SUSE Linux Enterprise Desktop 15 SP7

Verwaltungshandbuch

Verwaltungshandbuch

SUSE Linux Enterprise Desktop 15 SP7

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

Veröffentlicht: Dezember 11, 2025

https://documentation.suse.com

Copyright © 2006–2025 , 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 in Abschnitt „GNU Free Documentation License“.

Die SUSE Marken finden Sie in https://www.suse.com/company/legal/. Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern. Markensymbole (®, ™ usw.) kennzeichnen Marken von SUSE und ihren Tochtergesellschaften. Sternchen (*) kennzeichnen Marken von Drittanbietern.

Alle Informationen in diesem Buch wurden mit größter Sorgfalt zusammengestellt. Auch hierdurch kann jedoch keine hundertprozentige Richtigkeit gewährleistet werden. Weder SUSE LLC, ihre Tochtergesellschaften, die Autoren noch die Übersetzer können für mögliche Fehler und deren Folgen haftbar gemacht werden.

Inhalt

Vorwort xxii

1 Verfügbare Dokumentation xxii

2 Verbessern der Dokumentation xxiii

3 Konventionen in der Dokumentation xxiv

4 Support xxvi

Erläuterung zum Support für SUSE Linux Enterprise Desktop xxvi • Technologievorschauen xxvii

I HÄUFIGE TASKS 1

1 Bash-Shell und Bash-Skripte 2

1.1 Was ist „die Shell“? 2

Bash-Konfigurationsdateien 2 • Die Verzeichnisstruktur 5

1.2 Schreiben von Shell-Skripten 10

1.3 Umlenken von Befehlsereignissen 11

1.4 Verwenden von Aliassen 12

1.5 Verwenden von Variablen in der Bash-Shell 13

Verwenden von Argumentvariablen 14 • Verwenden der Variablenersetzung 15

1.6 Gruppieren und Kombinieren von Befehlen 16

1.7 Arbeiten mit häufigen Ablaufkonstrukten 17

Der Steuerungsbefehl „if“ 17 • Erstellen von Schleifen mit dem Befehl `for` 17

1.8 Weitere Informationen 18

2 sudo Grundlagen 19

2.1 Grundlegende Verwendung von **sudo** 19

Ausführung eines einzelnen Befehls 19 • Starten einer Shell 20

2.2 Konfigurieren von **sudo** 21

Bewährte Verfahren für die **sudo**-Konfiguration 22 • Erstellen einer benutzerspezifischen Konfigurationsdatei 22 • Erstellen von benutzerdefinierten Konfigurationen durch Gruppieren von Elementen 24 • Vereinfachen der Konfigurationen mithilfe von Aliasen 25 • Basiskonfigurationssyntax von sudoers 26 • Grundlegende sudoers-Regeln 27

2.3 Verwenden von **sudo** mit X.Org-Anwendungen 29

2.4 Weitere Informationen 30

3 Verwenden von YaST 31

3.1 YaST-Oberfläche im Überblick 31

3.2 Nützliche Tastenkombinationen 31

4 YaST im Textmodus 33

4.1 Navigation in Modulen 34

4.2 Erweiterte Tastenkombinationen 36

4.3 Einschränkung der Tastenkombinationen 37

4.4 YaST-Befehlszeilenoptionen 37

Installieren von Paketen über die Befehlszeile 37 • Arbeiten mit einzelnen Modulen 38 • Befehlszeilenparameter der YaST-Module 38

5 Ändern der Sprach- und Ländereinstellungen mit YaST 63

5.1 Ändern der Systemsprache 63

Bearbeiten von Systemsprachen mit YaST 64 • Wechseln der Standard-Systemsprache 66 • Sprachwechsel für Standard X- und GNOME-Anwendungen 67

5.2 Ändern der Länder- und Zeiteinstellungen 67

6 Verwalten von Benutzern mit YaST 70

6.1 Dialogfeld „Verwaltung von Benutzern und Gruppen“ 70

6.2 Verwalten von Benutzerkonten 72

6.3 Weitere Optionen für Benutzerkonten 75
Automatische Anmeldung und Anmeldung ohne Passwort 75 • Erzwingen von Passwortrichtlinien 76 • Verwalten von Quoten 77

6.4 Ändern der Standardeinstellungen für lokale Benutzer 80

6.5 Zuweisen von Benutzern zu Gruppen 80

6.6 Gruppen verwalten 81

6.7 Ändern der Methode zur Benutzerauthentifizierung 83

6.8 Standard-Systembenutzer 84

6.9 Standard-Systemgruppen 86

7 YaST-Online-Aktualisierung 88

7.1 Das Dialogfeld „Online-Aktualisierung“ 89

7.2 Installieren von Patches 90

7.3 Anzeigen von zurückgezogenen Patches 92

7.4 Automatische Online-Aktualisierungen 92

8 Installieren bzw. Entfernen von Software 96

8.1 Definition der Begriffe 96

8.2 Registrieren eines installierten Systems 98
Registrieren mit YaST 98 • Registrieren mit SUSEConnect 98

8.3 Verwenden des YaST-Software-Managers 99
Suche nach Software 99 • Installieren und Entfernen von Paketen oder Mustern 101 • Aktualisieren von

Paketen 103 • Paketabhängigkeiten 105 • Behandlung von Paketempfehlungen 106

8.4 Verwalten von Software-Repositorys und -Diensten 107

Hinzufügen von Software-Repositorys 108 • Verwalten von Repository-Eigenschaften 110 • Verwalten von Repository-Schlüsseln 111

8.5 Der GNOME Package Updater 111

8.6 Aktualisieren von Paketen mit *GNOME-Software* 114

9 Verwalten von Software mit Befehlszeilenwerkzeugen 116

9.1 Verwenden von zypper 116

Allgemeine Verwendung 116 • Verwenden von Zypper-Unterbefehle 118 • Installieren und Entfernen von Software mit zypper 118 • Aktualisieren von Software mit Zypper 124 • Ermitteln von Prozessen und Diensten, die gelöschte Dateien verwenden 130 • Verwalten von Repositorys mit Zypper 132 • Abfragen von Repositorys und Paketen mit Zypper 134 • Anzeigen von Paketinformationen 136 • Konfigurieren von Zypper 137 • Fehlersuche 137 • Zypper-Rollback-Funktion im Btrfs-Dateisystem 137 • Weitere Informationen 138

9.2 RPM – der Paket-Manager 138

Prüfen der Authentizität eines Pakets 139 • Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren 139 • Delta-RPM-Pakete 141 • RPM-Abfragen 141 • Installieren und Kompilieren von Quellpaketen 144 • Kompilieren von RPM-Pakten mit „build“ 146 • Werkzeuge für RPM-Archive und die RPM-Datenbank 147

10 Systemwiederherstellung und Snapshot-Verwaltung mit Snapper 148

10.1 Standardeinrichtung 149

Standardeinstellungen 150 • Typen von Snapshots 150 • Verzeichnisse, die aus Snapshots ausgenommen sind 151 • Anpassen der Einrichtung 152

10.2 Rückgängigmachen von Änderungen mit Snapper 156
Rückgängigmachen von Änderungen durch YaST oder Zypper 157 • Wiederherstellen von Dateien mit Snapper 162

10.3 System-Rollback durch Booten aus Snapshots 164
Snapshots nach dem Rollback 167 • Abrufen und Erkennen von Snapshot-Booteinträgen 168 • Nutzungsbeschränkungen 170

10.4 Aktivieren von Snapper in Benutzer-Startverzeichnissen 171
Installieren von pam_snapper und Erstellen von Benutzern 172 • Entfernen von Benutzern 172 • Manuelles Aktivieren von Snapshots in Startverzeichnissen 173

10.5 Erstellen und Bearbeiten von Snapper-Konfigurationen 173
Verwalten vorhandener Konfigurationen 175

10.6 Manuelles Erstellen und Verwalten von Snapshots 178
Snapshot-Metadaten 179 • Erstellen von Snapshots 181 • Bearbeiten von Snapshot-Metadaten 182 • Löschen von Snapshots 183

10.7 Automatisches Bereinigen von Snapshots 184
Bereinigen von nummerierten Snapshots 185 • Bereinigen von Zeitleisten-Snapshots 187 • Bereinigen von Snapshot-Paaren, die sich nicht unterscheiden 188 • Bereinigen manuell erstellter Snapshots 189 • Hinzufügen von Festplattenquotenunterstützung 189

10.8 Anzeigen von exklusiv für Snapshots verwendetem Festplattenspeicherplatz 191

10.9 Häufig gestellte Fragen 193

11 Live-Kernel-Patching mit KLP 194

11.1 Vorteile des Kernel Live Patching 194

11.2 Überblick über Kernel Live Patching 194
Umfang des Kernel Live Patching 196 • Einschränkungen des Kernel Live Patching 196

11.3 Aktivieren von Kernel Live Patching mit YaST 197

11.4 Aktivieren von Kernel Live Patching über die Befehlszeile 197

11.5 Durchführen von Kernel Live Patching 198
Prüfen des Ablaufdatums des Live-Patches 199

11.6 Fehlerbehebung bei Kernel Live Patching-Problemen 199
Manuelles Patch-Downgrade 199

12 Userspace-Live-Patching 201

12.1 Info zu Userspace-Live-Patching 201
Voraussetzungen 201 • Unterstützte Bibliotheken 202 • Verwenden von `libpulp` 202

12.2 Weitere Informationen 205

13 Transaktionsaktualisierungen 206

13.1 Nutzungsbeschränkungen 207

13.2 Aktivieren von `transactional-update` 209

13.3 Verwalten von automatischen Aktualisierungen 209

13.4 Das Kommando **`transactional-update`** 209

13.5 Fehlersuche 212

14 Remote-Grafiksitzungen mit VNC 213

14.1 Der **`vncviewer`**-Client 213
Verbinden mithilfe der vncviewer-CLI 213 • Verbinden mithilfe der vncviewer-GUI 214 • Benachrichtigungen zu unverschlüsselten Verbindungen 214

14.2 Remmina: Remote-Desktop-Client 215
Installation 215 • Hauptfenster 215 • Hinzufügen von Remote-Sitzungen 215 • Starten von Remote-Sitzungen 217 • Bearbeiten, Kopieren und Löschen gespeicherter Sitzungen 218 • Ausführen von Remote-Sitzungen über die Kommandozeile 219

14.3 Konfigurieren von einmaligen Sitzungen am VNC-Server 219
Verfügbare Konfigurationen 221 • Initiieren einer einmaligen VNC-Sitzung 222 • Konfigurieren einmaliger VNC-Sitzungen 222

14.4 Konfigurieren von permanenten VNC-Serversitzungen 223
Mit vncmanager initiierte VNC-Sitzung 224
14.5 Konfigurieren der Verschlüsselung am VNC-Server 227
14.6 Kompatibilität mit Wayland 228
15 Kopieren von Dateien mit RSync 230
15.1 Konzeptübersicht 230
15.2 Einfache Syntax 231
15.3 Lokales Kopieren von Dateien und Verzeichnissen 231
15.4 Remote-Kopieren von Dateien und Verzeichnissen 232
15.5 Konfigurieren und Verwenden eines Rsync-Servers 233
15.6 Weitere Informationen 236
II BOOTEN EINES LINUX-SYSTEMS 237
16 Einführung in den Bootvorgang 238
16.1 Terminologie 238
16.2 Der Linux-Bootvorgang 239
Initialisierungs- und Bootloader-Phase 239 • Die Kernel-Phase 241 • Die Phase init auf initramfs 244 • Die systemd-Phase 247
17 UEFI (Unified Extensible Firmware Interface) 248
17.1 Secure Boot 248
Implementierung in SUSE Linux Enterprise Desktop 249 • MOK (Machine Owner Key) 252 • Booten eines benutzerdefinierten Kernels 253 • Verwenden von Nicht-Inbox-Treibern 255 • Funktionen und Einschränkungen 256
17.2 Weitere Informationen 257
18 Der Bootloader GRUB 2 258
18.1 Hauptunterschiede zwischen GRUB Legacy und GRUB 2 258

18.2 Konfigurationsdateistruktur 259
Die Datei /boot/grub2/grub.cfg 260 • Die Datei /etc/default/grub 260 • Skripte in /etc/grub.d 264 • Zuordnung von BIOS-Laufwerken und Linux-Geräten 266 • Ändern von Menüeinträgen während des Bootvorgangs 266 • Festlegen eines Bootpassworts 268 • Autorisierter Zugriff auf Bootmenüeinträge 269

18.3 Konfigurieren des Bootloaders mit YaST 270
Speicherort des Bootloaders und Boot-Code-Optionen 271 • Anpassen der Festplattenreihenfolge 273 • Konfigurieren der erweiterten Optionen 273

18.4 Nützliche Befehle in GRUB 2 277

18.5 Rescue-Modus 278

18.6 Weitere Informationen 279

19 Der Daemon systemd 280

19.1 Das Konzept von systemd 280
Unit-Datei 281

19.2 Grundlegende Verwendung 282
Verwalten von Diensten auf einem laufenden System 283 • Dienste dauerhaft aktivieren/deaktivieren 285

19.3 Systemstart und Zielverwaltung 286
Ziele im Vergleich zu Runlevels 286 • Fehlersuche beim Systemstart 290 • System V-Kompatibilität 293

19.4 Verwalten von Diensten mit YaST 294

19.5 Anpassen systemd 295
Wo werden Unit-Dateien gespeichert? 295 • Überschreiben mit Drop-In-Dateien 296 • Manuelles Erstellen von Drop-in-Dateien 297 • Konvertieren von xinetd-Diensten in systemd 299 • Erstellen von benutzerdefinierten Zielen 300

19.6 Erweiterte Nutzung 301
Bereinigen von temporären Verzeichnissen 301 • Systemprotokoll 302 • Aufnahmen 302 • Laden

der Kernelmodule 303 • Ausführen von Aktionen vor dem Laden eines Dienstes 303 • Kernel-Steuergruppen (cgroups) 304 • Beenden von Diensten (Senden von Signalen) 305 • Wichtige Hinweise zum D-Bus-Dienst 306 • Fehlersuche für Dienste 306

19.7 `systemd`-Zeitgeber-Units 308

`systemd`-Zeitgebertypen 308 • `systemd`-Timer und Dienst-Units 308 • Beispiel aus der Praxis 309 • Verwalten von `systemd`-Zeitgebern 311

19.8 Weitere Informationen 311

III SYSTEM 312

20 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung 313

20.1 Laufzeitunterstützung 313

20.2 Kernel-Spezifikationen 314

21 **`journalctl`**: Abfragen des `systemd`-Journals 315

21.1 Festlegen des Journals als permanent 315

21.2 **`journalctl`**: Nützliche Schalter 316

21.3 Filtern der Journalausgabe 317

Filtern nach Bootnummer 317 • Filtern nach Zeitraum 317 • Filtern nach Feldern 318

21.4 Untersuchen von `systemd`-Fehlern 319

21.5 Konfiguration von journald 320

Ändern der Größenbeschränkung für das Journal 320 • Weiterleiten des Journals an `/dev/ttyX` 321 • Weiterleiten des Journals an die Syslog-Funktion 321

21.6 Filtern des `systemd`-Journals mit YaST 322

21.7 Abrufen von Protokollen in GNOME 322

22 **update-alternatives**: Verwalten mehrerer Befehls- und Dateiversionen 323

22.1 Übersicht 323

22.2 Einsatzbereiche 325

22.3 Überblick über Alternativen 325

22.4 Anzeigen von Details zu spezifischen Alternativen 326

22.5 Festlegen der Standardversion von Alternativen 326

22.6 Installieren von benutzerdefinierten Alternativen 327

22.7 Definieren von abhängigen Alternativen 329

23 Grundlegendes zu Netzwerken 332

23.1 IP-Adressen und Routing 335

IP-Adressen 336 • Netzmasken und Routing 336

23.2 IPv6 – das Internet der nächsten Generation 338

Vorteile 339 • Adresstypen und -struktur 341 • Koexistenz von IPv4 und IPv6 345 • IPv6 konfigurieren 346 • Weitere Informationen 347

23.3 Namensauflösung 348

23.4 Konfigurieren von Netzwerkverbindungen mit YaST 349

Konfigurieren der Netzwerkkarte mit YaST 349

23.5 NetworkManager 362

NetworkManager und **wicked** 363 • NetworkManager-Funktionalität und Konfigurationsdateien 364 • Steuern und Sperren von NetworkManager-Funktionen 364

23.6 Manuelle Netzwerkkonfiguration 364

Die **wicked**-Netzwerkkonfiguration 365 • Konfigurationsdateien 372 • Testen Sie die Konfiguration. 385 • Unit-Dateien und Startskripte 389

23.7 Einrichten von Bonding-Geräten 390
Hot-Plugging der Bond-Ports 393 • Vorhersehbares Benennungsschema 394

23.8 Einrichten von Team-Geräten für Netzwerk-Teaming 396
Anwendungsfall: Lastausgleich bei Netzwerk-Teaming 400 • Anwendungsfall: Failover bei Netzwerk-Teaming 401 • Anwendungsfall: VLAN zusätzlich zu Teamgerät 402

24 Druckerbetrieb 405

24.1 Der CUPS-Workflow 406

24.2 Methoden und Protokolle zum Anschließen von Druckern 407

24.3 Installation der Software 407

24.4 Netzwerkdrucker 408

24.5 Konfigurieren von CUPS mit Befehlszeilenwerkzeugen 409

24.6 Drucken über die Befehlszeile 411

24.7 Besondere Funktionen in SUSE Linux Enterprise Desktop 411
CUPS und Firewall 411 • Durchsuchen nach Netzwerkdruckern 412 • PPD-Dateien in mehreren Paketen 413

24.8 Fehlersuche 413
Drucker ohne Unterstützung für eine Standard-Druckersprache 414 • Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar 415 • Netzwerkdrucker-Verbindungen 415 • Fehlerhafte Ausdrucke ohne Fehlermeldung 418 • Deaktivierte Warteschlangen 418 • CUPS-Browsing: Löschen von Druckaufträgen 418 • Fehlerhafte Druckaufträge und Fehler bei der Datenübertragung 419 • Fehlersuche für CUPS 419 • Weitere Informationen 420

25 Über die grafische Benutzeroberfläche 421

25.1 X Window System 421

25.2 Installation und Konfiguration von Schriften 422
Anzeigen der installierten Schriften 423 • Anzeigen von Schriften 424 • Abfragen von Schriften 424 • Installieren von Schriften 425 • Konfigurieren der Darstellung von Schriften 425

25.3 GNOME-Konfiguration für Administratoren 434
Das `dconf`-System 434 • Systemweite Konfiguration 435 • Verwalten von Kachelfenstern auf Wayland 436 • Weitere Informationen 438

25.4 Umschalten zwischen Intel- und NVIDIA Optimus-GPUs mit SUSE Prime 439
Voraussetzungen 439 • Installieren und Verwenden von SUSE Prime 440 • Installieren von NVIDIA-Treibern 440

26 Zugriff auf Dateisysteme mit FUSE 442

26.1 Konfigurieren von FUSE 442

26.2 Einhängen einer NTFS-Partition 442

26.3 Weitere Informationen 443

27 Installieren von mehreren Kernel-Versionen 444

27.1 Aktivieren und Konfigurieren der Multiversions-Unterstützung 445
Automatisches Löschen nicht verwendeter Kernel 445 • Anwendungsfall: Löschen eines alten Kernels erst nach dem Neustart 447 • Anwendungsfall: Beibehalten alter Kernels als Fallback 447 • Anwendungsfall: Beibehalten einer bestimmten Kernel-Version 448

27.2 Installieren/Entfernen von mehreren Kernel-Versionen mit YaST 448

27.3 Installieren/Entfernen von mehreren Kernel-Versionen mit Zypper 449

28 Verwalten von Kernelmodulen 452

28.1 Auflisten der geladenen Module mit lsmod und modinfo 452

28.2 Einfügen und Entfernen von Kernelmodulen 453
Automatisches Laden von Kernelmodulen beim Booten 453 • Eintragen von Kernelmodulen in Sperrlisten mit modprobe 454

29 Gerätemanagement über dynamischen Kernel mithilfe von udev 456

29.1 Das /dev-Verzeichnis 456

29.2 uevents und udev des Kernels 456

29.3 Treiber, Kernel-Module und Geräte 457

29.4 Booten und erstes Einrichten des Geräts 458

29.5 Überwachen des aktiven udev-Daemons 458

29.6 Einflussnahme auf die Behandlung von Geräteereignissen durch den Kernel und udev-Regeln 459

Verwenden von Operatoren in udev-Regeln 462 • Verwenden von Ersetzungen in udev-Regeln 463 • Verwenden von udev-Übereinstimmungsschlüsseln 464 • Verwenden von udev-Zuweisungsschlüsseln 465

29.7 Dauerhafte Benennung von Geräten 467

29.8 Von udev verwendete Dateien 468

29.9 Weitere Informationen 469

30 Spezielle Systemfunktionen 470

30.1 Informationen zu speziellen Softwarepaketen 470

Das Paket bash und /etc/profile 470 • Das cron-Paket 471 • Stoppen der Cron-Statusmeldungen 472 • Protokolldateien: Paket logrotate 472 • Das Kommando **locate** 473 • Das Kommando **ulimit** 473 • Das Kommando **free** 474 • Manpages und Info-Seiten 475 • Auswählen von man-Seiten über den Befehl **man** 475 • Einstellungen für GNU Emacs 475

30.2 Virtuelle Konsolen 476

30.3 Tastaturbelegung 477

30.4 Sprach- und länderspezifische Einstellungen 477
Systemweite Locale-Einstellungen 478 • Einige Beispiele 479 • Locale-Einstellungen in ~/.i18n 481 • Einstellungen für die Sprachunterstützung 481 • Weitere Informationen 482

31 Verwendung von NetworkManager 483

31.1 Anwendungsfälle für den NetworkManager 483

31.2 Aktivieren oder Deaktivieren von NetworkManager 484

31.3 Konfigurieren von Netzwerkverbindungen 485
Verwalten von kabelgebundenen Netzwerkverbindungen 486 • Verwalten von drahtlosen Netzwerkverbindungen 487 • Aktivieren der Captive Portal-Erkennung beim Wireless-Betrieb 488 • Konfigurieren der WLAN-/Bluetooth-Karte als Zugriffspunkt 488 • NetworkManager und VPN 489

31.4 NetworkManager und Sicherheit 490
Benutzer- und Systemverbindungen 491 • Speichern von Passwörtern und Berechtigungsnachweisen 491 • Firewall-Zonen 492

31.5 Häufig gestellte Fragen 492

31.6 Fehlersuche 494

31.7 Weitere Informationen 495

IV HARDWAREKONFIGURATION 496

32 Einrichten der Systemtastaturbelegung 497

33 Einrichten von Soundkarten 498

34 Einrichten eines Druckers 502

34.1 Konfigurieren von Druckern 502
Hinzufügen von Treibern mit YaST 504 • Anpassen einer lokalen Druckerkonfiguration 505

34.2 Konfigurieren des Netzwerkdrucks in YaST 506
Verwenden von CUPS 506 • Verwenden von Nicht-CUPS-Druckservern 507

34.3 Freigeben von Druckern im Netzwerk 507

35 Einrichten eines Scanners 509

35.1 Konfigurieren eines HP All-In-One-Geräts 509

35.2 Gemeinsame Nutzung eines Scanners über das Netzwerk 510

35.3 Scannen über das Netzwerk 510

36 Energieverwaltung 511

36.1 Energiesparfunktionen 511

36.2 Advanced Configuration & Power Interface (ACPI) 512
Steuern der CPU-Leistung 513 • Fehlersuche 513

36.3 Ruhezustand für Festplatte 515

36.4 Fehlersuche 517
CPU-Frequenzsteuerung funktioniert nicht 517

37 Permanenter Speicher 518

37.1 Einführung 518

37.2 Begriffe 520

37.3 Einsatzbereiche 523
PMEM mit DAX 523 • PMEM mit BTT 523

37.4 Tools zur Verwaltung eines permanenten Speichers 524

37.5 Einrichten eines permanenten Speichers 525
Anzeigen des verfügbaren NVDIMM-Speichers 525 • Konfigurieren des Speichers als einzelnen PMEM-Namespace mit DAX 527 • Erstellen eines PMEM-Namespace mit BTT 529 • Platzieren des Dateisystemjournals auf PMEM/BTT 530

37.6 Weitere Informationen 531

V SERVICES 532

38 Serviceverwaltung mit YaST 533

39 Zeitsynchronisierung mit NTP 535

39.1 Konfigurieren eines NTP-Clients mit YaST 536
Start des NTP-Daemons 536 • Typ der Konfigurationsquelle 537 • Konfigurieren von Zeitservern 537

39.2 Manuelle Konfiguration von NTP im Netzwerk 539

39.3 Konfigurieren von NTS 540

39.4 Konfigurieren von `chronyd` zur Laufzeit mit **`chronyc`** 543

39.5 Dynamische Zeitsynchronisierung während der Laufzeit 544

39.6 Einrichten einer lokalen Referenzuhr 544

39.7 Uhrensynchronisierung mit einer externen Zeitreferenz (ETR) 545

VI FEHLERSUCHE 547

40 Hilfe und Dokumentation 548

40.1 Dokumentationsverzeichnis 548
Versionshinweise 549 • Dokumentation zu den einzelnen Paketen 549

40.2 Man Pages 550

40.3 Infoseiten 551

40.4 Online-Ressourcen 552

41 Erfassen der Systeminformationen für den Support 553

41.1 Anzeigen aktueller Systeminformationen 553

41.2 Erfassen von Systeminformationen mit supportconfig 554
Erstellen einer Serviceanforderungsnummer 554 • Upload-Ziele 555 • Erstellen eines supportconfig-Archivs mit YaST 555 • Erstellen eines supportconfig-Archivs über die Befehlszeile 558 • Informationen

zur Ausgabe von **supportconfig** 559 • Allgemeine Optionen für Supportconfig 560 • Überblick über den Archivinhalt 561

41.3 Übertragen von Informationen an den globalen technischen Support 564

41.4 Analysieren von Systeminformationen 566
SCA-Befehlszeilenwerkzeug 567 • SCA-Appliance 569 • Entwickeln von benutzerdefinierten Analyseschemata 582

41.5 Sammeln von Informationen bei der Installation 582

41.6 Unterstützung für Kernelmodule 583
Technischer Hintergrund 584 • Arbeiten mit nicht unterstützten Modulen 584

41.7 Weitere Informationen 585

42 Häufige Probleme und deren Lösung 586

42.1 Suchen und Sammeln von Informationen 586

42.2 Probleme beim Booten 589
GRUB 2-Bootloader wird nicht geladen 589 • Es wird keine Anmeldemaske oder Eingabeaufforderung angezeigt 590 • Keine grafische Anmeldung 591 • Einhängen der Root-Btrfs-Partition nicht möglich 591 • Erzwingen der Prüfung von root-Partitionen 592 • Auslagerungsgerät zum Booten deaktivieren 592 • Fehler bei GRUB 2 beim Neustarten auf einem Dual-Boot-System 592

42.3 Probleme bei der Anmeldung 592
Fehler trotz gültiger Kombination aus Benutzername und Passwort 592 • Keine Annahme einer gültigen Kombination aus Benutzername und Passwort 594 • Anmeldung bei verschlüsselter Home-Partition fehlgeschlagen 596 • Probleme mit dem GNOME-Desktop 597

42.4 Probleme mit dem Netzwerk 598
Probleme mit NetworkManager 603

42.5 Probleme mit Daten 603
Verwalten von Partitions-Images 603 • Verwenden des Rettungssystems 604

A Ein Beispielnetzwerk 613

B GNU licenses 614

Vorwort

1 Verfügbare Dokumentation

Online-Dokumentation

Unsere Dokumentation ist online verfügbar unter https://documentation.suse.com. Durchsuchen Sie die Dokumentation oder laden Sie sie in verschiedenen Formaten herunter.

Anmerkung: Neueste Aktualisierungen

Die neuesten Aktualisierungen sind normalerweise in der englischen Version dieser Dokumentation verfügbar.

SUSE Knowledgebase

Wenn Sie auf ein Problem stoßen, lesen Sie die technischen Informationsdokumente (TIDs), online verfügbar unter https://www.suse.com/support/kb/. Durchsuchen Sie die SUSE Knowledgebase nach bekannten Lösungen, die sich an den Bedürfnissen der Kunden orientieren.

Versionshinweise

Die Versionshinweise finden Sie unter https://www.suse.com/releasenotes/.

In Ihrem System

Für die Offline-Nutzung sind die Versionshinweise auch unter `/usr/share/doc/release-notes` auf Ihrem System verfügbar. Die Dokumentation zu den einzelnen Paketen finden Sie unter `/usr/share/doc/packages`.

Viele Befehle sind auch auf den *Handbuchseiten* beschrieben. Führen Sie zu deren Anzeige **`man`** gefolgt von einem bestimmten Befehlsnamen aus. Sollte der **`man`**-Befehl nicht auf Ihrem System installiert sein, müssen Sie es mit **`sudo zypper install man`** installieren.

2 Verbessern der Dokumentation

Feedback und Beiträge Ihrerseits zu dieser Dokumentation sind willkommen. Für Feedback stehen die folgenden Kanäle zur Verfügung:

Serviceanforderungen und Support

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

Zum Öffnen einer Service-Anforderung benötigen Sie ein SUSE-Abonnement, das beim SUSE Customer Center registriert ist. Gehen Sie zu https://scc.suse.com/support/requests, melden Sie sich an und klicken Sie auf *Neu erstellen*.

Fehlerberichte

Melden Sie Probleme mit der Dokumentation unter https://bugzilla.suse.com/.

Klicken Sie zur Vereinfachung dieses Vorgangs neben einer Überschrift in der HTML-Version dieses Dokuments auf das Symbol für *Report an issue* (Problem melden). Dadurch wird das richtige Produkt und die Kategorie in Bugzilla vorab ausgewählt und ein Link zum aktuellen Abschnitt hinzugefügt. Sie können somit sofort mit der Eingabe Ihres Berichts beginnen.

Ein Bugzilla-Konto ist erforderlich.

Beiträge

Wenn Sie zu dieser Dokumentation beitragen möchten, klicken Sie neben einer Überschrift in der HTML-Version dieses Dokuments auf das Symbol *Edit source document* (Quelldokument bearbeiten). So gelangen Sie zum Quellcode auf GitHub, wo Sie eine Pull-Anforderung öffnen können.

Ein GitHub-Konto ist erforderlich.

Anmerkung: *Edit source document* (Quelldokument bearbeiten) nur in englischer Version verfügbar

Die Symbole für *Edit source document* (Quelldokument bearbeiten) sind nur in der englischen Version der Dokumentation verfügbar. Für alle anderen Sprachen können Sie stattdessen die Symbole für *Report an issue* (Problem melden) verwenden.

Weitere Informationen zur Dokumentationsumgebung für diese Dokumentation finden Sie in der README des Repositorys.

E-Mail

Sie können auch E-Mails mit Fehlerberichten und Feedback zur Dokumentation an `doc-team@suse.com` senden. Geben Sie den Titel des Dokuments, die Produktversion und das Datum der Veröffentlichung des Dokuments an. Stellen Sie außerdem die entsprechende Abschnittsnummer und den Titel bereit (oder geben Sie die URL an), und fügen Sie eine kurze Beschreibung des Problems hinzu.

3 Konventionen in der Dokumentation

Im vorliegenden Dokument werden die folgenden Hinweise und typografischen Konventionen verwendet:

- `/etc/passwd`: Verzeichnis- und Dateinamen
- *`PLACEHOLDER`*: Ersetzen Sie *`PLACEHOLDER`* durch den tatsächlichen Wert
- `PATH`: Eine Umgebungsvariable
- **`ls`**, `--help`: Befehle, Optionen und Parameter
- `user`: Der Name eines Benutzers oder einer Gruppe
- `package_name`: Der Name eines Softwarepakets
- `Alt` , `Alt` – `F1` : Eine zu drückende Taste bzw. Tastenkombination. Tasten werden wie auf einer Tastatur in Großbuchstaben dargestellt.
- *Datei*, *Datei* › *Speichern unter*: Menüelemente, Schaltflächen
- *Chapter 1, „Example chapter“*: Ein Querverweis auf ein anderes Kapitel in diesem Handbuch.
- Befehle, die mit `root`-Privilegien ausgeführt werden müssen. Sie können diesen Befehlen auch den Befehl **`sudo`** voranstellen, um sie als nicht privilegierter Benutzer auszuführen:

```
# command
> sudo command
```

- Befehle, die von nicht privilegierten Benutzern ausgeführt werden können:

```
> command
```

- Befehle können durch ein Backslash-Zeichen (\) am Ende einer Zeile in zwei oder mehrere Zeilen aufgeteilt werden. Mit dem Backslash wird die Shell darüber informiert, dass der Befehlsaufruf nach dem Ende der Zeile fortgesetzt wird:

```
> echo a b \
c d
```

- Ein Codeblock, der sowohl den Befehl (mit vorangestellter Eingabeaufforderung) als auch die entsprechende von der Shell zurückgegebene Ausgabe anzeigt:

```
> command
output
```

- 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.

- Kompaktinfos

Ergänzende Informationen, beispielsweise zu unterschiedlichen Softwareversionen.

Hilfreiche Informationen, etwa als Richtlinie oder praktische Empfehlung.

4 Support

Nachfolgend finden Sie die Supportbestimmung für SUSE Linux Enterprise Desktop und allgemeine Informationen zu Technologievorschauen. Details über den Produktlebenszyklus finden Sie in https://www.suse.com/lifecycle.

Wenn Sie Anspruch auf Support haben, finden Sie Details zum Sammeln von Informationen für ein Support-Ticket unter https://documentation.suse.com/sles-15/html/SLES-all/cha-adm-support.html.

4.1 Erläuterung zum Support für SUSE Linux Enterprise Desktop

Sie benötigen ein entsprechendes Abonnement bei SUSE, um Support zu erhalten. Gehen Sie zur Anzeige der für Sie verfügbaren spezifischen Support-Angebote zu https://www.suse.com/support/ und wählen Sie das betreffende Produkt aus.

Die Support-Level sind folgendermaßen definiert:

L1

Problemermittlung: Technischer Support mit Informationen zur Kompatibilität, Nutzungs-Support, kontinuierliche Wartung, Informationssammlung und einfache Problembehandlung anhand der verfügbaren Dokumentation.

L2

Problemisolierung: Technischer Support zur Datenanalyse, Reproduktion von Kundenproblemen, Isolierung eines Problembereichs und Lösung für Probleme, die in Stufe 1 nicht gelöst wurden, sowie Vorbereitung für Stufe 3.

L3

Problembehebung: Technischer Support zur Lösung von Problemen durch technische Maßnahmen zur Behebung von Produktfehlern, die durch den Support der Stufe 2 erkannt wurden.

Vertragskunden und Partner erhalten SUSE Linux Enterprise Desktop mit L3-Support für alle Pakete, ausgenommen:

- Technologievorschauen
- Audio, Grafik, Schriftarten und Artwork
- Pakete, für die ein zusätzlicher Kundenvertrag erforderlich ist
- Pakete mit der Namensendung `-devel` (die Header-Dateien und ähnliche Entwicklerressourcen enthalten) werden nur zusammen mit den entsprechenden Hauptpaketen unterstützt.

SUSE unterstützt nur die Nutzung von Originalpaketen, also unveränderte und nicht kompilierte Pakete.

4.2 Technologievorschauen

Mit Technologievorschauen sind Pakete, Stacks oder Funktionen gemeint, die SUSE bereitstellt, um einen kurzen Einblick in bevorstehende Innovationen zu geben. Durch Technologievorschauen haben Sie die Möglichkeit, neue Technologien in Ihrer Umgebung zu testen. Über Ihr Feedback würden wir uns sehr freuen. Wenn Sie eine Technologievorschau testen, kontaktieren Sie bitte Ihre Ansprechpartner bei SUSE und teilen Sie ihnen Ihre Erfahrungen und Anwendungsfälle mit. Ihr Input ist für zukünftige Entwicklungen sehr hilfreich.

Technologievorschauen weisen die folgenden Einschränkungen auf:

- Technologievorschauen befinden sich noch in Entwicklung. Daher sind die Funktionen möglicherweise unvollständig, instabil oder aus anderen Gründen *nicht* für die Produktionsnutzung geeignet.
- Technologievorschauen werden *nicht* unterstützt.
- Technologievorschauen sind möglicherweise nur für bestimmte Hardwarearchitekturen verfügbar.

- Details und Funktionen von Technologievorschauen sind Änderungen unterworfen. Upgrades auf Folgeversionen sind demnach nicht möglich und erfordern eine Neuinstallation.
- SUSE kann feststellen, dass eine Vorschau nicht den Kunden- oder Marktanforderungen entspricht oder nicht mit den Unternehmensstandards übereinstimmt. Technologievorschauen können jederzeit aus einem Produkt entfernt werden. SUSE ist nicht verpflichtet, eine unterstützte Version dieser Technologie in der Zukunft bereitzustellen.

Eine Übersicht der Technologievorschauen, die im Lieferumfang Ihres Produkts enthalten sind, finden Sie in den Versionshinweisen unter https://www.suse.com/releasenotes.

I Häufige Tasks

1 Bash-Shell und Bash-Skripte 2

2 **sudo** Grundlagen 19

3 Verwenden von YaST 31

4 YaST im Textmodus 33

5 Ändern der Sprach- und Ländereinstellungen mit YaST 63

6 Verwalten von Benutzern mit YaST 70

7 YaST-Online-Aktualisierung 88

8 Installieren bzw. Entfernen von Software 96

9 Verwalten von Software mit Befehlszeilenwerkzeugen 116

10 Systemwiederherstellung und Snapshot-Verwaltung mit Snapper 148

11 Live-Kernel-Patching mit KLP 194

12 Userspace-Live-Patching 201

13 Transaktionsaktualisierungen 206

14 Remote-Grafiksitzungen mit VNC 213

15 Kopieren von Dateien mit RSync 230

1 Bash-Shell und Bash-Skripte

Heutzutage werden zunehmend Computer mit einer grafischen Bedienoberfläche (GUI) wie GNOME verwendet. GUIs bieten zwar viele Funktionen, kommen jedoch an ihre Grenzen, wenn automatische Aufgaben ausgeführt werden sollen. Shells sind eine gute Ergänzung für GUIs. In diesem Kapitel erhalten Sie einen Überblick über verschiedene Aspekte von Shells, in diesem Fall Bash-Shells.

1.1 Was ist „die Shell“?

Traditionell handelt es sich bei *der* Linux-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.

1.1.1 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 bei einem entfernten Computer mit SSH.

2. **Interaktive Nicht-Login-Shell.** Dies ist normalerweise beim Starten von xterm, konsole, gnome-terminal oder ähnlichen Befehlszeilenschnittstellen-Tools (CLI-Tools) der Fall.

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

Jede Shell liest andere Konfigurationsdateien. Die folgenden Tabellen zeigen die Login- und Nicht-Login-Shell-Konfigurationsdateien.

Tipp

Bash sucht die Konfigurationsdateien in einer bestimmten Reihenfolge, abhängig von der Art der Shell, in der sie ausgeführt wird. Weitere Informationen zu Bash finden Sie auf der man-Seite (**`man 1 bash`**). Suchen Sie nach der Überschrift `INVOCATION`.

TABELLE 1.1: BASH-KONFIGURATIONSDATEIEN FÜR LOGIN-SHELLS

Datei	Beschreibung
`/etc/profile`	Bearbeiten Sie diese Datei nicht, andernfalls werden Ihre Änderungen beim nächsten Update möglicherweise zerstört.
`/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 werden Ihre Änderungen beim nächsten Update möglicherweise zerstört.
`/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.

Zusätzlich verwendet die Bash-Shell einige weitere Dateien:

TABELLE 1.3: BESONDERE DATEIEN FÜR DIE BASH-SHELL

Datei	Beschreibung
`~/.bash_history`	Enthält eine Liste aller Befehle, die Sie eingegeben haben.
`~/.bash_logout`	Wird beim Abmelden ausgeführt.
`~/.alias`	Benutzerdefinierte Aliasse für häufig verwendete Befehle. Weitere Details zum Definieren von Aliassen finden Sie unter **`man 1 alias`**.

Shells zur Verhinderung der Anmeldung

Bestimmte Shells verhindern die Anmeldung von Benutzern im System: `/bin/false` und `/sbin/nologin`. Beide geben bei Anmeldeversuchen von Benutzern im System automatisch einen Fehler aus. Diese Methode war als Sicherheitsmaßnahme für Systembenutzer gedacht. Moderne Linux-Betriebssysteme kontrollieren den Systemzugriff jedoch inzwischen mit effektiveren Tools wie PAM und AppArmor.

Die Standardeinstellung von SUSE Linux Enterprise Desktop ist die Zuweisung von `/bin/bash` zu menschlichen Benutzern und `/bin/false` oder `/sbin/nologin` zu Systembenutzern. Dem Benutzer `nobody` ist aus historischen Gründen `/bin/bash` zugewiesen. Es handelt sich dabei um einen Benutzer mit minimalen Rechten, der standardmäßig als Systembenutzer verwendet wurde. Jegliche Sicherheit, die durch den Benutzer `nobody` erreicht wird, geht jedoch verloren, wenn er von mehreren Systembenutzern verwendet wird. Es sollte möglich sein, ihn in `/sbin/nologin` zu ändern. Am schnellsten lässt sich dies testen, wenn Sie die Änderung vornehmen und sehen, ob dadurch Dienste oder Anwendungen beschädigt werden.

Mit folgendem Befehl wird unter `/etc/passwd` aufgelistet, welche Shells allen Benutzern, Systembenutzern und menschlichen Benutzern zugewiesen sind. Die Ausgabe unterscheidet sich je nach Services und Benutzer in Ihrem System:

```
> sort -t: -k 7 /etc/passwd | awk -F: '{print $1"\t" $7}' | column -t
tux               /bin/bash
nobody            /bin/bash
root              /bin/bash
avahi             /bin/false
```

```
chrony            /bin/false
dhcpd             /bin/false
dnsmasq           /bin/false
ftpsecure         /bin/false
lightdm           /bin/false
mysql             /bin/false
postfix           /bin/false
rtkit             /bin/false
sshd              /bin/false
tftp              /bin/false
unbound           /bin/false
bin               /sbin/nologin
daemon            /sbin/nologin
ftp               /sbin/nologin
lp                /sbin/nologin
mail              /sbin/nologin
man               /sbin/nologin
nscd              /sbin/nologin
polkitd           /sbin/nologin
pulse             /sbin/nologin
qemu              /sbin/nologin
radvd             /sbin/nologin
rpc               /sbin/nologin
statd             /sbin/nologin
svn               /sbin/nologin
systemd-coredump  /sbin/nologin
systemd-network   /sbin/nologin
systemd-timesync  /sbin/nologin
usbmux            /sbin/nologin
vnc               /sbin/nologin
wwwrun            /sbin/nologin
messagebus        /usr/bin/false
scard             /usr/sbin/nologin
```

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.

Verzeichnis	Inhalt
`/bin`	Grundlegende binäre Dateien, z. B. Befehle, die der Systemadministrator und normale Benutzer brauchen. Enthält gewöhnlich auch die Shells, z. B. Bash.
`/boot`	Statische Dateien des Bootloaders.
`/dev`	Erforderliche Dateien für den Zugriff auf Host-spezifische Geräte.
`/etc`	Host-spezifische Systemkonfigurationsdateien.
`/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.
`/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.
`/windows`	Nur verfügbar, wenn sowohl Microsoft Windows* als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten.

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

`/bin`

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

`/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/`*`USERNAME`*

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 wie `.gconf/` und `.config`.

Anmerkung: Home-Verzeichnis in einer Netzwerkumgebung

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

`/lib`

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

`/media`

Enthält Einhängepunkte für Wechselmedien, z. B. CD-ROMs, 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 temporär 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-System-ressourcen. 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 wie `/usr/bin`, `/usr/sbin`, `/usr/local` und `/usr/share/doc`.

`/usr/bin`

Enthält Programme, die für den allgemeinen Zugriff verfügbar sind.

`/usr/sbin`

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

`/usr/local`

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

`/usr/share/doc`

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

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

Wenn HOWTOs (Verfahrensbeschreibungen) auf Ihrem System installiert sind, enthält `/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 auch unter *Tabelle 42.1, „Protokolldateien“* zur Verfügung.

`/windows`

Nur verfügbar, wenn sowohl Microsoft Windows als auch Linux auf Ihrem System installiert ist. Enthält die Windows-Daten, die auf der Windows-Partition Ihres Systems verfügbar sind. Ob Sie die Daten in diesem Verzeichnis bearbeiten können, hängt vom Dateisystem ab, das Ihre Windows-Partition verwendet. Falls es sich um FAT32 handelt, können Sie die Dateien in diesem Verzeichnis öffnen und bearbeiten. Für NTFS unterstützt SUSE Linux Enterprise Desktop auch den Schreibzugriff. Die Funktionalität des Treibers für das NTFS-3g-Dateisystem ist jedoch eingeschränkt.

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 den *Shebang*-Zeichen (`#!`), die angeben, dass diese Datei ein Skript ist. Der Interpreter, der nach dem *Shebang* angegeben wird, führt das Skript aus. In diesem Fall ist **`/bin/sh`** der angegebene Interpreter.

❷ Die zweite Zeile ist ein Kommentar, der mit dem Hash-Zeichen beginnt. Wir empfehlen Ihnen, schwierige Zeilen zu kommentieren. Richtiges Kommentieren erinnert Sie an den Zweck und die Funktion der Zeile. Auch andere Leser können dadurch Ihr Skript besser verstehen. Das Kommentieren wird in der Entwickler-Community als gute Vorgehensweise angesehen.

❸ Die dritte Zeile verwendet den integrierten Befehl **`echo`**, um den entsprechenden Text zu drucken.

Vor Ausführung dieses Skripts sind einige Voraussetzungen zu erfüllen:

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. Ein normaler Benutzer verfügt nicht über Schreibzugriff auf `/usr/bin`. Daher sollten Sie Ihre Skripte 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 Befehl 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 Befehlsereignissen

Jedes Kommando kann drei Kanäle für Eingabe oder Ausgabe verwenden:

- **Standardausgabe.** Dies ist der Standardausgabe-Kanal. Immer wenn ein Befehl eine Ausgabe erzeugt, verwendet es den Standardausgabe-Kanal.

- **Standardeingabe.** Wenn ein Kommando Eingaben von Benutzern oder anderen Kommandos benötigt, verwendet es diesen Kanal.

- **Standardfehler.** Befehle verwenden diesen Kanal zum Melden von Fehlern.

