mehr darauf zugreifen.

Die verschiedenen UEFI-Schlüssellisten sind vom ersten Typ, da es damit möglich ist, die Schlüssel, Treiber und Firmware-Fingerabdrücke online zu aktualisieren, hinzuzufügen und in Schwarze Listen einzutragen. Der zweite Variablentyp, also die „Boot Services Only Variables“, unterstützt die Implementierung von Secure Boot auf sichere, Open Source-freundliche und damit GPLv3-kompatible Weise.

SUSE wird mit `shim` gestartet, einem kleinen, einfachen EFI-Bootloader, der von SUSE und Microsoft signiert ist.

Damit kann `shim` geladen und ausgeführt werden.

Anschließend überprüft `shim`, ob der zu ladende Bootloader verbürgt ist. In der Standardsituation verwendet `shim` ein unabhängiges SUSE-Zertifikat, das in diesen Loader integriert ist. Darüber hinaus ermöglicht `shim` das „Registrieren“ weiterer Schlüssel, die Vorrag vor dem SUSE-Standardschlüssel erhalten. Im Folgenden werden diese Schlüssel als MOKs („Machine Owner Keys“) bezeichnet.

Danach überprüft und bootet der Bootloader den Kernel, und der Kernel überprüft und bootet seinerseits die Module.

11.1.2 MOK (Machine Owner Key)

Wenn der Benutzer (der „Machine Owner“, also der Eigentümer des Computers) eine Komponente im Bootvorgang ersetzen möchte, müssen MOKs (Machine Owner Keys) verwendet werden. Das Werkzeug `mokutils` hilft beim Signieren der Komponenten und beim Verwalten der MOKs.

Der Registrierungsvorgang beginnt mit dem Neubooten des Computers und dem Unterbrechen des Bootvorgangs (z. B. durch Drücken einer Taste), wenn `shim` geladen wird. `shim` geht dann in den Registrierungsmodus über, und der Benutzer kann den SUSE-Standardschlüssel durch

Schlüssel aus einer Datei auf der Bootpartition ersetzen. Auf Wunsch des Benutzers kann `shim` dann einen Hash dieser Datei berechnen und das Ergebnis in einer „Boot Services Only“-Variable ablegen. Damit ist `shim` in der Lage, Änderungen an der Datei zu erkennen, die außerhalb der Boot-Services vorgenommen wurden; so wird eine Manipulation der Liste der benutzergenehmigten MOKs unterbunden.

Diese Vorgänge laufen zum Zeitpunkt des Bootens ab – nunmehr wird nur überprüfter Code ausgeführt. Daher kann nur ein Benutzer, der direkt an der Konsole sitzt, die Schlüssel des Computereigentümers verwenden. Bei Malware oder bei einem Hacker mit Fernzugriff auf das Betriebssystem ist dies nicht möglich, da Hacker und Malware lediglich die Datei ändern können, nicht jedoch den Hash, der in der „Boot Services Only“-Variable gespeichert ist.

Nach dem Laden und Überprüfen durch `shim` ruft der Bootloader wiederum `shim` auf, um den Kernel zu überprüfen. So wird eine Duplizierung des Prüfcodes vermieden. `shim` greift hierzu auf dieselbe MOK-Liste zu und teilt dem Bootloader mit, ob der Kernel geladen weden kann.

Auf diese Weise können Sie Ihren eigenen Kernel oder Bootloader installieren. Sie müssen lediglich einen neuen Schlüsselsatz installieren und im Rahmen Ihrer physischen Anwesenheit beim ersten Neubooten bestätigen. Es gibt nicht nur einen MOK, sondern eine ganze MOK-Liste. Aus diesem Grund kann `shim` die Schlüssel von mehreren Herstellern als verbürgt betrachten, sodass auch Dual- und Multi-Boot-Funktionen mit dem Bootloader möglich sind.

11.1.3 Booten eines benutzerdefinierten Kernels

Die folgenden Ausführungen beruhen auf http://en.opensuse.org/openSUSE:UEFI#Booting_a_custom_kernel.

Secure Boot verhindert nicht die Nutzung eines selbst kompilierten Kernels. Sie müssen den Kernel mit Ihrem eigenen Zertifikat signieren und dieses Zertifikat für die Firmware oder den MOK bekanntgeben.

1. Erstellen Sie einen benutzerdefinierten X.509-Schlüssel und ein entsprechendes Zertifikat für die Signierung:

   ```
   openssl req -new -x509 -newkey rsa:2048 -keyout key.asc \
     -out cert.pem -nodes -days 666 -subj "/CN=$USER/"
   ```

   Weitere Informationen zum Erstellen von Zertifikaten finden Sie unter http://en.opensuse.org/openSUSE:UEFI_Image_File_Sign_Tools#Create_Your_Own_Certificate.

2. Verpacken Sie den Schlüssel und das Zertifikat als PKCS#12-Struktur:

```
openssl pkcs12 -export -inkey key.asc -in cert.pem \
  -name kernel_cert -out cert.p12
```

3. Generieren Sie eine NSS-Datenbank für **`pesign`**:

```
certutil -d . -N
```

4. Importieren Sie den Schlüssel und das Zertifikat aus PKCS#12 in die NSS-Datenbank:

```
pk12util -d . -i cert.p12
```

5. „Authentifizieren“ Sie den Kernel mit der neuen Signatur mithilfe von **`pesign`**:

```
pesign -n . -c kernel_cert -i arch/x86/boot/bzImage \
  -o vmlinuz.signed -s
```

6. Listen Sie die Signaturen im Kernel-Image auf:

```
pesign -n . -S -i vmlinuz.signed
```

   Zu diesem Zeitpunkt können Sie den Kernel wie gewohnt in `/boot` installieren. Der Kernel besitzt nun eine benutzerdefinierte Signatur, sodass das Zertifikat zum Signieren in die UEFI-Firmware oder in den MOK importiert werden muss.

7. Konvertieren Sie das Zertifikat zum Importieren in die Firmware oder den MOK in das DER-Format:

```
openssl x509 -in cert.pem -outform der -out cert.der
```

8. Kopieren Sie das Zertifikat aus Gründen des einfacheren Zugriffs in die ESP:

```
sudo cp cert.der /boot/efi/
```

9. Mit **`mokutil`** wird die MOK-Liste automatisch gestartet.

   - a. Importieren Sie das Zertifikat in MOK:

     ```
     mokutil --root-pw --import cert.der
     ```

     Mit der Option `--root-pw` kann der `root`-Benutzer direkt verwendet werden.

b. Prüfen Sie die Liste der Zertifikate, die für die Registrierung vorbereitet werden:

```
mokutil --list-new
```

c. Booten Sie das System neu; mit `shim` sollte MokManager gestartet werden. Um den Import des Zertifikats in die MOK-Liste zu bestätigen, müssen Sie das `root`-Passwort eingeben.

d. Prüfen Sie, ob der soeben importierte Schlüssel registriert wurde:

```
mokutil --list-enrolled
```

- a. Zum manuellen Starten des MOK gehen Sie alternativ wie folgt vor:
  Booten Sie den Computer neu

b. Drücken Sie im GRUB 2-Menü die Taste „`c`“.

c. Typ:

```
chainloader $efibootdir/MokManager.efi
boot
```

d. Wählen Sie *Enroll key from disk (Schlüssel von Festplatte registrieren)*.

e. Navigieren Sie zur Datei `cert.der`, und drücken Sie `Eingabetaste`.

f. Registrieren Sie den Schlüssel gemäß den Anweisungen. In der Regel drücken Sie hierzu „`0`“ und dann zum Bestätigen „`j`“.
  Alternativ können Sie einen neuen Schlüssel über das Firmware-Menü in die Signaturdatenbank aufnehmen.

11.1.4 Verwenden von Nicht-Inbox-Treibern

Das Hinzufügen von Nicht-Inbox-Treibern (also Treibern, die nicht in SUSE Linux Enterprise Server inbegriffen sind) wird bei der Installation mit aktiviertem Secure Boot nicht unterstützt. Der Signierschlüssel für SolidDriver/PLDP gilt standardmäßig nicht als vertrauenswürdig.

Es ist mit zwei Methoden möglich, Treiber von Drittanbietern bei der Installation mit aktiviertem Secure Boot zu nutzen. In beiden Fällen gilt:

- Fügen Sie die erforderlichen Schlüssel vor der Installation mithilfe von Firmware-/Systemverwaltungswerkzeugen in die Firmware-Datenbank ein. Diese Option ist von der jeweils verwendeten Hardware abhängig. Weitere Informationen erhalten Sie bei Ihrem Hardware-Händler.
- Verwenden Sie ein bootfähiges Treiber-ISO-Image von https://drivers.suse.com/ oder von Ihrem Hardware-Händler, mit dem die erforderlichen Schlüssel beim ersten Starten in die MOK-Liste eingetragen werden.

So tragen Sie die Treiberschlüssel mit dem bootfähigen Treiber-ISO-Image in die MOK-Liste ein:

1. Brennen Sie das obige ISO-Image auf eine leere CD/DVD.
2. Starten Sie die Installation von der neuen CD/DVD und halten Sie dabei die standardmäßigen Installationsmedien bzw. die URL zu einem Netzwerkinstallationsserver bereit.
   Wenn Sie eine Netzwerkinstallation vornehmen, geben Sie die URL der Netzwerkinstallationsquelle mit der Option `install=` in die Bootbefehlszeile ein.
   Bei einer Installation von optischen Speichermedien bootet das Installationsprogramm zunächst vom Treiber-Kit; anschließend werden Sie aufgefordert, den ersten Installationsdatenträger für das Produkt einzulegen.
3. Bei der Installation wird ein initrd mit aktualisierten Treibern herangezogen.

Weitere Informationen finden Sie unter https://drivers.suse.com/doc/Usage/Secure_Boot_Certificate.html.

11.1.5 Funktionen und Einschränkungen

Beim Booten im Secure Boot-Modus stehen die folgenden Funktionen zur Verfügung:

- Installation in den Speicherort des UEFI-Standard-Bootloaders (Mechanismus zum Beibehalten oder Wiederherstellen des EFI-Booteintrags).
- Neubooten über UEFI.
- Der Xen-Hypervisor wird mit UEFI gebootet, wenn kein Legacy-BIOS für das Fallback vorhanden ist.

- Unterstützung für das PXE-Booten mit UEFI IPv6.
- Unterstützung für den UEFI-Videomodus; der Kernel kann den Videomodus aus UEFI abrufen und den KMS-Modus mit denselben Parametern konfigurieren.
- Unterstützung für das UEFI-Booten von USB-Geräten.

Beim Booten im Secure Boot-Modus gelten die folgenden Einschränkungen:

- Um zu gewährleisten, dass Secure Boot nicht einfach umgangen werden kann, sind einige Kernelfunktionen beim Ausführen unter Secure Boot deaktiviert.
- Der Bootloader, der Kernel und die Kernelmodule müssen signiert sein.
- Kexec und Kdump sind deaktiviert.
- Der Ruhezustand (Suspend on Disk) ist deaktiviert.
- Der Zugriff auf `/dev/kmem` und `/dev/mem` ist nicht möglich, auch nicht als Root-Benutzer.
- Der Zugriff auf den E/A-Anschluss ist nicht möglich, auch nicht als Root-Benutzer. Alle X11-Grafiktreiber müssen einen Kerneltreiber verwenden.
- Der PCI-BAR-Zugriff über sysfs ist nicht möglich.
- `custom_method` in ACPI ist nicht verfügbar.
- debugfs für das Modul asus-wmi ist nicht verfügbar.
- Der Parameter `acpi_rsdp` hat keine Auswirkungen auf den Kernel.

11.2 Weiterführende Informationen

- http://www.uefi.org – UEFI-Homepage mit den aktuellen UEFI-Spezifikationen.
- Blogeinträge von Olaf Kirch und Vojtěch Pavlík (das obige Kapitel ist stark auf diese Einträge gestützt):
  - http://www.suse.com/blogs/uefi-secure-boot-plan/
  - http://www.suse.com/blogs/uefi-secure-boot-overview/
  - http://www.suse.com/blogs/uefi-secure-boot-details/
- http://en.opensuse.org/openSUSE:UEFI – UEFI mit openSUSE.

12 Der Bootloader GRUB 2

In diesem Kapitel wird die Konfiguration von GRUB 2, dem unter SUSE Linux Enterprise Server verwendeten Bootloader, beschrieben. Diese Anwendung ist der Nachfolger des bisherigen Bootloaders GRUB (nunmehr als „GRUB Legacy“ bezeichnet). GRUB 2 ist seit Version 12 als standardmäßiger Bootloader in SUSE® Linux Enterprise Server eingebunden. Für die Konfiguration der wichtigsten Einstellungen steht ein YaST-Modul bereit. Eine Übersicht über den Bootvorgang finden Sie in *Kapitel 10, Einführung in den Bootvorgang*. Weitere Informationen zur Unterstützung von Secure Boot finden Sie in *Kapitel 11, UEFI (Unified Extensible Firmware Interface)*.

12.1 Hauptunterschiede zwischen GRUB Legacy und GRUB 2

- Die Konfiguration wird in unterschiedlichen Dateien gespeichert.
- Es werden mehr Dateisysteme unterstützt (z. B. Btrfs).
- Dateien auf LVM- oder RAID-Geräten können direkt gelesen werden.
- Die Benutzeroberfläche kann übersetzt und mit Themen gestaltet werden.
- Es steht ein Mechanismus zum Laden von Modulen bereit, die weitere Funktionen (z. B. Dateisysteme) unterstützen.
- Es werden automatisch Boot-Einträge für andere Kernel und Betriebssysteme (z. B. Windows) gesucht und erzeugt.
- Eine minimale Konsole (ähnlich wie Bash aufgebaut) steht zur Verfügung.

12.2 Konfigurationsdateistruktur

Die Konfiguration von GRUB 2 umfasst die folgenden Dateien:

`/boot/grub2/grub.cfg`
: Diese Datei enthält die Konfiguration der Menüpunkte in GRUB 2. Die Datei ersetzt die Datei `menu.lst` in GRUB Legacy. `grub.cfg` wird automatisch mit dem Kommando **`grub2-mkconfig`** erzeugt und sollte nicht bearbeitet werden.

`/boot/grub2/custom.cfg`
: Diese optionale Datei wird beim Booten direkt aus `grub.cfg` erzeugt. Hiermit können Sie benutzerdefinierte Einträge in das Bootmenü aufnehmen. Ab SUSE Linux Enterprise Server werden diese Einträge auch geparst, wenn **`grub-once`** verwendet wird.

`/etc/default/grub`
: Diese Datei steuert die Benutzereinstellungen für GRUB 2 und enthält in der Regel zusätzliche Umgebungseinstellungen, beispielsweise Hintergründe und Themen.

Skripte unter `/etc/grub.d/`
: Die Skripte in diesem Verzeichnis werden beim Ausführen des Kommandos **`grub2-mkconfig`** gelesen. Die zugehörigen Anweisungen werden in die Hauptkonfigurationsdatei `/boot/grub/grub.cfg` integriert.

`/etc/sysconfig/bootloader`
: Diese Konfigurationsdatei wird bei der Konfiguration des Bootloaders mit YaST und bei jeder Installation eines neuen Kernels verwendet. Sie wird vom Perl Bootloader evaluiert, der die Bootloader-Konfigurationsdatei (z. B. `/boot/grub2/grub.cfg` für GRUB 2) entsprechend bearbeitet. `/etc/sysconfig/bootloader` ist keine GRUB 2-spezifische Konfigurationsdatei; die Werte dieser Datei gelten für alle Bootloader, die unter SUSE Linux Enterprise Server installiert sind.

`/boot/grub2/x86_64-efi`, `/boot/grub2/power-ieee1275`, `/boot/grub2/s390x`
: Diese Konfigurationsdateien enthalten architekturspezifische Optionen.

GRUB 2 kann auf mehrere Weisen gesteuert werden. Booteinträge aus einer vorhandenen Konfiguration können im grafischen Menü (Eröffnungsbildschirm) ausgewählt werden. Die Konfiguration wird aus der Datei `/boot/grub2/grub.cfg` geladen, die aus anderen Konfigurationsdateien kompiliert wird (siehe unten). Alle GRUB 2-Konfigurationsdateien gelten als Systemdateien und Sie benötigen `root`-Berechtigungen, um sie bearbeiten zu können.

Anmerkung: Aktivieren von Konfigurationsänderungen

Nach einer manuellen Änderung der GRUB 2-Konfigurationsdateien müssen Sie `grub2-mkconfig` ausführen, damit die Änderungen in Kraft treten. Wenn Sie die Konfiguration jedoch mit YaST bearbeitet haben, ist dies nicht nötig; `grub2-mkconfig` wird in diesem Fall automatisch ausgeführt.

12.2.1 Die Datei `/boot/grub2/grub.cfg`

Hinter dem grafischen Eröffnungsbildschirm mit dem Bootmenü steht die GRUB 2-Konfigurationsdatei `/boot/grub2/grub.cfg`, die alle Informationen zu allen Partitionen oder Betriebssystemen enthält, die über das Menü gebootet werden können.

GRUB 2 liest bei jedem Systemstart die Menüdatei direkt vom Dateisystem neu ein. Es besteht also kein Bedarf, GRUB 2 nach jeder Änderung an der Konfigurationsdatei neu zu installieren. Beim Installieren oder Entfernen von Kernels wird `grub.cfg` automatisch neu aufgebaut.

`grub.cfg` wird mit `grub2-mkconfig` aus der Datei `/etc/default/grub` und aus den Skripten im Verzeichnis `/etc/grub.d/` kompiliert. Ändern Sie die Datei daher in keinem Fall manuell. Bearbeiten Sie stattdessen die zugehörigen Ursprungsdateien, oder bearbeiten Sie die Konfiguration mit dem YaST-*Bootloader*-Modul (siehe *Abschnitt 12.3, „Konfigurieren des Bootloaders mit YaST“*).

12.2.2 Die Datei `/etc/default/grub`

Hier finden Sie allgemeinere Optionen für GRUB 2, beispielsweise den Zeitraum, über den das Menü angezeigt wird, oder das standardmäßig zu bootende Betriebssystem. Mit dem folgenden Kommando erhalten Sie eine Liste aller verfügbaren Optionen:

```
grep "export GRUB_DEFAULT" -A50 /usr/sbin/grub2-mkconfig | grep GRUB_
```

Neben den bereits definierten Variablen kann der Benutzer eigene Variablen festlegen und später in den Skripten im Verzeichnis `/etc/grub.d` verwenden.

Wenn Sie `/etc/default/grub` bearbeitet haben, führen Sie `grub2-mkconfig` aus, damit die Hauptkonfigurationsdatei entsprechend aktualisiert wird.

Anmerkung: Bereich

Alle in dieser Datei festgelegten Optionen sind allgemeine Optionen, die für alle Bootein-träge gelten. Mit den Konfigurationsoptionen GRUB_*_XEN_* legen Sie besondere Optionen für Xen-Kernel oder den Xen-Hypervisor fest. Weitere Informationen finden Sie unten.

`GRUB_DEFAULT`

Hiermit legen Sie den Bootmenüeintrag fest, der standardmäßig gebootet werden soll. Als Wert ist eine Zahl, der vollständige Name eines Menüeintrags oder der Eintrag „saved“ (Gespeichert) zulässig.

Mit `GRUB_DEFAULT=2` wird der dritte Bootmenüeintrag gebootet (gezählt ab 0).

Mit `GRUB_DEFAULT="2>0"` wird der erste Untermenüeintrag im dritten übergeordneten Menüeintrag gebootet.

Mit `GRUB_DEFAULT="Beispiel für Bootmenüeintrag"` wird der Menüeintrag mit dem Titel „Beispiel für Bootmenüeintrag“ gebootet.

Mit `GRUB_DEFAULT=saved` wird der Eintrag gebootet, der mit dem Kommando **`grub2-once`** oder **`grub2-set-default`** angegeben wurde. Während mit **`grub2-reboot`** der Standard-Booteintrag nur für das nächste Neubooten festgelegt wird, bestimmt **`grub2-set-default`** den Standard-Booteintrag bis zur nächsten Änderung. **`grub2-editenv list`** zeigt den nächsten Booteintrag an.

`GRUB_HIDDEN_TIMEOUT`

Hiermit wird ein bestimmter Zeitraum (in Sekunden) abgewartet, bis der Benutzer eine Taste drückt. Während dieses Zeitraums wird erst dann ein Menü angezeigt, wenn der Benutzer eine Taste drückt. Wird während des angegebenen Zeitraums keine Taste gedrückt, so wird die Steuerung an `GRUB_TIMEOUT` übergeben. `GRUB_HIDDEN_TIMEOUT=0` prüft zunächst, ob `Umschalttaste` gedrückt wurde. Falls ja, wird das Bootmenü angezeigt; ansonsten wird sofort der Standard-Menüeintrag gebootet. Dies ist die Standardeinstellung, wenn GRUB 2 nur ein bootfähiges Betriebssystem erkennt.

`GRUB_HIDDEN_TIMEOUT_QUIET`

Bei `false` wird ein Countdown-Zähler auf einem leeren Bildschirm angezeigt, wenn die Funktion `GRUB_HIDDEN_TIMEOUT` aktiv ist.

`GRUB_TIMEOUT`

Dies ist der Zeitraum (in Sekunden), über den das Bootmenü angezeigt wird, bevor der Standard-Booteintrag automatisch gebootet wird. Sobald Sie eine Taste drücken, wird die Zeitbegrenzung aufgehoben und GRUB 2 wartet darauf, dass Sie manuell die gewünschte Auswahl treffen. Mit `GRUB_TIMEOUT=-1` wird das Menü so lange angezeigt, bis Sie den gewünschten Booteintrag manuell auswählen.

`GRUB_CMDLINE_LINUX`

Die Einträge in dieser Zeile werden an die Booteinträge für den normalen Modus und den Wiederherstellungsmodus angehängt. Hiermit können Sie zusätzliche Kernel-Parameter im Booteintrag angeben.

`GRUB_CMDLINE_LINUX_DEFAULT`

Dieser Eintrag entspricht `GRUB_CMDLINE_LINUX`, jedoch mit dem Unterschied, dass die Einträge nur im normalen Modus angehängt werden.

`GRUB_CMDLINE_LINUX_RECOVERY`

Dieser Eintrag entspricht `GRUB_CMDLINE_LINUX`, jedoch mit dem Unterschied, dass die Einträge nur im Wiederherstellungsmodus angehängt werden.

`GRUB_CMDLINE_LINUX_XEN_REPLACE`

Dieser Eintrag ersetzt sämtliche `GRUB_CMDLINE_LINUX`-Parameter für alle Xen-Booteinträge.

`GRUB_CMDLINE_LINUX_XEN_REPLACE_DEFAULT`

Dieser Eintrag entspricht `GRUB_CMDLINE_LINUX_XEN_REPLACE`, jedoch mit dem Unterschied, dass nur Parameter für `GRUB_CMDLINE_LINUX_DEFAULT` ersetzt werden.

`GRUB_CMDLINE_XEN`

Mit diesem Eintrag werden die Kernel-Parameter ausschließlich für den Xen-Gastkernel bestimmt; die Funktionsweise entspricht `GRUB_CMDLINE_LINUX`.

`GRUB_CMDLINE_XEN_DEFAULT`

Dieser Eintrag entspricht `GRUB_CMDLINE_XEN`; die Funktionsweise entspricht `GRUB_CMDLINE_LINUX_DEFAULT`.

`GRUB_TERMINAL`

Hiermit wird ein Eingabe-/Ausgabe-Terminal-Geräte angegeben und aktiviert. Mögliche Werte sind `console` (PC-BIOS- und EFI-Konsolen), `serial` (serielle Terminals), `ofconsole` (Open-Firmware-Konsolen) sowie der Standardwert `gfxterm` (Ausgabe im Grafikmodus). Sollen mehrere Geräte aktiviert werden, setzen Sie die Optionen in Anführungszeichen, beispielsweise `GRUB_TERMINAL="console serial"`.

`GRUB_GFXMODE`

Dies ist die Auflösung für das grafische Terminal `gfxterm`. Hierbei sind ausschließlich die Modi verfügbar, die von Ihrer Grafikkarte (VBE) unterstützt werden. Die Standardeinstellung lautet „auto“; hiermit wird nach Möglichkeit eine bevorzugte Auflösung ausgewählt. Mit dem Kommando **`videoinfo`** in der GRUB 2-Kommandozeile werden die verfügbaren Bildschirmauflösungen für GRUB 2 angezeigt. Zum Öffnen der Kommandozeile drücken Sie C, wenn der GRUB 2-Bootmenübildschirm angezeigt wird.

Außerdem können Sie eine Farbtiefe an die Einstellung für die Auflösung anhängen, z. B. `GRUB_GFXMODE=1280x1024x24`.

`GRUB_BACKGROUND`

Hiermit legen Sie ein Hintergrundbild für das grafische Terminal `gfxterm` fest. Das Bild muss in einer Datei gespeichert sein, die GRUB 2 beim Booten lesen kann, und die Dateinamenerweiterung muss `.png`, `.tga`, `.jpg` oder `.jpeg` lauten. Falls erforderlich, wird das Bild auf die Bildschirmgröße skaliert.

`GRUB_DISABLE_OS_PROBER`

Bei `true` wird die automatische Suche nach anderen Betriebssystemen deaktiviert. Nur die Kernel-Images in `/boot/` und die Optionen aus Ihren eigenen Skripten in `/etc/grub.d/` werden erkannt.

`SUSE_BTRFS_SNAPSHOT_BOOTING`

Bei `true` kann GRUB 2 direkt in Snapper-Snapshots booten. Weitere Informationen finden Sie unter *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots“*.

Eine vollständige Liste der Optionen finden Sie im Handbuch zu GNU GRUB (http://www.gnu.org/software/grub/manual/grub.html#Simple-configuration). Eine vollständige Liste der zulässigen Parameter finden Sie unter http://en.opensuse.org/Linuxrc.

12.2.3 Skripte in `/etc/grub.d`

Die Skripte in diesem Verzeichnis werden beim Ausführen des Kommandos **`grub2-mkconfig`** gelesen, und die Anweisungen aus diesen Skripten werden in die Datei `/boot/grub2/grub.cfg` eingegliedert. Die Reihenfolge der Menüpunkte in `grub.cfg` ergibt sich aus der Reihenfolge, in der die Dateien in diesem Verzeichnis ausgeführt werden. Dateien mit einer Zahl am Anfang des Dateinamens werden zuerst ausgeführt, beginnend mit der niedrigsten Zahl. `00_header` wird beispielsweise vor `10_linux` ausgeführt, das wiederum vor `40_custom` ausgeführt wird. Dateien mit einem Buchstaben an der ersten Stelle im Dateinamen werden nach den Dateien mit Zahlen am Anfang ausgeführt. Nur ausführbare Dateien erzeugen beim Ausführen von **`grub2-mkconfig`** eine Ausgabe in `grub.cfg`. Standardmäßig sind alle Dateien im Verzeichnis `/etc/grub.d` ausführbar.

Tipp: Persistenter benutzerdefinierter Inhalt in `grub.cfg`

`/boot/grub2/grub.cfg` wird bei jedem Ausführen von **`grub2-mkconfig`** neu kompiliert, sodass benutzerdefinierte Inhalte verloren gehen. Möchten Sie die Zeilen direkt in `/boot/grub2/grub.cfg` einfügen, damit sie nach dem Ausführen von **`grub2-mkconfig`** nicht verloren gehen, fügen Sie sie zwischen den folgenden Zeilen ein:

```
### BEGIN /etc/grub.d/90_persistent ###
```

und

```
### END /etc/grub.d/90_persistent ###
```

Das Skript `90_persistent` sorgt dafür, dass diese Inhalte erhalten bleiben.

Hier finden Sie eine Liste der wichtigsten Skripten:

`00_header`

Hiermit werden Umgebungsvariablen festgelegt, beispielsweise der Speicherort von Systemdateien, Anzeigeeinstellungen, Themen und zuvor gespeicherte Einträge. Außerdem werden die Voreinstellungen aus der Datei `/etc/default/grub` importiert. In der Regel sind keine Änderungen an dieser Datei notwendig.

`10_linux`

Hiermit werden Linux-Kernel im root-Gerät erkannt und relevante Menüeinträge erstellt. Hierbei wird auch die zugehörige Option für den Wiederherstellungsmodus berücksichtigt (sofern aktiviert). Auf der Hauptmenüseite wird nur der jüngste Kernel angezeigt; weitere Kernel werden in einem Untermenü aufgeführt.

`30_os-prober`

Bei diesem Skript werden Linux und andere Betriebssysteme mithilfe von **`OS-prober`** gesucht und die Ergebnisse werden in das GRUB 2-Menü eingetragen. Das Skript bietet Abschnitte für die Erkennung bestimmter anderer Betriebssysteme (z. B. Windows oder macOS).

`40_custom`

Mit dieser Datei können Sie schnell und einfach benutzerdefinierte Booteinträge in `grub.cfg` einbinden. Der Bestandteil `exec tail -n +3 $0` am Anfang darf dabei nicht geändert werden.

Die Verarbeitungsreihenfolge ergibt sich aus den Zahlen am Anfang des Skriptnamens, wobei das Skript mit der niedrigsten Zahl zuerst ausgeführt wird. Wenn mehrere Skripte mit derselben Zahl beginnen, entscheidet die alphabetische Sortierung des vollständigen Namens über die endgültige Reihenfolge.

Tipp: `/boot/grub2/custom.cfg`

Wenn Sie `/boot/grub2/custom.cfg` erstellen und benutzerdefinierte Inhalte eintragen, werden diese Inhalte beim Booten automatisch gleich nach 40_custom in `/boot/grub40/grub.cfg` aufgenommen.

12.2.4 Zuordnung von BIOS-Laufwerken und Linux-Geräten

In GRUB Legacy wurden die Linux-Geräte mithilfe der Konfigurationsdatei `device.map` aus den Nummern der BIOS-Laufwerke abgeleitet. Die Zuordnung von BIOS-Laufwerken und Linux-Geräten ist jedoch nicht in jedem Fall fehlerfrei erkennbar. Wenn Sie beispielsweise die Reihenfolge der IDE- und SCSI-Laufwerke in der BIOS-Konfiguration vertauschen, entsteht in GRUB Legacy eine falsche Reihenfolge.

In GRUB 2 werden beim Erzeugen der Datei `grub.cfg` dagegen Geräte-ID-Zeichenfolgen (UUIDs) oder Dateisystemkennungen erzeugt, damit dieses Problem vermieden wird. In GRUB 2 wird eine interaktive temporäre Gerätezuordnung genutzt, die in der Regel ausreicht, insbesondere bei Systemen mit nur einer Festplatte.

Falls die automatische Zuordnung in GRUB 2 außer Kraft gesetzt werden soll, legen Sie eine benutzerdefinierte Zuordnungsdatei mit dem Dateinamen `/boot/grub2/device.map` an. Im nachfolgenden Beispiel wird die Zuordnung so geändert, dass `DISK 3` das Bootlaufwerk ist. Beachten Sie, dass die GRUB 2-Partitionsnummern mit `1` beginnen, nicht mit `0` wie in GRUB Legacy.

```
(hd1)  /dev/disk-by-id/DISK3 ID
(hd2)  /dev/disk-by-id/DISK1 ID
(hd3)  /dev/disk-by-id/DISK2 ID
```

12.2.5 Ändern von Menüeinträgen während des Bootvorgangs

Das direkte Bearbeiten von Menüeinträgen eröffnet einen Ausweg, wenn das System aufgrund einer fehlerhaften Konfiguration nicht mehr gebootet werden kann. Hiermit können Sie außerdem neue Einstellungen testen, ohne die bestehende Systemkonfiguration ändern zu müssen.

1. Wählen Sie im grafischen Bootmenü den zu bearbeitenden Eintrag mit den Pfeiltasten aus.
2. Drücken Sie E. Der Texteditor wird geöffnet.
3. Wechseln Sie mit den Pfeiltasten zur Zeile, die bearbeitet werden soll.

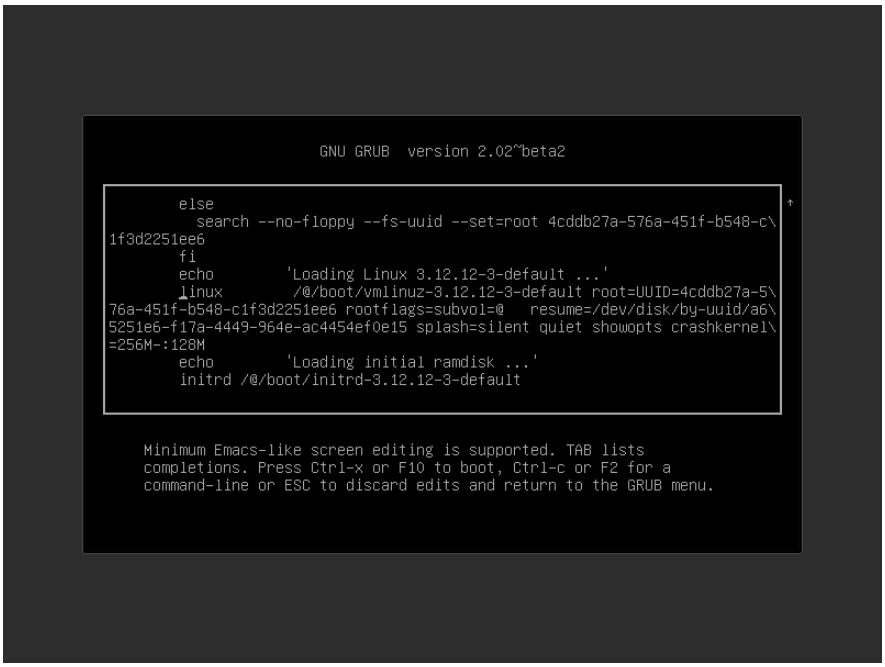


ABBILDUNG 12.1 BOOTEDITOR IN GRUB 2

Anschließend haben Sie zwei Möglichkeiten:

a. Zum Bearbeiten der Kernel-Parameter fügen Sie die gewünschten Parameter (jeweils durch ein Leerzeichen getrennt) am Ende der Zeile an, die mit `linux` oder `linuxefi` beginnt. Unter http://en.opensuse.org/Linuxrc finden Sie eine vollständige Liste der Parameter.

b. Alternativ bearbeiten Sie die zu ändernden Optionen, z. B. die Kernelversion. Mit der Taste `→|` erhalten Sie die möglichen Vervollständigungsoptionen.

4. Mit `F10` booten Sie das System mit den vorgenommenen Änderungen, mit `Esc` verwerfen Sie Ihre Änderungen und kehren zum GRUB 2-Menü zurück.

Auf diese Weise vorgenommene Änderungen gelten nur für den aktuellen Bootvorgang und werden nicht dauerhaft gespeichert.

Wichtig: Tastaturbelegung während des Bootvorgangs

Beim Bootvorgang ist nur die amerikanische Tastaturbelegung verfügbar. Weitere Informationen hierzu finden Sie unter *Abbildung 40.2, „US-Tastaturbelegung“*.

Anmerkung: Bootloader auf den Installationsmedien

Die Installationsmedien für Systeme mit herkömmlichen BIOS enthalten nach wie vor GRUB Legacy als Bootloader. Zum Hinzufügen von Bootoptionen wählen Sie einen Eintrag aus, und beginnen Sie mit der Eingabe. Die Ergänzungen des Installations-Booteintrags werden dauerhaft im installierten System gespeichert.

Anmerkung: Bearbeiten von GRUB 2-Menüeinträgen auf z Systems

Für IBM z Systems gelten andere Cursorbewegungen und andere Bearbeitungsbefehle. Weitere Informationen finden Sie unter *Abschnitt 12.4, „Unterschiede bei der Terminalnutzung auf z Systems“*.

12.2.6 Festlegen eines Bootpassworts

GRUB 2 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 Menüeinträge zu verhindern, können Sie ein Bootpasswort festlegen.

Wichtig: Booten erfordert ein Passwort

Das Bootpasswort muss dann bei jedem Booten eingegeben werden; das System wird also nicht automatisch gebootet.

Legen Sie das Bootpasswort gemäß den nachfolgenden Anweisungen fest. Alternativ verwenden Sie YaST (*Bootloader durch Passwort schützen*).

1. Verschlüsseln Sie das Passwort mit **`grub2-mkpasswd-pbkdf2`**:

   ```
   tux >  sudo grub2-mkpasswd-pbkdf2
   Password: ****
   Reenter password: ****
   PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.9CA4611006FE96BC77A...
   ```

2. Fügen Sie die resultierende Zeichenfolge zusammen mit dem Kommando **`set superusers`** in die Datei `/etc/grub.d/40_custom` ein.

```
set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.10000.9CA4611006FE96BC77A...
```

3. Führen Sie **grub2-mkconfig** aus, damit die Änderungen in die Hauptkonfigurationsdatei importiert werden.

Nach dem Neubooten werden Sie aufgefordert, einen Benutzernamen und ein Passwort einzugeben, sobald Sie versuchen, einen Menüeintrag zu booten. Geben Sie `root` und das Passwort ein, das Sie mit dem Kommando **grub2-mkpasswd-pbkdf2** erstellt haben. Wenn der Berechtigungsnachweis fehlerfrei ist, bootet das System den angegebenen Booteintrag.

Weitere Informationen finden Sie unter https://www.gnu.org/software/grub/manual/grub.html#Security.

12.3 Konfigurieren des Bootloaders mit YaST

Mit dem YaST-Modul ist die Konfiguration des Bootloaders auf Ihrem SUSE Linux Enterprise-Server am einfachsten. Wählen Sie im *YaST-Kontrollzentrum* die Option *System* › *Bootloader*. Das Modul zeigt die aktuelle Bootloader-Konfiguration des Systems und ermöglicht Ihnen, Änderungen vorzunehmen.

Verwenden Sie den Karteireiter *Boot-Code-Optionen*, um die Einstellungen in Bezug auf Typ, Speicherort und erweiterte Bootloader-Einstellungen anzuzeigen und zu ändern. Sie können festlegen, ob GRUB 2 im Standardmodus oder im EFI-Modus verwendet werden soll.

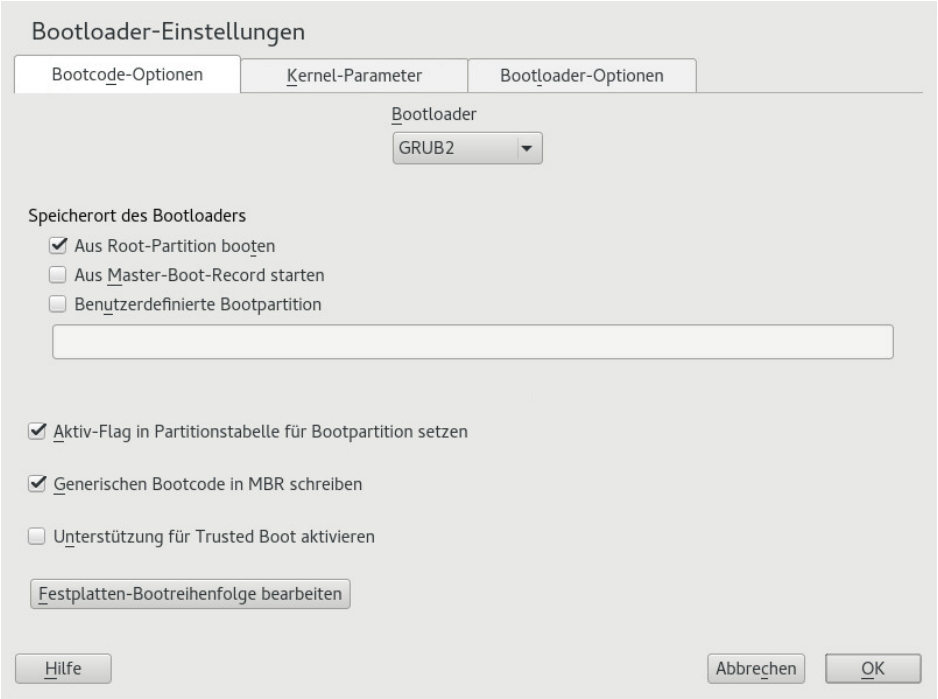


ABBILDUNG 12.2 BOOTCODE-OPTIONEN

Wichtig: GRUB2-EFI für EFI-Systeme erforderlich

Bei einem EFI-System können Sie nur GRUB2-EFI installieren, da das System ansonsten nicht mehr bootfähig ist.

Wichtig: Neuinstallation des Bootloaders

Um den Bootloader neu zu installieren, muss eine Einstellung in YaST geändert und wieder zurückgesetzt werden. Um beispielsweise GRUB2-EFI neu zu installieren, wählen Sie zuerst *GRUB2* aus und wechseln Sie sofort wieder zurück zu *GRUB2-EFI*.

Ansonsten wird der Bootloader möglicherweise nur zum Teil neu installiert.

Anmerkung: Benutzerdefinierter Bootloader

Wenn Sie einen anderen Bootloader außer den aufgeführten Bootloadern verwenden möchten, wählen Sie *Keinen Bootloader installieren*. Lesen Sie die Dokumentation Ihres Bootloaders sorgfältig durch, bevor Sie diese Option auswählen.

12.3.1 Speicherort des Bootloaders und Boot-Code-Optionen

Der Standardspeicherort des Bootloaders ist abhängig von der Partitionseinrichtung – es handelt sich entweder um den Master Boot Record (MBR) oder den Bootsektor der Partition `/`. Um den Speicherort des Bootloaders zu ändern, gehen Sie wie folgt vor:

PROZEDUR 12.1 SPEICHERORT DES BOOTLOADERS ÄNDERN

1. Wählen Sie den Karteireiter *Boot-Code-Optionen* und anschließend eine der folgenden Optionen für *Speicherort des Bootloaders*:

   Booten vom Master Boot Record

   Hiermit wird der Bootloader in den MBR der Festplatte installiert, auf der sich das Verzeichnis `/boot` befindet. In der Regel ist dies die Festplatte, die in `/` eingehängt ist. Falls `/boot` in einer anderen Partition auf einer anderen Festplatte eingehängt ist, wird entsprechend der MBR der anderen Festplatte herangezogen.

   Booten von der root-Partition

   Der Bootloader wird in den Bootsektor der Partition `/` installiert.

   Benutzerdefinierte Bootpartition

   Mit dieser Option können Sie den Speicherort des Bootloaders manuell angeben.

2. Klicken Sie zum Anwenden der Änderungen auf *OK*.

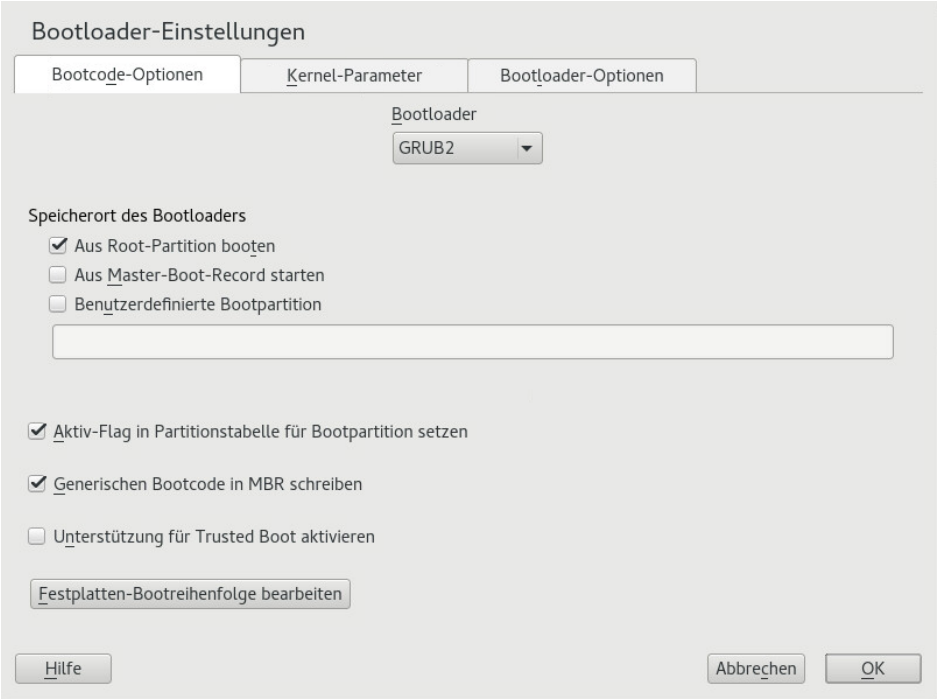


ABBILDUNG 12.3 CODE-OPTIONEN

Die Registerkarte *Boot-Code-Optionen* enthält die folgenden zusätzlichen Optionen:

Aktiv-Flag in Partitionstabelle für Bootpartition festlegen

Aktiviert die Partition, die das `/boot`-Verzeichnisdie PReP-Partition enthält. Verwenden Sie diese Option auf Systemen mit älterem BIOS und/oder älteren Betriebssystemen, da diese Systeme unter Umständen nicht von einer nicht aktiven Partition gebootet werden können. Diese Option kann problemlos aktiviert bleiben.

Generischen Bootcode in MBR schreiben

Wenn der MBR einen benutzerdefinierten „Nicht-GRUB-Code“ enthält, ersetzt diese Option diesen Code durch einen generischen, betriebssystemunabhängigen Code. Wenn Sie diese Option deaktivieren, ist das System eventuell nicht mehr bootfähig.

Unterstützung für Trusted Boot aktivieren

Startet TrustedGRUB2, womit die Funktion für Trusted Computing (Trusted Platform Module (TPM)) unterstützt wird. Weitere Informationen finden Sie unter https://github.com/Sirrix-AG/TrustedGRUB2.

12.3.2 Anpassen der Festplattenreihenfolge

Wenn der Rechner mit mehreren Festplatten ausgestattet ist, können Sie die Bootreihenfolge für die Festplatten festlegen. GRUB 2 wird auf der ersten Festplatte in der Liste installiert, wenn vom MBR gebootet wird. Auf dieser Festplatte wird SUSE Linux Enterprise Server standardmäßig installiert. Die restlichen Einträge in der Liste bilden Hinweise für den Geräte-Mapper von GRUB 2 (siehe *Abschnitt 12.2.4, „Zuordnung von BIOS-Laufwerken und Linux-Geräten“*).

Warnung: Nicht bootfähiges System

Der Standardwert gilt in der Regel für nahezu alle Bereitstellungen. Wenn Sie die Bootreihenfolge der Festplatten falsch ändern, ist das System beim nächsten Booten unter Umständen nicht mehr bootfähig. Dies ist beispielsweise der Fall, wenn die erste Festplatte in der Liste nicht in der BIOS-Bootreihenfolge aufgeführt und der MBR der anderen Festplatte in der Liste leer ist.

PROZEDUR 12.2 FESTLEGEN DER FESTPLATTENREIHENFOLGE

1. Öffnen Sie den Karteireiter *Boot-Code-Optionen*.
2. Klicken Sie auf *Festplatten-Bootreihenfolge bearbeiten*.
3. Ändern Sie bei mehreren aufgeführten Festplatten deren Reihenfolge mit einem Klick auf *Auf* oder *Ab*.
4. Klicken Sie zweimal auf *OK*, um die Änderungen zu speichern.

12.3.3 Konfigurieren der erweiterten Optionen

Erweiterte Boot-Optionen lassen sich über die Registerkarte *Bootloader-Optionen* konfigurieren.

12.3.3.1 Registerkarte *Bootloader-Optionen*

ABBILDUNG 12.4 BOOTLOADER-OPTIONEN

Zeitlimit des Bootloaders

Zum Ändern des Werts für *Zeitüberschreitung in Sekunden* geben Sie einen neuen Wert ein, und klicken Sie mit der Maus auf die entsprechenden Pfeilschaltfläche.

Fremdes OS testen

Mit dieser Option sucht der Bootloader nach anderen Systemen, z. B. Windows oder andere Linux-Installationen.

Menü beim Booten verbergen

Blendet das Bootmenü aus und bootet den Standardeintrag.

Anpassen des Standard-Boot-Eintrags

Wählen Sie den gewünschten Eintrag in der Liste „Standard-Bootabschnitt“ aus. Beachten Sie, dass das Zeichen „>“ im Namen des Booteintrags den Bootabschnitt und den zugehörigen Unterabschnitt begrenzt.

Bootloader durch Passwort schützen

Schützt den Bootloader und das System mit einem zusätzlichen Passwort. Weitere Informationen finden Sie unter *Abschnitt 12.2.6, „Festlegen eines Bootpassworts“*.

12.3.3.2 Registerkarte *Kernel-Parameter*

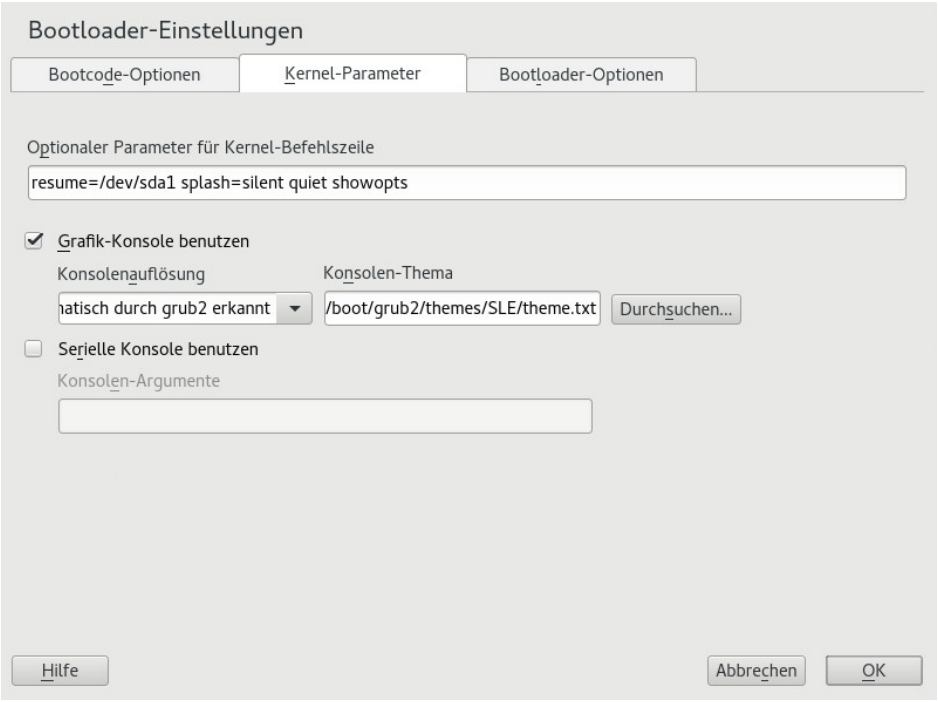


ABBILDUNG 12.5 KERNEL-PARAMETER

Konsolenauflösung

Mit der Option *Konsolenauflösung* legen Sie die standardmäßige Bildschirmauflösung für den Bootvorgang fest.

Kernel Command Line Parameter **(Kernel-Befehlszeilenparameter)**

Die optionalen Kernel-Parameter werden an die Standardparameter angehängt. Eine Liste aller zulässigen Parameter finden Sie unter http://en.opensuse.org/Linuxrc.

Grafik-Konsole benutzen

Wenn diese Option aktiviert ist, wird das Bootmenü nicht im Textmodus dargestellt, sondern in einem grafischen Begrüßungsbildschirm. Hierbei können Sie die Auflösung des Bootbildschirms über die Liste *Konsolenauflösung* festlegen und die Definitionsdatei für das grafische Thema mit der Dateiauswahl *Konsolen-Thema*.

Serielle Konsole verwenden

Wenn Ihr Computer über eine serielle Konsole gesteuert wird, aktivieren Sie diese Option und geben Sie an, welcher COM-Port in welcher Geschwindigkeit verwendet werden soll. Siehe `info grub` oder http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal.

12.4 Unterschiede bei der Terminalnutzung auf z Systems

Auf 3215- und 3270-Terminals gelten bestimmte Unterschiede und Einschränkungen beim Bewegen des Cursors und beim Verwenden von Bearbeitungskommandos in GRUB 2.

12.4.1 Einschränkungen

Interaktivität

Die Interaktivität wird dringend empfohlen. Bei der Eingabe erfolgt häufig keine visuelle Rückmeldung. Zum Ermitteln der Cursorposition geben Sie einen Unterstrich (_) ein.

Anmerkung: 3270 im Vergleich zu 3215

Das 3270-Terminal bietet eine bessere Darstellung und Bildschirmaktualisierung als das 3215-Terminal.

Cursorbewegung

Die „herkömmliche“ Cursorbewegung ist nicht möglich. Alt, Meta, Strg und die Cursortasten sind nicht funktionsfähig. Bewegen Sie den Cursor mit den Tastenkombinationen in *Abschnitt 12.4.2, „Tastenkombinationen“*.

Caret

Das Caret ^ dient als Steuerzeichen. Zur Eingabe eines Buchstabens mit Caret ^ geben Sie Folgendes ein: ^, ^, *BUCHSTABE*.

Geben Sie ein:

Die Eingabetaste-Taste ist nicht funktionsfähig; drücken Sie stattdessen ^–J.

12.4.2 Tastenkombinationen

Häufig ersetzt durch:	^–J	Erfassen („Eingabetaste“)
	^–L	Abbrechen, zum letzten „Status“ zurückkehren

	^ – I	Karteireiter ausfüllen (im Bearbeitungs- und Shell-Modus)
Verfügbare Tasten im Menümodus:	^ – A	Erster Eintrag
	^ – E	Letzter Eintrag
	^ – P	Vorheriger Eintrag
	^ – N	Nächster Eintrag
	^ – G	Vorherige Seite
	^ – C	Nächste Seite
	^ – F	Ausgewählten Eintrag booten oder Untermenü öffnen (entspricht ^ – J)
	E	Ausgewählten Eintrag bearbeiten
	C	GRUB-Shell öffnen
Verfügbare Tasten im Bearbeitungsmodus:	^ – P	Vorherige Zeile
	^ – N	Nächste Zeile
	^ – B	Ein Zeichen zurück
	^ – F	Ein Zeichen weiter
	^ – A	Zeilenanfang
	^ – E	Zeilenende
	^ – H	Rücktaste
	^ – D	Löschen

	^ – K	Zeile schließen
	^ – Y	Kopieren
	^ – O	Zeile öffnen
	^ – L	Bildschirm aktualisieren
	^ – X	Eintrag booten
	^ – C	GRUB-Shell öffnen
Verfügbare Tasten im Kommandozeilenmodus:	^ – P	Vorheriges Kommando
	^ – N	Nächstes Kommando im Verlauf
	^ – A	Zeilenanfang
	^ – E	Zeilenende
	^ – B	Ein Zeichen zurück
	^ – F	Ein Zeichen weiter
	^ – H	Rücktaste
	^ – D	Löschen
	^ – K	Zeile schließen
	^ – U	Zeile verwerfen
	^ – Y	Kopieren

12.5 Nützliche Kommandos in GRUB 2

`grub2-mkconfig`

Hiermit wird eine neue Datei `/boot/grub2/grub.cfg` auf der Grundlage von `/etc/default/grub` und der Skripten in `/etc/grub.d/` erzeugt.

BEISPIEL 12.1 VERWENDUNG VON GRUB2-MKCONFIG

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Tipp: Syntaxprüfung

Wenn Sie **`grub2-mkconfig`** ohne Parameter ausführen, wird die Konfiguration an STDOUT ausgegeben und kann dort abgerufen werden. Zur Syntaxprüfung führen Sie **`grub2-script-check`** aus, sobald die Datei `/boot/grub2/grub.cfg` geschrieben wurde.

Wichtig: Mit **`grub2-mkconfig`** können UEFI Secure Boottabellen nicht repariert werden

Wenn Sie UEFI Secure Boot verwenden und Ihr System GRUB 2 nicht mehr ordnungsgemäß erreichen kann, müssen Sie möglicherweise zusätzlich Shim neu installieren und die UEFI-Boottabelle regenerieren. Verwenden Sie hierzu das folgende Kommando:

```
root # shim-install --config-file=/boot/grub2/grub.cfg
```

`grub2-mkrescue`

Hiermit wird ein bootfähiges Rettungs-Image der installierten GRUB 2-Konfiguration erstellt.

BEISPIEL 12.2 VERWENDUNG VON GRUB2-MKRESCUE

```
grub2-mkrescue -o save_path/name.iso iso
```

`grub2-script-check`

Hiermit prüfen Sie die angegebene Datei auf Syntaxfehler.

BEISPIEL 12.3 VERWENDUNG VON GRUB2-SCRIPT-CHECK

```
grub2-script-check /boot/grub2/grub.cfg
```

`grub2-once`

Hiermit legen Sie den Standard-Booteintrag für den nächsten Bootvorgang fest (dies wird nicht dauerhaft gespeichert). Mit der Option `--list` erhalten Sie eine Liste der verfügbaren Booteinträge.

BEISPIEL 12.4 VERWENDUNG VON GRUB2-ONCE

```
grub2-once number_of_the_boot_entry
```

Tipp: **`grub2-once`**-Hilfe

Wenn Sie das Programm ohne Angabe von Optionen aufrufen, erhalten Sie eine vollständige Liste der zulässigen Optionen.

12.6 Weitere Informationen

Umfassende Informationen zu GRUB 2 finden Sie unter http://www.gnu.org/software/grub/. Ausführliche Informationen finden Sie auch auf der Infoseite für das Kommando **`grub`**. Weitere Informationen zu bestimmten Themen erhalten Sie auch, wenn Sie „GRUB 2“ in der Suchfunktion für technische Informationen unter http://www.suse.com/support als Suchwort eingeben.

13 Der Daemon systemd

Das Programm `systemd` trägt die Prozess-ID 1. Hiermit wird das System in der erforderlichen Form initialisiert. `systemd` wird direkt vom Kernel gestartet und widersteht dem Signal 9, das in der Regel Prozesse beendet. Alle anderen Programme werden entweder direkt von systemd oder von einem seiner untergeordneten Prozesse gestartet.

Ab SUSE Linux Enterprise Server 12 ersetzt systemd den beliebten System V-init-Daemon. `systemd` ist mit System V init uneingeschränkt kompatibel (init-Skripten werden unterstützt). Einer der wichtigsten Vorteile von systemd ist die deutliche Beschleunigung des Bootvorgangs, da die Dienststarts konsequent parallel ausgeführt werden. Darüber hinaus startet systemd einen Dienst nur dann, wenn er tatsächlich benötigt wird. Deamons werden nicht in jedem Fall beim Booten gestartet, sondern erst dann, wenn sie erstmalig benötigt werden. systemd unterstützt außerdem Kernel-Steuergruppen (cgroups), das Erstellen von Snapshots, das Wiederherstellen des Systemstatus und vieles mehr. Weitere Informationen finden Sie in http://www.freedesktop.org/wiki/Software/systemd/.

13.1 Das Konzept von &systemd

In diesem Abschnitt wird das Konzept von systemd eingehend beleuchtet.

13.1.1 Grundlagen von systemd

systemd ist ein System- und Sitzungsmanager für Linux und ist mit System V- und LSB-init-Skripts kompatibel. Die wichtigsten Funktionen sind:

- Konsequente Parallelisierung
- Starten von Diensten per Socket- und D-Bus-Aktivierung
- Starten der Daemons bei Bedarf
- Verfolgen der Prozesse, die Linux-cgroups nutzen
- Unterstützung für das Erstellen von Snapshots und Wiederherstellen des Systemstatus
- Einhängepunkte und Automount-Punkte
- Ausgereifte Dienststeuerlogik auf der Basis der Transaktionsabhängigkeiten

13.1.2 Unit-Datei

Eine Unit-Konfigurationsdatei enthält Informationen zu einem Dienst, Socket, Gerät, Einhängepunkt, Automount-Punkt, einer Auslagerungsdatei oder Partition, einem Startziel, einem überwachten Dateisystempfad, einem von systemd gesteuerten und überwachten Zeitgeber, einem Snapshot eines temporären Systemstatus, einem Ressourcenverwaltungs-Slice oder einer Gruppe extern erstellter Prozesse. „Unit-Datei“ ist in systemd ein generischer Term für Folgendes:

- **Dienst.** Informationen zu einem Prozess (z. B. Ausführung eines Daemon); Datei endet auf .service
- **Ziele.** Fassen Units zu Gruppen zusammen bzw. fungieren als Synchronisierungspunkte beim Starten; Datei endet auf .target
- **Sockets.** Informationen zu einem IPC- oder Netzwerk-Socket oder einem Dateisystem-FIFO, für die socketbasierte Aktivierung (wie `inetd`); Datei endet auf .socket
- **Pfad.** Dient als Auslöser von anderen Units (z. B. Ausführen eines Dienstes, wenn Dateien geändert werden); Datei endet auf .path
- **Zeitgeber.** Informationen zu einem gesteuerten Zeitgeber für die zeitgeberbasierte Aktivierung; Datei endet auf .timer
- **Einhängepunkt.** In der Regel automatisch durch den fstab-Generator erzeugt; Datei endet auf .mount
- **Automount-Punkt.** Informationen zu einem Dateisystem-Automount-Punkt; Datei endet auf .automount
- **Swap.** Informationen zu einem Auslagerungsgerät oder einer Auslagerungsdatei für das Arbeitsspeicher-Paging; Datei endet auf .swap
- **Gerät.** Informationen zu einer Geräte-Unit in der Geräte-Baumstruktur sysfs/udev(7); Datei endet auf .device
- **Bereich/Slice.** Konzept für die hierarchische Verwaltung von Ressourcen einer Prozessgruppe; Datei endet auf .scope/.slice

Weitere Informationen zu systemd.unit finden Sie unter http://www.freedesktop.org/software/systemd/man/systemd.unit.html.

13.2 Grundlegende Verwendung

Im System V-init-System werden Dienste mit mehreren Kommandos verarbeitet – mit init-Skripten, **`insserv`**, **`telinit`** und anderen. systemd erleichtert die Dienstverwaltung, da ein einziges Kommando die meisten Dienstverarbeitungsaufgaben abdeckt: **`systemctl`**. Hierbei gilt die Syntax „Kommando plus Subkommando“ wie bei **`git`** oder **`zypper`**:

```
systemctl GENERAL OPTIONS SUBCOMMAND SUBCOMMAND OPTIONS
```

Vollständige Anweisungen finden Sie in **`man 1 systemctl`**.

Tipp: Terminalausgabe und Bash-Vervollständigung

Wenn die Ausgabe an ein Terminal geht (und nicht an eine Pipe oder Datei usw.), senden die systemd-Kommandos standardmäßig eine ausführliche Ausgabe an einen Pager. Mit der Option `--no-pager` deaktivieren Sie den Paging-Modus.

systemd unterstützt außerdem die Bash-Vervollständigung. Hierbei geben Sie die ersten Buchstaben eines Subkommandos ein und drücken dann ⇥, um es automatisch zu vervollständigen. Diese Funktion ist nur in der `Bash`-Shell verfügbar und das Paket `bash-completion` muss installiert sein.

13.2.1 Verwalten von Diensten auf einem laufenden System

Die Subkommandos zum Verwalten der Dienste sind mit den entsprechenden Kommandos in System V-init identisch (**`start`**, **`stop`** usw.). Die allgemeine Syntax für Dienstverwaltungskommandos lautet wie folgt:

systemd

```
systemctl reload|restart|start|status|stop|... MY_SERVICE(S)
```

System V-init

```
rcMY_SERVICE(S) reload|restart|start|status|stop|...
```

Mit systemd können Sie mehrere Dienste gleichzeitig verwalten. Im Gegensatz zu System V-init, bei dem die init-Skripts einzeln nacheinander ausgeführt werden, führen Sie ein einziges Kommando aus, beispielsweise:

```
systemctl start MY_1ST_SERVICE MY_2ND_SERVICE
```

So rufen Sie eine Liste aller auf dem System verfügbaren Dienste ab:

```
systemctl list-unit-files --type=service
```

Die folgende Tabelle zeigt die wichtigsten Dienstverwaltungskommandos für systemd und System V-init:

TABELLE 13.1 BEFEHLE ZUR DIENSTEVERWALTUNG

Aufgabe	systemd-Kommando	System V-init-Kommando
Starten.	`start`	`start`
Stoppen.	`stop`	`stop`
Neu starten. Fährt Dienste herunter und startet sie dann neu. Wenn ein Dienst noch nicht ausgeführt wird, wird er gestartet.	`restart`	`restart`
Bedingt neu starten. Startet Dienste neu, wenn sie derzeit ausgeführt werden. Keine Auswirkung bei Diensten, die nicht ausgeführt werden.	`try-restart`	`try-restart`
Neu laden. Weist die Dienste an, die Konfigurationsdateien neu zu laden ohne die laufenden Vorgänge zu unterbrechen. Anwendungsbeispiel: Weisen Sie Apache an, eine bearbeitete Konfigurationsdatei `httpd.conf` neu zu laden. Nicht alle Dienste unterstützen das Neuladen.	`reload`	`reload`
Neu laden oder neu starten. Lädt Dienste neu, wenn das Neuladen unterstützt wird;	`reload-or-restart`	`n/a`

Aufgabe	systemd-Kommando	System V-init-Kommando
ansonsten werden die Dienste neu gestartet. Wenn ein Dienst noch nicht ausgeführt wird, wird er gestartet.		
Bedingt neu laden oder neu starten. Lädt Dienste neu, wenn das Neuladen unterstützt wird; ansonsten werden die Dienste neu gestartet, wenn sie derzeit ausgeführt werden. Keine Auswirkung bei Diensten, die nicht ausgeführt werden.	`reload-or-try-restart`	`n/a`
Ausführliche Statusinformationen abrufen. Zeigt Informationen zum Dienststatus. Das Kommando `systemd` bietet Details wie Beschreibung, ausführbare Datei, Status, cgroup und zuletzt durch den Dienst ausgegebene Meldungen (siehe *Abschnitt 13.6.8, „Fehlersuche für Dienste“*). Die Detailtiefe bei System V-init ist von Dienst zu Dienst unterschiedlich.	`status`	`status`
Kurze Statusinformationen abrufen. Gibt an, ob Dienste aktiv sind oder nicht.	`is-active`	`status`

13.2.2 Dienste dauerhaft aktivieren/deaktivieren

Mit den Dienstverwaltungskommandos im vorangegangenen Abschnitt können Sie die Dienste für die aktuelle Sitzung bearbeiten. Mit systemd können Sie Dienste außerdem dauerhaft aktivieren oder deaktivieren, so dass sie entweder automatisch bei Bedarf gestartet werden oder gar nicht verfügbar sind. Sie können dies mithilfe von YaST oder über die Kommandozeile tun.

13.2.2.1 Aktivieren/Deaktivieren von Diensten über die Kommandozeile

Die folgende Tabelle zeigt die wichtigsten Aktivierungs- und Deaktivierungskommandos für systemd und System V-init:

Wichtig: Service starten

Wenn ein Dienst über die Kommandozeile aktiviert wird, wird er nicht automatisch gestartet. Der Dienst wird beim nächsten Systemstart oder bei der nächsten Änderung des Runlevels/Ziels gestartet. Soll ein Dienst nach dem Aktivieren sofort gestartet werden, führen Sie explizit **`systemctl start`** *`MEIN_DIENST`* oder **`rc`** *`MEIN_DIENST`* **`start`** aus.

TABELLE 13.2 KOMMANDOS ZUM AKTIVIEREN UND DEAKTIVIEREN VON DIENSTEN

Aufgabe	`systemd-Kommando`	**System V-init-Kommando**
Aktivieren.	**`systemctl enable`** *`MEIN(E)_DIENST(E)`*	**`insserv`** *`MEIN(E)_DIENST(E)`*, **`chkconfig -a`** *`MEIN(E)_DIENST(E)`*
Deaktivieren.	**`systemctl disable`** *`MEIN(E)_DIENST(E)`***`.service`**	**`insserv -r`** *`MEIN(E)_DIENST(E)`*, **`chkconfig -d`** *`MEIN(E)_DIENST(E)`*
Überprüfen. Zeigt an, ob ein Dienst aktiviert ist oder nicht.	**`systemctl is-enabled`** *`MEIN_DIENST`*	**`chkconfig`** *`MEIN_DIENST`*
Erneut aktivieren. Ähnlich wie beim Neustarten eines Diensts, deaktiviert dieses Kommando einen Dienst und aktiviert ihn dann wieder. Nützlich, wenn ein Dienst mit den Standardein-	**`systemctl reenable`** *`MEIN_DIENST`*	n/v

Aufgabe	`systemd-Kommando`	System V-init-Kommando
stellungen erneut aktiviert werden soll.		
Maskierung. Nach dem „Deaktivieren“ eines Dienstes kann er weiterhin manuell aktiviert werden. Soll ein Dienst vollständig deaktiviert werden, maskieren Sie ihn. Mit Vorsicht verwenden.	**`systemctl mask`** *`MEIN_DIENST`*	n/v
Demaskieren. Ein maskierter Dienst kann erst dann wieder genutzt werden, wenn er demaskiert wurde.	**`systemctl unmask`** *`MEIN_DIENST`*	n/v

13.3 Systemstart und Zielverwaltung

Der gesamte Vorgang des Startens und Herunterfahrens des Systems wird von systemd verwaltet. Von diesem Gesichtspunkt aus kann der Kernel als Hintergrundprozess betrachtet werden, der alle anderen Prozesse verwaltet und die CPU-Zeit sowie den Hardwarezugriff entsprechend den Anforderungen anderer Programme anpasst.

13.3.1 Ziele im Vergleich zu Runlevels

Bei System V-init wurde das System in ein sogenanntes „Runlevel“ gebootet. Ein Runlevel definiert, wie das System gestartet wird und welche Dienste im laufenden System verfügbar sind. Die Runlevels sind numeriert. Die bekanntesten Runlevels sind `0` (System herunterfahren), `3` (Mehrbenutzermodus mit Netzwerk) und `5` (Mehrbenutzermodus mit Netzwerk und Anzeigemanager).

systemd führt mit den sogenannten „Ziel-Units“ ein neues Konzept ein. Dennoch bleibt die Kompatibilität mit dem Runlevel-Konzept uneingeschränkt erhalten. Die Ziel-Units tragen Namen statt Zahlen und erfüllen bestimmte Zwecke. Mit den Zielen `local-fs.target` und `swap.target` werden beispielsweise lokale Dateisysteme und Auslagerungsbereiche eingehängt.

Das Ziel `graphical.target` stellt ein Mehrbenutzersystem mit Netzwerk sowie Anzeigemanager-Funktionen bereit und entspricht Runlevel 5. Komplexe Ziele wie `graphical.target` fungieren als „Metaziele“, in denen eine Teilmenge anderer Ziele vereint ist. Mit systemd können Sie problemlos vorhandene Ziele kombinieren und so benutzerdefinierte Ziele bilden. Damit bietet dieses Kommando eine hohe Flexibilität.

Die nachfolgende Liste zeigt die wichtigsten systemd-Ziel-Units. Eine vollständige Liste finden Sie in **`man 7 systemd.special`**.

AUSGEWÄHLTE SYSTEMD-ZIEL-UNITS

`default.target`
: Das Ziel, das standardmäßig gebootet wird. Kein „reales“ Ziel, sondern ein symbolischer Link zu einem anderen Ziel wie `graphic.target`. Kann über YaST dauerhaft geändert werden (siehe *Abschnitt 13.4, „Verwalten von Services mit YaST“*). Soll das Ziel für eine einzige Sitzung geändert werden, geben Sie den Kernel-Parameter `systemd.unit=`*`MEIN_ZIEL.target`* am Bootprompt ein.

`emergency.target`
: Startet eine Notfall-Shell über die Konsole. Dieses Kommando darf nur an der Boot-Eingabeaufforderung im Format `systemd.unit=emergency.target` verwendet werden.

`graphical.target`
: Startet ein System mit Netzwerk, Mehrbenutzerunterstützung und Anzeigemanager.

`halt.target`
: Fährt das System herunter.

`mail-transfer-agent.target`
: Startet alle Dienste, die zum Senden und Empfangen von Mails erforderlich sind.

`multi-user.target`
: Startet ein Mehrbenutzersystem mit Netzwerk.

`reboot.target`
: Bootet das System neu.

`rescue.target`

Startet ein Einzelbenutzersystem ohne Netzwerk.

Damit die Kompatibilität mit dem Runlevel-System von System V-init gewährleistet bleibt, bietet systemd besondere Ziele mit der Bezeichnung `runlevelX.target`, denen die entsprechenden, mit `X` numerierten Runlevels zugeordnet sind.

Mit dem Kommando **`systemctl get-default`** ermitteln Sie das aktuelle Ziel.

TABELLE 13.3 SYSTEM V-RUNLEVELS UND `systemd`-ZIEL-UNITS

System V-Runlevel	`systemd`-Ziel	Beschreibung
0	`runlevel0.target`, `halt.target`, `poweroff.target`	System herunterfahren
1, S	`runlevel1.target`, `rescue.target`,	Einzelbenutzermodus
2	`runlevel2.target`, `multi-user.target`,	Lokaler Mehrbenutzermodus ohne entferntes Netzwerk
3	`runlevel3.target`, `multi-user.target`,	Mehrbenutzer-Vollmodus mit Netzwerk
4	`runlevel4.target`	Nicht verwendet/benutzerdefiniert
5	`runlevel5.target`, `graphical.target`,	Mehrbenutzer-Vollmodus mit Netzwerk und Anzeige-Manager
6	`runlevel6.target`, `reboot.target`,	Systemneustart

Wichtig: systemd ignoriert `/etc/inittab`

Die Runlevels in einem System V-init-System werden in `/etc/inittab` konfiguriert. Bei systemd wird diese Konfiguration *nicht* verwendet. Weitere Anweisungen zum Erstellen eines bootfähigen Ziels finden Sie unter *Abschnitt 13.5.3, „Erstellen von benutzerdefinierten Zielen“*.

13.3.1.1 Kommandos zum Ändern von Zielen

Mit den folgenden Kommandos arbeiten Sie mit den Ziel-Units:

Aufgabe	systemd-Kommando	System V-init-Kommando
Aktuelles Ziel/Runlevel ändern	**systemctl isolate** *MEIN_ZIEL*.target	**telinit** *X*
Zum standardmäßigen Ziel/Runlevel wechseln	**systemctl default**	n/v
Aktuelles Ziel/Runlevel abrufen	**systemctl list-units --type=target** Bei systemd sind in der Regel mehrere Ziele aktiv. Mit diesem Kommando werden alle derzeit aktiven Ziele aufgelistet.	**who -r** oder **runlevel**
Standard-Runlevel dauerhaft ändern	Verwenden Sie die Dienste-Verwaltung, oder führen Sie das folgende Kommando aus: **ln -sf /usr/lib/systemd/system/***MEIN_ZIEL*.target /etc/systemd/system/default.target	Verwenden Sie die Dienste-Verwaltung, oder ändern Sie die Zeile **id:** *X*:initdefault: in `/etc/inittab`
Standard-Runlevel für den aktuellen Bootprozess ändern	Geben Sie an der Boot-Eingabeaufforderung die folgende Option ein: **systemd.unit=** *MEIN_ZIEL*.target	Geben Sie an der Boot-Eingabeaufforderung die gewünschte Runlevel-Nummer ein.
Abhängigkeiten für ein Ziel/Runlevel anzeigen	**systemctl show -p "Requires"** *MEIN_ZIEL*.target **systemctl show -p "Wants"** *MEIN_ZIEL*.target „Requires“ (Benötigt) zeigt eine Liste der harten Abhängigkeiten (die in jedem Fall aufgelöst werden müssen), „Wants“	n/v

Aufgabe	systemd-Kommando	System V-init-Kommando
	(Erwünscht) dagegen eine Liste der weichen Abhängigkeiten (die nach Möglichkeit aufgelöst werden).	

13.3.2 Fehlersuche beim Systemstart

systemd bietet eine Möglichkeit, den Systemstartvorgang zu analysieren. Sie können die Liste der Dienste mit dem jeweiligen Status prüfen (ohne durch `/varlog/` blättern zu müssen). Mit systemd können Sie zudem den Startvorgang scannen und so ermitteln, wie lang das Starten der einzelnen Dienste dauert.

13.3.2.1 Prüfen des Startvorgangs der Dienste

Mit dem Kommando **`systemctl`** erzeugen Sie eine Liste aller Dienste, die seit dem Booten des Systems gestartet wurden. Hier werden alle aktiven Dienste wie im nachstehenden (gekürzten) Beispiel aufgeführt. Mit **`systemctl status`** *`MEIN_DIENST`* erhalten Sie weitere Informationen zu einem bestimmten Dienst.

BEISPIEL 13.1 LISTE DER AKTIVEN DIENSTE

```
root # systemctl
UNIT                        LOAD   ACTIVE SUB       JOB DESCRIPTION
[...]
iscsi.service               loaded active exited    Login and scanning of iSC+
kmod-static-nodes.service   loaded active exited    Create list of required s+
libvirtd.service            loaded active running   Virtualization daemon
nscd.service                loaded active running   Name Service Cache Daemon
ntpd.service                loaded active running   NTP Server Daemon
polkit.service              loaded active running   Authorization Manager
postfix.service             loaded active running   Postfix Mail Transport Ag+
rc-local.service            loaded active exited    /etc/init.d/boot.local Co+
rsyslog.service             loaded active running   System Logging Service
[...]
LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.

161 loaded units listed. Pass --all to see loaded but inactive units, too.
```

```
To show all installed unit files use 'systemctl list-unit-files'.
```

Soll die Ausgabe auf Dienste beschränkt werden, die nicht gestartet werden konnten, geben Sie die Option `--failed` an:

BEISPIEL 13.2 LISTE DER FEHLERHAFTEN DIENSTE

```
root # systemctl --failed
UNIT                    LOAD   ACTIVE SUB    JOB DESCRIPTION
apache2.service         loaded failed failed     apache
NetworkManager.service loaded failed failed     Network Manager
plymouth-start.service loaded failed failed     Show Plymouth Boot Screen

[...]
```

13.3.2.2 Fehlersuche für die Startzeit

Mit dem Kommando **`systemd-analyze`** führen Sie die Fehlersuche für die Startzeit durch. Hiermit werden der Gesamtzeitaufwand für den Startvorgang sowie eine Liste der beim Starten angeforderten Dienste angezeigt. Auf Wunsch kann auch eine SVG-Grafik erstellt werden, aus der hervorgeht, wie lange der Start der Dienste im Vergleich zu den anderen Diensten dauerte.

Auflisten der Startzeit des Systems

```
root # systemd-analyze
Startup finished in 2666ms (kernel) + 21961ms (userspace) = 24628ms
```

Auflisten der Startzeit der Dienste

```
root # systemd-analyze blame
  6472ms systemd-modules-load.service
  5833ms remount-rootfs.service
  4597ms network.service
  4254ms systemd-vconsole-setup.service
  4096ms postfix.service
  2998ms xdm.service
  2483ms localnet.service
  2470ms SuSEfirewall2_init.service
  2189ms avahi-daemon.service
  2120ms systemd-logind.service
  1210ms xinetd.service
  1080ms ntp.service
[...]
```

```
    75ms fbset.service
    72ms purge-kernels.service
    47ms dev-vda1.swap
    38ms bluez-coldplug.service
    35ms splash_early.service
```

Grafische Darstellung der Startzeit der Dienste

```
root # systemd-analyze plot > jupiter.example.com-startup.svg
```

13.3.2.3 Prüfen des gesamten Startvorgangs

Mit den obigen Kommandos prüfen Sie die gestarteten Dienste und den Zeitaufwand für den Start. Wenn Sie detailliertere Informationen benötigen, können Sie `systemd` anweisen, den gesamten Startvorgang ausführlich zu protokollieren. Geben Sie hierzu die folgenden Parameter an der Boot-Eingabeaufforderung ein:

```
systemd.log_level=debug systemd.log_target=kmsg
```

`systemd` schreibt die Protokollmeldungen nunmehr in den Kernel-Ringpuffer. Diesen Puffer zeigen Sie mit **`dmesg`** an:

```
dmesg -T | less
```

13.3.3 System V-Kompatibilität

systemd ist mit System V kompatibel, sodass Sie vorhandene System V-init-Skripte weiterhin nutzen können. Es gibt allerdings mindestens ein bekanntes Problem, bei dem ein System V-init-Skript nicht ohne Weiteres mit systemd zusammenarbeitet: Wenn Sie einen Dienst als ein anderer Benutzer über **`su`** oder **`sudo`** in init-Skripten starten, tritt der Fehler „Access denied“ (Zugriff verweigert) auf.

Wenn Sie den Benutzer mit **`su`** oder **`sudo`** ändern, wird eine PAM-Sitzung gestartet. Diese Sitzung wird beendet, sobald das init-Skript abgeschlossen ist. Als Folge wird auch der Service, der durch das init-Skript gestartet wurde, beendet. Als Workaround für diesen Fehler gehen Sie wie folgt vor:

1. Erstellen Sie einen Service-Datei-Wrapper mit demselben Namen wie das init-Skript und der Dateinamenerweiterung `.service`:

   ```
   [Unit]
   Description=DESCRIPTION
   After=network.target

   [Service]
   User=USER
   Type=forking (1)
   PIDFile=PATH TO PID FILE (1)
   ExecStart=PATH TO INIT SCRIPT start
   ExecStop=PATH TO INIT SCRIPT stop
   ExecStopPost=/usr/bin/rm -f PATH TO PID FILE (1)

   [Install]
   WantedBy=multi-user.target (2)
   ```

   Ersetzen Sie alle Werte in *`GROSSBUCHSTABEN`* durch die entsprechenden Werte.

   (1) Optional; nur zu verwenden, wenn mit dem init-Skript ein Daemon gestartet wird.

❷ `multi-user.target` startet ebenfalls das init-Skript, wenn Sie in `graphical.target` booten. Falls der Start nur beim Booten in den Display-Manager erfolgen soll, verwenden Sie hier `graphical.target`.

2. Starten Sie den Daemon mit **`systemctl start`** *ANWENDUNG*.

13.4 Verwalten von Services mit YaST

Grundlegende Aufgaben können auch mit dem YaST-Modul Dienste-Verwaltung ausgeführt werden. Hiermit werden das Starten, Stoppen, Aktivieren und Deaktivieren von Diensten unterstützt. Darüber hinaus können Sie den Status eines Dienstes abrufen und das Standardziel ändern. Starten Sie das YaST-Modul mit *YaST* › *System* › *Dienste-Verwaltung*.

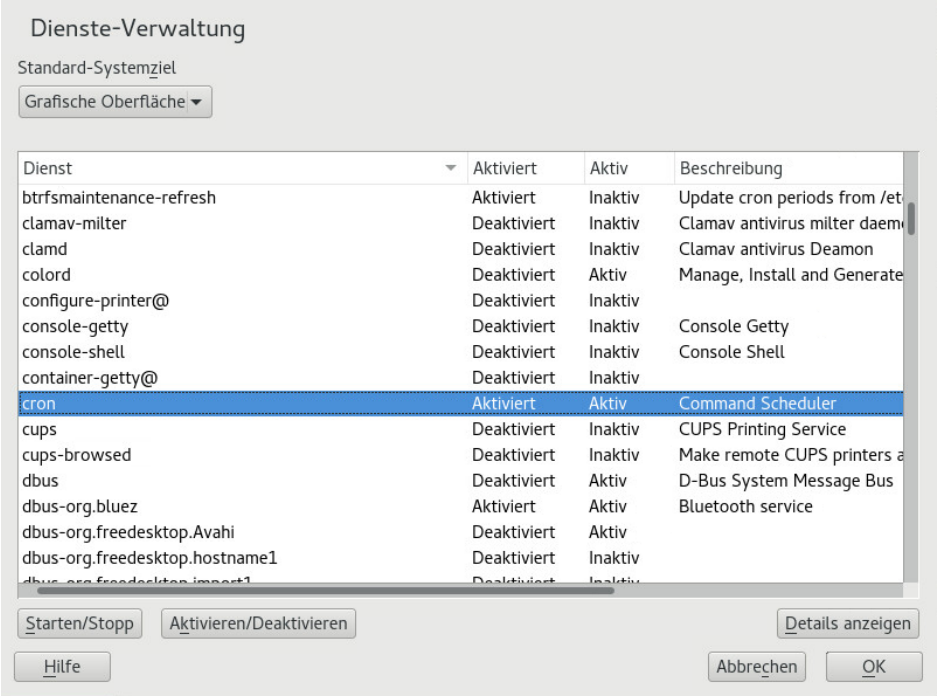


ABBILDUNG 13.1 SERVICES MANAGER

Ändern des *Standard-Systemziels*

Zum Ändern des Ziels, in das das System gebootet wird, wählen Sie ein Ziel in der Dropdown-Liste *Default System Target* aus. Die häufigsten Ziele sind *Graphical Interface* (Grafische Oberfläche; öffnet einen grafischen Anmeldebildschirm) und *Multi-User* (Mehrbenutzer; startet das System im Kommandozeilenmodus).

Starten und Stoppen eines Dienstes

Wählen Sie einen Dienst in der Tabelle aus. Die Spalte *Aktiv* zeigt, ob er derzeit ausgeführt wird (*Aktiv*) oder nicht (*Inactive*, Inaktiv). Mit *Start/Stop* (Starten/Stoppen) schalten Sie den Status um.

Durch das Starten und Stoppen eines Dienstes wird sein Status für die aktuelle Sitzung geändert. Soll der Status beim Neubooten geändert werden, müssen Sie den Dienst aktivieren oder deaktivieren.

Aktivieren oder Deaktivieren eines Dienstes

Wählen Sie einen Dienst in der Tabelle aus. Die Spalte *Aktiviert* zeigt, ob er derzeit *Aktiviert* oder *Deaktiviert* ist. Mit *Enable/Disable* (Aktivieren/Deaktivieren) schalten Sie den Status um.

Durch das Aktivieren bzw. Deaktivieren eines Dienstes legen Sie fest, ob er beim Booten gestartet werden soll (*Aktiviert*) oder nicht (*Deaktiviert*). Diese Einstellung wirkt sich nicht auf die aktuelle Sitzung aus. Soll der Status in der aktuellen Sitzung geändert werden, müssen Sie den Dienst starten oder stoppen.

Anzeigen von Statusmeldungen

Zum Anzeigen der Statusmeldungen für einen Dienst wählen Sie den gewünschten Dienst in der Liste aus und wählen Sie *Details anzeigen*. Die Ausgabe ist mit der Ausgabe des Befehls `systemctl -l status MEIN_DIENST` identisch.

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.

13.5 Anpassen von `systemd`

In den folgenden Abschnitten finden Sie einige Beispiele, wie Sie `systemd` individuell anpassen.

Warnung: Vermeiden der Überschreibung von Anpassungen

Passen Sie systemd stets in `/etc/systemd/` an, *nicht* in `/usr/lib/systemd/`. Ansonsten werden Ihre Änderungen bei der nächsten Aktualisierung von systemd überschrieben.

13.5.1 Anpassen von Dienstdateien

Die systemd-Dienstdateien befinden sich in `/usr/lib/systemd/system`. Zum Anpassen fahren Sie wie folgt fort:

1. Kopieren Sie die zu bearbeitenden Dateien aus `/usr/lib/systemd/system` in `/etc/systemd/system`. Behalten Sie die ursprünglichen Dateinamen bei.
2. Bearbeiten Sie die Kopien in `/etc/systemd/system`.
3. Mit dem Kommando **`systemd-delta`** erhalten Sie einen Überblick über Ihre Konfigurationsänderungen. Hiermit werden Konfigurationsdateien verglichen und ermittelt, die andere Konfigurationsdateien überschreiben. Weitere Informationen finden Sie auf der man-Seite zu **`systemd-delta`**.

Die geänderten Dateien in `/etc/systemd` haben Vorrang vor den Originaldateien in `/usr/lib/systemd/system`, sofern die Dateinamen identisch sind.

13.5.2 Erstellen von „Drop-in-Dateien“

Wenn eine Konfigurationsdatei nur um wenige Zeilen ergänzt oder nur ein kleiner Teil daraus geändert werden soll, können Sie sogenannte „Drop-in-Dateien“ verwenden. Mit den Drop-in-Dateien erweitern Sie die Konfiguration von Unit-Dateien, ohne die Unit-Dateien selbst bearbeiten oder überschreiben zu müssen.

Um beispielsweise einen einzigen Wert für den Dienst *`foobar`* in `/usr/lib/systemd/system/`*`foobar.service`* zu ändern, gehen Sie wie folgt vor:

1. Erstellen Sie ein Verzeichnis mit dem Namen `/etc/systemd/system/`*`MEIN_DIENST`*`.service.d/`.
   Beachten Sie das Suffix `.d`. Ansonsten muss der Name des Verzeichnisses mit dem Namen des Dienstes übereinstimmen, der mit der Drop-in-Datei gepatcht werden soll.
2. Erstellen Sie in diesem Verzeichnis eine Datei mit dem Namen *`whatevermodification`*`.conf`.
   Diese Datei darf nur eine Zeile mit dem zu ändernden Wert enthalten.
3. Speichern Sie Ihre Änderungen in die Datei. Die Datei wird als Erweiterung der Originaldatei verwendet.

13.5.3 Erstellen von benutzerdefinierten Zielen

Auf SUSE-Systemen mit System V-init wird Runlevel 4 nicht genutzt, so dass die Administratoren eine eigene Runlevel-Konfiguration erstellen können. Mit systemd können Sie beliebig viele benutzerdefinierte Ziele erstellen. Zum Einstieg sollten Sie ein vorhandenes Ziel anpassen, beispielsweise `graphical.target`.

1. Kopieren Sie die Konfigurationsdatei `/usr/lib/systemd/system/graphical.target` in `/etc/systemd/system/MEIN_ZIEL.target` und passen Sie sie nach Bedarf an.
2. Die im vorangegangenen Schritt kopierte Konfigurationsdatei enthält bereits die erforderlichen („harten“) Abhängigkeiten für das Ziel. Um auch die erwünschten („weichen“) Abhängigkeiten abzudecken, erstellen Sie ein Verzeichnis mit dem Namen `/etc/systemd/system/MEIN_ZIEL.target.wants`.
3. Legen Sie für jeden erwünschten Dienst einen symbolischen Link von `/usr/lib/systemd/system` in `/etc/systemd/system/MEIN_ZIEL.target.wants` an.
4. Sobald Sie alle Einstellungen für das Ziel festgelegt haben, laden Sie die systemd-Konfiguration neu. Damit wird das neue Ziel verfügbar:

   ```
   systemctl daemon-reload
   ```

13.6 Erweiterte Nutzung

In den nachfolgenden Abschnitten finden Sie weiterführende Themen für Systemadministratoren. Eine noch eingehendere Dokumentation finden Sie in der Serie von Lennart Pöttering zu systemd für Administratoren unter http://0pointer.de/blog/projects.

13.6.1 Bereinigen von temporären Verzeichnissen

`systemd` unterstützt das regelmäßige Bereinigen der temporären Verzeichnisse. Die Konfiguration aus der bisherigen Systemversion wird automatisch migriert und ist aktiv. `tmpfiles.d` (verwaltet temporäre Dateien) liest die Konfiguration aus den Dateien `/etc/tmpfiles.d/*.conf`, `/run/tmpfiles.d/*.conf` und `/usr/lib/tmpfiles.d/*.conf` aus. Die Konfiguration in `/etc/tmpfiles.d/*.conf` hat Vorrang vor ähnlichen Konfigurationen in den anderen beiden Verzeichnissen. (In `/usr/lib/tmpfiles.d/*.conf` speichern die Pakete die Konfigurationsdateien.)

Im Konfigurationsformat ist eine Zeile pro Pfad vorgeschrieben, wobei diese Zeile die Aktion und den Pfad enthalten muss und optional Felder für Modus, Eigentümer, Alter und Argument (je nach Aktion) enthalten kann. Im folgenden Beispiel wird die Verknüpfung der X11-Sperrdateien aufgehoben:

```
Type Path               Mode UID  GID  Age Argument
r    /tmp/.X[0-9]*-lock
```

So rufen Sie den Status aus dem tmpfile-Zeitgeber ab:

```
systemctl status systemd-tmpfiles-clean.timer
systemd-tmpfiles-clean.timer - Daily Cleanup of Temporary Directories
 Loaded: loaded (/usr/lib/systemd/system/systemd-tmpfiles-clean.timer; static)
 Active: active (waiting) since Tue 2014-09-09 15:30:36 CEST; 1 weeks 6 days ago
   Docs: man:tmpfiles.d(5)
         man:systemd-tmpfiles(8)

Sep 09 15:30:36 jupiter systemd[1]: Starting Daily Cleanup of Temporary Directories.
Sep 09 15:30:36 jupiter systemd[1]: Started Daily Cleanup of Temporary Directories.
```

Weitere Informationen zum Arbeiten mit temporären Dateien finden Sie unter **`man 5 tmpfiles.d`**.

13.6.2 Systemprotokoll

In *Abschnitt 13.6.8, „Fehlersuche für Dienste“* wird erläutert, wie Sie Protokollmeldungen für einen bestimmten Dienst anzeigen. Die Anzeige von Protokollmeldungen ist allerdings nicht auf Dienstprotokolle beschränkt. Sie können auch auf das gesamte von `systemd` geschriebene Protokoll (das sogenannte „Journal“) zugreifen und Abfragen darauf ausführen. Mit dem Befehl **`journalctl`** zeigen Sie das gesamte Protokoll an, beginnend mit den ältesten Einträgen. Informationen zu weiteren Optionen, beispielsweise zum Anwenden von Filtern oder zum Ändern des Ausgabeformats, finden Sie unter **`man 1 journalctl`**.

13.6.3 Aufnahmen

Mit dem Subkommando `isolate` können Sie den aktuellen Status von **`systemd`** als benannten Snapshot speichern und später wiederherstellen. Dies ist beim Testen von Diensten oder benutzerdefinierten Zielen hilfreich, weil Sie jederzeit zu einem definierten Status zurückkehren können. Ein Snapshot ist nur in der aktuellen Sitzung verfügbar; beim Neubooten wird er automatisch gelöscht. Der Snapshot-Name muss auf `.snapshot` enden.

Erstellen eines Snapshots

```
systemctl snapshot MY_SNAPSHOT.snapshot
```

Löschen eines Snapshots

```
systemctl delete MY_SNAPSHOT.snapshot
```

Anzeigen eines Snapshots

```
systemctl show MY_SNAPSHOT.snapshot
```

Aktivieren eines Snapshots

```
systemctl isolate MY_SNAPSHOT.snapshot
```

13.6.4 Laden der Kernelmodule

Mit `systemd` können Kernel-Module automatisch zum Bootzeitpunkt geladen werden, und zwar über die Konfigurationsdatei in `/etc/modules-load.d`. Die Datei sollte den Namen *`MODUL`*.conf haben und den folgenden Inhalt aufweisen:

```
# load module MODULE at boot time
MODULE
```

Falls ein Paket eine Konfigurationsdatei zum Laden eines Kernel-Moduls installiert, wird diese Datei unter `/usr/lib/modules-load.d` installiert. Wenn zwei Konfigurationsdateien mit demselben Namen vorhanden sind, hat die Datei unter `/etc/modules-load.d` Vorrang.

Weitere Informationen finden Sie auf der man-Seite `modules-load.d(5)`.

13.6.5 Ausführen von Aktionen vor dem Laden eines Dienstes

Bei System V mussten init-Aktionen, die vor dem Laden eines Diensts ausgeführt werden müssen, in `/etc/init.d/before.local` festgelegt werden. Dieses Verfahren wird in systemd nicht mehr unterstützt. Wenn Aktionen vor dem Starten von Diensten ausgeführt werden müssen, gehen Sie wie folgt vor:

Laden der Kernelmodule

Erstellen Sie eine Drop-in-Datei im Verzeichnis `/etc/modules-load.d` (Syntax siehe **`man modules-load.d`**).

Erstellen von Dateien oder Verzeichnissen, Bereinigen von Verzeichnissen, Ändern des Eigentümers

Erstellen Sie eine Drop-in-Datei in `/etc/tmpfiles.d` (Syntax siehe **`man tmpfiles.d`**).

Weitere Aufgaben

Erstellen Sie eine Systemdienstdatei (beispielsweise `/etc/systemd/system/before.service`) anhand der folgenden Schablone:

```
[Unit]
Before=NAME OF THE SERVICE YOU WANT THIS SERVICE TO BE STARTED BEFORE
[Service]
Type=oneshot
RemainAfterExit=true
ExecStart=YOUR_COMMAND
# beware, executable is run directly, not through a shell, check the man pages
# systemd.service and systemd.unit for full syntax
[Install]
# target in which to start the service
WantedBy=multi-user.target
#WantedBy=graphical.target
```

Sobald die Dienstdatei erstellt ist, führen Sie die folgenden Kommandos aus (als `root`):

```
systemctl daemon-reload
systemctl enable before
```

Bei jedem Bearbeiten der Dienstdatei müssen Sie Folgendes ausführen:

```
systemctl daemon-reload
```

13.6.6 Kernel-Steuergruppen (cgroups)

Auf einem traditionellen System-V-init-System kann ein Prozess nicht immer eindeutig dem Dienst zugeordnet werden, durch den er erzeugt wurde. Einige Dienste (z. B. Apache) erzeugen zahlreiche externe Prozesse (z. B. CGI- oder Java-Prozesse), die wiederum weitere Prozesse erzeugen. Eindeutige Zuweisungen sind damit schwierig oder völlig unmöglich. Wenn ein Dienst nicht ordnungsgemäß beendet wird, bleiben zudem ggf. einige untergeordnete Dienste weiterhin aktiv.

Bei systemd wird jeder Dienst in eine eigene cgroup aufgenommen, womit dieses Problem gelöst ist. cgroups sind eine Kernel-Funktion, mit der die Prozesse mit allen ihren untergeordneten Prozessen in hierarchisch strukturierten Gruppen zusammengefasst werden. Die cgroups werden dabei nach dem jeweiligen Dienst benannt. Da ein nicht privilegierter Dienst seine cgroup nicht „verlassen“ darf, ist es damit möglich, alle von einem Dienst erzeugten Prozesse mit dem Namen dieses Dienstes zu versehen.

Mit dem Kommando **`systemd-cgls`** erhalten Sie eine Liste aller Prozesse, die zu einem Dienst gehören. (Gekürztes) Beispiel für die Ausgabe:

BEISPIEL 13.3 AUFLISTEN ALLER PROZESSE, DIE ZU EINEM DIENST GEHÖREN

```
root # systemd-cgls --no-pager
├─1 /usr/lib/systemd/systemd --switched-root --system --deserialize 20
├─user.slice
│ └─user-1000.slice
│   ├─session-102.scope
│   │ ├─12426 gdm-session-worker [pam/gdm-password]
│   │ ├─15831 gdm-session-worker [pam/gdm-password]
│   │ ├─15839 gdm-session-worker [pam/gdm-password]
│   │ ├─15858 /usr/lib/gnome-terminal-server

[...]

└─system.slice
  ├─systemd-hostnamed.service
  │ └─17616 /usr/lib/systemd/systemd-hostnamed
  ├─cron.service
  │ └─1689 /usr/sbin/cron -n
  ├─ntpd.service
  │ └─1328 /usr/sbin/ntpd -p /var/run/ntp/ntpd.pid -g -u ntp:ntp -c /etc/ntp.conf
  ├─postfix.service
  │ ├─ 1676 /usr/lib/postfix/master -w
  │ ├─ 1679 qmgr -l -t fifo -u
  │ └─15590 pickup -l -t fifo -u
```

```
  ├─sshd.service
  │ └─1436 /usr/sbin/sshd -D

[...]
```

Weitere Informationen zu cpgroups finden Sie in *Buch „*System Analysis and Tuning Guide*", Kapitel 9 „Kernel Control Groups"*.

13.6.7 Beenden von Diensten (Senden von Signalen)

Wie in *Abschnitt 13.6.6, „Kernel-Steuergruppen (cgroups)"* erläutert, kann ein Prozess in einem System-V-init-System nicht immer eindeutig seinem übergeordneten Dienstprozess zugeordnet werden. Das erschwert das Beenden eines Dienstes und seiner untergeordneten Dienste. Untergeordnete Prozesse, die nicht ordnungsgemäß beendet wurden, bleiben als "Zombie-Prozess" zurück.

Durch das Konzept von systemd, mit dem jeder Dienst in einer eigenen cgroup abgegrenzt wird, können alle untergeordneten Prozesse eines Dienstes eindeutig erkannt werden, so dass Sie ein Signal zu diesen Prozessen senden können. Mit Use **`systemctl kill`** senden Sie die Signale an die Dienste. Eine Liste der verfügbaren Signale finden Sie in **`man 7 signals`**.

Senden von `SIGTERM` an einen Dienst

`SIGTERM` ist das standardmäßig gesendete Signal.

```
systemctl kill MY_SERVICE
```

Senden von *`SIGNAL`* an einen Dienst

Mit der Option `-s` legen Sie das zu sendende Signal fest.

```
systemctl kill -s SIGNAL MY_SERVICE
```

Auswählen von Prozessen

Standardmäßig sendet das Kommando **`kill`** das Signal an `alle` Prozesse der angegebenen cgroup. Sie können dies jedoch auf den Prozess `control` oder `main` beschränken. Damit können Sie beispielsweise das Neuladen der Konfiguration eines Dienstes mit dem Signal `SIGHUP` erzwingen:

```
systemctl kill -s SIGHUP --kill-who=main MY_SERVICE
```

Warnung: Beenden oder Neustarten des D-BUS-Dienstes wird nicht unterstützt.

Der D-Bus-Dienst fungiert als Meldungsbus für die Kommunikation zwischen den systemd-Clients und dem systemd-Manager, der als PID 1 ausgeführt wird. `dbus` ist zwar ein eigenständiger Dämon, bildet jedoch auch einen wesentlichen Bestandteil der init-Infrastruktur.

Das Beenden von `dbus` oder das Neustarten im laufenden System entspricht dem Versuch, PID 1 zu beenden oder neu zu starten. Hiermit wird die systemd-Client/Server-Kommunikation unterbrochen, sodass die meisten systemd-Funktionen unbrauchbar werden.

Das Beenden oder Neustarten von `dbus` wird daher weder empfohlen noch unterstützt.

13.6.8 Fehlersuche für Dienste

Standardmäßig ist die Ausgabe von systemd auf ein Minimum beschränkt. Wenn ein Dienst ordnungsgemäß gestartet wurde, erfolgt keine Ausgabe. Bei einem Fehler wird eine kurze Fehlermeldung angezeigt. Mit **`systemctl status`** können Sie jedoch die Fehlersuche für den Start und die Ausführung eines Dienstes vornehmen.

systemd umfasst einen Protokollierungsmechanismus („Journal“), mit dem die Systemmeldungen protokolliert werden. Auf diese Weise können Sie die Dienstmeldungen zusammen mit den Statusmeldungen abrufen. Das Kommando **`status`** hat eine ähnliche Funktion wie **`tail`** und kann zudem die Protokollmeldungen in verschiedenen Formaten anzeigen, ist also ein wirksames Hilfsmittel für die Fehlersuche.

Anzeigen von Fehlern beim Starten von Diensten

Wenn ein Dienst nicht gestartet wird, erhalten Sie mit **`systemctl status`** *`MEIN_DIENST`* eine ausführliche Fehlermeldung:

```
root # systemctl start apache2
Job failed. See system journal and 'systemctl status' for details.
root # systemctl status apache2
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)
   Active: failed (Result: exit-code) since Mon, 04 Jun 2012 16:52:26 +0200; 29s ago
   Process: 3088 ExecStart=/usr/sbin/start_apache2 -D SYSTEMD -k start (code=exited,
 status=1/FAILURE)
   CGroup: name=systemd:/system/apache2.service

Jun 04 16:52:26 g144 start_apache2[3088]: httpd2-prefork: Syntax error on line
```

```
205 of /etc/apache2/httpd.conf: Syntax error on li...alHost>
```

Anzeigen der letzten *n* Dienstmeldungen

Standardmäßig zeigt das Subkommando **status** die letzten zehn Meldungen an, die ein Dienst ausgegeben hat. Mit dem Parameter `--lines=`*n* legen Sie eine andere Anzahl fest:

```
systemctl status ntp
systemctl --lines=20 status ntp
```

Anzeigen von Dienstmeldungen im Anhängemodus

Mit der Option „--follow“ erhalten Sie einen `Live-Stream` mit Dienstmeldungen; diese Option entspricht **tail** `-f`:

```
systemctl --follow status ntp
```

Ausgabeformat der Meldungen

Mit dem Parameter `--output=`*mode* legen Sie das Ausgabeformat für die Dienstmeldungen fest. Die wichtigsten Modi sind:

`short`
: Das Standardformat. Zeigt die Protokollmeldungen mit einem Zeitstempel in Klartext an.

`verbose`
: Vollständige Ausgabe mit sämtlichen Feldern.

`cat`
: Kurze Ausgabe ohne Zeitstempel.

13.7 Weitere Informationen

Weitere Informationen zu systemd finden Sie in folgenden Online-Quellen:

Startseite

http://www.freedesktop.org/wiki/Software/systemd

systemd für Administratoren

Lennart Pöttering, einer der systemd-Autoren, hat eine Serie von Blogeinträgen verfasst. (Zum Zeitpunkt, als dieses Kapitel verfasst wurde, standen bereits 13 Einträge zur Verfügung.) Diese sind unter http://0pointer.de/blog/projects zu finden.

III System

14 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung 206

15 **`journalctl`**: Abfragen des `systemd`-Journals 209

16 Grundlegendes zu Netzwerken 217

17 Druckerbetrieb 298

18 Das X Window-System 314

19 Zugriff auf Dateisysteme mit FUSE 329

20 Verwalten von Kernelmodulen 331

21 Gerätemanagement über dynamischen Kernel mithilfe von `udev` 335

22 Live-Patching des Linux-Kernels mithilfe von kGraft 349

23 Spezielle Systemfunktionen 356

14 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung

SUSE® Linux Enterprise Server 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 Server 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 Server-64-Bit-Plattformen implementiert ist.

SUSE Linux Enterprise Server für die 64-Bit-Plattformen POWER, z Systems und AMD64/Intel 64 ist so ausgelegt, dass vorhandene 32-Bit-Anwendungen „ohne Änderungen in der 64-Bit-Umgebung ausführbar sind.“ Die entsprechenden 32-Bit-Plattformen sind ppc für POWER sowie x86 für AMD64/Intel 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 POWER-System führt die meisten Anwendungen im 32-Bit-Modus aus, es können aber auch 64-Bit-Anwendungen ausgeführt werden.

Anmerkung: Keine Unterstützung für die Erstellung von 32-Bit-Anwendungen

SUSE Linux Enterprise Server unterstützt die Erstellung von 32-Bit-Anwendungen nicht, sondern bietet lediglich Laufzeitunterstützung für 32-Bit-Binärdateien.

14.1 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.

Eine Ausnahme von dieser Regel ist PAM (Pluggable Authentication Modules). Während des Authentifizierungsprozesses verwendet SUSE Linux Enterprise Server PAM (austauschbare Authentifizierungsmodule) als Schicht für die Vermittlung zwischen Benutzer und Anwendung. Auf einem 64-Bit-Betriebssystem, das auch 32-Bit-Anwendungen ausführt, ist es stets erforderlich, beide Versionen eines PAM-Moduls zu installieren.

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

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

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

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

14.2 Kernel-Spezifikationen

Die 64-Bit-Kernel für AMD64/Intel 64, POWER und z Systems 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-POWER-Plattformen als 64-Bit-Programme kompiliert werden, damit sie ordnungsgemäß funktionieren. Bei IBM z Systems sind nicht alle ioctls 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: Kernel-ladbare Module

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 SUSE, 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.

15 `journalctl`: Abfragen des `systemd`-Journals

Mit dem Wechsel von herkömmlichen init-Skripten zu `systemd` in SUSE Linux Enterprise 12 (siehe *Kapitel 13, Der Daemon* `systemd`) wurde ein eigenes Protokolliersystem eingeführt, das als *Journal* bezeichnet wird. Alle Systemereignisse werden in das Journal geschrieben, so dass Sie keinen `syslog`-basierten Service mehr ausführen müssen.

Das Journal selbst ist ein Systemservice und wird mit `systemd` verwaltet. Die vollständige Bezeichnung des Service lautet `systemd-journald.service`. Hier werden Protokolldaten in strukturierten, indizierten Journalen erfasst und gespeichert. Die Daten basieren dabei auf den Protokollinformationen aus dem Kernel, von den Benutzerprozessen, aus der Standardeingabe und aus den Fehlern von Systemdiensten. Der Dienst `systemd-journald` ist standardmäßig aktiviert:

```
# systemctl status systemd-journald
systemd-journald.service - Journal Service
   Loaded: loaded (/usr/lib/systemd/system/systemd-journald.service; static)
   Active: active (running) since Mon 2014-05-26 08:36:59 EDT; 3 days ago
     Docs: man:systemd-journald.service(8)
           man:journald.conf(5)
 Main PID: 413 (systemd-journal)
   Status: "Processing requests..."
   CGroup: /system.slice/systemd-journald.service
           └─413 /usr/lib/systemd/systemd-journald
[...]
```

15.1 Festlegen des Journals als persistent

Das Journal speichert die Protokolldaten standardmäßig in `/run/log/journal/`. Das Verzeichnis `/run/` ist naturgemäß flüchtig, weshalb die Protokolldaten beim Neubooten verloren gehen. Um persistente Protokolldaten zu erzielen, muss das Verzeichnis `/var/log/journal/` mit den entsprechenden Angaben zu Eigentümer und Berechtigungen vorhanden sein, damit der systemd-journald-Service die Daten dort speichern kann. So können Sie das Verzeichnis mit `systemd` erstellen und die persistente Protokollierung aktivieren:

1. Öffnen Sie die Datei `/etc/systemd/journald.conf` als `root` zum Bearbeiten.

   ```
   # vi /etc/systemd/journald.conf
   ```

2. Heben Sie die Auskommentierung der Zeile auf, die mit `Storage=` beginnt, und ändern Sie sie wie folgt:

```
[...]
[Journal]
Storage=persistent
#Compress=yes
[...]
```

3. Speichern Sie die Datei, und starten Sie systemd-journald neu:

```
systemctl restart systemd-journald
```

15.2 Nützliche Schalter in `journalctl`

In diesem Abschnitt finden Sie einige häufig verwendete, nützliche Optionen, mit denen Sie das Standardverhalten von **`journalctl`** optimieren. Alle Schalter sind auf der man-Seite zu **`journalctl`** (**`man 1 journalctl`**) beschrieben.

Tipp: Meldungen für eine bestimmte ausführbare Datei

Sollen alle Journaleinträge für eine bestimmte ausführbare Datei angezeigt werden, geben Sie den vollständigen Pfad zu dieser Datei an:

```
journalctl /usr/lib/systemd/systemd
```

-f

Zeigt lediglich die jüngsten Protokollmeldungen an und gibt neue Protokolleinträge aus, sobald sie zum Journal hinzugefügt werden.

-e

Gibt die Meldungen aus und springt an das Ende des Journals, so dass im Pager die aktuellen Einträge sichtbar sind.

-r

Gibt die Meldungen des Journals in umgekehrter Reihenfolge aus (die jüngsten Einträge zuerst).

-k

Zeigt nur Kernel-Meldungen an. Dies entspricht der Feldzuordnung `_TRANSPORT=kernel` (siehe *Abschnitt 15.3.3, „Filtern nach Feldern“*).

-u

Zeigt nur Meldungen für die angegebene `systemd`-Einheit an. Dies entspricht der Feldzuordnung `_SYSTEMD_UNIT=UNIT` (siehe *Abschnitt 15.3.3, „Filtern nach Feldern“*).

```
# journalctl -u apache2
[...]
Jun 03 10:07:11 pinkiepie systemd[1]: Starting The Apache Webserver...
Jun 03 10:07:12 pinkiepie systemd[1]: Started The Apache Webserver.
```

15.3 Filtern der Journalausgabe

Wenn Sie **`journalctl`** ohne Schalter aufrufen, wird der gesamte Inhalt des Journals angezeigt (die ältesten Einträge an erster Stelle). Die Ausgabe kann mit bestimmten Schaltern und Feldern gefiltert werden.

15.3.1 Filtern nach Bootnummer

`journalctl` kann die Meldungen nach einem bestimmten System-Bootvorgang filtern. Zum Anzeigen einer Liste mit allen verfügbaren Bootvorgängen führen Sie Folgendes aus:

```
# journalctl --list-boots
-1 097ed2cd99124a2391d2cffab1b566f0 Mon 2014-05-26 08:36:56 EDT—Fri 2014-05-30 05:33:44
 EDT
 0 156019a44a774a0bb0148a92df4af81b Fri 2014-05-30 05:34:09 EDT—Fri 2014-05-30 06:15:01
 EDT
```

Die erste Spalte enthält den Boot-Offset: `0` für den aktuellen Bootvorgang, `-1` für den vorangegangenen Bootvorgang, `-2` für den davor erfolgten Bootvorgang usw. Die zweite Spalte zeigt die Boot-ID, gefolgt von den Zeitstempeln für Beginn und Ende des Zeitraums, über den das System nach dem Bootvorgang aktiv war.

Alle Meldungen für den aktuellen Bootvorgang anzeigen:

```
# journalctl -b
```

Wenn Sie die Journalmeldungen für den vorangegangenen Bootvorgang abrufen möchten, hängen Sie einen Offset-Parameter an. Im folgenden Beispiel werden die Meldungen für den vorangegangenen Bootvorgang ausgegeben:

```
# journalctl -b -1
```

Alternativ können Sie die Bootmeldungen nach der Boot-ID auflisten. Verwenden Sie hierzu das Feld _BOOT_ID:

```
# journalctl _BOOT_ID=156019a44a774a0bb0148a92df4af81b
```

15.3.2 Filtern nach Zeitraum

Sie können die Ausgabe von **`journalctl`** durch Angabe des Start- oder Enddatums filtern. Für Datumsangaben gilt das Format „2014-06-30 9:17:16“. Wenn Sie keine Uhrzeit angeben, wird Mitternacht (0:00 Uhr) angenommen. Wenn die Sekundenangabe fehlt, wird „:00“ angenommen. Wenn Sie kein Datum angeben, wird das aktuelle Datum angenommen. Statt eines numerischen Ausdrucks können Sie die Schlüsselwörter „gestern“, „heute“ oder „morgen“ angeben. Diese Wörter bezeichnen Mitternacht am Tag vor dem aktuellen Tag, am aktuellen Tag bzw. am Tag nach dem aktuellen Tag. Das Schlüsselwort „now“ (jetzt) verweist auf die aktuelle Uhrzeit am heutigen Tag. Auch relative Zeitangaben mit dem Präfix `-` oder `+` sind möglich. Diese Zeitangaben verweisen dann entsprechend auf eine Uhrzeit vor oder nach der aktuellen Uhrzeit.

Nur neue Meldungen ab jetzt anzeigen und Ausgabe entsprechend aktualisieren:

```
# journalctl --since "now" -f
```

Alle Meldungen ab der letzten Mitternacht bis 3:20 Uhr anzeigen:

```
# journalctl --since "today" --until "3:20"
```

15.3.3 Filtern nach Feldern

Sie können die Ausgabe des Journals nach bestimmten Feldern filtern. Die Syntax für ein abzugleichendes Feld lautet `FELDNAME=FILTERKRITERIUM`, beispielsweise `_SYSTEMD_UNIT=httpd.service`. Wenn Sie mehrere Filterkriterien in einer einzigen Abfrage angeben, werden die Ausgabemeldungen noch stärker gefiltert. Eine Liste der Standardfelder finden Sie auf der man-Seite **`man 7 systemd.journal-fields`**.

Meldungen anzeigen, die von einer bestimmten Prozess-ID erzeugt wurden:

```
# journalctl _PID=1039
```

Meldungen anzeigen, die zu einer bestimmten Benutzer-ID gehören:

```
# journalctl _UID=1000
```

Meldungen aus dem Kernel-Ring-Puffer anzeigen (entspricht der Ausgabe von **dmesg**):

```
# journalctl _TRANSPORT=kernel
```

Meldungen aus der Standard- oder Fehlerausgabe des Services anzeigen:

```
# journalctl _TRANSPORT=stdout
```

Nur Meldungen anzeigen, die von einem bestimmten Service erzeugt wurden:

```
# journalctl _SYSTEMD_UNIT=avahi-daemon.service
```

Wenn Sie zwei verschiedene Felder angeben, werden nur solche Einträge zurückgegeben, die beide Ausdrücke gleichzeitig erfüllen:

```
# journalctl _SYSTEMD_UNIT=avahi-daemon.service _PID=1488
```

Wenn Sie zwei Kriterien für dasselbe Feld angeben, werden alle Einträge zurückgegeben, die einen dieser Ausdrücke erfüllen:

```
# journalctl _SYSTEMD_UNIT=avahi-daemon.service _SYSTEMD_UNIT=dbus.service
```

Mit dem Begrenzungszeichen „+“ verbinden Sie zwei Ausdrücke mit einem logischen „OR“. Im folgenden Beispiel werden alle Meldungen aus dem Avahi-Service mit der Prozess-ID 1480 zusammen mit allen Meldungen vom D-Bus-Service gezeigt:

```
# journalctl _SYSTEMD_UNIT=avahi-daemon.service _PID=1480 + _SYSTEMD_UNIT=dbus.service
```

15.4 Untersuchen von `systemd`-Fehlern

In diesem Abschnitt wird an einem einfachen Beispiel erläutert, wie Sie die Fehler auffinden und beheben, die `systemd` beim Starten von **apache2** meldet.

1. Versuchen Sie, den apache2-Service zu starten:

```
# systemctl start apache2
Job for apache2.service failed. See 'systemctl status apache2' and 'journalctl -xn'
 for details.
```

2. Prüfen Sie den Status dieses Service:

```
# systemctl status apache2
apache2.service - The Apache Webserver
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)
   Active: failed (Result: exit-code) since Tue 2014-06-03 11:08:13 CEST; 7min ago
  Process: 11026 ExecStop=/usr/sbin/start_apache2 -D SYSTEMD -DFOREGROUND \
           -k graceful-stop (code=exited, status=1/FAILURE)
```

   Die ID des Prozesses, der den Fehler verursacht, lautet 11026.

3. Rufen Sie die ausführliche Version der Meldungen zur Prozess-ID 11026 ab:

```
# journalctl -o verbose _PID=11026
[...]
MESSAGE=AH00526: Syntax error on line 6 of /etc/apache2/default-server.conf:
[...]
MESSAGE=Invalid command 'DocumenttRoot', perhaps misspelled or defined by a module
[...]
```

4. Korrigieren Sie den Schreibfehler in `/etc/apache2/default-server.conf`, starten Sie den apache2-Service, und lassen Sie den Status ausgeben:

```
# systemctl start apache2 && systemctl status apache2
apache2.service - The Apache Webserver
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)
   Active: active (running) since Tue 2014-06-03 11:26:24 CEST; 4ms ago
  Process: 11026 ExecStop=/usr/sbin/start_apache2 -D SYSTEMD -DFOREGROUND
           -k graceful-stop (code=exited, status=1/FAILURE)
 Main PID: 11263 (httpd2-prefork)
   Status: "Processing requests..."
   CGroup: /system.slice/apache2.service
           ├─11263 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           ├─11280 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           ├─11281 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           ├─11282 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           ├─11283 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
           └─11285 /usr/sbin/httpd2-prefork -f /etc/apache2/httpd.conf -D [...]
```

15.5 Konfiguration von journald

Das Verhalten des systemd-journald-Service lässt sich in `/etc/systemd/journald.conf` festlegen. In diesem Abschnitt werden lediglich die grundlegenden Optionseinstellungen vorgestellt. Eine vollständige Beschreibung der Datei finden Sie auf der man-Seite **`man 5 journald.conf`**. Damit die Änderungen in Kraft treten, müssen Sie das Journal wie folgt neu starten:

```
# systemctl restart systemd-journald
```

15.5.1 Ändern der Größenbeschränkung für das Journal

Wenn die Journalprotokolldaten an einem persistenten Speicherort gespeichert werden (siehe *Abschnitt 15.1, „Festlegen des Journals als persistent“*), belegen sie bis zu 10 % des Dateisystems, auf dem sich `/var/log/journal` befindet. Ist `/var/log/journal` beispielsweise auf einer `/var`-Partition mit einer Kapazität von 30 GB gespeichert, so kann das Journal bis zu 3 GB des Festplattenspeichers belegen. Zum Bearbeiten dieser Größenbeschränkung ändern Sie die Option `SystemMaxUse` (und heben Sie die Auskommentierung dieser Option auf):

```
SystemMaxUse=50M
```

15.5.2 Weiterleiten des Journals an `/dev/ttyX`

Sie können das Journal an ein Terminalgerät weiterleiten, so dass Sie an einem bevorzugten Terminalbildschirm (beispielsweise `/dev/tty12`) über Systemmeldungen informiert werden. Ändern Sie die folgenden journald-Optionen:

```
ForwardToConsole=yes
TTYPath=/dev/tty12
```

15.5.3 Weiterleiten des Journals an die Syslog-Funktion

journald ist abwärtskompatibel zu herkömmlichen syslog-Implementierungen wie `rsyslog`. Prüfen Sie Folgendes:

- rsyslog ist installiert.

  ```
  # rpm -q rsyslog
  ```

```
rsyslog-7.4.8-2.16.x86_64
```

- Der rsyslog-Service ist aktiviert.

```
# systemctl is-enabled rsyslog
enabled
```

- Die Weiterleitung an syslog wird in `/etc/systemd/journald.conf` aktiviert.

```
ForwardToSyslog=yes
```

15.6 Filtern des systemd-Journals mit YaST

Mit dem YaST-Journalmodul filtern Sie das systemd-Journal schnell und einfach (ohne die journalctl-Syntax verwenden zu müssen). Installieren Sie das Modul mit **`sudo zypper in yast2-journal`** und starten Sie es dann in YaST mit *System* › *systemd Journal*. Alternativ starten Sie das Modul von der Befehlszeile aus mit dem Befehl **`sudo yast2 journal`**.

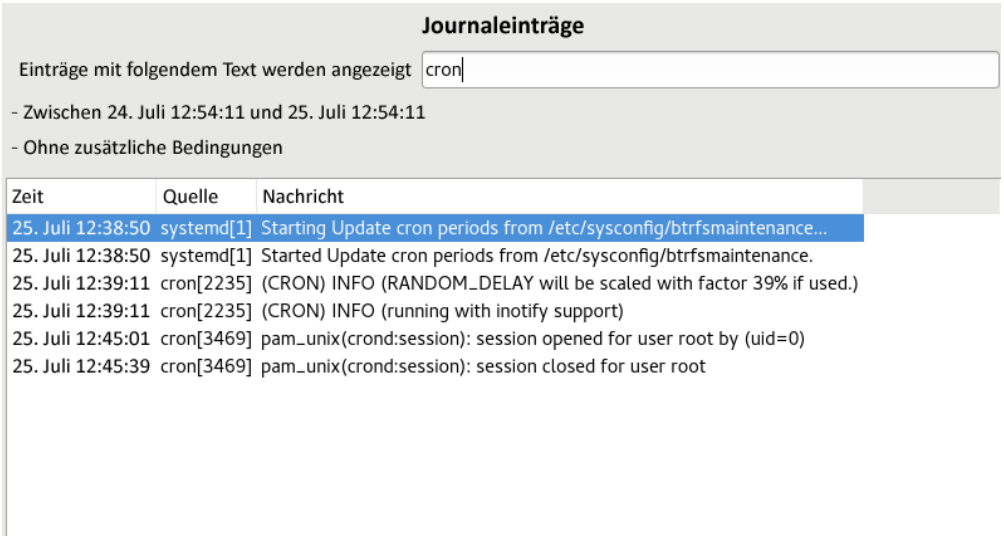


ABBILDUNG 15.1 YAST-SYSTEMD-JOURNAL

Das Modul zeigt die Protokolleinträge in einer Tabelle. Im Suchfeld oben suchen Sie nach Einträgen, die bestimmte Zeichen enthalten, ähnlich wie mit **`grep`**. Zum Filtern der Einträge nach Datum/Uhrzeit, Einheit, Datei oder Priorität klicken Sie auf *Change filters* (Filter ändern) und legen Sie die jeweiligen Optionen fest.

16 Grundlegendes zu Netzwerken

Linux stellt die erforderlichen Netzwerkwerkzeuge und -funktionen für die Integration in alle Arten von Netzwerkstrukturen zur Verfügung. Der Netzwerkzugriff über eine Netzwerkkarte kann mit YaST konfiguriert werden. Die manuelle Konfiguration ist ebenfalls möglich. In diesem Kapitel werden nur die grundlegenden Mechanismen und die relevanten Netzwerkkonfigurationsdateien behandelt.

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 *Verschiedene Protokolle aus der TCP/IP-Familie* aufgelisteten Protokolle dienen dem Datenaustausch zwischen zwei Computern über TCP/IP. Über TCP/IP verbundene Netzwerke bilden zusammen ein weltweites Netzwerk, das 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 RFCs finden Sie unter http://www.ietf.org/rfc.html.

VERSCHIEDENE PROTOKOLLE AUS DER TCP/IP-FAMILIE

TCP

Transmission Control Protocol: Ein verbindungsorientiertes sicheres Protokoll. Die zu übertragenden Daten werden zuerst von der Anwendung als Datenstrom gesendet und vom Betriebssystem in das passende Format konvertiert. Die entsprechende Anwendung auf dem Zielhost empfängt die Daten im ursprünglichen Datenstromformat, in dem sie anfänglich gesendet wurden. TCP ermittelt, ob Daten bei der Übertragung verloren gegangen sind oder beschädigt wurden. TCP wird immer dann implementiert, wenn die Datensequenz eine Rolle spielt.

UDP

User Datagram Protocol: Ein verbindungsloses, nicht sicheres Protokoll. Die zu übertragenden Daten werden in Form von anwendungsseitig generierten Paketen gesendet. Es ist nicht garantiert, in welcher Reihenfolge die Daten beim Empfänger eingehen, und ein Datenverlust ist immer möglich. UDP ist geeignet für datensatzorientierte Anwendungen. Es verfügt über eine kürzere Latenzzeit als TCP.

ICMP

Internet Control Message Protocol: Dies ist 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 beim Implementieren von IP Multicast.

Der Datenaustausch findet wie in *Abbildung 16.1, „Vereinfachtes Schichtmodell für TCP/IP“* 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 hardwareabhängigen Protokoll, z. B. Ethernet, unterstützt.

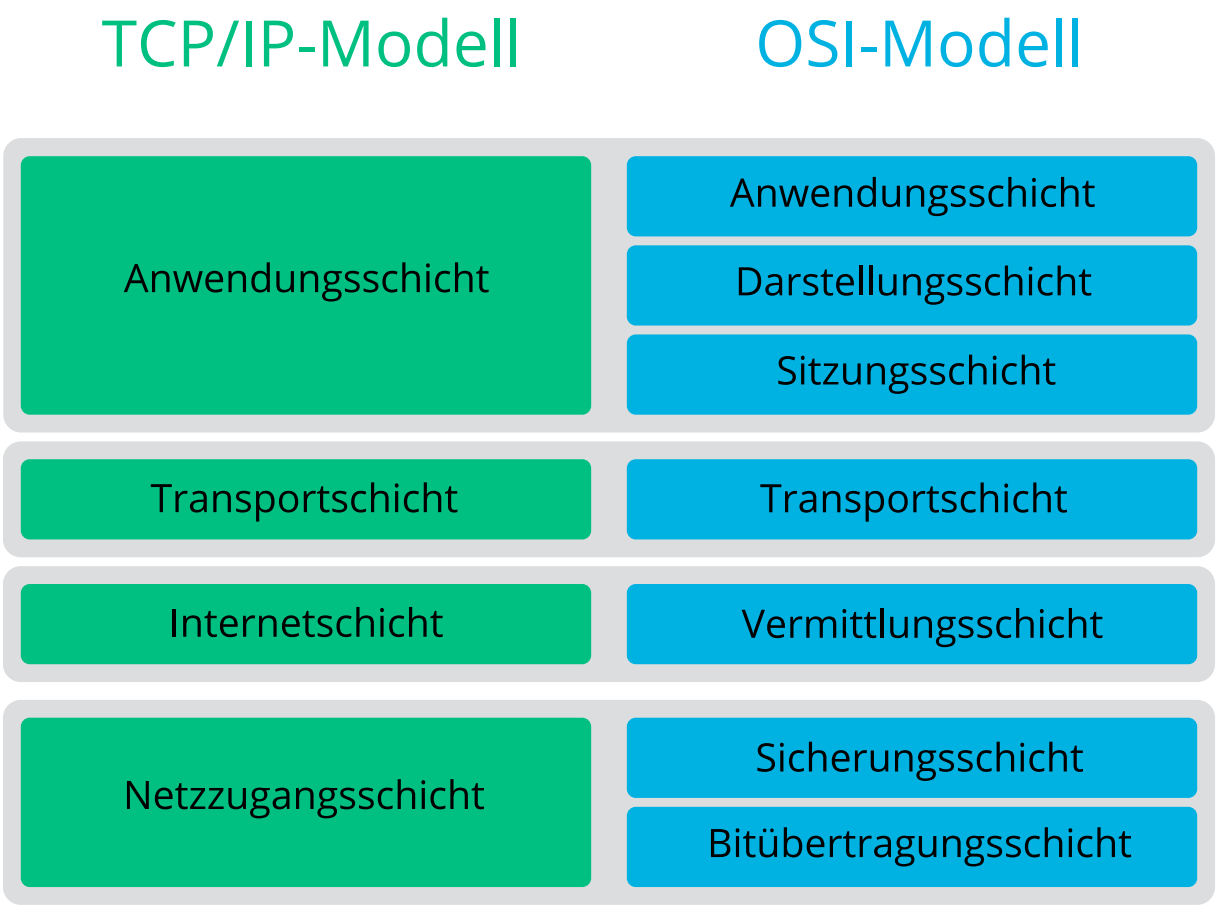


ABBILDUNG 16.1 VEREINFACHTES SCHICHTMODELL FÜR TCP/IP

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 *Paketen* gesammelt (sie können nicht alle auf einmal gesendet werden). 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 16.2, „TCP/IP-Ethernet-Paket“* dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

ABBILDUNG 16.2 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.