Zum Umlenken dieser Kanäle bestehen folgende Möglichkeiten:

`Command > File`
: Speichert die Ausgabe des Befehls in eine Datei; die bestehende Datei wird gelöscht. Beispielsweise schreibt der Befehl **`ls`** seine Ausgabe in die Datei `listing.txt`:

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

`Command >> File`
: Hängt die Ausgabe des Befehls an eine Datei an. Beispielsweise hängt der Befehl **`ls`** seine Ausgabe an die Datei `listing.txt` an:

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

`Command < File`
: Liest die Datei als Eingabe für den angegebenen Befehl. Beispielsweise liest der Befehl **`read`** den Inhalt der Datei in die Variable ein:

```
> read a < foo
```

`Command1 | Command2`
: Leitet die Ausgabe des linken Befehls als Eingabe für den rechten Befehl um. Beispiel: Der Befehl **`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, Fehlermeldungen werden jedoch 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 Befehle. 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 **unalias** 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 den Befehl **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 Variablen verwenden Sie **unset**:

```
> unset NAME
```

Die folgende Tabelle enthält gängige 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
`PATH`	Suchpfad der Shell, eine Liste von Verzeichnissen, die durch Doppelpunkte getrennt sind
`PS1`	Gibt die normale Eingabeaufforderung an, die vor jedem Befehl angezeigt wird
`PS2`	Gibt die sekundäre Eingabeaufforderung an, die beim Ausführen eines mehrzeiligen Befehls 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#pattern}`
: entfernt die kürzeste mögliche Übereinstimmung von links:

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

`${VAR##pattern}`
: entfernt die längste mögliche Übereinstimmung von links:

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

`${VAR%pattern}`
: entfernt die kürzeste mögliche Übereinstimmung von rechts:

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

`${VAR%%pattern}`
: 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 Befehlen

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

Die folgende Liste zeigt, wie sich Befehle gruppieren lassen:

`Command1 ; Command2`
: führt die Befehle 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
```

`Command1 && Command2`
: führt den rechten Befehl aus, wenn der linke Befehl erfolgreich war (logisches UND). Die folgende Zeile zeigt den Inahlt der Datei an und gibt deren Dateieigenschaften nur aus, wenn der vorherige Befehl erfolgreich war (vgl. mit dem vorherigen Eintrag in dieser Liste):

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

`Command1 || Command2`
: führt den rechten Befehl aus, wenn der linke Befehl 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

Um den Fluss Ihres Skripts zu steuern, verfügt eine Shell über die Konstrukte **`while`**, **`if`**, **`for`** und **`case`**.

1.7.1 Der Steuerungsbefehl „if“

Der Befehl **`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 https://bash.cyberciti.biz/guide/If..else..fi.

1.7.2 Erstellen von Schleifen mit dem Befehl **`for`**

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

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

1.8 Weitere 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:

- https://tldp.org/LDP/Bash-Beginners-Guide/html/index.html – Bash-Anleitung für Anfänger
- https://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html – BASH-Programmierung – Einführende schrittweise Anleitung
- https://tldp.org/LDP/abs/html/index.html – Anleitung für erweiterte Bash-Skripts
- https://www.grymoire.com/Unix/Sh.html – Sh - the Bourne Shell (Sh – die Bourne-Shell)

2 **sudo** Grundlagen

Für bestimmte Befehle sind root-Berechtigungen erforderlich. Die Anmeldung als `root` ist aus Sicherheitsgründen und zur Vermeidung von Fehlern jedoch nicht zu empfehlen. Es ist sicherer, sich als normaler Benutzer anzumelden und dann mit **`sudo`** Befehle mit höheren Rechten auszuführen.

Auf SUSE Linux Enterprise Desktop ist **`sudo`** standardmäßig auf eine ähnliche Funktionsweise wie **`su`** konfiguriert. **`sudo`** ist jedoch eine flexible Methode, mit der Benutzer Befehle mit den Rechten eines beliebigen anderen Benutzers ausführen können. 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 Befehls mit den Berechtigungen des Benutzers `wilber` zu erlauben. Der Zugriff auf den Befehl wird weiter eingeschränkt, wenn Befehlsoptionen nicht zugelassen werden. Während „su“ immer das `root`-Passwort für die Authentifizierung mit PAM erfordert, kann **`sudo`** für die Authentifizierung mit Ihren eigenen Berechtigungsnachweisen konfiguriert werden. Benutzer müssen folglich ihr `root`-Passwort nicht bekanntgeben, was die Sicherheit erhöht.

2.1 Grundlegende Verwendung von **sudo**

Im folgenden Kapitel wird die grundlegende Verwendung von **`sudo`** vorgestellt.

2.1.1 Ausführung eines einzelnen Befehls

Als normaler Benutzer können Sie alle Befehle als `root` ausführen, indem Sie **`sudo`** vor den Befehl setzen. Dadurch werden Sie aufgefordert, das root-Passwort anzugeben. Bei erfolgreicher Authentifizierung wird daraufhin der Befehl als `root` ausgeführt:

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

1. Der Befehl **`id -un`** druckt den Anmeldenamen des aktuellen Benutzers.
2. Das Passwort wird bei der Eingabe weder als Klartext noch durch maskierende Zeichen angezeigt.
3. Nur Kommandos, die mit **`sudo`** beginnen, werden mit höheren Rechten ausgeführt.
4. Die erhöhten Rechte bleiben für bestimmte Zeit erhalten, sodass Sie das `root`-Passwort nicht erneut eingeben müssen.

Tipp: E/A-Umleitung

Die E/A-Umleitung funktioniert nicht mit **`sudo`**:

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

Im oben genannten Beispiel werden nur die Befehle **`echo`** und **`cat`** mit erhöhten Rechten ausgeführt. Die Umleitung wird von der Shell des Benutzers mit Benutzerrechten ausgeführt. Für eine Umleitung mit erhöhten Rechten müssen Sie eine Shell starten wie in *Abschnitt 2.1.2, „Starten einer Shell“* beschrieben oder das **`dd`**-Dienstprogramm verwenden:

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

2.1.2 Starten einer Shell

Es ist nicht immer praktisch, **`sudo`** jedes mal zur Ausführung eines Kommandos mit erhöhten Rechten zu verwenden. Sie können zwar den Befehl **`sudo bash`** verwenden, doch zum Starten einer Shell empfiehlt sich die Verwendung einer der integrierten Methoden:

`sudo -s (<command>)`

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

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

```
tux:~ >
```

`sudo -i (<command>)`

Ähnlich wie `-s`, doch die Shell wird als Login-Shell gestartet. Dies bedeutet, dass die Startdateien (`.profile` etc.) der Shell verarbeitet werden und das aktuelle Arbeitsverzeichnis auf das Home-Verzeichnis des Zielbenutzers festgelegt wird.

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

Tipp: Umgebungsvariablen

Standardmäßig gibt **`sudo`** keine Umgebungsvariablen weiter. Dieses Verhalten kann mit der Option `env_reset` geändert werden (weitere Informationen finden Sie unter *Hilfreiche Flags und Optionen*).

2.2 Konfigurieren von **sudo**

`sudo` umfasst eine breite Palette an konfigurierbaren Optionen.

Anmerkung: Versehentliches Aussperren aus sudo

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

Warnung: Beispielkonfigurationen dienen ausschließlich zur Veranschaulichung

Die unten dargelegten Beispielregeln dienen ausschließlich zur Veranschaulichung. Hiermit soll die allgemeine Syntax der **`sudo`**-Konfigurationsdateien erläutert werden. Verwenden Sie diese Regeln nicht im realen Einsatz, da sie der Komplexität dieser Umgebungen nicht gerecht werden.

2.2.1 Bewährte Verfahren für die **sudo**-Konfiguration

Machen Sie sich zunächst mit einigen grundlegenden Regeln für die Verwaltung von **sudo**-Konfigurationen vertraut:

Immer `visudo` für die Bearbeitung von `sudo`-Konfigurationsdateien verwenden

Alle Änderungen an der **sudo**-Konfiguration sollten mit dem Kommando **visudo** vorgenommen werden. **visudo** ist ein maßgeschneidertes Tool, mit dem Sie die **sudo**-Konfigurationsdateien bearbeiten und grundlegende Syntaxprüfungen durchführen können, um sicherzustellen, dass die Konfiguration intakt und funktionsfähig bleibt. Eine fehlerhafte **sudo**-Konfiguration kann dazu führen, dass ein Benutzer aus dem eigenen System ausgesperrt wird.

Immer benutzerdefinierte Konfigurationen unter `/etc/sudoers.d/` erstellen

Benutzerdefinierte Konfigurationen müssen unter `/etc/sudoers.d/` abgelegt werden, damit sie von **sudo** abgerufen werden können. Die Einstellungen in den benutzerdefinierten Konfigurationen haben Vorrang vor den Einstellungen in der Standardkonfiguration unter `/etc/sudoers`.

Immer die Reihenfolge beachten, in der die Konfigurationen ausgelesen werden

Damit die benutzerdefinierten Konfigurationen in der richtigen Reihenfolge ausgelesen werden, stellen Sie ihnen eine Zahl voran. Verwenden Sie bei Bedarf auch führende Nullen. So wird `01_myfirstconfig` beispielsweise vor `10_myotherconfig` analysiert. Wenn eine Direktive in einer Datei festgelegt wurde, die vor einer anderen Datei mit dazu widersprüchlichen Informationen gelesen wird, wird die zuletzt gelesene Direktive angewendet.

Immer beschreibende Dateinamen verwenden

Legen Sie Dateinamen fest, aus denen Sie schließen können, was die Konfigurationsdatei bewirkt. So können Sie leichter nachverfolgen, was das **sudo**-Setup bezwecken soll.

2.2.2 Erstellen einer benutzerspezifischen Konfigurationsdatei

Erstellen Sie eine **sudo**-Konfigurationsdatei, mit der ein normaler Benutzer (`tux`) das Kommando **useradd** mit seinem eigenen Passwort statt mit dem `root`-Passwort ausführen kann.

BEISPIEL 2.1: ERSTELLEN EINER BENUTZERSPEZIFISCHEN KONFIGURATIONSDATEI

1. Erstellen Sie als Systemadministrator (`root`) eine benutzerdefinierte Konfigurationsdatei, in die die neuen benutzerspezifischen Direktiven aufgenommen werden sollen. Starten Sie hierzu **`visudo`**. Verwenden Sie sowohl eine Nummerierung als auch einen beschreibenden Namen:

```
# visudo -f /etc/sudoers.d/02_usermanagement
```

2. Erstellen Sie eine Regel, mit der `tux` die Binärdatei **`/usr/sbin/useradd`** in der gesamten Umgebung ausführen kann, für die diese **`sudo`**-Konfiguration gilt:

```
tux❶ ALL❷ = /usr/sbin/useradd❸
```

❶ Legen Sie den Benutzer oder die Gruppe fest. Listen Sie Benutzer nach Namen oder `#UID` und Gruppen nach `%GROUPNAME` auf. Mehrere Elemente müssen durch Kommas voneinander getrennt werden. Sollen Einträge negiert werden, verwenden Sie `!`.

❷ Geben Sie einen oder mehrere (durch Komma getrennte) Hosts an. Verwenden Sie (vollqualifizierte) Hostnamen oder IP-Adressen. Mit `ALL` wird diese Einstellung global auf allen Hosts erzwungen. Eine Negierung geben Sie mit `!` an.

❸ Geben Sie eine oder mehrere (durch Komma getrennte) ausführbare Dateien an. Beachten Sie dabei die folgenden Regeln:

`/usr/sbin/useradd`
: Werden keine zusätzlichen Optionen angegeben, kann jedes mögliche **`useradd`**-Kommando ausgeführt werden.

`/usr/sbin/useradd -c`
: Wenn Sie explizit eine Option angeben, ist ausschließlich diese Option zulässig. Andere Optionen stehen dem oben angegebenen Benutzer dann nicht zur Verfügung.

`/usr/sbin/useradd ""`
: Damit kann der Benutzer lediglich **`useradd`** ohne jegliche Optionen aufrufen.

Im Beispiel oben möchten Sie entweder alle Optionen und Unterbefehle zulassen oder sie aus Sicherheitsgründen auf einige wenige beschränken, aber einem Benutzer zu verbieten, überhaupt eine Option anzugeben, wäre in diesem Kontext sinnlos.

3. Damit der Benutzer sein eigenes Passwort anstelle des `root`-Passworts verwenden kann, fügen Sie die folgende Zeile hinzu:

```
Defaults:tux !targetpw
```

   Wenn dieses Flag aktiv ist, muss der Benutzer das Passwort des Zielbenutzers eingeben, das `root` lautet. Dieses Flag ist standardmäßig auf allen SUSE Linux Enterprise Desktop-Systemen aktiviert. Negieren Sie es mit `!`, um den Benutzer aufzufordern, statt des `root`-Passworts nur sein eigenes Passwort einzugeben.

4. Speichern Sie die Konfiguration, verlassen Sie den Editor und öffnen Sie eine zweite Shell, um zu testen, ob Ihre neue Konfiguration von **`sudo`** beachtet wird.

2.2.3 Erstellen von benutzerdefinierten Konfigurationen durch Gruppieren von Elementen

Bearbeiten Sie die Konfiguration aus *Beispiel 2.1, „Erstellen einer benutzerspezifischen Konfigurationsdatei“*, damit eine Gruppe benannter Benutzer das Kommando **`useradd`** ausführen kann, ohne das `root`-Passwort eingeben zu müssen. Fügen Sie außerdem das **`usermod`** und **`userdel`** zur Liste der Kommandos hinzu, die dieser Gruppe zur Verfügung stehen.

BEISPIEL 2.2: ERSTELLEN VON BENUTZERDEFINIERTEN KONFIGURATIONEN DURCH GRUPPIEREN VON ELEMENTEN

1. Zum Bearbeiten der Beispielkonfiguration öffnen Sie sie als Systemadministrator mit **`visudo`**:

```
# visudo /etc/sudoers.d/02_usermanagement
```

2. Fügen Sie der Regel zusätzliche Benutzer in einer durch Kommas getrennten Liste hinzu:

```
tux, wilber ALL = /usr/sbin/useradd
```

3. Damit die angegebenen Benutzer eine Liste von Kommandos ausführen können, geben Sie die Kommandos als durch Kommas getrennte Liste an:

```
tux, wilber ALL = /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/userdel
```

4. Damit die aufgeführten Benutzer ihr eigenes Passwort anstelle des `root`-Passworts verwenden können, fügen Sie die folgende Zeile hinzu:

```
Defaults:tux, wilber !targetpw
```

Wenn dieses Flag aktiv ist, müssen die aufgelisteten Benutzer das Passwort des Zielbenutzers eingeben, das `root` lautet. Dieses Flag ist standardmäßig auf allen SUSE Linux Enterprise Desktop-Systemen aktiviert. Negieren Sie es mit `!`, um die aufgeführten Benutzer aufzufordern, statt des `root`-Passworts nur das eigene Passwort einzugeben.

5. Speichern Sie die Konfiguration, verlassen Sie den Editor und öffnen Sie eine zweite Shell, um zu testen, ob Ihre neue Konfiguration von **`sudo`** beachtet wird.

2.2.4 Vereinfachen der Konfigurationen mithilfe von Aliasen

Mithilfe von Aliasen können Sie die benutzerdefinierte Konfiguration aus *Beispiel 2.2, „Erstellen von benutzerdefinierten Konfigurationen durch Gruppieren von Elementen“* noch weiter vereinfachen. Die Gruppierung von Elementen ist bis zu einem gewissen Grad hilfreich, aber die Verwendung globaler Aliasnamen für Benutzer, Kommandos und Hosts ist der effizienteste Weg, um eine übersichtliche und schlanke **`sudo`**-Konfiguration zu erhalten.

Es ist viel besser, Aliasnamen und Gruppen anstelle von Listen zu verwenden, um Änderungen in Ihrer Einrichtung zu berücksichtigen. Sollte ein Benutzer ausscheiden, entfernen Sie ihn einfach aus der globalen `User_Alias`-Deklaration in Ihrer Alias-Deklarationsdatei, anstatt alle separaten benutzerdefinierten Konfigurationsdateien zu durchsuchen. Das gleiche Verfahren gilt für alle anderen Arten von Aliasnamen (`Host_Alias`, `Cmnd_Alias` und `Runas_Alias`).

BEISPIEL 2.3: VEREINFACHEN DER KONFIGURATIONEN MITHILFE VON ALIASEN

1. Erstellen Sie eine neue Datei, die Ihre globalen Alias-Definitionen enthält:

```
# visudo /etc/sudoers.d/01_aliases
```

2. Fügen Sie die folgende Zeile hinzu, um den `TEAMLEADERS`-Alias zu erstellen:

```
User_Alias    TEAMLEADERS = tux, wilber
```

3. Fügen Sie die folgende Zeile hinzu, um den `USERMANAGEMENT`-Alias zu erstellen:

```
Cmnd_Alias    USERMANAGEMENT = /usr/sbin/useradd, /usr/sbin/usermod, /usr/sbin/
userdel
```

4. Speichern Sie Ihre Änderungen und beenden Sie **`visudo`**.

5. Starten Sie **`visudo`** als Systemadministrator und bearbeiten Sie die Beispielkonfigurationsdatei:

```
# visudo -f /etc/sudoers.d/02_usermanagement
```

6. Löschen Sie die vorherige Regel und ersetzen Sie sie durch die folgende Regel mit den oben definierten Aliasnamen:

```
TEAMLEADERS ALL = USERMANAGEMENT
```

7. Damit alle durch `User_Alias` definierten Benutzer ihr eigenes Passwort anstelle des `root`-Passworts verwenden können, fügen Sie die folgende Zeile hinzu:

```
Defaults:TEAMLEADERS !targetpw
```

8. Speichern Sie die Konfiguration, verlassen Sie den Editor und öffnen Sie eine zweite Shell, um zu testen, ob Ihre neue Konfiguration von **`sudo`** beachtet wird.

2.2.5 Basiskonfigurationssyntax von sudoers

Die sudoers-Konfigurationsdateien enthalten zwei Optionstypen: Zeichenketten und Flags. Zeichenketten 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 # is 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.

❷ Entfernen Sie das Zeichen `!`, um das gewünschte Flag zu aktivieren (ON).

❸ Weitere Informationen hierzu finden Sie in *Abschnitt 2.2.6, „Grundlegende sudoers-Regeln“*.

HILFREICHE FLAGS UND OPTIONEN

`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`

Bei diesem Flag fordert **`sudo`** zur Eingabe des `root`-Passworts auf. Die Standardeinstellung ist “OFF”.

```
Defaults !rootpw # Turn rootpw flag OFF
```

`env_reset`

Bei dieser Einstellung erstellt **`sudo`** eine Mindestumgebung mit `TERM`, `PATH`, `HOME`, `MAIL`, `SHELL`, `LOGNAME`, `USER`, `USERNAME` und `SUDO_*`. Zusätzlich werden Variablen, die in `env_keep` aufgelistet sind, aus der aufrufenden Umgebung importiert. 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 Befehlen verwendet werden. Außerdem ist es möglich, eine Option anzuwenden, die nur für eine bestimmte Reihe von Benutzern gültig ist.

Genauere Informationen zur sudoers-Konfigurationsdatei erhalten Sie mit **`man 5 sudoers`**.

2.2.6 Grundlegende sudoers-Regeln

Jede Regel befolgt folgendes Schema (`[]` markiert optionale Teile):

```
#Who      Where         As whom      Tag              What
```

```
User_List Host_List = [(User_List)] [NOPASSWD:|PASSWD:] Cmnd_List
```

SUDOERS-REGELSYNTAX

`User_List`

Eine oder mehrere (durch Komma getrennte) Kennungen: entweder einen Benutzernamen, eine Gruppe im Format `%GROUPNAME` oder eine Benutzer-ID im Format `#UID`. Eine Negierung wird mit dem Präfix `!` angegeben.

`Host_List`

Eine oder mehrere (durch Komma getrennte) Kennungen: Entweder ein (vollständig qualifizierter) Hostname oder eine IP-Adresse. Eine Negierung wird mit dem Präfix `!` angegeben. `ALL` ist eine häufige Wahl für `Host_List`.

`NOPASSWD:|PASSWD:`

Der Benutzer wird nicht aufgefordert, ein Passwort einzugeben, wenn Kommandos ausgeführt werden, die `Cmd_List` nach `NOPASSWD:` : entsprechen.
`PASSWD` ist die Standardeinstellung. Es muss nur angegeben werden, wenn sich sowohl `PASSWD` als auch `NOPASSWD` in derselben Zeile befinden:

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

`Cmnd_List`

Einen oder mehrere (durch Komma getrennte) Bezeichner: ein Pfad zu einer ausführbaren Datei, gefolgt von einem optionalen zulässigen Argument.

```
/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 Befehle 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: Unsichere Regeln

Verwenden Sie *keine* Regeln wie `ALL ALL = ALL` ohne `Defaults targetpw`. Andernfalls kann jeder Benutzer Befehle als `root` ausführen.

Wichtig: „winbind“ und „sudo“

Wenn Sie den Gruppennamen in der Datei `sudoers` angeben, verwenden Sie den NetBIOS-Domänennamen statt des Bereichs, beispielsweise:

```
%DOMAIN\\GROUP_NAME ALL = (ALL) ALL
```

Denken Sie bei winbindd daran, dass das Format auch von der Option `winbind separator` in der Datei `smb.conf` abhängt. Die Standardeinstellung ist `\`. Wird sie beispielsweise in `+` geändert, muss das Kontoformat in der Datei `sudoers` entsprechend `DOMAIN+GROUP_NAME` lauten.

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

Werden grafische Anwendungen mit **`sudo`** gestartet, führt dies normalerweise zu folgendem Fehler:

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

Eine einfache Behelfslösung ist xhost. Damit wird dem root-Benutzer vorübergehend der Zugriff auf die X-Sitzung des lokalen Benutzers gestattet. Dies erfolgt mit folgendem Befehl:

```
xhost si:localuser:root
```

Folgender Befehl entfernt den gewährten Zugriff:

```
xhost -si:localuser:root
```

Warnung: Potenzielles Sicherheitsproblem

Die Ausführung grafischer Anwendungen mit root-Rechten beeinträchtigt die Sicherheit. Es wird empfohlen, den root-Zugriff für eine grafische Anwendung nur in Ausnahmefällen zu aktivieren. Außerdem sollte der gewährte root-Zugriff sofort nach Schließen der grafischen Anwendung entzogen werden.

2.4 Weitere Informationen

Der Befehl **`sudo --help`** bietet einen kurzen Überblick über die verfügbaren Befehlszeilenoptionen und der Befehl **`man sudoers`** bietet detaillierte Informationen zu `sudoers` und dessen Konfiguration.

3 Verwenden von YaST

YaST ist ein SUSE Linux Enterprise Desktop-Tool mit einer grafischen Oberfläche für alle wesentlichen Installations- und Systemkonfigurationsaufgaben. Ob Sie Pakete aktualisieren, einen Drucker konfigurieren, Firewall-Einstellungen bearbeiten, einen FTP-Server einrichten oder eine Festplatte partitionieren müssen – mit YaST ist dies alles möglich. YaST ist in Ruby geschrieben und weist eine erweiterbare Architektur auf, die es ermöglicht, neue Funktionen über Module hinzuzufügen.

Weitere Informationen zu YaST sind auf der offiziellen Website des Projekts verfügbar unter https://yast.opensuse.org/.

3.1 YaST-Oberfläche im Überblick

YaST verfügt über zwei grafische Oberflächen. Die eine wird für grafische Desktop-Umgebungen wie KDE und GNOME verwendet. Die andere ist eine ncurses-basierte pseudo-grafische Oberfläche für Systeme ohne X-Server (weitere Informationen hierzu finden Sie in *Kapitel 4, YaST im Textmodus*).

In der grafischen Version von YaST sind alle Module in YaST nach Kategorie gruppiert. Über die Navigationsleiste erhalten Sie schnell Zugriff auf die Module in der gewünschten Kategorie. Im Suchfeld am oberen Rand lassen sich Module nach Namen suchen. Geben Sie zur Suche nach einem bestimmten Modul dessen Namen im Suchfeld ein. Danach sollten Sie beim Tippen die Module sehen, die der eingegebenen Zeichenfolge entsprechen.

Wichtig: Liste der installierten YaST-Module

Die Liste der installierten Module für die ncurses-basierte Version und die GUI-Version von YaST kann abweichen. Bevor Sie ein YaST-Modul starten, stellen Sie sicher, dass es für die von Ihnen verwendete YaST-Version installiert ist.

3.2 Nützliche Tastenkombinationen

Die grafische Version von YaST unterstützt Tastenkombinationen.

`Bildschirminhalt drucken`

Erstellt und speichert ein Bildschirmfoto. In bestimmten Desktop-Umgebungen funktioniert diese Kombination womöglich nicht.

`Umschalttaste` – `F4`

Aktiviert und deaktiviert die Farbpalette für Benutzer mit Sehbehinderungen.

`Umschalttaste` – `F7`

Aktiviert/Deaktiviert die Protokollierung von Fehlermeldungen (Debugging).

`Umschalttaste` – `F8`

Öffnet einen Dateidialog, über den Sie die Protokolldateien in einem benutzerdefinierten 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 und stoppt den Makro-Rekorder.

`Strg` – `Umschalttaste` – `Alt` – `P`

Gibt ein Makro wieder.

`Strg` – `Umschalttaste` – `Alt` – `S`

Zeigt den Formatvorlagen-Editor an.

`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.

4 YaST im Textmodus

Die ncurses-basierte pseudo-grafische YaST-Oberfläche sollte vor allem Systemadministratoren bei der Verwaltung von Systemen ohne X-Server unterstützen. Die Oberfläche bietet einige Vorteile im Vergleich zu herkömmlichen grafischen Benutzeroberflächen. Die Navigation auf der ncurses-Oberfläche erfolgt über die Tastatur. Für praktisch alle Oberflächenelemente stehen Tastenkombinationen zur Verfügung. Die ncurses-Oberfläche benötigt nur wenige Ressourcen und wird selbst auf langsamer Hardware schnell ausgeführt. Die ncurses-basierte Version von YaST lässt sich über eine SSH-Verbindung ausführen, damit Sie Remote-Systeme verwalten können. Denken Sie daran, dass die minimale unterstützte Größe des Terminal-Emulators, in dem Sie YaST ausführen, 80 x 25 Zeichen beträgt.

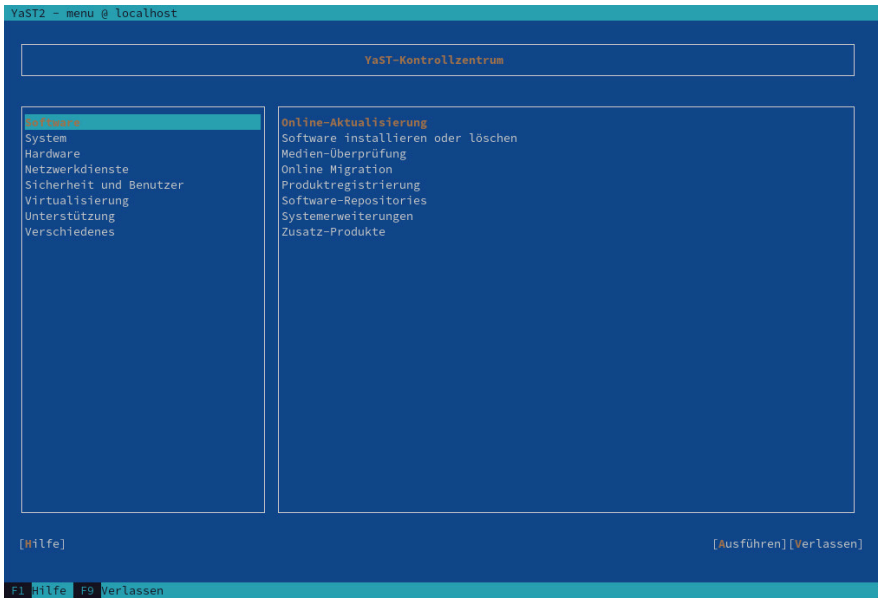


ABBILDUNG 4.1: HAUPTFENSTER VON YAST IM TEXTMODUS

Öffnen Sie zum Starten der ncurses-basierten Version von YaST das Terminal und führen Sie den Befehl **sudo yast2** aus. Navigieren Sie anhand der →| - oder Pfeiltasten durch die Oberflächenelemente wie Menüelemente, Felder und Schaltflächen. Auf alle Menüelemente und Schaltflächen in YaST wird über die entsprechenden Funktionstasten oder Tastenkombinationen zugegriffen. Beispielsweise brechen Sie den aktuellen Vorgang durch Drücken der F9 -Taste ab. Mit der F10 -Taste übernehmen Sie Änderungen. Bei jedem Menüelement und jeder Schaltfläche auf der ncurses-basierten Oberfläche von YaST ist in der Bezeichnung ein Buchstabe hervorgehoben. Dieser Buchstabe ist Teil der Tastenkombination, die dem Oberflächenelement zugewiesen wurde. Beispielsweise ist der Buchstabe Q auf der Schaltfläche *Beenden* hervorgehoben. Das bedeutet, dass Sie die Schaltfläche durch Drücken von Alt – Alt+B aktivieren können.

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.

4.1 Navigation in Modulen

Bei der folgenden Beschreibung der Steuerelemente in den YaST-Modulen wird davon ausgegangen, dass alle Kombinationen aus Funktionstasten und Alt -Taste funktionieren und nicht anderen globalen Funktionen zugewiesen sind. In *Abschnitt 4.3, „Einschränkung der Tastenkombinationen“* finden Sie Informationen zu möglichen Ausnahmen.

Wechseln zwischen Schaltflächen und Auswahllisten

Navigieren Sie zwischen den Schaltflächen und Einzelbildern mit den Auswahllisten mit →| . Mit der Tastenkombination Alt – →| oder Umschalttaste – →| navigieren Sie in der umgekehrten Richtung.

Navigieren in Auswahllisten

Mit den Pfeiltasten (↑ und ↓) können Sie sich zwischen den einzelnen Elementen in einem aktiven Rahmen, der eine Auswahlliste enthält, bewegen. Wenn einzelne Einträge länger sind als die Breite des Rahmens, verwenden Sie Umschalttaste – → oder Umschalttaste – ← für den horizontalen Bildlauf. Wenn über die Pfeiltaste die Auswahl zu einem anderen Rahmen übergeht, verwenden Sie stattdessen Strg – E oder Strg – A .

Arbeiten mit Schaltflächen, Optionsschaltflächen und Kontrollkästchen

Drücken Sie Leertaste oder Eingabetaste , um Schaltflächen mit leeren eckigen Klammern (Kontrollkästchen) oder leeren runden Klammern (Optionsschaltflächen) auszuwählen. 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 tatsächlich 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

Bestimmte 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

Verwenden Sie die Filter auf der linken Seite, um Pakete aufzulisten, die der angegebenen Zeichenkette entsprechen. 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*.

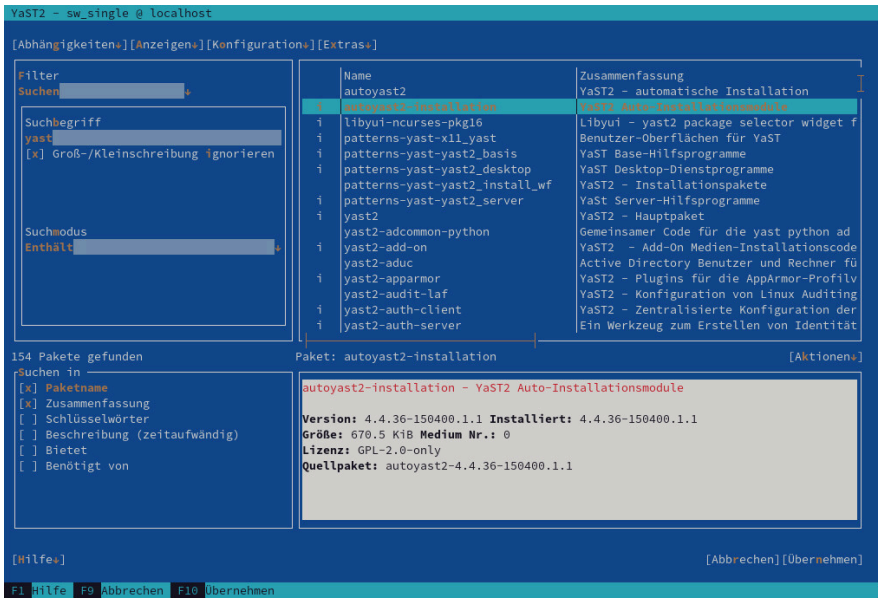


ABBILDUNG 4.2: DAS SOFTWARE-INSTALLATIONSMODUL

4.2 Erweiterte Tastenkombinationen

Die ncurses-basierte Version von YaST bietet einige erweiterte Tastenkombinationen.

Umschalttaste – F1

Zeigt eine Liste der erweiterten Tastenfunktionen.

Umschalttaste – F4

Ändert das Farbschema.

Strg – Q

Beendet die Anwendung.

Strg – L

Aktualisiert den Bildschirm.

Strg – D F1

Zeigt eine Liste der erweiterten Tastenfunktionen.

Strg – D Umschalttaste – D

Speichert das Dialogfeld als Bildschirmfoto in der Protokolldatei.

Strg – D Umschalttaste – Y

Öffnet YDialogSpy mit der Widget-Hierarchie.

4.3 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.

Verwenden von `Alt` statt `Esc`

Tastenkombinationen mit `Alt` können auch mit `Esc` anstelle von `Alt` ausgeführt werden. `Esc` – `H` beispielsweise ersetzt `Alt` – `H` . (Drücken Sie `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` (forward = vor) und `Strg` – `B` (backward = zurück).

Einschränkung der Funktionstasten

Die Funktionstasten (`F1` ... `F12`) werden auch für Funktionen verwendet. Bestimmte Funktionstasten können vom Terminal übernommen werden und stehen eventuell für YaST nicht zur Verfügung. Auf einer reinen Textkonsole sollten die Tastenkombinationen mit `Alt` und die Funktionstasten jedoch stets vollständig zur Verfügung stehen.

4.4 YaST-Befehlszeilenoptionen

Neben der Schnittstelle im Textmodus bietet YaST auch eine Befehlszeilenschnittstelle. Rufen Sie eine Liste der YaST-Befehlszeilenoptionen mit folgendem Befehl ab:

```
> sudo yast -h
```

4.4.1 Installieren von Paketen über die Befehlszeile

Wenn Sie den Namen des Pakets kennen und das Paket von einem aktiven Installations-Repository bereitgestellt wird, können Sie das Paket mithilfe der Befehlszeilenoption `-i` installieren:

```
> sudo yast -i package_name
```

oder

```
> sudo yast --install -i 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.

YaST bietet grundlegende Funktionen zur Verwaltung von Software von der Befehlszeile aus. Für anspruchsvollere Paketverwaltungsaufgaben sollten Sie Zypper verwenden. Weitere Informationen zu Zypper finden Sie in *Abschnitt 9.1, „Verwenden von zypper“*

4.4.2 Arbeiten mit einzelnen Modulen

Um Zeit zu sparen, können Sie einzelne YaST-Module mit folgendem Befehl starten:

```
> sudo yast module_name
```

Eine Liste aller auf Ihrem System verfügbaren Module können Sie mit **`yast -l`** oder **`yast --list`** anzeigen.

4.4.3 Befehlszeilenparameter der YaST-Module

Um die Verwendung von YaST-Funktionen in Skripts zu ermöglichen, bietet YaST Befehlszeilenunterstützung für einzelne Module. Die Befehlszeilenunterstützung steht jedoch nicht für alle Module zur Verfügung. Die verfügbaren Optionen eines Moduls zeigen Sie mit folgendem Befehl an:

```
> sudo yast module_name help
```

Wenn ein Modul keine Befehlszeilenunterstützung bietet, wird es im Textmodus gestartet und es wird folgende Meldung angezeigt:

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

In den nachfolgenden Abschnitten werden alle YaST-Module mit Befehlszeilenunterstützung beschrieben, und es werden alle zugehörigen Befehle und die verfügbaren Optionen kurz erläutert.

4.4.3.1 Häufige Befehle in YaST-Modulen

Alle YaST-Module unterstützen die folgenden Befehle:

help

Zeigt eine Liste der unterstützten Befehle des Moduls mit einer Beschreibung an:

```
> sudo yast lan help
```

longhelp

Wie **help**, zeigt jedoch zusätzlich eine detaillierte Liste der Optionen aller Befehle mit einer Beschreibung an:

```
> sudo yast lan longhelp
```

xmlhelp

Wie **longhelp**; die Ausgabe ist jedoch als XML-Dokument strukturiert und wird in eine Datei umgeleitet:

```
> sudo yast lan xmlhelp xmlfile=/tmp/yast_lan.xml
```

Interaktiv

Gibt den Modus *Interaktiv* ein. Damit führen Sie die Befehle des Moduls aus, ohne das Präfix **sudo yast** angeben zu müssen. Mit `exit` verlassen Sie den Interaktiv-Modus.

4.4.3.2 yast add-on

Fügt ein neues Add-on-Produkt aus dem angegebenen Pfad ein:

```
> sudo yast add-on http://server.name/directory/Lang-AddOn-CD1/
```

Sie können den Quellpfad mit den folgenden Protokollen angeben: http:// ftp:// nfs:// disk:// cd:// oder dvd://.

4.4.3.3 yast audit-laf

Öffnet und konfiguriert das Linux Audit Framework. Weitere Informationen finden Sie in *Buch „Security and Hardening Guide“*. **yast audit-laf** akzeptiert die folgenden Befehle:

set

Legt eine Option fest:

```
> sudo yast audit-laf set log_file=/tmp/audit.log
```

Mit **`yast audit-laf set help`** erhalten Sie eine vollständige Liste der Optionen.

show

Zeigt die Einstellungen für eine Option an:

```
> sudo yast audit-laf show diskspace
space_left: 75
space_left_action: SYSLOG
admin_space_left: 50
admin_space_left_action: SUSPEND
action_mail_acct: root
disk_full_action: SUSPEND
disk_error_action: SUSPEND
```

Mit **`yast audit-laf show help`** erhalten Sie eine vollständige Liste der Optionen.

4.4.3.4 yast dhcp-server

Verwaltet den DHCP-Server und konfiguriert dessen Einstellung. **`yast dhcp-server`** akzeptiert die folgenden Befehle:

Deaktivieren

Deaktiviert den DHCP-Serverdienst.

enable

Aktiviert den DHCP-Serverdienst.

Host

Konfiguriert Einstellungen für einzelne Hosts.

interface

Gibt an, welche Netzwerkschnittstelle überwacht werden soll:

```
> sudo yast dhcp-server interface current
Selected Interfaces: eth0
Other Interfaces: bond0, pbu, eth1
```

Mit **`yast dhcp-server interface help`** erhalten Sie eine vollständige Liste der Optionen.

Optionen

Verwaltet globale DHCP-Optionen. Mit **`yast dhcp-server options help`** erhalten Sie eine vollständige Liste der Optionen.

status

Gibt den Status des DHCP-Dienstes aus.

subnet

Verwaltet die DHCP-Subnetzoptionen. Mit **`yast dhcp-server subnet help`** erhalten Sie eine vollständige Liste der Optionen.

4.4.3.5 yast dns-server

Verwaltet die DNS-Serverkonfiguration. **`yast dns-server`** akzeptiert die folgenden Befehle:

acls

Zeigt die Einstellungen für die Zugriffssteuerungsliste an:

```
> sudo yast dns-server acls show
ACLs:
-----
 Name       Type        Value
 ---------------------------
 any        Predefined
 localips   Predefined
 localnets  Predefined
 none       Predefined
```

dnsrecord

Konfiguriert Zonenressourcen-Datensätze:

```
> sudo yast dnsrecord add zone=example.org query=office.example.org type=NS
 value=ns3
```

Mit **`yast dns-server dnsrecord help`** erhalten Sie eine vollständige Liste der Optionen.

forwarders

Konfiguriert DNS-Forwarder:

```
> sudo yast dns-server forwarders add ip=10.0.0.100
> sudo yast dns-server forwarders show
[...]
Forwarder IP
------------
10.0.0.100
```

Mit **`yast dns-server forwarders help`** erhalten Sie eine vollständige Liste der Optionen.

Host

Verarbeitet gleichzeitig „A“ und den zugehörigen „PTR“-Eintrag:

```
> sudo yast dns-server host show zone=example.org
```

Mit **yast dns-server host help** erhalten Sie eine vollständige Liste der Optionen.

logging

Konfiguriert die Protokollierungseinstellungen:

```
> sudo yast dns-server logging set updates=no transfers=yes
```

Mit **yast dns-server logging help** erhalten Sie eine vollständige Liste der Optionen.

mailserver

Konfiguriert die Zonen-Mailserver:

```
> sudo yast dns-server mailserver add zone=example.org mx=mx1 priority=100
```

Mit **yast dns-server mailserver help** erhalten Sie eine vollständige Liste der Optionen.

nameserver

Konfiguriert die Zonen-Nameserver:

```
> sudo yast dns-server nameserver add zone=example.com ns=ns1
```

Mit **yast dns-server nameserver help** erhalten Sie eine vollständige Liste der Optionen.

soa

Konfiguriert den SOA-Datensatz (Start of Authority):

```
> sudo yast dns-server soa set zone=example.org serial=2006081623 ttl=2D3H20S
```

Mit **yast dns-server soa help** erhalten Sie eine vollständige Liste der Optionen.

startup

Verwaltet den DNS-Serverdienst:

```
> sudo yast dns-server startup atboot
```

Mit **yast dns-server startup help** erhalten Sie eine vollständige Liste der Optionen.

transport

Konfiguriert die Regeln für den Zonentransport. Mit **yast dns-server transport help** erhalten Sie eine vollständige Liste der Optionen.

zones

Verwaltet die DNS-Zonen:

```
> sudo yast dns-server zones add name=example.org zonetype=master
```

Mit **`yast dns-server zones help`** erhalten Sie eine vollständige Liste der Optionen.

4.4.3.6 yast disk

Gibt Informationen zu allen Festplatten oder Partitionen aus. Hier wird ausschließlich der Befehle **`list`** mit einer der folgenden Optionen unterstützt:

disks

Zeigt eine Liste aller konfigurierten Festplatten im System an:

```
> sudo yast disk list disks
Device   | Size       | FS Type | Mount Point | Label | Model
---------+------------+---------+-------------+-------+-------------
/dev/sda | 119.24 GiB |         |             |       | SSD 840
/dev/sdb |  60.84 GiB |         |             |       | WD1003FBYX-0
```

Partitionen

Zeigt eine Liste aller Partitionen im System an:

```
> sudo yast disk list partitions
Device         | Size       | FS Type | Mount Point | Label | Model
---------------+------------+---------+-------------+-------+------
/dev/sda1      |   1.00 GiB | Ext2    | /boot       |       |
/dev/sdb1      |   1.00 GiB | Swap    | swap        |       |
/dev/sdc1      | 698.64 GiB | XFS     | /mnt/extra  |       |
/dev/vg00/home | 580.50 GiB | Ext3    | /home       |       |
/dev/vg00/root | 100.00 GiB | Ext3    | /           |       |
[...]
```

4.4.3.7 yast ftp-server

Konfiguriert die Einstellungen für den FTP-Server. **`yast ftp-server`** akzeptiert die folgenden Optionen:

SSL, TLS

Steuert sichere Verbindungen über SSL und TLS. SSL-Optionen gelten ausschließlich für `vsftpd`.

```
> sudo yast ftp-server SSL enable
> sudo yast ftp-server TLS disable
```

Zugriff

Konfiguriert die Zugriffsberechtigungen:

```
> sudo yast ftp-server access authen_only
```

Mit **`yast ftp-server access help`** erhalten Sie eine vollständige Liste der Optionen.

anon_access

Konfiguriert die Zugriffsberechtigungen für anonyme Benutzer:

```
> sudo yast ftp-server anon_access can_upload
```

Mit **`yast ftp-server anon_access help`** erhalten Sie eine vollständige Liste der Optionen.

anon_dir

Gibt das Verzeichnis für anonyme Benutzer an. Das Verzeichnis muss bereits auf dem Server vorhanden sein:

```
> sudo yast ftp-server anon_dir set_anon_dir=/srv/ftp
```

Mit **`yast ftp-server anon_dir help`** erhalten Sie eine vollständige Liste der Optionen.

chroot

Steuert die *change root*-Umgebung (chroot):

```
> sudo yast ftp-server chroot enable
> sudo yast ftp-server chroot disable
```

idle-time

Legt den maximal zulässigen Leerlaufzeitraum (in Minuten) fest, nach dem der FTP-Server die aktuelle Verbindung beendet:

```
> sudo yast ftp-server idle-time set_idle_time=15
```

logging

Gibt an, ob die Protokollmeldungen in einer Protokolldatei gespeichert werden sollen:

```
> sudo yast ftp-server logging enable
> sudo yast ftp-server logging disable
```

max_clients

Gibt die maximal zulässige Anzahl der gleichzeitig verbundenen Clients an:

```
> sudo yast ftp-server max_clients set_max_clients=1500
```

max_clients_ip

Gibt die maximal zulässige Anzahl der gleichzeitig über IP verbundenen Clients an:

```
> sudo yast ftp-server max_clients_ip set_max_clients=20
```

max_rate_anon

Gibt die maximal zulässige Datenübertragungsrate für anonyme Clients an (KB/s):

```
> sudo yast ftp-server max_rate_anon set_max_rate=10000
```

max_rate_authen

Gibt die maximal zulässige Datenübertragungsrate für lokal authentifizierte Benutzer an (KB/s):

```
> sudo yast ftp-server max_rate_authen set_max_rate=10000
```

port_range

Gibt den Portbereich für passive Verbindungsantworten an:

```
> sudo yast ftp-server port_range set_min_port=20000 set_max_port=30000
```

Mit **`yast ftp-server port_range help`** erhalten Sie eine vollständige Liste der Optionen.

show

Zeigt die Einstellungen für den FTP-Server an.

startup

Steuert die FTP-Startmethode:

```
> sudo yast ftp-server startup atboot
```

Mit **`yast ftp-server startup help`** erhalten Sie eine vollständige Liste der Optionen.

umask

Gibt die Datei-umask für `authenticated:anonymous`-Benutzer an:

```
> sudo yast ftp-server umask set_umask=177:077
```

welcome_message

Gibt den Text an, der angezeigt werden soll, wenn ein Benutzer eine Verbindung zum FTP-Server herstellt:

```
> sudo yast ftp-server welcome_message set_message="hello everybody"
```

4.4.3.8 yast http-server

Konfiguriert den HTTP-Server (Apache2). **`yast http-server`** akzeptiert die folgenden Befehle:

configure

Konfiguriert die Host-Einstellungen für den HTTP-Server:

```
> sudo yast http-server configure host=main servername=www.example.com \
 serveradmin=admin@example.com
```

Mit **`yast http-server configure help`** erhalten Sie eine vollständige Liste der Optionen.

hosts

Konfiguriert virtuelle Hosts:

```
> sudo yast http-server hosts create servername=www.example.com \
 serveradmin=admin@example.com documentroot=/var/www
```

Mit **`yast http-server hosts help`** erhalten Sie eine vollständige Liste der Optionen.

listen

Gibt die Ports und Netzwerkadressen an, die der HTTP-Server überwachen soll:

```
> sudo yast http-server listen add=81
> sudo yast http-server listen list
Listen Statements:
==================
:80
:81
> sudo yast http-server delete=80
```

Mit **`yast http-server listen help`** erhalten Sie eine vollständige Liste der Optionen.

mode

Aktiviert oder deaktiviert den Assistenten-Modus:

```
> sudo yast http-server mode wizard=on
```

modules

Steuert die Apache2-Servermodule:

```
> sudo yast http-server modules enable=php5,rewrite
> sudo yast http-server modules disable=ssl
> sudo http-server modules list
[...]
Enabled rewrite
Disabled ssl
Enabled php5
[...]
```

4.4.3.9 yast kdump

Konfiguriert die `kdump`-Einstellungen. Weitere Informationen zu `kdump` finden Sie in *Buch „System Analysis and Tuning Guide“, Kapitel 18 „Kexec and Kdump“, Abschnitt 18.7 „Basic Kdump configuration“*. **`yast kdump`**akzeptiert die folgenden Befehle:

copykernel

Kopiert den Kernel in das Dump-Verzeichnis.

customkernel

Gibt den Bestandteil *`kernel_string`* im Namen des benutzerdefinierten Kernels an. Das Namensschema lautet `/boot/vmlinu[zx]-`*`kernel_string`*`[.gz]`.