16.1 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 16.2, „IPv6 – Das Internet der nächsten Generation“*.

16.1.1 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 16.1, „IP-Adressen schreiben“* dargestellt geschrieben.

BEISPIEL 16.1 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. Sie 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.

16.1.2 Netzmasken und Routing

Mit Netzmasken werden die Adressräume eines Subnetzes definiert. Wenn sich in einem Subnetz zwei Hosts befinden, können diese direkt aufeinander zugreifen. Wenn sie sich nicht im selben Subnetz befinden, benötigen sie die Adresse eines Gateways, das den gesamten Verkehr für das Subnetz verarbeitet. 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 16.2, „Verknüpfung von IP-Adressen mit der Netzmaske“*. 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. Je mehr Bits den Wert `1` haben, desto kleiner ist also das Netzwerk. Da die Netzmaske immer aus mehreren aufeinander folgenden Bits mit dem

Wert `1` besteht, ist es auch möglich, die Anzahl der Bits in der Netzmaske zu zählen. In *Beispiel 16.2, „Verknüpfung von IP-Adressen mit der Netzmaske“* könnte das erste Netz mit 24 Bit auch als `192.168.0.0/24` geschrieben werden.

BEISPIEL 16.2 VERKNÜPFUNG VON IP-ADRESSEN MIT DER NETZMASKE

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
--------------------------------------------------------------
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:           192.     168.       0.       0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask    (255.255.255.0): 11111111 11111111 11111111 00000000
--------------------------------------------------------------
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:           213.      95.      15.       0
```

Ein weiteres Beispiel: Alle Computer, die über dasselbe Ethernetkabel angeschlossen sind, befinden sich in der Regel im selben Subnetz und sind direkt zugreifbar. Selbst wenn das Subnetz physisch durch Switches oder Bridges unterteilt ist, können diese Hosts weiter direkt erreicht werden.

IP-Adressen außerhalb des lokalen Subnetzes können nur erreicht werden, wenn für das Zielnetzwerk ein Gateway konfiguriert ist. In den meisten Fällen wird der gesamte externe Verkehr über lediglich ein Gateway gehandhabt. Es ist jedoch auch möglich, für unterschiedliche Subnetze mehrere Gateways zu konfigurieren.

Wenn ein Gateway konfiguriert wurde, werden alle externen IP-Pakete an das entsprechende Gateway gesendet. Dieses Gateway versucht anschließend, die Pakete auf dieselbe Weise – von Host zu Host – weiterzuleiten, bis sie den Zielhost erreichen oder ihre TTL-Zeit (Time to Live) abgelaufen ist.

SPEZIFISCHE ADRESSEN

Netzwerkbasisadresse

Dies ist die Netzmaske, die durch UND mit einer Netzwerkadresse verknüpft ist, wie in *Beispiel 16.2, „Verknüpfung von IP-Adressen mit der Netzmaske“* unter `Result` dargestellt. Diese Adresse kann keinem Host zugewiesen werden.

Rundrufadresse

Dies lässt sich auch wie folgt beschreiben: „Zugriff auf 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 Netzwerkbasisadresse verknüpft. Das obige Beispiel ergibt daher die Adresse 192.168.0.255. Diese Adresse kann keinem Host zugeordnet werden.

Lokaler Host

Die Adresse `127.0.0.1` ist auf jedem Host dem „Loopback-Device“ zugewiesen. Mit dieser Adresse und mit allen Adressen des vollständigen `127.0.0.0/8`-Loopback-Netzwerks (wie bei IPv4 beschrieben) kann eine Verbindung zu Ihrem Computer eingerichtet werden. Bei IPv6 gibt es nur eine Loopback-Adresse (`::1`).

Da IP-Adressen weltweit eindeutig sein müssen, können Sie keine 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 16.1, „Private IP-Adressdomänen“* aufgelistet.

TABELLE 16.1 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`

16.2 IPv6 – Das Internet der nächsten Generation

Wichtig: IBM z Systems: IPv6-Unterstützung

IPv6 wird von den CTC- und IUCV-Netzwerkverbindungen der IBM z Systems-Hardware nicht unterstützt.

Aufgrund der Entstehung des World Wide Web (WWW) hat das Internet in den letzten 15 Jahren ein explosives Wachstum mit einer immer größer werdenden Anzahl von Computern erfahren, die über TCP/IP kommunizieren. Seit Tim Berners-Lee bei CERN (http://public.web.cern.ch) 1990 das WWW erfunden hat, ist die Anzahl der Internethosts von ein paar tausend auf ca. 100 Millionen angewachsen.

Wie bereits erwähnt, besteht eine IPv4-Adresse nur aus 32 Bit. Außerdem gehen zahlreiche IP-Adressen verloren, da sie aufgrund der organisatorischen Bedingtheit der Netzwerke nicht verwendet werden können. Die Anzahl der in Ihrem Subnetz verfügbaren Adressen ist zwei hoch der Anzahl der Bits minus zwei. Ein Subnetz verfügt also beispielsweise über 2, 6 oder 14 Adressen. Um beispielsweise 128 Hosts mit dem Internet zu verbinden, benötigen Sie ein Subnetz mit 256 IP-Adressen, von denen nur 254 verwendbar sind, da zwei IP-Adressen für die Struktur des Subnetzes selbst benötigt werden: die Broadcast- und die Basisnetzwerkadresse.

Unter dem aktuellen IPv4-Protokoll sind DHCP oder NAT (Network Address Translation) die typischen Mechanismen, um einem potenziellen Adressmangel vorzubeugen. Kombiniert mit der Konvention, private und öffentliche Adressräume getrennt zu halten, können diese Methoden den Adressmangel sicherlich mäßigen. Das Problem liegt in der Konfiguration der Adressen, die schwierig einzurichten und zu verwalten ist. Um einen Host in einem IPv4-Netzwerk einzurichten, benötigen Sie mehrere Adressen, z. B. die IP-Adresse des Hosts, die Subnetzmaske, die Gateway-Adresse und möglicherweise die Adresse des Nameservers. 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.

16.2.1 Vorteile

Die wichtigste und augenfälligste Verbesserung durch das neue Protokoll ist der enorme Zuwachs des verfügbaren Adressraums. Eine IPv6-Adresse besteht aus 128-Bit-Werten und nicht aus den herkömmlichen 32 Bit. Dies ermöglicht mehrere Billiarden IP-Adressen.

IPv6-Adressen unterscheiden sich nicht nur hinsichtlich ihrer Länge gänzlich von ihren Vorgängern. Sie verfügen auch über eine andere interne Struktur, die spezifischere Informationen zu den Systemen und Netzwerken enthalten kann, zu denen sie gehören. Weitere Informationen hierzu finden Sie in *Abschnitt 16.2.2, „Adresstypen und -struktur“*.

In der folgenden Liste werden andere 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.
Wenn ein Router mit einem Switch verbunden ist, sollte der Router jedoch trotzdem periodische Anzeigen mit Flags senden, die den Hosts eines Netzwerks mitteilen, wie sie miteinander interagieren sollen. Weitere Informationen finden Sie im Artikel RFC 2462, auf der man-Seite `radvd.conf(5)` und im Artikel RFC 3315.

Mobilität

IPv6 ermöglicht es, einer Netzwerkschnittstelle gleichzeitig mehrere Adressen zuzuordnen. Benutzer können daher einfach auf mehrere Netzwerke zugreifen. Dies lässt sich mit den internationalen Roaming-Diensten vergleichen, die von Mobilfunkunternehmen angeboten werden. Wenn Sie das Mobilfunkgerät ins Ausland mitnehmen, meldet sich das Telefon automatisch bei einem ausländischen Dienst an, der sich im entsprechenden Bereich befindet. Sie können also überall unter der gleichen Nummer erreicht werden und können telefonieren, als wären Sie zu Hause.

Sichere Kommunikation

Bei IPv4 ist die Netzwerksicherheit eine Add-on-Funktion. IPv6 umfasst IPSec als eine seiner Kernfunktionen und ermöglicht es Systemen, über einen sicheren Tunnel zu kommunizieren, um das Ausspionieren durch Außenstehende über das Internet zu verhindern.

Abwärtskompatibilität

Realistisch gesehen, ist es unmöglich, das gesamte Internet auf einmal von IPv4 auf IPv6 umzustellen. Daher ist es wichtig, dass beide Protokolle nicht nur im Internet, sondern auf einem System koexistieren können. Dies wird durch kompatible Adressen (IPv4-Adressen können problemlos in IPv6-Adressen konvertiert werden) und die Verwendung von Tunnels gewährleistet. Weitere Informationen hierzu finden Sie unter *Abschnitt 16.2.3, „Koexistenz von IPv4 und IPv6“*. 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. Bei IPv6 ist dagegen eine deutlich feinere Vorgehensweise möglich: Die Server können die Hosts per *Multicasting* adressieren, also mehrere Hosts als Teil einer Gruppe. Dies unterscheidet sich vom *Broadcasting*, bei dem alle Hosts gleichzeitig adressiert werden, und vom *Unicasting*, bei dem jeder Host einzeln adressiert werden muss). Welche Hosts als Gruppe adressiert werden, kann je nach Anwendung unterschiedlich sein. Es gibt einige vordefinierte Gruppen, mit der beispielsweise alle Namenserver (die *Multicast-Gruppe „all name servers“*) oder alle Router (die *Multicast-Gruppe „all routers“*) angesprochen werden können.

16.2.2 Adresstypen und -struktur

Wie bereits erwähnt, hat das aktuelle IP-Protokoll zwei wichtige Einschränkungen: Es stehen zunehmend weniger IP-Adressen zur Verfügung und das Konfigurieren des Netzwerks und Verwalten der Routing-Tabellen wird komplexer und aufwändiger. IPv6 löst das erste Problem durch die Erweiterung des Adressraums auf 128 Bit. Das zweite Problem wird durch die Einführung einer hierarchischen Adressstruktur gemildert, 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. Sie werden durch Doppelpunkte (`:`) getrennt. Alle führenden Null-Byte innerhalb eines bestimmten Felds können ausgelassen werden, alle anderen Nullen jedoch nicht. Eine weitere Konvention ist, dass mehr als vier aufeinander folgenden Null-Byte mit einem doppelten Doppelpunkt zusammengefasst werden können. Jedoch ist pro Adresse nur ein solcher doppelter Doppelpunkt (`::`) zulässig. Diese Art der Kurznotation wird in *Beispiel 16.3, „Beispiel einer IPv6-Adresse“* dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

BEISPIEL 16.3 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 16.4, „IPv6-Adressen mit Angabe der Präfix-Länge“* 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 16.4 IPV6-ADRESSEN MIT ANGABE DER PRÄFIX-LÄNGE

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige sind unter *Unterschiedliche IPv6-Präfixe* aufgeführt.

UNTERSCHIEDLICHE IPV6-PRÄFIXE

`00`
: IPv4-über-IPv6-Kompatibilitätsadressen. Diese werden zur Erhaltung der Kompatibilität mit IPv4 verwendet. Für diesen Adresstyp wird ein Router benötigt, der IPv6-Pakete in IPv4-Pakete konvertieren kann. Mehrere spezielle Adressen, z. B. die für das Loopback-Device, verfügen ebenfalls über dieses Präfix.

`2` oder `3` als erste Stelle
: Aggregierbare globale Unicast-Adressen. Wie bei IPv4 kann eine Schnittstelle zugewiesen werden, um einen Teil eines bestimmten Subnetzes zu bilden. Aktuell stehen die folgenden Adressräume zur Verfügung: `2001::/16` (Adressraum Produktionsqualität) und `2002::/16` (6to4-Adressraum).

`fe80::/10`
: Link-local-Adressen. Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.

`fec0::/10`
: Site-local-Adressen. Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb des Organisationsnetzwerks, dem sie angehören. Damit entsprechen diese Adressen den bisherigen privaten Netzen (beispielsweise `10.x.x.x`).

`ff`
: Dies sind Multicast-Adressen.

Eine Unicast-Adresse besteht aus drei grundlegenden Komponenten:

Öffentliche Topologie
: Der erste Teil, der unter anderem auch eines der oben erwähnten Präfixe enthält, dient dem Routing des Pakets im öffentlichen Internet. Hier sind Informationen zum Provider oder der Institution kodiert, die den Netzwerkzugang bereitstellen.

Site-Topologie

Der zweite Teil enthält Routing-Informationen zu dem 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-Verbindungen) ein `EUI-64`-Token zuzuweisen.

Abgeleitet aus diesem Grundaufbau werden bei IPv6 fünf verschiedene Typen von Unicast-Adressen unterschieden:

`::` (nicht spezifiziert)

Ein Host verwendet diese Adresse als Quelladresse, wenn seine Netzwerkschnittstelle zum ersten Mal initialisiert wird (wobei die Adresse zu diesm Zeitpunkt 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 16.2.3, „Koexistenz von IPv4 und IPv6“*). 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 einer solchen Ziel- oder Quelladresse nicht an das Internet oder andere Subnetze weiterreichen. Diese Adressen zeichnen sich durch ein spezi-

elles 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 dürfen zwischen einzelnen Subnetzen geroutet werden, aber nicht außerhalb einer Organisation ins Internet gelangen. Solche Adressen werden für Intranets eingesetzt und sind ein Äquivalent zu den privaten IPv4-Adressen. Sie bestehen aus einem besonderen Präfix (`fec0::/10`), der Schnittstellen-ID und einem 16-Bit-Feld mit der Subnetz-ID. Die restlichen Stellen werden wieder mit Null-Bytes gefüllt.

Zusätzlich gibt es in IPv6 eine grundsätzlich neue Funktion: Einer Netzwerkschnittstelle werden in der Regel mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netzwerke zur Verfügung stehen. Eines dieser Netzwerke kann mit der MAC-Adresse und einem bekannten Präfix vollautomatisch konfiguriert werden, sodass nach der Aktivierung von IPv6 alle Hosts im lokalen Netz über Link-local-Adressen erreichbar sind. Durch die MAC-Adresse als Bestandteil der IP-Adresse ist jede dieser Adressen global eindeutig. Einzig die Teile der *Site-Topologie* und der *öffentlichen Topologie* können variieren, je nachdem in welchem Netz dieser Host aktuell zu erreichen ist.

Bewegt sich ein Host zwischen mehreren Netzen hin und her, braucht er mindestens zwei Adressen. Die eine, seine *Home-Adresse*, beinhaltet neben der Schnittstellen-ID die Informationen zu dem Heimatnetz, in dem der Computer normalerweise betrieben wird, und das entsprechende Präfix. Die Home-Adresse ist statisch und wird in der Regel nicht verändert. Alle Pakete, die für diesen Host bestimmt sind, werden ihm sowohl im eigenen als auch in fremden Netzen zugestellt. Möglich wird die Zustellung im Fremdnetz über wesentliche Neuerungen des IPv6-Protokolls, z. B. *Stateless Autoconfiguration* 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.

16.2.3 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 16.2.2, „Adresstypen und -struktur“*) sind hier die besten Lösungen.

IPv6-Hosts, die im (weltweiten) IPv4-Netzwerk mehr oder weniger isoliert sind, können über Tunnel kommunizieren: IPv6-Pakete werden als IPv4-Pakete gekapselt und so durch ein ein IPv4-Netzwerk übertragen. Ein *Tunnel* ist definiert als die Verbindung zwischen zwei IPv4-Endpunkten. Hierbei müssen die Pakete die IPv6-Zieladresse (oder das entsprechende Präfix) und die IPv4-Adresse des entfernten Hosts am Tunnelendpunkt enthalten. Einfache Tunnel können von den Administratoren zwischen ihren Netzwerken manuell und nach Absprache konfiguriert werden. Ein solches Tunneling wird *statisches Tunneling* genannt.

Trotzdem reicht manuelles Tunneling oft nicht aus, um die Menge der zum täglichen vernetzten Arbeiten nötigen Tunnel aufzubauen und zu verwalten. Aus diesem Grund wurden für IPv6 drei verschiedene Verfahren entwickelt, die das *dynamische Tunneling* erlauben:

6over4

IPv6-Pakete werden automatisch in IPv4-Pakete verpackt und über ein IPv4-Netzwerk versandt, in dem Multicasting aktiviert ist. IPv6 wird vorgespiegelt, das gesamte Netzwerk (Internet) sei ein einziges, riesiges LAN (Local Area Network). So wird der IPv4-Endpunkt des Tunnel automatisch ermittelt. Nachteile dieser Methode sind die schlechte Skalierbarkeit und die Tatsache, dass IP-Multicasting keineswegs im gesamten Internet verfügbar ist. Diese Lösung eignet sich für kleinere Netzwerke, die die Möglichkeit von IP-Multicasting bieten. Die zugrunde liegenden Spezifikationen sind in RFC 2529 enthalten.

6to4

Bei dieser Methode werden automatisch IPv4-Adressen aus IPv6-Adressen generiert. So können isolierte IPv6-Hosts über ein IPv4-Netz miteinander kommunizieren. Allerdings gibt es einige Probleme, die die Kommunikation zwischen den isolierten IPv6-Hosts und dem Internet betreffen. Diese Methode wird in RFC 3056 beschrieben.

IPv6 Tunnel Broker

Dieser Ansatz sieht spezielle Server vor, die für IPv6 automatisch dedizierte Tunnel anlegen. Diese Methode wird in RFC 3053 beschrieben.

16.2.4 IPv6 konfigurieren

Um IPv6 zu konfigurieren, müssen Sie auf den einzelnen Arbeitsstationen in der Regel keine Änderungen vornehmen. IPv6 ist standardmäßig aktiviert. Um IPv6 auf einem installierten System zu deaktivieren oder zu aktivieren, verwenden Sie das Modul YaST-*Netzwerkeinstellungen*. Aktivieren oder deaktivieren Sie auf dem Karteireiter *Globale Optionen* die Option *IPv6 aktivieren*, falls nötig. Zum vorübergehenden Aktivieren bis zum nächsten Neustart geben Sie `modprobe -i ipv6` als `root` ein. Nach dem Laden des IPv6-Moduls kann es nicht mehr entladen werden.

Aufgrund des Konzepts der automatischen Konfiguration von IPv6 wird der Netzwerkkarte eine Adresse im *Link-local*-Netzwerk zugewiesen. In der Regel werden Routing-Tabellen nicht auf Arbeitsstationen verwaltet. Bei Netzwerkroutern kann von der Arbeitsstation unter Verwendung des *Router-Advertisement-Protokolls* abgefragt werden, welches Präfix und welche Gateways implementiert werden sollen. Zum Einrichten eines IPv6-Routers kann das radvd-Programm verwendet werden. Dieses Programm informiert die Arbeitsstationen darüber, welches Präfix und welche Router für die IPv6-Adressen verwendet werden sollen. Alternativ können Sie die Adressen und das Routing auch mit zebra/quagga automatisch konfigurieren.

Weitere Informationen zum Einrichten verschiedneer Tunnel mit den Dateien in `/etc/sysconfig/network` finden Sie auf der man-Seite zu `ifcfg-tunnel` (`man ifcfg-tunnel`).

16.2.5 Weiterführende Informationen

Das komplexe IPv6-Konzept wird im obigen Überblick nicht vollständig abgedeckt. Weitere ausführliche Informationen zu dem neuen Protokoll finden Sie in den folgenden Online-Dokumentationen und -Büchern:

http://www.ipv6.org/

Alles rund um IPv6.

http://www.ipv6day.org

Alle Informationen, die Sie benötigen, um Ihr eigenes IPv6-Netzwerk zu starten.

http://www.ipv6-to-standard.org/

Die Liste der IPv6-fähigen Produkte.

http://www.bieringer.de/linux/IPv6/

Hier finden Sie den Beitrag „Linux IPv6 HOWTO“ und viele verwandte Links zum Thema.

RFC 2460

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).

16.3 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.

Ein Beispiel für einen vollständigen Namen wäre `jupiter.example.com`, geschrieben im Format `Hostname.Domäne`. Ein vollständiger Name, der als *Fully Qualified Domain Name* oder kurz als FQDN bezeichnet wird, besteht aus einem Host- und einem Domänennamen (`example.com`). Ein Bestandteil des Domänennamens ist die *Top Level Domain* oder TLD (`com`).

Aus historischen Gründen ist die Zuteilung der TLDs etwas verwirrend. So werden in den USA traditionell dreibuchstabige 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 Namenserver, hält also nicht die Daten aller Computer im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere Namenserver weiterdelegieren.

An der Spitze der Hierarchie befinden sich die *Root-Namenserver*. Die root-Namenserver verwalten die Domänen der obersten Ebene (Top Level Domains) und werden vom Network Information Center (NIC) verwaltet. Der Root-Namenserver kennt die jeweils für eine Top Level Domain zuständigen Namenserver. Weitere Informationen zu TLD-NICs finden Sie unter http://www.internic.net.

Der DNS bietet viel mehr Möglichkeiten als die bloße Namensauflösung. Der Namenserver weiß auch, welcher Host für eine ganze Domäne Emails annimmt, der so genannte *Mail Exchanger (MX)*.

Damit auch Ihr Computer einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Nameserver mit einer IP-Adresse bekannt sein. Ein Namensserver kann einfach mithilfe von YaST angegeben werden. Die Konfiguration des Nameserverzugriffs unter SUSE® Linux Enterprise Server ist in *Abschnitt 16.4.1.4, „Konfigurieren des Hostnamens und des DNS“* beschrieben. Eine Beschreibung zum Einrichten Ihres Nameservers finden Sie in *Kapitel 25, Domain Name System (DNS)*.

Eng verwandt mit DNS ist das Protokoll `whois`. Mit dem gleichnamigen Programm können Sie schnell ermitteln, wer für eine bestimmte Domäne verantwortlich ist.

Anmerkung: MDNS- und .local-Domänennamen

Die Domäne `.local` der obersten Stufe wird vom Resolver als link-local-Domäne behandelt. DNS-Anforderungen werden als Multicast-DNS-Anforderungen anstelle von normalen DNS-Anforderungen gesendet. Wenn Sie in Ihrer Nameserver-Konfiguration die Domäne `.local` verwenden, müssen Sie diese Option in `/etc/host.conf` ausschalten. Weitere Informationen finden Sie auf der man-Seite `host.conf`.

Wenn Sie MDNS während der Installation ausschalten möchten, verwenden Sie `nomdns=1` als Boot-Parameter.

Weitere Informationen zum Multicast-DNS finden Sie unter http://www.multicastdns.org.

16.4 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 16.5, „Manuelle Netzwerkkonfiguration“*.

Alle Netzwerkschnittstellen mit aktivierter Verbindung (also mit angeschlossenem Netzwerkkabel) werden automatisch konfiguriert. Zusätzliche Hardware kann jederzeit nach Abschluss der Installation auf dem installierten System konfiguriert werden. In den folgenden Abschnitten wird die Netzwerkkonfiguration für alle von SUSE Linux Enterprise Server unterstützten Netzwerkverbindungen beschrieben.

Tipp: IBM z Systems: Hotplug-fähige Netzwerkkarten

Auf den IBM z Systems-Plattformen werden Hotplug-fähige Netzwerkkarten unterstützt, aber nicht deren automatische Netzwerkintegration über DHCP (wie beim PC). Nach der Erkennung muss die Schnittstelle manuell konfiguriert werden.

16.4.1 Konfigurieren der Netzwerkkarte mit YaST

Zur Konfiguration verkabelter oder drahtloser Netzwerkkarten in YaST wählen Sie *System* › *Netzwerkeinstellungen*. Nach dem Öffnen des Moduls zeigt YaST das Dialogfeld *Netzwerkeinstellungen* mit den vier Karteireitern *Globale Optionen*, *Übersicht*, *Hostname/DNS* und *Routing* an.

Auf dem Karteireiter *Globale Optionen* können allgemeine Netzwerkoptionen wie die Netzwerkeinrichtungsmethode, IPv6 und allgemeine DHCP-Optionen festgelegt werden. Weitere Informationen finden Sie unter *Abschnitt 16.4.1.1, „Konfigurieren globaler Netzwerkoptionen“*.

Der Karteireiter *Übersicht* enthält Informationen über installierte Netzwerkschnittstellen und -konfigurationen. Jede korrekt erkannte Netzwerkkarte wird dort mit ihrem Namen aufgelistet. In diesem Dialogfeld können Sie Karten manuell konfigurieren, entfernen oder ihre Konfiguration ändern. Informationen zum manuellen Konfigurieren von Karten, die nicht automatisch erkannt wurden, finden Sie unter *Abschnitt 16.4.1.3, „Konfigurieren einer unerkannten Netzwerkkarte“*. Informationen zum Ändern der Konfiguration einer bereits konfigurierten Karte finden Sie unter *Abschnitt 16.4.1.2, „Ändern der Konfiguration einer Netzwerkkarte“*.

Auf dem Karteireiter *Hostname/DNS* können der Hostname des Computers sowie die zu verwendenden Nameserver festgelegt werden. Weitere Informationen finden Sie unter *Abschnitt 16.4.1.4, „Konfigurieren des Hostnamens und des DNS“*.

Der Karteireiter *Routing* wird zur Konfiguration des Routings verwendet. Weitere Informationen finden Sie unter *Abschnitt 16.4.1.5, „Konfigurieren des Routings“*.

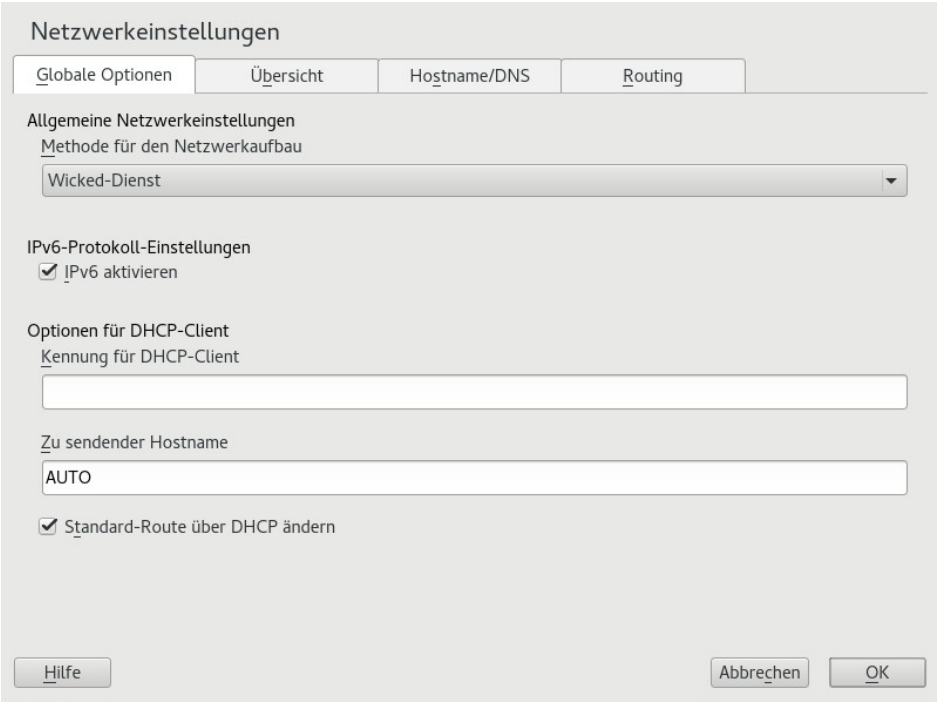


ABBILDUNG 16.3 KONFIGURIEREN DER NETZWERKEINSTELLUNGEN

16.4.1.1 Konfigurieren globaler Netzwerkoptionen

Auf dem Karteireiter *Globale Optionen* des YaST-Moduls *Netzwerkeinstellungen* können wichtige globale Netzwerkoptionen wie die Verwendung der Optionen NetworkManager, IPv6 und DHCP-Client festgelegt werden. Diese Einstellungen sind für alle Netzwerkschnittstellen anwendbar.

Anmerkung: NetworkManager von der Arbeitsplatzrechnererweiterung bereitgestellt

NetworkManager wird nun von der Arbeitsplatzrechnererweiterung bereitgestellt. Aktivieren Sie zur Installation von NetworkManager das Repository für die Arbeitsplatzrechnererweiterung und wählen Sie die NetworkManager-Pakete aus.

Unter *Netzwerkeinrichtungsmethode* wählen Sie die Methode aus, mit der Netzwerkverbindungen verwaltet werden sollen. Wenn die Verbindungen für alle Schnittstellen über das Desktop-Applet NetworkManager verwaltet werden sollen, wählen Sie *NetworkManager-Dienst* aus. NetworkManager eignet sich besonders für den Wechsel zwischen verschiedenen verkabelten und drahtlosen Netzwerken. Wenn Sie keine Desktop-Umgebung ausführen oder wenn Ihr Rechner ein Xen-Server oder ein virtuelles System ist oder Netzwerkdienste wie DHCP oder DNS in Ihrem Netzwerk zur Verfügung stellt, verwenden Sie die Methode *Wicked-Dienst*. Beim Einsatz von NetworkManager sollte `nm-applet` verwendet werden, um Netzwerkoptionen zu konfigurieren. Die Karteireiter *Übersicht*, *Hostname/DNS* und *Routing* des Moduls *Netzwerkeinstellungen* sind dann deaktiviert. Weitere Informationen zu NetworkManager finden Sie in der Dokumentation für SUSE Linux Enterprise Desktop.

Geben Sie unter *IPv6-Protokoll-Einstellungen* an, ob Sie das IPv6-Protokoll verwenden möchten. IPv6 kann parallel zu IPv4 verwendet werden. IPv6 ist standardmäßig aktiviert. In Netzwerken, die das IPv6-Protokoll nicht verwenden, können die Antwortzeiten jedoch schneller sein, wenn dieses Protokoll deaktiviert ist. Zum Deaktivieren von IPv6 deaktivieren Sie die Option *IPv6 aktivieren*. Wenn IPv6 deaktiviert ist, lädt der Kernel das IPv6-Modul nicht mehr automatisch. Diese Einstellung wird nach einem Neustart übernommen.

Unter *Optionen für DHCP-Client* konfigurieren Sie die Optionen für den DHCP-Client. Die *Kennung für DHCP-Client* muss innerhalb eines Netzwerks für jeden DHCP-Client eindeutig sein. Wenn dieses Feld leer bleibt, wird standardmäßig die Hardware-Adresse der Netzwerkschnittstelle als Kennung übernommen. Falls Sie allerdings mehrere virtuelle Computer mit der gleichen Netzwerkschnittstelle und damit der gleichen Hardware-Adresse ausführen, sollten Sie hier eine eindeutige Kennung in beliebigem Format eingeben.

Unter *Zu sendender Hostname* wird eine Zeichenkette angegeben, die für das Optionsfeld „Hostname“ verwendet wird, wenn der DHCP-Client Nachrichten an den DHCP-Server sendet. Einige DHCP-Server aktualisieren Nameserver-Zonen gemäß diesem Hostnamen (dynamischer DNS). Bei einigen DHCP-Servern muss das Optionsfeld *Zu sendender Hostname* in den DHCP-Nachrichten der Clients zudem eine bestimmte Zeichenkette enthalten. Übernehmen Sie die Einstellung `AUTO`, um den aktuellen Hostnamen zu senden (d. h. der aktuelle in `/etc/HOSTNAME` festgelegte Hostname). Soll kein Hostname gesendet werden, leeren Sie dieses Feld.

Wenn die Standardroute nicht gemäß den Informationen von DHCP geändert werden soll, deaktivieren Sie *Standardroute über DHCP ändern*.

16.4.1.2 Ändern der Konfiguration einer Netzwerkkarte

Wenn Sie die Konfiguration einer Netzwerkkarte ändern möchten, wählen Sie die Karte aus der Liste der erkannten Karten unter *Netzwerkeinstellungen* › *Übersicht* in YaST aus, und klicken Sie auf *Bearbeiten*. Das Dialogfeld *Netzwerkkarten-Setup* wird angezeigt. Hier können Sie die Kartenkonfiguration auf den Karteireitern *Allgemein*, *Adresse* und *Hardware* anpassen.

16.4.1.2.1 IP-Adressen konfigurieren

Die IP-Adresse der Netzwerkkarte oder die Art der Festlegung dieser IP-Adresse kann auf dem Karteireiter *Adresse* im Dialogfeld *Einrichten der Netzwerkkarte* festgelegt werden. Die Adressen IPv4 und IPv6 werden unterstützt. Für die Netzwerkkarte können die Einstellungen *Keine IP-Adresse* (nützlich für eingebundene Geräte), *Statisch zugewiesene IP-Adresse* (IPv4 oder IPv6) oder *Dynamische Adresse* über *DHCP* und/oder *Zeroconf* zugewiesen werden.

Wenn Sie *Dynamische Adresse* verwenden, wählen Sie, ob *Nue DHCP-Version 4* (für IPv4), *Nur DHCP-Version 6* (für IPv6) oder *DHCP-Version 4 und 6* verwendet werden soll.

Wenn möglich wird die erste Netzwerkkarte mit einer Verbindung, die bei der Installation verfügbar ist, automatisch zur Verwendung der automatischen Adressenkonfiguration mit DHCP konfiguriert.

Anmerkung: IBM z Systems und DHCP

Auf IBM z Systems-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 (Internet Service Provider) Ihnen aber keine statische IP-Adresse zugewiesen hat. Wenn Sie DHCP verwenden möchten, konfigurieren Sie dessen Einstellungen im Dialogfeld *Netzwerkeinstellungen* des YaST-Konfigurationsmoduls für Netzwerkkarten auf dem Karteireiter *Globale Optionen* unter *Optionen für DHCP-Client*. In einer virtuellen Hostumgebung, in der mehrere Hosts über dieselbe Schnittstelle kommunizieren, müssen diese anhand der *Kennung für DHCP-Client* unterschieden werden.

DHCP eignet sich gut zur Client-Konfiguration, aber zur Server-Konfiguration ist es nicht ideal. Wenn Sie eine statische IP-Adresse festlegen möchten, gehen Sie wie folgt vor:

1. Wählen Sie im YaST-Konfigurationsmodul für Netzwerkkarten auf dem Karteireiter *Übersicht* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.
2. Wählen Sie auf dem Karteireiter *Adresse* die Option *Statisch zugewiesene IP-Adresse* aus.
3. Geben Sie die *IP-Adresse* ein. Es können beide Adressen, IPv4 und IPv6, verwendet werden. Geben Sie die Netzwerkmaske in *Teilnetzmaske* ein. Wenn die IPv6-Adresse verwendet wird, benutzen Sie *Teilnetzmaske* für die Präfixlänge im Format `/64`.
   Optional kann ein voll qualifizierter *Hostname* für diese Adresse eingegeben werden, der in die Konfigurationsdatei `/etc/hosts` geschrieben wird.
4. Klicken Sie auf *Weiter*.
5. Klicken Sie auf *OK*, um die Konfiguration zu aktivieren.

Anmerkung: Schnittstellenaktivierung und Link-Erkennung

Bei der Aktivierung einer Netzwerkschnittstelle sucht **`wicked`** nach einem Träger und die IP-Konfiguration wird erst dann angewendet, wenn ein Link erkannt wurde. Wenn die Konfiguration unabhängig vom Link-Status angewendet werden soll (etwa wenn Sie einen Dienst testen, der eine bestimmte Adresse überwacht), können Sie die Link-Verbindung überspringen. Hängen Sie hierzu die Variable `LINK_REQUIRED=no` an die Konfigurationsdatei der Schnittstelle unter `/etc/sysconfig/network/ifcfg` an.

Darüber hinaus können Sie mit der Variablen `LINK_READY_WAIT=5` die Zeitüberschreitung (in Sekunden) für das Erkennen eines Links festlegen.

Weitere Informationen zu den `ifcfg-*`-Konfigurationsdateien finden Sie unter *Abschnitt 16.5.2.5, „`/etc/sysconfig/network/ifcfg-*`“* und **`man 5 ifcfg`**.

Wenn Sie die statische Adresse verwenden, werden die Namenserver und das Standard-Gateway nicht automatisch konfiguriert. Informationen zur Konfiguration von Namenservern finden Sie unter *Abschnitt 16.4.1.4, „Konfigurieren des Hostnamens und des DNS“*. Informationen zur Konfiguration eines Gateways finden Sie unter *Abschnitt 16.4.1.5, „Konfigurieren des Routings“*.

16.4.1.2.2 Konfigurieren von mehreren Adressen

Ein Netzwerkgerät kann mehrere IP-Adressen haben.

Anmerkung: Aliasse stellen eine Kompatibilitätsfunktion dar

Diese sogenannten Aliasse oder Kennungen sind nur mit IPv4 verwendbar. Bei IPv6 werden sie ignoriert. Bei der Verwendung von `iproute2`-Netzwerkschnittstellen können eine oder mehrere Adressen vorhanden sein.

Gehen Sie folgendermaßen vor, wenn Sie weitere Adressen für Ihre Netzwerkkarte mithilfe von YaST einrichten möchten:

1. Wählen Sie im YaST-Dialogfeld *Netzwerkeinstellungen* auf dem Karteireiter *Übersicht* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.
2. Klicken Sie auf dem Karteireiter *Adresse* › *Zusätzliche Adressen* auf *Hinzufügen*.
3. Geben Sie die *IPv4-Adresskennung*, die *IP-Adresse* und die *Netzmaske* ein. Nehmen Sie den Schnittstellennamen nicht in den Aliasnamen auf.
4. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

16.4.1.2.3 Ändern des Gerätenamens und der Udev-Regeln

Der Gerätename der Netzwerkkarte kann während des laufenden Betriebs geändert werden. Es kann auch festgelegt werden, ob udev die Netzwerkkarte über die Hardware-Adresse (MAC) oder die Bus-ID erkennen soll. Die zweite Option ist bei großen Servern vorzuziehen, um den Hotplug-Austausch der Karten zu erleichtern. Mit YaST legen Sie diese Optionen wie folgt fest:

1. Wählen Sie im YaST-Dialogfeld *Netzwerkeinstellungen* auf dem Karteireiter *Übersicht* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.
2. Öffnen Sie den Karteireiter *Hardware*. Der aktuelle Gerätename wird unter *Udev-Regeln* angezeigt. Klicken Sie auf *Ändern*.
3. Wählen Sie aus, ob udev die Karte über die *MAC-Adresse* oder die *Bus-ID* erkennen soll. Die aktuelle MAC-Adresse und Bus-ID der Karte werden im Dialogfeld angezeigt.
4. Aktivieren Sie zum Ändern des Gerätenamens die Option *Gerätenamen ändern* und bearbeiten Sie den Namen.

5. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

16.4.1.2.4 Ändern des Kernel-Treibers für Netzwerkkarten

Für einige Netzwerkkarten sind eventuell verschiedene Kernel-Treiber verfügbar. Wenn die Karte bereits konfiguriert ist, ermöglicht YaST die Auswahl eines zu verwendenden Kernel-Treibers in einer Liste verfügbarer Treiber. Es ist auch möglich, Optionen für den Kernel-Treiber anzugeben. Mit YaST legen Sie diese Optionen wie folgt fest:

1. Wählen Sie im YaST-Modul Netzwerkeinstellungen auf dem Karteireiter *Übersicht* in der Liste der erkannten Karten eine Netzwerkkarte aus, und klicken Sie auf *Bearbeiten*.
2. Öffnen Sie den Karteireiter *Hardware*.
3. Wählen Sie den zu verwendenden Kernel-Treiber unter *Modulname* aus. Geben Sie die entsprechenden Optionen für den ausgewählten Treiber unter *Optionen* im Format **`=`** = *`WERT`* ein. Wenn mehrere Optionen verwendet werden, sollten sie durch Leerzeichen getrennt sein.
4. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

16.4.1.2.5 Aktivieren des Netzwerkgeräts

Wenn Sie die Methode mit **`wicked`** verwenden, können Sie Ihr Gerät so konfigurieren, dass es wahlweise beim Systemstart, beim Anschließen des Kabels, beim Erkennen der Karte, manuell oder nie startet. Wenn Sie den Gerätestart ändern möchten, gehen Sie wie folgt vor:

1. Wählen Sie in YaST unter *System* › *Netzwerkeinstellungen* in der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.
2. In der Karteireiter *Allgemein* wählen Sie den gewünschten Eintrag unter *Geräte-Aktivierung*. Wählen Sie *Beim Systemstart*, um das Gerät beim Booten des Systems zu starten. Wenn *Bei Kabelanschluss* aktiviert ist, wird die Schnittstelle auf physikalische Netzwerkverbindungen überwacht. Wenn *Falls hot-plugged* aktiviert ist, wird die Schnittstelle festgelegt, wenn sie verfügbar ist. Dies gleicht der Option *Bei Systemstart*, führt jedoch nicht zu einem Fehler beim Systemstart, wenn die Schnittstelle nicht vorhanden ist. Wählen Sie *Manuell*, wenn Sie die Schnittstelle manuell mit **`ifup`** steuern möchten. Wählen Sie *Nie*, wenn das Gerät nicht gestartet werden soll. Bei *NFSroot* verhält sich ähnlich wie *Beim System-*

start, allerdings fährt der Befehl **`systemctl stop network`** die Schnittstelle bei dieser Einstellung nicht herunter; der `network`-Dienst wirkt sich auch auf den `wicked`-Dienst aus, sofern **`wicked`** aktiv ist. Diese Einstellung empfiehlt sich bei einem NFS- oder iSCSI-Root-Dateisystem.

3. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

Tipp: NFS als Root-Dateisystem

Auf (festplattenlosen) Systemen, in denen die Stammpartition über das Netzwerk als NFS-Freigabe eingehängt ist, müssen Sie beim Konfigurieren des Netzwerkgeräts, über das die NFS-Freigabe erreichbar ist, besonders vorsichtig vorgehen.

Wenn Sie das System herunterfahren oder neu booten, werden in der standardmäßigen Reihenfolge zunächst die Netzwerkverbindungen deaktiviert und anschließend die Stammpartition ausgehängt. Bei einem NFS-Root kann dies zu Problemen führen: Die Stammpartition kann nicht fehlerfrei ausgehängt werden, da die Netzwerkverbindung zur NFS-Freigabe schon nicht mehr aktiviert ist. Damit das System nicht das relevante Netzwerkgerät deaktiviert, öffnen Sie die Registerkarte gemäß *Abschnitt 16.4.1.2.5, „Aktivieren des Netzwerkgeräts“* und wählen Sie unter *Geräteaktivierung* die Option *Bei NFSroot*.

16.4.1.2.6 Einrichten der Größe der maximalen Transfereinheit

Sie können eine maximale Transfereinheit (MTU) für die Schnittstelle festlegen. MTU bezieht sich auf die größte zulässige Paketgröße in Byte. Eine größere MTU bringt eine höhere Bandbreiteneffizienz. Große Pakete können jedoch eine langsame Schnittstelle für einige Zeit belegen und die Verzögerung für nachfolgende Pakete vergrößern.

1. Wählen Sie in YaST unter *System* › *Netzwerkeinstellungen* in der Liste der erkannten Karten eine Netzwerkkarte aus und klicken Sie auf *Bearbeiten*.

2. Wählen Sie im Karteireiter *Allgemein* den gewünschten Eintrag aus der Liste *Set MTU* (MTU festlegen).

3. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

16.4.1.2.7 Multifunktionale PCIe-Geräte

Multifunktionale Geräte, die LAN, iSCSI und FCoE unterstützen, werden unterstützt. Mit dem YaST FCoE-Client (`yast2 fcoe-client`) werden die privaten Flags in zusätzlichen Spalten angezeigt, um dem Benutzer zu erlauben, das für FCoE vorgesehene Gerät auszuwählen. Mit dem YaST-Netzwerkmodul (`yast2 lan`) werden „Geräte, die nur als Speicher dienen“, von der Netzwerkkonfiguration ausgeschlossen.

Weitere Informationen zu FCoE erhalten Sie im *Buch „*Storage Administration Guide*”, Kapitel 15 „Fibre Channel Storage over Ethernet Networks: FCoE”, Abschnitt 15.3 „Managing FCoE Services with YaST”*.

16.4.1.2.8 InfiniBand-Konfiguration für IPoIB (IP-over-InfiniBand)

1. Wählen Sie in YaST unter *System* › *Netzwerkeinstellungen* das InfiniBand-Gerät aus und klicken Sie auf *Bearbeiten*.
2. Wählen Sie auf dem Karteireiter *Allgemein* einen der *IPoIB*-Modi (IP-over-InfiniBand) aus: *Verbunden* (Standard) oder *Datagramm*.
3. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

Weitere Informationen zu InfiniBand finden Sie in der Datei `/usr/src/linux/Documentation/infiniband/ipoib.txt`.

16.4.1.2.9 Konfigurieren der Firewall

Sie müssen nicht die genaue Firewall-Konfiguration durchführen, wie unter *Buch „*Security Guide*”, Kapitel 15 „Masquerading and Firewalls”, Abschnitt 15.4.1 „Configuring the Firewall with YaST”* beschrieben. Sie können die grundlegende Firewall-Konfiguration für Ihr Gerät als Teil der Geräteeinrichtung festlegen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie das YaST-Modul *System* › *Netzwerkeinstellungen*. Wählen Sie im Karteireiter *Übersicht* eine Karte aus der Liste erkannter Karten und klicken Sie auf *Bearbeiten*.
2. Öffnen Sie den Karteireiter *Allgemein* des Dialogfelds *Netzwerkeinstellungen*.
3. Legen Sie die *Firewall-Zone* fest, der Ihre Schnittstelle zugewiesen werden soll. Mit den zur Verfügung stehenden Optionen können Sie

Firewall deaktiviert

Diese Option ist nur verfügbar, wenn die Firewall deaktiviert ist und nicht ausgeführt wird. Verwenden Sie diese Option nur, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird.

Automatisches Zuweisen von Zonen

Diese Option ist nur verfügbar, wenn die Firewall aktiviert ist. Die Firewall wird ausgeführt und die Schnittstelle wird automatisch einer Firewall-Zone zugewiesen. Die Zone, die das Stichwort `Beliebig` enthält, oder die externe Zone wird für solch eine Schnittstelle verwendet.

Interne Zone (ungeschützt)

Die Firewall wird ausgeführt, aber es gibt keine Regeln, die diese Schnittstelle schützen. Verwenden Sie diese Option, wenn Ihr Computer Teil eines größeren Netzwerks ist, das von einer äußeren Firewall geschützt wird. Sie ist auch nützlich für die Schnittstellen, die mit dem internen Netzwerk verbunden sind,wenn der Computer über mehrere Netzwerkschnittstellen verfügt.

Demilitarisierte Zone

Eine demilitarisierte Zone ist eine zusätzliche Verteidigungslinie zwischen einem internen Netzwerk und dem (feindlichen) Internet. Die dieser Zone zugewiesenen Hosts können vom internen Netzwerk und vom Internet erreicht werden, können jedoch nicht auf das interne Netzwerk zugreifen.

Externe Zone

Die Firewall wird an dieser Schnittstelle ausgeführt und schützt sie vollständig vor anderem (möglicherweise feindlichem) Netzwerkverkehr. Dies ist die Standardoption.

4. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

16.4.1.3 Konfigurieren einer unerkannten Netzwerkkarte

Wenn eine Netzwerkkarte nicht ordnungsgemäß erkannt wird, so wird diese Karte nicht in der Liste der erkannten Karten aufgeführt. Wenn Sie sich nicht sicher sind, ob Ihr System über einen Treiber für die Karte verfügt, können Sie sie manuell konfigurieren. Sie können auch spezielle Netzwerkgerätetypen konfigurieren, z. B. Bridge, Bond, TUN oder TAP. So konfigurieren Sie eine nicht erkannte Netzwerkkarte (oder ein spezielles Gerät):

1. Klicken Sie im Dialogfeld *System* › *Netzwerkeinstellungen* › *Übersicht* in YaST auf *Hinzufügen*.

2. Legen Sie den *Gerätetyp* der Schnittstelle im Dialogfeld *Hardware* mit Hilfe der verfügbaren Optionen fest und geben Sie einen *Konfigurationsnamen* ein. Wenn es sich bei der Netzwerkkarte um ein PCMCIA- oder USB-Gerät handelt, aktivieren Sie das entsprechende Kontrollkästchen und schließen Sie das Dialogfeld durch Klicken auf *Weiter*. Ansonsten können Sie den Kernel *Modulname* definieren, der für die Karte verwendet wird, sowie gegebenenfalls dessen *Optionen*.
   Unter *Ethtool-Optionen* können Sie die von **`ifup`** für die Schnittstelle verwendeten **`Ethtool`**-Optionen einstellen. Weitere Informationen zu den verfügbaren Optionen finden Sie auf der man-Seite **`ethtool`**.
   Wenn die Optionszeichenkette mit einem `-` beginnt (z. B. `-K SCHNITTSTELLENNAME rx on`), wird das zweite Wort der Zeichenkette durch den aktuellen Schnittstellennamen ersetzt. In allen andern Fällen (z. B. `autoneg off speed 10`) setzt **`ifup`** dem Eintrag die Zeichenfolge `-s SCHNITTSTELLENNAME` voran.

3. Klicken Sie auf *Weiter*.

4. Konfigurieren Sie die benötigten Optionen wie die IP-Adresse, die Geräteaktivierung oder die Firewall-Zone für die Schnittstelle auf den Karteireitern *Allgemein*, *Adresse* und *Hardware*. Weitere Informationen zu den Konfigurationsoptionen finden Sie in *Abschnitt 16.4.1.2, „Ändern der Konfiguration einer Netzwerkkarte“*.

5. Wenn Sie für den Gerätetyp der Schnittstelle die Option *Drahtlos* gewählt haben, konfigurieren Sie im nächsten Dialogfeld die drahtlose Verbindung.

6. Zum Aktivieren der neuen Netzwerkkonfiguration bestätigen Sie die Einstellungen.

16.4.1.4 Konfigurieren des Hostnamens und des DNS

Wenn Sie die Netzwerkkonfiguration während der Installation noch nicht geändert haben und die Ethernet-Karte bereits verfügbar war, wurde automatisch ein Hostname für Ihren Rechner erstellt, und DHCP wurde aktiviert. Dasselbe gilt für die Namensservicedaten, die Ihr Host für die Integration in eine Netzwerkumgebung 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 Namenserver-Suchliste ändern möchten, gehen Sie wie folgt vor:

1. Wechseln Sie zum Karteireiter *Netzwerkeinstellungen* › *Hostname/DNS* im Modul *System* in YaST.

2. Geben Sie den *Hostnamen* und bei Bedarf auch den *Domänennamen* ein. Die Domäne ist besonders wichtig, wenn der Computer als Mailserver fungiert. Der Hostname ist global und gilt für alle eingerichteten Netzwerkschnittstellen.
   Wenn Sie zum Abrufen einer IP-Adresse DHCP verwenden, wird der Hostname Ihres Computers automatisch durch DHCP festgelegt. Sie sollten dieses Verhalten deaktivieren, wenn Sie Verbindungen zu verschiedenen Netzwerken aufbauen, da Sie verschiedene Hostnamen zuweisen können und das Ändern des Hostnamens beim Ausführen den grafischen Desktop verwirren kann. Zum Deaktivieren von DHCP, damit Sie eine IP-Adresse erhalten, deaktivieren Sie *Hostnamen über DHCP ändern*.
   Mithilfe von *Hostnamen zu Loopback-IP zuweisen* wird der Hostname mit der IP-Adresse `127.0.0.2` (Loopback) in `/etc/hosts` verknüpft. Diese Option ist hilfreich, wenn der Hostname jederzeit, auch ohne aktives Netzwerk, auflösbar sein soll.

3. Legen Sie unter *DNS-Konfiguration ändern* fest, wie die DNS-Konfiguration (Namenserver, Suchliste, Inhalt der Datei `/etc/resolv.conf`) geändert wird.
   Wenn die Option *Standardrichtlinie verwenden* ausgewählt ist, wird die Konfiguration vom Skript **`netconfig`** verwaltet, das die statisch definierten Daten (mit YaST oder in den Konfigurationsdateien) mit dynamisch bezogenen Daten (vom DHCP-Client oder NetworkManager) zusammenführt. Diese Standardrichtlinie ist in der Regel ausreichend.
   Wenn die Option *Nur manuell* ausgewählt ist, darf **`netconfig`** die Datei `/etc/resolv.conf` nicht ändern. Jedoch kann diese Datei manuell bearbeitet werden.

Wenn die Option *Benutzerdefinierte Richtlinie* ausgewählt ist, muss eine Zeichenkette für die *benutzerdefinierte Richtlinienregel* angegeben werden, welche die Zusammenführungsrichtlinie definiert. Die Zeichenkette besteht aus einer durch Kommas getrennten Liste mit Schnittstellennamen, die als gültige Quelle für Einstellungen betrachtet werden. Mit Ausnahme vollständiger Schnittstellennamen sind auch grundlegende Platzhalter zulässig, die mit mehreren Schnittstellen übereinstimmen. Beispiel: `eth* ppp?` richtet sich zuerst an alle eth- und dann an alle ppp0-ppp9-Schnittstellen. Es gibt zwei spezielle Richtlinienwerte, die angeben, wie die statischen Einstellungen angewendet werden, die in der Datei `/etc/sysconfig/network/config` definiert sind:

`STATIC`
: Die statischen Einstellungen müssen mit den dynamischen Einstellungen zusammengeführt werden.

`STATIC_FALLBACK`
: Die statischen Einstellungen werden nur verwendet, wenn keine dynamische Konfiguration verfügbar ist.

Weitere Informationen finden Sie auf der man-Seite zu **`netconfig`**(8) (**`man 8 netconfig`**).

4. Geben Sie die *Namenserver* ein und füllen Sie die *Domänensuchliste* aus. Nameserver müssen in der IP-Adresse angegeben werden (z. B. 192.168.1.116), nicht im Hostnamen. Namen, die im Karteireiter *Domänensuche* angegeben werden, sind Namen zum Auflösen von Hostnamen ohne angegebene Domäne. Wenn mehr als eine *Suchdomäne* verwendet wird, müssen die Domänen durch Kommas oder Leerzeichen getrennt werden.

5. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

Der Hostname kann auch mit YaST über die Kommandozeile bearbeitet werden. Die Änderungen in YaST treten sofort in Kraft (im Gegensatz zur manuellen Bearbeitung der Datei `/etc/HOSTNAME`). Zum Ändern des Hostnamens führen Sie das folgende Kommando aus:

```
yast dns edit hostname=HOSTNAME
```

Zum Ändern der Namenserver führen Sie die folgenden Kommandos aus:

```
yast dns edit nameserver1=192.168.1.116
yast dns edit nameserver2=192.168.1.117
yast dns edit nameserver3=192.168.1.118
```

16.4.1.5 Konfigurieren des Routings

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. Navigieren Sie in YaST zu *Netzwerkeinstellungen* › *Routing*.
2. Geben Sie die IP-Adresse für das *Standard-Gateway* ein (gegebenenfalls IPv4 und IPv6). Das Standard-Gateway stimmt mit jedem möglichen Ziel überein. Falls jedoch ein Eintrag in der Routingtabelle vorliegt, der mit der angegebenen Adresse übereinstimmt, wird dieser Eintrag anstelle der Standardroute über das Standard-Gateway verwendet.
3. In der *Routing-Tabelle* können weitere Einträge vorgenommen werden. Geben Sie die IP-Adresse für das *Ziel*-Netzwerk, die IP-Adresse des *Gateways* und die *Netzmaske* ein. Wählen Sie das *Gerät* aus, durch das der Datenverkehr zum definierten Netzwerk geroutet wird (das Minuszeichen steht für ein beliebiges Gerät). Verwenden Sie das Minuszeichen `-`, um diese Werte frei zu lassen. Verwenden Sie `default` im Feld *Ziel*, um in der Tabelle ein Standard-Gateway einzugeben.

   Anmerkung: Priorisieren einer Route

   Wenn mehrere Standardrouten verwendet werden, kann die Metrik-Option verwendet werden, um festzulegen, welche Route eine höhere Priorität hat. Geben Sie zur Angabe der Metrik-Option `- Metrik`*`NUMMER`* unter *Optionen* ein. Die Route mit der höchsten Metrik wird als Standard verwendet. Wenn das Netzwerkgerät getrennt wird, wird seine Route entfernt und die nächste verwendet. Der aktuelle Kernel verwendet jedoch keine Metrik bei statischem Routing (im Gegensatz zu Routing-Daemons wie `multipathd`).
4. Wenn das System ein Router ist, aktivieren Sie bei Bedarf die Optionen *IPv4-Weiterleitung* und *IPv6-Weiterleitung* in den *Netzwerkeinstellungen*.
5. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

16.4.2 IBM z Systems: Konfigurieren von Netzwerkgeräten

SUSE Linux Enterprise Server für IBM z Systems unterstützt mehrere Typen von Netzwerkschnittstellen. YaST kann zur Konfiguration dieser Schnittstellen verwendet werden.

16.4.2.1 Das qeth-hsi-Gerät

Wenn dem installierten System eine `qeth-hsi`-Schnittstelle (Hipersockets) hinzugefügt werden soll, starten Sie in YaST das Modul *System › Netzwerkeinstellungen*. Wählen Sie eines der Geräte mit der Bezeichnung *Hipersocket* aus, um es als READ-Geräteadresse zu verwenden, und klicken Sie auf *Bearbeiten*. Geben Sie die Gerätenummern für den Lese-, den Schreib- und den Steuerkanal ein (Beispiel für Gerätenummernformat: `0.0.0800`). Klicken Sie anschließend auf „Weiter“. Im Dialogfeld *Konfiguration der Netzwerkadresse* geben Sie die IP-Adresse und die Netzmaske für die neue Schnittstelle an. Klicken Sie danach auf *Weiter* und *OK*, um die Netzwerkkonfiguration zu beenden.

16.4.2.2 Das qeth-ethernet-Gerät

Wenn Sie dem installierten System eine `qeth-ethernet`-Schnittstelle (IBM OSA Express Ethernet Card) hinzufügen möchten, starten Sie in YaST das Modul *System › Netzwerkeinstellungen*. 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 *Bearbeiten*. Geben Sie eine Gerätenummer für den Lese-, den Schreib- und den Steuerkanal ein (Beispiel für Gerätenummernformat: `0.0.0700`). Geben Sie den erforderlichen Portnamen, die Portnummer (falls zutreffend), einige zusätzliche Optionen (siehe *Linux für IBM z Systems: Handbücher für Gerätetreiber, Funktionen und Befehle* als Referenz, http://www.ibm.com/developerworks/linux/linux390/documentation_suse.html), Ihre IP-Adresse und eine entsprechende Netzmaske ein. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *OK*.

16.4.2.3 Das ctc-Gerät

Wenn Sie dem installierten System eine `ctc`-Schnittstelle (IBM Parallel CTC Adapter) hinzufügen möchten, starten Sie in YaST das Modul *System › Netzwerkeinstellungen*. Wählen Sie eines der Geräte mit der Bezeichnung *IBM Parallel CTC Adapter* aus, um es als Lesekanal zu verwenden und klicken Sie auf *Konfigurieren*. Wählen Sie die *Geräteeinstellungen* für Ihre Geräte aus (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 *OK*.

Warnung: Ende der CTC-Unterstützung

Die Nutzung dieser Schnittstelle ist veraltet. Diese Schnittstelle wird in künftigen Versionen von SUSE Linux Enterprise Server nicht mehr unterstützt.

16.4.2.4 Das lcs-Gerät

Wenn Sie dem installierten System eine `lcs`-Schnittstelle (IBM OSA-2 Adapter) hinzufügen möchten, starten Sie in YaST das Modul *System* › *Netzwerkeinstellungen*. 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 z Systems: Handbücher für Gerätetreiber, Funktionen und Befehle* als Referenz, http://www.ibm.com/developerworks/linux/linux390/documentation_suse.html), Ihre IP-Adresse und eine entsprechende Netzmaske ein. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *OK*.

16.4.2.5 Das IUCV-Gerät

Wenn Sie dem installierten System eine `iucv`-Schnittstelle (IUCV) hinzufügen möchten, starten Sie in YaST das Modul *System* › *Netzwerkeinstellungen*. Wählen Sie eines der Geräte mit der Bezeichnung *IUCV* und klicken Sie auf *Bearbeiten*. YaST fordert Sie auf, den Namen Ihres IUCV-Partners (*Peer*) einzugeben. Geben Sie den Namen ein (beachten Sie die Groß-/Kleinschreibung) und wählen Sie *Weiter*. Geben Sie sowohl Ihre *IP-Adresse* als auch die *Entfernte IP-Adresse* Ihres Partners ein. Stellen Sie bei Bedarf die MTU-Größe über die Option *MTU festlegen* im Karteireiter *Allgemein* ein. Beenden Sie die Netzwerkkonfiguration mit *Weiter* und *OK*.

Warnung: Ende der IUCV-Unterstützung

Die Nutzung dieser Schnittstelle ist veraltet. Diese Schnittstelle wird in künftigen Versionen von SUSE Linux Enterprise Server nicht mehr unterstützt.

16.5 Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte 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.

16.5.1 Die `wicked`-Netzwerkkonfiguration

Das Werkzeug und die Bibilothek mit der Bezeichnung `wicked` bilden ein neues Framework für die Netzwerkkonfiguration.

Eine der Herausforderungen der traditionellen Netzwerkschnittstellenverwaltung liegt darin, dass verschiedene Netzwerkverwaltungsschichten in einem einzigen Skript oder maximal zwei Skripten vermischt werden. Diese Skripte interagieren auf nicht eindeutig definierte Weise miteinander. So entstehen unvorhersehbare Probleme, undurchsichtige Einschränkungen und Konventionen und vieles mehr. Verschiedene Schichten mit speziellen Kniffen für unterschiedliche Szenarien machen die Wartungsarbeit nicht gerade leichter. Die verwendeten Adresskonfigurationsprotokolle werden über Daemons wie dhcpcd implementiert, die eher notdürftig mit der restlichen Infrastruktur zusammenarbeiten. Die Schnittstellennamen werden anhand von merkwürdigen Schemata, die eine erhebliche udev-Unterstützung erfordern, dauerhaft identifiziert.

wicked verfolgt einen anderen Ansatz, bei dem das Problem nach mehreren Gesichtspunkten zerlegt wird. Die einzelnen Verfahren dabei sind nicht völlig neuartig, doch eröffnen die Ideen und Konzepte aus anderen Projekten unterm Strich eine bessere Gesamtlösung.

Ein mögliches Verfahren ist das Client/Server-Modell. wicked ist hiermit in der Lage, standardisierte Funktionen für Bereiche wie die Adresskonfiguration zu definieren, die gut in das Framework als Ganzes eingebunden sind. Über eine bestimmte Adresskonfiguration kann der Administrator beispielsweise festlegen, dass eine Schnittstelle mit DHCP oder IPv4 zeroconf konfiguriert werden soll. In diesem Fall holt der Adresskonfigurationsdienst lediglich das Lease vom Server ein und übergibt es an den wicked-Serverprozess, mit dem die Anforderungen Adressen und Routen installiert werden.

Das zweite Verfahren zur Problemzerlegung ist die Erzwingung der Schichten. Für alle Arten von Netzwerkschnittstellen kann ein dbus-Service definiert werden, mit dem die Geräteschicht der Netzwerkschnittstelle konfiguriert wird – ein VLAN, eine Bridge, ein Bonding oder ein paravirtualisiertes Gerät. Häufig verwendete Funktionen, z. B. die Adresskonfiguration, wird über gemeinsame Services implementiert, die sich in einer Schicht oberhalb dieser gerätespezifischen Services befinden, ohne dass sie eigens implementiert werden müssen.

Im wicked-Framework werden diese beiden Aspekte durch eine Vielzahl von dbus-Services zusammengeführt, die den Netzwerkschnittstellen je nach ihrem Typ zugeordnet werden. Im Folgenden finden Sie einen kurzen Überblick über die aktuelle Objekthierarchie in wicked.

Die Netzwerkschnittstelle wird jeweils als untergeordnetes Objekt von `/org/opensuse/Network/Interfaces` dargestellt. Die Bezeichnung des untergeordneten Objekts ergibt sich aus dem zugehörigen Wert für ifindex. Die Loopback-Schnittstelle (in der Regel ifindex 1) ist beispielsweise `/org/opensuse/Network/Interfaces/1`, und die erste registrierte Ethernet-Schnittstelle ist `/org/opensuse/Network/Interfaces/2`.

Jede Netzwerkschnittstelle ist mit einer „Klasse“ verknüpft, mit der die unterstützten dbus-Schnittstellen ausgewählt werden. Standardmäßig gehören alle Netzwerkschnittstellen zur Klasse `netif`, und wicked ordnet automatisch alle Schnittstellen zu, die mit dieser Klasse kompatibel sind. In der aktuellen Implementierung gilt dies für die folgenden Schnittstellen:

org.opensuse.Network.Interface
: Allgemeine Funktionen für Netzwerkschnittstellen, z. B. Herstellen oder Beenden der Verbindung, Zuweisen einer MTU und vieles mehr.

org.opensuse.Network.Addrconf.ipv4.dhcp,
org.opensuse.Network.Addrconf.ipv6.dhcp,
org.opensuse.Network.Addrconf.ipv4.auto
: Adresskonfigurationsservices für DHCP, IPv4 zeroconf usw.

Darüber hinaus können die Netzwerkschnittstellen bestimmte Konfigurationsmechanismen erfordern oder anbieten. Bei einem Ethernet-Gerät benötigen Sie beispielsweise Funktionen zum Steuern der Verbindungsgeschwindigkeit, zum Abgeben der Prüfsummenberechnung usw. Ethernet-Geräte gehören daher zu einer eigenen Klasse (`netif-ethernet`), die wiederum eine Subklasse von `netif` ist. Aus diesem Grund umfassen die dbus-Schnittstellen, die mit einer Ethernet-Schnittstelle verknüpft sind, alle oben aufgeführten Services und zusätzlich den Service `org.opensuse.Network.Ethernet`, der ausschließlich für Objekte der Klasse `netif-ethernet` verfügbar ist.

Ebenso bestehen Klassen für Schnittstellentypen wie Bridges, VLANs, Bonds oder InfiniBands.

Wie interagieren Sie mit einer Schnittstelle wie VLAN (die im Grunde genommen eine virtuelle Netzwerkschnittstelle über einem Ethernet-Gerät bildet), die erst noch erstellt werden muss? Hierfür werden Factory-Schnittstellen in wicked definiert, beispielsweise `org.opensuse.Net-`

work.VLAN.Factory. Diese Factory-Schnittstellen bieten nur eine einzige Funktion, mit der Sie eine Schnittstelle mit dem gewünschten Typ erstellen. Die Factory-Schnittstellen sind dem Listenknoten /org/opensuse/Network/Interfaces zugeordnet.

16.5.1.1 wicked-Architektur und -Funktionen

Der wicked-Dienst umfasst mehrere Teile, wie in *Abbildung 16.4, „wicked-Architektur“* dargestellt.

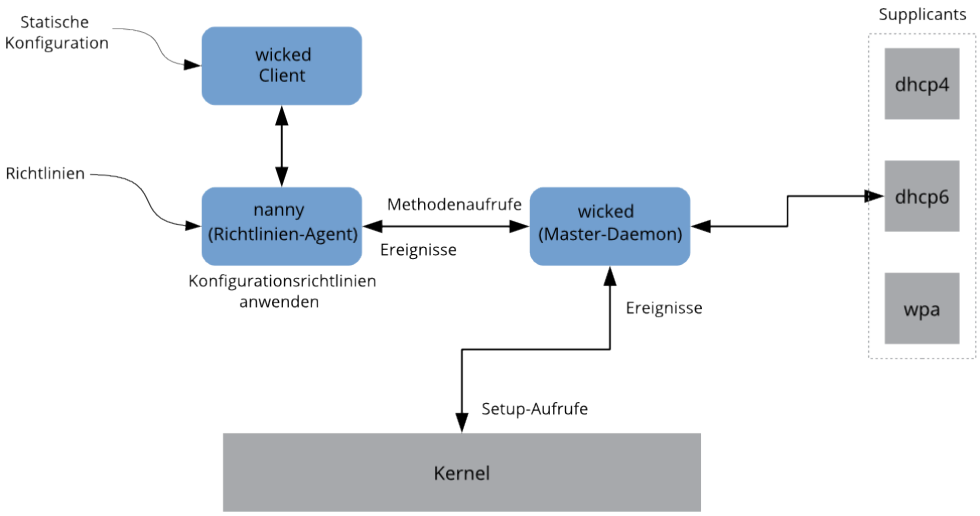


ABBILDUNG 16.4 wicked-ARCHITEKTUR

wicked unterstützt derzeit Folgendes:

- Konfigurationsdatei-Back-Ends zum Analysieren von /etc/sysconfig/network-Dateien im SUSE-Format.
- Internes Konfigurationsdatei-Back-End zur Darstellung der Netzwerkschnittstellenkonfiguration in XML.
- Hoch- und Herunterfahren für „normale“ Netzwerkschnittstellen wie Ethernet oder InfiniBand, außerdem für VLAN-, Bridge-, Bonds-, TUN-, TAP-, Dummy-, MacVLan-, MacVTap-, HSI-, QETH- und IUCV-Geräte sowie für drahtlose Geräte (derzeit auf nur ein WPA-PSK-/EAP-Netzwerk beschränkt).
- Integrierter DHCPv4-Client und integrierter DHCPv6-Client.

- Der nanny-Daemon (standardmäßig aktiviert) fährt konfigurierte Schnittstellen automatisch hoch, wenn das Gerät verfügbar ist (Schnittstellen-Hotplugging), und richtet die IP-Konfiguration ein, wenn eine Verbindung (Träger) erkannt wird. Weitere Informationen finden Sie unter *Abschnitt 16.5.1.3, „Nanny“*.
- `wicked` wurde als eine Gruppe von DBus-Diensten implementiert, die mit systemd integriert sind. Daher sind die üblichen **`systemctl`**-Kommandos auch für `wicked` gültig.

16.5.1.2 Verwendung von `wicked`

Bei SUSE Linux Enterprise wird `wicked` standardmäßig ausgeführt. Mit dem folgenden Befehl stellen Sie fest, welche Elemente derzeit aktiviert sind und ob sie ausgeführt werden:

Auf openSUSE Leap wird `wicked` standardmäßig auf Desktop- oder Serverhardware ausgeführt. Auf Mobilgeräte-Hardware wird standardmäßig NetworkManager ausgeführt. Mit dem folgenden Befehl stellen Sie fest, welche Elemente derzeit aktiviert sind und ob sie ausgeführt werden:

```
systemctl status network
```

Wenn `wicked` aktiviert ist, erhalten Sie die folgende Ausgabe (Beispiel):

```
wicked.service - wicked managed network interfaces
    Loaded: loaded (/usr/lib/systemd/system/wicked.service; enabled)
    ...
```

Falls andere Elemente ausgeführt werden (z. B. NetworkManager) und Sie zu `wicked` wechseln möchten, halten Sie zunächst die ausgeführten Elemente an und aktivieren Sie dann `wicked`:

```
systemctl is-active network && \
systemctl stop      network
systemctl enable --force wicked
```

Beim nächsten Booten werden damit die wicked-Services aktiviert, die Alias-Verknüpfung von `network.service` und `wicked.service` wird erstellt, und das Netzwerk wird gestartet.

Starten des Serverprozesses:

```
systemctl start wickedd
```

Hiermit werden sowohl **`wicked`** (der Hauptserver) und die zugehörigen Supplicants gestartet:

```
/usr/lib/wicked/bin/wickedd-auto4 --systemd --foreground
/usr/lib/wicked/bin/wickedd-dhcp4 --systemd --foreground
/usr/lib/wicked/bin/wickedd-dhcp6 --systemd --foreground
```

```
/usr/sbin/wickedd --systemd --foreground
/usr/sbin/wickedd-nanny --systemd --foreground
```

Fahren Sie dann das Netzwerk hoch:

```
systemctl start wicked
```

Alternativ verwenden Sie das `network`-Alias:

```
systemctl start network
```

Bei diesen Kommandos werden die standardmäßigen oder die systemeigenen Konfigurationsquellen verwendet, die in `/etc/wicked/client.xml` definiert sind.

Zum Aktivieren der Fehlersuche legen Sie `WICKED_DEBUG_` in `/etc/sysconfig/network/config` fest, beispielsweise:

```
WICKED_DEBUG="all"
```

Sollen einige Aspekte ausgelassen werden:

```
WICKED_DEBUG="all,-dbus,-objectmodel,-xpath,-xml"
```

Mit dem Clientprogramm rufen Sie die Schnittstellendaten für alle Schnittstellen bzw. für die mit *IFNAME* angegebenen Schnittstellen ab:

```
wicked show all
wicked show IFNAME
```

Als XML-Ausgabe:

```
wicked show-xml all
wicked show-xml IFNAME
```

Starten einer bestimmten Schnittstelle:

```
wicked ifup eth0
wicked ifup wlan0
...
```

Da keine Konfigurationsquelle angegeben ist, prüft der wicked-Client die Standard-Konfigurationsquellen, die in `/etc/wicked/client.xml` definiert sind:

1. `firmware:` iSCSI Boot Firmware Table (iBFT)
2. `compat:` `ifcfg`-Dateien; aus Kompatibilitätsgründen implementiert

Alle Informationen, die `wicked` aus diesen Quellen für eine bestimmte Schnittstelle erhält, werden übernommen und angewendet. Die geplante Reihenfolge lautet `firmware`, dann `compat`. Diese Reihenfolge wird unter Umständen demnächst geändert.

Weitere Informationen finden Sie auf der man-Seite zu **`wicked`**.

16.5.1.3 Nanny

Der ereignis- und richtliniengestützte Daemon nanny ist für asynchrone oder unverlangte Szenarien zuständig, beispielsweise für das Hotplugging von Geräten. Der nanny-Daemon hilft also dabei, verzögerte oder vorübergehend ausgefallene Dienste zu starten oder neu zu starten. Nanny überwacht Veränderungen an den Geräten und Verknüpfungen und bindet neue Geräte gemäß dem aktuellen Richtliniensatz ein. Nanny fährt aufgrund von angegebenen Einschränkungen zur Zeitüberschreitung mit dem Einrichten fort, auch wenn **`ifup`** bereits beendet ist.

Standardmäßig ist der nanny-Daemon im System aktiv. Er wird in der Konfigurationsdatei `/etc/wicked/common.xml` aktiviert:

```
<config>
  ...
  <use-nanny>true</use-nanny>
</config>
```

Durch diese Einstellung wenden ifup und ifreload eine Richtlinie mit der effektiven Konfiguration auf den Daemon an; anschließend führt nanny die Konfiguration von `wicked` aus und sorgt so für die Hotplug-Unterstützung. Der Daemon wartet im Hintergrund auf Ereignisse oder Änderungen (beispielsweise auf neue Geräte oder auf die Erkennung eines Trägers).

16.5.1.4 Starten von mehreren Schnittstellen

Bei Bonds und Bridges ist es unter Umständen sinnvoll, die gesamte Gerätetopologie in einer einzigen Datei zu definieren (ifcfg-bondX) und alle Geräte in einem Arbeitsgang hochzufahren. Mit wicked können Sie dann die Schnittstellennamen der obersten Ebene (für den Bridge oder den Bond) angeben und so die gesamte Konfiguration hochfahren:

```
wicked ifup br0
```

Dieser Befehl richtet automatisch die Bridge und ihre Abhängigkeiten in der richtigen Reihenfolge ein, ohne dass die Abhängigkeiten (Ports usw.) getrennt aufgeführt werden müssten.

So fahren Sie mehrere Schnittstellen mit einem einzigen Befehl hoch:

```
wicked ifup bond0 br0 br1 br2
```

Oder auch alle Schnittstellen:

```
wicked ifup all
```

16.5.1.5 Verwenden von Tunneln mit Wicked

Wenn Sie Tunnels mit Wicked verwenden müssen, wird `TUNNEL_DEVICE` hierfür verwendet. Die Option erlaubt es, einen optionalen Gerätenamen anzugeben, um den Tunnel an das Gerät zu binden. Die getunnelten Pakete werden nur über dieses Gerät geleitet.

Weitere Informationen erhalten Sie mit dem Kommando **`man 5 ifcfg-tunnel`**.

16.5.1.6 Einarbeiten von inkrementellen Änderungen

Bei **`wicked`** müssen Sie eine Schnittstelle zum Neukonfigurieren nicht vollständig herunterfahren (sofern dies nicht durch den Kernel erforderlich ist). Wenn Sie beispielsweise eine weitere IP-Adresse oder Route für eine statisch konfigurierte Netzwerkschnittstelle hinzufügen möchten, tragen Sie die IP-Adresse in die Schnittstellendefinition ein und führen Sie den „ifup“-Vorgang erneut aus. Der Server aktualisiert lediglich die geänderten Einstellungen. Dies gilt für Optionen auf Verbindungsebene (z. B. die MTU oder die MAC-Adresse des Geräts) sowie auf Netzwerkebene, beispielsweise die Adressen, Routen oder gar der Adresskonfigurationsmodus (z. B. bei der Umstellung einer statischen Konfiguration auf DHCP).

Bei virtuellen Schnittstellen, in denen mehrere physische Geräte miteinander verbunden werden (z. B. Bridges oder Bonds), ist die Vorgehensweise naturgemäß komplizierter. Bei Bond-Geräten können bestimmte Parameter nicht geändert werden, wenn das Gerät eingeschaltet ist. Ansonsten würde ein Fehler auftreten.

Als Alternative können Sie stattdessen untergeordnete Geräte des Bonds oder der Bridge hinzufügen oder entfernen oder auch die primäre Schnittstelle eines Bonds festlegen.

16.5.1.7 wicked-Erweiterungen: Adresskonfiguration

`wicked` lässt sich mithilfe von Shell-Skripten erweitern. Diese Erweiterungen können in der Datei `config.xml` definiert werden.

Derzeit werden mehrere Erweiterungsklassen unterstützt:

- Verbindungskonfiguration: Skripte zum Einrichten der Verbindungsschicht eines Geräts gemäß der Konfiguration, die vom Client bereitgestellt wurde, sowie zum Entfernen dieser Schicht.
- Adresskonfiguration: Skripte zum Verwalten der Konfiguration einer Geräteadresse. Die Adresskonfiguration und DHCP werden in der Regel von **`wicked`** selbst verwaltet, können jedoch auch in Form von Erweiterungen implementiert werden.
- Firewall-Erweiterung: Mit diesen Skripten werden Firewall-Regeln angewendet.

Erweiterungen umfassen im Normalfall ein Start- und Stopp-Kommando, eine optionale „pid-Datei“ sowie eine Reihe von Umgebungsvariablen, die an das Skript übergeben werden.

In `etc/server.xml` finden Sie ein Beispiel für eine Firewall-Erweiterung:

```
<dbus-service interface="org.opensuse.Network.Firewall">
 <action name="firewallUp"   command="/etc/wicked/extensions/firewall up"/>
 <action name="firewallDown" command="/etc/wicked/extensions/firewall down"/>

 <!-- default environment for all calls to this extension script -->
 <putenv name="WICKED_OBJECT_PATH" value="$object-path"/>
 <putenv name="WICKED_INTERFACE_NAME" value="$property:name"/>
 <putenv name="WICKED_INTERFACE_INDEX" value="$property:index"/>
</dbus-service>
```

Die Erweiterung wird an den Tag `<dbus-service>` angehängt und definiert auszuführende Kommandos für die Aktionen dieser Schnittstelle. In der Deklaration können außerdem Umgebungsvariablen, die an die Aktion übergeben werden sollen, definiert und initialisiert werden.

16.5.1.8 wicked-Erweiterungen: Konfigurationsdateien

Auch die Arbeit mit Konfigurationsdateien kann mithilfe von Skripten erweitert werden. DNS-Aktualisierungen über Leases werden beispielsweise letztlich von dem Skript `extensions/resolver` verarbeitet, dessen Verhalten in `server.xml` konfiguriert ist:

```
<system-updater name="resolver">
 <action name="backup" command="/etc/wicked/extensions/resolver backup"/>
 <action name="restore" command="/etc/wicked/extensions/resolver restore"/>
 <action name="install" command="/etc/wicked/extensions/resolver install"/>
 <action name="remove" command="/etc/wicked/extensions/resolver remove"/>
```

```
</system-updater>
```

Sobald eine Aktualisierung in `wicked` eingeht, wird das Lease durch die Systemaktualisierungsroutinen analysiert, und die entsprechenden Kommandos (`backup`, `install` usw.) im Auflöserskript werden aufgerufen. Hiermit werden wiederum die DNS-Einstellungen über **`/sbin/netconfig`** konfiguriert; als Fallback muss die Datei `/etc/resolv.conf` manuell geschrieben werden.

16.5.2 Konfigurationsdateien

Dieser Abschnitt bietet einen Überblick über die Netzwerkkonfigurationsdateien und erklärt ihren Zweck sowie das verwendete Format.

16.5.2.1 `/etc/wicked/common.xml`

Die Datei `/etc/wicked/common.xml` enthält allgemeine Definitionen, die von allen Anwendungen verwendet werden sollten. Sie wird von den anderen Konfigurationsdateien in diesem Verzeichnis als Quelle verwendet/eingeschlossen. Obwohl Sie diese Datei zum Aktivieren der Fehlerbehebung für alle `wicked`-Komponenten verwenden können, empfehlen wir, hierfür die Datei `/etc/wicked/local.xml` zu verwenden. Nach dem Anwenden von Wartungsaktualisierungen können Ihre Änderungen verloren gehen, da die Datei `/etc/wicked/common.xml` möglicherweise überschrieben wird. Die Datei `/etc/wicked/common.xml` enthält `/etc/wicked/local.xml` in der Standardinstallation, daher müssen Sie in der Regel `/etc/wicked/common.xml` nicht bearbeiten.

Falls Sie `nanny` deaktivieren möchten, indem Sie für `<use-nanny>` den Wert `false` festlegen, starten Sie den Dienst `wickedd.service` neu und führen Sie anschließend das folgende Kommando aus, um alle Konfigurationen und Richtlinien anzuwenden:

```
wicked ifup all
```

Anmerkung: Konfigurationsdateien

Die Programme `wickedd`, `wicked` oder `nanny` versuchen, die Datei `/etc/wicked/common.xml` zu lesen, wenn sie über keine eigene Konfigurationsdatei verfügen.

16.5.2.2 /etc/wicked/server.xml

Die Datei `/etc/wicked/server.xml` wird vom Serverprozess `wickedd` beim Starten gelesen. Die Datei speichert Erweiterungen zu der Datei `/etc/wicked/common.xml`. Zusätzlich konfiguriert diese Datei die Handhabung von Resolvern und den Empfang von Informationen von `addrconf`-Supplicants, z. B. DHCP.

Es wird empfohlen, erforderliche Änderungen an dieser Datei der separaten Datei `/etc/wicked/server-local.xml` hinzuzufügen. Diese wird von `/etc/wicked/server.xml` eingeschlossen. Durch Verwenden einer separaten Datei vermeiden Sie das Überschrieben Ihrer Änderungen bei Wartungsaktualisierungen.

16.5.2.3 /etc/wicked/client.xml

Die Datei `/etc/wicked/client.xml` wird vom Kommando **`wicked`** verwendet. Die Datei gibt den Speicherort eines Skripts an, der beim Ermitteln von Geräten, die von ibft verwaltet werden, verwendet wird. Außerdem konfiguriert die Datei die Speicherpositionen der Konfigurationen von Netzwerkschnittstellen.

Es wird empfohlen, erforderliche Änderungen an dieser Datei in der separaten Datei `/etc/wicked/client-local.xml` hinzuzufügen. Diese wird von `/etc/wicked/server.xml` eingeschlossen. Durch Verwenden einer separaten Datei vermeiden Sie das Überschrieben Ihrer Änderungen bei Wartungsaktualisierungen.

16.5.2.4 /etc/wicked/nanny.xml

Die Datei `/etc/wicked/nanny.xml` konfiguriert die Typen der Verbindungsschichten. Es wird empfohlen, spezielle Konfigurationen der separaten Datei `/etc/wicked/nanny-local.xml` hinzuzufügen, um den Verlust der Änderungen bei Wartungsaktualisierungen zu vermeiden.

16.5.2.5 /etc/sysconfig/network/ifcfg-*

Diese Dateien enthalten die herkömmlichen Konfigurationsdaten für Netzwerkschnittstellen. In SUSE Linux Enterprise 11 war dies das einzige unterstützte Format neben der iBFT-Firmware.

Anmerkung: **wicked** und ifcfg-*-Dateien

wicked liest diese Dateien, wenn Sie das Präfix compat: angeben. Gemäß der Standardkonfiguration von SUSE Linux Enterprise Server in /etc/wicked/client.xml berücksichtigt **wicked** diese Dateien noch vor den XML-Konfigurationsdateien in /etc/wicked/ifconfig.

Der Schalter --ifconfig wird überwiegend zu Testzwecken verwendet. Wenn dieser Schalter angegeben ist, werden die in /etc/wicked/ifconfig definierten standardmäßigen Konfigurationsquellen nicht angewendet.

Die ifcfg-*-Dateien enthalten Informationen wie den Startmodus und die IP-Adresse. Mögliche Parameter sind auf der man-Seite für den Befehl ifup beschrieben. Wenn eine allgemeine Einstellung nur für eine bestimmte Bedienoberfläche verwendet werden soll, können außerdem alle Variablen aus den Dateien dhcp und wireless in den ifcfg-*-Dateien verwendet werden. Jedoch sind die meisten /etc/sysconfig/network/config-Variablen global und lassen sich in ifcfg-Dateien nicht überschreiben. Beispielsweise sind die Variablen NETCONFIG_* global.

Weitere Informationen zum Konfigurieren der macvlan- und der macvtab-Schnittstelle finden Sie auf den man-Seiten zu ifcfg-macvlan und ifcfg-macvtap. Für eine macvlan-Schnittstelle benötigen Sie beispielsweise eine ifcfg-macvlan0-Datei mit den folgenden Einstellungen:

```
STARTMODE='auto'
MACVLAN_DEVICE='eth0'
#MACVLAN_MODE='vepa'
#LLADDR=02:03:04:05:06:aa
```

Informationen zu ifcfg.template finden Sie unter *Abschnitt 16.5.2.6, „/etc/sysconfig/network/config, /etc/sysconfig/network/dhcp und /etc/sysconfig/network/wireless“*.

System z IBM z Systems unterstützt USB nicht. Die Namen der Schnittstellendateien und Netzwerkaliase enthalten z Systems-spezifische Elemente wie qeth.

16.5.2.6 /etc/sysconfig/network/config, /etc/sysconfig/network/dhcp und /etc/sysconfig/network/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. Einige der Varia-

blen von `/etc/sysconfig/network/config` können auch in `ifcfg-*`-Dateien verwendet werden, wo sie eine höhere Priorität erhalten. Die Datei `/etc/sysconfig/network/ifcfg.template` listet Variablen auf, die mit einer Reichweite pro Schnittstelle angegeben werden können. Jedoch sind die meisten `/etc/sysconfig/network/config`-Variablen global und lassen sich in ifcfg-Dateien nicht überschreiben. Beispielsweise sind die Variablen `NETWORKMANAGER` oder `NETCONFIG_*` global.

Anmerkung: Verwenden von DHCPv6

In SUSE Linux Enterprise 11 konnte DHCPv6 selbst auf Netzwerken genutzt werden, deren IPv6-RAs (Router Advertisements) nicht fehlerfrei konfiguriert waren. Ab SUSE Linux Enterprise 12 verlangt DHCPv6 (richtigerweise), dass mindestens ein Router im Netzwerk RAs aussendet, aus denen hervorgeht, dass das Netzwerk über DHCPv6 verwaltet wird.

In Netzwerken, in denen der Router nicht ordnungsgemäß konfiguriert werden kann, können Sie dieses Verhalten mit einer `ifcfg`-Option außer Kraft setzen. Geben Sie hierzu `DHCLIENT6_MODE='managed'` in der `ifcfg`-Datei an. Alternativ wenden Sie diese Behelfslösung mit einem Bootparameter im Installationssystem an:

```
ifcfg=eth0=dhcp6,DHCLIENT6_MODE=managed
```

16.5.2.7 `/etc/sysconfig/network/routes` und `/etc/sysconfig/network/ifroute-*`

Das statische Routing von TCP/IP-Paketen wird mit den Dateien `/etc/sysconfig/network/routes` und `/etc/sysconfig/network/ifroute-*` bestimmt. Alle statischen Routen, die für verschiedene Systemaufgaben benötigt werden, können in `/etc/sysconfig/network/routes` angegeben werden: Routen zu einem Host, Routen zu einem Host über Gateways und Routen zu einem Netzwerk. Definieren Sie für jede Schnittstelle, die individuelles Routing benötigt, eine zusätzliche Konfigurationsdatei: `/etc/sysconfig/network/ifroute-*`. Ersetzen Sie das Platzhalterzeichen (`*`) durch den Namen der Schnittstelle. Die folgenden Einträge werden in die Routing-Konfigurationsdatei aufgenommen:

```
# Destination     Gateway           Netmask           Interface  Options
```

Das Routenziel steht in der ersten Spalte. Diese Spalte kann die IP-Adresse eines Netzwerks oder Hosts bzw. (im Fall von *erreichbaren* Nameservern) den voll qualifizierten Netzwerk- oder Hostnamen enthalten. Die Netzwerkadresse muss in der CIDR-Notation (Adresse mit entsprechender Routing-Präfixlänge) angegeben werden, z. B. 10.10.0.0/16 für IPv4-Routen oder fc00::/7 für IPv6-Routen. Das Schlüsselwort `default` gibt an, dass die Route des Standard-Gateways in derselben Adressfamilie wie der Gateway ist. Bei Geräten ohne Gateway verwenden Sie die expliziten Ziele 0.0.0.0/0 oder ::/0.

Die zweite Spalte enthält das Standard-Gateway oder ein Gateway, über das der Zugriff auf einen Host oder ein Netzwerk erfolgt.

Die dritte Spalte wird nicht mehr verwendet; hier wurde bislang die IPv4-Netzmaske des Ziels angegeben. Für IPv6-Routen, für die Standardroute oder bei Verwendung einer Präfixlänge (CIDR-Notation) in der ersten Spalte tragen Sie hier einen Strich (`-`) ein.

Die vierte Spalte enthält den Namen der Schnittstelle. Wenn Sie in dieser Spalte nur einen Strich (`-`) statt eines Namens angeben, kann dies zu unerwünschtem Verhalten in `/etc/sysconfig/network/routes` führen. Weitere Informationen finden Sie auf der man-Seite zu `routes`.

In einer (optionalen) fünften Spalte können Sie besondere Optionen angeben. Weitere Informationen finden Sie auf der man-Seite zu `routes`.

BEISPIEL 16.5 GEBRÄUCHLICHE NETZWERKSCHNITTSTELLEN UND BEISPIELE FÜR STATISCHE ROUTEN

```
# --- IPv4 routes in CIDR prefix notation:
# Destination     [Gateway]         -                 Interface
127.0.0.0/8       -                 -                 lo
204.127.235.0/24  -                 -                 eth0
default           204.127.235.41    -                 eth0
207.68.156.51/32  207.68.145.45     -                 eth1
192.168.0.0/16    207.68.156.51     -                 eth1

# --- IPv4 routes in deprecated netmask notation"
# Destination     [Dummy/Gateway]   Netmask           Interface
#
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

# --- IPv6 routes are always using CIDR notation:
# Destination     [Gateway]               -           Interface
2001:DB8:100::/64 -                       -           eth0
```

```
2001:DB8:100::/32 fe80::216:3eff:fe6d:c042 -           eth0
```

16.5.2.8 /etc/resolv.conf

In `/etc/resolv.conf` wird die Domäne angegeben, zu der der Host gehört (Schlüsselwort `search`). Mit der Option `search` können Sie bis zu sechs Domänen mit insgesamt 256 Zeichen angeben. Bei der Auflösung eines Namens, der nicht voll qualifiziert ist, wird versucht, einen solchen zu generieren, indem die einzelnen `search`-Einträge angehängt werden. Mit der Option `nameserver` können Sie bis zu drei Nameserver angeben (jeweils in einer eigenen Zeile). Kommentare sind mit einer Raute (`#`) oder einem Semikolon (`;`) gekennzeichnet. Ein Beispiel finden Sie in *Beispiel 16.6, „/etc/resolv.conf“*.

Jedoch darf `/etc/resolv.conf` nicht manuell bearbeitet werden. Stattdessen wird es vom Skript **`netconfig`** generiert. Um die statische DNS-Konfiguration ohne YaST zu definieren, bearbeiten Sie die entsprechenden Variablen in der Datei `/etc/sysconfig/network/config` manuell:

`NETCONFIG_DNS_STATIC_SEARCHLIST`
: Liste der DNS-Domänennamen, die für die Suche nach Hostname verwendet wird

`NETCONFIG_DNS_STATIC_SERVERS`
: Liste der IP-Adressen des Nameservers, die für die Suche nach Hostname verwendet wird

`NETCONFIG_DNS_FORWARDER`
: Name des zu konfigurierenden DNS-Forwarders, beispielsweise `bind` oder `resolver`

`NETCONFIG_DNS_RESOLVER_OPTIONS`
: Verschiedene Optionen, die in `/etc/resolv.conf` geschrieben werden, beispielsweise:

```
debug attempts:1 timeout:10
```

Weitere Informationen finden Sie auf der man-Seite zu `resolv.conf`.

`NETCONFIG_DNS_RESOLVER_SORTLIST`
: Liste mit bis zu 10 Einträgen, beispielsweise:

```
130.155.160.0/255.255.240.0 130.155.0.0
```

Weitere Informationen finden Sie auf der man-Seite zu `resolv.conf`.

Zum Deaktivieren der DNS-Konfiguration mit netconfig setzen Sie `NETCONFIG_DNS_POLICY=''`. Weitere Informationen zu **`netconfig`** finden Sie auf der man-Seite zu `netconfig(8)` (**`man 8 netconfig`**).

BEISPIEL 16.6 `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

16.5.2.9 /sbin/netconfig

`netconfig` ist ein modulares Tool zum Verwalten zusätzlicher Netzwerkkonfigurationseinstellungen. Es führt statisch definierte Einstellungen mit Einstellungen zusammen, die von automatischen Konfigurationsmechanismen wie DHCP oder PPP gemäß einer vordefinierten Richtlinie bereitgestellt wurden. Die erforderlichen Änderungen werden dem System zugewiesen, indem die netconfig-Module aufgerufen werden, die für das Ändern einer Konfigurationsdatei und den Neustart eines Service oder eine ähnliche Aktion verantwortlich sind.

`netconfig` erkennt drei Hauptaktionen. Die Kommandos **`netconfig modify`** und **`netconfig remove`** werden von Daemons wie DHCP oder PPP verwendet, um Einstellungen für netconfig hinzuzufügen oder zu entfernen. Nur das Kommando **`netconfig update`** steht dem Benutzer zur Verfügung:

`modify`

Das Kommando **`netconfig modify`** ändert die aktuelle Schnittstellen- und Service-spezifischen dynamischen Einstellungen und aktualisiert die Netzwerkkonfiguration. Netconfig liest Einstellungen aus der Standardeingabe oder einer Datei, die mit der Option `--lease-file` *`DATEINAME`* angegeben wurde, und speichert sie intern bis zu einem System-Reboot oder der nächsten Änderungs- oder Löschaktion). Bereits vorhandene Einstellungen für dieselbe Schnittstellen- und Service-Kombination werden überschrieben. Die Schnittstelle wird durch den Parameter `-i` *`SCHNITTSTELLENNAME`* angegeben. Der Service wird durch den Parameter `-s` *`SERVICENAME`* angegeben.

`Entfernen`

Das Kommando **`netconfig remove`** entfernt die dynamischen Einstellungen, die von einer Änderungsaktion für die angegebene Schnittstellen- und Service-Kombination bereitgestellt wurden, und aktualisiert die Netzwerkkonfiguration. Die Schnittstelle wird durch den Parameter `-i` *`SCHNITTSTELLENNAME`* angegeben. Der Service wird durch den Parameter `-s` *`SERVICENAME`* angegeben.

`Aktualisieren`

Das Kommando **`netconfig update`** aktualisiert die Netzwerkkonfiguration mit den aktuellen Einstellungen. Dies ist nützlich, wenn sich die Richtlinie oder die statische Konfiguration geändert hat. Verwenden Sie den Parameter `-m`*`MODULE_TYPE`*, wenn nur ein angegebener Dienst aktualisiert werden soll (`dns`, `nis` oder `ntp`).

Die Einstellungen für die netconfig-Richtlinie und die statische Konfiguration werden entweder manuell oder mithilfe von YaST in der Datei `/etc/sysconfig/network/config` definiert. Die dynamischen Konfigurationseinstellungen von Tools zur automatischen Konfiguration wie DHCP oder PPP werden von diesen Tools mit den Aktionen **`netconfig modify`** und **`netconfig remove`** direkt bereitgestellt. Wenn NetworkManager aktiviert ist, verwendet netconfig (im Richtlinienmodus `auto`) nur NetworkManager-Einstellungen und ignoriert Einstellungen von allen anderen Schnittstellen, die mit der traditionellen ifup-Methode konfiguriert wurden. Wenn NetworkManager keine Einstellung liefert, werden als Fallback statische Einstellungen verwendet. Eine gemischte Verwendung von NetworkManager und der **`wicked`**-Methode wird nicht unterstützt.

Weitere Informationen über **`netconfig`** finden Sie auf **`man 8 netconfig`**.

16.5.2.10 `/etc/hosts`

In dieser Datei werden, wie in *Beispiel 16.7, „`/etc/hosts`“* gezeigt, IP-Adressen zu Hostnamen zugewiesen. Wenn kein Namenserver 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 16.7 `/etc/hosts`

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
```

```
192.168.2.101 venus.example.com venus
```

16.5.2.11 /etc/networks

Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen. Weitere Informationen hierzu finden Sie unter *Beispiel 16.8, „/etc/networks“*.

BEISPIEL 16.8 `/etc/networks`

```
loopback    127.0.0.0
localnet    192.168.0.0
```

16.5.2.12 /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 immer auf einer separaten Zeile eingegeben werden. Kommentare werden durch ein `#`-Zeichen eingeleitet. Die verfügbaren Parameter sind in *Tabelle 16.2, „Parameter für /etc/host.conf“* aufgeführt. Ein Beispiel für `/etc/host.conf` wird in *Beispiel 16.9, „/etc/host.conf“* gezeigt.

TABELLE 16.2 PARAMETER FÜR /ETC/HOST.CONF

order *hosts*, *bind*	Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente (getrennt durch Leerzeichen oder Kommas):
	Hosts: Sucht die `/etc/hosts`-Datei
	bind: Greift auf einen Namenserver zu
	nis: Verwendet NIS
multi *on/off*	Legt fest, ob ein in `/etc/hosts` eingegebener Host mehrere IP-Adressen haben kann.

nospoof *on* spoofalert *on/off*	Diese Parameter beeinflussen das *spoofing* des Namenservers, haben aber keinen Einfluss auf die Netzwerkkonfiguration.
trim *Domänenname*	Der angegebene Domänenname wird vor dem Auflösen des Hostnamens von diesem abgeschnitten (insofern der Hostname diesen Domänennamen enthält). Diese Option ist nur dann von Nutzen, wenn in der Datei `/etc/hosts` nur Namen aus der lokalen Domäne stehen, diese aber auch mit angehängtem Domänennamen erkannt werden sollen.

BEISPIEL 16.9 `/etc/host.conf`

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

16.5.2.13 `/etc/nsswitch.conf`

Mit der GNU C Library 2.0 wurde *Name Service Switch* (NSS) eingeführt. Weitere Informationen hierzu finden Sie auf der man-Seite 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 16.10, „/etc/nsswitch.conf“* dargestellt. Kommentaren werden `#`-Zeichen vorangestellt. Der Eintrag unter der `hosts`-Datenbank bedeutet, dass Anfragen über DNS an `/etc/hosts` (`files`) gehen (siehe *Kapitel 25, Domain Name System (DNS)*).

BEISPIEL 16.10 `/etc/nsswitch.conf`

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns
```

```
services:   db files
protocols:  db files
rpc:        files
ethers:     files
netmasks:   files
netgroup:   files nis
publickey:  files

bootparams: files
automount:  files nis
aliases:    files nis
shadow:     compat
```

Die über NSS verfügbaren „Datenbanken“ sind in *Tabelle 16.3, „Über /etc/nsswitch.conf verfügbare Datenbanken“* aufgelistet.
Die Konfigurationsoptionen für NSS-Datenbanken sind in *Tabelle 16.4, „Konfigurationsoptionen für NSS-„Datenbanken““* aufgelistet.

TABELLE 16.3 ÜBER /ETC/NSSWITCH.CONF VERFÜGBARE DATENBANKEN

`aliases`	Mail-Aliasse, die von `sendmail` implementiert werden. Siehe **`man 5 aliases`**.
`ethers`	Ethernet-Adressen
`Netzmasken`	Liste von Netzwerken und ihrer Teilnetzmasken. Wird nur benötigt, wenn Sie Subnetting nutzen.
`Gruppe`	Benutzergruppen, die von `getgrent` verwendet werden. Weitere Informationen hierzu finden Sie auch auf der man-Seite für den Befehl **`group`**.
`hosts`	Hostnamen und IP-Adressen, die von `gethostbyname` und ähnlichen Funktionen verwendet werden.
`netgroup`	Im Netzwerk gültige Host- und Benutzerlisten zum Steuern von Zugriffsberechtigungen. Weitere Informationen hierzu finden Sie auf der man-Seite für `netgroup(5)`.

`networks`	Netzwerknamen und -adressen, die von `getnetent` verwendet werden.
`publickey`	Öffentliche und geheime Schlüssel für Secure_RPC, verwendet durch NFS and NIS+.
`passwd`	Benutzerpasswörter, die von `getpwent` verwendet werden. Weitere Informationen hierzu finden Sie auf der man-Seite `passwd(5)`.
`protocols`	Netzwerkprotokolle, die von `getprotoent` verwendet werden. Weitere Informationen hierzu finden Sie auf der man-Seite für `protocols(5)`.
`rpc`	Remote Procedure Call-Namen und -Adressen, die von `getrpcbyname` und ähnlichen Funktionen verwendet werden.
`services`	Netzwerkdienste, die von `getservent` verwendet werden.
`shadow`	Shadow-Passwörter der Benutzer, die von `getspnam` verwendet werden. Weitere Informationen hierzu finden Sie auf der man-Seite für `shadow(5)`.

TABELLE 16.4 KONFIGURATIONSOPTIONEN FÜR NSS-„DATENBANKEN“

`Dateien`	Direkter Dateizugriff, z. B. `/etc/aliases`
`db`	Zugriff über eine Datenbank
`nis`, `nisplus`	NIS, siehe auch *Buch „*Security Guide*“, Kapitel 3 „Using NIS“*
`dns`	Nur bei `hosts` und `networks` als Erweiterung verwendbar

`compat`	Nur bei `passwd`, `shadow` und `group` als Erweiterung verwendbar

16.5.2.14 `/etc/nscd.conf`

Mit dieser Datei wird nscd (Name Service Cache Daemon) konfiguriert. Weitere Informationen hierzu finden Sie auf den man-Seiten `nscd(8)` und `nscd.conf(5)`. Standardmäßig werden die Systemeinträge von `passwd`, `groups` und `hosts` von nscd gecacht. Dies ist für die Leistung von Verzeichnisdiensten wie NIS and LDAP wichtig, denn andernfalls muss für jeden Zugriff auf Namen, Gruppen oder Hosts die Netzwerkverbindung verwendet werden.

Wenn das Caching für `passwd` aktiviert wird, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Zum Verkürzen dieser Wartezeit starten Sie nscd wie folgt neu:

```
systemctl restart nscd
```

16.5.2.15 `/etc/HOSTNAME`

`/etc/HOSTNAME` enthält den vollständigen Hostnamen (FQHN). Der vollständige Hostname besteht aus dem eigentlichen Hostnamen und der Domäne. Die Datei darf nur eine einzige Zeile enthalten (in der der Hostname angegeben ist). Diese Angabe wird beim Booten des Rechners gelesen.

16.5.3 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`**.

Das Kommando **`ip`** ändert 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.

Anmerkung: **ifconfig** und **route** sind veraltet

Die Werkzeuge **ifconfig** und **route** sind veraltet. Verwenden Sie stattdessen **ip**. Bei **ifconfig** sind die Schnittstellennamen beispielsweise auf 9 Zeichen begrenzt.

16.5.3.1 Konfigurieren einer Netzwerkschnittstelle mit **ip**

ip ist ein Werkzeug zum Anzeigen und Konfigurieren von Netzwerkgeräten, Richtlinien-Routing und Tunneln.

ip ist ein sehr komplexes Werkzeug. Seine allgemeine Syntax ist **ip** *OPTIONS OBJECT COMMAND*. Sie können mit folgenden Objekten arbeiten:

Verbindung
: Dieses Objekt stellt ein Netzwerkgerät dar.

Adresse
: Dieses Objekt stellt die IP-Adresse des Geräts dar.

Nachbar
: Dieses Objekt stellt einen ARP- oder NDISC-Cache-Eintrag dar.

route
: Dieses Objekt stellt den Routing-Tabelleneintrag dar.

Regel
: Dieses Objekt stellt eine Regel in der Routing-Richtlinien-Datenbank dar.

maddress
: Dieses Objekt stellt eine Multicast-Adresse dar.

mroute
: Dieses Objekt stellt einen Multicast-Routing-Cache-Eintrag dar.

tunnel
: Dieses Objekt stellt einen Tunnel über IP dar.

Wird kein Kommando angegeben, wird das Standardkommando verwendet (normalerweise **list**).

Ändern Sie den Gerätestatus mit dem Befehl **ip link set** *DEVICE_NAME* . Wenn Sie beispielsweise das Gerät eth0 deaktivieren möchten, geben Sie **ip link set** `eth0 down ein`. Um es wieder zu aktivieren, verwenden Sie **ip link set** `eth0 up`.

Nach dem Aktivieren eines Geräts können Sie es konfigurieren. Verwenden Sie zum Festlegen der IP-Adresse **ip addr add** *IP_ADDRESS* `+ dev` *DEVICE_NAME*. Wenn Sie beispielsweise die Adresse der Schnittstelle eth0 mit dem standardmäßigen Broadcast (Option `brd`) auf 192.168.12.154/30 einstellen möchten, geben Sie **ip addr** `add 192.168.12.154/30 brd + dev eth0` ein.

Damit die Verbindung funktioniert, müssen Sie außerdem das Standard-Gateway konfigurieren. Geben Sie **ip route add** `gateway_ip_address` ein, wenn Sie ein Gateway für Ihr System festlegen möchten. Um eine IP-Adresse in eine andere Adresse zu übersetzen, verwenden Sie **nat**: **ip route add nat** `ip_address` **via** `other_ip_address`.

Zum Anzeigen aller Geräte verwenden Sie **ip link ls**. Wenn Sie nur die aktiven Schnittstellen abrufen möchten, verwenden Sie **ip link ls up**. Um Schnittstellenstatistiken für ein Gerät zu drucken, geben Sie **ip -s link ls** `device_name` ein. Um die Adressen Ihrer Geräte anzuzeigen, geben Sie **ip addr** ein. In der Ausgabe von **ip addr** finden Sie auch Informationen zu MAC-Adressen Ihrer Geräte. Wenn Sie alle Routen anzeigen möchten, wählen Sie **ip route show**.

Weitere Informationen zur Verwendung von **ip** erhalten Sie, indem Sie **ip** `help` eingeben oder die man-Seite `ip(8)` aufrufen. Die Option `help` ist zudem für alle **ip**-Unterkommandos 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`.

16.5.3.2 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-Datagram, an den Ziel-Host zu senden. Dabei wird eine sofortige Antwort angefordert. Wenn dies funktioniert, zeigt **ping** eine entsprechende Meldung an. Dies weist darauf hin, dass die Netzwerkverbindung ordnungsgemäß arbeitet.

ping testet nicht nur die Funktion der Verbindung zwischen zwei Computern, es bietet darüber hinaus grundlegende Informationen zur Qualität der Verbindung. In *Beispiel 16.11, „Ausgabe des ping-Befehls“* sehen Sie ein Beispiel der **ping**-Ausgabe. Die vorletzte Zeile enthält Informationen zur Anzahl der übertragenen Pakete, der verlorenen Pakete und der Gesamtlaufzeit von **ping**.

Als Ziel können Sie einen Hostnamen oder eine IP-Adresse verwenden, z. B. `ping example.com` oder `ping 192.168.3.100`. Das Programm sendet Pakete, bis Sie 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 example.com` ein.

BEISPIEL 16.11 AUSGABE DES PING-BEFEHLS

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (192.168.3.100): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

Das Standardintervall zwischen zwei Paketen beträgt eine Sekunde. Zum Ändern des Intervalls bietet das ping-Kommando die Option `-i`. Wenn beispielsweise das Ping-Intervall auf zehn Sekunden erhöht werden soll, geben Sie `ping -i 10 example.com` ein.

In einem System mit mehreren Netzwerkgeräten ist es manchmal nützlich, wenn der ping-Befehl über eine spezifische Schnittstellenadresse gesendet wird. Verwenden Sie hierfür die Option `--I` mit dem Namen des ausgewählten Geräts. Beispiel: `ping -I wlan1 example.com`.

Weitere Optionen und Informationen zur Verwendung von ping erhalten Sie, indem Sie `ping --h` eingeben oder die man-Seite `ping (8)` aufrufen.

Tipp: Ping-Ermittlung für IPv6-Adressen

Verwenden Sie für IPv6-Adressen das Kommando `ping6`. Hinweis: Zur Ping-Ermittlung für Link-Local-Adressen müssen Sie die Schnittstelle mit `-I` angeben. Das folgende Kommando funktioniert, wenn die Adresse über `eth1` erreichbar ist:

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

16.5.4 Unit-Dateien und Startskripte

Neben den beschriebenen Konfigurationsdateien gibt es noch systemd-Unit-Dateien und verschiedene Skripte, die beim Booten des Computers die Netzwerkdienste laden. Diese werden gestartet, wenn das System auf das Ziel `multi-user.target` umgestellt wird. Eine Beschreibung für einige Unit-Dateien und Skripte finden Sie unter *Einige Unit-Dateien und Startskripte für Netzwerkprogramme*. Weitere Informationen zu `systemd` finden Sie unter *Kapitel 13, Der Daemon* `systemd`; weitere Informationen zu den `systemd`-Zielen finden Sie auf der man-Seite zu `systemd.special` (**`man systemd.special`**).

EINIGE UNIT-DATEIEN UND STARTSKRIPTE FÜR NETZWERKPROGRAMME

`network.target`

`network.target` ist das systemd-Ziel für das Netzwerk, es ist jedoch abhängig von den Einstellungen, die der Systemadministrator angegeben hat.

Weitere Informationen finden Sie unter http://www.freedesktop.org/wiki/Software/systemd/NetworkTarget/.

`multi-user.target`

`multi-user.target` ist das systemd-Ziel für ein Mehrbenutzersystem mit allen erforderlichen Netzwerkdiensten.

`xinetd`

Startet xinetd. Mit xinetd können Sie Serverdienste auf dem System verfügbar machen. Beispielsweise kann er vsftpd starten, sobald eine FTP-Verbindung initiiert wird.

`rpcbind`

Startet das rpcbind-Dienstprogramm, das RPC-Programmnummern in universelle Adressen konvertiert. Es ist für RPC-Dienste wie NFS-Server erforderlich.

`ypserv`

Startet den NIS-Server.

`ypbind`

Startet den NIS-Client.

`/etc/init.d/nfsserver`

Startet den NFS-Server.

`/etc/init.d/postfix`

Steuert den postfix-Prozess.

16.6 Grundlegende Routereinrichtung

Ein Router ist ein Netzwerkgerät, das Daten hin und zurück an mehr als ein Netzwerk zustellt und von diesen empfängt (Netzwerkpakete). Ein Router wird häufig zum Verbinden Ihres lokalen Netzwerks mit dem Remote-Netzwerk (Internet) oder zum Verbinden lokaler Netzwerksegmente verwendet. Mit SUSE Linux Enterprise Server können Sie einen Router mit Funktionen wie Network Address Translation (NAT) oder erweiterten Firewalls erstellen.

Im Folgenden sind grundlegende Schritte beschrieben, mit denen Sie SUSE Linux Enterprise Server in einen Router umfunktionieren können.

1. Aktivieren Sie die Weiterleitung, beispielsweise in der Datei `/etc/sysctl.d/50-router.conf` aktivieren

   ```
   net.ipv4.conf.all.forwarding = 1
   net.ipv6.conf.all.forwarding = 1
   ```

   Stellen Sie dann ein statisches IPv4- und IPv6-IP-Setup für die Schnittstellen bereit. Durch das Aktivieren der Weiterleitung werden mehrere Mechanismen deaktiviert. Beispielsweise akzeptiert IPv6 keine IPv6-RAs (Router Advertisements) mehr, wodurch ebenfalls die Erstellung einer Standardroute vermieden wird.

2. In vielen Situationen, beispielsweise wenn Sie über mehr als eine Schnittstelle auf das gleiche Netzwerk zugreifen können oder wenn in der Regel VPN verwendet wird (und sich bereits auf „normalen Multihome-Hosts“ befindet), müssen Sie den Reverse-Path-Filter für IPv4 deaktivieren (diese Funktion ist derzeit für IPv6 nicht vorhanden):

   ```
   net.ipv4.conf.all.rp_filter = 0
   ```

   Stattdessen ist auch das Filtern mit Firewall-Einstellungen möglich.

3. Um ein IPv6-RA zu akzeptieren (vom Router auf eine externe, Uplink- oder ISP-Schnittstelle) und wieder eine IPv6-Standardroute (oder auch eine speziellere Route) zu erstellen, legen Sie Folgendes fest:

   ```
   net.ipv6.conf.${ifname}.accept_ra = 2
   net.ipv6.conf.${ifname}.autoconf = 0
   ```

   (Hinweis: „`eth0.42`“ muss in einem durch Punkte getrennten sysfs-Pfad als `eth0/42` angegeben werden.)

Weitere Beschreibungen zum Routerverhalten und zu Weiterleitungsabhängigkeiten sind unter https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt zu finden.

Um IPv6 auf Ihren internen (DMZ-)Schnittstellen bereitzustellen und den eigenen Router als IPv6-Router bekanntzugeben sowie „autoconf“ der Netzwerke für die Clients auszuführen, installieren und konfigurieren Sie `radvd` in der Datei `/etc/radvd.conf`. Beispiel:

```
interface eth0
{
    IgnoreIfMissing on;         # do not fail if interface missed

    AdvSendAdvert on;           # enable sending RAs
    AdvManagedFlag on;          # IPv6 addresses managed via DHCPv6
    AdvOtherConfigFlag on;      # DNS, NTP... only via DHCPv6

    AdvDefaultLifetime 3600;    # client default route lifetime of 1 hour

    prefix 2001:db8:0:1::/64    # (/64 is default and required for autoconf)
    {
        AdvAutonomous off;         # Disable address autoconf (DHCPv6 only)

        AdvValidLifetime 3600;     # prefix (autoconf addr) is valid 1 h
        AdvPreferredLifetime 1800; # prefix (autoconf addr) is prefered 1/2 h
    }
}
```

Konfigurieren Sie zuletzt die Firewall. In SuSEfirewall2 müssen Sie `FW_ROUTE="yes"` festlegen (sonst wird auch das Weiterleiten von sysctl wieder zurück gesetzt) und nach Bedarf die Schnittstellen in den Zonenvariablen `FW_DEV_INT`, `FW_DEV_EXT` (und `FW_DEV_DMZ`), vielleicht auch `FW_MASQUERADE="yes"` und `FW_MASQ_DEV` angeben.

16.7 Einrichten von Bonding-Geräten

Für bestimmte Systeme sind Netzwerkverbindungen erforderlich, die die normalen Anforderungen an die Datensicherheit oder Verfügbarkeit von typischen Ethernet-Geräten übertreffen. In diesen Fällen lassen sich mehrere Ethernet-Geräte zu einem einzigen Bonding-Gerät zusammenschließen.

Die Konfiguration des Bonding-Geräts erfolgt dabei über die Bonding-Moduloptionen. Das Verhalten ergibt sich im wesentlichen aus dem Modus des Bonding-Geräts. Standardmäßig gilt `active-backup`; wenn das aktive Slave-Gerät ausfällt, wird also ein anderes Slave-Gerät aktiviert. Die folgenden Bonding-Modi stehen zur Auswahl:

0 (balance-rr)

Die Pakete werden per Round-Robin von der ersten bis zur letzten verfügbaren Schnittstelle übertragen. Bietet Fehlertoleranz und Lastausgleich.

1 (active-backup)

Nur eine Netzwerkschnittstelle ist aktiv. Wenn diese Schnittstelle ausfällt, wird eine andere Schnittstelle aktiv. Dies ist die Standardeinstellung für SUSE Linux Enterprise Server. Bietet Fehlertoleranz.

2 (balance-xor)

Der Datenverkehr wird gemäß der folgenden Richtlinie auf alle verfügbaren Schnittstellen aufgeteilt: `[(Quell-MAC-Adresse mit XOR mit Ziel-MAC-Adresse XOR Pakettyp-ID) Modulo-Slave-Anzahl]` Erfordert Unterstützung durch den Switch. Bietet Fehlertoleranz und Lastausgleich.

3 (broadcast)

Der gesamte Datenverkehr wird per Broadcast an alle Schnittstellen übertragen. Erfordert Unterstützung durch den Switch. Bietet Fehlertoleranz.

4 (802.3ad)

Aggregiert mehrere Schnittstellen zu einer Gruppe, in der dieselben Geschwindigkeits- und Duplexeinstellungen gelten. Erfordert **`ethtool`**-Unterstützung durch die Schnittstellentreiber sowie einen Switch, der die dynamische Link-Aggregation nach IEEE 802.3ad unterstützt und entsprechend konfiguriert ist. Bietet Fehlertoleranz und Lastausgleich.

5 (balance-tlb)

Adaptiver Übertragungslastausgleich. Erfordert **`ethtool`**-Unterstützung durch die Schnittstellentreiber, jedoch keine Unterstützung durch den Switch. Bietet Fehlertoleranz und Lastausgleich.

6 (balance-alb)

Adaptiver Lastausgleich. Erfordert **`ethtool`**-Unterstützung durch die Schnittstellentreiber, jedoch keine Unterstützung durch den Switch. Bietet Fehlertoleranz und Lastausgleich.

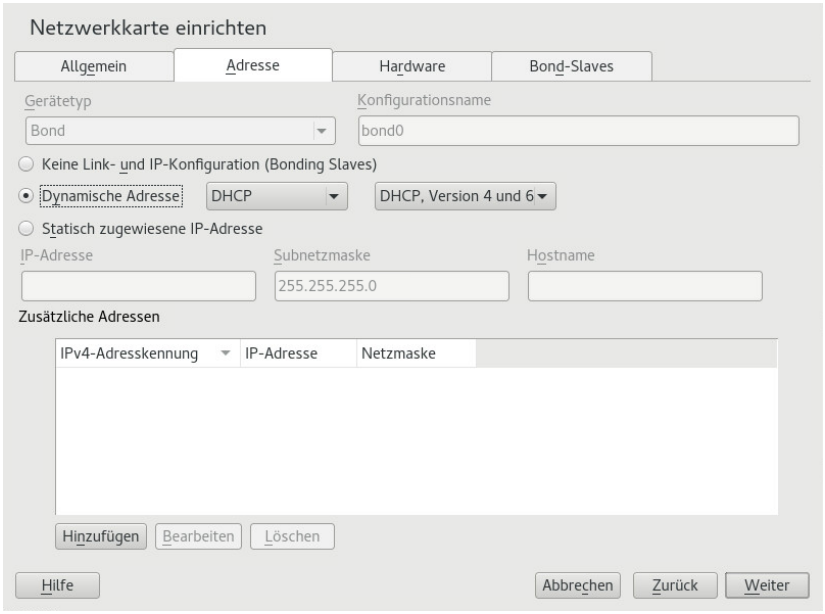
Eine ausführlichere Beschreibung der Modi finden Sie unter https://www.kernel.org/doc/Documentation/networking/bonding.txt.

Tipp: Bonding und Xen

Der Einsatz von Bonding-Geräten empfiehlt sich nur für Computer, in denen mehrere physische Netzwerkkarten eingebaut sind. Bei den meisten Konstellationen sollten Sie die Bonding-Konfiguration daher lediglich in Dom0 verwenden. Die Bond-Einrichtung in einem VM-Gast-System ist dabei nur dann sinnvoll, wenn dem VM-Gast mehrere Netzwerkkarten zugewiesen sind.

Zum Konfigurieren eines Bonding-Geräts gehen Sie wie folgt vor:

1. Führen Sie *YaST* › *System* › *Netzwerkeinstellungen* aus.
2. Wählen Sie *Hinzufügen* und ändern Sie die Einstellung unter *Gerätetyp* in *Bond*. Fahren Sie mit *Weiter* fort.



3. Geben Sie an, wie dem Bonding-Gerät eine IP-Adresse zugewiesen werden soll. Hierfür stehen drei Methoden zur Auswahl:

   - No IP Address (Keine IP-Adresse)
   - Dynamic Address (with DHCP or Zeroconf) (Dynamische Adresse (mit DHCP oder Zeroconf))
   - Statisch zugewiesene IP-Adresse

   Wählen Sie die passende Methode für Ihre Umgebung aus.

4. Wählen Sie auf dem Karteireiter *Bond-Slaves* die Ethernet-Geräte aus, die in den Bond aufgenommen werden sollen. Aktivieren Sie hierzu die entsprechenden Kontrollkästchen.

5. Bearbeiten Sie die *Bond-Treiberoptionen* und wählen Sie einen Bonding-Modus aus.

6. Der Parameter `miimon=100` muss unter *Bond-Treiberoptionen* angegeben werden. Ohne diesen Parameter wird die Datenintegrität nicht regelmäßig überprüft.

7. Klicken Sie auf *Weiter*, und beenden Sie YaST mit *OK*. Das Gerät wird erstellt.

16.7.1 Hot-Plugging von Bonding-Slaves

In bestimmten Netzwerkumgebungen (z. B. High Availability) muss eine Bonding-Slave-Schnittstelle durch eine andere Schnittstelle ersetzt werden. Dieser Fall tritt beispielsweise ein, wenn ein Netzwerkgerät wiederholt ausfällt. Die Lösung ist hier das Hot-Plugging der Bonding-Slaves.

Der Bond wird wie gewohnt konfiguriert (gemäß **`man 5 ifcfg-bonding`**), beispielsweise:

```
ifcfg-bond0
          STARTMODE='auto' # or 'onboot'
          BOOTPROTO='static'
          IPADDR='192.168.0.1/24'
          BONDING_MASTER='yes'
          BONDING_SLAVE_0='eth0'
          BONDING_SLAVE_1='eth1'
          BONDING_MODULE_OPTS='mode=active-backup miimon=100'
```

Die Slaves werden mit `STARTMODE=hotplug` und `BOOTPROTO=none` angegeben:

```
ifcfg-eth0
          STARTMODE='hotplug'
```

```
          BOOTPROTO='none'

ifcfg-eth1
          STARTMODE='hotplug'
          BOOTPROTO='none'
```

Bei `BOOTPROTO=none` werden die ethtool-Optionen herangezogen (sofern bereitgestellt), es wird jedoch kein Link zu **`ifup eth0 eingerichtet`**. Dies ist darin begründet, dass die Slave-Schnittstelle durch den Bond-Master gesteuert wird.

Bei `STARTMODE=hotplug` wird die Slave-Schnittstelle dem Bond automatisch zugefügt, wenn diese verfügbar ist.

Die `udev`-Regeln in `/etc/udev/rules.d/70-persistent-net.rules` müssen so angepasst werden, dass der Abgleich mit dem Gerät über die Bus-ID (das udev-Schlüsselwort `KERNELS` entspricht „SysFS BusID“, wie in **`hwinfo --netcard`** dargestellt) statt über die MAC-Adresse erfolgt. So ist es möglich, defekte Hardware auszutauschen (eine Netzwerkkarte in demselben Steckplatz, jedoch mit einer anderen MAC), und es treten keine Verwechselungen auf, wenn der Bond die MAC-Adresse aller Slaves ändert.

Beispiel:

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
KERNELS=="0000:00:19.0", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"
```

Beim Booten wartet der systemd-Service `network.service` nicht darauf, dass die Hot-Plug-Slaves einsatzbereit sind, sondern es wird die Bereitschaft des gesamten Bonds abgewartet, wofür mindestens ein verfügbarer Slave erforderlich ist. Wenn eine Slave-Schnittstelle aus dem System entfernt wird (durch Aufheben der Bindung an den NIC-Treiber, durch **`rmmod`** des NIC-Treibers oder durch normales PCI-Hot-Plug-Entfernen), so entfernt der Kernel die betreffende Schnittstelle automatisch aus dem Bond. Wird eine neue Karte in das System eingebaut (Austausch der Hardware im Steckplatz), benennt `udev` diese Karte anhand der Regel für busgestützte permanente Namen in den Namen des Slaves um und ruft **`ifup`** für die Karte auf. Mit dem **`ifup`**-Aufruf tritt die Karte automatisch in den Bond ein.

16.8 Einrichten von Team-Geräten für Netzwerk-Teaming

Der Begriff „Link-Aggregation“ ist der allgemeine Begriff zum Beschreiben der Kombination (oder Aggregation) einer Netzwerkverbindung zum Bereitstellen einer logischen Ebene. Manchmal stoßen Sie auf Begriffe wie „Channel-Teaming“, „Ethernet-Bonding“, „Port Truncating“ usw. Dies sind Synonyme des Begriffs und bezeichnen dasselbe Konzept.

Dieses Konzept ist allgemein bekannt als „Bonding“ und wurde ursprünglich in den Linux-Kernel integriert (Informationen zur ursprünglichen Implementierung finden Sie in *Abschnitt 16.7, „Einrichten von Bonding-Geräten“*). Der Begriff *Netzwerk-Teaming* wird zum Bezeichnen der neuen Implementierung dieses Konzepts verwendet.

Der Hauptunterschied zwischen Bonding und Netzwerk-Teaming ist der, dass das Teaming eine Reihe an kleinen Kernel-Modulen bereitstellt, die für die Bereitstellung einer Schnittstelle für die teamd-Instanzen verantwortlich sind. Alles andere wird im Userspace verarbeitet. Dies unterscheidet sich von der ursprünglichen Bondings-Implementierung, die alle ihre Funktionen ausschließlich im Kernel enthält. Einen Vergleich finden Sie unter *Tabelle 16.5, „Funktionsvergleich zwischen Bonding und Team“*.

TABELLE 16.5 FUNKTIONSVERGLEICH ZWISCHEN BONDING UND TEAM

Funktion	Bonding	Team
Broadcast, Round-Robin-TX-Richtlinie	Ja	Ja
Active-Backup-TX-Richtlinie	Ja	Ja
LACP-Unterstützung (802.3ad)	Ja	Ja
Hashbasierte TX-Richtlinie	Ja	Ja
Benutzer kann Hashfunktion festlegen	Nein	Ja
TX-Lastenausgleichsunterstützung	Ja	Ja
TX-Lastenausgleichsunterstützung für LACP	Nein	Ja

Funktion	Bonding	Team
Ethtool-Link-Überwachung	Ja	Ja
ARP-Link-Überwachung	Ja	Ja
NS/NA-Link-Überwachung (IPv6)	Nein	Ja
RCU-Sperre in TX-/RX-Pfaden	Nein	Ja
Portpriorität und Stickiness	Nein	Ja
Separate Einrichtung der Link-Überwachung nach Port	Nein	Ja
Einrichtung der Link-Überwachung für mehrere Ports	begrenzt	Ja
VLAN-Unterstützung	Ja	Ja
Stapeln mehrerer Geräte	Ja	Ja

Quelle: http://libteam.org/files/teamdev.pp.pdf

Beide Implementierungen, Bonding und Netzwerk-Teaming, können parallel verwendet werden. Netzwerk-Teaming ist eine Alternative zur bestehenden Bondings-Implementierung. Es ersetzt das Bonding nicht.

Netzwerk-Teaming kann für verschiedene Anwendungsfälle verwendet werden. Die beiden wichtigsten Anwendungsfälle werden später erläutert und umfassen:

- Lastausgleich zwischen Netzwerkgeräten.
- Failover von einem Netzwerkgerät zu einem anderen, falls eines der Geräte einen Fehler aufweist.

Zurzeit ist kein YaST-Modul vorhanden, dass das Erstellen eines Teaming-Geräts unterstützt. Sie müssen Netzwerk-Teaming manuell konfigurieren. Das allgemeine Verfahren ist unten dargestellt und kann auf alle Netzwerk-Teaming-Konfigurationen angewendet werden:

PROZEDUR 16.1 ALLGEMEINES VERFAHREN

1. Stellen Sie sicher, dass alle erforderlichen Pakete installiert sind. Installieren Sie die Pakete `libteam-tools`, `libteamdctl0` und `python-libteam`.

2. Erstellen Sie eine Konfigurationsdatei unter `/etc/sysconfig/network/`. In der Regel ist dies `ifcfg-team0`. Benötigen Sie mehr als ein Netzwerk-Teaming-Gerät, teilen Sie ihnen aufsteigende Nummern zu.
   Diese Konfigurationsdatei enthält mehrere Variablen, die auf den man-Seiten erläutert werden (siehe **`man ifcfg`** und **`man ifcfg-team`**). Eine Beispielkonfiguration finden Sie im System in der Datei `/etc/sysconfig/network/ifcfg.template`.

3. Entfernen Sie die Konfigurationsdatei der Schnittstellen, die für das Teaming-Gerät verwendet werden (in der Regel `ifcfg-eth0` und `ifcfg-eth1`).
   Es wird empfohlen, eine Sicherung zu erstellen und beide Dateien zu löschen. Wicked legt die Konfigurationsdateien mit den erforderlichen Parametern für Teaming neu an.

4. Optional können Sie überprüfen, ob alle Angeben in der Konfigurationsdatei von Wicked enthalten sind:

   ```
   wicked show-config
   ```

5. Starten Sie das Netzwerk-Teaming-Gerät `team0`:

   ```
   wicked ifup all team0
   ```

   Falls Sie zusätzliche Informationen zur Fehlersuche benötigen, verwenden Sie die Option `--debug all` nach dem Subkommando **`all`**.

6. Überprüfen Sie den Status des Netzwerk-Teaming-Geräts. Führen Sie hierzu die folgenden Kommandos aus:

   - Status der teamd-Instanz von Wicked abrufen:

     ```
     wicked ifstatus --verbose team0
     ```

   - Status der gesamten Instanz abrufen:

     ```
     teamdctl team0 state
     ```

   - systemd-Status der teamd-Instanz abrufen:

     ```
     systemctl status teamd@team0
     ```

   Jedes Kommando zeigt eine etwas andere Ansicht abhängig von Ihren Anforderungen an.

7. Falls Sie nachträglich Änderungen in der Datei `ifcfg-team0` vornehmen müssen, laden Sie die Konfiguration der Datei mit folgendem Kommando neu:

   ```
   wicked ifreload team0
   ```

Verwenden Sie *nicht* **`systemctl`** zum Starten oder Stoppen des Teaming-Geräts! Verwenden Sie stattdessen das Kommando **`wicked`**, wie oben gezeigt.

So entfernen Sie das Teaming-Gerät vollständig:

PROZEDUR 16.2 ENTFERNEN EINES TEAMGERÄTS

1. Halten Sie das Netzwerk-Teaming-Gerät `team0` an:

   ```
   wicked ifdown team0
   ```

2. Benennen Sie die Datei `/etc/sysconfig/network/ifcfg-team0` in `/etc/sysconfig/network/.ifcfg-team0` um. Wenn ein Punkt vor dem Dateinamen steht, ist er für Wicked „unsichtbar“. Falls Sie die Konfiguration tatsächlich nicht mehr benötigen, können Sie die Datei auch entfernen.

3. Laden Sie die Konfiguration neu:

   ```
   wicked ifreload all
   ```

16.8.1 Anwendungsfall: Lastenausgleich mit Netzwerk-Teaming

Der Lastenausgleich wird zum Verbessern der Bandbreite verwendet. Verwenden Sie die folgende Konfigurationsdatei zum Erstellen eines Netzwerk-Teaming-Geräts mit Funktionen für den Lastenausgleich. Fahren Sie mit *Prozedur 16.1, „Allgemeines Verfahren“* fort, um das Gerät einzurichten. Überprüfen Sie die Ausgabe mit **`teamdctl`**.

BEISPIEL 16.12 KONFIGURATION FÜR LASTENAUSGLEICH MIT NETZWERK-TEAMING

```
STARTMODE=auto ❶
BOOTPROTO=static ❷
IPADDRESS="192.168.1.1/24" ❷
IPADDR6="fd00:deca:fbad:50::1/64" ❷

TEAM_RUNNER="loadbalance" ❸
TEAM_LB_TX_HASH="ipv4,ipv6,eth,vlan"
TEAM_LB_TX_BALANCER_NAME="basic"
TEAM_LB_TX_BALANCER_INTERVAL="100"

TEAM_PORT_DEVICE_0="eth0" ❹
TEAM_PORT_DEVICE_1="eth1" ❹

TEAM_LW_NAME="ethtool" ❺
TEAM_LW_ETHTOOL_DELAY_UP="10" ❻
TEAM_LW_ETHTOOL_DELAY_DOWN="10" ❻
```

❶ Steuert das Starten des Teaming-Geräts. Der Wert `auto` bedeutet, dass die Schnittstelle eingerichtet wird, wenn der Netzwerkdienst verfügbar ist, und bei jedem Reboot automatisch gestartet wird.
Falls Sie das Gerät selbst steuern müssen (und das automatische Starten vermeiden möchten) legen Sie für `STARTMODE` den Wert `manual` fest.

❷ Legt eine statische IP-Adresse fest (hier `192.168.1.1` für IPv4 und `fd00:deca:fbad:50::1` für IPv6).
Wenn das Netzwerk-Teaming-Gerät eine dynamische IP-Adresse verwenden soll, legen Sie `BOOTPROTO="dhcp"` fest und entfernen (oder kommentieren) Sie die Zeile mit `IPADDRESS` und `IPADDR6`.

❸ Legt für `TEAM_RUNNER` den Wert `loadbalance` fest, um den Modus für den Lastenausgleich zu aktivieren.

❹ Gibt ein oder mehrere Geräte an, die aggregiert werden sollen, um das Netzwerk-Teaming-Gerät zu bilden.

❺ Definiert eine Verbindungsüberwachung, die den Status der untergeordneten Geräte überwacht. Mit dem Standardwert `ethtool` wird nur überprüft, ob das Gerät aktiv und erreichbar ist. Hierdurch erfolgt die Überprüfung recht schnell. Jedoch wird nicht überprüft, ob das Gerät wirklich Pakete senden und empfangen kann.
Wenn Sie wirklich sicher sein müssen, dass die Verbindung einwandfrei funktioniert, verwenden Sie die Option `arp_ping`. Damit werden Ping-Kommandos an einen beliebigen Host geschickt (dies ist in der Variable `TEAM_LW_ARP_PING_TARGET_HOST` konfiguriert). Nur, wenn die Antworten empfangen werden, wird das Netzwerk-Teaming-Gerät als aktiv betrachtet.

❻ Definiert die Verzögerung in Millisekunden zwischen dem Verbindungsaufbau (oder -abbau) und der Benachrichtigung des Runner.

16.8.2 Anwendungsfall: Failover mit Netzwerk-Teaming

Failover wird verwendet, um eine hohe Verfügbarkeit kritischer Netzwerk-Teaming-Geräte sicherzustellen, indem ein paralleles Sicherungsnetzwerkgerät verwendet wird. Das Sicherungsnetzwerkgerät ist ständig aktiv und übernimmt die Funktionen, wenn das Hauptgerät ausfällt.

Verwenden Sie die folgende Konfigurationsdatei zum Erstellen eines Netzwerk-Teaming-Geräts mit Failover-Funktionen. Fahren Sie mit *Prozedur 16.1, „Allgemeines Verfahren“* fort, um das Gerät einzurichten. Überprüfen Sie die Ausgabe mit **`teamdctl`**.

BEISPIEL 16.13 KONFIGURATION FÜR DHCP-NETZWERK-TEAMING-GERÄT

```
STARTMODE=auto ❶
BOOTPROTO=static ❷
IPADDR="192.168.1.2/24" ❷
IPADDR6="fd00:deca:fbad:50::2/64" ❷

TEAM_RUNNER=activebackup ❸
TEAM_PORT_DEVICE_0="eth0" ❹
TEAM_PORT_DEVICE_1="eth1" ❹

TEAM_LW_NAME=ethtool ❺
TEAM_LW_ETHTOOL_DELAY_UP="10" ❻
TEAM_LW_ETHTOOL_DELAY_DOWN="10" ❻
```

❶ Steuert das Starten des Teaming-Geräts. Der Wert `auto` bedeutet, dass die Schnittstelle eingerichtet wird, wenn der Netzwerkdienst verfügbar ist, und bei jedem Reboot automatisch gestartet wird.

Falls Sie das Gerät selbst steuern müssen (und das automatische Starten vermeiden möchten) legen Sie für `STARTMODE` den Wert `manual` fest.

2. Legt eine statische IP-Adresse fest (hier `192.168.1.2` für IPv4 und `fd00:deca:fbad:50::2` für IPv6).
   Wenn das Netzwerk-Teaming-Gerät eine dynamische IP-Adresse verwenden soll, legen Sie `BOOTPROTO="dhcp"` fest und entfernen (oder kommentieren) Sie die Zeile mit `IPADDRESS` und `IPADDR6`.
3. Legt für `TEAM_RUNNER` den Wert `activebackup` fest, um den Failover-Modus zu aktivieren.
4. Gibt ein oder mehrere Geräte an, die aggregiert werden sollen, um das Netzwerk-Teaming-Gerät zu bilden.
5. Definiert eine Verbindungsüberwachung, die den Status der untergeordneten Geräte überwacht. Mit dem Standardwert `ethtool` wird nur überprüft, ob das Gerät aktiv und erreichbar ist. Hierdurch erfolgt die Überprüfung recht schnell. Jedoch wird nicht überprüft, ob das Gerät wirklich Pakete senden und empfangen kann.
   Wenn Sie wirklich sicher sein müssen, dass die Verbindung einwandfrei funktioniert, verwenden Sie die Option `arp_ping`. Damit werden Ping-Kommandos an einen beliebigen Host geschickt (dies ist in der Variable `TEAM_LW_ARP_PING_TARGET_HOST` konfiguriert). Nur, wenn die Antworten empfangen werden, wird das Netzwerk-Teaming-Gerät als aktiv betrachtet.
6. Definiert die Verzögerung in Millisekunden zwischen dem Verbindungsaufbau (oder -abbau) und der Benachrichtigung des Runner.

16.8.3 Anwendungsfall: VLAN gegenüber Teamgerät

VLAN ist eine Abkürzung für *Virtual Local Area Network* (virtuelles lokales Netzwerk). Es ermöglicht die Ausführung mehrerer *logischer* (virtueller) Ethernets über ein einzelnes physisches Ethernet. Es teilt das Netzwerk in verschiedene Broadcast-Domänen auf, sodass Pakete nur zwischen den Ports, die für dasselbe VLAN bestimmt sind, umgeschaltet werden müssen.

Im nachfolgenden Anwendungsfall werden zwei statische VLANs oberhalb eines Teamgeräts angelegt:

- `vlan0`, an die IP-Adresse `192.168.10.1` gebunden
- `vlan1`, an die IP-Adresse `192.168.20.1` gebunden

Führen Sie dazu die folgenden Schritte aus:

1. Aktivieren Sie die VLAN-Tags am Switch. Soll der Lastenausgleich für das Teamgerät erfolgen, muss der Switch das *LACP* (Link Aggregation Control Protocol, 802.3ad) unterstützen. Weitere Informationen finden Sie im Hardware-Handbuch.

2. Legen Sie fest, ob ein Lastenausgleich oder ein Failover für das Teamgerät verwendet werden soll. Richten Sie das Teamgerät gemäß den Anweisungen unter *Abschnitt 16.8.1, „Anwendungsfall: Lastenausgleich mit Netzwerk-Teaming“* oder *Abschnitt 16.8.2, „Anwendungsfall: Failover mit Netzwerk-Teaming“* ein.

3. Erstellen Sie unter `/etc/sysconfig/network` die Datei `ifcfg-vlan0` mit folgendem Inhalt:

```
STARTMODE="auto"
BOOTPROTO="static" ❶
IPADDR='192.168.10.1/24' ❷
ETHERDEVICE="team0" ❸
VLAN_ID="0" ❹
VLAN='yes'
```

   ❶ Definiert eine feste IP-Adresse, angegeben in `IPADDR`.

   ❷ Definiert die IP-Adresse, hier mit der Netzmaske.

   ❸ Enthält die eigentliche Schnittstelle für die VLAN-Schnittstelle, hier das Teamgerät (`team0`).

   ❹ Gibt eine eindeutige ID für das VLAN an. Nach Möglichkeit sollten der Dateiname und die `VLAN_ID` dem Namen `ifcfg-vlan`*`VLAN_ID`* entsprechen. In diesem Fall ist die `VLAN_ID` gleich `0`, sodass sich der Dateiname `ifcfg-vlan0` ergibt.

4. Kopieren Sie die Datei `/etc/sysconfig/network/ifcfg-vlan0` in `/etc/sysconfig/network/ifcfg-vlan1` und ändern Sie die folgenden Werte:

   - `IPADDR` von `192.168.10.1/24` in `192.168.20.1/24`.
   - `VLAN_ID` von `0` in `1`.

5. Starten Sie die beiden VLANs:

```
root # wicked ifup vlan0 vlan1
```

6. Prüfen Sie die Ausgabe von **`ifconfig`**:

```
root # ifconfig -a
[...]
vlan0     Link encap:Ethernet  HWaddr 08:00:27:DC:43:98
          inet addr:192.168.10.1 Bcast:192.168.10.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedc:4398/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:816 (816.0 b)

vlan1     Link encap:Ethernet  HWaddr 08:00:27:DC:43:98
          inet addr:192.168.20.1 Bcast:192.168.20.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedc:4398/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:816 (816.0 b)
```

16.9 Softwaredefiniertes Networking mit Open vSwitch

Softwaredefiniertes Networking (SDN) bedeutet eine Trennung des Systems, das steuert, wohin der Datenverkehrs gesendet wird (die *Steuerebene*), vom zugrunde liegenden System, das den Datenverkehr zum ausgewählten Ziel weiterleitet (die *Datenebene*, auch *Weiterleitungsebene* genannt). Dies bedeutet, dass die Funktionen, die zuvor von einem einzelnen, in der Regel nicht flexiblen, Switch erbracht wurden, jetzt zwischen einem Switch (Datenebene) und seinem Controller (Steuerebene) aufgeteilt werden können. In diesem Modell ist der Controller programmierbar und funktioniert sehr flexibel und passt sich schnell an sich ändernde Netzwerkbedingungen an.

Open vSwitch ist eine Software, die einen verteilten Switch mit mehreren Ebenen implementiert, der mit dem OpenFlow-Protokoll kompatibel ist. OpenFlow erlaubt es einer Controller-Anwendung, die Konfiguration eines Switch zu bearbeiten. OpenFlow baut als Ebene auf dem TCP-Protokoll auf und wird in einer Reihe von Hardware und Software implementiert. Ein einzelner Controller kann daher mehrere, sehr unterschiedliche Switches unterstützen.

16.9.1 Vorteile von Open vSwitch

Softwaredefiniertes Networking mit Open vSwitch bietet einige Vorteile, vor allem wenn es gemeinsam mit virtuellen Computern verwendet wird:

- Networking-Zustände können einfach identifiziert werden.
- Netzwerke und ihre Live-Zustände können von einem Host auf einen anderen übertragen werden.
- Netzwerkdynamiken sind nachverfolgbar und externe Software kann dafür konfiguriert werden, auf diese zu antworten.
- Sie können Tags in Netzwerkpaketen anwenden und so einstellen, dass sie identifizieren, von welchem bzw. an welchen Computer sie gesendet werden, und andere Netzwerkkontexte verwalten. Zuweisungsregeln für Tags können konfiguriert und migriert werden.
- Open vSwitch implementiert das GRE-Protokoll (*Generic Routing Encapsulation*). Dies erlaubt es Ihnen beispielsweise, private Netzwerke virtueller Computer miteinander zu verbinden.
- Open vSwitch kann eigenständig verwendet werden, ist jedoch für die Integration mit Networking-Hardware konzipiert und kann Hardware-Switches steuern.

16.9.2 Installieren von Open vSwitch

1. Installieren Sie Open vSwitch und ergänzende Pakete:

   ```
   root # zypper install openvswitch openvswitch-switch
   ```

   Wenn Sie Open vSwitch zusammen mit dem KVM-Hypervisor verwenden möchten, installieren Sie zusätzlich `tunctl` . Wenn Sie Open vSwitch zusammen mit dem Xen-Hypervisor verwenden möchten, installieren Sie zusätzlich `openvswitch-kmp-xen` .

2. Aktivieren Sie den Open vSwitch-Dienst:

   ```
   root # systemctl enable openvswitch
   ```

3. Starten Sie entweder den Computer neu oder verwenden Sie **`systemctl`**, um den Open vSwitch-Dienst sofort zu starten:

   ```
   root # systemctl start openvswitch
   ```

4. Um zu überprüfen, ob Open vSwitch richtig aktiviert wurde, verwenden Sie das Kommando:

```
root # systemctl status openvswitch
```

16.9.3 Überblick über Open vSwitch-Daemons und -Dienstprogramme

Open vSwitch besteht aus mehreren Komponenten. Hierzu gehören ein Kernel-Modul und verschiedenste Userspace-Komponenten. Das Kernel-Modul wird zur Beschleunigung des Datenpfads verwendet, ist für eine Minimalinstallation von Open vSwitch jedoch nicht erforderlich.

16.9.3.1 Daemons

Die zentralen ausführbaren Dateien von Open vSwitch sind die zugehörigen zwei Daemons. Wenn Sie den `openvswitch`-Dienst starten, starten Sie die Daemons indirekt.

Der Haupt-Daemon (**`ovs-vswitchd`**) von Open vSwitch stellt die Implementierung eines Switch bereit. Der Datenbank-Daemon (**`ovsdb-server`**) von Open vSwitch dient der Datenbank, in der die Konfiguration und der Zustand von Open vSwitch gespeichert werden.

16.9.3.2 Dienstprogramme

Open vSwitch wird außerdem mit mehreren Dienstprogrammen bereitgestellt, die die Arbeit damit vereinfachen. Die folgende Liste ist nicht vollständig, es werden nur die wichtigsten Kommandos beschrieben.

`ovsdb-tool`

Open vSwitch-Datenbanken erstellen, aufrüsten, komprimieren und abfragen. Transaktionen auf Open vSwitch-Datenbanken durchführen.

`ovs-appctl`

Einen aktiven **`ovs-vswitchd`**- oder **`ovsdb-server`**-Daemon konfigurieren.

`ovs-dpctl`, **`ovs-dpctl-top`**

Datenpfade erstellen, bearbeiten, visualisieren und löschen. Die Verwendung dieses Werkzeugs kann zu einem Konflikt mit **`ovs-vswitchd`** führen, wenn dieser auch Datenpfade verwaltet. Daher wird es oft nur zu Diagnostikzwecken verwendet.

ovs-dpctl-top erstellt eine Visualisierung ähnlich wie **top** - für Datenpfade.

ovs-ofctl

Alle Switches verwalten, die dem OpenFlow-Protokoll unterliegen. **ovs-ofctl** ist nicht auf die Interaktion mit Open vSwitch beschränkt.

ovs-vsctl

Bietet eine Schnittstelle auf höchster Ebene für die Konfigurationsdatenbank. Sie kann zum Abfragen und Bearbeiten der Datenbank verwendet werden. Konkret zeigt sie den Zustand von **ovs-vswitchd** und kann zur Konfiguration verwendet werden.

16.9.4 Erstellen einer Bridge mit Open vSwitch

In der folgenden Beispielkonfiguration wird der Wicked-Netzwerkdienst standardmäßig auf SUSE Linux Enterprise Server verwendet. Weitere Informationen zu Wicked finden Sie unter *Abschnitt 16.5, „Manuelle Netzwerkkonfiguration“*.

Wenn Sie Open vSwitch installiert und gestartet haben, gehen Sie wie folgt vor:

1. Um eine Bridge zur Verwendung durch Ihren virtuellen Computer zu konfigurieren, erstellen Sie eine Datei mit folgendem Inhalt:

```
STARTMODE='auto' ❶
BOOTPROTO='dhcp' ❷
OVS_BRIDGE='yes' ❸
OVS_BRIDGE_PORT_DEVICE_1='eth0' ❹
```

❶ Richten Sie die Bridge automatisch ein, wenn der Netzwerkdienst gestartet wird.

❷ Das zu verwendende Protokoll für die Konfiguration der IP-Adresse.

❸ Kennzeichnen Sie die Konfiguration als Open vSwitch-Bridge.

❹ Wählen Sie aus, welche(s) Gerät(e) zur Bridge hinzugefügt werden soll(en). Um mehr Geräte hinzuzufügen, fügen Sie zusätzliche Zeilen für jedes der Geräte in der Datei hinzu:

```
OVS_BRIDGE_PORT_DEVICE_SUFFIX='DEVICE'
```

Das *SUFFIX* kann eine beliebige alphanummerische Zeichenfolge darstellen. Stellen Sie jedoch sicher, dass das *SUFFIX* für jedes Gerät eindeutig ist, um das Überschreiben einer vorherigen Definition zu vermeiden.

Speichern Sie die Datei im Verzeichnis `/etc/sysconfig/network` mit dem Namen `ifcfg-br0`. Anstelle von *`br0`* können Sie jeden beliebigen Namen verwenden. Jedoch muss der Dateiname mit `ifcfg-` beginnen.
Informationen zu weiteren Optionen finden Sie auf den man-Seiten von `ifcfg` (**`man 5 ifcfg`**) und `ifcfg-ovs-bridge` (**`man 5 ifcfg-ovs-bridge`**).

2. Starten Sie nun die Bridge:

```
root # wicked ifup br0
```

Wenn Wicked fertig ist, sollte es den Namen der Bridge und daneben den Zustand `up` ausgeben.

16.9.5 Verwenden von Open vSwitch direkt mit KVM

Nach dem Erstellen der Bridge (wie in *Abschnitt 16.9.4, „Erstellen einer Bridge mit Open vSwitch“* beschrieben) können Sie Open vSwitch zum Verwalten des Netzwerkzugriffs auf virtuelle Computer verwenden, die mit KVM/QEMU erstellt wurden.

1. Um die Möglichkeiten von Wicked am besten nutzen zu können, führen Sie weitere Änderungen an der zuvor konfigurierten Bridge durch. Öffnen Sie die zuvor erstellte Datei `/etc/sysconfig/network/ifcfg-br0` und fügen Sie eine Zeile für ein weiteres Port-Gerät hinzu:

```
OVS_BRIDGE_PORT_DEVICE_2='tap0'
```

Legen Sie zusätzlich für `BOOTPROTO` den Wert `none` fest. Die Datei sollte nun wie folgt aussehen:

```
STARTMODE='auto'
BOOTPROTO='none'
OVS_BRIDGE='yes'
OVS_BRIDGE_PORT_DEVICE_1='eth0'
OVS_BRIDGE_PORT_DEVICE_2='tap0'
```

Das neue Port-Gerät *`tap0`* wird im nächsten Schritt konfiguriert.

2. Fügen Sie nun eine Konfigurationsdatei für das Gerät *`tap0`* hinzu:

```
STARTMODE='auto'
BOOTPROTO='none'
```

```
TUNNEL='tap'
```

Speichern Sie die Datei im Verzeichnis `/etc/sysconfig/network` mit dem Namen `ifcfg-tap0`.

Tipp: Anderen Benutzern den Zugriff auf das Tap-Gerät erlauben

Um dieses Tap-Gerät über einen virtuellen Computer verwenden zu können, der als Benutzer ohne `root`-Berechtigungen gestartet wurde, fügen Sie Folgendes hinzu:

```
TUNNEL_SET_OWNER=USER_NAME
```

Um den Zugriff für eine ganze Gruppe zu erlauben, fügen Sie Folgendes hinzu:

```
TUNNEL_SET_GROUP=GROUP_NAME
```

3. Öffnen Sie schließlich die Konfiguration für das Gerät, das als das erste `OVS_BRIDGE_PORT_DEVICE`-Gerät definiert ist. Wenn Sie den Namen nicht geändert haben, sollte dies `eth0` sein. Öffnen Sie daher `/etc/sysconfig/network/ifcfg-eth0` und stellen Sie sicher, dass die folgenden Optionen festgelegt sind:

```
STARTMODE='auto'
BOOTPROTO='none'
```

Wenn die Datei noch nicht vorhanden ist, erstellen Sie sie.

4. Starten Sie die Bridge-Schnittstelle mithilfe von Wicked neu:

```
root # wicked ifreload br0
```

Dies löst auch das erneute Laden der neu definierten Bridge-Port-Geräte aus.

5. Verwenden Sie zum Starten eines virtuellen Computers beispielsweise:

```
root # qemu-kvm \
-drive file=/PATH/TO/DISK-IMAGE (1) \
-m 512 -net nic,vlan=0,macaddr=00:11:22:EE:EE:EE \
-net tap,ifname=tap0,script=no,downscript=no (2)
```

(1) Pfad zum QEMU-Laufwerksabbild, das Sie starten möchten.

2 Verwenden Sie das zuvor erstellte Tap-Gerät (`tap0`).

Weitere Informationen zur Verwendung von KVM/QEMU finden Sie im *Buch „Virtualization Guide"*.

16.9.6 Verwenden von Open vSwitch mit `libvirt`

Nach Erstellen der Bridge, wie zuvor in *Abschnitt 16.9.4, „Erstellen einer Bridge mit Open vSwitch"* beschrieben, können Sie die Bridge zu einem vorhandenen virtuellen Computer hinzufügen, der mit `libvirt` verwaltet wird. Da `libvirt` Open vSwitch-Bridges bereits teilweise unterstützt, können Sie die in *Abschnitt 16.9.4, „Erstellen einer Bridge mit Open vSwitch"* erstellte Bridge ohne weitere Änderungen an der Networking-Konfiguration verwenden.

1. Öffnen Sie die Domänen-XML-Datei für den gewünschten virtuellen Computer:

```
root # virsh edit VM_NAME
```

   Ersetzen Sie *`VM-NAME`* durch den Namen des gewünschten virtuellen Computers. Hiermit wird Ihr Standardtexteditor geöffnet.

2. Suchen Sie nach einem Abschnitt, der mit `<interface type="...">` beginnt und mit `</interface>` endet, um den Networking-Abschnitt des Dokuments zu finden.
   Ersetzen Sie den vorhandenen Abschnitt durch einen Networking-Abschnitt, der etwa so aussieht:

```
<interface type='bridge'>
  <source bridge='br0'/>
  <virtualport type='openvswitch'/>
</interface>
```

   Wichtig: Kompatibilität von `virsh iface-*` und Virtual Machine Manager mit Open vSwitch

   Zurzeit wird die Open vSwitch-Kompatibilität von `libvirt` nicht über die **`virsh iface-*`**-Werkzeuge und Virtual Machine Manager verfügbar gemacht. Wenn Sie eines dieser Werkzeuge verwenden, kann die Konfiguration beschädigt werden.

3. Sie können die virtuellen Computer nun wie üblich starten oder neu starten.

Weitere Informationen zur Verwendung von `libvirt` finden Sie im *Buch „Virtualization Guide"*.

16.9.7 Weitere Informationen

http://openvswitch.org/support/

Dokumentationsabschnitt der Open vSwitch-Projekt-Website

https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

Whitepaper der Open Networking Foundation zum softwaredefinierten Networking und zum OpenFlow-Protokoll

17 Druckerbetrieb

SUSE® Linux Enterprise Server unterstützt zahlreiche Druckermodelle (auch entfernte Netzwerkdrucker). Drucker können manuell oder mit YaST konfiguriert werden. Anleitungen zur Konfiguration finden Sie unter *Buch „Bereitstellungshandbuch", Kapitel 11 „Einrichten von Hardware-Komponenten mit YaST", Abschnitt 11.3 „Einrichten eines Druckers"*. Grafische Dienstprogramme und Dienstprogramme an der Kommandozeile sind verfügbar, um Druckaufträge zu starten und zu verwalten. Wenn Ihr Drucker nicht wie erwartet verwendet werden kann, lesen Sie die Informationen unter *Abschnitt 17.8, „Fehlersuche"*.

Das Standarddrucksystem in SUSE Linux Enterprise Server ist CUPS (Common Unix Printing System).

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 (USB, Ethernet oder WLAN) 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. Wenn PostScript-Dokumente direkt vom Drucker verarbeitet und im Drucksystem nicht in weiteren Phasen konvertiert werden müssen, reduziert sich die Anzahl der möglichen Fehlerquellen.

Derzeit wird PostScript von PDF als Standardformat für Druckaufträge abgelöst. PostScript + PDF-Drucker, die PDF-Dateien (neben PostScript-Dateien) direkt drucken können, sind bereits am Markt erhältlich. Bei herkömmlichen PostScript-Druckern müssen PDF-Dateien während des Druck-Workflows in PostScript konvertiert werden.

Standarddrucker (Sprachen wie PCL und ESC/P)

Bei den bekannten Druckersprachen kann das Drucksystem PostScript-Druckaufträge mit 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 adäquates Druckergebnis. Linux ist unter Umständen nicht in der

Lage, einige spezielle Druckerfunktionen anzusprechen. Mit Ausnahme von HP und Epson gibt es derzeit keinen Druckerhersteller, der Linux-Treiber entwickeln und sie den Linux-Distributoren unter einer Open-Source-Lizenz zur Verfügung stellen würde.

Proprietäre Drucker (auch GDI-Drucker genannt)

Diese Drucker unterstützen keine der gängigen Druckersprachen. Sie verwenden eigene, undokumentierte Druckersprachen, die geändert werden können, wenn neue Versionen eines Modells auf den Markt gebracht werden. Für diese Drucker sind in der Regel nur Windows-Treiber verfügbar. Weitere Informationen finden Sie unter *Abschnitt 17.8.1, „Drucker ohne Unterstützung für eine Standard-Druckersprache“*.

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.linuxfoundation.org/OpenPrinting/

Die OpenPrinting-Homepage mit der Druckerdatenbank. In der Online-Datenbank wird 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 Server-Version nicht aufgewiesen hat. Die Datenbank gibt daher nicht notwendigerweise den richtigen Status, sondern nur eine Annäherung an diesen an.

http://pages.cs.wisc.edu/~ghost/

Die Ghostscript-Website

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

Liste inbegriffener Ghostscript-Treiber.

17.1 Der CUPS-Workflow

Der Benutzer erstellt einen Druckauftrag. Der Druckauftrag besteht aus den zu druckenden Daten plus Informationen für den Spooler. Hierzu gehören der Name des Druckers oder der Druckerwarteschlange sowie (optional) Angaben für den Filter, z. B. druckerspezifische Optionen.

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

Der Filter konvertiert die von der druckenden Anwendung generierten Daten (in der Regel PostScript oder PDF, aber auch ASCII, JPEG usw.) in druckerspezifische Daten (PostScript, PCL, ESC/P usw.). Die Funktionen des Druckers sind in den PPD-Dateien beschrieben. Eine PPD-Datei enthält druckspezifische 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 in druckerspezifische Daten. Hierzu ist ein für den Drucker geeigneter Druckertreiber erforderlich. Das Back-End empfängt die druckerspezifischen Daten vom Filter und leitet sie an den Drucker weiter.

17.2 Methoden und Protokolle zum Anschließen von Druckern

Es gibt mehrere Möglichkeiten, einen Drucker an das System anzuschließen. Die Konfiguration von CUPS unterscheidet nicht zwischen einem lokalen Drucker und einem Drucker, der über das Netzwerk an das System angeschlossen ist. Weitere Informationen zum Anschließen von Druckern finden Sie im Beitrag *CUPS in aller Kürze* unter http://en.opensuse.org/SDB:CUPS_in_a_Nutshell.

System z Von der z/VM bereitgestellte Drucker und ähnliche Geräte, die lokal an IBM z Systems-Mainframes angeschlossen werden, werden von CUPS 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: Ändern der Anschlüsse bei einem laufenden System

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

17.3 Installation der Software

PPD (PostScript Printer Description, PostScript-Druckerbeschreibung) ist die Computersprache, die die Eigenschaften, z. B. die Auflösung und Optionen wie die Verfügbarkeit einer Duplexeinheit, beschreibt. Diese Beschreibungen sind für die Verwendung der unterschiedlichen Druckeroptionen in CUPS erforderlich. Ohne eine PPD-Datei würden die Druckdaten in einem „rohen“ Zustand an den Drucker weitergeleitet werden, was in der Regel nicht erwünscht ist.

Um einen PostScript-Drucker zu konfigurieren, sollten Sie sich zunächst eine geeignete PPD-Datei beschaffen. Die Pakete `manufacturer-PPDs` und `OpenPrintingPPDs-postscript` enthalten zahlreiche PPD-Dateien. Weitere Informationen hierzu finden Sie unter *Abschnitt 17.7.3, „PPD-Dateien in unterschiedlichen Paketen“* und *Abschnitt 17.8.2, „Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar“*.

Neue PPD-Dateien können im Verzeichnis `/usr/share/cups/model/` gespeichert oder dem Drucksystem mit YaST hinzugefügt werden (siehe *Buch „*Bereitstellungshandbuch*“, Kapitel 11 „Einrichten von Hardware-Komponenten mit YaST“, Abschnitt 11.3.1.1 „Hinzufügen von Treibern mit YaST“*). Die PPD-Dateien lassen sich anschließend während der Druckereinrichtung auswählen.

Seien Sie vorsichtig, wenn Sie gleich ein ganzes Software-Paket eines Druckerherstellers installieren sollen. Durch eine solche Installation entfällt die Unterstützung durch SUSE Linux Enterprise Server. Außerdem funktionieren die Druckerkommandos unter Umständen anders und das System kann möglicherweise keine Geräte anderer Hersteller mehr adressieren. Aus diesem Grund wird das Installieren von Herstellersoftware nicht empfohlen.

17.4 Netzwerkdrucker

Ein Netzwerkdrucker kann unterschiedliche Protokolle unterstützen - einige sogar gleichzeitig. Die meisten unterstützten Protokolle sind standardisiert, und doch versuchen einige Hersteller, diesen Standard abzuändern. Treiber werden meist nur für einige wenige Betriebsssysteme angeboten. 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`.

socket

Socket bezeichnet eine Verbindung, über die die einfachen Druckdaten direkt an einen TCP-Socket gesendet werden. Einige der am häufigsten verwendeten Socket-Ports sind `9100` oder `35`. Die Syntax der Geräte-URI (Uniform Resource Identifier) lautet: socket://*`IP.FÜR.DEN.DRUCKER`*:*`Port`*, beispielsweise: `socket://192.168.2.202:9100/`.

LPD (Line Printer Daemon)

Das LDP-Protokoll wird in RFC 1179 beschrieben. Bei diesem Protokoll werden bestimmte auftragsspezifische Daten (z. B. die ID der Druckerwarteschlange) vor den eigentlichen Druckdaten gesendet. Beim Konfigurieren des LDP-Protokolls muss daher eine Druckerwarteschlange 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. Die Portnummer für einen LPD-Dienst lautet `515`. Ein Beispiel für einen Gerät-URI ist `lpd://192.168.2.202/LPT1`.

IPP (Internet Printing Protocol)

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

SMB (Windows-Freigabe)

CUPS unterstützt auch das Drucken auf freigegebenen Druckern unter Windows. Das für diesen Zweck verwendete Protokoll ist SMB. SMB verwendet die Portnummern `137`, `138` und `139`. Beispiele für Geräte-URIs sind `smb://Benutzer:Passwort@Arbeitsgruppe/smb.example.com/Drucker`, `smb://Benutzer:Passwort@smb.example.com/Drucker` und `smb://smb.example.com/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 Kommando **`nmap`** ermitteln, das Bestandteil des Pakets `nmap` ist. **`nmap`** überprüft einen Host auf offene Ports. Beispiel:

```
nmap -p 35,137-139,515,631,9100-10000 IP.OF.THE.PRINTER
```

17.5 Konfigurieren von CUPS mit Kommandozeilenwerkzeugen

CUPS kann mit Kommandozeilenwerkzeugen kofiguriert werden, beispielsweise **lpinfo**, **lpadmin** oder **lpoptions**. Sie benötigen einen Geräte-URI, der aus einem Back-End (z. B. USB) und Parametern besteht. Zum Bestimmen von gültigen Geräte- URIs auf Ihrem System verwenden Sie das Kommando **lpinfo -v | grep „:/“**:

```
# lpinfo -v | grep ":/"
direct usb://ACME/FunPrinter%20XL
network socket://192.168.2.253
```

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

```
lpadmin -p QUEUE -v DEVICE-URI -P PPD-FILE -E
```

Das Gerät (`-v`) ist anschließend als *WARTESCHLANGE* (`-p`) verfügbar und verwendet die angegebene PPD-Datei (`-P`). Das bedeutet, dass Sie die PPD-Datei und das Geräte-URI 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 usb://ACME/FunPrinter%20XL -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

Im folgenden Beispiel wird ein Netzwerkdrucker konfiguriert:

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \
/usr/share/cups/model/Postscript-level1.ppd.gz -E
```

Weitere Optionen von **lpadmin** finden Sie auf der man-Seiten von `lpadmin(8)`.

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

1. Zeigen Sie zunächst alle Optionen an:

   ```
   lpoptions -p QUEUE -l
   ```

   Beispiel:

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

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

2. Ändern Sie die Option mit **`lpadmin`**:

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

3. Prüfen Sie die neue Einstellung:

   ```
   lpoptions -p QUEUE -l

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

Wenn ein normaler Benutzer **`lpoptions`** ausführt, werden die Einstellungen in `~/.cups/lpoptions` geschrieben. Jedoch werden die `root`-Einstellungen in to `/etc/cups/lpoptions` geschrieben.

17.6 Drucken über die Kommandozeile

Um den Druckvorgang über die Kommandozeile zu starten, geben Sie **`lp -d`** *`NAME_DER_WARTESCHLANGE`* *`DATEINAME`* ein und ersetzen Sie 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`*.

17.7 Besondere Funktionen in SUSE Linux Enterprise Server

Mehrere CUPS-Funktionen wurden für SUSE Linux Enterprise Server angepasst. Im Folgenden werden einige der wichtigsten Änderungen beschrieben.

17.7.1 CUPS und Firewall

Nach einer Standardinstallation von SUSE Linux Enterprise Server ist SuSEFirewall2 aktiv, und die externen Netzwerkschnittstellen sind in der `externen Zone` konfiguriert, die eingehenden Datenverkehr blockiert. Weitere Informationen zur SUSEFirewall2-Konfiguration finden Sie in *Buch „Security Guide", Kapitel 15 „Masquerading and Firewalls", Abschnitt 15.4 „SuSEFirewall2"* und unter http://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings.

17.7.1.1 CUPS-Client

Normalerweise wird der CUPS-Client auf einem normalen Arbeitsplatzrechner ausgeführt, die sich in einer verbürgten Netzwerkumgebung hinter einer Firewall befindet. In diesem Fall empfiehlt es sich, die Netzwerkschnittstelle in der `internen Zone` zu konfigurieren, damit der Arbeitsplatzrechner innerhalb des Netzwerks erreichbar ist.

17.7.1.2 CUPS-Server

Wenn der CUPS-Server Teil der durch eine Firewall geschützten verbürgten Netzwerkumgebung ist, sollte die Netzwerkschnittstelle in der `internen Zone` der Firewall konfiguriert sein. Es ist nicht empfehlenswert, einen CUPS-Server in einer nicht verbürgten Netzwerkumgebung einzurichten, es sei denn, Sie sorgen dafür, dass er durch besondere Firewall-Regeln und Sicherheitseinstellungen in der CUPS-Konfiguration geschützt wird.

17.7.2 Durchsuchen nach Netzwerkdruckern

CUPS-Server geben regelmäßig die Verfügbarkeit und die Statusinformationen von freigegebenen Druckern im Netzwerk bekannt. Die Clients können auf diese Informationen zugreifen und beispielsweise in Druckdialogfeldern eine Liste der verfügbaren Drucker anzeigen. Dies wird als „Browsing" (Durchsuchen) bezeichnet.

Die CUPS-Server geben ihre Druckerwarteschlangen entweder über das herkömmliche CUPS-Browsing-Protokoll oder über Bonjour/DND-SD im Netzwerk bekannt. Um Netzwerkdruckerwarteschlangen durchsuchen zu können, muss der Dienst `cups-browsed` auf allen Clients ausgeführt werden, die über CUPS-Server drucken. `cups-browsed` wird standardmäßig nicht gestartet. Zum Starten für die aktuelle Sitzung führen Sie den Befehl **`sudo systemctl start cups-browsed`** aus. Damit der Dienst nach dem Booten automatisch gestartet wird, aktivieren Sie ihn mit dem Befehl **`sudo systemctl enable cups-browsed`** auf allen Clients.

Falls das Durchsuchen nach dem Starten von `cups-browsed` nicht funktioniert, geben der oder die CUPS-Server die Netzwerkdruckerwarteschlangen vermutlich über Bonjour/DND-SD bekannt. In diesem Fall müssen Sie zusätzlich das Paket `avahi` installieren und den zugehörigen Dienst mit **`sudo systemctl start avahi-daemon`** auf allen Clients starten.

17.7.3 PPD-Dateien in unterschiedlichen Paketen

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

Die Konfiguration, die nur PPD-Dateien und keine weiteren Informationsquellen verwendet, hat den Vorteil, dass die PPD-Dateien in `/usr/share/cups/model/` beliebig geändert werden können. Wenn Sie beispielsweise PostScript-Drucker nutzen, können die PPD-Dateien direkt in `/usr/share/cups/model/` kopiert werden (wenn sie nicht bereits im Paket `manufacturer-PPDs` oder `OpenPrintingPPDs-postscript` vorhanden sind), um eine optimale Konfiguration der Drucker zu erzielen.

Weitere PPD-Dateien erhalten Sie mit den folgenden Paketen:

- gutenprint: Gutenprint-Treiber und zugehörige PPDs
- splix: Splix-Treiber und zugehörige PPDs
- OpenPrintingPPDs-ghostscript: PPDs für integrierte Ghostscript-Treiber
- OpenPrintingPPDs-hpijs: PPDs für den HPIJS-Treiber für Drucker, die nicht von HP stammen

17.8 Fehlersuche

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

17.8.1 Drucker ohne Unterstützung für eine Standard-Druckersprache

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

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

Einige Hersteller stellen für ihre Drucker proprietäre Treiber zur Verfügung. Der Nachteil proprietärer Druckertreiber ist, dass es keine Garantie gibt, dass diese mit dem installierten Drucksystem funktionieren oder 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 viel Zeit darauf aufzuwenden, einen herstellerspezifischen Linux-Treiber in Gang zu bringen, ist es unter Umständen kostengünstiger, einen Drucker zu erwerben, der eine Standarddruckersprache unterstützt (vorzugsweise PostScript). 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.

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

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

17.8.3 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.
Vorausgesetzt, dass **lpd** aktiv ist und der Host Abfragen akzeptiert, rufen Sie mit dem folgenden Befehl (als `root`) einen Statusbericht für *WARTESCHLANGE* auf dem Remote-*HOST* ab:

```
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 erhalten wie in *Beispiel 17.1, „Fehlermeldung von* **lpd**“ gezeigt, wird das Problem durch den entfernten **lpd** verursacht.

BEISPIEL 17.1 FEHLERMELDUNG VON `lpd`

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

Entfernten **cupsd** prüfen

Ein CUPS-Netzwerkserver kann die Warteschlangen standardmäßig alle 30 Sekunden per Broadcast über den UDP-Port `631` senden. Demzufolge kann mit dem folgenden Kommando getestet werden, ob im Netzwerk ein CUPS-Netzwerkserver mit aktivem Broadcast vorhanden ist. Stoppen Sie unbedingt Ihren lokalen CUPS-Daemon, bevor Sie das Kommando ausführen.

```
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 17.2, „Broadcast vom CUPS-Netzwerkserver“* dargestellt.

BEISPIEL 17.2 BROADCAST VOM CUPS-NETZWERKSERVER

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

`System z` Berücksichtigen Sie, dass IBM z Systems-Ethernet-Geräte 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 Machine

Spooler, die in einer Print Server Machine ausgeführt werden, verursachen gelegentlich Probleme, wenn sie mehrere Druckaufträge bearbeiten müssen. Da dies durch den Spooler in der Print Server Machine verursacht wird, gibt es keine Möglichkeit, dieses Problem zu beheben. Sie haben jedoch die Möglichkeit, den Spooler in der Print Server Machine zu umgehen, indem Sie den an die Print Server Machine angeschlossenen Drucker über den TCP-Socket direkt kontaktieren. Siehe *Abschnitt 17.4, „Netzwerkdrucker“*.
Auf diese Weise wird die Print Server Machine 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 Machine kennen. Wenn der Drucker eingeschaltet und an die Print Server Machine angeschlossen ist, kann dieser TCP-Port in der Regel mit dem Dienstprogramm **nmap** aus dem Paket nmap ermittelt werden, wenn die Print Server Machine einige Zeit eingeschaltet ist. Beispiel: **nmap** *IP-Adresse* gibt die folgende Ausgabe für eine Print Server Machine 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 Machine angeschlossenen Drucker über TCP-Socket an Port `9100` angesprochen werden kann. **`nmap`** prüft standardmäßig nur einige allgemein bekannte Ports, die in `/usr/share/nmap/nmap-services` aufgeführt sind. Um alle möglichen Ports zu überprüfen, verwenden Sie den Befehl **`nmap -p`** *AUSGANGS-PORT-ZIEL-PORT IP-ADRESSE*. Dies kann einige Zeit dauern. Weitere Informationen finden Sie auf der man-Seite zu **`ypbind`**.
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.

17.8.4 Fehlerhafte Ausdrucke ohne Fehlermeldung

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

17.8.5 Deaktivierte Warteschlangen

Wenn die Datenübertragung zum Empfänger auch nach mehreren Versuchen nicht erfolgreich ist, meldet das CUPS-Back-End, z. B. `USB` oder `socket`, dem Drucksystem (an **`cupsd`**) einen Fehler. Das Backend bestimmt, wie viele erfolglose Versuche angemessen sind, bis die Datenübertragung als unmöglich gemeldet 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 Kommando **`cupsenable`** wieder aktivieren.

17.8.6 CUPS-Browsing: Löschen von Druckaufträgen

Wenn ein CUPS-Netzwerkserver seine Warteschlangen den Client-Hosts via Browsing bekannt macht und auf den Host-Clients ein geeigneter lokaler **cupsd** aktiv ist, akzeptiert der Client-**cupsd** Druckaufträge von Anwendungen und leitet sie an den **cupsd** auf dem Server weiter. Wenn **cupsd** auf dem Server 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. Dies liegt daran, dass der Client-**cupsd** den Druckauftrag als abgeschlossen betrachtet, wenn dieser an den Server-**cupsd** weitergeleitet wurde.

Soll der Druckauftrag auf dem Server gelöscht werden, ermitteln Sie die Auftragsnummer auf dem Server mit einem Kommando wie **lpstat -h cups.example.com -o**. Hierbei wird vorausgesetzt, dass der Server den Druckauftrag noch nicht erledigt (also noch nicht vollständig an den Drucker gesendet) hat. So löschen Sie den Druckauftrag anhand der abgerufenen Auftragsnummer auf dem Server:

```
cancel -h cups.example.com QUEUE-JOBNUMBER
```

17.8.7 Fehlerhafte Druckaufträge und Fehler bei der Datenübertragung

Wenn Sie während des Druckvorgangs den Drucker oder den Computer abschalten, bleiben Druckaufträge in der Warteschlange. Der Druckvorgang wird wieder aufgenommen, sobald der Computer (bzw. der Drucker) wieder eingeschaltet wird. Fehlerhafte Druckaufträge müssen mit **cancel** aus der Warteschlange entfernt werden.

Wenn ein Druckauftrag beschädigt ist oder ein Fehler bei der Datenübertragung zwischen Host und Drucker auftritt, kann der Drucker die Daten nicht ordnungsgemäß verarbeiten und es werden unzählige Blätter mit unlesbaren Zeichen bedruckt. So reparieren Sie dieses Problem:

1. Um den Druckvorgang zu beenden, entfernen Sie das Papier aus Tintenstrahldruckern oder öffnen Sie die Papierzufuhr bei Laserdruckern. Qualitativ hochwertige Drucker sind mit einer Taste zum Abbrechen des aktuellen Druckauftrags ausgestattet.
2. Der Druckauftrag befindet sich möglicherweise noch in der Warteschlange, da die Aufträge erst dann entfernt werden, wenn sie vollständig an den Drucker übertragen wurden. Geben Sie **lpstat -o** oder **lpstat -h cups.example.com -o** ein, um zu prüfen, über

welche Warteschlange aktuell gedruckt wird. Löschen Sie den Druckauftrag mit **cancel** *WARTESCHLANGE*-*AUFTRAGSNUMMER* oder **cancel -h cups.example.com** *WARTESCHLANGE*-*AUFTRAGSNUMMER*.

3. Auch wenn der Druckauftrag aus der Warteschlange gelöscht wurde, werden einige Daten weiter an den Drucker gesendet. Prüfen Sie, ob ein CUPS-Backend-Prozess für die entsprechende Warteschlange ausgeführt wird und wenn ja, beenden Sie ihn.

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.

17.8.8 Fehlersuche für CUPS

Suchen Sie Probleme in CUPS 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.

17.8.9 Weiterführende Informationen

Ausführliche Informationen zum Drucken unter SUSE Linux finden Sie in der openSUSE-Supportdatenbank unter http://en.opensuse.org/Portal:Printing. Lösungen zu vielen spezifischen Problemen finden Sie in der SUSE Knowledgebase (http://www.suse.com/support/). Die relevanten Themen finden Sie am schnellsten mittels einer Textsuche nach `CUPS`.

18 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 finden Sie grundlegende Informationen zur X-Konfiguration und Hintergrundinformationen zur Verwendung von Schriftarten in SUSE Linux Enterprise Server.

In der Regel muss das X Window System nicht konfiguriert werden. Die Hardware wird beim Starten von X dynamisch erkannt. Die Nutzung von `xorg.conf` ist daher überholt. Wenn Sie die Funktionsweise von X dennoch mit benutzerdefinierten Optionen ändern möchten, können Sie die Konfigurationsdateien unter `/etc/X11/xorg.conf.d/` entsprechend bearbeiten.

Tipp: IBM z Systems: Konfigurieren der grafischen Bedieneroberfläche

IBM z Systems 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 z Systems finden Sie in *Buch „Bereitstellungshandbuch", Kapitel 4 „Installation auf IBM z Systems"*.

18.1 Installation und Konfiguration von Schriften

Schriften in Linux lassen sich in zwei Gruppen gliedern:

Outline-Schriften oder Vektorschriften

Enthält eine mathematische Beschreibung als Informationen zum Zeichnen der Form einer Glyphe. Die Glyphen können dabei auf eine beliebige Größe skaliert werden, ohne dass die Qualität darunter leidet. Bevor Sie eine solche Schrift (oder Glyphe) verwenden können, müssen die mathematischen Beschreibungen in ein Raster überführt werden. Dieser Vorgang wird als *Schriftrasterung* bezeichnet. Beim *Schrift-Hinting* (in der Schrift eingebettet) wird das Rendering-Ergebnis für eine bestimmte Größe optimiert. Die Rasterung und das Hinting erfolgen mit der FreeType-Bibliothek.

Unter Linux werden häufig die Formate PostScript Typ 1 und Typ 2, TrueType und OpenType verwendet.

Bitmap- oder Rasterschriften

Besteht aus einer Pixelmatrix, die auf eine bestimmte Schriftgröße abgestimmt ist. Bitmap-Schriften lassen sich äußerst schnell und einfach rendern. Im Gegensatz zu Vektorschriften können Bitmap-Schriften jedoch nicht ohne Qualitätseinbußen skaliert werden. Diese Schriften werden daher meist in unterschiedlichen Größen bereitgestellt. Selbst heute noch werden Bitmap-Schriften in der Linux-Konsole und teils auch auf Terminals verwendet.

Unter Linux sind das Portable Compiled Format (PCF) und das Glyph Bitmap Distribution Format (BDF) die häufigsten Formate.

Das Erscheinungsbild dieser Schriften wird durch zwei wichtige Faktoren beeinflusst:

- Auswählen einer geeigneten Schriftfamilie
- Rendern der Schrift mit einem Algorithmus, der optisch ansprechende Ergebnisse bewirkt.

Der letzte Punkt ist nur für Vektorschriften relevant. Die beiden obigen Punkte sind stark subjektiv; dennoch müssen einige Standardvorgaben festgelegt werden.

Linux-Schriftrenderingsysteme bestehen aus mehreren Bibliotheken mit unterschiedlichen Beziehungen. Die grundlegende Schriftrenderingbibilothek FreeType (http://www.freetype.org/) konvertiert die Schriftglyphen von unterstützten Formaten in optimierte Bitmap-Glyphen. Der Renderingvorgang wird durch einen Algorithmus und die zugehörigen Parameter gesteuert (unter Umständen patentrechtlich geschützt).

Alle Programme und Bibliotheken, die mit FreeType arbeiten, sollten auf die Fontconfig (http://www.fontconfig.org/)-Bibliothek zurückgreifen. In dieser Bibliothek werden die Schriftkonfigurationen von Benutzern und vom System gesammelt. Wenn ein Benutzer die Fontconfig-Einstellung ergänzt, entstehen durch diese Änderung Fontconfig-fähige Anwendungen.

Ein eingehenderes OpenType-Shaping für Skripte wie Arabic, Han oder Phags-Pa und andere höhere Textverarbeitung erfolgt mit Harfbuzz (http://www.harfbuzz.org/) oder Pango (http://www.pango.org/).

18.1.1 Anzeigen der installierten Schriften

Mit dem Kommando **rpm** oder **fc-list** erhalten Sie einen Überblick über die Schriften, die auf dem System installiert sind. Beide Kommandos liefern eine aussagekräftige Antwort, geben dabei jedoch (je nach System- und Benutzerkonfiguration) ggf. unterschiedliche Listen zurück:

rpm

rpm zeigt die auf dem System installierten Software-Pakete an, in denen sich Schriften befinden:

```
rpm -qa '*fonts*'
```

Alle Schriftpakete sollten mit diesem Ausdruck aufgefunden werden. Unter Umständen gibt das Kommando jedoch einige falsch positive Einträge zurück, beispielsweise `fonts-config` (dies ist weder eine Schrift noch sind hier Schriften enthalten).

fc-list

Mit **fc-list** erhalten Sie einen Überblick darüber, welche Schriftfamilien verfügbar sind und ob diese auf dem System oder in Ihrem Benutzerverzeichnis installiert sind:

```
fc-list ':' family
```

Anmerkung: Kommando **fc-list**

Das Kommando **fc-list** ist eine Erweiterung zur Fontconfig-Bibliothek. Aus Fontconfig – oder genauer gesagt, aus dem Cache – lassen sich zahlreiche interessante Informationen ermitteln. Unter **man 1 fc-list** finden Sie weitere Einzelheiten.

18.1.2 Anzeigen von Schriften

Mit dem Kommando **ftview** (Paket `ft2demos`) sowie unter http://fontinfo.opensuse.org/ sehen Sie, wie eine installierte Schriftfamilie dargestellt wird. Soll beispielsweise die Schrift FreeMono in 14 Punkt angezeigt werden, verwenden Sie **ftview** wie folgt:

```
ftview 14 /usr/share/fonts/truetype/FreeMono.ttf
```

Unter http://fontinfo.opensuse.org/ erfahren Sie, welche Schriftschnitte (normal, fett, kursiv etc.) und welche Sprachen unterstützt werden.

18.1.3 Abfragen von Schriften

Mit dem Kommando **fc-match** fragen Sie ab, welche Schrift für ein angegebenes Muster verwendet wird.

Wenn das Muster beispielsweise eine bereits installierte Schrift enthält, gibt **fc-match** den Dateinamen, die Schriftfamilie und den Schriftschnitt zurück:

```
tux > fc-match 'Liberation Serif'
LiberationSerif-Regular.ttf: "Liberation Serif" "Regular"
```

Ist die gewünschte Schrift nicht auf dem System vorhanden, greifen die Ähnlichkeitsregeln von Fontconfig und es werden verfügbare Schriften mit der größtmöglichen Ähnlichkeit gesucht. Ihre Anforderung wird also ersetzt:

```
tux > fc-match 'Foo Family'
DejaVuSans.ttf: "DejaVu Sans" "Book"
```

Fontconfig unterstützt *Aliase*: Ein Name wird durch den Namen einer anderen Schriftfamilie ersetzt. Ein typisches Beispiel sind generische Namen wie „sans-serif“, „serif“ und „monospace“. Diese Alias-Namen können durch echte Familiennamen und sogar durch eine Präferenzliste mit Familiennamen ersetzt werden:

```
tux > for font in serif sans mono; do fc-match "$font" ; done
DejaVuSerif.ttf: "DejaVu Serif" "Book"
DejaVuSans.ttf: "DejaVu Sans" "Book"
DejaVuSansMono.ttf: "DejaVu Sans Mono" "Book"
```

Das Ergebnis auf Ihrem System kann abweichen, abhängig davon, welche Schriften derzeit installiert sind.

Anmerkung: Ähnlichkeitsregeln in Fontconfig

Fontconfig gibt *immer* eine reale Schriftfamilie (sofern mindestens eine Familie installiert ist) für die angegebene Anforderung zurück, die so ähnlich ist wie möglich. Die „Ähnlichkeit“ ist abhängig von den internen Metriken von Fontconfig sowie von den Fontconfig-Einstellungen des Benutzers oder Administrators.

18.1.4 Installieren von Schriften

Zum Installieren einer neuen Schrift stehen die folgenden wichtigsten Verfahren zur Auswahl:

1. Installieren Sie die Schriftdateien (z. B. `*.ttf` oder `*.otf`) manuell in ein bekanntes Schriftverzeichnis. Wenn die Schriften systemweit verfügbar sein sollen, verwenden Sie das Standardverzeichnis `/usr/share/fonts`. Für die Installation in Ihrem Benutzerverzeichnis verwenden Sie `~/.config/fonts`.
   Falls Sie nicht die standardmäßigen Verzeichnisse verwenden möchten, können Sie in Fontconfig ein anderes Verzeichnis auswählen. Hierzu geben Sie das Element `<dir>` an. Weitere Informationen finden Sie in *Abschnitt 18.1.5.2, „Kurzer Einblick in Fontconfig-XML“*.

2. Installieren Sie die Schriften mit **`zypper`**. Zahlreiche Schriften sind bereits als Paket verfügbar, beispielsweise in der SUSE-Distribution oder im Repository M17N:fonts (http://download.opensuse.org/repositories/M17N:/fonts/). Fügen Sie das Repository mit dem nachfolgenden Kommando in die Liste ein. So fügen Sie beispielsweise ein Repository für SLE 12 hinzu:

   ```
   sudo zypper ar
        http://download.opensuse.org/repositories/M17N:/fonts/SLE_12_SP5/
   ```

   `FONT_FAMILY_NAME` ermitteln Sie mit dem folgenden Kommando:

   ```
   sudo zypper se 'FONT_FAMILY_NAME*fonts'
   ```

18.1.5 Konfigurieren der Darstellung von Schriften

Je nach Renderingmedium und Schriftgröße entstehen womöglich keine zufriedenstellenden Ergebnisse. Ein durchschnittlicher Monitor hat beispielsweise eine Auflösung von 100dpi. Bei dieser Auflösung sind die Pixel zu groß und die Glyphen wirken plump und unförmig.

Für niedrigere Auflösungen stehen mehrere Algorithmen bereit, z. B. Anti-Aliasing (Graustufenglättung), Hinting (Anpassen an das Raster) oder Subpixel-Rendering (Verdreifachen der Auflösung in eine Richtung). Diese Algorithmen können dabei von Schriftformat zu Schriftformat unterschiedlich sein.

Wichtig: Patentprobleme beim Subpixel-Rendering

Das Subpixel-Rendering wird nicht in SUSE-Distributionen verwendet. FreeType2 unterstützt zwar diesen Algorithmus, allerdings unterliegt er mehreren Patenten, die Ende 2019 auslaufen. Die eingestellten Optionen für das Subpixel-Rendering in Fontconfig wirken sich daher nur dann aus, wenn das System eine FreeType2-Bibilothek enthält, in der das Subpixel-Rendering kompiliert ist.

Mit Fontconfig können Sie den Rendering-Algorithmus für einzelne Schriften oder auch für eine Gruppe von Schriften gleichzeitig auswählen.

18.1.5.1 Konfigurieren von Schriften mit `sysconfig`

SUSE Linux Enterprise Server umfasst eine `sysconfig`-Schicht oberhalb von Fontconfig. Dies ist ein guter Ausgangspunkt, um mit der Schriftkonfiguration zu experimentieren. Zum Ändern der Standardeinstellungen bearbeiten Sie die Konfigurationsdatei `/etc/sysconfig/fonts-config`. (Alternativ verwenden Sie das YaST-Modul sysconfig.) Führen nach dem Bearbeiten der Datei **`fonts-config`** aus:

```
sudo /usr/sbin/fonts-config
```

Starten Sie die Anwendung neu, damit der Effekt sichtbar wird. Beachten Sie Folgendes:

- Einige Anwendungen müssen nicht neu gestartet werden. Firefox liest die Fontconfig-Konfiguration beispielsweise in regelmäßigen Abständen aus. Auf soeben erstellten oder neu geladenen Registerkarten werden die Schriftkonfigurationen erst später sichtbar.
- Nach jedem Installieren oder Entfernen eines Pakets wird automatisch das Skript **`fonts-config`** aufgerufen. (Ist dies nicht der Fall, so ist das Schriften-Software-Paket fehlerhaft.)
- Jede sysconfig-Variable kann vorübergehend mit der Kommandozeilenoption **`fonts-config`** überschrieben werden. Weitere Informationen finden Sie in **`fonts-config --help`**.

Es können verschiedene sysconfig-Variablen geändert werden. Weitere Informationen finden Sie auf der man-Seite **`man 1 fonts-config`** oder auf der Hilfeseite des YaST-Moduls sysconfig. Beispiele für Variablen:

Verwendung der Rendering-Algorithmen

Nutzen Sie beispielsweise `FORCE_HINTSTYLE`, `FORCE_AUTOHINT`, `FORCE_BW`, `FORCE_BW_MONOSPACE`, `USE_EMBEDDED_BITMAPS` und `EMBEDDED_BITMAP_LANGAGES`

Präferenzliste generischer Aliase

Verwenden Sie `PREFER_SANS_FAMILIES`, `PREFER_SERIF_FAMILIES`, `PREFER_MONO_FAMILIES` und `SEARCH_METRIC_COMPATIBLE`

In der nachfolgenden Liste finden Sie einige Konfigurationsbeispiele, sortiert von den „am leichtesten lesbaren“ Schriften (stärkerer Kontrast) zu den „ansprechendsten“ Schriften (stärker geglättet).

Bitmap-Schriften

Die Präferenz für die Bitmap-Schriften bestimmen Sie über die `PREFER_*_FAMILIES`-Variablen. Beachten Sie das Beispiel im Hilfeabschnitt zu diesen Variablen. Bitmap-Schriften werden schwarzweiß dargestellt und nicht geglättet und sie stehen nur in bestimmten Größen zur Verfügung. Nutzen Sie ggf.

```
SEARCH_METRIC_COMPATIBLE="no"
```

zum Deaktivieren der Ersetzungen der Familienname auf Basis der Metrikkompatibilität.

Skalierbare, schwarzweiß dargestellte Schriften

Skalierbare Schriften, die ohne Antialiasing gerendert werden, können ähnliche Ergebnisse liefern wie Bitmap-Schriften, wobei die Schriften weiterhin skalierbar bleiben. Verwenden Sie Schriften mit gutem Hinting, beispielsweise die Liberation-Schriftfamilien. Bislang sind leider nur wenige Schriften mit gutem Hinting erhältlich. Mit der folgenden Variablen erzwingen Sie diese Methode:

```
FORCE_BW="yes"
```

Nichtproportionale, schwarzweiß dargestellte Schriften

Nichtproportionale Schriften werden nur ohne Antialiasing gerendert; ansonsten verwenden Sie die Standardeinstellungen:

```
FORCE_BW_MONOSPACE="yes"
```

Standardeinstellungen

Alle Schriften werden mit Antialiasing gerendert. Schriften mit gutem Hinting werden mit dem *Byte-Code-Interpreter*) gerendert, die übrigen Schriften mit Autohinter (`hintstyle=hintslight`). Behalten Sie die Standardeinstellungen für alle relevanten sysconfig-Variablen bei.

CFF-Schriften

Die Schriften werden im CFF-Format verwendet. Im Hinblick auf die aktuellen Verbesserungen in FreeType2 sind diese Schriften im Allgemeinen leichter lesbar als die standardmäßigen TrueType-Schriften. Probieren Sie sie aus, indem Sie das Beispiel `PREFER_*_FAMILIES` verwenden. Auf Wunsch können Sie sie wie folgt dunkler und fetter darstellen:

```
SEARCH_METRIC_COMPATIBLE="no"
```

Standardmäßig werden sie mit `hintstyle=hintslight` gerendert. Eine weitere Möglichkeit:

```
SEARCH_METRIC_COMPATIBLE="no"
```

Nur Autohinter

Auch für Schriften mit gutem Hinter wird Autohinter aus FreeType2 verwendet. Dies kann zu fetteren, manchmal unscharfen Buchstaben mit niedrigerem Kontrast führen. Mit der folgenden Variablen aktivieren Sie dies:

```
FORCE_AUTOHINTER="yes"
```

Mit `FORCE_HINTSTYLE` steuern Sie den Hinting-Grad.

18.1.5.2 Kurzer Einblick in Fontconfig-XML

Bei Fontconfig wird das Konfigurationsformat *eXtensible Markup Language* (XML) genutzt. Diese wenigen Beispiele sollen keine erschöpfende Referenz darstellen, sondern lediglich einen kurzen Überblick bieten. Weitere Informationen und Anregungen finden Sie in **`man 5 fonts-conf`** oder `/etc/fonts/conf.d/`.

Die zentrale Fontconfig-Konfigurationsdatei ist `/etc/fonts/fonts.conf` und umfasst unter anderem das gesamte Verzeichnis `/etc/fonts/conf.d/`. Änderungen an Fontconfig können an zwei Stellen vorgenommen werden:

FONTCONFIG-KONFIGURATIONSDATEIEN

1. **Systemweite Änderungen.** Bearbeiten Sie die Datei `/etc/fonts/local.conf`. (Standardmäßig enthält diese Datei ein leeres `fontconfig`-Element.)
2. **Benutzerspezifische Änderungen.** Bearbeiten Sie die Datei `~/.config/fontconfig/fonts.conf`. Speichern Sie die Fontconfig-Konfigurationsdateien in das Verzeichnis `~/.config/fontconfig/conf.d/`.

Benutzerspezifische Änderungen überschreiben die systemweiten Einstellungen.

Anmerkung: Veraltete Benutzerkonfigurationsdatei

Die Datei `~/.fonts.conf` ist als veraltet gekennzeichnet und darf nicht mehr verwendet werden. Verwenden Sie stattdessen die Datei `~/.config/fontconfig/fonts.conf`.

Jede Konfigurationsdatei muss ein `fontconfig`-Element enthalten. Die minimale Datei sieht daher wie folgt aus:

```
<?xml version="1.0"?>
   <!DOCTYPE fontconfig SYSTEM "fonts.dtd">
   <fontconfig>
   <!-- Insert your changes here -->
   </fontconfig>
```

Falls die Standardverzeichnisse nicht ausreichen, fügen Sie das `dir`-Element mit dem gewünschten Verzeichnis ein:

```
<dir>/usr/share/fonts2</dir>
```

Fontconfig sucht *rekursiv* nach den Schriften.

Mit dem folgenden Fontconfig-Snippet können Sie die Algorithmen für das Schriftrendering auswählen (siehe *Beispiel 18.1, „Festlegen von Rendering-Algorithmen“*):

BEISPIEL 18.1 FESTLEGEN VON RENDERING-ALGORITHMEN

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

```
  <string>FAMILY_NAME</string>
 </test>
 <edit name="antialias" mode="assign">
  <bool>true</bool>
 </edit>
 <edit name="hinting" mode="assign">
  <bool>true</bool>
 </edit>
 <edit name="autohint" mode="assign">
  <bool>false</bool>
 </edit>
 <edit name="hintstyle" mode="assign">
  <const>hintfull</const>
 </edit>
</match>
```

Sie können verschiedene Eigenschaften der Schriften zunächst ausprobieren. Mit dem `<test>`-Element können Sie beispielsweise die Schriftfamilie (siehe Beispiel), das Größenintervall, den Zeichenabstand, das Schriftformat und andere Eigenschaften testen. Wenn Sie `<test>` vollständig löschen, werden alle `<edit>`-Elemente auf sämtliche Schriften angewendet (globale Änderung).

BEISPIEL 18.2 ALIASE UND ERSETZUNGEN VON FAMILIENNAMEN

Regel 1

```
<alias>
 <family>Alegreya SC</family>
 <default>
  <family>serif</family>
 </default>
</alias>
```

Regel 2

```
<alias>
 <family>serif</family>
 <prefer>
  <family>Droid Serif</family>
 </prefer>
</alias>
```

Regel 3

```
<alias>
```

```
 <family>serif</family>
 <accept>
  <family>STIXGeneral</family>
 </accept>
</alias>
```

Mit den Regeln in *Beispiel 18.2, „Aliase und Ersetzungen von Familiennamen“* wird eine *priorisierte Familienliste* (PFL) erzeugt. Je nach Element werden verschiedene Aktionen ausgeführt:

`<default>` in *Regel 1*
: Mit dieser Regel wird ein `serif`-Familienname *an das Ende* der PFL angehängt.

`<prefer>` in *Regel 2*
: Mit dieser Regel wird „Droid Serif“ *direkt vor* dem ersten Auftreten von `serif` in der PFL eingefügt, wenn `Alegreya SC` in der PFL vorliegt.

`<accept>` in *Regel 3*
: Mit dieser Regel wird ein „STIXGeneral“-Familienname *direkt nach* dem ersten Auftreten des `serif`-Familiennamens in die PFL eingefügt.

Wenn alle Snippets in der Reihenfolge *Regel 1* - *Regel 2* - *Regel 3* ausgeführt werden und der Benutzer „Alegreya SC“ anfordert, wird die PFL wie in *Tabelle 18.1, „Erzeugen einer PFL aus Fontconfig-Regeln“* dargestellt erzeugt.

TABELLE 18.1 ERZEUGEN EINER PFL AUS FONTCONFIG-REGELN

Reihenfolge	Aktuelle PFL
Anforderung	`Alegreya SC`
Regel 1	`Alegreya SC`, `serif`
Regel 2	`Alegreya SC`, `Droid Serif`, `serif`
Regel 3	`Alegreya SC`, `Droid Serif`, `serif`, `STIXGeneral`

In den Fontconfig-Metriken hat der Familienname die höchste Priorität vor anderen Mustern wie Schriftschnitt, Größe usw. Fontconfig prüft, welche Familie derzeit auf dem System installiert ist. Wenn „Alegreya SC“ installiert ist, gibt Fontconfig diese Schrift zurück. Ansonsten wird „Droid Serif“ angefordert usw.

Gehen Sie vorsichtig vor. Wenn die Reihenfolge der Fontconfig-Snippets geändert wird, gibt Fontconfig unter Umständen andere Ergebnisse zurück (siehe *Tabelle 18.2, „Ergebnisse beim Erzeugen der PFL aus Fontconfig-Regeln mit anderer Reihenfolge“*).

TABELLE 18.2 ERGEBNISSE BEIM ERZEUGEN DER PFL AUS FONTCONFIG-REGELN MIT ANDERER REIHENFOLGE

Reihenfolge	Aktuelle PFL	Hinweis
Anforderung	`Alegreya SC`	Dieselbe Anforderung wie oben.
Regel 2	`Alegreya SC`	`serif` nicht FPL, kein Ersatz
Regel 3	`Alegreya SC`	`serif` nicht FPL, kein Ersatz
Regel 1	`Alegreya SC`, `serif`	`Alegreya SC` in PFL vorhanden, Ersatz vorgenommen

Anmerkung: Implikation.

Betrachten Sie das Alias `<default>` als Klassifizierung oder Einbeziehung dieser Gruppe (sofern nicht installiert). Wie das Beispiel zeigt, muss `<default>` stets vor den Aliasen `<prefer>` und `<accept>` dieser Gruppe stehen.

Die Klassifizierung `<default>` ist nicht auf die generischen Aliase serif, sans-serif und monospace beschränkt. Ein ausführlicheres Beispiel finden Sie in `/usr/share/fontconfig/conf.avail/30-metric-aliases.conf`.

Mit dem nachfolgenden Fontconfig-Snippet in *Beispiel 18.3, „Aliase und Ersetzungen von Familiennamen“* wird eine `serif`-Gruppe erstellt. Jede Familie in dieser Gruppe kann andere Familien ersetzen, wenn eine vorangehende Schrift nicht installiert ist.

BEISPIEL 18.3 ALIASE UND ERSETZUNGEN VON FAMILIENNAMEN

```
<alias>
 <family>Alegreya SC</family>
 <default>
  <family>serif</family>
 </default>
</alias>
<alias>
```

```
 <family>Droid Serif</family>
 <default>
  <family>serif</family>
 </default>
</alias>
<alias>
 <family>STIXGeneral</family>
 <default>
  <family>serif</family>
 </default>
</alias>
<alias>
 <family>serif</family>
 <accept>
  <family>Droid Serif</family>
  <family>STIXGeneral</family>
  <family>Alegreya SC</family>
 </accept>
</alias>
```

Die Priorität ergibt sich aus der Reihenfolge im Alias `<accept>`. Ebenso können stärkere Aliase `<prefer>` verwendet werden.

Beispiel 18.2, „Aliase und Ersetzungen von Familiennamen“ wird durch *Beispiel 18.4, „Aliase und Ersetzungen von Familiennamen“* ergänzt.

BEISPIEL 18.4 ALIASE UND ERSETZUNGEN VON FAMILIENNAMEN

Regel 4

```
<alias>
 <family>serif</family>
 <accept>
  <family>Liberation Serif</family>
 </accept>
</alias>
```

Regel 5

```
<alias>
 <family>serif</family>
 <prefer>
  <family>DejaVu Serif</family>
 </prefer>
</alias>
```

Die erweiterte Konfiguration aus *Beispiel 18.4, „Aliase und Ersetzungen von Familiennamen“* würde die folgende PFL-Entwicklung bewirken:

TABELLE 18.3 ERGEBNISSE BEIM ERZEUGEN EINER PFL AUS FONTCONFIG-REGELN

Reihenfolge	Aktuelle PFL
Anforderung	`Alegreya SC`
Regel 1	`Alegreya SC`, `serif`
Regel 2	`Alegreya SC`, `Droid Serif`, `serif`
Regel 3	`Alegreya SC`, `Droid Serif`, `serif`, `STIXGeneral`
Regel 4	`Alegreya SC`, `Droid Serif`, `serif`, `Liberation Serif`, `STIXGeneral`
Regel 5	`Alegreya SC`, `Droid Serif`, `DejaVu Serif`, `serif`, `Liberation Serif`, `STIXGeneral`

Anmerkung: Auswirkungen.

- Wenn mehrere `<accept>`-Deklarationen für denselben generischen Namen vorhanden sind, hat die zuletzt geparste Deklaration „Vorrang“. Beim Erstellen einer systemweiten Konfiguration sollten Sie `<accept>` **nach Möglichkeit nicht nach** dem Benutzer(`/etc/fonts/conf.d/*-user.conf`) angeben.
- Wenn mehrere `<prefer>`-Deklarationen für denselben generischen Namen vorhanden sind, hat die zuletzt geparste Deklaration „Vorrang“. In der systemweiten Konfiguration sollten Sie `<prefer>` **nicht vor** dem Benutzer angeben.
- Jede `<prefer>`-Deklaration überschreibt die `<accept>`-Deklarationen für denselben generischen Namen. Wenn der Administrator dem Benutzer die Möglichkeit geben möchte, auch `<accept>` zu verwenden (nicht nur `<prefer>`), sollte der Administrator `<prefer>` nicht in der systemweiten Konfiguration angeben. Die meisten Benutzer beschränken sich jedoch lediglich auf `<prefer>`, sodass dies keine negativen Auswirkungen haben sollte. `<prefer>` kommt auch in systemweiten Konfigurationen zum Einsatz.

18.2 Weiterführende Informationen

Installieren Sie die `xorg-docs`-Pakete, um detailliertere Informationen zu X11 zu erhalten. Auf der man-Seite **`man 5 xorg.conf`** finden Sie weitere Informationen zum Format der manuellen Konfiguration (falls erforderlich). Weitere Informationen zur X11-Entwicklung finden Sie auf der Startseite des Projekts unter http://www.x.org.

Die Treiber befinden sich in `xf86-video-*`-Paketen, beispielsweise `xf86-video-nv`. Viele der Treiber, die mit diesen Paketen geliefert werden, sind ausführlich in der zugehörigen man-Seite beschrieben. Wenn Sie beispielsweise den `nv`-Treiber verwenden, erhalten Sie weitere Informationen auf der man-Seite **`man 4 nv`**.

Informationen über Treiber von anderen Herstellern sollten in `/usr/share/doc/packages/<paketname>` zur Verfügung stehen. Beispielsweise ist die Dokumentation von `x11-video-nvidiaG03` nach der Installation des Pakets in `/usr/share/doc/packages/x11-video-nvidiaG03` verfügbar.

19 Zugriff auf Dateisysteme mit FUSE

FUSE ist das Akronym für *File System in User Space* (Dateisystem im Userspace). Das bedeutet, Sie können ein Dateisystem als nicht privilegierter Benutzer konfigurieren und einhängen. Normalerweise müssen Sie für diese Aufgabe als `root` angemeldet sein. FUSE alleine ist ein Kernel-Modul. In Kombination mit Plug-Ins kann FUSE auf nahezu alle Dateisysteme wie SSH-Fernverbindungen, ISO-Images und mehr erweitert werden.

19.1 Konfigurieren von FUSE

Bevor Sie FUSE installieren können, müssen Sie das Paket `fuse` installieren. Abhängig vom gewünschten Dateisystem benötigen Sie zusätzliche Plugins, die in verschiedenen Paketen verfügbar sind.

In der Regel muss FUSE nicht konfiguriert werden. Jedoch empfiehlt es sich, ein Verzeichnis anzulegen, in dem Sie alle Ihre Einhängepunkte speichern. Sie können beispielsweise das Verzeichnis `~/mounts` anlegen und dort Ihre Unterverzeichnisse für die verschiedenen Dateisysteme einfügen.

19.2 Einhängen einer NTFS-Partition

NTFS (*New Technology File System*) ist das Standard-Dateisystem von Windows. Unter normalen Umständen ist ein nicht privilegierter Benutzer nicht in der Lage, NTFS-Blockgeräte über die externe FUSE-Bibliothek einzuhängen. Für das nachfolgende Verfahren zum Einhängen einer Windows-Partition sind daher Root-Berechtigungen erforderlich.

1. Melden Sie sich als `root` an und installieren Sie das Paket `ntfs-3g`. Dies finden Sie in SUSE Linux Enterprise Workstation Extension.
2. Erstellen Sie ein Verzeichnis, das als Einhängepunkt genutzt werden soll, z. B. `~/mounts/windows`.

3. Finden Sie heraus, welche Windows-Partition Sie brauchen. Starten Sie das Partitionierungsmodul von YaST und ermitteln Sie die Partition, die zu Windows gehört; nehmen Sie jedoch keine Änderungen vor. Alternativ können Sie sich als `root` anmelden und `/sbin/fdisk -l` ausführen. Suchen Sie Partitionen mit dem Partitionstyp `HPFS/NTFS`.

4. Hängen Sie die Partition im Schreib-Lese-Modus ein. Ersetzen Sie den Platzhalter *DEVICE* durch Ihre entsprechende Windows-Partition:

   ```
   ntfs-3g /dev/DEVICE MOUNT POINT
   ```

   Um die Windows-Partition im schreibgeschützten Modus zu verwenden, hängen Sie `-o ro` an:

   ```
   ntfs-3g /dev/DEVICE MOUNT POINT -o ro
   ```

   Der Befehl **ntfs-3g** hängt das angegebene Gerät mit der aktuellen Benutzer- (UID) und Gruppen-ID (GID) ein. Sollen die Schreibberechtigungen auf einen anderen Benutzer eingestellt werden, rufen Sie mit dem Befehl **id** `USER` die Ausgabe der UID- und GID-Werte ab. Legen Sie ihn fest mit:

   ```
   id tux
   uid=1000(tux) gid=100(users) groups=100(users),16(dialout),33(video)
   ntfs-3g /dev/DEVICE MOUNT POINT -o uid=1000,gid=100
   ```

   Weitere Optionen finden Sie auf der man-Seite.

Zum Aushängen der Ressource starten Sie **fusermount -u** *MOUNT POINT*.

19.3 Weiterführende Informationen

Weitere Informationen finden Sie auf der Homepage http://fuse.sourceforge.net von FUSE.

20 Verwalten von Kernelmodulen

Linux ist als monolithischer Kernel ausgelegt, kann jedoch mithilfe von Kernelmodulen erweitert werden. Diese besonderen Objekte lassen sich je nach Bedarf in den Kernel einfügen und wieder entfernen. Mit Kernelmodulen können also Treiber und Schnittstellen, die nicht im Kernel selbst enthalten sind, eingefügt und entfernt werden. Linux bietet einige Befehle zum Verwalten der Kernelmodule.

20.1 Auflisten der geladenen Module mit lsmod und modinfo

Der Befehl **`lsmod`** zeigt die derzeit geladenen Kernelmodule. Dieser Befehl liefert beispielsweise die folgende Ausgabe:

```
tux >  lsmod
Module                  Size  Used by
snd_usb_audio         188416  2
snd_usbmidi_lib        36864  1 snd_usb_audio
hid_plantronics        16384  0
snd_rawmidi            36864  1 snd_usbmidi_lib
snd_seq_device         16384  1 snd_rawmidi
fuse                  106496  3
nfsv3                  45056  1
nfs_acl                16384  1 nfsv3
```

Die Ausgabe ist in drei Spalten gegliedert. Die Spalte `Modul` enthält den Namen der geladenen Module, die Spalte `Größe` entsprechend die Größe der einzelnen Module. Aus der Spalte `Verwendet von` gehen die Anzahl und der Name der verweisenden Module hervor. Diese Liste ist unter Umständen nicht vollständig.

Ausführliche Informationen zu einem bestimmten Kernelmodul erhalten Sie mit dem Befehl **`modinfo`** *`MODULNAME`*, wobei *`MODULNAME`* für den Namen des gewünschten Kernelmoduls steht. Die **`modinfo`**-Binärdatei befindet sich im Verzeichnis `/sbin`, die nicht zur PATH-Umgebungsvariable des Benutzers gehört. Wenn Sie den Befehl **`modinfo`** als normaler Benutzer ausführen, müssen Sie daher den vollständigen Pfad zur Binärdatei angeben:

```
$ /sbin/modinfo kvm
filename:       /lib/modules/4.4.57-18.3-default/kernel/arch/x86/kvm/kvm.ko
license:        GPL
author:         Qumranet
```

```
srcversion:     BDFD8098BEEA517CB75959B
depends:        irqbypass
intree:         Y
vermagic:       4.4.57-18.3-default SMP mod_unload modversions
signer:         openSUSE Secure Boot Signkey
sig_key:        03:32:FA:9C:BF:0D:88:BF:21:92:4B:0D:E8:2A:09:A5:4D:5D:EF:C8
sig_hashalgo:   sha256
parm:           ignore_msrs:bool
parm:           min_timer_period_us:uint
parm:           kvmclock_periodic_sync:bool
parm:           tsc_tolerance_ppm:uint
parm:           lapic_timer_advance_ns:uint
parm:           halt_poll_ns:uint
parm:           halt_poll_ns_grow:int
parm:           halt_poll_ns_shrink:int
```

20.2 Einfügen und Entfernen von Kernelmodulen

Kernelmodule können durchaus mit den Befehlen `insmod` und `rmmod` eingefügt und entfernt werden; allerdings wird das Werkzeug `modprobe` empfohlen. `modprobe` bietet mehrere wichtige Vorteile, beispielsweise die automatische Auflösung von Abhängigkeiten und Einträge in schwarze Listen.

Wenn Sie keine Parameter angeben, wird mit dem Befehl `modprobe` ein angegebenes Kernelmodul installiert. `modprobe` muss mit Root-Berechtigungen ausgeführt werden:

```
tux > sudo modprobe acpi
```

Zum Entfernen eines Kernelmoduls geben Sie den Parameter `-r` an:

```
sudo modprobe -r acpi
```

20.2.1 Automatisches Laden von Kernelmodulen beim Booten

Statt die Kernelmodule manuell zu laden, können Sie sie mit dem Dienst `systemd-modules-load.service` automatisch beim Booten laden lassen. Zum Aktivieren eines Kernelmoduls fügen Sie eine `.conf`-Datei in das Verzeichnis `/etc/modules-load.d/` ein. Die Konfigurationsdatei sollte dabei denselben Namen erhalten wie das Modul selbst, beispielsweise:

```
/etc/modules-load.d/rt2800usb.conf
```

Die Konfigurationsdatei muss den Namen des Kernelmoduls enthalten (z. B. `rt2800usb`).

Mit dem beschriebenen Verfahren laden Sie Kernelmodule ohne Parameter. Falls Sie ein Kernelmodul mit bestimmten Optionen laden möchten, fügen Sie stattdessen eine Konfigurationsdatei in das Verzeichnis `/etc/modprobe.d/` ein. Die Datei muss die Dateinamenerweiterung `.conf` haben. Für den Dateinamen gilt die folgende Namenskonvention: `priority-modulename.conf`, beispielsweise `50-thinkfan.conf`. Die Konfigurationsdatei muss den Namen des Kernelmoduls und die gewünschten Parameter enthalten. Mit dem folgenden Beispielbefehl erstellen Sie eine Konfigurationsdatei mit dem Namen des Kernelmoduls und den zugehörigen Parametern:

```
echo "options thinkpad_acpi fan_control=1" | sudo tee /etc/modprobe.d/thinkfan.conf
```

Anmerkung: Laden der Kernelmodule

Die meisten Kernelmodule werden automatisch durch das System geladen, sobald ein Gerät erkannt wird oder ein Userspace bestimmte Funktionen angefordert. Sie müssen die Module daher nur in seltenen Fällen manuell in `/etc/modules-load.d/` aufnehmen.

20.2.2 Eintragen von Kernelmodulen in schwarze Listen mit modprobe

Wenn ein Kernelmodul in eine schwarze Liste eingetragen wird, kann es beim Booten nicht mehr geladen werden. Dies ist von Nutzen, wenn Sie ein Modul deaktivieren möchten, das vermutlich Probleme auf dem System verursacht. Mit dem Werkzeug `insmod` oder `modprobe` können Sie Kernelmodule, die auf einer schwarzen Liste stehen, dennoch manuell laden.

Zum Eintragen eines Moduls in eine schwarze Liste tragen Sie die Zeile `blacklist` *`MODULNAME`* in die Datei `/etc/modprobe.d/50-blacklist.conf` ein. Beispiel:

```
blacklist nouveau
```

Erzeugen Sie mit dem Befehl **`mkinitrd`** (als root) ein neues `initrd`-Image und booten Sie den Computer neu. Diese Schritte können mit dem folgenden Befehl ausgeführt werden:

```
su
echo "blacklist nouveau" >> /etc/modprobe.d/50-blacklist.conf && mkinitrd && reboot
```

Soll ein Kernel-Modul nur vorübergehend deaktiviert werden, tragen Sie es direkt beim Booten in die Blacklist ein. Drücken Sie hierzu im Bootbildschirm die Taste E. Sie gelangen zu einem minimalen Editor, in dem Sie die Bootparameter bearbeiten können. Wechseln Sie zur Zeile, die wie folgt aufgebaut ist:

```
linux /boot/vmlinuz...splash= silent quiet showopts
```

Hängen Sie den Befehl **modprobe.blacklist=*MODULNAME*** an das Ende der Zeile an. Beispiel:

```
linux /boot/vmlinuz...splash= silent quiet showopts modprobe.blacklist=nouveau
```

Drücken Sie die Taste F10 oder Strg–X. Der Computer wird mit der angegebenen Konfiguration gebootet.

Soll ein Kernelmodul dauerhaft über GRUB in eine Schwarze Liste eingetragen werden, öffnen Sie die Datei `/etc/default/grub` zum Bearbeiten und hängen Sie die Option **modprobe.blacklist=*MODULNAME*** an den Befehl **GRUB_CMD_LINUX** an. Führen Sie dann den Befehl **sudo grub2-mkconfig -o /boot/grub2/grub.cfg** aus, damit die Änderungen in Kraft treten.

21 Gerätemanagement über dynamischen Kernel mithilfe von udev

Der Kernel kann fast jedes Gerät in einem 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. Die Benutzer eines bestimmten Geräts müssen über Änderungen im erkannten Status dieses Geräts informiert werden. udev bietet die erforderliche Infrastruktur, um die Geräteknotendateien und symbolischen Links im `/dev`-Verzeichnis dynamisch zu warten. `udev`-Regeln bieten eine Methode, um externe Werkzeuge an die Ereignisverarbeitung des Kernelgeräts anzuschließen. Auf diese Weise können Sie die `udev`-Gerätebehandlung anpassen, indem Sie bestimmte Skripte hinzufügen, die als Teil der Kernel-Gerätebehandlung ausgeführt werden, oder indem Sie zusätzliche Daten zur Auswertung bei der Gerätebehandlung anfordern und importieren.

21.1 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 Kernels 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 gerendert. Manuell erstellte oder bearbeitete Dateien sind nicht dazu ausgelegt, einen Neustart zu überstehen. Statische Dateien und Verzeichnisse, die unabhängig vom Status des entsprechenden Kernel-Geräts immer im `/dev`-Verzeichnis vorhanden sein sollten, können mit systemd-tmpfiles erstellt werden. Die Konfigurationsdateien finden Sie in `/usr/lib/tmpfiles.d/` und `/etc/tmpfiles.d/`. Weitere Informationen finden Sie auf der man-Seite `systemd-tmpfiles(8)`.

21.2 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`-Dämon liest und parst beim Start alle Regeln aus den Dateien `/usr/lib/udev/rules.d/*.rules` und `/etc/udev/rules.d/*.rules` und lädt sie dauerhaft in den Speicher. Wenn Regeldateien geändert, hinzugefügt oder entfernt werden, kann der Dämon ihre Arbeitsspeicherrepräsentation mithilfe des Befehls **`udevadm control --reload`** wieder laden. Weitere Informationen zu den `udev`-Regeln und deren Syntax finden Sie unter *Abschnitt 21.6, „Einflussnahme auf das Gerätemanagement über dynamischen Kernel mithilfe von* udev*-Regeln“*.

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 symbolische Links hinzufügen oder Programme hinzufügen, die ausgeführt werden sollen, nachdem der Geräteknoten erstellt wurde. Die Treiber-Core-`uevents` werden von einem Kernel-Netlink-Socket empfangen.

21.3 Treiber, Kernel-Module und Geräte

Die Kernel-Bus-Treiber prüfen, ob Geräte vorhanden sind. Für jedes erkannte Gerät erstellt der Kernel eine interne Gerätestruktur, während der Treiber-Core ein uevent an den `udev`-Dämon sendet. 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 Aliasse 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. Dies alles wird automatisch von `udev` ausgelöst.

21.4 Booten und erstes Einrichten des Geräts

Alle Geräteereignisse, die während des Bootvorgangs stattfinden, bevor der `udev`-Daemon ausgeführt wird, gehen verloren. Dies liegt daran, dass die Infrastruktur für die Behandlung dieser Ereignisse sich auf dem Root-Dateisystem befindet und zu diesem Zeitpunkt nicht verfügbar ist. Diesen Verlust fängt der Kernel mit der Datei `uevent` ab, die sich im Geräteverzeichnis jedes Geräts im sysfs-Dateisystem befindet. Durch das Schreiben von `add` in die entsprechende Datei sendet der Kernel dasselbe Ereignis, das während des Bootvorgangs verloren gegangen ist, neu. Eine einfache Schleife über alle `uevent`-Dateien in `/sys` löst alle Ereignisse erneut aus, um die Geräteknoten zu erstellen und die Geräteeinrichtung durchzuführen.

Beispielsweise kann eine USB-Maus, die während des Bootvorgangs vorhanden ist, nicht durch die frühe Bootlogik initialisiert werden, da der Treiber zum entsprechenden Zeitpunkt nicht verfügbar ist. Das Ereignis für die Geräteerkennung ist verloren gegangen und konnte kein Kernel-Modul für das Gerät finden. Anstatt manuell nach angeschlossenen Geräten zu suchen, fordert `udev` alle Geräteereignisse aus dem Kernel an, wenn das Root-Dateisystem verfügbar ist. Das Ereignis für die USB-Maus wird also erneut ausgeführt. Jetzt wird das Kernel-Modul auf dem eingehängten Root-Dateisystem gefunden und die USB-Maus kann initialisiert werden.

Vom 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.

21.5 Überwachen des aktiven udev-Daemons

Das Programm **`udevadm monitor`** kann verwendet werden, um die Treiber-Core-Ereignisse und das Timing der udev-Ereignisprozesse zu visualisieren.

```
UEVENT[1185238505.276660] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1 (usb)
UDEV  [1185238505.279198] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1 (usb)
UEVENT[1185238505.279527] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV  [1185238505.285573] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10 (input)
UDEV  [1185238505.305026] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10 (input)
UEVENT[1185238505.305442] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/mouse2 (input)
UEVENT[1185238505.306440] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/event4 (input)
```

```
UDEV  [1185238505.325384] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/event4 (input)
UDEV  [1185238505.342257] add   /devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/
input10/mouse2 (input)
```

Die `UEVENT`-Zeilen zeigen die Ereignisse an, die der Kernel an Netlink gesendet hat. Die `UDEV`-Zeilen zeigen die fertig gestellten `udev`-Ereignisbehandlungsroutinen an. Das Timing wird in Mikrosekunden angegeben. Die Zeit zwischen `UEVENT` und `UDEV` ist die Zeit, die udev benötigt hat, um dieses Ereignis zu verarbeiten oder der udev-Daemon hat eine Verzögerung bei der Ausführung der Synchronisierung dieses Ereignisses mit zugehörigen und bereits ausgeführten Ereignissen erfahren. Beispielsweise warten Ereignisse für Festplattenpartitionen immer, bis das Ereignis für den primären Datenträger fertig gestellt ist, da die Partitionsereignisse möglicherweise auf die Daten angewiesen sind, die das Ereignis für den primären Datenträger von der Hardware angefordert hat.

`udevadm monitor --env` zeigt die vollständige Ereignisumgebung an:

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

`udev sendet auch Meldungen an syslog.` Die Standard-syslog-Priorität, die steuert, welche Meldungen an syslog gesendet werden, wird in der `udev`-Konfigurationsdatei `/etc/udev/udev.conf` angegeben. Die Protokollpriorität des ausgeführten Dämons kann mit **`udevadm control --log_priority=`** *`LEVEL/NUMBER`* geändert werden.

21.6 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. Ereignisse werden mit allen Regeln abgeglichen, die in den Verzeichnissen `/usr/lib/udev/rules.d/` (Standardregeln) und `/etc/udev/rules.d` (systemspezifische Konfiguration) enthalten sind.

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 symbolische Links hinzufügen oder ein bestimmtes Programm als Teil der Ereignisbehandlung ausführen. Falls keine übereinstimmende Regel gefunden wird, wird der standardmäßige Geräteknotenname verwendet, um den Geräteknoten zu erstellen. Ausführliche Informationen zur Regelsyntax und den bereitgestellten Schlüsseln zum Abgleichen oder Importieren von Daten werden auf der man-Seite von `udev` beschrieben. Nachfolgend finden Sie einige Beispielregeln, die Sie in die grundlegende Regelsyntax von `udev` einführen. Sämtliche Beispielregeln stammen aus dem `udev`-Standardregelsatz, der sich in `/usr/lib/udev/rules.d/50-udev-default.rules` befindet.

BEISPIEL 21.1 udev**-BEISPIELREGELN**

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

Die Regel `Konsole` besteht aus drei Schlüsseln: einem Übereinstimmungsschlüssel (`KERNEL`) und zwei Zuweisungsschlüsseln (`MODE`, `OPTIONS`). Der Übereinstimmungsschlüssel `KERNEL` durchsucht die Geräteliste nach Elementen des Typs `console`. Nur exakte Übereinstimmungen sind gültig und lösen die Ausführung dieser Regel aus. Der Zuweisungsschlüssel `MODE` weist dem

Geräteknoten spezielle Berechtigungen zu, in diesem Fall Lese- und Schreibberechtigung nur für den Eigentümer des Geräts. Der Schlüssel `OPTIONS` bewirkt, dass diese Regel auf Geräte dieses Typs als letzte Regel angewendet wird. Alle nachfolgenden Regeln, die mit diesem Gerätetyp übereinstimmen, werden nicht mehr angewendet.

Die Regel `serial devices` steht in `50-udev-default.rules` nicht mehr zur Verfügung; es lohnt sich jedoch, sie sich dennoch anzusehen. Sie besteht aus zwei Übereinstimmungsschlüsseln (`KERNEL` und `ATTRS`) und einem Zuweisungsschlüssel (`SYMLINK`). Der Übereinstimmungsschlüssel `KERNEL` sucht nach allen Geräten des Typs `ttyUSB`. Durch den Platzhalter `*` trifft dieser Schlüssel auf mehrere dieser Geräte zu. Der zweite Übereinstimmungsschlüssel (`ATTRS`) überprüft, ob die Attributdatei `product` in `sysfs` der jeweiligen `ttyUSB`-Geräte eine bestimmte Zeichenkette enthält. Der Zuweisungsschlüssel `SYMLINK` bewirkt, dass dem Gerät unter `/dev/pilot` ein symbolischer Link hinzugefügt wird. Der Operator dieses Schlüssels (`+=`) weist udev an, diese Aktion auch dann auszuführen, wenn dem Gerät bereits durch frühere (oder auch erst durch spätere) Regeln andere symbolische Links hinzugefügt wurden. Die Regel wird nur angewendet, wenn die Bedingungen beider Übereinstimmungsschlüssel erfüllt sind.

Die Regel `printer` gilt nur für USB-Drucker. Sie enthält zwei Übereinstimmungsschlüssel (`SUBSYSTEM` und `KERNEL`), die beide zutreffen müssen, damit die Regel angewendet wird. Die drei Zuweisungsschlüssel legen den Namen dieses Gerätetyps fest (`NAME`), die Erstellung symbolischer Gerätelinks (`SYMLINK`) sowie die Gruppenmitgliedschaft dieses Gerätetyps (`GROUP`). Durch den Platzhalter `*` im Schlüssel `KERNEL` trifft diese Regel auf mehrere `lp`-Druckergeräte zu. Sowohl der Schlüssel `NAME` als auch der Schlüssel `SYMLINK` verwenden Ersetzungen, durch die der Zeichenkette der interne Gerätename hinzugefügt wird. Der symbolische Link für den ersten `lp`-USB-Drucker würde zum Beispiel `/dev/usblp0` lauten.

Die Regel `kernel firmware loader` weist udev an, während der Laufzeit weitere Firmware mittels eines externen Hilfsskripts zu laden. Der Übereinstimmungsschlüssel `SUBSYSTEM` sucht nach dem Subsystem `firmware`. Der Schlüssel `ACTION` überprüft, ob bereits Geräte des Subsystems `firmware` hinzugefügt wurden. Der Schlüssel `RUN+=` löst die Ausführung des Skripts `firmware.sh` aus, das die noch zu ladende Firmware lokalisiert.

Die folgenden allgemeinen Eigenschaften treffen auf alle Regeln zu:

- Jede Regel besteht aus einem oder mehreren, durch Kommas getrennten Schlüssel-/Wertepaaren.
- Die Aktion eines Schlüssels wird durch seinen Operator festgelegt. `udev`-Regeln unterstützen verschiedene Operatoren.
- Jeder angegebene Wert muss in Anführungszeichen eingeschlossen sein.

- Jede Zeile der Regeldatei stellt eine Regel dar. Falls eine Regel länger als eine Zeile ist, verbinden Sie die Zeilen wie bei jeder anderen Shell-Syntax mit `\`.
- `udev`-Regeln unterstützen Shell-typische Übereinstimmungsregeln für die Schemata `*`, `?` und `[]`.
- `udev-Regeln unterstützen Ersetzungen.`

21.6.1 Verwenden von Operatoren in udev-Regeln

Bei der Erstellung von Schlüsseln stehen Ihnen je nach gewünschtem Schlüsseltyp mehrere Operatoren zur Auswahl. Übereinstimmungsschlüssel werden in der Regel zum Auffinden eines Wertes verwendet, der entweder mit dem Suchwert übereinstimmt oder explizit nicht mit dem gesuchten Wert übereinstimmt. Übereinstimmungsschlüssel enthalten einen der folgenden Operatoren:

`==`
: Suche nach übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

`!=`
: Suche nach nicht übereinstimmendem Wert. Wenn der Schlüssel ein Suchschema enthält, sind alle Ergebnisse gültig, die mit diesem Schema übereinstimmen.

Folgende Operatoren können für Zuweisungsschlüssel verwendet werden:

`=`
: Weist einem Schlüssel einen Wert zu. Wenn der Schlüssel zuvor aus einer Liste mit mehreren Werten bestand, wird der Schlüssel durch diesen Operator auf diesen Einzelwert zurückgesetzt.

`+=`
: Fügt einem Schlüssel, der eine Liste mehrerer Einträge enthält, einen Wert hinzu.

`:=`
: Weist einen endgültigen Wert zu. Eine spätere Änderung durch nachfolgende Regeln ist nicht möglich.

21.6.2 Verwenden von Ersetzungen in udev-Regeln

`udev`-Regeln unterstützen sowohl Platzhalter als auch Ersetzungen. Diese setzen Sie genauso ein wie in anderen Skripten. Folgende Ersetzungen können in `udev`-Regeln verwendet werden:

`%r`, `$root`
: Standardmäßig das Geräteverzeichnis `/dev`.

`%p`, `$devpath`
: Der Wert von `DEVPATH`.

`%k`, `$kernel`
: Der Wert von `KERNEL` oder der interne Gerätename.

`%n`, `$number`
: Die Gerätenummer.

`%N`, `$tempnode`
: Der temporäre Name der Gerätedatei.

`%M`, `$major`
: Die höchste Nummer des Geräts.

`%m`, `$minor`
: Die niedrigste Nummer des Geräts.

`%s{`*`ATTRIBUTE`*`}`, `$attr{`*`ATTRIBUTE`*`}`
: Der Wert eines `sysfs`-Attributs (das durch *`ATTRIBUTE`* festgelegt ist).

`%E{`*`VARIABLE`*`}`, `$env{`*`VARIABLE`*`}`
: Der Wert einer Umgebungsvariablen (die durch *`VARIABLE`* festgelegt ist).

`%c`, `$result`
: Die Ausgabe von `PROGRAM`.

`%%`
: Das `%`-Zeichen.

`$$`
: Das `$`-Zeichen.

21.6.3 Verwenden von udev-Übereinstimmungsschlüsseln

Übereinstimmungsschlüssel legen Bedingungen fest, die erfüllt sein müssen, damit eine `udev`-Regel angewendet werden kann. Folgende Übereinstimmungsschlüssel sind verfügbar:

`ACTION`
: Der Name der Ereignisaktion, z. B. `add` oder `remove` beim Hinzufügen oder Entfernen eines Geräts.

`DEVPATH`
: Der Gerätepfad des Ereignisgeräts, zum Beispiel `DEVPATH=/bus/pci/drivers/ipw3945` für die Suche nach allen Ereignissen in Zusammenhang mit dem Treiber ipw3945.

`KERNEL`
: Der interne Name (Kernel-Name) des Ereignisgeräts.

`SUBSYSTEM`
: Das Subsystem des Ereignisgeräts, zum Beispiel `SUBSYSTEM=usb` für alle Ereignisse in Zusammenhang mit USB-Geräten.

`ATTR{`*`DATEINAME`*`}`
: `sysfs`-Attribute des Ereignisgeräts. Für die Suche nach einer Zeichenkette im Attributdateinamen `vendor` können Sie beispielsweise `ATTR{vendor}==„On[sS]tream“` verwenden.

`KERNELS`
: Weist `udev` an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätenamen zu durchsuchen.

`SUBSYSTEMS`
: Weist `udev` an, den Gerätepfad aufwärts nach einem übereinstimmenden Geräte-Subsystemnamen zu durchsuchen.

`DRIVERS`
: Weist `udev` an, den Gerätepfad aufwärts nach einem übereinstimmenden Gerätetreibernamen zu durchsuchen.

`ATTRS{`*`DATEINAME`*`}`
: Weist `udev` an, den Gerätepfad aufwärts nach einem Gerät mit übereinstimmenden `sysfs`-Attributwerten zu durchsuchen.

`ENV{SCHLÜSSEL}`

Der Wert einer Umgebungsvariablen, zum Beispiel `ENV{ID_BUS}=„ieee1394` für die Suche nach allen Ereignissen in Zusammenhang mit der FireWire-Bus-ID.

`PROGRAM`

Weist `udev` an, ein externes Programm auszuführen. Damit es erfolgreich ist, muss das Programm mit Beendigungscode Null abschließen. Die Programmausgabe wird in STDOUT geschrieben und steht dem Schlüssel `RESULT` zur Verfügung.

`RESULT`

Überprüft die Rückgabezeichenkette des letzten `PROGRAM`-Aufrufs. Diesen Schlüssel können Sie entweder sofort der Regel mit dem `PROGRAM`-Schlüssel hinzufügen oder erst einer nachfolgenden Regel.

21.6.4 Verwenden von udev-Zuweisungsschlüsseln

Im Gegensatz zu den oben beschriebenen Übereinstimmungsschlüsseln beschreiben Zuweisungsschlüssel keine Bedingungen, die erfüllt werden müssen. Sie weisen den Geräteknoten, die von `udev` gewartet werden, Werte, Namen und Aktionen zu.

`NAME`

Der Name des zu erstellenden Geräteknotens. Nachdem der Knotenname durch eine Regel festgelegt wurde, werden alle anderen Regeln mit dem Schlüssel `NAME`, die auf diesen Knoten zutreffen, ignoriert.

`SYMLINK`

Der Name eines symbolischen Links, der dem zu erstellenden Knoten hinzugefügt werden soll. Einem Geräteknoten können mittels mehrerer Zuweisungsregeln symbolische Links hinzugefügt werden. Ebenso können Sie aber mehrere symbolische Links für einen Knoten auch in einer Regel angeben. Die Namen der einzelnen symbolischen Links müssen in diesem Fall jeweils durch ein Leerzeichen getrennt sein.

`OWNER, GROUP, MODE`

Die Berechtigungen für den neuen Geräteknoten. Die hier angegebenen Werte überschreiben sämtliche kompilierten Werte.

`ATTR{SCHLÜSSEL}`

Gibt einen Wert an, der in ein `sysfs`-Attribut des Ereignisgeräts geschrieben werden soll. Wenn der Operator `==` verwendet wird, überprüft dieser Schlüssel, ob der Wert eines `sysfs`-Attributs mit dem angegebenen Wert übereinstimmt.

`ENV{SCHLÜSSEL}`

Weist `udev` an, eine Umgebungsvariable zu exportieren. Wenn der Operator `==` verwendet wird, überprüft dieser Schlüssel, ob der Wert einer Umgebungsvariable mit dem angegebenen Wert übereinstimmt.

`RUN`

Weist `udev` an, der Liste der für dieses Gerät auszuführenden Programme ein Programm hinzuzufügen. Sie sollten hier nur sehr kurze Aufgaben angeben. Anderenfalls laufen Sie Gefahr, dass weitere Ereignisse für dieses Gerät blockiert werden.

`LABEL`

Fügt der Regel eine Bezeichnung hinzu, zu der ein `GOTO` direkt wechseln kann.

`GOTO`

Weist `udev` an, mehrere Regeln auszulassen und direkt mit der Regel fortzufahren, die die von `GOTO` angegebene Bezeichnung enthält.

`IMPORT{TYP}`

Lädt Variablen in die Ereignisumgebung, beispielsweise die Ausgabe eines externen Programms. `udev` kann verschiedene Variablentypen importieren. Wenn kein Typ angegeben ist, versucht `udev` den Typ anhand des ausführbaren Teils der Dateiberechtigungen selbst zu ermitteln.

- `program` weist `udev` an, ein externes Programm auszuführen und dessen Ausgabe zu importieren.
- `file` weist `udev` an, eine Textdatei zu importieren.
- `parent` weist `udev` an, die gespeicherten Schlüssel des übergeordneten Geräts zu importieren.

`WAIT_FOR_SYSFS`

Weist `udev` an, auf die Erstellung der angegebenen `sysfs`-Datei für ein bestimmtes Gerät zu warten. Beispiel: `WAIT_FOR_SYSFS=„ioerr_cnt“` fordert `udev` auf, so lange zu warten, bis die Datei `ioerr_cnt` erstellt wurde.

`OPTIONEN`

Der Schlüssel `OPTION` kann mehrere Werte haben:

- `last_rule` weist `udev` an, alle nachfolgenden Regeln zu ignorieren.
- `ignore_device` weist `udev` an, dieses Ereignis komplett zu ignorieren.
- `ignore_remove` weist `udev` an, alle späteren Entfernungsereignisse für dieses Gerät zu ignorieren.
- `all_partitions` weist `udev` an, für alle vorhandenen Partitionen eines Blockgeräts Geräteknoten zu erstellen.

21.7 Permanente Gerätebenennung

Das dynamische Geräteverzeichnis und die Infrastruktur für die `udev`-Regeln ermöglichen die Bereitstellung von stabilen Namen für alle Laufwerke unabhängig von ihrer Erkennungsreihenfolge oder der für das Gerät verwendeten Verbindung. Jedes geeignete Blockgerät, das der Kernel erstellt, wird von Werkzeugen mit speziellen Kenntnissen über bestimmte Busse, Laufwerktypen oder Dateisysteme untersucht. Gemeinsam mit dem vom dynamischen Kernel bereitgestellten Geräteknotennamen 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
```

21.8 Von udev verwendete Dateien

`/sys/*`

Virtuelles, vom Linux-Kernel bereitgestelltes Dateisystem, das alle zur Zeit bekannten Geräte exportiert. Diese Informationen werden von `udev` zur Erstellung von Geräteknoten in `/dev` verwendet.

`/dev/*`

Dynamisch erstellte Geräteknoten und mit systemd-tmpfiles erstellte statische Inhalte. Weitere Informationen finden Sie auf der man-Seite `systemd-tmpfiles(8)`.

Die folgenden Dateien und Verzeichnisse enthalten die entscheidenden Elemente der `udev`-Infrastruktur:

`/etc/udev/udev.conf`

Wichtigste `udev`-Konfigurationsdatei.

`/etc/udev/rules.d/*`

Systemspezifische `udev`-Ereigniszuordnungsregeln Hier können Sie benutzerdefinierte Regeln hinzufügen, um die Standardregeln aus `/usr/lib/udev/rules.d/*` zu bearbeiten oder zu überschreiben.

Dateien werden in alphanumerischer Reihenfolge geparst. Regeln aus Dateien mit höherer Priorität modifizieren oder überschreiben Regeln mit niedrigerer Priorität. Je niedriger die Zahl, desto höher die Priorität.

`/usr/lib/udev/rules.d/*`

Standard-`udev`-Ereigniszuordnungsregeln Die Dateien in diesem Verzeichnis gehören zu Paketen und werden durch Aktualisierungen überschrieben. Hier keinesfalls Dateien hinzufügen, entfernen oder bearbeiten; verwenden Sie stattdessen `/etc/udev/rules.d`.

`/usr/lib/udev/*`

Von den `udev`-Regeln aufgerufene Helferprogramme.

`/usr/lib/tmpfiles.d/` and `/etc/tmpfiles.d/`

Verantwortlich für statische `/dev`-Inhalte.

21.9 Weiterführende Informationen

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

`udev`

Allgemeine Informationen zu `udev`, Schlüsseln, Regeln und anderen wichtigen Konfigurationsbelangen.

`udevadm`

`udevadm` kann dazu verwendet werden, das Laufzeitverhalten von `udev` zu kontrollieren, Kernel-Ereignisse abzurufen, die Ereigniswarteschlange zu verwalten und einfache Methoden zur Fehlersuche bereitzustellen.

`udevd`

Informationen zum `udev`-Ereignisverwaltungs-Daemon.

22 Live-Patching des Linux-Kernels mithilfe von kGraft

In diesem Dokument werden die Grundlagen der Live-Patching-Technologie kGraft erläutert und Sie finden hier Richtlinien für den SLE Live Patching-Dienst.

Die Live-Patching-Technologie kGraft führt das Patching zur Laufzeit für den LinuxKernel aus, ohne den Kernel anhalten zu müssen. So erzielen Sie die maximale Betriebszeit (und damit die maximale Verfügbarkeit) des Systems, was insbesondere bei unternehmenswichtigen Systemen von Bedeutung ist. Durch das dynamische Patching des Kernels können Benutzer auch kritische Sicherheitsaktualisierungen installieren, ohne bis zu einer geplanten Ausfallzeit warten zu müssen.

Ein kGraft-Patch ist ein Kernel-Modul, das ganze Funktionen im Kernel ersetzt. kGraft bietet hauptsächlich eine kernelinterne Infrastruktur für die Integration des gepatchten Codes mit dem Kernel-Basiscode zur Laufzeit.

Der SLE Live Patching-Dienst wird zusätzlich zur normalen SUSE Linux Enterprise Server-Wartung erbracht. kGraft-Patches, die über SLE Live Patching verteilt werden, ergänzen die normalen SLES-Wartungsaktualisierungen. SLE Live Patching kann über herkömmliche Aktualisierungsstapel und -verfahren bereitgestellt werden.

Die Angaben in diesem Dokument gelten für die AMD64/Intel 64- und POWER-Architekturen. Sollten Sie eine andere Architektur nutzen, können die Verfahren von den hier beschriebenen abweichen.

22.1 Vorteile von kGraft

Das Live-Kernel-Patching mit kGraft eignet sich insbesondere als rasche Reaktion in Notfällen (wenn schwere Schwachstellen bekannt sind und sobald wie möglich behoben werden sollen oder wenn schwere Probleme mit der Systemstabilität vorliegen, für die eine Fehlerbehebung bekannt ist). In geplanten Aktualisierungen, bei denen die Zeit keine entscheidende Rolle spielt, kommt dieses Verfahren nicht zum Einsatz.

Typische Anwendungsfälle für kGraft sind beispielsweise Speicherdatenbanken mit enormen Mengen an Arbeitsspeicher, bei denen eine Bootdauer von 15 Minuten oder länger nicht ungewöhnlich ist, umfangreiche Simulationen, die mehrere Wochen oder Monate ohne Neustart ausgeführt werden müssen, oder Infrastrukturbausteine, die ununterbrochene Dienste für viele Kunden erbringen.

Als Hauptvorteil von kGraft muss der Kernel unter keinen Umständen angehalten werden, nicht einmal für kurze Zeit.

Ein kGraft-Patch ist ein `.ko`-Kernel-Modul in einem RPM-Paket. Der Patch wird mit dem Befehl **`insmod`** in den Kernel eingefügt, sobald das Paket installiert oder aktualisiert wird. kGraft ersetzt ganze Funktionen im Kernel, selbst wenn sie gerade ausgeführt werden. Ein aktualisiertes kGraft-Modul kann bei Bedarf einen vorhandenen Patch ersetzen.

Zudem ist kGraft schlank – es ist nur wenig Code erforderlich, da andere standardmäßige Linux-Technologien eingebunden werden.

22.2 Low-Level-Funktion von kGraft

kGraft führt das Patching über die ftrace-Infrastruktur aus. Im Folgenden wird die Implementierung auf der AMD64-/Intel-64-Architektur beschrieben.

Zum Patchen einer Kernel-Funktion benötigt kGraft etwas Platz am Anfang der Funktion, damit ein Sprung zu einer neuen Funktion eingefügt werden kann. Dieser Platz wird bei der Kernel-Kompilierung durch GCC mit aktivierter Funktionsprofilerstellung zugewiesen. Insbesondere wird eine 5 Byte umfassende Aufrufanweisung an den Anfang der Kernel-Funktionen eingebracht. Beim Booten eines derart ausgerüsteten Kernels werden die Profilerstellungsaufrufe durch 5-Byte-Nulloperationsanweisungen (NOP-Anweisungen) ersetzt.

Zu Beginn des Patching-Vorgangs wird das erste Byte durch die INT3-(Haltepunkt-)Anweisung ersetzt. So wird die Atomarität des 5-Byte-Anweisungsersatzes sichergestellt. Die weiteren vier Byte werden durch die Adresse zur neuen Funktion ersetzt. Schließlich wird das erste Byte durch den JMP-Opcode (Long Jump) ersetzt.

Mithilfe von IPI-NMIs (Inter-Processor Non-Maskable Interrupts) werden spekulative Decodierungswarteschlangen anderer CPUs im System entleert. So kann die Umstellung auf die neue Funktion erfolgen, ohne den Kernel anhalten zu müssen, nicht einmal für äußerst kurze Zeit. Die Unterbrechungen durch die IPI-NMIs messen sich nach Millisekunden und gelten nicht als Systemunterbrechungen, da der Kernel trotz dieser Unterbrechungen weiterläuft.

Aufrufer werden nicht gepatcht. Stattdessen werden die NOPs des Aufgerufenen durch ein JMP zur neuen Funktion ersetzt. JMP-Anweisungen bleiben dauerhaft erhalten. Hierdurch sind die Funktionszeiger gesichert (auch in Strukturen) und alte Daten müssen nicht für den Fall aufgehoben werden, dass der Patch rückgängig gemacht wird.

Diese Schritte allein würden allerdings nicht ausreichen: Die Funktionen werden nichtatomar ausgetauscht; eine neue, fehlerfreie Funktion in einem Teil des Kernels könnte dennoch eine alte Funktion an anderer Stelle aufrufen oder umgekehrt. Wenn die Semantik der Funktionsschnittstellen im Patch geändert würde, wäre Chaos unvermeidbar.

Bis alle Funktionen ersetzt sind, gilt daher ein „Trampolinverfahren“ ähnlich RCU (Read-Copy-Update, Lesen-Kopieren-Aktualisieren), damit die einzelnen Userspace-Threads, Kernel-Threads und Kernel-Interrupts fortlaufend einheitliche „Weltsicht“ behalten. Bei jedem Kernel-Ein- und -Ausstieg wird ein threadspezifisches Flag gesetzt. So ist gewährleistet, dass eine alte Funktion stets eine andere alte Funktion aufruft und eine neue Funktion stets eine neue. Sobald für alle Prozesse das Flag für das „neue Universum“ gesetzt ist, ist das Patching abgeschlossen, die Trampoline können abgebaut werden und der Code kann mit voller Geschwindigkeit und ohne Leistungseinbußen laufen, abgesehen von einem extrem langen Sprung bei den einzelnen gepatchten Funktionen.

22.3 Installieren von kGraft-Patches

In diesem Abschnitt werden die Aktivierung der Live Patching-Erweiterung für SUSE Linux Enterprise sowie die Installation der kGraft-Patches beschrieben.

22.3.1 Aktivierung von SLE Live Patching

So aktivieren Sie SLE Live Patching auf dem System:

1. Falls das SLES-System noch nicht registriert ist, holen Sie dies jetzt nach. Die Registrierung kann wahlweise während der Systeminstallation oder nachträglich mit dem YaST-Modul *Produktregistrierung* (`yast2 registration`) ausgeführt werden. Klicken Sie nach der Registrierung auf *Ja*. Die Liste der verfügbaren Online-Aktualisierungen wird angezeigt.
   Wenn das SLES-System bereits registriert, SLE Live Patching jedoch noch nicht aktiviert ist, öffnen Sie das YaST-Modul *Produktregistrierung* (`yast2 registration`) und klicken Sie auf *Erweiterungen auswählen*.

2. Wählen Sie in der Liste der verfügbaren Erweiterungen den Eintrag *SUSE Linux Enterprise Live Patching 12* und klicken Sie auf *Weiter*.

3. Bestätigen Sie die Lizenzvereinbarung und klicken Sie auf *Weiter*.

4. Geben Sie den Registrierungscode für SLE Live Patching ein und klicken Sie auf *Weiter*.

5. Prüfen Sie die *Installationszusammenfassung* und die ausgewählten *Schemata*. Das Schema `Live Patching` muss zur Installation ausgewählt sein.

6. Schließen Sie die Installation mit *Akzeptieren* ab. Hiermit werden die grundlegenden kGraft-Komponenten zusammen mit dem anfänglichen Live-Patch auf dem System installiert.

22.3.2 Aktualisieren des Systems

1. SLE Live Patching-Aktualisierungen werden in einer Form verteilt, bei der die Patches mithilfe von standardmäßigen SLE-Aktualisierungsstapeln angewendet werden können. Der anfängliche Live-Patch kann mit **`zypper patch`**, mit der YaST-Online-Aktualisierung oder einem gleichwertigen Verfahren aktualisiert werden.

2. Der Kernel wird bei der Installation des Pakets automatisch gepatcht. Die Aufrufe der alten Kernel-Funktionen werden jedoch erst dann vollständig beseitigt, wenn alle Prozesse aus dem Ruhezustand aufgeweckt wurden und der Aktualisierung nicht mehr im Wege stehen. Dies kann sehr lange dauern. Dennoch gelten Prozesse im Ruhezustand, die die alten Kernel-Funktionen nicht nutzen, nicht als Sicherheitsrisiko. In der aktuellen Version von kGraft kann der nächste kGraft-Patch dennoch erst dann angewendet werden, wenn alle Prozesse die Kernel-Userspace-Grenze überschritten haben, sodass die gepatchten Funktionen aus dem vorherigen Patch nicht mehr genutzt werden.
   Der globale Patching-Status ist aus dem Flag in `/sys/kernel/kgraft/in_progress` ersichtlich. Der Wert `1` bedeutet, dass Prozesse im Ruhezustand vorliegen, die noch aufgeweckt werden müssen. (Der Patching-Vorgang ist also noch nicht abgeschlossen.) Der Wert `0` bedeutet, dass alle Prozesse ausschließlich die gepatchten Funktionen nutzen und dass der Patching-Vorgang abgeschlossen ist. Alternativ rufen Sie diese Angaben mit dem Befehl **`kgr status`** ab.

Sie können das Flag auch für einzelne Prozesse ermitteln. Prüfen Sie jeweils die Zahl unter `/proc/PROZESSNUMMER/kgr_in_progress` für die betreffenden Prozesse. Der Wert `1` weist wiederum auf Prozesse im Ruhezustand hin, die noch aufgeweckt werden müssen. Alternativ rufen Sie die Liste der Prozesse im Ruhezustand mit dem Befehl **`kgr blocking`** ab.

22.4 Patch-Lebenszyklus

Mit **`zypper lifecycle`** rufen Sie das Ablaufdatum der Live-Patches ab. Prüfen Sie, ob das Paket `lifecycle-data-sle-live-patching` installiert ist.