```
> sudo yast kdump customkernel kernel=kdump
```

Mit **`yast kdump customkernel help`** erhalten Sie eine vollständige Liste der Optionen.

dumpformat

Gibt das (Komprimierungs-)Format für das Dump-Kernel-Image an. Die verfügbaren Formate lauten „none“, „ELF“, „compressed“ und „lzo“:

```
> sudo yast kdump dumpformat dump_format=ELF
```

dumplevel

Gibt die Nummer für den Dump-Filterungsgrad an (0 bis 31):

```
> sudo yast kdump dumplevel dump_level=24
```

dumptarget

Gibt das Ziel zum Speichern von Dump-Images an:

```
> sudo kdump dumptarget target=ssh server=name_server port=22 \
```

```
dir=/var/log/dump user=user_name
```

Mit **`yast kdump dumptarget help`** erhalten Sie eine vollständige Liste der Optionen.

immediatereboot

Gibt an, ob das System nach dem Speichern des Core im Kdump-Kernel sofort neu gestartet werden soll:

```
> sudo yast kdump immediatereboot enable
> sudo yast kdump immediatereboot disable
```

keepolddumps

Gibt die Anzahl der aufzubewahrenden bisherigen Dump-Images an. Mit dem Wert 0 werden alle Images aufbewahrt:

```
> sudo yast kdump keepolddumps no=5
```

kernelcommandline

Gibt die Befehlszeile an, die an den kdump-Kernel übergeben werden muss:

```
> sudo yast kdump kernelcommandline command="ro root=LABEL=/"
```

kernelcommandlineappend

Gibt die Befehlszeile an, die an die standardmäßige Zeichenkette für die Befehlszeile *angehängt* werden muss:

```
> sudo yast kdump kernelcommandlineappend command="ro root=LABEL=/"
```

notificationcc

Gibt eine Email-Adresse an, an die eine Kopie der Benachrichtigungen gesendet werden soll:

```
> sudo yast kdump notificationcc email="user1@example.com user2@example.com"
```

notificationto

Gibt eine Email-Adresse an, an die die Benachrichtigungen gesendet werden sollen:

```
> sudo yast kdump notificationto email="user1@example.com user2@example.com"
```

show

Zeigt die `kdump`-Einstellungen an:

```
> sudo yast kdump show
```

```
Kdump is disabled
Dump Level: 31
Dump Format: compressed
Dump Target Settings
target: file
file directory: /var/crash
Kdump immediate reboots: Enabled
Numbers of old dumps: 5
```

smtppass

Gibt die Datei an, die das SMTP-Passwort (in Klartext) für das Senden von Benachrichtigungen enthält:

```
> sudo yast kdump smtppass pass=/path/to/file
```

smtpserver

Gibt den Hostnamen des SMTP-Servers an, über den die Benachrichtigungen gesendet werden sollen:

```
> sudo yast kdump smtpserver server=smtp.server.com
```

smtpuser

Gibt den SMTP-Benutzernamen an, über den die Benachrichtigungen gesendet werden sollen:

```
> sudo yast kdump smtpuser user=smtp_user
```

startup

Aktiviert oder deaktiviert die Startoptionen:

```
> sudo yast kdump startup enable alloc_mem=128,256
> sudo yast kdump startup disable
```

4.4.3.10 yast keyboard

Konfiguriert die Systemtastatur für virtuelle Konsolen. Dies wirkt sich nicht auf die Tastatureinstellungen in grafischen Benutzerumgebungen wie GNOME oder KDE aus. **`yast keyboard`** akzeptiert die folgenden Befehle:

list

Zeigt eine Liste aller verfügbaren Tastaturbelegungen an.

set

Aktiviert eine neue Einstellung für die Tastaturbelegung:

```
> sudo yast keyboard set layout=czech
```

Zusammenfassung

Zeigt die aktuelle Tastaturkonfiguration an.

4.4.3.11 yast lan

Konfiguriert Netzwerkkarten. **`yast lan`** akzeptiert die folgenden Befehle:

fügen Sie beispielsweise Folgendes ein:

Konfiguriert eine neue Netzwerkkarte:

```
> sudo yast lan add name=vlan50 ethdevice=eth0 bootproto=dhcp
```

Mit **`yast lan add help`** erhalten Sie eine vollständige Liste der Optionen.

delete

Löscht eine vorhandene Netzwerkkarte:

```
> sudo yast lan delete id=0
```

Bearbeiten

Ändert die Konfiguration einer vorhandenen Netzwerkkarte:

```
> sudo yast lan edit id=0 bootproto=dhcp
```

list

Zeigt eine Zusammenfassung der Netzwerkkartenkonfiguration an:

```
> sudo yast lan list
id name,           bootproto
0 Ethernet Card 0, NONE
1 Network Bridge,  DHCP
```

4.4.3.12 yast language

Konfiguriert Systemsprachen. **`yast language`** akzeptiert die folgenden Befehle:

list

Zeigt eine Liste aller verfügbaren Sprachen an.

set

Gibt die Hauptsystemsprachen und sekundären Sprachen an:

```
> sudo yast language set lang=cs_CZ languages=en_US,es_ES no_packages
```

4.4.3.13 yast mail

Zeigt die Konfiguration des Mailsystems an:

```
> sudo yast mail summary
```

4.4.3.14 yast nfs

Steuert den NFS-Client. **`yast nfs`** akzeptiert die folgenden Befehle:

fügen Sie beispielsweise Folgendes ein:

Fügt eine neue NFS-Einhängung ein:

```
> sudo yast nfs add spec=remote_host:/path/to/nfs/share file=/local/mount/point
```

Mit **`yast nfs add help`** erhalten Sie eine vollständige Liste der Optionen.

delete

Löscht eine vorhandene NFS-Einhängung:

```
> sudo yast nfs delete spec=remote_host:/path/to/nfs/share file=/local/mount/point
```

Mit **`yast nfs delete help`** erhalten Sie eine vollständige Liste der Optionen.

Bearbeiten

Ändert eine vorhandene NFS-Einhängung:

```
> sudo yast nfs edit spec=remote_host:/path/to/nfs/share \
 file=/local/mount/point type=nfs4
```

Mit **`yast nfs edit help`** erhalten Sie eine vollständige Liste der Optionen.

list

Zeigt eine Liste der vorhandenen NFS-Einhängungen an:

```
> sudo yast nfs list
Server            Remote File System    Mount Point    Options
-----------------------------------------------------------------
nfs.example.com   /mnt                  /nfs/mnt       nfs
```

```
nfs.example.com   /home/tux/nfs_share   /nfs/tux       nfs
```

4.4.3.15 yast nfs-server

Konfiguriert den NFS-Server. **`yast nfs-server`** akzeptiert die folgenden Befehle:

fügen Sie beispielsweise Folgendes ein:

Fügt ein Verzeichnis zum Exportieren ein:

```
> sudo yast nfs-server add mountpoint=/nfs/export hosts=*.allowed_hosts.com
```

Mit **`yast nfs-server add help`** erhalten Sie eine vollständige Liste der Optionen.

delete

Löscht ein Verzeichnis aus dem NFS-Export:

```
 > sudo yast nfs-server delete mountpoint=/nfs/export
```

set

Gibt zusätzliche Parameter für den NFS-Server an:

```
> sudo yast nfs-server set enablev4=yes security=yes
```

Mit **`yast nfs-server set help`** erhalten Sie eine vollständige Liste der Optionen.

start

Startet den NFS-Serverdienst:

```
> sudo yast nfs-server start
```

stop

Hält den NFS-Serverdienst an:

```
> sudo yast nfs-server stop
```

Zusammenfassung

Zeigt eine Zusammenfassung der NFS-Serverkonfiguration an:

```
> sudo yast nfs-server summary
NFS server is enabled
NFS Exports
* /mnt
* /home

NFSv4 support is enabled.
The NFSv4 domain for idmapping is localdomain.
NFS Security using GSS is enabled.
```

4.4.3.16 yast nis

Konfiguriert den NIS-Client. **`yast nis`** akzeptiert die folgenden Befehle:

configure

Ändert globale Einstellungen für einen NIS-Client:

```
> sudo yast nis configure server=nis.example.com broadcast=yes
```

Mit **`yast nis configure help`** erhalten Sie eine vollständige Liste der Optionen.

Deaktivieren

Deaktiviert den NIS-Client:

```
> sudo yast nis disable
```

enable

Aktiviert den Computer als NIS-Client:

```
> sudo yast nis enable server=nis.example.com broadcast=yes automounter=yes
```

Mit **`yast nis enable help`** erhalten Sie eine vollständige Liste der Optionen.

Suche

Zeigt die verfügbaren NIS-Server für eine bestimmte Domäne an:

```
> sudo yast nis find domain=nisdomain.com
```

Zusammenfassung

Zeigt eine Konfigurationszusammenfassung für einen NIS-Client an.

4.4.3.17 yast nis-server

Konfiguriert einen NFS-Server. **`yast nis-server`** akzeptiert die folgenden Befehle:

master

Konfiguriert einen NIS-Master-Server:

```
> sudo yast nis-server master domain=nisdomain.com yppasswd=yes
```

Mit **`yast nis-server master help`** erhalten Sie eine vollständige Liste der Optionen.

slave

Konfiguriert einen NIS-Worker-Server:

```
> sudo yast nis-server slave domain=nisdomain.com master_ip=10.100.51.65
```

Mit **`yast nis-server slave help`** erhalten Sie eine vollständige Liste der Optionen.

stop

Hält einen NIS-Server an:

```
> sudo yast nis-server stop
```

Zusammenfassung

Zeigt eine Konfigurationszusammenfassung für einen NIS-Server an:

```
> sudo yast nis-server summary
```

4.4.3.18 yast proxy

Konfiguriert Proxy-Einstellungen. **`yast proxy`** akzeptiert die folgenden Befehle:

Authentifizierung mit

Gibt die Authentifizierungsoptionen für den Proxy an:

```
> sudo yast proxy authentication username=tux password=secret
```

Mit **`yast proxy authentication help`** erhalten Sie eine vollständige Liste der Optionen.

enable, disable

Aktiviert oder deaktiviert die Proxy-Einstellungen.

set

Ändert die aktuellen Proxy-Einstellungen:

```
> sudo yast proxy set https=proxy.example.com
```

Mit **`yast proxy set help`** erhalten Sie eine vollständige Liste der Optionen.

Zusammenfassung

Zeigt die Proxy-Einstellungen an.

4.4.3.19 yast rdp

Steuert die Remote-Desktop-Einstellungen. **`yast rdp`** akzeptiert die folgenden Befehle:

allow

Gestattet den Remote-Zugriff auf den Desktop des Servers:

```
> sudo yast rdp allow set=yes
```

list

Zeigt die Konfigurationszusammenfassung für den Remote-Desktop an.

4.4.3.20 yast samba-client

Konfiguriert die Samba-Client-Einstellungen. **`yast samba-client`** akzeptiert die folgenden Befehle:

configure

Ändert globale Einstellungen für Samba:

```
> sudo yast samba-client configure workgroup=FAMILY
```

isdomainmember

Überprüft, ob der Rechner Mitglied einer Domäne ist:

```
> sudo yast samba-client isdomainmember domain=SMB_DOMAIN
```

joindomain

Nimmt den Computer als Mitglied in eine Domäne auf:

```
> sudo yast samba-client joindomain domain=SMB_DOMAIN user=username password=pwd
```

winbind

Aktiviert oder deaktiviert die Winbind-Services (den `winbindd`-Daemon):

```
> sudo yast samba-client winbind enable
> sudo yast samba-client winbind disable
```

4.4.3.21 yast samba-server

Konfiguriert Samba-Server-Einstellungen. **`yast samba-server`** akzeptiert die folgenden Befehle:

Backend

Gibt das Back-End zum Speichern der Benutzerdaten an:

```
> sudo yast samba-server backend smbpasswd
```

Mit **`yast samba-server backend help`** erhalten Sie eine vollständige Liste der Optionen.

configure

Konfiguriert globale Einstellungen für den Samba-Server:

```
> sudo yast samba-server configure workgroup=FAMILY description='Home server'
```

Mit **`yast samba-server configure help`** erhalten Sie eine vollständige Liste der Optionen.

list

Zeigt eine Liste der verfügbaren Freigaben an:

```
> sudo yast samba-server list
Status     Type Name
============================
Disabled   Disk profiles
Enabled    Disk print$
Enabled    Disk homes
Disabled   Disk groups
Enabled    Disk movies
Enabled    Printer printers
```

role

Gibt die Funktion des Samba-Servers an:

```
> sudo yast samba-server role standalone
```

Mit **`yast samba-server role help`** erhalten Sie eine vollständige Liste der Optionen.

service

Aktiviert oder deaktiviert die Samba-Dienste (`smb` und `nmb`):

```
> sudo yast samba-server service enable
> sudo yast samba-server service disable
```

share

Manipuliert eine einzelne Samba-Freigabe:

```
> sudo yast samba-server share name=movies browseable=yes guest_ok=yes
```

Mit **`yast samba-server share help`** erhalten Sie eine vollständige Liste der Optionen.

4.4.3.22 yast security

Steuert die Sicherheitsstufe des Hosts. **`yast security`** akzeptiert die folgenden Befehle:

level

Gibt die Sicherheitsstufe des Hosts an:

```
> sudo yast security level server
```

Mit **`yast security level help`** erhalten Sie eine vollständige Liste der Optionen.

set

Legt den Wert einer bestimmten Option fest:

```
> sudo yast security set passwd=sha512 crack=yes
```

Mit **`yast security set help`** erhalten Sie eine vollständige Liste der Optionen.

Zusammenfassung

Zeigt eine Zusammenfassung der aktuellen Sicherheitskonfiguration an:

```
sudoyast security summary
```

4.4.3.23 yast sound

Konfiguriert Soundkarteneinstellungen. **`yast sound`** akzeptiert die folgenden Befehle:

fügen Sie beispielsweise Folgendes ein:

Konfiguriert eine neue Soundkarte. Falls keine Parameter angegeben sind, fügt der Befehl die erste erkannte Soundkarte hinzu.

```
> sudo yast sound add card=0 volume=75
```

Mit **`yast sound add help`** erhalten Sie eine vollständige Liste der Optionen.

channels

Zeigt eine Liste der verfügbaren Lautstärkekanäle einer Soundkarte an:

```
> sudo yast sound channels card=0
Master 75
PCM 100
```

modules

Zeigt eine Liste aller verfügbaren Sound-Kernel-Module an:

```
> sudo yast sound modules
snd-atiixp ATI IXP AC97 controller (snd-atiixp)
snd-atiixp-modem ATI IXP MC97 controller (snd-atiixp-modem)
snd-virtuoso Asus Virtuoso driver (snd-virtuoso)
[...]
```

playtest

Spielt einen Testsound über eine Soundkarte ab:

```
> sudo yast sound playtest card=0
```

Entfernen

Entfernt eine konfigurierte Soundkarte:

```
> sudo yast sound remove card=0
> sudo yast sound remove all
```

set

Gibt neue Werte für eine Soundkarte an:

```
> sudo yast sound set card=0 volume=80
```

show

Zeigt ausführliche Informationen zu einer Soundkarte an:

```
> sudo yast sound show card=0
Parameters of card 'ThinkPad X240' (using module snd-hda-intel):

align_buffer_size
 Force buffer and period sizes to be multiple of 128 bytes.
bdl_pos_adj
 BDL position adjustment offset.
beep_mode
 Select HDA Beep registration mode (0=off, 1=on) (default=1).
 Default Value: 0
enable_msi
 Enable Message Signaled Interrupt (MSI)
[...]
```

Zusammenfassung

Gibt eine Konfigurationszusammenfassung für alle Soundkarten im System aus:

```
> sudo yast sound summary
```

ein Laufwerk zu

Gibt die Lautstärke einer Soundkarte an:

```
sudoyast sound volume card=0 play
```

4.4.3.24 yast sysconfig

Steuert die Variablen in Dateien unter `/etc/sysconfig`. **`yast sysconfig`** akzeptiert die folgenden Befehle:

Löschen

Legt eine leeren Wert für eine Variable fest:

```
> sudo yast sysconfig clear=POSTFIX_LISTEN
```

Tipp: Variable in mehreren Dateien

Wenn die Variable in mehreren Dateien vorhanden ist, verwenden Sie die Syntax *`VARIABLE_NAME$FILE_NAME`*:

```
> sudo yast sysconfig clear=CONFIG_TYPE$/etc/sysconfig/mail
```

Details

Zeigt ausführliche Informationen zu einer Variable an:

```
> sudo yast sysconfig details variable=POSTFIX_LISTEN
Description:
Value:
File: /etc/sysconfig/postfix
Possible Values: Any value
Default Value:
Configuration Script: postfix
Description:
 Comma separated list of IP's
 NOTE: If not set, LISTEN on all interfaces
```

list

Zeigt eine Zusammenfassung der geänderten Variablen an. Mit **`all`** werden alle Variablen und ihre zugehörigen Werte angezeigt:

```
> sudo yast sysconfig list all
AOU_AUTO_AGREE_WITH_LICENSES="false"
AOU_ENABLE_CRONJOB="true"
AOU_INCLUDE_RECOMMENDS="false"
[...]
```

set

Legt einen Wert für eine Variable fest:

```
> sudo yast sysconfig set DISPLAYMANAGER=gdm
```

Tipp: Variable in mehreren Dateien

Wenn die Variable in mehreren Dateien vorhanden ist, verwenden Sie die Syntax *VARIABLE_NAME*$*FILE_NAME*:

```
> sudo yast sysconfig set CONFIG_TYPE$/etc/sysconfig/mail=advanced
```

4.4.3.25 yast tftp-server

Konfiguriert einen TFTP-Server. **yast tftp-server** akzeptiert die folgenden Befehle:

Verzeichnis

Gibt das Verzeichnis für den TFTP-Server an:

```
> sudo yast tftp-server directory path=/srv/tftp
> sudo yast tftp-server directory list
Directory Path: /srv/tftp
```

status

Steuert den Status des TFTP-Serverdienstes:

```
> sudo yast tftp-server status disable
> sudo yast tftp-server status show
Service Status: false
> sudo yast tftp-server status enable
```

4.4.3.26 yast timezone

Konfiguriert die Zeitzone. **yast timezone** akzeptiert die folgenden Befehle:

list

Zeigt eine Liste aller verfügbaren Zeitzonen an, gruppiert nach Region:

```
> sudo yast timezone list
```

```
Region: Africa
Africa/Abidjan (Abidjan)
Africa/Accra (Accra)
Africa/Addis_Ababa (Addis Ababa)
[...]
```

set

Gibt neue Werte für die Zeitzonenkonfiguration an:

```
> sudo yast timezone set timezone=Europe/Prague hwclock=local
```

Zusammenfassung

Zeigt eine Zusammenfassung der Zeitzonenkonfiguration an:

```
> sudo yast timezone summary
Current Time Zone: Europe/Prague
Hardware Clock Set To: Local time
Current Time and Date: Mon 12. March 2018, 11:36:21 CET
```

4.4.3.27 yast users

Verwaltet Benutzerkonten. **`yast users`** akzeptiert die folgenden Befehle:

fügen Sie beispielsweise Folgendes ein:

Fügt einen neuen Benutzer hinzu:

```
> sudo yast users add username=user1 password=secret home=/home/user1
```

Mit **`yast users add help`** erhalten Sie eine vollständige Liste der Optionen.

delete

Löscht ein vorhandenes Benutzerkonto:

```
> sudo yast users delete username=user1 delete_home
```

Mit **`yast users delete help`** erhalten Sie eine vollständige Liste der Optionen.

Bearbeiten

Ändert ein vorhandenes Benutzerkonto:

```
> sudo yast users edit username=user1 password=new_secret
```

Mit **`yast users edit help`** erhalten Sie eine vollständige Liste der Optionen.

list

Zeigt eine Liste der vorhandenen Benutzer an, gefiltert nach dem Benutzertyp:

```
> sudo yast users list system
```

Mit **`yast users list help`** erhalten Sie eine vollständige Liste der Optionen.

show

Zeigt Details zu einem Benutzer an:

```
> sudo yast users show username=wwwrun
Full Name: WWW daemon apache
List of Groups: www
Default Group: wwwrun
Home Directory: /var/lib/wwwrun
Login Shell: /sbin/nologin
Login Name: wwwrun
UID: 456
```

Mit **`yast users show help`** erhalten Sie eine vollständige Liste der Optionen.

5 Ändern der Sprach- und Ländereinstellungen mit YaST

In diesem Kapitel wird erläutert, wie Sie Sprach- und Ländereinstellungen konfigurieren. Sie können die Sprache global für das gesamte System, individuell für bestimmte Benutzer oder Desktops oder auch vorübergehend für einzelne Anwendungen ändern. Außerdem können Sie sekundäre Sprachen konfigurieren und die Datums- und Ländereinstellungen anpassen.

Wenn Sie in verschiedenen Ländern oder in einer mehrsprachigen Umgebung arbeiten, sollten Sie Ihr System entsprechend konfigurieren. SUSE® Linux Enterprise Desktop kann verschiedene `locales` parallel verarbeiten. Eine Locale bezeichnet eine Reihe von Parametern, die die Sprache und die Ländereinstellungen, die in der Benutzeroberfläche angezeigt werden, definiert.

Die Hauptsystemsprache wird während der Installation ausgewählt und die Tastatur- und Zeitzoneneinstellungen werden entsprechend angepasst. Sie können jedoch zusätzliche Sprachen installieren und festlegen, welche der installierten Sprachen als Standard dienen soll.

Verwenden Sie für diese Aufgaben das YaST-Sprachmodul wie unter *Abschnitt 5.1, „Ändern der Systemsprache“* beschrieben. Installieren Sie sekundäre Sprachen, um optionale Sprachumgebungen nutzen zu können, wenn Anwendungen oder Desktops in anderen Sprachen als der Primärsprache gestartet werden sollen.

Mit dem YaST-Zeitzonenmodul können Sie Ihre Länder- und Zeitzoneneinstellungen entsprechend anpassen. Sie können damit auch Ihre Systemuhr mit einem Zeitserver synchronisieren. Detaillierte Informationen finden Sie in *Abschnitt 5.2, „Ändern der Länder- und Zeiteinstellungen“*.

5.1 Ändern der Systemsprache

Abhängig davon, wie Sie Ihren Desktop nutzen und ob Sie das ganze System oder nur die Desktop-Umgebung in eine andere Sprache umschalten möchten, haben Sie verschiedene Möglichkeiten:

Globales Ändern der Systemsprache

Gehen Sie vor wie unter *Abschnitt 5.1.1, „Bearbeiten von Systemsprachen mit YaST“* und *Abschnitt 5.1.2, „Wechseln der Standard-Systemsprache“* beschrieben, um zusätzliche lokalisierte Pakete mit YaST zu installieren und die Standardsprache festzulegen. Die Änderungen

treten nach dem nächsten Anmelden in Kraft. Um sicherzustellen, dass das ganze System die Änderung übernommen hat, starten Sie das System neu oder beenden Sie alle laufenden Dienste, Anwendungen und Programme und starten Sie sie wieder neu.

Ändern der Sprache nur für den Desktop

Vorausgesetzt die gewünschten Sprachpakete wurden wie unten beschrieben mit YaST für Ihre Desktop-Umgebung installiert, können Sie die Sprache Ihres Desktops über das Desktop-Kontrollzentrum ändern. Weitere Informationen finden Sie in *Buch „GNOME-Benutzerhandbuch“, Kapitel 3 „Anpassen Ihrer Einstellungen“, Abschnitt 3.2 „Konfigurieren der Spracheinstellungen“*. Nach dem Neustart des X-Servers übernimmt Ihr gesamter Desktop die neue Sprachauswahl. Anwendungen, die nicht zu Ihrem Desktop-Rahmen gehören, werden von dieser Änderung nicht beeinflusst und können immer noch in der Sprache angezeigt werden, die in YaST festgelegt war.

Temporärer Sprachwechsel für nur eine Anwendung

Sie können auch eine einzelne Anwendung in einer anderen Sprache (die bereits mit YaST installiert wurde) ausführen. Starten Sie die Anwendung zu diesem Zweck von der Befehlszeile aus, indem Sie den Sprachcode wie unter *Abschnitt 5.1.3, „Sprachwechsel für Standard X- und GNOME-Anwendungen“* beschrieben angeben.

5.1.1 Bearbeiten von Systemsprachen mit YaST

YaST unterstützt zwei verschiedene Sprachkategorien:

Primäre Sprache

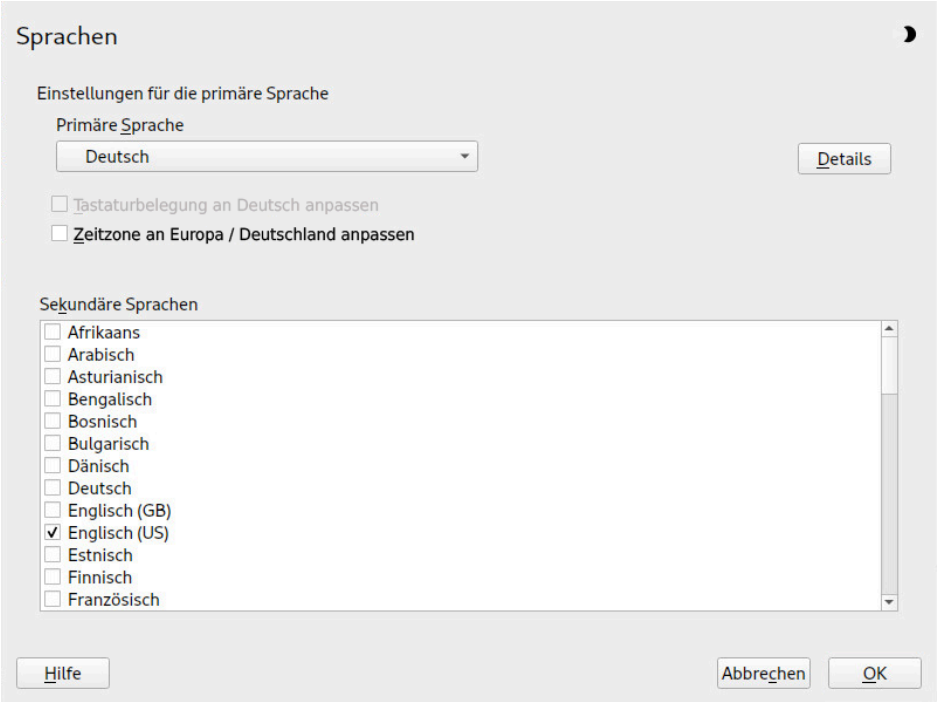
Die in YaST festgelegter primäre Sprache gilt für das gesamte System, einschließlich YaST und der Desktop-Umgebung. Diese Sprache wird immer benutzt, wenn sie verfügbar ist, es sei denn, Sie legen manuell eine andere Sprache fest.

Sekundäre Sprachen

Installieren Sie sekundäre Sprachen, um Ihr System mehrsprachig zu machen. Die als sekundär installierten Sprachen können bei Bedarf manuell ausgewählt werden. Verwenden Sie beispielsweise eine sekundäre Sprache, um eine Anwendung in einer bestimmten Sprache zu starten und Texte in dieser Sprache zu verarbeiten.

Legen Sie vor der Installation weiterer Sprachen fest, welche dieser Sprachen als Standard-Systemsprache (primäre Sprache) fungieren soll.

Starten Sie YaST, um auf das YaST-Sprachmodul zuzugreifen, und klicken Sie auf *System* › *Sprache*. Starten Sie alternativ das Dialogfeld *Sprachen* direkt, indem Sie **`sudo yast2 language &`** von einer Befehlszeile aus ausführen.



VORGEHEN 5.1: INSTALLIEREN VON ZUSÄTZLICHEN SPRACHEN

Wenn Sie weitere Sprachen installieren, können Sie mit YaST auch verschiedene Locale-Einstellungen für den `root`-Benutzer festlegen. Informationen hierzu finden Sie in *Schritt 4*. Mit der Option *Locale-Einstellungen für den Benutzer „root“* wird festgelegt, wie die Locale-Variablen (`LC_*`) in der Datei `/etc/sysconfig/language` für `root` festgelegt werden. Diese Elemente können Sie auf dieselbe Locale wie bei normalen Benutzern einstellen. Alternativ können Sie angeben, dass eine Änderung der Sprache keine Auswirkungen haben soll, oder lediglich die Variable `RC_LC_CTYPE` auf dieselben Werte wie für normale Benutzer einstellen. Die Variable `RC_LC_CTYPE` bestimmt die Lokalisierung für sprachspezifische Funktionsaufrufe.

1. Wählen Sie zum Hinzufügen von Sprachen im YaST-Modul *Sekundäre Sprachen*, die installiert werden sollen.

2. Um eine Sprache als Standardsprache einzurichten, müssen Sie sie als *Primäre Sprache* festlegen.

3. Passen Sie außerdem die Tastatur an die neue primäre Sprache an und stellen Sie eventuell eine andere Zeitzone ein.

Tipp: Erweiterte Einstellungen

Wählen Sie in YaST für erweiterte Tastatur- oder Zeitzoneneinstellungen die Optionen *Hardware* › *Systemtastaturbelegung* oder *System* › *Datum und Uhrzeit*. Weitere Informationen finden Sie in *Kapitel 32, Einrichten der Systemtastaturbelegung* und *Abschnitt 5.2, „Ändern der Länder- und Zeiteinstellungen“*.

4. Klicken Sie auf *Details*, um die für den `root`-Benutzer spezifischen Spracheinstellungen zu ändern.

    a. Legen Sie für *Locale-Einstellungen für den Benutzer root* die gewünschten Werte fest. Weitere Informationen erhalten Sie durch Klicken auf *Hilfe*.

    b. Entscheiden Sie, ob Sie für `root` die *UTF-8-Kodierung verwenden* möchten.

5. Wenn Ihre Locale nicht in der verfügbaren Liste der primären Sprachen enthalten war, versuchen Sie, diese unter *Detaillierte Locale-Einstellung* anzugeben. Dies kann jedoch dazu führen, dass bestimmte Locales unvollständig sind.

6. Bestätigen Sie die Änderungen in den Dialogfeldern mit *OK*. Wenn Sie sekundäre Sprachen ausgewählt haben, installiert YaST die lokalisierten Softwarepakete für die zusätzlichen Sprachen.

Das System ist nun mehrsprachig. Um jedoch eine Anwendung in einer Sprache starten zu können, die nicht als primäre Sprache festgelegt wurde, müssen Sie die gewünschte Sprache explizit wie unter *Abschnitt 5.1.3, „Sprachwechsel für Standard X- und GNOME-Anwendungen“* beschrieben festlegen.

5.1.2 Wechseln der Standard-Systemsprache

So ändern Sie die Standardsprache für ein System global:

1. Starten Sie das YaST-Sprachmodul.

2. Wählen Sie die gewünschte neue Systemsprache als *Primäre Sprache* aus.

> **Wichtig: Löschen früherer Systemsprachen**
>
> Wenn Sie zu einer anderen primären Sprache wechseln, wird das lokalisierte Softwarepaket für die frühere primäre Sprache aus dem System entfernt. Wenn die Standard-Systemsprache gewechselt, die frühere primäre Sprache jedoch als zusätzliche Sprache beibehalten werden soll, fügen Sie diese als *Sekundäre Sprache* hinzu, indem Sie das entsprechende Kontrollkästchen aktivieren.

3. Passen Sie die Tastatur- und Zeitzonenoptionen wunschgemäß an.
4. Bestätigen Sie die Änderungen mit *OK*.
5. Starten Sie nach der Anwendung der Änderungen in YaST alle aktuellen X-Sitzungen neu (zum Beispiel durch Abmelden und erneutes Anmelden), damit Ihre neuen Spracheinstellungen in YaST und die Desktop-Anwendungen übernommen werden.

5.1.3 Sprachwechsel für Standard X- und GNOME-Anwendungen

Nach der Installation der entsprechenden Sprache mit YaST können Sie eine einzelne Anwendung in einer anderen Sprache ausführen.

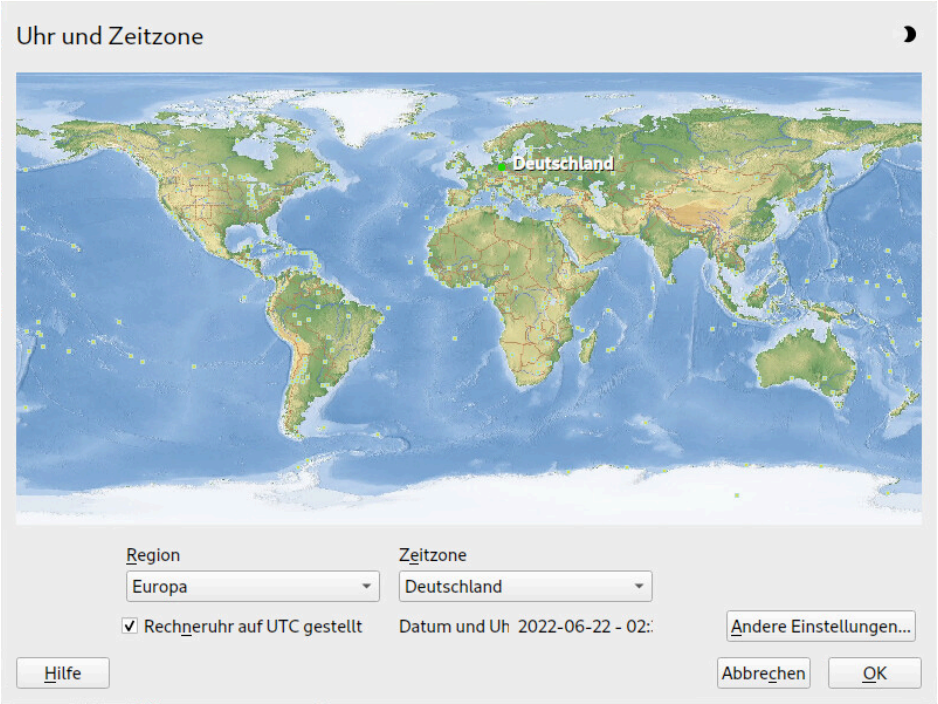
Starten Sie die Anwendung von der Befehlszeile aus, indem Sie folgenden Befehl verwenden:

```
LANG=LANGUAGE application
```

Um beispielsweise f-spot auf Deutsch auszuführen, führen Sie den Befehl **`LANG=de_DE f-spot`** aus. Verwenden Sie für andere Sprachen den entsprechenden Sprachcode. Mit dem Befehl **`locale`** `-av` können Sie eine Liste aller verfügbaren Sprachcodes abrufen.

5.2 Ändern der Länder- und Zeiteinstellungen

Passen Sie mithilfe des YaST-Moduls für Datum und Uhrzeit das Systemdatum sowie die Uhrzeit- und Zeitzoneninformationen an die Region an, in der Sie arbeiten. Starten Sie YaST, um auf das YaST-Modul zuzugreifen, und klicken Sie auf *System* › *Datum und Uhrzeit*. Starten Sie alternativ das Dialogfeld *Uhr und Zeitzone* direkt, indem Sie **`sudo yast2 timezone &`** von einer Befehlszeile aus ausführen.



Wählen Sie zunächst eine allgemeine Region, beispielsweise *Europa*. Wählen Sie dann das für Sie passende Land aus, beispielsweise *Deutschland*.

Passen Sie je nachdem, welche Betriebssysteme auf Ihrem Arbeitsplatzrechner ausgeführt werden, die Einstellungen der Rechneruhr entsprechend an.

- Wenn auf Ihrem Rechner ein anderes Betriebssystem ausgeführt wird, beispielsweise Microsoft Windows*, verwendet Ihr System möglicherweise die lokale Zeit und nicht UTC. Deaktivieren Sie in diesem Fall *Hardware-Uhr auf UTC festgelegt*.

- Wenn auf Ihrem Rechner nur Linux ausgeführt wird, stellen Sie die Rechneruhr auf UTC (Universal Time Coordinated) ein. Hiermit wird die Umstellung von der Standardzeit auf die Sommerzeit automatisch durchgeführt.

Wichtig: Einstellen der Rechneruhr auf UTC

Die Umschaltung von der Standardzeit auf die Sommerzeit (und umgekehrt) erfolgt nur dann automatisch, wenn die Rechneruhr (CMOS-Uhr) auf UTC eingestellt ist. Dies gilt auch dann, wenn Sie die automatische Zeitsynchronisierung mit NTP nutzen, weil die automatische Synchronisierung nur dann vorgenommen wird, wenn die Zeitdifferenz zwischen der Rechneruhr und der Systemuhr weniger als 15 Minuten beträgt.

Eine falsche Systemzeit kann zu schwerwiegenden Problemen führen (verpasste Datensicherungen, verloren gegangene E-Mails, Fehler beim Einhängen in Ferndateisysteme usw.). Es wird daher dringend empfohlen, die Rechneruhr *immer* auf UTC einzustellen.

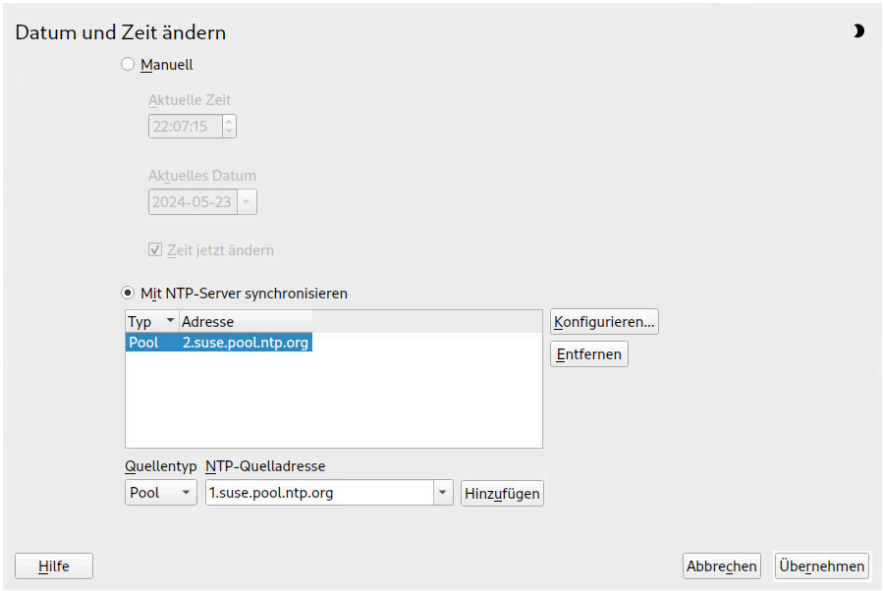
Sie können das Datum und die Uhrzeit manuell ändern oder Ihren Computer mit einem NTP-Server synchronisieren lassen, entweder permanent oder nur zur Festlegung Ihrer Hardware-Uhr.

VORGEHEN 5.2: MANUELLES ANPASSEN VON DATUM UND UHRZEIT

1. Klicken Sie im YaST-Zeitzonenmodul auf *Andere Einstellungen*, um Datum und Uhrzeit festzulegen.
2. Wählen Sie *Manuell* aus und geben Sie das Datum und die Uhrzeit ein.
3. Bestätigen Sie Ihre Änderungen.

VORGEHEN 5.3: FESTLEGEN VON DATUM UND UHRZEIT ÜBER NTP-SERVER

1. Klicken Sie auf *Andere Einstellungen*, um das aktuelle Datum und die Uhrzeit festzulegen.
2. Wählen Sie *Mit NTP-Server synchronisieren* aus.
3. Geben Sie die Adresse eines NTP-Servers ein, falls sie nicht bereits eingetragen ist.



4. Mit der Schaltfläche *Konfigurieren* können Sie die erweiterte NTP-Konfiguration öffnen. Weitere Informationen finden Sie in *Abschnitt 39.1, „Konfigurieren eines NTP-Clients mit YaST“*.
5. Bestätigen Sie Ihre Änderungen.

6 Verwalten von Benutzern mit YaST

Während der Installation haben Sie möglicherweise einen lokalen Benutzer für Ihr System erstellt. Mit dem YaST-Modul *Verwaltung von Benutzern und Gruppen* können Sie Benutzer hinzufügen und vorhandene Benutzer bearbeiten. Darüber hinaus können Sie das System für die Authentifizierung von Benutzern über einen Netzwerkserver konfigurieren.

6.1 Dialogfeld „Verwaltung von Benutzern und Gruppen“

Zur Verwaltung von Benutzern oder Gruppen starten Sie YaST, und klicken Sie auf *Sicherheit und Benutzer* › *Verwaltung von Benutzern und Gruppen*. Starten Sie alternativ das Dialogfeld *Verwaltung von Benutzern und Gruppen* direkt, indem Sie `sudo yast2 users &` an einer Befehlszeile ausführen.

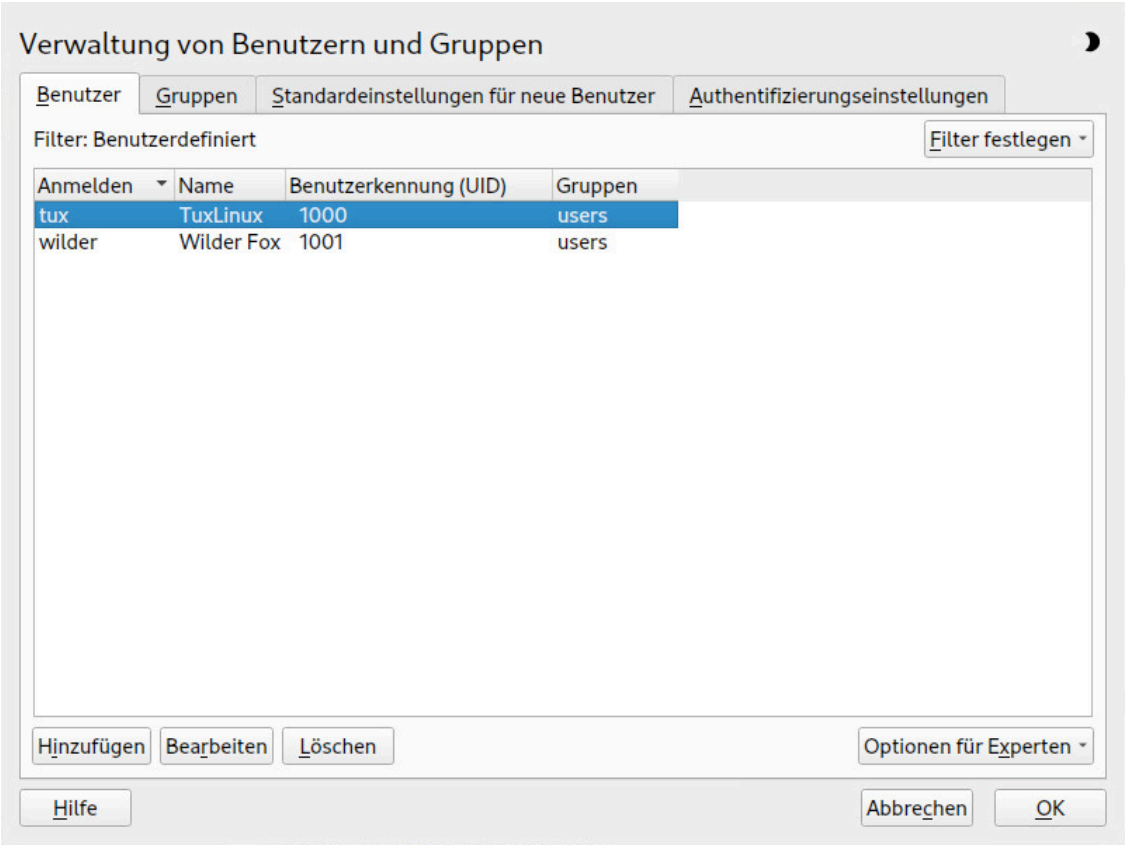


ABBILDUNG 6.1: YAST – VERWALTUNG VON BENUTZERN UND GRUPPEN

Jedem Benutzer wird eine systemweite Benutzer-ID (UID) zugewiesen. Neben den Benutzern, die sich an Ihrem Computer anmelden können, gibt es außerdem eine Reihe von *Systembenutzern* nur für den internen Gebrauch. Jeder Benutzer wird einer oder mehreren Gruppen zugewiesen. Ähnlich wie bei den *Systembenutzern* gibt es auch *Systemgruppen* für den internen Gebrauch.

Im Hauptfenster werden mehrere Registerkarten angezeigt, und zwar abhängig von der Gruppe der Benutzern (lokale Benutzer, Netzwerkbenutzer, Systembenutzer), die Sie anzeigen und ändern möchten. Über die Registerkarten können Sie die folgenden Aufgaben ausführen:

Verwalten von Benutzerkonten

Auf der Registerkarte *Benutzer* können Sie Benutzerkonten erstellen, ändern, löschen oder vorübergehend deaktivieren (siehe *Abschnitt 6.2, „Verwalten von Benutzerkonten“*). Weitere Informationen zur Durchsetzung von Passwortrichtlinien, zur Verwendung von verschlüsselten Home-Verzeichnissen oder zur Verwaltung von Festplattenquoten finden Sie unter *Abschnitt 6.3, „Weitere Optionen für Benutzerkonten“*.

Ändern der Standardeinstellungen

Die Einstellungen auf der Registerkarte *Standardeinstellungen für neue Benutzer* legen fest, wie lokale Benutzerkonten erstellt werden. Informationen zur Änderung der Standardgruppenzuweisung oder des Standardpfads und der Zugriffsberechtigungen für Home-Verzeichnisse erhalten Sie unter *Abschnitt 6.4, „Ändern der Standardeinstellungen für lokale Benutzer“*.

Zuweisen von Benutzern zu Gruppen

Informationen zur Änderung der Gruppenzuweisung für einzelne Benutzer erhalten Sie unter *Abschnitt 6.5, „Zuweisen von Benutzern zu Gruppen“*.

Gruppen verwalten

Auf der Registerkarte *Gruppen* können Sie Gruppen hinzufügen, ändern oder löschen. Informationen hierzu erhalten Sie unter *Abschnitt 6.6, „Gruppen verwalten“*.

Ändern der Methode zur Benutzerauthentifizierung

Wenn Ihr Computer mit einem Netzwerk verbunden ist, das Benutzerauthentifizierungsmethoden wie NIS oder LDAP unterstützt, können Sie auf der Registerkarte *Einstellungen für Authentifizierung* zwischen verschiedenen Authentifizierungsmethoden wählen. Weitere Informationen hierzu finden Sie in *Abschnitt 6.7, „Ändern der Methode zur Benutzerauthentifizierung“*.

Für die Verwaltung von Benutzern und Gruppen bietet das Dialogfeld ähnliche Funktionen. Sie können einfach zwischen den Ansichten für die Verwaltung von Benutzern und Gruppen umschalten, indem Sie oben im Dialogfeld den entsprechenden Karteireiter auswählen.

Mit Filteroptionen definieren Sie die zu bearbeitenden Benutzer oder Gruppen: Klicken Sie auf der Registerkarte *Benutzer* oder *Gruppe* auf *Filter festlegen*, sodass die Benutzer oder Gruppen angezeigt werden. Diese werden nach bestimmten Kategorien aufgeführt, z. B. *Lokale Benutzer* oder *LDAP-Benutzer* (falls zutreffend). Mit *Filter festlegen* › *Benutzerdefinierte Filtereinstellung* können Sie außerdem einen benutzerdefinierten Filter einrichten und verwenden.

Je nach Filter stehen im Dialogfeld nicht alle nachfolgend beschriebenen Optionen und Funktionen zur Verfügung.

6.2 Verwalten von Benutzerkonten

Mit YaST können Sie Benutzerkonten erstellen, bearbeiten, löschen oder vorübergehend deaktivieren. Ändern Sie keine Benutzerkonten, es sei denn, Sie sind ein erfahrener Benutzer oder Administrator.

Anmerkung: Ändern der Benutzer-IDs bestehender Benutzer

Als Eigentümer einer Datei wird nicht der Name des betreffenden Benutzers, sondern seine Benutzer-ID angegeben. Bei der Änderung einer Benutzer-ID werden die Dateien im Home-Verzeichnis des betreffenden Benutzers automatisch an die neue ID angepasst. Das Eigentum an Dateien, die der Benutzer an anderer Stelle im Dateisystem erstellt hat, geht bei einer Änderung der Benutzer-ID allerdings verloren. Um es zu erhalten, müssten Sie den Eigentümer der Dateien manuell ändern.

Die folgenden Anweisungen zeigen Ihnen, wie Sie Standardbenutzerkonten einrichten. Weitere Optionen finden Sie unter *Abschnitt 6.3, „Weitere Optionen für Benutzerkonten“*.

VORGEHEN 6.1: HINZUFÜGEN ODER BEARBEITEN VON BENUTZERKONTEN

1. Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen*, und klicken Sie dort auf *Benutzer*.
2. Definieren Sie mithilfe von *Filter festlegen* die Menge der Benutzer, die Sie verwalten möchten. Das Dialogfeld zeigt eine Liste der Benutzer im System und die Gruppen, zu denen die Benutzer gehören.
3. Wenn Sie Optionen für einen vorhandenen Benutzer bearbeiten möchten, wählen Sie einen Eintrag aus und klicken Sie dann auf *Bearbeiten*.
   Zum Erstellen eines neuen Benutzerkontos klicken Sie auf *Hinzufügen*.

4. Geben Sie die entsprechenden Benutzerdaten auf dem ersten Karteireiter an, beispielsweise *Benutzername* (zur Anmeldung verwendet) und *Passwort*. Diese Daten reichen aus, um einen neuen Benutzer zu erstellen. Wenn Sie jetzt auf *OK* klicken, weist das System automatisch eine Benutzer-ID zu und legt alle anderen Werte als Standard fest.

5. Aktivieren Sie *Empfang von System-Emails*, wenn alle Systembenachrichtigungen an die Mailbox dieses Benutzers zugestellt werden sollen. Dadurch wird ein Email-Alias für den `root`-Benutzer erstellt und der Benutzer kann die System-Email lesen, ohne sich vorher als `root`-Benutzer anmelden zu müssen.
   Die durch Systemdienste gesendeten Emails werden in der lokalen Mailbox unter `/var/spool/mail/`*`USERNAME`* abgelegt, wobei mit *`USERNAME`* der Anmeldename des ausgewählten Benutzers gemeint ist. Emails können mit dem Befehl **`mail`** gelesen werden.

6. Auf der Registerkarte *Details* können Sie Details wie die Benutzer-ID oder den Pfad zum Home-Verzeichnis des betreffenden Benutzers anpassen.
   Wenn Sie das Home-Verzeichnis eines bestehenden Benutzers an einen anderen Ort verschieben müssen, geben Sie den Pfad des neuen Home-Verzeichnisses hier an und verschieben Sie den Inhalt des aktuellen Home-Verzeichnisses mithilfe von *An anderen Speicherort verschieben*. Anderenfalls wird ein neues Home-Verzeichnis ohne die bereits vorhandenen Daten erstellt.

7. Um zu erzwingen, dass die Benutzer ihr Passwort in regelmäßigen Abständen ändern, oder um andere Passwortoptionen festzulegen, wechseln Sie zu *Passworteinstellungen* und passen Sie die Optionen entsprechend an. Weitere Einzelheiten finden Sie unter *Abschnitt 6.3.2, „Erzwingen von Passwortrichtlinien“*.

8. Wenn Sie alle Optionen nach Ihren Wünschen festgelegt haben, klicken Sie auf *OK*.

9. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern. Ein neu hinzugefügter Benutzer kann sich nun mithilfe des von Ihnen erstellten Anmeldenamens und Passworts beim System anmelden.
   Sollen alle Änderungen gespeichert werden, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen, klicken Sie alternativ auf *Optionen für Experten* › *Änderungen jetzt schreiben*.

Warnung: Benennen Sie das `root`-Konto nicht um

Es ist zwar technisch möglich, das `root`-Konto umzubenennen, aber bestimmte Anwendungen, Skripte oder Produkte von Drittanbietern sind möglicherweise auf die Existenz eines Benutzers namens `root` angewiesen. Eine solche Konfiguration zielt zwar immer auf

individuelle Umgebungen ab, aber die notwendigen Anpassungen können durch Aktualisierungen des Herstellers überschrieben werden, sodass dies eine laufende Aufgabe und keine einmalige Einstellung ist. Dies trifft vor allem bei komplexen Konfigurationen mit Anwendungen von Drittanbietern zu, bei denen mit jedem beteiligten Anbieter abgeklärt werden muss, ob eine Umbenennung des `root`-Kontos unterstützt wird.

Da die Auswirkungen der Umbenennung des `root`-Kontos nicht vorhersehbar sind, unterstützt SUSE die Umbenennung des `root`-Kontos nicht.

In der Regel geht es bei der Umbenennung eines `root`-Kontos darum, es zu verbergen oder es unvorhersehbar zu machen. Für `/etc/passwd` sind jedoch `644` Berechtigungen für normale Benutzer erforderlich, sodass jeder Benutzer des Systems den Anmeldenamen für die Benutzer-ID 0 abrufen kann. Bessere Methoden zur Absicherung des `root`-Kontos finden Sie in *Buch „Security and Hardening Guide“, Kapitel 14 „User management“, Abschnitt 14.5 „Restricting* `root` *logins“* und *Buch „Security and Hardening Guide“, Kapitel 14 „User management“, Abschnitt 14.5.3 „Restricting SSH logins“*.

Tipp: Zuordnung von Benutzer-IDs

Die (lokale) Benutzer-ID sollte der ID im Netzwerk zugeordnet werden. Binden Sie beispielsweise einen neuen (lokalen) Benutzer auf einem Laptop mit derselben Benutzer-ID in eine Netzwerkumgebung ein. Dadurch wird gewährleistet, dass die Eigentümerschaft an den Dateien, die der Benutzer „offline“ erstellt, dieselbe ist wie bei der Erstellung der Dateien direkt im Netzwerk.

VORGEHEN 6.2: DEAKTIVIEREN ODER LÖSCHEN VON BENUTZERKONTEN

1. Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen*, und klicken Sie dort auf *Benutzer*.

2. Um ein Benutzerkonto vorübergehend zu deaktivieren, ohne es zu löschen, wählen Sie es in der Liste aus und klicken Sie auf *Bearbeiten*. Wählen Sie *Benutzernamen deaktivieren* aus. Der Benutzer kann sich erst wieder an Ihrem Rechner anmelden, wenn Sie das Konto erneut aktiviert haben.

3. Um ein Benutzerkonto zu löschen, wählen Sie den Benutzer in der Liste aus und klicken Sie auf *Löschen*. Wählen Sie aus, ob auch das Home-Verzeichnis des betreffenden Benutzers gelöscht werden soll oder ob die Daten beibehalten werden sollen.

6.3 Weitere Optionen für Benutzerkonten

Neben den Einstellungen für Standard-Benutzerkonten bietet SUSE® Linux Enterprise Desktop noch weitere Optionen. Dies sind beispielsweise Optionen, mit denen Sie Passwortrichtlinien durchsetzen, verschlüsselte Home-Verzeichnisse verwenden oder Festplattenquoten für Benutzer und Gruppen festlegen.

6.3.1 Automatische Anmeldung und Anmeldung ohne Passwort

Wenn Sie in der GNOME-Desktop-Umgebung arbeiten, können Sie die *Automatische Anmeldung* für einen bestimmten Benutzer sowie die *Anmeldung ohne Passwort* für sämtliche Benutzer konfigurieren. Mit der Option für die automatische Anmeldung wird ein Benutzer beim Booten automatisch in der Desktop-Umgebung angemeldet. Diese Funktion kann nur für jeweils einen Benutzer aktiviert werden. Mit der Option für die Anmeldung ohne Passwort können sich sämtliche Benutzer beim System anmelden, nachdem sie ihren Benutzernamen im Anmeldemanager eingegeben haben.

Warnung: Sicherheitsrisiko

Die Aktivierung der *Automatischen Anmeldung* bzw. der *Anmeldung ohne Passwort* ist auf einem Computer, zu dem mehrere Personen Zugang haben, ein Sicherheitsrisiko. Wenn keine Authentifizierung erforderlich ist, erhält jeder Benutzer Zugriff auf Ihr System und Ihre Daten. Verwenden Sie diese Funktion nicht, wenn Ihr System vertrauliche Daten enthält.

Zur Aktivierung der automatischen Anmeldung oder der Anmeldung ohne Passwort greifen Sie auf diese Funktionen in der *Verwaltung von Benutzern und Gruppen* von YaST über *Optionen für Experten* › *Einstellungen für das Anmelden* zu.

6.3.2 Erzwingen von Passwortrichtlinien

Bei einem System mit mehreren Benutzern ist es ratsam, mindestens grundlegende Sicherheitsrichtlinien für Passwörter zu erzwingen. Die Benutzer sollten ihre Passwörter regelmäßig ändern und starke Passwörter verwenden, die nicht so leicht herausgefunden werden können. Gehen Sie bei lokalen Benutzern wie folgt vor:

VORGEHEN 6.3: KONFIGURIEREN VON PASSWORTEINSTELLUNGEN

1. Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen*, und klicken Sie dort auf den Karteireiter *Benutzer*.
2. Wählen Sie den Benutzer aus und klicken Sie auf *Bearbeiten*.
3. Öffnen Sie die Registerkarte *Passworteinstellungen*. Die letzte Passwortänderung des Benutzers wird auf der Registerkarte angezeigt.
4. Aktivieren Sie *Passwortänderung erzwingen*, um zu erzwingen, dass der Benutzer sein Passwort bei der nächsten Anmeldung ändert.
5. Legen Sie zur Erzwingung einer regelmäßigen Passwortänderung eine *Maximale Anzahl von Tagen für das gleiche Passwort* und eine *Minimale Anzahl von Tagen für das gleiche Passwort* fest.
6. Legen Sie unter *Tage vor Ablauf des Passworts warnen* eine bestimmte Anzahl von Tagen fest, um den Benutzer vor Ablauf seines Passworts an die Passwortänderung zu erinnern.
7. Legen Sie unter *Tage nach Ablauf des Passworts Anmeldevorgang möglich* eine bestimmte Anzahl von Tagen fest, um den Zeitraum einzuschränken, innerhalb dessen sich der Benutzer trotz abgelaufenem Passwort anmelden kann.
8. Sie können auch ein bestimmtes Ablaufdatum für das gesamte Konto festlegen. Das *Ablaufdatum* muss im Format `YYYY-MM-DD` eingegeben werden. Diese Einstellung hängt nicht mit dem Passwort zusammen, sondern gilt für das Konto selbst.
9. Weitere Informationen zu den Optionen und den Standardwerten erhalten Sie über die Schaltfläche *Hilfe*.
10. Übernehmen Sie die Änderungen mit *OK*.

6.3.3 Verwalten von Quoten

Um zu verhindern, dass die Systemkapazität ohne Benachrichtigung zur Neige geht, können Systemadministratoren Quoten für Benutzer oder Gruppen einrichten. Quoten können für ein oder mehrere Dateisysteme definiert werden und beschränken den Speicherplatz, der verwendet werden kann, sowie die Anzahl der Inodes (Index-Knoten), die hier erstellt werden können. Inodes sind Datenstrukturen eines Dateisystems, die grundlegende Informationen über normale Datei-, Verzeichnis- oder andere Dateisystemobjekte speichern. Sie speichern alle Attribute eines Dateisystemobjekts (z. B. Eigentümer des Objekts und Berechtigungen wie Lesen, Schreiben oder Ausführen), mit Ausnahme des Dateinamens und des Dateiinhalts.

SUSE Linux Enterprise Desktop ermöglicht die Verwendung von `soft`- und `hard`-Quoten. Zusätzlich können Kulanzintervalle definiert werden, damit Benutzer oder Gruppen ihre Quoten vorübergehend um bestimmte Werte überschreiten können.

Softlimit

Definiert eine Warnstufe, bei dem die Benutzer informiert werden, sobald sie sich ihrer Grenze nähern. Die Administratoren können die Benutzer auffordern, die Partition zu bereinigen und die Datenmenge auf der Partition zu vermindern. Der Wert für ein Softlimit ist in der Regel niedriger als der Wert für ein Hardlimit.

Hardlimit

Definiert die Grenze, ab der Schreibanforderungen verweigert werden. Sobald das Hardlimit erreicht wird, können keine Daten mehr gespeichert werden und Anwendungen können unter Umständen abstürzen.

Kulanzzeitraum

Definiert den Zeitraum zwischen dem Überschreiten des Softlimits und der Ausgabe der Warnmeldung. In der Regel ein relativ niedriger Wert von einer oder mehreren Stunden.

VORGEHEN 6.4: AKTIVIEREN DER QUOTENUNTERSTÜTZUNG FÜR EINE PARTITION

Wenn Sie Quoten für bestimmte Benutzer und Gruppen konfigurieren möchten, müssen Sie zunächst in YaST im Dialogfeld „Festplatte vorbereiten: Expertenmodus“ die Quotenunterstützung für die entsprechende Partition aktivieren.

1. Wählen Sie in YaST die Optionsfolge *System* › *Partitionieren*, und klicken Sie dann auf *Ja*, um fortzufahren.
2. Wählen Sie unter *Festplatte vorbereiten: Expertenmodus* die Partition, für die Sie Quoten aktivieren möchten, und klicken Sie dann auf *Bearbeiten*.

3. Klicken Sie auf *Optionen für Fstab* und aktivieren Sie *Kontingentunterstützung (Quota) aktivieren*. Falls das Paket `quota` noch nicht installiert ist, wird es automatisch installiert, sobald Sie die entsprechende Meldung mit *Ja* bestätigen.

4. Bestätigen Sie Ihre Änderungen und beenden Sie *Festplatte vorbereiten: Expertenmodus*.

5. Vergewissern Sie sich, dass der Dienst `quotaon` ausgeführt wird, indem Sie den folgenden Befehl ausführen:

   ```
   > sudo systemctl status quotaon.service
   ```

   Er sollte als `active` gekennzeichnet sein. Wenn dies nicht der Fall ist, starten Sie ihn mit dem Befehl **`systemctl start quotaon.service`**.

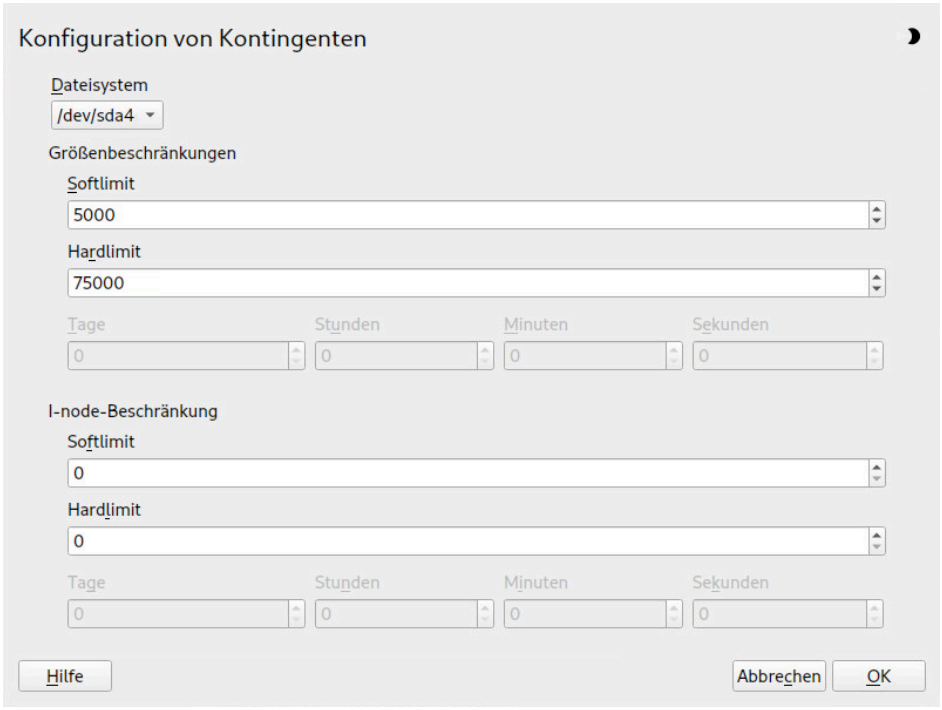
VORGEHEN 6.5: EINRICHTEN VON QUOTEN FÜR BENUTZER ODER GRUPPEN

Nun können Sie für spezifische Benutzer oder Gruppen Soft- bzw. Hardquoten definieren und Zeiträume als Kulanzintervalle festlegen.

1. Wählen Sie in YaST im Dialogfeld *Verwaltung von Benutzern und Gruppen* den Benutzer bzw. die Gruppe aus, für den/die Sie Quoten festlegen möchten, und klicken Sie dann auf *Bearbeiten*.

2. Wählen Sie auf dem Karteireiter *Plugins* den Eintrag *Konfiguration der Benutzerquote* aus und klicken Sie dann auf *Aufrufen*, um das Dialogfeld *Konfiguration von Kontingenten* zu öffnen.

3. Wählen Sie unter *Dateisystem* die Partition aus, auf die die Quote angewendet werden soll.



4. Beschränken Sie im Bereich *Größenbeschränkungen* den Speicherplatz. Geben Sie die Anzahl der 1-KB-Blöcke an, über die der Benutzer bzw. die Gruppe auf dieser Partition verfügen kann. Geben Sie einen Wert für *Softlimit* und einen für *Hardlimit* an.

5. Zudem können Sie die Anzahl der Inodes beschränken, über die der Benutzer bzw. die Gruppe auf der Partition verfügen kann. Geben Sie im Bereich für die *Inodes-Limits* ein *Softlimit* und ein *Hardlimit* ein.

6. Kulanzintervalle können nur definiert werden, wenn der Benutzer bzw. die Gruppe das für die Größe bzw. die Inodes festgelegte Softlimit bereits überschritten hat. Anderenfalls sind die zeitbezogenen Textfelder nicht aktiviert. Geben Sie den Zeitraum an, für den der Benutzer bzw. die Gruppe die oben festgelegten Limits überschreiten darf.

7. Bestätigen Sie die Einstellungen mit *OK*.

8. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern.
   Sollen alle Änderungen gespeichert werden, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen, klicken Sie alternativ auf *Optionen für Experten* › *Änderungen jetzt schreiben*.

SUSE Linux Enterprise Desktop umfasst auch Kommandozeilen-Tools wie `repquota` oder `warnquota`. Die Systemadministratoren können mit diesen Tools die Festplattennutzung steuern oder Email-Benachrichtigungen an Benutzer senden, die ihre Quote überschritten haben. Mit **`quota_nld`** können Administratoren auch Kernel-Meldungen über überschrittene Speicherquoten an D-BUS weiterleiten. Weitere Informationen finden Sie auf der Manpage für `repquota`, `warnquota` und **`quota_nld`**.

6.4 Ändern der Standardeinstellungen für lokale Benutzer

Beim Erstellen von neuen lokalen Benutzern werden von YaST verschiedene Standardeinstellungen verwendet. Zu diesen Einstellungen zählen unter anderem die Gruppe des Benutzers oder die Zugriffsberechtigungen für das Home-Verzeichnis des Benutzers. Sie können diese Standardeinstellungen entsprechend Ihren Anforderungen ändern:

1. Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen*, und klicken Sie dort auf den Karteireiter *Standardeinstellungen für neue Benutzer*.
2. Zur Änderung der Gruppe, der neue Benutzer automatisch angehören sollen, wählen Sie unter *Standardgruppe* eine andere Gruppe aus.
3. Wenn Sie als Standardpfad für das Home-Verzeichnis neuer Benutzer nicht `/home/USERNAME` verwenden möchten, ändern Sie den Eintrag unter *Pfadpräfix für Home-Verzeichnis*.
4. Wenn Sie die Standardberechtigungsmodi für neu erstellte Home-Verzeichnisse ändern möchten, ändern Sie den umask-Wert unter *Umask für Home-Verzeichnis*. Weitere Informationen zu 'umask' finden Sie unter *Buch „Security and Hardening Guide“, Kapitel 19 „Access control lists in Linux“* sowie auf der Manpage für **`umask`**.
5. Informationen zu den einzelnen Optionen erhalten Sie über die Schaltfläche *Hilfe*.
6. Übernehmen Sie die Änderungen mit *OK*.

6.5 Zuweisen von Benutzern zu Gruppen

Lokale Benutzer werden mehreren Gruppen zugewiesen. Diese Zuweisung erfolgt gemäß den Standardeinstellungen, die Sie über das Dialogfeld *Verwaltung von Benutzern und Gruppen* auf dem Karteireiter *Standardeinstellungen für neue Benutzer* aufrufen können. Im nächsten Abschnitt

erfahren Sie, wie Sie die Gruppenzuweisung eines einzelnen Benutzers ändern. Informationen zur Änderung der Standardgruppenzuweisung für neue Benutzer erhalten Sie unter *Abschnitt 6.4, „Ändern der Standardeinstellungen für lokale Benutzer“*.

VORGEHEN 6.6: ÄNDERN DER GRUPPENZUWEISUNG EINES BENUTZERS

1. Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen*, und klicken Sie dort auf *Benutzer*. Dort werden Benutzer und die Gruppen aufgelistet, denen sie angehören.
2. Klicken Sie auf *Bearbeiten* und wechseln Sie zum Karteireiter *Details*.
3. Um die Gruppe zu ändern, zu der der Benutzer gehört, klicken Sie auf *Standardgruppe* und wählen Sie die betreffende Gruppe in der Liste aus.
4. Um den Benutzer zusätzlichen sekundären Gruppen zuzuweisen, aktivieren Sie die zugehörigen Kontrollkästchen in der Liste *Zusätzliche Gruppen*.
5. Klicken Sie zum Anwenden der Änderungen auf *OK*.
6. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern.
   Sollen alle Änderungen gespeichert werden, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen, klicken Sie alternativ auf *Optionen für Experten* › *Änderungen jetzt schreiben*.

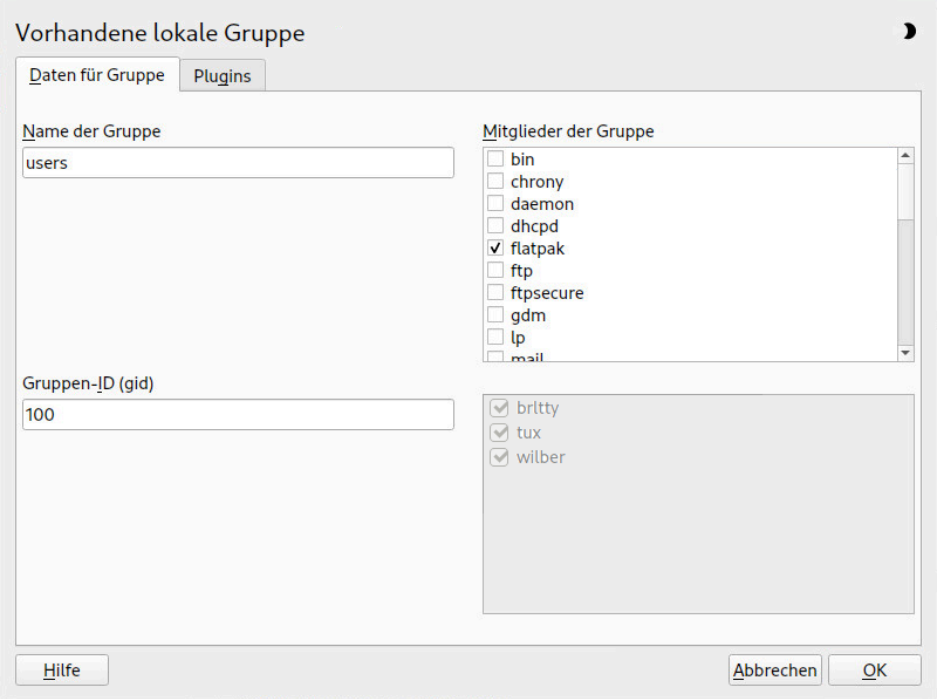
6.6 Gruppen verwalten

Mit YaST können Sie schnell und einfach Gruppen hinzufügen, bearbeiten und löschen.

VORGEHEN 6.7: ERSTELLEN UND BEARBEITEN VON GRUPPEN

1. Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen*, und klicken Sie dort auf den Karteireiter *Gruppen*.
2. Definieren Sie mithilfe von *Filter festlegen* die Menge der Gruppen, die Sie verwalten möchten. Im Dialogfeld werden die Gruppen im System aufgelistet.
3. Um eine neue Gruppe zu erstellen, klicken Sie auf *Hinzufügen*.
4. Um eine vorhandene Gruppe zu ändern, wählen Sie sie aus und klicken Sie dann auf *Bearbeiten*.

5. Geben Sie im folgenden Dialogfeld die Daten ein bzw. ändern Sie sie. Die Liste auf der rechten Seite zeigt einen Überblick aller verfügbaren Benutzer und Systembenutzer, die Mitglieder der Gruppe sein können.



6. Wenn Sie vorhandene Benutzer einer neuen Gruppe hinzufügen möchten, wählen Sie sie in der Liste der möglichen *Gruppenmitglieder* aus, indem Sie das entsprechende Kontrollkästchen aktivieren. Wenn Sie sie aus der Gruppe entfernen möchten, deaktivieren Sie das Kontrollkästchen.

7. Klicken Sie zum Anwenden der Änderungen auf *OK*.

8. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern.
   Sollen alle Änderungen gespeichert werden, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen, klicken Sie alternativ auf *Optionen für Experten* › *Änderungen jetzt schreiben*.

Es können nur Gruppen gelöscht werden, die keine Gruppenmitglieder enthalten. Um eine Gruppe zu löschen, wählen Sie sie in der Liste aus und klicken Sie auf *Löschen*. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen und die Änderungen zu speichern. Sollen alle Änderungen gespeichert werden, ohne das Dialogfeld *Verwaltung von Benutzern und Gruppen* zu schließen, klicken Sie alternativ auf *Optionen für Experten* › *Änderungen jetzt schreiben*.

6.7 Ändern der Methode zur Benutzerauthentifizierung

Wenn Ihr Computer an ein Netzwerk angeschlossen ist, können Sie die Authentifizierungsmethode ändern. Folgende Optionen sind verfügbar:

NIS

Die Benutzer werden zentral auf einem NIS-Server für alle Systeme im Netzwerk verwaltet. Weitere Informationen finden Sie im *Buch „Security and Hardening Guide“, Kapitel 3 „Using NIS“*.

SSSD

Der *System Security Services Daemon* (SSSD) kann Benutzerdaten lokal im Cache speichern und den Benutzern den Zugriff auf diese Daten ermöglichen, selbst wenn der eigentliche Verzeichnisdienst (vorübergehend) nicht erreichbar ist. Weitere Informationen finden Sie im *Buch „Security and Hardening Guide“, Kapitel 4 „Setting up authentication clients using YaST“, Abschnitt 4.2 „SSSD“*.

Samba

Die SMB-Authentifizierung wird häufig in heterogenen Linux- und Windows-Netzwerken verwendet. Weitere Informationen finden Sie im *Buch „Security and Hardening Guide“, Kapitel 7 „Active Directory support“*.

Gehen Sie wie folgt vor, um die Authentifizierungsmethode zu ändern:

1. Öffnen Sie in YaST das Dialogfeld *Verwaltung von Benutzern und Gruppen*.
2. Klicken Sie auf den Karteireiter *Einstellungen für Authentifizierung*, um eine Übersicht über die verfügbaren Authentifizierungsmethoden und die aktuellen Einstellungen anzuzeigen.
3. Wenn Sie die Authentifizierungsmethode ändern möchten, klicken Sie auf *Konfigurieren* und wählen Sie die Authentifizierungsmethode aus, die Sie bearbeiten möchten. Damit werden die YaST-Module zur Client-Konfiguration aufgerufen. Informationen zur Konfiguration des entsprechenden Client finden Sie in folgenden Abschnitten:

   NIS: *Buch „Security and Hardening Guide“, Kapitel 3 „Using NIS“, Abschnitt 3.2 „Configuring NIS clients“*

   LDAP: *Buch „Security and Hardening Guide“, Kapitel 4 „Setting up authentication clients using YaST“, Abschnitt 4.1 „Configuring an authentication client with YaST“*

SSSD: *Buch „Security and Hardening Guide“, Kapitel 4 „Setting up authentication clients using YaST“, Abschnitt 4.2 „SSSD“*

4. Kehren Sie nach der Übernahme der Konfiguration zum Überblick unter *Verwaltung von Benutzern und Gruppen* zurück.

5. Klicken Sie auf *OK*, um das Verwaltungsdialogfeld zu schließen.

6.8 Standard-Systembenutzer

SUSE Linux Enterprise Desktop legt standardmäßig Benutzernamen an, die nicht gelöscht werden können. Diese Benutzer sind in der Regel in der Linux Standard Base definiert (siehe https://refspecs.linuxfoundation.org/lsb.shtml ↗). Die folgende Liste zeigt die gängigen Benutzernamen und ihren Zweck:

STANDARDMÄßIG INSTALLIERTE GÄNGIGE BENUTZERNAMEN

`bin`,
`daemon`
: Legacy-Benutzer zur Kompatibilität mit älteren Anwendungen. Neue Anwendungen sollten diesen Benutzernamen nicht mehr verwenden.

`gdm`
: Verwendung im GNOME Display Manager (GDM) zur Bereitstellung grafischer Anmeldungen und zur Verwaltung von lokalen Displays und Ferndisplays.

`lp`
: Verwendung durch den Printer-Daemon für das Common Unix Printing System (CUPS).

`mail`
: Reservierter Benutzer für Mailerprogramme wie **`sendmail`** oder **`postfix`**.

`man`
: Verwendung durch man für den Zugriff auf man-Seiten.

`messagebus`
: Für den Zugriff auf den D-Bus (Desktop-Bus), einen Software-Bus für die prozessübergreifende Kommunikation. Der Daemon lautet `dbus-daemon`.

`nobody`
: Benutzer, der keine Dateien besitzt und keinen Gruppen mit Berechtigungen angehört. Wird mittlerweile nur noch bedingt eingesetzt, da Linux Standard Base ein separates Benutzerkonto für die einzelnen Daemons empfiehlt.

`nscd`
: Verwendung durch den Name Service Caching Daemon. Dieser Daemon fungiert als Look-up-Dienst und steigert die NIS- und LDAP-Leistung. Der Daemon lautet `nscd`.

`polkitd`
: Verwendung durch das PolicyKit Authorization Framework, mit dem Autorisierungsanforderungen für Prozesse ohne Berechtigungen definiert und verarbeitet werden. Der Daemon lautet `polkitd`.

`postfix`
: Verwendung durch den Postfix-Mailer.

`pulse`
: Verwendung durch den Pulseaudio-Soundserver.

`root`
: Verwendung durch den Systemadministrator. Bietet alle entsprechenden Berechtigungen.

`rpc`
: Verwendung durch den Befehl **`rpcbind`**, einem RPC-Port-Mapper.

`rtkit`
: Verwendung durch das Paket `rtkit` als D-Bus-Systemdienst für den Echtzeit-Planungsmodus.

`salt`
: Benutzer für die parallele Fernausführung durch Salt. Der Daemon lautet `salt-master`.

`scard`
: Benutzer für die Kommunikation mit Smartcards und Lesegeräten. Der Daemon lautet `pcscd`.

`srvGeoClue`
: Verwendung durch den GeoClue D-Bus-Dienst zur Bereitstellung von Standortinformationen.

`sshd`

Verwendung durch den Secure Shell-Daemon (SSH) für die sichere und verschlüsselte Kommunikation über ein unsicheres Netzwerk.

`statd`

Verwendung durch das Network Status Monitor-Protokoll (NSM), das im Daemon `rpc.statd` implementiert ist und zur Überwachung auf Reboot-Benachrichtigungen dient.

`systemd-coredump`

Wird vom Befehl **`/usr/lib/systemd/systemd-coredump`** zum Abrufen, Speichern und Verarbeiten von Kernel-Dumps verwendet.

`systemd-timesync`

Verwendung durch den Befehl **`/usr/lib/systemd/systemd-timesyncd`** zur Synchronisierung der lokalen Systemuhr mit einem entfernten Network Time Protocol (NTP)-Server.

6.9 Standard-Systemgruppen

Standardmäßig erstellt SLE mehrere Benutzergruppen, die von Systemdiensten verwendet werden. In der folgenden Liste werden Beispiele für erforderliche und häufige optionale Gruppen beschrieben.

`root`

Administrative Gruppe mit allen Berechtigungen.

`bin`

Zur Kompatibilität mit älteren Anwendungen enthalten. Neue Anwendungen sollten diese Gruppe nicht verwenden.

`daemon`

Wurde zuvor verwendet, um den Zugriff von Daemons auf das System einzuschränken. Daemons sollten jetzt unter ihrer eigenen UID/GID ausgeführt werden, um sie voneinander zu trennen.

`audio`

Berechtigungen für Audiogeräte.

`gdm`

Berechtigungen für den GNOME Display Manager.

`chrony`
: Berechtigungen für den Zeitsynchronisierungsdienst.

`kvm`
: Berechtigungen für das QEMU-Maschinenemulator-Toolkit.

`libvirt`
: Berechtigungen für den Virtualisierungsstapel.

`lp`
: Berechtigungen für den Druckerbetrieb.

`mail`
: Berechtigungen für Email-Dienste.

`man`
: Spezifische Berechtigungen für Handbuchseiten und den Befehl **`man`**.

`sshd`
: Berechtigungen für den SSH-Kommunikationsprotokoll-Daemon.

7 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 in *Abschnitt 8.5, „Der GNOME Package Updater“*. Dieses Kapitel behandelt das alternative Tool für die Aktualisierung von Software-Paketen: die YaST-Online-Aktualisierung.

Die aktuellen Patches für SUSE® Linux Enterprise Desktop 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 Desktop noch nicht registriert haben, starten Sie die *Produktregistrierung* 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 *Abschnitt 8.4, „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 Abonnement abgelaufen ist. In der Regel umfasst SUSE Linux Enterprise Desktop 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// .

Anmerkung: Firewall-Einstellungen zum Erhalten von Aktualisierungen

Wenn sich Ihr System hinter einer Firewall befindet, die ausgehenden Datenverkehr blockiert, stellen Sie sicher, dass auf den Ports 80 und 443 Verbindungen zu `https://scc.suse.com/` und `https://updates.suse.com` zugelassen sind, damit Sie die Updates erhalten können. Weitere Informationen z. B. über IP-Adressen und die Konfiguration eines Proxy-Servers finden Sie in https://www.suse.com/support/kb/doc/?id=000021034 .

SUSE bietet Aktualisierungen mit verschiedenen Relevanzstufen:

Sicherheitsaktualisierungen

Beseitigen ernsthafte Sicherheitsrisiken und sollten stets installiert werden.

Empfohlene Aktualisierungen

Beseitigen Probleme, die Ihrem Rechner schaden können.

Optionale Aktualisierungen

Beseitigen nicht sicherheitsrelevante Probleme oder bieten Verbesserungen.

7.1 Das Dialogfeld „Online-Aktualisierung“

Zum Öffnen des Dialogfelds *Online-Aktualisierung* starten Sie YaST, und wählen Sie *Software* › *Online-Aktualisierung*. Alternativ starten Sie das Modul von der Befehlszeile aus mit dem Befehl **`yast2 online_update`**.

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

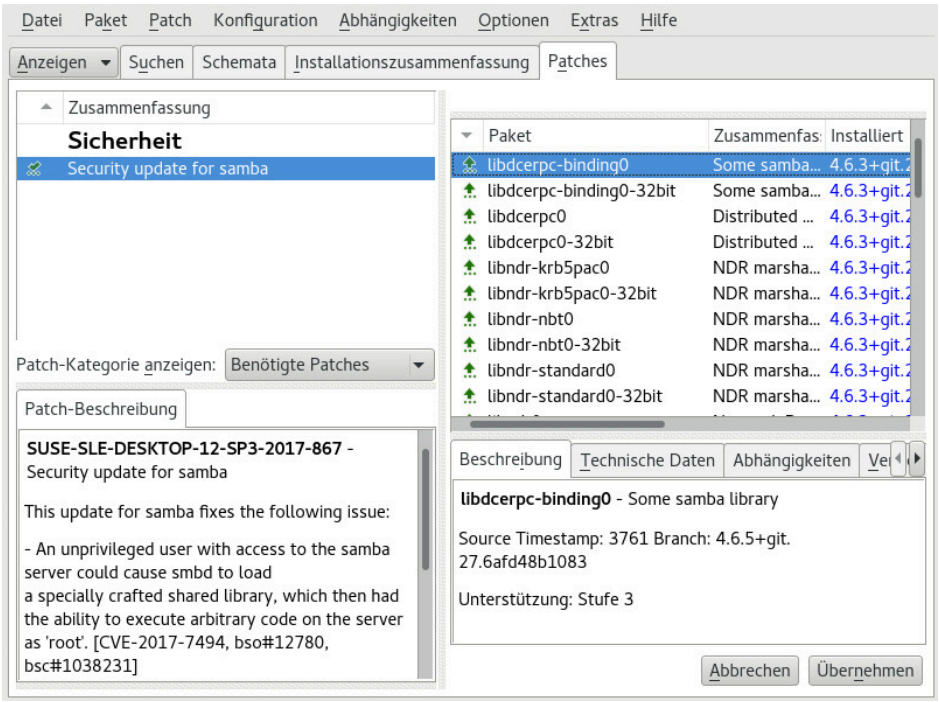


ABBILDUNG 7.1: YAST-ONLINE-AKTUALISIERUNG

Unter *Zusammenfassung* im linken Bereich werden die verfügbaren Patches für SUSE Linux Enterprise Desktop aufgeführt. Die Patches werden nach Sicherheitsrelevanz sortiert: `security`, `recommended` und `optional`. 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 Desktop.

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 `Security` und `Recommended` 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.

7.2 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 derzeit für Ihr System verfügbaren Patches (ausgenommen Patches, die als `optional` gekennzeichnet 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.

VORGEHEN 7.1: ANWENDEN VON PATCHES MIT DER YAST-ONLINE-AKTUALISIERUNG

1. Starten Sie YaST, und wählen Sie *Software* › *Online-Aktualisierung*.
2. Sollen alle neuen derzeit für Ihr System verfügbaren Patches (ausgenommen Patches, die als `optional` gekennzeichnet sind), automatisch angewendet werden, dann klicken Sie auf *Anwenden* oder *Übernehmen*.
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 7.1, „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 Sicherheitsaktualisierungen ohne Ausnahme

      Heben Sie die Auswahl der mit `security` gekennzeichneten 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 ein Paket in der 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.

7.3 Anzeigen von zurückgezogenen Patches

Wartungsaktualisierungen werden gründlich getestet, damit das Risiko, einen Fehler zu verursachen, auf ein Minimum reduziert wird. Wenn ein Patch tatsächlich einen Fehler enthält, wird er automatisch zurückgezogen. Es wird ein neues Update (mit einer höheren Versionsnummer) herausgegeben, um den fehlerhaften Patch rückgängig zu machen, und es wird verhindert, dass dieser erneut installiert wird. Auf dem Karteireiter *Paketklassifizierung* können Sie zurückgezogene Patches und deren Verlauf anzeigen.

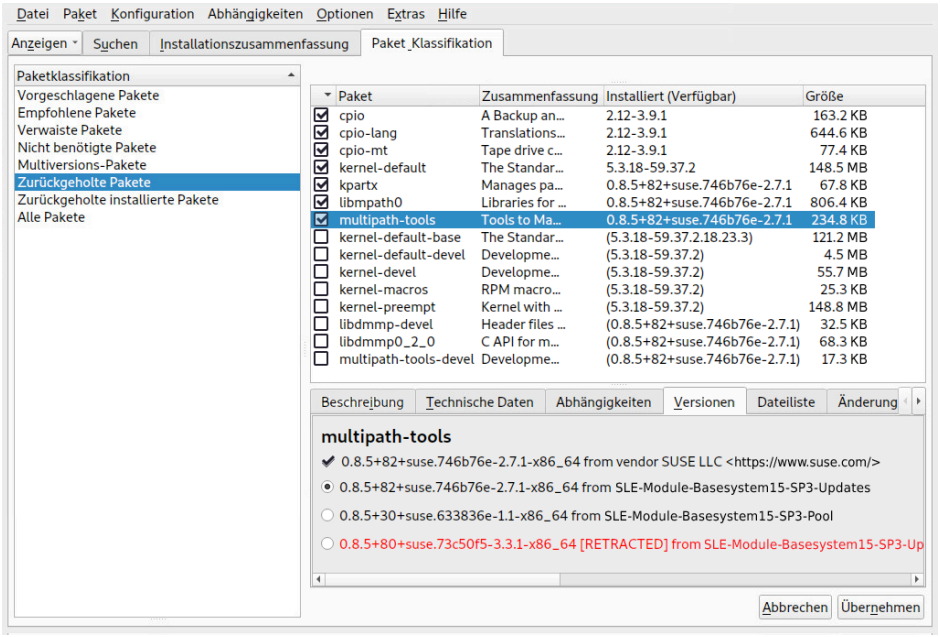


ABBILDUNG 7.2: ANZEIGEN VON ZURÜCKGEZOGENEN PATCHES UND DEREN VERLAUF

7.4 Automatische Online-Aktualisierungen

Bei YaST können Sie automatische Aktualisierungen mit täglichem, wöchentlichem oder monatlichem Zeitplan konfigurieren. Installieren Sie das Paket `yast2-online-update-configuration`.

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.

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

Auf dem Karteireiter *Patches* im YaST-*Software*-Modul finden Sie die verfügbaren und installierten Patches, einschließlich der Verweise auf Fehlerberichte und CVE-Bulletins.

VORGEHEN 7.2: KONFIGURIEREN DER AUTOMATISCHEN ONLINE-AKTUALISIERUNG

1. Nach der Installation starten Sie YaST und wählen Sie *Software* › *Online-Aktualisierung* aus. Wählen Sie *Konfiguration* › *Online-Aktualisierung*. Falls `yast2-online-update-configuration` nicht installiert ist, werden Sie dazu aufgefordert.

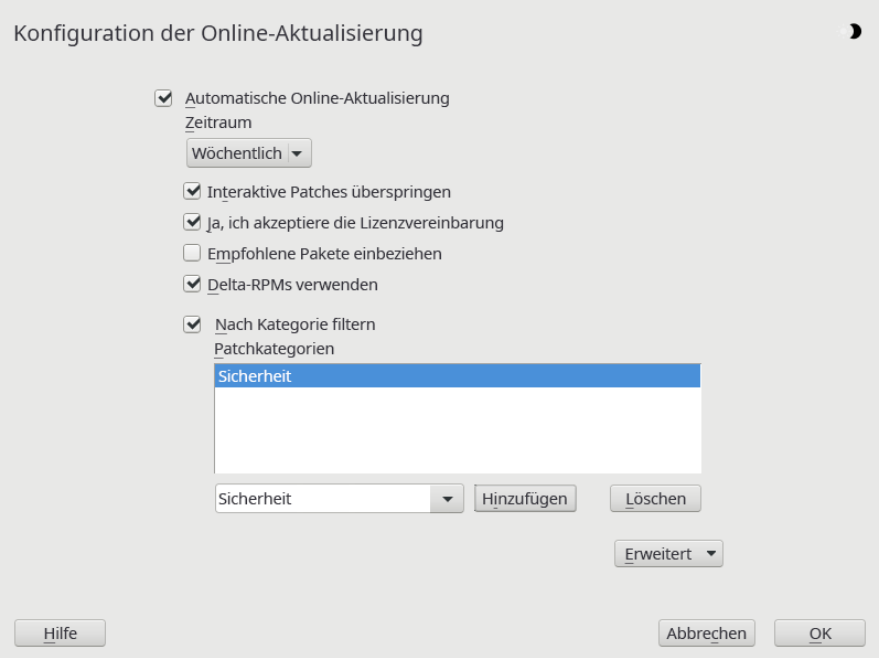


ABBILDUNG 7.3: KONFIGURATION DER YAST-ONLINE-AKTUALISIERUNG

   Sie können das Modul auch mit dem Befehl **`yast2 online_update_configuration`** von der Befehlszeile aus starten.

2. Legen Sie das Aktualisierungsintervall fest: *Täglich*, *Wöchentlich* oder *Monatlich*.

3. Bei manchen Patches ist möglicherweise das Eingreifen des Administrators erforderlich, beispielsweise wenn wichtige Services neu gestartet werden. Es könnte zum Beispiel eine Aktualisierung für Docker Open Source Engine sein, bei der alle Container neu gestartet

werden müssen. Vor der Installation dieser Patches wird der Benutzer über die Konsequenzen informiert und aufgefordert, die Installation des Patchs zu bestätigen. Derartige Patches werden als „Interaktive Patches“ bezeichnet.
Bei der automatischen Installation von Patches wird angenommen, dass Sie die Installation von interaktiven Patches akzeptiert haben. Wenn Sie diese Patches vor der Installation lieber prüfen möchten, aktivieren Sie das Kontrollkästchen für *Interaktive Patches überspringen*. In diesem Fall werden interaktive Patches beim automatischen Patching übersprungen. Stellen Sie sicher, dass Sie regelmäßig eine manuelle Online-Aktualisierung ausführen, um zu prüfen, ob interaktive Patches zur Installation bereitstehen.

4. Damit Lizenzvereinbarungen automatisch akzeptiert werden, aktivieren Sie die Option *Lizenzen zustimmen*.

5. Sollen alle Pakete automatisch installiert werden, die durch die aktualisierten Pakete empfohlen werden, aktivieren Sie *Empfohlene Pakete einbeziehen*.

6. Soll die Verwendung von Delta-RPMs (aus Leistungsgründen) deaktiviert werden, deaktivieren Sie *Delta-RPMs verwenden*.

7. Sollen die Patches nach Kategorie gefiltert werden (z. B. Sicherheits-Patches oder empfohlene Patches), aktivieren Sie das Kontrollkästchen für *Nach Kategorie filtern*, und fügen Sie die entsprechenden Patch-Kategorien aus der Liste hinzu. Es werden nur Patches aus den ausgewählten Kategorien installiert. Es hat sich bewährt, nur automatische *Sicherheit*-Aktualisierungen zu aktiveren und alle anderen manuell zu prüfen. Patches sind normalerweise zuverlässig, doch Sie sollten Nicht-Sicherheit-Patches testen und ein Rollback durchführen, wenn dabei Probleme auftreten.

   - In der Kategorie *Paketverwaltung und YaST* werden Patches für die Paketverwaltung sowie YaST-Funktionen und -Module zur Verfügung gestellt.
   - Patches der Kategorie *Sicherheit* enthalten wichtige Aktualisierungen und Fehlerkorrekturen.
   - Patches der Kategorie *Empfohlen* sind optionale Fehlerkorrekturen und Verbesserungen.
   - Die Kategorie *Optional* enthält neue Pakete.
   - Die Kategorie *Sonstige* entspricht der Kategorie „Verschiedenes“.
   - Die Kategorie *Dokument* wird nicht genutzt.

8. Bestätigen Sie Ihre Konfiguration durch Klicken auf *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.

8 Installieren bzw. Entfernen von Software

Mit dem Softwareverwaltungsmodul von YaST können Sie nach Softwarepaketen suchen und diese installieren und entfernen. Wenn Sie Pakete installieren, löst YaST automatisch alle Abhängigkeiten auf. Um Pakete zu installieren, die sich nicht auf dem Installationsmedium befinden, können Sie Software-Repositorys und YaST hinzufügen, um sie zu verwalten. Sie können Ihr System auch auf dem neuesten Stand halten, indem Sie Softwareaktualisierungen mit dem Aktualisierungs-Applet verwalten.

Der YaST-Software-Manager ermöglicht die Verwaltung von Softwarequellen auf Ihrem System. Es gibt zwei Versionen dieses YaST-Moduls: eine grafische Version für X Window und eine textbasierte Version für die Verwendung mit der Befehlszeile. Im Folgenden wird die grafische Variante beschrieben. Weitere Informationen zum textbasierten YaST finden Sie in *Kapitel 4, YaST im Textmodus*.

Anmerkung: Bestätigung und Überprüfung der Änderungen

Wenn Sie Pakete installieren, aktualisieren oder entfernen, treten alle Änderungen im Software-Manager nur dann in Kraft, wenn Sie auf *Akzeptieren* oder *Anwenden* klicken. YaST führt eine Liste mit allen Aktionen, so dass Sie Ihre Änderungen prüfen und bearbeiten können, bevor sie endgültig in das System übernommen werden.

8.1 Definition der Begriffe

Die folgenden Begriffe sind für die Vorgänge beim Installieren und Entfernen von Software in SUSE Linux Enterprise Desktop unerlässlich.

Repository

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

(Repository-)Alias/Repository-Name

Kurzname für ein Repository (in Zypper als `Alias` und in YaST als *Repository-Name* bezeichnet). Dieser Name kann vom Benutzer beim Hinzufügen eines Repositorys ausgewählt werden und muss eindeutig sein.

Repository-Beschreibungsdateien

Jedes Repository enthält Dateien mit einer Beschreibung des Repository-Inhalts (Paketnamen, Versionen usw.). Diese Repository-Beschreibungsdateien werden in einen lokalen Cache heruntergeladen, der von YaST genutzt wird.

Produkt

Bezeichnung für ein Produkt als Ganzes, z. B. SUSE® Linux Enterprise Desktop.

Muster

Ein Muster ist eine installierbare Gruppe von Paketen, die einem bestimmten Zweck dient. Das `Laptop`-Muster enthält beispielsweise alle Pakete, die in einer mobilen Rechnerumgebung benötigt werden. Die Muster definieren Paketabhängigkeiten (z. B. erforderliche oder empfohlene Pakete) und ein Teil der Pakete ist bereits für die Installation markiert. Damit ist sichergestellt, dass die wichtigsten Pakete für einen bestimmten Zweck auf dem System zur Verfügung stehen, sobald das Muster installiert wurde. Bei Bedarf können Sie Pakete in einem Schema manuell auswählen bzw. die Auswahl manuell aufheben.

Paket

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

Patch

Eine Programmdatei oder eine Zusammenstellung von Programmdateien, die von SUSE herausgegeben wird, um Fehler in SUSE-Produkten zu beseitigen. Ein Patch kann eine oder mehrere Dateien enthalten, die vorhandene ausführbare Dateien, Programme, Anwendungen oder Dokumente ersetzen oder verbessern.

Ein Patch enthält mindestens ein Paket und kann durch Delta-RPMs angewendet werden. Unter Umständen werden auch Abhängigkeiten zu Paketen aufgebaut, die noch nicht installiert wurden.

Auflösbares Objekt

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

Delta-RPM

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

Paketabhängigkeiten

Einige Pakete sind von anderen Paketen abhängig, wie zum Beispiel freigegebene Bibliotheken. Anders gesagt: Für ein bestimmtes Paket können andere Pakete erforderlich (`require`) sein. Falls diese erforderlichen Pakete nicht vorhanden sind, kann das Paket auch nicht installiert werden. Zusätzlich zu Abhängigkeiten (Paketanforderungen), die erfüllt sein müssen, empfehlen (`recommend`) einige Pakete andere Pakete. Diese empfohlenen Pakete werden nur dann installiert, wenn sie zur Verfügung stehen. Ansonsten werden sie ignoriert, und das Paket, das diese Pakete empfiehlt, wird dennoch problemlos installiert.

8.2 Registrieren eines installierten Systems

Wenn Sie die Registrierung bei der Installation übersprungen haben oder Ihr System erneut registrieren möchten, können Sie die Registrierung jederzeit durchführen. Verwenden Sie das YaST-Modul *Produktregistrierung* oder das Befehlszeilenwerkzeug **`SUSEConnect`**.

8.2.1 Registrieren mit YaST

Zum Registrieren des Systems starten Sie YaST und navigieren Sie zu *Software* und dann zu *Produktregistrierung*.

Standardmäßig wird das System beim SUSE Customer Center registriert. Wenn Ihr Unternehmen lokale Registrierungsserver bereitstellt, können Sie einen Server in der Liste der automatisch erkannten Server auswählen oder die URL manuell angeben.

8.2.2 Registrieren mit SUSEConnect

Mit dem folgenden Befehl nehmen Sie die Registrierung über die Befehlszeile vor:

```
> sudo SUSEConnect -r REGISTRATION_CODE -e EMAIL_ADDRESS
```

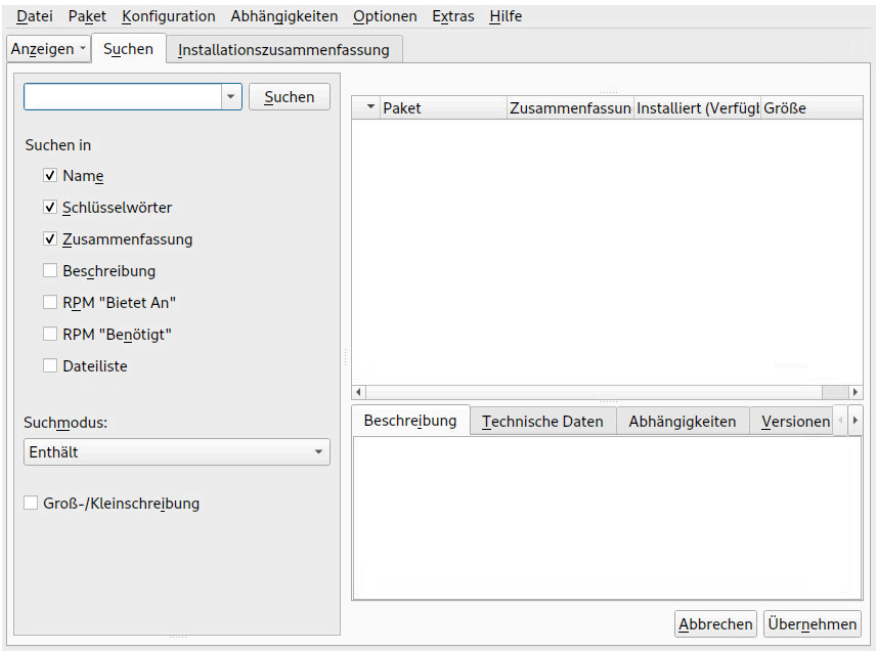
Ersetzen Sie *`REGISTRATION_CODE`* durch den Registrierungscode, den Sie mit Ihrer Version von SUSE Linux Enterprise Desktop erhalten haben. Ersetzen Sie *`EMAIL_ADDRESS`* durch die E-Mail-Adresse für das SUSE-Konto, mit dem Sie oder Ihr Unternehmen die Abonnements verwalten.

Soll die Registrierung über einen lokalen Registrierungsserver erfolgen, geben Sie auch die URL des Servers an:

```
> sudo SUSEConnect -r REGISTRATION_CODE -e EMAIL_ADDRESS --url "URL"
```

8.3 Verwenden des YaST-Software-Managers

Starten Sie den Software-Manager im *YaST-Kontrollzentrum* mit *Software › Software installieren oder löschen*.



8.3.1 Suche nach Software

Der YaST-Software-Manager kann Pakete oder Schemata aus allen aktuell aktivierten Repositorys installieren. Er bietet verschiedene Ansichten und Filter, damit Sie die gesuchte Software bequem finden können. Die Ansicht *Suchen* ist die Standardansicht für das Fenster. Zum Ändern der Ansicht klicken Sie auf *Ansicht*, und wählen Sie einen der nachstehenden Einträge im Dropdown-Feld aus. Die ausgewählte Ansicht wird in einer neuen Registerkarte geöffnet.

ANSICHTEN FÜR DIE SUCHE NACH PAKETEN ODER MUSTERN

Schemata

Listet alle verfügbaren Muster für die Installation auf Ihrem System auf.

Paketgruppen

Listet alle Pakete nach Gruppen sortiert auf, z. B. *Grafik*, *Programmierung* oder *Sicherheit*.

Sprachen

Filter zur Auflistung aller Pakete, die zum Hinzufügen einer neuen Systemsprache erforderlich sind.

Repositorys

Filter zur Auflistung von Paketen nach Repository. Halten Sie beim Klicken auf die Namen von Repositorys die `Strg` -Taste gedrückt, um mehrere Repositorys auszuwählen. Das „Pseudo-Repository“ *@System* listet alle derzeit installierten Pakete auf.

Services

Zeigt an, welche Pakete zu einem bestimmten Modul oder einer bestimmten Erweiterung gehören. Wählen Sie einen Eintrag aus (z. B. `Basesystem` oder `High Availability`), um eine Liste der Pakete anzuzeigen, die zu diesem Modul oder dieser Erweiterung gehören.

Suche

Ermöglicht die Suche nach einem Paket anhand von bestimmten Kriterien. Geben Sie einen Suchbegriff ein und drücken Sie `Eingabetaste` . Verfeinern Sie Ihre Suche, indem Sie einen Suchort in *Suchen in* angeben und den *Suchmodus* ändern. Wenn Sie beispielsweise den Namen des Pakets nicht kennen, sondern nur den Namen der gesuchten Anwendung, schließen Sie die *Beschreibung* des Pakets in den Suchvorgang ein.

Installationsüberblick

Wenn Sie bereits Pakete zur Installation, zur Aktualisierung oder zum Löschen ausgewählt haben, zeigt die Ansicht die Änderungen, die auf Ihr System angewendet werden, sobald Sie auf *Akzeptieren* klicken. Um in dieser Ansicht nach Paketen mit einem bestimmten Status zu filtern, aktivieren oder deaktivieren Sie die entsprechenden Kontrollkästchen. Drücken Sie `Umschalttaste` – `F1` , um Details zu den Statusflags zu erhalten.

Tipp: Suchen nach Paketen, die keinem aktiven Repository angehören

Um alle Pakete aufzulisten, die keinem aktiven Repository angehören, wählen Sie *Ansicht* › *Repositorys* › *@System* und anschließend *Sekundärer Filter* › *Nicht gepflegte Pakete*. Dies ist beispielsweise nützlich, wenn Sie ein Repository gelöscht haben und sicherstellen möchten, dass keine Pakete aus diesem Repository installiert bleiben.

Tipp: Online-Suche nach Software

Die Online-Suchfunktion ermöglicht die Suche nach Paketen in allen registrierten und nicht registrierten Modulen und Erweiterungen.

VORGEHEN 8.1: ONLINE-SUCHE NACH SOFTWARE

Führen Sie zur Online-Suche nach Software die folgenden Schritte aus:

1. Öffnen Sie das Online-Suchfenster mit *Extras* › *Online suchen*.
2. Geben Sie einen *Paketnamen* ein und drücken Sie `Eingabetaste` oder klicken Sie auf *Suchen*. YaST kontaktiert das SUSE-Kundencenter und zeigt die Ergebnisse in einer Tabelle an, einschließlich des Moduls oder der Erweiterung der einzelnen Pakete. Wählen Sie ein Paket aus, um weitere Details zu sehen.
3. Wählen Sie eines oder mehrere Pakete für die Installation aus, indem Sie auf die entsprechende Tabellenzeile klicken und *Auswahl umschalten* auswählen. Alternativ können Sie auch auf eine Zeile doppelklicken. Wenn das Paket zu einem nicht registrierten Modul oder einer Erweiterung gehört, fordert YaST Sie zur Bestätigung von dessen Registrierung auf.
4. Klicken Sie auf *Weiter*, überprüfen Sie die Änderungen und installieren Sie die Pakete.

8.3.2 Installieren und Entfernen von Paketen oder Mustern

Einige Pakete sind von anderen Paketen abhängig, wie zum Beispiel freigegebene Bibliotheken. Einige Pakete können nicht gleichzeitig nebeneinander auf einem System bestehen. Falls möglich, löst YaST diese Abhängigkeiten oder Konflikte automatisch auf. Wenn Ihre Wahl einen Abhängigkeitskonflikt verursacht, der nicht automatisch gelöst werden kann, müssen Sie diesen Konflikt manuell lösen, wie unter *Abschnitt 8.3.4, „Paketabhängigkeiten“* beschrieben.

Anmerkung: Entfernen von Paketen

Wenn Sie bestimmte Pakete löschen möchten, entfernt YaST standardmäßig nur die ausgewählten Pakete. Falls YaST auch alle anderen Pakete entfernen soll, die nach dem Löschen der angegebenen Pakete nicht mehr benötigt werden, wählen Sie im Hauptmenü den Eintrag *Optionen* › *Beim Löschen von Paketen bereinigen*.

1. Suchen Sie nach Paketen wie unter *Abschnitt 8.3.1, „Suche nach Software“* beschrieben.

2. Die gefundenen Pakete werden im rechten Fensterbereich aufgelistet. Klicken Sie zur Installation oder zum Entfernen eines Pakets mit der rechten Maustaste auf *Installieren* bzw. *Löschen*. Wenn die relevante Option nicht verfügbar ist, prüfen Sie den Paketstatus, den das Symbol vor dem Paketnamen angibt – drücken Sie `Umschalttaste` – `F1` , um Hilfe zu erhalten.

   #### Tipp: Anwenden einer Aktion auf alle aufgelisteten Pakete

   Wenn Sie eine Aktion auf alle im rechten Bereich aufgelisteten Pakete anwenden möchten, wechseln Sie zum Hauptmenü, und wählen Sie eine Aktion in *Paket* › *Alle in dieser Liste*.

3. Um ein Muster zu installieren, klicken Sie mit der rechten Maustaste auf den Namen des Musters und wählen Sie *Installieren*.

4. Es ist nicht möglich, ein Muster zu entfernen. Wählen Sie stattdessen die zu entfernenden Pakete für das Muster aus und markieren Sie diese Pakete zum Löschen.

5. Wiederholen Sie zur Auswahl weiterer Pakete die oben genannten Schritte.

6. Bevor Sie Ihre Änderungen übernehmen, können Sie sie überprüfen und bearbeiten. Klicken Sie hierzu auf *Ansicht* › *Installationsüberblick*. Standardmäßig werden alle Pakete aufgelistet, deren Status sich ändern wird.

7. Um den Status für ein Paket zurückzusetzen, klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie einen der folgenden Einträge aus: *Beibehalten*, falls das Paket zur Löschung oder Aktualisierung vorgesehen war, bzw. *Nicht installieren*, falls es zur Installation geplant war. Klicken Sie zum Verwerfen der Änderungen und zum Schließen des Software-Managers auf *Abbrechen* und *Verwerfen*.

8. Wenn Sie fertig sind, klicken Sie auf *Anwenden*, damit Ihre Änderungen übernommen werden.

9. Wenn YaST zusätzliche Abhängigkeiten findet, zeigt es eine Liste der entsprechenden Pakete an, die installiert, aktualisiert oder entfernt werden müssen. Klicken Sie auf *Weiter*, um sie zu akzeptieren.
   Wenn alle ausgewählten Pakete installiert, aktualisiert bzw. gelöscht sind, wird der YaST-Software-Manager automatisch beendet.

Anmerkung: Installation von Quellpaketen

Das Installieren von Quellpaketen mit dem YaST-Software-Manager ist zurzeit nicht möglich. Verwenden Sie zu diesem Zweck das Befehlszeilenwerkzeug **`zypper`**. Weitere Informationen finden Sie in *Abschnitt 9.1.3.5, „Installieren oder Herunterladen von Quellpaketen“*.

8.3.3 Aktualisieren von Paketen

Anstatt einzelne Pakete zu aktualisieren, können Sie auch alle installierten Pakete oder alle Pakete aus einem bestimmten Repository aktualisieren. Bei der Sammelaktualisierung von Paketen werden im Allgemeinen die folgenden Aspekte berücksichtigt:

- Prioritäten der Repositorys, aus denen das Paket stammt,
- Architektur des Pakets (z. B. AMD64/Intel 64),
- Versionsnummer des Pakets,
- Hersteller des Pakets.

Die Aspekte, die die Auswahl der Aktualisierungskandidaten am stärksten beeinflussen, sind abhängig von der jeweils ausgewählten Aktualisierungsoption.

1. Um alle installierten Pakete auf die jeweils aktuelle Version zu aktualisieren, wählen Sie im Hauptmenü die Option *Paket* › *Alle Pakete* › *Aktualisieren, wenn neuere Version verfügbar*. Alle Repositorys werden gemäß der folgenden Richtlinie nach möglichen Aktualisierungskandidaten durchsucht: YaST versucht zuerst die Suche auf Pakete zu begrenzen, die dieselbe Architektur und denselben Hersteller wie das installierte Paket aufweisen. Werden Pakete gefunden, wird daraus der „bestmögliche“ Aktualisierungskandidat gemäß dem nachstehenden Verfahren ausgewählt. Wird jedoch kein vergleichbares Paket desselben Herstellers gefunden, so wird die Suche auf alle Pakete mit derselben Architektur ausge-

weitet. Wenn immer noch kein vergleichbares Paket aufgefunden werden kann, werden alle Pakete betrachtet und der „bestmögliche“ Aktualisierungskandidat wird anhand der folgenden Kriterien ermittelt:

1. Repository-Priorität: Das Paket aus dem Repository mit der höchsten Priorität wird verwendet.

2. Wenn bei dieser Auswahl mehrere Pakete infrage kommen, wird das Paket mit der „bestmöglichen“ Architektur verwendet (bestmöglich: dieselbe Architektur wie beim installierten Paket).

Wenn das resultierende Paket eine höhere Versionsnummer aufweist als das installierte Paket, wird das installierte Paket aktualisiert und durch den ausgewählten Aktualisierungskandidaten ersetzt.
Bei dieser Option wird versucht, Änderungen an der Architektur und am Hersteller der installierten Pakete zu vermeiden; unter bestimmten Umständen werden diese Änderungen jedoch zugelassen.

Anmerkung: Bedingungslos aktualisieren

Wenn Sie stattdessen *Paket* › *Alle Pakete* › *Bedingungslos aktualisieren* verwenden, werden dieselben Kriterien angewendet, wobei der aufgefundene Paketkandidat bedingungslos aktualisiert wird. Die Auswahl dieser Option kann also zu einem Downgrade des Pakets führen.

2. Um sicherzustellen, dass die Pakete für eine Sammelaktualisierung aus einem bestimmten Repository stammen, gehen Sie wie folgt vor:

   a. Wählen Sie das Repository aus, von dem aus die Aktualisierung erfolgen soll, wie unter *Abschnitt 8.3.1, „Suche nach Software“* beschrieben.

   b. Klicken Sie auf der rechten Seite des Fensters auf *Systempakete auf die Versionen in diesem Repository umstellen*. Damit wird YaST explizit ermöglicht, den Paketanbieter beim Austauschen der Pakete zu wechseln.
   Sobald Sie auf *Akzeptieren* klicken, werden alle installierten Pakete durch Pakete aus diesem Repository ersetzt, sofern verfügbar. Dabei können der Hersteller und die Architektur wechseln, und unter Umständen wird sogar ein Downgrade für bestimmte Pakete durchgeführt.

c. Um dies zu vermeiden, klicken Sie auf *Umstellung der Systempakete auf die Versionen in diesem Repository abbrechen*. Sie können diesen Vorgang nur so lange abbrechen, bis Sie auf die Schaltfläche *Akzeptieren* geklickt haben.

3. Bevor Sie Ihre Änderungen übernehmen, können Sie sie überprüfen und bearbeiten. Klicken Sie hierzu auf *Ansicht* › *Installationsüberblick*. Standardmäßig werden alle Pakete aufgelistet, deren Status sich ändern wird.

4. Sobald alle Optionen gemäß Ihren Anforderungen festgelegt sind, bestätigen Sie Ihre Änderungen mit *Akzeptieren*. Die Sammelaktualisierung wird gestartet.

8.3.4 Paketabhängigkeiten

Die meisten Pakete hängen von anderen Paketen ab. Wenn ein Paket beispielsweise eine freigegebene Bibliothek verwendet, hängt es von dem Paket ab, das diese Bibliothek bereitstellt. Bestimmte Pakete können nicht gleichzeitig nebeneinander bestehen und verursachen einen Konflikt. (Sie können beispielsweise nur einen Mail Transfer Agent, Sendmail oder Postfix, installieren.) Beim Installieren oder Entfernen von Software stellt der Software-Manager sicher, dass keine Abhängigkeiten oder Konflikte ungelöst bleiben, um die Systemintegrität zu gewährleisten.

Falls es nur eine Lösung zur Behebung einer Abhängigkeit oder eines Konflikts gibt, erfolgt dies automatisch. Mehrere Lösungen verursachen immer einen Konflikt, der manuell gelöst werden muss. Wenn das Lösen eines Konflikts eine Hersteller- oder Architekturänderung erfordert, muss dieser ebenfalls manuell gelöst werden. Wenn Sie zum Übernehmen von Änderungen im Software-Manager auf *Übernehmen* klicken, erhalten Sie eine Übersicht über alle Aktionen, die vom automatischen Resolver ausgelöst wurden und die Sie bestätigen müssen.

Standardmäßig werden Abhängigkeiten automatisch geprüft. Eine Prüfung erfolgt jedes Mal, wenn Sie einen Paketstatus ändern (z. B. durch Markieren eines Pakets zum Installieren oder Löschen). Dies ist generell nützlich, kann jedoch beim manuellen Lösen eines Abhängigkeitskonflikts anstrengend werden. Zum Deaktivieren dieser Funktion wechseln Sie zum Hauptmenü, und deaktivieren Sie *Abhängigkeiten* › *Autom. überprüfen*. Führen Sie eine Abhängigkeitsprüfung manuell mit *Abhängigkeiten* › *Jetzt überprüfen* durch. Eine Konsistenzprüfung wird stets durchgeführt, wenn Sie die Auswahl mit *Übernehmen* bestätigen.

Um die Abhängigkeiten eines Pakets zu prüfen, klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie *Auflösungsinformation anzeigen*. Eine Darstellung der Abhängigkeiten wird geöffnet. Pakete, die bereits installiert sind, werden in einem grünen Rahmen angezeigt.

Anmerkung: Manuelle Auflösung von Paketkonflikten

Wenn Sie noch keine Erfahrung haben, folgen Sie den Vorschlägen von YaST bei der Behandlung von Paketkonflikten, sonst können Sie die Konflikte eventuell nicht lösen. Bedenken Sie, dass jede Änderung, die Sie vornehmen, andere Konflikte verursachen kann, d. h., Sie können ganz schnell einer stetig wachsenden Anzahl an Konflikten gegenüberstehen. Halten Sie in einem solchen Fall den Software-Manager über *Abbrechen* an. *Verwerfen* Sie alle Ihre Änderungen und beginnen Sie noch einmal von vorne.

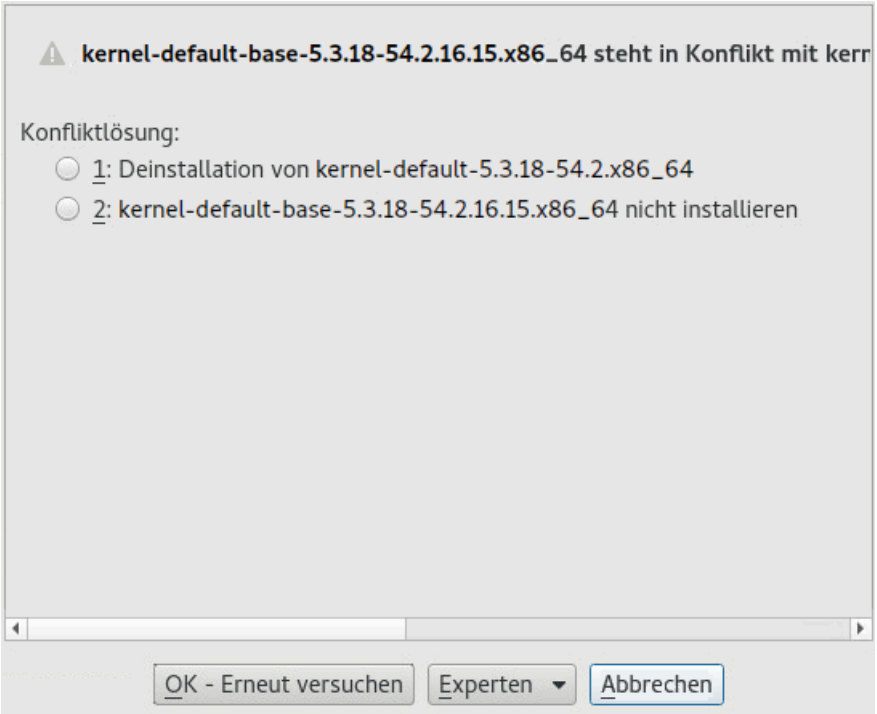


ABBILDUNG 8.1: KONFLIKTVERWALTUNG DES SOFTWARE-MANAGERS

8.3.5 Behandlung von Paketempfehlungen

Neben den starken Abhängigkeiten, die zum Ausführen eines Programms erforderlich sind (z. B. eine bestimmte Bibliothek), können für ein Paket auch schwache Abhängigkeiten gelten, die beispielsweise weitere Funktionen oder Transaktionen bieten. Diese schwachen Abhängigkeiten werden als „Paketempfehlungen“ bezeichnet.

Wenn ein neues Paket installiert wird, werden Paketempfehlungen weiterhin standardmäßig installiert. Bei der Aktualisierung eines vorhandenen Pakets werden fehlende Empfehlungen nicht automatisch installiert. Um dies zu ändern, legen Sie `PKGMGR_RECOMMENDED="yes"` in `/`

`etc/sysconfig/yast2` fest. Sollen alle fehlenden Empfehlungen für bereits installierte Pakete installiert werden, starten Sie *YaST* › *Software-Manager* und wählen Sie *Extras* › *Alle passenden empfohlenen Pakete installieren*.

Soll die Installation der empfohlenen Pakete beim Installieren neuer Pakete deaktiviert werden, deaktivieren Sie im YaST-Software-Manager die Option *Abhängigkeiten* › *Empfohlene Pakete installieren*. Wenn Sie die Pakete über das Befehlszeilenwerkzeug Zypper installieren, geben Sie die Option `--no-recommends.` an.

8.4 Verwalten von Software-Repositorys und -Diensten

Zum Installieren von Software von Drittanbietern nehmen Sie Software-Repositorys in das System auf. Standardmäßig werden Produkt-Repositorys wie SUSE Linux Enterprise Desktop-DVD 15 SP7 und das zugehörige Aktualisierungs-Repository automatisch konfiguriert, wenn Sie Ihr System registrieren. Weitere Informationen zur Registrierung finden Sie in *Buch „Installationshandbuch“, Kapitel 5 „Installationsschritte“, Abschnitt 5.6 „Registrierung“* oder *Buch „Upgradehandbuch“, Kapitel 4 „Offline-Upgrade“, Abschnitt 4.7 „Registrieren des Systems“*. Abhängig vom ursprünglich ausgewählten Produkt kann eventuell auch ein zusätzliches Repository mit Übersetzungen, Wörterbüchern usw. konfiguriert werden.

Zur Verwaltung der Repositorys starten Sie YaST, und wählen Sie *Software* › *Software-Repositorys*. Das Dialogfeld *Konfigurierte Software-Repositorys* wird geöffnet. Hier können Sie auch Abonnements für *Dienste* verwalten, indem Sie den Eintrag *Ansicht* oben rechts im Dialogfeld zu *Alle Dienste* ändern. Ein Dienst in diesem Kontext bezeichnet einen *Repository Index Service* (RIS), der ein oder mehrere Software-Repositorys anbieten kann. Ein solcher Dienst kann dynamisch von seinem Administrator oder Hersteller geändert werden.

Jedes Repository enthält Dateien mit einer Beschreibung des Repository-Inhalts (Paketnamen, Versionen usw.). YaST lädt diese Repository-Beschreibungsdateien in einen lokalen Cache herunter. Um deren Integrität sicherzustellen, können Software-Repositorys mit dem GPG-Schlüssel des Repository Maintainers signiert werden. Immer, wenn Sie ein neues Repository hinzufügen, bietet YaST die Möglichkeit, seinen Schlüssel zu importieren.

Warnung: Einstufen externer Softwarequellen als vertrauenswürdig

Vergewissern Sie sich vor dem Hinzufügen externer Software-Repositorys zu Ihrer Repository-Liste, dass das betreffende Repository vertrauenswürdig ist. SUSE trägt keine Verantwortung für Probleme, die durch die Installation von Software aus Software-Repositorys von Drittanbietern auftreten.

8.4.1 Hinzufügen von Software-Repositorys

Sie können Repositorys von DVD/CD, einem USB-Flash-Laufwerk, einem lokalen Verzeichnis, einem ISO-Image oder von einer Netzwerkquelle hinzufügen.

Zum Hinzufügen von Repositorys über das Dialogfeld *Konfigurierte Software-Repositorys* in YaST gehen Sie wie folgt vor:

1. Klicken Sie auf *Hinzufügen*.
2. Wählen Sie eine der Optionen im Dialogfeld:

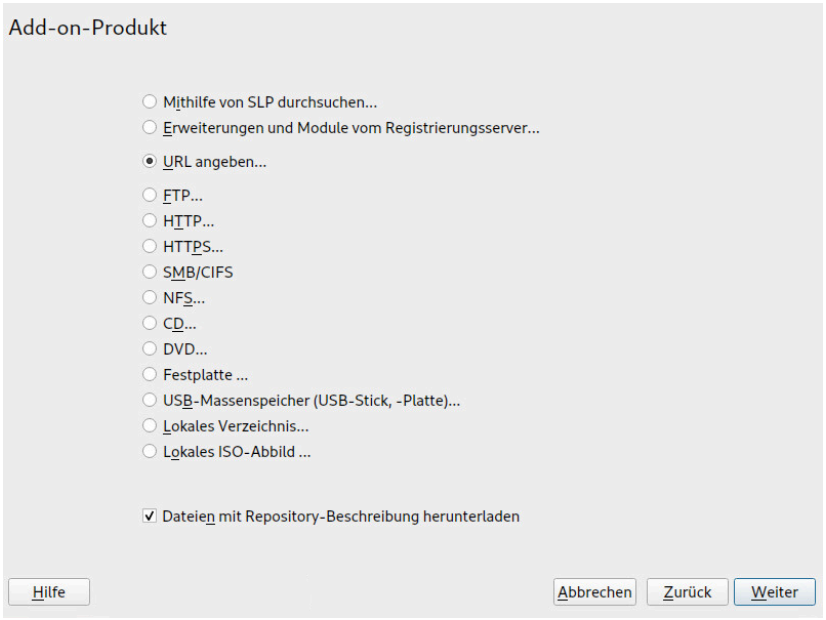


ABBILDUNG 8.2: HINZUFÜGEN EINES SOFTWARE-REPOSITORYS

- Durchsuchen Sie das Netzwerk nach Installationsservern, die ihre Services per SLP bekanntgeben. Wählen Sie hierzu *Mithilfe von SLP durchsuchen*, und klicken Sie auf *Weiter*.

- Um ein Repository von einem Wechsellaufwerk hinzuzufügen, wählen Sie die entsprechende Option aus und legen Sie das Medium ein bzw. schließen Sie das USB-Gerät an den Rechner an. Klicken Sie auf *Weiter*, um mit der Installation zu beginnen.

- Bei den meisten Repositorys werden Sie aufgefordert, den Pfad (oder die URL) des Mediums anzugeben, sobald Sie die entsprechende Option ausgewählt und auf *Weiter* geklickt haben. Die Angabe eines *Repository-Namens* ist optional. Wenn kein Name angegeben ist, verwendet YaST den Produktnamen oder die URL als Repository-Namen.

Die Option *Dateien mit Repository-Beschreibung herunterladen* ist standardmäßig aktiviert. Wenn Sie diese Option deaktivieren, lädt YaST die Dateien später bei Bedarf automatisch herunter.

3. Je nach hinzugefügtem Repository werden Sie aufgefordert, den GPG-Schlüssel des Repositorys zu importieren oder eine Lizenz zu akzeptieren.
   Nach dem Bestätigen beginnt YaST mit dem Herunterladen und Analysieren der Metadaten. Das Repository wird in die Liste *Konfigurierte Repositorys* aufgenommen.

4. Bei Bedarf bearbeiten Sie die *Eigenschaften* des Repositorys gemäß den Anweisungen in *Abschnitt 8.4.2, „Verwalten von Repository-Eigenschaften“*.

5. Bestätigen Sie Ihre Änderungen mit *OK*. Das Konfigurationsdialogfeld wird geschlossen.

6. Nachdem Sie das Repository erfolgreich hinzugefügt haben, wird der Software-Manager gestartet, und Sie können Pakete aus diesem Repository installieren. Detaillierte Informationen finden Sie in *Kapitel 8, Installieren bzw. Entfernen von Software*.

8.4.2 Verwalten von Repository-Eigenschaften

In der Übersicht *Konfigurierte Software-Repositorys* unter *Software-Repositorys* können Sie die folgenden Repository-Eigenschaften ändern:

Status

Der Repository-Status kann *Aktiviert* oder *Deaktiviert* lauten. Sie können nur Pakete von Repositorys installieren, die aktiviert sind. Soll ein Repository vorübergehend deaktiviert werden, wählen Sie das gewünschte Repository aus, und deaktivieren Sie die Option *Aktivieren*. Alternativ können Sie auf einen Repository-Namen doppelklicken und so den Status umschalten. Mit *Löschen* wird ein Repository vollständig gelöscht.

Aktualisieren

Bei der Aktualisierung eines Repositorys wird dessen Inhaltsbeschreibung (Paketnamen, Versionen usw.) in einen lokalen Cache heruntergeladen, der von YaST genutzt wird. Für statische Repositorys wie CDs oder DVDs genügt dies einmal, wohingegen Repositorys mit sich häufig änderndem Inhalt häufig aktualisiert werden sollten. Die einfachste Möglichkeit, einen Repository-Cache auf dem neuesten Stand zu halten, bietet die Option *Automatisch aktualisieren*. Zur manuellen Aktualisierung klicken Sie auf *Aktualisieren* und wählen Sie eine der Optionen.

Heruntergeladene Pakete nicht löschen

Pakete von entfernten Repositorys werden vor der Installation heruntergeladen. Standardmäßig werden sie bei einer erfolgreichen Installation gelöscht. Wenn Sie *Heruntergeladene Pakete nicht löschen* aktivieren, werden die heruntergeladenen Pakete beibehalten. Der Download-Speicherort wird in `/etc/zypp/zypp.conf` konfiguriert. Standardmäßig ist dies `/var/cache/zypp/packages`.

Priorität

Die *Priorität* eines Repositorys ist ein Wert zwischen `1` und `200`, wobei `1` die höchste und `200` die niedrigste Priorität bezeichnet. Alle mit YaST hinzugefügten Repositorys erhalten standardmäßig die Priorität `99`. Wenn Sie keinen bestimmten Prioritätswert für ein Repository festlegen möchten, können Sie auch den Wert `0` angeben. Das Repository erhält in diesem Fall die Standardpriorität (`99`). Wenn ein Paket in mehr als einem Repository vorhanden ist, hat das Repository mit der höchsten Priorität Vorrang. Damit können Sie vermeiden, dass Pakete unnötig aus dem Internet heruntergeladen werden, weil ein lokales Repository (beispielsweise eine DVD) eine höhere Priorität erhält.

Wichtig: Priorität im Gegensatz zu Version

Das Repository mit der höchsten Priorität wird auf jeden Fall bevorzugt. Stellen Sie daher sicher, dass das Update-Repository immer die höchste Priorität hat, andernfalls installieren Sie womöglich eine veraltete Version, die erst beim nächsten Online-Update aktualisiert wird.

Name und URL

Wenn Sie den Namen oder die URL eines Repositorys ändern möchten, wählen Sie das Repository mit einem einfachen Klick in der Liste aus und klicken Sie dann auf *Bearbeiten*.

8.4.3 Verwalten von Repository-Schlüsseln

Um deren Integrität sicherzustellen, können Software-Repositorys mit dem GPG-Schlüssel des Repository Maintainers signiert werden. Immer, wenn Sie ein neues Repository hinzufügen, bietet YaST Ihnen an, seinen Schlüssel zu importieren. Überprüfen Sie ihn wie jeden anderen GPG-Schlüssel und stellen Sie sicher, dass er nicht geändert wird. Wenn Sie feststellen, dass der Schlüssel geändert wurde, könnte es sich um einen Fehler im Repository handeln. Deaktivieren Sie das Repository als Installationsquelle, bis Sie die Ursache für die Schlüsseländerung kennen.

Klicken Sie zur Verwaltung aller importierten Schlüssel auf *GPG-Schlüssel* im Dialogfeld *Konfigurierte Software-Repositorys*. Wählen Sie einen Eintrag mit der Maus. Die Schlüsseleigenschaften werden unten im Fenster angezeigt. Sie können Schlüssel *hinzufügen*, *bearbeiten* oder *löschen*, indem Sie auf die entsprechende Schaltfläche klicken.

8.5 Der GNOME Package Updater

SUSE stellt fortlaufend Sicherheitspatches und Aktualisierungen für Ihr Softwareprodukt bereit. Diese werden mit den am Desktop vorhandenen Tools oder durch Ausführen des Moduls in *YaST-Online-Aktualisierung* installiert. In diesem Abschnitt wird beschrieben, wie das System vom GNOME-Desktop aus mit dem *Paket-Updater* aktualisiert wird.

Im Gegensatz zum YaST Online Update-Modul bietet der GNOME-*Paket-Updater* nicht nur die Installation von Patches der Aktualisierungs-Repositorys, sondern auch neue Versionen von bereits installierten Paketen. (Patches beheben Sicherheitsprobleme oder Fehlfunktionen. Die

Funktionalität und Versionsnummer wird in der Regel nicht geändert. Neue Versionen eines Pakets erhöhen die Versionsnummer und fügen Funktionen hinzu oder führen wichtige Änderungen ein.)

Sobald neue Patches oder Paketaktualisierungen verfügbar sind, zeigt GNOME eine Benachrichtigung im Benachrichtigungsbereich oder auf einem Sperrbildschirm an.

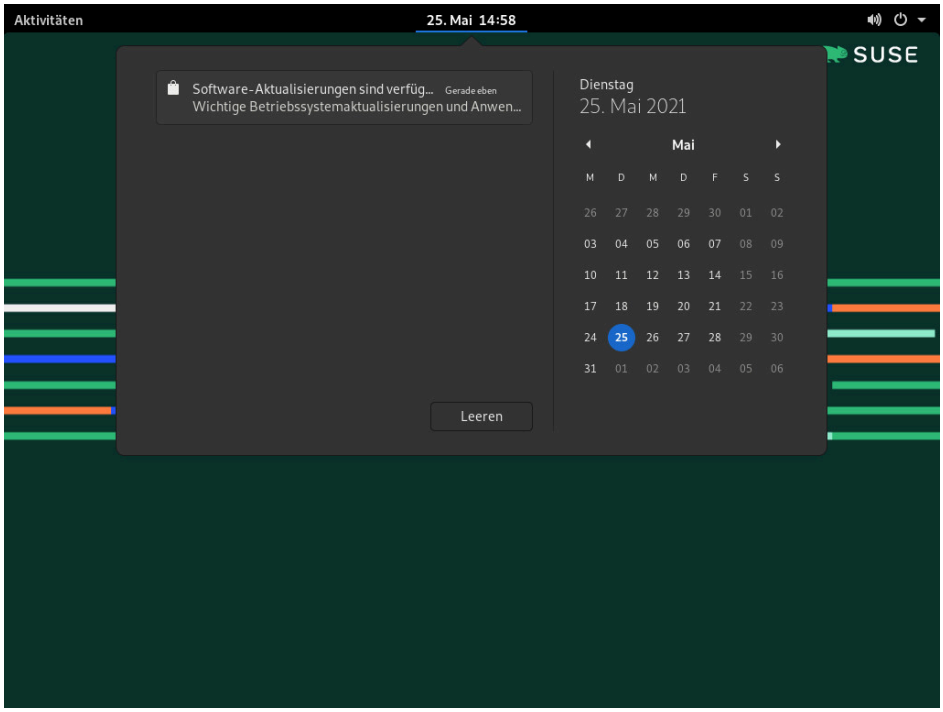
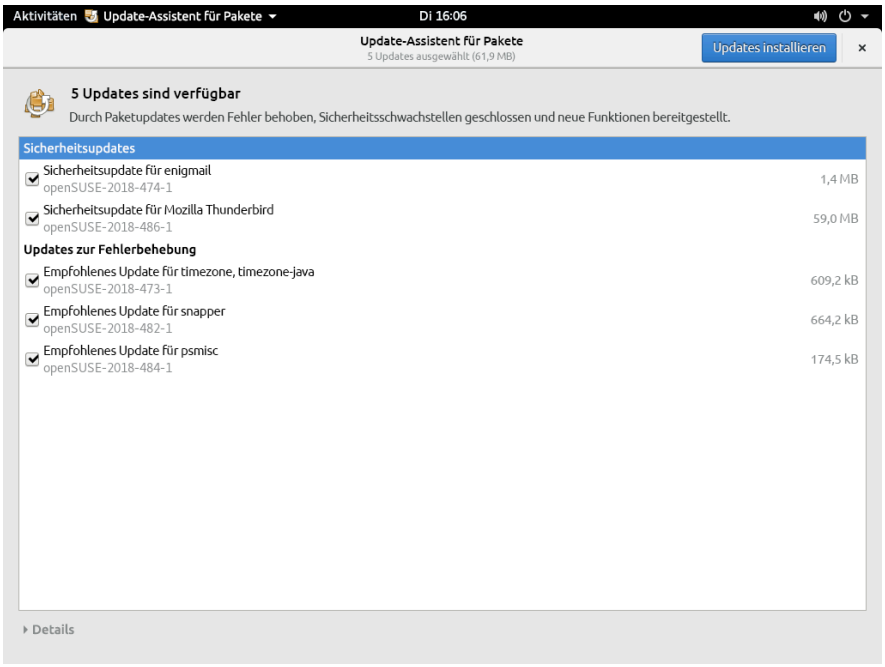


ABBILDUNG 8.3: AKTUALISIERUNGSBENACHRICHTIGUNG AUF DEM GNOME-DESKTOP

Zur Konfiguration der Benachrichtigungseinstellungen für den *Paket-Updater* starten Sie GNOME *Einstellungen* und wählen Sie *Benachrichtigungen* › *Paket-Updater* aus.

VORGEHEN 8.2: INSTALLIEREN VON PATCHES UND AKTUALISIERUNGEN MIT DEM GNOME-PAKET-UPDATER

1. Klicken Sie zum Installieren der Patches und Aktualisierungen auf die Benachrichtigung. Der GNOME-*Paket-Updater* wird geöffnet. Alternativ kann der Updater unter *Aktivitäten* geöffnet werden. Geben Sie dazu `package U` ein und wählen Sie *Paket-Updater* aus.



2. Aktualisierungen werden in vier Kategorien eingeteilt:

   Sicherheitsaktualisierungen (Patches)

   Beseitigen ernsthafte Sicherheitsrisiken und sollten stets installiert werden.

   Empfohlene Aktualisierungen (Patches)

   Beseitigen Probleme, die Ihrem Rechner schaden können. Es wird dringend empfohlen, diese zu installieren.

   Optionale Aktualisierungen (Patches)

   Beseitigen nicht sicherheitsrelevante Probleme oder bieten Verbesserungen.

   Sonstige Aktualisierungen

   Neue Versionen von installierten Paketen.

   Alle verfügbaren Aktualisierungen werden zur Installation ausgewählt. Sollten Sie nicht alle Aktualisierungen installieren wollen, heben Sie zunächst die Auswahl von unerwünschten Aktualisierungen auf. Es wird dringend empfohlen, immer alle Sicherheitsaktualisierungen und empfohlenen Aktualisierungen zu installieren.
   Klicken Sie auf den Titel einer Aktualisierung und dann auf *Details*, um detaillierte Informationen dazu zu erhalten. Die Informationen werden in einem Feld unterhalb der Paketliste angezeigt.

3. Klicken Sie auf *Updates installieren*, um die Installation zu starten.

4. Bei einigen Aktualisierungen ist es möglicherweise erforderlich, den Rechner neu zu starten oder sich abzumelden. Prüfen Sie die Meldung, die nach der Installation angezeigt wird, um Anweisungen zu erhalten.

8.6 Aktualisieren von Paketen mit *GNOME-Software*

Zusätzlich zum GNOME *Paket-Updater* stellt GNOME die *GNOME Software* mit folgenden Funktionen bereit:

- Installieren, Aktualisieren und Entfernen von Software, die als RPM über PackageKit bereitgestellt wurde
- Installieren, Aktualisieren und Entfernen von Software, die als Flatpak bereitgestellt wurde
- Installieren, Aktualisieren und Entfernen von GNOME-Shell-Erweiterungen (https://extensions.gnome.org)
- Aktualisieren von Firmware für Hardwaregeräte mit *Linux Vendor Firmware Service* (LVFS, https://fwupd.org)

GNOME Software bietet auch Screenshots, Bewertungen und Rezensionen für Software.

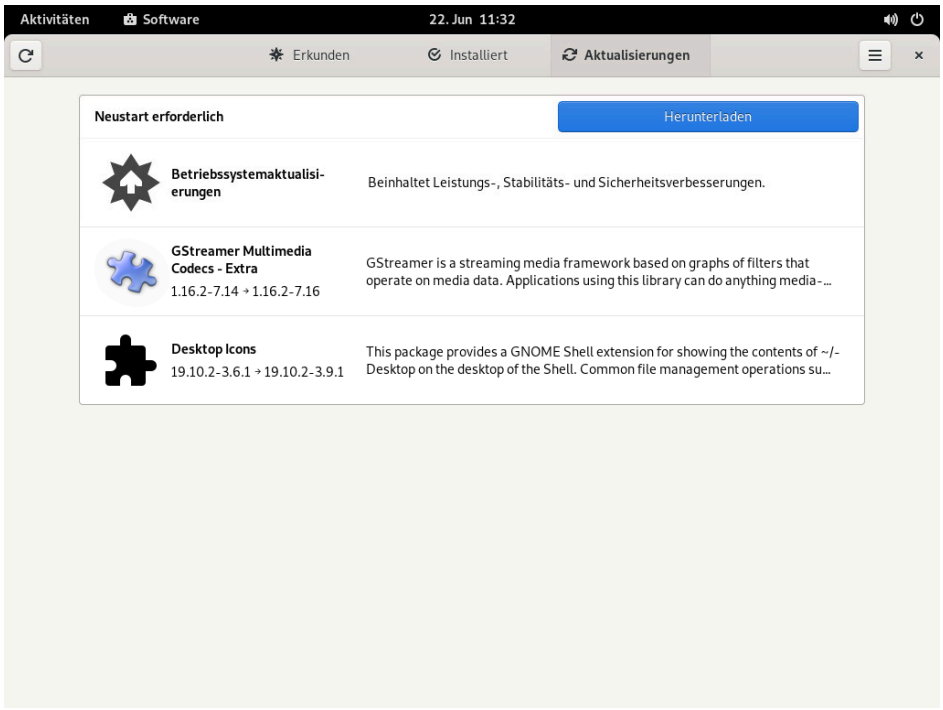


ABBILDUNG 8.4: *GNOME SOFTWARE* – ANSICHT *AKTUALISIERUNGEN*

GNOME Software unterscheidet sich von den anderen von SUSE Linux Enterprise Desktop bereitgestellten Tools wie folgt:

- Anders als YaST oder Zypper zum Installieren von Software als RPM-Paket ist *GNOME Software* auf Software beschränkt, die AppStream-Metadaten bereitstellt. Dies beinhaltet die meisten Desktop-Anwendungen.
- Während der GNOME *Package Updater* Pakete im laufenden System aktualisiert (und Sie zum Neustart der entsprechenden Anwendungen zwingt), lädt *GNOME Software* die Updates herunter und wendet sie nach dem nächsten Neustart an.

9 Verwalten von Software mit Befehlszeilenwerkzeugen

Dieses Kapitel behandelt zypper und RPM, zwei Befehlszeilenwerkzeuge zum Verwalten von Software. Eine Definition der in diesem Kontext verwendeten Terminologie (beispielsweise `repository`, `patch` oder `update`) finden Sie in *Abschnitt 8.1, „Definition der Begriffe“*.

9.1 Verwenden von zypper

Über den Befehlszeilen-Paketmanager Zypper können Sie Pakete installieren, aktualisieren und entfernen. Auch Repositorys werden hiermit verwaltet. Damit können Sie Software per Fernzugriff oder mithilfe von Shell-Skripten verwalten.

9.1.1 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`** *`COMMAND`* ein.

Zypper-Befehle

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

```
> sudo zypper patch
```

Globale Optionen

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

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

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

Befehlsspezifische Optionen

Um die spezifischen Optionen für einen bestimmten Befehl zu verwenden, geben Sie sie direkt nach dem Befehl ein.

```
> 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 werden Lizenzen automatisch akzeptiert.

Argumente

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

```
> sudo zypper install mplayer
```

Manche Optionen erfordern auch ein einzelnes Argument. Der folgende Befehl listet alle bekannten Muster auf:

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

Sie können alle obigen Optionen kombinieren. Beispielsweise werden mit dem folgenden Befehl `mc`- und `vim`-Pakete mithilfe des `factory`-Repositorys installiert und ausführlich angegeben:

```
> sudo zypper -v install --from factory mc vim
```

Mit der Option `--from` bleiben alle Repositorys aktiviert (damit alle Abhängigkeiten aufgelöst werden können), wenn das Paket aus dem angegebenen Repository abgerufen wird. `--repo` ist ein Alias für `--from`. Sie können beide verwenden.

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

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

Zypper unterstützt die globale Option `--userdata` *`STRING`*. 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.

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

9.1.2 Verwenden von Zypper-Unterbefehle

Die Zypper-Unterbefehle sind ausführbare Dateien und befinden sich im Verzeichnis, das mit der Konfigurationsoption `zypper_execdir` festgelegt wurde. Standardmäßig ist dies `/usr/lib/zypper/commands`. Wenn ein Unterbefehle dort nicht zu finden ist, werden die restlichen $PATH-Speicherorte automatisch von Zypper danach durchsucht. Auf diese Weise können Sie Ihre eigenen lokalen Erweiterungen erstellen und im Benutzerbereich speichern.

Die Ausführung von Unterbefehlen in der Zypper-Shell sowie die Verwendung globaler Zypper-Optionen wird nicht unterstützt.

Listen Sie die verfügbaren Unterbefehle auf:

```
> zypper help subcommand
[...]
Available zypper subcommands in '/usr/lib/zypper/commands'

  appstream-cache
  lifecycle
  migration
  search-packages

Zypper subcommands available from elsewhere on your $PATH

  log                   Zypper logfile reader
                            (/usr/sbin/zypper-log)
```

Zeigen Sie den Hilfe-Bildschirm für einen Unterbefehl an:

```
> zypper help appstream-cache
```

9.1.3 Installieren und Entfernen von Software mit zypper

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

```
> 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.

9.1.3.1 Auswählen, welche Pakete zu installieren oder zu entfernen sind

Es gibt verschiedene Möglichkeiten, mit den Befehlen **`zypper install`** und **`zypper remove`** auf Pakete zu verweisen.

Nach dem genauen Paketnamen

```
> sudo zypper install MozillaFirefox
```

Nach dem genauen Namen und der Versionsnummer des Pakets

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

Nach dem Repository-Alias und Paketnamen

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

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

Nach dem Paketnamen mit Wildcards

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. Der folgende Befehl installiert alle Pakete, deren Name mit „Moz“ beginnt:

```
> 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:

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

Nach Funktion

Wenn Sie beispielsweise ein Paket installieren möchten, ohne dessen Namen zu kennen, sind die Funktionen von Nutzen. Der folgende Befehl startet die Installation des Pakets `MozillaFirefox`:

```
> 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:

```
> 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).

```
> sudo zypper install 'firefox>=74.2'
```

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

```
> sudo zypper install 'firefox.x86_64>=74.2'
```

Nach dem Pfad der RPM-Datei

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

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

9.1.3.2 Kombinieren der Installation und der Entfernung von Paketen

Zum gleichzeitigen Installieren und Entfernen von Paketen verwenden Sie die Modifikatoren `+/-`. Verwenden Sie zum Installieren von `emacs` und zum gleichzeitigen Entfernen von `vim` Folgendes:

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

Verwenden Sie zum Entfernen von `emacs` und zum gleichzeitigen Installieren von `vim` Folgendes:

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

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

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

9.1.3.3 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`:

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

9.1.3.4 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 Befehl (**`install`**, **`remove`** und **`patch`**) angegeben werden, wie im Folgenden erkennbar:

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

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

9.1.3.5 Installieren oder Herunterladen von Quellpaketen

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

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

Bei Ausführung als `root`-Benutzer lautet der Standardspeicherort für die Installation von Quellpaketen `/usr/src/packages/` und `~/rpmbuild`. 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:

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

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

```
> 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 9.1.6, „Verwalten von Repositorys mit Zypper“*.

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

```
> 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:

```
> 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`.

9.1.3.6 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:

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

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

Anmerkung: Deaktivierte Installationsmedien

Repositorys von den Installationsmedien von SUSE Linux Enterprise Desktop werden weiterhin konfiguriert, doch nach der erfolgreichen Installation deaktiviert. Sie können anstelle der Online-Repositorys die Option `--plus-content` verwenden, um Pakete von den Installationsmedien zu installieren. Stellen Sie vor dem Aufruf von **zypper** sicher, dass das Installationsmedium verfügbar ist. Legen Sie dazu beispielsweise die DVD im Laufwerk des Rechners ein.

9.1.3.7 Dienstprogramme

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

```
> 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 den folgenden Befehl:

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

Dieser Befehl 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.

9.1.4 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. Das Upgraden von SUSE Linux Enterprise Desktop wird in *Buch „Upgradehandbuch", Kapitel 2 „Upgrade-Pfade und -Methoden"* erläutert.

9.1.4.1 Installieren aller erforderlichen Patches

Neue Versionen installierter Pakete lassen sich am zuverlässigsten durch *Patching* von SUSE Linux Enterprise Desktop installieren. Es garantiert, dass alle erforderlichen Pakete mit den richtigen Versionen installiert werden, und stellt sicher, dass Paketversionen, die als *in Konflikt stehend* angesehen werden, ausgelassen werden.

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

```
> 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. Die erfolgreiche Ausführung von **`zypper patch`** gewährleistet, dass Versionspakete mit Schwachstellen nur dann installiert werden, wenn Sie die entsprechende Ausnahme bestätigen. Beachten Sie, dass das offizielle Aktualisierungs-Repository erst verfügbar ist, nachdem Sie Ihre SUSE Linux Enterprise Desktop-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:

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

Um auch optionale Patches zu installieren, verwenden Sie Folgendes:

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

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

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

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

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

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

```
> 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:

```
> 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.

9.1.4.2 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`**:

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

Dieser Befehl 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 **`zypper list-patches`**.

Liste aller Patches

Um alle für SUSE Linux Enterprise Desktop 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 den Befehl **`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=`*`NUMBER`*. Fügen Sie Kommas zwischen den Fehlernummern hinzu, um nach Patches mit Bezug zu mehreren Bugzilla-Problemen zu suchen, z. B.:

```
> 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=`*`NUMBER`*. Fügen Sie Kommas zwischen den CVE-Nummern hinzu, um nach Patches mit Bezug zu mehreren CVE-Datenbankeinträgen zu suchen, z. B.:

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

Abrufen von zurückgezogenen Patches

Im Codestream von SUSE Linux Enterprise 15 werden bestimmte Patches automatisch zurückgezogen. Wartungsaktualisierungen werden gründlich getestet, denn das Risiko, dass Aktualisierungen einen neuen Fehler mit sich bringen, kann nicht ausgeschlossen werden. Wenn sich herausstellt, dass ein Update einen Fehler enthält, wird ein neues Update (mit einer höheren Versionsnummer) herausgegeben, um das fehlerhafte Update rückgängig zu machen, und es wird verhindert, dass dieses erneut installiert wird. Sie können die zurückgezogenen Patches mit **`zypper`** abrufen:

```
> zypper lp --all |grep retracted
SLE-Module-Basesystem15-SP3-Updates | SUSE-SLE-Module-Basesystem-15-SP3-2021-1965
 | recommended | important | ---    | retracted  | Recommended update for multipath-
tools
SLE-Module-Basesystem15-SP3-Updates | SUSE-SLE-Module-Basesystem-15-SP3-2021-2689
```

```
 | security    | important | ---    | retracted  | Security update for cpio
SLE-Module-Basesystem15-SP3-Updates | SUSE-SLE-Module-Basesystem-15-SP3-2021-3655
 | security    | important | reboot | retracted  | Security update for the Linux
 Kernel
```

So erhalten Sie ausführliche Informationen zu einem zurückgezogenen (oder einem beliebigen) Patch:

```
> zypper patch-info SUSE-SLE-Product-SLES-15-2021-2689
Loading repository data...
Reading installed packages...

Information for patch SUSE-SLE-Product-SLES-15-2021-2689:
---------------------------------------------------------
Repository  : SLE-Product-SLES15-LTSS-Updates
Name        : SUSE-SLE-Product-SLES-15-2021-2689
Version     : 1
Arch        : noarch
Vendor      : maint-coord@suse.de
Status      : retracted
Category    : security
Severity    : important
Created On  : Mon 16 Aug 2021 03:44:00 AM PDT
Interactive : ---
Summary     : Security update for cpio
Description :
    This update for cpio fixes the following issues:

    It was possible to trigger Remote code execution due to a integer overflow
    (CVE-2021-38185, bsc#1189206)

    UPDATE:
    This update was buggy and could lead to hangs, so it has been retracted.
    There will be a follow up update.
    [...]
```

Patch mit Paketkonflikten

```
Information for patch openSUSE-SLE-15.3-2022-333:
-------------------------------------------------
Repository  : Update repository with updates from SUSE Linux Enterprise 15
Name        : openSUSE-SLE-15.3-2022-333
Version     : 1
Arch        : noarch
Vendor      : maint-coord@suse.de
Status      : needed
Category    : security
```

```
Severity    : important
Created On  : Fri Feb  4 09:30:32 2022
Interactive : reboot
Summary     : Security update for xen
Description :
    This update for xen fixes the following issues:

    - CVE-2022-23033: Fixed guest_physmap_remove_page not removing the p2m mappings.
 (XSA-393) (bsc#1194576)
    - CVE-2022-23034: Fixed possible DoS by a PV guest Xen while unmapping a grant.
 (XSA-394) (bsc#1194581)
    - CVE-2022-23035: Fixed insufficient cleanup of passed-through device IRQs.
 (XSA-395) (bsc#1194588)
Provides    : patch:openSUSE-SLE-15.3-2022-333 = 1
Conflicts   : [22]
    xen.src < 4.14.3_06-150300.3.18.2
    xen.noarch < 4.14.3_06-150300.3.18.2
    xen.x86_64 < 4.14.3_06-150300.3.18.2
    xen-devel.x86_64 < 4.14.3_06-150300.3.18.2
    xen-devel.noarch < 4.14.3_06-150300.3.18.2
[...]
```

Der obige Patch steht mit betroffenen oder angreifbaren Versionen von 22 Paketen in Konflikt. Wenn eines dieser betroffenen oder anfälligen Pakete installiert wird, löst dies einen Konflikt aus, und der Patch wird als *erforderlich* klassifiziert. **`zypper patch`** versucht, alle verfügbaren Patches zu installieren. Auftretende Probleme werden gemeldet, und Sie werden informiert, dass nicht alle Aktualisierungen installiert wurden. Zur Behebung des Konflikts können Sie die betroffenen oder angreifbaren Pakete entweder aktualisieren oder entfernen. Mit SUSE-Aktualisierungs-Repositorys lassen sich auch reparierte Pakete übermitteln, sodass Konflikte routinemäßig in Form von Aktualisierungen behoben werden. Sollte ein Paket nicht aktualisiert werden können (z. B. aufgrund von Abhängigkeitsproblemen oder Paketsperren), wird der Benutzer gebeten, das Löschen dieses Pakets zu genehmigen, woraufhin das Paket gelöscht wird.