```
tux > zypper lifecycle

Product end of support
Codestream: SUSE Linux Enterprise Server 12             2024-10-31
SUSE Linux Enterprise Server 12 SP2                     n/a*

Extension end of support
SUSE Linux Enterprise Live Patching                     2017-10-31

Package end of support if different from product:
SUSEConnect                                Now, installed 0.2.41-18.1, update available
 0.2.42-19.3.1
apache2-utils                              Now


*) See https://www.suse.com/lifecycle  for latest information
```

Sobald das Ablaufdatum eines Patches erreicht ist, werden keine weiteren Live-Patches für diese Kernelversion mehr bereitgestellt. Planen Sie die Aktualisierung des Kernels rechtzeitig vor dem Ende des Live-Patch-Lebenszyklus ein.

22.5 Entfernen eines kGraft-Patches

So entfernen Sie einen kGraft-Patch:

1. Entfernen Sie zunächst den Patch selbst mit Zypper:

   ```
   zypper rm kgraft-patch-3_12_32-25-default
   ```

2. Booten Sie dann den Computer neu.

22.6 Hängengebliebene Kernel-Ausführungsthreads

Die Kernel-Threads müssen auf kGraft vorbereitet werden. Software von Drittanbietern ist unter Umständen nicht für die kGraft-Einführung bereit und die Kernel-Module dieser Software erzeugen ggf. Kernel-Ausführungsthreads. Diese Threads blockieren den Patching-Vorgang auf Dauer. Als Notmaßnahme bietet kGraft die Möglichkeit, den Patching-Prozess zwangsweise zu beenden, ohne abzuwarten, bis alle Ausführungsthreads den Sicherheitskontrollpunkt überschritten haben. Schreiben Sie hierzu den Wert `0` in `/sys/kernel/kgraft/in_progress`. Wenden Sie sich an den SUSE-Support, bevor Sie dieses Verfahren ausführen.

22.7 Das Werkzeug **kgr**

Verschiedene kGraft-Verwaltungsaufgaben lassen sich mit dem Werkzeug **kgr** vereinfachen. Verfügbare Befehle:

kgr status
: Zeigt den Gesamtstatus des kGraft-Patching (`ready` oder `in_progress`).

kgr patches
: Zeigt eine Liste der geladenen kGraft-Patches.

kgr blocking
: Zeigt eine Liste der Prozesse, die das Beenden des kGraft-Patching verhindern. Standardmäßig werden nur die PIDs aufgeführt. Mit `-v` werden die Kommandozeilen ausgegeben (falls vorhanden). Mit einem weiteren Schalter `-v` werden auch Stapel-Traces angegeben.

Weitere Informationen finden Sie unter **man kgr**.

22.8 Umfang der kGraft-Technologie

kGraft beruht auf dem Ersetzen von Funktionen. Die Datenstruktur kann mit kGraft nur indirekt geändert werden. Änderungen an der Kernel-Datenstruktur verlangen daher besondere Vorsicht; bei zu großen Änderungen muss das System ggf. neu gebootet werden. Außerdem kann kGraft unter Umständen nicht mit Situationen umgehen, in denen der alte Kernel von einem Compiler kompiliert wird und der neue Patch von einem zweiten Compiler.

Aufgrund der Funktionsweise von kGraft ist die Unterstützung für Drittanbieter-Module, die Kernel-Threads erzeugen, begrenzt.

22.9 Umfang von SLE Live Patching

SLE Live Patching umfasst Fehlerbehebungen für SUSE-Sicherheitsanfälligkeiten (Common Vulnerability Scoring System, CVSS) ab Stufe 7 sowie Fehlerbehebungen hinsichtlich der Systemstabilität oder Datenbeschädigung. Unter Umständen kann nicht für alle Fehlerbehebungen, die die obigen Kriterien erfüllen, ein Live-Patch bereitgestellt werden. SUSE behält sich das Recht vor, Fehlerbehebungen zu überspringen, wenn die Erzeugung eines Kernel-Live-Patches aus technischen Gründen nicht praktikabel ist. Weitere Informationen zu CVSS 3.0 als Grundlage für die SUSE CVSS-Einstufung finden Sie unter https://www.first.org/cvss/.

22.10 Interaktion mit den Supportprozessen

Wenn Sie gemeinsam mit dem SUSE-Support bestimmte technische Probleme beheben, erhalten Sie ggf. einen sogenannten PTF (Program Temporary Fix, temporäre Programm-Fehlerbehebung). PTFs können für verschiedene Pakete ausgegeben werden, z. B. für Pakete, die die Grundlage von SLE Live Patching bilden.

Die kGraft-PTFs, die die Bedingungen im vorherigen Abschnitt erfüllen, können wie gewohnt installiert werden; SUSE sorgt dabei dafür, dass das betreffende System nicht neu gebootet werden muss und dass künftige Live-Aktualisierungen problemlos angewendet werden können.

PTFs für den Basis-Kernel unterbrechen den Live-Patching-Vorgang. Erstens: Wenn Sie den PTF-Kernel installieren, müssen Sie das System neu booten, da der Kernel als Ganzes nicht zur Laufzeit ersetzt werden kann. Zweitens: Ein zweiter Neustart ist erforderlich, damit der PTF durch normale Wartungsaktualisierungen ersetzt wird, für die die Live-Patches ausgegeben werden.

PTFs für andere Pakete in SLE Live Patching können wie reguläre PTFs mit den üblichen Zusicherungen behandelt werden.

23 Spezielle Systemfunktionen

In diesem Kapitel erhalten Sie zunächst Informationen zu den verschiedenen Softwarepaketen, zu den virtuellen Konsolen und zur Tastaturbelegung. Hier finden Sie Hinweise zu Software-Komponenten, wie `bash`, `cron` und `logrotate`, da diese im Laufe der letzten Veröffentlichungszyklen geändert oder verbessert wurden. Selbst wenn sie nur klein sind oder als nicht besonders wichtig eingestuft werden, sollten die Benutzer ihr Standardverhalten ändern, da diese Komponenten häufig eng mit dem System verbunden sind. Das Kapitel endet mit einem Abschnitt mit sprach- und landesspezifischen Einstellungen (I18N und L10N).

23.1 Informationen zu speziellen Softwarepaketen

Die Programme `bash`, `cron`, `logrotate`, `locate`, `ulimit` und `free` spielen für Systemadministratoren und viele Benutzer eine wichtige Rolle. man-Seiten und info-Seiten sind hilfreiche Informationsquellen zu Befehlen, sind jedoch nicht immer verfügbar. GNU Emacs ist ein beliebter konfigurierbarer Texteditor.

23.1.1 Das Paket `bash` und `/etc/profile`

Bash ist die Standard-System-Shell. Wenn sie als Anmelde-Shell verwendet wird, werden mehrere Initialisierungsdateien gelesen. Bash verarbeitet die entsprechenden Informationen in der Reihenfolge dieser Liste:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Nehmen Sie benutzerdefinierte Einstellungen in `~/.profile` oder `~/.bashrc` vor. Um die richtige Verarbeitung der Dateien zu gewährleisten, müssen die Grundeinstellungen aus `/etc/skel/.profile` oder `/etc/skel/.bashrc` in das Home-Verzeichnis des Benutzers kopiert wer-

den. 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.

23.1.2 Das cron-Paket

Mit Cron lassen sich automatisch zu bestimmten Zeitpunkten Befehle im Hintergrund ausführen. cron greift auf speziell formatierte Zeittabellen zu, wobei bereits mehrere standardmäßige Tabellen in diesem Werkzeug enthalten sind. Bei Bedarf können die Benutzer auch benutzerdefinierte Tabellen angeben.

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 23.1, „Eintrag in /etc/crontab“*, wird `root` eingegeben. Die paketspezifischen Tabellen in `/etc/cron.d` weisen alle dasselbe Format auf. Informationen hierzu finden Sie auf der man-Seite zu **`cron`** (**`man cron`**).

BEISPIEL 23.1 EINTRAG IN /ETC/CRONTAB

```
1-59/5 * * * *   root   test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Sie können `/etc/crontab` nicht bearbeiten, indem Sie den Befehl **`crontab -e`** bearbeiten. Die Datei muss direkt in einem Editor geladen, geändert und dann gespeichert werden.

Einige Pakte installieren Shell-Skripten in die Verzeichnisse `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly`, deren Ausführung durch `/usr/lib/cron/run-crons` gesteuert wird. `/usr/lib/cron/run-crons` wird alle 15 Minuten von der Haupttabelle (`/etc/crontab`) ausgeführt. Hiermit wird gewährleistet, dass vernachlässigte Prozesse zum richtigen Zeitpunkt ausgeführt werden können.

Um die Skripten `hourly`, `daily` oder andere Skripten für regelmäßige Wartungsarbeiten zu benutzerdefinierten Zeiten auszuführen, entfernen Sie regelmäßig die Zeitstempeldateien mit `/etc/crontab`-Einträgen (siehe *Beispiel 23.2, „/etc/crontab: Entfernen der Zeitstempeldateien“* – u. a. wird `hourly` vor jeder vollen Stunde und `daily` einmal täglich um 2:14 Uhr entfernt).

BEISPIEL 23.2 /ETC/CRONTAB: ENTFERNEN DER ZEITSTEMPELDATEIEN

```
59 *  * * *     root  rm -f /var/spool/cron/lastrun/cron.hourly
14 2  * * *     root  rm -f /var/spool/cron/lastrun/cron.daily
29 2  * * 6     root  rm -f /var/spool/cron/lastrun/cron.weekly
44 2  1 * *     root  rm -f /var/spool/cron/lastrun/cron.monthly
```

Sie können auch `DAILY_TIME` in `/etc/sysconfig/cron` auf die Zeit einstellen, zu der `cron.daily` gestartet werden soll. Mit `MAX_NOT_RUN` stellen Sie sicher, dass die täglichen Aufgaben auch dann ausgeführt werden, wenn der Computer zur angegebenen `DAILY_TIME` und auch eine längere Zeit danach nicht eingeschaltet ist. Die maximale Einstellung von `MAX_NOT_RUN` sind 14 Tage.

Die täglichen Systemwartungsaufträge werden zum Zwecke der Übersichtlichkeit auf mehrere Skripts verteilt. Sie sind im Paket `aaa_base` enthalten. `/etc/cron.daily` enthält beispielsweise die Komponenten `suse.de-backup-rpmdb`, `suse.de-clean-tmp` oder `suse.de-cron-local`.

23.1.3 Stoppen der Cron-Statusmeldungen

Um die Email-Flut einzudämmen, die durch die Cron-Statusmeldungen entsteht, wird der Standardwert für `SEND_MAIL_ON_NO_ERROR` in `/etc/sysconfig/cron` bei neuen Installationen auf "`no`" (nein) eingestellt. Selbst mit der Einstellung "`no`" (nein) wird die Cron-Datenausgabe weiterhin an die `MAILTO`-Adresse gesendet, wie auf der man-Seite zu Cron beschrieben.

Bei einer Aktualisierung wird empfohlen, diese Werte gemäß Ihren Anforderungen einzustellen.

23.1.4 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. Weitere Informationen finden Sie unter *Buch „*System Analysis and Tuning Guide*", Kapitel 3 „Analyzing and Managing System Log Files", Abschnitt 3.3 „Managing Log Files with* **logrotate**".

23.1.5 Der Befehl „locate“

`locate`, ein Kommando zum schnellen Suchen von Dateien, ist nicht im Standardumfang der installierten Software enthalten. Falls gewünscht, können Sie das Paket `mlocate`, den Nachfolger des Pakets `findutils-locate`, installieren. Der Prozess updatedb wird jeden Abend etwa 15 Minuten nach dem Booten des Systems gestartet.

23.1.6 Der Befehl „ulimit“

Mit dem Kommando **`ulimit`** (*user limits*) ist es möglich, Begrenzungen für die Verwendung von Systemressourcen festzulegen und anzuzeigen. **`ulimit`** ist besonders nützlich für die Begrenzung des verfügbaren Arbeitsspeichers für Anwendungen. Damit kann eine Anwendung daran gehindert werden, zu viele Systemressourcen zu reservieren und damit das Betriebssystem zu verlangsamen oder sogar aufzuhängen.

`ulimit` kann mit verschiedenen Optionen verwendet werden. Verwenden Sie zum Begrenzen der Speicherauslastung die in *Tabelle 23.1, „`ulimit`: Einstellen von Ressourcen für Benutzer“* aufgeführten Optionen.

TABELLE 23.1 `ulimit`: EINSTELLEN VON RESSOURCEN FÜR BENUTZER

`-m`	Die maximale nicht auslagerbare festgelegte Größe
`-v`	Die maximale Größe des virtuellen Arbeitsspeichers, der der Shell zur Verfügung steht
`-s`	Die maximale Größe des Stapels
`-c`	Die maximale Größe der erstellten Kerndateien

`-a`	Alle aktuellen Grenzwerte werden gemeldet

Systemweite Standardeinträge werden unter `/etc/profile` festgelegt. Die direkte Bearbeitung dieser Datei wird nicht empfohlen, da die Änderungen bei einer Systemaufrüstung überschrieben werden. Mit `/etc/profile.local` können Sie die systemweiten Profileinstellungen anpassen. Benutzerspezifische Einstellungen sind unter `~USER/.bashrc` vorzunehmen.

BEISPIEL 23.3 ULIMIT: EINSTELLUNGEN IN ~/.BASHRC

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

Die Speicherzuteilungen müssen in KB erfolgen. Weitere Informationen erhalten Sie mit **`man bash`**.

Wichtig: Unterstützung für **`ulimit`**

`ulimit`-Direktiven werden nicht von allen Shells unterstützt. PAM (z. B. `pam_limits`) bietet umfassende Anpassungsfunktionen als Alternative zu **`ulimit`**.

23.1.7 Der Befehl „free“

Der Befehl **`free`** zeigt die Größe des insgesamt vorhandenen freien und verwendeten physischen Arbeitsspeichers und Auslagerungsspeichers im System sowie die vom Kernel verwendeten Puffer und den verwendeten Cache an. 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 mit dem Befehl **mmap** abgerufen werden können. (siehe **man mmap**).

Der Kernel enthält zusätzlich andere Caches, wie beispielsweise den *slab-Cache*, in dem die für den Netzwerkzugriff verwendeten Caches gespeichert werden. Dies erklärt die Unterschiede zwischen den Zählern in `/proc/meminfo`. Die meisten, jedoch nicht alle dieser Zähler, können über `/proc/slabinfo` aufgerufen werden.

Wenn Sie jedoch herausfinden möchten, wie viel RAM gerade verwendet wird, dann finden Sie diese Information in `/proc/meminfo`.

23.1.8 man-Seiten und Info-Seiten

Für einige GNU-Anwendungen (wie beispielsweise tar) sind keine man-Seiten mehr vorhanden. Verwenden Sie für diese Befehle die Option `--help`, um eine kurze Übersicht über die info-Seiten zu erhalten, in der Sie detailliertere Anweisungen erhalten. info befindet sich im Hypertextsystem von GNU. Eine Einführung in dieses System erhalten Sie, wenn Sie **info** `info` eingeben. Info-Seiten können mit Emacs angezeigt werden, wenn Sie **emacs** `-f info` eingeben oder mit **info** direkt in einer Konsole angezeigt werden. Sie können auch tkinfo, xinfo oder das Hilfesystem zum Anzeigen von info-Seiten verwenden.

23.1.9 Auswählen von man-Seiten über das Kommando **man**

Geben Sie **man** *MAN-SEITE* ein, um eine man-Seite zu lesen. Wenn bereits eine man-Seite mit demselben Namen in anderen Abschnitten vorhanden ist, werden alle vorhandenen Seiten mit den zugehörigen Abschnittsnummern aufgeführt. Wählen Sie die aus, die Sie anzeigen möchten. Wenn Sie innerhalb einiger Sekunden keine Abschnittsnummer eingeben, wird die erste man-Seite angezeigt.

Zur Rückkehr zum standardmäßigen Systemverhalten legen Sie `MAN_POSIXLY_CORRECT=1` in einer Shell-Initialisierungsdatei wie `~/.bashrc` fest.

23.1.10 Einstellungen für GNU Emacs

GNU Emacs ist eine komplexe Arbeitsumgebung. In den folgenden Abschnitten werden die beim Starten von GNU Emacs verarbeiteten Dateien beschrieben. Weitere Informationen hierzu erhalten Sie online unter http://www.gnu.org/software/emacs/.

Beim Starten liest Emacs mehrere Dateien, in denen die Einstellungen für den Benutzer, den Systemadministrator und den Distributor zur Anpassung oder Vorkonfiguration enthalten sind. Die Initialisierungsdatei `~/.emacs` ist in den Home-Verzeichnissen der einzelnen Benutzer von `/etc/skel` installiert. `.emacs` wiederum liest die Datei `/etc/skel/.gnu-emacs`. Zum Anpassen des Programms kopieren Sie `.gnu-emacs` in das Home-Verzeichnis (mit **`cp /etc/skel/.gnu-emacs ~/.gnu-emacs`**) und nehmen Sie dort die gewünschten Einstellungen vor.

`.gnu-emacs` definiert die Datei `~/.gnu-emacs-custom` als `custom-file`. Wenn Benutzer in Emacs Einstellungen mit den `customize`-Optionen vornehmen, werden die Einstellungen in `~/.gnu-emacs-custom` gespeichert.

Bei SUSE Linux Enterprise Server 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-Add-on-Paketen, wie `psgml`, automatisch geladen werden. Konfigurationsdateien dieses Typs sind ebenfalls unter `/usr/share/emacs/site-lisp` gespeichert und beginnen immer mit `suse-start-`. Der lokale Systemadministrator kann systemweite Einstellungen in `default.el` festlegen.

Weitere Informationen zu diesen Dateien finden Sie in der Info-Datei zu Emacs unter *Init File:* `info:/emacs/InitFile`. Informationen zum Deaktivieren des Ladens dieser Dateien (sofern erforderlich) stehen dort ebenfalls zur Verfügung.

Die Komponenten von Emacs sind in mehrere Pakete unterteilt:

- Das Basispaket `emacs`.
- `emacs-x11` (in der Regel installiert): das Programm *mit* X11-Support.
- `emacs-nox`: das Programm *ohne* X11-Support.
- `emacs-info`: Online-Dokumentation im info-Format.

- `emacs-el`: die nicht kompilierten Bibliotheksdateien in Emacs Lisp. Sie sind während der Laufzeit nicht erforderlich.
- Verschiedene Add-On-Pakete können bei Bedarf installiert werden: `emacs-auctex` (LaTeX), `psgml` (SGML und XML), `gnuserv` (Client- und Server-Vorgänge) und andere.

23.2 Virtuelle Konsolen

Linux ist ein Multitasking-System für den Mehrbenutzerbetrieb. Die Vorteile dieser Funktionen können auch auf einem eigenständigen PC-System genutzt werden. Im Textmodus stehen sechs virtuelle Konsolen zur Verfügung. Mit den Tastenkombinationen Alt–F1 bis Alt–F6 können Sie zwischen den Konsolen umschalten. Die siebte Konsole ist für X und reserviert und in der zehnten Konsole werden Kernel-Meldungen angezeigt.

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.

23.3 Tastaturzuordnung

Um die Tastaturzuordnung der Programme zu standardisieren, wurden Änderungen an folgenden Dateien vorgenommen:

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.emacs
/etc/skel/.gnu-emacs
/etc/skel/.vimrc
/etc/csh.cshrc
/etc/termcap
/usr/share/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
```

```
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

Diese Änderungen betreffen nur Anwendungen, die **terminfo**-Einträge verwenden oder deren Konfigurationsdateien direkt geändert werden (**vi**, **emacs** usw.). Anwendungen, die nicht im Lieferumfang des Systems enthalten sind, sollten an diese Standards angepasst werden.

Unter X kann die Compose-Taste (Multi-Key) gemäß `/etc/X11/Xmodmap` aktiviert werden.

Weitere Einstellungen sind mit der X-Tastaturerweiterung (XKB) möglich. Diese Erweiterung wird auch von der Desktop-Umgebung GNOME (gswitchit) verwendet.

Tipp: Weiterführende Informationen

Informationen zu XKB finden Sie in den Dokumenten, die unter `/usr/share/doc/packages/xkeyboard-config` (Teil des Pakets `xkeyboard-config`) aufgelistet sind.

23.4 Sprach- und länderspezifische Einstellungen

Das System wurde zu einem großen Teil internationalisiert und kann an lokale Gegebenheiten angepasst werden. Die Internationalisierung (*I18N*) ermöglicht eine spezielle Lokalisierung (*L10N*). Die Abkürzungen I18N und L10N wurden von den ersten und letzten Buchstaben der englischsprachigen Begriffe und der Anzahl der dazwischen stehenden ausgelassenen Buchstaben abgeleitet.

Die Einstellungen werden mit `LC_`-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dies bezieht sich nicht nur auf die *native Sprachunterstützung*, sondern auch auf die Kategorien *Meldungen* (Sprache) *Zeichensatz*, *Sortierreihenfolge*, *Uhrzeit und Datum*, *Zahlen* und *Währung*. Diese Kategorien können direkt über eine eigene Variable oder indirekt mit einer Master-Variable in der Datei `language` festgelegt werden (weitere Informationen erhalten Sie auf der man-Seite zu **locale).**

`RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`

Diese Variablen werden ohne das Präfix `RC_` an die Shell weitergegeben und stehen für die aufgelisteten Kategorien. Die betreffenden Shell-Profile werden unten aufgeführt. Die aktuelle Einstellung lässt sich mit dem Befehl **locale** anzeigen.

`RC_LC_ALL`

Sofern diese Variable festgelegt ist, setzt Sie die Werte der bereits erwähnten Variablen außer Kraft.

`RC_LANG`

Falls keine der zuvor genannten Variablen festgelegt ist, ist dies das Fallback. Standardmäßig wird nur `RC_LANG` festgelegt. Dadurch wird es für die Benutzer einfacher, eigene Werte einzugeben.

`ROOT_USES_LANG`

Eine Variable, die entweder den Wert `yes` oder den Wert `no` aufweist. Wenn die Variable auf `no` gesetzt ist, funktioniert `root` immer in der POSIX-Umgebung.

Die Variablen können über den sysconfig-Editor von YaST 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>]]
```

23.4.1 Beispiele

Sprach- und Ländercode sollten immer gleichzeitig eingestellt werden. Die Spracheinstellungen entsprechen der Norm ISO 639, die unter http://www.evertype.com/standards/iso639/iso639-en.html und http://www.loc.gov/standards/iso639-2/ verfügbar ist. Die Ländercodes sind in ISO 3166 aufgeführt (siehe http://en.wikipedia.org/wiki/ISO_3166).

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. Diese Einstellung ist nun überflüssig, da UTF-8 auch das Eurosymbol enthält. Sie ist nur nützlich, wenn eine Anwendung ISO-8859-15 anstelle von UTF-8 unterstützt.

Änderungen an `/etc/sysconfig/language` werden mit der folgenden Prozesskette aktiviert:

- Für die Bash: `/etc/profile` liest `/etc/profile.d/lang.sh`, die ihrerseits `/etc/sysconfig/language` analysiert.
- Für tcsh: `/etc/profile` liest `/etc/profile.d/lang.csh`, die ihrerseits `/etc/sysconfig/language` analysiert.

So wird sichergestellt, dass sämtliche Änderungen an `/etc/sysconfig/language` bei der nächsten Anmeldung in der entsprechenden Shell verfügbar sind, ohne dass sie manuell aktiviert werden müssen.

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 z. B. `LC_MESSAGES=es_ES` auf, damit die Meldungen stattdessen auf Spanisch angezeigt werden.

23.4.2 Locale-Einstellungen in `~/.i18n`

Wenn Sie mit den Locale-Systemstandardwerten nicht zufrieden sind, können Sie die Einstellungen in `~/.i18n` ändern. Achten Sie dabei jedoch auf die Einhaltung der Bash-Scripting-Syntax. Die Einträge in `~/.i18n` setzen die Systemstandardwerte aus `/etc/sysconfig/language` außer Kraft. Verwenden Sie dieselben Variablennamen, jedoch ohne das Namespace-Präfix `RC_`. Nutzen Sie beispielsweise `LANG` anstatt `RC_LANG`:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

23.4.3 Einstellungen für die Sprachunterstützung

Die Dateien in der Kategorie *Meldungen* werden generell im entsprechenden Sprachverzeichnis (wie beispielsweise `en`) gespeichert, damit ein Fallback vorhanden ist. Wenn Sie für `LANG` den Wert `en_US` festlegen und in `/usr/share/locale/en_US/LC_MESSAGES` keine Meldungsdatei vorhanden ist, wird ein Fallback auf `/usr/share/locale/en/LC_MESSAGES` ausgeführt.

Darüber hinaus kann eine Fallback-Kette definiert werden, beispielsweise für Bretonisch zu Französisch oder für Galizisch zu Spanisch oder Portugiesisch:

```
LANGUAGE=„br_FR:fr_Fr“
```

```
LANGUAGE=„gl_ES:es_ES:pt_PT“
```

Wenn Sie möchten, können Sie die norwegischen Varianten Nynorsk und Bokmål (mit zusätzlichem Fallback auf `no`) verwenden:

```
LANG=„nn_NO“
```

```
LANGUAGE=„nn_NO:nb_NO:no“
```

oder

```
LANG=„nb_NO“
```

```
LANGUAGE=„nb_NO:nn_NO:no“
```

Beachten Sie, das bei Norwegisch auch `LC_TIME` anders behandelt wird.

Ein mögliches Problem ist, dass ein Trennzeichen, das zum Trennen von Zifferngruppen verwendet wird, nicht richtig erkannt wird. Dies passiert, wenn `LANG` auf einen aus zwei Buchstaben bestehenden Sprachcode wie `de` eingestellt ist, die Definitionsdatei, die glibc verwendet, jedoch in `/usr/share/lib/de_DE/LC_NUMERIC` gespeichert ist. Daher muss `LC_NUMERIC` auf `de_DE` gesetzt sein, damit das System die Trennzeichendefinition erkennen kann.

23.4.4 Weiterführende Informationen

- *The GNU C Library Reference Manual*, Kapitel „Locales and Internationalization“. Dieses Handbuch ist in `glibc-info` enthalten. Das Paket befindet sich im SUSE Linux Enterprise-SDK. Das SDK ist ein Modul für SUSE Linux Enterprise und steht über einen Online-Kanal im SUSE Customer Center zur Verfügung. Alternativ dazu können Sie http://download.suse.com/ aufrufen, nach `SUSE Linux Enterprise Software Development Kit`

suchen und das SDK von dort herunterladen. Weitere Informationen finden Sie in *Buch „Bereitstellungshandbuch", Kapitel 14 „Installieren von Modulen, Erweiterungen und Add-on-Produkten von Drittanbietern"*.

- 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, verfügbar unter http://tldp.org/HOWTO/Unicode-HOWTO-1.html.

IV Services

24 Zeitsynchronisierung mit NTP 370

25 Domain Name System (DNS) 377

26 DHCP 404

27 Verteilte Nutzung von Dateisystemen mit NFS 421

28 Samba 434

29 Bedarfsweises Einhängen mit autofs 457

30 SLP 466

31 Der HTTP-Server Apache 470

32 Einrichten eines FTP-Servers mit YaST 517

33 Der Proxyserver Squid 522

34 Web Based Enterprise Management mit SFCB 549

24 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 erfüllt häufig nicht die Anforderungen bestimmter Anwendungen, beispielsweise Datenbanken oder Cluster. Die manuelle Korrektur der Systemzeit würde schwerwiegende Probleme nach sich ziehen; das Zurückstellen kann beispielsweise zu Fehlfunktionen wichtiger Anwendungen führen. Die Systemzeiten der in einem Netzwerk zusammengeschlossenen Computer müssen in der Regel synchronisiert werden. Es empfiehlt sich aber nicht, die Zeiten manuell anzugleichen. Vielmehr sollten Sie dazu NTP verwenden. Der NTP-Dienst passt die Systemzeit ständig anhand zuverlässiger Zeitserver im Netzwerk an. Zudem ermöglicht er die Verwaltung lokaler Referenzuhren, beispielsweise funkgesteuerter Uhren.

24.1 Konfigurieren eines NTP-Client mit YaST

Der NTP-Daemon (`ntpd`) im `ntp`-Paket ist so voreingestellt, dass die Uhr des lokalen Computers als Zeitreferenz verwendet wird. Das Verwenden der Hardware-Uhr ist jedoch nur eine Ausweichlösung, wenn keine genauere Zeitquelle verfügbar ist. YaST erleichtert die Konfiguration von NTP-Clients.

24.1.1 Grundlegende Konfiguration

Die NTP-Client-Konfiguration mit YaST (*Netzwerkdienste* › *NTP-Konfiguration*) benötigt zwei Dialogfelder. Legen Sie den Startmodus `ntpd` und den abzufragenden Server auf dem Karteireiter *Allgemein Einstellungen* fest.

Nur manuell

Wählen Sie *Nur manuell*, wenn der `ntpd`-Daemon manuell gestartet werden soll.

Ohne Daemon synchronisieren

Wählen Sie *Ohne Daemon synchronisieren* aus, um die Systemzeit regelmäßig festzulegen, ohne dass `ntpd` ständig ausgeführt wird. Sie können das *Synchronisierungsintervall in Minuten* festlegen.

Jetzt und beim Booten

Wählen Sie *Jetzt und beim Booten*, um `ntpd` automatisch beim Booten des Systems zu starten. Diese Einstellung wird empfohlen.

24.1.2 Ändern der Basiskonfiguration

Die Server und anderen Zeitquellen für die Abfrage durch den Client sind im unteren Bereich im Karteireiter *Allgemeine Einstellungen* aufgelistet. Bearbeiten Sie diese Liste nach Bedarf mithilfe der Optionen *Hinzufügen*, *Bearbeiten* und *Löschen*. *Mit* Protokoll anzeigen können die Protokolldateien Ihres Clients angezeigt werden.

Klicken Sie auf *Hinzufügen*, um eine neue Quelle für Zeitinformationen hinzuzufügen. Wählen Sie im nachfolgenden Dialogfeld den Quellentyp aus, mit dem die Zeitsynchronisierung vorgenommen werden soll. Mit den zur Verfügung stehenden Optionen können Sie

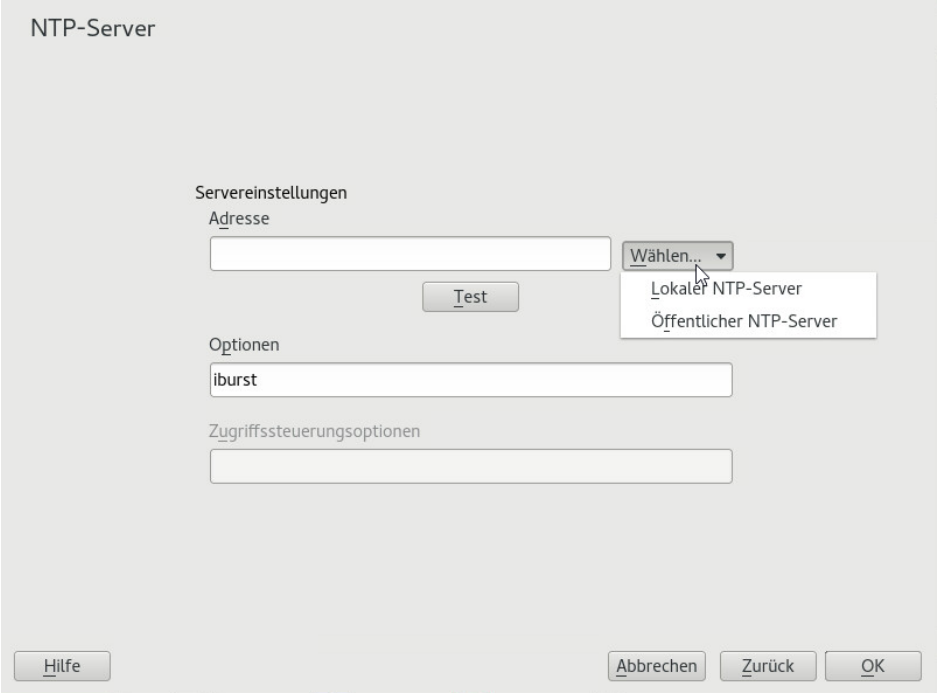


ABBILDUNG 24.1 YAST: NTP-SERVER

Server

Geben Sie in der Dropdown-Liste unter *Auswählen* (siehe *Abbildung 24.1, „YaST: NTP-Server“*) 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*. Überprüfen Sie im Hauptdialogfeld die Verfügbarkeit des ausgewählten Servers mit *Test*. Unter *Optionen* können Sie weitere Optionen für `ntpd` einstellen.

Mit den *Access Control Options* (Zugriffskontrolloptionen) können Sie die Aktionen einschränken, die der entfernte Computer mit dem Daemon Ihres Computers ausführen kann. Dieses Feld ist nur aktiviert, wenn die Option *Restrict NTP Service to Configured Servers Only* (NTP-Dienst auf konfigurierte Server beschränken) auf dem Karteireiter *Sicherheitseinstellungen* aktiviert ist (siehe *Abbildung 24.2, „Erweiterte NTP-Konfiguration: Sicherheitseinstellungen“*). Die Optionen entsprechen den `restrict`-Klauseln der Datei `/etc/ntp.conf`. Die Klausel `nomodify notrap noquery` verhindert beispielsweise, dass der Server die NTP-Einstellungen Ihres Computers ändern und die Trap-Funktion (eine Fernprotokollierungsfunktion für Ereignisse) Ihres NTP-Daemons verwenden kann. Diese Einschränkungen werden besonders für Server außerhalb Ihrer Kontrolle empfohlen (z. B. im Internet).

Ziehen Sie bezüglich detaillierter Informationen `/usr/share/doc/packages/ntp-doc` zurate (Bestandteil des `ntp-doc`-Pakets).

Peer

Ein Peer ist ein Computer, mit dem eine symmetrische Beziehung eingerichtet wird: Er fungiert sowohl als Zeitserver als auch als Client. Wenn Sie einen Peer im selben Netzwerk anstelle eines Servers verwenden möchten, geben Sie die Adresse des Systems ein. Der Rest des Dialogfelds ist mit dem Dialogfeld *Server* identisch.

Funkuhr

Wenn eine Funkuhr für die Zeitsynchronisierung in Ihrem System verwendet werden soll, geben Sie Uhrtyp, Gerätezahl, Gerätename und weitere Optionen in diesem Dialogfeld ein. Klicken Sie auf *Treiber-Kalibirierung*, um den Treiber genauer einzustellen. Detaillierte Informationen zum Betrieb einer lokalen Funkuhr finden Sie in `/usr/share/doc/packages/ntp-doc/refclock.html`.

Ausgangs-Broadcast

Zeitinformationen und Abfragen können im Netzwerk auch per Broadcast übermittelt werden. Geben Sie in diesem Dialogfeld die Adresse ein, an die Broadcasts gesendet werden sollen. Die Option für Broadcasts sollte nur aktiviert werden, wenn Ihnen eine zuverlässige Zeitquelle, etwa eine funkgesteuerte Uhr, zur Verfügung steht.

Eingangs-Broadcast

Wenn Ihr Client die entsprechenden Informationen per Broadcast erhalten soll, geben Sie in diesen Feldern die Adresse ein, von der die jeweiligen Pakete akzeptiert werden sollen.

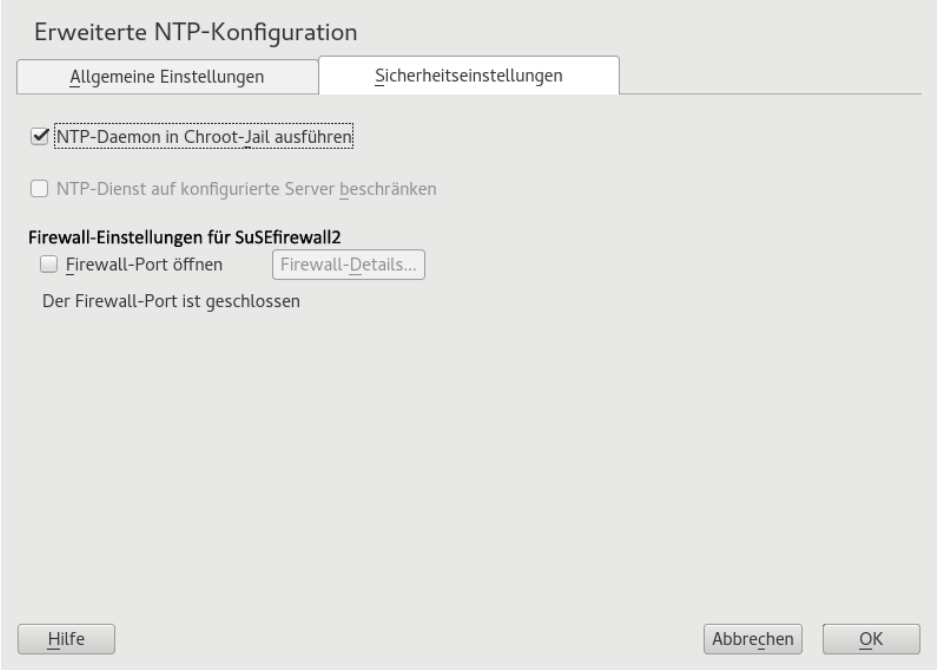


ABBILDUNG 24.2 ERWEITERTE NTP-KONFIGURATION: SICHERHEITSEINSTELLUNGEN

Legen Sie auf dem Karteireiter *Sicherheitseinstellungen* (siehe *Abbildung 24.2, „Erweiterte NTP-Konfiguration: Sicherheitseinstellungen“*) fest, ob `ntpd` in einem „Chroot Jail“ gestartet werden soll. Standardmäßig ist *NTP-Daemon in Chroot-Jail ausführen* nicht aktiviert. Die Chroot-Jail-Option erhöht die Sicherheit im Falle eines Angriffs über `ntpd`, da der Angreifer daran gehindert wird, das gesamte System zu beeinträchtigen.

Die Option *NTP-Dienst auf konfigurierte Server beschränken* erhöht die Sicherheit Ihres Systems. Wenn gewählt, verhindert diese Option, dass entfernte Computer die NTP-Einstellungen Ihres Computers anzeigen und ändern und die Trap-Funktion für die Fernprotokollierung von Ereignissen verwenden können. Nach dem Aktivieren gelten diese Einschränkungen für alle entfern-

ten Computer, es sei denn, Sie überschreiben die Zugriffskontrolloptionen für einzelne Computer in der Liste der Zeitquellen auf dem Karteireiter *Allgemeine Einstellungen*. Allen anderen entfernten Computern wird nur die Abfrage der lokalen Zeit erlaubt.

Aktivieren Sie *Firewall-Port öffnen*, wenn SuSEFirewall2 aktiviert ist (Standardeinstellung). Wenn Sie den Port geschlossen lassen, können Sie keine Verbindung zum Zeitserver herstellen.

24.2 Manuelle Konfiguration von NTP 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 folgende Zeile hinzufügen:

```
server ntp.example.com
```

Wenn Sie weitere Zeitserver hinzufügen möchten, fügen Sie zusätzliche Zeilen mit dem Schlüsselwort `server` ein. Nach dem Initialisieren von `ntpd` mit dem Befehl **`systemctl start ntp`** dauert es etwa eine Stunde, bis die Uhrzeit 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, wenn der Computer eingeschaltet wird. Die Korrektur kommt umgehend zum Einsatz und führt zu einer größeren Stabilität der Systemzeit.

Es gibt zwei Möglichkeiten, den NTP-Mechanismus als Client zu verwenden: Erstens kann der Client in regelmäßigen Abständen die Zeit von einem bekannten Server abfragen. Wenn viele Clients vorhanden sind, kann dies zu einer starken Auslastung des Servers führen. Zweitens kann der Client auf NTP-Broadcasts warten, die von Broadcast-Zeitservern im Netzwerk gesendet werden. Dieser Ansatz hat den Nachteil, dass die Qualität des Servers unbekannt ist und dass ein Server, der falsche Informationen sendet, zu schwerwiegenden Problemen führen kann.

Wenn die Zeit per Broadcast ermittelt wird, ist der Servername nicht erforderlich. Geben Sie in diesem Fall die Zeile `broadcastclient` in die Konfigurationsdatei `/etc/ntp.conf` ein. Wenn ein oder mehrere bekannte Zeitserver exklusiv verwendet werden sollen, geben Sie die Namen in der Zeile ein, die mit `servers` beginnt.

24.3 Dynamische Zeitsynchronisierung während der Laufzeit

Wenn das System ohne Netzwerkverbindung startet, fährt `ntpd` zwar hoch, kann jedoch nicht die DNS-Namen der in der Konfigurationsdatei festgelegten Zeitserver auflösen. Dies kann vorkommen, wenn Sie NetworkManager mit einem verschlüsselten WLAN verwenden.

Wenn `ntpd` die DNS-Namen während der Laufzeit auflösen soll, müssen Sie die Option `Dynamisch` festlegen. Wenn die Netzwerkverbindung dann einige Zeit nach dem Start aufgebaut wird, überprüft `ntpd` die Namen erneut und kann die Zeitserver zum Abrufen der Zeit erreichen.

Bearbeiten Sie `/etc/ntp.conf` manuell und fügen Sie `Dynamisch` zu einem oder mehreren `Server` einträgen hinzu:

```
server ntp.example.com dynamic
```

Oder verwenden Sie YaST, und gehen Sie folgendermaßen vor:

1. Klicken Sie in YaST auf *Netzwerkdienste* › *NTP-Konfiguration*.
2. Wählen Sie den Server aus, der konfiguriert werden soll. Klicken Sie anschließend auf *Bearbeiten*.
3. Aktivieren Sie das Feld *Optionen* und fügen Sie `Dynamisch` hinzu. Verwenden Sie ein Leerzeichen zum Trennen, falls bereits andere Optionen eingetragen sind.
4. Klicken Sie auf *OK*, um das Dialogfeld für die Bearbeitung zu schließen. Wiederholen Sie den vorherigen Schritt, um alle Server wunschgemäß zu ändern.
5. Klicken Sie abschließend auf *OK*, um die Einstellungen zu speichern.

24.4 Einrichten einer lokalen Referenzuhr

Das Software-Paket `ntpd` enthält Treiber für das Verbinden lokaler Referenzuhren. Eine Liste unterstützter Uhren steht im Paket `ntp-doc` in der Datei `/usr/share/doc/packages/ntp-doc/refclock.html` zur Verfügung. Jeder Treiber ist mit einer Nummer verknüpft. In NTP wird die eigentliche Konfiguration mit Pseudo-IP-Adressen durchgeführt. Die Uhren werden so in die Datei `/etc/ntp.conf` eingegeben, als ob sie im Netzwerk vorhanden wären. Zu diesem Zweck

werden Ihnen spezielle IP-Adressen im Format `127.127.T.U` zugewiesen. Hierbei steht *`T`* für den Uhrentyp und legt fest, welcher Treiber verwendet wird, und *`U`* steht für die Einheit (unit), die die verwendete Schnittstelle bestimmt.

Im Regelfall verfügen die einzelnen Treiber über spezielle Parameter, die die Konfigurationsdetails beschreiben. Die Datei `/usr/share/doc/packages/ntp-doc/drivers/driver`*`NN`*`.html` (*`NN`* steht für die Anzahl der Treiber) bietet Informationen zum jeweiligen Uhrentyp. Für die Uhr vom „Typ 8“ (Funkuhr über serielle Schnittstelle) ist ein zusätzlicher Modus erforderlich, der die Uhr genauer angibt. Das Conrad DCF77-Empfängermodul weist beispielsweise Modus 5 auf. Wenn diese Uhr als bevorzugte Referenz verwendet werden soll, geben Sie das Schlüsselwort `prefer` an. Die vollständige `server`-Zeile für ein Conrad DCF77-Empfängermodul sieht folgendermaßen aus:

```
server 127.127.8.0 mode 5 prefer
```

Für andere Uhren gilt dasselbe Schema. Nach der Installation des Pakets `ntp-doc` steht die Dokumentation für ntp im Verzeichnis `/usr/share/doc/packages/ntp-doc` zur Verfügung. Die Datei `/usr/share/doc/packages/ntp-doc/refclock.html` enthält Links zu den Treiberseiten, auf denen die Treiberparameter beschrieben werden.

24.5 Uhrensynchronisierung mit einer externen Zeitreferenz (ETR)

Unterstützung für Uhrensynchronisierung mit einer externen Zeitreferenz (ETR) ist verfügbar. Die externe Zeitreferenz sendet alle 2**20 (2 hoch 20) Millisekunden ein Oszillatorsignal und ein Synchronisierungssignal, um die Tageszeit-Uhren aller angeschlossenen Server synchron zu halten.

Zur Verfügbarkeit können zwei ETR-Einheiten an einen Computer angeschlossen werden. Wenn die Uhr um mehr als die Toleranz zum Prüfen der Synchronisierung abweicht, erhalten alle CPUs eine Rechnerprüfung, die darauf hinweist, dass die Uhr nicht synchronisiert ist. In diesem Fall werden sämtliche DASD-E/A an XRC-fähige Geräte gestoppt, bis die Uhr wieder synchron ist.

Die ETR-Unterstützung wird mithilfe von zwei `sysfs`-Attributen aktiviert; führen Sie die folgenden Kommandos als `root` aus:

```
echo 1 > /sys/devices/system/etr/etr0/online
echo 1 > /sys/devices/system/etr/etr1/online
```

25 Domain Name System (DNS)

DNS (Domain Name System) ist zur Auflösung der Domänen- und Hostnamen in IP-Adressen erforderlich. So wird die IP-Adresse 192.168.2.100 beispielsweise dem Hostnamen `jupiter` zugewiesen. Bevor Sie Ihren eigenen Namenserver einrichten, sollten Sie die allgemeinen Informationen zu DNS in *Abschnitt 16.3, „Namensauflösung“* lesen. Die folgenden Konfigurationsbeispiele gelten für BIND, den standardmäßigen DNS-Server.

25.1 DNS-Terminologie

Zone

Der Domänen-Namespace wird in Regionen, so genannte Zonen, unterteilt. So ist beispielsweise `example.com` der Bereich (oder die Zone) `example` der Domäne `com`.

DNS-Server

Der DNS-Server ist ein Server, auf dem der Name und die IP-Informationen für eine Domäne gespeichert sind. Sie können einen primären DNS-Server für die Masterzone, einen sekundären Server für die Slave-Zone oder einen Slave-Server ohne jede Zone für das Caching besitzen.

DNS-Server der Masterzone

Die Masterzone beinhaltet alle Hosts aus Ihrem Netzwerk und der DNS-Server der Masterzone speichert die aktuellen Einträge für alle Hosts in Ihrer Domäne.

DNS-Server der Slave-Zone

Eine Slave-Zone ist eine Kopie der Masterzone. Der DNS-Server der Slave-Zone erhält seine Zonendaten mithilfe von Zonentransfers von seinem 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. Zum Aktivieren verschiedener Konfigurationsquellen in einer Konfiguration wird `netconfig` verwendet (siehe auch **`man 8 netconfig`**).

Datensatz

Der Eintrag besteht aus Informationen zu Namen und IP-Adresse. Die unterstützten Einträge und ihre Syntax sind in der BIND-Dokumentation beschrieben. Einige spezielle Einträge sind beispielsweise:

NS-Eintrag

Ein NS-Eintrag informiert die Namenserver darüber, welche Computer für eine bestimmte Domänenzone zuständig sind.

MX-Eintrag

Die MX (Mailaustausch)-Einträge beschreiben die Computer, die für die Weiterleitung von Mail über das Internet kontaktiert werden sollen.

SOA-Eintrag

Der SOA (Start of Authority)-Eintrag ist der erste Eintrag in einer Zonendatei. Der SOA-Eintrag wird bei der Synchronisierung von Daten zwischen mehreren Computern über DNS verwendet.

25.2 Installation

Zur Installation eines DNS-Servers starten Sie YaST, und wählen Sie *Software* › *Software installieren oder löschen*. Wählen Sie *Ansicht* › *Schemata* und schließlich *DHCP- und DNS-Server* aus. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

Alternativ geben Sie den folgenden Befehl in der Befehlszeile ein:

```
zypper in -t pattern dhcp_dns_server
```

25.3 Konfiguration mit YaST

Verwenden Sie das DNS-Modul von YaST, um einen DNS-Server für das lokale Netzwerk zu konfigurieren. Beim ersten Starten des Moduls werden Sie von einem Assistenten aufgefordert, einige grundlegende Entscheidungen hinsichtlich der Serveradministration zu treffen. Mit dieser Ersteinrichtung wird eine grundlegende Serverkonfiguration vorgenommen. Für erweiterte Konfigurationsaufgaben, beispielsweise zum Einrichten von ACLs, für Protokollaufgaben, TSIG-Schlüssel und andere Optionen, verwenden Sie den Expertenmodus.

25.3.1 Assistentenkonfiguration

Der Assistent besteht aus drei Schritten bzw. Dialogfeldern. An bestimmten Stellen im Dialogfeld können Sie in den Konfigurationsmodus für Experten wechseln.

1. Wenn Sie das Modul zum ersten Mal starten, wird das Dialogfeld *Forwarder-Einstellungen* (siehe *Abbildung 25.1, „DNS-Server-Installation: Forwarder-Einstellungen“*) geöffnet. Die *Richtlinie für lokale DNS-Auflösung* bietet die folgenden Optionen:

   - *Zusammenführen von Forwardern ist deaktiviert*
   - *Automatisches Zusammenführen*
   - *Zusammenführen von Forwardern ist aktiviert*
   - *Benutzerdefinierte Konfiguriation* – Wenn die *benutzerdefinierte Konfiguriation* aktiviert ist, können Sie die *benutzerdefinierte Richtlinie* angeben. Standardmäßig (Option *Automatisches Zusammenführen* ist aktiviert) ist die *benutzerdefinierte Richtlinie* auf `automatisch` eingestellt; hier können Sie die Schnittstellennamen jedoch selbst festlegen oder aus den beiden besonderen Richtliniennamen `STATIC` und `STATIC_FALLBACK` wählen.

   Geben Sie unter *Forwarder für lokale DNS-Auflösung* den zu verwendenden Service an: *System-Nameserver werden verwendet*, *Dieser Nameserver (Bind)* oder *Lokaler dnsmasq-Server*. Weitere Informationen zu diesen Einstellungen finden Sie auf der man-Seite **`man 8 netconfig`**.

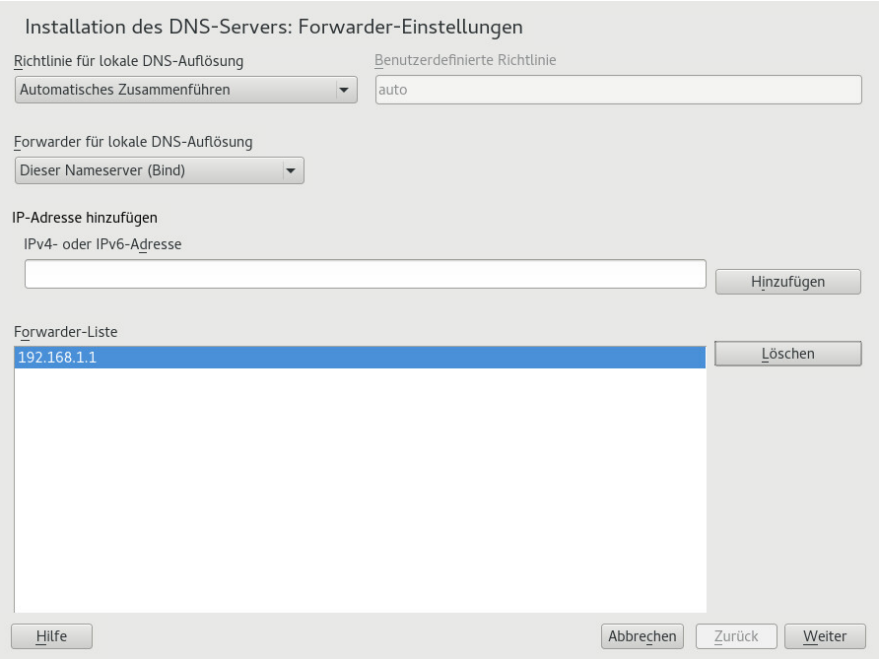


ABBILDUNG 25.1 DNS-SERVER-INSTALLATION: FORWARDER-EINSTELLUNGEN

Forwarders sind DNS-Server, an die der DNS-Server Abfragen sendet, die er nicht selbst bearbeiten kann. Geben Sie ihre IP-Adresse ein und klicken Sie auf *Hinzufügen*.

2. Das Dialogfeld *DNS-Zonen* besteht aus mehreren Teilen und ist für die Verwaltung von Zonendateien zuständig, wie in *Abschnitt 25.6, „Zonendateien“* beschrieben. Bei einer neuen müssen Sie unter *Name der Zone* einen Namen angeben. Um eine Reverse Zone hinzuzufügen, muss der Name auf `.in-addr.arpa` enden. Wählen Sie zum Schluss den *Typ* (Master, Slave oder Forward) aus. Weitere Informationen hierzu finden Sie unter *Abbildung 25.2, „DNS-Server-Installation: DNS-Zonen“*. Klicken Sie auf *bearbeiten*, um andere Einstellungen für eine bestehende Zone zu konfigurieren. Zum Entfernen einer klicken Sie auf *Zone löschen*.

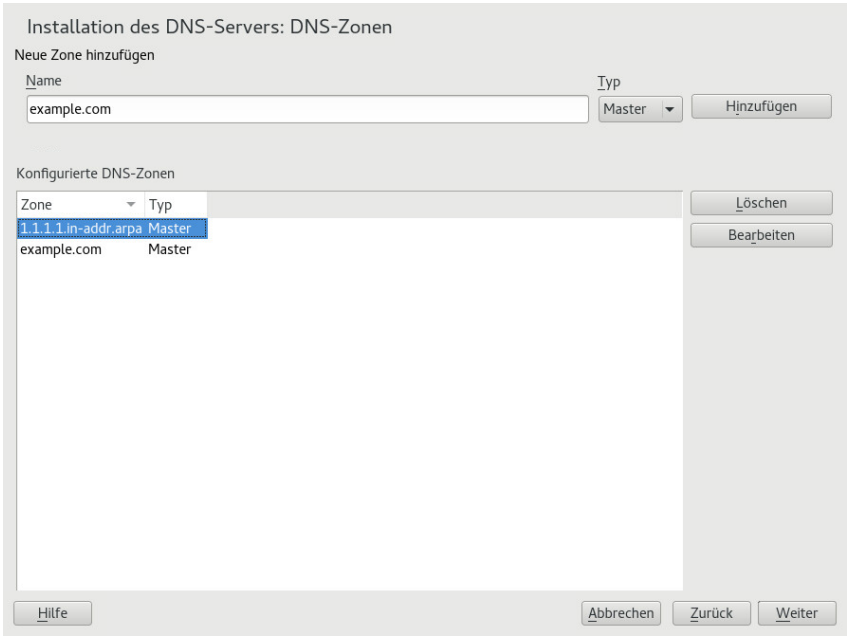


ABBILDUNG 25.2 DNS-SERVER-INSTALLATION: DNS-ZONEN

3. Im letzten Dialogfeld können Sie den DNS-Port in der Firewall öffnen, indem Sie auf *Firewall-Port öffnen* klicken. Legen Sie anschließend fest, ob der DNS-Server beim Booten gestartet werden soll (*Ein* oder *Aus*). Außerdem können Sie die LDAP-Unterstützung aktivieren. Weitere Informationen hierzu finden Sie unter *Abbildung 25.3, „DNS-Server-Installation: Wizard beenden“*.

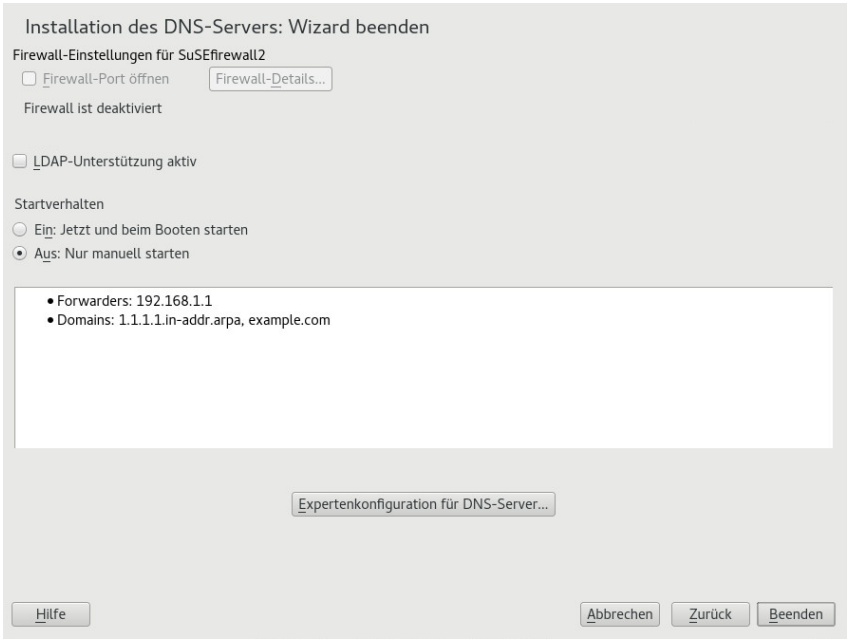


ABBILDUNG 25.3 DNS-SERVER-INSTALLATION: WIZARD BEENDEN

25.3.2 Konfiguration für Experten

Nach dem Starten des Moduls öffnet YaST ein Fenster, in dem mehrere Konfigurationsoptionen angezeigt werden. Nach Abschluss dieses Fensters steht eine DNS-Server-Konfiguration mit Grundfunktionen zur Verfügung:

25.3.2.1 Start

Legen Sie unter *Start* fest, ob der DNS-Server beim Booten des Systems oder manuell gestartet werden soll. Um den DNS-Server sofort zu starten, klicken Sie auf *DNS-Server nun starten*. Um den DNS-Server anzuhalten, klicken Sie auf *DNS-Server nun anhalten*. Zum Speichern der aktuellen Einstellungen wählen Sie *Jetzt Einstellungen speichern und DNS-Server neu laden*. 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 erfasst, wenn er neu gestartet oder aufgefordert wird, seine Konfiguration neu zu laden.

25.3.2.2 Forwarder

Falls Ihr lokaler DNS-Server eine Anforderung nicht beantworten kann, versucht er, diese Anforderung an einen *Forwarder* weiterzuleiten, falls dies so konfiguriert wurde. Dieser Forwarder kann manuell zur *Forwarder-Liste* hinzugefügt werden. Wenn der Forwarder nicht wie bei Einwahlverbindungen statisch ist, wird die Konfiguration von *netconfig* verarbeitet. Weitere Informationen über netconfig finden Sie auf **`man 8 netconfig`**.

25.3.2.3 Grundlegende Optionen

In diesem Abschnitt werden grundlegende Serveroptionen festgelegt. Wählen Sie im Menü *Option* das gewünschte Element aus, und geben Sie dann den Wert im entsprechenden Textfeld an. Nehmen Sie den neuen Eintrag auf, indem Sie auf *Hinzufügen* klicken.

25.3.2.4 Protokollierung

Um festzulegen, was und wie der DNS-Server protokollieren soll, wählen Sie *Protokollieren* aus. Geben Sie unter *Protokolltyp* an, wohin der DNS-Server die Protokolldaten schreiben soll. Verwenden Sie das systemweite Protokoll durch Auswahl von *Systemprotokoll*, oder geben Sie durch Auswahl von *Datei* eine andere Datei an. In letzterem Fall müssen Sie außerdem einen Namen, die maximale Dateigröße in Megabyte und die Anzahl der zu speichernden Versionen von Protokolldateien angeben.

Weitere Optionen sind unter *Zusätzliches Protokollieren* verfügbar. Durch Aktivieren von *Alle DNS-Abfragen protokollieren* wird *jede* Abfrage protokolliert. In diesem Fall kann die Protokolldatei extrem groß werden. Daher sollte diese Option nur zur Fehlersuche aktiviert werden. Um den Datenverkehr zu protokollieren, der während Zonenaktualisierungen zwischen dem DHCP- und dem DNS-Server stattfindet, aktivieren Sie *Zonen-Updates protokollieren*. Um den Datenverkehr während eines Zonentransfers von Master zu Slave zu protokollieren, aktivieren Sie *Zonen-Transfer protokollieren*. Weitere Informationen hierzu finden Sie unter *Abbildung 25.4, „DNS-Server: Protokollieren“*.

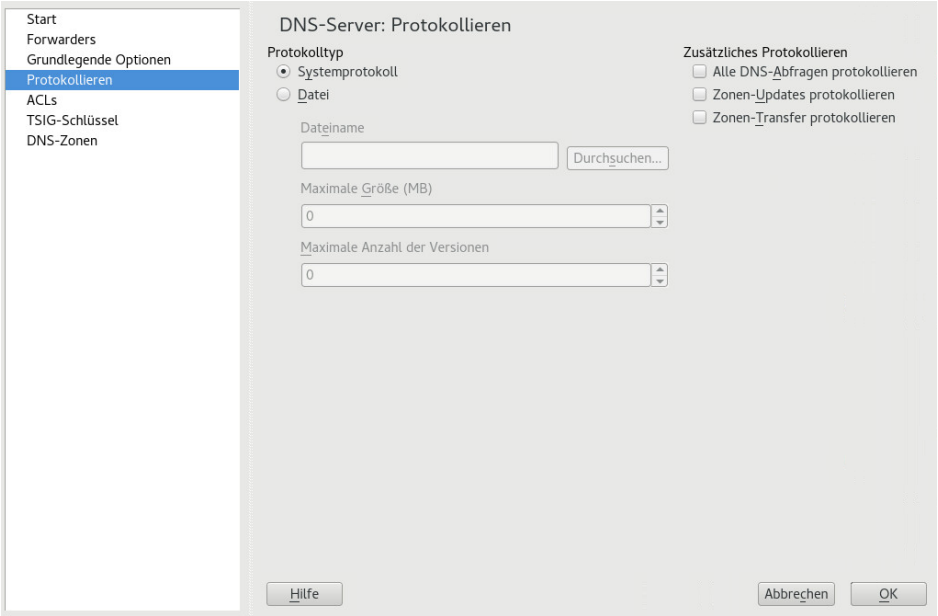


ABBILDUNG 25.4 DNS-SERVER: PROTOKOLLIEREN

25.3.2.5 ACLs

In diesem Dialogfeld 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:

```
{ 192.168.1/24; }
```

Die Syntax der Konfigurationsdatei erfordert, dass die Adresse mit einem Strichpunkt endet und in geschwungenen Klammern steht.

25.3.2.6 TSIG-Schlüssel

Der Hauptzweck von TSIG-Schlüsseln (Transaction Signatures = Transaktionssignaturen) ist die Sicherung der Kommunikation zwischen DHCP- und DNS-Servern. Diese werden unter *Abschnitt 25.8, „Sichere Transaktionen“* 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 *Erzeugen*.

Wenn Sie einen vorher erstellten Schlüssel verwenden möchten, lassen Sie das Feld *Schlüssel-ID* leer und wählen die Datei, in der der gewünschte Schlüssel gespeichert wurde, unter *Dateiname*. Dann bestätigen Sie die Auswahl mit *Hinzufügen*.

25.3.2.7 DNS-Zonen (Hinzufügen einer Slave-Zone)

Wenn Sie eine Slave-Zone hinzufügen möchten, klicken Sie auf *DNS-Zonen*, wählen Sie den Zonentyp *Slave* aus, geben Sie den Namen der neuen Zone ein und klicken Sie auf *Hinzufügen*.

Geben Sie im *Zonen-Editor* unter *IP des Master DNS-Servers* den Master an, von dem der Slave die Daten abrufen soll. Um den Zugriff auf den Server zu beschränken, wählen Sie eine der ACLs aus der Liste aus.

25.3.2.8 DNS-Zonen (Hinzufügen einer Master-Zone)

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*. Beim Hinzufügen einer Masterzone ist auch eine Reverse Zone erforderlich. Wenn Sie beispielsweise die Zone `example.com` hinzufügen, die auf Hosts in einem Subnetz `192.168.1.0/24` zeigt, sollten Sie auch eine Reverse Zone für den betreffenden IP-Adressbereich erstellen. Per Definition sollte dieser den Namen `1.168.192.in-addr.arpa` erhalten.

25.3.2.9 DNS-Zonen (Bearbeiten einer Master-Zone)

Wenn Sie eine Masterzone bearbeiten möchten, klicken Sie auf *DNS-Zonen*, wählen Sie die Masterzone in der Tabelle aus und klicken Sie auf *Bearbeiten*. Dieses Dialogfeld besteht aus mehreren Seiten: *Grundlagen* (die zuerst geöffnete Seite), *DNS-Einträge*, *MX-Einträge*, *SOA* und *Einträge*.

Im grundlegenden Dialogfeld in *Abbildung 25.5, „DNS-Server: Zonen-Editor (Grundlagen)“* können Sie die Einstellungen für das dynamische DNS festlegen und auf Optionen für Zonentransfers an Clients und Slave-Namenserver zugreifen. Zum Zulassen dynamischer Aktualisierungen von Zonen wählen Sie *Dynamische Updates erlauben* sowie 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.

Wählen Sie im Dialogfeld *Grundlagen* aus, ob Zonen-Transfers aktiviert werden sollen. Verwenden Sie die aufgelisteten ACLs, um festzulegen, wer Zonen herunterladen kann.

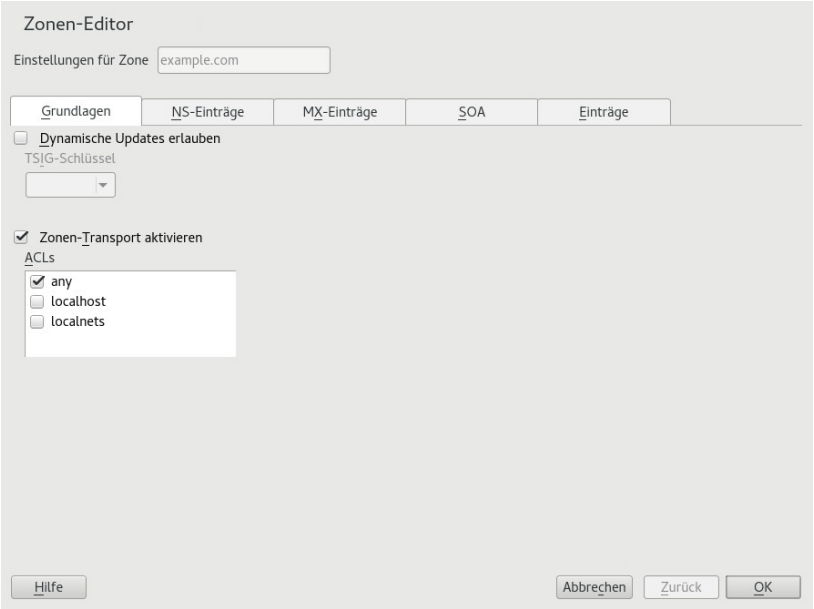


ABBILDUNG 25.5 DNS-SERVER: ZONEN-EDITOR (GRUNDLAGEN)

Zonen-Editor (NS-Einträge)

Im Dialogfeld *NS-Einträge* können Sie alternative Nameserver für die angegebenen Zonen definieren. Vergewissern Sie sich, dass Ihr eigener Namenserver 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*. Weitere Informationen hierzu finden Sie unter *Abbildung 25.6, „DNS-Server: Zonen-Editor (DNS-Einträge)“*.

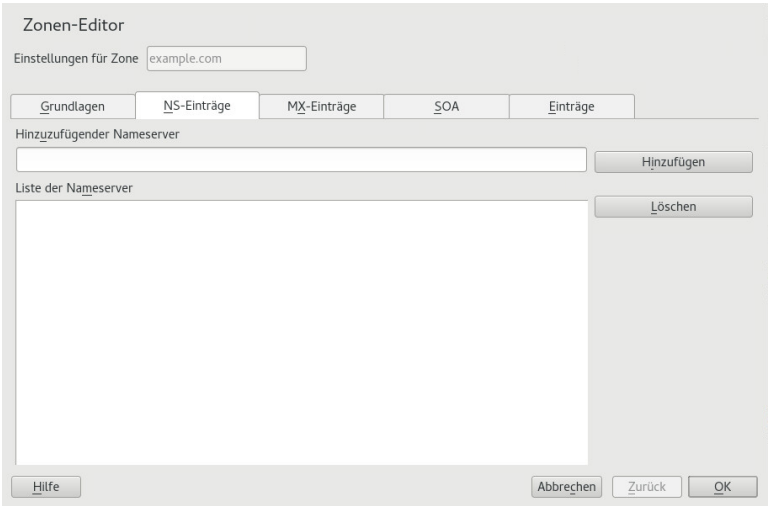


ABBILDUNG 25.6 DNS-SERVER: ZONEN-EDITOR (DNS-EINTRÄGE)

Zonen-Editor (MX-Einträge)

Um einen Mailserver für die aktuelle Zone zur bestehenden Liste hinzuzufügen, geben Sie die entsprechende Adresse und den entsprechenden Prioritätswert ein. Bestätigen Sie den Vorgang anschließend durch Auswahl von *Hinzufügen*. Weitere Informationen hierzu finden Sie unter *Abbildung 25.7, „DNS-Server: Zonen-Editor (MX-Einträge)“*.

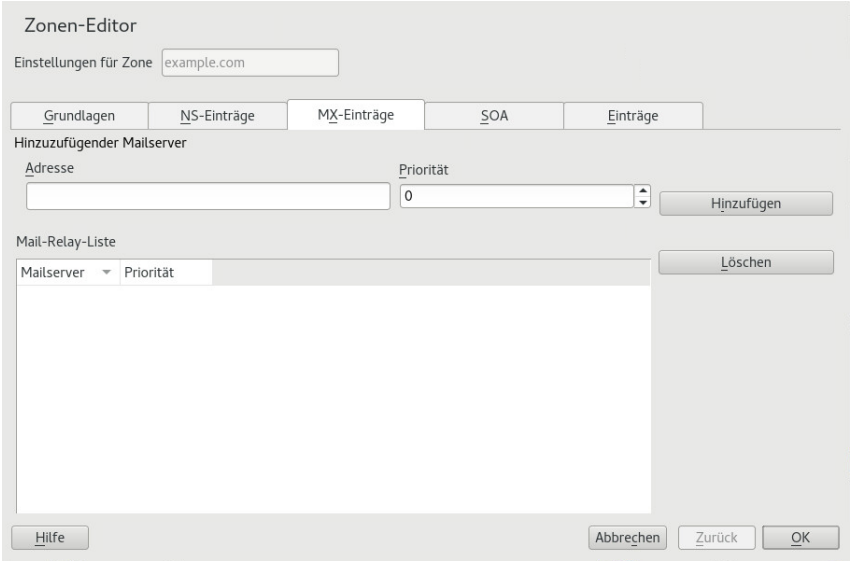


ABBILDUNG 25.7 DNS-SERVER: ZONEN-EDITOR (MX-EINTRÄGE)

Zonen-Editor (SOA)

Auf dieser Seite können Sie SOA (Start of Authority)-Einträge erstellen. Eine Erklärung der einzelnen Optionen finden Sie in *Beispiel 25.6, „Die Datei „/var/lib/named/example.com.zone““*. Das Ändern von SOA-Datensätzen wird für dynamischen Zonen, die über LDAP verwaltet werden, nicht unterstützt.

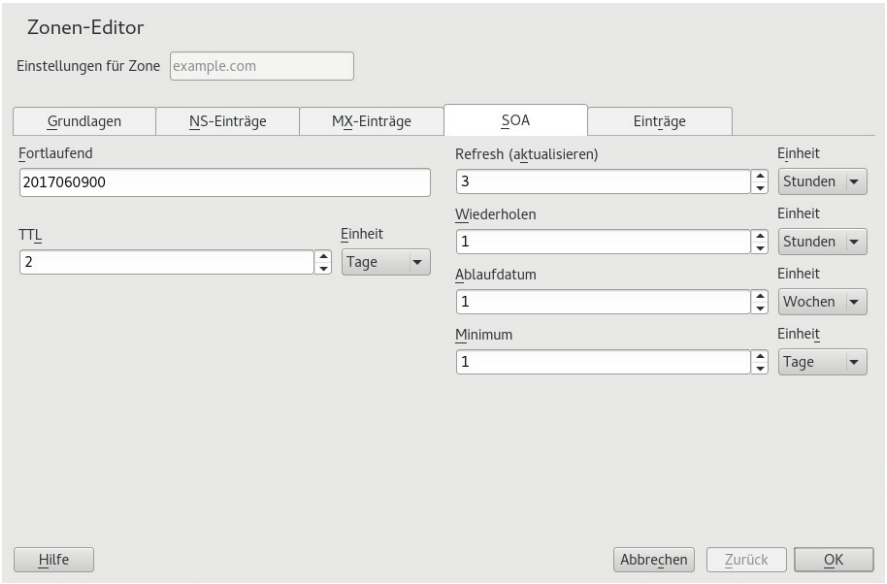


ABBILDUNG 25.8 DNS-SERVER: ZONEN-EDITOR (SOA)

Zonen-Editor (Einträge)

In diesem Dialogfeld wird die Namenauflösung verwaltet. Geben Sie unter *Eintragschlüssel* den Hostnamen an, und wählen Sie anschließend den Typ aus. Der Typ *A* bezeichnet den Haupteintrag. Der Wert hierfür sollte eine IP-Adresse (IPv4) sein. Für IPv6-Adressen verwenden Sie *AAAA*. *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, wie zum Beispiel:

```
hostname.example.com. IN A 192.168.0.1
1.0.168.192.in-addr.arpa IN PTR hostname.example.com.
```

25.3.2.9.1 Hinzufügen von Reverse Zones

So fügen Sie eine Reverse Zone hinzu:

1. Starten Sie *YaST* › *DNS-Server* › *DNS-Zonen*.
2. Falls Sie noch keine Forward-Masterzone angelegt haben, holen Sie dies jetzt nach und *bearbeiten* Sie sie.

3. Geben Sie auf der Registerkarte *Einträge* den entsprechenden *Eintragsschlüssel* und *Eintragswert* an. Legen Sie dann den Eintrag mit *Hinzufügen* an und bestätigen Sie den Vorgang mit *OK*. Wenn YaST eine Meldung ausgibt, dass ein Eintrag für einen Nameserver fehlt, geben Sie diesen Eintrag auf der Registerkarte *DNS-Einträge* an.

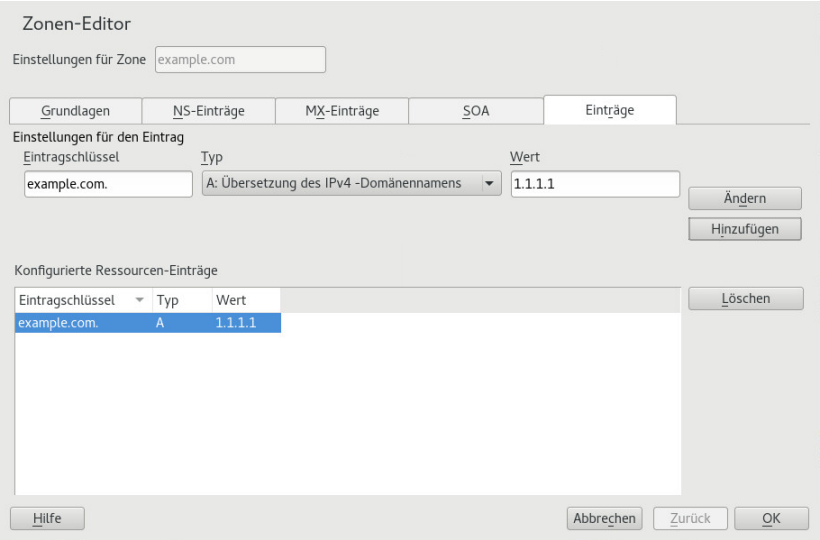


ABBILDUNG 25.9 HINZUFÜGEN EINES EINTRAGS FÜR EINE MASTERZONE

4. Fügen Sie im Fenster *DNS-Zonen* eine Reverse-Masterzone hinzu.

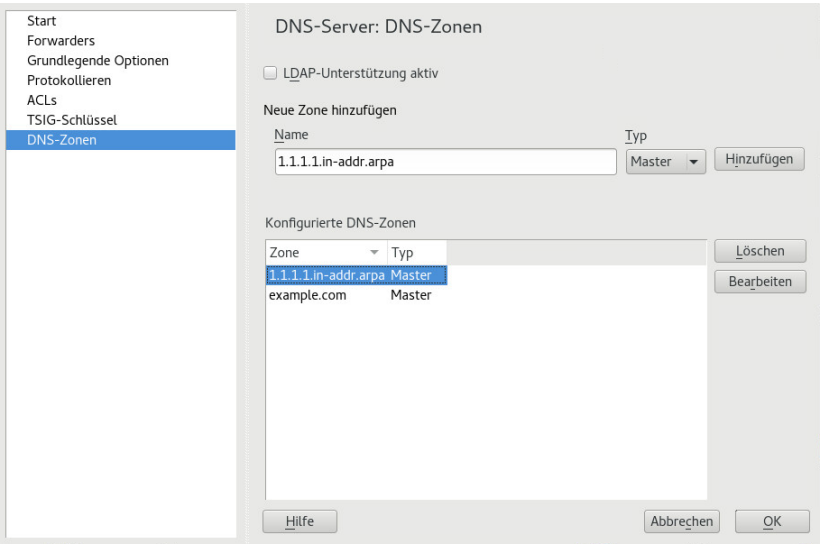


ABBILDUNG 25.10 HINZUFÜGEN EINER REVERSE ZONE

5. *Bearbeiten* Sie die Reverse Zone. Auf der Registerkarte *Einträge* wird der Eintragstyp *PTR: Umgekehrte Übersetzung* aufgeführt. Geben Sie den entsprechenden *Eintragsschlüssel* und *Eintragswert* an, klicken Sie auf *Hinzufügen* und bestätigen Sie den Vorgang mit *OK*.

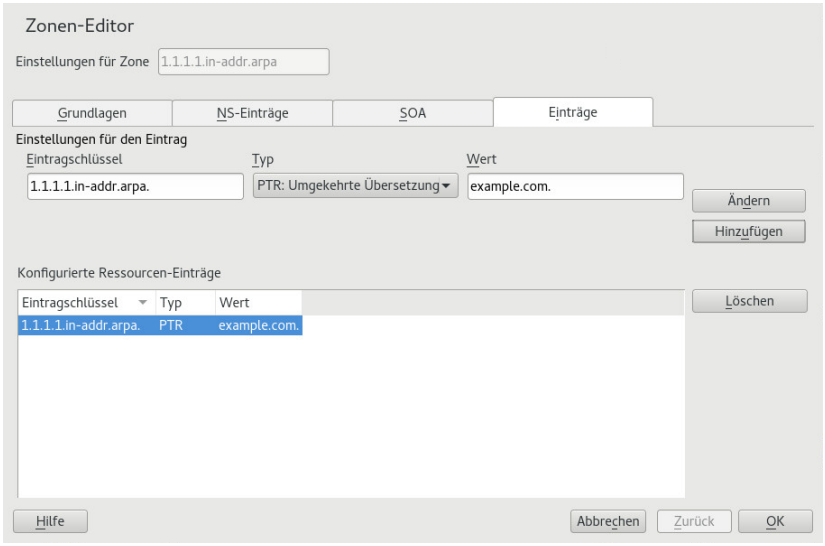


ABBILDUNG 25.11 HINZUFÜGEN EINES REVERSE-EINTRAGS

Fügen Sie bei Bedarf einen Nameserver-Eintrag hinzu.

Tipp: Bearbeiten der Reverse Zone

Wechseln Sie nach dem Hinzufügen einer Forward Zone wieder in das Hauptmenü und wählen Sie die Reverse Zone zur Bearbeitung aus. Markieren Sie im Karteireiter *Grundlagen* das Kontrollkästchen *Einträge automatisch generieren aus* und wählen Sie Ihre Forward Zone aus. Auf diese Weise werden alle Änderungen an der Forward Zone automatisch in der Reverse Zone aktualisiert.

25.4 Starten des BIND-Nameservers

Bei SUSE® Linux Enterprise Server-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 Namenauflösung, ohne dass Ihnen der DNS des Anbieters bekannt sein muss. BIND führt die Namenauflösung 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 Namenauflösung

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 zur Veranschaulichung finden Sie unter `/usr/share/doc/packages/bind/config`.

Tipp: Automatische Anpassung der Namenserverinformationen

Je nach Typ der Internet- bzw. Netzwerkverbindung können die Namenserverinformationen automatisch an die aktuellen Bedingungen angepasst werden. Legen Sie die Variable `NETCONFIG_DNS_POLICY` in der Datei `/etc/sysconfig/network/config` dazu auf `auto` fest.

Richten Sie jedoch erst eine offizielle Domäne ein, wenn Sie eine Domäne von der zuständigen Stelle zugewiesen bekommen. 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.

Starten Sie den Nameserver mit dem Befehl **`systemctl start named`** als `root`. Prüfen Sie mit **`systemctl status named`**, ob der Nameserverprozess „named“ ordnungsgemäß gestartet wurde. Testen Sie den Nameserver umgehend auf dem lokalen System mit den Programmen **`host`** oder **`dig`**. Sie sollten `localhost` als Standardserver mit der Adresse `127.0.0.1` zurückgeben. Ist dies nicht der Fall, enthält `/etc/resolv.conf` vermutlich einen falschen Nameservereintrag oder die Datei ist nicht vorhanden. Geben Sie beim ersten Test **`host`** `127.0.0.1` ein. Dieser Eintrag sollte immer funktionieren. Wenn Sie eine Fehlermeldung erhalten, überprüfen Sie mit **`systemctl status named`**, ob der Server tatsächlich ausgeführt wird. Wenn der Nameserver nicht startet oder sich ungewöhnlich verhält, prüfen Sie die Ausgabe von **`journalctl -e`**.

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 25.1, „Weiterleitungsoptionen in named.conf“* handelt es sich lediglich um Beispiele. Passen Sie diese Einträge an Ihr eigenes Setup an.

BEISPIEL 25.1 WEITERLEITUNGSOPTIONEN IN NAMED.CONF

```
options {
        directory "/var/lib/named";
        forwarders { 10.11.12.13; 10.11.12.14; };
        listen-on { 127.0.0.1; 192.168.1.116; };
```

```
        allow-query { 127/8; 192.168/16 };
        notify no;
};
```

Auf den Eintrag `options` folgen Einträge für die Zone, `localhost` und `0.0.127.in-addr.arpa`. Der Eintrag `type hint` unter „.“ sollte immer vorhanden sein. Die entsprechenden Dateien müssen nicht bearbeitet werden und sollten so funktionieren, wie sie sind. Achten Sie außerdem darauf, dass jeder Eintrag mit einem „;“ abgeschlossen ist und dass sich die geschweiften Klammern an der richtigen Position befinden. Nach dem Ändern der Konfigurationsdatei `/etc/named.conf` oder der Zonendateien müssen Sie BIND anweisen, diese Datei(en) erneut zu lesen. Führen Sie hierzu den Befehl **`systemctl reload named`** aus. Dieselbe Wirkung erzielen Sie, wenn Sie den Nameserver mit **`systemctl restart named`** anhalten und neu starten. Sie können den Server jederzeit mit **`systemctl stop named`** anhalten.

25.5 Die Konfigurationsdatei /etc/named.conf

Alle Einstellungen für den BIND-Namenserver 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 25.2, „Eine Grundversion von /etc/named.conf“*.

BEISPIEL 25.2 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";
};
```

25.5.1 Wichtige Konfigurationsoptionen

directory "*DATEINAME*";

Gibt das Verzeichnis an, in dem BIND die Dateien mit den Zonendaten finden kann. In der Regel ist dies `/var/lib/named`.

forwarders { *IP-ADRESSE*; };

Gibt die Namenserver (zumeist des Anbieters) an, an die DNS-Anforderungen weitergeleitet werden sollen, wenn sie nicht direkt aufgelöst werden können. Ersetzen Sie *IP-ADRESSE* durch eine IP-Adresse wie `192.168.1.116`.

forward first;

Führt dazu, dass DNS-Anforderungen weitergeleitet werden, bevor versucht wird, sie über die Root-Namenserver aufzulösen. Anstatt `forward first` kann `forward only` verwendet werden. Damit werden alle Anforderungen weitergeleitet, ohne dass sie an die Root-Namenserver gesendet werden. Dies ist bei Firewall-Konfigurationen sinnvoll.

listen-on port 53 { 127.0.0.1; *IP-ADRESSE*; };

Informiert BIND darüber, an welchen Netzwerkschnittstellen und Ports Client-Abfragen akzeptiert werden sollen. `port 53` muss nicht explizit angegeben werden, 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 Platzhalteradressen.

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 `192.168.2.0/24`. Der Wert `/24` am Ende ist ein abgekürzter Ausdruck für die Netzmaske, hier `255.255.255.0`).

allow-transfer ! *;;

Legt fest, welche Hosts Zonentransfers anfordern können. Im vorliegenden Beispiel werden solche Anforderungen mit `! *` vollständig verweigert. Ohne diesen Eintrag können Zonentransfer ohne Einschränkungen von jedem beliebigen Ort aus angefordert werden.

statistics-interval 0;

Ohne diesen Eintrag generiert BIND im Systemjournal 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. Damit wird bei jedem Ausführen dieses Vorgangs ein Eintrag im Systemjournal 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.

Eine Liste der verfügbaren Optionen finden Sie auf der man-Seite **`man 5 named.conf`**.

25.5.2 Protokollierung

Der Umfang, die Art und Weise und der Ort der Protokollierung kann in BIND extensiv konfiguriert werden. Normalerweise sollten die Standardeinstellungen ausreichen. In *Beispiel 25.3, „Eintrag zur Deaktivierung der Protokollierung“* sehen Sie die einfachste Form eines solchen Eintrags, bei dem jegliche Protokollierung unterdrückt wird.

BEISPIEL 25.3 EINTRAG ZUR DEAKTIVIERUNG DER PROTOKOLLIERUNG

```
logging {
        category default { null; };
};
```

25.5.3 Zoneneinträge

BEISPIEL 25.4 ZONENEINTRAG FÜR „EXAMPLE.COM“

```
zone "example.com" in {
      type master;
      file "example.com.zone";
      notify no;
};
```

Geben Sie nach `zone` den Namen der zu verwaltenden Domäne (`example.com`) an, gefolgt von `in` und einem Block relevanter Optionen in geschweiften Klammern, wie in *Beispiel 25.4, „Zoneneintrag für „example.com““* 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 25.5, „Zoneneintrag für „example.net““* gezeigt.

BEISPIEL 25.5 ZONENEINTRAG FÜR „EXAMPLE.NET“

```
zone "example.net" in {
      type slave;
      file "slave/example.net.zone";
      masters { 10.0.0.1; };
};
```

Zonenoptionen:

type master;

Durch die Angabe `master` wird BIND darüber informiert, dass der lokale Namenserver für die Zone zuständig ist. Dies setzt voraus, dass eine Zonendatei im richtigen Format erstellt wurde.

type slave;

Diese Zone wird von einem anderen Namenserver übertragen. Sie muss zusammen mit `masters` verwendet werden.

type hint;

Die Zone `.` vom Typ `hint` wird verwendet, um den root-Namenserver festzulegen. Diese Zonendefinition kann unverändert beibehalten werden.

file `example.com.zone` or file „slave/example.net.zone“;

In diesem Eintrag wird die Datei angegeben, in der sich die Zonendaten für die Domäne befinden. Diese Datei ist für einen Slave nicht erforderlich, da die betreffenden Daten von einem anderen Namenserver abgerufen werden. Um zwischen Master- und Slave-Dateien zu unterscheiden, verwenden Sie das Verzeichnis `slave` für die Slave-Dateien.

importserver { *SERVER_IP_ADRESSE*; };

Dieser Eintrag ist nur für Slave-Zonen erforderlich. Er gibt an, von welchem Namenserver 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 keine Zonenaktualisierungen zulässig. Der oben stehende Eintrag hat dieselbe Wirkung, da `! *` solche Aktivitäten effektiv unterbindet.

25.6 Zonendateien

Zwei Arten von Zonendateien sind erforderlich. Eine Art ordnet IP-Adressen Hostnamen zu, die andere stellt Hostnamen für IP-Adressen bereit.

Tipp: Verwenden des Punkts in Zonendateien

Im Verzeichnis "." hat eine wichtige Bedeutung in den Zonendateien. Bei Angabe von Hostnamen ohne abschließenden Punkt (.) wird die Zone angehängt. Vollständige Hostnamen mit vollständiger Domäne benötigen den abschließenden Punkt (.), damit die Domäne nicht erneut hinzugefügt wird. Ein fehlender oder falsch platzierter „." ist wahrscheinlich die häufigste Ursache von Fehlern bei der Namenserverkonfiguration.

Der erste zu betrachtende Fall ist die Zonendatei `example.com.zone`, die für die Domäne `example.com` zuständig ist (siehe *Beispiel 25.6, „Die Datei „/var/lib/named/example.com.zone““*).

BEISPIEL 25.6 DIE DATEI „/VAR/LIB/NAMED/EXAMPLE.COM.ZONE“

```
1.  $TTL 2D
2.  example.com. IN SOA      dns  root.example.com. (
3.               2003072441  ; serial
4.               1D          ; refresh
5.               2H          ; retry
6.               1W          ; expiry
7.               2D )        ; minimum
8.
9.               IN NS       dns
10.              IN MX       10 mail
11.
12. gate         IN A        192.168.5.1
13.              IN A        10.0.0.1
14. dns          IN A        192.168.1.116
15. mail         IN A        192.168.3.108
16. jupiter      IN A        192.168.2.100
17. venus        IN A        192.168.2.101
18. saturn       IN A        192.168.2.102
19. mercury      IN A        192.168.2.103
20. ntp          IN CNAME    dns
21. dns6         IN A6  0    2002:c0a8:174::
```

Zeile 1:

`$TTL` legt die Standardlebensdauer fest, die für alle Einträge in dieser Datei gelten soll. In diesem Beispiel sind die Einträge zwei Tage lang gültig (`2 D`).

Zeile 2:

Hier beginnt der SOA (Start of Authority)-Steuereintrag:

- Der Name der zu verwaltenden Domäne ist `example.com` an der ersten Stelle. Dieser Eintrag endet mit „`.`“, da anderenfalls die Zone ein zweites Mal angefügt würde. Alternativ kann hier `@` eingegeben werden. In diesem Fall wird die Zone aus dem entsprechenden Eintrag in `/etc/named.conf` extrahiert.

- Nach `IN SOA` befindet sich der Name des Namenservers, der als Master für diese Zone fungiert. Der Name wird von `dns` zu `dns.example.com` erweitert, da er nicht mit „`.`“ endet.

- Es folgt die E-Mail-Adresse der für diesen Namenserver zuständigen Person. Da das Zeichen `@` bereits eine besondere Bedeutung hat, wird hier stattdessen „`.`“ eingegeben. Für `root@example.com` lautet der Eintrag `root.example.com.`. Im Verzeichnis „`.`“ muss angehängt werden, damit die Zone nicht hinzugefügt wird.

- Durch `(` werden alle Zeilen bis einschließlich `)` in den SOA-Eintrag aufgenommen.

Zeile 3:

Die Seriennummer (`serial`) ist eine beliebige Nummer, die sich bei jeder Änderung der Datei erhöht. Sie wird benötigt, um die sekundären Namenserver (Slave-Server) über Änderungen zu informieren. Hierfür hat sich eine 10-stellige Nummer aus Datum und Ausführungsnummer in der Form JJJJMMMTTNN als übliches Format etabliert.

Zeile 4:

Die Aktualisierungsrate (`refresh rate`) gibt das Zeitintervall an, in dem die sekundären Namenserver die Seriennummer (`serial`) der Zone überprüfen. In diesem Fall beträgt dieses Intervall einen Tag.

Zeile 5:

Die Wiederholungsrate (`retry`) gibt das Zeitintervall an, nach dem ein sekundärer Namenserver bei einem Fehler erneut versucht, Kontakt zum primären Server herzustellen. In diesem Fall sind dies zwei Stunden.

Zeile 6:

Die Ablaufzeit (`expiry`) gibt den Zeitraum an, nach dem ein sekundärer Server die im Cache gespeicherten Daten verwirft, wenn er keinen erneuten Kontakt zum primären Server herstellen konnte. Hier eine Woche.

Zeile 7:

Die letzte Angabe im SOA-Eintrag gibt die negative Cache-Lebensdauer `negative caching TTL` an – die Zeitdauer, die Ergebnisse nicht aufgelter DNS-Abfragen von anderen Servern im Cache gespeichert werden knen.

Zeile 9:

`IN NS` gibt den für diese Domäne verantwortlichen Namenserver an. `dns` wird zu `dns.example.com` erweitert; der Eintrag endet nicht auf einen „`.`“. Es kann mehrere solche Zeilen geben – eine für den primären und jeweils eine für jeden sekundären Namenserver. Wenn `notify` in `/etc/named.conf` nicht auf `no` gesetzt ist, werden alle hier aufgeführten Namenserver über die Änderungen an den Zonendaten informiert.

Zeile 10:

Der MX-Eintrag gibt den Mailserver an, der Emails für die Domäne `example.com` annimmt, verarbeitet und weiterleitet. In diesem Beispiel ist dies der Host `mail.example.com`. Die Zahl vor dem Hostnamen ist der Präferenzwert. Wenn mehrere MX-Einträge vorliegen, wird zuerst der Mailserver mit dem kleinsten Wert herangezogen. Falls die Mails nicht an diesen Server zugestellt werden können, wird der Eintrag mit höherem Wert verwendet.

Zeilen 12-19:

Dies sind die eigentlichen Adresseinträge, in denen den Hostnamen eine oder mehrere IP-Adressen zugewiesen werden. Die Namen werden hier ohne „`.`“ aufgelistet, da sie ihre Domäne nicht enthalten. Daher wird ihnen allen `example.com` hinzugefügt. Dem Host `gate` werden zwei IP-Adressen zugewiesen, da er zwei Netzwerkkarten aufweist. Bei jeder traditionellen Hostadresse (IPv4) wird der Eintrag mit `A` gekennzeichnet. Wenn es sich um eine IPv6-Adresse handelt, wird der Eintrag mit `AAAA` gekennzeichnet.

Anmerkung: IPv6-Syntax

Die Syntax des IPv6-Eintrags unterscheidet sich geringfügig von der Syntax von IPv4. Aufgrund der Möglichkeit einer Fragmentierung müssen Informationen zu fehlenden Bits vor der Adresse angegeben werden. Um die IPv6-Adresse mit dem erforderlichen Wert „0“ auszufüllen, fügen Sie an der korrekten Stelle in der Adresse zwei Doppelpunkte hinzu.

```
pluto     AAAA 2345:00C1:CA11::1234:5678:9ABC:DEF0
pluto     AAAA 2345:00D2:DA11::1234:5678:9ABC:DEF0
```

Zeile 20:

Der Alias `ntp` kann zur Adressierung von `dns` (`CNAME` steht für *canonical name* (kanonischer Name)) verwendet werden.

Die Pseudodomäne `in-addr.arpa` wird für Reverse-Lookups zur Auflösung von IP-Adressen in Hostnamen verwendet. Sie wird in umgekehrter Notation an den Netzwerk-Teil der Adresse angehängt. `192.168` wird also in `168.192.in-addr.arpa` aufgelöst. Weitere Informationen hierzu finden Sie unter *Beispiel 25.7, „Reverse-Lookup“*.

BEISPIEL 25.7 REVERSE-LOOKUP

```
1.  $TTL 2D
2.  168.192.in-addr.arpa.   IN SOA dns.example.com. root.example.com. (
3.                          2003072441      ; serial
4.                          1D              ; refresh
5.                          2H              ; retry
6.                          1W              ; expiry
7.                          2D )            ; minimum
8.
9.                          IN NS           dns.example.com.
10.
11. 1.5                     IN PTR          gate.example.com.
12. 100.3                   IN PTR          www.example.com.
13. 253.2                   IN PTR          cups.example.com.
```

Zeile 1:

$TTL definiert die Standard-TTL, die für alle Einträge hier gilt.

Zeile 2:

Die Konfigurationsdatei muss Reverse-Lookup für das Netzwerk `192.168` aktivieren. Wenn die Zone `168.192.in-addr.arpa` heißt, sollte sie nicht zu den Hostnamen hinzugefügt werden. Alle Domänen werden daher in vollständiger Form eingegeben: mit ihrer Domäne und mit schließendem „`.`“). Die restlichen Einträge entsprechen den im vorherigen Beispiel (`example.com`) beschriebenen Einträgen.

Zeilen 3-7:

Siehe vorheriges Beispiel für `example.com`.

Zeile 9:

Diese Zeile gibt wieder den für diese Zone verantwortlichen Namenserver 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.

25.7 Dynamische Aktualisierung von Zonendaten

Der Ausdruck *dynamische Aktualisierung* bezieht sich auf Vorgänge, bei denen Einträge in den Zonendateien eines Masterservers hinzugefügt, geändert oder gelöscht werden. Dieser Mechanismus wird in RFC 2136 beschrieben. Die dynamische Aktualisierung wird individuell für jeden Zoneneintrag durch Hinzufügen einer optionalen `allow-update`- bzw. `update-policy`-Regel konfiguriert. Dynamisch zu aktualisierende Zonen sollten nicht von Hand bearbeitet werden.

Die zu aktualisierenden Einträge werden mit dem Befehl **`nsupdate`** an den Server übermittelt. Die genaue Syntax dieses Befehls können Sie der man-Seite für nsupdate (**`man 8 nsupdate`**) entnehmen. Aus Sicherheitsgründen sollten solche Aktualisierungen mithilfe von TSIG-Schlüsseln durchgeführt werden, wie in *Abschnitt 25.8, „Sichere Transaktionen“* beschrieben.

25.8 Sichere Transaktionen

Sichere Transaktionen können mit 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 mit dem folgenden Befehl einen TSIG-Schlüssel (genauere Informationen 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` eingefügt werden. Zum Einschließen einer externen Datei verwenden Sie:

```
include  "filename"
```

Ersetzen Sie `filename` durch einen absoluten Pfad zu Ihrer Datei mit den Schlüsseln.

Damit Server `host1` den Schlüssel für `host2` verwenden kann (in diesem Beispiel mit der Adresse `10.1.2.3`), muss die Datei `/etc/named.conf` des Servers folgende Regel enthalten:

```
server 10.1.2.3 {
  keys { host1-host2. ;};
};
```

Analoge Einträge müssen in die Konfigurationsdateien von `host2` aufgenommen werden.

Fügen Sie TSIG-Schlüssel für alle ACLs (Access Control Lists, Zugriffssteuerungslisten, nicht zu verwechseln mit Dateisystem-ACLs) hinzu, die für IP-Adressen und -Adressbereiche definiert sind, um Transaktionssicherheit zu gewährleisten. Der entsprechende Eintrag könnte wie folgt aussehen:

```
allow-update { key host1-host2. ;};
```

Dieses Thema wird eingehender im *Referenzhandbuch für BIND-Administratoren* (unter `update-policy`) erörtert.

25.9 DNS-Sicherheit

DNSSEC (DNS-Sicherheit) wird in RFC 2535 beschrieben. Die für DNSSEC verfügbaren Werkzeuge werden im BIND-Handbuch erörtert.

Einer als sicher betrachteten Zone müssen ein oder mehrere Zonenschlüssel zugeordnet sein. Diese werden mit **`dnssec-keygen`** erstellt, genau wie die Host-Schlüssel. Zurzeit wird der DSA-Verschlüsselungsalgorithmus zum Erstellen dieser Schlüssel verwendet. Die generierten öffentlichen Schlüssel sollten mithilfe einer `$INCLUDE`-Regel in die entsprechende Zonendatei aufgenommen werden.

Mit dem Kommando **`dnssec-signzone`** können Sie Sets von generierten Schlüsseln (`keyset-` Dateien) erstellen, sie auf sichere Weise in die übergeordnete Zone übertragen und sie signieren. Auf diese Weise werden die Dateien generiert, die in die einzelnen Zonen in `/etc/named.conf` aufgenommen werden sollen.

25.10 Weiterführende Informationen

Weitere Informationen können Sie dem *Referenzhandbuch für BIND-Administratoren* im Paket `bind-doc` entnehmen, das unter `/usr/share/doc/packages/bind/arm` installiert ist. Außerdem könnten Sie die RFCs zurate ziehen, auf die im Handbuch verwiesen wird, sowie die in BIND enthaltenen man-Seiten. `/usr/share/doc/packages/bind/README.SUSE` enthält aktuelle Informationen zu BIND in SUSE Linux Enterprise Server.

26 DHCP

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 Clientseite den NetworkManager verwenden, brauchen Sie den Client 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 z Systems: DHCP-Unterstützung

Auf IBM z Systems-Plattformen funktioniert DHCP nur bei Schnittstellen, die die OSA- und OSA Express-Netzwerkkarten verwenden. Nur diese Karten verfügen über eine für die Autokonfigurationsfunktionen von DHCP erforderliche MAC-Adresse.

Eine Möglichkeit zur Konfiguration von DHCP-Servern besteht darin, jeden Client mithilfe der Hardwareadresse seiner Netzwerkkarte zu identifizieren (die in den meisten Fällen statisch ist) und anschließend diesen Client bei jeder Verbindung zum Server mit identischen Einstellungen zu versorgen. Zum anderen kann DHCP aber auch so konfiguriert werden, dass der Server jedem relevanten Client 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.

In diesem Kapitel wird der DHCP-Server im gleichen Subnetz wie die Workstations (`192.168.2.0/24`) mit `192.168.2.1` als Gateway ausgeführt. Er hat die feste IP-Adresse `192.168.2.254` und bedient die beiden Adressbereiche `192.168.2.10` bis `192.168.2.20` und `192.168.2.100` bis `192.168.2.200`.

Neben IP-Adresse und Netzmaske werden dem Client nicht nur der Computer- und Domänenname, sondern auch das zu verwendende Gateway und die Adressen der Nameserver mitgeteilt. Im Übrigen können auch mehrere andere Parameter zentral konfiguriert werden, z. B. ein Zeitserver, von dem die Clients die aktuelle Uhrzeit abrufen können, oder ein Druckserver.

26.1 Konfigurieren eines DHCP-Servers mit YaST

Zur Installation eines DNS-Servers starten Sie YaST, und wählen Sie *Software* › *Software installieren oder löschen*. Wählen Sie *Filter* › *Schemata* und schließlich *DHCP- und DNS-Server* aus. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

Wichtig: LDAP-Unterstützung

Das DHCP-Modul von YaST kann 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. Soll LDAP verwendet werden, richten Sie die LDAP-Umgebung ein, bevor Sie den DHCP-Server konfigurieren.

Weitere Informationen zu LDAP finden Sie unter *Buch „Security Guide", Kapitel 5 „LDAP—A Directory Service"*.

Das DHCP-Modul von YaST (`yast2-dhcp-server`) ermöglicht die Einrichtung Ihres eigenen DHCP-Servers für das lokale Netzwerk. Das Modul kann im Assistentenmodus oder im Expertenkonfigurationsmodus ausgeführt werden.

26.1.1 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. Führen Sie dazu die folgenden Schritte aus:

1. Wählen Sie in dieser Liste die Schnittstelle aus, die der DHCP-Server überwachen soll, und klicken Sie auf *Auswählen*. Wählen Sie anschließend die Option *Firewall für gewählte Schnittstelle öffnen*, um die Firewall für diese Schnittstelle zu öffnen, und klicken Sie auf *Weiter*. Weitere Informationen hierzu finden Sie unter *Abbildung 26.1, „DHCP-Server: Kartenauswahl“*.

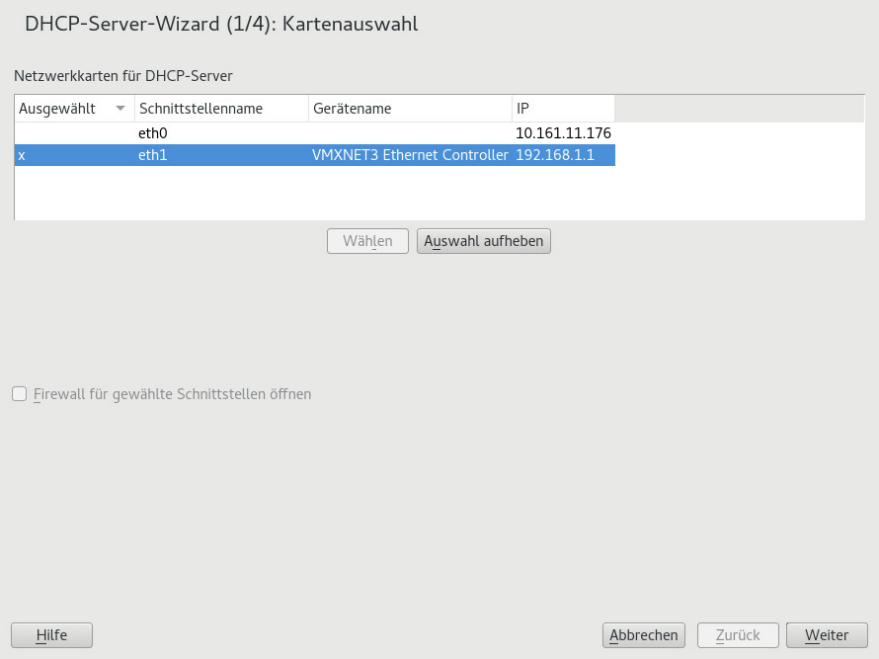


ABBILDUNG 26.1 DHCP-SERVER: KARTENAUSWAHL

2. Geben Sie anhand des Kontrollkästchens an, ob Ihre DHCP-Einstellungen automatisch von einem LDAP-Server gespeichert werden sollen. In den Textfeldern 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 Namenserver, Adressen eines Druck- und WINS-Servers (für gemischte Netzwerkumgebungen mit Windows- und Linux-Clients), Gateway-Adressen und Leasing-Zeit. Weitere Informationen hierzu finden Sie unter *Abbildung 26.2, „DHCP-Server: Globale Einstellungen“*.

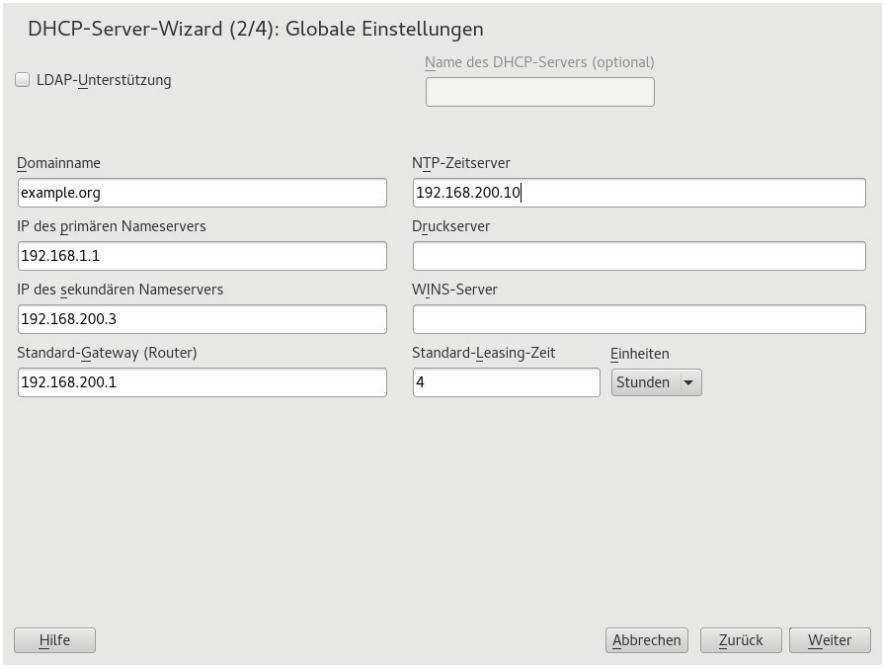


ABBILDUNG 26.2 DHCP-SERVER: GLOBALE EINSTELLUNGEN

3. 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. Weitere Informationen hierzu finden Sie unter *Abbildung 26.3, „DHCP-Server: Dynamisches DHCP“*.

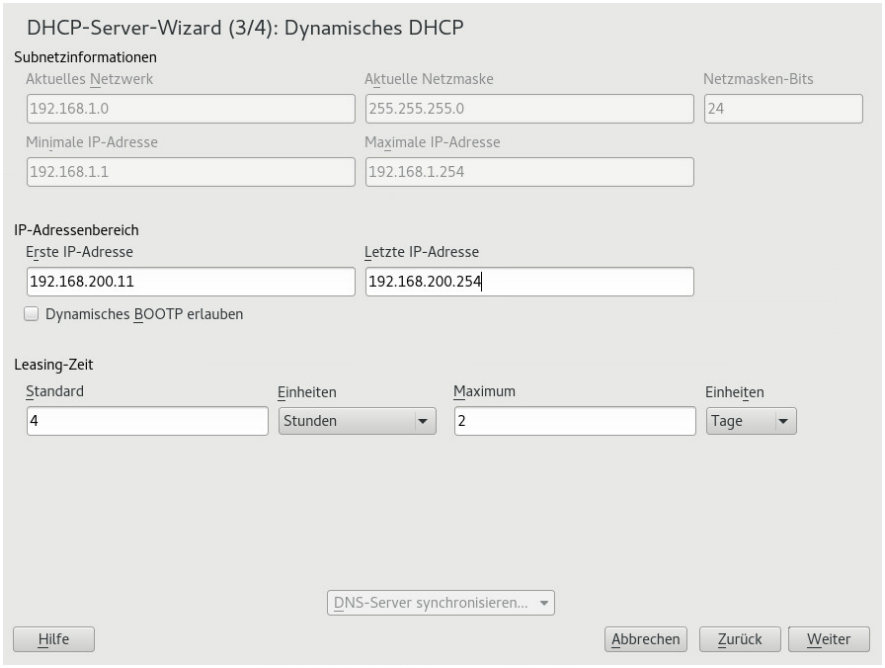


ABBILDUNG 26.3 DHCP-SERVER: DYNAMISCHES DHCP

4. Geben Sie an, auf welche Weise der DHCP-Server gestartet werden soll. Legen Sie fest, ob der DHCP-Server automatisch beim Booten des Systems oder bei Bedarf manuell (z. B. zu Testzwecken) gestartet werden soll. Klicken Sie auf *Verlassen*, um die Konfiguration des Servers abzuschließen. Weitere Informationen hierzu finden Sie unter *Abbildung 26.4, „DHCP-Server: Start“*.

ABBILDUNG 26.4 DHCP-SERVER: START

5. Statt der Verwendung des dynamischen DHCP, wie in den vorigen Schritten beschrieben, können Sie den Server auch so konfigurieren, dass Adressen in fast statischer Weise zugewiesen werden. Geben Sie in die Textfelder im unteren Teil eine Liste der in dieser Art zu verwaltenden Clients ein. Geben Sie vor allem *Name* und *IP-Adresse* für einen solchen Client an, die *Hardware-Adresse* und den *Netzwerktyp* (Token-Ring oder Ethernet). Ändern Sie die oben angezeigte Liste der Clients mit *Hinzufügen*, *Bearbeiten* und *Löschen*. Weitere Informationen hierzu finden Sie unter *Abbildung 26.5, „DHCP-Server: Host-Verwaltung“*.

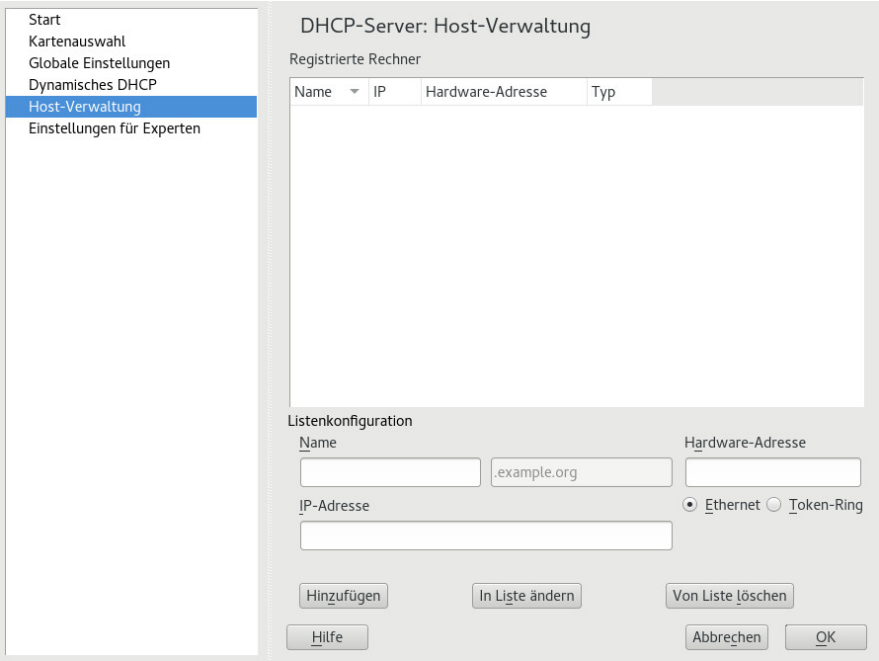


ABBILDUNG 26.5 DHCP-SERVER: HOST-VERWALTUNG

26.1.2 DHCP-Server-Konfiguration (Experten)

Zusätzlich zu den bisher erwähnten Konfigurationsmethoden gibt es einen Expertenkonfigurationsmodus, mit dem Sie die Einrichtung des DHCP-Servers detailgenau ändern können. Zum Starten der Expertenkonfiguration klicken Sie auf *Expertenkonfiguration für DHCP-Server* im Dialogfeld *Start* (siehe *Abbildung 26.4, „DHCP-Server: Start“*).

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 im Chroot-Jail und kann auf den Rest des Systems nicht zugreifen. Im unteren Bereich des Dialogfelds sehen Sie eine Baumstruktur mit den bereits definierten Deklarationen. Diese verändern Sie mit *Hinzufügen*, *Löschen* und *Bearbeiten*. Wenn Sie *Erweitert* wählen, werden zusätzliche Experten-Dialogfelder angezeigt. Weitere Informationen hierzu finden Sie unter *Abbildung 26.6, „DHCP-Server: Chroot Jail und Deklarationen“*. Nach der Auswahl von *Hinzufügen* legen Sie den hinzuzufügenden Deklara-

tionstyp 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.

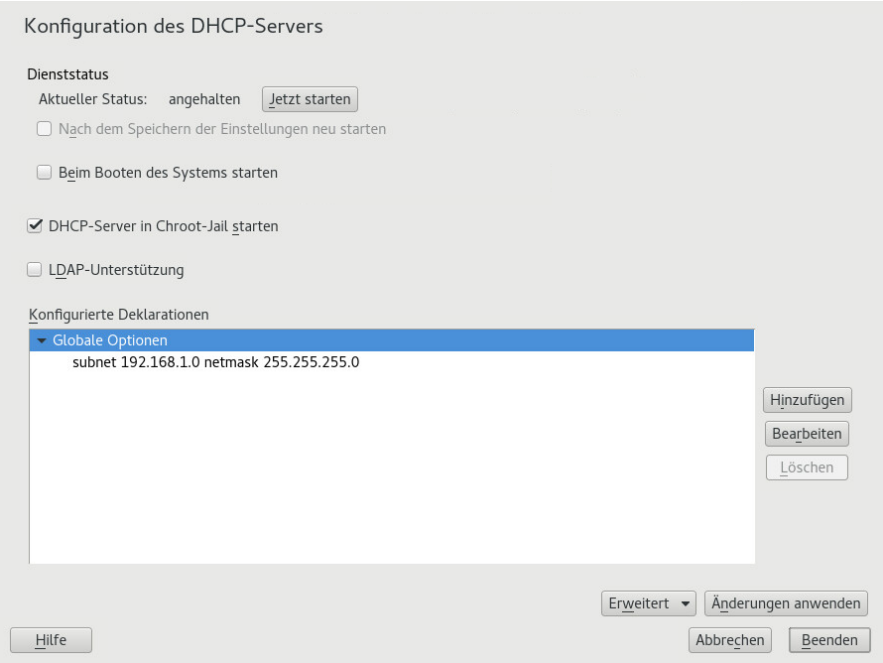


ABBILDUNG 26.6 DHCP-SERVER: CHROOT JAIL UND DEKLARATIONEN

Auswählen des Deklarationstyps

Die *Globalen Optionen* des DHCP-Servers bestehen aus mehreren 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 Subnetzes (siehe *Abbildung 26.7, „DHCP-Server: Wählen eines Deklarationstyps“*).

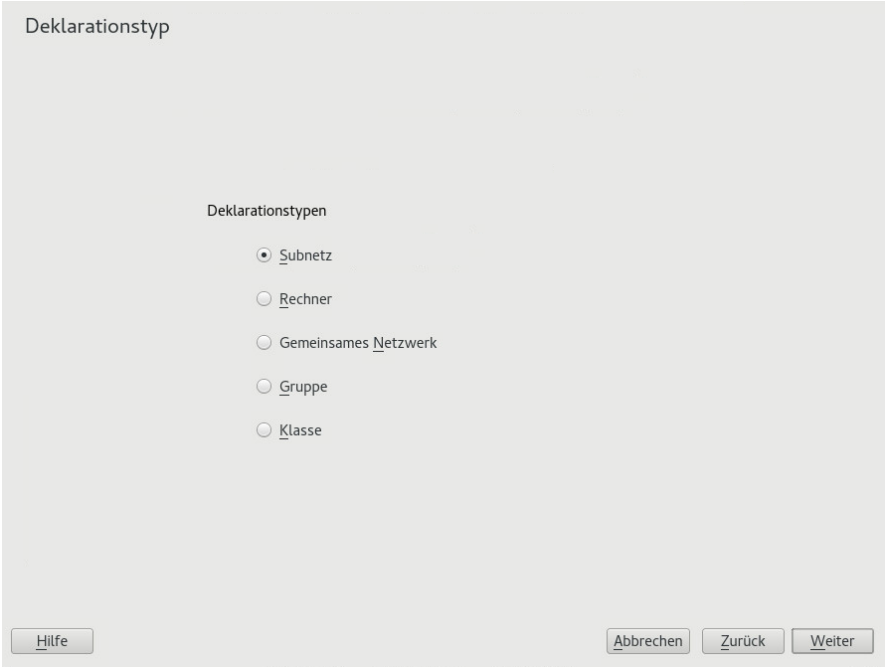


ABBILDUNG 26.7 DHCP-SERVER: WÄHLEN EINES DEKLARATIONSTYPS

Konfiguration des Subnetzes

In diesem Dialogfeld können Sie ein neues Subnetz mit seiner IP-Adresse und Netzmaske angeben. In der Mitte des Dialogfelds ändern Sie die Startoptionen des DHCP-Servers für das ausgewählte Subnetz mit den Optionen *Hinzufügen*, *Bearbeiten* und *Löschen*. Um einen dynamischen DNS für das Subnetz einzurichten, wählen Sie *Dynamisches DNS*.

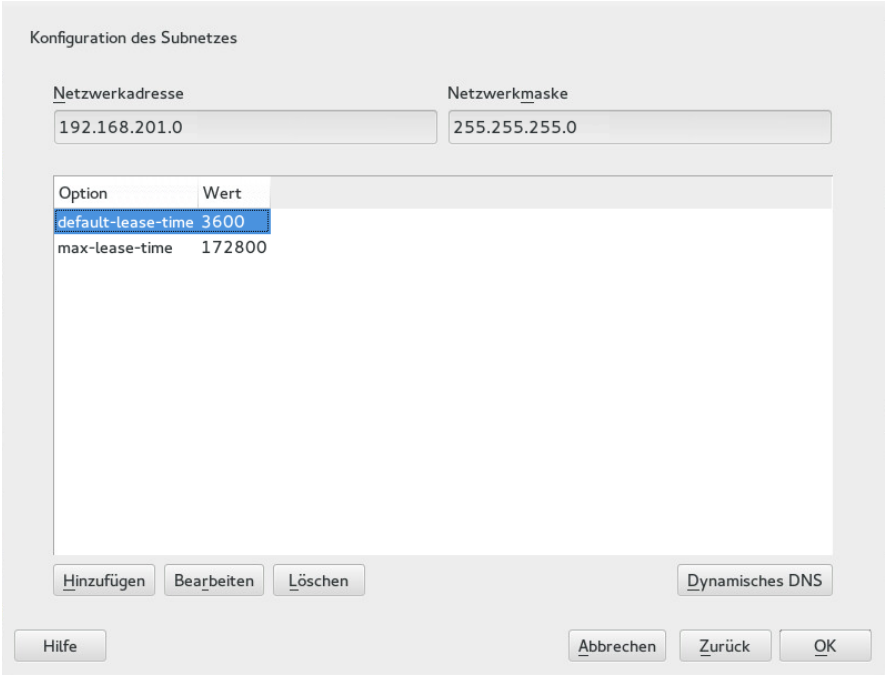


ABBILDUNG 26.8 DHCP-SERVER: KONFIGURIEREN VON SUBNETZEN

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 26.10, „DHCP-Server: Schnittstellenkonfiguration für dynamisches DNS“*).

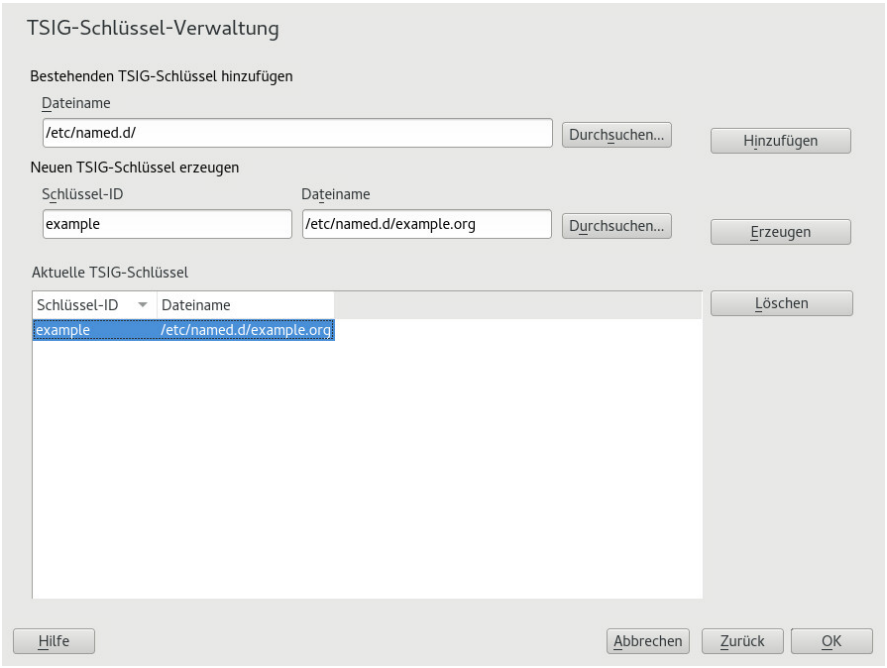


ABBILDUNG 26.9 DHCP SERVER: TSIG-KONFIGURATION

Dynamisches DNS: Schnittstellenkonfiguration

Jetzt können Sie das dynamische DNS für das Subnetz aktivieren, indem Sie *Dynamisches DNS für dieses Subnetz aktivieren* wählen. Danach aktivieren Sie im Dropdown-Feld 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 Namenserver für beide Zonen an. Wenn Sie *OK* wählen, gelangen Sie wieder zum Dialogfeld für die Subnetzkonfiguration (siehe *Abbildung 26.8, „DHCP-Server: Konfigurieren von Subnetzen“*). Wenn Sie noch einmal auf *OK* klicken, gelangen Sie wieder zum ursprünglichen Dialogfeld für die Expertenkonfiguration.

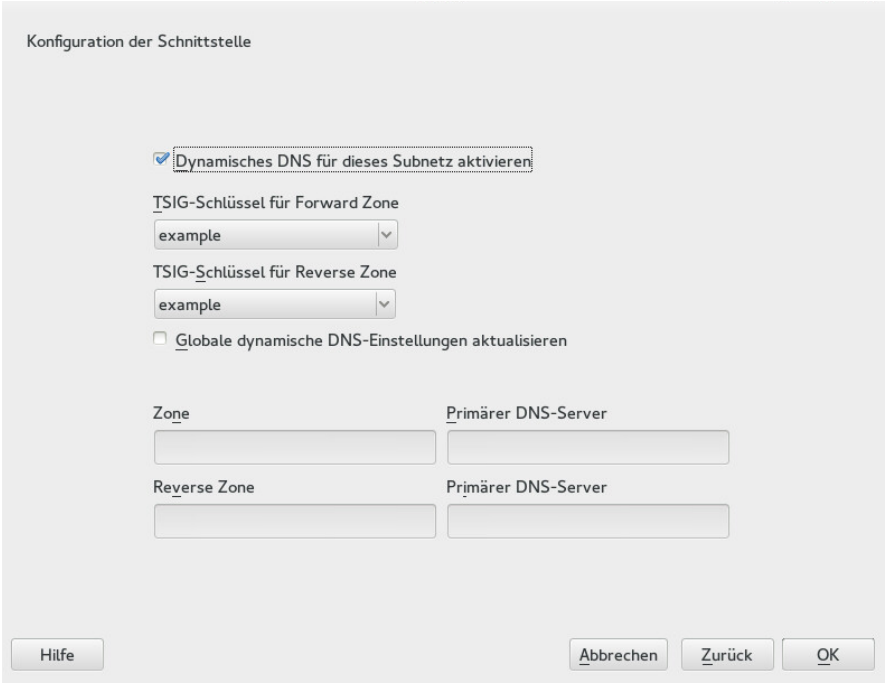


ABBILDUNG 26.10 DHCP-SERVER: SCHNITTSTELLENKONFIGURATION FÜR DYNAMISCHES DNS

Netzwerkschnittstellenkonfiguration

Wenn Sie die Schnittstellen festlegen möchten, die vom DHCP-Server überwacht werden sollen, und die Firewall-Konfiguration anpassen, wählen Sie im Dialogfeld für die Expertenkonfiguration *Erweitert* › *Schnittstellenkonfiguration*. In 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 müssen und der Server-Host durch eine Firewall geschützt ist, 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 26.11, „DHCP-Server: Netzwerkschnittstelle und Firewall“*). Jetzt können Sie zum ursprünglichen Dialogfeld zurückkehren, indem Sie auf *OK* klicken.

ABBILDUNG 26.11 DHCP-SERVER: NETZWERKSCHNITTSTELLE UND FIREWALL

Nach Abschluss aller Konfigurationsschritte schließen Sie das Dialogfeld mit *OK*. Der Server wird jetzt mit seiner neuen Konfiguration gestartet.

26.2 DHCP-Softwarepakete

Sowohl der DHCP-Server als auch die DHCP-Clients stehen für SUSE Linux Enterprise Server zur Verfügung. Der vom Internet Systems Consortium (ISC) herausgegebene DHCP-Server `dhcpd` stellt die Serverfunktionalität zur Verfügung. Auf der Clientseite befinden sich `dhcp-client` (ebenfalls von ISC) sowie Werkzeuge aus dem `wicked`-Paket.

Standardmäßig werden die `wicked`-Werkzeuge mit den Diensten `wicked-dhcp4` und `wicked-dhcp6` installiert. Beide Services werden automatisch bei jedem Booten des Systems gestartet und übernehmen die Überwachung auf einem DHCP-Server. Sie kommen ohne eine Konfigu-

rationsdatei aus und funktionieren im Normalfall ohne weitere Konfiguration. Für komplexere Situationen greifen Sie auf `dhcp-client` von ISC zurück, das sich über die Konfigurationsdateien `/etc/dhclient.conf` und `/etc/dhclient6.conf` steuern lässt.

26.3 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 26.1, „Die Konfigurationsdatei „/etc/dhcpd.conf““* an.