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:

```
> zypper list-patches --all --cve
Issue | No.           | Patch             | Category    | Severity  | Status
------+---------------+-------------------+-------------+-----------+----------
cve   | CVE-2019-0287 | SUSE-SLE-Module.. | recommended | moderate  | needed
cve   | CVE-2019-3566 | SUSE-SLE-SERVER.. | recommended | moderate  | not needed
[...]
```

9.1.4.3 Installieren neuer Paketversionen

Wenn ein Repository neue Pakete enthält, aber keine Patches zur Verfügung stellt, zeigt **zypper patch** keinerlei Wirkung. Verwenden Sie zum Aktualisieren aller installierten Pakete mit neueren verfügbaren Versionen den folgenden Befehl:

```
> sudo zypper update
```

Wichtig

zypper update ignoriert problematische Pakete. Ist ein Paket beispielsweise gesperrt, überspringt **zypper update** dieses Paket auch dann, wenn eine höhere Version verfügbar ist. Umgekehrt meldet **zypper patch** einen Konflikt, wenn das Paket als angreifbar eingestuft wird.

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

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

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

```
> zypper list-updates
```

Dieser Befehl 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:

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

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

9.1.4.4 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 Befehl erhalten Sie eine entsprechende Liste:

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

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

9.1.5 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:

```
> 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: Befehl, mit dem der Prozess ausgeführt wurde
Service: Dienstname (nur wenn der Befehl einem Systemdienst zugeordnet 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.

```
> 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"`

Befehle 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 19, Der Daemon* `systemd`.

9.1.6 Verwalten von Repositorys mit Zypper

Sämtliche Installations- und Patch-Befehle von Zypper sind von der Liste der bekannten Repositorys abhängig. Um alle dem System bekannten Repositorys aufzulisten, verwenden Sie den Befehl:

```
> zypper repos
```

Das Ergebnis ist der folgenden Ausgabe ähnlich:

BEISPIEL 9.1: ZYPPER – LISTE DER BEKANNTEN REPOSITORYS

```
> zypper repos
# | Alias         | Name           | Enabled | Refresh
--+---------------+----------------+---------+--------
1 | SLEHA-15-GEO | SLEHA-15-GEO   | Yes     | No
2 | SLEHA-15      | SLEHA-15       | Yes     | No
3 | SLES15        | SLES15         | Yes     | No
```

Bei der Angabe von Repositorys kann in verschiedenen Befehlen ein Alias, URI oder eine Repository-Nummer aus der Ausgabe des Befehls **`zypper repos`** verwendet werden. Ein Repository-Alias ist eine Kurzform des Repository-Namens, der in Repository-Befehle 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 den folgenden Befehl, um alle Details aufzulisten:

```
> zypper repos -d
```

9.1.6.1 Hinzufügen von Repositorys

Zum Hinzufügen eines Repository, führen Sie Folgendes aus:

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

`URI` kann ein Internet-Repository, eine Netzwerkressource, ein Verzeichnis oder eine CD oder DVD sein (für Details siehe https://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.

9.1.6.2 Aktualisieren von Repositorys

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

```
> sudo zypper refresh
```

Anmerkung: Standardverhalten von **`zypper`**

Standardmäßig führen bestimmte Befehle **`refresh`** automatisch aus, sodass dieses Kommando nicht explizit aufgerufen werden muss.

Mit dem Befehl **`refresh`** können Sie auch Änderungen in deaktivierten Repositorys anzeigen, indem Sie die Option `--plus-content` verwenden:

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

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

9.1.6.3 Entfernen von Repositorys

Wenn ein Repository von der Liste entfernt werden soll, verwenden Sie den Befehl **`zypper removerepo`** zusammen mit dem Alias oder der Nummer des zu löschenden Repositorys. Um beispielsweise das Repository `SLEHA-12-GEO` aus *Beispiel 9.1, „Zypper – Liste der bekannten Repositorys“* zu entfernen, verwenden Sie einen der folgenden Befehle:

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

9.1.6.4 Ändern von Repositorys

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

```
> 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* einen der folgenden Werte annehmen 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`:

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

9.1.7 Abfragen von Repositorys und Paketen mit Zypper

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

```
> zypper products
> zypper patterns
> zypper packages
> zypper patches
```

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

9.1.7.1 Suchen nach Software

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`

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

Einfache Suche nach dem genauen Paketnamen `MozillaFirefox`

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

Suche auf Paketbeschreibungen und -zusammenfassungen ausdehnen

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

Nur Pakete anzeigen, die nicht bereits installiert sind

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

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

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

9.1.7.2 Suchen nach Paketen in allen SLE-Modulen

Mit dem Unterbefehl **`search-packages`** suchen Sie Pakete innerhalb und außerhalb der aktuell aktivierten SLE-Module. Mit diesem Befehl wird das SUSE Customer Center kontaktiert und alle Module werden nach passenden Paketen durchsucht, wie zum Beispiel:

```
> zypper search-packages package1 package2
```

`zypper search-packages` bietet die folgenden Optionen:

- Suchen nach einer genauen Übereinstimmung mit der Suchzeichenkette: `-x`, `--match-exact`
- Gruppieren der Ergebnisse nach Modul (Standard: Nach Paket gruppieren): `-g`, `--group-by-module`
- Anzeigen detaillierterer Informationen zu Paketen: `-d`, `--details`
- Ausgeben von Suchergebnissen in XML: `--xmlout`

9.1.7.3 Suchen nach bestimmten Funktionen

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 den folgenden Befehl:

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

`what-provides` *`PACKAGE_NAME`* ähnelt dem Befehl **`rpm -q --whatprovides`** *`PACKAGE_NAME`*. 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.

9.1.7.4 Anzeigen von Paketinformationen

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`:

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

9.1.8 Anzeigen von Paketinformationen

SUSE-Produkte werden im Allgemeinen 10 Jahre lang unterstützt. Häufig können Sie diesen standardmäßigen Lebenszyklus anhand der erweiterten Supportangebote von SUSE verlängern und drei Jahre Support erhalten. Den genauen Support-Lebenszyklus für Ihr Produkt finden Sie unter https://www.suse.com/lifecycle.

Mit dem Befehl **`zypper lifecycle`** ermitteln Sie den Lebenszyklus Ihres Produkts und des unterstützten Pakets (siehe unten):

```
# zypper lifecycle
    Product end of support
Codestream: SUSE Linux Enterprise Server 15             2028-07-31
    Product: SUSE Linux Enterprise Server 15 SP3        n/a*

Module end of support
Basesystem Module                                       n/a*
```

```
Desktop Applications Module                              n/a*
Server Applications Module                               n/a*

Package end of support if different from product:
autofs                                  Now, installed 5.1.3-7.3.1, update available
 5.1.3-7.6.1
```

9.1.9 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 Vorlage 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.

9.1.10 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:

```
> sudo zypper refresh
```

Falls das nicht wirkt, probieren Sie Folgendes:

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

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

9.1.11 Zypper-Rollback-Funktion im Btrfs-Dateisystem

Wenn das Btrfs-Dateisystem in der Stammpartition verwendet wird und **`snapper`** 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 zu diesem Thema finden Sie in *Kapitel 10, Systemwiederherstellung und Snapshot-Verwaltung mit Snapper*.

9.1.12 Weitere Informationen

Wenn Sie weitere Informationen zur Verwaltung von Software über die Befehlszeile benötigen, geben Sie **`zypper help`** oder **`zypper help`** *`COMMAND`* ein oder rufen Sie die man-Seite **`zypper(8)`** auf. Eine ausführliche Befehlsreferenz mit `cheat sheets` zu den wichtigsten Befehlen sowie Informationen zur Verwendung von Zypper in Skripten und Anwendungen finden Sie unter https://en.opensuse.org/SDB:Zypper_usage. Eine Liste der Software-Änderungen in der aktuellen SUSE Linux Enterprise Desktop-Version finden Sie unter https://en.opensuse.org/openSUSE:Zypper_versions.

9.2 RPM – der Paket-Manager

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

`rpm` hat fünf Modi: Softwarepakete installieren, de-installieren oder aktualisieren, die RPM-Datenbank neu aufbauen, Anfragen an die RPM-Datenbank bzw. an einzelne RPM-Archive richten, Pakete auf Integrität überprüfen und Pakete signieren. **`rpmbuild`** dient dazu, installierbare Pakete aus den unverfälschten Quellen herzustellen.

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

Tipp: Pakete zur Software-Entwicklung

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

9.2.1 Prüfen der Authentizität eines Pakets

RPM-Pakete sind mit GPG signiert. Verwenden Sie zum Verifizieren der Signatur eines RPM-Pakets den Befehl **`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:

```
> 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.

9.2.2 Verwalten von Paketen: Installieren, Aktualisieren und Deinstallieren

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

Mit den Optionen `-U` oder `--upgrade` und `-F` oder `--freshen` kann ein Paket (z. B. **`rpm -F`** *`PACKAGE`*.rpm) aktualisiert werden. 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` in 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 dieser Dateien ist in `/var/adm/rpmconfig-check` 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.

Um ein Paket zu entfernen, geben Sie **`rpm -e`** *`PACKAGE`* ein. Dieser Befehl 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.

9.2.3 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:

```
> 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:

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

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

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

Technische Informationen finden Sie unter `/usr/share/doc/packages/deltarpm/README`.

9.2.4 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 im *Tabelle 9.1, „Wichtige Optionen für RPM-Abfragen“*.

TABELLE 9.1: WICHTIGE OPTIONEN FÜR RPM-ABFRAGEN

`-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 (zur Verwendung mit `-l`, `-c` oder `-d`)
`--provides`	Funktionen des Pakets auflisten, die ein anderes Paket mit `--requires` anfordern kann
`--requires`, `-R`	Fähigkeiten, die das Paket benötigt
`--scripts`	Installationsskripten (preinstall, postinstall, uninstall)

Beispielsweise gibt der Befehl **`rpm -q -i wget`** die in *Beispiel 9.2, „`rpm -q -i wget`“* gezeigte Information aus.

BEISPIEL 9.2: `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 15
```

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

```
> rpm -q -f /bin/rpm /usr/bin/wget
rpm-4.14.1-lp151.13.10.x86_64
wget-1.19.5-lp151.4.1.x86_64
```

Wenn nur ein Teil des Dateinamens bekannt ist, verwenden Sie ein Shell-Skript, wie in *Beispiel 9.3, „Skript für die Suche nach Paketen“* gezeigt. Übergeben Sie den partiellen Dateinamen als Parameter beim Aufruf des Skripts.

BEISPIEL 9.3: 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`** *PACKAGE* 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 9.2: RPM-ÜBERPRÜFUNGSOPTIONEN

5	MD5-Prüfsumme
S	Dateigröße

L	Symbolischer Link
T	Änderungszeit
D	Major- und Minor-Gerätenummern
U	Besitzer
G	Gruppe
M	Modus (Berechtigungen und Dateityp)

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

```
> 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 aufzubauen. Legen Sie zuvor eine Sicherungskopie der alten Datenbank an. Das **`cron`**-Skript **`cron.daily`** erstellt tägliche Kopien der Datenbank (gepackt mit GZIP) und speichert sie 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`.

9.2.5 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` verfügbar sein (sofern Sie keine benutzerdefinierten Einstellungen in einer Datei wie `/etc/rpmrc` angegeben haben):

`SOURCES`
: für die ursprünglichen Quellen (`.tar.bz2`- oder `.tar.gz`-Dateien usw.) und für distributionsspezifische Anpassungen (meist `.diff`- oder `.patch`-Dateien)

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

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

`RPMS`
: Speicherort der fertigen Binärpakete

`SRPMS`
: Speicherort der Quell-RPMs

Wenn Sie ein Quellpaket mit YaST installieren, werden alle notwendigen Komponenten in `/usr/src/packages` installiert: die Quellen und Anpassungen in `SOURCES` und die 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-1.19.5.tar.bz2
/usr/src/packages/SOURCES/wgetrc.patch
/usr/src/packages/SPECS/wget.spec
```

rpmbuild `-bX /usr/src/packages/SPECS/wget.spec` startet die Kompilierung. *X* ist ein Platzhalter für verschiedene Stufen des build-Prozesses (Einzelheiten erhalten Sie in der Ausgabe von `--help` oder in der RPM-Dokumentation). Nachfolgend wird nur eine kurze Erläuterung gegeben:

`-bp`
: Bereiten Sie die 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 sich das Binärpaket in `/usr/src/packages/RPMS` befinden.

`-ba`
: Wie `-bb`, jedoch mit der Erstellung des zusätzlichen Quell-RPM. Nach erfolgreicher Kompilierung sollte sich das Binärpaket in `/usr/src/packages/SRPMS` befinden.

`--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 nicht mehr verwendet wird. Benötigen Sie die Funktion weiterhin, verwenden Sie die Option `--buildroot` als Alternative.

9.2.6 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 *DIRECTORY* fest. Im Unterschied zu **rpm** sucht der Befehl **build** die `.spec`-Datei im Quellverzeichnis. Wenn Sie, wie im obigen Beispiel, `wget` neu erstellen möchten und die DVD unter `/media/dvd` im System eingehängt ist, verwenden Sie als Benutzer `root` folgende Befehle:

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

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

Das 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 den Befehl **rpm** auf eine der oben erwähnten Stufen zu beschränken. Greifen Sie mit **build** `--help` und durch Lesen der Manpage für **build** auf zusätzliche Informationen zu.

9.2.7 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 in *Kapitel 8, Installieren bzw. Entfernen von Software*.

10 Systemwiederherstellung und Snapshot-Verwaltung mit Snapper

Mit Snapper werden Dateisystem-Snapshots erstellt und verwaltet. Durch Dateisystem-Snapshots kann eine Kopie des Zustands eines Dateisystems zu einem bestimmten Zeitpunkt beibehalten werden. Die Standardeinrichtung von Snapper lässt ein Rollback von Systemänderungen zu. Sie können es jedoch auch zum Erstellen von Sicherungen der Benutzerdaten auf Wechseldatenträgern verwenden. Als Basis für diese Funktion verwendet Snapper das Btrfs-Dateisystem oder LVM-Volumes mit Thin Provisioning mit einem XFS- oder Ext4-Dateisystem.

Snapper verfügt über eine Befehlszeilen-Schnittstelle und eine YaST-Schnittstelle. Mit Snapper können Sie Dateisystem-Snapshots zu den folgenden Dateisystemtypen erstellen und verwalten:

- Btrfs, ein Kopie-beim-Schreiben-Betriebssystem für Linux, das nativ Dateisystem-Snapshots von Subvolumes unterstützt. (Subvolumes sind separat einhängbare Dateisysteme in einer physischen Partition.)
  Sie können auch von `Btrfs`-Snapshots booten. Weitere Informationen finden Sie in *Abschnitt 10.3, „System-Rollback durch Booten aus Snapshots“*.
- LVM-Volumes mit Thin Provisioning formatiert mit XFS oder Ext4.

Mit Snapper können die folgenden Aufgaben ausgeführt werden:

- Systemänderungen rückgängig machen, die von **`zypper`** und YaST vorgenommen wurden. Ausführliche Informationen finden Sie in *Abschnitt 10.2, „Rückgängigmachen von Änderungen mit Snapper“*.
- Dateien aus früheren Snapshots wiederherstellen. Ausführliche Informationen finden Sie in *Abschnitt 10.2.2, „Wiederherstellen von Dateien mit Snapper“*.
- System-Rollback durch Booten aus einem Snapshot vornehmen. Ausführliche Informationen finden Sie in *Abschnitt 10.3, „System-Rollback durch Booten aus Snapshots“*.
- Im laufenden System manuell Snapshots erstellen und verwalten. Ausführliche Informationen finden Sie in *Abschnitt 10.6, „Manuelles Erstellen und Verwalten von Snapshots“*.

10.1 Standardeinrichtung

Snapper unter SUSE Linux Enterprise Desktop wird als Werkzeug zum Rückgängigmachen und Wiederherstellen von Systemänderungen eingerichtet. Standardmäßig ist die root-Partition (`/`) von SUSE Linux Enterprise Desktop mit `Btrfs` formatiert. Das Erstellen von Snapshots wird automatisch aktiviert, wenn die root-Partition (`/`) groß genug ist (mehr als ca. 16 GB). Snapshots auf anderen Partitionen als `/` werden standardmäßig deaktiviert.

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:

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

Aktivieren Sie dann die verschiedenen Snapshot-Typen gemäß den Anweisungen unter *Abschnitt 10.1.4.1, „Deaktivieren/Aktivieren von Snapshots“*.

Bei einem Btrfs-root-Dateisystem muss für Snapshots ein Dateisystem mit Subvolumes konfiguriert sein, wie vom Installationsprogramm vorgeschlagen. Die Partition muss zudem mindestens 16 GB groß sein.

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.

Folglich müssen Partitionen mit Snapshots größer sein als Partitionen ohne Snapshots. Die genaue Speichermenge ist dabei stark abhängig von der Anzahl der Snapshots und vom Umfang der Änderungen an den Daten. Als Faustregel sollten Sie für diese Partitionen doppelt so viel Speicherplatz vorsehen wie normalerweise. Um zu verhindern, dass es zu wenig Speicherplatz gibt, werden alte Snapshots automatisch bereinigt. Weitere Informationen finden Sie in *Abschnitt 10.1.4.4, „Steuern der Snapshot-Archivierung“*.

10.1.1 Standardeinstellungen

Festplatten größer als 16 GB

- Konfigurationsdatei: `/etc/snapper/configs/root`
- `USE_SNAPPER=yes`
- `TIMELINE_CREATE=no`

Festplatten kleiner als 16 GB

- Konfigurationsdatei: nicht erstellt
- `USE_SNAPPER=no`
- `TIMELINE_CREATE=yes`

10.1.2 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. Bei der YaST-Methode für die Betriebssysteminstallation (Standard) sind Zeitleisten-Snapshots aktiviert, außer für das root-Dateisystem. Sie können die Aufnahme von Snapshots auf der Zeitachse in unterschiedlichen Intervallen konfigurieren: stündlich, täglich, wöchentlich, monatlich und jährlich. Alte Snapshots werden automatisch gelöscht. Standardmäßig wird der erste Snapshot der letzten zehn Tage, Monate und Jahre beibehalten.

Installations-Snapshots

Immer wenn Sie eines oder mehrere Pakete mit Zypper oder YaST installieren, werden drei Installationsmomentaufnahmen erstellt. Wird eine wichtige Systemkomponente installiert (z. B. der Kernel), wird das Snapshot-Paar als wichtig gekennzeichnet. Alte Snapshots werden automatisch gelöscht. Installations-Snapshots sind standardmäßig aktiviert.

Verwaltungs-Snapshots

Immer wenn Sie mit Zypper oder YaST Änderungen am System vornehmen, wird ein Snapshot-Paar erstellt: ein Snapshot vor der Systemänderung („pre“) und ein weiterer nach der Systemänderung („post“). Alte Snapshots werden automatisch gelöscht. Administrations-Snapshots sind standardmäßig aktiviert.

10.1.3 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.

`/home`

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

`/opt`

Produkte von Drittanbietern werden in der Regel im Verzeichnis `/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`

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`

Dieses Verzeichnis enthält viele Variablendateien, einschließlich Protokolle, temporäre Caches und Drittanbieterprodukte in `/var/opt`. Es ist der Standardspeicherort für Images und Datenbanken von virtuellen Maschinen. Daher wird dieses Subvolume so erstellt, dass alle Variablendaten von Snapshots ausgeschlossen werden und „Kopie beim Schreiben“ deaktiviert ist.

10.1.4 Anpassen der Einrichtung

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

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

Deaktivieren. `snapper -c root set-config "TIMELINE_CREATE=no"`
Bei der YaST-Methode für die Betriebssysteminstallation (Standard) sind Zeitleisten-Snapshots aktiviert, außer für das root-Dateisystem.

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: Legen Sie `USE_SNAPPER` auf `yes` in `/etc/sysconfig/yast2` fest.

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

10.1.4.2 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, zu 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>
```

10.1.4.3 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 Desktop ist mit dem Subvolume `/@/` konfiguriert, das als unabhängiger Root für dauerhafte Subvolumes wie `/opt`, `/srv` oder `/home` und andere 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.

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

Der zugehörige Eintrag in `/etc/fstab` muss wie folgt lauten:

```
/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.

10.1.4.4 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 10.5.1, „Verwalten vorhandener Konfigurationen“*.

10.1.4.5 Verwenden von Snapper auf LVM-Volumes mit Thin Provisioning

Neben Snapshots auf `Btrfs`-Dateisystemen unterstützt Snapper auch das Erstellen 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 „Installationshandbuch“, Kapitel 7 „Festplatte vorbereiten: Expertenmodus“, Abschnitt 7.3 „LVM-Konfiguration“*.

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

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

Sie können diese Konfiguration gemäß den Anweisungen unter *Abschnitt 10.5.1, „Verwalten vorhandener Konfigurationen“* an Ihre Anforderungen anpassen.

10.2 Rückgängigmachen von Änderungen mit Snapper

Snapper unter SUSE Linux Enterprise Desktop 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 10.1.4.1, „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 10.3, „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 10.3, „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.

10.2.1 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.

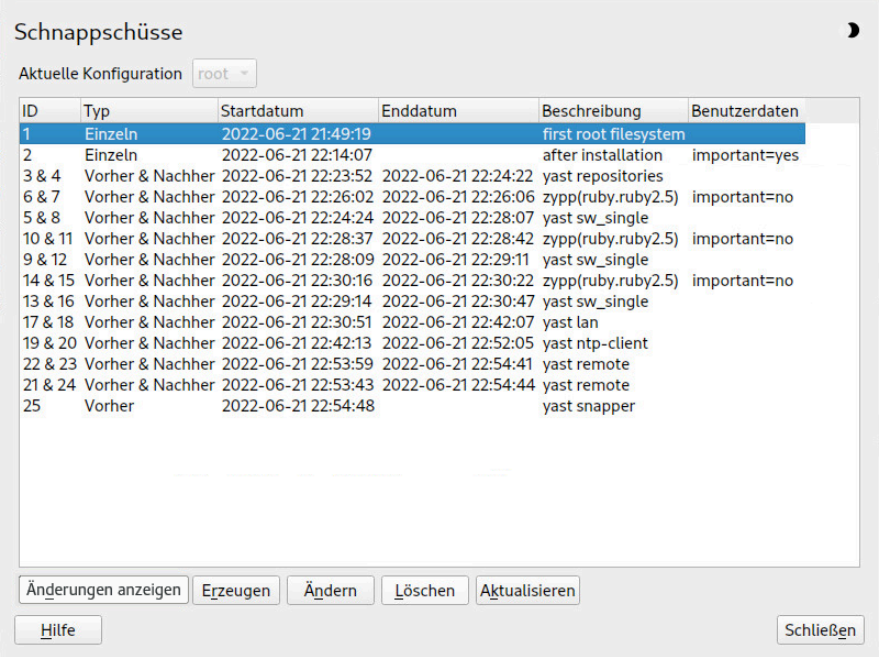
Mit dem YaST-Snapper-Modul oder mit dem **`snapper`**-Befehlszeilenwerkzeug können Sie Dateien aus dem „Pre-Snapshot“ wiederherstellen und so die Änderungen durch YaST/Zypper rückgängig machen. Durch den Vergleich der beiden Snapshots mit diesen Werkzeugen erkennen Sie außerdem, welche Dateien geändert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

VORGEHEN 10.1: 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.

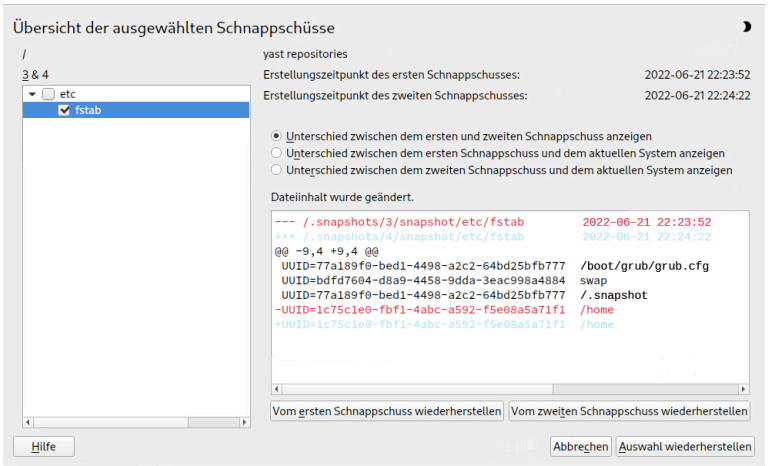
2. Unter *Aktuelle Konfiguration* muss die Option *root* eingestellt sein. Dies ist im Prinzip immer der Fall, sofern Sie nicht eigene Snapper-Konfigurationen manuell hinzugefügt haben.

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 und Post*. Für YaST-Snapshots wird die Bezeichnung `zypp(y2base)` in der Spalte *Beschreibung* angezeigt, für Zypper-Snapshots die Bezeichnung `zypp(zypper)`.

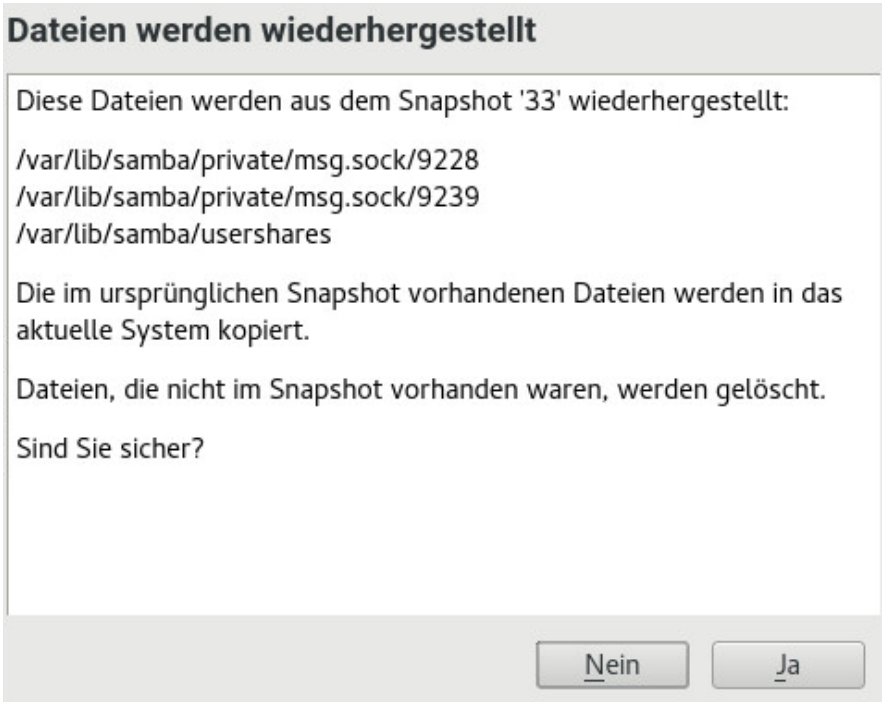


4. Klicken Sie auf *Änderungen anzeigen*. Die Liste der Dateien, bei denen Unterschiede zwischen den beiden Snapshots bestehen, wird geöffnet.

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*.

VORGEHEN 10.2: RÜCKGÄNGIGMACHEN VON ÄNDERUNGEN MIT DEM BEFEHL `snapper`

1. Rufen Sie eine Liste der YaST- und Zypper-Snapshots ab, indem Sie **`snapper list -t pre-post`** ausführen. Für YaST-Snapshots wird die Bezeichnung `yast` *`MODULE_NAME`* in der Spalte *Beschreibung* angezeigt, für Zypper-Snapshots die Bezeichnung `zypp(zypper)`.

```
> sudo snapper list -t pre-post
Pre # | Post # | Pre Date                     | Post Date                    | Description
------+--------+------------------------------+------------------------------+-------------
311   | 312    | Tue 06 May 2018 14:05:46 CEST | Tue 06 May 2018 14:05:52 CEST | zypp(y2base)
340   | 341    | Wed 07 May 2018 16:15:10 CEST | Wed 07 May 2018 16:15:16 CEST | zypp(zypper)
342   | 343    | Wed 07 May 2018 16:20:38 CEST | Wed 07 May 2018 16:20:42 CEST | zypp(y2base)
344   | 345    | Wed 07 May 2018 16:21:23 CEST | Wed 07 May 2018 16:21:24 CEST | zypp(zypper)
346   | 347    | Wed 07 May 2018 16:41:06 CEST | Wed 07 May 2018 16:41:10 CEST | zypp(y2base)
348   | 349    | Wed 07 May 2018 16:44:50 CEST | Wed 07 May 2018 16:44:53 CEST | zypp(y2base)
350   | 351    | Wed 07 May 2018 16:46:27 CEST | Wed 07 May 2018 16:46:38 CEST | zypp(y2base)
```

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

```
> 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..POST FILENAME`* aus. Wenn Sie *`FILENAME`* nicht angeben, wird die Diff-Ansicht für alle Dateien angezeigt.

```
> 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..POST FILENAMES`* aus. Wenn Sie *`FILENAMES`* nicht angeben, werden alle geänderten Dateien wiederhergestellt.

```
> 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 *Verwaltung von Benutzern und Gruppen* empfohlen.

10.2.2 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 10.5, „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. Ausführliche Informationen finden Sie in *Abschnitt 10.3, „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.

VORGEHEN 10.3: WIEDERHERSTELLEN VON DATEIEN MIT DEM *SNAPPER*-MODUL IN YAST

1. Starten Sie das *Snapper*-Modul in 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*.

VORGEHEN 10.4: WIEDERHERSTELLEN VON DATEIEN MIT DEM BEFEHL `snapper`

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

   ```
   > 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 Befehl erhalten Sie eine Liste der geänderten Dateien in einem bestimmten Snapshot:

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

   Ersetzen Sie *`SNAPSHOT_ID`* durch die ID des Snapshots, aus dem die Dateien wiederhergestellt werden sollen.

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

   ```
   > 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:

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

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

10.3 System-Rollback durch Booten aus Snapshots

Mit der GRUB 2-Version in SUSE Linux Enterprise Desktop 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 Desktop 15 SP7 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 10.2, „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 befinden. Um dies zu überprüfen, führen Sie `sudo /sbin/btrfs filesystem show` aus. `Total devices 1` muss ausgegeben werden. Wenn mehr als `1` Gerät aufgeführt ist, wird Ihr Setup nicht unterstützt.

Anmerkung: Verzeichnisse, die aus Snapshots ausgenommen sind

Verzeichnisse, die aus Snapshots ausgeschlossen sind, beispielsweise `/srv` (vollständige Liste siehe *Abschnitt 10.1.3, „Verzeichnisse, die aus Snapshots ausgenommen sind“*), können sich auf separaten Geräten befinden.

- Das System muss über den installierten Bootlader bootfähig sein.
- Nur der Inhalt des Subvolumes `/` wird zurückgesetzt. Es ist nicht möglich, andere Subvolumes einzubeziehen.

So führen Sie ein Rollback aus einem bootfähigen Snapshot aus:

1. Booten Sie das System. Wählen Sie im Bootmenü den Eintrag *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:

   ```
   > 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 in *Abschnitt 10.3.1, „Snapshots nach dem Rollback“*.

Es ist sinnvoll, eine Beschreibung für den Snapshot mit der Option `-d` hinzuzufügen. 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 `after installation` erkennbar.

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

10.3.1 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 finden Sie in *Abschnitt 10.7, „Automatisches Bereinigen von Snapshots“*. Wenn der Snapshot wichtige Daten enthält, extrahieren Sie die Daten aus dem Snapshot, bevor er entfernt wird.

10.3.1.1 Beispiel für einen Rollback-Snapshot

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

```
# 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.

```
# 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 |     |         |                       |
```

10.3.2 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 10.1: BOOTLOADER: SNAPSHOTS

Warnung: Das Booten von Xen von einem Btrfs-Snapshot mit UEFI schlägt aktuell fehl

Weitere Informationen finden Sie in https://www.suse.com/support/kb/doc/?id=000020602.

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

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

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

❷ Bezeichnung des Betriebssystems.

❹ Datum im Format `YYYY-MM-DD`.

❺ Uhrzeit im Format `HH:MM`.

❻ 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:

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

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

10.3.3 Nutzungsbeschränkungen

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

10.3.3.1 Verzeichnisse, die aus Snapshots ausgenommen sind

Snapshots des root-Dateisystems enthalten nicht alle Verzeichnisse. Weitere Informationen und Begründungen finden Sie unter *Abschnitt 10.1.3, „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`**.

10.3.3.2 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.

10.4 Aktivieren von Snapper in Benutzer-Startverzeichnissen

Sie können Snapshots für das Verzeichnis `/home` der Benutzer aktivieren, womit eine Reihe von Anwendungsfällen unterstützt wird:

- Verwaltung der jeweils eigenen Snapshots und Rollbacks durch die einzelnen Benutzer
- Systembenutzer, z. B. Datenbank-, System- und Netzwerkadministratoren, die Kopien der Konfigurationsdateien, Dokumentation usw. nachverfolgen möchten
- Samba-Freigaben mit Startverzeichnissen und dem Btrfs-Back-End

Die einzelnen Benutzerverzeichnisse sind jeweils ein Btrfs-Subvolume von `/home`. Dies kann manuell eingerichtet werden (siehe *Abschnitt 10.4.3, „Manuelles Aktivieren von Snapshots in Startverzeichnissen“*). `pam_snapper` bietet jedoch eine komfortablere Alternative. Mit dem Paket `pam_snapper` werden das Modul `pam_snapper.so` und die Hilfsskripte installiert, mit denen die Benutzererstellung und die Snapper-Konfiguration automatisiert werden.

`pam_snapper` sorgt für die Integration in den Befehl **`useradd`**, in PAM (Pluggable Authentication Modules) und in Snapper. Snapshots werden standardmäßig beim An- und Abmelden eines Benutzers und zusätzlich in bestimmten Abständen erstellt, wenn Benutzer längere Zeit angemeldet bleiben. Sie können die Standardeinstellungen mit den gewohnten Snapper-Befehlen und Konfigurationsdateien ändern.

10.4.1 Installieren von pam_snapper und Erstellen von Benutzern

Der einfachste Einstieg gelingt mit einem neuen `/home`-Verzeichnis, das mit Btrfs formatiert ist, und ganz ohne Benutzer. Installieren `pam_snapper`:

```
# zypper in pam_snapper
```

Fügen Sie diese Zeile in `/etc/pam.d/common-session` ein:

```
session optional pam_snapper.so
```

Verwenden Sie das Skript **`/usr/lib/pam_snapper/pam_snapper_useradd.sh`**, um einen neuen Benutzer und ein neues Home-Verzeichnis zu erstellen. Standardmäßig führt das Skript einen Probelauf aus. Ersetzen Sie `DRYRUN=1` im Skript durch `DRYRUN=0`. Nun können Sie einen neuen Benutzer erstellen:

```
# /usr/lib/pam_snapper/pam_snapper_useradd.sh \
username group passwd=password
Create subvolume '/home/username'
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
```

Die Dateien aus `/etc/skel` werden beim ersten Anmelden des Benutzers in sein Startverzeichnis kopiert. Rufen Sie Ihre Snapper-Konfigurationen ab und prüfen Sie, ob die Konfiguration des Benutzers erstellt wurde:

```
# snapper list --all
Config: home_username, subvolume: /home/username
Type   | # | Pre # | Date | User | Cleanup | Description | Userdata
-------+---+-------+------+------+---------+-------------+---------
single | 0 |       |      | root |         | current     |
```

Im Lauf der Zeit umfasst diese Ausgabe eine Liste der Snapshots, die der Benutzer mit den standardmäßigen Snapper-Befehlen verwalten kann.

10.4.2 Entfernen von Benutzern

Entfernen Sie Benutzer mit dem Skript **`/usr/lib/pam_snapper/pam_snapper_userdel.sh`**. Standardmäßig führt das Skript einen Probelauf aus. Ersetzen Sie `DRYRUN=1` im Skript daher durch `DRYRUN=0`. Damit werden der Benutzer, das Start-Subvolume des Benutzers und die Snapper-Konfiguration entfernt und alle Snapshots gelöscht.

```
# /usr/lib/pam_snapper/pam_snapper_userdel.sh username
```

10.4.3 Manuelles Aktivieren von Snapshots in Startverzeichnissen

Mit diesen Schritten richten Sie die Startverzeichnisse der Benutzer manuell für Snapper ein. `/home` muss mit Btrfs formatiert sein und die Benutzer dürfen noch nicht erstellt worden sein.

```
# btrfs subvol create /home/username
# snapper -c home_username create-config /home/username
# sed -i -e "s/ALLOW_USERS=\"\"/ALLOW_USERS=\"username\"/g" \
/etc/snapper/configs/home_username
# yast users add username=username home=/home/username password=password
# chown username.group /home/username
# chmod 755 /home/username/.snapshots
```

10.5 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 in *Abschnitt 10.5.1.1, „Konfigurationsdaten“*.

Anmerkung: Erforderliche Mindestgröße des root-Dateisystems für Snapshots

Wie unter *Abschnitt 10.1, „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 aktuell 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>
```

Er wird mit der folgenden Formel berechnet: *ROOT_BASE_SIZE* * (1 + *BTRFS_INCREASE_PERCENTAGE*/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 (beispielsweise **`snapper -c myconfig list`**).

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

```
> 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 10.5.1, „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` für den Befehl create-config an:

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

10.5.1 Verwalten vorhandener Konfigurationen

Der Befehl **`snapper`** bietet verschiedene Unterbefehle für die Verwaltung von vorhandenen Konfigurationen. Sie können sie auflisten, anzeigen, löschen und bearbeiten:

Auflisten von Konfigurationen

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

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

Anzeigen einer Konfiguration

Mit dem Unterbefehl **`snapper -c`** *`CONFIG`* **`get-config`** zeigen Sie die angegebene Konfiguration an. Ersetzen Sie *`CONFIG`* durch einen der Konfigurationsnamen in **`snapper list-configs`**. Weitere Informationen zu den Konfigurationsoptionen finden Sie in *Abschnitt 10.5.1.1, „Konfigurationsdaten“*.

Zum Anzeigen der Standardkonfiguration führen Sie den folgenden Befehl aus:

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

Bearbeiten einer Konfiguration

Verwenden Sie den Unterbefehl **`snapper -c`** *`CONFIG`* **`set-config`** *`OPTION=VALUE`*, um eine Option in der angegebenen Konfiguration zu ändern. Ersetzen Sie *`CONFIG`* durch einen der Konfigurationsnamen in **`snapper list-configs`**. Eine Liste der möglichen Werte für *`OPTION`* und *`VALUE`* finden Sie in *Abschnitt 10.5.1.1, „Konfigurationsdaten“*.

Löschen einer Konfiguration

Verwenden Sie das Unterkommando **`snapper -c CONFIG delete-config`** zum Löschen einer Konfiguration. Ersetzen Sie *`CONFIG`* durch einen der Konfigurationsnamen in **`snapper list-configs`**.

10.5.1.1 Konfigurationsdaten

Jede Konfiguration enthält eine Liste von Optionen, die über die Befehlszeile bearbeitet werden können. Die folgende Liste zeigt weitere Details zu den einzelnen Optionen. Zum Ändern eines Werts führen Sie **`snapper -c CONFIG set-config "KEY=VALUE"`** aus.

`ALLOW_GROUPS`, `ALLOW_USERS`

Erteilt regulären Benutzern die erforderlichen Berechtigungen zum Verwenden von Snapshots. Weitere Informationen zu diesem Thema finden Sie in *Abschnitt 10.5.1.2, „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 ist `"yes"`.

`EMPTY_*`

Definiert den Bereinigungsalgorithmus für Snapshot-Paare mit identischen Pre- und Post-Snapshots. Ausführliche Informationen finden Sie in *Abschnitt 10.7.3, „Bereinigen von Snapshot-Paaren, die sich nicht unterscheiden“*.

`FSTYPE`

Dateisystemtyp der Partition. Bearbeiten Sie diese Datei nicht.

Der Standardwert ist `"btrfs"`.

`NUMBER_*`

Definiert den Bereinigungsalgorithmus für Installations- und Verwaltungs-Snapshots. Ausführliche Informationen finden Sie in *Abschnitt 10.7.1, „Bereinigen von nummerierten Snapshots“*.

`QGROUP` / `SPACE_LIMIT`

Fügt Quotenunterstützung zu Bereinigungs-Algorithmen hinzu. Ausführliche Informationen finden Sie in *Abschnitt 10.7.5, „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 10.5.1.2, „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) festgelegt 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 ist `"no"`.

`TIMELINE_CREATE`

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

Der Standardwert ist `"no"`.

`TIMELINE_CLEANUP` / `TIMELINE_LIMIT_*`

Definiert den Bereinigungsalgorithmus für Zeitleisten-Snapshots. Ausführliche Informationen finden Sie in *Abschnitt 10.7.2, „Bereinigen von Zeitleisten-Snapshots“*.

10.5.1.2 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 diesen Zweck erstellen Sie Konfigurationen, die Berechtigungen für Benutzer und/oder Gruppen gewähren. 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.

VORGEHEN 10.5: ERMÖGLICHEN DER VERWENDUNG VON SNAPPER FÜR NORMALE BENUTZER

Alle Schritte in diesem Verfahren müssen von `root` ausgeführt werden.

1. Falls noch keine Snapper-Konfiguration vorhanden ist, erstellen Sie eine Konfiguration für die Partition oder das Subvolume, in der/dem der Benutzer Snapper verwenden soll. Weitere Anweisungen finden Sie unter *Abschnitt 10.5, „Erstellen und Bearbeiten von Snapper-Konfigurationen“*. Beispiel:

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

2. Die Konfigurationsdatei wird unter `/etc/snapper/configs/CONFIG` erstellt, wobei CONFIG der Wert ist, den Sie mit `-c/--config` im vorherigen Schritt angegeben haben (beispielsweise `/etc/snapper/configs/web_data`). Passen Sie die Datei entsprechend Ihrer Anforderungen an. Weitere Informationen finden Sie in *Abschnitt 10.5.1, „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:

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

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

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

10.6 Manuelles Erstellen und Verwalten von Snapshots

Snapper ist nicht auf das automatische Erstellen und Verwalten von Snapshots über eine Konfiguration beschränkt. Mit dem Befehlszeilenwerkzeug 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 10.5, „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. Sollen Snapshots für Ihre

eigene Konfiguration erstellt oder verwaltet werden, müssen Sie diese Konfiguration explizit auswählen. Verwenden Sie das Dropdown-Feld *Aktuelle Konfiguration* in YaST oder geben Sie den Schalter `-c` in der Befehlszeile an (**`snapper -c`** *`MYCONFIG COMMAND`*).

10.6.1 Snapshot-Metadaten

Ein Snapshot besteht jeweils aus dem Snapshot selbst und aus bestimmten 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 den Befehl **`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 10.6.1.1, „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 eine durch Kommas getrennte 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 10.7, „Automatisches Bereinigen von Snapshots“*.

10.6.1.1 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. Jeder Nachher-Snapshot (`pre`) entspricht einem Vorher-Snapshot (`post`). Dies wird beispielsweise für automatische YaST/Zypper-Snapshots verwendet.

`post`

Snapshot eines Dateisystems *nach* einer Änderung. Jeder Nachher-Snapshot (`post`) entspricht einem Vorher-Snapshot (`pre`). Dies wird beispielsweise für automatische YaST/Zypper-Snapshots verwendet.

`single`

Eigenständiger Snapshot. Dies wird beispielsweise für automatische stündliche Snapshots verwendet. Dies ist der Standardtyp beim Erstellen von Snapshots.

10.6.1.2 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 10.5.1, „Verwalten vorhandener Konfigurationen“*).

number

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.

10.6.2 Erstellen von Snapshots

Führen Sie zum Erstellen eines Snapshots den Befehl **`snapper create`** aus oder klicken Sie im YaST-Modul *Snapper* auf *Erstellen*. In den nachfolgenden Beispielen wird erläutert, wie Sie Snapshots über die Befehlszeile erstellen. Die YaST-Schnittstelle für Snapper wird hier nicht explizit beschrieben, bietet jedoch die gleiche Funktionalität.

Tipp: Snapshot-Beschreibung

Geben Sie stets eine aussagekräftige Beschreibung an, mit der der Zweck des Snapshots auch später noch eindeutig erkennbar ist. Mit der Option `--userdata` können Sie auch weitere Informationen angeben.

`snapper create --from` *17* **`--description "with package2"`**

Erstellt aus einem bestehenden Snapshot einen eigenständigen Snapshot (Typ „Einzeln“). Er wird durch die Zahl des Snapshots von **`snapper list`** angegeben. (Dies gilt für Snapper Version 0.8.4 und neuere Versionen.)

`snapper create --description "Snapshot for week 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 "Cleanup 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 "Daily data backup" --cleanup-algorithm timeline`

Erstellt einen eigenständigen Snapshot (Einzeltyp) für die benutzerdefinierte Konfiguration (`home`) mit einer Beschreibung. Der Snapshot wird automatisch gelöscht, sobald die Kriterien für den Zeitleisten-Bereinigungsalgorithmus in der Konfiguration erfüllt sind.

`snapper create --type pre --print-number --description "Before the Apache config cleanup" --userdata "important=yes"`

Erstellt einen Snapshot vom `pre`-Typ und gibt die Snapshot-Nummer aus. Erster Befehl zum Erstellen eines Snapshot-Paars, mit dem der „Vorher“- und „Nachher“-Zustand festgehalten wird. Der Snapshot wird als wichtig gekennzeichnet.

`snapper create --type post --pre-number 30 --description "After the Apache config cleanup" --userdata "important=yes"`

Erstellt einen Snapshot vom `post`-Typ, gepaart mit der `pre`-Snapshot-Nummer `30`. Zweiter Befehl zum Erstellen eines Snapshot-Paars, mit dem der „Vorher“- und „Nachher“-Zustand festgehalten wird. Der Snapshot wird als wichtig gekennzeichnet.

`snapper create --command` *`COMMAND`* `--description "Before and after COMMAND"`

Erstellt automatisch ein Snapshot-Paar vor und nach dem Ausführen von *`COMMAND`*. Diese Option ist nur verfügbar, wenn Snapper in der Befehlszeile verwendet wird.

10.6.3 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 Befehlszeile bearbeiten. Die Anpassung ist über die YaST-Oberfläche ganz einfach.

Um einen Snapshot in der Befehlszeile 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 auf `timeline` festgelegt.

`snapper --config home modify --description "daily backup" -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.

10.6.4 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 Befehlszeilenwerkzeug 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: Nicht referenzierte Snapshots löschen

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 in *Abschnitt 10.6.1.2, „Bereinigungsalgorithmen“*.

10.7 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.

10.7.1 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 diese Option aktiviert, werden Snapshot-Paare gelöscht, wenn die Gesamtzahl der Snapshots eine mit `NUMBER_LIMIT`und/oder `NUMBER_LIMIT_IMPORTANT` angegeben Anzahl *und* ein mit `NUMBER_MIN_AGE` angegebenes Alter überschreitet. Gültige Werte sind: `yes` (Aktivieren), `no` (Deaktivieren).
Der Standardwert ist `"yes"`.
Beispielbefehl zum Ändern oder Festlegen:

```
> 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. 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`. Die Bereinigungsalgorithmen löschen Snapshots über dem angegebenen Maximalwert, ohne den Snapshot und den Speicherplatz im Dateisystem zu berücksichtigen. Die Algorithmen löschen auch Snapshots über dem Mindestwert, bis die Grenzwerte für den Snapshot und das Dateisystem erreicht sind.
Beispielbefehl zum Ändern oder Festlegen:

```
> sudo snapper -c CONFIG set-config "NUMBER_LIMIT=10"
```

Wichtig: Bereichswerte im Vergleich zu Fixwerten

Wenn die Quotenunterstützung aktiviert ist (siehe *Abschnitt 10.7.5, „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 ist `"1800"`.
Beispielbefehl zum Ändern oder Festlegen:

```
> sudo snapper -c CONFIG set-config "NUMBER_MIN_AGE=864000"
```

Anmerkung: Grenzwert und Alter

`NUMBER_LIMIT`, `NUMBER_LIMIT_IMPORTANT` und `NUMBER_MIN_AGE` werden immer bewertet. 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 keine Snapshots beibehalten möchten, die über ein bestimmtes Alter hinausgehen, legen Sie `NUMBER_LIMIT*` auf `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
```

10.7.2 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 diese Option aktiviert, werden Snapshots gelöscht, wenn die Gesamtzahl der Snapshots eine mit `TIMELINE_LIMIT_*` angegeben Anzahl *und* ein mit `TIMELINE_MIN_AGE` angegebenes Alter überschreitet. Gültige Einstellungen: `yes`, `no`.

Der Standardwert ist `"yes"`.

Beispielbefehl zum Ändern oder Festlegen:

```
> 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 ist `"1800"`.