BEISPIEL 26.1 DIE KONFIGURATIONSDATEI „/ETC/DHCPD.CONF“

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "example.com";
option domain-name-servers 192.168.1.116;
option broadcast-address 192.168.2.255;
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0
 {
  range 192.168.2.10 192.168.2.20;
  range 192.168.2.100 192.168.2.200;
 }
```

Diese einfache Konfigurationsdatei reicht bereits aus, damit der DHCP-Server im Netzwerk IP-Adressen zuweisen kann. Bitte achten Sie insbesondere auf die Semikolons am Ende jeder Zeile, ohne die dhcpd nicht startet.

Die Beispieldatei lässt sich in drei Abschnitte unterteilen. Im ersten Abschnitt wird definiert, wie viele Sekunden eine IP-Adresse standardmäßig an einen anfragenden Client geleast wird, bevor dieser eine Verlängerung anfordern sollte (`default-lease-time`). Hier wird auch festgelegt, wie lange ein Computer maximal eine vom DHCP-Server vergebene IP-Adresse behalten darf, ohne für diese eine Verlängerung anfordern zu müssen (`max-lease-time`).

Im zweiten Abschnitt werden einige grundsätzliche Netzwerkparameter global festgelegt:

- Die Zeile `option domain-name` enthält die Standarddomäne des Netzwerks.
- Mit dem Eintrag `option domain-name-servers` können Sie bis zu drei Werte für die DNS-Server angeben, die zur Auflösung von IP-Adressen in Hostnamen (und umgekehrt) verwendet werden sollen. Idealerweise sollten Sie vor dem Einrichten von DHCP einen Namenserver auf dem Computer oder im Netzwerk konfigurieren. Dieser Nameserver sollte für jede dynamische Adresse jeweils einen Hostnamen und umgekehrt bereithalten. Weitere Informationen zum Konfigurieren eines eigenen Namenservers finden Sie in *Kapitel 25, Domain Name System (DNS)*.
- 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. In der Regel ist gerade bei kleineren Netzwerken 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 26.1, „Die Konfigurationsdatei „/etc/dhcpd.conf““* können Clients Adressen zwischen `192.168.2.10` und `192.168.2.20` oder `192.168.2.100` und `192.168.2.200` zugewiesen werden.

Nach dem Bearbeiten dieser wenigen Zeilen sollten Sie bereits in der Lage sein, den DHCP-Daemon mit dem Befehl **`systemctl start dhcpd`** zu aktivieren. Der DHCP-Daemon ist sofort einsatzbereit. Mit dem Befehl **`rcdhcpd`** `check-syntax` können Sie eine kurze Überprüfung der Konfigurationsdatei vornehmen. Sollte wider Erwarten ein Problem mit der Konfiguration auftreten (der Server wird beispielsweise mit einem Fehler beendet oder gibt beim Starten nicht `done` zurück), finden Sie in der zentralen Systemprotokolldatei, die mit dem Kommando **`journalctl`** abgefragt werden kann, weitere Informationen dazu (siehe *Kapitel 15, **`journalctl`**: Abfragen des `systemd`-Journals*).

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 **`systemctl start dhcpd`** eingeben und die Dateien werden automatisch kopiert.

26.3.1 Clients mit statischen IP-Adressen

DHCP lässt sich auch verwenden, um einem bestimmten Client eine vordefinierte statische Adresse zuzuweisen. Solche expliziten Adresszuweisungen haben Vorrang vor dynamischen Adressen aus dem Pool. Im Unterschied zu den dynamischen verfallen die statischen Adressinformationen nie, z. B. wenn nicht mehr genügend freie Adressen zur Verfügung stehen und deshalb eine Neuverteilung unter den Clients erforderlich ist.

Zur Identifizierung eines mit einer statischen Adresse konfigurierten Clients verwendet dhcpd die Hardware-Adresse. Dies ist eine global eindeutige, fest definierte Zahl aus sechs Oktettpaaren, über die jedes Netzwerkgerät verfügt, z. B. `00:30:6E:08:EC:80`. Werden die entsprechenden Zeilen, wie z. B. in *Beispiel 26.2, „Ergänzungen zur Konfigurationsdatei“* zur Konfigurationsdatei von *Beispiel 26.1, „Die Konfigurationsdatei „/etc/dhcpd.conf““* hinzugefügt, weist der DHCP-Daemon dem entsprechenden Client immer dieselben Daten zu.

BEISPIEL 26.2 ERGÄNZUNGEN ZUR KONFIGURATIONSDATEI

```
host jupiter {
hardware ethernet 00:30:6E:08:EC:80;
fixed-address 192.168.2.100;
}
```

Der Name des entsprechenden Clients (`host` *`HOSTNAME`*, hier `jupiter`) wird in die erste Zeile und die MAC-Adresse wird in die zweite Zeile eingegeben. Auf Linux-Hosts kann die MAC-Adresse mit dem Befehl **`ip`** `link show` gefolgt vom Netzwerkgerät (z. B. `eth0`) ermittelt werden. Die Ausgabe sollte in etwa wie folgt aussehen:

```
link/ether 00:30:6E:08:EC:80
```

Im vorherigen Beispiel wird also dem Client, dessen Netzwerkkarte die MAC-Adresse `00:30:6E:08:EC:80` hat, automatisch die IP-Adresse `192.168.2.100` und der Hostname `jupiter` zugewiesen. Als Hardwaretyp kommt heutzutage in aller Regel `ethernet` zum Einsatz, wobei durchaus auch das vor allem bei IBM-Systemen häufig zu findende `token-ring` unterstützt wird.

26.3.2 Die SUSE Linux Enterprise Server-Version

Aus Sicherheitsgründen enthält bei SUSE Linux Enterprise Server der DHCP-Server von ISC den non-root/chroot-Patch von Ari Edelkind. Damit kann dhcpd mit der Benutzer-ID `nobody` und in einer chroot-Umgebung (`/var/lib/dhcp`) ausgeführt werden. Um dies zu ermöglichen, muss sich die Konfigurationsdatei `dhcpd.conf` im Verzeichnis `/var/lib/dhcp/etc` befinden. Sie wird vom Init-Skript beim Start automatisch dorthin kopiert.

Dieses Verhalten lässt sich über Einträge in der Datei `/etc/sysconfig/dhcpd` steuern. Um den dhcpd ohne chroot-Umgebung laufen zu lassen, setzen Sie die Variable `DHCPD_RUN_CHROOTED` in der Datei `/etc/sysconfig/dhcpd` auf „no“.

Damit der dhcpd auch in der chroot-Umgebung Hostnamen auflösen kann, müssen außerdem einige weitere Konfigurationsdateien kopiert werden:

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

Diese Dateien werden beim Starten des Init-Skripts in das Verzeichnis `/var/lib/dhcp/etc/` kopiert. Berüchsichtigen Sie die Kopien bei Aktualisierungen, die benötigt werden, wenn sie durch ein Skript wie `/etc/ppp/ip-up` dynamisch modifiziert werden. Falls in der Konfigurationsdatei anstelle von Hostnamen nur IP-Adressen verwendet werden, sind jedoch keine Probleme zu erwarten.

Wenn in Ihrer Konfiguration weitere Dateien in die chroot-Umgebung kopiert werden müssen, können Sie diese mit der Variablen `DHCPD_CONF_INCLUDE_FILES` in der Datei `/etc/sysconfig/dhcpd` festlegen. Damit der dhcp-Daemon aus der chroot-Umgebung heraus auch nach einem Neustart des syslog-Daemons weiter protokollieren kann, befindet sich der zusätzliche Eintrag `SYSLOGD_ADDITIONAL_SOCKET_DHCP` in der Datei `/etc/sysconfig/syslog`.

26.4 Weiterführende Informationen

Weitere Informationen zu DHCP finden Sie auf der Website des *Internet Systems Consortium* (http://www.isc.org/products/DHCP/). Weitere Informationen finden Sie zudem auf den man-Seiten `dhcpd`, `dhcpd.conf`, `dhcpd.leases` und `dhcp-options`.

27 Verteilte Nutzung von Dateisystemen mit NFS

Das *NFS*-Protokoll (*Network File System*) sorgt für den Zugriff auf Dateien auf einem Server, der ähnlich wie der Zugriff auf lokale Dateien erfolgt.

27.1 Überblick

Über das standardisierte, erprobte und weithin unterstützte NFS-Netzwerkprotokoll (*Network File System*) können Dateien durch separate Hosts gemeinsam genutzt werden.

Über den NIS (*Network Information Service*) lässt sich eine zentrale Benutzerverwaltung im Netzwerk einrichten. Die Kombination aus NFS und NIS sorgt für die Zugriffskontrolle im Netzwerk anhand von Datei- und Verzeichnisrechten. NFS mit NIS macht ein Netzwerk für den Benutzer transparent.

In der Standardkonfiguration vertraut NFS dem Netzwerk uneingeschränkt – und damit auch jedem Computer, der mit einem vertrauenswürdigen Netzwerk verbunden ist. Alle Benutzer mit Administratorrechten auf einem Computer mit physischem Zugriff auf ein Netzwerk, dem der NFS-Server vertraut, können auf sämtliche Dateien zugreifen, die der Server zur Verfügung stellt.

Diese Sicherheitsstufe reicht in vielen Fällen aus, beispielsweise wenn das vertrauenswürdige Netzwerk tatsächlich vollständig privat ist, das Netzwerk sich in einem einzigen Schrank oder Computerraum befindet und kein unbefugter Zugriff möglich ist. In anderen Fällen ist die Notwendigkeit, einem ganzen Teilnetz als einer einzigen Einheit zu vertrauen, dagegen restriktiv und es besteht Bedarf an einem feiner abgestuften Vertrauensverhältnis. Für diese Fälle unterstützt NFS verschiedene Sicherheitsstufen mithilfe der *Kerberos*Infrastruktur. Für Kerberos ist NFSv4 erforderlich, wobei diese Version standardmäßig verwendet wird. Weitere Informationen finden Sie im *Buch „*Security Guide*", Kapitel 6 „Network Authentication with Kerberos"*.

Die folgenden Begriffe werden im YaST-Modul verwendet.

Exporte

Ein von einem NFS-Server *exportiertes* Verzeichnis, das von Clients in ihr System integriert werden kann.

NFS-Client

Der NFS-Client ist ein System, das NFS-Dienste eines NFS-Servers über das NFS-Protokoll verwendet. Das TCP/IP-Protokoll ist bereits in den Linux-Kernel integriert, weshalb keine zusätzliche Software installiert werden muss.

NFS-Server

Der NFS-Server stellt NFS-Dienste für Clients bereit. Ein laufender Server ist von den folgenden Daemons abhängig: `nfsd` (Worker), `idmapd` (ID-Name-Zuordnung für NFSv4, nur für bestimmte Szenarien), `statd` (Dateisperren) und `mountd` (Einhängeanforderungen).

NFSv3

NFSv3 ist die Implementierungsversion 3, die „alte“ zustandslose NFS, die die Clientauthentifizierung unterstützt.

NFSv4

NFSv4 ist die neue Implementationsversion 4, die die sichere Benutzerauthentifizierung über Kerberos unterstützt. Für NFSv4 ist nur ein einzelner Port erforderlich; diese Version eignet sich daher besser für Umgebungen hinter einer Firewall als NFSv3.
Das Protokoll wird als http://tools.ietf.org/html/rfc3530 angegeben.

pNFS

Parallel NFS, eine Protokollerweiterung für NFSv4. Alle pNFS-Clients können direkt auf die Daten auf einem NFS-Server zugreifen.

Wichtig: DNS erforderlich

Im Prinzip können alle Exporte allein mit IP-Adressen vorgenommen werden. Es ist ratsam, über ein funktionierendes DNS-System zu verfügen, um Zeitüberschreitungen zu vermeiden. DNS ist zumindest für die Protokollierung erforderlich, weil der mountd-Daemon Reverse-Lookups ausführt.

27.2 Installieren des NFS-Servers

Der NFS-Server ist kein Bestandteil der Standardinstallation. Zum Installieren des NFS-Servers mit YaST wählen Sie *Software* › *Software installieren oder löschen*, wählen Sie *Schemata* und aktivieren Sie die Option *Dateiserver* im Abschnitt *Serverfunktionen*. Klicken Sie auf *Übernehmen*. Die erforderlichen Pakete werden installiert.

Wie NIS ist NFS ein Client-Server-System. Ein Rechner kann jedoch beides gleichzeitig sein – er kann Dateisysteme im Netzwerk zur Verfügung stellen (exportieren) und Dateisysteme anderer Hosts mounten (importieren).

Anmerkung: Lokales Einhängen von NFS-Volumes auf dem exportierenden Server

Das lokale Einhängen von NFS-Volumes auf dem exportierenden Server wird in SUSE Linux Enterprise Server nicht unterstützt.

27.3 Konfigurieren des NFS-Servers

Die Konfiguration eines NFS-Servers kann über YaST oder manuell erfolgen. NFS kann für die Authentifizierung auch mit Kerberos kombiniert werden.

27.3.1 Exportieren von Dateisystemen mit YaST

Mit YaST können Sie einen Computer im Netzwerk als NFS-Server bereitstellen. Dies ist ein Server, der Verzeichnisse und Dateien an alle Hosts, die ihm Zugriff gewähren, oder an alle Mitglieder einer Gruppe exportiert. Der Server kann so außerdem Anwendungen bereitstellen, ohne dass die Anwendungen auf allen Hosts lokal installiert sein müssen.

Verfahren Sie wie folgt, um einen solchen Server einzurichten:

PROZEDUR 27.1 EINRICHTEN EINES NFS-SERVERS

1. Starten Sie YaST, und wählen Sie *Netzwerkdienste* › *NFS-Server* (siehe *Abbildung 27.1, „Konfiguration des NFS-Servers“*). Sie werden ggf. aufgefordert, weitere Software zu installieren.

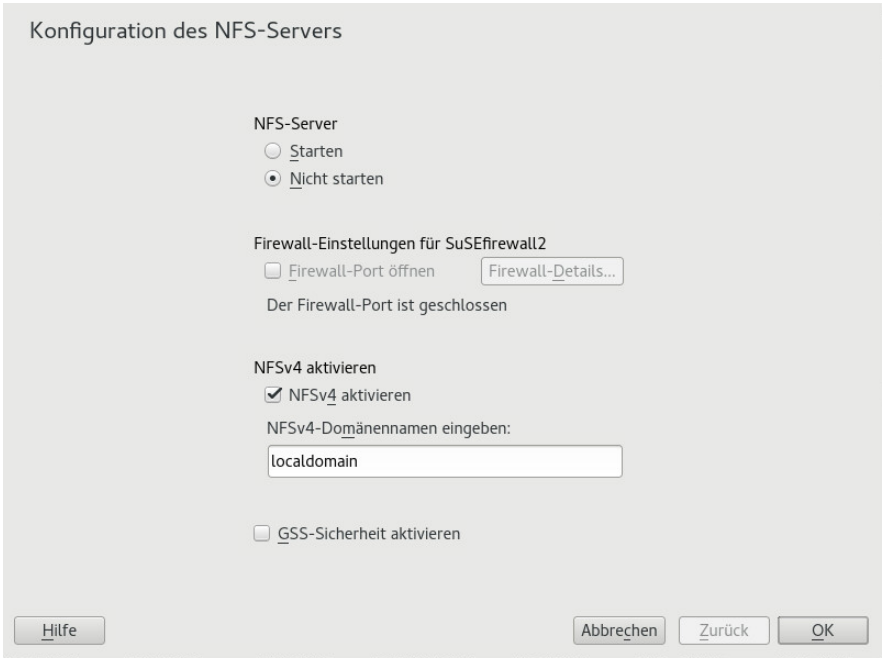


ABBILDUNG 27.1 KONFIGURATION DES NFS-SERVERS

2. Aktivieren Sie das Optionsfeld *Start*.

3. Wenn eine Firewall im System aktiv ist (SuSEFirewall2), aktivieren Sie die Option *Firewall-Ports öffnen*. YaST aktiviert den `nfs`-Service und passt so die Konfiguration für den NFS-Server an.

4. Überlegen Sie, ob die Verwendung der Option *NFSv4 aktivieren* angebracht ist. Wenn Sie NFSv4 deaktivieren, unterstützt YaST lediglich NFSv3. Informationen zum Aktivieren von NFSv2 finden Sie in *Anmerkung: NFSv2*.

   - Ist NFSv4 aktiviert, geben Sie außerdem den entsprechenden NFSv4-Domänennamen ein. Dieser Parameter gilt für den `idmapd`-Daemon, der für Kerberos-Einrichtungen oder für Fälle, in denen die Clients nicht mit numerischen Benutzernamen arbeiten können, erforderlich ist. Behalten Sie den Wert `localdomain` (den Standardwert) bei, wenn Sie `idmapd` nicht ausführen oder keine speziellen Anforderungen haben. Weitere Informationen zum `idmapd`-Daemon finden Sie unter `/etc/idmapd.conf`.

5. Klicken Sie auf *GSS-Sicherheit aktivieren*, wenn Sie einen sicheren Zugriff auf den Server benötigen. Als Voraussetzung hierfür muss Kerberos in der Domäne installiert sein und sowohl der Server als auch der Client müssen kerberisiert sein. Mit *Weiter* wechseln Sie zum nächsten Konfigurationsdialogfeld.

6. Klicken Sie im oberen Bereich des Dialogfelds auf *Verzeichnis hinzufügen*. Das Verzeichnis wird exportiert.

7. Falls Sie die zulässigen Hosts nicht bereits konfiguriert haben, wird automatisch ein weiteres Dialogfeld geöffnet, in dem Sie die Client-Informationen und Optionen angeben. Geben Sie den Platzhalter für den Host ein. (In der Regel können Sie die Standardeinstellungen beibehalten).
   Es gibt vier mögliche Typen von Platzhalterzeichen für den Host, die für jeden Host festgelegt werden können: ein einzelner Host (Name oder IP-Adresse), Netzgruppen, Platzhalterzeichen (wie `*`, womit angegeben wird, dass alle Computer auf den Server zugreifen können) und IP-Netzwerke.
   Weitere Informationen zu diesen Optionen finden Sie auf der man-Seite zu `exports`.

8. Klicken Sie zum Beenden der Konfiguration auf *Beenden*.

27.3.2 Manuelles Exportieren von Dateisystemen

Die Konfigurationsdateien für den NFS-Exportdienst lauten `/etc/exports` und `/etc/sysconfig/nfs`. Neben diesen Dateien ist `/etc/idmapd.conf` für die NFSv4-Serverkonfiguration mit kerberisiertem NFS oder für Fälle, in denen die Clients keine numerischen Benutzernamen verarbeiten können, erforderlich.

Führen Sie den Start bzw. Neustart der Dienste mit dem Befehl **`systemctl restart nfsserver.service`** aus. Hiermit wird auch der RPC-Portmapper neu gestartet, der vom NFS-Server benötigt wird.

Damit der NFS-Server bei jedem Booten gestartet wird, führen Sie **`sudo systemctl enable nfsserver`** aus.

Anmerkung: NFSv4

NFSv4 ist die aktuelle Version des NFS-Protokolls für SUSE Linux Enterprise Server. Die Verzeichnisse werden nunmehr in NFSv4 auf dieselbe Weise für das Exportieren vorbereitet wie in NFSv3.

In SUSE Linux Enterprise Server 11 war das Einhängen mit Einbindung in `/etc/exports` obligatorisch. Dies wird weiterhin unterstützt, ist jedoch überholt.

`/etc/exports`

Die Datei `/etc/exports` enthält eine Liste mit Einträgen. Mit jedem Eintrag wird ein Verzeichnis angegeben, das freigegeben wird. Zudem wird angegeben, wie das Verzeichnis freigegeben wird. Ein typischer Eintrag in `/etc/exports` besteht aus:

```
/SHARED/DIRECTORY   HOST(OPTION_LIST)
```

Beispiel:

```
/export/data   192.168.1.2(rw,sync)
```

Hier wird die IP-Adresse `192.168.1.2` verwendet, um den erlaubten Client zu identifizieren. Sie können auch den Namen des Hosts, ein Platzhalterzeichen, mit dem mehrere Hosts angegeben werden (`*.abc.com`, `*` usw.) oder Netzwerkgruppen (`@my-hosts`) verwenden).

Eine detaillierte Erläuterung aller Optionen und der entsprechenden Bedeutungen finden Sie auf der man-Seite zu **`exports`** (**`man exports`**).

Falls Sie `/etc/exports` bei laufendem NFS-Server geändert haben, müssen Sie den Server neu starten, damit die Änderungen in Kraft treten: **`sudo systemctl restart nfsserver`**.

`/etc/sysconfig/nfs`

Die Datei `/etc/sysconfig/nfs` enthält einige Parameter, die das Verhalten des NFSv4-Server-Daemon bestimmen. Der Parameter `NFS4_SUPPORT` muss dabei auf `yes` (Standard) gesetzt werden. Der Parameter `NFS4_SUPPORT` bestimmt, ob der NFS-Server NFSv4-Exporte und -Clients unterstützt.

Falls Sie `/etc/sysconfig/nfs` bei laufendem NFS-Server geändert haben, müssen Sie den Server neu starten, damit die Änderungen in Kraft treten: **`sudo systemctl restart nfsserver`**.

Tipp: Einhängeoptionen

In SUSE Linux Enterprise Server 11 war das Einhängen mit `--bind` in `/etc/exports` obligatorisch. Dies wird weiterhin unterstützt, ist jedoch überholt. Die Verzeichnisse werden nunmehr in NFSv4 auf dieselbe Weise für das Exportieren vorbereitet wie in NFSv3.

Anmerkung: NFSv2

Wenn NFS-Clients weiterhin von NFSv2 abhängig sind, aktivieren Sie es auf dem Server in `/etc/sysconfig/nfs`, indem Sie Folgendes festlegen:

```
NFSD_OPTIONS="-V2"
MOUNTD_OPTIONS="-V2"
```

Überprüfen Sie nach Neustart des Diensts mit dem folgenden Kommando, ob Version 2 verfügbar ist:

```
tux > cat /proc/fs/nfsd/versions
+2 +3 +4 +4.1 -4.2
```

`/etc/idmapd.conf`

Ab SLE 12 SP1 ist der `idmapd`-Daemon nur dann erforderlich, wenn die Kerberos-Authentifizierung verwendet wird oder die Clients keine numerischen Benutzernamen verarbeiten können. Linux-Clients können numerische Benutzernamen seit dem Linux-Kernel 2.6.39 verarbeiten. Der `idmapd`-Daemon führt die Name-ID-Zuordnung für NFSv4-Anforderungen an den Server aus und schickt Antworten an den Client.

Falls `idmapd` erforderlich ist, muss dieser Daemon auf dem NFSv4-Server ausgeführt werden. Die Name-ID-Zuordnung auf dem Client erfolgt mit **`nfsidmap`** das vom Paket bereitgestellt wird. `nfs-client`.

Stellen Sie sicher, dass Benutzernamen und IDs (uid) Benutzern auf eine einheitliche Weise auf allen Rechnern zugewiesen werden, auf denen möglicherweise Dateisysteme mit NFS freigegeben werden. Dies kann mit NIS, LDAP oder einem beliebigen einheitlichen Domänenauthentifizierungsmechanismus in Ihrer Domäne erreicht werden.

Der Parameter `Domain` muss in der Datei `/etc/idmapd.conf` für den Client und den Server identisch festgelegt sein. Wenn Sie sich nicht sicher sind, belassen Sie die Domäne in den Server- und den Clientdateien als `localdomain`. Eine Beispielkonfigurationsdatei sieht folgendermaßen aus:

```
[General]
Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]
Nobody-User = nobody
```

```
Nobody-Group = nobody
```

Starten Sie den `idmapd`-Daemon mit **`systemctl start nfs-idmapd`**. Falls Sie `/etc/idmapd.conf` bei laufendem Daemon geändert haben, müssen Sie den Daemon neu starten, damit die Änderungen in Kraft treten: **`systemctl start nfs-idmapd`**.
Weitere Informationen finden Sie auf den man-Seiten zu `idmapd` und `idmapd.conf` (`man idmapd` und `man idmapd.conf`).

27.3.3 NFS mit Kerberos

Wenn die Kerberos-Authentifizierung für NFS verwendet werden soll, muss die GSS-Sicherheit (Generic Security Services) aktiviert werden. Wählen Sie im ersten YaST-NFS-Server-Dialogfeld die Option *GSS-Sicherheit aktivieren*. Zur Verwendung dieser Funktion muss ein funktionierender Kerberos-Server zur Verfügung stehen. YaST richtet diesen Server nicht ein, sondern nutzt lediglich die über den Server bereitgestellten Funktionen. Wenn Sie die Authentifizierung mittels Kerberos verwenden möchten, müssen Sie zusätzlich zur YaST-Konfiguration mindestens die nachfolgend beschriebenen Schritte ausführen, bevor Sie die NFS-Konfiguration ausführen:

1. Stellen Sie sicher, dass sich Server und Client in derselben Kerberos-Domäne befinden. Beide müssen auf denselben KDC-Server (Key Distribution Center) zugreifen und die Datei `krb5.keytab` gemeinsam verwenden (der Standardspeicherort auf allen Rechnern lautet `/etc/krb5.keytab`). Weitere Informationen zu Kerberos finden Sie unter *Buch „*Security Guide*“, Kapitel 6 „Network Authentication with Kerberos“*.
2. Starten Sie den gssd-Dienst auf dem Client mit **`systemctl start rpc-gssd.service`**.
3. Starten Sie den svcgssd-Dienst auf dem Server mit **`systemctl start rpc-svcgssd.service`**.

Bei der Kerberos-Authentifizierung muss der `idmapd`-Daemon ebenfalls auf dem Server ausgeführt werden. Weitere Informationen finden Sie unter `/etc/idmapd.conf`.

Weitere Informationen zum Konfigurieren eines kerberisierten NFS finden Sie über die Links in *Abschnitt 27.5, „Weiterführende Informationen“*.

27.4 Konfigurieren der Clients

Wenn Sie Ihren Host als NFS-Client konfigurieren möchten, müssen Sie keine zusätzliche Software installieren. Alle erforderlichen Pakete werden standardmäßig installiert.

27.4.1 Importieren von Dateisystemen mit YaST

Autorisierte Benutzer können NFS-Verzeichnisse eines NFS-Servers über das YaST-NFS-Clientmodul in den lokalen Dateibaum einhängen. Führen Sie dazu die folgenden Schritte aus:

PROZEDUR 27.2 IMPORTIEREN VON NFS-VERZEICHNISSEN

1. Starten Sie das YaST-NFS-Client-Modul.
2. Klicken Sie auf dem Karteireiter *NFS-Freigaben* auf *Hinzufügen*. Geben Sie den Hostnamen des NFS-Servers, das zu importierende Verzeichnis und den Einhängepunkt an, an dem das Verzeichnis lokal eingehängt werden soll.
3. Wenn Sie NFSv4 verwenden, wählen Sie die Option *NFSv4 aktivieren* auf der Registerkarte *Einstellungen*. Der *NFSv4-Domainname* muss zudem denselben Wert aufweisen, der beim NFSv4-Server verwendet wird. Die Standarddomäne ist `localdomain`.
4. Wenn die Kerberos-Authentifizierung für NFS verwendet werden soll, muss die GSS-Sicherheit aktiviert werden. Wählen Sie *GSS-Sicherheit aktivieren*.
5. Wenn Sie eine Firewall nutzen und den Zugriff auf den Dienst von Ferncomputern aus zulassen möchten, aktivieren Sie auf dem Karteireiter *NFS-Einstellungen* die Option *Firewall-Port öffnen*. Der Status der Firewall wird neben dem Kontrollkästchen angezeigt.
6. Klicken Sie zum Speichern der Änderungen auf *OK*.

Die Konfiguration wird in `/etc/fstab` geschrieben und die angegebenen Dateisysteme werden eingehängt. Wenn Sie den YaST-Konfigurationsclient zu einem späteren Zeitpunkt starten, wird auch die vorhandene Konfiguration aus dieser Datei gelesen.

Tipp: NFS als Root-Dateisystem

Auf (festplattenlosen) Systemen, in denen die Stammpartition über das Netzwerk als NFS-Freigabe eingehängt ist, müssen Sie beim Konfigurieren des Netzwerkgeräts, über das die NFS-Freigabe erreichbar ist, besonders vorsichtig vorgehen.

Wenn Sie das System herunterfahren oder neu booten, werden in der standardmäßigen Reihenfolge zunächst die Netzwerkverbindungen deaktiviert und anschließend die Stammpartition ausgehängt. Bei einem NFS-Root kann dies zu Problemen führen: Die Stammpartition kann nicht fehlerfrei ausgehängt werden, da die Netzwerkverbindung zur

NFS-Freigabe schon nicht mehr aktiviert ist. Damit das System nicht das relevante Netzwerkgerät deaktiviert, öffnen Sie die Registerkarte gemäß *Abschnitt 16.4.1.2.5, „Aktivieren des Netzwerkgeräts“* und wählen Sie unter *Geräteaktivierung* die Option *Bei NFSroot*.

27.4.2 Manuelles Importieren von Dateisystemen

Voraussetzung für den manuellen Import eines Dateisystems von einem NFS-Server ist ein aktiver RPC-Port-Mapper. Der Start des `nfs`-Dienstes erfordert einige Vorsicht; starten Sie ihn daher mit **`systemctl start nfs`** als `root`. Danach können ferne Dateisysteme mit **`mount`** wie lokale Partitionen in das Dateisystem eingehängt werden:

```
tux > sudo mount HOST:REMOTE-PATHLOCAL-PATH
```

Geben Sie zum Beispiel zum Import von Benutzerverzeichnissen vom `nfs.example.com`-Rechner folgendes Kommando ein:

```
tux > sudo mount nfs.example.com:/home /home
```

27.4.2.1 Verwenden des Diensts zum automatischen Einhängen

Ferne Dateisysteme können mit dem autofs-Daemon automatisch eingehängt werden. Fügen Sie den folgenden Eintrag in der Datei `/etc/auto.master` hinzu:

```
/nfsmounts /etc/auto.nfs
```

Nun fungiert das Verzeichnis `/nfsmounts` als Root-Verzeichnis für alle NFS-Einhängungen auf dem Client, sofern die Datei `auto.nfs` entsprechend ausgefüllt wurde. Der Name `auto.nfs` wurde nur der Einfachheit halber ausgewählt – Sie können einen beliebigen Namen auswählen. Fügen Sie der Datei `auto.nfs` wie folgt Einträge für alle NFS-Einhängungen hinzu:

```
localdata -fstype=nfs server1:/data
nfs4mount -fstype=nfs4 server2:/
```

Aktivieren Sie die Einstellungen mit **`systemctl start autofs`** als `root`. In diesem Beispiel wird `/nfsmounts/localdata`, das Verzeichnis `/data` von `server1`, mit NFS eingehängt und `/nfsmounts/nfs4mount` von `server2` wird mit NFSv4 eingehängt.

Wenn die Datei `/etc/auto.master` während der Ausführung des autofs-Diensts bearbeitet wird, muss die automatische Einhängung mit **`systemctl restart autofs`** erneut gestartet werden, damit die Änderungen wirksam werden.

27.4.2.2 Manuelles Bearbeiten von `/ect/fstab`

Ein typischer NFSv3-Einhängeeintrag in `/etc/fstab` sieht folgendermaßen aus:

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

Bei NFSv4-Einhängepunkten geben Sie `nfs4` statt `nfs` in die dritte Spalte ein:

```
nfs.example.com:/data /local/pathv4 nfs4 rw,noauto 0 0
```

Mit der Option `noauto` wird verhindert, dass das Dateisystem beim Starten automatisch eingehängt wird. Wenn Sie das jeweilige Dateisystem manuell einhängen möchten, können Sie das Einhängekommando auch kürzen, indem Sie nur den Einhängepunkt angeben:

```
tux > sudo mount /local/path
```

Anmerkung: Einhängen beim Starten

Wenn die Option `noauto` nicht angegeben ist, wird das Einhängen dieser Dateisysteme beim Start durch die init-Skripte des Systems geregelt.

27.4.3 pNFS (paralleles NFS)

NFS wurde in den 1980er-Jahren entwickelt und gehört damit zu den ältesten Protokollen. Zum Freigeben kleinerer Dateien ist NFS völlig ausreichend. Wenn Sie dagegen große Dateien übertragen möchten oder wenn eine große Anzahl Clients auf die Daten zugreifen soll, wird ein NFS-Server rasch zu einer Engstelle, die die Systemleistungen erheblich beeinträchtigt. Dies liegt daran, dass die Dateien rasch größer werden, wobei die relative Ethernet-Geschwindigkeit nicht ganz mithalten kann.

Wenn Sie eine Datei von einem normalen NFS-Server anfordern, werden die Metadaten der Datei nachgeschlagen, die Daten dieser Datei werden zusammengestellt und die Datei wird schließlich über das Netzwerk an den Client übertragen. Der Leistungsengpass wird jedoch in jedem Fall ersichtlich, unabhängig davon, wie groß oder klein die Dateien sind:

- Bei kleinen Dateien dauert das Sammeln der Metadaten am längsten..
- Bei großen Dateien dauert das Übertragen der Daten vom Server auf den Client am längsten.

pNFS (paralleles NFS) trennt die Metadaten des Dateisystems vom Speicherort der Daten und überwindet so diese Einschränkungen. Für pNFS sind dabei zwei Arten von Servern erforderlich:

- Ein *Metadaten-* oder *Steuerungsserver*, der den gesamten verbleibenden Verkehr (nicht den Datenverkehr) abwickelt
- Mindestens ein *Speicherserver*, auf dem sich die Daten befinden

Der Metadatenserver und die Speicherserver bilden gemeinsam einen einzigen logischen NFS-Server. Wenn ein Client einen Lese- oder Schreibvorgang startet, teilt der Metadatenserver dem NFSv4-Client mit, auf welchem Speicherserver der Client auf die Dateiblöcke zugreifen soll. Der Client kann direkt auf dem Server auf die Daten zugreifen.

SUSE Linux Enterprise Server unterstützt pNFS nur auf der Clientseite.

27.4.3.1 Konfigurieren eines pNTP-Clients mit YaST

Befolgen Sie die Anweisungen unter *Prozedur 27.2, „Importieren von NFS-Verzeichnissen“*; aktivieren Sie jedoch das Kontrollkästchen *pNFS (v4.1)* und (optional) *NFSv4-Freigabe*. YaST führt alle erforderlichen Schritte aus und schreibt die erforderlichen Optionen in die Datei `/etc/exports`.

27.4.3.2 Manuelles Konfigurieren eines pNTP-Clients

Beginnen Sie gemäß *Abschnitt 27.4.2, „Manuelles Importieren von Dateisystemen“*. Der Großteil der Konfiguration wird durch den NFSv4-Server ausgeführt. Der einzige Unterschied für pNFS besteht darin, dass die Option `minorversion` und der Metadatenserver *`MDS_SERVER`* in das Kommando **`mount`** eingefügt werden:

```
tux > sudo mount -t nfs4 -o minorversion=1 MDS_SERVER MOUNTPOINT
```

Als Hilfe für die Fehlersuche ändern Sie den Wert im Dateisystem `/proc`:

```
tux > sudo echo 32767 > /proc/sys/sunrpc/nfsd_debug
tux > sudo echo 32767 > /proc/sys/sunrpc/nfs_debug
```

27.5 Weiterführende Informationen

Außer auf den man-Seiten zu **`exports`**, **`nfs`** und **`mount`** stehen Informationen zum Konfigurieren eines NFS-Servers und -Clients unter `/usr/share/doc/packages/nfsidmap/README` zur Verfügung. Weitere Online-Dokumentation finden Sie auf folgenden Websites:

- Die detaillierte technische Dokumentation finden Sie online unter SourceForge (http://nfs.sourceforge.net/).
- Anweisungen zum Einrichten eines kerberisierten NFS finden Sie unter NFS Version 4 Open Source Reference Implementation (http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html).
- Falls Sie Fragen zu NFSv4 haben, lesen Sie die Linux NFSv4-FAQ (http://www.citi.umich.edu/projects/nfsv4/linux/faq/).

28 Samba

Mit Samba kann ein Unix-Computer als Datei- und Druckserver für macOS-, Windows- und OS/2-Computer konfiguriert werden. Samba ist mittlerweile ein sehr umfassendes und komplexes Produkt. Konfigurieren Sie Samba mit YaST oder indem Sie die Konfigurationsdatei manuell bearbeiten.

28.1 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. Microsoft veröffentlichte das Protokoll, damit 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 z Systems: NetBIOS-Unterstützung

IBM z Systems 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 von Samba unterstütztes Protokoll. CIFS definiert ein Standardprotokoll für den Fernzugriff auf Dateisysteme über das Netzwerk, das Benutzergruppen die netzwerkweite Zusammenarbeit und gemeinsame Dokumentbenutzung ermöglicht.

NetBIOS

NetBIOS ist eine Softwareschnittstelle (API) für die Kommunikation zwischen Computern, die einen Name Service bereitstellen. Mit diesem Dienst können die an das Netzwerk angeschlossenen Computer Namen für sich reservieren. Nach dieser Reservierung können die Computer anhand ihrer Namen adressiert werden. Für die Überprüfung der Namen gibt

es keine zentrale Instanz. Jeder Computer im Netzwerk kann beliebig viele Namen reservieren, solange die Namen noch nicht Gebrauch sind. Die NetBIOS-Schnittstelle kann in unterschiedlichen Netzwerkarchitekturen implementiert werden. Eine Implementierung, die relativ eng mit der Netzwerkhardware arbeitet, ist NetBEUI (häufig auch als NetBIOS bezeichnet). Mit NetBIOS implementierte Netzwerkprotokolle sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

Die per TCP/IP übermittelten NetBIOS-Namen haben nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun. NetBIOS ist ein eigener, vollständig unabhängiger Namensraum. Es empfiehlt sich jedoch, für eine einfachere Administration NetBIOS-Namen zu vergeben, die den jeweiligen DNS-Hostnamen entsprechen, oder DNS nativ zu verwenden. Für einen Samba-Server ist dies die Voreinstellung.

Samba-Server

Samba-Server stellt SMB/CIFS-Dienste sowie NetBIOS over IP-Namensdienste für Clients zur Verfügung. Für Linux gibt es drei Dämonen für Samba-Server: smbd für SMB/CIFS-Dienste, nmbd für Naming Services und winbind für Authentifizierung.

Samba-Client

Der Samba-Client ist ein System, das Samba-Dienste von einem Samba-Server über das SMB-Protokoll nutzt. Das Samba-Protokoll wird von gängigen Betriebssystemen wie Windows und MacOS 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 den Samba-Client keinen Dämon auszuführen.

Freigaben

SMB-Server stellen den Clients Ressourcen 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. Clients können mit diesem Namen auf den Drucker zugreifen.

DC

Ein Domänencontroller (DC) ist ein Server, der Konten in der Domäne verwaltet. Zur Datenreplikation stehen zusätzliche Domain Controller in einer Domäne zur Verfügung.

28.2 Installieren eines Samba-Servers

Zur Installation eines Samba-Servers starten Sie YaST, und wählen Sie *Software* › *Software installieren oder löschen*. Wählen Sie *Anzeigen* › *Schemata* und dann *Dateiserver*. Bestätigen Sie die Installation der erforderlichen Pakete, um den Installationsvorgang abzuschließen.

28.3 Starten und Stoppen von Samba

Sie können den Samba-Server automatisch (beim Booten) oder manuell starten bzw. stoppen. Start- und Stopprichtlinien sind Teil der Samba-Serverkonfiguration mit YaST, die in *Abschnitt 28.4.1, „Konfigurieren eines Samba-Servers mit YaST“* beschrieben ist.

Beenden Sie die Dienste für Samba. Geben Sie hierzu in einer Befehlszeile den Befehl **`systemctl stop smb nmb`** ein und starten Sie die Dienste dann mit **`systemctl start nmb smb`** neu. `winbind` wird bei Bedarf durch den Dienst `smb` eingestellt.

Tipp: `winbind`

`winbind` ist ein unabhängiger Dienst und wird als solcher auch als einzelnes `samba-winbind`-Paket angeboten.

28.4 Konfigurieren eines Samba-Servers

Es gibt zwei Möglichkeiten, Samba-Server in SUSE® Linux Enterprise Server zu konfigurieren: mit YaST oder manuell. Bei der manuellen Konfiguration können Sie mehr Details einstellen, allerdings müssen Sie ohne den Komfort der Bedienoberfläche von YaST zurechtkommen.

28.4.1 Konfigurieren eines Samba-Servers mit YaST

Um einen Samba-Server zu konfigurieren, starten Sie YaST und wählen Sie *Netzwerkdienste* › *Samba-Server*.

28.4.1.1 Anfängliche Samba-Konfiguration

Wenn Sie dieses Modul zum ersten Mal starten, wird das Dialogfeld *Samba-Installation* geöffnet, und Sie werden aufgefordert, einige grundlegende Entscheidungen zur Verwaltung des Servers zu treffen. Am Ende des Konfigurationsvorgangs werden Sie aufgefordert, das Samba-Administratorpasswort (*Samba-Root-Passwort*) einzugeben). Bei späteren Starts wird das Dialogfeld *Samba-Konfiguration* geöffnet.

Der Dialog *Samba-Installation* umfasst zwei Schritte und optionale detaillierte Einstellungen:

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 Primary Domain Controller (PDC), Backup Domain Controller (BDC) oder nicht als Domain Controller agieren soll. Fahren Sie mit *Weiter* fort.

Falls Sie keine detaillierte Serverkonfiguration vornehmen möchten, bestätigen Sie dies mit *OK*. Legen Sie dann im abschließenden Popup-Feld das *root-Passwort für Samba* fest.

Sie können alle Einstellungen später im Dialogfeld *Samba-Konfiguration* auf den Karteireitern *Start*, *Freigaben*, *Identität*, *Verbürgte Domänen* und *LDAP-Einstellungen* ändern.

28.4.1.2 Erweiterte Samba-Konfiguration

Beim ersten Start des Samba-Servermoduls wird das Dialogfeld *Samba-Konfiguration* direkt nach den beiden Anfangsschritten (siehe *Abschnitt 28.4.1.1, „Anfängliche Samba-Konfiguration“*) geöffnet. Hier passen Sie Ihre Samba-Server-Konfiguration an.

Klicken Sie nach dem Bearbeiten Ihrer Konfiguration auf *OK*, um Ihre Einstellungen zu speichern.

28.4.1.2.1 Starten des Servers

Auf dem Karteireiter *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 28.3, „Starten und Stoppen von Samba“*.

Auf diesem Karteireiter 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.

28.4.1.2.2 Freigaben

Legen Sie auf dem Karteireiter *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.

Mit *Benutzern die Freigabe ihrer Verzeichnisse erlauben* können Mitglieder der Gruppe in *Zulässige Gruppe* ihre eigenen Verzeichnisse für andere Benutzer freigeben. Zum Beispiel `users` für eine lokale Reichweite oder `DOMAIN\Users` für eine domänenweite Freigabe. Der Benutzer muss außerdem sicherstellen, dass die Berechtigungen des Dateisystems den Zugriff zulassen. Mit *Maximale Anzahl an Freigaben* begrenzen Sie die Gesamtzahl der erstellbaren Freigaben. Wenn Sie den Zugriff auf Benutzerfreigaben ohne Authentifizierung zulassen möchten, aktivieren Sie *Gastzugriff erlauben*.

28.4.1.2.3 Identität

Auf dem Karteireiter *Identität* legen Sie fest, zu welcher Domäne der Host gehört (*Grundeinstellungen*) und ob ein alternativer Hostname im Netzwerk (*NetBIOS-Hostname*) verwendet werden soll. Microsoft Windows Internet Name Service (WINS) kann auch zur Namensauflösung benutzt werden. Aktivieren Sie in diesem Fall *WINS zur Hostnamenauflösung verwenden* und entscheiden Sie, ob Sie *WINS-Server via DHCP abrufen* möchten. Zum Festlegen globaler Einstellungen für Experten oder einer Quelle zur Benutzerauthentifizierung (zum Beispiel LDAP- anstelle von TDB-Datenbank) klicken Sie auf *Erweiterte Einstellungen*.

28.4.1.2.4 Verbürgte Domänen

Sie ermöglichen Benutzern anderer Domänen den Zugriff auf Ihre Domäne, indem Sie die entsprechenden Einstellungen in dem Karteireiter *Verbürgte Domänen* vornehmen. Klicken Sie zum Hinzufügen einer neuen Domäne auf *Hinzufügen*. Zum Entfernen der ausgewählten Domäne klicken Sie auf *Löschen*.

28.4.1.2.5 LDAP-Einstellungen

In dem Karteireiter *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 zur LDAP-Konfiguration finden Sie unter *Buch „*Security Guide*", Kapitel 5 „LDAP—A Directory Service"*.

28.4.2 Manuelles Konfigurieren des Servers

Wenn Sie Samba als Server verwenden möchten, installieren Sie `samba`. Die Hauptkonfigurationsdatei für 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 folgenden Abschnitte enthalten die einzelnen Datei- und Druckerfreigaben:

- [homes]
- [Profile]
- [Benutzer]
- [Gruppen]
- [Drucker]
- [drucken$]

Auf diese Weise können unterschiedliche Optionen für die einzelnen Freigaben festgelegt werden (oder auch global im Abschnitt `[global]`), sodass die Konfigurationsdatei einfacher zu verstehen ist.

28.4.2.1 Der Abschnitt „global"

Die folgenden Parameter im Abschnitt `[global]` sind den Gegebenheiten Ihres Netzwerks anzupassen, damit Ihr Samba-Server in einer Windows-Umgebung von anderen Computern über SMB erreichbar ist.

`Arbeitsgruppe = ARBEITSGRUPPE`

Mit dieser Zeile wird der Samba-Server einer Arbeitsgruppe zugeordnet. Ersetzen Sie `ARBEITSGRUPPE` durch eine entsprechende Arbeitsgruppe Ihrer Netzwerkumgebung. Der Samba-Server erscheint mit seinem DNS-Namen, sofern der Name noch nicht an ein anderes Gerät im Netzwerk vergeben ist. Wenn der DNS-Name nicht verfügbar ist, kann der Servername mithilfe von `netbiosname=`*`MEINNAME`* festgelegt werden. Weitere Details zu diesem Parameter finden Sie auf der man-Seite `smb.conf`.

`os level = 20`

Anhand dieses Parameters entscheidet Ihr Samba-Server, ob er versucht, LMB (Local Master Browser) für seine Arbeitsgruppe zu werden. Wählen Sie einen niedrigen Wert wie etwa `2`, damit ein vorhandenes Windows-Netz nicht durch einen falsch konfigurierten Samba-Server gestört wird. Weitere Informationen zu diesem Thema finden Sie im Kapitel „Netzwerk-Browser“ im Samba 3-HOWTO; weitere Informationen zum Samba 3-HOWTO finden Sie unter *Abschnitt 28.9, „Weiterführende Informationen“*.

Wenn im Netzwerk kein anderer SMB-Server (z. B. ein Windows 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.

28.4.2.2 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 28.1 EINE CD-ROM-FREIGABE

```
[cdrom]
       comment = Linux CD-ROM
       path = /media/cdrom
       locking = No
```

`[cdrom]` **und** `comment`

Der Abschnittseintrag `[cdrom]` stellt den Namen der Freigabe dar, 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 28.2 FREIGABE [HOMES]

```
[homes]
```

```
        comment = Home Directories
        valid users = %S
        browseable = No
        read only = No
        inherit acls = Yes
```

[homes]

Insoweit keine ausdrückliche Freigabe mit dem Freigabenamen des Benutzers existiert, der die Verbindung zum SMB-Server herstellt, wird aufgrund der `[homes]`-Freigabe dynamisch eine Freigabe generiert. 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 Benutzerverzeichnisses 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`.

Warnung: Keine Freigabe von NFS-Einhängungen für Samba

Wenn Sie `NFS`-Einhängungen für Samba freigeben, kann dies zu Datenverlust führen. Diese Vorgehensweise wird daher nicht unterstützt. Installieren Sie Samba direkt auf dem Dateiserver oder ziehen Sie Alternativen wie `iSCSI` in Erwägung.

28.4.2.3 Sicherheitsstufen (Security Levels)

Jeder Zugriff auf eine Freigabe kann für mehr Sicherheit durch ein Passwort geschützt werden. SMB bietet die folgenden Möglichkeiten zur Überprüfung von Berechtigungen:

Sicherheitsstufe „Benutzer“ (`security = user`)

Diese Variante führt das Konzept des Benutzers in SMB ein. Jeder Benutzer muss sich beim Server mit seinem Passwort anmelden. Nach der Authentifizierung kann der Server dann abhängig vom Benutzernamen Zugriff auf die einzelnen exportierten Freigaben gewähren.

Sicherheitsstufe „ADS“ (`security = ADS`)

In diesem Modus fungiert Samba als Domänenmitglied in einer Active Directory-Umgebung. Für den Betrieb in diesem Modus muss auf dem Computer, auf dem Samba ausgeführt wird, Kerberos installiert und konfiguriert sein. Der Computer, auf dem Samba verwendet wird, muss in den ADS-Bereich integriert sein. Dies kann mithilfe des YaST-Moduls *Windows-Domänenmitgliedschaft* erreicht werden.

Sicherheitsstufe „Domäne“ (`security = domain`)

Dieser Modus funktioniert nur korrekt, wenn der Computer in eine Windows NT-Domäne integriert wurde. Samba versucht, den Benutzernamen und das Passwort zu validieren, indem es diese an einen Window NT-Primär-Controller oder Backup Domain Controller weiterleitet. Ein Windows NT-Server wäre ausreichend. Er erwartet, dass der Parameter für das verschlüsselte Passwort auf `ja` festgelegt wurde.

Die Sicherheit auf Freigabe-, Benutzer-, Server- und Domänenebene (Share, User, Server und Domain 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 im Samba 3-HOWTO. Wenn sich mehrere Server auf einem System befinden, beachten Sie die Optionen `interfaces` und `bind interfaces only`.

28.5 Konfigurieren der Clients

Clients können auf den Samba-Server nur über TCP/IP zugreifen. NetBEUI oder NetBIOS über IPX können mit Samba nicht verwendet werden.

28.5.1 Konfigurieren eines Samba-Clients mit YaST

Konfigurieren Sie einen Samba-Client, um auf Ressourcen (Dateien oder Drucker) auf dem Samba- oder Windows-Server zuzugreifen. Geben Sie im Dialogfeld *Netzwerkdienste* › *Windows-Domänenmitgliedschaft* die NT- oder Active Directory-Domäne oder -Arbeitsgruppe an. Wenn Sie *Zusätzlich SMB-Informationen für Linux-Authentifizierung verwenden* aktivieren, erfolgt die Benutzerauthentifizierung über den Samba, NT- oder Kerberos-Server.

Klicken Sie für erweiterte Konfigurationsoptionen auf *Einstellungen für Experten*. Sie können z. B. über die Tabelle *Serververzeichnisse einhängen* das automatische Einhängen des Server-Basisverzeichnisses bei der Authentifizierung aktivieren. Auf diese Weise können Benutzer auf Ihre Home-Verzeichnisse zugreifen, wenn sie auf CIFS gehostet werden. Einzelheiten finden Sie auf der man-Seite zu `pam_mount`.

Bestätigen Sie zum Abschluss alle Einstellungen, um die Konfiguration zu beenden.

28.6 Samba als Anmeldeserver

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich Benutzer nur mit einem gültigen Konto und zugehörigem Passwort anmelden dürfen. In einem Windows-basierten Netzwerk wird diese Aufgabe von einem Primary Domain Controller (PDC) übernommen. Sie können einen Windows NT-Server verwenden, der als PDC konfiguriert ist; diese Aufgabe kann aber auch mithilfe eines Samba-Servers ausgeführt werden. Es müssen Einträge im Abschnitt `[global]` von `smb.conf` vorgenommen werden. Diese werden in *Beispiel 28.3, „Abschnitt „global“ in smb.conf“* beschrieben.

BEISPIEL 28.3 ABSCHNITT „GLOBAL“ IN SMB.CONF

```
[global]
    workgroup = WORKGROUP
    domain logons = Yes
    domain master = Yes
```

Die Benutzerkonten und Passwörter müssen in ein Windows-konformes Verschlüsselungsformat umgewandelt werden. Verwenden Sie hierfür den Befehl **smbpasswd** `-a name`. Da nach dem Windows-Domänenkonzept auch die Computer selbst ein Domänenkonto benötigen, wird dieses mit den folgenden Kommandos angelegt:

```
useradd hostname\$
smbpasswd -a -m hostname
```

Mit dem Befehl **useradd** wird ein Dollarzeichen hinzugefügt. Der Befehl **smbpasswd** fügt dieses bei der Verwendung des Parameters `-m` automatisch hinzu. In der kommentierten Beispielkonfiguration (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) sind Einstellungen enthalten, die diese Aufgabe automatisieren.

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\$
```

Um sicherzustellen, dass Samba dieses Skript korrekt ausführen kann, wählen Sie einen Samba-Benutzer mit den erforderlichen Administratorberechtigungen und fügen Sie ihn zur Gruppe `ntadmin` hinzu. Anschließend können Sie allen Mitgliedern der Linux-Gruppe den Status `Domain Admin` zuweisen, indem Sie folgendes Kommando eingeben:

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

28.7 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 SUSE Linux Enterprise Server zu Active Directory (AD) beitreten lassen.

So erfolgt der Beitritt zu einer AD-Domäne:

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.

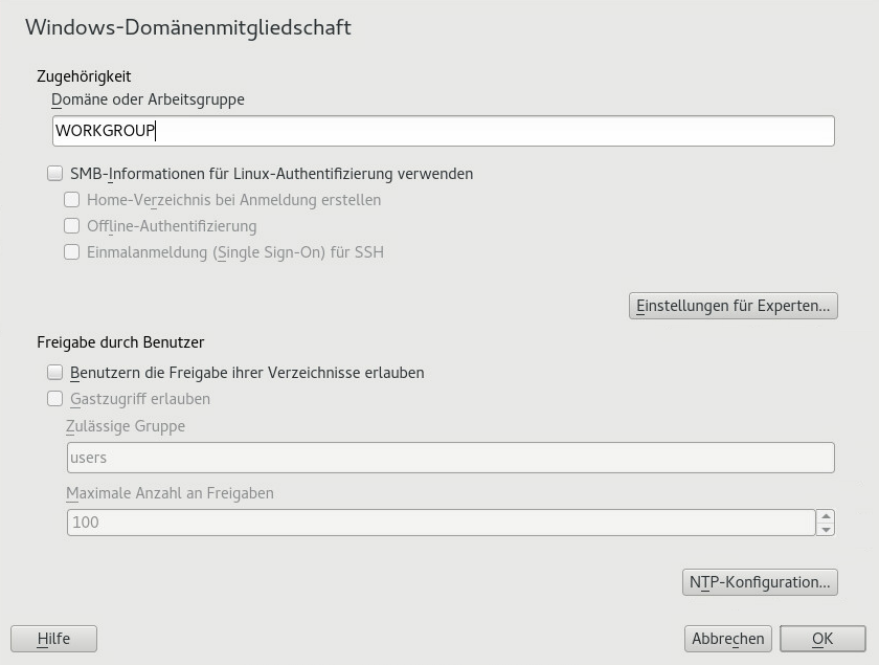


ABBILDUNG 28.1 FESTLEGEN DER WINDOWS-DOMÄNENMITGLIEDSCHAFT

4. Aktivieren Sie *Zusätzlich SMB-Informationen für Linux-Authentifikation verwenden*, um die SMB-Quelle für die Linux-Authentifizierung auf dem Server zu nutzen.

5. Klicken Sie auf *OK* 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*.
   Ihr Server ist jetzt so eingerichtet, dass alle Authentifizierungsdaten vom Active Directory-Domänencontroller abgerufen werden.

Tipp: Identitätszuordnung

In einer Umgebung mit mehreren Samba-Servern werden die UIDs und GIDs nicht einheitlich erstellt. Die UIDs, die den Benutzern zugewiesen werden, sind abhängig von der Reihenfolge, in der sich diese Benutzer erstmalig anmelden. Dies führt zu UID-Konflikten

über die Server hinweg. Zur Behebung dieses Problems ist die Identitätszuordnung erforderlich. Weitere Einzelheiten finden Sie unter https://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/idmapper.html.

28.8 Weitere Themen

In diesem Abschnitt lernen Sie fortgeschrittene Vefahren zur Verwaltung des Client- und des Serverteils der Samba-Suite kennen.

28.8.1 Transparente Dateikomprimierung mit Btrfs

Mit Samba können die Clients die Flags für die Datei- und Verzeichniskomprimierung für Freigaben, die sich im Btrfs-Dateisystem befinden, im Fernverfahren bearbeiten. Windows Explorer bietet im Dialogfeld *Datei* › *Eigenschaften* › *Erweitert* die Möglichkeit, die Dateien/Verzeichnisse zur transparenten Komprimierung zu kennzeichnen:

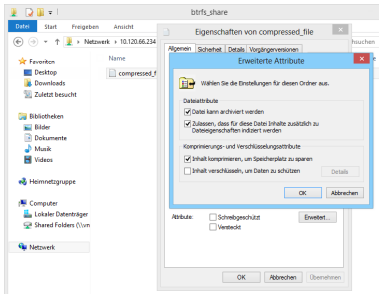


ABBILDUNG 28.2 DIALOGFELD *ERWEITERTE ATTRIBUTE* IN WINDOWS EXPLORER

Die zur Komprimierung gekennzeichneten Dateien werden beim Zugreifen oder Ändern transparent durch das zugrunde liegende Dateisystem komprimiert bzw. dekomprimiert. Damit sparen Sie Speicherplatz, doch beim Zugreifen auf die Datei wird die CPU stärker beansprucht. Neue Dateien und Verzeichnisse übernehmen das Komprimierungs-Flag vom übergeordneten Verzeichnis, sofern sie nicht mit der Option FILE_NO_COMPRESSION erstellt werden.

Komprimierte Dateien und Verzeichnisse werden in Windows Explorer anders dargestellt als nicht komprimierte Dateien und Verzeichnisse:

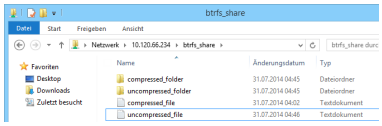


ABBILDUNG 28.3 WINDOWS EXPLORER-ANZEIGE MIT KOMPRIMIERTEN DATEIEN

Sie können die Komprimierung der Samba-Freigabe wahlweise manuell aktivieren (fügen Sie hierzu

```
vfs objects = btrfs
```

in die Freigabekonfiguration in `/etc/samba/smb.conf` ein) oder mit YaST. Wählen Sie hierzu *Netzwerkdienste* › *Samba-Server* › *Hinzufügen*, und aktivieren Sie die Option *Btrfs-Funktionen verwenden*.

Eine allgemeine Übersicht über die Komprimierung in Btrfs finden Sie in *Buch* „Storage Administration Guide", *Kapitel 1 „Overview of File Systems in Linux", Abschnitt 1.2.2.1 „Mounting Compressed Btrfs File Systems"*.

28.8.2 Aufnahmen

Snapshots (auch als Schattenkopien bezeichnet) sind Kopien des Zustands eines Subvolumens in einem Dateisystem zu einem bestimmten Zeitpunkt. Die Verwaltung dieser Snapshots in Linux erfolgt mit Snapper. Die Snapshots werden auf dem Btrfs-Dateisystem sowie auf LVM-Volumes mit Thin-Provisioning unterstützt. Die Samba-Suite unterstützt die Verwaltung von Remote-Snapshots über das FSRVP-Protokoll sowohl auf Server- als auch auf Clientseite.

28.8.2.1 Frühere Versionen

Die Snapshots auf einem Samba-Server können für entfernte Windows-Clients als Datei- oder Verzeichnis-Vorgängerversionen gezeigt werden.

Zum Aktivieren von Snapshots auf einem Samba-Server müssen die folgenden Voraussetzungen erfüllt sein:

- Die SMB-Netzwerkfreigabe befindet sich auf einem Btrfs-Subvolume.
- Für den Pfad der SMB-Netzwerkfreigabe ist eine zugehörige Snapper-Konfigurationsdatei vorhanden. Sie können die Snapper-Datei wie folgt erstellen:

  ```
  snapper -c <cfg_name> create-config /path/to/share
  ```

Weitere Informationen zu Snapper finden Sie in *Kapitel 7, Systemwiederherstellung und Snapshot-Verwaltung mit Snapper*.

- Der Snapshot-Verzeichnisbaum muss den Zugriff für relevante Benutzer ermöglichen. Weitere Informationen finden Sie auf der man-Seite zu vfs_snapper (`man 8 vfs_snapper`) im Abschnitt zu den Berechtigungen.

Sollen Remote-Snapshots unterstützt werden, müssen Sie die Datei `/etc/samba/smb.conf` bearbeiten. Verwenden Sie hierzu wahlweise *YaST › Netzwerkdienste › Samba-Server*, oder bearbeiten Sie den relevanten Freigabeabschnitt manuell mit

```
vfs objects = snapper
```

Damit die manuellen Änderungen an `smb.conf` in Kraft treten, müssen Sie den Samba-Service wie folgt neu starten:

```
systemctl restart nmb smb
```

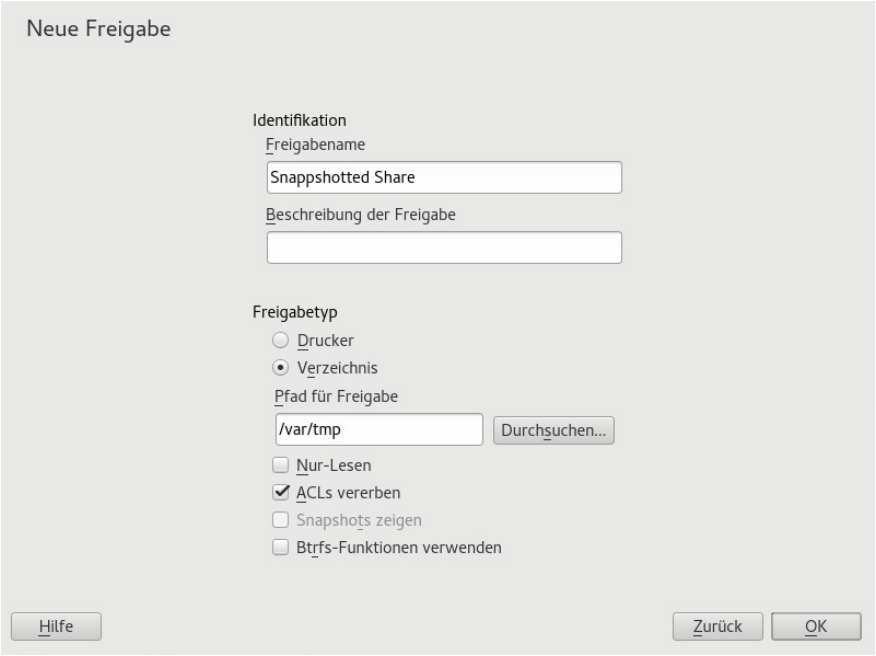


ABBILDUNG 28.4 HINZUFÜGEN EINER NEUEN SAMBA-FREIGABE MIT AKTIVIERTER SNAPSHOT-AUFNAHME

Nach der Konfiguration können Sie auf die Snapshots, die Snapper für den Samba-Freigabepfad erstellt hat, in Windows Explorer über die Registerkarte *Vorgängerversionen* für eine Datei oder ein Verzeichnis zugreifen.

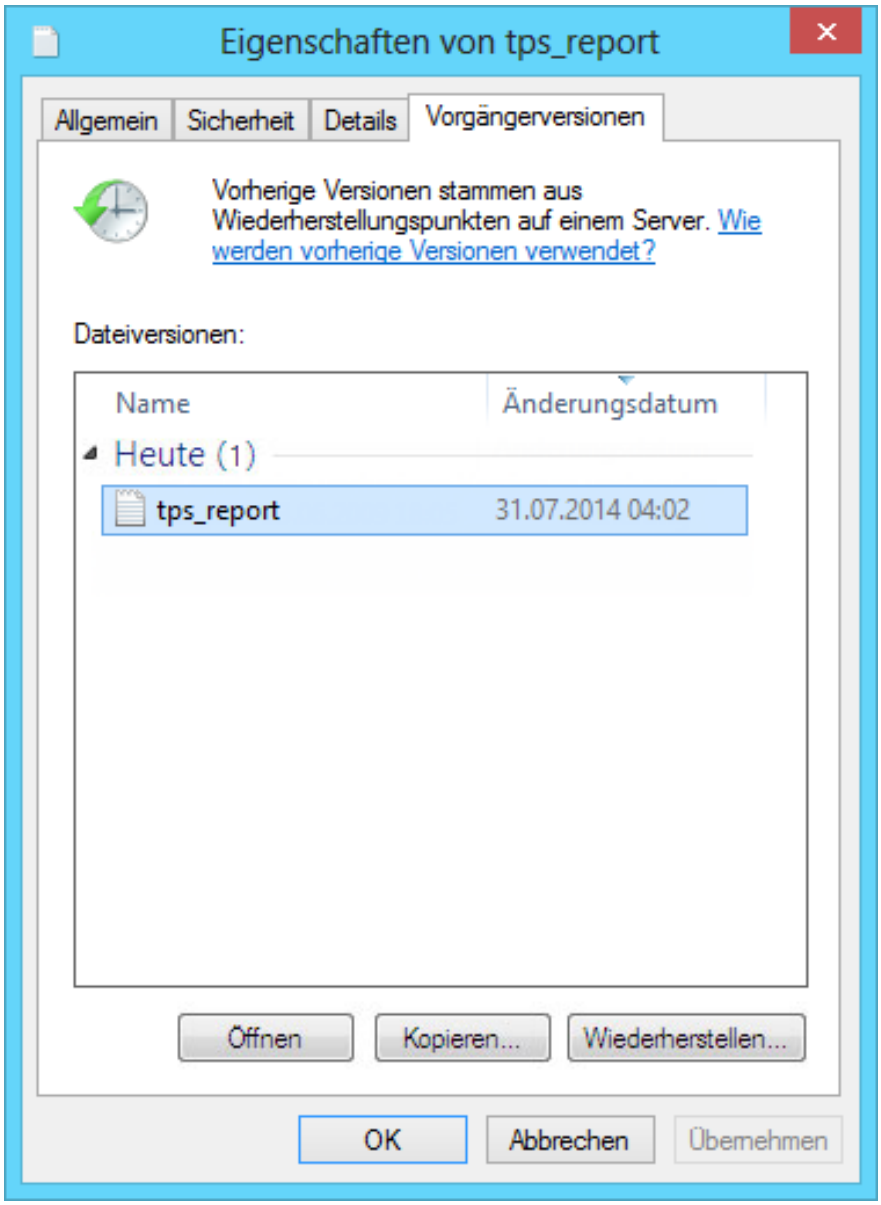


ABBILDUNG 28.5 DIE REGISTERKARTE *VORGÄNGERVERSIONEN* IN WINDOWS EXPLORER

28.8.2.2 Remote-Snapshots für Freigaben

Standardmäßig können Snapshots lediglich lokal auf dem Samba-Server erstellt und gelöscht werden (mit dem Kommandozeilenprogramm Snapper oder mit der Zeitleistenfunktion in Snapper).

Sie können Samba so konfigurieren, dass Anfragen zum Erstellen und Löschen von Snapshots für Freigaben verarbeitet werden, die von entfernten Hosts über das FSRVP (File Server Remote VSS-Protokoll) gesendet werden.

Neben den Konfigurationsschritten und Voraussetzungen in *Abschnitt 28.8.2.1, „Frühere Versionen“* ist die folgende globale Konfiguration in `/etc/samba/smb.conf` erforderlich:

```
[global]
rpc_daemon:fssd = fork
registry shares = yes
include = registry
```

FSRVP-Clients (auch **`rpcclient`** in Samba und **`DiskShadow.exe`** in Windows Server 2012) können dann Samba anweisen, einen Snapshot für eine bestimmte Freigabe zu erstellen und den Snapshot als neue Freigabe zu zeigen.

28.8.2.3 Fernverwaltung von Snapshots in Linux mit **`rpcclient`**

Das Paket `samba-client` umfasst einen FSRVP-Client, der im Fernverfahren eine Anfrage an einen Windows-/Samba-Server stellen kann, einen Snapshot für eine bestimmte Freigabe zu erstellen und zu zeigen. Anschließend können Sie die gezeigte Freigabe mit den vorhandenen Werkzeugen in SUSE Linux Enterprise Server einhängen und die Dateien in dieser Freigabe sichern. Die Anfragen werden über die Binärdatei **`rpcclient`** an den Server gesendet.

BEISPIEL 28.4 ANFORDERN EINES SNAPSHOTS FÜR EINE WINDOWS SERVER 2012-FREIGABE MIT `rpcclient`

Stellen Sie eine Verbindung zum Server `win-server.example.com` als Administrator in der Domäne `EXAMPLE` her:

```
# rpcclient -U 'EXAMPLE\Administrator' ncacn_np:win-server.example.com[ndr64,sign]
Enter EXAMPLE/Administrator's password:
```

Überprüfen Sie, ob die SMB-Freigabe für **`rpcclient`** sichtbar ist:

```
rpcclient $> netshareenum
netname: windows_server_2012_share
remark:
path:   C:\Shares\windows_server_2012_share
password:       (null)
```

Überprüfen Sie, ob die SMB-Freigabe das Erstellen von Snapshots unterstützt:

```
rpcclient $> fss_is_path_sup windows_server_2012_share \
UNC \\WIN-SERVER\windows_server_2012_share\ supports shadow copy requests
```

Fordern Sie die Erstellung eines Snapshots für eine Freigabe an:

```
rpcclient $> fss_create_expose backup ro windows_server_2012_share
```

```
13fe880e-e232-493d-87e9-402f21019fb6: shadow-copy set created
13fe880e-e232-493d-87e9-402f21019fb6(1c26544e-8251-445f-be89-d1e0a3938777): \
\\WIN-SERVER\windows_server_2012_share\ shadow-copy added to set
13fe880e-e232-493d-87e9-402f21019fb6: prepare completed in 0 secs
13fe880e-e232-493d-87e9-402f21019fb6: commit completed in 1 secs
13fe880e-e232-493d-87e9-402f21019fb6(1c26544e-8251-445f-be89-d1e0a3938777): \
share windows_server_2012_share@{1C26544E-8251-445F-BE89-D1E0A3938777} \
exposed as a snapshot of \\WIN-SERVER\windows_server_2012_share\
```

Überprüfen Sie, ob der Snapshot der Freigabe durch den Server gezeigt wird:

```
rpcclient $> netshareenum
netname: windows_server_2012_share
remark:
path:   C:\Shares\windows_server_2012_share
password:       (null)

netname: windows_server_2012_share@{1C26544E-8251-445F-BE89-D1E0A3938777}
remark: (null)
path:   \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy{F6E6507E-F537-11E3-9404-
B8AC6F927453}\Shares\windows_server_2012_share\
password:       (null)
```

Versuchen Sie, den Snapshot der Freigabe zu löschen:

```
rpcclient $> fss_delete windows_server_2012_share \
13fe880e-e232-493d-87e9-402f21019fb6 1c26544e-8251-445f-be89-d1e0a3938777
13fe880e-e232-493d-87e9-402f21019fb6(1c26544e-8251-445f-be89-d1e0a3938777): \
\\WIN-SERVER\windows_server_2012_share\ shadow-copy deleted
```

Überprüfen Sie, ob der Snapshot der Freigabe durch den Server entfernt wurde:

```
rpcclient $> netshareenum
netname: windows_server_2012_share
remark:
path:   C:\Shares\windows_server_2012_share
password:       (null)
```

28.8.2.4 Fernverwaltung von Snapshots in Windows mit `DiskShadow.exe`

Sie können Snapshots von SMB-Freigaben auf dem Linux Samba-Server auch über die Windows-Umgebung, die als Client auftritt, verwalten. Mit dem Dienstprogramm **`DiskShadow.exe`** in Windows Server 2012 verwalten Sie Remote-Freigaben ähnlich wie mit **`rpcclient`** (siehe *Abschnitt 28.8.2.3, „Fernverwaltung von Snapshots in Linux mit `rpcclient`“*). Zunächst muss jedoch der Samba-Server ordnungsgemäß eingerichtet werden.

Im Folgenden wird erläutert, wie Sie einen Samba-Server so konfigurieren, dass der Windows Server-Client die Snapshots der Freigaben auf dem Samba-Server verwalten kann. *`EXAMPLE`* ist der Name der Active Directory-Domäne in der Testumgebung, `fsrvp-server.example.com` ist der Hostname des Samba-Servers und `/srv/smb` ist der Pfad zur SMB-Freigabe.

PROZEDUR 28.1 AUSFÜHRLICHE KONFIGURATION DES SAMBA-SERVERS

1. Treten Sie der Active Directory-Domäne mithilfe von YaST bei. Weitere Informationen, *Abschnitt 28.7, „Samba-Server im Netzwerk mit Active Directory“*.

2. Prüfen Sie, ob der DNS-Eintrag der Active Directory-Domäne korrekt ist:

```
fsrvp-server:~ # net -U 'Administrator' ads dns register \
fsrvp-server.example.com <IP address>
Successfully registered hostname with DNS
```

3. Erstellen Sie ein Btrfs-Subvolume unter `/srv/smb`:

```
fsrvp-server:~ # btrfs subvolume create /srv/smb
```

4. Erstellen Sie eine Snapper-Konfigurationsdatei für den Pfad `/srv/smb`:

```
fsrvp-server:~ # snapper -c <snapper_config> create-config /srv/smb
```

5. Erstellen Sie eine neue Freigabe mit dem Pfad `/srv/smb` und aktivieren Sie in YaST das Kontrollkästchen *Snapshots zeigen*. Fügen Sie in jedem Fall die folgenden Snippets in den globalen Abschnitt der Datei `/etc/samba/smb.conf` ein (siehe *Abschnitt 28.8.2.2, „Remote-Snapshots für Freigaben“*):

```
[global]
 rpc_daemon:fssd = fork
 registry shares = yes
 include = registry
```

6. Starten Sie Samba mit **`systemctl restart nmb smb`** neu.

7. Konfigurieren Sie die Snapper-Berechtigungen:

```
fsrvp-server:~ # snapper -c <snapper_config> set-config \
ALLOW_USERS="EXAMPLE\\\\Administrator EXAMPLE\\\\win-client$"
```

Überprüfen Sie, ob alle unter ALLOW_USERS aufgeführten Benutzer auch die Berechtigung für das Traversal des Unterverzeichnisses `.snapshots` besitzen.

```
fsrvp-server:~ # snapper -c <snapper_config> set-config SYNC_ACL=yes
```

Wichtig: Escape-Zeichen bei Pfaden

Gehen Sie mit dem Escape-Zeichen „\“ vorsichtig vor! Setzen Sie das Escape-Zeichen zweimal, damit der Wert in `/etc/snapper/configs/<snapper_config>` ordnungsgemäß auskommentiert wird.

„EXAMPLE\win-client$“ bezeichnet das Windows-Clientkonto. Die anfänglichen FSRVP-Anfragen von Windows werden mit diesem Konto ausgegeben.

8. Erteilen Sie dem Windows-Clientkonto die erforderlichen Berechtigungen:

```
fsrvp-server:~ # net -U 'Administrator' rpc rights grant \
"EXAMPLE\\win-client$" SeBackupPrivilege
Successfully granted rights.
```

Für den Benutzer „EXAMPLE\Administrator“ muss das obige Kommando nicht ausgeführt werden, da diese Konto bereits die Berechtigungen besitzt.

PROZEDUR 28.2 EINRICHTEN DES WINDOWS-CLIENTS UND AUSFÜHREN VON `DiskShadow.exe`

1. Booten Sie Windows Server 2012 (Beispiel-Hostname: WIN-CLIENT).
2. Treten Sie derselben Active Directory-Domäne EXAMPLE bei wie mit dem SUSE Linux Enterprise Server.
3. Booten Sie den Computer neu.
4. Öffnen Sie die Powershell.
5. Starten Sie **`DiskShadow.exe`**, und beginnen Sie den Sicherungsvorgang:

```
PS C:\Users\Administrator.EXAMPLE> diskshadow.exe
```

```
Microsoft DiskShadow version 1.0
Copyright (C) 2012 Microsoft Corporation
On computer:  WIN-CLIENT,  6/17/2014 3:53:54 PM

DISKSHADOW> begin backup
```

6. Geben Sie an, dass die Schattenkopie auch beim Beenden des Programms, beim Zurücksetzen und beim Neubooten erhalten bleiben soll:

```
DISKSHADOW> set context PERSISTENT
```

7. Überprüfen Sie, ob die angegebene Freigabe Snapshots unterstützt, und erstellen Sie einen Snapshot:

```
DISKSHADOW> add volume \\fsrvp-server\sles_snapper

DISKSHADOW> create
Alias VSS_SHADOW_1 for shadow ID {de4ddca4-4978-4805-8776-cdf82d190a4a} set as \
 environment variable.
Alias VSS_SHADOW_SET for shadow set ID {c58e1452-c554-400e-a266-d11d5c837cb1} \
 set as environment variable.

Querying all shadow copies with the shadow copy set ID \
 {c58e1452-c554-400e-a266-d11d5c837cb1}

 * Shadow copy ID = {de4ddca4-4978-4805-8776-cdf82d190a4a}     %VSS_SHADOW_1%
    - Shadow copy set: {c58e1452-c554-400e-a266-d11d5c837cb1}  %VSS_SHADOW_SET%
    - Original count of shadow copies = 1
    - Original volume name: \\FSRVP-SERVER\SLES_SNAPPER\ \
      [volume not on this machine]
    - Creation time: 6/17/2014 3:54:43 PM
    - Shadow copy device name:
      \\FSRVP-SERVER\SLES_SNAPPER@{31afd84a-44a7-41be-b9b0-751898756faa}
    - Originating machine: FSRVP-SERVER
    - Service machine: win-client.example.com
    - Not exposed
    - Provider ID: {89300202-3cec-4981-9171-19f59559e0f2}
    - Attributes:  No_Auto_Release Persistent FileShare

Number of shadow copies listed: 1
```

8. Beenden Sie den Sicherungsvorgang:

```
DISKSHADOW> end backup
```

9. Versuchen Sie, den erstellten Snapshot zu löschen, und überprüfen Sie, ob er tatsächlich gelöscht wurde:

```
DISKSHADOW> delete shadows volume \\FSRVP-SERVER\SLES_SNAPPER\
Deleting shadow copy {de4ddca4-4978-4805-8776-cdf82d190a4a} on volume \
 \\FSRVP-SERVER\SLES_SNAPPER\ from provider \
{89300202-3cec-4981-9171-19f59559e0f2} [Attributes: 0x04000009]...

Number of shadow copies deleted: 1

DISKSHADOW> list shadows all

Querying all shadow copies on the computer ...
No shadow copies found in system.
```

28.9 Weiterführende Informationen

Die Dokumentation zu Samba ist im Paket `samba-doc` enthalten, das standardmäßig nicht installiert wird. Installieren Sie das Paket mit **`zypper install samba-doc`**. Wenn Samba installiert ist, können Sie in die Kommandozeile **`apropos`** `samba` eingeben und einige man-Seiten aufrufen. 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`. Auch in der Datei `/usr/share/doc/packages/samba/README.SUSE` finden Sie zusätzliche Informationen zu Samba.

Das Samba-Team stellt in Samba HOWTO (siehe https://wiki.samba.org) einen Abschnitt zur Fehlerbehebung zur Verfügung. In Teil V ist außerdem eine ausführliche Anleitung zum Überprüfen der Konfiguration enthalten.

29 Bedarfsweises Einhängen mit autofs

Das Programm `autofs` hängt automatisch festgelegte Verzeichnisse bedarfsweise ein. Das Programm beruht auf einem Kernel-Modul, das für hohe Effizienz sorgt, und kann sowohl lokale Verzeichnisse als auch Netzwerkfreigaben verwalten. Diese automatischen Einhängepunkte werden nur dann eingehängt, wenn auf sie zugegriffen wird; nach einem bestimmten Zeitraum ohne Aktivität werden sie wieder ausgehängt. Dieses bedarfsweise Verfahren spart Bandweite und bewirkt höhere Leistungen als das statische Einhängen mit `/etc/fstab`. `autofs` ist das Steuerungsskript und **`automount`** das Kommando (der Daemon), mit dem das automatische Einhängen ausgeführt wird.

29.1 Installation

`autofs` ist nicht standardmäßig in SUSE Linux Enterprise Server installiert. Um die Funktionen für das automatische Einhängen zu nutzen, installieren Sie das Programm zunächst mit

```
sudo zypper install autofs
```

29.2 Konfiguration

`autofs` muss manuell konfiguriert werden. Bearbeiten Sie hierzu die Konfigurationsdateien mit einem Texteditor, z. B. **`vim`**. Die Konfiguration von `autofs` umfasst zwei grundlegende Schritte: die *master*-Zuordnungsdatei und bestimmte Zuordnungsdateien.

29.2.1 Die Master-Zuordnungsdatei

Die standardmäßige Master-Konfigurationsdatei für `autofs` ist `/etc/auto.master`. Soll der Speicherort dieser Datei geändert werden, bearbeiten Sie den Wert der Option `DEFAULT_MASTER_MAP_NAME` in `/etc/sysconfig/autofs`. Beispiel für SUSE Linux Enterprise Server:

```
#
# Sample auto.master file
```

```
# This is an automounter map and it has the following format
# key [ -mount-options-separated-by-comma ] location
# For details of the format look at autofs(5). (1)
#
#/misc  /etc/auto.misc (2)
#/net -hosts
#
# Include /etc/auto.master.d/*.autofs (3)
#
#+dir:/etc/auto.master.d
#
# Include central master map if it can be found using
# nsswitch sources.
#
# Note that if there are entries for /net or /misc (as
# above) in the included master map any keys that are the
# same will not be seen as the first read key seen takes
# precedence.
#
+auto.master (4)
```

(1) Auf der man-Seite zu `autofs` (**`man 5 autofs`**) finden Sie viele nützliche Informationen zum Format der Automounter-Zuordnungen.

(2) Diese einfache Syntax für die Automounter-Zuordnung ist standardmäßig auskommentiert (#), liefert jedoch ein gutes Beispiel.

(3) Falls die Master-Zuordnung in mehrere Dateien aufgeteilt werden muss, heben Sie die Auskommentierung der Zeile auf und platzieren Sie die Zuordnungen (mit dem Suffix `.autofs`) im Verzeichnis `/etc/auto.master.d/`.

(4) `+auto.master` sorgt dafür, dass die richtige Master-Zuordnung auch bei Verwendung von NIS problemlos auffindbar ist (weitere Informationen zu NIS siehe *Buch „Security Guide", Kapitel 3 „Using NIS", Abschnitt 3.1 „Configuring NIS Servers"*).

Die Einträge in `auto.master` enthalten drei Felder mit der folgenden Syntax:

```
mount point      map name      options
```

Einhängepunkt

Basisspeicherort, an dem das `autofs`-Dateisystem angehängt wird, z. B. `/home`.

Zuordnungsname

Name einer Zuordnungsquelle für das Einhängen. Weitere Informationen zur Syntax der Zuordnungsdateien finden Sie in *Abschnitt 29.2.2, „Zuordnungsdateien"*.

Optionen

Diese Optionen (sofern angegeben) werden als Standardeinstellungen für alle Einträge in der Zuordnung angewendet.

Tipp: Weitere Informationen

Weitere Informationen zu den einzelnen Werten für die optionalen Angaben `map-type` (Zuordnungstyp), `format` (Format) und `options` (Optionen) finden Sie auf der man-Seite zu *auto.master* (`man 5 auto.master`).

Der folgende Eintrag in `auto.master` weist `autofs` an, in `/etc/auto.smb` nachzuschlagen und Einhängepunkte im Verzeichnis `/smb` zu erstellen.

```
/smb    /etc/auto.smb
```

29.2.1.1 Direktes Einhängen

Beim direkten Einhängen wird ein Einhängepunkt im Pfad erstellt, der in der entsprechenden Zuordnungsdatei angegeben ist. Geben Sie in `auto.master` nicht den Einhängepunkt an, sondern ersetzen Sie den Eintrag im Feld für den Einhängepunkt durch `/-`. Die folgende Zeile weist `autofs` beispielsweise an, einen Einhängepunkt im Pfad zu erstellen, der in `auto.smb` angegeben ist:

```
/-        /etc/auto.smb
```

Tipp: Zuordnungen ohne vollständigen Pfad

Wenn die Zuordnungsdatei nicht mit dem vollständigen lokalen Pfad oder Netzwerkpfad angegeben ist, wird die Datei über die NSS-Konfiguration (Name Service Switch) ermittelt:

```
/-        auto.smb
```

29.2.2 Zuordnungsdateien

Wichtig: Andere Zuordnungstypen

Dateien sind der häufigste Zuordnungstyp für das automatische Einhängen mit `autofs`, es gibt jedoch noch weitere Typen. Eine Zuordnungsspezifikation kann beispielsweise die Ausgabe eines Kommandos oder auch das Ergebnis einer LDAP- oder Datenbankabfrage sein. Weitere Informationen zu Zuordnungstypen finden Sie auf der man-Seite **`man 5 auto.master`**.

Zuordnungsdateien bestimmen den Speicherort der Quelle (lokal oder im Netzwerk) sowie den Einhängepunkt, an dem die Quelle lokal eingehängt werden soll. Für die Zuordnungen gilt ein ähnliches allgemeines Format wie für die Master-Zuordnung. Der Unterschied ist, dass die *Optionen* zwischen dem Einhängepunkt und dem Speicherort angegeben sind, also nicht am Ende des Eintrags:

```
mount point      options      location
```

Die Zuordnungsdateien dürfen nicht als ausführbar markiert sein. Mit **`chmod -x`** *`ZUORDNUNGSDATEI`* entfernen Sie die ausführbaren Teile.

Einhängepunkt

Gibt an, wo der Quellspeicherort eingehängt werden soll. Dies kann entweder der Name eines einzelnen Verzeichnisses sein (*indirektes* Einhängen), das dem in `auto.master` angegebenem Basiseinhängepunkt hinzugefügt werden soll, oder der vollständige Pfad des Einhängepunkts (direktes Einhängen, siehe *Abschnitt 29.2.1.1, „Direktes Einhängen“*).

Optionen

Zeigt eine optionale, durch Kommas getrennte Liste der Einhängeoptionen für die entsprechenden Einträge an. Wenn `auto.master` ebenfalls Optionen für diese Zuordnungsdatei enthält, werden diese Optionen an das Ende der Liste angehängt.

location

Gibt den Pfad an, von dem aus das Dateisystem eingehängt werden soll. Dies ist in der Regel ein NFS- oder SMB-Volume mit dem üblichen Format `Hostname:Pfadname`. Wenn das einzuhängende Dateisystem mit einem Schrägstrich (`/`) beginnt (z. B. lokale `/dev`-Einträge oder smbfs-Freigaben), muss ein Doppelpunkt (:) vorangestellt werden, z. B. `:/dev/sda1`.

29.3 Funktionsweise und Fehlersuche

In diesem Abschnitt wird erläutert, wie Sie die Funktionsweise des `autofs`-Dienstes steuern und weitere Fehlersuchinformationen durch zusätzliche Einstellungen für die Automounter-Funktionsweise abrufen.

29.3.1 Steuern des `autofs`-Dienstes

Die Funktionsweise des `autofs`-Dienstes wird mit dem Kommando `systemd` gesteuert. Die allgemeine Syntax für das Kommando **`systemctl`** für `autofs` lautet

```
sudo systemctl SUB_COMMAND autofs
```

`SUB_COMMAND` steht hierbei für:

enable
: Startet den Automounter-Daemon beim Booten.

start
: Startet den Automounter-Daemon.

stop
: Stoppt den Automounter-Daemon. Automatische Einhängepunkte sind nicht verfügbar.

status
: Gibt den aktuellen Status des `autofs`-Dienstes zusammen mit einem Teil einer zugehörigen Protokolldatei aus.

restart
: Stoppt und startet den Automounter, wobei alle laufenden Daemons beendet und neue Daemons gestartet werden.

reload
: Prüft die aktuelle `auto.master`-Zuordnung, startet die Daemons neu, deren Einträge geändert wurden, und startet neue Daemons für neue Einträge.

29.3.2 Fehlersuche bei Automounter-Problemen

Falls Probleme beim Einhängen von Verzeichnissen mit `autofs` auftreten, führen Sie den **`automount`**-Daemon manuell aus und beachten Sie die Ausgabemeldungen:

1. Stoppen Sie `autofs`.

   ```
   sudo systemctl stop autofs
   ```

2. Führen Sie **`automount`** auf einem Terminal manuell im Vordergrund aus und aktivieren Sie die ausführliche Ausgabe.

   ```
   sudo automount -f -v
   ```

3. Greifen Sie auf einem anderen Terminal auf die Einhängepunkte zu (z. B. **`cd`** oder **`ls`**) und versuchen Sie, die automatisch einzuhängenden Dateisysteme einhängen zu lassen.

4. Ermitteln Sie anhand der Ausgabe von **`automount`** auf dem ersten Terminal, warum das Einhängen nicht erfolgt ist oder gar nicht erst versucht wurde.

29.4 Automatisches Einhängen als NFS-Freigabe

Das nachfolgende Verfahren zeigt, wie Sie `autofs` für das automatische Einhängen einer NFS-Freigabe konfigurieren, die sich im Netzwerk befindet. Hierbei werden die oben aufgeführten Informationen verwendet und es wird vorausgesetzt, dass Sie mit NFS-Exporten vertraut sind. Weitere Informationen zu NFS finden Sie in *Kapitel 27, Verteilte Nutzung von Dateisystemen mit NFS*.

1. Bearbeiten Sie die Master-Zuordnungsdatei `/etc/auto.master`:

   ```
   sudo vim /etc/auto.master
   ```

   Fügen Sie einen neuen Eintrag für den neuen NFS-Einhängepunkt am Ende von `/etc/auto.master` an:

   ```
   /nfs      /etc/auto.nfs      --timeout=10
   ```

   Hiermit erhält `autofs` die folgenden Informationen: Der Basiseinhängepunkt lautet `/nfs`, die NFS-Freigaben sind in der Zuordnung `/etc/auto.nfs` angegeben und alle Freigaben in dieser Zuordnung werden nach 10 Sekunden Inaktivität automatisch ausgehängt.

2. Erstellen Sie eine neue Zuordnungsdatei für NFS-Freigaben:

```
sudo vim /etc/auto.nfs
```

`/etc/auto.nfs` enthält in der Regel je eine separate Zeile pro NFS-Freigabe. Das Format wird in *Abschnitt 29.2.2, „Zuordnungsdateien“* beschrieben. Fügen Sie die Zeile ein, in der der Einhängepunkt und die Netzwerkadresse der NFS-Freigabe aufgeführt sind:

```
export      jupiter.com:/home/geeko/doc/export
```

Mit der obigen Zeile wird das Verzeichnis `/home/geeko/doc/export` auf dem Host `jupiter.com` bei Bedarf automatisch in das Verzeichnis `/nfs/export` auf dem lokalen Host eingehängt (`/nfs` wird aus der `auto.master`-Zuordnung entnommen). Das Verzeichnis `/nfs/export` wird automatisch durch `autofs` angelegt.

3. Falls Sie dieselbe NFS-Freigabe bereits statisch eingehängt haben, kommentieren Sie optional die zugehörige Zeile in `/etc/fstab` aus. Ein Beispiel für diese Zeile:

```
#jupiter.com:/home/geeko/doc/export /nfs/export nfs defaults 0 0
```

4. Laden Sie `autofs` neu und prüfen Sie die Funktionsweise:

```
sudo systemctl restart autofs
```

```
# ls -l /nfs/export
total 20
drwxr-xr-x  6 1001 users 4096 Oct 25 08:56 ./
drwxr-xr-x  3 root root     0 Apr  1 09:47 ../
drwxr-xr-x  5 1001 users 4096 Jan 14  2013 .images/
drwxr-xr-x 10 1001 users 4096 Aug 16  2013 .profiled/
drwxr-xr-x  3 1001 users 4096 Aug 30  2013 .tmp/
drwxr-xr-x  4 1001 users 4096 Oct 25 08:56 SLE-12-manual/
```

Wenn die Liste der Dateien auf der entfernten Freigabe angezeigt wird, funktioniert `autofs` einwandfrei.

29.5 Weitere Themen

Dieser Abschnitt befasst sich mit Themen, die über die grundlegende Einführung in `autofs` hinausgehen: automatisches Einhängen von NFS-Freigaben, die sich im Netzwerk befinden, Verwenden von Platzhalterzeichen in Zuordnungsdateien sowie spezielle Informationen für das CIFS-Dateisystem.

29.5.1 `/net`-Einhängepunkt

Dieser Helper-Einhängepunkt ist nützlich, wenn zahlreiche NFS-Freigaben vorhanden sind. Mit `/net` werden bei Bedarf alle NFS-Freigaben im lokalen Netzwerk automatisch eingehängt. Dieser Eintrag ist in der `auto.master`-Datei bereits vorhanden. Kommentieren Sie diesen Eintrag aus und starten Sie `autofs` neu:

```
/net      -hosts
```

```
systemctl restart autofs
```

Wenn Sie beispielsweise einen Server mit dem Namen `jupiter` nutzen, auf dem sich eine NFS-Freigabe mit dem Namen `/export` befindet, hängen Sie es mit folgendem Kommando

```
# cd /net/jupiter/export
```

an der Befehlszeile ein.

29.5.2 Verwenden von Platzhalterzeichen beim automatischen Einhängen von Unterverzeichnissen

Wenn ein Verzeichnis mit Unterverzeichnissen vorliegt, die einzeln automatisch eingehängt werden sollen – beispielsweise das Verzeichnis `/home` mit den Benutzerverzeichnissen der verschiedenen Benutzer –, dann bietet `autofs` eine geschickte Lösung.

Für Benutzerverzeichnisse fügen Sie die folgende Zeile in `auto.master` ein:

```
/home      /etc/auto.home
```

Ergänzen Sie nun die Datei `/etc/auto.home` mit der richtigen Zuordnung, so dass die Benutzerverzeichnisse der einzelnen Benutzer automatisch eingehängt werden. Erstellen Sie beispielsweise separate Einträge für die Verzeichnisse:

```
wilber      jupiter.com:/home/wilber
penguin      jupiter.com:/home/penguin
tux      jupiter.com:/home/tux
[...]
```

Dies ist äußerst umständlich, da Sie die Liste der Benutzer in `auto.home` verwalten müssen. Statt des Einhängepunkts können Sie ein Sternchen (*) angeben und statt des einzuhängenden Verzeichnisses das Und-Zeichen (&):

```
*      jupiter:/home/&
```

29.5.3 Automatisches Einhängen des CIFS-Dateisystems

Soll eine SMB/CIFS-Freigabe automatisch eingehängt werden (weitere Informationen zum SMB/CIFS-Protokoll siehe *Kapitel 28, Samba*), müssen Sie die Syntax der Zuordnungsdatei bearbeiten. Fügen Sie `-fstype=cifs` in das Optionsfeld ein und stellen Sie dem Speicherort der Freigabe einen Doppelpunkt (:) voran.

```
mount point      -fstype=cifs      ://jupiter.com/export
```

30 SLP

Um einen Netzwerkclient konfigurieren zu können, benötigen Sie eingehende Kenntnisse zu den Diensten, die über das Netzwerk bereitgestellt werden (z. B. Drucken oder LDAP). Als Erleichterung der Konfiguration dieser Dienste auf einem Netzwerkclient wurde das SLP („service location protocol“) entwickelt. SLP teilt allen Clients im lokalen Netzwerk die Verfügbarkeit und die Konfigurationsdaten ausgewählter Dienste mit. Anwendungen mit SLP-Unterstützung können diese Informationen verarbeiten und damit automatisch konfiguriert werden.

SUSE® Linux Enterprise Server unterstützt die Installation von per SLP bekannt gegebenen Installationsquellen und beinhaltet viele Systemdienste mit integrierter Unterstützung für SLP. Nutzen Sie SLP, um vernetzten Clients zentrale Funktionen wie Installationsserver, YOU-Server, Dateiserver oder Druckserver auf Ihrem System zur Verfügung zu stellen. Dienste mit SLP-Unterstützung sind beispielsweise login, ntp, openldap2, postfix, rpasswd, rsyncd, saned, sshd (über fish), vnc und ypserv.

Alle Pakete, die zur Verwendung von SLP-Diensten auf einem Netzwerkclient erforderlich sind, werden standardmäßig installiert. Falls Sie jedoch Dienste via SLP *bereitstellen* möchten, müssen Sie sicherstellen, dass auch das Paket `openslp-server` installiert wird.

30.1 Das SLP-Frontend **`slptool`**

Mit dem Kommandozeilenwerkzeug **`slptool`** werden SLP-Dienste abgefragt und registriert. Die Abfragefunktionen sind bei der Diagnose von Nutzen. Im Folgenden werden die wichtigsten Subkommandos von **`slptool`** aufgeführt. Mit **`slptool`** `--help` werden alle verfügbaren Optionen und Funktionen aufgelistet.

findsrvtypes

Zeigt eine Liste aller Dienste an, die im Netzwerk verfügbar sind.

```
tux >  slptool findsrvtypes
service:install.suse:nfs
service:install.suse:ftp
service:install.suse:http
service:install.suse:smb
service:ssh
```

```
service:fish
service:YaST.installation.suse:vnc
service:smtp
service:domain
service:management-software.IBM:hardware-management-console
service:rsync
service:ntp
service:ypserv
```

findsrvs *DIENSTTYP*

Zeigt eine Liste aller Server an, die den gewünschten *DIENSTTYP* bereitstellen.

```
tux >  slptool findsrvs service:ntp
service:ntp://ntp.example.com:123,57810
service:ntp://ntp2.example.com:123,57810
```

findattrs *DIENSTTYP* **HOST**

Zeigt eine Liste der Attribute für den *DIENSTTYP* auf dem *HOST* an.

```
tux >  slptool findattrs service:ntp://ntp.example.com
(owner=tux),(email=tux@example.com)
```

register *DIENSTTYP* **//** *HOST* **:** *PORT* **"(***ATTRIBUT=WERT***),(***ATTRIBUT=WERT***)"**

Registriert den *DIENSTTYP* auf dem *HOST*, wobei optional eine Liste mit Attributen angegeben werden kann.

```
slptool register service:ntp://ntp.example.com:57810 \
"(owner=tux),(email=tux@example.com)"
```

deregister *DIENSTTYP* **//** *HOST*

Hebt die Registrierung des *DIENSTTYPS* auf dem *HOST* auf.

```
slptool deregister service:ntp://ntp.example.com
```

Weitere Informationen erhalten Sie mit dem Kommando **`slptool --help`**.

30.2 Bereitstellen von Diensten über SLP

Zum Bereitstellen von SLP-Diensten muss der SLP-Daemon (`slpd`) ausgeführt werden. Wie die meisten Systemdienste unter SUSE Linux Enterprise Server wird der `slpd`-Daemon über ein separates Startskript gesteuert. Nach der Installation ist der Daemon standardmäßig inaktiv.

Zum Aktivieren für die aktuelle Sitzung führen Sie den Befehl **`sudo systemctl start slpd`** aus. Wenn `slpd` beim Systemstart aktiviert werden soll, führen Sie den Befehl **`sudo systemctl enable slpd`** aus.

Viele Anwendungen unter SUSE Linux Enterprise Server verfügen durch die `libslp`-Bibliothek 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. Im folgenden Beispiel wird ein Scannerdienst registriert:

```
## 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 Diensttyp (`scanner.sane`) und die Adresse, unter der der Dienst auf dem Server verfügbar ist. *`$HOSTNAME`* wird automatisch durch den vollständigen Hostnamen ersetzt. Abgetrennt durch einen Doppelpunkt folgt nun der Name des TCP-Ports, auf dem der entsprechende Dienst gefunden werden kann. Geben Sie nun die Sprache an, in der der Dienst angekündigt werden soll, und die Gültigkeitsdauer der Registrierung in Sekunden. Diese Angaben müssen durch Kommas von der Dienst-URL getrennt werden. Wählen Sie für die Registrierungsdauer einen Wert zwischen `0` und `65535`. `0` verhindert die Registrierung. `Mit` 65535 werden alle Einschränkungen aufgehoben.

Die Registrierungsdatei enthält außerdem die beiden Variablen `watch-port-tcp` und `description`. `watch-port-tcp` koppelt die SLP-Dienstankündigung daran, ob der entsprechende Dienst aktiv ist, indem `slpd` den Status des Diensts überprüft. Die zweite Variable enthält eine genauere Beschreibung des Diensts, die in den entsprechenden Browsern angezeigt wird.

Tipp: YaST und SLP

Einige von YaST bereitgestellte Services, wie ein Installationsserver oder YOU-Server, führen diese Registrierung automatisch aus, wenn Sie SLP in den Modul-Dialogfeldern aktivieren. Dann erstellt YaST Registrierungsdateien für diese Dienste.

Statische Registrierung über `/etc/slp.reg`

Der einzige Unterschied zwischen dieser Methode und der Prozedur mit `/etc/slp.reg.d` besteht darin, dass alle Dienste in einer zentralen Datei gruppiert sind.

Dynamische Registrierung über `slptool`

Wenn ein Dienst dynamisch ohne Verwendung von Konfigurationsdateien registriert werden soll, verwenden Sie das Kommandozeilenprogramm slptool. Dasselbe Programm kann auch die Registrierung eines bestehenden Dienstangebots aufheben, ohne `slpd` neu zu starten. Weitere Informationen finden Sie in *Abschnitt 30.1, „Das SLP-Frontend `slptool`“*.

30.2.1 Einrichten eines SLP-Installationsservers

Die Bereitstellung der Installationsdaten über SLP im Netzwerk erleichtert die Netzwerkinstallation deutlich, da die Installationsdaten (z. B. IP-Adresse des Servers oder Pfad zu den Installationsmedien) automatisch über eine SLP-Abfrage angefordert werden. Weitere Anweisungen finden Sie unter *Buch „*Bereitstellungshandbuch*“, Kapitel 8 „Einrichten des Servers, auf dem sich die Installationsquellen befinden“*.

30.3 Weiterführende Informationen

RFC 2608, 2609, 2610

RFC 2608 befasst sich mit der Definition von SLP im Allgemeinen. RFC 2609 geht näher auf die Syntax der verwendeten Dienst-URLs ein und RFC 2610 thematisiert DHCP über SLP.

http://www.openslp.org

Die Homepage des OpenSLP-Projekts.

`/usr/share/doc/packages/openslp`

Dieses Verzeichnis enthält die Dokumentation für SLP, die im Lieferumfang des `openslp-server`-Pakets enthalten ist, z. B. eine `README.SUSE`-Datei mit den SUSE Linux Enterprise Server-Details, die RFCs und zwei einführende HTML-Dokumente. Programmierer, die an den SLP-Funktionen interessiert sind, finden weitere Informationen im *Programmierhandbuch*, das im Paket `openslp-devel` im SUSE-SDK (Software Development Kit) enthalten ist.

31 Der HTTP-Server Apache

Gemäß der Umfrage von http://www.netcraft.com/ ist der HTTP-Server Apache (oder kurz "Apache") weltweit der meistgenutzte Webserver. Der von der Apache Software Foundation (http://www.apache.org/) entwickelte Apache-Server läuft auf fast allen Betriebssystemen. SUSE® Linux Enterprise Server umfasst Apache, Version 2.4. 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.

31.1 Kurzanleitung

In diesem Abschnitt finden Sie Informationen zum schnellen Einrichten und Starten von Apache. Zur Installation und Konfiguration von Apache müssen Sie `root`-Benutzer sein.

31.1.1 Anforderungen

Vergewissern Sie sich, dass folgende Voraussetzungen erfüllt sind, bevor Sie den Apache-Webserver einrichten:

1. Das Netzwerk des Computers ist ordnungsgemäß konfiguriert. Weitere Informationen zu diesem Thema finden Sie unter *Kapitel 16, Grundlegendes zu Netzwerken*.

2. Durch Synchronisierung mit einem Zeitserver ist sichergestellt, dass die Systemzeit des Computers genau ist. Die exakte Uhrzeit ist für Teile des HTTP-Protokolls nötig. Weitere Informationen zu diesem Thema finden Sie unter *Kapitel 24, Zeitsynchronisierung mit NTP*.

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 (`80`) geöffnet. Lassen Sie dazu in SUSEFirewall2 den Service *HTTP-Server* in der externen Zone zu. Dies können Sie mithilfe von YaST erledigen. Weitere Informationen finden Sie in *Buch „Security Guide", Kapitel 15 „Masquerading and Firewalls", Abschnitt 15.4.1 „Configuring the Firewall with YaST"*.

31.1.2 Installation

Apache ist in der Standardinstallation von SUSE Linux Enterprise Server nicht enthalten. Zum Installieren von Apache mit einer vordefinierten Standardkonfiguration „“ gehen Sie wie folgt vor:

PROZEDUR 31.1 INSTALLATION VON APACHE MIT DER STANDARDKONFIGURATION

1. Starten Sie YaST, und wählen Sie *Software* › *Software installieren oder löschen*.
2. Wählen Sie *Ansicht* › *Schemata* und schließlich *Web- und LAMP-Server*.
3. Bestätigen Sie die Installation der abhängigen Pakete, um den Installationsvorgang abzuschließen.

31.1.3 Start

Sie können Apache automatisch beim Booten oder manuell starten.

Um sicherzustellen, dass Apache beim Booten des Computers in den Zielen `multi-user.target` und `graphical.target` automatisch gestartet wird, führen Sie das folgende Kommando aus:

```
root # systemctl enable apache2
```

Weitere Informationen zu den systemd-Zielen in SUSE Linux Enterprise Server sowie eine Beschreibung zu YaST *Services Manager* finden Sie unter *Abschnitt 13.4, „Verwalten von Services mit YaST“*.

Über die Shell starten Sie Apache manuell mit dem Kommando **`systemctl start apache2`**.

PROZEDUR 31.2 ÜBERPRÜFEN, OB APACHE AUSGEFÜHRT WIRD

Werden beim Starten von Apache keine Fehlermeldungen angezeigt, bedeutet dies im Normalfall, dass der Webserver ausgeführt wird. So überprüfen Sie, ob Apache ausgeführt wird:

1. Starten Sie einen Webbrowser und öffnen Sie http://localhost/.
   Wenn Apache ausgeführt wird, wird eine Testseite mit der Meldung „It works!“ angezeigt.
2. Wenn diese Seite nicht angezeigt wird, lesen Sie den Abschnitt *Abschnitt 31.9, „Fehlerbehebung“*.

Nachdem der Webserver nun läuft, können Sie eigene Dokumente hinzufügen, die Konfiguration an Ihre Anforderungen anpassen und weitere Module mit den benötigten Funktionen installieren.

31.2 Konfigurieren von Apache

SUSE Linux Enterprise Server bietet zwei Konfigurationsoptionen:

- *Manuelle Konfiguration von Apache*
- *Konfigurieren von Apache mit YaST*

Bei der manuellen Konfiguration können Sie mehr Details einstellen, allerdings müssen Sie ohne den Komfort der Bedienoberfläche von YaST zurechtkommen.

Wichtig: Neuladen oder -starten von Apache nach Konfigurationsänderungen

Damit Konfigurationsänderungen wirksam werden, ist in den meisten Fällen ein erneutes Laden (in einigen Fällen auch ein Neustart) von Apache erforderlich. Laden Sie Apache manuell mit **`systemctl reload apache2`** neu oder verwenden Sie eine der in *Abschnitt 31.3, „Starten und Beenden von Apache“* beschriebenen Neustartoptionen.

Wenn Sie Apache mit YaST konfigurieren, kann dieser Schritt automatisch ausgeführt werden. Stellen Sie dazu *HTTP-Service* auf *Aktiviert* ein, wie in *Abschnitt 31.2.3.2, „HTTP-Server-Konfiguration“* beschrieben.

31.2.1 Apache-Konfigurationsdateien

Dieser Abschnitt enthält eine Übersicht über die Apache-Konfigurationsdateien. Wenn Sie die Konfiguration mit YaST vornehmen, müssen Sie diese Dateien nicht bearbeiten. Die Informationen können jedoch nützlich sein, wenn Sie später auf die manuelle Konfiguration umstellen möchten.

Die Konfigurationsdateien von Apache befinden sich in zwei verschiedenen Verzeichnissen:

- `/etc/sysconfig/apache2`
- `/etc/apache2/`

31.2.1.1 /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.

31.2.1.2 /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 *Direktiven* genannt). Die Konfigurationsoptionen dieser Dateien sind hinreichend dokumentiert und werden daher an dieser Stelle nicht näher erläutert.

Die Apache-Konfigurationsdateien gliedern sich wie folgt:

```
/etc/apache2/
     |
     |- charset.conv
     |- conf.d/
     |   |
     |   |- *.conf
     |
     |- default-server.conf
     |- errors.conf
     |- httpd.conf
     |- listen.conf
     |- magic
     |- mime.types
     |- mod_*.conf
     |- server-tuning.conf
     |- ssl.*
     |- ssl-global.conf
     |- sysconfig.d
     |   |
     |   |- global.conf
     |   |- include.conf
     |   |- loadmodule.conf . .
     |
     |- uid.conf
     |- vhosts.d
```

```
|   |- *.conf
```

APACHE-KONFIGURATIONSDATEIEN IN /ETC/APACHE2/

`charset.conv`

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 entsprechenden 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. Weitere Informationen finden Sie unter *Abschnitt 31.2.2.1.1, „Namensbasierte virtuelle Hosts“*.

`magic`

Diese Datei enthält Daten für das Modul mime_magic, mit dessen Hilfe Apache den MIME-Typ unbekannter Dateien ermittelt. Ändern Sie diese Datei nicht.

`mime.types`

Diese Datei enthält die dem System bekannten MIME-Typen (genau genommen ist diese Datei eine Verknüpfung mit `/etc/mime.types`). Bearbeiten Sie diese Datei nicht. MIME-Typen, die hier nicht aufgelistet sind, sollten Sie der Datei `mod_mime-defaults.conf` hinzufügen.

`mod_*.conf`

Dies sind die Konfigurationsdateien der in der Standardinstallation enthaltenen Module. Weitere Informationen hierzu erhalten Sie unter *Abschnitt 31.4, „Installieren, Aktivieren und Konfigurieren von Modulen“*. Die Konfigurationsdateien optionaler Module befinden sich im Verzeichnis `conf.d`.

`server-tuning.conf`

Diese Datei enthält Konfigurationsdirektiven für verschiedene MPMs (siehe *Abschnitt 31.4.4, „Multiprocessing-Module“*) und allgemeine Konfigurationsoptionen, die sich auf die Leistung von Apache auswirken. Sie können diese Datei bearbeiten, sollten den Webserver anschließend aber gründlich testen.

`ssl-global.conf` **und** `ssl.*`

Diese Dateien enthalten die globale SSL-Konfiguration und die SSL-Zertifikatdaten. Weitere Informationen hierzu erhalten Sie unter *Abschnitt 31.6, „Einrichten eines sicheren Webservers mit SSL“*.

`sysconfig.d/*.conf`

Diese Konfigurationsdateien werden automatisch aus `/etc/sysconfig/apache2` generiert. Ändern Sie diese Dateien nicht. Bearbeiten Sie stattdessen die Dateien unter `/etc/sysconfig/apache2`. Speichern Sie in diesem Verzeichnis keine anderen Konfigurationsdateien.

`uid.conf`

Diese Datei gibt die Benutzer- und Gruppen-ID an, unter der Apache läuft. Ändern Sie diese Datei nicht.

`vhosts.d/*.conf`

In diesem Verzeichnis wird die virtuelle Host-Konfiguration gespeichert. Das Verzeichnis enthält Vorlagendateien für virtuelle Hosts mit und ohne SSL. Alle Dateien in diesem Verzeichnis mit der Erweiterung `.conf` sind automatisch Bestandteil der Apache-Konfiguration. Weitere Informationen finden Sie unter *Abschnitt 31.2.2.1, „Virtuelle Hostkonfiguration“*.

31.2.2 Manuelle Konfiguration von Apache

Wenn Sie den Apache-Webserver manuell konfigurieren möchten, müssen Sie die Klartext-Konfigurationsdateien als `root`-Benutzer bearbeiten.

31.2.2.1 Virtuelle Hostkonfiguration

Virtueller Host bezieht sich auf die Fähigkeit von Apache, mehrere URI (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.

Verwenden Sie zum Auflisten aller vorhandenen virtuellen Hosts das Kommando **`apache2ctl -S`**. Dadurch wird eine Liste mit dem Standardserver und allen virtuellen Hosts zusammen mit deren IP-Adressen und überwachenden Ports ausgegeben. Zusätzlich enthält die Liste einen Eintrag für jeden virtuellen Host mit dessen Speicherort in den Konfigurationsdateien.

Virtuelle Hosts können mit YaST (siehe *Abschnitt 31.2.3.1.4, „Virtuelle Hosts“*) 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 Basiskonfiguration 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.

Bei der Verwendung von namenbasierten virtuellen Hosts empfiehlt es sich, eine Standardkonfiguration einzurichten, die verwendet wird, wenn ein Domänenname nicht mit einer virtuellen Hostkonfiguration übereinstimmt. Der virtuelle Standardhost ist der Host, dessen Konfiguration zuerst geladen wird. Da die Reihenfolge der Konfigurationsdateien durch den Dateinamen bestimmt wird, starten Sie den Dateinamen der Konfiguration des virtuellen Standardhosts mit einem Unterstrich `_`, um sicherzustellen, dass sie zuerst geladen wird (z. B. `_default_vhost.conf`).

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/2.4/mod/quickreference.html.

31.2.2.1.1 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.

Erstellen Sie zunächst je einen `<VirtualHost>`-Block für die einzelnen zu bedienenden namensbasierten Hosts. Jeder `<VirtualHost>`-Block muss mindestens eine `ServerName`-Direktive enthalten, mit der die zu bedienenden Hosts zugewiesen werden, sowie eine `DocumentRoot`-Direktive, aus der der Speicherort im Dateisystem hervorgeht, an dem sich der Inhalt für diesen Host befindet.

BEISPIEL 31.1 EINFACHE BEISPIELE FÜR NAMENSBASIERTE `VirtualHost`-EINTRÄGE

```
<VirtualHost *:80>
# This first-listed virtual host is also the default for *:80
ServerName www.example.com
ServerAlias example.com
DocumentRoot /srv/www/htdocs/domain
</VirtualHost>

<VirtualHost *:80>
ServerName other.example.com
```

```
DocumentRoot /srv/www/htdocs/otherdomain
</VirtualHost>
```

In einer namensbasierten virtuellen Hostkonfiguration übernimmt das `VirtualHost`-Anfangstag die IP-Adresse (bzw. den vollständig qualifizierten Domänennamen) als Argument. Eine Portnummer-Direktive ist optional.

Anstelle der IP-Adresse wird auch ein Platzhalterzeichen (*) akzeptiert. IPv6-Adressen müssen in eckige Klammern eingeschlossen werden.

BEISPIEL 31.2 NAMENSBASIERTE `VirtualHost`-DIREKTIVEN

```
<VirtualHost 192.168.3.100:80>
  ...
</VirtualHost>

<VirtualHost 192.168.3.100>
  ...
</VirtualHost>

<VirtualHost *:80>
  ...
</VirtualHost>

<VirtualHost *>
  ...
</VirtualHost>

<VirtualHost [2002:c0a8:364::]>
  ...
</VirtualHost>
```

31.2.2.1.2 IP-basierte virtuelle Hosts

Bei dieser alternativen virtuellen Hostkonfiguration werden auf einem Computer mehrere IPs eingerichtet. Auf einer Apache-Instanz befinden sich mehrere Domänen, denen jeweils eine eigene IP zugewiesen ist.

Auf dem physischen Server muss für jeden IP-basierten virtuellen Host eine eigene IP-Adresse eingerichtet sein. Falls der Computer nicht über die entsprechende Anzahl an Netzwerkkarten verfügt, können auch virtuelle Netzwerkschnittstellen verwendet werden (IP-Aliasing).

Das folgende Beispiel zeigt Apache auf einem Computer mit der IP `192.168.3.100`, auf dem sich zwei Domänen mit den zusätzlichen IPs `192.168.3.101` und `192.168.3.102` befinden. Für jeden virtuellen Server wird ein eigener `VirtualHost`-Block benötigt.

BEISPIEL 31.3 IP-BASIERTE `VirtualHost`-DIREKTIVEN

```
<VirtualHost 192.168.3.101>
  ...
</VirtualHost>

<VirtualHost 192.168.3.102>
  ...
</VirtualHost>
```

In diesem Beispiel sind nur für die beiden zusätzlichen IP-Adressen (also nicht für `192.168.3.100`) `VirtualHost`-Direktiven angegeben. Sollte für `192.168.3.100` 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.

31.2.2.1.3 Basiskonfiguration eines virtuellen Hosts

Die Konfiguration eines virtuellen Hosts sollte mindestens die folgenden Direktiven enthalten, um den virtuellen Host einzurichten. 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 die separate Analyse der Zugriffsdaten für jeden einzelnen Host ermöglicht. `/var/log/apache2/` ist das Standardverzeichnis für die Protokolldateien von Apache.

Wie bereits erwähnt, ist standardmäßig auf das gesamte Dateisystem kein Zugriff möglich. Die Verzeichnisse, in die Sie die Dateien gestellt haben, mit denen Apache arbeiten soll – zum Beispiel das Verzeichnis `DocumentRoot` –, müssen daher explizit entsperrt werden:

```
<Directory "/srv/www/www.example.com/htdocs">
  Require all granted
</Directory>
```

Anmerkung: `Require all granted`

In vorherigen Versionen von Apache wurde die Anweisung `Require all granted` wie folgt ausgedrückt:

```
Order allow,deny
Allow from all
```

Diese alte Syntax wird vom `mod_access_compat`-Modul nach wie vor unterstützt.

Die vollständige Basiskonfiguration eines virtuellen Hosts sieht wie folgt aus:

BEISPIEL 31.4 BASISKONFIGURATION `eines virtuellen Hosts`

```
<VirtualHost 192.168.3.100>
  ServerName www.example.com
  DocumentRoot /srv/www/www.example.com/htdocs
  ServerAdmin webmaster@example.com
  ErrorLog /var/log/apache2/www.example.com_log
  CustomLog /var/log/apache2/www.example.com-access_log common
  <Directory "/srv/www/www.example.com/htdocs">
  Require all granted
  </Directory>
```

```
</VirtualHost>
```

31.2.3 Konfigurieren von Apache mit YaST

Zur Konfiguration des Webservers mit YaST starten Sie YaST, und wählen Sie *Netwerkdienste* › *HTTP-Server*. Wenn Sie dieses Modul zum ersten Mal starten, wird der *HTTP-Server-Assistent* geöffnet und sie werden aufgefordert, einige grundlegende Entscheidungen zur Verwaltung des Servers zu treffen. Nach Fertigstellung des Assistenten wird das Dialogfeld *HTTP-Server-Konfiguration* geöffnet, sobald Sie das *HTTP-Server*-Modul aufrufen. Weitere Informationen finden Sie unter *Abschnitt 31.2.3.2, „HTTP-Server-Konfiguration“*.

31.2.3.1 HTTP-Server-Assistent

Der HTTP-Server-Assistent besteht aus fünf Schritten. Im letzten Schritt des Assistenten können Sie den Expertenkonfigurationsmodus aufrufen, in dem Sie weitere spezielle Einstellungen vornehmen können.

31.2.3.1.1 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 *Firewall-Port 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. Wenn Sie über mehrere Netzwerkschnittstellen verfügen, klicken Sie auf *Firewall-Details*, um festzulegen, an welchen Schnittstellen die Ports geöffnet werden sollen.

Klicken Sie auf *Weiter*, um mit der Konfiguration fortzufahren.

31.2.3.1.2 Module

Mit der Konfigurationsoption *Module* aktivieren bzw. deaktivieren Sie die vom Webserver unterstützten Skriptsprachen. Informationen zur Aktivierung bzw. Deaktivierung anderer Module erhalten Sie unter *Abschnitt 31.2.3.2.2, „Servermodule“*. Klicken Sie auf *Weiter*, um das nächste Dialogfeld zu öffnen.

31.2.3.1.3 Standardhost

Diese Option betrifft den Standard-Webserver. Wie in *Abschnitt 31.2.2.1, „Virtuelle Hostkonfiguration“* 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*.

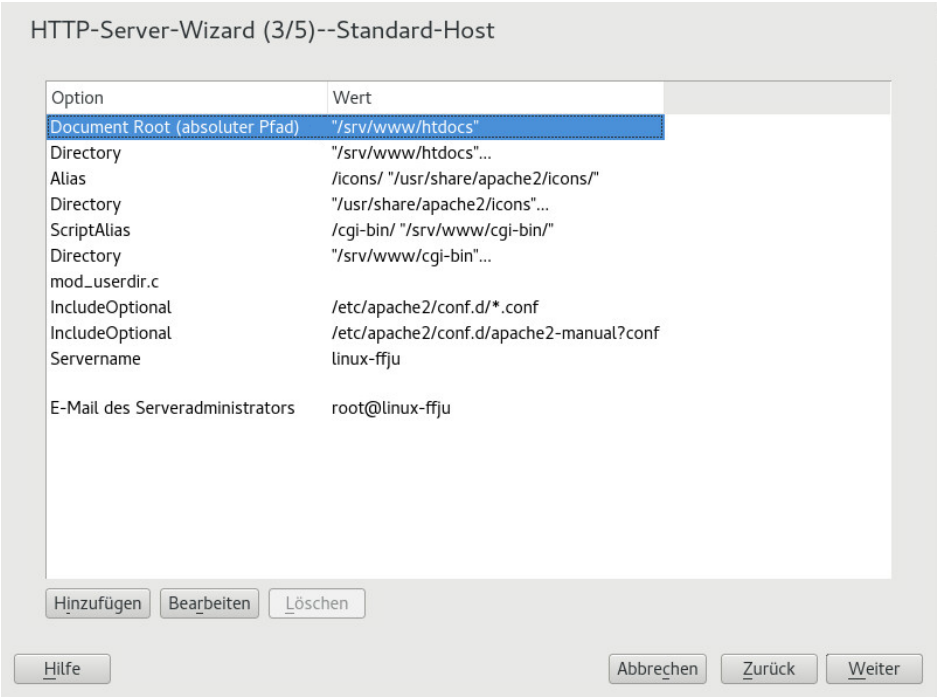


ABBILDUNG 31.1 HTTP-SERVER-ASSISTENT: STANDARDHOST

Für den Server gelten folgende Standardeinstellungen:

`Document-Root`

Der absolute Pfad des Verzeichnisses, aus dem Apache die Dateien für diesen Host bedient. Dies ist standardmäßig `/srv/www/htdocs`.

`Alias`

Mit `Alias`-Direktiven können URLs zu Speicherorten in physischen Dateisystemen 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 /icons` für die in der Verzeichnisindex-Ansicht angezeigten Apache-Symbole verweist auf `/usr/share/apache2/icons`.

`ScriptAlias`

Ähnlich wie die `Alias`-Direktive ordnet die `ScriptAlias`-Direktive eine URL einem Speicherort im Dateisystem zu. Der Unterschied besteht darin, dass `ScriptAlias` als Zielverzeichnis einen CGI-Speicherort für die Ausführung von CGI-Skripten festlegt.

`Verzeichnis`

Unter den `Verzeichnis`-Einstellungen können Sie eine Gruppe von Konfigurationsoptionen zusammenfassen, die nur für das angegebene Verzeichnis gelten.

Hier werden auch die Zugriffs- und Anzeigeoptionen für die Verzeichnisse `/srv/www/htdocs`, `/usr/share/apache2/icons` und `/srv/www/cgi-bin` konfiguriert. Eine Änderung dieser Standardeinstellungen sollte nicht erforderlich sein.

`Einbeziehen`

Hier können weitere Konfigurationsdateien hinzugefügt werden. Zwei `Include`-Direktiven sind bereits vorkonfiguriert: `/etc/apache2/conf.d/` ist das Verzeichnis für die Konfigurationsdateien externer Module. Durch diese Direktive werden alle Dateien in diesem Verzeichnis mit der Erweiterung `.conf` eingeschlossen. Durch die zweite Direktive, `/etc/apache2/conf.d/apache2-manual.conf`, wird die Konfigurationsdatei `apache2-manual` eingeschlossen.

`Servername`

Hier wird die Standard-URL festgelegt, über die Clients den Webserver kontaktieren. Verwenden Sie einen qualifizierten 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.

Klicken Sie am Ende der Seite *Standardhost* auf *Weiter*, um mit der Konfiguration fortzufahren.

31.2.3.1.4 Virtuelle Hosts

In diesem Schritt zeigt der Assistent eine Liste der bereits konfigurierten virtuellen Hosts an (siehe *Abschnitt 31.2.2.1, „Virtuelle Hostkonfiguration“*). Wenn Sie vor dem Starten des YaST-HTTP-Assistenten keine manuellen Änderungen vorgenommen haben, ist kein virtueller Host vorhanden.

Zum Hinzufügen eines Hosts klicken Sie auf *Hinzufügen*, um ein Dialogfeld zu öffnen, in das Sie grundlegende Informationen über den Host eingeben, z. B. *Servername*, *Übergeordnetes Verzeichnis der Server-Inhalte* (`DocumentRoot`) und *Administrator-E-Mail*. Unter *Server-Auflösung* legen Sie fest, wie der Host identifiziert wird (nach seinem Namen oder nach seiner IP-Adresse). Geben Sie den Namen oder die IP-Adresse unter *Change Virtual Host ID* (Virtuelle Host-ID ändern) an.

Klicken Sie auf *Weiter*, um mit dem zweiten Teil der virtuellen Hostkonfiguration fortzufahren.

Im zweiten Teil der virtuellen Hostkonfiguration legen Sie fest, ob CGI-Skripten zugelassen sind und welches Verzeichnis für diese Skripten verwendet wird. Dort können Sie auch SSL aktivieren. Wenn Sie SSL aktivieren, müssen Sie auch den Zertifikatpfad angeben. Informationen über SSL und Zertifikate finden Sie in *Abschnitt 31.6.2, „Konfigurieren von Apache mit SSL“*. 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 *Public HTML aktivieren* stellen Sie den Inhalt der öffentlichen Benutzerverzeichnisse (`~USER/public_html/`) auf dem Server unter `http://www.example.com/~USER` bereit.

Wichtig: Erstellen virtueller Hosts

Virtuelle Hosts können Sie nicht völlig willkürlich hinzufügen. Wenn Sie namensbasierte virtuelle Hosts hinzufügen möchten, müssen die Hostnamen im Netzwerk aufgelöst sein. Bei IP-basierten virtuellen Hosts darf jeder verfügbaren IP-Adresse nur ein Host zugewiesen sein.

31.2.3.1.5 Zusammenfassung

Dies ist der abschließende Schritt des Assistenten. Legen Sie hier fest, wie und wann der Apache-Server gestartet werden soll: beim Boot-Vorgang oder manuell. Außerdem erhalten Sie in diesem Schritt eine kurze Zusammenfassung Ihrer bisherigen Konfiguration. Wenn Sie mit den Einstellungen zufrieden sind, schließen Sie die Konfiguration mit *Verlassen* ab. Zum Ändern bestimmter Einstellungen klicken Sie so oft auf *Zurück* , bis das entsprechende Dialogfeld angezeigt wird. Über *Expertenkonfiguration für HTTP-Server* können Sie hier auch das in *Abschnitt 31.2.3.2, „HTTP-Server-Konfiguration“* beschriebene Dialogfeld öffnen.

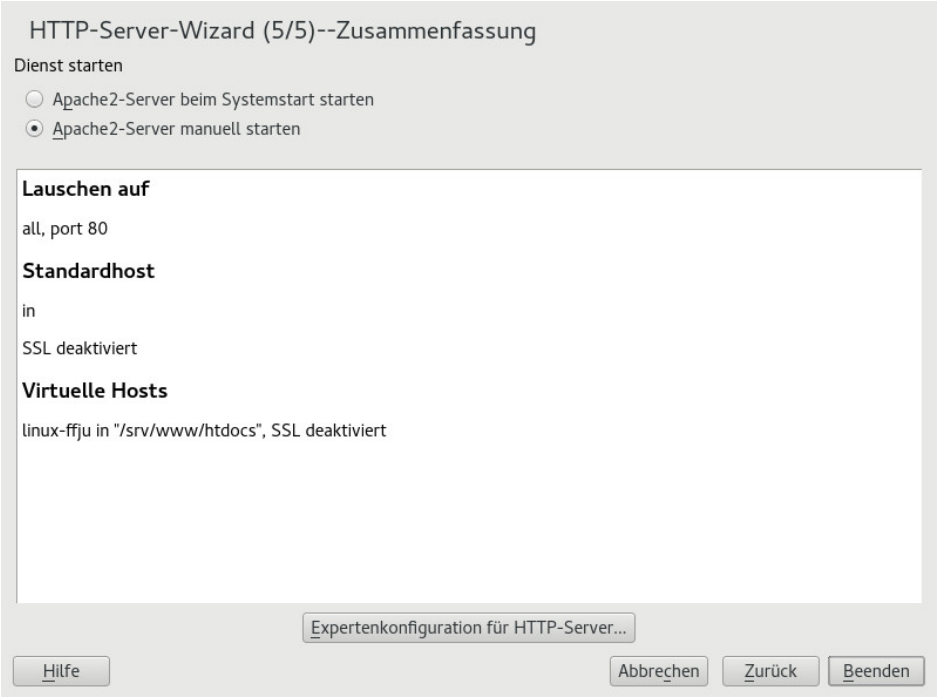


ABBILDUNG 31.2 HTTP-SERVER-ASSISTENT: ZUSAMMENFASSUNG

31.2.3.2 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 verlassen Sie das Konfigurationsmodul und Ihre Konfigurationsänderungen werden verworfen.

31.2.3.2.1 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. Die Option *Firewall-Port öffnen* sollte immer aktiviert sein, weil ansonsten der Webserver von außen nicht erreichbar ist. Das Schließen des Ports ist nur in Testsituationen sinnvoll, in denen kein externer Zugriff auf den Webserver erforderlich ist. Wenn Sie über mehrere Netzwerkschnittstellen verfügen, klicken Sie auf *Firewall-Details*, um festzulegen, an welchen Schnittstellen die Ports geöffnet werden sollen.

Über die Schaltfläche *Protokolldateien* können Sie die Zugriffs- oder die Fehlerprotokolldatei 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. Weitere Informationen finden Sie in *Abschnitt 31.3, „Starten und Beenden von Apache“*. Diese Kommandos sind sofort wirksam und ihre Protokollmeldungen werden auch sofort angezeigt.

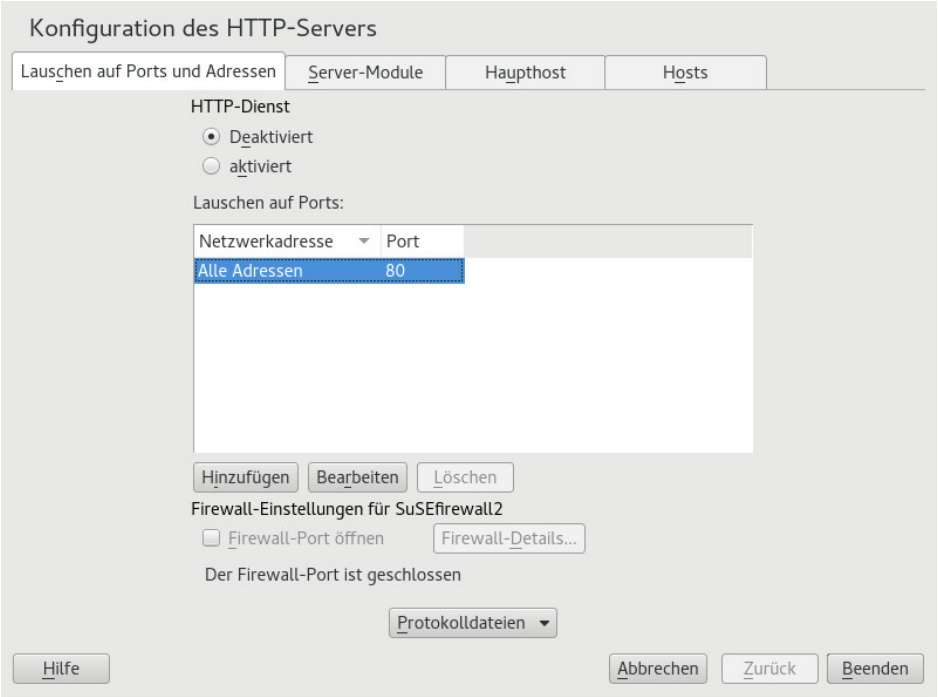


ABBILDUNG 31.3 KONFIGURATION DES HTTP-SERVERS: ÜBERWACHEN VON PORTS UND ADRESSEN

31.2.3.2.2 Servermodule

Über *Status wechseln* können Sie Apache2-Module aktivieren und deaktivieren. Über *Modul hinzufügen* können Sie weitere Module hinzufügen, die zwar bereits installiert, aber noch nicht in dieser Liste aufgeführt sind. Weitere Informationen über Module finden Sie in *Abschnitt 31.4, „Installieren, Aktivieren und Konfigurieren von Modulen“*.

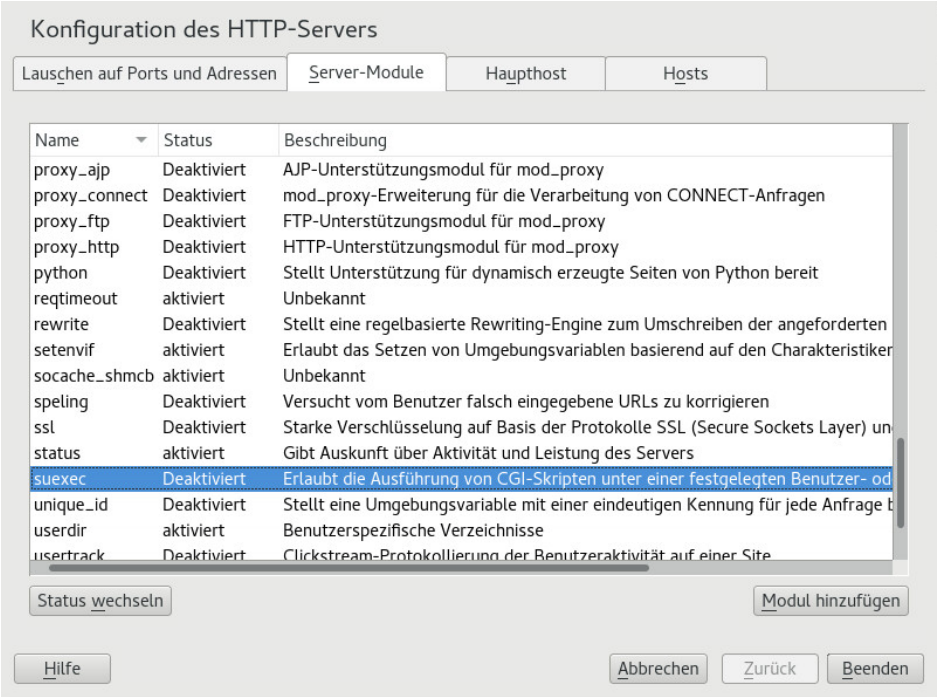


ABBILDUNG 31.4 KONFIGURATION DES HTTP-SERVERS: SERVER-MODULE

31.2.3.2.3 Haupthost oder Hosts

Diese Dialogfelder sind mit den bereits beschriebenen identisch. in *Abschnitt 31.2.3.1.3, „Standardhost“* und *Abschnitt 31.2.3.1.4, „Virtuelle Hosts“* beschriebenen Dialogfeldern.

31.3 Starten und Beenden von Apache

Bei Konfiguration mit YaST, wie in *Abschnitt 31.2.3, „Konfigurieren von Apache mit YaST“* beschrieben, wird Apache beim Booten des Computers in `multi-user.target` und `graphical.target` gestartet. Diese Funktionsweise können Sie mit YaST *Services Manager* oder dem Kommandozeilenwerkzeug **`systemctl`** (**`systemctl enable`** oder **`systemctl disable`**) ändern.

Mit den Kommandos **`systemctl`** bzw. **`apachectl`** können Sie Apache auf einem laufenden System starten, stoppen und ändern.

Allgemeine Informationen zu **`systemctl`**-Kommandos finden Sie unter *Abschnitt 13.2.1, „Verwalten von Diensten auf einem laufenden System“*.

`systemctl status apache2`

Überprüft, ob Apache gestartet wurde.

`systemctl start apache2`

Startet Apache, sofern es noch nicht läuft.

`systemctl stop apache2`

Stoppt Apache durch Beenden des übergeordneten Prozesses.

`systemctl restart apache2`

Beendet Apache und startet es danach neu. Falls der Webserver noch nicht gelaufen ist, wird er nun gestartet.

`systemctl try-restart apache2`

Stoppt Apache und startet es erneut, vorausgesetzt, es wird bereits ausgeführt.

`systemctl reload apache2`

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: Neustart von Apache in Produktionsumgebungen

Mit diesem Kommando können Änderungen in der Apache-Konfiguration aktiviert werden, ohne dass die Verbindung unterbrochen wird.

`systemctl stop apache2`

Hält den Webserver nach einer Zeitdauer an, die mit `GracefulShutdownTimeout` konfiguriert wurde, um sicherzustellen, dass die bestehenden Anforderungen abgeschlossen werden können.

`apachectl 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.

`apachectl status` und **`apachectl fullstatus`**

Erstellt einen Dump des kurzen oder vollständigen Statusfensters. Das Modul `mod_status` muss aktiviert und ein Textbrowser (z. B. **`links`** oder **`w3m`**) muss installiert sein. Außerdem muss `/etc/sysconfig/apache2` unter `APACHE_SERVER_FLAGS` das Flag `status` enthalten.

Tipp: Weitere Flags

Wenn Sie weitere Flags für die Kommandos festlegen, werden diese an den Webserver übergeben.

31.4 Installieren, Aktivieren und Konfigurieren von Modulen

Die Apache-Software ist modular aufgebaut. Alle Funktionen außer einigen Kernaufgaben werden von Modulen durchgeführt Dies geht sogar so weit, dass selbst HTTP durch ein Modul verarbeitet wird (`http_core`).

Apache-Module können bei der Entwicklung in die Apache-Binaries kompiliert oder während der Laufzeit dynamisch geladen werden. Informationen zum dynamischen Laden von Modulen erhalten Sie unter *Abschnitt 31.4.2, „Aktivieren und Deaktivieren von Modulen“*.

Apache-Module lassen sich in vier Kategorien einteilen:

Basismodule

Basismodule sind standardmäßig in Apache enthalten. In Apache in SUSE Linux Enterprise Server sind nur `mod_so` (zum Laden anderer Module) und `http_core` kompiliert. Alle anderen Module sind als gemeinsam genutzte Objekte verfügbar: Sie sind nicht in der Server-Binärdatei enthalten, sondern können zur Laufzeit eingebunden werden.

Erweiterungsmodule

Im Allgemeinen sind Erweiterungsmodule im Apache-Softwarepaket enthalten, jedoch nicht statisch im Server kompiliert. In SUSE Linux Enterprise Server 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 Enterprise Server umfasst jedoch mehrere Module.

Multiprocessing-Module (MPMs)

Multiprocessing-Module (MPMs) sind dafür verantwortlich, Anforderungen an den Webserver anzunehmen und zu verarbeiten, und stellen damit das Kernstück der Webserver-Software dar.

31.4.1 Installieren von Modulen

Wenn Sie die in *Abschnitt 31.1.2, „Installation“* beschriebene Standardinstallation vorgenommen haben, sind folgende Module bereits installiert: alle Basis- und Erweiterungsmodule, das Multiprocessing-Modul Prefork MPM sowie das externe Modul `mod_python`.

In YaST können Sie weitere externe Module installieren. Starten Sie dazu YaST und wählen Sie *Software* › *Software-Management*. Wählen Sie danach *Ansicht* › *Suche* und suchen Sie nach *apache*. Die Ergebnisliste zeigt nun neben anderen Paketen alle verfügbaren externen Apache-Module an.

31.4.2 Aktivieren und Deaktivieren von Modulen

Sie können bestimmte Module entweder manuell oder mit YaST aktivieren oder deaktivieren. In YaST müssen die Skriptsprachmodule (PHP5, Perl und Python) mit der im Abschnitt *Abschnitt 31.2.3.1, „HTTP-Server-Assistent“* beschriebenen Modulkonfiguration aktiviert oder deaktiviert werden. Alle anderen Module werden, wie im Abschnitt *Abschnitt 31.2.3.2.2, „Servermodule“* beschrieben, aktiviert oder deaktiviert.

Mit den Kommandos **`a2enmod`** *`MODUL`* bzw. **`a2dismod`** *`MODUL`* können Sie die Module stattdessen manuell aktivieren oder deaktivieren. **`a2enmod -l`** gibt eine Liste aller derzeit 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 unter `/etc/apache2/conf.d/` und werden standardmäßig in `/etc/apache2/default-server.conf` geladen. Für eine feinere

Steuerung können Sie die Einbeziehung in `/etc/apache2/default-server.conf` auskommentieren und sie nur zu bestimmten virtuellen Hosts hinzufügen. Beispiele hierzu finden Sie in der Datei `/etc/apache2/vhosts.d/vhost.template`.

31.4.3 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/2.4/mod/.

`mod_actions`

Bietet Methoden zur Ausführung eines Skripts, wenn ein bestimmter MIME-Typ (z. B. `application/pdf`), eine Datei mit einer bestimmten Erweiterung (z. B. `.rpm`) oder eine bestimmte Anforderungsmethode (z. B. `GET`) verlangt wird. Dieses Modul ist standardmäßig aktiviert.

`mod_alias`

Dieses Modul stellt die Direktiven `Alias` und `Redirect` bereit. Damit können Sie eine URI einem bestimmten Verzeichnis zuordnen (`Alias`) bzw. eine angeforderte URL umleiten. Dieses Modul ist standardmäßig aktiviert.

`mod_auth*`

Die Authentifizierungsmodule bieten verschiedene Methoden zur Authentifizierung: Basisauthentifizierung mit `mod_auth_basic` oder Digest-Authentifizierung mit `mod_auth_digest`.

`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/2.4/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_env`

Steuert die Umgebungsvariablen, die an CGI-Skripten oder SSI-Seiten übergeben werden. Sie können Umgebungsvariablen festlegen oder aufheben oder von der Shell übergeben, die den httpd-Prozess aufgerufen hat. Dieses Modul ist standardmäßig aktiviert.

`mod_expires`

Mit `mod_expires` legen Sie fest, wie häufig Ihre Dokumente über Proxy- und Browser-Caches durch Zustellung eines `Expires`-Header aktualisiert werden. Dieses Modul ist standardmäßig aktiviert.

`mod_http2`

Dank `mod_http2` unterstützt Apache das HTTP/2-Protokoll. Dies kann durch Angabe von `Protocols h2 http/1.1` in einem `VirtualHost` aktiviert werden.

`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`

Das MIME-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/2.4/content-negotiation.html. Dieses Modul ist standardmäßig aktiviert.

`mod_rewrite`

Dieses Modul stellt die gleiche Funktionalität wie `mod_alias` bereit, bietet aber mehr Funktionen und ist somit flexibler. Mit `mod_rewrite` können Sie URLs auf Basis verschiedener Regeln umleiten, Header anfordern und einiges mehr.

`mod_setenvif`

Legt Umgebungsvariablen auf der Basis von Details aus der Client-Anforderung fest, z. B. die Browserzeichenfolge, die der Client sendet, oder die IP-Adresse des Clients. Dieses Modul ist standardmäßig aktiviert.

`mod_spelling`

`mod_speling` versucht, typografische Fehler in URLs, beispielsweise die Groß-/Kleinschreibung, automatisch zu korrigieren.

`mod_ssl`

Dieses Modul ermöglicht verschlüsselte Verbindungen zwischen dem Webserver und den Clients. Weitere Informationen finden Sie in *Abschnitt 31.6, „Einrichten eines sicheren Webservers mit SSL“*. 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`

`mod_suexec` ermöglicht die Ausführung von CGI-Skripten unter einem anderen Benutzer oder einer anderen Gruppe. Dieses Modul ist standardmäßig aktiviert.

`mod_userdir`

Dieses Modul ermöglicht benutzerspezifische Verzeichnisse unter *`~USER/`*. In der Konfiguration muss die `UserDir`-Direktive angegeben sein. Dieses Modul ist standardmäßig aktiviert.

31.4.4 Multiprocessing-Module

SUSE Linux Enterprise Server bietet zwei Multiprocessing-Module (MPMs) für Apache:

- *Prefork-MPM*
- *Worker-MPM*

31.4.4.1 Prefork-MPM

Das Prefork-MPM implementiert einen Prefork-Webserver, der keine Threads verwendet. Mit diesem Modul verhält sich der Webserver, was die Handhabung von Anforderungen betrifft, ähnlich wie Apache Version 1.x: Er isoliert jede einzelne Anforderung und verarbeitet sie in einem separaten untergeordneten Prozess (Forking). Eine Beeinträchtigung aller Anforderungen durch wenige problematische Anforderungen und somit eine Sperre des Webservers lassen sich dadurch vermeiden.

Die prozessbasierte Vorgehensweise des Prefork-MPM bietet zwar Stabilität, konsumiert aber mehr Systemressourcen wie das Worker-MPM. Für UNIX-basierte Betriebssysteme gilt das Prefork-MPM als Standard-MPM.

Wichtig: MPMs in diesem Dokument

In diesem Dokument wird davon ausgegangen, dass Apache mit dem Prefork-MPM verwendet wird.

31.4.4.2 Worker-MPM

Das Worker-MPM implementiert einen Multithread-Webserver. Ein Thread ist die „Lightweight-Version“ eines Prozesses. Der Vorteil von Threads gegenüber Prozessen ist deren geringerer Ressourcenkonsum. Anstatt lediglich untergeordnete Prozesse zu erstellen (Forking), verarbeitet das Worker-MPM Anforderungen durch Threads mit Serverprozessen. Die untergeordneten Prefork-Prozesse sind auf mehrere Threads verteilt (Multithreading). Diese Ansatzweise macht den Apache-Server durch den geringeren Ressourcenkonsum leistungsfähiger als mit dem Prefork-MPM.

Ein Hauptnachteil ist die Instabilität des Worker-MPM: Ein fehlerhafter Thread kann sich auf alle Threads eines Prozesses auswirken. Im schlimmsten Fall fällt der Server dadurch aus. Besonders bei gleichzeitiger Verwendung des 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 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.

31.4.5 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.

`mod_apparmor`

Unterstützt Apache bei der AppArmor-Einschränkung auf einzelne cgi-Skripte, die von Modulen wie `mod_php5` und `mod_perl` benutzt werden.

Paketname: `apache2-mod_apparmor`
Weitere Informationen: *Buch „*Security Guide"

`mod_perl`

`mod_perl` ermöglicht die Ausführung von Perl-Skripten in einem eingebetteten Interpreter. Durch den dauerhaften, im Server eingebetteten Interpreter lassen sich Verzögerungen durch den Start eines externen Interpreters und den Start von Perl vermeiden.

Paketname: `apache2-mod_perl`
Konfigurationsdatei: `/etc/apache2/conf.d/mod_perl.conf`
Weitere Informationen: `/usr/share/doc/packages/apache2-mod_perl`

`mod_php5`

PHP ist eine serverseitige, plattformübergreifende, in HTML eingebettete Skriptsprache.

Paketname: `apache2-mod_php5`
Konfigurationsdatei: `/etc/apache2/conf.d/php5.conf`
Weitere Informationen: `/usr/share/doc/packages/apache2-mod_php5`

`mod_python`

`mod_python` bettet Python in den Apache-Webserver ein. Dies bringt Ihnen einen erheblichen Leistungsgewinn und zusätzliche Flexibilität bei der Entwicklung webbasierter Anwendungen.

Paketname: `apache2-mod_python`
Weitere Informationen: `/usr/share/doc/packages/apache2-mod_python`

`mod_security`

`mod_security` bietet eine Firewall zum Schutz von Webanwendungen vor verschiedenen Angriffen. Auch die Überwachung des HTTP-Datenverkehrs und die Echtzeitanalyse werden damit ermöglicht.

Paketname: `apache2-mod_security2`
Konfigurationsdatei: `/etc/apache2/conf.d/mod_security2.conf`
Weitere Informationen: `/usr/share/doc/packages/apache2-mod_security2`
Dokumentation: http://modsecurity.org/documentation/

31.4.6 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. Das Installationsverzeichnis ist `/usr/lib64/apache2`.
- `/usr/sbin/apxs2-prefork`: Für die Entwicklung von Prefork-MPM-Modulen. Das Installationsverzeichnis ist `/usr/lib64/apache2-prefork`.
- `/usr/sbin/apxs2-worker`: Für die Entwicklung von Worker-MPM-Modulen. Das Installationsverzeichnis ist `/usr/lib64/apache2-worker`.

Mit den folgenden Kommandos installieren und aktivieren Sie ein Modul aus dem Quellcode:

```
cd /path/to/module/source
apxs2 -cia MODULE.c
```

wobei das Modul mit `-c` kompiliert, mit `-i` installiert und mit `-a` aktiviert wird. Alle weiteren Optionen von **`apxs2`** werden auf der man-Seite `apxs2(1)` beschrieben.

31.5 Aktivieren von CGI-Skripten

Die Common Gateway Interface (CGI) von Apache ermöglicht die Erstellung dynamischer Inhalte mit Programmen bzw. sogenannten CGI-Skripten. CGI-Skripten können in jeder beliebigen Programmiersprache geschrieben sein. In der Regel werden aber die Skriptsprachen Perl oder PHP verwendet.

Damit Apache in der Lage ist, die von CGI-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 31.4.2, „Aktivieren und Deaktivieren von Modulen“*.

Warnung: CGI-Sicherheit

Die Zulassung der CGI-Skriptausführung auf dem Server ist ein Sicherheitsrisiko. Weitere Informationen finden Sie in *Abschnitt 31.8, „Vermeiden von Sicherheitsproblemen“*.

31.5.1 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-Skripten konfiguriert. Wenn Sie eine virtuelle Hostkonfiguration erstellt haben (siehe *Abschnitt 31.2.2.1, „Virtuelle Hostkonfiguration“*) und Ihre CGI-Skripten in einem Host-spezifischen Verzeichnis ablegen möchten, müssen Sie das betreffende Verzeichnis entsperren und für CGI-Skripten konfigurieren.

BEISPIEL 31.5 CGI-KONFIGURATION FÜR VIRTUELLE HOSTS

```
ScriptAlias /cgi-bin/ "/srv/www/www.example.com/cgi-bin/" (1)

<Directory "/srv/www/www.example.com/cgi-bin/">
 Options +ExecCGI (2)
 AddHandler cgi-script .cgi .pl (3)
 Require all granted (4)
</Directory>
```

(1) Fordert Apache auf, alle Dateien in diesem Verzeichnis als CGI-Skripten zu behandeln

(2) Aktiviert die Ausführung von CGI-Skripten

(3) Fordert den Server auf, Dateien mit den Erweiterungen .pl und .cgi als CGI-Skripten zu behandeln. passen Sie diese Anweisung entsprechend Ihren Anforderungen an

(4) Die `Require`-(Anfordern-)Direktive bestimmt den standardmäßigen Zugriffsstatus. In diesem Fall wird der uneingeschränkte Zugriff auf das angegebenene Verzeichnis erteilt. Weitere Informationen zur Authentifizierung und Autorisierung finden Sie in http://httpd.apache.org/docs/2.4/howto/auth.html.

31.5.2 Ausführen eines Beispielskripten

Die CGI-Programmierung unterscheidet sich von der herkömmlichen Programmierung insoweit, als CGI-Programmen und -Skripten ein MIME-Typ-Header wie `Content-type: text/html` vorangestellt werden muss. Dieser Header wird an den Client gesendet, damit er weiß, welchen Inhaltstyp er empfängt. Darüber hinaus muss die Skriptausgabe vom Client, in der Regel einem Webbrowser, verstanden werden – dies ist in der Regel 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/www.example.com/cgi-bin/`), und benennen Sie es in `test.cgi` um. Bearbeiten Sie die Datei so, dass sie `#!/bin/sh` als erste Zeile enthält.

Dateien, auf die der Webserver zugreifen kann, sollten im Besitz des `root`-Benutzers sein. Weitere Informationen hierzu finden Sie im Abschnitt *Abschnitt 31.8, „Vermeiden von Sicherheitsproblemen“*. Da der Webserver unter einem anderen Benutzer ausgeführt wird, müssen CGI-Skripten von jedermann ausgeführt und gelesen werden können. Wechseln Sie daher in das CGI-Verzeichnis und führen Sie den Befehl **`chmod 755 test.cgi`** aus, um die entsprechenden Berechtigungen einzurichten.

Rufen Sie danach `http://localhost/cgi-bin/test.cgi` oder `http://example.com/cgi-bin/test.cgi` auf. Nun sollte der „CGI/1.0-Testskriptbericht“ angezeigt werden.

31.5.3 CGI-Fehlerbehebung

Wenn Sie nach der Ausführung des CGI-Testskripten statt des Testskriptberichts eine Fehlermeldung erhalten, überprüfen Sie Folgendes:

CGI-FEHLERBEHEBUNG

- *Haben Sie den Server nach der Konfigurationsänderung neu geladen?* Falls nicht, laden Sie ihn mit **`systemctl reload apache2`** neu.
- *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.

31.6 Einrichten eines sicheren Webservers mit SSL

Wenn sensible Daten wie Kreditkarteninformationen zwischen Webserver und Client übertragen werden, ist eine sichere, verschlüsselte Verbindung mit Authentifizierung wünschenswert. `mod_ssl` bietet mittels der Protokolle Secure Sockets Layer (SSL) und Transport Layer Security (TLS) eine sichere Verschlüsselung für die HTTP-Kommunikation zwischen einem Client und dem Webserver. Wenn Sie SSL/TLS verwenden, wird zwischen dem Webserver und dem Client eine private Verbindung eingerichtet. Die Datenintegrität bleibt dadurch gewährleistet und Client und Server können sich gegenseitig authentifizieren.

Zu diesem Zweck sendet der Server vor der Beantwortung von Anforderungen an eine URL ein SSL-Zertifikat mit Informationen, die die Identität des Servers nachweisen. Dies garantiert, dass der Server eindeutig der richtige Endpunkt der Kommunikation ist. Außerdem wird durch das Zertifikat eine verschlüsselte Verbindung zwischen dem Client und dem Server hergestellt, die sicherstellt, dass Informationen ohne das Risiko der Freigabe sensitiver Klartextinhalte übertragen werden.

`mod_ssl` implementiert die SSL/TLS-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://`).

31.6.1 Erstellen eines SSL-Zertifikats

Wenn Sie SSL/TLS mit dem Webserver einsetzen möchten, müssen Sie ein SSL-Zertifikat erstellen. Dieses Zertifikat ist für die Autorisierung zwischen Webserver und Client erforderlich, damit beide Endpunkte jeweils die Identität des anderen Endpunkts überprüfen können. Zum Nachweis der Zertifikatintegrität muss das Zertifikat von einer Organisation signiert sein, der jeder der beteiligten Benutzer vertraut.

Sie können drei Zertifikatsarten erstellen: ein „Dummy“-Zertifikat, das nur zu Testzwecken verwendet wird, ein selbst signiertes Zertifikat für einen bestimmten Benutzerkreis, der Ihnen vertraut, und ein Zertifikat, das von einer unabhängigen, öffentlich bekannten Zertifizierungsstelle (CA) signiert wurde.

Die Zertifikaterstellung besteht aus zwei Schritten: Zunächst wird ein privater Schlüssel für die Zertifizierungsstelle generiert und danach wird das Serverzertifikat mit diesem Schlüssel signiert.

Tipp: Weiterführende Informationen

Weitere Informationen über das Konzept von SSL/TLS und diesbezügliche Festlegungen finden Sie unter http://httpd.apache.org/docs/2.4/ssl/ssl_intro.html.

31.6.1.1 Erstellen eines „Dummy“-Zertifikats

Zum Erstellen eines Dummy-Zertifikats rufen Sie das Skript **`/usr/bin/gensslcert`** auf. Es erstellt oder überschreibt die unten aufgelisteten Dateien. Verwenden Sie die optionalen Schalter von **`gensslcert`**, um die Feineinstellungen für das Zertifikat vorzunehmen. Rufen Sie **`/usr/bin/gensslcert`** `-h` auf, um weitere Informationen zu erhalten.

- `/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: Nur zu Testzwecken

Verwenden Sie Dummy-Zertifikate niemals in Produktionsumgebungen, sondern nur zum Testen.

31.6.1.2 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 (CA) signiertes Zertifikat aus. Die Besucher einer solchen Website erhalten eine Warnung wie „Diese Website ist nicht vertrauenswürdig“, da die Webbrowser keine eigensignierten Zertifikate erkennen.

Wichtig: Eigensignierte Zertifikate

Verwenden Sie selbst signierte Zertifikate nur auf einem Webserver, auf den Benutzer zugreifen, denen Sie bekannt sind und die Ihnen als Zertifizierungsstelle vertrauen. Für einen öffentlichen Online-Versand wäre ein solches Zertifikat z. B. nicht geeignet.

Zunächst generieren Sie einen Antrag auf Ausstellung eines Zertifikats (CSR). Hierzu verwenden Sie `openssl` mit dem Zertifikatsformat `PEM`. In diesem Schritt werden Sie aufgefordert, einen Passwortsatz anzugeben und mehrere Fragen zu beantworten. Merken Sie sich diesen Passwortsatz; Sie werden ihn später benötigen.

```
sudo openssl req -new > new.cert.csr
Generating a 1024 bit RSA private key
..++++++
.........++++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:❶
Verifying - Enter PEM pass phrase:❷
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:❸
State or Province Name (full name) [Some-State]:❹
Locality Name (eg, city) []:❺
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]: 6
Organizational Unit Name (eg, section) []: 7
Common Name (for example server FQDN, or YOUR name) []: 8
Email Address []: 9

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: 10
An optional company name []: 11
```

1. Geben Sie Ihren Passwortsatz ein,
2. ... wiederholen Sie die Eingabe (und merken Sie sie sich).
3. Geben Sie Ihren zwei Buchstaben umfassenden Ländercode ein, z. B. `GB` oder `CZ`.
4. Geben Sie den Namen des Bundeslands oder Kantons ein, in dem Sie leben.
5. Geben Sie den Namen des Ortes ein, z. B. `Prag`.
6. Geben Sie den Namen der Organisation ein, für die Sie arbeiten.
7. Geben Sie Ihre Organisationseinheit ein oder lassen Sie dieses Feld leer, wenn Sie keine Organisationseinheit besitzen.
8. Geben Sie den Domänennamen des Servers bzw. Ihren Vor- und Nachnamen ein.
9. Geben Sie Ihre geschäftliche Email-Adresse ein.
10. Lassen Sie das Challenge-Passwort leer; ansonsten müssen Sie es bei jedem Neustart des Apache-Webservers eingeben.
11. Geben Sie optional den Namen des Unternehmens ein oder lassen Sie dieses Feld leer.

Nun können Sie das Zertifikat generieren. Verwenden Sie **`openssl`** erneut und nutzen Sie wieder das standardmäßige `PEM`-Format für das Zertifikat.

PROZEDUR 31.3 GENERIEREN DES ZERTIFIKATS

1. Exportieren Sie den privaten Teil des Schlüssels in `new.cert.key`. Sie werden aufgefordert, den Passwortsatz einzugeben, den Sie beim Erstellen des Zertifizierungsantrags (CSR) festgelegt haben.

   ```
   sudo openssl rsa -in privkey.pem -out new.cert.key
   ```

2. Generieren Sie den öffentlichen Teil des Zertifikats gemäß den Daten, die Sie im Ausstellungsantrag angegeben haben. Mit der Option `-days` geben Sie den Zeitraum (in Tagen) an, nach dem das Zertifikat abläuft. Sie können ein Zertifikat widerrufen oder vor Ablauf ersetzen.

```
sudo openssl x509 -in new.cert.csr -out new.cert.cert -req \
-signkey new.cert.key -days 365
```

3. Kopieren Sie die Zertifikatsdateien in die entsprechenden Verzeichnisse, so dass sie vom Apache-Server gelesen werden können. Achten Sie darauf, dass der private Schlüssel `/etc/apache2/ssl.key/server.key` nicht allgemein lesbar ist, das öffentliche PEM-Zertifikat `/etc/apache2/ssl.crt/server.crt` dagegen schon.

```
sudo cp new.cert.cert /etc/apache2/ssl.crt/server.crt
sudo cp new.cert.key /etc/apache2/ssl.key/server.key
```

Tipp: Speicherort des öffentlichen Zertifikats

Der letzte Schritt besteht darin, die öffentliche Zertifikatdatei aus dem Verzeichnis `/etc/apache2/ssl.crt/server.crt` in ein Verzeichnis zu kopieren, in dem die Benutzer auf die Datei zugreifen können. Aus diesem Verzeichnis können die Benutzer sie in ihren Webbrowsern der Liste der bekannten und vertrauenswürdigen Zertifizierungsstellen hinzufügen. Wäre die Zertifizierungsstelle nicht in dieser Liste enthalten, würde der Browser melden, dass das Zertifikat von einer unbekannten Zertifizierungsstelle ausgegeben wurde.

31.6.1.3 Anfordern eines offiziell signierten Zertifikats

Es gibt mehrere 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. Eine Liste der am häufigsten genutzten Zertifizierungsstellen finden Sie unter https://en.wikipedia.org/wiki/Certificate_authority#Providers.

Wenn Sie ein offiziell signiertes Zertifikat anfordern, senden Sie kein Zertifikat an die Zertifizierungsstelle, sondern eine CSR (Certificate Signing Request, Zertifikatsignierungsanforderung). Geben Sie zum Erstellen einer CSR den folgenden Befehl ein:

```
openssl req -new -newkey rsa:2048 -nodes -keyout newkey.pem -out newreq.pem
```

Sie werden aufgefordert, einen Distinguished Name (DN) einzugeben. 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`.

31.6.2 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 *Buch „Security Guide”, Kapitel 15 „Masquerading and Firewalls”, Abschnitt 15.4.1 „Configuring the Firewall with YaST”*).

Der SSL-Modus wird standardmäßig in der globalen Serverkonfiguration aktiviert. Falls er auf Ihrem Host deaktiviert wurde, aktivieren Sie ihn mithilfe des folgenden Kommandos: **`a2enmod ssl`**. Um SSL schließlich aktivieren zu können, muss der Server mit dem Flag „SSL“ gestartet werden. Rufen Sie dazu **`a2enflag SSL`** auf (Groß- und Kleinschreibung beachten!). Wenn Sie sich zuvor entschieden haben, Ihr Serverzertifikat durch ein Passwort zu verschlüsseln, sollten Sie auch den Wert von `APACHE_TIMEOUT` in `/etc/sysconfig/apache2` 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 *Abschnitt 31.2.2.1, „Virtuelle Hostkonfiguration“*.

Kopieren Sie zum Starten die Vorlage zu `/etc/apache2/vhosts.d/MYSSL-HOST.conf` und bearbeiten Sie diese. Es sollte ausreichen, die Werte für die folgenden Anweisungen anzupassen:

- `DocumentRoot`
- `ServerName`
- `ServerAdmin`
- `ErrorLog`
- `TransferLog`

31.6.2.1 Namensbasierte virtuelle Hosts und SSL

Auf einem Server mit nur einer IP-Adresse können standardmäßig nicht mehrere SSL-aktivierte virtuelle Hosts laufen. Für ein namensbasiertes virtuelles Hosting muss Apache wissen, welcher Servername angefordert wurde. Das Problem ist dabei, dass SSL-Verbindungen erst gelesen werden können, nachdem die Verbindung (unter Verwendung des standardmäßigen virtuellen Hosts) bereits hergestellt wurde. Demzufolge erhalten Benutzer eine Warnmeldung, die besagt, dass das Zertifikat nicht mit dem Servernamen übereinstimmt.

SUSE Linux Enterprise Server bietet eine Erweiterung des SSL-Protokolls namens Server Name Indication (SNI), die dieses Problem behebt, indem der Name der virtuellen Domäne als Teil der SSL-Verhandlung gesendet wird. Dies ermöglicht dem Server ein frühes „Umschalten“ zur korrekten virtuellen Domäne, wodurch der Browser das richtige Zertifikat erhält.

SNI ist in SUSE Linux Enterprise Server standardmäßig aktiviert. Für die Aktivierung von namensbasierten virtuellen Hosts für SSL müssen Sie den Server wie in *Abschnitt 31.2.2.1.1, „Namensbasierte virtuelle Hosts“* beschrieben konfigurieren. (Beachten Sie, dass für SSL Port `443` anstelle von Port `80` benötigt wird.)

Wichtig: SNI - Browserunterstützung

SNI muss auf der Client-Seite unterstützt werden. SNI wird allerdings von den meisten Browsern unterstützt, ausgenommen von bestimmten älteren Browsern. Weitere Informationen finden Sie unter https://en.wikipedia.org/wiki/Server_Name_Indication#Support.

Mit der Direktive `SSLStrictSNIVHostCheck` konfigurieren Sie die Handhabung von Browsern ohne SNI-Fähigkeit. Wenn SNI in der Serverkonfiguration auf `on` gesetzt ist, werden Browser ohne SNI-Fähigkeit für alle virtuellen Hosts abgelehnt. Wenn für SNI `on` in einer `VirtualHost`-Direktive festgelegt ist, wird der Zugriff auf den konkreten virtuellen Host abgelehnt.

Wenn in der Serverkonfiguration `off` festgelegt ist, verhält sich der Server wie ohne SNI-Unterstützung. SSL-Anforderungen werden durch den *ersten* (für Port 443) definierten virtuellen Host bearbeitet.

31.7 Ausführen mehrerer Apache-Instanzen auf demselben Server

Ab SUSE® Linux Enterprise Server 12 SP1 können Sie mehrere Apache-Instanzen auf einem einzigen Server ausführen. So erhalten Sie mehrere Vorteile im Vergleich zum Ausführen mehrerer virtueller Hosts (siehe *Abschnitt 31.2.2.1, „Virtuelle Hostkonfiguration“*):

- Wenn ein virtueller Host zeitweise deaktiviert werden muss, müssen Sie die Webserver-Konfiguration ändern und den Webserver neu starten, damit die Änderung in Kraft tritt.
- Wenn Probleme bei einem einzigen virtuellen Host auftreten, müssen alle virtuellen Hosts neu gestartet werden.

Sie können die standardmäßige Apache-Instanz wie gewohnt ausführen:

```
sytemctl start apache2
```

Hiermit wird die standardmäßige Datei `/etc/sysconfig/apache2` gelesen. Falls die Variable `APACHE_HTTPD_CONF` in der Datei nicht festgelegt wurde oder die Datei ganz fehlt, wird stattdessen die Datei `/etc/apache2/httpd.conf` gelesen.

Zum Aktivieren einer anderen Apache-Instanz führen Sie Folgendes aus:

```
systemctl start apache2@INSTANCE_NAME
```

Beispiel:

```
systemctl start apache2@example_web.org
```

Standardmäßig verwendet die Instanz `/etc/apache2@example_web.org/httpd.conf` als Hauptkonfigurationsdatei. Diese kann durch Festlegen von `APACHE_HTTPD_CONF` in `/etc/sysconfig/apache2@example_web.org` überschrieben werden.

Das nachfolgende Beispiel zeigt, wie Sie eine weitere Instanz von Apache einrichten. Alle Befehle müssen dabei als `root` ausgeführt werden.

PROZEDUR 31.4 KONFIGURIEREN EINER WEITEREN APACHE-INSTANZ

1. Erstellen Sie eine neue Konfiguration auf der Grundlage von `/etc/sysconfig/apache2`, beispielsweise `/etc/sysconfig/apache2@example_web.org`:

   ```
   cp /etc/sysconfig/apache2 /etc/sysconfig/apache2@example_web.org
   ```

2. Bearbeiten Sie die Datei `/etc/sysconfig/apache2@example_web.org` und ändern Sie die Zeile mit

   ```
   APACHE_HTTPD_CONF
   ```

   mit dem YaST-sysconfig-Editor auf

   ```
   APACHE_HTTPD_CONF="/etc/apache2/httpd@example_web.org.conf"
   ```

3. Erstellen Sie die Datei `/etc/apache2/httpd@example_web.org.conf` auf der Grundlage von `/etc/apache2/httpd.conf`.

   ```
   cp /etc/apache2/httpd.conf /etc/apache2/httpd@example_web.org.conf
   ```

4. Bearbeiten Sie die Datei `/etc/apache2/httpd@example_web.org.conf` und ändern Sie

   ```
   Include /etc/apache2/listen.conf
   ```

   mit dem YaST-sysconfig-Editor auf

   ```
   Include /etc/apache2/listen@example_web.org.conf
   ```

   Prüfen Sie alle Direktiven und passen Sie sie an Ihre Anforderungen an. Ändern Sie bei Bedarf

   ```
   Include /etc/apache2/global.conf
   ```

   und erstellen Sie für jede Instanz eine neue Datei `global@example_web.org.conf`. Es wird empfohlen,

```
ErrorLog /var/log/apache2/error_log
```

mit dem YaST-sysconfig-Editor auf

```
ErrorLog /var/log/apache2/error@example_web.org_log
```

zu ändern, sodass separate Protokolle für die einzelnen Instanzen geführt werden.

5. Erstellen Sie die Datei `/etc/apache2/listen@example_web.org.conf` auf der Grundlage von `/etc/apache2/listen.conf`.

```
cp /etc/apache2/listen.conf /etc/apache2/listen@example_web.org.conf
```

6. Bearbeiten Sie die Datei `/etc/apache2/listen@example_web.org.conf` und ändern Sie

```
Listen 80
```

in die Portnummer, an der die neue Instanz ausgeführt werden soll, beispielsweise 82:

```
Listen 82
```

Wenn die neue Apache-Instanz über ein sicheres Protokoll ausgeführt werden soll (siehe *Abschnitt 31.6, „Einrichten eines sicheren Webservers mit SSL“*), ändern Sie außerdem die Zeile

```
Listen 443
```

beispielsweise in

```
Listen 445
```

7. Starten Sie die neue Apache-Instanz:

```
systemctl start apache2@example_web.org
```

8. Prüfen Sie, ob der Server ausgeführt wird. Geben Sie hierzu `http://Servername:82` in den Webbrowser ein. Falls Sie den Namen der Fehlerprotokolldatei für die neue Instanz geändert hatten, können Sie ihn prüfen:

```
tail -f /var/log/apache2/error@example_web.org_log
```

Beim Einrichten mehrerer Apache-Instanzen auf demselben Server sind mehrere Punkte zu beachten:

- Die Datei `/etc/sysconfig/apache2@INSTANZNAME` kann dieselben Variablen wie `/etc/sysconfig/apache2` enthalten, also auch Einstellungen für das Laden von Modulen und MPM-Einstellungen.
- Die standardmäßige Apache-Instanz muss nicht ausgeführt werden, wenn andere Instanzen laufen.
- Die Apache-Helper-Dienstprogramme **`a2enmod`**, **`a2dismod`** und **`apachectl`** werden für die standardmäßige Apache-Instanz ausgeführt, sofern in der Umgebungsvariable `HTTPD_INSTANCE` nicht anderweitig festgelegt. Im folgenden Beispiel

  ```
  export HTTPD_INSTANCE=example_web.org
  a2enmod access_compat
  a2enmod status
  apachectl start
  ```

  werden die Module `access_compat` und `status` in die Variable `APACHE_MODULES` in der Datei `/etc/sysconfig/apache2@example_web.org` eingefügt; anschließend wird die Instanz `example_web.org` gestartet.

31.8 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.

31.8.1 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, sobald es möglich ist, ausgeführt werden sollten. Die Sicherheitsankündigungen von SUSE stehen unter folgenden Adressen zur Verfügung:

- **Webseite.** http://www.suse.com/support/security/
- **Mailinglisten-Archiv.** http://lists.opensuse.org/opensuse-security-announce/
- **Liste der Informationen zur Sicherheit.** http://www.suse.com/support/update/

31.8.2 DocumentRoot-Berechtigungen

In SUSE Linux Enterprise Server sind das `DocumentRoot`-Verzeichnis `/srv/www/htdocs` und das CGI-Verzeichnis `/srv/www/cgi-bin` standardmäßig dem Benutzer bzw. der Gruppe `root` zugeordnet. Diese Berechtigungen sollten nicht geändert werden. Wenn diese Verzeichnisse für alle Benutzer modifizierbar sind, kann 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.

31.8.3 Zugriff auf das Dateisystem

Standardmäßig wird in `/etc/apache2/httpd.conf` der Zugriff auf das gesamte Dateisystem verweigert. Diese Direktiven sollten Sie nicht überschreiben. Aktivieren Sie stattdessen explizit den Zugriff auf die Verzeichnisse, die Apache lesen muss. Weitere Informationen finden Sie in *Abschnitt 31.2.2.1.3, „Basiskonfiguration eines virtuellen Hosts“*. Achten Sie dabei darauf, dass keine unbefugten Personen auf kritische Dateien wie Passwort- oder Systemkonfigurationsdateien zugreifen können.

31.8.4 CGI-Skripten

Interaktive Skripten in Perl, PHP, SSI oder anderen Programmiersprachen können im Prinzip jeden beliebigen Befehl ausführen und stellen damit generell ein Sicherheitsrisiko dar. 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 Skripten zu überprüfen.

Es ist durchaus üblich, sich die Skriptverwaltung durch eine Einschränkung der Skriptausführung zu vereinfachen. Dabei wird die Ausführung von CGI-Skripten auf bestimmte Verzeichnisse eingeschränkt, statt sie global zuzulassen. Die Direktiven `ScriptAlias` und `Option ExecCGI` werden zur Konfiguration verwendet. In der Standardkonfiguration von SUSE Linux Enterprise Server ist es generell nicht gestattet, CGI-Skripts von jedem beliebigen Ort aus auszuführen.

Alle CGI-Skripten werden unter dem gleichen Benutzer ausgeführt. Es kann daher zu Konflikten zwischen verschiedenen Skripten kommen. Abhilfe schafft hier das Modul suEXEC, das die Ausführung von CGI-Skripten unter einem anderen Benutzer oder einer anderen Gruppe ermöglicht.

31.8.5 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. Benutzern ist es allerdings nicht erlaubt, `Option`-Direktiven mit `mod_userdir` zu überschreiben (siehe hierzu die Konfigurationsdatei `/etc/apache2/mod_userdir.conf`).

31.9 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:

Ausgabe des Subkommandos `apache2.service`:

Statt den Webserver mit der Binärdatei `/usr/sbin/apache2ctl` zu starten und zu stoppen, verwenden Sie das Kommando **`systemctl`** (siehe *Abschnitt 31.3, „Starten und Beenden von Apache“*). **`systemctl status apache2`** bietet umfassende Informationen über Fehler und stellt außerdem Tipps und Hinweise zur Behebung von Konfigurationsfehlern zur Verfügung.

Protokolldateien und Ausführlichkeitsgrad

Bei schwerwiegenden und nicht schwerwiegenden Fehlern finden Sie mögliche Ursachen in den Apache-Protokolldateien, insbesondere in der standardmäßig im Verzeichnis `/var/log/apache2/error_log` gespeicherten Fehlerprotokolldatei. Mit der Direktive `LogLevel` können Sie im Übrigen die Ausführlichkeit der protokollierten Meldungen einstellen. Dies ist z. B. nützlich, wenn Sie mehr Details benötigen.

Tipp: Ein einfacher Test

Sie können die Apache-Protokollmeldungen mit dem Befehl **`tail -F /var/log/apache2/`***`MY_ERROR_LOG`* überwachen. Führen Sie dann **`systemctl restart apache2`** aus. Versuchen Sie anschließend eine Verbindung mit einem Browser herzustellen und überprüfen Sie dort die Ausgabe.

Firewall und Ports

Es wird häufig versäumt, 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 31.2.3, „Konfigurieren von Apache mit YaST“*). Bei der manuellen Konfiguration von Apache können Sie die Ports für HTTP und HTTPS in der Firewall über das Firewall-Modul von YaST öffnen.

Falls sich Ihr Problem nicht mithilfe der vorgenannten Ressourcen beheben lässt, finden Sie weitere Informationen in der Apache-Fehlerdatenbank, die online unter http://httpd.apache.org/bug_report.html zur Verfügung steht. Sie können sich auch an die Apache-Benutzer-Community wenden, die Sie über eine Mailingliste unter http://httpd.apache.org/userslist.html erreichen.

31.10 Weiterführende Informationen

Das Paket `apache2-doc`, das an verschiedenen Orten bereitgestellt wird, enthält das vollständige Apache-Handbuch für die lokale Installation und Referenz. Das Handbuch ist nicht in der Standardinstallation enthalten. Am schnellsten installieren Sie es mit dem Befehl **`zypper in apache2-doc`**. Nach der Installation steht das Apache-Handbuch unter http://localhost/manual/ zur Verfügung. Unter http://httpd.apache.org/docs-2.4/ können Sie auch im Web darauf zugreifen. SUSE-spezifische Konfigurationstipps finden Sie im Verzeichnis `/usr/share/doc/packages/apache2/README.*`.

31.10.1 Apache 2.4

Eine Liste der neuen Funktionen in Apache 2.4 finden Sie unter http://httpd.apache.org/docs/2.4/new_features_2_4.html. Upgrade-Informationen von Version 2.2 auf Version 2.4 erhalten Sie unter http://httpd.apache.org/docs-2.4/upgrading.html.

31.10.2 Apache Module

Weitere Informationen zu externen Apache-Modulen, die kurz im Abschnitt *Abschnitt 31.4.5, „Externe Module“* beschrieben werden, finden Sie an folgenden Orten:

`mod_apparmor`
: http://en.opensuse.org/SDB:AppArmor

`mod_auth_kerb`
: http://modauthkerb.sourceforge.net/

`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_security`

http://modsecurity.org/

31.10.3 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/2.4/developer/

31.10.4 Verschiedene Informationsquellen

Wenn Sie in SUSE Linux Enterprise Server Probleme mit Apache haben, werfen Sie einen Blick in die technische Informationssuche unter http://www.suse.com/support. 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.

32 Einrichten eines FTP-Servers mit YaST

Mithilfe des YaST-*FTP-Server*-Moduls können Sie Ihren Rechner für die Funktion als FTP (File Transfer Protocol)-Server konfigurieren. Anonyme bzw. authentifizierte Benutzer können mithilfe des FTP-Protokolls eine Verbindung zu Ihrem Rechner herstellen und Dateien herunterladen. Abhängig von der Konfiguration können sie auch Dateien auf den FTP-Server hochladen. YaST nutzt vsftpd (Very Secure FTP Daemon).

Wenn das YaST-FTP Server-Modul in Ihrem System nicht verfügbar ist, installieren Sie das Paket `yast2-ftp-server`.

Führen Sie zum Konfigurieren des FTP-Servers mit YaST die folgenden Schritte aus:

1. Öffnen Sie das YaST-Kontrollzentrum, und wählen Sie *Netzwerkdienste* › *FTP-Server*, oder führen Sie das Kommando **`yast2 ftp-server`** als `root` aus.

2. Wenn auf Ihrem System kein FTP-Server installiert ist, werden Sie gefragt, welcher Server installiert werden soll, wenn das YaST-FTP-Server-Modul gestartet wird. Wählen Sie einen Server aus, und bestätigen Sie den Dialog.

3. Konfigurieren Sie im Dialogfeld *Start* die Optionen für den Startvorgang des FTP-Servers. Weitere Informationen finden Sie unter *Abschnitt 32.1, „Starten des FTP-Servers“*.
   Konfigurieren Sie im Dialogfeld *Allgemein* die FTP-Verzeichnisse, eine Begrüßung, die Masken zum Erstellen von Dateien sowie andere Parameter. Weitere Informationen finden Sie unter *Abschnitt 32.2, „Allgemeine FTP-Einstellungen“*.
   Legen Sie im Dialogfeld *Leistung* die Parameter fest, die sich auf das Laden des FTP-Servers auswirken. Weitere Informationen finden Sie unter *Abschnitt 32.3, „FTP-Leistungseinstellungen“*.
   Legen Sie im Dialogfeld *Authentifizierung* fest, ob der FTP-Server für anonyme und/oder authentifizierte Benutzer verfügbar sein soll. Weitere Informationen finden Sie unter *Abschnitt 32.4, „Authentifizierung “*.
   Konfigurieren Sie im Dialogfeld *Einstellungen für Experten*den Betriebsmodus des FTP-Servers, der SSL-Verbindungen sowie die Firewall-Einstellungen. Weitere Informationen finden Sie unter *Abschnitt 32.5, „Einstellungen für Experten“*.

4. Klicken Sie auf *Beenden*, um die Konfigurationen zu speichern.

32.1 Starten des FTP-Servers

Legen Sie im Bereich *Dienststart* des Dialogfelds *FTP-Start* die Art und Weise fest, in der der FTP-Server gestartet wird. Sie können den Server entweder automatisch während des Systemstarts oder manuell starten. Wenn der FTP-Server erst bei einer FTP-Verbindungsanfrage gestartet werden soll, wählen Sie *Via xinetd* aus.

Der aktuelle Status des FTP-Servers wird im Bereich *An- und ausschalten* im Dialogfeld *FTP-Start* angezeigt. Starten Sie den FTP-Server, indem Sie auf *FTP-Server jetzt starten* klicken. Um den Server zu stoppen, klicken Sie auf *Stoppen FTP*. Nachdem Sie die Servereinstellungen geändert haben, klicken Sie auf *Einstellungen speichern und FTP jetzt neu starten*. Ihre Konfigurationen werden gespeichert, wenn Sie das Konfigurationsmodul mit *Beenden* verlassen.

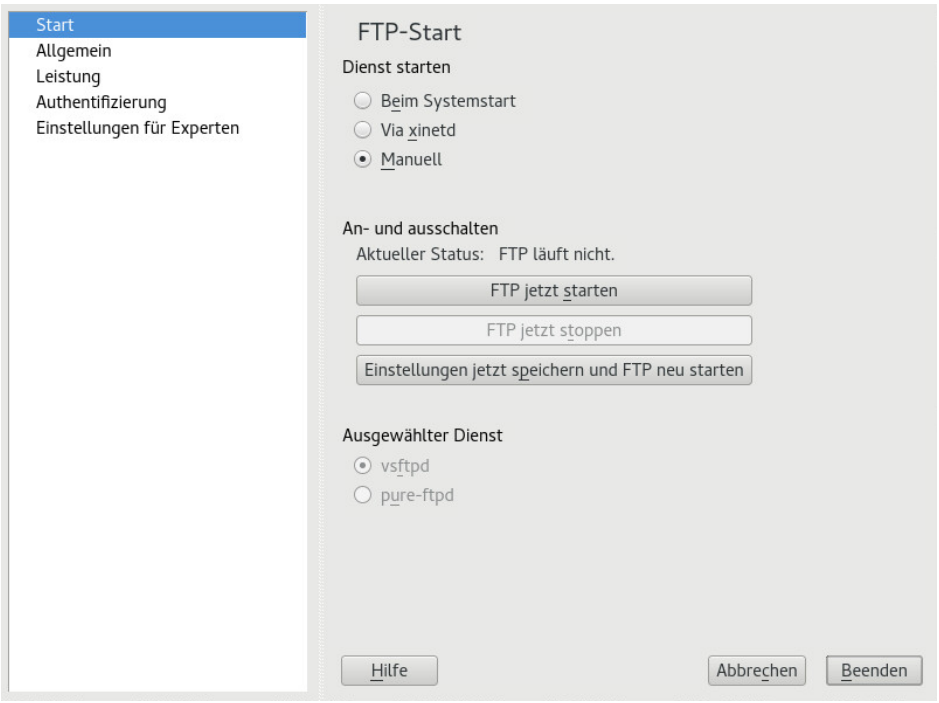


ABBILDUNG 32.1 FTP-SERVERKONFIGURATION - START

32.2 Allgemeine FTP-Einstellungen

Im Bereich *Allgemeine Einstellungen* des Dialogfelds *Allgemeine FTP-Einstellungen* können Sie die *Willkommensnachricht* festlegen, die nach der Verbindungsherstellung zum FTP-Server angezeigt wird.

Wenn Sie die Option *Chroot Everyone* (Alle platzieren) aktivieren, werden alle lokalen Benutzer nach der Anmeldung in einem Chroot Jail in ihrem Home-Verzeichnis platziert Diese Option hat Auswirkungen auf die Sicherheit, besonders wenn die Benutzer über Uploadberechtigungen oder Shellzugriff verfügen, daher sollten Sie beim Aktivieren dieser Option mit Bedacht vorgehen.

Wenn Sie die Option *Ausführliche Protokollierung* aktivieren, werden alle FTP-Anfragen und -Antworten protokolliert.

Sie können die Berechtigungen für Dateien, die von anonymen und/oder authentifizierten Benutzern erstellt wurden, mit umask einschränken. Legen Sie die Dateierstellungsmaske für anonyme Benutzer in *Umask für anonyme Benutzer* fest und die Dateierstellungsmaske für authentifizierte Benutzer in *Umask für authentifizierte Benutzer*. Die Masken sollten als Oktalzahlen mit führender Null eingegeben werden. Weitere Informationen zu umask finden Sie auf der man-Seite für umask (`man 1p umask`).

Legen Sie im Bereich *FTP-Verzeichnisse* die für anonyme und autorisierte Benutzer verwendeten Verzeichnisse fest. Wenn Sie auf *Durchsuchen* klicken, können Sie ein zu verwendendes Verzeichnis aus dem lokalen Dateisystem wählen. Das standardmäßige FTP-Verzeichnis für anonyme Benutzer ist `/srv/ftp`. Beachten Sie, dass vsftpd keine Verzeichnisschreibrechte für alle Benutzer erteilt. Stattdessen wird das Unterverzeichnis `upload` mit Schreibberechtigungen für anonyme Benutzer erstellt.

32.3 FTP-Leistungseinstellungen

Legen Sie im Dialogfeld *Leistung* die Parameter fest, die sich auf das Laden des FTP-Servers auswirken. *Max. Lerrlaufzeit* entspricht der Maximalzeit (in Minuten), die der Remote-Client zwischen FTP-Kommandos pausieren darf. Bei einer längeren Inaktivität wird die Verbindung zum Remote-Client getrennt. *Max. Clients für eine IP* bestimmt die maximale Clientanzahl, die von einer einzelnen IP-Adresse aus verbunden sein können. *Max. Clients* bestimmt die maximale Clientanzahl, die verbunden sein können. Alle zusätzlichen Clients erhalten eine Fehlermeldung.

Die maximale Datenübertragungsrate (in KB/s) wird in *Lovale Max Rate* (Lokale max. Rate) für lokale authentifizierte Benutzer und in *Anonymous Max Rate* (Anonyme max. Rate) für anonyme Benutzer festgelegt. Der Standardwert für diese Einstellung ist `0`, was für eine unbegrenzte Datenübertragungsrate steht.

32.4 Authentifizierung

Im Bereich *Anonyme und lokale Benutzer aktivieren/deaktivieren* des Dialogfelds *Authentifizierung* können Sie festlegen, welche Benutzer auf Ihren FTP-Server zugreifen dürfen. Folgende Optionen stehen zur Verfügung: nur anonymen Benutzern, nur authentifizierten Benutzern oder beiden Benutzergruppen Zugriff erteilen.

Sollen die Benutzer in der Lage sein, Dateien auf den FTP-Server hochzuladen, aktivieren Sie die Option *Hochladen aktivieren* im Bereich *Hochladen* des Dialogfelds *Authentifizierung*. Hier können Sie das Hochladen und das Erstellen von Verzeichnissen sogar für anonyme Benutzer zulassen, indem Sie das entsprechende Kontrollkästchen aktivieren.

Anmerkung: vsftp – Heraufladen von Dateien für anonyme Benutzer zulassen

Wenn ein vsftpd-Server verwendet wird und anonyme Benutzer Dateien hochladen oder Verzeichnisse erstellen dürfen, muss ein Unterverzeichnis mit Schreibberechtigung für alle Benutzer im anonymen FTP-Verzeichnis erstellt werden.

32.5 Einstellungen für Experten

Ein FTP-Server kann im aktiven oder passiven Modus ausgeführt werden. Standardmäßig wird der Server im passiven Modus ausgeführt. Um in den aktiven Modus zu wechseln, deaktivieren Sie die Option *Passiven Modus aktivieren* im Dialogfeld *Einstellungen für Experten*. Sie können außerdem den Portbereich ändern, der auf dem Server für den Datenstrom verwendet wird, indem Sie die Optionen *Min Port für Pas.- Modus* und *Max Port für Pas.-Modus* bearbeiten.

Wenn die Kommunikation zwischen den Clients und dem Server verschlüsselt sein soll, können Sie *SSL aktivieren*. Wählen Sie dazu die Protokollversionen aus, die unterstützt werden sollen, und geben Sie das DSA-Zertifikat an, das für SSL-verschlüsselte Verbindungen verwendet werden soll.

Wenn Ihr System von einer Firewall geschützt wird, aktivieren Sie *Port in Firewall öffnen*, um eine Verbindung zum FTP-Server zu ermöglichen.

32.6 Weiterführende Informationen

Weitere Informationen zum FTP-Server finden Sie auf den man-Seiten zu **vsftpd** und **vsftpd.conf**.

33 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 Objektanforderungen 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. Ein Vorteil 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:

- Verteilung der Last auf mehrere miteinander kommunizierende Hierarchien von Proxyservern
- Definition strenger Zugriffssteuerungslisten für alle Clients, die auf den Proxy zugreifen
- Zulassen oder Verweigern des Zugriffs auf bestimmte Webseiten mithilfe anderer Anwendungen
- 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 das News-Protokoll oder Video-Konferenzen-Protokolle. Da Squid nur das UDP-Protokoll für die Bereitstellung von Kommunikation zwischen verschiedenen Caches unterstützt, werden zahlreiche Multimedia-Programme nicht unterstützt.

33.1 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.

33.1.1 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 die Firewall-Konfiguration eine DMZ enthält, sollte der Proxy in dieser Zone betrieben werden. Unter *Abschnitt 33.6, „Konfigurieren eines transparenten Proxy“* wird beschrieben, wie Sie einen *transparenten* Proxy implementieren. Dadurch wird die Konfiguration der Clients erleichtert, da sie in diesem Fall keine Informationen zum Proxy benötigen.

33.1.2 Mehrere Caches

Mehrere Instanzen von Squid können für den Austausch von Objekten konfiguriert werden. Dadurch verringert sich die Gesamtlast im System und die Wahrscheinlichkeit erhöht sich, ein Objekt aus dem lokalen Netzwerk abrufen zu können. 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 anfordern kann.

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 Subnetz 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 Anfordern der Objekte zu finden, sendet ein Cache eine ICP-Anforderung an alle gleichgeordneten Proxys. Die gleichgeordneten Proxys beantworten diese Anforderungen über ICP-Antworten. Wenn das Objekt erkannt wurde, verwenden sie einen `HIT`-Code, wenn nicht, einen `MISS`-Code.

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.

Anmerkung: Wie vermeidet Squid die Verdoppelung von Objekten?

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.

33.1.3 Caching von Internetobjekten

Viele im Netzwerk verfügbaren Objekte sind nicht statisch, wie beispielsweise dynamisch generierte Seiten und TLS/SSL-verschlüsselte Inhalte. Derartige Objekte werden nicht im Cache gespeichert, da sie sich bei jedem Zugriff ändern.

Um zu bestimmen, wie lange Objekte im Cache gespeichert werden sollen, wird Objekten einer von mehreren Status 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, können ebenfalls verwendet werden.

Objekte im Cache werden in der Regel aufgrund mangelnden Speicherplatzes ersetzt. Dazu werden Algorithmen wie LRU (last recently used) verwendet. Dies bedeutet, dass der Proxy die Objekte löscht, die am längsten nicht mehr angefordert wurden.

33.2 Systemanforderungen

Die Systemanforderungen hängen weitgehend von der maximalen Netzwerkauslastung ab, die das System tragen muss. Prüfen Sie daher die Belastungsspitzen, da diese mehr als das Vierfache des Tagesdurchschnitts betragen können. Im Zweifelsfall ist es vorzuziehen, die Systemanforderungen zu hoch einzuschätzen. Wenn Squid an der Grenze seiner Leistungsfähigkeit arbeitet, kann es zu erheblichen Einbußen in der Qualität des Diensts führen. Die folgenden Abschnitte widmen sich den einzelnen Systemfaktoren in der Reihenfolge ihrer Wichtigkeit:

1. RAM-Größe
2. CPU-Geschwindigkeit/physische CPU-Cores
3. Größe des Festplatten-Cache
4. Festplatten/SSDs und ihre Architektur

33.2.1 RAM

Der von Squid benötigte Arbeitsspeicher (RAM) steht in direktem Verhältnis zur Anzahl der Objekte im Cache. RAM ist wesentlich schneller als eine Festplatte/SSD. Daher ist es sehr wichtig, dass genügend Arbeitsspeicher für den Squid-Vorgang zur Verfügung steht, da die Systemleistung erheblich eingeschränkt ist, wenn die Swap-Festplatte verwendet wird.

Außerdem speichert Squid Cache-Objekt-Bezüge und häufig angeforderte Objekte im Hauptspeicher, um das Abrufen dieser Daten zu beschleunigen. Außerdem gibt es andere Daten, die Squid im Arbeitsspeicher benötigt, beispielsweise eine Tabelle mit allen IP-Adressen, einen exakten Domänennamen-Cache, die am häufigsten angeforderten Objekte, Zugriffssteuerungslisten, Puffer usw.

33.2.2 Prozessor

Squid ist so eingestellt, dass es am besten mit niedrigeren Prozessor-Core-Zahlen arbeitet (4–8 physische Cores), wobei jeder höchste Leistung bietet. Technologien, die virtuelle Cores bereitstellen, wie Hyperthreading, können sich negativ auf die Leistung auswirken.

Um mehrere CPU-Cores am besten zu nutzen, ist es notwendig, mehrere Worker-Threads einzurichten, die in verschiedene Caching-Geräte schreiben. Standardmäßig ist die Unterstützung mehrerer Cores deaktiviert.

33.2.3 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 mehr als 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 128 KB/s. Wenn dieser Datenverkehr vollständig im Cache gespeichert wird, ergeben sich in einer Stunde 460 MB. Bei der Annahme, dass dieser Datenverkehr in nur 8 Arbeitsstunden generiert wird, würden 3,6 GB an einem einzigen Tag erreicht werden. Da in der Regel 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.

33.2.4 Festplatten-/SSD-Architektur

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) oder *random read performance* (Zufallsleseleistung) beschrieben – gemessen in Millisekunden. Da die Datenblöcke, die Squid von der Festplatte/SSD liest oder auf die Festplatte/SSD schreibt, tendenziell eher klein sind, ist die Zugriffszeit/Leseleistung der Festplatte/SSD entscheidender als ihr Datendurchsatz.

Für die Verwendung als Proxy sind Festplatten mit hoher Rotationsgeschwindigkeit oder SSDs die beste Wahl. Bei der Verwendung von Festplatten kann es besser sein, mehrere kleinere Festplatten zu verwenden. Dabei sollte jede ein einzelnes Cache-Verzeichnis aufweisen, um übermäßige Lesezeiten zu vermeiden.

Die Verwendung von RAID-Systemen bietet eine erhöhte Zuverlässigkeit, bedeutet jedoch Einschränkungen bei der Geschwindigkeit. Vermeiden Sie jedoch aus Leistungsgründen (Software-)RAID5 und ähnliche Einstellungen.

Die Wahl des Dateisystems ist in der Regel nicht entscheidend. Jedoch kann mit der Einhängeoption `noatime` die Leistung verbessert werden. Squid stellt eigene Zeitstempel bereit und erfordert daher nicht, dass das Dateisystem die Zugriffszeiten überwacht.

33.3 Grundlegende Verwendung von Squid

Installieren Sie das Paket, falls es nicht bereits installiert ist `squid` . `squid` gehört nicht zu den Paketen, die standardmäßig auf SUSE Linux Enterprise Server installiert werden.

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 Namenserver 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 Nameserver angegeben werden, da Squid nicht startet, wenn kein DNS-Server in `/etc/resolv.conf` gefunden wird.

33.3.1 Starten von Squid

Verwenden Sie zum Starten von Squid Folgendes:

```
tux > sudo systemctl start squid
```

Wenn Sie möchten, dass Squid zusammen mit dem System gestartet wird, aktivieren Sie den Dienst mit **`systemctl enable squid`**.

33.3.2 Überprüfen, ob Squid ausgeführt wird

Wählen Sie zum Überprüfen, ob Squid ausgeführt wird, eine der folgenden Optionen:

- Mithilfe von **`systemctl`**:

  ```
  tux > systemctl status squid
  ```

  Die Ausgabe dieses Kommandos sollte Folgendes für Squid anzeigen: `loaded` (geladen) und `active (running)` (aktiv (wird ausgeführt)).

- Mithilfe von Squid:

  ```
  tux > sudo squid -k check | echo $?
  ```

  Die Ausgabe dieses Befehls sollte `0` lauten, kann jedoch zusätzliche Warnungen oder Meldungen umfassen.

Um die Funktionsfähigkeit von Squid im lokalen System zu testen, wählen Sie eine der folgenden Optionen:

- Zum Testen können Sie **`squidclient`** verwenden, ein Kommandozeilenwerkzeug, das die Antwort auf eine Webanforderung ausgeben kann, ähnlich wie **`wget`** oder **`curl`**.
  Anders als diese Werkzeuge verbindet **`squidclient`** sich automatisch mit dem Standard-Proxy-Setup von Squid, `localhost:3128`. Wenn Sie jedoch die Konfiguration von Squid geändert haben, müssen Sie **`squidclient`** mithilfe von Kommandozeilenoptionen so konfigurieren, dass es andere Einstellungen verwendet. Weitere Informationen erhalten Sie mit **`squidclient --help`**.

BEISPIEL 33.1 EINE ANFORDERUNG MIT `squidclient`

```
tux > squidclient http://www.example.org
HTTP/1.1 200 OK
Cache-Control: max-age=604800
Content-Type: text/html
Date: Fri, 22 Jun 2016 12:00:00 GMT
Expires: Fri, 29 Jun 2016 12:00:00 GMT
Last-Modified: Fri, 09 Aug 2013 23:54:35 GMT
Server: ECS (iad/182A)
Vary: Accept-Encoding
X-Cache: HIT
x-ec-custom-error: 1
Content-Length: 1270
X-Cache: MISS from moon (1)
X-Cache-Lookup: MISS from moon:3128
Via: 1.1 moon (squid/3.5.16) (2)
Connection: close

<!doctype html>
<html>
<head>
    <title>Example Domain</title>
[...]
</body>
</html>
```

Die in *Beispiel 33.1, „Eine Anforderung mit* **`squidclient`**“ angezeigte Ausgabe kann in zwei Teile aufgeteilt werden:

1. Die Protokoll-Header der Antwort: die Zeilen vor der leeren Zeile.
2. Der eigentliche Inhalt der Antwort: die Zeilen nach der leeren Zeile.

Um zu überprüfen, ob Squid verwendet wird, sehen Sie sich im Header die ausgewählten Zeilen an:

1. Der Wert `X-Cache` im Header gibt an, dass das angeforderte Dokument nicht im Squid-Cache (`MISS`) des Computers `moon` gespeichert war.
   Das Beispiel oben enthält zwei `X-Cache`-Zeilen. Sie können den ersten `X-Cache`-Header ignorieren. Er wird von der internen Caching-Software erstellt, die vom Webserver stammt.
2. Der Wert `Via` im Header gibt die HTTP-Version, den Namen des Computers und die verwendete Squid-Version an.

- Mithilfe eines Browsers: Richten Sie `localhost` als Proxy und `3128` als Port ein. Sie können dann eine Seite laden und die Antwort-Header in der Kontrollleiste *Netzwerk* des *Inspektors* oder der *Entwicklertools* des Browsers überprüfen. Die Header sollten ähnlich wie in *Beispiel 33.1, „Eine Anforderung mit* **`squidclient`**“ reproduziert werden.

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. Legen Sie daher ACLs (Access Control Lists = Zugriffssteuerungslisten) fest, die den Zugriff auf den Proxy steuern. Nach Bearbeiten der Konfigurationsdatei muss Squid neu geladen oder neu gestartet werden. Weitere Informationen zu ACLs finden Sie in *Abschnitt 33.5.2, „Optionen für die Zugriffssteuerung“*.

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`.

33.3.3 Stoppen, Neuladen und Neustarten von Squid

Zum Neuladen von Squid stehen die folgenden Verfahren zur Auswahl:

- Mithilfe von **`systemctl`**:

```
root # systemctl reload squid
```

Alternativ:

```
root # systemctl restart squid
```

- Verwenden von YaST:
  Klicken Sie im Squid-Modul auf die Schaltfläche *Einstellungen jetzt speichern und Squid neu starten*.

Zum Anhalten von Squid stehen die folgenden Verfahren zur Auswahl:

- Mithilfe von **`systemctl`**:

```
root # systemctl stop squid
```

- Verwenden von YaST
  Klicken Sie im Squid-Modul auf die Schaltfläche *Squid jetzt stoppen*.

Das Herunterfahren von Squid kann einige Zeit dauern, da Squid bis zu eine halbe Minute wartet, bis die Verbindungen zu den Clients unterbrochen und die Daten auf die Festplatte geschrieben werden (siehe Option `shutdown_lifetime` in `/etc/squid/squid.conf`),

Warnung: Beenden von Squid

Das Beenden von Squid mit **`kill`** oder **`killall`** kann den Cache beschädigen. Damit Squid neu gestartet werden kann, müssen beschädigte Caches gelöscht werden.

33.3.4 Entfernen von Squid

Durch das Entfernen von Squid aus dem System werden die Cache-Hierarchie und die Protokolldateien nicht entfernt. Um diese zu entfernen, müssen Sie das Verzeichnis `/var/cache/squid` manuell löschen.

33.3.5 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 Konfigura-

tion erforderlich ist (siehe *Abschnitt 25.4, „Starten des BIND-Nameservers“*). 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 `NETCONFIG_DNS_POLICY` gesteuert. Legen Sie `NETCONFIG_DNS_POLICY` mit dem YaST-sysconfig-Editor auf `""` fest.

Fügen Sie anschließend den lokalen DNS-Server in der Datei `/etc/resolv.conf` hinzu. Verwenden Sie die IP-Adresse `127.0.0.1` für `localhost`. Auf diese Weise kann Squid immer den lokalen Nameserver finden, wenn er gestartet wird.

Um den Zugriff auf den Nameserver des Anbieters zu ermöglichen, geben Sie ihn zusammen mit seiner IP-Adresse in der Konfigurationsdatei `/etc/named.conf` unter `forwarders` an. Mit dynamischem DNS kann dies automatisch während des Verbindungsaufbaus erreicht werden. Setzen Sie hierzu die sysconfig-Variable `NETCONFIG_DNS_POLICY` mit dem YaST-sysconfig-Editor auf `auto`.

Statisches DNS

Beim statischen DNS finden beim Verbindunsgsaufbau keine automatischen DNS-Anpassungen statt, sodass auch keine sysconfig-Variablen geändert werden müssen. Sie müssen jedoch den lokalen DNS-Server in der Datei `/etc/resolv.conf`, wie unter *Dynamisches DNS* beschrieben, angeben. Außerdem muss der statische Nameserver des Anbieters zusammen mit seiner IP-Adresse manuell in der Datei `/etc/named.conf` unter `Forwarders` angegeben werden.

Tipp: DNS und Firewall

Wenn eine Firewall ausgeführt wird, müssen Sie sicherstellen, dass DNS-Anforderungen durchgelassen werden.

33.4 Das YaST-Squid-Modul

Das YaST-Squid-Modul enthält die folgenden Registerkarten:

Start

Gibt an, wie Squid gestartet wird und welcher Firewall-Port auf welchen Schnittstellen geöffnet ist.

HTTP-Ports

Definiert alle Ports, die Squid auf HTTP-Anforderungen von Clients überwacht.

Aktualisierungsschemata

Gibt an, wie Squid die Objekte im Cache behandelt.

Cache-Einstellungen

Definiert Einstellungen für den Cache-Speicher, die maximale und minimale Objektgröße und vieles mehr.

Cache-Verzeichnis

Definiert das übergeordnete Verzeichnis, in dem Squid alle Cache-Swap-Dateien speichert.

Zugriffssteuerung

Steuert den Zugriff auf den Squid-Server mithilfe von ACL-Gruppen.

Protokollierung und Zeitüberschreitung

Definiert die Pfade zu den Protokolldateien für Zugriff, Cache und Cache-Speicher sowie die Zeitüberschreitung für die Verbindungen und die Client-Lebensdauer.

Sonstige

Legt die Sprache und die Email-Adresse des Administrators fest.

33.5 Die Squid-Konfigurationsdatei

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.

Viele Einträge sind kommentiert und beginnen deshalb mit dem Kommentarzeichen `#`. Die relevanten Spezifikationen finden Sie am Ende der Zeile. Die angegebenen Werte entsprechen in der Regel den Standardwerten, daher hat das Entfernen der Kommentarzeichen ohne Ändern der Parameter in der Regel keine Auswirkungen. Lassen Sie die kommentierten Zeilen nach Möglichkeit unverändert und geben Sie die Optionen zusammen mit den geänderten Werten 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.

Manchmal werden Squid-Optionen hinzugefügt, entfernt oder geändert. Daher kann Squid möglicherweise aufhören, ordnungsgemäß zu funktionieren, wenn Sie die alte `squid.conf`-Datei verwenden.

33.5.1 Allgemeine Konfigurationsoptionen

Nachfolgend finden Sie eine Liste mit einer Auswahl an Konfigurationsoptionen für Squid. Die Liste ist nicht vollständig. Das Squid-Paket enthält eine vollständige Liste mit einfacher Veranschaulichung in der Datei `/etc/squid/squid.conf.documented`.

`http_port` *`PORT`*

Dies ist der Port, den Squid auf Client-Anforderungen überwacht. Der Standardport ist `3128`, `8080` wird jedoch ebenfalls häufig verwendet.

`cache_peer` *`HOSTNAME TYP PROXY-PORT ICP-PORT`*

Mit dieser Option kann ein Netzwerk mit Caches erstellt werden, die zusammen arbeiten. Der Cache-Peer ist ein Computer, der auch ein Netzwerk-Cache hostet und in einer Beziehung zu Ihrem eigenen steht. Der Typ der Beziehung wird als *`TYP`* angegeben. Der Typ kann entweder `parent` oder `sibling` sein.

Geben Sie als *HOSTNAME* den Namen oder die IP-Adresse des verwendeten Proxy an. Geben Sie für *PROXY-PORT* die Portnummer zur Verwendung in einem Browser an (in der Regel `8080`). Legen Sie für *ICP-PORT* den Wert `7` oder, wenn der ICP-Port des übergeordneten Proxy nicht bekannt ist und seine Verwendung für den Anbieter nicht wichtig ist, den Wert `0` fest.

Damit Squid sich wie ein Webbrowser verhält und nicht wie ein Proxy, verbieten Sie die Verwendung des ICP-Protokolls. Sie können dies verbieten, indem Sie die Optionen `default` und `no-query` anhängen.

`cache_mem` *GRÖSSE*

Diese Option 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` *SPEICHERTYP CACHE-VERZEICHNIS CACHE-GRÖSSE EBENE-1-VERZEICHNISSE EBENE-2-VERZEICHNISSE*

Die Option `cache_dir` legt das Verzeichnis für den Festplatten-Cache fest. In der Standardkonfiguration auf SUSE Linux Enterprise Server erstellt Squid keinen Festplatten-Cache.

Der Platzhalter *SPEICHERTYP* kann einen der folgenden Werte haben:

- Verzeichnisbasierte Speichertypen: `ufs`, `aufs` (Standard), `diskd`. Alle drei Typen sind Variationen des Speicherformats `ufs`. Dabei wird `ufs` als Teil des Squid-Core-Threads ausgeführt, `aufs` wird in einem separaten Thread ausgeführt und `diskd` verwendet einen separaten Prozess. Dies bedeutet, dass die letzten beiden Typen das Blockieren von Squid aufgrund von Datenträger-E/A vermeiden.

- Datenbankbasierte Speichersysteme: `rock`. Dieses Speicherformat basiert auf einer einzelnen Datenbankdatei, in der jedes Objekt eine oder mehrere Arbeitsspeichereinheiten einer festen Größe („Slots“) einnimmt.

Im Folgenden werden nur die Parameter für Speichertypen beschrieben, die auf `ufs` basieren. `rock` weist etwas andere Parameter auf.

Der Parameter *CACHE-VERZEICHNIS* steht für das Verzeichnis des Festplatten-Cache. Standardmäßig lautet dieses `/var/cache/squid`. *CACHE-GRÖSSE* ist die maximale Größe dieses Verzeichnisses in Megabyte. Der festgelegte Standardwert ist 100 MB. Legen Sie eine Größe zwischen 50 % und maximal 80 % des verfügbaren Speicherplatzes fest.

Die letzten zwei Werte *EBENE-1-VERZEICHNISSE* und *EBENE-2-VERZEICHNISSE* geben an, wie viele Unterverzeichnisse im *CACHE-VERZEICHNIS* erstellt werden. Standardmäßig werden 16 Unterverzeichnisse auf der ersten Ebene unter *CACHE-VERZEICHNIS* und 256 jeweils innerhalb dieser Ebenen erstellt. Diese Werte sollten nur nach reiflicher Überlegung erhöht werden, da zu viele Verzeichnisse zu Leistungsproblemen führen können.

Wenn ein Cache von mehreren Datenträgern gemeinsam verwendet wird, müssen Sie mehrere `cache_dir`-Zeilen angeben.

`cache_access_log` *PROTOKOLLDATEI*,
`cache_log` *PROTOKOLLDATEI*,
`cache_store_log` *PROTOKOLLDATEI*

Diese drei Optionen geben die Pfade an, in denen Squid alle Aktionen protokolliert. In der Regel muss hier nichts geändert werden. Bei hoher Auslastung von Squid kann es sinnvoll sein, Cache und Protokolldateien auf mehrere Datenträger zu verteilen.

`client_netmask` *NETZMASKE*

Diese Option ermöglicht die Maskierung von IP-Adressen des Client in der Protokolldatei, indem eine Teilnetzmaske angewendet wird. Um beispielsweise für die letzte Zahl der IP-Adresse `0` festzulegen, geben Sie `255.255.255.0` an.

`ftp_user` *E-MAIL*

Diese Option ermöglicht die Einstellung des Passworts, das Squid für die anonyme FTP-Anmeldung verwenden soll. Geben Sie hier eine gültige E-Mail-Adresse ein, da manche FTP-Server diese auf Gültigkeit überprüfen.

`cache_mgr` *E-MAIL*

Bei unerwartetem Absturz sendet Squid eine Nachricht an diese E-Mail-Adresse. Der Standardwert ist *webmaster*.

`logfile_rotate` *WERT*

Wenn Sie **`squid`** `-k rotate` ausführen, kann **`Squid`** ein Rotationssystem für Protokolldateien einführen. Bei diesem Prozess werden die Dateien nummeriert und nach dem Erreichen des angegebenen Werts wird die älteste Datei überschrieben. Der Standardwert ist `10`. Hierdurch werden Protokolldateien mit den Nummern 0 bis 9 rotiert.

Auf SUSE Linux Enterprise Server erfolgt die Rotation der Protokolldateien jedoch mithilfe von `logrotate` und der Konfigurationsdatei `/etc/logrotate.d/squid` automatisch.

`append_domain` *DOMÄNE*

Verwenden Sie *append_domain*, um anzugeben, welche Domäne automatisch angefügt wird, wenn keine angegeben wurde. In der Regel wird hier die eigene Domäne angegeben, sodass bei der Angabe von *www* im Browser ein Zugriff auf Ihren eigenen Webserver erfolgt.

`forwarded_for` *STATUS*

Ist für diese Option `on` festgelegt, wird eine Zeile wie die folgende zum Header hinzugefügt:

```
X-Forwarded-For: 192.168.0.1
```

Wenn Sie für diese Option `off` festlegen, entfernt Squid die IP-Adresse und den Systemnamen des Client aus den HTTP-Anforderungen.

`negative_ttl` *ZEIT*,
`negative_dns_ttl` *ZEIT*

Sind diese Optionen festgelegt, speichert Squid manche Fehlertypen im Cache, wie beispielsweise `404`-Antworten. Squid lässt dann keine neuen Anforderungen mehr zu, selbst wenn die Ressource verfügbar wäre.

Standardmäßig sind für `negative_ttl` der Wert `0` und für `negative_dns_ttl` der Wert `1 minutes` festgelegt. Dies bedeutet, dass negative Antworten auf Webanforderungen standardmäßig nicht im Cache gespeichert werden und negative Antworten auf DNS-Anforderungen für eine Minute im Cache gespeichert werden.

`never_direct allow` *ACL-NAME*

Um zu verhindern, dass Squid Anforderungen direkt aus dem Internet entgegennimmt, müssen Sie mit der Option `never_direct` die Verbindung mit einem anderen Proxy erzwingen. Dieser muss zuvor unter `cache_peer` angegeben worden sein. Wenn `all` als *ACL-NAME* angegeben ist, werden alle Anforderungen direkt an den übergeordneten Proxy (`parent`) weitergeleitet. Dies kann beispielsweise dann erforderlich sein, wenn Sie einen Anbieter verwenden, der die Verwendung der eigenen Proxys vorschreibt oder der durch seine Firewall direkten Internetzugriff verweigert.

33.5.2 Optionen für die Zugriffssteuerung

Squid bietet ein detailliertes System für die Steuerung des Zugriffs auf den Proxy. Diese ACLs (Access Control Lists = Zugriffssteuerungslisten) sind 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 passiert nur dann, wenn eine entsprechende `http_access`-Regel vorhanden ist.

Die Syntax für die Option `acl` lautet:

```
acl ACL_NAME TYPE DATA
```

Die Platzhalter innerhalb dieser Syntax stehen für Folgendes:

- 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.

Sollen Regeln in das YaST-Squid-Modul eingefügt werden, öffnen Sie das Modul und klicken Sie auf die Registerkarte *Zugriffssteuerung*. Klicken Sie unter der Liste der ACL-Gruppen auf *Hinzufügen* und geben Sie den Namen Ihrer Regel, den Typ und die zugehörigen Parameter ein.

Weitere Informationen zu den Typen von ACL-Regeln finden Sie in der Squid-Dokumentation unter http://www.squid-cache.org/Versions/v3/3.5/cfgman/acl.html.

BEISPIEL 33.2 DEFINIEREN VON ACL-REGELN

```
acl mysurfers srcdomain .example.com ❶
acl teachers src 192.168.1.0/255.255.255.0 ❷
acl students src 192.168.7.0-192.168.9.0/255.255.255.0 ❸
acl lunch time MTWHF 12:00-15:00 ❹
```

❶ Diese ACL legt fest, dass `mysurfers` alle Benutzer sind, die von `.example.com` kommen (wie durch Reverse-Lookup für die IP bestimmt wurde).

❷ Diese ACL legt fest, dass `teachers` die Benutzer von Computern sind, deren IP-Adressen mit `192.168.1.` beginnen.

❸ Diese ACL legt fest, dass `students` die Benutzer von Computern sind, deren IP-Adressen mit `192.168.7.`, `192.168.8.` oder `192.168.9.` starten.

❹ Diese ACL legt fest, dass `lunch` eine Zeit an den Tagen Montag, Dienstag, ... Freitag zwischen 12 und 15 Uhr ist.

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 festgelegt werden. `localhost` und `all` wurden bereits oben festgelegt. Sie können den Zugriff dafür verweigern oder erlauben mit `deny` bzw. `allow`. 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 muss immer `http_access deny all` sein. 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
```

Geben Sie für eine bessere Lesbarkeit in der Konfigurationsdatei `/etc/squid/squid.conf` alle `http_access`-Optionen in einem Block an.

`url_rewrite_program` *PFAD*

Geben Sie mit dieser Optionen einen URL-Rewriter an. Dies kann beispielsweise squidGuard sein (`/usr/sbin/squidGuard`), der das Blockieren unerwünschter URLs ermöglicht. Damit kann der Internetzugriff individuell für verschiedene Benutzergruppen mithilfe von Proxy-Authentifizierung und entsprechenden ACLs gesteuert werden.
Weitere Informationen zu squidGuard finden Sie in *Abschnitt 33.8, „squidGuard“*.

`auth_param basic program PFAD`

Wenn Benutzer auf dem Proxy authentifiziert werden müssen, geben Sie ein geeignetes Programm an, beispielsweise `/usr/sbin/pam_auth`. Beim ersten Ausführen von **`pam_auth`** wird ein Anmeldefenster geöffnet, in dem der Benutzer den Benutzernamen und das Passwort eingeben muss. Außerdem ist 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
```

Wird in der Option `acl proxy_auth` der Wert `REQUIRED` verwendet, bedeutet dies, dass alle gültigen Benutzernamen akzeptiert werden. `REQUIRED` kann auch durch eine Liste mit erlaubten Benutzernamen ersetzt werden.

`ident_lookup_access allow ACL-NAME`

Lassen Sie damit eine ident-Anforderung für alle Clients, die mit einer ACL des Typs `src` festgelegt sind, ausführen, um die Identität der einzelnen Benutzer zu ermitteln. Alternativ dazu (verwenden Sie dies für alle Clients) können Sie die vordefinierte ACL `all` als *`ACL-NAME`* anwenden.

Auf allen Clients, die durch `ident_lookup_access` abgedeckt sind, muss ein ident-Daemon ausgeführt werden. Unter Linux können Sie `pidentd` (package `pidentd`) als ident-Daemon verwenden. Für andere Betriebssysteme ist in der Regel kostenlose Software verfügbar. Um sicherzustellen, dass nur Clients mit einem erfolgreichen ident-Lookup zulässig sind, definieren Sie eine entsprechende ACL:

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

Wird in der Option `acl identhosts ident` der Wert `REQUIRED` verwendet, bedeutet dies, dass alle gültigen Benutzernamen akzeptiert werden. `REQUIRED` kann auch durch eine Liste mit erlaubten Benutzernamen ersetzt werden.

Durch die Verwendung von `ident` kann die Zugriffszeit erheblich reduziert werden, da die ident-Lookups für jede Anforderung wiederholt werden.

33.6 Konfigurieren eines transparenten Proxy

In der Regel arbeiten Sie folgendermaßen mit Proxyservern: Der Webbrowser sendet Anforderungen an einen bestimmten Port des Proxyservers und der Proxy liefert immer diese erforderlichen Objekte, unabhängig davon, ob sie sich im Cache befinden oder nicht. In manchen Fällen ist die Verwendung des transparenten Proxy-Modus von Squid empfehlenswert:

- Wenn aus Sicherheitsgründen alle Clients einen Proxy für den Zugriff auf das Internet verwenden sollten.
- Wenn alle Clients einen Proxy verwenden müssen, unabhängig davon, ob sie sich dessen bewusst sind.
- Wenn der Proxy in einem Netzwerk verschoben wird, die vorhandenen Clients jedoch ihre alte Konfiguration beibehalten müssen.

Ein transparenter 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 bereits andeutet, verläuft der gesamte Prozess für den Benutzer transparent.

PROZEDUR 33.1 SQUID ALS EIN TRANSPARENTER PROXY (BEFEHLSZEILE)

1. Fügen Sie in der Datei `/etc/squid/squid.conf` in der Zeile mit der Option `http_port` den Parameter `transparent` hinzu:

   ```
   http_port 3128 transparent
   ```

2. Starten Sie Squid neu:

   ```
   tux > sudo systemctl restart squid
   ```

3. Richten Sie SuSEFirewall2 so ein, dass HTTP-Datenverkehr an den in `http_proxy` angegebenen Port umgeleitet wird (im Beispiel oben war dies Port 3128). Bearbeiten Sie hierzu die Konfigurationsdatei `/etc/sysconfig/SuSEfirewall2`.
   In diesem Beispiel wird angenommen, dass Sie die folgenden Geräte verwenden:

   - Auf das Internet zeigendes Gerät: `FW_DEV_EXT="eth1"`
   - Auf das Netzwerk zeigendes Gerät: `FW_DEV_INT="eth0"`

Definieren Sie Ports und Dienste (siehe `/etc/services`) auf der Firewall, auf die von nicht verbürgten (externen) Netzwerken, wie beispielsweise dem Internet, zugegriffen wird. 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, Domänennamen-Dienst). Dieser Dienst wird häufig verwendet. Entfernen Sie andernfalls einfach `domain` aus dem obigen Eintrag und legen Sie für die folgende Option `no` fest:

```
FW_SERVICE_DNS="yes"
```

Die Option `FW_REDIRECT` ist sehr wichtig, da sie für das tatsächliche Umleiten des HTTP-Datenverkehrs auf einen bestimmten Port verwendet wird. In der Konfigurationsdatei wird die Syntax in einem Kommentar über der Option erläutert:

```
# Format:
# list of <source network>[,<destination network>,<protocol>[,dport[:lport]]
# Where protocol is either tcp or udp. dport is the original
# destination port and lport the port on the local machine to
# redirect the traffic to
#
# An exclamation mark in front of source or destination network
# means everything EXCEPT the specified network
```

Das heißt:

1. Geben Sie die IP-Adresse und die Netzmaske der internen Netzwerke an, die auf die Proxy-Firewall zugreifen.

2. Geben Sie die IP-Adresse und die Netzmaske an, an die diese Clients ihre Anforderungen senden. Geben Sie bei Webbrowsern die Netzwerke `0/0` an. Dieser Platzhalter bedeutet „überallhin“.

3. Geben Sie den ursprünglichen Port an, an den diese Anforderungen gesendet werden.

4. Geben Sie den Port an, an den alle diese Anforderungen umgeleitet werden. In dem Beispiel unten werden Webdienste (Port `80`) an den Proxy-Port (Port `3128`) umgeleitet. Wenn mehr Netzwerke oder Dienste hinzugefügt werden sollen, trennen Sie diese durch ein Leerzeichen im entsprechenden Eintrag.
   Da Squid auch andere Protokolle als HTTP unterstützt, können Sie auch Anforderungen von anderen Ports zum Proxy umleiten. Beispielsweise können Sie auch Port 21 (FTP) und Port 443 (HTTPS oder SSL) umleiten.

Daher könnten Sie für eine Squid-Konfiguration das folgende Kommando verwenden:

```
FW_REDIRECT="192.168.0.0/16,0/0,tcp,80,3128"
```

4. Stellen Sie sicher, dass in der Konfigurationsdatei `/etc/sysconfig/SuSEfirewall2` der Eintrag `START_FW` auf `"yes"` festgelegt ist.

5. Starten Sie SuSEFirewall2 neu:

```
tux > sudo systemctl restart SuSEfirewall2
```

6. Sehen Sie sich die Squid-Protokolle unter `/var/log/squid/access.log` an, um zu überprüfen, ob alles ordnungsgemäß funktioniert. Führen Sie einen Portscan auf dem Computer von einem Computer außerhalb Ihres Netzwerks durch, um zu überprüfen, ob alle Ports korrekt konfiguriert sind. Nur die Webdienste (Port 80) sollten verfügbar sein. Um die Ports mit **`nmap`** zu scannen, verwenden Sie:

```
nmap -O IP_ADDRESS
```

PROZEDUR 33.2 SQUID ALS EIN TRANSPARENTER PROXY (YAST)

1. Starten Sie das YaST-Squid-Modul:

   a. Aktivieren Sie im Karteireiter *Start* die Option *Firewall-Ports öffnen*. Klicken Sie auf *Firewall-Details*, um die Schnittstellen auszuwählen, über die der Port geöffnet werden soll. Diese Option ist nur verfügbar, wenn die Firewall aktiviert ist.

   b. Wählen Sie im Karteireiter *HTTP-Ports* die erste Zeile mit dem Port `3128` aus.

   c. Klicken Sie auf die Schaltfläche *Bearbeiten*. Es öffnet sich ein kleines Fenster, in dem Sie den aktuellen HTTP-Port bearbeiten können. Wählen Sie *Transparent* aus.

d. Klicken Sie abschließend auf *OK*.

2. Konfigurieren Sie die Firewall-Einstellungen so, wie unter *Schritt 3* in *Prozedur 33.1, „Squid als ein transparenter Proxy (Befehlszeile)“* beschrieben.

33.7 Verwenden der Cache-Manager-CGI von Squid (`cachemgr.cgi`)

Die Cache-Manager-CGI (Common Gateway Interface; `cachemgr.cgi`) ist ein CGI-Dienstprogramm für die Anzeige der Statistiken zur Arbeitsspeichernutzung eines laufenden Squid-Prozesses. Außerdem bietet er eine bequeme Methode zur Verwaltung des Cache und zur Anzeige der Statistiken ohne Anmeldung beim Server.

PROZEDUR 33.3 EINRICHTEN VON `cachemgr.cgi`

1. Stellen Sie sicher, dass der Apache-Webserver auf Ihrem System ausgeführt wird. Konfigurieren Sie Apache, wie in *Kapitel 31, Der HTTP-Server Apache* beschrieben. Lesen Sie insbesondere *Abschnitt 31.5, „Aktivieren von CGI-Skripten“*. Um zu überprüfen, ob Apache bereits ausgeführt wird, verwenden Sie:

   ```
   tux > sudo systemctl status apache2
   ```

   Wenn `inactive` angezeigt wird, können Sie Apache mit den Standardeinstellungen von SUSE Linux Enterprise Server starten:

   ```
   tux > sudo systemctl start apache2
   ```

2. Aktivieren Sie nun `cachemgr.cgi` in Apache. Erstellen Sie hierzu eine Konfigurationsdatei für ein `ScriptAlias`.
   Erstellen Sie die Datei im Verzeichnis `/etc/apache2/conf.d` und nennen Sie sie `cachemgr.conf`. Fügen Sie Folgendes in der Datei hinzu:

   ```
   ScriptAlias /squid/cgi-bin/ /usr/lib64/squid/

   <Directory "/usr/lib64/squid/">
   Options +ExecCGI
   AddHandler cgi-script .cgi
   Require host HOST_NAME
   </Directory>
   ```

Ersetzen Sie *HOSTNAME* durch den Hostnamen des Computers, über den Sie auf `cachemgr.cgi` zugreifen möchten. Dies erlaubt es nur Ihrem Computer, auf `cachemgr.cgi` zuzugreifen. Um den Zugriff von allen Computern zu erlauben, verwenden Sie stattdessen `Require all granted`.

3.
   - Wenn Squid und Ihr Apache-Webserver auf demselben Computer ausgeführt werden, sollten keine Änderungen an `/etc/squid/squid.conf` notwendig sein. Überprüfen Sie jedoch, ob `/etc/squid/squid.conf` die folgenden Zeilen enthält:

     ```
     http_access allow manager localhost
     http_access deny manager
     ```

     Diese Zeilen erlauben Ihnen den Zugriff auf die Manager-Schnittstelle über Ihren eigenen Computer (`localhost`), jedoch nicht über andere Computer.

   - Wenn Squid und Ihr Apache-Webserver auf verschiedenen Computern ausgeführt werden, müssen Sie zusätzliche Regeln hinzufügen, um den Zugriff über das CGI-Skript auf Squid zu erlauben. Geben Sie eine ACL für Ihren Server an (ersetzen Sie *WEBSERVER-IP* durch die IP-Adresse Ihres Webservers):

     ```
     acl webserver src WEB_SERVER_IP/255.255.255.255
     ```

     Stellen Sie sicher, dass die folgenden Regeln in der Konfigurationsdatei enthalten sind. Verglichen mit der Standardkonfiguration ist nur die Regel in der Mitte neu. Jedoch ist die Sequenz wichtig.

     ```
     http_access allow manager localhost
     http_access allow manager webserver
     http_access deny manager
     ```

4. *(Optional)* Optional können Sie ein oder mehrere Passwörter für `cachemgr.cgi` konfigurieren. Dies erlaubt auch den Zugriff auf weitere Aktionen, wie das Schließen des Cache per Fernzugriff oder das Anzeigen weiterer Informationen zum Cache. Konfigurieren Sie hierfür die Optionen `cache_mgr` und `cachemgr_passwd` mit einem oder mehreren Passwörtern für den Manager und einer Liste der erlaubten Aktionen.

Beispiel: Verwenden Sie die folgende Konfiguration, um explizit das Anzeigen der Indexseite, des Menüs und des 60-minütigen Durchschnitts der Zähler ohne Authentifizierung zu aktivieren, das Umschalten des Offline-Modus mithilfe des Passworts `secretpassword` zu aktivieren und alles andere vollständig zu deaktivieren:

```
cache_mgr user
cachemgr_passwd none index menu 60min
cachemgr_passwd secretpassword offline_toggle
cachemgr_passwd disable all
```

`cache_mgr` legt einen Benutzernamen fest. `cache_mgr` legt fest, welche Aktionen mit welchen Passwort erlaubt sind.
Die Schlüsselwörter `none` und `disable` haben besondere Eigenschaften: `none` entfernt die Notwendigkeit eines Passworts, `disable` inaktiviert die Funktion vollständig.
Die vollständige Liste der Aktionen finden Sie nach der Anmeldung bei `cachemgr.cgi`. Wie die Operation in der Konfigurationsdatei zu referenzieren ist, sehen Sie in der Zeichenkette nach `&operation=` in der URL der Aktionsseite. `all` ist ein besonderes Schlüsselwort und steht für alle Aktionen.

5. Laden Sie Squid und Apache neu, nachdem die Konfigurationsdatei geändert wurde:

```
tux > sudo systemctl reload squid
```

6. Um die Statistiken anzuzeigen, rufen Sie die Seite `cachemgr.cgi` auf, die Sie zuvor eingerichtet haben. Diese könnte beispielsweise `http://webserver.example.org/squid/cgi-bin/cachemgr.cgi` lauten.
Wählen Sie den richtigen Server und geben Sie, falls dies festgelegt wurde, den Benutzernamen und das Passwort ein. Klicken Sie dann auf *Fortsetzen* und blättern Sie durch die verschiedenen Statistiken.

33.8 squidGuard

In diesem Abschnitt wird keine umfassende Konfiguration von squidGuard erläutert. Er gibt lediglich eine Einführung und einige Hinweise zur Verwendung. 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 Skripten, wie JavaScript.

PROZEDUR 33.4 EINRICHTEN VON SQUIDGUARD

1. Vor der Verwendung müssen Sie `squidGuard` installieren.
2. Geben Sie eine Datei mit der Minimalkonfiguration als `/etc/squidguard.conf` an. Konfigurationsbeispiele finden Sie unter http://www.squidguard.org/Doc/examples.html. Später können Sie mit komplizierteren Konfigurationseinstellungen experimentieren.
3. Erstellen Sie als Nächstes eine HTML-Seite mit „Zugriff verweigert“ oder eine CGI-Seite, zu der Squid umgeleitet werden kann, wenn der Client eine Website anfordert, die auf der schwarzen Liste steht. Die Verwendung von Apache wird dringend empfohlen.
4. 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
```

5. Eine weitere Option, `redirect_children`, konfiguriert die Zahl von „redirect“-Prozessen (in diesem Fall squidGuard), die auf dem Rechner ausgeführt werden. Je mehr Prozesse Sie angeben, desto mehr RAM ist erforderlich. Versuchen Sie zuerst niedrige Zahlen, beispielsweise `4`:

   ```
   redirect_children 4
   ```

6. Lassen Sie Squid abschließend die neue Konfiguration laden; führen Sie hierzu **`systemctl reload squid`** aus. Testen Sie nun Ihre Einstellungen mit einem Browser.

33.9 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://cord.de/calamaris-english. Dieses Werkzeug gehört nicht zum standardmäßigen Installationsumfang von SUSE Linux Enterprise Server. Zum Verwenden installieren Sie das Paket `calamaris`.

Melden Sie sich als `root` an und geben Sie Folgendes ein:

```
cat access1.log [access2.log access3.log] | calamaris OPTIONS > reportfile
```

Wenn Sie mehr als eine Protokolldatei verwenden, stellen Sie sicher, dass sie chronologisch geordnet sind, wobei ältere Dateien zuerst aufgelistet werden. Dies können Sie erreichen, indem Sie die Dateien eine nach der anderen wie im Beispiel oben auflisten oder indem Sie `access{1..3}.log` verwenden.

`calamaris` erfordert die folgenden Optionen:

`-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 man-Seite des Programms (**`man calamaris`**.

Typisches Beispiel:

```
cat access.log.{10..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.

33.10 Weiterführende 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.

Außerdem sind Mailinglisten für Squid unter http://www.squid-cache.org/Support/mailing-lists.html verfügbar.

34 Web Based Enterprise Management mit SFCB

34.1 Einführung und grundlegendes Konzept

SUSE® Linux Enterprise Server (SLES) stellt eine Sammlung verschiedener, auf offenen Standards beruhender Werkzeuge für die einheitliche Verwaltung unterschiedlicher Computersysteme und -umgebungen bereit. In unseren Unternehmenslösungen sind die von der Distributed Management Task Force vorgeschlagenen Standards implementiert. Deren grundlegenden Komponenten werden in den folgenden Abschnitten beschrieben.

Die Distributed Management Task Force, Inc (DMTF) ist eine industrieführende Organisation, die sich maßgeblich mit der Entwicklung von Verwaltungsstandards für Unternehmens- und Internetumgebungen befasst. Ihr Ziel ist die Vereinheitlichung von Verwaltungsstandards und Verwaltungsinitiativen und damit die Ermöglichung von integrierten, kostengünstigen und auf verschiedenen Systemen einsetzbaren Lösungen. Die DMTF-Standards umfassen allgemeine Systemverwaltungskomponenten für die Steuerung und Kommunikation. Ihre Lösungen sind unabhängig von Plattformen und Technologien. Zu ihren Schlüsseltechnologien gehören unter anderem *Web Based Enterprise Management* und *Common Information Model*.

Web Based Enterprise Management (WBEM) umfasst eine Reihe von Verwaltungs- und Internet-Standardtechnologien. WBEM wurde zur Vereinheitlichung der Verwaltung von Computerumgebungen in Unternehmen entwickelt. Dieser Standard bietet der Industrie die Möglichkeit, eine gut integrierte Sammlung von Verwaltungstools auf Basis von Web-Technologien bereitzustellen. WBEM besteht aus den folgenden Standards:

- Ein Datenmodell: der Common Information Model-Standard (CIM-Standard)
- Eine Kodierungsspezifikation: CIM-XML-Kodierungsspezifikation
- Ein Transportmechanismus: CIM-Vorgänge über HTTP

Common Information Model ist ein konzeptuelles Informationsmodell, das die Systemverwaltung beschreibt. Es ist nicht an eine bestimmte Implementierung gebunden und ermöglicht den Austausch von Verwaltungsdaten zwischen Verwaltungssystemen, Netzwerken, Diensten und Anwendungen. CIM umfasst zwei Teile: die CIM-Spezifikation und das 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*. Das Metaschema unterstützt außerdem *Bezeichnungen* und *Verknüpfungen* als *Klassentypen* und *Verweise* als *Eigenschaftstypen*.

- Das *CIM-Schema* enthält die eigentlichen Modellbeschreibungen. Es legt einen Klassensatz mit Eigenschaften und Verknüpfungen fest, die ein verständliches 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 verwaltet die Kommunikation zwischen CIMOM-Anbietern und dem CIM-Client, auf dem der Administrator das System 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. Diese Anbieter interagieren direkt mit der Hardware.

Standards Based Linux Instrumentation for Manageability (SBLIM) ist eine Sammlung von Tools, die zur Unterstützung von Web-Based Enterprise Management (WBEM) entwickelt wurden. SUSE® Linux Enterprise Server nutzt den Open Source-CIMOM (bzw. CIM-Server) des SBLIM-Projekts, den *Small Footprint CIM Broker*.

Der *Small Footprint CIM Broker* ist ein CIM-Server für integrierte Umgebungen bzw. für Umgebungen mit eingeschränkten Ressourcen. Bei seiner Entwicklung wurde insbesondere auf einen modulartigen Charakter und eine Lightweight-Struktur geachtet. Er basiert auf offenen Standards und unterstützt CMPI-Anbieter, CIM-XML-Verschlüsselung und das *Managed Object Format (MOF)*. Er lässt sich sehr genau konfigurieren und bietet selbst bei einem Ausfall des Anbieters Stabilität. Außerdem ist er problemlos zugänglich, da er verschiedene Übertragungsprotokolle wie HTTP, HTTPS, Unix Domain Sockets, Service Location Protocol (SLP) und Java Database Connectivity (JDBC) unterstützt.

34.2 Einrichten des SFCB

Zum Einrichten der Small Footprint CIM Broker (SFCB)-Umgebung muss in YaST während der Installation von SUSE Linux Enterprise Server das Schema *Web-Based Enterprise Management* aktiviert sein. Alternativ können Sie das Muster als Komponente auswählen, die auf einem bereits aktiven Server installiert wird. Stellen Sie sicher, dass auf Ihrem System die folgenden Pakete installiert sind:

cim-schema, Common Information Model-Schema (CIM)

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.

cmpi-bindings-pywbem

Enthält einen Adapter zum Entwickeln und Ausführen von CMPI-ähnlichen CIM-Anbietern in Python.

cmpi-pywbem-base

Enthält CIM-Anbieter für ein Basissystem.

cmpi-pywbem-power-management

Enthält auf DSP1027 basierende Energieverwaltungsanbieter.

python-pywbem

Enthält ein Python-Modul für den Aufruf von CIM-Operationen über das WBEM-Protokoll zur Abfrage und Aktualisierung verwalteter Objekte.

cmpi-provider-register, Dienstprogramm für die CIMOM-neutrale Anbieterregistrierung

Enthält ein Dienstprogramm, das die Registrierung von CMPI-Anbieterpaketen bei jedem auf dem System vorhandenen CIMOM zulässt.

sblim-sfcb, Small Footprint CIM Broker

Enthält den Small Footprint CIM Broker (SFCB). Dies ist ein CIM-Server, der CIM-Operationen über das HTTP-Protokoll unterstützt. Dieser robuste CIM-Server hat einen geringen Ressourcenbedarf und ist daher bestens für integrierte Umgebungen und für Umgebungen mit eingeschränkten Ressourcen geeignet. SFCB unterstützt Anbieter, die für das Common Manageability Programming Interface (CMPI) entwickelt wurden.

sblim-sfcc

Enthält Laufzeitbibliotheken für die Small Footprint CIM Client-Bibliothek.

sblim-wbemcli

Enthält eine WBEM-Kommandozeilenschnittstelle. Dieser eigenständige Kommandozeilen-WBEM-Client eignet sich besonders für grundlegende Systemverwaltungsaufgaben.

smis-providers

Enthält Anbieter zur Instrumentalisierung der Volumes und Snapshots auf dem Linux-Dateisystem. Diese basieren auf dem SMI-S-Volume-Verwaltungsprofil von SNIA bzw. auf dem Profil zum Kopieren von Diensten.

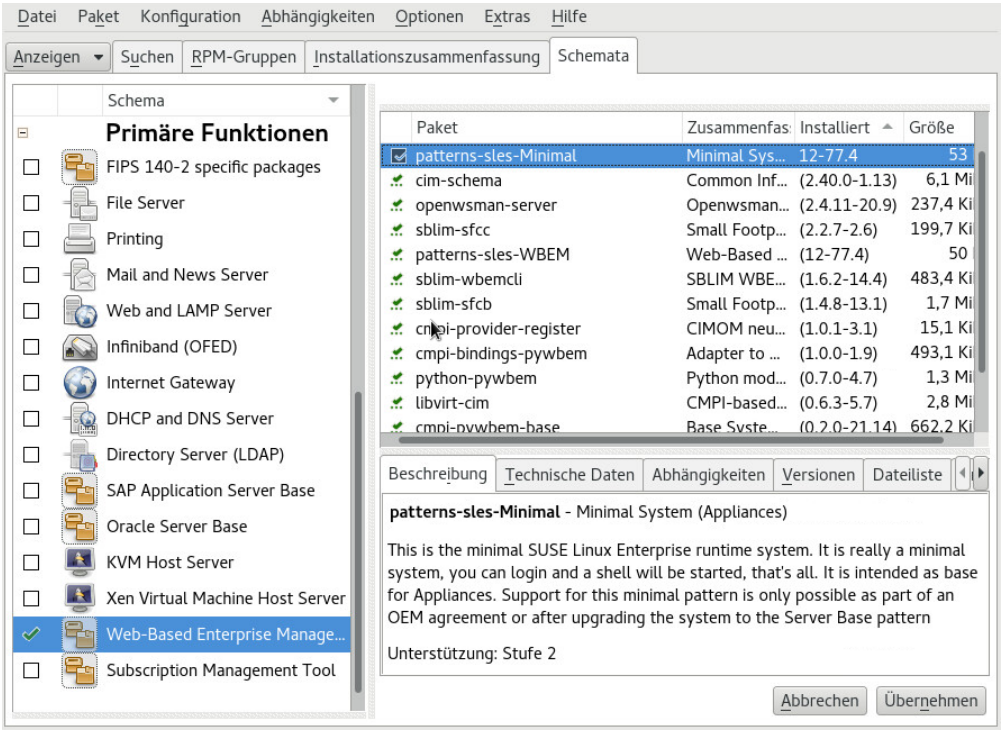


ABBILDUNG 34.1 PAKETAUSWAHL FÜR DAS WEB-BASED ENTERPRISE MANAGEMENT-MUSTER

34.2.1 Installieren zusätzlicher Anbieter

Das Softwarerepository von SUSE® Linux Enterprise Server enthält weitere CIM-Anbieter, die nicht im Web-Based Enterprise Management-Installationsschema enthalten sind. Deren Liste sowie deren Installationsstatus können Sie einsehen, indem Sie das Schema `sblim-cmpi-` im

YaST-Softwareinstallationsmodul durchsuchen. Diese Anbieter decken verschiedene Aufgaben der Systemverwaltung ab, wie DHCP, NFS oder die Einstellung der Kernel-Parameter. Sie sollten diejenigen Anbieter installieren, die Sie mit SFCB verwenden möchten.

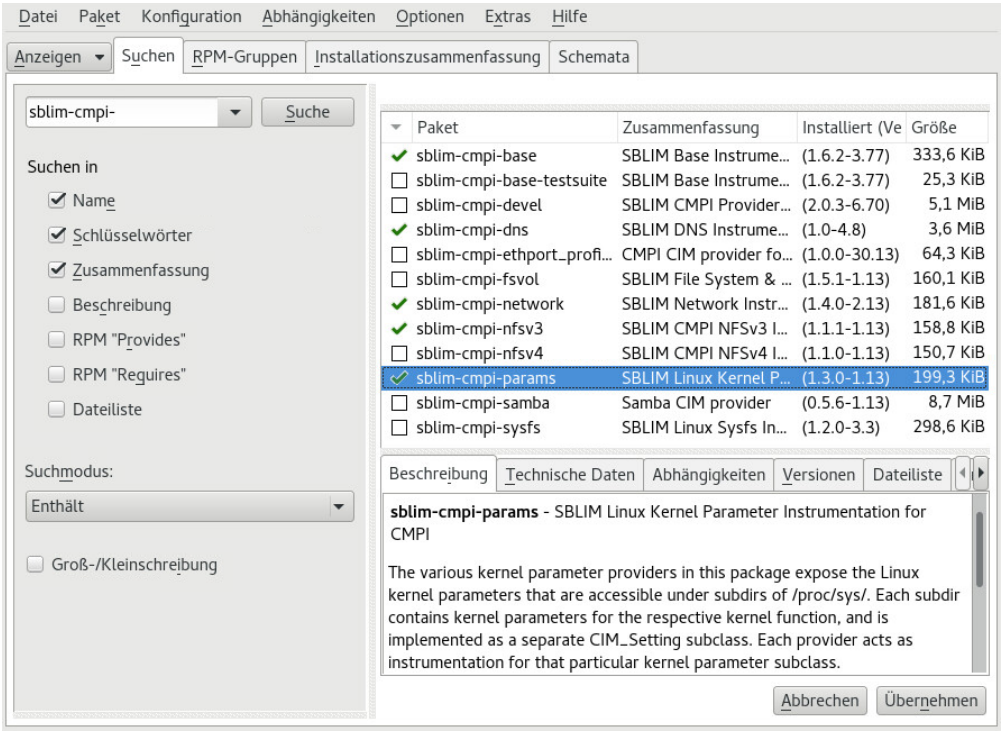


ABBILDUNG 34.2 PAKETAUSWAHL ZUSÄTZLICHER CIM-ANBIETER

34.2.2 Starten und Stoppen von SFCB und Überprüfen des SFCB-Status

Der sfcbd-Daemon des CIM-Servers wird gemeinsam mit der Web-Based Enterprise Management-Software installiert und beim Systemstart automatisch gestartet. In folgender Tabelle wird beschrieben, wie der sfcbd-Daemon gestartet, beendet und sein Status überprüft wird.

TABELLE 34.1 KOMMANDOS ZUR VERWALTUNG VON SFCBD

Job	Linux Befehl
Starten Sie sfcbd	Geben Sie in der Kommandozeile **`systemctl start sfcb`** als `root` ein.
sfcbd stoppen	Geben Sie in der Kommandozeile **`systemctl stop sfcb`** als `root` ein.

Job	Linux Befehl
sfcbd-Status prüfen	Geben Sie in der Kommandozeile **`systemctl status sfcb`** als `root` ein.

34.2.3 Absichern des Zugriffs

Die Standardkonfiguration von SFCB ist ziemlich sicher. Sie sollten allerdings sicherstellen, dass auch der Zugriff auf die SFCB-Komponenten den Sicherheitsanforderungen Ihres Unternehmens entspricht.

34.2.3.1 Zertifikate

Für eine sichere Kommunikation via SSL (Secure Socket Layers) ist ein Zertifikat erforderlich. Bei der Installation von SFCB wird ein eigensigniertes Zertifikat generiert.

Den Pfad auf dieses Standardzertifikat können Sie durch den Pfad eines kommerziellen oder eines anderen eigensignierten Zertifikats ersetzen. Dazu müssen Sie die Einstellung `sslCertificateFilePath: PFAD_DATEINAME` in der Datei `/etc/sfcb/sfcb.cfg` ändern. Die Datei muss im PEM-Format vorliegen.

Das standardmäßig generierte Serverzertifikat befindet sich in folgender Datei:

`/etc/sfcb/server.pem`

Anmerkung: Pfade zu SSL-Zertifikaten

Die standardmäßig generierten Zertifikatdateien `servercert.pem` und `serverkey.pem` befinden sich im Verzeichnis `/etc/ssl/servercerts`. Die Dateien `/etc/sfcb/client.pem`, `/etc/sfcb/file.pem` und `/etc/sfcb/server.pem` sind symbolische Links auf diese Dateien.

Zum Generieren eines neuen Zertifikats geben Sie in die Kommandozeile folgendes Kommando als `root` ein:

```
tux > sh /usr/share/sfcb/genSslCert.sh
Generating SSL certificates in .
Generating a 2048 bit RSA private key
```

```
.....................................................................+++
.+++
writing new private key to '/var/tmp/sfcb.0Bjt69/key.pem'
-----
```

Das Skript generiert die Zertifikate `client.pem`, `file.pem` und `server.pem` standardmäßig im aktuellen Arbeitsverzeichnis. Wenn die Zertifikate im Verzeichnis `/etc/sfcb` generiert werden sollen, müssen Sie das Verzeichnis an das Kommando anfügen. Falls diese Dateien bereits vorhanden sind, wird eine Warnung angezeigt, da die alten Zertifikate nicht einfach überschrieben werden können.