BEISPIEL 10.1: 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 immer beide bewertet. 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.

10.7.3 Bereinigen von Snapshot-Paaren, die sich nicht unterscheiden

Wie in *Abschnitt 10.1.2, „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 ist `"yes"`.

`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 ist `"1800"`.

10.7.4 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.

10.7.5 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.

Btrfs-Quotas werden Subvolumes zugewiesen, nicht Benutzern. Zusätzlich zur Verwendung von Btrfs-Quotas können Sie Quotas für Festplattenspeicherplatz zu Benutzern und Gruppen zuweisen (beispielsweise mit dem Befehl **`quota`**).

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 10.5, „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. Es wird daher empfohlen, 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.

10.8 Anzeigen von exklusiv für Snapshots verwendetem Festplattenspeicherplatz

Snapshots geben Daten frei, um den Speicherplatz effizient zu nutzen. Daher wird mit üblichen Befehlen wie **du** und **df** der belegte Speicherplatz nicht genau gemessen. Wenn Sie in Btrfs mit aktivierten Quotas Speicherplatz freigeben möchten, müssen Sie wissen, wie viel exklusiver Speicherplatz von jedem Snapshot belegt wird, im Gegensatz zum gemeinsamen Speicherplatz. Snapper ab Version 0.6 gibt den belegten Festplattenspeicherplatz für jeden Snapshot in der Spalte `Used Space` an:

```
# snapper --iso list
  # | Type   | Pre # | Date                | User | Used Space | Cleanup | Description
       | Userdata
----+--------+-------+---------------------+------+------------+---------
+----------------------+-------------
 0  | single |       |                     | root |            |         | current
       |
 1* | single |       | 2019-07-22 13:08:38 | root |  16.00 KiB |         | first root
 filesystem |
 2  | single |       | 2019-07-22 14:21:05 | root |  14.23 MiB | number  | after
 installation    | important=yes
 3  | pre    |       | 2019-07-22 14:26:03 | root | 144.00 KiB | number  | zypp(zypper)
       | important=no
 4  | post   |     3 | 2019-07-22 14:26:04 | root | 112.00 KiB | number  |
       | important=no
 5  | pre    |       | 2019-07-23 08:19:36 | root | 128.00 KiB | number  | zypp(zypper)
       | important=no
 6  | post   |     5 | 2019-07-23 08:19:43 | root |  80.00 KiB | number  |
       | important=no
 7  | pre    |       | 2019-07-23 08:20:50 | root | 256.00 KiB | number  | yast sw_single
       |
 8  | pre    |       | 2019-07-23 08:23:22 | root | 112.00 KiB | number  |
 zypp(ruby.ruby2.5)    | important=no
 9  | post   |     8 | 2019-07-23 08:23:35 | root |  64.00 KiB | number  |
       | important=no
10  | post   |     7 | 2019-07-23 08:24:05 | root |  16.00 KiB | number  |
       |
```

Mit dem Befehl **btrfs** wird der von Snapshots belegte Speicherplatz anders angezeigt:

```
# btrfs qgroup show -p /
qgroupid         rfer         excl parent
--------         ----         ---- ------
0/5          16.00KiB     16.00KiB ---
```

```
[...]
0/272         3.09GiB     14.23MiB 1/0
0/273         3.11GiB    144.00KiB 1/0
0/274         3.11GiB    112.00KiB 1/0
0/275         3.11GiB    128.00KiB 1/0
0/276         3.11GiB     80.00KiB 1/0
0/277         3.11GiB    256.00KiB 1/0
0/278         3.11GiB    112.00KiB 1/0
0/279         3.12GiB     64.00KiB 1/0
0/280         3.12GiB     16.00KiB 1/0
1/0           3.33GiB    222.95MiB ---
```

In der Spalte `qgroupid` wird die Kennung für jedes Subvolume angezeigt und eine Kombination aus qgroup-Ebene und ID zugewiesen.

In der Spalte `rfer` wird die Gesamtanzahl der Daten angezeigt, auf die im Subvolume verwiesen wird.

In der Spalte `excl` werden die exklusiven Daten in jedem Subvolume angezeigt.

In der Spalte `parent` wird die übergeordnete qgroup der Subvolumes angezeigt.

Im letzten Element `1/0` wird die Gesamtanzahl für die übergeordnete qgroup angezeigt. Im obigen Beispiel werden 222,95 MiB freigegeben, wenn alle Subvolumes entfernt werden. Führen Sie folgenden Befehl aus, um zu sehen, welche Snapshots den einzelnen Subvolumes zugeordnet sind:

```
# btrfs subvolume list -st /
ID gen top level path
-- --- --------- ----
267 298 266  @/.snapshots/1/snapshot
272 159 266  @/.snapshots/2/snapshot
273 170 266  @/.snapshots/3/snapshot
274 171 266  @/.snapshots/4/snapshot
275 287 266  @/.snapshots/5/snapshot
276 288 266  @/.snapshots/6/snapshot
277 292 266  @/.snapshots/7/snapshot
278 296 266  @/.snapshots/8/snapshot
279 297 266  @/.snapshots/9/snapshot
280 298 266  @/.snapshots/10/snapshot
```

Ein Upgrade von einem Service Pack auf das nächste führt zu Snapshots, die viel Festplattenspeicherplatz in den System-Subvolumes belegen. Es wird daher empfohlen, diese Snapshots manuell zu löschen, sobald Sie sie nicht mehr benötigen. Ausführliche Informationen finden Sie in *Abschnitt 10.6.4, „Löschen von Snapshots“*.

10.9 Häufig gestellte Fragen

F: *Warum zeigt Snapper nie Änderungen in `/var/log`, `/tmp` und anderen Verzeichnissen an?*

A: Bestimmte Verzeichnisse werden aus Snapshots ausgeschlossen. Weitere Informationen und Begründungen finden Sie unter *Abschnitt 10.1.3, „Verzeichnisse, die aus Snapshots ausgenommen sind“*. Sollen für einen Pfad keine Snapshots angefertigt werden, legen Sie ein Subvolume für diesen Pfad an.

F: *Kann ich einen Snapshot über den Bootloader booten?*

A: Ja. Weitere Informationen finden Sie in *Abschnitt 10.3, „System-Rollback durch Booten aus Snapshots“*.

F: *Kann ein Snapshot geschützt werden, sodass er nicht gelöscht wird?*

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 10.6.2, „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:

   ```
   > sudo snapper list -a
   ```

2. Merken Sie sich die Zahl der Snapshots, deren Löschung Sie verhindern möchten.

3. Führen Sie den folgenden Befehl aus und ersetzen Sie die Zahlenplatzhalter durch die Zahlen, die Sie sich gemerkt haben:

   ```
   > 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/.

11 Live-Kernel-Patching mit KLP

In diesem Dokument werden die Grundlagen der Kernel Live Patching-Technologie (KLP) erläutert und Sie finden hier Richtlinien für den SLE Live Patching-Dienst.

Mit KLP können die neuesten Sicherheitsaktualisierungen ohne Neustart auf Linux-Kernel angewendet werden. So erzielen Sie die maximale Betriebszeit und Verfügbarkeit des Systems, was insbesondere bei unternehmenswichtigen Systemen von Bedeutung ist.

Die Angaben in diesem Dokument gelten für die AMD64/Intel 64-, POWER- und IBM Z-Architekturen.

11.1 Vorteile des Kernel Live Patching

KLP bietet mehrere Vorteile.

- Wenn Unternehmen bestimmte Compliance-Zertifizierungen beantragen oder beibehalten möchten, sind sie darauf angewiesen, eine große Anzahl an Servern automatisch auf dem neuesten Stand zu halten. KLP kann dazu beitragen, die Compliance zu erzielen und gleichzeitig den Bedarf an kostspieligen Wartungsfenstern zu senken.
- Unternehmen, die mit Verträgen zur Vereinbarung zum Servicelevel arbeiten, müssen für Ihr System ein bestimmtes Maß an Verfügbarkeit und Betriebszeit garantieren. Mit Live Patching ist es möglich, Systeme ohne Ausfallzeiten zu patchen.
- KLP ist Teil des standardmäßigen Systemaktualisierungsmechanismus, sodass keine besondere Schulung oder Einführung komplizierter Wartungsroutinen anfällt.

11.2 Überblick über Kernel Live Patching

Kernel-Live-Patches werden in Form von Paketen mit modifiziertem Code bereitgestellt, die vom Kernel-Hauptpaket getrennt sind. Die Live-Patches sind kumulativ; der jeweils neueste Patch enthält also alle Fehlerbehebungen aus den vorhergehenden Patches für das Kernel-Paket. Jedes Kernel-Live-Paket ist an die genaue Kernel-Version gebunden, für die es ausgegeben wird. Die Versionsnummer des Live-Patch-Pakets erhöht sich bei jedem Hinzufügen von Fehlerbehebungen.

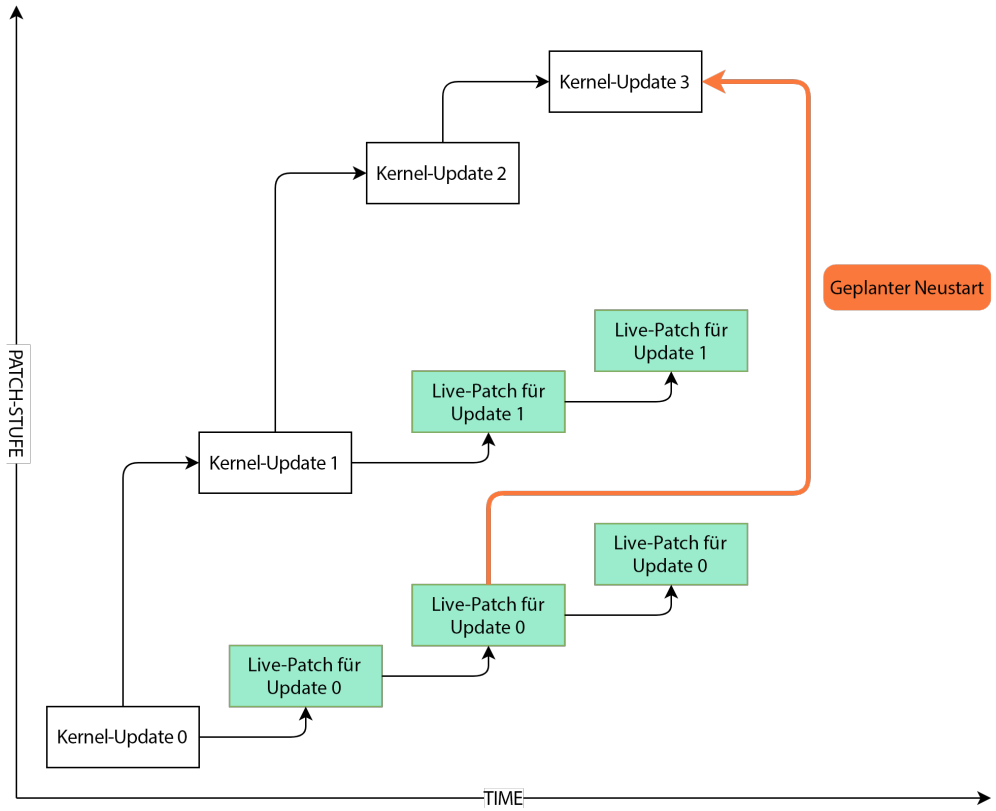
Anmerkung: Live-Patches und der ausgeführte Kernel

Um den Kernel-Patching-Status zu bestimmen, verwenden Sie den Befehl **`klp -v patches`**. Die Ausgabe des Befehls **`uname`** ändert sich für gepatchte Kernel nicht.

Wichtig: Live-Patches im Vergleich zu Kernel-Aktualisierungen

Live-Patches enthalten nur wichtige Korrekturen und ersetzen keine regulären Kernel-Updates, die einen Neustart erfordern. Betrachten Sie Live-Patches als vorübergehende Maßnahmen, die den Kernel schützen, bis ein ordnungsgemäßes Kernel-Update und ein Neustart vorgenommen werden.

Das folgende Diagramm veranschaulicht die allgemeine Beziehung zwischen Live-Patches und Kernel-Updates. Die Liste der CVEs (Common Vulnerabilities and Exposures) und Fehlerberichte, die vom derzeit aktiven Live-Patch behoben wurden, kann mit dem Befehl **`klp -v patches`** angezeigt werden.



Es ist möglich, mehrere Versionen des Kernel-Pakets zusammen mit den jeweiligen Live-Patches zu installieren. Diese Pakete lösen keine Konflikte aus. Sie können aktualisierte Kernel-Paket zusammen mit Live-Patches für den ausgeführten Kernel installieren. In diesem Fall werden Sie möglicherweise aufgefordert, das System neu zu starten. Benutzer mit SLE Live Patching-Abonnements haben Anspruch auf technischen Support, solange Live-Patch-Aktualisierungen für den ausgeführten Kernel vorliegen (siehe *Abschnitt 11.5.1, „Prüfen des Ablaufdatums des Live-Patches“*).

Wenn KLP aktiviert ist, umfasst jede Kernel-Aktualisierung auch ein Live-Patch-Paket. Dieser Live-Patch enthält keine Korrekturen und dient als Seed für zukünftige Live-Patches für den entsprechenden Kernel. Diese leeren, grundlegenden Patches werden als `initial patches` bezeichnet.

11.2.1 Umfang des Kernel Live Patching

Das Live-Patching von SLE umfasst Korrekturen für Schwachstellen und Fehlerbehebungen des SUSE Common Vulnerability Scoring System (CVSS; SUSE CVSS basiert auf dem CVSS v3.1-System) Level 7+ in Verbindung mit Systemstabilität oder Datenbeschädigungen. Es ist jedoch nicht in jedem Fall technisch praktikabel, Live-Patches für alle Fehlerbehebungen in den angegebenen Kategorien zu erstellen. SUSE behält sich daher das Recht vor, Fehlerbehebungen in Situationen zu überspringen, in denen ein Kernel-Live-Patch aus technischen Gründen nicht möglich ist. Derzeit werden mehr als 95 % der geeigneten Fehlerbehebungen als Live-Patches bereitgestellt. Weitere Informationen zum CVSS (der Grundlage für die SUSE-CVSS-Einstufung) finden Sie unter Common Vulnerability Scoring System SIG (https://www.first.org/cvss/).

11.2.2 Einschränkungen des Kernel Live Patching

Kernel Live Patching (KLP) umfasst das Ersetzen von Funktionen und das ordnungsgemäße Verarbeiten des Austauschs von voneinander abhängigen Funktionssätzen. Hierbei werden Aufrufe von älterem Code an aktualisierten Code weitergeleitet, der sich an einem anderen Speicherort befindet. Änderungen in den Datenstrukturen erschweren die Situation, da die Daten beibehalten werden und nicht erweitert oder neu interpretiert werden können. Es gibt zwar einige Methoden für die indirekte Veränderung von Datenstrukturen, doch bestimmte Fehlerbehebungen können nicht in Live-Patches konvertiert werden. In dieser Situation ist ein Neustart des Systems die einzige Möglichkeit, die Fehlerbehebungen anzuwenden.

11.3 Aktivieren von Kernel Live Patching mit YaST

Um KLP auf Ihrem System zu aktivieren, benötigen Sie aktive Live-Patching-Abonnements für SLES und SLE. Besuchen Sie das SUSE Customer Center (https://scc.suse.com/), um den Status Ihrer Abonnements zu überprüfen und einen Registrierungscode für das SLE-Live-Patching-Abonnement zu erhalten.

So aktivieren Sie Kernel Live Patching auf dem System:

1. Führen Sie den Befehl **`yast2 registration`** aus und klicken Sie auf *Erweiterungen auswählen*.
2. Wählen Sie in der Liste der verfügbaren Erweiterungen den Eintrag *SUSE Linux Enterprise Live Patching 15* und klicken Sie auf *Weiter*.
3. Bestätigen Sie die Lizenzvereinbarung und klicken Sie auf *Weiter*.
4. Geben Sie Ihren Registrierungscode für SLE Live Patching ein und klicken Sie auf *Weiter*.
5. Prüfen Sie den *Installationsüberblick* und die ausgewählten *Schemata*. Die Schemata `Live Patching` und `SLE Live Patching Lifecycle Data` sollten automatisch für die Installation zusammen mit zusätzlichen Paketen ausgewählt werden, um Abhängigkeiten gerecht zu werden.
6. Schließen Sie die Installation mit *Akzeptieren* ab. Dadurch werden die Basiskomponenten von Kernel Live Patching auf Ihrem System installiert sowie der ursprüngliche Live-Patch und die erforderlichen Abhängigkeiten.

11.4 Aktivieren von Kernel Live Patching über die Befehlszeile

Um Kernel Live Patching zu aktivieren, benötigen Sie aktive Live-Patching-Abonnements für SLES und SLES. Besuchen Sie das SUSE Customer Center (https://scc.suse.com/), um den Status Ihrer Abonnements zu überprüfen und einen Registrierungscode für das SLES-Live-Patching-Abonnement zu erhalten.

1. Führen Sie **`sudo SUSEConnect --list-extensions`**. Beachten Sie den genauen Aktivierungsbefehl für SLES Live Patching. Beispielausgabe des Befehls (gekürzt):

   ```
   $ SUSEConnect --list-extensions
   ```

```
...
SUSE Linux Enterprise Live Patching 15 SP7 x86_64
Activate with: SUSEConnect -p sle-module-live-patching/15.7/x86_64 \
  -r ADDITIONAL REGCODE
```

2. Aktivieren Sie SLES Live Patching mit dem erhaltenen Befehl, gefolgt von `-r` *`LIVE_PATCHING_REGISTRATION_CODE`*, beispielsweise:

```
SUSEConnect -p sle-module-live-patching/15.7/x86_64 \
  -r LIVE_PATCHING_REGISTRATION_CODE
```

3. Installieren Sie die erforderlichen Pakete und Abhängigkeiten mit dem Befehl **`zypper install -t pattern lp_sles`**.

Zu diesem Zeitpunkt sind die Live-Patches für das System bereits angewendet.

So funktioniert der Prozess hinter den Kulissen: Wenn das Paketinstallationssystem erkennt, dass ein installierter Kernel vorhanden ist, der live gepatcht werden kann, und dass ein Live-Patch dafür im Software-Kanal vorhanden ist, wählt das System den Live-Patch für die Installation aus. Der Kernel erhält dann die Live-Patch-Fehlerbehebungen *als Teil der Paketinstallation*. Der Live-Patch für den Kernel wird noch vor Abschluss der Produktinstallation durchgeführt.

11.5 Durchführen von Kernel Live Patching

Kernel-Live-Patches werden im Rahmen von regulären Systemaktualisierungen installiert. Es sind jedoch einige Dinge zu beachten.

- Der Kernel ist live-gepatcht, wenn ein `kernel-livepatch-*`-Paket für den aktuellen Kernel installiert wurde. Mit dem Befehl **`zypper se --details kernel-livepatch-*`** können Sie prüfen, welche Kernel-Live-Patch-Pakete auf Ihrem System installiert sind.

- Wenn das Paket `kernel-default` installiert ist, fordert der Update-Manager Sie auf, das System neu zu starten. Damit diese Meldung nicht angezeigt wird, können Sie Kernel-Aktualisierungen aus dem Patching-Vorgang herausfiltern. Hierzu können Sie Paketsperren mit Zypper hinzufügen. Mit SUSE Multi-Linux Manager ist es auch möglich, Kanalinhalte zu filtern (siehe Live-Patching mit SUSE Multi-Linux Manager (https://documentation.suse.com/suma/5.0/en/suse-manager/administration/live-patching.html)).

- Sie können den Patching-Status mit dem Befehl **`klp status`** prüfen. Zur Untersuchung installierter Patches führen Sie den Befehl **`klp -v patches`** aus.

- Denken Sie daran: Es können zwar mehrere Kernel-Pakete auf dem System installiert sein, doch es kann immer nur eines dieser Pakete ausgeführt werden, nicht mehrere Pakete gleichzeitig. Ebenso können mehrere Live-Patch-Pakete installiert sein, doch es wird immer nur ein Live-Patch in den Kernel geladen.
- Der aktive Live-Patch ist in der `initrd` enthalten. Bei einem unvorhergesehenen Neustart fährt das System also mit den angewendeten Live-Patches hoch, sodass Sie das Patching nicht wiederholen müssen.

11.5.1 Prüfen des Ablaufdatums des Live-Patches

Stellen Sie sicher, dass das `lifecycle-data-sle-module-live-patching` installiert ist, und führen Sie dann den Befehl **`zypper lifecycle`** aus. In Abschnitt `Package end of support if different from product` der Ausgabe sehen Sie das Ablaufdatum für den jeweiligen Live-Patch.

Jeder Live-Patch wird ein Jahr ab Veröffentlichung des zugrunde liegenden Kernel-Pakets aktualisiert. Auf der Seite Maintained kernels, patch updates and lifecycle (https://www.suse.com/products/live-patching/current-patches/) können Sie das Ablaufdatum anhand der ausgeführten Kernel-Version prüfen, ohne die Produkterweiterung zu installieren.

11.6 Fehlerbehebung bei Kernel Live Patching-Problemen

11.6.1 Manuelles Patch-Downgrade

Wenn der neueste Live-Patch Probleme verursacht, können Sie ein Downgrade des aktuell installierten Live-Patches auf die vorhergehende Version durchführen. Es wird empfohlen, das Patch-Downgrade vorzunehmen, bevor das System erste Probleme zeigt. Denken Sie daran, dass ein System mit Kernel-Warnungen oder Kernel-Fehlerspuren im Systemprotokoll unter Umständen nicht für das Patch-Downgrade-Verfahren geeignet ist. Wenn Sie nicht sicher sind, ob das System die Anforderungen für ein Patch-Downgrade erfüllt, fragen Sie den technischen Support von SUSE.

VORGEHEN 11.1: MANUELLES PATCH-DOWNGRADE

1. Ermitteln Sie den automatischen Live-Patch mit dem Befehl **`klp -v patches`**. Der aktuell ausgeführte Patch befindet sich in der Zeile, die mit `RPM:` beginnt. Beispiel:

   ```
   RPM: kernel-livepatch-6_4_0-150700_38-default-1-150700.1.23.x86_64
   ```

   `6_4_0-150600_9-default` im Beispiel oben bezeichnet die genaue ausgeführte Kernel-Version.

2. Verwenden Sie den Befehl **`zypper search -s kernel-livepatch-`***`RUNNING_KERNEL_VERSION`***`-default`**, um nach früheren Patch-Versionen zu suchen. Der Befehl gibt eine Liste der verfügbaren Paketversionen zurück. Denken Sie daran, dass die Versionsnummer bei jeder Veröffentlichung eines neuen Live-Patch-Pakets um eins erhöht wird. Wählen Sie die Versionsnummer aus, die um eine Veröffentlichung niedriger ist als die aktuelle Version.

3. Installieren Sie die gewünschte Version mit dem Befehl **`zypper in --oldpackage kernel-livepatch-`***`RUNNING_KERNEL_VERSION`***`-default=`***`DESIRED_VERSION`**.

12 Userspace-Live-Patching

Dieses Kapitel beschreibt die Grundprinzipien und die Verwendung von Userspace-Live-Patching.

12.1 Info zu Userspace-Live-Patching

Das Userspace-Live-Patching (ULP) bezeichnet die Anwendung von Patches auf Bibliotheken, die von laufenden Prozessen verwendet werden, ohne diese zu unterbrechen. Jedes Mal, wenn eine Sicherheitskorrektur als Live-Patch verfügbar ist, werden die Kundendienste nach der Anwendung des Live-Patches ohne Neustart der Prozesse gesichert.

ULP wird auf folgenden Architekturen unterstützt:

- AMD64/Intel 64
- ppc64le (ab SUSE Linux Enterprise Desktop 15 SP7)

Live-Patching-Vorgänge werden mit dem Werkzeug `ulp` durchgeführt, das Teil von `libpulp` ist. `libpulp` ist ein Framework, das aus der `libpulp.so`-Bibliothek und der **`ulp`**-Binärdatei besteht, die dafür sorgt, dass Bibliotheken live gepatcht werden können, und Live-Patches anwendet.

Tipp

Sie können den Befehl **`ulp`** entweder als normaler Benutzer oder als privilegierter Benutzer über den Mechanismus **`sudo`** ausführen. Der Unterschied besteht darin, dass Sie durch Ausführen von **`ulp`** über **`sudo`** Informationen über ausgeführte Prozesse oder Patch-Prozesse nach `root` anzeigen können.

12.1.1 Voraussetzungen

Für das ULP müssen zwei Anforderungen erfüllt sein.

- Installieren Sie das ULP auf Ihrem System, indem Sie Folgendes ausführen:

```
> sudo zypper in libpulp0 libpulp-tools
```

- Anwendungen mit gewünschter Live-Patch-Unterstützung müssen vor dem Laden der Bibliothek `libpulp.so.0` gestartet werden. Weitere Einzelheiten finden Sie in *Abschnitt 12.1.3, „Verwenden von `libpulp`“*.

12.1.2 Unterstützte Bibliotheken

Derzeit werden nur `glibc` und `openssl` (`openssl1_1` und `openssl-3`) unterstützt. Weitere Pakete werden verfügbar sein, sobald sie für das Live-Patching vorbereitet sind. Um `glibc`- und `openssl-1_1`--Live-Patches zu erhalten, installieren Sie folgende Pakete:

```
> zypper install glibc-livepatches openssl-1_1-livepatches openssl-3-livepatches
```

12.1.3 Verwenden von `libpulp`

Um Live-Patching für eine Anwendung zu aktivieren, müssen Sie die Bibliothek `libpulp.so.0` beim Starten der Anwendung vorladen:

```
> LD_PRELOAD=/usr/lib64/libpulp.so.0 APPLICATION_CMD
```

12.1.3.1 Prüfen, ob Live-Patching für eine Bibliothek möglich ist

Prüfen Sie mit dem folgenden Befehl, ob Live-Patching für eine Bibliothek möglich ist:

```
> ulp livepatchable PATH_TO_LIBRARY
```

12.1.3.2 Prüfen, ob eine `.so`-Datei ein Live-Patch-Container ist

Ein gemeinsam genutztes Objekt (`.so`) ist ein Live-Patch-Container, wenn es die ULP-Patch-Beschreibung enthält. Sie können dies mit dem folgenden Befehl überprüfen:

```
> readelf -S SHARED_OBJECT | grep .ulp
```

Wenn die Ausgabe zeigt, dass das gemeinsam genutzte Objekt sowohl als den Abschnitt `.ulp` als auch `.ulp.rev` enthält, handelt es sich um einen Live-Patch-Container.

12.1.3.3 Anwenden von Live-Patches

Von SUSE bereitgestellte Live-Patches werden über die üblichen Updates ausgeliefert, wenn folgende Pakete installiert sind: `glibc-livepatches` `openssl-livepatches` `openssl-3-livepatches`.

Benutzerdefinierte Live-Patches werden mit dem Befehl **`ulp trigger`** angewendet. Beispiel:

```
> ulp trigger -p PID LIVEPATCH.so
```

Ersetzen Sie `PID` durch die Prozess-ID des laufenden Prozesses, der die zu patchende Bibliothek verwendet, und `LIVEPATCH.so` durch die tatsächliche Live-Patch-Datei. Der Befehl gibt eine der folgenden Statusmeldungen zurück:

ERFOLG

Der Live-Patching-Vorgang war erfolgreich.

ÜBERSPRUNGEN

Der Patch wurde übersprungen, da er nicht für eine Bibliothek konzipiert wurde, die bei diesem Prozess geladen wird.

FEHLER

Es ist ein Fehler aufgetreten und Sie können weitere Informationen abrufen, indem Sie den internen `libpulp`-Nachrichtenpuffer prüfen. Weitere Informationen zu diesem Thema finden Sie in *Abschnitt 12.1.3.6, „Anzeigen der internen Nachrichtenwarteschlange“*.

Es ist auch möglich, mehrere Live-Patches anzuwenden, indem Sie z. B. Platzhalter verwenden:

```
> ulp trigger '*.so'
```

Der Befehl versucht, jeden Patch im aktuellen Ordner auf jeden Prozess anzuwenden, der die Bibliothek `libpulp` geladen hat. Wenn der Patch nicht für den Prozess geeignet ist, wird er automatisch übersprungen. Am Ende zeigt das Werkzeug an, wie viele Patches es erfolgreich auf wie viele Prozesse angewendet hat.

12.1.3.4 Zurücksetzen von Live-Patches

Mit dem Befehl **`ulp trigger`** können Sie Live-Patches zurücksetzen. Für das Zurücksetzen von Live-Patches stehen zwei Möglichkeiten zur Auswahl. Sie können einen Live-Patch zurücksetzen, indem Sie den Schalter `--revert` verwenden und den Live-Patch-Container übergeben:

```
> ulp trigger -p PID --revert LIVEPATCH.so
```

Alternativ können Sie alle Patches einer bestimmten Bibliothek entfernen, beispielsweise:

```
> ulp trigger -p PID --revert-all=LIBRARY
```

In dem Beispiel steht *LIBRARY* für die entsprechende Bibliothek, beispielsweise für `libcrypto.so.1.1`.

Der letztgenannte Ansatz kann nützlich sein, wenn der Quellcode des ursprünglichen Live-Patches nicht verfügbar ist. Oder Sie möchten einen bestimmten alten Patch entfernen und einen neuen anwenden, während die Zielanwendung weiterhin einen sicheren Code ausführt, z. B.:

```
> ulp trigger -p PID  --revert-all=libcrypto.so.1.1 new_livepatch2.so
```

12.1.3.5 Anzeigen angewendeter Patches

Mit dem folgenden Befehl können Sie überprüfen, auf welche Anwendungen Live-Patches angewendet wurden:

```
> ulp patches
```

Die Ausgabe zeigt, welche Bibliotheken live gepatcht werden können und welche Patches in Programme geladen werden und welche Fehler die Patches beheben:

```
PID: 10636, name: test
  Livepatchable libraries:
    in /lib64/libc.so.6:
      livepatch: libc_livepatch1.so
        bug labels: jsc#SLE-0000
    in /usr/lib64/libpulp.so.0:
```

Sie können auch feststellen, welche Funktionen durch den Live-Patch gepatcht werden:

```
> ulp dump LIVEPATCH.so
```

12.1.3.6 Anzeigen der internen Nachrichtenwarteschlange

Protokollmeldungen von `libpulp.so` werden in einem Puffer innerhalb der Bibliothek gespeichert und nur angezeigt, wenn der Benutzer dies anfordert. Um diese Meldungen anzuzeigen, führen Sie Folgendes aus:

```
> ulp messages -p PID
```

12.2 Weitere Informationen

Weitere Informationen zu `libpulp` finden Sie im Git-Repository (https://github.com/SUSE/libpulp) des Projekts.

13 Transaktionsaktualisierungen

Transaktionsaktualisierungen sind in SUSE Linux Enterprise Desktop als Technologievorschau für die Aktualisierung von SLES verfügbar, wenn das root-Dateisystem schreibgeschützt ist. Transaktionsaktualisierungen sind atomar – alle Aktualisierungen werden nur angewendet, wenn alle erfolgreich sind – und unterstützen Rollbacks. Es ist kein laufendes System betroffen, da Änderungen erst aktiviert werden, nachdem das System neu gebootet wurde. Da Reboots eine Störung darstellen, muss der Administrator entscheiden, ob ein Reboot kostspieliger ist als die Störung laufender Dienste. Wenn Reboots zu kostspielig sind, sollten Sie keine Transaktionsaktualisierungen verwenden.

Transaktionsaktualisierungen werden täglich vom Skript **`transactional-update`** ausgeführt. Das Skript prüft auf verfügbare Aktualisierungen. Falls Aktualisierungen vorhanden sind, erstellt es im Hintergrund einen neuen Snapshot des root-Dateisystems. Danach ruft es die Aktualisierungen von den Versionskanälen ab. Sobald der neue Snapshot aktualisiert wurde, wird er als aktiv gekennzeichnet und wird nach dem nächsten Reboot des Systems zum neuen standardmäßigen root-Dateisystem. Wenn **`transactional-update`** automatisch ausgeführt wird (das Standardverhalten), wird das System auch neu gebootet. Sowohl die Zeitdauer für den Aktualisierungsvorgang als auch das Wartungsfenster für den Reboot sind konfigurierbar.

Es können nur Pakete aktualisiert werden, die Teil des Snapshots des root-Dateisystems sind. Sollten die Pakete Dateien enthalten, die nicht Teil des Snapshots sind, dann könnte die Aktualisierung fehlschlagen oder das System beschädigen.

RPMs, die eine Lizenz benötigen, um akzeptiert zu werden, können nicht aktualisiert werden.

13.1 Nutzungsbeschränkungen

Derzeit gibt es bestimmte Einschränkungen bei der Funktionalität von Transaktionsaktualisierungen. Für die folgenden Pakete kann der Befehl **`transactional-update`** nicht verwendet werden:

- Die standardmäßige `index.html`-Seite von `nginx` ist möglicherweise nicht verfügbar.
- `tomcat-webapps` und `tomcat-admin-webapps`
- `phpMyAdmin`
- `sca-appliance-*`
- `mpi-selector`
- `emacs` funktioniert mit Ausnahme von Emacs-Spielen
- `bind` und `bind-chrootenv`
- `docbook*`
- `sblim-sfcb*`
- `texlive*`
- `iso_ent`
- `openjade`
- `opensp`
- `pcp`
- `plymouth`
- `postgresql-server-10`
- `pulseaudio-gdm-hooks`
- `smartmontools`

Die Aktualisierungskomponente des Systeminstallationsprogramms funktioniert nicht bei einem schreibgeschützten Dateisystem, weil es Transaktionsaktualisierungen nicht unterstützt.

Weitere Überlegungen:

- Es ist sinnvoll, den Zeitraum zwischen der Aktualisierung des Systems und dem Reboot des Rechners so kurz wie möglich zu halten.
- Es kann immer nur eine Aktualisierung angewendet werden. Nach jeder Aktualisierung und nach dem Anwenden der nächsten Aktualisierung muss ein Reboot erfolgen.
- **`update-alternatives`** sollte nach einer Transaktionsaktualisierung erst nach dem Reboot des Rechners ausgeführt werden.
- Erstellen Sie nach einer Transaktionsaktualisierung neue Systembenutzer oder Systemgruppen erst nach einem Reboot. Normale Benutzer und Gruppen (UID > 1000, GID > 1000) können jedoch erstellt werden.
- YaST ist noch nicht mit Transaktionsaktualisierungen vertraut. Es funktioniert nicht, wenn ein YaST-Modul zusätzliche Pakete installieren muss. Normale Systemvorgänge, die Konfigurationsdateien in `/etc`-Arbeit ändern.
- Für `php7-fastcgi` müssen Sie manuell einen symbolischen Link erstellen (`/srv/www/cgi-bin/php`), der auf `/usr/bin/php-cgi` zeigt.
- `ntp` ist Teil des Legacy-Moduls für die Migration von älteren SLES-Versionen. Es wird nicht auf einer neueren Installation von SUSE Linux Enterprise Desktop unterstützt und wurde ersetzt durch `chrony`. Wenn Sie `ntp` weiterhin verwenden, ist eine Neuinstallation erforderlich, damit die transaktionalen Updates korrekt funktionieren.
- `sblim-sfcb`: Das gesamte sblim-Ökosystem ist mit Transaktionsaktualisierungen kompatibel.
- **`btrfs-defrag`** aus dem Paket `btrfsmaintenance` funktioniert nicht mit einem schreibgeschützten Root-Dateisystem.
- Für **`btrfs-balance`** muss die Variable `BTRFS_BALANCE_MOUNTPOINTS` in `/etc/sysconfig/btrfsmaintenance` von `/` in `/.snapshots` geändert werden.
- Für **`btrfs-scrub`** muss die Variable `BTRFS_SCRUB_MOUNTPOINTS` in `/etc/sysconfig/btrfsmaintenance` von `/` in `/.snapshots` geändert werden.

13.2 Aktivieren von `transactional-update`

Sie müssen das Transaktionsserver-Modul bei der Systeminstallation aktivieren und dann die Transaktionsserver-Rolle auswählen. Die spätere Installation von Paketen vom Transaktionsserver-Modul in einem laufenden System wird NICHT unterstützt und könnte das System beschädigen.

Das Ändern des Subvolume-Layouts der Root-Partition oder das Ablegen von Unterverzeichnissen oder Subvolumes der Root-Partition in eigenen Partitionen (außer `/home`, `/var`, `/srv` und `/opt`) wird nicht unterstützt und kann das System beschädigen.

13.3 Verwalten von automatischen Aktualisierungen

Automatische Aktualisierungen werden von einem **`systemd.timer`** gesteuert, der einmal pro Tag ausgeführt wird. Damit werden alle Aktualisierungen angewendet und **`rebootmgrd`** wird informiert, dass der Rechner neu gebootet werden muss. Die Uhrzeit für die Ausführung der Aktualisierung kann angepasst werden. Weitere Informationen hierzu finden Sie unter systemd.timer(5). Informationen zum Anpassen des Wartungsfensters, in dem festgelegt wird, wann **`rebootmgrd`** das System neu bootet, finden Sie unter rebootmgrd(8).

Automatische Transaktionsaktualisierungen werden deaktiviert mit dem Befehl:

```
# systemctl --now disable transactional-update.timer
```

13.4 Das Kommando **`transactional-update`**

Mit dem Befehl **`transactional-update`** ist eine atomare Installation oder das Entfernen von Aktualisierungen möglich. Aktualisierungen werden nur dann angewendet, wenn alle erfolgreich installiert werden können. Mit **`transactional-update`** wird ein Snapshot von Ihrem System vor Anwenden der Aktualisierung erstellt. Dieser Snapshot kann wiederhergestellt werden. Alle Änderungen werden erst nach dem Reboot aktiv.

`--continue`

: Mit der Option **`--continue`** werden mehrere Änderungen an einem bestehenden Snapshot vorgenommen, ohne dass neu gebootet werden muss.

Das standardmäßige Verhalten von **`transactional-update`** besteht darin, einen neuen Snapshot vom aktuellen root-Dateisystem zu erstellen. Wenn Sie etwas vergessen, etwa die Installation eines neuen Pakets, müssen Sie einen Reboot ausführen, um die früheren Änderungen anzuwenden. Danach muss der Befehl **`transactional-update`** erneut ausgeführt werden, um das vergessene Paket zu installieren, und es muss erneut ein Reboot erfolgen. Sie können den Befehl **`transactional-update`** nicht mehrmals ohne Reboot zum Hinzufügen weiterer Änderungen zum Snapshot ausführen. Dadurch würden separate unabhängige Snapshots erstellt werden, die nicht die Änderungen der früheren Snapshots enthalten. Mit der Option **`--continue`** können Sie jedoch so viele Änderungen vornehmen, wie Sie möchten, ohne neu booten zu müssen. Es wird jedes Mal ein neuer Snapshot erstellt, der jeweils alle Änderungen der früheren Snapshots sowie die neuen Änderungen enthält. Wiederholen Sie diesen Vorgang beliebig oft und booten Sie das System neu, sobald der letzte Snapshot alle gewünschten Änderungen enthält. Der letzte Snapshot wird dann das neue Root-Dateisystem.

Als weitere nützliche Funktion der Option **`--continue`** können Sie jeden beliebigen vorhandenen Snapshot als Basis für Ihren neuen Snapshot auswählen. Im folgenden Beispiel wird gezeigt, wie **`transactional-update`** ausgeführt wird, um ein neues Paket in einem Snapshot basierend auf Snapshot 13 zu installieren. Danach wird es erneut ausgeführt, um ein weiteres Paket zu installieren:

```
# transactional-update pkg install package_1
```

```
# transactional-update --continue 13 pkg install package_2
```

Die Option **`--continue [num]`** ruft **`snapper create --from`** auf, siehe *Abschnitt 10.6.2, „Erstellen von Snapshots“*.

`cleanup`

Wenn das aktuelle root-Dateisystem mit dem aktiven root-Dateisystem identisch ist (nach einem Reboot, bevor **`transactional-update`** einen neuen Snapshot mit Aktualisierungen erstellt), wird für alle alten Snapshots ohne Bereinigungsalgorithmus ein Bereinigungsalgorithmus festgelegt. Dadurch wird sichergestellt, dass alte Snapshots von Snapper gelöscht werden. (Weitere Informationen finden Sie im Abschnitt zu Bereinigungsalgorithmen in Snapper (8).) Dadurch werden auch alle nicht referenzierten (und damit ungenutzten) `/etc`-Overlay-Verzeichnisse in `/var/lib/overlay` entfernt:

```
# transactional-update cleanup
```

`pkg in/install`

Installiert einzelne Paket aus den verfügbaren Kanälen mit dem Befehl **`zypper install`**. Mit diesem Befehl werden auch PTF(Program Temporary Fix)-RPM-Dateien installiert.

```
# transactional-update pkg install package_name
```

oder

```
# transactional-update pkg install rpm1 rpm2
```

`pkg rm/remove`

Entfernt einzelne Pakete vom aktiven Snapshot mit dem Befehl **`zypper remove`**. Mit diesem Befehl werden auch PTF-RPM-Dateien entfernt.

```
# transactional-update pkg remove package_name
```

`pkg up/update`

Aktualisiert einzelne Pakete vom aktiven Snapshot mit dem Befehl **`zypper update`**. Es können nur Pakete aktualisiert werden, die Teil des Snapshots des Basisdateisystems sind.

```
# transactional-update pkg update package_name
```

`up/update`

Wenn neue Aktualisierungen verfügbar sind, wird ein neuer Snapshot erstellt und mit **`zypper up/update`** der Snapshot aktualisiert.

```
# transactional-update up
```

`dup`

Wenn neue Aktualisierungen verfügbar sind, wird ein neuer Snapshot erstellt und mit **`zypper dup –no-allow-vendor-change`** der Snapshot aktualisiert. Der Snapshot wird anschließend aktiviert und wird nach einem Reboot zum neuen root-Dateisystem.

```
# transactional-update dup
```

`patch`

Wenn neue Aktualisierungen verfügbar sind, wird ein neuer Snapshot erstellt und mit **`zypper patch`** der Snapshot aktualisiert.

```
# transactional-update patch
```

`rollback`

Damit wird das Standard-Subvolume festgelegt. In Systemen mit einem Schreiben-Lesen-Dateisystem wird **`snapper rollback`** aufgerufen. In einem Nur-Lesen-Dateisystem ohne Argument wird das aktuelle System als neues standardmäßiges root-Dateisystem festge-

legt. Wenn Sie eine Zahl angeben, wird dieser Snapshot als das standardmäßige root-Dateisystem verwendet. In einem Nur-Lesen-Dateisystem werden keine zusätzlichen Snapshots erstellt.

```
# transactional-update rollback snapshot_number
```

`grub.cfg`

Damit wird eine neue GRUB2-Konfiguration erstellt. Manchmal muss die Boot-Konfiguration angepasst werden, beispielsweise durch Hinzufügen zusätzlicher Kernel-Parameter. Bearbeiten Sie */etc/default/grub*, führen Sie **transactional-update grub.cfg** aus und booten Sie dann neu, um die Änderung zu aktivieren. Sie müssen sofort einen Reboot ausführen, da ansonsten die neue GRUB2-Konfiguration bei der nächsten Ausführung von **transactional-update** mit dem Standardwert überschrieben wird.

```
# transactional-update grub.cfg
```

`reboot`

Dieser Parameter löst nach dem Abschluss der Aktion einen Reboot aus.

```
# transactional-update dup reboot
```

`--help`

Damit wird ein Hilfe-Bildschirm mit Optionen und Unterbefehlen gedruckt.

```
# transactional-update --help
```

13.5 Fehlersuche

Führen Sie bei einem fehlerhaften Upgrade **supportconfig** aus, um Protokolldaten zu erfassen. Übermitteln Sie die resultierenden Dateien einschließlich `/var/log/transactional-update.log` an den SUSE-Support.

14 Remote-Grafiksitzungen mit VNC

Über VNC (Virtual Network Computing) haben Sie über einen Grafik-Desktop Zugriff auf einen Remote-Rechner und können Remote-Grafikanwendungen ausführen. VNC ist plattformunabhängig und greift auf den Remote-Rechner über ein beliebiges Betriebssystem zu. In diesem Kapitel wird beschrieben, wie mit den Desktop-Clients vncviewer und Remmina eine Verbindung zu einem VNC-Server hergestellt und wie ein VNC-Server betrieben wird.

SUSE Linux Enterprise Desktop 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.

Ein VNC-Server kann beide Sitzungen gleichzeitig auf verschiedenen Ports bieten, eine geöffnete Sitzung kann jedoch nicht von einem Typ in den anderen konvertiert werden.

14.1 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 Desktop ist **`vncviewer`**, der im Paket `tigervnc` bereitgestellt wird.

14.1.1 Verbinden mithilfe der vncviewer-CLI

Mit folgendem Befehl können Sie den VNC-Viewer starten und eine Sitzung mit dem Server initiieren:

```
> vncviewer jupiter.example.com:1
```

Anstelle der VNC-Anmeldenummer können Sie auch die Portnummer mit zwei Doppelpunkten angeben:

```
> 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 beim Konfigurieren eines VNC-Servers auf dem Zielcomputer ausgewählt wird. Weitere Informationen finden Sie unter *Abschnitt 14.4, „Konfigurieren von permanenten VNC-Serversitzungen“*.

14.1.2 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 14.1.1, „Verbinden mithilfe der vncviewer-CLI“* ein und klicken Sie auf *Connect* (Verbinden).

ABBILDUNG 14.1: VNCVIEWER

14.1.3 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.

14.2 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.

14.2.1 Installation

Zum Verwenden von Remmina überprüfen Sie, ob das Paket `remmina` auf Ihrem System installiert ist. Falls nicht, installieren Sie es. Denken Sie daran, auch das VNC-Plugin für Remmina zu installieren:

```
# zypper in remmina remmina-plugin-vnc
```

14.2.2 Hauptfenster

Starten Sie Remmina mit dem Befehl **`remmina`**.

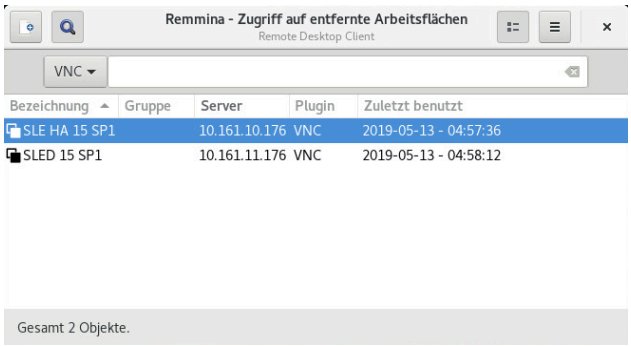


ABBILDUNG 14.2: HAUPTFENSTER VON REMMINA

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.

14.2.3 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.

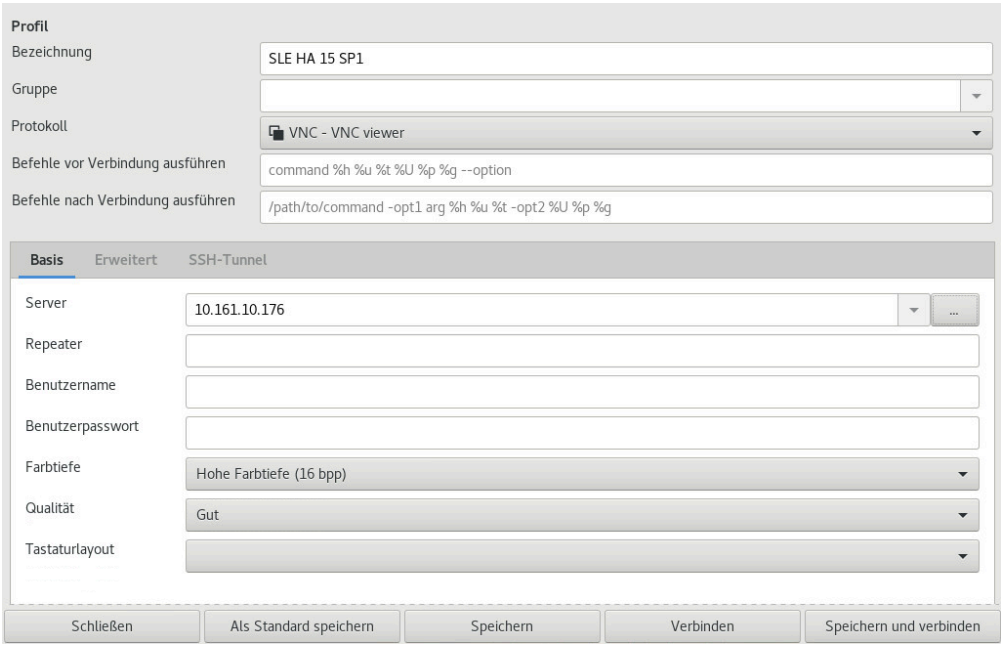


ABBILDUNG 14.3: REMOTE DESKTOP PREFERENCE

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 nun im Hauptfenster angezeigt.