```
tux > sh /usr/share/sfcb/genSslCert.sh /etc/sfcb
Generating SSL certificates in .
WARNING: server.pem SSL Certificate file already exists.
         old file will be kept intact.
WARNING: client.pem SSL Certificate trust store already exists.
         old file will be kept intact.
```

Sie müssen die alten Zertifikate aus dem Dateisystem entfernen und das Kommando erneut ausführen.

Weitere Informationen, wie Sie die Verwendung von Zertifikaten durch SFCB verändern, finden Sie unter *Abschnitt 34.2.3.3, „Authentifizierung “*.

34.2.3.2 Ports

Standardmäßig akzeptiert SFCB die gesamte Kommunikation über den sicheren Port 5989. Die folgenden Abschnitte befassen sich mit der Einrichtung des Kommunikationsports und der empfohlenen Konfiguration.

Port 5989 (sicher)

Der sichere Port, den SFCB für die Kommunikation via HTTPS-Dienste verwendet. Dies ist der Standard. Bei dieser Einstellung wird die gesamte Kommunikation zwischen dem CIMOM und den Clientanwendungen für die Internet-Übertragung zwischen Servern und Arbeitsstationen verschlüsselt. Damit Benutzer den SFCB-Server erreichen, müssen sie sich bei der Clientanwendung authentifizieren. Es wird empfohlen, diese Einstellung beizubehalten. In Routern und Firewalls (sofern zwischen Clientanwendung und überwachten Knoten eingerichtet) muss dieser Port offen sein, damit der SFCB CIMOM mit den erforderlichen Anwendungen kommunizieren kann.

Port 5988 (nicht sicher)

Der nicht sichere Port, den SFCB für die Kommunikation via HTTP-Dienste verwendet. Diese Einstellung ist standardmäßig deaktiviert. 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. Diese Einstellung wird nur für das Debuggen von Problemen mit dem CIMOM empfohlen. Nach der Behebung des Problems sollten Sie diese Portoption sofort wieder deaktivieren. In Routern und Firewalls zwischen Clientanwendung und überwachten Knoten muss dieser Port offen sein, damit der SFCB CIMOM mit Anwendungen, für die ein nicht sicherer Zugriff erforderlich ist, kommunizieren kann.

Informationen zur Änderung der Standard-Portzuweisungen finden Sie in *Abschnitt 34.2.3.2, „Ports“*.

34.2.3.3 Authentifizierung

SFCB unterstützt die HTTP-Basisauthentifizierung sowie die Authentifizierung mittels Clientzertifikaten (HTTP über SSL-Verbindungen). Die HTTP-Basisauthentifizierung wird in der SFCB-Konfigurationsdatei (standardmäßig `/etc/sfcb/sfcb.cfg`) durch Einstellung von `doBasicAuth =true` aktiviert. Die SUSE® Linux Enterprise Server-Installation von SFCB unterstützt PAM (Pluggable Authentication Modules); der lokale Root-Benutzer kann sich daher mit den lokalen Root-Benutzerberechtigungen beim SFCB CIMOM authentifizieren.

Wenn die Konfigurationseigenschaft `sslClientCertificate` auf `accept` oder `require` gesetzt ist, fordert der SFCB HTTP-Adapter bei einer Verbindung via HTTP über SSL (HTTPS) ein Zertifikat vom Client an. Wenn `require` eingestellt ist, **muss** der Client ein gültiges Zertifikat bereitstellen (gemäß dem in `sslClientTrustStore` angegebenen Trust Store des Clients). Falls der Client kein solches Zertifikat bereitstellt, wird die Verbindung vom CIM-Server abgelehnt.

Die Einstellung `sslClientCertificate =accept` legt keine eindeutige Authentifizierung fest. Sie ist aber sehr nützlich, wenn sowohl die Authentifizierung mittels Clientzertifikat als auch die Basisauthentifizierung erlaubt sind. Wenn der Client ein gültiges Zertifikat bereitstellen kann, wird eine HTTPS-Verbindung eingerichtet und es findet keine Basisauthentifizierung statt. Wird kein Zertifikat bereitgestellt oder kann dieses nicht verifiziert werden, findet stattdessen die HTTP-Basisauthentifizierung statt.

34.3 SFCB CIMOM-Konfiguration

SFCB ist eine Lightweight-Implementierung des CIM-Servers, die aber ebenfalls umfassend konfiguriert werden kann. Ihr Verhalten wird durch verschiedene Optionen gesteuert. Sie können den SFCB-Server mit drei Methoden steuern:

- durch Einstellen der entsprechenden Umgebungsvariablen
- mittels Kommandozeilenoptionen
- durch Änderungen in seiner Konfigurationsdatei

34.3.1 Umgebungsvariablen

Verschiedene Umgebungsvariablen wirken sich direkt auf das Verhalten von SFCB aus. Zur Übernahme dieser Änderungen müssen Sie den SFCB-Daemon mit **`systemctl restart sfcb`** neu starten.

`PFAD`
: Gibt den Pfad zum Daemon `sfcbd` und den Dienstprogrammen an.

`LD_LIBRARY_PATH`
: Gibt den Pfad zu den sfcb-Laufzeitbibliotheken an. Alternativ können Sie diesen Pfad zur systemweiten Konfigurationsdatei des dynamischen Ladeprogramms `/etc/ld.so.conf` hinzufügen.

`SFCB_PAUSE_PROVIDER`
: Gibt den Namen des Anbieters an. Der SFCB-Server wird nach dem erstmaligen Laden des Anbieters angehalten. Dies gibt Ihnen die Gelegenheit, an den Prozess des Anbieters einen Laufzeitdebugger für die Fehlersuche anzuhängen.

`SFCB_PAUSE_CODEC`
: Gibt den Namen des SFCB-Codecs an (unterstützt aktuell nur `http`. Der SFCB-Server wird nach dem erstmaligen Laden des Codec angehalten. Dies gibt Ihnen die Gelegenheit, an den Prozess einen Laufzeitdebugger anzuhängen.

`SFCB_TRACE`
: Legt die Stufe der Debug-Meldungen für SFCB fest. Gültige Werte sind 0 (keine Debug-Meldungen) bzw. 1 (wichtige Debug-Meldungen) bis 4 (alle Debug-Meldungen). Der Standardwert ist 1.

`SFCB_TRACE_FILE`

SFCB gibt seine Debug-Meldungen standardmäßig über die Standardfehlerausgabe (STDERR) aus. Mit dieser Variablen können Sie eine andere Datei für die Ausgabe der Debug-Meldungen einstellen.

`SBLIM_TRACE`

Legt die Stufe der Debug-Meldungen für SBLIM-Anbieter fest. Gültige Werte sind 0 (keine Debug-Meldungen) bzw. 1 (wichtige Debug-Meldungen) bis 4 (alle Debug-Meldungen).

`SBLIM_TRACE_FILE`

SBLIM-Anbieter geben ihre Debug-Meldungen standardmäßig über STDERR aus. Mit dieser Variablen können Sie eine andere Datei für die Ausgabe der Debug-Meldungen einstellen.

34.3.2 Befehlszeilenoptionen

`sfcbd` Der SFCB-Daemon sfcbd bietet verschiedene Kommandozeilenoptionen, mit denen bestimmte Laufzeitfunktionen ein- und ausgeschaltet werden können. Diese Optionen werden beim Start des SFCB-Daemons eingegeben.

`-c, --config-file=`*`DATEI`*

Beim Start des SFCB-Daemons liest der Daemon seine Konfiguration standardmäßig aus der Datei `/etc/sfcb/sfcb.cfg` ein. Mit dieser Option können Sie eine andere Konfigurationsdatei angeben.

`-d, --daemon`

Führt sfcbd und seine untergeordneten Prozesse im Hintergrund aus.

`-s, --collect-stats`

Aktiviert die Statistikerfassung während der Laufzeit. In diesem Fall werden während der Laufzeit verschiedene sfcbd-Statistiken in die Datei `sfcbStat` im aktuellen Arbeitsverzeichnis geschrieben. Standardmäßig werden keine Statistiken erfasst.

`-l, --syslog-level=`*`PROTOKOLLSTUFE`*

Bestimmt die Ausführlichkeit für die Systemprotokollierung. *`PROTOKOLLSTUFE`* kann LOG_INFO, LOG_DEBUG oder LOG_ERR (Standard) sein.

`-k, --color-trace=`*`LOGLEVEL`*

Druckt die Trace-Ausgabe in unterschiedlichen Farben, was das Debugging erleichtert.

`-t, --trace-components=`*NUMMER*

Aktiviert Trace-Meldungen auf Komponentenebene. *NUMMER* ist dabei ein mit dem logischen Operator OR gebildetes Bitmask-Integer, das festlegt, für welche Komponente ein Trace erstellt werden soll. Mit `-t ?` können Sie eine Liste sämtlicher Komponenten mit ihren Bitmask-Integern abrufen:

```
tux > sfcbd -t ?
---   Traceable Components:     Int       Hex
---             providerMgr:       1  0x0000001
---             providerDrv:       2  0x0000002
---              cimxmlProc:       4  0x0000004
---              httpDaemon:       8  0x0000008
---                 upCalls:      16  0x0000010
---                encCalls:      32  0x0000020
---         ProviderInstMgr:      64  0x0000040
---        providerAssocMgr:     128  0x0000080
---                providers:     256  0x0000100
---              indProvider:     512  0x0000200
---        internalProvider:    1024  0x0000400
---              objectImpl:    2048  0x0000800
---                   xmlIn:    4096  0x0001000
---                  xmlOut:    8192  0x0002000
---                 sockets:   16384  0x0004000
---               memoryMgr:   32768  0x0008000
---                msgQueue:   65536  0x0010000
---              xmlParsing:  131072  0x0020000
---          responseTiming:  262144  0x0040000
---               dbpdaemon:  524288  0x0080000
---                     slp: 1048576  0x0100000
```

Ein nützlicher Wert, der Aufschluss über die internen Funktionen von sfcbd gibt, aber nicht zu viele Meldungen generiert, ist `-t` *2019*.

34.3.3 SFCB-Konfigurationsdatei

SFCB liest seine Laufzeitkonfiguration nach dem Start aus der Konfigurationsdatei `/etc/sfcb/sfcb.cfg` ein. Dieses Verhalten kann beim Starten mit der Option `-c` überschrieben werden.

Die Konfigurationsdatei enthält pro Zeile ein Options-/Wertepaar (`Option` : *WERT*). Diese Datei können Sie in jedem Texteditor bearbeiten, der die Datei in einem von der Umgebung unterstützten Format speichert.

Jede Einstellung in dieser Datei, deren Optionen durch ein Nummernzeichen (#) auskommentiert sind, verwendet die Standardeinstellung.

Die folgende Liste enthält möglicherweise nicht alle Optionen. Die vollständige Liste finden Sie im Inhalt von `/etc/sfcb/sfcb.cfg` und `/usr/share/doc/packages/sblim-sfcb/README`.

34.3.3.1 httpPort

Beschreibung

Gibt die Nummer des lokalen Ports an, den SFCB auf nicht sichere HTTP-Anforderungen von CIM-Clients überwacht. Die Standardeinstellung ist `5988`.

Syntax

`httpPort:` *`PORTNUMMER`*

34.3.3.2 enableHttp

Beschreibung

Legt fest, ob SFCB HTTP-Clientverbindungen akzeptiert. Die Standardeinstellung ist `false`.

Syntax

`enableHttp:` *`OPTION`*

Option	Beschreibung
true	Aktiviert HTTP-Verbindungen.
false	Deaktiviert HTTP-Verbindungen.

34.3.3.3 httpProcs

Beschreibung

Legt die maximale Anzahl gleichzeitiger HTTP-Clientverbindungen fest, ab der neu eingehende HTTP-Anforderungen blockiert werden. Die Standardeinstellung ist `8`.

Syntax

`httpProcs:` *`MAX_ANZAHL_VERBINDUNGEN`*

34.3.3.4 httpUserSFCB, httpUser

Beschreibung

Diese Optionen legen fest, unter welchem Benutzer der HTTP- Server ausgeführt wird. Wenn `httpUserSFCB` auf `true` gesetzt ist, wird HTTP unter demselben Benutzer ausgeführt wie der SFCB-Hauptprozess. Bei `false` wird der für `httpUser` angegebene Benutzername verwendet. Diese Einstellung wird für HTTP- und HTTPS-Server verwendet. `httpUser` *muss* angegeben sein, wenn `httpUserSFCB` auf `false` gesetzt ist. Die Standardeinstellung ist `true`.

Syntax

```
httpUserSFCB: true
```

34.3.3.5 httpLocalOnly

Beschreibung

Gibt an, ob HTTP-Anforderungen auf localhost eingeschränkt werden. Die Standardeinstellung ist `false`.

Syntax

```
httpLocalOnly: false
```

34.3.3.6 httpsPort

Beschreibung

Gibt die Nummer des lokalen Ports an, den SFCB auf HTTPS-Anforderungen von CIM-Clients überwacht. Die Standardeinstellung ist `5989`.

Syntax

```
httpsPort: portnummer
```

34.3.3.7 enableHttps

Beschreibung

Legt fest, ob SFCB HTTPS-Clientverbindungen akzeptiert. Die Standardeinstellung ist `true`.

Syntax

```
enableHttps: option
```

Option	Beschreibung
true	Aktiviert HTTPS-Verbindungen.
false	Deaktiviert HTTPS-Verbindungen.

34.3.3.8 httpsProcs

Beschreibung

Legt die maximale Anzahl gleichzeitiger HTTPS-Clientverbindungen fest, ab der neu eingehende HTTPS-Anforderungen blockiert werden. Die Standardeinstellung ist `8`.

Syntax

`httpsProcs:` *`MAX_ANZAHL_VERBINDUNGEN`*

34.3.3.9 enableInterOp

Beschreibung

Legt fest, ob SFCB den *interop*-Namespace für die Unterstützung von Bezeichnungen bereitstellt. Die Standardeinstellung ist `true`.

Syntax

`enableInterOp:` *`OPTION`*

Option	Beschreibung
true	Aktiviert den interop-Namespace.
false	Deaktiviert den interop-Namespace.

34.3.3.10 provProcs

Beschreibung

Legt die maximale Anzahl gleichzeitiger Anbieterprozesse fest. Wenn nach Erreichen dieser Anzahl eine neu eingehende Anforderung das Laden eines neuen Anbieters erfordert, wird zunächst automatisch einer der vorhandenen Anbieter entladen. Die Standardeinstellung ist `32`.

Syntax

`provProcs:` *`MAX_ANZAHL_PROZESSE`*

34.3.3.11 doBasicAuth

Beschreibung

Legt fest, ob vor dem Akzeptieren einer Anforderung eine Basisauthentifizierung an der Benutzer-ID des Clients durchgeführt wird. Die Standardeinstellung ist `true`, d. h. für den Client wird die Basisauthentifizierung durchgeführt.

Syntax

`doBasicAuth:` *`OPTION`*

Option	Beschreibung
true	Aktiviert die Basisauthentifizierung.
false	Deaktiviert die Basisauthentifizierung.

34.3.3.12 basicAuthLib

Beschreibung

Gibt den Namen der lokalen Bibliothek an. Der SFCB-Server lädt die Bibliothek zur Authentifizierung der Benutzer-ID des Clients. Die Standardeinstellung ist `sfcBasicPAMAuthentication`.

Syntax

`provProcs:` *`MAX_ANZAHL_PROZESSE`*

34.3.3.13 useChunking

Beschreibung

Diese Option aktiviert bzw. deaktiviert die Verwendung von HTTP/HTTPS-„Chunking“. Wenn aktiviert, gibt der Server große Mengen an Antwortdaten an den Client in kleineren „Chunks“ zurück, statt sie im Puffer zu sammeln und auf einmal zurückzusenden. Die Standardeinstellung ist `true`.

Syntax

`useChunking:` *`OPTION`*

Option	Beschreibung
true	Aktiviert HTTP/HTTPS-Daten-Chunking.
false	Deaktiviert HTTP/HTTPS-Daten-Chunking.

34.3.3.14 keepaliveTimeout

Beschreibung

Legt die maximale Zeit in Sekunden fest, die der SFCB-HTTP-Prozess innerhalb einer Verbindung auf die nächste Anforderung wartet, bevor er beendet wird. Bei der Einstellung `0` wird HTTP-Keep-Alive deaktiviert. Die Standardeinstellung ist `0`.

Syntax

`keepaliveTimeout:` *`SEKUNDEN`*

34.3.3.15 keepaliveMaxRequest

Beschreibung

Legt die maximale Anzahl aufeinanderfolgender Anforderungen innerhalb einer Verbindung fest. Bei der Einstellung `0` wird HTTP-Keep-Alive deaktiviert. Die Standardeinstellung ist `10`.

Syntax

`keepaliveMaxRequest:` *`ANZAHL_VERBINDUNGEN`*

34.3.3.16 registrationDir

Beschreibung

Gibt das Registrierungsverzeichnis an, das die Registrierungsdaten der Anbieter, den Staging-Bereich und das statische Repository enthält. Die Standardeinstellung ist `/var/lib/sfcb/registration`.

Syntax

`registrationDir:` *`VERZEICHNIS`*

34.3.3.17 providerDirs

Beschreibung

Gibt eine durch Leerzeichen getrennte Liste mit Verzeichnissen an, die SFCB nach Anbieterbibliotheken durchsucht. Die Standardeinstellung ist `/usr/lib64 /usr/lib64 /usr/lib64/cmpi`.

Syntax

`providerDirs:` *`VERZEICHNIS`*

34.3.3.18 providerSampleInterval

Beschreibung

Legt das Intervall in Sekunden fest, in dem der Anbietermanager nach unbeschäftigten Anbietern sucht. Die Standardeinstellung ist `30`.

Syntax

`providerSampleInterval:` *`SEKUNDEN`*

34.3.3.19 providerTimeoutInterval

Beschreibung

Legt die Zeit in Sekunden fest, nach der ein unbeschäftigter Anbieter vom Anbietermanager entladen wird. Die Standardeinstellung ist `60`.

Syntax

`providerTimeoutInterval:` *`SEKUNDEN`*

34.3.3.20 providerAutoGroup

Beschreibung

Sofern in der Registrierungsdatei des Anbieters keine andere Gruppe angegeben ist und diese Option auf `true` gesetzt ist, werden alle Anbieter der gleichen gemeinsam genutzten Bibliothek im gleichen Prozess ausgeführt.

Syntax

`providerAutoGroup:` *`OPTION`*

Option	Beschreibung
true	Aktiviert die Gruppierung von Anbietern.
false	Deaktiviert die Gruppierung von Anbietern.

34.3.3.21 sslCertificateFilePath

Beschreibung

Gibt den Namen der Datei an, die das Serverzertifikat enthält. Die Datei muss im PEM-Format vorliegen (Privacy Enhanced Mail, RFC 1421 und RFC 1424). Diese Datei ist nur erforderlich, wenn `enableHttps` auf `true` gesetzt ist. Die Standardeinstellung ist `/etc/sfcb/server.pem`.

Syntax

`sslCertificateFilePath:` *`PFAD`*

34.3.3.22 sslKeyFilePath

Beschreibung

Gibt den Namen der Datei an, die den privaten Schlüssel für das Serverzertifikat enthält. Die Datei muss im PEM-Format vorliegen und darf nicht durch einen Passwortsatz geschützt sein. Diese Datei wird nur benötigt, wenn `enableHttps` auf `true` gesetzt ist. Die Standardeinstellung ist `/etc/sfcb/file.pem`.

Syntax

`sslKeyFilePath:` *`PFAD`*

34.3.3.23 sslClientTrustStore

Beschreibung

Gibt den Namen der Datei an, die die von der Zertifizierungsstelle ausgegebenen oder eigensignierten Zertifikate der Clients enthält. Die Datei muss im PEM-Format vorliegen, ist aber nur erforderlich, wenn `sslClientCertificate` auf `accept` oder `require` gesetzt ist. Die Standardeinstellung ist `/etc/sfcb/client.pem`.

Syntax

`sslClientTrustStore:` *`PFAD`*

34.3.3.24 sslClientCertificate

Beschreibung

Legt fest, wie SFCB die Authentifizierung auf Basis von Clientzertifikaten handhabt. Bei `ignore` wird kein Zertifikat vom Client angefordert. Bei `accept` wird zwar ein Zertifikat vom Client angefordert, die Authentifizierung schlägt jedoch nicht fehl, wenn der Client keines bereitstellt. Bei `require` wird die Clientverbindung abgelehnt, wenn der Client kein gültiges Zertifikat bereitstellt. Die Standardeinstellung ist `ignore`.

Syntax

`sslClientCertificate:` *`OPTION`*

Option	Beschreibung
ignore	Deaktiviert die Anforderung eines Clientzertifikats.
Akzeptieren	Aktiviert die Anforderung eines Clientzertifikats.

Option	Beschreibung
	Schlägt jedoch nicht fehl, wenn kein Zertifikat bereitgestellt wird.
require	Lehnt die Clientverbindung ab, wenn kein gültiges Zertifikat bereitgestellt wird.

34.3.3.25 certificateAuthLib

Beschreibung

Gibt den Namen der lokalen Bibliothek an, mit deren Hilfe die Benutzerauthentifizierung auf Basis des Clientzertifikats durchgeführt wird. Die Benutzerauthentifizierung findet nur statt, wenn `sslClientCertificate` nicht auf `ignore` gesetzt ist. Die Standardeinstellung ist `sfcCertificateAuthentication`.

Syntax

`certificateAuthLib:` *`DATEI`*

34.3.3.26 traceLevel

Beschreibung

Legt die Trace-Stufe für SFCB fest. Diese Einstellung kann durch die Umgebungsvariable `SFCB_TRACE_LEVEL` überschrieben werden. Die Standardeinstellung ist `0`.

Syntax

`traceLevel:` *`NUMMER_DER_STUFE`*

34.3.3.27 traceMask

Beschreibung

Legt die Trace-Maske für SFCB fest. Diese Einstellung kann durch die Kommandozeilenoption `--trace-components` überschrieben werden. Die Standardeinstellung ist `0`.

Syntax

`traceMask:` *`MASKE`*

34.3.3.28 traceFile

Beschreibung

Legt die Trace-Datei für SFCB fest. Diese Einstellung kann durch die Umgebungsvariable `SFCB_TRACE_FILE` überschrieben werden. Die Standardeinstellung ist `stderr` (Standardfehlerausgabe).

Syntax

`traceFile:` *`AUSGABE`*

34.4 Erweiterte SFCB-Tasks

In diesem Kapitel werden erweiterte Tasks in Verbindung mit SFCB behandelt. Zu deren Verständnis benötigen Sie grundlegende Kenntnisse des Linux-Dateisystems und Erfahrungen mit der Linux-Kommandozeile. In diesem Kapitel werden folgende Tasks beschrieben:

- Installieren von CMPI-Anbietern
- Testen von SFCB
- Verwenden des CIM-Clients **`wbemcli`**

34.4.1 Installieren von CMPI-Anbietern

Zur Installation eines CMPI-Anbieters müssen Sie seine gemeinsam genutzte Bibliothek in eines der von der Konfigurationsoption `providerDirs` angegebenen Verzeichnisse kopieren (siehe *Abschnitt 34.3.3.17, „providerDirs“*). Außerdem muss der Anbieter korrekt mit den Kommandos **`sfcbstage`** und **`sfcbrepos`** registriert werden.

Das Anbieterpaket ist in der Regel für SFCB vorbereitet. Bei seiner Installation wird also darauf geachtet, dass der Anbieter korrekt registriert wird. Die meisten SBLIM-Anbieter sind für SFCB vorbereitet.

34.4.1.1 Klassenrepository

Das *Klassenrepository* ist der Ort, an dem SFCB Informationen über die CIM-Klassen speichert. Es besteht in der Regel aus einem Verzeichnisbaum mit Namespace-Komponenten. Typische CIM-Namespaces sind `root/cimv2` oder `root/interop`, die in der Regel mit den entsprechenden Verzeichnispfaden des Klassenrepositorys im Dateisystem übereinstimmen:

`/var/lib/sfcb/registration/repository/root/cimv2`

und

`/var/lib/sfcb/registration/repository/root/interop`

Jedes Namespace-Verzeichnis enthält die Datei `classSchemas`. Die Datei enthält eine kompilierte binäre Darstellung aller CIM-Klassen, die unter diesem Namespace registriert sind. Außerdem enthält sie die erforderlichen Informationen über deren CIM-Unterklassen.

Darüber hinaus kann jedes Namespace-Verzeichnis eine Datei mit dem Namen `qualifiers` enthalten, die alle Qualifizierer des Namespace enthält. Beim Neustart von sfcbd untersucht der Klassenanbieter das Verzeichnis `/var/lib/sfcb/registration/repository/` und seine Unterverzeichnisse, um festzustellen, welche Namespaces registriert sind. Danach werden die `classSchemas`-Dateien entschlüsselt und die Klassenhierarchien der einzelnen Namespaces erstellt.

34.4.1.2 Hinzufügen neuer Klassen

SFCB kann CIM-Klassen nicht online ändern. Zum Hinzufügen, Ändern oder Entfernen von Klassen müssen Sie offline sein und den SFCB-Dienst anschließend mit **`systemctl restart sfcb`** neu starten, damit die Änderungen registriert werden.

Zum Speichern der Klassen- und Registrierungsdaten der Anbieter verwendet SFCB einen Zwischenspeicher, den so genannten *Staging-Bereich*. Auf SUSE® Linux Enterprise Server-Systemen ist dies die Verzeichnisstruktur unter `/var/lib/sfcb/stage/`.

Zum Hinzufügen eines neuen Anbieters führen Sie die folgenden Schritte aus:

- Kopieren Sie die Definitionsdateien mit den Anbieterklassen in das Unterverzeichnis `./mofs` des Staging-Verzeichnisses (`/var/lib/sfcb/stage/mofs`).
- Kopieren Sie die Registrierungsdatei mit den Namen der Klassen, dem Anbietertyp und dem Namen der ausführbaren Bibliotheksdatei in das Unterverzeichnis `./regs`.

Das Staging-Verzeichnis enthält zwei Standard-„mof“-Dateien (Klassendefinitionen): `indication.mof` und `interop.mof`. Die MOF-Dateien unter dem Root-Staging-Verzeichnis `/var/lib/sfcb/stage/mofs` müssen nach der Ausführung des Kommandos `sfcbrepos` in jeden Namespace kopiert werden. Die Datei `interop.mof` muss nur in den *interop*-Namespace kompiliert werden.

Das Verzeichnislayout kann dann wie folgt aussehen:

```
tux > ls /var/lib/sfcb/stage
default.reg  mofs  regs
```

```
tux > ls /var/lib/sfcb/stage/mofs
indication.mof  root
```

```
tux > ls /var/lib/sfcb/stage/mofs/root
cimv2  interop  suse  virt
```

```
tux > ls -1 /var/lib/sfcb/stage/mofs/root/cimv2 | less
Linux_ABIParameter.mof
Linux_BaseIndication.mof
Linux_Base.mof
Linux_DHCPElementConformsToProfile.mof
Linux_DHCPEntity.mof
[..]
OMC_StorageSettingWithHints.mof
OMC_StorageVolumeDevice.mof
OMC_StorageVolume.mof
OMC_StorageVolumeStorageSynchronized.mof
OMC_SystemStorageCapabilities.mof
```

```
tux > ls -1 /var/lib/sfcb/stage/mofs/root/interop
```

```
ComputerSystem.mof
ElementConformsToProfile.mof
HostSystem.mof
interop.mof
Linux_DHCPElementConformsToProfile.mof
[..]
OMC_SMIElementSoftwareIdentity.mof
OMC_SMISubProfileRequiresProfile.mof
OMC_SMIVolumeManagementSoftware.mof
ReferencedProfile.mof
RegisteredProfile.mof
```

```
tux > ls -1 /var/lib/sfcb/stage/regs
AllocationCapabilities.reg
Linux_ABIParameter.reg
Linux_BaseIndication.reg
Linux_DHCPGlobal.reg
Linux_DHCPRegisteredProfile.reg
[..]
OMC_Base.sfcb.reg
OMC_CopyServices.sfcb.reg
OMC_PowerManagement.sfcb.reg
OMC_Server.sfcb.reg
RegisteredProfile.reg
```

```
tux > cat /var/lib/sfcb/stage/regs/Linux_DHCPRegisteredProfile.reg
[Linux_DHCPRegisteredProfile]
   provider: Linux_DHCPRegisteredProfileProvider
   location: cmpiLinux_DHCPRegisteredProfile
   type: instance
   namespace: root/interop
#
[Linux_DHCPElementConformsToProfile]
   provider: Linux_DHCPElementConformsToProfileProvider
   location: cmpiLinux_DHCPElementConformsToProfile
   type: instance association
   namespace: root/cimv2
#
[Linux_DHCPElementConformsToProfile]
   provider: Linux_DHCPElementConformsToProfileProvider
   location: cmpiLinux_DHCPElementConformsToProfile
   type: instance association
   namespace: root/interop
```

SFCB verwendet für jeden Anbieter eine angepasste Anbieterregistrierungsdatei.

Anmerkung: Registrierungsdateien von SBLIM-Anbietern

Alle SBLIM-Anbieter der SBLIM-Website enthalten bereits eine Registrierungsdatei, die zur Generierung der für SFCB benötigten .reg-Datei verwendet wird.

Das Format der SFCB-Registrierungsdatei sieht wie folgt aus:

```
[<class-name>]
   provider: <provide-name>
   location: <library-name>
   type: [instance] [association] [method] [indication]
   group: <group-name>
   unload: never
   namespace: <namespace-for-class> ...
```

wobei:

`<klassenname>`
: Der Name der CIM-Klasse (erforderlich)

`<anbietername>`
: Der Name des CMPI-Anbieters (erforderlich)

`<standortname>`
: Der Name der Anbieterbibliothek (erforderlich)

`type`
: Der Typ des Anbieters (erforderlich). Hier kann es sich um jede Kombination der folgenden Typen handeln: `Instanz`, `Verknüpfung`, `Methode` oder `Bezeichnung`.

`<gruppenname>`
: Zur Minimierung der benötigten Laufzeitressourcen können mehrere Anbieter zu Gruppen zusammengefasst und unter einem einzigen Prozess ausgeführt werden. Alle unter dem gleichen <gruppennamen> registrierten Anbieter werden unter dem gleichen Prozess ausgeführt. Standardmäßig wird jeder Anbieter als separater Prozess ausgeführt.

`unload`
: Legt die Richtlinie zum Entladen des Anbieters fest. Zur Zeit wird nur die Option `never` (nie) unterstützt. Es wird also nicht überprüft, ob der Anbieter leerläuft, er wird daher auch nicht entladen. Standardmäßig wird ein Anbieter dann entladen, wenn er das in der Konfigurationsdatei angegebene Leerlaufzeitlimit überschreitet.

`namespace`

Eine Liste der Namespaces, für die dieser Anbieter ausgeführt werden kann. Die Liste ist erforderlich, auch wenn hier für die meisten Anbieter `root/cimv2` angegeben werden kann.

Wenn sich alle Klassendefinitionen und Anbieterregistrierungsdateien im Staging-Bereich befinden, müssen Sie das SFCB-Klassenrepository mit dem Kommando **`sfcbrepos`** `-f` neu erstellen.

Auf diese Weise können Sie Klassen hinzufügen, ändern oder entfernen. Nach der Neuerstellung des Klassenrepositorys müssen Sie SFCB mit dem Kommando **`systemctl restart sfcb`** neu starten.

Als Alternative enthält das SFCB-Paket ein Dienstprogramm, mit dem die MOF-Klassen- und Registrierungsdateien der Anbieter in die richtigen Verzeichnisse des Staging-Bereichs kopiert werden können.

`sfcbstage` `-r [anbieter.reg] [klasse1.mof] [klasse2.mof] ...`

Auch nach Ausführung dieses Kommandos müssen Sie das Klassenrepository neu erstellen und den SFCB-Dienst neu starten.

34.4.2 Testen von SFCB

Das SFCB-Paket enthält die beiden Testskripte **`wbemcat`** und **`xmltest`**.

`wbemcat` sendet CIM-XML-Raw-Daten via HTTP-Protokoll an den angegebenen SFCB-Host (standardmäßig „localhost“), der Port 5988 überwacht. Danach zeigt es die zurückgegebenen Ergebnisse an. Die folgende Datei enthält die CIM-XML-Darstellung einer EnumerateClasses-Standardanforderung:

```
<?xml version="1.0" encoding="utf-8"?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
  <MESSAGE ID="4711" PROTOCOLVERSION="1.0">
    <SIMPLEREQ>
      <IMETHODCALL NAME="EnumerateClasses">
        <LOCALNAMESPACEPATH>
          <NAMESPACE NAME="root"/>
          <NAMESPACE NAME="cimv2"/>
        </LOCALNAMESPACEPATH>
        <IPARAMVALUE NAME="ClassName">
          <CLASSNAME NAME=""/>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="DeepInheritance">
          <VALUE>TRUE</VALUE>
```

```
        </IPARAMVALUE>
        <IPARAMVALUE NAME="LocalOnly">
          <VALUE>FALSE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="IncludeQualifiers">
          <VALUE>FALSE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="IncludeClassOrigin">
          <VALUE>TRUE</VALUE>
        </IPARAMVALUE>
      </IMETHODCALL>
    </SIMPLEREQ>
  </MESSAGE>
</CIM>
```

Wenn diese Anforderung an den SFCB CIMOM gesendet wird, gibt sie eine Liste aller unterstützten Klassen zurück, für die Anbieter registriert sind. Sie speichern die Datei nun zum Beispiel unter dem Dateinamen `cim_xml_test.xml`.

```
tux > wbemcat cim_xml_test.xml | less
HTTP/1.1 200 OK
Content-Type: application/xml; charset="utf-8"
Content-Length: 337565
Cache-Control: no-cache
CIMOperation: MethodResponse

<?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0">
<SIMPLERSP>
<IMETHODRESPONSE NAME="EnumerateClasses">
[..]
<CLASS NAME="Linux_DHCPParamsForEntity" SUPERCLASS="CIM_Component">
<PROPERTY.REFERENCE NAME="GroupComponent" REFERENCECLASS="Linux_DHCPEntity">
</PROPERTY.REFERENCE>
<PROPERTY.REFERENCE NAME="PartComponent" REFERENCECLASS="Linux_DHCPParams">
</PROPERTY.REFERENCE>
</CLASS>
</IRETURNVALUE>
</IMETHODRESPONSE>
</SIMPLERSP>
</MESSAGE>
</CIM>
```

Welche Klassen aufgelistet werden, richtet sich nach den auf Ihrem System installierten Anbietern.

Auch das zweite Skript **xmltest** sendet eine CIM-XML-Raw-Testdatei an den SFCB CIMOM. Danach vergleicht es die zurückgegebenen Ergebnisse mit einer zuvor gespeicherten „OK“-Ergebnisdatei. Falls noch keine passende „OK“-Datei vorhanden ist, wird diese für den späteren Gebrauch erstellt:

```
tux > xmltest cim_xml_test.xml
Running test cim_xml_test.xml ... OK
        Saving response as cim_xml_test.OK
root # xmltest cim_xml_test.xml
Running test cim_xml_test.xml ... Passed
```

34.4.3 CIM-Kommandozeilenclient: wbemcli

Neben **wbemcat** und **xmltest** enthält das SBLIM-Projekt den erweiterten CIM-Kommandozeilenclient **wbemcli**. Der Client sendet CIM-Anforderungen an den SFCB-Server und zeigt die zurückgegebenen Ergebnisse an. Er ist unabhängig von der CIMOM-Bibliothek und kann mit allen WBEM-konformen Implementierungen verwendet werden.

Wenn Sie zum Beispiel alle von den auf Ihrem SFCB registrierten SBLIM-Anbietern implementierten Klassen auflisten wollen, senden Sie eine „EnumerateClasses“-Anforderung (siehe Beispiel) an den SFCB:

```
tux > wbemcli -dx ec http://localhost/root/cimv2
To server: <?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0"><SIMPLEREQ><IMETHODCALL \
    NAME="EnumerateClasses"><LOCALNAMESPACEPATH><NAMESPACE NAME="root"> \
    </NAMESPACE><NAMESPACE NAME="cimv2"></NAMESPACE> \
    </LOCALNAMESPACEPATH>
<IPARAMVALUE NAME="DeepInheritance"><VALUE>TRUE</VALUE> \
    </IPARAMVALUE>
<IPARAMVALUE NAME="LocalOnly"><VALUE>FALSE</VALUE></IPARAMVALUE>
<IPARAMVALUE NAME="IncludeQualifiers"><VALUE>FALSE</VALUE> \
    </IPARAMVALUE>
<IPARAMVALUE NAME="IncludeClassOrigin"><VALUE>TRUE</VALUE> \
    </IPARAMVALUE>
</IMETHODCALL></SIMPLEREQ>
</MESSAGE></CIM>
From server: Content-Type: application/xml; charset="utf-8"
From server: Content-Length: 337565
From server: Cache-Control: no-cache
From server: CIMOperation: MethodResponse
From server: <?xml version="1.0" encoding="utf-8" ?>
```

```
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0">
<SIMPLERSP>
<IMETHODRESPONSE NAME="EnumerateClasses">
<IRETURNVALUE>
<CLASS NAME="CIM_ResourcePool" SUPERCLASS="CIM_LogicalElement">
<PROPERTY NAME="Generation" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="ElementName" TYPE="string">
</PROPERTY>
<PROPERTY NAME="Description" TYPE="string">
</PROPERTY>
<PROPERTY NAME="Caption" TYPE="string">
</PROPERTY>
<PROPERTY NAME="InstallDate" TYPE="datetime">
</PROPERTY>
[..]
<CLASS NAME="Linux_ReiserFileSystem" SUPERCLASS="CIM_UnixLocalFileSystem">
<PROPERTY NAME="FSReservedCapacity" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="TotalInodes" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="FreeInodes" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="ResizeIncrement" TYPE="uint64">
<VALUE>0</VALUE>
</PROPERTY>
<PROPERTY NAME="IsFixedSize" TYPE="uint16">
<VALUE>0</VALUE>
</PROPERTY>
[..]
```

Die Option `-dx` zeigt den tatsächlichen XML-Text an, der von **`wbemcli`** an den SFCB gesendet wurde, und den tatsächlich zurückgegebenen XML-Text. Im oben gezeigten Beispiel wurde als erste von zahlreichen Klassen `CIM_ResourcePool` zurückgegeben, gefolgt von `Linux_ReiserFileSystem`. Ähnliche Einträge werden auch für alle anderen registrierten Klassen zurückgegeben.

Ohne die Option `-dx` zeigt **`wbemcli`** lediglich eine kompakte Darstellung der zurückgegebenen Daten an:

```
tux > wbemcli ec http://localhost/root/cimv2
localhost:5988/root/cimv2:CIM_ResourcePool Generation=,ElementName=, \
    Description=,Caption=,InstallDate=,Name=,OperationalStatus=, \
    StatusDescriptions=,Status=,HealthState=,PrimaryStatus=, \
    DetailedStatus=,OperatingStatus=,CommunicationStatus=,InstanceID=, \
```

```
    PoolID=,Primordial=,Capacity=,Reserved=,ResourceType=, \
    OtherResourceType=,ResourceSubType=, \AllocationUnits=
localhost:5988/root/cimv2:Linux_ReiserFileSystem FSReservedCapacity=, \
    TotalInodes=,FreeInodes=,ResizeIncrement=,IsFixedSize=,NumberOfFiles=, \
    OtherPersistenceType=,PersistenceType=,FileSystemType=,ClusterSize=, \
    MaxFileNameLength=,CodeSet=,CasePreserved=,CaseSensitive=, \
    CompressionMethod=,EncryptionMethod=,ReadOnly=,AvailableSpace=, \
    FileSystemSize=,BlockSize=,Root=,Name=,CreationClassName=,CSName=, \
    CSCreationClassName=,Generation=,ElementName=,Description=,Caption=, \
    InstanceID=,InstallDate=,OperationalStatus=,StatusDescriptions=, \
    Status=,HealthState=,PrimaryStatus=,DetailedStatus=,OperatingStatus= \
    ,CommunicationStatus=,EnabledState=,OtherEnabledState=,RequestedState= \
    ,EnabledDefault=,TimeOfLastStateChange=,AvailableRequestedStates=, \
    TransitioningToState=,PercentageSpaceUse=
    [..]
```

34.5 Weiterführende Informationen

WEITERE INFORMATIONEN ZU WBEM UND SFCB FINDEN SIE AUF FOLGENDEN WEBSITES:

http://www.dmtf.org

Website der Distributed Management Task Force

http://www.dmtf.org/standards/wbem/

Website zu Web-Based Enterprise Management (WBEM)

http://www.dmtf.org/standards/cim/

Website zu Common Information Model (CIM)

http://sblim.wiki.sourceforge.net/

Website zu Standards Based Linux Instrumentation (SBLIM)

http://sblim.sourceforge.net/wiki/index.php/Sfcb

Website zu Small Footprint CIM Broker (SFCB)

http://sblim.sourceforge.net/wiki/index.php/Providers

SBLIM-Anbieterpakete

V Mobile Computer

35 Mobile Computernutzung mit Linux 582

36 Verwendung von NetworkManager 595

37 Energieverwaltung 607

35 Mobile Computernutzung mit Linux

Die mobile Computernutzung wird meist mit Notebooks, PDAs, Mobiltelefonen (und dem Datenaustausch zwischen diesen Geräten) in Verbindung gebracht. An Notebooks oder Desktop-Systeme können aber auch mobile Hardware-Komponenten, wie externe Festplatten, Flash-Laufwerke und Digitalkameras, angeschlossen sein. Ebenso zählen zahlreiche Software-Komponenten zu den Bestandteilen mobiler Computerszenarien und einige Anwendungen sind sogar speziell für die mobile Verwendung vorgesehen.

35.1 Notebooks

Die Hardware von Notebooks unterscheidet sich von der eines normalen Desktopsystems. Dies liegt daran, dass Kriterien wie Austauschbarkeit, Platzanforderungen und Energieverbrauch berücksichtigt werden müssen. Die Hersteller von mobiler Hardware haben Standardschnittstellen wie PCMCIA (Personal Computer Memory Card International Association), Mini PCI und Mini PCIe entwickelt, die zur Erweiterung der Hardware von Laptops verwendet werden können. Dieser Standard bezieht sich auf Speicherkarten, Netzwerkschnittstellenkarten und externe Festplatten.

35.1.1 Energieeinsparung

Durch die Integration von energieoptimierten Systemkomponenten bei der Herstellung von Notebooks erhöht sich die Eignung der Geräte für die Verwendung ohne Zugang zum Stromnetz. Ihr Beitrag zur Energieeinsparung ist mindestens so wichtig wie der des Betriebssystems. SUSE® Linux Enterprise Server unterstützt verschiedene Methoden, die den Energieverbrauch eines Notebooks steuern und sich bei Akkubetrieb auf die Betriebsdauer auswirken. In der folgenden Liste werden die Möglichkeiten zur Energieeinsparung in absteigender Reihenfolge ihrer Wirksamkeit angegeben:

- Drosselung der CPU-Geschwindigkeit.
- Ausschalten der Anzeigebeleuchtung während Pausen.

- Manuelle Anpassung der Anzeigebeleuchtung.
- Ausstecken nicht verwendeter, Hotplug-fähiger Zubehörteile (USB-CD-ROM, externe Maus, nicht verwendete PCMCIA-Karten usw.).
- Ausschalten der Festplatte im Ruhezustand.

Ausführliche Hintergrundinformationen zur Energieverwaltung in SUSE Linux Enterprise Server finden Sie in *Kapitel 37, Energieverwaltung*.

35.1.2 Integration in unterschiedlichen Betriebsumgebungen

Ihr System muss sich an unterschiedliche Betriebsumgebungen anpassen können, wenn es für mobile Computernutzung verwendet werden soll. Viele Dienste hängen von der Umgebung ab und die zugrunde liegenden Clients müssen neu konfiguriert werden. SUSE Linux Enterprise Server übernimmt diese Aufgabe für Sie.

ABBILDUNG 35.1 INTEGRIEREN EINES MOBILEN COMPUTERS IN EINE BESTEHENDE UMGEBUNG

Bei einem Notebook beispielsweise, das zwischen einem kleinen Heimnetzwerk zu Hause und einem Firmennetzwerk hin und her pendelt, sind folgende Dienste betroffen:

Netzwerk

Dazu gehören IP-Adresszuweisung, Namensauflösung, Internet-Konnektivität und Konnektivität mit anderen Netzwerken.

Druckvorgang

Die aktuelle Datenbank der verfügbaren Drucker und ein verfügbarer Druckserver (abhängig vom Netzwerk) müssen vorhanden sein.

E-Mail und Proxys

Wie beim Drucken muss die Liste der entsprechenden Server immer aktuell sein.

X (Grafische Umgebung)

Wenn Ihr Notebook zeitweise an einen Projektor oder einen externen Monitor angeschlossen ist, müssen verschiedene Anzeigekonfigurationen verfügbar sein.

SUSE Linux Enterprise Server bietet mehrere Möglichkeiten, Laptops in vorhandene Betriebsumgebungen zu integrieren:

NetworkManager

NetworkManager bietet die Möglichkeit, einfach und automatisch zwischen Netzwerkumgebungen oder unterschiedlichen Netzwerktypen, wie mobiles Breitband (GPRS, EDGE oder 3G), WLAN und Ethernet zu wechseln. NetworkManager unterstützt die WEP- und WPA-PSK-Verschlüsselung in drahtlosen LANs. Auch DFÜ-Verbindungen werden unterstützt. Der GNOME-Desktop bietet ein Frontend für NetworkManager. Weitere Informationen finden Sie unter *Abschnitt 36.3, „Konfigurieren von Netzwerkverbindungen“*.

TABELLE 35.1 ANWENDUNGSBEISPIELE FÜR DEN NETWORKMANAGER

Computer	Verwendung des NetworkManagers
Der Computer ist ein Notebook.	Ja
Der Computer wird mit verschiedenen Netzwerken verbunden.	Ja
Der Computer stellt Netzwerkdienste bereit (z. B. DNS oder DHCP).	Nein
Der Computer hat eine statische IP-Adresse.	Nein

Verwenden Sie die Werkzeuge von YaST zur Konfiguration der Netzwerkverbindungen, wenn die Netzwerkkonfiguration nicht automatisch vom NetworkManager übernommen werden soll.

Tipp: DNS-Konfiguration und verschiedene Arten von Netzwerkverbindungen

Wenn Sie oft mit Ihrem Laptop reisen und zwischen verschiedenen Arten von Netzwerkverbindungen wechseln, funktioniert NetworkManager gut, wenn alle DNS-Adressen korrekt mit DHCP zugewiesen wurden. Wenn einige Verbindungen statische DNS-Adressen verwenden, fügen Sie sie zur Option `NETCONFIG_DNS_STATIC_SERVERS` in `/etc/sysconfig/network/config` hinzu.

SLP

Das Service Location Protocol (SLP) vereinfacht die Verbindung eines Notebooks mit einem bestehenden Netzwerk. Ohne SLP benötigt der Administrator eines Notebooks normalerweise detaillierte Kenntnisse über die im Netzwerk verfügbaren Dienste. SLP sendet die Verfügbarkeit eines bestimmten Diensttyps an alle Clients in einem lokalen Netzwerk. Anwendungen, die SLP unterstützen, können die von SLP weitergeleiteten Informationen verarbeiten und automatisch konfiguriert werden. SLP kann auch zur Installation eines Systems verwendet werden und minimiert dabei den Aufwand bei der Suche nach einer geeigneten Installationsquelle. Weitere Informationen zu SLP finden Sie unter *Kapitel 30, SLP*.

35.1.3 Software-Optionen

Bei der mobilen Nutzung gibt es verschiedene Aufgabenbereiche, die von dedizierter Software abgedeckt werden: Systemüberwachung (insbesondere der Ladezustand des Akkus), Datensynchronisierung sowie drahtlose Kommunikation mit angeschlossenen Geräten und dem Internet. In den folgenden Abschnitten werden die wichtigsten Anwendungen behandelt, die SUSE Linux Enterprise Server für jede Aufgabe bietet.

35.1.3.1 Systemüberwachung

SUSE Linux Enterprise Server umfasst zwei Werkzeuge zur Systemüberwachung:

Energieverwaltung

Power-Management ist eine Anwendung für die Einstellung der mit der Energieeinsparung zusammenhängenden Verhaltensweisen des GNOME-Desktops. Diese Anwendung finden Sie in der Regel unter *Rechner* › *Kontrollzentrum* › *System* › *Power-Management*.

Systemmonitor

Der *Systemmonitor* fasst messbare Systemparameter in einer Überwachungsumgebung zusammen. Die Informationen werden standardmäßig auf drei Karteireitern ausgegeben. *Processes* (Prozesse) enthält detaillierte Informationen zu den aktuell ausgeführten Prozessen, wie CPU-Last, Speicherauslastung oder Prozess-ID und Priorität. Die Präsentation und Filterung der erfassten Daten kann angepasst werden – um einen neuen Typ von Prozessinformationen hinzuzufügen, klicken Sie mit der linken Maustaste auf die Kopfzeile der Tabelle, und wählen Sie die Spalte aus, die Sie zur Ansicht hinzufügen oder daraus ausblenden möchten. Es ist auch möglich, verschiedene Systemparameter auf verschiedenen Datenseiten zu überwachen oder die Daten von mehreren Computern parallel über das Netzwerk zu sammeln. Auf dem Karteireiter *Ressourcen* wird die CPU-, Arbeitsspeicher- und Netzwerkauslastung grafisch dargestellt, und der Karteireiter *Dateisystem* enthält eine Liste aller Partitionen und ihrer Nutzung.

35.1.3.2 Datensynchronisierung

Beim ständigen Wechsel zwischen der Arbeit auf einem mobilen Computer, der vom Netzwerk getrennt ist, und der Arbeit an einer vernetzten Arbeitsstation in einem Büro müssen die verarbeiteten Daten stets auf allen Instanzen synchronisiert sein. Dazu gehören E-Mail-Ordner, Verzeichnisse und einzelne Dateien, die für die Arbeit unterwegs und im Büro vorliegen müssen. Die Lösung sieht für beide Fälle folgendermaßen aus:

Synchronisieren von E-Mail

Verwenden eines IMAP-Kontos zum Speichern der E-Mails im Firmennetzwerk. Greifen Sie dann auf die E-Mails vom Arbeitsplatzrechner aus über einen beliebigen, nicht verbundenen IMAP-fähigen E-Mail-Client wie Mozilla Thunderbird oder Evolution zu, wie im *Buch „GNOME-Benutzerhandbuch"* beschrieben. Der E-Mail-Client muss so konfiguriert sein, dass für `Gesendete Nachrichten` immer derselbe Ordner aufgerufen wird. Dadurch wird gewährleistet, dass nach Abschluss der Synchronisierung alle Nachrichten mit den zugehörigen Statusinformationen verfügbar sind. Verwenden Sie zum Senden von Nachrichten einen im Mail-Client implementierten SMTP-Server anstatt des systemweiten MTA-Postfix oder Sendmail, um zuverlässige Rückmeldungen über nicht gesendete Mail zu erhalten.

Synchronisieren von Dateien und Verzeichnissen

Es gibt mehrere Dienstprogramme, die sich für die Synchronisierung von Daten zwischen Notebook und Arbeitsstation eignen. Am meisten verwendet wird ein Kommandozeilen-Tool namens `rsync`. Weitere Informationen hierzu finden Sie auf dessen man-Seite (`man 1 rsync`).

35.1.3.3 Drahtlose Kommunikation: WLAN

WLAN weist unter diesen drahtlosen Technologien die größte Reichweite auf und ist daher das einzige System, das für den Betrieb großer und zuweilen sogar räumlich getrennter Netzwerke geeignet ist. Einzelne Computer können untereinander eine Verbindung herstellen und so ein unabhängiges drahtloses Netzwerk bilden oder auf das Internet zugreifen. Als *Zugriffspunkte* bezeichnete Geräte können als Basisstationen für WLAN-fähige Geräte und als Zwischengeräte für den Zugriff auf das Internet fungieren. Ein mobiler Benutzer kann zwischen verschiedenen Zugriffspunkten umschalten, je nachdem, welcher Zugriffspunkt die beste Verbindung aufweist. Wie bei der Mobiltelefonie steht WLAN-Benutzern ein großes Netzwerk zur Verfügung, ohne dass sie für den Zugriff an einen bestimmten Standort gebunden sind.

WLAN-Karten kommunizieren über den 802.11-Standard, der von der IEEE-Organisation festgelegt wurde. 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 (siehe *Tabelle 35.2, „Überblick über verschiedene WLAN-Standards"*). Zusätzlich implementieren viele Firmen Hardware mit herstellerspezifischen Funktionen oder Funktionsentwürfen.

TABELLE 35.2 ÜBERBLICK ÜBER VERSCHIEDENE WLAN-STANDARDS

Name (802.11)	Frequenz (GHz)	Maximale Übertragungsrate (MBit/s)	Hinweis
a	5	54	Weniger anfällig für Interferenzen
b	2.4	11	Weniger üblich
g	2.4	54	Weit verbreitet, abwärtskompatibel mit 11b

Name (802.11)	Frequenz (GHz)	Maximale Übertragungsrate (MBit/s)	Hinweis
n	2.4 und/oder 5	300	Common
ac	5	bis zu etwa 865	Weite Verbreitung bis 2015 erwartet
ad	60	bis zu etwa 7000	2012 veröffentlicht, derzeit weniger gebräuchlich; in SUSE Linux Enterprise Server nicht unterstützt

802.11-Legacy-Karten werden in SUSE® Linux Enterprise Server nicht unterstützt. Die meisten Karten mit 802.11 a/b/g/n werden unterstützt. Neuere Karten entsprechen in der Regel dem Standard 802.11n, Karten, die 802.11g verwenden, sind jedoch noch immer erhältlich.

35.1.3.3.1 Betriebsmodi

Bei der Arbeit mit drahtlosen Netzwerken werden verschiedene Verfahren und Konfigurationen verwendet, um schnelle, qualitativ hochwertige und sichere Verbindungen herzustellen. In der Regel arbeitet Ihre WLAN-Karte im *Modus „Verwaltet“*. Für die unterschiedlichen Betriebsarten sind allerdings unterschiedliche Einrichtungen erforderlich. Drahtlose Netzwerke lassen sich in vier Netzwerkmodi klassifizieren:

Modus „Verwaltet“ (Infrastrukturmodus) über Zugriffspunkt (Standardmodus)

Verwaltete Netzwerke verfügen über ein verwaltendes Element: den Zugriffspunkt In diesem Modus (auch als Infrastrukturmodus oder Standardmodus bezeichnet) laufen alle Verbindungen der WLAN-Stationen im Netzwerk über den Zugriffspunkt, der auch als Verbindung zu einem Ethernet fungieren kann. Um sicherzustellen, dass nur autorisierte Stationen eine Verbindung herstellen können, werden verschiedene Authentifizierungsverfahren (WPA usw.) verwendet. Dies ist zudem der Hauptmodus, bei dem der niedrigste Energieverbrauch entsteht.

Ad-hoc-Modus (Peer-To-Peer-Netzwerk)

Ad-hoc-Netzwerke weisen keinen Zugriffspunkt auf. Die Stationen kommunizieren direkt miteinander, daher ist ein Ad-hoc-Netzwerk in der Regel langsamer als ein verwaltetes Netzwerk. Übertragungsbereich und Anzahl der teilnehmenden Stationen sind jedoch in Ad-hoc-Netzwerken stark eingeschränkt. Sie unterstützen auch keine WPA-Authentifizierung. Nicht alle Karten können außerdem den Ad-hoc-Modus zuverlässig unterstützen.

Master-Modus

Im Master-Modus fungiert die WLAN-Karte als Zugriffspunkt (sofern die Karte diesen Modus unterstützt). Details zu Ihrer WLAN-Karte finden Sie unter http://linux-wless.passys.nl.

Mesh-Modus

WLAN-Mesh-Netzwerke sind in einer *Mesh-Topologie* angeordnet. Die Verbindung eines WLAN-Mesh-Netzwerks wird auf alle WLAN-Mesh-*Knoten* verteilt. Jeder Knoten, der zu diesem Netzwerk gehört, ist mit anderen Knoten verbunden, so dass die Verbindung gemeinsam von allen Knoten genutzt wird (und dies durchaus auch in einem großen Bereich). (In SLE12 nicht unterstützt.)

35.1.3.3.2 Authentifizierung

Da ein drahtloses Netzwerk wesentlich leichter abgehört und manipuliert werden kann als ein Kabelnetzwerk, beinhalten die verschiedenen Standards Authentifizierungs- und Verschlüsselungsmethoden.

Ältere WLAN-Karten unterstützen lediglich WEP (Wired Equivalent Privacy). Da sich WEP jedoch als unsicher herausgestellt hat, hat die WLAN-Branche die Erweiterung WPA definiert, bei dem die Schwächen von WEP ausgemerzt sein sollen. WPA (teilweise synonym mit WPA2) sollte als standardmäßige Authentifizierungsmethode genutzt werden.

In der Regel kann der Benutzer die Authentifizierungsmethode nicht wählen. Wird eine Karte beispielsweise im Modus „Verwaltet“ betrieben, so wird die Authentifizierung durch den Zugriffspunkt festgelegt. In NetworkManager wird die Authentifizierungsmethode angezeigt.

35.1.3.3.3 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 nicht zu verschlüsseln.

Einige Hersteller haben „Dynamic WEP“ implementiert, das nicht dem Standard entspricht. Es funktioniert exakt wie WEP und weist dieselben Schwächen auf, außer dass der Schlüssel regelmäßig von einem Schlüsselverwaltungsdienst geändert wird.

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.

35.1.3.4 Drahtlose Kommunikation: Bluetooth

Bluetooth weist das breiteste Anwendungsspektrum von allen drahtlosen Technologien auf. Es kann, ebenso wie IrDA, für die Kommunikation zwischen Computern (Notebooks) und PDAs oder Mobiltelefonen verwendet werden. Außerdem kann es zur Verbindung mehrerer Computer innerhalb des zulässigen Bereichs verwendet werden. Des Weiteren wird Bluetooth zum Anschluss drahtloser Systemkomponenten, beispielsweise Tastatur oder Maus, verwendet. Die

Reichweite dieser Technologie reicht jedoch nicht aus, um entfernte Systeme über ein Netzwerk zu verbinden. WLAN ist die optimale Technologie für die Kommunikation durch physische Hindernisse, wie Wände.

35.1.3.5 Drahtlose Kommunikation: IrDA

IrDA ist die drahtlose Technologie mit der kürzesten Reichweite. Beide Kommunikationspartner müssen sich in Sichtweite voneinander befinden. Hindernisse, wie Wände, können nicht überwunden werden. Eine mögliche Anwendung von IrDA ist die Übertragung einer Datei von einem Notebook auf ein Mobiltelefon. Die kurze Entfernung zwischen Notebook und Mobiltelefon wird mit IrDa überbrückt. Die Langstreckenübertragung der Datei an den Empfänger erfolgt über das mobile Netzwerk. Ein weiterer Anwendungsbereich von IrDA ist die drahtlose Übertragung von Druckaufträgen im Büro.

35.1.4 Datensicherheit

Idealerweise schützen Sie die Daten auf Ihrem Notebook mehrfach gegen unbefugten Zugriff. Mögliche Sicherheitsmaßnahmen können in folgenden Bereichen ergriffen werden:

Schutz gegen Diebstahl

Schützen Sie Ihr System stets nach Möglichkeit gegen Diebstahl. Im Einzelhandel ist verschiedenes Sicherheitszubehör, wie beispielsweise Ketten, verfügbar.

Komplexe Authentifizierung

Verwenden Sie die biometrische Authentifizierung zusätzlich zur standardmäßigen Authentifizierung über Anmeldung und Passwort. SUSE Linux Enterprise Server unterstützt die Authentifizierung per Fingerabdruck.

Sichern der Daten auf dem System

Wichtige Daten sollten nicht nur während der Übertragung, sondern auch auf der Festplatte verschlüsselt sein. Dies gewährleistet die Sicherheit der Daten im Falle eines Diebstahls. Die Erstellung einer verschlüsselten Partition mit SUSE Linux Enterprise Server wird in *Buch „*Security Guide*", Kapitel 11 „Encrypting Partitions and Files"* beschrieben. Es ist außerdem möglich, verschlüsselte Home-Verzeichnisse beim Hinzufügen des Benutzers mit YaST zu erstellen.

Wichtig: Datensicherheit und Suspend to Disk

Verschlüsselte Partitionen werden bei Suspend to Disk nicht ausgehängt. Daher sind alle Daten auf diesen Partitionen für jeden verfügbar, dem es gelingt, die Hardware zu stehlen und einen Resume-Vorgang für die Festplatte durchführt.

Netzwerksicherheit

Jeder Datentransfer muss sicher erfolgen, unabhängig von der Übertragungsart. Allgemeine, Linux und Netzwerke betreffende Sicherheitsrisiken sind in *Buch „*Security Guide*", Kapitel 1 „Security and Confidentiality"* beschrieben.

35.2 Mobile Hardware

SUSE Linux Enterprise Server unterstützt die automatische Erkennung mobiler Speichergeräte über FireWire (IEEE 1394) oder USB. Der Ausdruck *mobiles Speichergerät* bezieht sich auf jegliche Arten von FireWire- oder USB-Festplatten, Flash-Laufwerken oder Digitalkameras. Alle Geräte werden automatisch erkannt und konfiguriert, wenn sie mit dem System über die entsprechende Schnittstelle verbunden werden. Der Dateimanager in GNOME ermöglicht die flexible Handhabung von mobilen Hardwaregeräten. Zum sicheren Aushängen dieser Medien verwenden Sie die GNOME-Funktion *Unmount Volume* (Volumen aushängen) im Dateimanager. Weitere Informationen finden Sie unter *Buch „*GNOME-Benutzerhandbuch*"*.

Externe Festplatten (USB und FireWire)

Wenn eine externe Festplatte ordnungsgemäß vom System erkannt wird, wird das zugehörige Symbol in der Dateiverwaltung angezeigt. Durch Klicken auf das Symbol wird der Inhalt des Laufwerks angezeigt. Sie können hier Verzeichnisse und Dateien erstellen, bearbeiten und löschen. Möchten Sie eine Festplatte umbenennen, wählen Sie das entsprechende Menüelement aus dem Kontextmenü aus, das sich bei einem Rechtsklick öffnet. Die Namensänderung wird nur im Dateimanager angezeigt. Der Deskriptor, durch den das Gerät in `/media` eingehängt wurde, bleibt unbeeinflusst.

USB-Flash-Laufwerke

Diese Geräte werden vom System genau wie externe Festplatten behandelt. Ebenso können Sie die Einträge im Dateimanager umbenennen.

35.3 Mobiltelefone und PDAs

Ein Desktopsystem oder Notebook kann über Bluetooth oder IrDA mit einem Mobiltelefon kommunizieren. Einige Modelle unterstützen beide Protokolle, andere nur eines von beiden. Die Anwendungsbereiche für die beiden Protokolle und die entsprechende erweiterte Dokumentation wurde bereits in *Abschnitt 35.1.3.3, „Drahtlose Kommunikation: WLAN“* erwähnt. Die Konfiguration dieser Protokolle auf den Mobiltelefonen selbst wird in den entsprechenden Handbüchern beschrieben.

35.4 Weiterführende Informationen

Die zentrale Informationsquelle für alle Fragen in Bezug auf mobile Geräte und Linux ist http://tuxmobil.org/. Verschiedene Bereiche dieser Website befassen sich mit den Hardware- und Software-Aspekten von Notebooks, PDAs, Mobiltelefonen und anderer mobiler Hardware.

Einen ähnlichen Ansatz wie den unter http://tuxmobil.org/, finden Sie auch unter http://www.linux-on-laptops.com/. Hier finden Sie Informationen zu Notebooks und Handhelds.

SUSE unterhält eine deutschsprachige Mailingliste, die sich mit dem Thema Notebooks befasst. Weitere Informationen hierzu finden Sie unter http://lists.opensuse.org/opensuse-mobile-de/. In dieser Liste diskutieren Benutzer alle Aspekte der mobilen Computernutzung mit SUSE Linux Enterprise Server. Einige Beiträge sind auf Englisch, doch der größte Teil der archivierten Informationen liegt in deutscher Sprache vor. http://lists.opensuse.org/opensuse-mobile/ ist für Beiträge in englischer Sprache vorgesehen.

36 Verwendung von NetworkManager

NetworkManager ist die ideale Lösung für Notebooks und andere portable Computer. Es unterstützt die neuesten Verschlüsselungstypen und Standards für Netzwerkverbindungen, einschließlich Verbindungen zu Netzwerken, die nach 802.1X geschützt sind. 802.1X ist die „anschlussbasierte Netzwerkzugriffssteuerung des IEEE-Standards für lokale und innerstädtische Netzwerke“. Wenn Sie viel unterwegs sind und NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen verkabelten und drahtlosen Netzwerken zu verschwenden. NetworkManager kann automatisch eine Verbindung zu bekannten drahtlosen Netzwerken aufbauen oder mehrere Netzwerkverbindungen parallel verwalten – die schnellste Verbindung wird in diesem Fall als Standard verwendet. Darüber hinaus können Sie zwischen verfügbaren Netzwerken manuell wechseln und Ihre Netzwerkverbindung über ein Miniprogramm im Systemabschnitt der Kontrollleiste verwalten.

Anstelle nur einer Verbindung können mehrere Verbindungen gleichzeitig aktiv sein. Dies ermöglicht Ihnen, Ihr Notebook von einem Ethernet zu trennen und drahtlos verbunden zu bleiben.

36.1 Anwendungsbeispiele für den NetworkManager

NetworkManager enthält eine ausgereifte und intuitive Bedienoberfläche, über die Benutzer mühelos zwischen Netzwerkumgebungen wechseln können. In den folgenden Fällen ist der NetworkManager jedoch ungeeignet:

- Ihr Computer stellt Netzwerkdienste für andere Computer in Ihrem Netzwerk bereit (es handelt sich zum Beispiel um einen DHCP- oder DNS-Server)
- Ihr Computer ist ein Xen-Server oder Ihr System ein virtuelles System innerhalb von Xen.

36.2 Aktivieren oder Deaktivieren von NetworkManager

Auf Notebook-Computern ist NetworkManager standardmäßig aktiviert. Es lässt sich jedoch jederzeit im YaST-Modul „Netzwerkeinstellungen“ aktivieren oder deaktivieren.

1. Starten Sie YaST und gehen Sie zu *System* › *Netzwerkeinstellungen*.

2. Das Dialogfeld *Netzwerkeinstellungen* wird geöffnet. Klicken Sie auf den Karteireiter *Globale Optionen*.

3. Zum Konfigurieren und Verwalten der Netzwerkverbindungen mit NetworkManager gehen Sie wie folgt vor:

   a. Wählen Sie im Feld *Netzwerkeinrichtungsmethode* die Option *Benutzergesteuert mithilfe von NetworkManager*.

   b. Klicken Sie auf *OK*, und schließen Sie YaST.

   c. Konfigurieren Sie die Netzwerkverbindungen mit NetworkManager gemäß den Anweisungen in *Abschnitt 36.3, „Konfigurieren von Netzwerkverbindungen“*.

4. Zum Deaktivieren von NetworkManager und Steuern des Netzwerks mit Ihrer eigenen Konfiguration gehen Sie wie folgt vor:

   a. Wählen Sie im Feld *Netzwerkeinrichtungsmethode* die Option *Controlled by wicked* (Steuerung mit wicked).

   b. Klicken Sie auf *OK*.

   c. Richten Sie Ihre Netzwerkkarte mit YaST mithilfe der automatischen Konfiguration durch DHCP oder mithilfe einer statischen IP-Adresse ein.
   Eine ausführliche Beschreibung der Netzwerkkonfiguration mit YaST finden Sie in *Abschnitt 16.4, „Konfigurieren von Netzwerkverbindungen mit YaST“*.

36.3 Konfigurieren von Netzwerkverbindungen

Konfigurieren Sie nach der Aktivierung von NetworkManager in YaST Ihre Netzwerkverbindungen mit dem NetworkManager-Frontend, das in GNOME verfügbar ist. Hier sehen Sie Registerkarten für alle Arten von Netzwerkverbindungen, z. B. verkabelte, drahtlose, mobile Breitband-, DSL- und VPN-Verbindungen.

Zum Öffnen des Dialogfelds für die Netzwerkkonfiguration in GNOME öffnen Sie aus dem Statusmenü das Einstellungsmenü, und klicken Sie dort auf den Eintrag *Netzwerk*.

Anmerkung: Verfügbarkeit von Optionen

Abhängig von Ihrer Systemeinrichtung dürfen Sie möglicherweise keine Verbindungen konfigurieren. In einer abgesicherten Umgebung sind eventuell einige Optionen gesperrt oder erfordern eine `root`-Berechtigung. Erfragen Sie Einzelheiten bei Ihrem Systemadministrator.

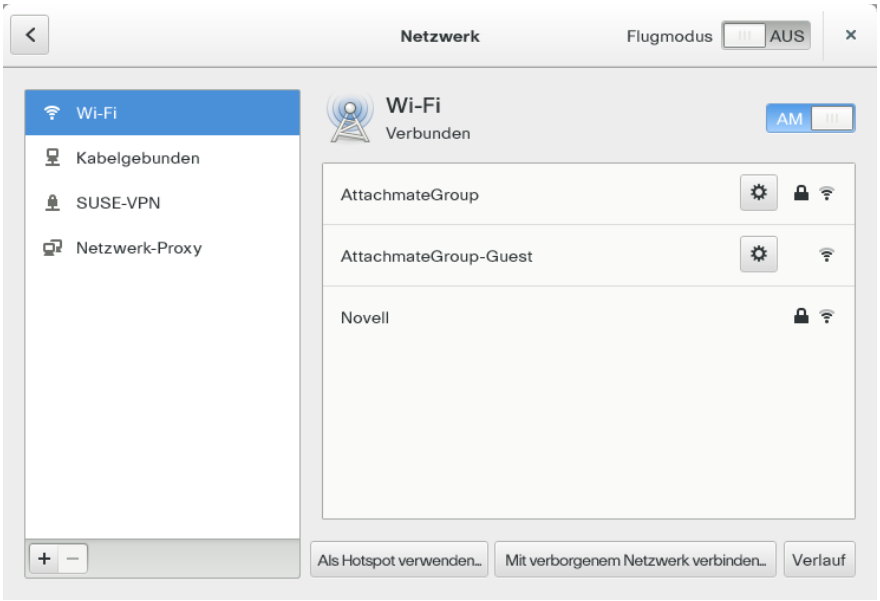


ABBILDUNG 36.1 DIALOGFELD „NETZWERKVERBINDUNGEN“ IN GNOME

PROZEDUR 36.1 HINZUFÜGEN UND BEARBEITEN VON VERBINDUNGEN

1. Öffnen Sie das Dialogfeld „NetworkManager-Konfiguration“.
2. So fügen Sie eine Verbindung hinzu:
   a. Klicken Sie links unten auf das +-Symbol.
   b. Wählen Sie den von Ihnen bevorzugten Verbindungstyp aus, und folgen Sie den Anweisungen.
   c. Wenn Sie fertig sind, klicken Sie auf *Hinzufügen*.
   d. Nachdem Sie Ihre Änderungen bestätigt haben, erscheint die neu konfigurierte Netzwerkverbindung im Statusmenü in der Liste der verfügbaren Netzwerke.
3. So bearbeiten Sie eine Verbindung:
   a. Wählen Sie den zu bearbeitenden Eintrag aus.

b. Klicken Sie auf das Zahnradsymbol, um das Dialogfeld *Verbindungseinstellungen* zu öffnen.

c. Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf *Anwenden*, um diese zu speichern.

d. Wenn die Verbindung als Systemverbindung zur Verfügung stehen soll, wechseln Sie zur Registerkarte *Identität* und aktivieren Sie dort das Kontrollkästchen *Anderen Benutzern zur Verfügung stellen*. Weitere Informationen zu Benutzer- und Systemverbindungen finden Sie unter *Abschnitt 36.4.1, „Benutzer- und Systemverbindungen“*.

36.3.1 Verwalten von kabelgebundenen Netzwerkverbindungen

Wenn Ihr Computer mit einem kabelgebundenen Netzwerk verbunden ist, verwenden Sie NetworkManager zur Verwaltung der Verbindung.

1. Öffnen Sie das Statusmenü und klicken Sie auf *Verkabelt*, um die Verbindungsdetails zu ändern oder die Verbindung zu deaktivieren.
2. Zum Ändern der Einstellungen klicken Sie auf *Einstellungen für kabelgebundenes Netzwerk* und danach auf das Zahnradsymbol.
3. Zum Deaktivieren aller Netzwerkverbindungen aktivieren Sie den *Flugzeugmodus*.

36.3.2 Verwalten von drahtlosen Netzwerkverbindungen

Die sichtbaren drahtlosen Netzwerke werden im Menü des GNOME NetworkManager-Miniprogramms unter *Drahtlose Netzwerke* aufgeführt. Die Signalstärke der einzelnen Netzwerke wird ebenfalls im Menü angezeigt. Verschlüsselte drahtlose Netzwerke sind mit einem blauen Schildsymbol gekennzeichnet.

PROZEDUR 36.2 VERBINDEN MIT EINEM SICHTBAREN DRAHTLOSEN NETZWERK

1. Zum Verbinden mit einem sichtbaren drahtlosen Netzwerk öffnen Sie das Statusmenü, und klicken Sie auf *WLAN*.
2. Klicken Sie auf *Aktivieren*.
3. Klicken Sie auf *Netzwerk auswählen*, wählen Sie Ihr drahtloses Netzwerk aus, und klicken Sie auf *Verbinden*.

4. Wenn das Netzwerk verschlüsselt ist, öffnet sich ein Konfigurationsdialogfeld. Es gibt den Verschlüsselungstyp des Netzwerks an und enthält Textfelder für die Eingabe der Anmeldedaten.

PROZEDUR 36.3 VERBINDEN MIT EINEM NICHT SICHTBAREN, DRAHTLOSEN NETZWERK

1. Zum Verbinden mit einem Netzwerk, das seine Dienstkennung (SSID oder ESSID) nicht aussendet und daher nicht automatisch erkannt werden kann, öffnen Sie das Statusmenü und klicken Sie auf *WLAN*.
2. Klicken Sie auf *WLAN-Einstellungen*, um das detaillierte Einstellungsmenü zu öffnen.
3. Stellen Sie sicher, dass Ihr drahtloses Netzwerk aktiviert ist, und klicken Sie dann auf *Mit verborgenem Netzwerk verbinden*.
4. Geben Sie im daraufhin angezeigten Dialogfeld unter *Netzwerkname* die SSID oder ESSID ein und legen Sie gegebenenfalls die Verschlüsselungsparameter fest.

Die Verbindung zu einem drahtlosen Netzwerk, das explizit gewählt wurde, wird so lange wie möglich aufrecht erhalten. Wenn dabei ein Netzwerkkabel angeschlossen ist, werden alle Verbindungen, für die *Stay connected when possible (Nach Möglichkeit verbunden bleiben)* festgelegt wurde, hergestellt, während die drahtlose Verbindung bestehen bleibt.

36.3.3 Konfigurieren der WLAN-/Bluetooth-Karte als Zugriffspunkt

Wenn Ihre WLAN-/Bluetooth-Karte den Zugriffspunktmodus unterstützt, können Sie NetworkManager zur Konfiguration verwenden.

1. Öffnen Sie das Statusmenü, und klicken Sie auf *WLAN*.
2. Klicken Sie auf *WLAN-Einstellungen*, um das detaillierte Einstellungsmenü zu öffnen.
3. Klicken Sie auf *Als Hotspot verwenden* und folgen Sie den Anweisungen.
4. Verwenden Sie zur Verbindung mit dem Hotspot von einem Remote-Computer die im Dialogfeld angezeigten Anmeldedaten.

36.3.4 NetworkManager und VPN

NetworkManager unterstützt verschiedene Technologien für virtuelle private Netzwerke (VPN). Für jede Technologie bietet SUSE Linux Enterprise Server ein Basispaket mit generischer Unterstützung für NetworkManager. Zusätzlich müssen Sie auch das entsprechende Desktop-spezifische Paket für Ihr Miniprogramm installieren.

OpenVPN

Installieren Sie zur Verwendung dieser VPN-Technik:

- `NetworkManager-openvpn`
- `NetworkManager-openvpn-gnome`

vpnc (Cisco AnyConnect)

Installieren Sie zur Verwendung dieser VPN-Technik:

- `NetworkManager-vpnc`
- `NetworkManager-vpnc-gnome`

PPTP (Point-to-Point-Tunneling-Protokoll)

Installieren Sie zur Verwendung dieser VPN-Technik:

- `NetworkManager-pptp`
- `NetworkManager-pptp-gnome`

Im folgenden Verfahren wird beschrieben, wie Sie Ihren Computer mithilfe von NetworkManager als OpenVPN-Client einrichten können. Das Einrichten anderer VPN-Typen funktioniert auf die gleiche Weise.

Stellen Sie sicher, dass das Paket `NetworkManager-openvpn-gnome` installiert ist und alle Abhängigkeiten aufgelöst wurden, bevor Sie starten.

PROZEDUR 36.4 EINRICHTEN VON OPENVPN MIT NETWORKMANAGER

1. Öffnen Sie die *Einstellungen* der Anwendung, indem Sie auf die Statussymbole am rechten Ende der Kontrollleiste und anschließend auf das Symbol mit dem Schraubenschlüssel und dem Schraubendreher klicken. Wählen Sie im Fenster *All Settings* (Alle Einstellungen) die Option *Network* (Netzwerk).
2. Klicken Sie auf das Symbol +.

3. Wählen Sie *VPN* und anschließend *OpenVPN* aus.

4. Wählen Sie bei *Authentication* den Authentifizierungstyp. Wählen Sie entsprechend der Konfiguration Ihres OpenVPN-Servers, *Certificates (TLS)* (Zertifikate (TLS) oder *Password with Certificates (TLS)* (Passwort mit Zertifikaten (TLS)).

5. Geben Sie die erforderlichen Werte in die entsprechenden Textfelder ein. In unserem Beispiel sind dies:

Gateway	Der Remote-Endpunkt des VPN-Servers
User name (Benutzername)	Der Benutzer (nur verfügbar, wenn Sie *Password with Certificates (TLS)* ausgewählt haben)
Password (Passwort)	Das Passwort für den Benutzer (nur verfügbar, wenn Sie *Password with Certificates (TLS)* ausgewählt haben)
User Certificate (Benutzerzertifikat)	`/etc/openvpn/client1.crt`
CA Certificate (CA-Zertifikat)	`/etc/openvpn/ca.crt`
Private Key (Privater Schlüssel)	`/etc/openvpn/client1.key`

6. Schließen Sie die Konfiguration ab, indem Sie auf *Add* (Hinzufügen) klicken.

7. Um die Verbindung zu aktivieren, klicken Sie in der Kontrollleiste *Netzwerk* der Anwendung *Einstellungen* auf den Umschalter. Alternativ können Sie auf die Statussymbole am rechten Ende der Kontrollleiste klicken. Klicken Sie auf den Namen Ihres VPN und dann auf *Verbinden*.

36.4 NetworkManager und Sicherheit

Der NetworkManager unterscheidet zwischen zwei Typen von drahtlosen Verbindungen: verbürgte und unverbürgte Verbindungen. Eine verbürgte Verbindung ist jedes Netzwerk, das Sie in der Vergangenheit explizit ausgewählt haben. Alle anderen sind unverbürgt. Verbürgte Ver-

bindungen werden anhand des Namens und der MAC-Adresse des Zugriffspunkts identifiziert. Durch Verwendung der MAC-Adresse wird sichergestellt, dass Sie keinen anderen Zugriffspunkt mit dem Namen Ihrer verbürgten Verbindung verwenden können.

NetworkManager scannt in regelmäßigen Abständen nach verfügbaren drahtlosen Netzwerken. Wenn mehrere verbürgte Netzwerke gefunden werden, wird automatisch das zuletzt verwendete ausgewählt. Wenn keines der Netzwerke vertrauenswürdig ist, wartet NetworkManager auf Ihre Auswahl.

Wenn die Verschlüsselungseinstellung geändert wird, aber Name und MAC-Adresse gleich bleiben, versucht NetworkManager, eine Verbindung herzustellen. Zuvor werden Sie jedoch aufgefordert, die neuen Verschlüsselungseinstellungen zu bestätigen und Aktualisierungen, z. B. einen neuen Schlüssel, bereitzustellen.

Wenn Sie von der Verwendung einer drahtlosen Verbindung in den Offline-Modus wechseln, blendet NetworkManager die SSID oder ESSID aus. So wird sichergestellt, dass die Karte nicht mehr verwendet wird.

36.4.1 Benutzer- und Systemverbindungen

NetworkManager kennt zwei Verbindungsarten: `Benutzer-` und `System-` Verbindungen. Bei Benutzerverbindungen handelt es sich um Verbindungen, die für NetworkManager verfügbar werden, sobald sich der erste Benutzer anmeldet. Alle erforderlichen Legitimationsdaten werden vom Benutzer angefordert, und wenn er sich abmeldet, werden die Verbindungen getrennt und aus NetworkManager entfernt. Als Systemverbindung definierte Verbindungen können für alle Benutzer freigegeben werden und sind direkt nach dem Start von NetworkManager verfügbar, bevor sich Benutzer angemeldet haben. Für Systemverbindungen müssen alle Berechtigungsnachweise zum Zeitpunkt der Verbindungserstellung angegeben werden. Über Systemverbindungen können automatisch Verbindungen mit Netzwerken hergestellt werden, für die eine Autorisierung erforderlich ist. Informationen zum Konfigurieren von Benutzer- oder Systemverbindungen mit NetworkManager finden Sie unter *Abschnitt 36.3, „Konfigurieren von Netzwerkverbindungen“*.

36.4.2 Speichern von Passwörtern und Berechtigungsnachweisen

Wenn Sie Ihre Berechtigungsnachweise nicht bei jedem Verbindungsversuch mit einem verschlüsselten Netzwerk erneut eingeben wollen, können Sie den GNOME Keyring Manager verwenden, um Ihre Berechtigungsnachweise verschlüsselt und durch Master-Passwort geschützt auf der Festplatte zu speichern.

NetworkManager kann auch seine Zertifikate für sichere Verbindungen (z. B. verschlüsselte Kabel-, Funk- oder VPN-Verbindungen) vom Zertifikatspeicher abrufen. Weitere Informationen hierzu finden Sie im *Buch „Security Guide", Kapitel 12 „Certificate Store"*.

36.5 Häufig gestellte Fragen

Nachfolgend finden Sie einige häufig gestellte Fragen zum Konfigurieren spezieller Netzwerkoptionen mit NetworkManager.

36.5.1. *Wie kann eine Verbindung an ein bestimmtes Gerät gebunden werden?*

Standardmäßig sind Verbindungen in NetworkManager gerätetypspezifisch: Sie gelten für alle physischen Geräte desselben Typs. Wenn mehrere physische Geräte pro Verbindungsart verfügbar sind (z. B. wenn Ihr Gerät mit zwei Ethernet-Karten ausgestattet ist), können Sie eine Verbindung an ein bestimmtes Gerät binden.

Schlagen Sie dafür in GNOME zunächst die MAC-Adresse Ihres Geräts in der *Verbindungsinformation* nach, die über das Miniprogramm zur Verfügung steht, oder verwenden Sie die Ausgabe von Kommandozeilenwerkzeugen wie `nm-tool` oder `wicked show all`. Starten Sie dann das Dialogfeld zur Konfiguration von Netzwerkverbindungen und wählen Sie die Verbindung aus, die Sie ändern möchten. Geben Sie auf der Registerkarte *Verkabelt* oder *Drahtlos* die *MAC-Adresse* des Geräts ein und bestätigen Sie Ihre Änderungen.

36.5.2. *Wie wird ein bestimmter Zugriffspunkt angegeben, wenn mehrere Zugriffspunkte mit derselben ESSID erkannt werden?*

Wenn mehrere Zugriffspunkte mit unterschiedlichen Funkfrequenzbereichen (a/b/g/n) verfügbar sind, wird standardmäßig der Zugriffspunkt mit dem stärksten Signal automatisch gewählt. Um diesen Vorgang außer Kraft zu setzen, verwenden Sie das Feld *BSSID* beim Konfigurieren Ihrer drahtlosen Verbindungen.

Der Basic Service Set Identifier (BSSID) identifiziert jedes Basic Service Set eindeutig. In einem Basic Service Set der Infrastruktur entspricht die BSSID der MAC-Adresse des drahtlosen Zugriffspunkts. In einem unabhängigen (Ad-hoc) Basic Service Set entspricht die BSSID einer lokal verwalteten MAC-Adresse, die aus einer 46-Bit-Zufallszahl generiert wird.

Starten Sie den Dialog die die Konfiguration von Netzwerkverbindungen wie in *Abschnitt 36.3, „Konfigurieren von Netzwerkverbindungen“* beschrieben. Wählen Sie die drahtlose Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Geben Sie im Karteireiter *Drahtlos* die BSSID ein.

36.5.3. *Wie werden Netzwerkverbindungen mit anderen Computern freigegeben?*

Das primäre Gerät (das Gerät, das mit dem Internet verbunden ist) benötigt keine spezielle Konfiguration. Jedoch müssen Sie das Gerät, das mit dem lokalen Hub oder Computer verbunden ist, wie folgt konfigurieren:

1. Starten Sie den Dialog düe die Konfiguration von Netzwerkverbindungen wie in *Abschnitt 36.3, „Konfigurieren von Netzwerkverbindungen“* beschrieben. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Wechseln Sie zum Karteireiter *IPv4-Einstellungen* und aktivieren Sie im Dropdown-Feld *Methode* die Option *Shared to other computers* (Für andere Computer freigegeben). Damit ist die Weiterleitung von IP-Netzwerkverkehr möglich und ein DHCP-Server wird auf dem Gerät ausgeführt. Bestätigen Sie Ihre Änderungen in NetworkManager.

2. Da der DCHP-Server den Port 67 verwendet, stellen Sie sicher, dass dieser nicht durch die Firewall blockiert ist: Starten Sie YaST auf dem Computer, der die Verbindungen nutzen möchte, und wählen Sie *Sicherheit und Benutzer* › *Firewall*. Wechseln Sie zur Kategorie *Erlaubte Dienste*. Wenn *DCHP-Server* nicht bereits als *Erlaubter Dienst* angezeigt ist, wählen Sie *DCHP-Server* aus *Services to Allow* (Erlaubte Dienste) und klicken Sie auf *Hinzufügen*. Bestätigen Sie Ihre Änderungen in YaST.

36.5.4. *Wie kann statische DNS-Information mit automatischen (DHCP-, PPP-, VPN-) Adressen bereitgestellt werden?*

Falls ein DHCP-Server ungültige DNS-Informationen (und/oder Routen) liefert, können Sie diese überschreiben. Starten Sie den Dialog düe die Konfiguration von Netzwerkverbindungen wie in *Abschnitt 36.3, „Konfigurieren von Netzwerkverbindungen“* beschrieben. Wählen Sie die Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Öffnen Sie den Karteireiter *IPv4-Einstellungen* und aktivieren Sie im Dropdown-Feld *Methode*

die Option *Automatic (DHCP) addresses only* (Nur automatische (DHCP-)Adressen). Geben Sie die DNS-Information in die Felder *DNS-Server* und *Suchdomänen* ein. Sollen automatisch abgerufene Routen ignoriert werden, klicken Sie auf *Routes* (Routen) und aktivieren Sie das Kontrollkästchen *Ignore automatically obtained routes* (Automatisch abgerufene Routen ignorieren). Bestätigen Sie Ihre Änderungen.

36.5.5. *Wie kann NetworkManager dazu veranlasst werden, eine Verbindung zu passwortgeschützten Netzwerken aufzubauen, bevor sich ein Benutzer anmeldet?*

Definieren Sie eine `Systemverbindung`, die für solche Zwecke verwendet werden kann. Weitere Informationen hierzu finden Sie in *Abschnitt 36.4.1, „Benutzer- und Systemverbindungen“*.

36.6 Fehlersuche

Es können Verbindungsprobleme auftreten. Bei NetworkManager sind unter anderem die Probleme bekannt, dass das Miniprogramm nicht startet oder eine VPN-Option fehlt. Die Methoden zum Lösen und Verhindern dieser Probleme hängen vom verwendeten Werkzeug ab.

NetworkManager-Desktop-Applet wird nicht gestartet

Das Miniprogramm wird automatisch gestartet, wenn das Netzwerk für die NetworkManager-Steuerung eingerichtet ist. Wenn das Miniprogramm/Widget nicht gestartet wird, überprüfen Sie, ob NetworkManager in YaST aktiviert ist (siehe *Abschnitt 36.2, „Aktivieren oder Deaktivieren von NetworkManager“*). Überprüfen Sie dann, ob das NetworkManager-gnome-Paket installiert ist.

Wenn das Desktop-Miniprogramm installiert ist, aber aus einem unbestimmten Grund nicht ausgeführt wird, starten Sie es manuell. Wenn das Desktop-Miniprogramm installiert ist, aber nicht ausgeführt wird, starten Sie es manuell über das Kommando **`nm-applet`**.

Das NetworkManager-Applet beinhaltet keine VPN-Option

Die Unterstützung für NetworkManager-Miniprogramme sowie VPN für NetworkManager wird in Form separater Pakete verteilt. Wenn Ihr NetworkManager-Applet keine VPN-Option enthält, überprüfen Sie, ob die Pakete mit der NetworkManager-Unterstützung für Ihre VPN-Technologie installiert sind. Weitere Informationen finden Sie unter *Abschnitt 36.3.4, „NetworkManager und VPN“*.

Keine Netzwerkverbindung verfügbar

Wenn Sie Ihre Netzwerkverbindung korrekt konfiguriert haben und alle anderen Komponenten für die Netzwerkverbindung (Router etc.) auch gestartet sind und ausgeführt werden, ist es manchmal hilfreich, die Netzwerkschnittstellen auf Ihrem Computer erneut zu starten. Melden Sie sich dazu bei einer Befehlszeile als `root` an und führen Sie den Befehl **`systemctl restart wicked`** aus.

36.7 Weiterführende Informationen

Weitere Informationen zu NetworkManager finden Sie auf den folgenden Websites und in folgenden Verzeichnissen:

Projektseite von NetworkManager

http://projects.gnome.org/NetworkManager/

Dokumentation zu den einzelnen Paketen

Sehen Sie sich auch die neuesten Informationen zu NetworkManager und dem GNOME-Miniprogramm in den folgenden Verzeichnissen an:

- `/usr/share/doc/packages/NetworkManager/`,
- `/usr/share/doc/packages/NetworkManager-gnome/`.

37 Energieverwaltung

System z Die in diesem Kapitel beschriebenen Funktionen und Hardware-Elemente sind auf den Plattformen IBM z Systems nicht vorhanden. Das Kapitel ist für diese Plattformen daher irrelevant.

Die Energieverwaltung ist insbesondere bei Notebook-Computern von großer Wichtigkeit, sie ist jedoch auch für andere Systeme sinnvoll. ACPI (Advanced Configuration & Power Interface) ist auf allen modernen Computern (Laptops, Desktops, Server) verfügbar. Für Energieverwaltungstechnologien sind geeignete Hardware- und BIOS-Routinen erforderlich. Die meisten Notebooks und modernen Desktops und Server erfüllen diese Anforderungen. Es ist außerdem möglich, die CPU-Frequenzskalierung zu steuern, um Energie zu sparen oder den Geräuschpegel zu senken.

37.1 Energiesparfunktionen

Energiesparfunktionen sind nicht nur für die mobile Verwendung von Notebooks von Bedeutung, sondern auch für Desktop-Systeme. Die Hauptfunktionen und ihre Verwendung im ACPI sind:

Standby

Nicht unterstützt.

Suspend (in Arbeitsspeicher)

In diesem Modus wird der gesamte Systemstatus in den RAM geschrieben. Anschließend wird das gesamte System mit Ausnahme des RAM in den Ruhezustand versetzt. In diesem Zustand verbraucht der Computer sehr wenig Energie. Der Vorteil dieses Zustands besteht darin, dass innerhalb weniger Sekunden die Arbeit nahtlos wieder aufgenommen werden kann, ohne dass ein Booten des Systems oder ein Neustart der Anwendungen erforderlich ist. Diese Funktion entspricht ACPI-Zustand `S3`.

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 Herstel-

ler bieten Hybridvarianten dieses Modus an, beispielsweise RediSafe bei IBM Thinkpads. Der entsprechende ACPI-Zustand ist `S4`. In Linux wird „suspend to disk“ über Kernel-Routinen durchgeführt, die von ACPI unabhängig sind.

Anmerkung: UUID für Swap-Partitionen bei Formatierung über **mkswap** geändert

Falls möglich, sollten bestehende Swap-Partitionen nicht mit **`mkswap`** neu formatiert werden. Durch die Neuformatierung mit **`mkswap`** ändert sich der UUID-Wert der Swap-Partition. Nehmen Sie die Neuformatierung entweder über YaST vor (dabei wird `/etc/fstab` aktualisiert) oder passen Sie `/etc/fstab` manuell an.

Akku-Überwachung

ACPI überprüft den Akkuladestatus und stellt entsprechende Informationen bereit. Außerdem koordiniert es die Aktionen, die beim Erreichen eines kritischen Ladestatus durchzuführen sind.

Automatisches Ausschalten

Nach dem Herunterfahren wird der Computer ausgeschaltet. Dies ist besonders wichtig, wenn der Computer automatisch heruntergefahren wird, kurz bevor der Akku leer ist.

Steuerung der Prozessorgeschwindigkeit

In Verbindung mit der CPU gibt es drei Möglichkeiten, Energie zu sparen: Frequenz- und Spannungsskalierung (auch PowerNow! oder Speedstep), Drosselung und Versetzen des Prozessors in den Ruhezustand (C-Status). Je nach Betriebsmodus des Computers können diese Methoden auch kombiniert werden.

37.2 Advanced Configuration & Power Interface (ACPI)

Die ACPI (erweiterte Konfigurations- und Energieschnittstelle) wurde entwickelt, um dem Betriebssystem die Einrichtung und Steuerung der einzelnen Hardware-Komponenten zu ermöglichen. ACPI löst sowohl Power-Management Plug and Play (PnP) als auch Advanced Power Management (APM) ab. Diese Schnittstelle bietet Informationen zu Akku, Netzteil, Temperatur, Ventilator und Systemereignissen wie „Deckel schließen“ oder „Akku-Ladezustand niedrig“.

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 journald gemeldet. Weitere Informationen zum Abrufen der Protokollmeldungen im Journal finden Sie unter *Kapitel 15, `journalctl`: Abfragen des `systemd`-Journals*. Weitere Informationen zur Fehlersuche bei ACPI-Problemen finden Sie in *Abschnitt 37.2.2, „Fehlersuche“*.

37.2.1 Steuern der CPU-Leistung

Mit der CPU sind Energieeinsparungen auf drei verschiedene Weisen möglich:

- Frequenz- und Spannungsskalierung
- Drosseln der Taktfrequenz (T-Status)
- Versetzen des Prozessors in den Ruhezustand (C-Status)

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.

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. Im Allgemeinen empfiehlt sich die dynamische Frequenzskalierung mit Steuerung durch den On-Demand-Governor im Kernel.

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.

Detaillierte Informationen hierzu finden Sie in *Buch „System Analysis and Tuning Guide“, Kapitel 11 „Power Management“*.

37.2.2 Fehlersuche

Es gibt zwei verschiedene Arten von Problemen. Einerseits kann der ACPI-Code des Kernel Fehler enthalten, die nicht rechtzeitig erkannt wurden. In diesem Fall wird eine Lösung zum Herunterladen bereitgestellt. Häufiger 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 nicht booten lässt, kann eventuell einer der folgenden Bootparameter Abhilfe schaffen:

pci=noacpi
: ACPI nicht zum Konfigurieren der PCI-Geräte verwenden.

acpi=ht
: Nur eine einfache Ressourcenkonfiguration durchführen. ACPI nicht für andere Zwecke verwenden.

acpi=off
: ACPI deaktivieren.

Warnung: Probleme beim Booten ohne ACPI

Einige neuere Computer (insbesondere SMP- und AMD64-Systeme) benötigen ACPI zur korrekten Konfiguration der Hardware. Bei diesen Computern kann die Deaktivierung von ACPI zu Problemen führen.

Manchmal ist der Computer durch Hardware gestört, die über USB oder FireWire angeschlossen ist. Wenn ein Computer nicht hochfährt, stecken Sie nicht benötigte Hardware aus und versuchen Sie es erneut.

Überwachen Sie nach dem Booten die Bootmeldungen des Systems mit dem Befehl `dmesg -T | grep -2i acpi` (oder überwachen Sie alle Meldungen, da das Problem möglicherweise nicht durch ACPI verursacht wurde). Wenn bei der Analyse einer ACPI-Tabelle ein Fehler auftritt,

kann die wichtigste Tabelle – die DSDT (*Differentiated System Description Table*) – durch eine verbesserte Version ersetzt werden. In diesem Fall wird die fehlerhafte DSDT des BIOS ignoriert. Das Verfahren wird in *Abschnitt 37.4, „Fehlersuche“* erläutert.

In der Kernel-Konfiguration gibt es einen Schalter zur Aktivierung der ACPI-Fehlersuchmeldungen. Wenn ein Kernel mit ACPI-Fehlersuche kompiliert und installiert ist, werden detaillierte Informationen angezeigt.

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.

37.2.2.1 Weiterführende Informationen

- http://tldp.org/HOWTO/ACPI-HOWTO/ (detailliertes ACPI HOWTO, enthält DSDT-Patches)
- http://www.acpi.info (technische Daten zur Advanced Configuration & Power Interface)
- http://acpi.sourceforge.net/dsdt/index.php (DSDT-Patches von Bruno Ducrot)

37.3 Ruhezustand für Festplatte

In Linux kann die Festplatte vollständig ausgeschaltet werden, wenn sie nicht benötigt wird, oder sie kann in einem energiesparenderen oder ruhigeren Modus betrieben werden. Bei modernen 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 mit dem Kommando **`hdparm`** ausprobieren.

Hiermit können verschiedene Festplatteneinstellungen bearbeitet werden. Die Option `-y` schaltet die Festplatte sofort in den Stand-by-Modus. `-Y` versetzt sie in den Ruhezustand. **`hdparm`** `-S` *`X`* führt dazu, dass die Festplatte nach einen bestimmten Inaktivitätszeitraum abgeschaltet wird. Ersetzen Sie *`X`* wie folgt: `0` deaktiviert diesen Mechanismus, sodass die Festplatte kontinuierlich ausgeführt wird. Werte von `1` bis `240` werden mit 5 Sekunden multipliziert. Werte von `241` bis `251` entsprechen 1- bis 11-mal 30 Minuten.

Die internen Energiesparoptionen der Festplatte lassen sich über die Option `-B` steuern. Wählen Sie einen Wert `0` (maximale Energieeinsparung) bis `255` (maximaler Durchsatz). Das Ergebnis hängt von der verwendeten Festplatte ab und ist schwer einzuschätzen. Die Geräuschentwicklung einer Festplatte können Sie mit der Option `-M` reduzieren. Wählen Sie einen Wert von `128` (ruhig) bis `254` (schnell).

Häufig ist es nicht so einfach, die Festplatte in den Ruhezustand zu versetzen. Bei Linux führen zahlreiche Prozesse Schreibvorgänge auf der Festplatte durch, wodurch diese wiederholt aus dem Ruhezustand reaktiviert wird. Daher sollten Sie unbedingt verstehen, wie Linux mit Daten umgeht, die auf die Festplatte geschrieben werden müssen. Zunächst werden alle Daten im RAM-Puffer gespeichert. Dieser Puffer wird vom `pdflush`-Daemon überwacht. Wenn die Daten ein bestimmtes Alter erreichen oder wenn der Puffer bis zu einem bestimmten Grad gefüllt ist, wird der Pufferinhalt auf die Festplatte übertragen. Die Puffergröße ist dynamisch und hängt von der Größe des Arbeitsspeichers und von der Systemlast ab. Standardmäßig werden für pdflush kurze Intervalle festgelegt, um maximale Datenintegrität zu erreichen. Das Programm überprüft den Puffer alle fünf Sekunden und schreibt die Daten auf die Festplatte. Die folgenden Variablen sind interessant:

`/proc/sys/vm/dirty_writeback_centisecs`
: Enthält die Verzögerung bis zur Reaktivierung eines pdflush-Threads (in Hundertstelsekunden).

`/proc/sys/vm/dirty_expire_centisecs`
: Definiert, nach welchem Zeitabschnitt eine schlechte Seite spätestens ausgeschrieben werden sollte. Der Standardwert ist `3000`, was 30 Sekunden bedeutet.

`/proc/sys/vm/dirty_background_ratio`
: Maximaler Prozentsatz an schlechten Seiten, bis pdflush damit beginnt, sie zu schreiben. Die Standardeinstellung ist `5` %.

`/proc/sys/vm/dirty_ratio`
: Wenn die schlechten Seiten diesen Prozentsatz des gesamten Arbeitsspeichers überschreiten, werden Prozesse gezwungen, während ihres Zeitabschnitts Puffer mit schlechten Seiten anstelle von weiteren Daten zu schreiben.

Warnung: Beeinträchtigung der Datenintegrität

Änderungen an den Einstellungen für den `pdflush`-Aktualisierungs-Daemon gefährden die Datenintegrität.

Abgesehen von diesen Prozessen schreiben protokollierende Journaling-Dateisysteme, wie `Btrfs`, `Ext3`, `Ext4` und andere ihre Metadaten unabhängig von `pdflush`, was ebenfalls das Abschalten der Festplatte verhindert.

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 `ja` gesetzt wird, greift postfix wesentlich seltener auf die Festplatte zu.

37.4 Fehlersuche

Alle Fehler- und Alarmmeldungen werden im Systemjournal gespeichert, das Sie mit dem Kommando **`journalctl`** abrufen können (weitere Informationen siehe *Kapitel 15, **`journalctl`**: Abfragen des `systemd`-Journals*). In den folgenden Abschnitten werden die häufigsten Probleme behandelt.

37.4.1 CPU-Frequenzsteuerung funktioniert nicht

Rufen Sie die Kernel-Quellen auf, um festzustellen, ob der verwendete Prozessor unterstützt wird. Möglicherweise ist ein spezielles Kernel-Modul bzw. eine Moduloption erforderlich, um die CPU-Frequenzsteuerung zu aktivieren. Wenn das `kernel-source`-Paket installiert ist, finden Sie diese Informationen unter `/usr/src/linux/Documentation/cpu-freq/*`.

37.5 Weiterführende Informationen

- http://en.opensuse.org/SDB:Suspend_to_RAM – Anleitung zur Einstellung von „Suspend to RAM“
- http://old-en.opensuse.org/Pm-utils – Anleitung zur Änderung des allgemeinen Suspend-Frameworks

VI Fehlersuche

38 Hilfe und Dokumentation 615

39 Erfassen der Systeminformationen für den Support 621

40 Häufige Probleme und deren Lösung 648

38 Hilfe und Dokumentation

Im Lieferumfang von SUSE® Linux Enterprise Server sind verschiedene Informationen und Dokumentationen enthalten, viele davon bereits in Ihr installiertes System integriert.

Dokumentation unter `/usr/share/doc`

Dieses traditionelle Hilfe-Verzeichnis enthält verschiedene Dokumentationsdateien sowie die Hinweise zur Version Ihres Systems. Außerdem enthält es Informationen über die im Unterverzeichnis `packages` installierten Pakete. Weitere Informationen finden Sie unter *Abschnitt 38.1, „Dokumentationsverzeichnis“*.

man-Seiten und Infoseiten für Shell-Kommandos

Wenn Sie mit der Shell arbeiten, brauchen Sie die Optionen der Kommandos nicht auswendig zu kennen. Die Shell bietet normalerweise eine integrierte Hilfefunktion mit man-Seiten und Infoseiten. Weitere Informationen dazu finden Sie unter *Abschnitt 38.2, „man-Seiten“* und *Abschnitt 38.3, „Infoseiten“*.

Desktop-Hilfezentren

Das Hilfezentrum des GNOME-Desktops (Hilfe) bietet zentralen Zugriff auf die wichtigsten Dokumentationsressourcen auf Ihrem System in durchsuchbarer Form. Zu diesen Ressourcen zählen die Online-Hilfe für installierte Anwendungen, man-Seiten, Infoseiten sowie die mit Ihrem Produkt gelieferten SUSE-Handbücher.

Separate Hilfepakete für einige Anwendungen

Beim Installieren von neuer Software mit YaST wird die Softwaredokumentation in der Regel automatisch installiert und in der Hilfe auf Ihrem Desktop angezeigt. Jedoch können einige Anwendungen, beispielsweise GIMP, über andere Online-Hilfepakete verfügen, die separat mit YaST installiert werden können und nicht in die Hilfe integriert werden.

38.1 Dokumentationsverzeichnis

Das traditionelle Verzeichnis zum Suchen von Dokumentationen in Ihrem installierten Linux-System finden Sie unter `/usr/share/doc`. Das Verzeichnis enthält normalerweise Informationen zu den auf Ihrem System installierten Paketen sowie Versionshinweise, Handbücher usw.

Anmerkung: Inhalte abhängig von installierten Paketen

In der Linux-Welt stehen Handbücher und andere Dokumentationen in Form von Paketen zur Verfügung, ähnlich wie Software. Wie viele und welche Informationen Sie unter `/usr/share/docs` finden, hängt auch von den installierten (Dokumentations-) Paketen ab. Wenn Sie die hier genannten Unterverzeichnisse nicht finden können, prüfen Sie, ob die entsprechenden Pakete auf Ihrem System installiert sind, und fügen Sie sie gegebenenfalls mithilfe von YaST hinzu.

38.1.1 SUSE-Handbücher

Wir bieten unsere Handbücher im HTML- und PDF-Format in verschiedenen Sprachen an. Im Unterverzeichnis `Handbuch` finden Sie HTML-Versionen der meisten für Ihr Produkt verfügbaren SUSE-Handbücher. Eine Übersicht über sämtliche für Ihr Produkt verfügbare Dokumentation finden Sie im Vorwort der Handbücher.

Wenn mehr als eine Sprache installiert ist, enthält `/usr/share/doc/manual` möglicherweise verschiedene Sprachversionen der Handbücher. Die HTML-Versionen der SUSE-Handbücher stehen auch in der Hilfe an beiden Desktops zur Verfügung. Informationen zum Speicherort der PDF- und HTML-Versionen des Handbuchs auf Ihrem Installationsmedium finden Sie in den Versionshinweisen zu SUSE Linux Enterprise Server. Sie stehen auf Ihrem installierten System unter `/usr/share/doc/release-notes/` oder online auf Ihrer produktspezifischen Webseite unter http://www.suse.com/releasenotes/ zur Verfügung.

38.1.2 Dokumentation zu den einzelnen Paketen

Im Verzeichnis `packages` befindet sich die Dokumentation zu den auf Ihrem System installierten Software-Paketen. Für jedes Paket wird das entsprechende Unterverzeichnis `/usr/share/doc/packages/`*`Paketname`* erstellt. Es enthält README-Dateien für das Paket und manchmal Beispiele, Konfigurationsdateien und zusätzliche Skripten. In der folgenden Liste werden die typischen Dateien vorgestellt, die unter `/usr/share/doc/packages` zu finden sind. Diese Einträge sind nicht obligatorisch, und viele Pakete enthalten möglicherweise nur einige davon.

`AUTOREN`
: Liste der wichtigsten Entwickler.

`BUGS`

Bekannte Programmfehler oder Fehlfunktionen. Enthält möglicherweise auch einen Link zur Bugzilla-Webseite, auf der alle Programmfehler 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`

So installieren Sie dieses Paket auf Ihrem System. Da das Paket bereits installiert ist, wenn Sie diese Datei lesen können, können Sie den Inhalt dieser Datei bedenkenlos ignorieren.

`README`, `README.*`

Allgemeine Informationen zur Software, z. B. den Zweck und die Art ihrer Verwendung.

`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.

38.2 man-Seiten

man-Seiten sind ein wichtiger Teil des Linux-Hilfesystems. Sie erklären die Verwendung der einzelnen Befehle und deren Optionen und Parameter. Sie greifen auf man-Seiten mit dem Befehl **`man`** gefolgt vom Namen des jeweiligen Befehls zu, z. B. **`man ls`**.

Die man-Seiten werden direkt in der Shell angezeigt. Blättern Sie mit den Tasten Bild ↑ und Bild ↓ nach oben bzw. unten. Mit Pos 1 und Ende gelangen Sie an den Anfang bzw. das Ende eines Dokuments. und mit Q schließen Sie die man-Seiten. Weitere Informationen über den Befehl **man** erhalten Sie durch Eingabe von **man man**. man-Seiten sind in Kategorien unterteilt, wie in *Tabelle 38.1, „Manualpages – Kategorien und Beschreibungen“* gezeigt (diese Einteilung wurde direkt von der man-Seite für den Befehl „man“ übernommen).

TABELLE 38.1 MANUALPAGES – KATEGORIEN UND BESCHREIBUNGEN

Nummer	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

Jede man-Seite besteht aus den Abschnitten *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* und *AUTHOR*. Je nach Befehlstyp stehen möglicherweise auch weitere Abschnitte zur Verfügung.

38.3 Infoseiten

Eine weitere wichtige Informationsquelle sind Infoseiten. Diese sind im Allgemeinen ausführlicher als man-Seiten. Hier finden Sie nicht nur die Kommandozeilenoptionen, sondern manchmal sogar ganze Lernprogramme oder Referenzdokumentation. Die Infoseite für einen bestimmten Befehl zeigen Sie an, indem Sie **`info`** gefolgt vom Namen des Befehls eingeben, z. B. **`info ls`**. Infoseiten werden direkt in der Shell in einem Viewer angezeigt, in dem Sie zwischen den verschiedenen Abschnitten, so genannten „Knoten, navigieren können“. Mit Leertaste blättern Sie vorwärts und mit <– zurück. Innerhalb eines Knotens können Sie auch mit Bild ↑ und Bild ↓ navigieren, jedoch gelangen Sie nur mit Leertaste und <– zum vorherigen bzw. nächsten Knoten. Drücken Sie Q, um den Anzeigemodus zu beenden. Nicht für jedes Kommando gibt es eine Infoseite und umgekehrt.

38.4 Online-Ressourcen

Zusätzlich zu den Online-Versionen der SUSE-Handbücher, die unter `/usr/share/doc` installiert sind, können Sie auch auf die produktspezifischen Handbücher und Dokumentationen im Internet zugreifen. Eine Übersicht über alle Dokumentationen für SUSE Linux Enterprise Server erhalten Sie auf der produktspezifischen Dokumentations-Website unter http://www.suse.com/doc/.

Wenn Sie zusätzliche produktbezogene Informationen suchen, können Sie auch die folgenden Websites besuchen:

Technischer Support von SUSE

Falls Sie Fragen haben oder Hilfe bei technischen Problemen benötigen, steht der technische Support von SUSE unter http://www.suse.com/support/ bereit.

SUSE-Foren

Es gibt verschiedene Foren, in denen Sie sich an Diskussionen über SUSE-Produkte beteiligen können. Eine Liste finden Sie in http://forums.suse.com/.

SUSE Conversations

Eine Online-Community, die Artikel, Tipps, Fragen und Antworten und kostenlose Tools zum Download bietet: http://www.suse.com/communities/conversations/

GNOME-Dokumentation

Dokumentation für GNOME-Benutzer, -Administratoren und -Entwickler finden Sie unter http://library.gnome.org/.

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). Dies ist die wahrscheinlich umfangreichste Dokumentationsressource für Linux. Sie finden dort durchaus Lernprogramme, 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. Ein Teil der TLDP-Dokumentation ist auch unter SUSE Linux Enterprise Server verfügbar.

Sie können auch allgemeine Such-Engines ausprobieren. Sie können beispielsweise die Suchbegriffe `Linux CD-RW Hilfe` oder `OpenOffice Dateikonvertierung` eingeben, wenn Sie Probleme mit dem Brennen von CDs bzw. mit der LibreOffice-Dateikonvertierung haben.

39 Erfassen der Systeminformationen für den Support

Das Paket hostinfo in `SUSE Linux Enterprise Server` ermöglicht einen raschen Überblick über alle relevanten Systeminformationen eines Computers. Hier können Systemadministratoren außerdem ermitteln, ob ein Computer unbrauchbare (nicht unterstützte) Kernels enthält oder ob Drittanbieterpakete installiert sind.

Bei Problemen wird ein detaillierter Systembericht mit dem Kommandozeilenwerkzeug **`supportconfig`** oder mit dem YaST-*Support*-Modul erzeugt. Beide Werkzeuge sammeln Informationen zum System, etwa aktuelle Kernel-Version, Hardware, installierte Pakete, Partitionseinrichtung und einiges mehr. Hierbei wird ein TAR-Archiv mit Dateien ausgegeben. Wenn Sie eine Service-Anforderung öffnen, können Sie das TAR-Archiv für den globalen technischen Support heraufladen. Der Support hilft Ihnen, das gemeldete Problem zu lokalisieren und zu beheben.

Darüber hinaus können Sie die **`supportconfig`**-Ausgabe auf bekannte Probleme hin analysieren und so die Fehlerbehebung noch beschleunigen. SUSE Linux Enterprise Server bietet hierzu eine Anwendung und ein Kommandozeilenwerkzeug für die `supportconfig-Analyse` (SCA).

39.1 Anzeigen aktueller Systeminformationen

Mit dem Paket `hostinfo` erhalten Sie schnell und einfach eine Übersicht über alle relevanten Systeminformationen, sobald Sie sich bei einem Server anmelden. Nach der Installation auf einem Computer zeigt die Konsole die folgenden Informationen für jeden `root`-Benutzer an, der sich bei diesem Computer anmeldet:

BEISPIEL 39.1 AUSGABE VON `hostinfo` BEIM ANMELDEN ALS `root`

```
Hostname:                earth
Current As Of:           Wed 12 Mar 2014 03:57:05 PM CET
Distribution:            SUSE Linux Enterprise Server 12
 -Service Pack:          0
Architecture:            x86_64
Kernel Version:          3.12.12-3-default
```

```
 -Installed:              Mon 10 Mar 2014 03:15:05 PM CET
 -Status:                 Not Tainted
Last Updated Package:     Wed 12 Mar 2014 03:56:43 PM CET
 -Patches Needed:         0
 -Security:               0
 -3rd Party Packages:     0
IPv4 Address:             ens3 192.168.1.1
Total/Free/+Cache Memory: 983/95/383 MB (38% Free)
Hard Disk:                /dev/sda 10 GB
```

Wenn die Ausgabe auf einen `unbrauchbaren` Kernel-Status hinweist, finden Sie weitere Details in *Abschnitt 39.6, „Unterstützung für Kernelmodule“*.

39.2 Erfassen von Systeminformationen mit supportconfig

Zum Erstellen eines TAR-Archivs mit detaillierten Systeminformationen, die Sie an den globalen technischen Support übertragen können, verwenden Sie entweder direkt das Kommandozeilenwerkzeug **`supportconfig`** oder das YaST-*Support*-Modul. Das Kommandozeilenwerkzeug wird im Paket `supportutils` bereitgestellt, das standardmäßig installiert ist. Das YaST-*Support*-Modul baut zudem auf dem Kommandozeilenwerkzeug auf.

39.2.1 Erstellen einer Serviceanforderungsnummer

supportconfig-Archive können jederzeit erzeugt werden. Wenn Sie die supportconfig-Daten an den globalen technischen Support übertragen möchten, müssen Sie jedoch zunächst eine Service-Anforderungs-Nummer erstellen. Diese Nummer benötigen Sie, um das Archiv an den Support heraufladen zu können.

Zum Erstellen einer Service-Anforderung wechseln Sie zu https://scc.suse.com/support/requests, und befolgen Sie die Anweisungen auf dem Bildschirm. Schreiben Sie sich die 12-stellige Service-Anforderungs-Nummer auf.

Anmerkung: Datenschutzerklärung

SUSE und Micro Focus behandeln die Systemberichte als vertraulich. Weitere Informationen zum Datenschutz finden Sie unter https://www.suse.com/company/policies/privacy/.

39.2.2 Upload-Ziele

Sobald Sie eine Service-Anforderungs-Nummer erstellt haben, können Sie Ihre supportconfig-Archive gemäß den Anweisungen in *Prozedur 39.1, „Übertragen von Informationen an den Support mithilfe von YaST“* oder *Prozedur 39.2, „Übertragen von Informationen an den Support über die Kommandozeile“* an den globalen technischen Support heraufladen. Verwenden Sie eines der folgenden Upload-Ziele:

- Kunden in den USA: ftp://ftp.novell.com/incoming
- EMEA (Europa, Nahost und Afrika): ftp://support-ftp.suse.com/in

Alternativ können Sie das TAR-Archiv auch an Ihre Service-Anforderung anhängen und die URL für Service-Anforderungen verwenden: https://scc.suse.com/support/requests.

39.2.3 Erstellen eines supportconfig-Archivs mit YaST

Gehen Sie wie folgt vor, wenn Sie Ihre Systeminformationen mithilfe von YaST erfassen möchten:

1. Starten Sie YaST, und öffnen Sie das *Support*-Modul.

2. Klicken Sie auf *Berichts-Tarball erstellen*.

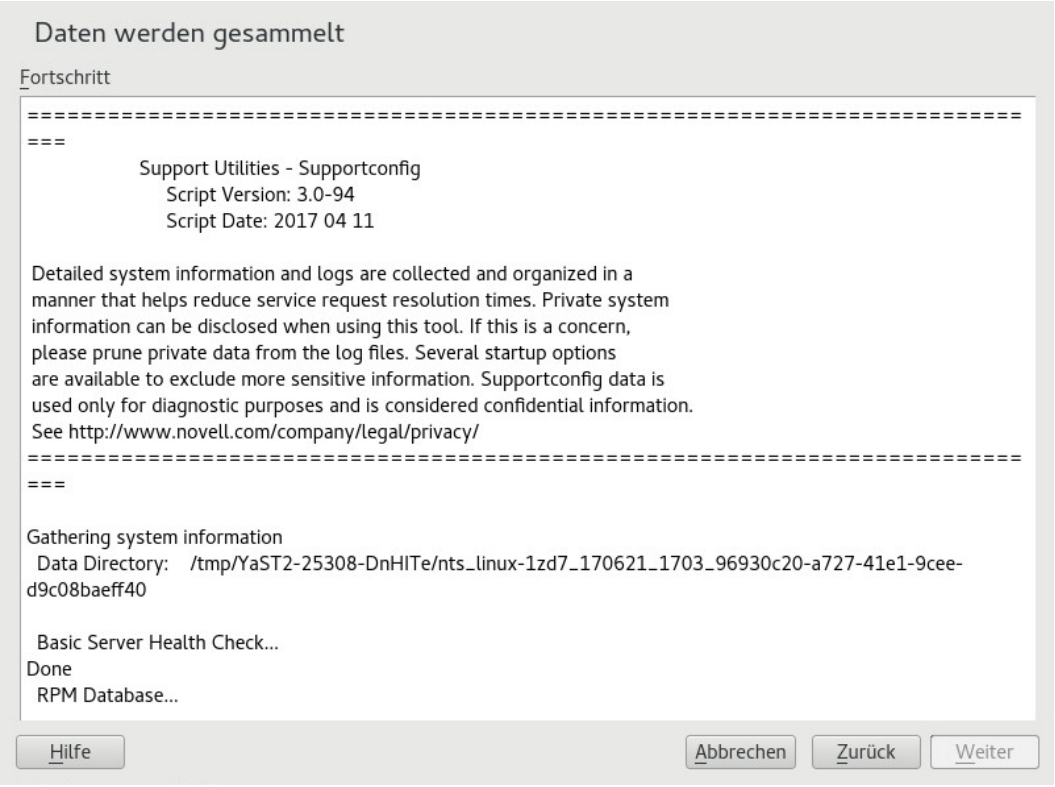
3. Wählen Sie im nächsten Fenster eine der supportconfig-Optionen in der Optionsliste aus. Die Option *Benutzerdefinierte Einstellungen (für Experten) verwenden* ist standardmäßig aktiviert. Wenn Sie die Berichtfunktion zuerst testen möchten, verwenden Sie *Nur eine minimale Anzahl von Informationen sammeln*. Weitere Hintergrundoptionen zu den weiteren Optionen finden Sie auf der man-Seite zu **`supportconfig`**.
   Fahren Sie mit *Weiter* fort.

4. Geben Sie Ihre Kontaktdaten ein. Die Daten werden in die Datei `basic-environment.txt` geschrieben und in das zu erstellende Archiv aufgenommen.

5. Soll das Archiv nach Abschluss der Datenerfassung an den globalen technischen Support gesendet werden, müssen Sie *Upload-Informationen* angeben. YaST schlägt automatisch einen Upload-Server vor. Wenn Sie diesen Server ändern möchten, erfahren Sie in *Abschnitt 39.2.2, „Upload-Ziele“*, welche Upload-Server verfügbar sind.
   Soll das Archiv erst später gesendet werden, können Sie die *Upload-Informationen* leer lassen.

6. Fahren Sie mit *Weiter* fort.

7. Es wird nun mit dem Sammeln der Informationen begonnen.



Fahren Sie nach Ende des Vorgangs mit *Weiter* fort.

8. Prüfen der Datensammlung: Wählen Sie den *Dateinamen* einer Protokolldatei aus. Der Inhalt dieser Datei wird in YaST angezeigt. Entfernen Sie bei Bedarf die Dateien, die nicht in das TAR-Archiv aufgenommen werden sollen, mit *Aus Daten entfernen*. Fahren Sie mit *Weiter* fort.

9. Speichern Sie das TAR-Archiv. Wenn Sie das YaST-Modul als `root`-Benutzer gestartet hatten, schlägt YaST standardmäßig den Ordner `/var/log` als Speicherort für das Archiv vor (ansonsten Ihr Benutzerverzeichnis). Das Format des Dateinamens lautet `nts_HOST_DATUM_UHRZEIT.tbz`.

10. Soll das Archiv direkt an den Support heraufgeladen werden, muss die Aktion *Protokolldatei-Tarball an URL heraufladen* aktiviert sein. Hier ist das *Upload-Ziel* angegeben, das YaST in *Schritt 5* vorgeschlagen hat. Wenn Sie das Upload-Ziel ändern möchten, erfahren Sie in *Abschnitt 39.2.2, „Upload-Ziele“*, welche Upload-Server verfügbar sind.

11. Um das Heraufladen zu überspringen, deaktivieren Sie die Option *Protokolldatei-Tarball zu URL heraufladen*.

12. Bestätigen Sie die Änderungen. Das YaST-Modul wird geschlossen.

39.2.4 Erstellen eines supportconfig-Archivs über die Kommandozeile

Mit dem nachstehenden Verfahren erstellen Sie ein supportconfig-Archiv, ohne das Archiv direkt an den Support zu übertragen. Zum Heraufladen müssen Sie das entsprechende Kommando mit den zugehörigen Optionen ausführen (siehe *Prozedur 39.2, „Übertragen von Informationen an den Support über die Kommandozeile“*).

1. Öffnen Sie eine Shell und melden Sie sich als `root` an.

2. Führen Sie **`supportconfig`** ohne Optionen aus. Damit werden die Standard-Systeminformationen gesammelt.

3. Warten Sie, bis das Tool den Vorgang beendet hat.

4. Der Standardspeicherort für das Archiv befindet sich unter `/var/log` und hat das Dateinamenformat `nts_HOST_DATUM_UHRZEIT.tbz`.

39.2.5 Allgemeine Optionen für Supportconfig

Das Dienstprogramm **supportconfig** wird in der Regel ohne Optionen aufgerufen. Zeigen Sie mit eine Liste aller Optionen für **supportconfig** `mit -h` an oder lesen Sie die man-Seite. Die folgende Liste enthält eine kurze Übersicht einiger gängiger Fälle:

Vermindern des Umfangs der erfassten Informationen

Verwenden Sie die Minimal-Option (`-m`):

```
supportconfig -m
```

Begrenzen der Informationen auf ein bestimmtes Thema

Wenn Sie in der standardmäßigen **supportconfig**-Ausgabe bereits ein Problem festgestellt haben und dieses Problem auf einen bestimmten Bereich oder eine bestimmte Funktionsgruppe beschränkt ist, sollten Sie die erfassten Informationen beim nächsten Ausführen von **supportconfig** auf diesen Bereich begrenzen. Wenn Sie beispielsweise ein Problem mit LVM erkannt haben und daher eine Änderung testen möchten, die Sie vor Kurzem an der LVM-Konfiguration hatten, reicht es völlig aus, nur die minimalen supportconfig-Informationen zu LVM zu erfassen:

```
supportconfig -i LVM
```

Eine vollständige Liste der Funktionsschlüsselwörter, mit denen Sie die erfassten Informationen auf einen bestimmten Bereich begrenzen, erhalten Sie mit dem

```
supportconfig -F
```

Aufnehmen zusätzlicher Kontaktinformationen in die Ausgabe:

```
supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

(alle in einer Zeile)

Sammeln von bereits rotierten Protokolldateien

```
supportconfig -l
```

Nützlich ist dies insbesondere in Umgebungen mit hohem Protokollierungsaufkommen sowie nach einem Kernel-Crash, wenn syslog die Protokolldateien nach dem Neustart rotiert.

39.3 Übertragen von Informationen an den globalen technischen Support

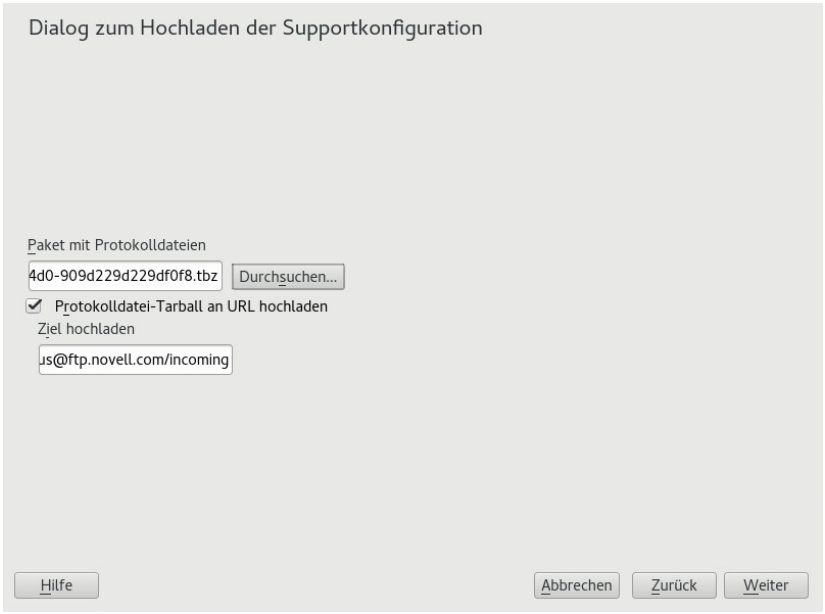
Zum Übertragen der Systeminformationen an den globalen technischen Support verwenden Sie das YaST-*Support*-Modul oder das Befehlszeilenprogramm `supportconfig`. Falls Serverprobleme auftreten und Sie Hilfe benötigen, müssen Sie zunächst eine Serviceanforderung öffnen. Weitere Informationen finden Sie unter *Abschnitt 39.2.1, „Erstellen einer Serviceanforderungsnummer“*.

In den nachfolgenden Beispielen fungiert die Zahl *12345678901* als Platzhalter für die Service-Anforderungs-Nummer. Ersetzen Sie die Zahl *12345678901* durch die Service-Anforderungs-Nummer, die Sie in *Abschnitt 39.2.1, „Erstellen einer Serviceanforderungsnummer“* erstellt haben.

PROZEDUR 39.1 ÜBERTRAGEN VON INFORMATIONEN AN DEN SUPPORT MITHILFE VON YAST

Im nachfolgenden Verfahren wird angenommen, dass Sie bereits ein supportconfig-Archiv erstellt, jedoch noch nicht heraufgeladen haben. Nehmen Sie in jedem Fall Ihre Kontaktdaten in das Archiv auf (siehe *Abschnitt 39.2.3, „Erstellen eines supportconfig-Archivs mit YaST“*, *Schritt 4*). Weitere Anweisungen zum Erzeugen und Übertragen eines supportconfig-Archivs in einem einzigen Arbeitsgang finden Sie in *Abschnitt 39.2.3, „Erstellen eines supportconfig-Archivs mit YaST“*.

1. Starten Sie YaST, und öffnen Sie das *Support*-Modul.
2. Klicken Sie auf *Heraufladen*.
3. Geben Sie unter *Paket mit Protokolldateien* den Pfad zum vorhandenen supportconfig-Archiv ein, oder klicken Sie auf *Durchsuchen*, und wechseln Sie zu dem Ordner, in dem sich das Archiv befindet.
4. YaST schlägt automatisch einen Upload-Server vor. Wenn Sie diesen Server ändern möchten, erfahren Sie in *Abschnitt 39.2.2, „Upload-Ziele“*, welche Upload-Server verfügbar sind.



Fahren Sie mit *Weiter* fort.

5. Klicken Sie auf *Fertig stellen*.

PROZEDUR 39.2 ÜBERTRAGEN VON INFORMATIONEN AN DEN SUPPORT ÜBER DIE KOMMANDOZEILE

Im nachfolgenden Verfahren wird angenommen, dass Sie bereits ein supportconfig-Archiv erstellt, jedoch noch nicht heraufgeladen haben. Weitere Anweisungen zum Erzeugen und Übertragen eines supportconfig-Archivs in einem einzigen Arbeitsgang finden Sie in *Abschnitt 39.2.3, „Erstellen eines supportconfig-Archivs mit YaST“*.

1. Server mit Internetkonnektivität:

   a. Führen Sie das folgende Kommando aus, um das Standard-Uploadziel zu verwenden:

   ```
   supportconfig -ur 12345678901
   ```

   b. Verwenden Sie das folgende sichere Upload-Ziel:

   ```
   supportconfig -ar 12345678901
   ```

2. Server *ohne* Internetkonnektivität

   a. Führen Sie Folgendes aus:

   ```
   supportconfig -r 12345678901
   ```

b. Laden Sie das Archiv `/var/log/nts_SR12345678901*tbz` manuell auf einen unserer FTP-Server herauf. Der richtige Server ist abhängig von Ihrem Standort. Einen Überblick finden Sie unter *Abschnitt 39.2.2, „Upload-Ziele“*.

3. Sobald das TAR-Archiv im Eingangsverzeichnis unseres FTP-Servers eingeht, wird es automatisch an Ihre Service-Anforderung angehängt.

39.4 Analysieren von Systeminformationen

Die mit **`supportconfig`** erstellten Systemberichte können auf bekannte Probleme hin analysiert werden, so dass die Fehlerbehebung noch beschleunigt wird. SUSE Linux Enterprise Server bietet hierzu eine Anwendung und ein Kommandozeilenwerkzeug für die `supportconfig-Analyse` (SCA). Die SCA-Appliance ist ein serverseitiges, nicht interaktives Werkzeug. Das SCA-Werkzeug (**`scatool`**) wird auf der Client-Seite über die Kommandozeile ausgeführt. Beide Werkzeuge analysieren die supportconfig-Archive von betroffenen Servern. Die erste Serveranalyse erfolgt in der SCA-Appliance oder auf dem Arbeitsplatzrechner, auf dem scatool ausgeführt wird. Auf dem Produktionsserver werden keine Analysezyklen durchgeführt.

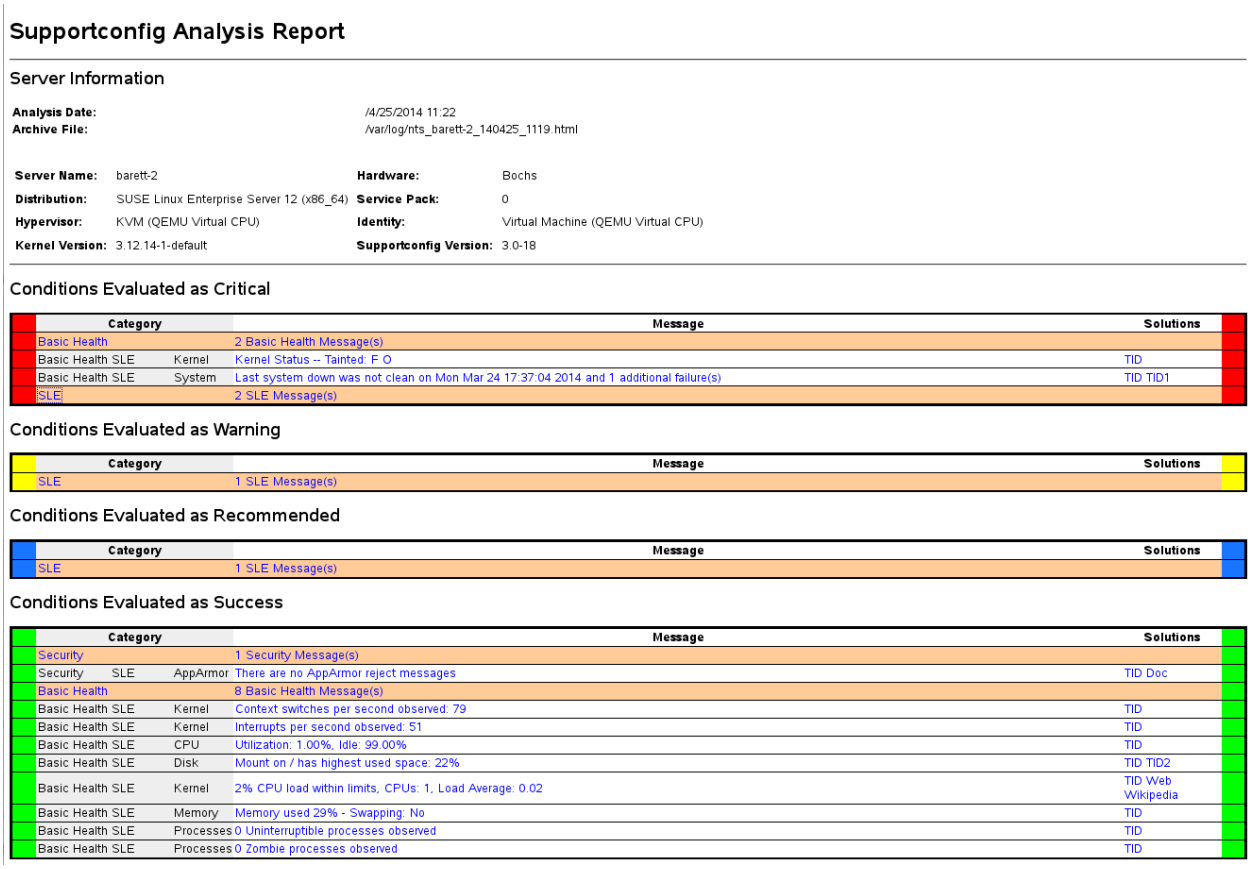
Sowohl für die Appliance als auch für das Kommandozeilenwerkzeug sind zusätzliche produktspezifische Schemata erforderlich, damit die supportconfig-Ausgabe für die entsprechenden Produkte analysiert werden kann. Jedes Schema ist ein Skript, mit dem ein supportconfig-Archiv auf genau ein bekanntes Problem hin analysiert und ausgewertet wird. Die Schemata stehen als RPM-Pakete zur Verfügung.

Wenn Sie beispielsweise supportconfig-Archive analysieren möchten, die auf einem Computer mit SUSE Linux Enterprise 11 erzeugt wurden, müssen Sie dort das Paket `sca-patterns-sle11` zusammen mit dem SCA-Werkzeug installieren (oder auf dem Computer, der als SCA-Appliance-Server dienen soll). Zum Analysieren von supportconfig-Archiven, die auf einem Rechner mit SUSE Linux Enterprise 10 erzeugt wurden, benötigen Sie das Paket `sca-patterns-sle10`.

Sie können außerdem eigene Schemata entwickeln (kurze Beschreibung siehe *Abschnitt 39.4.3, „Entwickeln von benutzerdefinierten Analyseschemata“*).

39.4.1 SCA-Kommandozeilenwerkzeug

Mithilfe des SCA-Kommandozeilenwerkzeugs können Sie einen lokalen Rechner sowohl mit **supportconfig** als auch mit den auf dem lokalen Rechner installierten Analyseschemata analysieren. Das Werkzeug erstellt einen HTML-Bericht mit den Analyseergebnissen. Ein Beispiel finden Sie in *Abbildung 39.1, „Mit dem SCA-Werkzeug erstellter HTML-Bericht“*.



Supportconfig Analysis Report

Server Information

Analysis Date:	/4/25/2014 11:22		
Archive File:	/var/log/nts_barett-2_140425_1119.html		
Server Name:	barett-2	**Hardware:**	Bochs
Distribution:	SUSE Linux Enterprise Server 12 (x86_64)	**Service Pack:**	0
Hypervisor:	KVM (QEMU Virtual CPU)	**Identity:**	Virtual Machine (QEMU Virtual CPU)
Kernel Version:	3.12.14-1-default	**Supportconfig Version:**	3.0-18

Conditions Evaluated as Critical

Category			Message	Solutions
Basic Health			2 Basic Health Message(s)	
Basic Health	SLE	Kernel	Kernel Status -- Tainted: F O	TID
Basic Health	SLE	System	Last system down was not clean on Mon Mar 24 17:37:04 2014 and 1 additional failure(s)	TID TID1
SLE			2 SLE Message(s)	

Conditions Evaluated as Warning

Category	Message	Solutions
SLE	1 SLE Message(s)	

Conditions Evaluated as Recommended

Category	Message	Solutions
SLE	1 SLE Message(s)	

Conditions Evaluated as Success

Category			Message	Solutions
Security			1 Security Message(s)	
Security	SLE	AppArmor	There are no AppArmor reject messages	TID Doc
Basic Health			8 Basic Health Message(s)	
Basic Health	SLE	Kernel	Context switches per second observed: 79	TID
Basic Health	SLE	Kernel	Interrupts per second observed: 51	TID
Basic Health	SLE	CPU	Utilization: 1.00%, Idle: 99.00%	TID
Basic Health	SLE	Disk	Mount on / has highest used space: 22%	TID TID2
Basic Health	SLE	Kernel	2% CPU load within limits, CPUs: 1, Load Average: 0.02	TID Web Wikipedia
Basic Health	SLE	Memory	Memory used 29% - Swapping: No	TID
Basic Health	SLE	Processes	0 Uninterruptible processes observed	TID
Basic Health	SLE	Processes	0 Zombie processes observed	TID

ABBILDUNG 39.1 MIT DEM SCA-WERKZEUG ERSTELLTER HTML-BERICHT

Das Kommando **scatool** wird mit dem Paket `sca-server-report` bereitgestellt. Die Installation erfolgt nicht standardmäßig. Darüber hinaus benötigen Sie das Paket `sca-patterns-base` sowie alle produktspezifischen Pakete `sca-patterns-*` für das Produkt, das auf dem Rechner installiert ist, auf dem das Kommando **scatool** ausgeführt werden soll.

Führen Sie das Kommando **scatool** als `root`-Benutzer oder mit **sudo** aus. Beim Aufrufen des SCA-Werkzeugs können Sie wahlweise ein vorhandenes **supportconfig**-TAR-Archiv analysieren oder auch ein neues Archiv erzeugen und im gleichen Arbeitsgang analysieren. Das Werkzeug bietet zudem eine interaktive Konsole (mit automatischer Ausfüllung der Karteireiter) sowie die Möglichkeit, **supportconfig** auf einem externen Rechner auszuführen und die anschließende Analyse auf dem lokalen Rechner vorzunehmen.

Einige Kommandobeispiele:

`sudo scatool -s`

Ruft **`supportconfig`** auf und erzeugt ein neues supportconfig-Archiv auf dem lokalen Rechner. Analysiert das Archiv auf bekannte Probleme mithilfe der passenden SCA-Analyseschemata für das installierte Produkt. Zeigt den Pfad zum HTML-Bericht an, der aus den Analyseergebnissen erzeugt wird. Der Bericht wird in der Regel in dasselbe Verzeichnis geschrieben wie das supportconfig-Archiv.

`sudo scatool -s -o` *`/opt/sca/reports/`*

Wie **`sudo scatool -s`**, mit dem Unterschied, dass der HTML-Bericht in den mit der Option `-o` angegebenen Pfad geschrieben wird.

`sudo scatool -a` *`PFAD_ZU_TARBALL_ODER_VERZEICHNIS`*

Analysiert die angegebene supportconfig-Archivdatei (oder das angegebene Verzeichnis, in das das supportconfig-Archiv extrahiert wurde). Der erzeugte HTML-Bericht wird an demselben Speicherort gespeichert wie das supportconfig-Archiv oder -Verzeichnis.

`sudo scatool -a` *`SLES_SERVER.COMPANY.COM`*

Stellt eine SSH-Verbindung zu einem externen Server *`SLES_SERVER.COMPANY.COM`* her und führt **`Supportconfig`** auf dem Server aus. Das supportconfig-Archiv wird dann auf den lokalen Rechner zurückkopiert und dort analysiert. Der erzeugte HTML-Bericht wird standardmäßig in das Verzeichnis `/var/log` gespeichert. (Auf dem Server *`SLES_SERVER.COMPANY.COM`* wird ausschließlich das Supportconfig-Archiv erstellt.)

`sudo scatool -c`

Startet die interaktive Konsole für **`scatool`**. Zum Abrufen der verfügbaren Kommandos drücken Sie zweimal →|.

Weitere Optionen und Informationen erhalten Sie mit dem Kommando **`sudo scatool -h`** und auf der man-Seite zu **`scatool`**.

39.4.2 SCA-Appliance

Wenn Sie die supportconfig-Archive mit der SCA-Appliance analysieren, müssen Sie einen dedizierten Server (oder einen dedizierten virtuellen Computer) als SCA-Appliance-Server konfigurieren. Auf dem SCA-Appliance-Server können Sie dann supportconfig-Archive von allen Rechnern im Unternehmen analysieren, auf denen SUSE Linux Enterprise Server oder SUSE Linux

Enterprise Desktop ausgeführt wird. Zum Analysieren laden Sie die gewünschten supportconfig-Archive einfach auf den Appliance-Server herauf. Ein weiterer Eingriff Ihrerseits ist nicht erforderlich. In einer MariaDB-Datenbank verfolgt die SCA-Appliance alle bereits analysierten supportconfig-Archive. Sie können die SCA-Berichte direkt über die Webschnittstelle der Appliance lesen. Alternativ können Sie in der Appliance angeben, dass der HTML-Bericht per Email an einen verwaltungsbefugten Benutzer gesendet werden soll. Weitere Informationen finden Sie unter *Abschnitt 39.4.2.5.4, „Senden von SCA-Berichten per E-Mail“*.

39.4.2.1 Schnelleinführung zur Installation

Zum raschen Installieren und Einrichten der SCA-Appliance über die Kommandozeile gehen Sie nach den folgenden Anweisungen vor. Das Verfahren richtet sich an fortgeschrittene Benutzer und umfasst lediglich die reinen Installations- und Einrichtungskommandos. Weitere Informationen finden Sie in der detaillierteren Beschreibung in *Abschnitt 39.4.2.2, „Voraussetzungen“* bis *Abschnitt 39.4.2.3, „Installation und grundlegende Einrichtung“*.

VORAUSSETZUNGEN

- Web- und LAMP-Schema
- Web- und Skripterstellungsmodul (zur Auswahl dieses Moduls muss der Rechner registriert sein).

Anmerkung: Erforderliche `root`-Berechtigungen

Alle Befehle im folgenden Vorgang müssen als `root` ausgeführt werden.

PROZEDUR 39.3 INSTALLATION MIT HERAUFLADEN ÜBER ANONYMEN FTP-ZUGANG

Sobald die Appliance eingerichtet ist und ausgeführt wird, sind keine weiteren manuellen Eingriffe mehr erforderlich. Diese Methode zur Einrichtung der Appliance eignet sich daher ideal für das Erstellen und Heraufladen von supportconfig-Archiven mithilfe von Cron-Aufträgen.

1. Melden Sie sich auf dem Rechner, auf dem die Appliance installiert werden soll, bei einer Konsole an, und führen Sie folgende Kommandos aus:

```
zypper install sca-appliance-* sca-patterns-* vsftpd
systemctl enable apache2
systemctl start apache2
```

```
systemctl enable vsftpd
systemctl start vsftpd
yast ftp-server
```

2. Wählen Sie im YaST-FTP-Server-Modul Folgendes: *Authentifizierung* › *Heraufladen aktivieren* › *Anonyme Benutzer dürfen hochladen* › *Beenden* › *Ja*. Der Ordner */srv/ftp/upload* wird erstellt.

3. Führen Sie folgende Befehle aus:

```
systemctl enable mysql
systemctl start mysql
mysql_secure_installation
setup-sca -f
```

Bei der sicheren MySQL-Erstellung (mysql_secure_installation) wird ein `root`-Passwort für MariaDB erstellt.

PROZEDUR 39.4 INSTALLATION MIT HERAUFLADEN ÜBER SCP/TMP

Bei dieser Methode zum Einrichten der Appliance ist ein manueller Eingriff erforderlich (das SSH-Passwort muss eingegeben werden).

1. Melden Sie sich auf dem Rechner, auf dem die Appliance installiert werden soll, bei einer Konsole an:

2. Führen Sie folgende Befehle aus:

```
zypper install sca-appliance-* sca-patterns-*
systemctl enable apache2
systemctl start apache2
sudo systemctl enable mysql
systemctl start mysql
mysql_secure_installation
setup-sca
```

39.4.2.2 Voraussetzungen

Zum Ausführen eines Appliance-Servers müssen folgende Voraussetzungen erfüllt sein:

- Alle Pakete `sca-appliance-*`.
- Paket `sca-patterns-base`. Zusätzlich alle produktspezifischen Pakete `sca-patterns-*` für den Typ der supportconfig-Archive, die mit der Appliance analysiert werden sollen.

- Apache
- PHP
- MariaDB
- Anonymer FTP-Server (optional)

39.4.2.3 Installation und grundlegende Einrichtung

Wie in *Abschnitt 39.4.2.2, „Voraussetzungen“* beschrieben, bestehen mehrere Abhängigkeiten der SCA-Appliance von anderen Paketen. Aus diesem Grund sind einige Vorbereitungsmaßnahmen erforderlich, bevor Sie den SCA-Appliance-Server installieren und einrichten können:

1. Für Apache und MariaDB installieren Sie die Installationsschemata `Web` und `LAMP`.
2. Richten Sie Apache und MariaDB ein (und optional einen anonymen FTP-Server). Weitere Informationen hierzu finden Sie unter *Kapitel 31, Der HTTP-Server Apache* und *Kapitel 32, Einrichten eines FTP-Servers mit YaST*.
3. Konfigurieren Sie Apache und MariaDB für das Starten beim Systemstart:

   ```
   sudo systemctl enable apache2 mysql
   ```

4. Starten Sie beide Services:

   ```
   sudo systemctl start apache2 mysql
   ```

Sie können nun die SCA-Appliance gemäß den Anweisungen in *Prozedur 39.5, „Installieren und Konfigurieren der SCA-Appliance“* installieren und einrichten.

PROZEDUR 39.5 INSTALLIEREN UND KONFIGURIEREN DER SCA-APPLIANCE

Nach dem Installieren der Pakete nehmen Sie mit dem Skript **`setup-sca`** die grundlegende Konfiguration der MariaDB-Administrations-/Berichtdatenbank vor, die von der SCA-Appliance genutzt wird.

Hiermit können Sie die folgenden Optionen für das Heraufladen der supportconfig-Archive von den Rechnern in die SCA-Appliance konfigurieren:

- **`scp`**
- Anonymer FTP-Server

1. Installieren Sie die Appliance und die SCA-Basisschema-Bibliothek:

```
sudo zypper install sca-appliance-* sca-patterns-base
```

2. Installieren Sie außerdem die Schemapakete für die zu analysierenden supportconfig-Archive. Wenn sich beispielsweise Server mit SUSE Linux Enterprise Server 11 und SUSE Linux Enterprise 12 in Ihrer Umgebung befinden, installieren Sie sowohl das Paket `sca-patterns-sle11` als auch das Paket `sca-patterns-sle12`.
So installieren Sie alle verfügbaren Pakete:

```
zypper install sca-patterns-*
```

3. Nehmen Sie mit dem Skript **`setup-sca`** die grundlegende Einrichtung der SCA-Appliance vor. Der Aufruf dieses Skripts ist abhängig davon, ob die supportconfig-Archive auf den SCA-Appliance-Server heraufgeladen werden sollen:

   - Wenn Sie einen anonymen FTP-Server konfiguriert haben, bei dem das Verzeichnis `/srv/ftp/upload` genutzt wird, führen Sie das Einrichtungsskript mit der Option `-f` aus, und befolgen Sie die Anweisungen auf dem Bildschirm:

     ```
     setup-sca -f
     ```

     #### Anmerkung: FTP-Server mit anderem Verzeichnis

     Wenn der FTP-Server ein anderes Verzeichnis verwendet (also nicht das Verzeichnis `/srv/ftp/upload`), passen Sie zunächst die folgenden Konfigurationsdateien so an, dass sie auf das richtige Verzeichnis verweisen: `/etc/sca/sdagent.conf` und `/etc/sca/sdbroker.conf`.

   - Sollen supportconfig-Dateien mit **`scp`** in das Verzeichnis `/tmp` des SCA-Appliance-Servers heraufgeladen werden, rufen Sie das Einrichtungsskript ohne Parameter auf, und befolgen Sie die Anweisungen auf dem Bildschirm:

     ```
     setup-sca
     ```

   Das Einrichtungsskript überprüft, ob die Voraussetzungen erfüllt sind, und konfiguriert die erforderlichen Komponenten. Sie werden zur Eingabe von zwei Passwörtern aufgefordert: das MySQL-`root`-Passwort für die eingerichtete MariaDB sowie ein Webbenutzer-Passwort, mit dem Sie sich bei der Webschnittstelle der SCA-Appliance anmelden.

4. Geben Sie das vorhandene MariaDB-`root`-Passwort ein. Damit kann die SCA-Appliance eine Verbindung zur MariaDB herstellen.

5. Definieren Sie ein Passwort für den Webbenutzer. Dieses Passwort wird in die Datei `/srv/www/htdocs/sca/web-config.php` geschrieben und als Passwort für den Benutzer `scdiag` eingerichtet. Sowohl der Benutzername als auch das Passwort können jederzeit geändert werden (siehe *Abschnitt 39.4.2.5.1, „Passwort für die Webschnittstelle“*).

Nach erfolgter Installation und Einrichtung ist die SCA-Appliance einsatzbereit (siehe *Abschnitt 39.4.2.4, „Verwenden der SCA-Appliance“*). Sie sollten jedoch bestimmte Optionen noch bearbeiten, beispielsweise das Passwort für die Webschnittstelle oder die Quelle für die SCA-Schemaaktualisierungen ändern, den Archivierungsmodus aktivieren oder Email-Benachrichtigungen konfigurieren. Weitere Informationen finden Sie in *Abschnitt 39.4.2.5, „Anpassen der SCA-Appliance“*.

Warnung: Datenschutz

Die Berichte auf dem SCA-Appliance-Server enthalten sicherheitsrelevante Daten zu den Rechnern, auf denen die supportconfig-Archive analysiert wurden. Schützen Sie daher die Daten auf dem SCA-Appliance-Server vor unbefugtem Zugriff.

39.4.2.4 Verwenden der SCA-Appliance

Sie können vorhandene supportconfig-Archive manuell in die SCA-Appliance heraufladen oder neue supportconfig-Archive erstellen und im gleichen Arbeitsgang in die SCA-Appliance heraufladen. Das Heraufladen kann über FTP oder SCP erfolgen. In beiden Fällen benötigen Sie die URL, unter der sich die SCA-Appliance befindet. Zum Heraufladen über FTP muss ein FTP-Server für die SCA-Appliance installiert sein (siehe *Prozedur 39.5, „Installieren und Konfigurieren der SCA-Appliance“*).

39.4.2.4.1 Heraufladen von supportconfig-Archiven an die SCA-Appliance

- So können Sie ein supportconfig-Archiv erstellen und über einen (anonymen) FTP-Zugang heraufladen:

```
sudo supportconfig -U "ftp://SCA-APPLIANCE.COMPANY.COM/upload"
```

- So können Sie ein supportconfig-Archiv erstellen und über SCP heraufladen:

```
sudo supportconfig -U "scp://SCA-APPLIANCE.COMPANY.COM/tmp"
```

  Sie werden aufgefordert, das `root`-Benutzerpasswort für den Server einzugeben, auf dem die SCA-Appliance ausgeführt wird.

- Zum manuellen Heraufladen von einem oder mehreren Archiven kopieren Sie die vorhandenen Archivdateien (in der Regel unter `/var/log/nts_*.tbz`) in die SCA-Appliance. Als Ziel verwenden Sie entweder das Verzeichnis `/tmp` oder das Verzeichnis `/srv/ftp/upload` des Appliance-Servers (wenn FTP für den SCA-Appliance-Server konfiguriert ist).

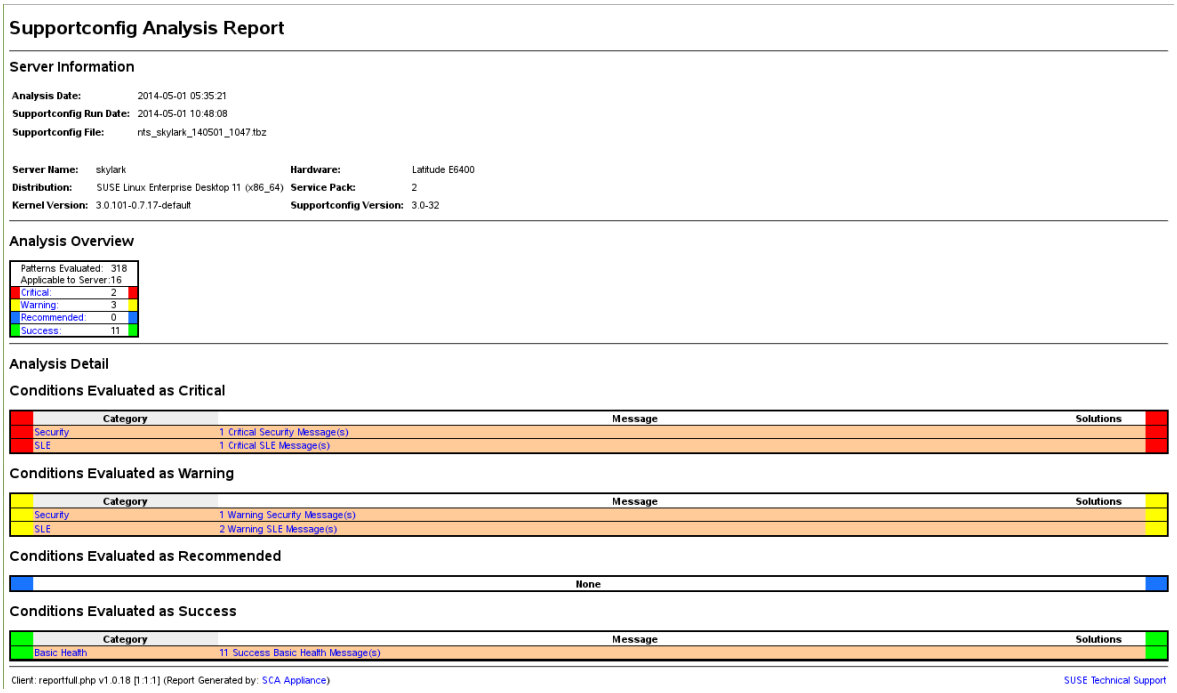
39.4.2.4.2 Anzeigen von SCA-Berichten

Die SCA-Berichte können auf jedem Rechner angezeigt werden, auf dem ein Browser installiert ist und der auf die Berichtindexseite der SCA-Appliance zugreifen kann.

1. Starten Sie einen Webbrowser, und aktivieren Sie JavaScript und Cookies.
2. Als URL geben Sie die Berichtindexseite der SCA-Appliance ein.

   ```
   https://sca-appliance.company.com/sca
   ```

   Fragen Sie im Zweifelsfall Ihren Systemadministrator.
3. Sie werden aufgefordert, einen Benutzernamen und ein Passwort für die Anmeldung einzugeben.



Supportconfig Analysis Report

Server Information

Analysis Date: 2014-05-01 05:35:21
Supportconfig Run Date: 2014-05-01 10:48:08
Supportconfig File: nts_skylark_140501_1047.tbz

Server Name: skylark
Distribution: SUSE Linux Enterprise Desktop 11 (x86_64)
Kernel Version: 3.0.101-0.7.17-default
Hardware: Latitude E6400
Service Pack: 2
Supportconfig Version: 3.0-32

Analysis Overview

Patterns Evaluated:	318
Applicable to Server:	16
Critical:	2
Warning:	3
Recommended:	0
Success:	11

Analysis Detail

Conditions Evaluated as Critical

Category	Message	Solutions
Security	1 Critical Security Message(s)	
SLE	1 Critical SLE Message(s)	

Conditions Evaluated as Warning

Category	Message	Solutions
Security	1 Warning Security Message(s)	
SLE	2 Warning SLE Message(s)	

Conditions Evaluated as Recommended

None

Conditions Evaluated as Success

Category	Message	Solutions
Basic Health	11 Success Basic Health Message(s)	

Client: reportfull.php v1.0.18 [1.1.1] (Report Generated by: SCA Appliance)
SUSE Technical Support

ABBILDUNG 39.2 MIT DER SCA-APPLIANCE ERSTELLTER HTML-BERICHT

4. Nach erfolgter Anmeldung klicken Sie auf das Datum des gewünschten Berichts.

5. Klicken Sie zunächst auf die Kategorie *Grundstatus*.

6. Klicken Sie in der Spalte *Nachricht* auf einen Eintrag. Der entsprechende Artikel in der SUSE Knowledgebase wird geöffnet. Lesen Sie die vorgeschlagene Lösung, und befolgen Sie die Anweisungen.

7. Wenn die Spalte *Lösungen* im *Supportconfig-Analysebericht* weitere Einträge enthält, klicken Sie auf diese Einträge. Lesen Sie die vorgeschlagene Lösung, und befolgen Sie die Anweisungen.

8. Suchen Sie in der SUSE Knowledgebase (http://www.suse.com/support/kb/) nach Ergebnissen, die direkt mit dem für SCA erkannten Problem zusammenhängen. Bearbeiten Sie die Probleme.

9. Suchen Sie nach Ergebnissen, die proaktiv bearbeitet werden können, damit künftige Probleme vermieden werden.

39.4.2.5 Anpassen der SCA-Appliance

In den nachfolgenden Abschnitten erfahren Sie, wie Sie das Passwort für die Webschnittstelle und die Quelle für die SCA-Schemaaktualisierungen ändern, den Archivierungsmodus aktivieren und Email-Benachrichtigungen archivieren.

39.4.2.5.1 Passwort für die Webschnittstelle

Zur Anmeldung bei der Webschnittstelle der SCA-Appliance benötigen Sie einen Benutzernamen und ein Passwort. Der Standard-Benutzername lautet `scdiag` und das Standardpasswort ist `linux` (sofern nicht anders festgelegt, siehe *Prozedur 39.5, „Installieren und Konfigurieren der SCA-Appliance“*). Ändern Sie das Standard-Passwort so bald wie möglich in ein sicheres Passwort. Auch den Benutzernamen können Sie bearbeiten.

PROZEDUR 39.6 ÄNDERN DES BENUTZERNAMENS ODER DES PASSWORTS FÜR DIE WEBSCHNITTSTELLE

1. Melden Sie sich an der Systemkonsole des SCA-Appliance-Servers als `root`-Benutzer an.
2. Öffnen Sie die Datei `/srv/www/htdocs/sca/web-config.php` in einem Editor.
3. Ändern Sie die Werte für `$username` und `$password`.
4. Speichern und schließen Sie die Datei.

39.4.2.5.2 Aktualisierungen der SCA-Schemata

Standardmäßig werden alle Pakete `sca-patterns-*` regelmäßig mit einem `root` Cron-Auftrag aktualisiert, mit dem jeden Abend das Skript `sdagent-patterns` ausgeführt wird, das wiederum **`zypper update sca-patterns-*`** startet. Bei einer normalen Systemaktualisierung werden alle SCA-Appliance- und Schemapakete aktualisiert. So aktualisieren Sie die SCA-Appliance und die Schemata manuell:

```
sudo zypper update sca-*
```

Die Aktualisierungen werden standardmäßig aus dem Aktualisierungs-Respository für SUSE Linux Enterprise 12 SP5 installiert. Bei Bedarf können Sie die Quelle der Aktualisierungen in einen SMT-Server ändern. Beim Ausführen von **`zypper update sca-patterns-*`** durch `sdagent-patterns` werden die Aktualisierungen über den derzeit konfigurierten Aktualisierungskanal abgerufen. Wenn sich dieser Kanal auf einem SMT-Server befindet, werden die Pakete von diesem Server abgerufen.

PROZEDUR 39.7 DEAKTIVIEREN DER AUTOMATISCHEN AKTUALISIERUNG DER SCA-SCHEMATA

1. Melden Sie sich an der Systemkonsole des SCA-Appliance-Servers als `root`-Benutzer an.
2. Öffnen Sie die Datei `/etc/sca/sdagent-patterns.conf` in einem Editor.
3. Ändern Sie den Eintrag

   ```
   UPDATE_FROM_PATTERN_REPO=1
   ```

   in

   ```
   UPDATE_FROM_PATTERN_REPO=0
   ```
4. Speichern und schließen Sie die Datei. Die Änderung tritt ohne Neustart des Rechners in Kraft.

39.4.2.5.3 Archivierungsmodus

Alle supportconfig-Archive werden aus der SCA-Appliance gelöscht, sobald sie analysiert und die zugehörigen Ergebnisse in der MariaDB-Datenbank gespeichert wurden. Wenn Sie Kopien der supportconfig-Archive eines Rechners aufheben, kann dies allerdings ggf. eine spätere Fehlerbehebung erleichtern. Standardmäßig ist der Archivierungsmodus deaktiviert.

PROZEDUR 39.8 AKTIVIEREN DES ARCHIVIERUNGSMODUS IN DER SCA-APPLIANCE

1. Melden Sie sich an der Systemkonsole des SCA-Appliance-Servers als `root`-Benutzer an.
2. Öffnen Sie die Datei `/etc/sca/sdagent.conf` in einem Editor.
3. Ändern Sie den Eintrag

   ```
   ARCHIVE_MODE=0
   ```

   in

   ```
   ARCHIVE_MODE=1
   ```
4. Speichern und schließen Sie die Datei. Die Änderung tritt ohne Neustart des Rechners in Kraft.

Sobald der Archivierungsmodus aktiviert ist, werden die supportconfig-Dateien nicht mehr von der SCA-Appliance gelöscht, sondern im Verzeichnis `/var/log/archives/saved` gespeichert.

39.4.2.5.4 Senden von SCA-Berichten per E-Mail

Die SCA-Appliance kann für jede analysierte supportconfig-Datei einen HTML-Bericht per Email schicken. Diese Funktion ist standardmäßig deaktiviert. Wenn Sie sie aktivieren, können Sie eine Liste von E-Mail-Adressen definieren, an die die Berichte gesendet werden sollen, sowie die Statusnachrichtenebene festlegen, die das Versenden der Berichte auslöst (`STATUS_NOTIFY_LEVEL`).

MÖGLICHE WERTE FÜR `STATUS_NOTIFY_LEVEL`

$STATUS_OFF

Deaktiviert das Senden von HTML-Berichten.

$STATUS_CRITICAL

Sendet nur SCA-Berichte, die den Status CRITICAL enthalten.

$STATUS_WARNING

Sendet nur SCA-Berichte, die den Status WARNING oder CRITICAL enthalten.

$STATUS_RECOMMEND

Sendet nur SCA-Berichte, die den Status RECOMMEND, WARNING oder CRITICAL enthalten.

$STATUS_SUCCESS

Sendet SCA-Berichte, die den Status SUCCESS, RECOMMEND, WARNING oder CRITICAL enthalten.

PROZEDUR 39.9 KONFIGURIEREN VON EMAIL-BENACHRICHTIGUNGEN FÜR SCA-BERICHTE

1. Melden Sie sich an der Systemkonsole des SCA-Appliance-Servers als `root`-Benutzer an.
2. Öffnen Sie die Datei `/etc/sca/sdagent.conf` in einem Editor.
3. Wechseln Sie zum Eintrag `STATUS_NOTIFY_LEVEL`. Standardmäßig ist hier `$STATUS_OFF` festgelegt (Email-Benachrichtigungen sind deaktiviert).
4. Zum Aktivieren der Email-Benachrichtigungen ändern Sie `$STATUS_OFF` in die Statusebene, ab der die Email-Berichte gesendet werden sollen, beispielsweise:

   ```
   STATUS_NOTIFY_LEVEL=$STATUS_SUCCESS
   ```

   Weitere Informationen finden Sie unter *Mögliche Werte für* `STATUS_NOTIFY_LEVEL`.

5. So definieren Sie die Liste der Empfänger, an die die Berichte gesendet werden sollen:

   a. Wechseln Sie zum Eintrag `EMAIL_REPORT='root'`.

   b. Ersetzen Sie `root` durch eine Liste der Email-Adressen, an die die SCA-Berichte gesendet werden sollen. Die Email-Adressen müssen jeweils durch ein Komma getrennt werden. Beispiel:

   ```
   EMAIL_REPORT='tux@my.company.com wilber@your.company.com'
   ```

6. Speichern und schließen Sie die Datei. Die Änderungen treten ohne Neustart des Rechners in Kraft. Alle künftigen SCA-Berichte werden an die angegebenen Adressen gesendet.

39.4.2.6 Sichern und Wiederherstellen der Datenbank

Mit dem Kommando **`scadb`** können Sie die MariaDB-Datenbank, in der die SCA-Berichte gespeichert werden, sichern und wiederherstellen.

PROZEDUR 39.10 SICHERN DER DATENBANK

1. Melden Sie sich an der Systemkonsole des Servers, auf dem die SCA-Appliance ausgeführt wird, als `root`-Benutzer an.

2. Versetzen Sie die Appliance mit dem folgenden Kommando in den Wartungsmodus:

   ```
   scadb maint
   ```

3. Starten Sie die Sicherung mit:

   ```
   scadb backup
   ```

   Die Daten werden in einem TAR-Archiv gespeichert: `sca-backup-*sql.gz`.

4. Wenn Sie mit der Schemaerstellungsdatenbank eigene Schemata entwickelt haben (siehe *Abschnitt 39.4.3, „Entwickeln von benutzerdefinierten Analyseschemata“*), sichern Sie diese Daten ebenfalls:

   ```
   sdpdb backup
   ```

   Die Daten werden in einem TAR-Archiv gespeichert: `sdp-backup-*sql.gz`.

5. Kopieren Sie die folgenden Daten auf einen anderen Rechner oder auf ein externes Speichermedium:

   - `sca-backup-*sql.gz`
   - `sdp-backup-*sql.gz`
   - `/usr/lib/sca/patterns/local` (nur wenn Sie benutzerdefinierte Schemata erstellt haben)

6. Reaktivieren Sie die SCA-Appliance mit:

```
scadb reset agents
```

PROZEDUR 39.11 WIEDERHERSTELLEN DER DATENBANK

Zum Wiederherstellen der Datenbank aus der Sicherung gehen Sie wie folgt vor:

1. Melden Sie sich an der Systemkonsole des Servers, auf dem die SCA-Appliance ausgeführt wird, als `root`-Benutzer an.
2. Kopieren Sie die jüngsten TAR-Archive mit der Bezeichnung `sca-backup-*sql.gz` und `sdp-backup-*sql.gz` auf den SCA-Appliance-Server.
3. Dekomprimieren Sie die Dateien mit:

```
gzip -d *-backup-*sql.gz
```

4. Importieren Sie die Daten mit dem folgenden Kommando in die Datenbank:

```
scadb import sca-backup-*sql
```

5. Wenn Sie mit der Schemaerstellungsdatenbank eigene Schemata entwickelt haben, importieren Sie außerdem die nachfolgenden Daten mit:

```
sdpdb import sdp-backup-*sql
```

6. Wenn Sie benutzerdefinierte Schemata verwenden, stellen Sie außerdem die Datei `/usr/lib/sca/patterns/local` aus den Sicherungsdaten wieder her.
7. Reaktivieren Sie die SCA-Appliance mit:

```
scadb reset agents
```

8. Aktualisieren Sie die Schemamodule in der Datenbank mit:

```
sdagent-patterns -u
```

39.4.3 Entwickeln von benutzerdefinierten Analyseschemata

Die SCA-Appliance bietet eine umfangreiche Schemaentwicklungsumgebung (die SCA-Schemadatenbank), mit der Sie eigene, benutzerdefinierte Schemata erstellen können. Schemata können in jeder beliebigen Programmiersprache geschrieben sein. Damit sie für das supportconfig-Analyseverfahren zur Verfügung stehen, müssen sie im Verzeichnis `/usr/lib/sca/patterns/local` gespeichert und ausführbar gemacht werden. Die benutzerdefinierten Schemata werden dann im Rahmen des Analyseberichts sowohl von der SCA-Appliance als auch vom SCA-Werkzeug für neue supportconfig-Archive ausgeführt. Weitere Anweisungen zum Erstellen (und Testen) der benutzerdefinierten Schemata finden Sie unter http://www.suse.com/communities/conversations/sca-pattern-development/.

39.5 Sammeln von Informationen bei der Installation

Während der Installation ist **`supportconfig`** nicht verfügbar. Sie können Protokolldateien von YaST jedoch mithilfe von **`save_y2logs`** sammeln. Dieses Kommando erstellt ein `.tar.xz`-Archiv im Verzeichnis `/tmp`.

Wenn bereits früh Probleme bei der Installation auftreten, können Sie möglicherweise Informationen aus der durch **`linuxrc`** erstellten Protokolldatei sammeln. **`linuxrc`** ist ein kleines Kommando, das vor dem Start von YaST ausgeführt wird. Diese Protokolldatei finden Sie unter `/var/log/linuxrc.log`.

Wichtig: Installationsprotokolldateien sind im installierten System nicht verfügbar

Die während der Installation verfügbaren Protokolldateien sind im installierten System nicht mehr verfügbar. Speichern Sie die Installationsprotokolldateien ordnungsgemäß, während das Installationsprogramm noch ausgeführt wird.

39.6 Unterstützung für Kernelmodule

Eine wichtige Anforderung für jedes Enterprise-Betriebssystem ist der Grad der Unterstützung für die jeweilige Umgebung. Kernelmodule sind die wichtigsten Bindeglieder zwischen der Hardware („Controller“) und dem Betriebssystem. Die Kernelmodule in SUSE Linux Enterprise umfassen jeweils das Flag `supported`, das drei mögliche Werte annehmen kann:

- „Ja“, daher `supported`
- „Extern“, daher `supported`
- „“ (leer, nicht festgelegt), daher `unsupported`

Es gelten die folgenden Regeln:

- Alle Module eines selbst rückkompilierten Kernels sind standardmäßig als nicht unterstützt gekennzeichnet.
- Kernelmodule, die von den SUSE-Partnern unterstützt und über das `SUSE SolidDriver-Programm` bereitgestellt, sind als „extern“ gekennzeichnet.
- Wenn das Flag `supported` nicht gesetzt ist, wird der Kernel beim Laden dieses Moduls unbrauchbar. Unbrauchbare Kernel werden nicht unterstützt. Nicht unterstützte Kernel-Module befinden sich in einem separaten RPM-Paket (`kernel-`*`FLAVOR`*`-extra`), das lediglich für SUSE Linux Enterprise Desktop und für die Arbeitsplatzrechnererweiterung für SUSE Linux Enterprise zur Verfügung steht. Diese Kernel werden standardmäßig nicht geladen (*`FLAVOR`* = `default` | `xen` |...). Darüber hinaus sind diese nicht unterstützten Module im Installationsprogramm nicht verfügbar, und das Kernelpaket `kernel-`*`FLAVOR`*`-extra` ist kein Bestandteil der SUSE Linux Enterprise-Medien.
- Kernelmodule, die nicht unter einer zur Lizenz des Linux-Kernels kompatiblen Lizenz bereitgestellt werden, machen den Kernel ebenfalls unbrauchbar. Weitere Informationen finden Sie unter `/usr/src/linux/Documentation/sysctl/kernel.txt` und dem Status `/proc/sys/kernel/tainted`.

39.6.1 Technischer Hintergrund

- Linux-Kernel: Der Standardwert für `/proc/sys/kernel/unsupported` bei SUSE Linux Enterprise `12 SP5` lautet 2 (`do not warn in syslog when loading unsupported modules` [keine Warnung im Syslog, wenn nicht unterstützte Module geladen werden]).

Dieser Standardwert wird im Installationsprogramm und im installierten System verwendet. Weitere Informationen finden Sie unter `/usr/src/linux/Documentation/sysctl/kernel.txt`.

- **`modprobe`**: Das Dienstprogramm **`modprobe`** zum Prüfen der Modulabhängigkeiten und zum Laden der Module prüft den Wert des Flags `supported`. Beim Wert „Ja“ oder „Extern“ wird das Modul geladen, ansonsten nicht. Weitere Informationen, wie Sie dieses Verhalten außer Kraft setzen, finden Sie in *Abschnitt 39.6.2, „Arbeiten mit nicht unterstützten Modulen“*.

Anmerkung: Support

SUSE bietet im Allgemeinen keine Unterstützung für das Entfernen von Speichermodulen mit **`modprobe -r`**.

39.6.2 Arbeiten mit nicht unterstützten Modulen

Die allgemeine Unterstützung ist wichtig. Dennoch können Situationen eintreten, in denen ein nicht unterstütztes Modul erforderlich ist (beispielsweise zu Testzwecken, für die Fehlersuche oder wenn der Hardware-Hersteller ein HotFix bereitstellt).

- Zum Überschreiben des Standardwerts bearbeiten Sie die Datei `/etc/modprobe.d/10-unsupported-modules.conf`, und ändern Sie den Wert der Variablen `allow_unsupported_modules` in `1`. Falls in der initrd ein nicht unterstütztes Modul erforderlich ist, müssen Sie zur Aktualisierung der initrd auch **`dracut`** `-f` ausführen.
  Falls Sie nur einmalig versuchen möchten, ein Modul zu laden, verwenden Sie die Option `--allow-unsupported-modules` für **`modprobe`**. Weitere Informationen finden Sie auf der man-Seite zu **`modprobe`**.

- Während der Installation werden nicht unterstützte Module u. U. über Treiberaktualisierungs-Datenträger hinzugefügt und entsprechend geladen. Soll das Laden von nicht unterstützten Modulen beim Booten und zu späteren Zeitpunkten erzwungen werden, verwenden Sie die Kernel-Befehlszeile `oem-modules`. Beim Installieren und Initialisieren des Pakets `suse-module-tools` wird das Kernel-Flag `TAINT_NO_SUPPORT` (`/proc/sys/kernel/tainted`) ausgewertet. Ist das Kernel bereits unbrauchbar, wird `allow_unsupported_modules` aktiviert. Damit wird verhindert, dass nicht unterstützte Module im zu installierenden System zu Fehlern führen. Wenn während der Installation keine nicht unterstütz-

ten Module vorhanden sind und die andere spezielle Kernel-Befehlszeilenoption (`oem-modules=1`) nicht verwendet wird, so werden nicht unterstützte Module dennoch standardmäßig nicht zugelassen.

Beachten Sie, dass der Kernel und das gesamte System nicht mehr durch SUSE unterstützt werden, sobald nicht unterstützte Module geladen und ausgeführt werden.

39.7 Weiterführende Informationen

- **`man supportconfig`** – man-Seite zu **`supportconfig`**.
- **`man supportconfig.conf`** – man-Seite zur supportconfig-Konfigurationsdatei.
- **`man scatool`** – man-Seite zu **`scatool`**.
- **`man scadb`** – man-Seite zu **`scadb`**.
- **`man setup-sca`** – man-Seite zu **`setup-sca`**.
- https://mariadb.com/kb/en/ – Dokumentation zur MariaDB.
- http://httpd.apache.org/docs/ und *Kapitel 31, Der HTTP-Server Apache* – Dokumentation zum Apache-Webserver.
- *Kapitel 32, Einrichten eines FTP-Servers mit YaST* – Dokumentation zum Einrichten eines FTP-Servers.
- http://www.suse.com/communities/conversations/sca-pattern-development/ – Anweisungen zum Erstellen (und Testen) benutzerdefinierter SCA-Schemata.
- http://www.suse.com/communities/conversations/basic-server-health-check-supportconfig/ – Grundlegende Server-Integritätsprüfung mit supportconfig.
- https://www.novell.com/communities/coolsolutions/cool_tools/create-your-own-supportconfig-plugin/ – Erstellen eines eigenen supportconfig-Plug-ins.
- http://www.suse.com/communities/conversations/creating-a-central-supportconfig-repository/ – Erstellen eines zentralen supportconfig-Repositorys.

40 Häufige Probleme und deren Lösung

In diesem Kapitel werden mögliche Probleme und deren Lösungen beschrieben. Auch wenn Ihre Situation nicht genau auf die hier beschriebenen Probleme zutreffen mag, finden Sie vielleicht einen ähnlichen Fall, der Ihnen Hinweise zur Lösung Ihres Problems liefert.

40.1 Suchen und Sammeln von Informationen

Linux gibt äußerst detailliert Aufschluss über die Vorgänge in Ihrem System. Es gibt mehrere Quellen, die Sie bei einem Problem mit Ihrem System zurate ziehen können. Die meisten davon beziehen sich auf Linux-Systeme im Allgemeinen doch einige sind speziell auf SUSE Linux Enterprise Server-Systeme ausgerichtet. Die meisten Protokolldateien können mit YaST angezeigt werden (*Verschiedenes* › *Startprotokoll anzeigen*).

Mit YaST können Sie alle vom Support-Team benötigten Systeminformationen sammeln. Wählen Sie *Andere* › *Support* und dann die Kategorie Ihres Problems aus. Wenn alle Informationen gesammelt wurden, können Sie diese an Ihre Support-Anfrage anhängen.

Nachfolgend finden Sie eine Liste der wichtigsten Protokolldateien mit einer Beschreibung ihrer typischen Einsatzbereiche. Eine Tilde (`~`) in einer Pfadangabe verweist auf das Home-Verzeichnis des aktuellen Benutzers.

TABELLE 40.1 PROTOKOLLDATEIEN

Protokolldatei	Beschreibung
`~/.xsession-errors`	Meldungen von den zurzeit ausgeführten Desktop-Anwendungen.
`/var/log/apparmor/`	Protokolldateien von AppArmor (Detailinformationen finden Sie unter *Buch* „Security Guide“).
`/var/log/audit/audit.log`	Protokolldatei von Audit, um Zugriffe auf Dateien, Verzeichnisse oder Ressourcen Ihres Systems sowie Systemaufrufe zu verfolgen. Ausführliche Informationen erhalten Sie unter *Buch* „Security Guide“.

Protokolldatei	Beschreibung
`/var/log/mail.*`	Meldungen vom Email-System.
`/var/log/NetworkManager`	NetworkManager-Protokolldatei zur Erfassung von Problemen hinsichtlich der Netzwerkkonnektivität
`/var/log/samba/`	Verzeichnis, das Protokollmeldungen vom Samba-Server und -Client enthält.
`/var/log/warn`	Alle Meldungen vom Kernel und dem Systemprotokoll-Daemon mit der Protokollstufe „Warnung“ oder höher.
`/var/log/wtmp`	Binärdatei mit Benutzeranmeldedatensätzen für die aktuelle Computersitzung. Die Anzeige erfolgt mit **`last`**.
`/var/log/Xorg.*.log`	Unterschiedliche Start- und Laufzeitprotokolldateien des X Window System. Hilfreich für die Fehlersuche bei Problemen beim Start von X.
`/var/log/YaST2/`	Verzeichnis, das die Aktionen von YAST und deren Ergebnissen enthält.
`/var/log/zypper.log`	Protokolldatei von Zypper.

Neben den Protokolldateien versorgt Ihr Computer Sie auch mit Informationen zum laufenden System. Weitere Informationen hierzu finden Sie unter *Tabelle 40.2: Systeminformationen mit dem `/proc`-Dateisystem*

TABELLE 40.2 SYSTEMINFORMATIONEN MIT DEM `/proc`-DATEISYSTEM

Datei	Beschreibung
`/proc/cpuinfo`	Enthält Prozessorinformationen wie Typ, Fabrikat, Modell und Leistung.

Datei	Beschreibung
`/proc/dma`	Zeigt die aktuell verwendeten DMA-Kanäle an.
`/proc/interrupts`	Zeigt an, welche Interrupts verwendet werden und wie viele bisher verwendet wurden.
`/proc/iomem`	Zeigt den Status des E/A (Eingabe/Ausgabe)-Speichers an.
`/proc/ioports`	Zeigt an, welche E/A-Ports zurzeit verwendet werden.
`/proc/meminfo`	Zeigt den Speicherstatus 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.

Abgesehen vom Dateisystem `/proc` exportiert der Linux-Kernel Informationen mit dem Modul `sysfs`, einem speicherinternen Dateisystem. Dieses Modul stellt Kernelobjekte, deren Attribute und Beziehungen dar. Weitere Informationen zu `sysfs` finden Sie im Kontext von udev im Abschnitt *Kapitel 21, Gerätemanagement über dynamischen Kernel mithilfe von* `udev`. *Tabelle 40.3* enthält einen Überblick über die am häufigsten verwendeten Verzeichnisse unter `/sys`.

TABELLE 40.3 SYSTEMINFORMATIONEN MIT DEM `/sys`-DATEISYSTEM

Datei	Beschreibung
`/sys/block`	Enthält Unterverzeichnisse für jedes im System ermittelte Blockgerät. Im Allgemeinen handelt es sich dabei meistens um Geräte vom Typ Datenträger.
`/sys/bus`	Enthält Unterverzeichnisse für jeden physischen Bustyp.

Datei	Beschreibung
`/sys/class`	Enthält Unterverzeichnisse, die nach den Funktionstypen der Geräte (wie Grafik, Netz, Drucker usw.) gruppiert sind.
`/sys/device`	Enthält die globale Gerätehierarchie.

Linux bietet mehrere Werkzeuge für die Systemanalyse und -überwachung. Unter *Buch „*System Analysis and Tuning Guide*", Kapitel 2 „System Monitoring Utilities"* 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, verfügbaren Referenzen für detailliertere Lösungen sowie Querverweisen auf andere Szenarien, die mit diesem Szenario in Zusammenhang stehen.

40.2 Probleme bei der Installation

Probleme bei der Installation sind Situationen, wenn die Installation eines Computers nicht möglich ist. Der Vorgang kann entweder nicht ausgeführt oder das grafische Installationsprogramm 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.

40.2.1 Überprüfen von Medien

Wenn Probleme bei der Verwendung des SUSE Linux Enterprise Server-Installationsmediums auftreten, können Sie die Integrität des Installationsmediums überprüfen. Starten Sie von dem Medium aus und wählen Sie im Startmenü die Option *Installationsmedium prüfen* aus. Starten Sie in einem aktiven System YaST, und wählen Sie *Software* › *Medienprüfung*. Wenn Sie ein Installationsmedium von SUSE Linux Enterprise Server überprüfen möchten, legen Sie das Medium in das Laufwerk ein, und klicken Sie in YaST im Fenster *Medienprüfung* auf *Prüfvorgang starten*. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen. Wenn Fehler gefunden werden,

sollten Sie dieses Medium nicht für die Installation verwenden. Bei selbst gebrannten Medien können Medienprobleme auftreten. Durch Brennen des Mediums bei niedriger Geschwindigkeit (4x) können Probleme vermieden werden.

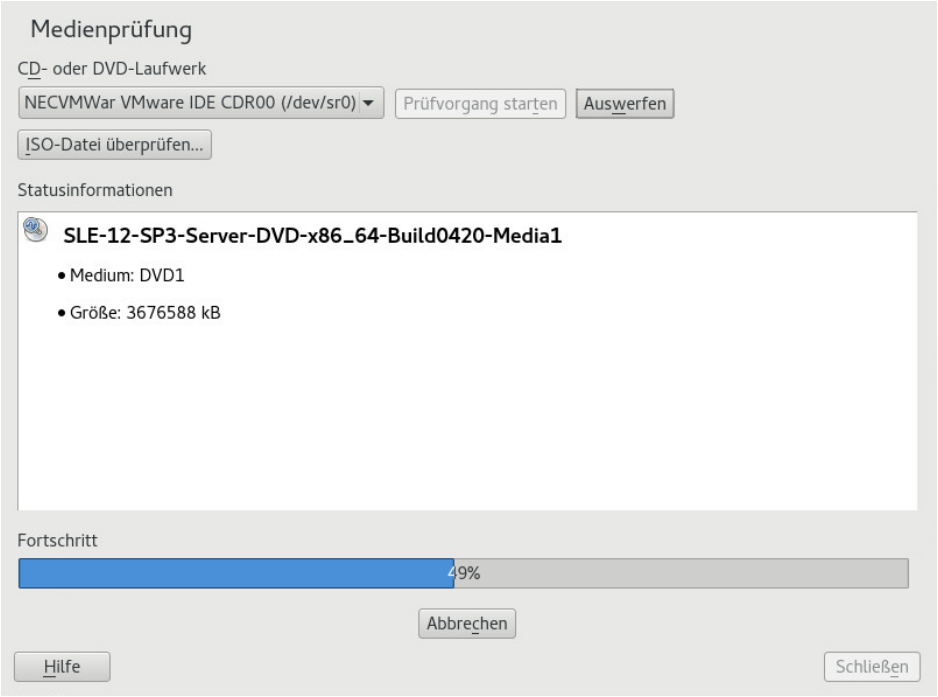


ABBILDUNG 40.1 ÜBERPRÜFEN VON MEDIEN

40.2.2 Kein bootfähiges DVD-Laufwerk verfügbar

Wenn Ihr Computer über kein bootfähiges DVD-ROM-Laufwerk verfügt bzw. das von Ihnen verwendete Laufwerk von Linux nicht unterstützt wird, gibt es mehrere Möglichkeiten zur Installation Ihres Computers ohne integriertem DVD-Laufwerk:

Verwenden eines externen Boot-Devices

Wenn der Startvorgang vom BIOS Ihres Computers und dem Installationskernel unterstützt wird, können Sie ihn von einem externen DVD-Laufwerk oder einem USB-Speichergerät aus ausführen. Weitere Anweisungen zum Erstellen eines bootfähigen Ziels finden Sie in *Buch „Bereitstellungshandbuch", Kapitel 6 „Installation mit YaST", Abschnitt 6.2.2 „PC (AMD64/Intel 64/ARM AArch64): Systemstart"*.

Netzwerk-Boot über PXE

Wenn ein Rechner kein DVD-Laufwerk aufweist, jedoch eine funktionierende Ethernet-Verbindung verfügbar ist, führen Sie eine vollständig netzwerkbasierte Installation durch. Details finden Sie im *Buch „*Bereitstellungshandbuch*", Kapitel 10 „Installationen auf Remote-Systemen", Abschnitt 10.1.3 „Installation auf entfernten Systemen über VNC – PXE-Boot und Wake-on-LAN"* und *Buch „*Bereitstellungshandbuch*", Kapitel 10 „Installationen auf Remote-Systemen", Abschnitt 10.1.6 „Installation auf entfernten Systemen über SSH – PXE-Boot und Wake-on-LAN"*.

40.2.2.1 Externe Boot-Devices

Linux unterstützt die meisten DVD-Laufwerke. Wenn das System kein DVD-Laufwerk aufweist, kann ein externes, über USB, FireWire oder SCSI angeschlossenes DVD-Laufwerk 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.

Wenn Sie die Installation von einer Live-CD aus ausführen, können Sie auch ein „Live-Flash-Laufwerk" erstellen, von dem aus der Bootvorgang ausgeführt wird.

40.2.3 Vom Installationsmedium kann nicht gebootet werden

Wenn ein Computer nicht vom Installationsmedium booten kann, ist im BIOS möglicherweise eine falsche Bootsequenz eingestellt. In der BIOS-Boot-Sequenz muss das DVD-Laufwerk als erster Eintrag zum Booten festgelegt sein. Andernfalls versucht der Computer, von einem anderen Medium zu booten, normalerweise von der Festplatte. Anweisungen zum Ändern der BIOS-Boot-Sequenz finden Sie in der Dokumentation zu Ihrer Hauptplatine 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 eingeblendet 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). In der Regel muss die Taste Entf, F1 oder Esc gedrückt werden. Halten Sie diese Taste gedrückt, bis der Bildschirm mit dem BIOS-Setup angezeigt wird.

PROZEDUR 40.1 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 dem Untereintrag *BOOT SEQUENCE* (BOOTSEQUENZ) oder *BOOT ORDER* (BOOTREIHENFOLGE). Zum Ändern der Einstellungen drücken Sie Bild ↑ oder Bild ↓, bis das DVD-Laufwerk an erster Stelle aufgeführt wird.
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 40.2 ÄNDERN DER BOOTSEQUENZ IN EINEM SCSI-BIOS (ADAPTEC-HOSTADAPTER)

1. Öffnen Sie das Setup, indem Sie die Tastenkombination Strg–A drücken.
2. Wählen Sie *Disk Utilities* (Festplattendienstprogramme) aus. Nun werden die angeschlossenen Hardwarekomponenten angezeigt.
   Notieren Sie sich die SCSI-ID Ihres DVD-Laufwerks.
3. Verlassen Sie das Menü mit Esc.
4. Öffnen Sie *Configure Adapter Settings* (Adaptereinstellungen konfigurieren). Wählen Sie unter *Additional Options* (Zusätzliche Optionen) den Eintrag *Boot Device Options* (Boot-Gerät-Optionen) aus, und drücken Sie Eingabetaste.
5. Geben Sie die ID des DVD-Laufwerks ein, und drücken Sie erneut 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 40.2 US-TASTATURBELEGUNG

40.2.4 Computer kann nicht gebootet werden

Bei bestimmter Hardware, insbesondere bei sehr alter bzw. sehr neuer, kann bei der Installation ein Fehler auftreten. Oft ist dies darauf zurückzuführen, dass dieser Hardwaretyp im Installationskernel noch nicht oder nicht mehr unterstützt wird; oft führen auch bestimmte Funktionen dieses Kernels, beispielsweise ACPI (Advanced Configuration and Power Interface), bei bestimmter Hardware zu Problemen.

Wenn Ihr System über den standardmäßigen Modus für die *Installation* (Installation) im ersten Installations-Bootbildschirm nicht installiert werden kann, gehen Sie folgendermaßen vor:

1. Belassen Sie die DVD im Laufwerk und booten Sie den Computer über die Tastenkombination Strg–Alt–Entf bzw. über den Reset-Knopf der Hardware neu.
2. Drücken Sie, sobald der Bootbildschirm angezeigt wird, F5, navigieren Sie mithilfe der Pfeiltasten der Tastatur zu *Keine ACPI* und drücken Sie Eingabetaste, um den Boot- und Installationsvorgang zu starten. Mit dieser Option wird die Unterstützung für ACPI-Energieverwaltungstechniken deaktiviert.
3. Fahren Sie wie in *Buch „Bereitstellungshandbuch", Kapitel 6 „Installation mit YaST"* beschrieben mit der Installation fort.

Wenn es hierbei zu Problemen kommt, fahren Sie wie oben beschrieben fort, wählen Sie jedoch in diesem Fall *Sichere Einstellungen* aus. Mit dieser Option wird die Unterstützung für ACPI und DMA (Direct Memory Access) deaktiviert. Mit dieser Option kann die meiste Hardware gebootet werden.

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 weitere mit ACPI in Zusammenhang stehende Kernel-Parameter, die vor dem Booten zu Installationszwecken an der Booteingabeaufforderung 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.

`pnpacpi=off`

Diese Option ist für Probleme mit seriellen oder parallelen Ports vorgesehen, wenn Ihr BIOS-Setup falsche Interrupts oder Ports enthält.

`notsc`

Hiermit wird der Zeitstempelzähler deaktiviert. Diese Option dient der Umgehung von Timing-Problemen auf Ihren Systemen. Es handelt sich um eine recht neue Funktion, die insbesondere dann nützlich sein kann, wenn Sie auf Ihrem Rechner Rückwärtsentwicklungen bemerken, insbesondere zeitbezogene Rückwärtsentwicklungen. Gilt auch für Fälle, in denen keinerlei Reaktion mehr zu verzeichnen ist.

`nohz=off`

Hiermit wird die nohz-Funktion deaktiviert. Wenn der Rechner nicht mehr reagiert, ist diese Option vielleicht die Lösung. Andernfalls wird sie Ihnen kaum nützlich sein.

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 Bootmenü 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.

40.2.5 Grafisches Installationsprogramm lässt sich nicht starten

Nachdem Sie das Medium 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.

PROZEDUR 40.3 ÄNDERN DER BILDSCHIRMAUFLÖSUNG FÜR DIE INSTALLATION

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 *Buch „Bereitstellungshandbuch", Kapitel 6 „Installation mit YaST"* beschrieben, mit der Installation fort.

PROZEDUR 40.4 INSTALLATION IM TEXTMODUS

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 *Buch „Bereitstellungshandbuch", Kapitel 6 „Installation mit YaST"* beschrieben, mit der Installation fort.

PROZEDUR 40.5 VNC-INSTALLATION

1. Booten Sie zu Installationszwecken.
2. Geben Sie an der Bootoptionen-Eingabeaufforderung folgenden Text ein:

   ```
   vnc=1 vncpassword=SOME_PASSWORD
   ```

   Ersetzen Sie *BELIEBIGES_PASSWORT* durch das für die VNC-Installation zu verwendende Passwort.
3. Wählen Sie *Installation* aus und drücken Sie dann Eingabetaste, um die Installation zu starten.
   Anstatt direkt in die Routine für die grafische Installation einzusteigen, wird das System weiterhin im Textmodus 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, geben Sie die Adressinformationen ein, die von den Installationsroutinen auf dem zukünftigen SUSE Linux Enterprise Server-Computer bereitgestellt werden, und drücken Sie Eingabetaste:

   ```
   http://IP_ADDRESS_OF_MACHINE: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 *Buch „Bereitstellungshandbuch", Kapitel 6 „Installation mit YaST"* beschrieben, mit der Installation fort.

Wichtig: Plattformübergreifende Unterstützung

Die Installation über VNC kann mit jedem Browser und unter jedem beliebigen Betriebssystem vorgenommen werden, vorausgesetzt, die Java-Unterstützung ist aktiviert.

Geben Sie auf Aufforderung die IP-Adresse und das Passwort für Ihren VNC-Viewer ein. Daraufhin wird ein Fenster mit den installationsbezogenen Dialogfeldern geöffnet. Fahren Sie wie gewohnt mit der Installation fort.

40.2.6 Nur ein minimalistischer Bootbildschirm wird eingeblendet

Sie haben das Medium in das Laufwerk eingelegt, die BIOS-Routinen sind abgeschlossen, das System zeigt jedoch den grafischen Bootbildschirm nicht an. Stattdessen wird eine sehr minimalistische textbasierte Oberfläche angezeigt. Dies kann auf Computern der Fall sein, die für die Darstellung eines grafischen Bootbildschirms nicht ausreichend Grafikspeicher aufweisen.

Obwohl der textbasierte Bootbildschirm minimalistisch wirkt, bietet er nahezu dieselbe Funktionalität wie der grafische:

Bootoptionen

Im Gegensatz zur grafischen Oberfläche können die unterschiedlichen Bootoptionen nicht mithilfe der Cursortasten der Tastatur ausgewählt werden. Das Bootmenü des Expertenmodus-Bootbildschirms ermöglicht die Eingabe einiger Schlüsselwörter an der Booteingabeaufforderung. Diese Schlüsselwörter sind den Optionen in der grafischen Version zugeordnet. Treffen Sie Ihre Wahl und drücken Sie Eingabetaste, um den Bootvorgang zu starten.

Benutzerdefinierte Bootoptionen

Geben Sie nach der Auswahl einer Bootoption das entsprechende Schlüsselwort an der Booteingabeaufforderung ein. Sie können auch einige benutzerdefinierte Bootoptionen eingeben (siehe *Abschnitt 40.2.4, „Computer kann nicht gebootet werden“*). Wenn Sie den Installationsvorgang starten möchten, drücken Sie Eingabetaste.

Bildschirmauflösungen

Ermitteln Sie mit den Funktionstasten (F1 bis F12) die Bildschirmauflösung für die Installation. Wenn Sie im Expertenmodus, also im Textmodus, booten müssen, drücken Sie F3.

40.2.7 Protokolldateien

Weitere Informationen zu Protokolldateien, die während der Installation erstellt werden, finden Sie in *Abschnitt 39.5, „Sammeln von Informationen bei der Installation“*.

40.3 Probleme beim Booten

Probleme beim Booten sind Fälle, in denen Ihr System nicht vorschriftsmäßig gebootet wird, das Booten also nicht mit dem erwarteten Ziel und Anmeldebildschirm erfolgt.

40.3.1 GRUB 2-Bootloader wird nicht geladen

Wenn die Hardware vorschriftsmäßig funktioniert, ist möglicherweise der Bootloader beschädigt und Linux kann auf dem Computer nicht gestartet werden. In diesem Fall muss der Bootloader repariert werden. Dazu müssen Sie das Rettungssystem starten wie in *Abschnitt 40.6.2, „Verwenden des Rettungssystems“* beschrieben und den Anweisungen in *Abschnitt 40.6.2.4, „Bearbeiten und erneutes Installieren des Bootloaders“* folgen.

Alternativ können Sie den Bootloader mit dem Rettungssystem wie folgt reparieren. Booten Sie den Computer von den Installationsmedien. Wählen Sie im Bootbildschirm die Option *Mehr* › *Linux-System booten*. Wählen Sie die Festplatte aus, auf der sich das installierte System und der Kernel mit den Kernel-Standardoptionen befinden.

Wenn das System gebootet wird, starten Sie YaST und wechseln Sie zu *System* › *Bootloader*. Prüfen Sie, ob die Option *Generischen Bootcode in MBR schreiben* aktiviert ist, und klicken Sie auf *OK*. Ein beschädigte Bootloader wird überschrieben und damit repariert, ein fehlender Bootloader wird installiert.

Die Grunde 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 2 wird möglicherweise einfach deshalb nicht gestartet, weil die Festplatte mit den aktuellen BIOS-Einstellungen nicht gefunden wird.

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.

40.3.2 Keine grafische Anmeldung

Wenn der Computer hochfährt, jedoch der grafische Anmelde-Manager nicht gebootet wird, müssen Sie entweder hinsichtlich der Auswahl des standardmäßigen systemd-Ziels oder der Konfiguration des X-Window-Systems mit Problemen rechnen. Zum Prüfen des aktuellen systemd-Standardziels führen Sie das Kommando **`sudo systemctl get-default`** aus. Wenn *nicht* `der Wert graphical.target` zurückgegeben wird, führen Sie das Kommando **`sudo systemctl isolate graphical.target`** aus. Wird der grafische Anmeldebildschirm geöffnet, melden Sie sich an, starten Sie *YaST* › *System* › *Dienste-Verwaltung*, und legen Sie für *Default System Target* (Standard-Systemziel) den Wert *Graphical Interface* (Grafische Oberfläche) fest. Von nun an bootet das System in den grafischen Anmeldebildschirm.

Falls der grafische Anmeldebildschirm auch nicht nach dem Booten oder dem Wechsel zum grafischen Ziel gestartet wird, ist die Desktop- oder X Window-Software möglicherweise fehlerhaft konfiguriert oder beschädigt. Suchen Sie in den Protokolldateien von `/var/log/Xorg.*.log` nach detaillierten Meldungen vom X-Server beim versuchten Start. Wenn beim Starten des Desktops ein Fehler auftritt, werden möglicherweise Fehlermeldungen im Systemjournal protokolliert, die Sie mit dem Kommando **`journalctl`** abfragen können (weitere Informationen finden Sie in *Kapitel 15, `journalctl`: Abfragen des `systemd`-Journals*). 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.

40.3.3 Einhängen der Root-Btrfs-Partition nicht möglich

Wenn eine `btrfs`-Root-Partition beschädigt wird, haben Sie folgende Möglichkeiten:

- Hängen Sie die Partition mit der Option `-o recovery` ein.
- Falls dies nicht funktioniert, führen Sie **`btrfs-zero-log`** auf der Root-Partition aus.

40.3.4 Erzwingen der Prüfung von Root-Partitionen

Wenn die Root-Partition beschädigt wird, verwenden Sie den Parameter `forcefsck` am Bootprompt. Hierdurch wird die Option `-f` (force = zwingen) an das Kommando **`fsck`** übergeben.

40.4 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.).

40.4.1 Fehler trotz gültiger Kombination aus Benutzername und Passwort

Dieser Fall tritt in der Regel ein, wenn das System zur Verwendung von Netzwerkauthentifizierung oder Verzeichnisdiensten konfiguriert wurde und aus unbekannten Gründen 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 häufige Ursachen dafür aufgeführt, weshalb Anmeldungen nicht ordnungsgemäß verarbeitet werden können, obwohl der Computer funktionstüchtig zu sein scheint:

- Es liegt ein Problem mit der Netzwerkfunktion vor. Weitere Anweisungen hierzu finden Sie in *Abschnitt 40.5, „Probleme mit dem Netzwerk“*.
- DNS ist zurzeit nicht funktionsfähig (dadurch ist GNOME 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 40.5, „Probleme mit dem Netzwerk“*.
- Wenn das System für die Verwendung von Kerberos konfiguriert ist, 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 Hintergrundinfomationen zu PAM (Password Authentification Module) und der Syntax der betroffenen Konfigurationsdateien finden Sie in *Buch „Security Guide", Kapitel 2 „Authentication with PAM"*.

- Die Home-Partition ist verschlüsselt. Weitere Informationen zu diesem Thema finden Sie in *Abschnitt 40.4.3, „Anmeldung bei verschlüsselter Home-Partition fehlgeschlagen"*.

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 Bootbildschirm mit einer Eingabeaufforderung eingeblendet.
2. Drücken Sie `Esc`. Der Eröffnungsbildschirm wird geschlossen und Sie gelangen zum textgestützten GRUB 2-Menü.
3. Drücken Sie `B`. Der GRUB 2-Editor wird geöffnet.
4. Fügen Sie den folgenden Parameter an die Zeile mit den Kernel-Parametern an:

   ```
   systemd.unit=rescue.target
   ```

5. Drücken Sie `F10`.
6. Geben Sie Benutzername und Passwort für `root` ein.
7. Nehmen Sie alle erforderlichen Änderungen vor.
8. Booten Sie in den vollen Mehrbenutzer- und Netzwerkbetrieb, indem Sie **`systemctl isolate graphical.target`** an der Kommandozeile eingeben.

40.4.2 Keine Annahme einer gültigen Kombination aus Benutzername und Passwort

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. Sollte sich der Benutzer nicht mehr an sein Passwort erinnern, können Sie es mithilfe des YaST-Moduls für die Benutzerverwaltung ändern. Achten Sie auf die Feststelltaste und deaktivieren Sie sie gegebenenfalls.
2. Melden Sie sich als `root` an, und prüfen Sie das Systemjournal mit **`journalctl -e`** auf Fehlermeldungen aus dem Anmeldevorgang und von PAM.
3. Versuchen Sie, sich von einer 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 GNOME-Desktop ausfindig zu machen. Weitere Informationen hierzu finden Sie in *Abschnitt 40.4.4, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“*.
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 der Desktop aufgrund beschädigter Konfigurationsdateien nicht aufgerufen werden konnte, fahren Sie mit *Abschnitt 40.4.4, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“* fort.

Im Folgenden sind allgemeine Gründe aufgelistet, aus denen eine Netzwerkauthentifizierung für einen bestimmten Benutzer auf einem bestimmten Computer fehlschlagen könnte:

- 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 Home-Verzeichnis 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 das Systemjournal mit **`journalctl -e`** > Datei. 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 einer Konsole aus anzumelden (mit Strg–Alt–F1). Wenn dies gelingt, liegt der Fehler nicht bei PAM oder dem Verzeichnisserver mit dem Home-Verzeichnis des Benutzers, da die Authentifizierung dieses Benutzers auf diesem Computer möglich ist. Versuchen Sie, mögliche Probleme mit dem X-Window-System oder dem GNOME-Desktop ausfindig zu machen. Weitere Informationen hierzu finden Sie in *Abschnitt 40.4.4, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“*.

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 der Desktop aufgrund beschädigter Konfigurationsdateien nicht aufgerufen werden konnte, fahren Sie mit *Abschnitt 40.4.4, „Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop“* fort.

40.4.3 Anmeldung bei verschlüsselter Home-Partition fehlgeschlagen

Bei Laptops ist es empfehlenswert, die Home-Partition zu verschlüsseln. Wenn Sie sich bei Ihrem Laptop nicht anmelden können, gibt es dafür normalerweise einen einfachen Grund: Ihre Partition konnte nicht entsperrt werden.

Beim Booten müssen Sie den Passwortsatz eingeben, damit Ihre verschlüsselte Partition entsperrt wird. Wenn Sie den Passwortsatz nicht eingeben, wird der Boot-Vorgang fortgesetzt und die Partition bleibt gesperrt.

Gehen Sie folgendermaßen vor, um die verschlüsselte Partition zu entsperren:

1. Schalten Sie zur Textkonsole um, indem Sie auf Strg–Alt–F1 drücken.
2. Melden Sie sich als `root` an.
3. Starten Sie den Entsperrvorgang erneut mit:

   ```
   systemctl restart home.mount
   ```
4. Geben Sie Ihren Passwortsatz ein, um die verschlüsselte Partition zu entsperren.
5. Beenden Sie die Textkonsole und wechseln Sie mit Alt–F7 zum Anmeldebildschirm.
6. Melden Sie sich wie gewöhnlich an.

40.4.4 Anmeldung erfolgreich, jedoch Problem mit GNOME-Desktop

Wenn dies der Fall ist, sind Ihre GNOME-Konfigurationsdateien vermutlich 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. Das Problem kann in diesem Fall 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. Schalten Sie durch Drücken von Strg–Alt–F1 auf eine Textkonsole um.
2. Melden Sie sich mit Ihrem Benutzernamen an.
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. Melden Sie sich erneut an, führen Sie jedoch keine Anwendungen aus.

6. Stellen Sie Ihre individuellen Anwendungskonfigurationsdaten wieder her (einschließlich der Daten des Evolution-Email-Client), indem Sie das Verzeichnis `~/.gconf-ORIG-RECOVER/apps/` wie folgt 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 wiederherzustellen, und konfigurieren Sie die restlichen Anwendungen neu.

40.5 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 derer Sie die Ursache jeglicher Netzwerkprobleme ermitteln können.

PROZEDUR 40.6 ERKENNEN VON NETZWERKPROBLEMEN

Gehen Sie zur Überprüfung der Netzwerkverbindung Ihres Computers folgendermaßen vor:

1. Wenn Sie eine Ethernet-Verbindung nutzen, überprüfen Sie zunächst die Hardware. Vergewissern Sie sich, dass das Netzwerkkabel ordnungsgemäß am Computer und Router (oder Hub etc.) angeschlossen ist. Die Kontrolllämpchen neben dem Ethernet-Anschluss sollten beide leuchten.
   Wenn keine Verbindung hergestellt werden kann, testen Sie, ob Ihr Netzwerkkabel funktionstüchtig ist, wenn es mit einem anderen Computer verbunden wird. Wenn dies der Fall ist, ist das Problem auf Ihre Netzwerkkarte zurückzuführen. Wenn Ihre Netzwerkeinrichtung Hubs oder Switches enthält, sind diese möglicherweise auch fehlerhaft.

2. Bei einer drahtlosen Verbindung testen Sie, ob die drahtlose Verbindung von anderen Computern hergestellt werden kann. Ist dies nicht der Fall, sollten Sie das Problem an den Administrator des drahtlosen Netzwerks weiterleiten.

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 Namendienst, der ausgefallen ist oder Fehlfunktionen aufweist, kann die Funktionalität des Netzwerks auf vielfältige Weise beeinträchtigen. Wenn die Authentifizierung für einen lokalen Rechner über einen oder mehrere Netzwerkserver erfolgt und diese Server aufgrund von Problemen bei der Namenauflösung nicht auffindbar sind, können sich die Benutzer noch nicht einmal anmelden. Die Rechner in einem Netzwerk, das von einem ausgefallenen Nameserver verwaltet wird, können einander nicht „sehen“ und nicht miteinander 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`-Unterverzeichnis nicht gefunden wird, weil der NFS-Server ausgefallen ist.

   Samba (Dateidienst)

   Wenn eine Anwendung Daten benötigt, die in einem Verzeichnis auf einem fehlerhaften Samba-Server gespeichert sind, kann sie nicht aufgerufen werden oder weist Fehlfunktionen auf.

   NIS (Benutzerverwaltung)

   Wenn Ihr SUSE Linux Enterprise Server-System hinsichtlich der Bereitstellung der Benutzerdaten von einem fehlerhaften NIS-Server abhängig ist, können sich Benutzer nicht bei diesem Computer anmelden.

LDAP (Benutzerverwaltung)

Wenn Ihr SUSE Linux Enterprise Server-System hinsichtlich der Bereitstellung der Benutzerdaten von einem fehlerhaften LDAP-Server abhängig ist, können sich Benutzer nicht bei diesem Computer anmelden.

Kerberos (Authentifizierung)

Die Authentifizierung funktioniert nicht und die Anmeldung bei den Computern schlägt fehl.

CUPS (Netzwerkdruck)

Die Benutzer können nicht drucken.

4. Überprüfen Sie, ob die Netzwerkserver aktiv sind und ob Ihre Netzwerkeinrichtung das Herstellern einer Verbindung ermöglicht:

Wichtig: Einschränkungen

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`** *`IP-ADRESSE/HOSTNAME`* (ersetzen Sie IP-ADRESSE/HOSTNAME durch den Hostnamen oder die IP-Adresse des Servers) können Sie überprüfen, ob die einzelnen Server verfügbar sind und ob vom Netzwerk aus auf sie zugegriffen werden kann. Wenn dieses Kommando erfolgreich ist, besagt dies, dass der von Ihnen gesuchte Host aktiv ist und dass der Namendienst 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`** *`IP-ADRESSE`* oder *`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 Namendienst nicht vorschriftsmäßig konfiguriert, oder der verwendete Hostname ist falsch. Weitere Prüfungen dieser Arten finden Sie unter *Schritt 4.b*. Wenn der Ping-Versuch weiterhin erfolglos ist, ist entweder Ihre Netzwerkkarte nicht vorschriftsmäßig konfiguriert bzw. Ihre Netzwerk-Hardware ist fehlerhaft.

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 Kommando die IP-Adresse dieses Host zurückgegeben wird, ist der Namendienst aktiv. Wenn es bei diesem **`host`**-Kommando 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 Namenserver 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 Domänennamen richtig sind:

```
search FULLY_QUALIFIED_DOMAIN_NAME
nameserver IPADDRESS_OF_NAMESERVER
```

Diese Datei kann die Adresse eines oder mehrerer Namenserver enthalten, mindestens einer davon muss aber richtig sein, um die Namenauflösung für Ihren Host bereitzustellen. Wenn nötig, können Sie diese Datei auf der Registerkarte „Hostname/DNS“ des YaST-Moduls „Netzwerkeinstellungen“ anpassen.
Wenn die Netzwerkverbindung über DHCP erfolgt, aktivieren Sie DHCP, damit der Hostname und die Namensdienstinformationen geändert werden. Wählen Sie hierzu *Hostname über DHCP festlegen* (kann global für alle Schnittstellen oder auch separat für die einzelnen Schnittstellen eingestellt werden) und *Nameserver und Suchliste über DHCP aktualisieren* im YaST-Netzwerkeinstellungsmodul (Registerkarte „Hostname/DNS“).

`/etc/nsswitch.conf`

Aus dieser Datei geht hervor, wo Linux nach Namendienstinformationen 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 Namenserver zu verwenden. Normalerweise werden diese Einträge automatisch von YaST verwaltet, 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 25, Domain Name System (DNS)*. 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 Namendienst mit Sicherheit als Ursache ausschließen können, überprüfen Sie die Konfiguration Ihrer Netzwerkkarte.
Prüfen Sie mit dem Kommando **`ip addr show`** *`NETZWERKGERÄT`*, ob dieses Gerät ordnungsgemäß konfiguriert wurde. Prüfen Sie, ob die `inet address` mit der Netzmaske (*`/MASK`*) ordnungsgemäß konfiguriert ist. 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_DOMÄNENNAME`* (Ausführung als `root`) die Netzwerkroute dieser Anforderungen überwachen. Mit diesem Kommando 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 ersicht-

lich, ob dieser Sprung 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.

40.5.1 Probleme mit NetworkManager

Grenzen Sie Probleme mit der Netzwerkkonnektivität wie unter *Prozedur 40.6, „Erkennen von Netzwerkproblemen“* beschrieben ein. Wenn die Ursache bei NetworkManager zu liegen scheint, gehen Sie wie folgt vor, um Protokolle abzurufen, die Hinweise für den Grund der NetworkManager-Probleme enthalten:

1. Öffnen Sie eine Shell und melden Sie sich als `root` an.
2. Starten Sie NetworkManager neu.

   ```
   systemctl restart Network.Manager
   ```

3. Öffnen Sie eine Website, beispielsweise http://www.opensuse.org, als normaler Benutzer, um zu überprüfen, ob Sie eine Verbindung herstellen können.
4. Erfassen Sie sämtliche Informationen zum Status von NetworkManager in `/var/log/NetworkManager`.

Weitere Informationen zu NetworkManager finden Sie unter*Kapitel 36, Verwendung von NetworkManager*.

40.6 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, als das Problem auftrat.

40.6.1 Verwalten von Partitions-Images

In manchen Fällen müssen Sie eine Sicherung einer ganzen Partition oder sogar der gesamten Festplatte erstellen. Im Lieferumfang von Linux ist das Werkzeug **dd** enthalten, das eine exakte Kopie Ihrer Festplatte erstellen kann. In Kombination mit **gzip** wird dabei Speicherplatz gespart.

PROZEDUR 40.7 SICHERN UND WIEDERHERSTELLEN VON FESTPLATTEN

1. Starten Sie eine Shell als `root`-Benutzer.
2. Wählen Sie das Quellgerät aus. Typischerweise lautet es wie `/dev/sda` (bezeichnet als *SOURCE*).
3. Entscheiden Sie, wo das Image gespeichert werden soll (bezeichnet als *BACKUP_PATH*). Der Speicherort darf sich nicht auf dem Quellgerät befinden. Mit anderen Worten: Wenn Sie eine Sicherung von `/dev/sda` erstellen, muss das Image nicht unter `/dev/sda` gespeichert werden.
4. Führen Sie die Kommandos zur Erstellung einer komprimierten Image-Datei aus:

   ```
   dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
   ```

5. Stellen Sie die Festplatte mithilfe der folgenden Kommandos wieder her:

   ```
   gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
   ```

Wenn Sie eine Partition nur sichern müssen, ersetzen Sie den Platzhalter *QUELLE* durch Ihre entsprechende Partition. In diesem Fall kann sich Ihre Image-Datei auf derselben Festplatte befinden, allerdings in einer anderen Partition.

40.6.2 Verwenden des Rettungssystems

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.

Zum Beheben dieser Situationen bietet SUSE Linux Enterprise Server ein Rettungssystem, das Sie booten können. 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.
- Eine Wiederherstellung ab einem fehlerhaft installierten Gerätetreiber oder einem nicht verwendbaren Kernel kann durchgeführt werden.
- Die Größe von Partitionen kann mithilfe des parted-Kommandos verändert werden. Weitere Informationen zu diesem Werkzeug 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 vom Original-Installationsmedium booten.

Anmerkung: IBM z Systems: Starten des Rettungssystems

Auf IBM z Systems kann das Installationssystem zur Rettung herangezogen werden. Zum Starten des Rettungssystems beachten Sie die Anweisungen in *Abschnitt 40.7, „IBM z Systems: Verwenden von initrd als Rettungssystem“*.

1. Legen Sie das Installationsmedium in Ihr DVD-Laufwerk ein.
2. Booten Sie das System neu.
3. Drücken Sie im Boot-Fenster F4 und wählen Sie *DVD-ROM*. Wählen Sie dann im Hauptmenü die Option *Rettungssystem*.

4. Geben Sie an der Eingabeaufforderung `Rescue: root` ein. Ein Passwort ist nicht erforderlich.

Wenn Ihnen kein DVD-Laufwerk zur Verfügung steht, können Sie das Rettungssystem von einer Netzwerkquelle booten. Das nachfolgende Beispiel bezieht sich auf das entfernte Booten – wenn Sie ein anderes Boot-Medium verwenden, beispielsweise eine DVD, ändern Sie die Datei `info` entsprechend, und führen Sie den Boot-Vorgang wie bei einer normalen Installation aus.

1. Geben Sie die Konfiguration Ihres PXE-Boot-Setups ein und fügen Sie die Zeilen `install=`*`protocol`*`://`*`instsource`* und `rescue=1` hinzu. Wenn das Reparatursystem gestartet werden soll, verwenden Sie stattdessen `repair=1`. 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“, wie im *Buch „*Bereitstellungshandbuch*“, Kapitel 9 „Vorbereitung des Bootvorgangs für das Zielsystem“, Abschnitt 9.7 „Wake-on-LAN“* erläutert.
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, die über die Tasten Alt–F1 bis Alt–F6 aufgerufen werden.

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`** und **`shutdown`**, **`ip`** und **`ss`** für die Netzwerkwartung. Das Verzeichnis `/usr/bin` enthält den vi-Editor, find, less sowie SSH.

Die Systemmeldungen können über das Kommando **`dmesg`** angezeigt werden; mit **`journalctl`** rufen Sie das Systemprotokoll ab.

40.6.2.1 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 folgendes Kommando:

   ```
   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.

40.6.2.2 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. Das System enthält die Dienstprogramme für die Überprüfung und Reparatur der Dateisysteme `btrfs`, `ext2`, `ext3`, `ext4`, `reiserfs`, `xfs`, `dosfs` und `vfat`. Nutzen Sie das Kommando **`fsck.`** *`FILESYSTEM`*; wenn Sie beispielsweise eine Dateisystemprüfung für `btrfs` ausführen möchten, verwenden Sie **`fsck.btrfs`**.

40.6.2.3 Zugriff auf das installierte System

Wenn Sie vom Rettungssystem aus auf das installierte System zugreifen müssen, ist dazu eine *change-root*-Umgebung erforderlich. Beispiele: Bearbeiten der Bootloader-Konfiguration oder Ausführen eines Dienstprogramms zur Hardwarekonfiguration.

Gehen Sie zur Einrichtung einer change-root-Umgebung, die auf dem installierten System basiert, folgendermaßen vor:

1.

   ### Tipp: Importieren von LVM-Volume-Gruppen

   Wenn Sie ein LVM-Setup verwenden (allgemeinere Informationen siehe *Buch „Storage Administration Guide"*), importieren Sie alle vorhandenen Volume-Gruppen, damit Sie das oder die Geräte auffinden und einhängen können:

   ```
   rootvgimport -a
   ```

   Ermitteln Sie mit **`lsblk`**, welcher Knoten zur Stammpartition gehört. Im Beispiel ist dies `/dev/sda2`:

   ```
   lsblk
   NAME        MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
   sda           8:0    0 149,1G  0 disk
   ├─sda1        8:1    0     2G  0 part  [SWAP]
   ├─sda2        8:2    0    20G  0 part  /
   └─sda3        8:3    0   127G  0 part
     └─cr_home 254:0    0   127G  0 crypt /home
   ```

2. Hängen Sie die Stammpartition vom installierten System aus ein:

   ```
   mount /dev/sda2 /mnt
   ```

3. Hängen Sie die Partitionen `/proc`, `/dev` und `/sys` ein:

   ```
   mount -t proc none /mnt/proc
   mount --rbind /dev /mnt/dev
   mount --rbind /sys /mnt/sys
   ```

4. Nun können Sie per „change root" in die neue Umgebung wechseln und dabei die `bash`-Shell beibehalten:

   ```
   chroot /mnt /bin/bash
   ```

5. Abschließend hängen Sie die restlichen Partitionen vom installierten System ein:

   ```
   mount -a
   ```

6. 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: Einschränkungen

Obwohl Sie über uneingeschränkten Zugriff auf die Dateien und Anwendungen des installierten Systems verfügen, gibt es einige Beschränkungen. Der Kernel, der ausgeführt wird, ist der Kernel, der mit dem Rettungssystem gebootet wurde, nicht mit der change-root-Umgebung. Er unterstützt nur essenzielle Hardware und das Hinzufügen von Kernel-Modulen über das installierte System ist nur möglich, wenn die Kernel-Versionen genau übereinstimmen. Überprüfen Sie immer die Version des aktuell ausgeführten (Rettungssytem-) Kernels mit **`uname -r`** und stellen Sie fest, ob im Verzeichnis `/lib/modules` in der change-root-Umgebung passende Unterverzeichnisse vorhanden sind. Wenn dies der Fall ist, können Sie die installierten Module verwenden. Andernfalls müssen Sie diese in den richtigen Version von einem anderen Medium, z. B. einem Flash-Laufwerk, bereitstellen. In den meisten Fällen weicht die Kernel-Version des Rettungssystems von der des installierten ab – dann können Sie z. B. nicht einfach auf eine Soundkarte zugreifen. Der Aufruf einer grafischen Bedienoberfläche ist ebenfalls nicht möglich.

Beachten Sie außerdem, dass Sie die „change-root“-Umgebung verlassen, wenn Sie die Konsole mit Alt–F1 bis Alt–F6 umschalten.

40.6.2.4 Bearbeiten und erneutes Installieren des Bootloaders

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 *Abschnitt 40.6.2.3, „Zugriff auf das installierte System“* erläuterten erforderlichen Schritte für den Zugriff auf das installierte System aus.

2. Prüfen Sie, ob der GRUB 2-Bootloader auf dem System installiert ist. Falls nicht, installieren Sie das Paket `grub2` und führen Sie Folgendes aus:

```
grub2-install /dev/sda
```

3. Prüfen Sie, ob die nachfolgend angegebenen Dateien gemäß den in *Kapitel 12, Der Bootloader GRUB 2* erläuterten GRUB 2-Konfigurationsgrundlagen ordnungsgemäß konfiguriert sind, und wenden Sie gegebenenfalls die Fehlerbehebungen an.

   - `/etc/default/grub`
   - `/boot/grub2/device.map` (optionale Datei; nur vorhanden, wenn sie manuell erstellt wurde)
   - `/boot/grub2/grub.cfg` (diese Datei wird automatisch generiert; nicht bearbeiten)
   - `/etc/sysconfig/bootloader`

4. Installieren Sie den Bootloader mit folgender Befehlssequenz neu:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. 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
```

40.6.2.5 Korrektur der Kernel-Installation

Ein Kernel-Update kann einen neuen Fehler verursachen, der sich auf Ihr System auswirken kann. Es kann z. B. ein Treiber für eine Hardwarekomponente in Ihrem System falsch sein, weshalb Sie nicht auf die Komponente zugreifen und diese nicht verwenden können. Kehren Sie in diesem Fall zum letzten funktionierenden Kernel zurück (sofern er im System verfügbar ist) oder installieren Sie den Original-Kernel vom Installationsmedium.

Tipp: So erhalten Sie die aktuellsten Kernels nach dem Update

Um Fehler beim Booten durch eine fehlerhaften Kernel-Aktualisierung zu vermeiden, können Sie die Multiversionsfunktion für Kernel nutzen und `libzypp` mitteilen, welche Kernel Sie nach der Aktualisierung erhalten möchten.

Damit z. B. immer die beiden letzten Kernels und der aktuell ausgeführte erhalten bleiben, fügen Sie

```
multiversion.kernels = latest,latest-1,running
```

zur Datei `/etc/zypp/zypp.conf` hinzu. Weitere Informationen finden Sie in *Buch „Bereitstellungshandbuch", Kapitel 15 „Installieren von mehreren Kernel-Versionen"*.

Ähnlich verhält es sich, wenn Sie einen defekten Treiber für ein nicht durch SUSE Linux Enterprise Server unterstütztes Gerät neu installieren oder aktualisieren müssen. Wenn z. B. ein Hardwarehersteller ein bestimmtes Gerät verwendet, wie einen Hardware-RAID-Controller, für den es erforderlich ist, dass ein Binärtreiber durch das Betriebssystem erkannt wird. Der Hersteller veröffentlicht in der Regel ein Treiberupdate (DUD) mit der korrigierten oder aktualisierten Version des benötigten Treibers.

In beiden Fällen müssen Sie im Rettungsmodus auf das installierte System zugreifen und das mit dem Kernel zusammenhängende Problem beheben, da das System andernfalls nicht korrekt booten wird:

1. Booten Sie von den SUSE Linux Enterprise Server-Installationsmedien.
2. Überspringen Sie diese Schritt, wenn Sie eine Wiederherstellung nach einer fehlerhaften Kernel-Aktualisierung durchführen. Wenn Sie eine Driver Update Disk (DUD) verwenden, drücken Sie `F6`, um die Treiberaktualisierung nach der Anzeige des Bootmenüs zu laden, wählen Sie den Pfad oder die URL für die Treiberaktualisierung aus und bestätigen Sie die Auswahl mit *Ja*.
3. Wählen Sie im Bootmenü den Eintrag *Rettungssystem*, und drücken Sie `Eingabetaste`. Wenn Sie eine DUD verwenden, werden Sie aufgefordert, den Speicherplatz der Treiberaktualisierung anzugeben.
4. Geben Sie an der Eingabeaufforderung `Rescue: root` ein. Ein Passwort ist nicht erforderlich.

5. Hängen Sie das Zielsystem manuell ein und führen Sie „change root“ in die neue Umgebung durch. Weitere Informationen finden Sie unter *Abschnitt 40.6.2.3, „Zugriff auf das installierte System“*.

6. Wenn Sie eine DUD verwenden, installieren oder aktualisieren Sie das fehlerhafte Treiberpaket. Stellen Sie stets sicher, dass die installierte Kernel-Version exakt mit der Version des Treibers übereinstimmt, den Sie installieren möchten.
   Wenn Sie eine fehlerhafte Installation einer Treiberaktualisierung korrigieren, können Sie nach dem folgenden Verfahren den Originaltreiber vom Installationsmedium installieren.

   a. Identifizieren Sie Ihr DVD-Laufwerk mit **`hwinfo --cdrom`** und hängen Sie es mit **`mount /dev/sr0 /mnt`** ein.

   b. Navigieren Sie zum Verzeichnis, in dem Ihre Kernel-Dateien auf der DVD gespeichert sind, z. B. **`cd /mnt/suse/x86_64/`**.

   c. Installieren Sie die benötigten `kernel-*`-, `kernel-*-base`- und `kernel-*-extra`-Pakete mit dem Kommando **`rpm -i`**.

7. Aktualisieren Sie Konfigurationsdateien und initialisieren Sie den Bootloader gegebenenfalls neu. Weitere Informationen finden Sie in *Abschnitt 40.6.2.4, „Bearbeiten und erneutes Installieren des Bootloaders“*.

8. Entfernen Sie alle bootbaren Medien aus dem Systemlaufwerk und booten Sie neu.

40.7 IBM z Systems: Verwenden von initrd als Rettungssystem

Wenn der Kernel von SUSE Linux Enterprise Server für IBM z Systems aktualisiert oder geändert wird, kann es zu einem versehentlichen Neustart des Systems in einem instabilen Zustand kommen, sodass Fehler bei Standardverfahren von IPLing im installierten System auftreten. In diesem Fall können Sie das Installationssystem zur Rettung heranziehen.

Führen Sie den IPL-Vorgang für SUSE Linux Enterprise Server für das IBM z Systems-Installationssystem gemäß den Anweisungen in *Buch „*Bereitstellungshandbuch*“, Kapitel 4 „Installation auf IBM z Systems“, Abschnitt 4.2 „Vorbereitung der Installation“* aus. Wählen Sie *Start Installation* (Installation starten), und geben Sie alle erforderlichen Parameter ein. Nach dem Laden des Installati-

onssystems werden Sie aufgefordert, den Anzeigetyp für die Steuerung der Installation anzugeben. Wählen Sie `SSH` aus. Nun können Sie sich mit SSH als `root` ohne Passwort beim System anmelden.

Zu diesem Zeitpunkt sind noch keine Festplatten konfiguriert. Sie müssen Sie konfigurieren, um fortfahren zu können.

PROZEDUR 40.8 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 40.9 KONFIGURIEREN EINER ZFCP-FESTPLATTE

1. Für die Konfiguration einer zFCP-Festplatte muss zunächst der zFCP-Adapter konfiguriert werden. Das geschieht mit folgendem Befehl:

   ```
   zfcp_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:

   ```
   zfcp_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.

Damit ist das Rettungssystem vollständig eingerichtet, und Sie können mit der Reparatur des installierten Systems beginnen. Weitere Informationen zur Reparatur der häufigsten Probleme finden Sie in *Abschnitt 40.6.2, „Verwenden des Rettungssystems“*.

A Aktualisierungen der Dokumentation

In diesem Kapitel finden Sie die Änderungen, die am Inhalt dieses Dokuments vorgenommen wurden.

Dieses Handbuch wurde in den folgenden Zeiträumen aktualisiert:

- *Abschnitt A.1, „September 2018 (Wartungsaktualisierung der Dokumentation für SUSE Linux Enterprise Server 12 SP3)“*
- *Abschnitt A.2, „Juni 2018 (Wartungsaktualisierung der Dokumentation für SUSE Linux Enterprise Server 12 SP3)“*
- *Abschnitt A.3, „Dezember 2017 (Wartungsversion von SUSE Linux Enterprise Server 12 SP3)“*
- *Abschnitt A.4, „September 2017 (ursprüngliche Version von SUSE Linux Enterprise Server 12 SP3)“*
- *Abschnitt A.5, „November 2016 (ursprüngliche Freigabe von SUSE Linux Enterprise Server 12 SP2)“*
- *Abschnitt A.6, „März 2016 (Wartungsversion von SUSE Linux Enterprise Server 12 SP1)“*
- *Abschnitt A.7, „Dezember 2015 (ursprüngliche Freigabe von SUSE Linux Enterprise Server 12 SP1)“*
- *Abschnitt A.8, „Februar 2015 (Wartungsaktualisierung der Dokumentation)“*
- *Abschnitt A.9, „Oktober 2014 (ursprüngliche Version von SUSE Linux Enterprise Server 12)“*

A.1 September 2018 (Wartungsaktualisierung der Dokumentation für SUSE Linux Enterprise Server 12 SP3)

Fehlerbehebungen

- Verweise auf `pure-ftpd` aus *Kapitel 32, Einrichten eines FTP-Servers mit YaST* entfernt (https://bugzilla.opensuse.com/show_bug.cgi?id=1101631).
- Erläuterung verschiedener Speicherorte für `udev`-Regeldateien und Aktualisierung des Namens der Standardregeldatei in *Kapitel 21, Gerätemanagement über dynamischen Kernel mithilfe von* `udev` (https://bugzilla.suse.com/show_bug.cgi?id=1103082)
- Korrektur eines Befehls und von dessen Hauptseitenverweis in *Abschnitt 13.6.2, „Systemprotokoll“* (https://bugzilla.suse.com/show_bug.cgi?id=1104266)

A.2 Juni 2018 (Wartungsaktualisierung der Dokumentation für SUSE Linux Enterprise Server 12 SP3)

Kapitel 10, Einführung in den Bootvorgang

Vollständige Überarbeitung des Kapitels und Ergänzung systemspezifischer Informationen für IBM z Systems (https://bugzilla.opensuse.com/show_bug.cgi?id=1046514)

Kapitel 14, 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung

Löschen der Dokumentation zur Erstellung von 32-Bit-Anwendungen in einem 64-Bit-System Dieser Vorgang wird von SUSE Linux Enterprise Server nicht unterstützt (https://bugzilla.suse.com/show_bug.cgi?id=1092434).

Abschnitt 16.7, „Einrichten von Bonding-Geräten“

Beschreibungen für alle Bonding-Modi hinzugefügt (Dok.-Kommentar Nr. 35319).

Kapitel 12, Der Bootloader GRUB 2

- *Abschnitt 8.4.2, „Mit `vncmanager` initiierte VNC-Sitzung“* wurde hinzugefügt (Fate-Nr. 319319).
- Auflistung der Videomodi in GRUB mit **`videoinfo`**, **`vbeinfo`** ist nicht mehr aktuell. Weitere Informationen hierzu finden Sie in *Abschnitt 12.2.2, „Die Datei `/etc/default/grub`“* (https://bugzilla.opensuse.com/show_bug.cgi?id=1074026).

Chapter 22, Live-Patching des Linux-Kernels mithilfe von kGraft

- POWER wird für kGraft-Live-Patches unterstützt, siehe *Chapter 22, Live-Patching des Linux-Kernels mithilfe von kGraft* (https://bugzilla.opensuse.com/show_bug.cgi?id=1074844).

Kapitel 12, Der Bootloader GRUB 2

- Ersetzen Sie **grub2-reboot** durch **grub2-once**, um den Standard-Booteintrag nur für den nächsten Bootvorgang zu ändern, siehe *Abschnitt 12.2.2, „Die Datei /etc/default/grub“* (https://bugzilla.opensuse.com/show_bug.cgi?id=1071210).

A.3 Dezember 2017 (Wartungsversion von SUSE Linux Enterprise Server 12 SP3)

Allgemein

- Verschiedene kleinere Korrekturen und Hinzufügungen zur Dokumentation auf Grundlage des technischen Feedbacks.
- Alle Verweise auf das Paket `faillog` entfernt, das nicht mehr erhältlich ist (https://bugzilla.suse.com/show_bug.cgi?id=710788).

Chapter 22, Live-Patching des Linux-Kernels mithilfe von kGraft

kGraft-Patches sind für Sicherheitslücken von CVSS 7+ verfügbar, siehe *Section 22.9, “Umfang von SLE Live Patching”* (https://bugzilla.suse.com/show_bug.cgi?id=1068181).

Fehlerbehebungen

- Option `-alwaysshared` für persistente VNC-Verbindung zu *Prozedur 8.2, „Starten einer permanenten VNC-Sitzung mit **vncserver**“* hinzugefügt (https://bugzilla.suse.com/show_bug.cgi?id=1081409).
- Hinweis gelöscht, der einen Verweis auf YaST für *DEFAULT-Optionen in *Abschnitt 12.2.2, „Die Datei /etc/default/grub“* enthielt (https://bugzilla.suse.com/show_bug.cgi?id=1017728).
- Abschnitte von *Abschnitt 12.3.1, „Speicherort des Bootloaders und Boot-Code-Optionen“* aufeinander abgestimmt und weitere Details bereitgestellt (https://bugzilla.suse.com/show_bug.cgi?id=1017737).

- `~/.alias` zu *Abschnitt 1.1.1, „Die Bash-Konfigurationsdateien“* hinzugefügt (https://bugzilla.suse.com/show_bug.cgi?id=1062209).
- Tipp für den Import von Volume-Gruppen zu *Abschnitt 40.6.2.3, „Zugriff auf das installierte System“* hinzugefügt (https://bugzilla.suse.com/show_bug.cgi?id=1051369).
- Beschreibung der Boot-Festplattenreihenfolge in *Abschnitt 12.3.2, „Anpassen der Festplattenreihenfolge“* (https://bugzilla.suse.com/show_bug.cgi?id=1017731)
- *VGA-Modus* in *Abbildung 12.5, „Kernel-Parameter“* ersetzt (https://bugzilla.suse.com/show_bug.cgi?id=1017753).
- *Abschnitt 12.2.3, „Skripte in `/etc/grub.d`“* aktualisiert und vereinfacht (https://bugzilla.suse.com/show_bug.cgi?id=1017726).

A.4 September 2017 (ursprüngliche Version von SUSE Linux Enterprise Server 12 SP3)

Allgemein

- Verschiedene kleinere Korrekturen und Hinzufügungen zur Dokumentation auf Grundlage des technischen Feedbacks.
- Alle Verweise auf das Paket `faillog` entfernt, das nicht mehr erhältlich ist (https://bugzilla.suse.com/show_bug.cgi?id=710788).

Kapitel 4, YaST

- Neues Kapitel über die YaST-GUI hinzugefügt und Hinweis auf erweiterte Tastenkombinationen (https://bugzilla.suse.com/show_bug.cgi?id=1010039).

Kapitel 5, YaST im Textmodus

- *Abschnitt 5.2, „Erweiterte Tastenkombinationen“* wurde hinzugefügt (https://bugzilla.suse.com/show_bug.cgi?id=1010039).

Kapitel 6, Verwalten von Software mit Kommandozeilen-Tools

- *Abschnitt 6.1.5.2, „Aktualisieren von Repositorys“* wurde hinzugefügt (Fate-Nr. 319486).
- *Abschnitt 6.1.3.1, „Installieren aller erforderlichen Patches“* aktualisiert (Fate-Nr. 320653).
- *Abschnitt 6.1.6.3, „Verwendung von* **`zypper info`**“ wurde hinzugefügt (Fate-Nr. 321104).

Kapitel 7, Systemwiederherstellung und Snapshot-Verwaltung mit Snapper

- Hinweis, dass Snapshots von Snapper-Rollbacks automatisch gelöscht werden Siehe *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots“* und *Abschnitt 7.3.1, „Snapshots nach dem Rollback“* (Fate-Nr. 321773).
- Unter *Abschnitt 7.4, „Erstellen und Bearbeiten von Snapper-Konfigurationen“* ausführliche Informationen zur Berechnung der Mindestgröße des Root-Dateisystems zum Aktivieren von Snapshots eingefügt (https://bugzilla.suse.com/show_bug.cgi?id=1036175).
- Erwähnung des Btrfs-Standard-Subvolumes und dessen Beschränkungen (https://bugzilla.suse.com/show_bug.cgi?id=1045884)

Kapitel 8, Fernzugriff mit VNC

- Informationen zur verschlüsselten Kommunikation korrigiert und Abschnitt *Abschnitt 8.5, „Verschlüsselte VNC-Kommunikation“* über deren Einrichtung eingefügt (https://bugzilla.suse.com/show_bug.cgi?id=1029117).

Kapitel 9, Kopieren von Dateien mit RSync

- Ehemaliges Kapitel über *Dateisynchronisierung* vollständig überarbeitet, Schwerpunkt liegt nun auf Rsync.

Kapitel 13, Der Daemon `systemd`

- System V-init-Befehl **`chkconfig`** in die Vergleichstabelle in *Abschnitt 13.2.2.1, „Aktivieren/Deaktivieren von Diensten über die Kommandozeile“* eingefügt (Dok.-Kommentar Nr. 30251).

Kapitel 16, Grundlegendes zu Netzwerken

- Mehrere Dok.-Kommentare in *Abschnitt 16.8, „Einrichten von Team-Geräten für Netzwerk-Teaming“* korrigiert.

Kapitel 21, Gerätemanagement über dynamischen Kernel mithilfe von `udev`

- **`udevadm`**-Befehle korrigiert.

Chapter 22, Live-Patching des Linux-Kernels mithilfe von kGraft

Section 22.4, “Patch-Lebenszyklus” aktualisiert (Fate-Nr. 322212).

Kapitel 23, Spezielle Systemfunktionen

- Doppelte Inhalte aus *Abschnitt 23.1.4, „Protokolldateien: Paket logrotate“* entfernt.

Teil II, „Booten eines Linux-Systems“

- Reihenfolge der Kapitel entsprechend der Reihenfolge beim Bootvorgang neu geordnet.

Kapitel 33, Der Proxyserver Squid

- Erläuterung des YaST-Squid-Moduls

Fehlerbehebungen

- Befehl für den Start von Apache2, **`httpd2`**, durch **`apache2ctl`** ersetzt (https://bugzilla.suse.com/show_bug.cgi?id=1042437).
- Tippfehler in einem als Verweis genannten RFC-Dokument in *Abschnitt 16.2.5, „Weiterführende Informationen“* korrigiert (https://bugzilla.suse.com/show_bug.cgi?id=1045881).
- Unter *Abschnitt 40.6, „Probleme mit Daten“* Verweis auf ein YaST-Modul gelöscht, das nicht mehr erhältlich ist (https://bugzilla.suse.com/show_bug.cgi?id=1052675).

A.5 November 2016 (ursprüngliche Freigabe von SUSE Linux Enterprise Server 12 SP2)

Allgemein

- Die neue E-Mail-Adresse für Rückmeldungen zur Dokumentation lautet `doc-team@suse.com`.
- Die Dokumentation für Docker Open Source Engine wurde überarbeitet und hat die neue Bezeichnung *Docker Guide* (Docker-Handbuch) erhalten.

Kapitel 3, YaST-Online-Aktualisierung

- In *Abschnitt 3.3, „Automatische Online-Updates“* ist erwähnt, dass nach der automatischen Online-Aktualisierung das System nicht automatisch neu gestartet wird (Dok.-Kommentar Nr. 30116).

Kapitel 6, Verwalten von Software mit Kommandozeilen-Tools

- Mit **`zypper patch`** werden optionale Patches nicht mehr standardmäßig installiert. Verwenden Sie zum Installieren optionaler Patches den Parameter `--with-optional` (Fate-Nr. 320447).

Kapitel 7, Systemwiederherstellung und Snapshot-Verwaltung mit Snapper

- `/var/cache` und `/var/lib/libvirt/images` zu *Abschnitt 7.1.2, „Verzeichnisse, die aus Snapshots ausgenommen sind“* hinzugefügt (Fate-Nr. 320834).
- *Abschnitt 7.6, „Automatisches Bereinigen von Snapshots“* hinzugefügt. Er umfasst auch die Dokumentation zur neuen Quotenunterstützung von Snapper (Fate-Nr. 312751).
- *F:* hinzugefügt (Fate-Nr. 318799).

Kapitel 10, Einführung in den Bootvorgang

- Benutzern wurde der Rat gegeben, das Dateisystem zu reparieren, wenn das Root-Dateisystem beim Starten einen Fehler aufweist (Fate-Nr. 320443).

Kapitel 12, Der Bootloader GRUB 2

- Hinweis zur Unterstützung von **`grub-once`** durch `/boot/grub2/custom.cfg` zu *Abschnitt 12.2, „Konfigurationsdateistruktur“* hinzugefügt (Fate-Nr. 319632).
- *Abschnitt 7.3.2, „Abrufen und Erkennen von Snapshot-Booteinträgen“* hinzugefügt (Fate-Nr. 317972 und Fate-Nr. 318101).
- Informationen zur Secure Boot-Unterstützung zu *Abschnitt 12.3.1, „Speicherort des Bootloaders und Boot-Code-Optionen“* hinzugefügt (Fate-Nr. 316553).

Kapitel 16, Grundlegendes zu Netzwerken

- Abschnitt zu Netzwerk-Teaming (Fate-Nr. 320468) hinzugefügt, siehe *Abschnitt 16.8, „Einrichten von Team-Geräten für Netzwerk-Teaming“*.
- `TUNNEL_DEVICE` für Wicked (Fate-Nr. 317977, *Abschnitt 16.5.1.5, „Verwenden von Tunneln mit Wicked“*) erwähnt.

Kapitel 24, Zeitsynchronisierung mit NTP

- Informationen zur Startoption *Ohne Daemon synchronisieren* hinzugefügt. „Chroot jail“ ist nicht mehr der Standard (Fate Nr. 320392).

Anmerkung: NFSv2

- Hinweis zum Aktivieren von NFSv2 hinzugefügt (https://bugzilla.suse.com/show_bug.cgi?id=919708).

Kapitel 33, Der Proxyserver Squid

- Kapitel zu Squid 3.5 aktualisiert (Fate-Nr. 319674).

Abschnitt 39.5, „Sammeln von Informationen bei der Installation“

- Abschnitt zu Protokolldateien, die während der Installation erstellt werden, hinzugefügt (Fate-Nr. 320015).

Fehlerbehebungen

- Falsche Dienstnamen für NFS mit Kerberos (https://bugzilla.suse.com/show_bug.cgi?id=983230).
- Live-Patches werden gemäß dem SUSE-CVSS-Score freigegeben (https://bugzilla.suse.com/show_bug.cgi?id=992101).

A.6 März 2016 (Wartungsversion von SUSE Linux Enterprise Server 12 SP1)

Kapitel 10, Einführung in den Bootvorgang

Hinweis zur initramfs-Migration von swap zu LVM hinzugefügt (https://bugzilla.suse.com/show_bug.cgi?id=).

A.7 Dezember 2015 (ursprüngliche Freigabe von SUSE Linux Enterprise Server 12 SP1)

Allgemein

- *Buch „Subscription Management Tool for SLES 12 SP5"* ist nun Bestandteil der Dokumentation für SUSE Linux Enterprise Server.
- Die von SUSE bereitgestellten Add-ons wurden in Module und Erweiterungen umbenannt. Die Handbücher wurden entsprechend aktualisiert.
- Verschiedene kleinere Korrekturen und Hinzufügungen zur Dokumentation auf Grundlage des technischen Feedbacks.
- Der Registrierungsdienst wurde von Novell Customer Center in SUSE Customer Center geändert.
- In YaST befindet sich *Netzwerkeinstellungen* nun in der Gruppe *System*. *Netzwerkgeräte* entfällt (https://bugzilla.suse.com/show_bug.cgi?id=867809).

Kapitel 7, Systemwiederherstellung und Snapshot-Verwaltung mit Snapper

- Informationen zum neuen Schalter `--sync` für **`snapper delete`** in *Abschnitt 7.5.4, „Löschen von Snapshots"* (Fate-Nr. 317066) hinzugefügt.
- *Abschnitt 7.3.2, „Abrufen und Erkennen von Snapshot-Booteinträgen"* hinzugefügt (Fate-Nr. 317972 und Fate-Nr. 318101).
- Tipp zum Ausführen eines Rollbacks in den ursprünglichen Installationszustand oder in den Zustand vor einer Systemaktualisierung zu *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots"* hinzugefügt (Fate-Nr. 317973 und Fate-Nr. 317900).
- *Abschnitt 7.1.3.3, „Erstellen und Einhängen neuer Subvolumes"* hinzugefügt (Fate-Nr. 318805, https://bugzilla.suse.com/show_bug.cgi?id=910602).

Kapitel 8, Fernzugriff mit VNC

- Einen Hinweis in einen Abschnitt umgewandelt, Informationen zu VNC mit standardmäßigem gesicherten Protokoll hinzugefügt (Fate-Nr. 318936) und `tightvnc` entfernt (wird komplett durch `tigervnc` ersetzt). Alles in *Abschnitt 8.3.1, „Verfügbare Konfigurationen“*.

Kapitel 6, Verwalten von Software mit Kommandozeilen-Tools

- *Abschnitt 6.1.4, „Ermitteln von Prozessen und Diensten, die gelöschte Dateien verwenden“* hinzugefügt (Fate-Nr. 318827).
- Weitere Beispiele für **`zypper list-patches --cve`** in *Abschnitt 6.1.3.1, „Installieren aller erforderlichen Patches“* hinzugefügt (Fate-Nr. 319053).
- *Abschnitt 6.1.2.6, „Installieren von Paketen aus deaktivierten Repositorys“* sowie einen Tipp zum Entfernen aller `debuginfo`-Pakete in *Abschnitt 6.1.2, „Installieren und Entfernen von Software mit zypper“* hinzugefügt (Fate-Nr. 316287).
- Satz über den notwendigen Neustart des Systems nach Anwenden eines bestimmten Patches eingefügt. (Fate-Nr. 317872).

Kapitel 15, `journalctl`: Abfragen des `systemd`-Journals

- Abschnitt *Abschnitt 15.6, „Filtern des `systemd`-Journals mit YaST“* hinzugefügt (Fate-Nr. 318486).

Kapitel 12, Der Bootloader GRUB 2

- Gesamtes Kapitel gemäß der aktuellen GRUB-Version aktualisiert/vereinfacht, sowohl Kommandozeilenversion als auch YaST-Version.

Kapitel 11, UEFI (Unified Extensible Firmware Interface)

- *Abschnitt 11.1.4, „Verwenden von Nicht-Inbox-Treibern“* hinzugefügt (Fate-Nr. 317593).

Kapitel 16, Grundlegendes zu Netzwerken

- Nanny ist nunmehr in *Abschnitt 16.5.1.3, „Nanny“* standardmäßig aktiviert (Fate-Nr. 318977).
- *Abschnitt 16.6, „Grundlegende Routereinrichtung“* hinzugefügt (Fate-Nr. 317121, https://bugzilla.suse.com/show_bug.cgi?id=870132 ↗).
- *Abschnitt 16.9, „Softwaredefiniertes Networking mit Open vSwitch“* hinzugefügt (Fate-Nr. 318497).

Kapitel 25, Domain Name System (DNS)

- *Abschnitt 25.3.2.9.1, „Hinzufügen von Reverse Zones“* hinzugefügt (Dok.-Kommentar Nr. 1356).

Kapitel 27, Verteilte Nutzung von Dateisystemen mit NFS

- Tipp hinzugefügt, dass das Einhängen per `--bind` nicht mehr für NFSv4-Einhängen in *Abschnitt 27.3.2, „Manuelles Exportieren von Dateisystemen“* erforderlich ist (Fate-Nr. 316311).

Verfügbare Software zur Datensynchronisierung

- Cloud-Computing für die Dateisynchronisierung erwähnt.

Kapitel 31, Der HTTP-Server Apache

- **`CA.sh`** durch das explizite Kommando **`openssl`** in *Abschnitt 31.6.1.3, „Anfordern eines offiziell signierten Zertifikats“* ersetzt (Dok.-Kommentar Nr. 28367).
- *Abschnitt 31.7, „Ausführen mehrerer Apache-Instanzen auf demselben Server“* hinzugefügt (Fate-Nr. 317786).
- Kapitel gemäß der aktuellen Apache-Version 2.4 aktualisiert (Fate-Nr. 319012).

Kapitel 40, Häufige Probleme und deren Lösung

- Verfahren zur Neuinstallation von GRUB 2 in *Abschnitt 40.6.2.4, „Bearbeiten und erneutes Installieren des Bootloaders“* optimiert.

Teil III, „System“

- *Chapter 22, Live-Patching des Linux-Kernels mithilfe von kGraft* hinzugefügt (Fate-Nr. 313296 und Fate-Nr. 313438).

Fehlerbehebungen

- Veralteter Dienst `acpid.service` entfernt (https://bugzilla.suse.com/show_bug.cgi?id=918655).
- Falscher Titel in *Chapter 22, Live-Patching des Linux-Kernels mithilfe von kGraft* korrigiert (https://bugzilla.suse.com/show_bug.cgi?id=954250).

- Falscher Pfadname in *Kapitel 31, Der HTTP-Server Apache* korrigiert (https://bugzilla.suse.com/show_bug.cgi?id=949395).
- Absatz über das standardmäßig aktivierte sichere Booten in *Abschnitt 11.1.1, „Implementierung auf SUSE Linux Enterprise Server“* hinzugefügt (https://bugzilla.suse.com/show_bug.cgi?id=879486).
- Dokumentation zu schreibgeschützten VNC-Passwörtern in *Abschnitt 8.4, „Permanente VNC-Sitzungen“* entfernt, da diese in SUSE Linux Enterprise Server nicht verfügbar sind (https://bugzilla.suse.com/show_bug.cgi?id=941307).
- Verfahren zum Zugreifen auf das installierte System im Rettungsmodus in *Abschnitt 40.6.2.3, „Zugriff auf das installierte System“* korrigiert (https://bugzilla.suse.com/show_bug.cgi?id=918217).
- Neuen Tipp zum Aktualisieren der Datei „initramfs“ nach dem Ändern der Standardkonfiguration für **`sysctl`** in *Abschnitt 10.2.2.1, „Die `initramfs`-Datei“* hinzugefügt (https://bugzilla.suse.com/show_bug.cgi?id=927506).
- Tipp hinzugefügt, wie verhindert wird, dass böswillige Benutzer das Netzwerkgerät auf NFS-Roots in *Abschnitt 27.4.1, „Importieren von Dateisystemen mit YaST“* und *Abschnitt 16.4.1.2.5, „Aktivieren des Netzwerkgeräts“* deaktivieren (https://bugzilla.suse.com/show_bug.cgi?id=938152).
- Irreführende Angaben zu `kernel-`*`FLAVOR`*`-extra` in *Abschnitt 39.6, „Unterstützung für Kernelmodule“* korrigiert (http://bugzilla.suse.com/show_bug.cgi?id=922976).
- Btrfs/Snapper: Snapshots mit neuen Subvolumes werden nicht gelöscht (https://bugzilla.suse.com/show_bug.cgi?id=910602).
- Btrfs-Dokumentation auf separatem Subvolume unter /var/lib und Unterstützung (https://bugzilla.suse.com/show_bug.cgi?id=930424).

A.8 Februar 2015 (Wartungsaktualisierung der Dokumentation)

Kapitel 13, Der Daemon `systemd`

Rechtschreibfehler in einem Befehl behoben (https://bugzilla.suse.com/show_bug.cgi?id=900219).

A.9 Oktober 2014 (ursprüngliche Version von SUSE Linux Enterprise Server 12)

Allgemein

- Gesamte KDE-Dokumentation und sämtliche Verweise auf KDE entfernt, da KDE nicht mehr angeboten wird.
- Alle Verweise auf SuSEconfig entfernt, da SuSEconfig nicht mehr unterstützt wird (Fate-Nr. 100011).
- System V-init durch systemd ersetzt (Fate-Nr. 310421). Betroffene Teile der Dokumentation aktualisiert.
- YaST-Runlevel-Editor durch Services-Manager ersetzt (Fate-Nr. 312568). Betroffene Teile der Dokumentation aktualisiert.
- Alle Verweise auf ISDN-Unterstützung entfernt, da keine ISDN-Unterstützung mehr erfolgt (Fate-Nr. 314594).
- Alle Verweise auf das YaST-DSL-Modul entfernt, da dieses nicht mehr angeboten wird (Fate-Nr. 316264).
- Alle Verweise auf das YaST-Modemmodul entfernt, da dieses nicht mehr angeboten wird (Fate-Nr. 316264).
- Btrfs ist nunmehr das Standard-Dateisystem für die Root-Partition (Fate-Nr. 315901). Betroffene Teile der Dokumentation aktualisiert.
- **`dmesg`** bietet nunmehr Zeitstempel in Klartext in einem ähnlichen Format wie `ctime()` (Fate-Nr. 316056). Betroffene Teile der Dokumentation aktualisiert.
- syslog und syslog-ng wurden durch rsyslog ersetzt (Fate-Nr. 316175). Betroffene Teile der Dokumentation aktualisiert.
- MariaDB wird nunmehr als relationale Datenbank anstelle von MySQL angeboten (Fate-Nr. 313595). Betroffene Teile der Dokumentation aktualisiert.
- SUSE-Produkte sind nicht mehr unter http://download.novell.com erhältlich, sondern unter http://download.suse.com. Links entsprechend angepasst.
- Das Novell Customer Center wurde durch das SUSE Customer Center ersetzt. Betroffene Teile der Dokumentation aktualisiert.

- `/var/run` wird als tmpfs eingehängt (Fate-Nr. 303793). Betroffene Teile der Dokumentation aktualisiert.
- Die folgenden Architekturen werden nicht mehr unterstützt: IA64 und x86. Betroffene Teile der Dokumentation aktualisiert.
- Das herkömmliche Verfahren zum Einrichten des Netzwerks mit `ifconfig` wurde durch `wicked` ersetzt. Betroffene Teile der Dokumentation aktualisiert.
- Zahlreiche Netzwerkkommandos sind überholt und wurden durch neuere Kommandos ersetzt (in den meisten Fällen **`ip`**. Betroffene Teile der Dokumentation aktualisiert.

  `arp`: **`ip neighbor`**
  `ifconfig`: **`ip addr`**, **`ip link`**
  `iptunnel`: **`ip tunnel`**
  `iwconfig`: **`iw`**
  `nameif`: **`ip link`**, **`ifrename`**
  `netstat`: **`ss`**, **`ip route`**, **`ip -s link`**, **`ip maddr`**
  `route`: **`ip route`**

- Verschiedene kleinere Korrekturen und Hinzufügungen zur Dokumentation auf Grundlage des technischen Feedbacks.

Kapitel 3, YaST-Online-Aktualisierung

- YaST bietet eine Option zum Aktivieren und Deaktivieren der Verwendung von Delta-RPMs (Fate-Nr. 314867).
- Vor dem Installieren von Patches, für die ein Neustart erforderlich ist, werden Sie durch YaST benachrichtigt, und Sie können über die weitere Vorgehensweise entscheiden.

Kapitel 39, Erfassen der Systeminformationen für den Support

- Abschnitt hinzugefügt: *Abschnitt 39.1, „Anzeigen aktueller Systeminformationen“* (Fate-Nr. 315869).
- Abschnitt über das Werkzeug für die supportconfig-Analyse (SCA-Werkzeug) und die SCA-Appliance hinzugefügt: *Abschnitt 39.4, „Analysieren von Systeminformationen“* (Fate-Nr. 315699).

- Abschnitt hinzugefügt *Abschnitt 39.6, „Unterstützung für Kernelmodule“* (http://bugzilla.suse.com/show_bug.cgi?id=869159).
- Kapitel aktualisiert und umstrukturiert.

Kapitel 5, YaST im Textmodus

- Informationen zum Filtern und Auswählen von Paketen im Software-Installationsmodul hinzugefügt.

Kapitel 6, Verwalten von Software mit Kommandozeilen-Tools

- Dokumentation zum rug-Kompatibilitätsmodus von Zypper entfernt (Fate-Nr. 317708).
- *Abschnitt 6.1.6, „Abfragen von Repositorys und Paketen mit Zypper“* umgeschrieben.

Kapitel 7, Systemwiederherstellung und Snapshot-Verwaltung mit Snapper

- Kapitel aktualisiert und neue Funktionen eingefügt (Fate-Nr. 312751, Fate-Nr. 316238, Fate-Nr. 316233, Fate-Nr. 316232, Fate-Nr. 316222, Fate-Nr. 316203, Fate-Nr. 316222).
- Abschnitt hinzugefügt: *Abschnitt 7.3, „System-Rollback durch Booten aus Snapshots“* (Fate-Nr. 316231, Fate-Nr. 316221, Fate-Nr. 316541, Fate-Nr. 316522).

Kapitel 8, Fernzugriff mit VNC

- Der VNC-Standardviewer ist nunmehr `tigervnc`.
- Korrekturen zum Starten des Fenstermanagers in persistenten VNC-Sitzungen hinzugefügt.

Kapitel 10, Einführung in den Bootvorgang

- Kapitel erheblich verkürzt, da System V-Init durch systemd ersetzt wurde. systemd wird nunmehr in einem separaten Kapitel beschrieben: *Kapitel 13, Der Daemon* `systemd`.

Kapitel 13, Der Daemon `systemd`

- Neues Kapitel zu systemd und zur YaST-Dienste-Verwaltung hinzugefügt (Fate-Nr. 316631, Fate-Nr. 312568).
- Neuer Abschnitt zum Laden der Kernelmodule (http://bugzilla.suse.com/show_bug.cgi?id=892349 ↗).

Kapitel 15, **`journalctl`***: Abfragen des* `systemd`*-Journals*

Neues Kapitel hinzugefügt (http://bugzilla.suse.com/show_bug.cgi?id=878352 ↗).

Kapitel 12, Der Bootloader GRUB 2

- GRUB-Legacy-Dokumentation durch ein neues Kapitel zu GRUB 2 ersetzt.
- Unterstützung für LILO wurde eingestellt.
- Neuer Abschnitt hinzugefügt: *Abschnitt 12.4, „Unterschiede bei der Terminalnutzung auf z Systems“*.

Kapitel 11, UEFI (Unified Extensible Firmware Interface)

- Kapitel aktualisiert und neue Funktionen hinzugefügt (Fate-Nr. 314510, Fate-Nr. 316365).
- Anleitungen dazu, wo das SUSE-Schlüsselzertifikat zu finden ist, hinzugefügt (Dok.-Kommentar Nr. 25080).

Kapitel 17, Druckerbetrieb

Kapitel und Abschnitt gemäß der neuen CUPS-Version und gemäß dem Aspekt, dass PDF nunmehr häufig als Druckdatenformat verwendet wird, aktualisiert (Fate-Nr. 314630).

Kapitel 18, Das X Window-System

- Kapitel aktualisiert, so dass die dynamische Konfiguration bei jedem Starten berücksichtigt wird.
- wurde geändert.*Abschnitt 18.1, „Installation und Konfiguration von Schriften“*

Kapitel 16, Grundlegendes zu Netzwerken

- NetworkManager ist nun Teil der Arbeitsplatzrechnererweiterung: *Abschnitt 16.4.1.1, „Konfigurieren globaler Netzwerkoptionen“* (Fate-Nr. 316888).
- Abschnitt zu neuem **`wicked`** -Framework für die Netzwerkkonfiguration hinzugefügt: *Abschnitt 16.5, „Manuelle Netzwerkkonfiguration“* (Fate-Nr. 316649).
- Zusätzliche Optionen für `/etc/resolv.conf` beschrieben: *Abschnitt 16.5.2, „Konfigurationsdateien“* (Fate-Nr. 316048).

Kapitel 30, SLP

- Kapitel umgeschrieben, so dass deutlich mehr Informationen zum Kommando **`slptool`** angeboten werden.

Kapitel 25, Domain Name System (DNS)

- Das YaST-DNS-Modul unterstützt nunmehr die Konfiguration von Forwardern (Fate-Nr. 309036).

Kapitel 26, DHCP

- dhcpcd entfernt (wird nicht mehr angeboten; Fate-Nr. 316111).

Kapitel 28, Samba

- Abschnitt hinzugefügt: *Abschnitt 28.8, „Weitere Themen“*.
- Abschnitt hinzugefügt: *Abschnitt 28.8.1, „Transparente Dateikomprimierung mit Btrfs“*.
- Abschnitt hinzugefügt: *Abschnitt 28.8.2, „Aufnahmen“*.

Kapitel 27, Verteilte Nutzung von Dateisystemen mit NFS

- Die Konfiguration von NFSv4-Freigaben ist nunmehr größtenteils identisch mit NFSv3; insbesondere die bislang erforderliche Einstellung für das Einhängen mit Einbindung entfällt (Fate-Nr. 315589).
- Das lokale Einhängen von NFS-Volumes auf dem exportierenden Server wird nicht unterstützt.

Kapitel 29, Bedarfsweises Einhängen mit autofs

- Kapitel zu `autofs` hinzugefügt (Fate-Nr. 316185).

Kapitel 31, Der HTTP-Server Apache

- Verweise zu mono und mod_mono entfernt (kein Bestandteil der Distribution mehr).
- Kapitel zur Apache-Version 2.4 aktualisiert (Fate-Nr. 316067).
- Überholte Anweisung `NameVirtualHost` entfernt und *Abschnitt 31.2.2.1, „Virtuelle Hostkonfiguration“* entsprechend aktualisiert.
- Direktiven `Reihenfolge`, `Zulassen` und `Verweigern` mit Standardwert `Anforderungen` aktualisiert.
- Fiktives Unternehmen „Snake Oil“ aus *Abschnitt 31.6, „Einrichten eines sicheren Webservers mit SSL“* entfernt.

Kapitel 32, Einrichten eines FTP-Servers mit YaST

- `pure-ftpd` wurde eingestellt (Fate-Nr. 315176, Fate-Nr. 316308).

Kapitel 37, Energieverwaltung

- Veraltete Verweise auf das Paket `pm-utils` entfernt.

Kapitel 40, Häufige Probleme und deren Lösung

- Neuer Abschnitt hinzugefügt: *Abschnitt 40.3.3, „Einhängen der Root-Btrfs-Partition nicht möglich“* (Fate-Nr. 308679, Fate-Nr. 315126).
- Abschnitt zu überholtem YaST-Reparaturmodul entfernt (Fate-Nr. 308679).

WLAN-Konfiguration

- Kapitel über WLAN-Konfiguration mit YaST entfernt, da das WLAN über NetworkManager konfiguriert werden kann: *Kapitel 36, Verwendung von NetworkManager*.

Tablet PCs

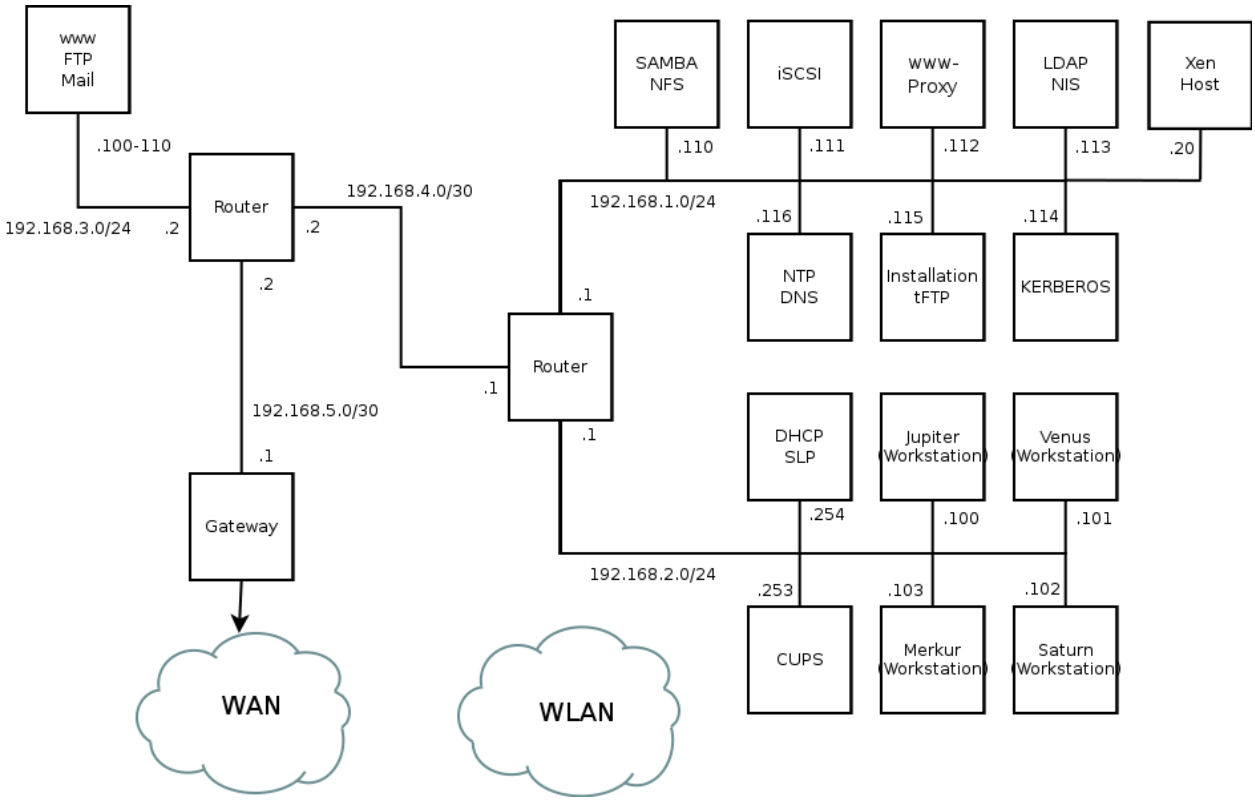
- Überholtes Kapitel zu Tablet-PCs entfernt.

Fehlerbehebungen

- Abschnitt hinzugefügt *Abschnitt 39.6, „Unterstützung für Kernelmodule“* (http://bugzilla.suse.com/show_bug.cgi?id=869159).
- Neues Kapitel hinzugefügt (*Kapitel 15, **journalctl**: Abfragen des systemd-Journals*http://bugzilla.suse.com/show_bug.cgi?id=878352)..

B Ein Beispielnetzwerk

Dieses Beispielnetzwerk wird in allen Kapiteln über das Netzwerk in der Dokumentation zu SUSE Linux Enterprise Server herangezogen.



C GNU-Lizenzen

Dieser Anhang enthält die freie GNU-Dokumentationslizenz (GNU Free Documentation License) Version 1.2.

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.