14.2.4 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).

14.2.4.1 Schnellstart von Remote-Sitzungen

Mit dem Dropdown-Feld und dem Textfeld oben im Hauptfenster können Sie eine Remote-Sitzung per Schnellstart beginnen, ohne die Verbindungsdetails anzugeben und zu speichern.

ABBILDUNG 14.4: SCHNELLSTART

Wählen Sie das Kommunikationsprotokoll in der Dropdownliste 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` .

14.2.4.2 Öffnen von gespeicherten Remote-Sitzungen

Zum Öffnen einer bestimmten Remote-Sitzung doppelklicken Sie in der Sitzungsliste auf diese Sitzung.

14.2.4.3 Fenster der Remote-Sitzungen

Die Remote-Sitzungen werden in Registerkarten eines separaten Fensters geöffnet. Jede Registerkarte enthält eine Sitzung. Die Symbolleiste auf der linken Seite des Fensters hilft Ihnen beim Verwalten der Fenster/Sitzungen. Schalten Sie beispielsweise den Vollbildmodus um, passen Sie die Größe des Fensters an die Anzeigegröße der Sitzung, senden Sie bestimmte Tastenanschläge an die Sitzung, machen Sie Screenshots der Sitzung oder legen Sie die Bildqualität fest.

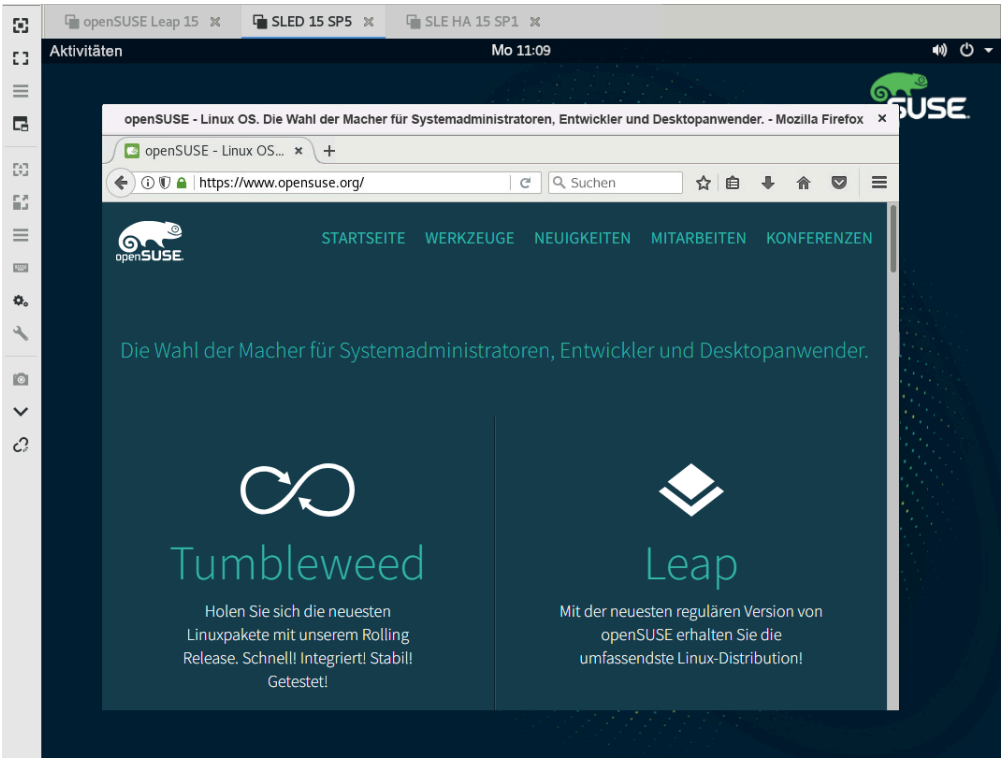


ABBILDUNG 14.5: REMMINA-REMOTE-SITZUNG MIT ANZEIGE

14.2.5 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 14.2.3, „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*.

14.2.6 Ausführen von Remote-Sitzungen über die Kommandozeile

Mit der folgenden Syntax öffnen Sie eine Remote-Sitzung über die Befehlszeile oder aus einer Stapeldatei heraus, ohne zunächst das Hauptanwendungsfenster zu öffnen:

```
> remmina -c profile_name.remmina
```

Die Profildateien von Remmina werden im Verzeichnis `.local/share/remmina/` Ihres Benutzerverzeichnisses 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.

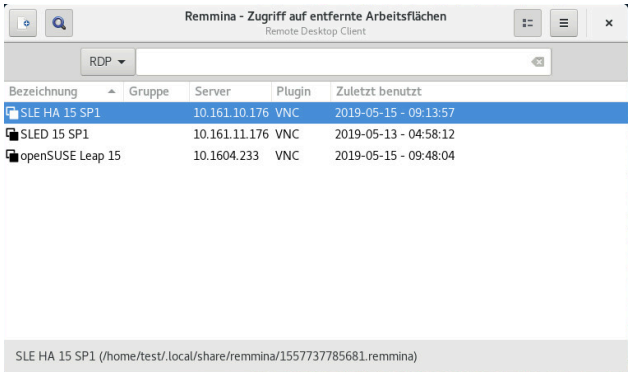


ABBILDUNG 14.6: PFAD ZUR PROFILDATEI

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.

14.3 Konfigurieren von einmaligen Sitzungen am VNC-Server

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.

VORGEHEN 14.1: 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 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.

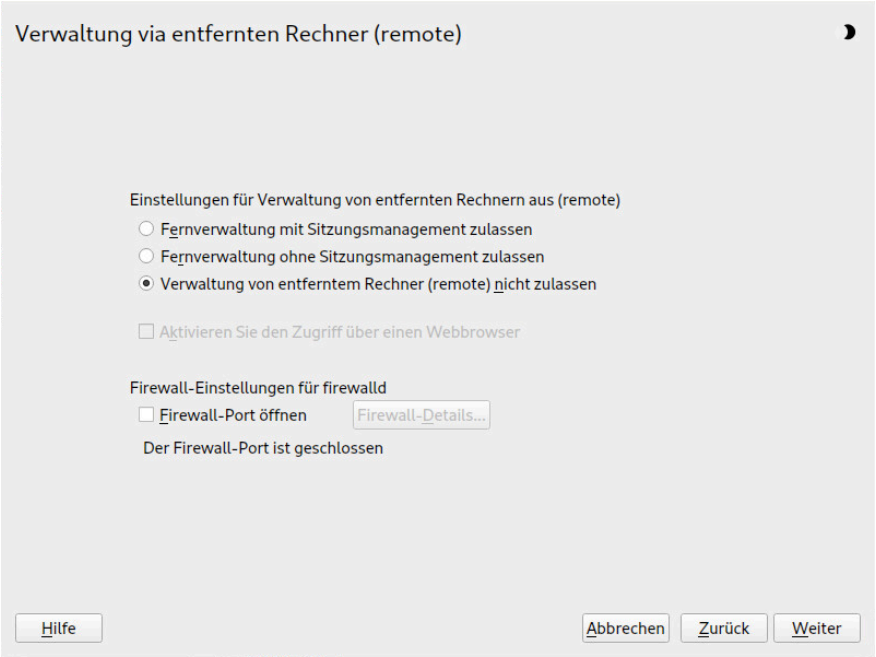


ABBILDUNG 14.7: FERNVERWALTUNG

14.3.1 Verfügbare Konfigurationen

Die Standardkonfiguration von SUSE Linux Enterprise Desktop 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. Bitten Sie Ihren Systemadministrator um Detailinformationen, wenn Sie die Konfiguration ändern müssen.

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. Wenn Sie das selbstsignierte Zertifikat verwenden, müssen Sie vor dem ersten Herstellen einer Verbindung die Signatur bestätigen – sowohl im VNC-Viewer als auch im Webbrowser.

Tipp

Bestimmte VNC-Clients weigern sich, eine sichere Verbindung über das standardmäßige selbstsignierte Zertifikat herzustellen. Beispielsweise überprüft der Vinagre-Client die Zertifizierung anhand des globalen GnuTLS-Vertrauensspeichers und es tritt ein Fehler auf, wenn das Zertifikat selbstsigniert ist. Verwenden Sie in einem solchen Fall entweder eine andere Verschlüsselungsmethode als `x509` oder generieren Sie ein ordnungsgemäß signiertes Zertifikat für den VNC-Server und importieren Sie es in den Systemvertrauensspeicher des Clients.

14.3.2 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 14.1, „Der* **`vncviewer`***-Client“*. Alternativ können Sie einen JavaScript-fähigen Webbrowser verwenden, um die VNC-Sitzung anzuzeigen. Geben Sie hierzu folgende URL ein: `http://jupiter.example.com:5801`.

14.3.3 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 einen JavaScript-Client (`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 Befehl:

```
> sudo systemctl reload xvnc.socket
```

Wichtig: Firewall und VNC-Ports

Wenn Sie die entfernte Verwaltung wie in *Prozedur 14.1, „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 and Hardening Guide“, Kapitel 23 „Masquerading and firewalls“*.

14.4 Konfigurieren von permanenten VNC-Serversitzungen

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 Schulungssitzungen, bei denen der Schulungsleiter 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 14.1, „Der* **`vncviewer`***-Client“*. Alternativ können Sie einen JavaScript-fähigen Webbrowser verwenden, um die VNC-Sitzung anzuzeigen. Geben Sie hierzu folgende URL ein: `http://jupiter.example.com:5801`.

14.4.1 Mit vncmanager initiierte VNC-Sitzung

VORGEHEN 14.2: 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.

14.4.1.1 Konfigurieren von permanenten VNC-Sitzungen

Sobald Sie die VNC-Sitzungsverwaltung gemäß *Prozedur 14.2, „Aktivieren von permanenten VNC-Sitzungen“* aktiviert haben, können Sie wie gewohnt eine Verbindung zur Remote-Sitzung über den herstellen, z. B. **vncviewer**vncviewer oder Remmina. 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. Wenn Ihre Desktop-Umgebung Symbole in der Taskleiste nicht unterstützt, führen Sie **vncmanager-controller** manuell aus.

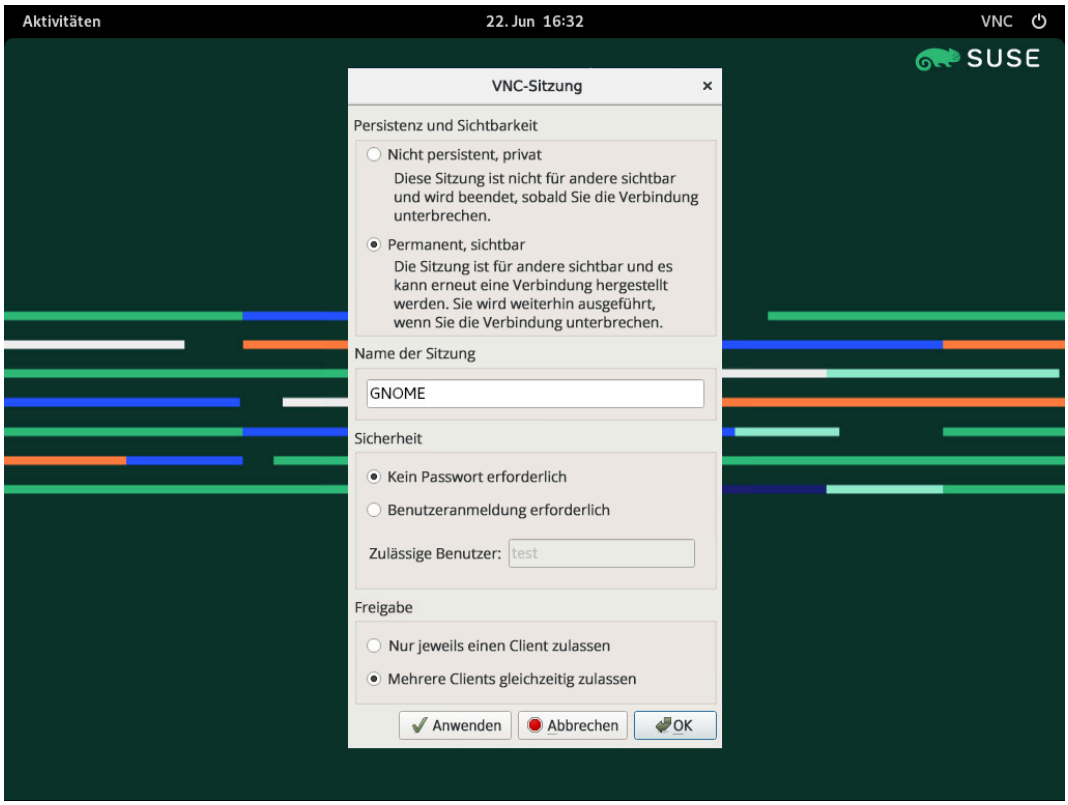


ABBILDUNG 14.8: VNC-SITZUNGSEINSTELLUNGEN

Verschiedene Einstellungen beeinflussen das Verhalten der VNC-Sitzung:

Nicht persistent, privat

Dies entspricht einer einmaligen Sitzung. Diese ist für andere nicht sichtbar und wird beendet, sobald Sie die Verbindung zur Sitzung trennen. Weitere Informationen finden Sie in *Abschnitt 14.3, „Konfigurieren von einmaligen Sitzungen am VNC-Server“*.

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. Die gültigen Benutzernamen werden im Textfeld *Zulässige Benutzer* angezeigt.

Nur jeweils einen Client zulassen

Mehrere Benutzer können nicht gleichzeitig der permanenten Sitzung beitreten.

Mehrere Clients gleichzeitig zulassen

Mehrere Benutzer können gleichzeitig der permanenten Sitzung beitreten. Nützlich für Remote-Präsentationen oder Schulungssitzungen.

Bestätigen Sie Ihre Auswahl mit *OK*.

14.4.1.2 Beitreten zu permanenten VNC-Sitzungen

Sobald Sie eine permanente VPC-Sitzung gemäß *Abschnitt 14.4.1.1, „Konfigurieren von permanenten VNC-Sitzungen“* eingerichtet haben, können Sie dieser Sitzung über den VNC-Viewer beitreten. Nachdem der VNC-Client eine Verbindung zum Server aufgebaut hat, werden Sie gefragt, ob Sie eine neue Sitzung erstellen oder der bestehenden Sitzung beitreten möchten:

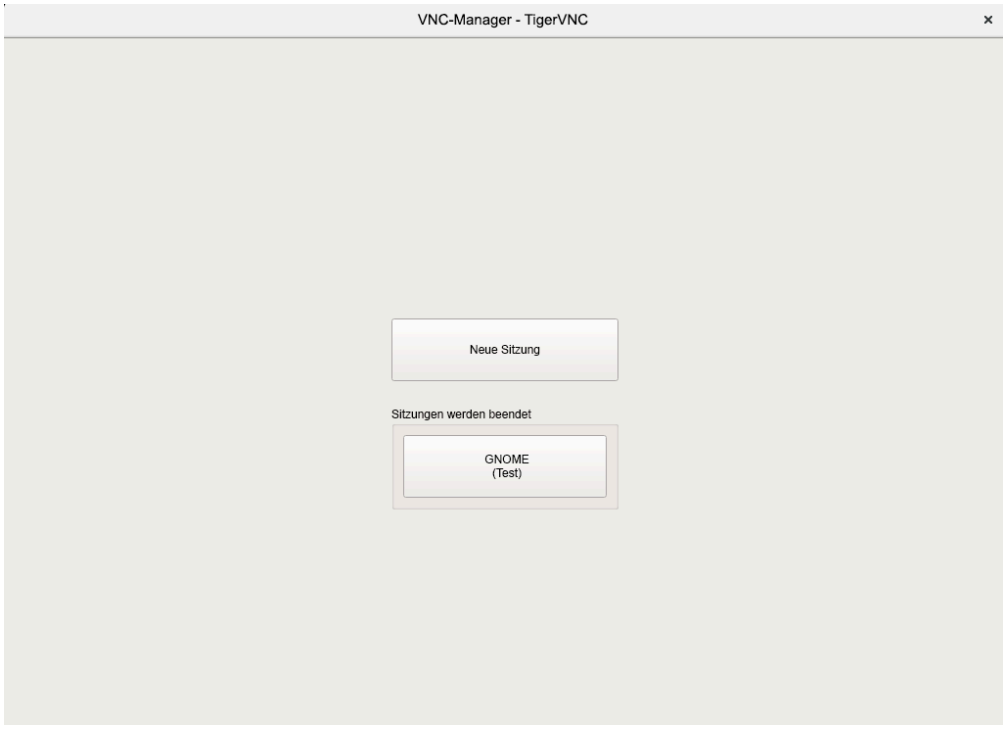


ABBILDUNG 14.9: BEITRETEN ZU EINER PERMANENTEN VNC-SITZUNG

Wenn Sie auf den Namen der bestehenden Sitzung klicken, werden Sie ggf. aufgefordert, Ihren Berechtigungsnachweis anzugeben, abhängig von den Einstellungen für die dauerhafte Sitzung.

14.5 Konfigurieren der Verschlüsselung am VNC-Server

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 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 geän-

dert 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

Bestimmte VNC-Clients weigern sich, eine sichere Verbindung über das standardmäßige selbstsignierte Zertifikat herzustellen. Beispielsweise überprüft der Vinagre-Client die Zertifizierung anhand des globalen GnuTLS-Vertrauensspeichers und es tritt ein Fehler auf, wenn das Zertifikat selbstsigniert ist. Verwenden Sie in einem solchen Fall entweder eine andere Verschlüsselungsmethode als `x509` oder generieren Sie ein ordnungsgemäß signiertes Zertifikat für den VNC-Server und importieren Sie es in den Systemvertrauensspeicher des Clients.

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 `Connection not encrypted!` an).

14.6 Kompatibilität mit Wayland

Die Funktion der entfernten Verwaltung (VNC) basiert auf X11 und kann zu einem leeren Bildschirm führen, wenn Wayland aktiviert ist. Der Display-Manager muss so konfiguriert werden, dass er X11 anstelle von Wayland verwendet. Für `gdm` bearbeiten Sie `/etc/gdm/custom.conf`.

Fügen Sie der Konfigurationsdatei im Abschnitt `[daemon]` den Eintrag `WaylandEnable=false` hinzu. Bei der Anmeldung muss der Benutzer auch eine X11-kompatible Sitzung wählen. Wenn Sie die Wayland-Option für GNOME entfernen möchten, können Sie das Paket `gnome-session-wayland` entfernen und sperren.

15 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.

15.1 Konzeptübersicht

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.

15.2 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*.

15.3 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:

```
> 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/` einzufügen. Wenn Sie den Schrägstrich nicht einfügen, wird die Datei `backup.tar.xz` in `/var/backup` (also in eine Datei) kopiert und *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:

```
> rsync -avz tux /var/backup/
```

Die Kopie befindet sich im absoluten Pfad `/var/backup/tux/`.

15.4 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):

```
> rsync -avz file.tar.xz  tux@192.168.1.1:
```

Alternativ sind auch die folgenden Befehle möglich und äquivalent:

```
> rsync -avz file.tar.xz 192.168.1.1:~
> 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 remote in das Verzeichnis `/var/backup/` auf dem Host `192.168.1.1` kopiert:

```
> 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`.

15.5 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`-Host mit einem *backup*-Ziel. In diesem Ziel können Sie Ihre Sicherungskopien speichern. So erstellen Sie einen Rsync-Server:

VORGEHEN 15.1: 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:

   ```
   # mkdir /var/backup
   ```

2. Legen Sie das Eigentum fest. In diesem Fall ist der Benutzer `tux` in der Gruppe `users` der Eigentümer des Verzeichnisses:

   ```
   # chown tux.users /var/backup
   ```

3. Konfigurieren Sie den rsyncd-Daemon.
   Die Konfigurationsdatei wird in eine Hauptdatei und bestimmte „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 ein Verzeichnis `/etc/rsyncd.d/`:

      ```
      # 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:

```
# chmod 0600 /etc/rsyncd.secrets
```

4. Starten und aktivieren Sie den rsyncd-Daemon:

```
# systemctl enable rsyncd
# systemctl start rsyncd
```

5. Testen Sie den Zugriff auf den Rsync-Server:

```
> 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. Dies ist nützlich, um Ihre Übertragungen zu debuggen.

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.

15.6 Weitere Informationen

Csync

Bidirektionales Dateisynchronisierungswerkzeug, siehe https://csync.org/.

RSnapshot

Erstellt inkrementelle Sicherungen, siehe https://rsnapshot.org.

Unison

Bidirektionales Dateisynchronisierungswerkzeug – ähnlich wie CSync, jedoch mit grafischer Benutzeroberfläche, siehe https://github.com/bcpierce00/unison.

Rear

Disaster Recovery-Framework, siehe *Administration Guide* im Kapitel zur SUSE Linux Enterprise-Hochverfügbarkeit *Disaster Recovery with Rear (Relax-and-Recover)* (https://documentation.suse.com/sle-ha/15/html/SLE-HA-all/cha-ha-rear.html).

II Booten eines Linux-Systems

16 Einführung in den Bootvorgang 238

17 UEFI (Unified Extensible Firmware Interface) 248

18 Der Bootloader GRUB 2 258

19 Der Daemon `systemd` 280

16 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 vom Bootloader GRUB 2 gestartet. Anschließend wird der Bootvorgang 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.

16.1 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 Dateisystemtreiber eingehängt werden muss. SUSE Linux Enterprise Desktop verwendet ausschließlich ein `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`.

16.2 Der Linux-Bootvorgang

Der Linux-Bootvorgang besteht aus mehreren Phasen, von denen jede einer anderen Komponente entspricht:

1. *Abschnitt 16.2.1, „Initialisierungs- und Bootloader-Phase“*
2. *Abschnitt 16.2.2, „Die Kernel-Phase“*
3. *Abschnitt 16.2.3, „Die Phase init auf initramfs“*
4. *Abschnitt 16.2.4, „Die systemd-Phase“*

16.2.1 Initialisierungs- und Bootloader-Phase

Während der Initialisierungsphase wird die Computerhardware eingerichtet und die Geräte werden vorbereitet. Dieser Prozess unterscheidet sich je nach Hardware-Architektur.

SUSE Linux Enterprise Desktop 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 18, Der Bootloader GRUB 2*.

16.2.1.1 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 kann eine FAT-formatierte Systempartition von Festplatten mit GPT-Partitionstabelle 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 ruft das Boot-Image vom Boot-Server ab und startet das System unabhängig von lokalen Festplatten.

16.2.1.2 Initialisierungs- und Bootloader-Phase auf IBM Z

Bei IBM Z muss der Boot-Vorgang durch einen Bootloader namens **`zipl`** (ursprüngliches z-Programmladen) initialisiert werden. Obwohl **`zipl`** das Lesen mehrerer Dateisysteme unterstützt, unterstützt es nicht das SLE-Standarddateisystem (Btrfs) oder das Booten aus Snapshots. SUSE Linux Enterprise Desktop nutzt somit einen zweistufigen Boot-Vorgang, der gewährleistet, dass Btrfs zum Boot-Zeitpunkt vollständig unterstützt wird:

1. **`zipl`** bootet aus der Partition `/boot/zipl`, die mit dem Dateisystem Ext2, Ext3, Ext4 oder XFS formatiert werden kann. 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 `init-grub` 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. Er liest seine Konfiguration aus `/boot/grub2/grub.cfg` und lädt den eigentlichen Kernel und das initramfs aus `/boot`. Der neue Kernel wird nun über Kexec geladen.

16.2.2 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.

16.2.2.1 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, sodass 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`.

16.2.2.1.1 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 spezielle Situationen, in denen Sie `initramfs` manuell neu generieren müssen:

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.

Öffnen oder erstellen Sie die Datei `/etc/dracut.conf.d/10-`*`DRIVER`*`.conf` und fügen Sie folgende Zeile hinzu (beachten Sie das vorangestellte Leerzeichen):

```
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 16.1, „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.

Erstellen Sie dazu die entsprechenden Einträge in `/etc/fstab` und hängen Sie die neuen Einträge (z. B. mit **`mount -a`** und/oder **`swapon -a`**) ein.

Fahren Sie mit *Prozedur 16.1, „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 16.1, „Generieren eines initramfs“*.

Fahren Sie mit *Prozedur 16.1, „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 16.1, „Generieren eines initramfs“* beschrieben vorgehen.

Hinzufügen oder entfernen von Swap-Geräten, Neuerstellen des Swap-Bereichs

Wann immer Sie ein Swap-Gerät hinzufügen oder entfernen oder einen Swap-Bereich mit einer anderen UUID neu erstellen, aktualisieren Sie das initramfs wie in *Prozedur 16.1, „Generieren eines initramfs“* beschrieben. Möglicherweise müssen Sie auch die `GRUB_CMDLINE_*`-Variablen aktualisieren, die die Option `resume=` in `/etc/default/grub` enthalten, und dann `/boot/grub2/grub.cfg` wie in *Abschnitt 18.2.1, „Die Datei `/boot/grub2/grub.cfg`“* beschrieben neu generieren.

VORGEHEN 16.1: GENERIEREN EINES INITRAMFS

Wichtig

Alle Befehle des folgenden Verfahrens müssen als `root`-Benutzer ausgeführt werden.

1. Geben Sie Ihr `/boot`-Verzeichnis ein:

```
# cd /boot
```

2. Erzeugen Sie eine neue `initramfs`-Datei mit **`dracut`** und ersetzen Sie dabei *`MY_INITRAMFS`* durch einen Dateinamen Ihrer Wahl:

```
# dracut MY_INITRAMFS
```

   Führen Sie alternativ **`dracut -f`** *`FILENAME`* aus und ersetzen Sie damit eine vorhandene init-Datei.

3. (Überspringen Sie diesen Schritt, wenn Sie im vorangegangenen Schritt **`dracut -f`** ausgeführt haben.) Erstellen Sie einen symbolischen Link von der `initramfs`-Datei, die Sie im vorangegangenen Schritt erstellt haben, zu `initrd`:

```
#  ln -sf MY_INITRAMFS initrd
```

4. Unter der Architektur IBM z müssen Sie zudem **`grub2-install`** ausführen.

16.2.3 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 16.1, „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 `udev`.

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

Abhängig von den geladenen Modulen generiert der Kernel Geräteereignisse. `udev` verarbeitet diese Ereignisse und generiert die erforderlichen speziellen Blockdateien auf einem RAM-Dateisystem in `/dev`. Ohne diese speziellen Dateien wäre ein Zugriff auf das Dateisystem und andere Geräte nicht möglich.

Verwalten von RAID- und LVM-Setups

Wenn Ihr System so konfiguriert ist, dass das root-Dateisystem sich unter RAID oder LVM befindet, richtet `init` 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 Desktop unterstützt das Booten von einem sekundären iSCSI-Ziel, wenn das primäre Ziel nicht verfügbar ist.

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.

16.2.3.1 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. Das Installationssystem startet auch `systemd` aus `initramfs` nicht – 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 16.2.2.1, „Die `initramfs`-Datei“* erwähnt, beginnt der Boot-Vorgang mit einem Mindestsatz an Treibern, die für die meisten Hardware-Konfigurationen verwendet werden können. Bei Rechnern mit AArch64, POWER und AMD64/Intel 64 löst **`linuxrc`** zunächst eine Hardware-Abfrage aus, durch die die Treiber ermittelt werden, die sich für Ihre Hardware-Konfiguration eignen. Unter IBM Z muss beispielsweise über linuxrc oder parmfile eine Liste der Treiber und deren 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 19.6.4, „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.

16.2.4 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 der System- und Servicemanager von Linux. 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. Ausführliche Informationen finden Sie in *Kapitel 19, Der Daemon* `systemd`.

17 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 in https://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 Desktop implementiert sind.

17.1 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 Desktop-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 „vertrauenswürdigen“ Schlüssel signiert ist – sei es ein OS-Bootloader, ein Treiber im Flash-Speicher einer bestimmten 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.

17.1.1 Implementierung in SUSE Linux Enterprise Desktop

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.

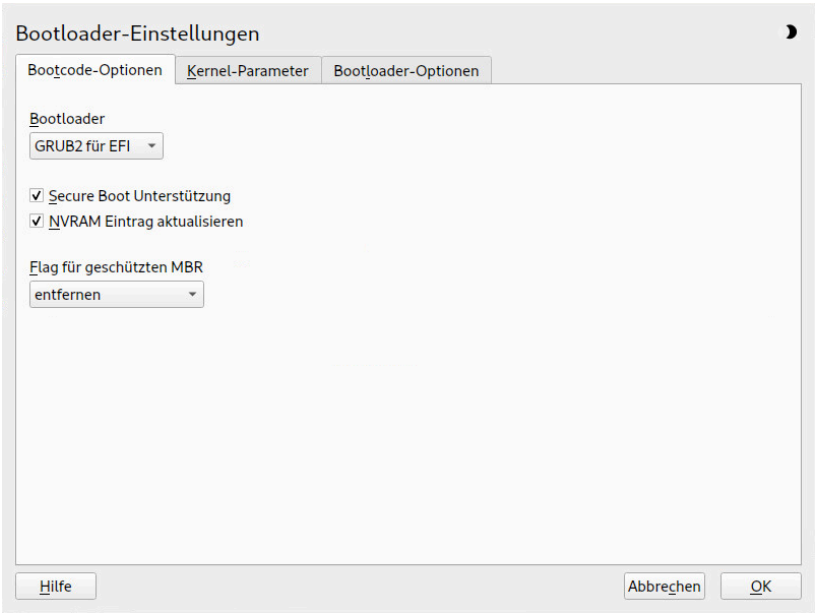


ABBILDUNG 17.1: SECURE BOOT-UNTERSTÜTZUNG

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 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.

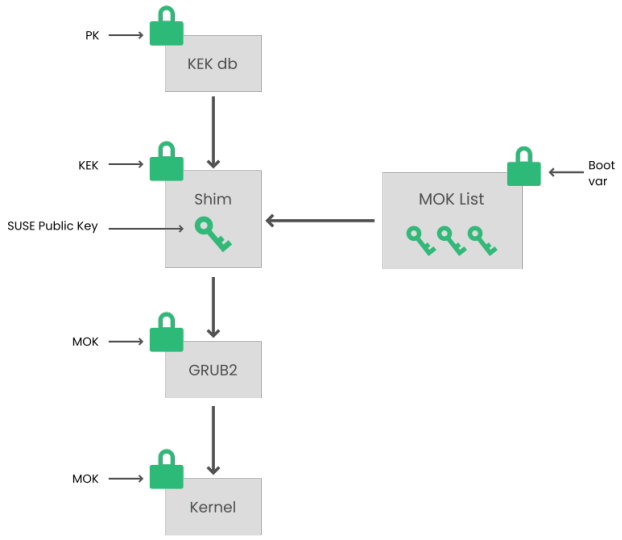


ABBILDUNG 17.2: UEFI: SECURE BOOT-VORGANG

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.

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) als auch aus 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.

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 Vorrang 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.

17.1.2 MOK (Machine Owner Key)

Wenn bestimmte Kernels, Treiber oder andere Komponenten im Startprozess ersetzt werden sollen, müssen Sie Machine Owner Keys (MOKs) verwenden. Das Werkzeug `mokutil` unterstützt Sie bei der Verwaltung der MOKs.

Sie können mit `mokutil` eine MOK-Registrierungsanforderung erstellen. Die Anforderung wird in der UEFI-Laufzeit(RT)-Variablen `MokNew` gespeichert. Beim nächsten Booten erkennt der `shim`-Bootloader `MokNew` und lädt `MokManager`, was Ihnen mehrere Optionen bietet. Sie können die

Optionen *Enroll key from disk* (Schlüssel vom Datenträger registrieren) und *Enroll hash from disk* (Hash vom Datenträger registrieren) verwenden, um MokList den Schlüssel hinzuzufügen. Mit der Option *MOK registrieren* kopieren Sie einen Schlüssel aus der `MokNew`-Variablen.

Das Registrieren eines Schlüssels vom Datenträger erfolgt normalerweise, wenn der Shim `grub2` nicht laden kann und ein Fallback auf das Laden von MokManager erfolgt. Da `MokNew` noch nicht vorhanden ist, haben Sie die Möglichkeit, den Schlüssel in der UEFI-Partition zu suchen.

17.1.3 Booten eines benutzerdefinierten Kernels

Die folgenden Ausführungen beruhen auf https://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 https://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.

17.1.4 Verwenden von Nicht-Inbox-Treibern

Das Hinzufügen von Nicht-Inbox-Treibern (also Treibern, die nicht in SUSE Linux Enterprise Desktop 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=` 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 in https://drivers.suse.com/doc/Usage/Secure_Boot_Certificate.html.

17.1.5 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.
- Seit SUSE Linux Enterprise Server 15 SP3 werden Kexec und Kdump im Secure Boot-Modus unterstützt.

Beim Booten im Secure Boot-Modus gelten die folgenden Einschränkungen:

- Um zu gewährleisten, dass Secure Boot nicht einfach umgangen werden kann, sind bestimmte Kernelfunktionen beim Ausführen unter Secure Boot deaktiviert.
- Der Bootloader, der Kernel und die Kernelmodule müssen signiert sein.
- 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.

17.2 Weitere Informationen

- https://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):
  - https://www.suse.com/c/uefi-secure-boot-plan/
  - https://www.suse.com/c/uefi-secure-boot-overview/
  - https://www.suse.com/c/uefi-secure-boot-details/
- https://en.opensuse.org/openSUSE:UEFI – UEFI mit openSUSE.

18 Der Bootloader GRUB 2

In diesem Kapitel wird die Konfiguration von GRUB 2, dem unter SUSE Linux Enterprise Desktop 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 Desktop eingebunden. Für die Konfiguration der wichtigsten Einstellungen steht ein YaST-Modul bereit. Eine Übersicht über den Bootvorgang finden Sie in *Kapitel 16, Einführung in den Bootvorgang*. Weitere Informationen zur Unterstützung von Secure Boot finden Sie in *Kapitel 17, UEFI (Unified Extensible Firmware Interface)*.

18.1 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.

18.2 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` sollte nicht bearbeitet werden. Die Datei wird automatisch durch den Befehl **`grub2-mkconfig -o /boot/grub2/grub.cfg`** generiert.

`/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 Desktop 12 SP2 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 gelesen **`grub2-mkconfig -o /boot/grub2/grub.cfg`**. Die zugehörigen Anweisungen werden in die Hauptkonfigurationsdatei `/boot/grub/grub.cfg` integriert.

`/etc/sysconfig/bootloader`
: Diese Konfigurationsdatei enthält bestimmte Grundeinstellungen wie den Bootloader-Typ und ob die UEFI Secure Boot-Unterstützung aktiviert werden soll.

`/boot/grub2/x86_64-efi`, `/boot/grub2/power-ieee1275`
: 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 -o /boot/grub2/grub.cfg`** ausführen, damit die Änderungen in Kraft treten. Sollten Sie die Konfiguration jedoch mit YaST geändert haben, ist dies nicht nötig, da YaST diesen Befehl automatisch ausführt.

18.2.1 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 aus der Datei `/etc/default/grub` und den Skripten kompiliert, die sich beim Ausführen des Befehls **`grub2-mkconfig -o /boot/grub2/grub.cfg`** im Verzeichnis `/etc/grub.d/` befinden. 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 18.3, „Konfigurieren des Bootloaders mit YaST“*).

18.2.2 Die Datei `/etc/default/grub`

In dieser Datei 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 Befehl erhalten Sie eine Liste aller verfügbaren Optionen:

```
> grep "export GRUB_DEFAULT" -A50 /usr/sbin/grub2-mkconfig | grep GRUB_
```

Sie können benutzerdefinierte Variablen einführen und sie später in den Skripten im Verzeichnis `/etc/grub.d` verwenden.

Aktualisieren Sie nach der Bearbeitung von `/etc/default/grub` die Hauptkonfigurationsdatei mit **`grub2-mkconfig -o /boot/grub2/grub.cfg`**.

Anmerkung: Bereich

Alle in dieser Datei angegebenen Optionen sind allgemeine Optionen, die für alle Booteinträge gelten. Zu den für einen Xen-Hypervisor spezifischen Optionen gehört die Teilzeichenfolge `_XEN_`.

Wichtig: Versehen von inneren Anführungszeichen mit Escape-Zeichen

Komplexere Optionen mit Leerzeichen erfordern Anführungszeichen, damit sie als eine Option verarbeitet werden. Solche inneren Anführungszeichen müssen korrekt mit Escape-Zeichen versehen werden, zum Beispiel:

```
GRUB_CMDLINE_LINUX_XEN="debug loglevel=9 log_buf_len=5M \"ddebug_query=file
 drivers/xen/xen-acpi-processor.c +p\""
```

`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="Example boot menu entry"` wird der Menüeintrag mit dem Titel „Example boot menu entry“ gebootet.

Mit `GRUB_DEFAULT=saved` wird der Eintrag gebootet, der mit dem Befehl **`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, 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 die `GRUB_CMDLINE_LINUX`-Parameter für alle Xen-Boot-Einträge.

`GRUB_CMDLINE_LINUX_XEN_REPLACE_DEFAULT`

Dieser Eintrag entspricht `GRUB_CMDLINE_LINUX_XEN_REPLACE`, jedoch mit dem Unterschied, dass nur Parameter von `GRUB_CMDLINE_LINUX_DEFAULT` ersetzt werden.

`GRUB_CMDLINE_XEN`

Diese Einträge werden an die Xen-Menüeinträge des Xen-Hypervisors für den normalen Modus und den Wiederherstellungsmodus übergeben. Beispiel:

```
GRUB_CMDLINE_XEN="loglvl=all guest_loglvl=all"
```

Tipp: Xen-Hypervisor-Optionen

Eine vollständige Liste der Xen-Hypervisor-Optionen finden Sie unter https://xen-bits.xen.org/docs/unstable/misc/xen-command-line.html.

`GRUB_CMDLINE_XEN_DEFAULT`

Dieser Eintrag entspricht `GRUB_CMDLINE_XEN`, jedoch mit dem Unterschied, dass die Einträge nur im normalen Modus angehängt werden.

`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`. Sie können nur Modi verwenden, die von Ihrer Grafikkarte (VBE) unterstützt werden. Die Standardeinstellung lautet „auto“; hiermit wird nach Möglichkeit eine bevorzugte Auflösung ausgewählt. Mit dem Befehl **`videoinfo`** in der GRUB 2-Befehlszeile werden die verfügbaren Bildschirmauflösungen für GRUB 2 angezeigt. Zum Öffnen der Befehlszeile 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 in *Abschnitt 10.3, „System-Rollback durch Booten aus Snapshots“*.

Eine vollständige Liste der Optionen finden Sie im Handbuch zu GNU GRUB (https://www.gnu.org/software/grub/manual/grub/grub.html#Simple-configuration).

18.2.3 Skripte in `/etc/grub.d`

Die Skripte in diesem Verzeichnis werden beim Ausführen des Befehls **`grub2-mkconfig -o /boot/grub2/grub.cfg`** gelesen. Ihre Anweisungen sind in `/boot/grub2/grub.cfg` integriert. 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 `grub.cfg` eine Ausgabe in **`grub2-mkconfig`**. Standardmäßig sind alle Dateien im Verzeichnis `/etc/grub.d` ausführbar.

Tipp: Permanenter benutzerdefinierter Inhalt in `grub.cfg`

`/boot/grub2/grub.cfg` wird bei jedem Ausführen von **`grub2-mkconfig`** neu kompiliert, sodass benutzerdefinierte Inhalte verloren gehen. Um Ihre Zeilen direkt in `/boot/grub2/grub.cfg` einzufügen, ohne dass sie nach der Ausführung von **`grub2-mkconfig`** verloren gehen, fügen Sie sie zwischen 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 die Datei `/boot/grub2/custom.cfg` erstellen und mit Inhalt füllen, wird sie automatisch beim Booten direkt hinter `40_custom` in `/boot/grub2/grub.cfg` eingefügt.

18.2.4 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. Die GRUB 2-Partitionsnummern beginnen mit `1`, nicht mit `0` wie in GRUB 2 Legacy.

```
(hd1)  /dev/disk-by-id/DISK3 ID
(hd2)  /dev/disk-by-id/DISK1 ID
(hd3)  /dev/disk-by-id/DISK2 ID
```

18.2.5 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.

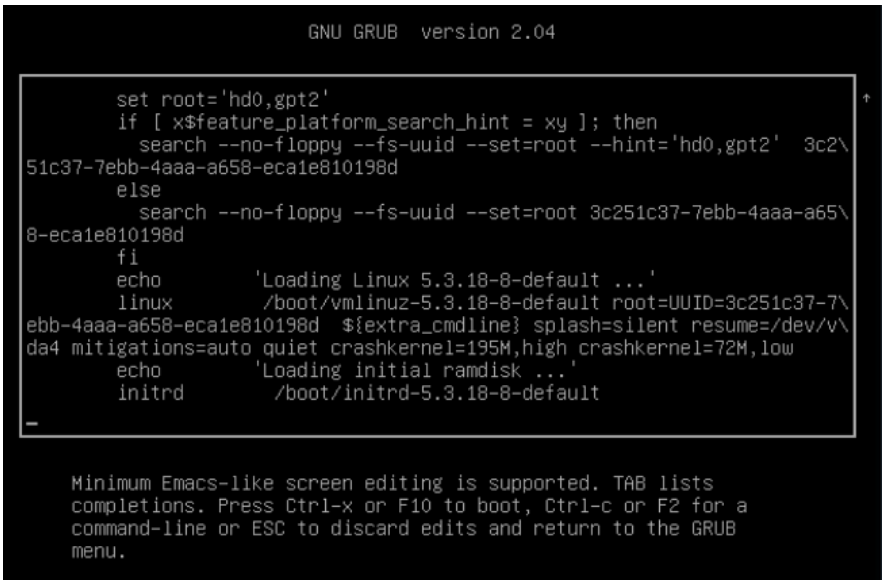


ABBILDUNG 18.1: BOOTEDITOR IN GRUB 2

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 https://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 im *Buch „Installationshandbuch“, Kapitel 9 „Fehlersuche“, Abschnitt 9.3 „Vom Installationsmedium kann nicht gebootet werden“, 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 Bootparametern wählen Sie einen Eintrag aus und beginnen Sie mit der Eingabe. Die Ergänzungen des Installations-Booteintrags werden dauerhaft im installierten System gespeichert.

18.2.6 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:`**:

```
> 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 Befehl **`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 zum Importieren der Änderungen in der Hauptkonfigurationsdatei Folgendes aus:

```
> sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Nach dem Neubooten werden Sie von GRUB 2 aufgefordert, einen Benutzernamen und ein Passwort einzugeben, sobald Sie versuchen, einen Menüeintrag zu booten. Geben Sie `root` und das Passwort ein, das Sie während des Befehls **`grub2-mkpasswd-pbkdf2`** eingegeben haben. Wenn der Berechtigungsnachweis fehlerfrei ist, bootet das System den angegebenen Booteintrag.

Weitere Informationen finden Sie in https://www.gnu.org/software/grub/manual/grub/grub.html#Security↗.

18.2.7 Autorisierter Zugriff auf Bootmenüeinträge

Sie können GRUB 2 so konfigurieren, dass der Zugriff auf die Bootmenüeinträge abhängig von der Autorisierungsstufe gewährt wird. Sie können mehrere mit Passwörtern geschützte Benutzerkonten konfigurieren und ihnen Zugriff auf verschiedene Menüeinträge zuweisen. So konfigurieren Sie die Autorisierung in GRUB 2:

1. Erstellen und verschlüsseln Sie ein Passwort für jedes Benutzerkonto, das Sie in GRUB 2 verwenden möchten. Führen Sie den Befehl **`grub2-mkpasswd-pbkdf2`** aus (siehe *Abschnitt 18.2.6, „Festlegen eines Bootpassworts“*).

2. Löschen Sie die Datei `/etc/grub.d/10_linux`. Damit wird die Ausgabe der standardmäßigen GRUB 2-Menüeinträge verhindert.

3. Bearbeiten Sie die Datei `/boot/grub2/custom.cfg` und fügen Sie manuell benutzerdefinierte Menüeinträge hinzu. Die folgende Schablone ist ein Beispiel, das Sie je nach Anwendungsfall individuell anpassen können:

```
set superusers=admin
password admin ADMIN_PASSWORD
password maintainer MAINTAINER_PASSWORD

menuentry 'Operational mode' {
  insmod ext2
  set root=hd0,1
  echo 'Loading Linux ...'
  linux /boot/vmlinuz root=/dev/vda1 $GRUB_CMDLINE_LINUX_DEFAULT $GRUB_CMDLINE_LINUX
 mode=operation
  echo 'Loading Initrd ...'
  initrd /boot/initrd
}

menuentry 'Maintenance mode' --users maintainer {
  insmod ext2
```

```
  set root=hd0,1
  echo 'Loading Linux ...'
  linux /boot/vmlinuz root=/dev/vda1 $GRUB_CMDLINE_LINUX_DEFAULT $GRUB_CMDLINE_LINUX
 mode=maintenance
  echo 'Loading Initrd ...'
  initrd /boot/initrd
}
```

4. Importieren Sie die Änderungen in der Hauptkonfigurationsdatei:

```
> sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Im obigen Beispiel:

- Das GRUB 2-Menü hat zwei Einträge – *Operational mode* (Betriebsmodus) und *Maintenance mode* (Wartungsmodus).
- Wenn kein Benutzer angegeben ist, ist der Zugriff auf beide Bootmenüeinträge möglich, doch niemand kann auf die GRUB 2-Befehlszeile zugreifen oder vorhandene Menüeinträge bearbeiten.
- Der `admin`-Benutzer kann auf die GRUB 2-Befehlszeile zugreifen und vorhandene Menüeinträge bearbeiten.
- Der `maintenance`-Benutzer kann den Menüeintrag für die Wiederherstellung auswählen.

18.3 Konfigurieren des Bootloaders mit YaST

Mit dem YaST-Modul ist die Konfiguration des Bootloaders auf Ihrem SUSE Linux Enterprise Desktop 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.

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.

18.3.1 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:

VORGEHEN 18.1: 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 root-Partition

   Mit dieser Option können Sie den Speicherort des Bootloaders manuell angeben.

2. Klicken Sie auf *OK*, um die Änderungen zu übernehmen.

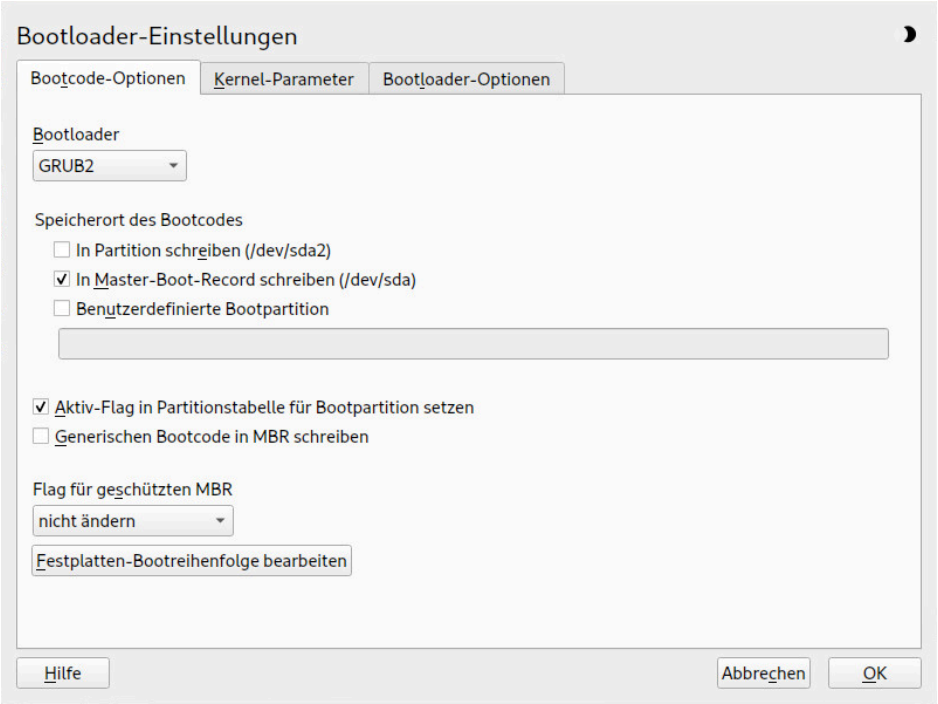


ABBILDUNG 18.2: BOOT-CODE-OPTIONEN

Die Registerkarte *Boot-Code-Optionen* enthält die folgenden zusätzlichen Optionen:

Aktives Flag in Partitionstabelle für Bootpartition festlegen

Aktiviert die Partition, die das Verzeichnis `/boot` enthält. Bei POWER-Systemen wird die PReP-Partition aktiviert. 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 hierzu finden Sie in https://github.com/Sirrix-AG/TrustedGRUB2.

Der Abschnitt *Flag für geschützten MBR* enthält folgende Optionen:

set

Diese Option eignet sich für das herkömmliche Booten mit Legacy-BIOS.

Entfernen

Diese Option eignet sich für das UEFI-Booten.

nicht ändern

Dies ist in der Regel die beste Option, wenn bereits ein funktionsfähiges System vorliegt.

In den meisten Fällen verwendet YaST standardmäßig die jeweils richtige Option.

18.3.2 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 Desktop standardmäßig installiert. Die restlichen Einträge in der Liste bilden Hinweise für den Geräte-Mapper von GRUB 2 (siehe *Abschnitt 18.2.4, „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 Festplatten in der Liste leer ist.

VORGEHEN 18.2: FESTLEGEN DER FESTPLATTENREIHENFOLGE

1. Öffnen Sie die Registerkarte *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.

18.3.3 Konfigurieren der erweiterten Optionen

Erweiterte Bootparameter lassen sich über die Registerkarte *Bootloader-Optionen* konfigurieren.

18.3.3.1 Registerkarte *Bootloader-Optionen*

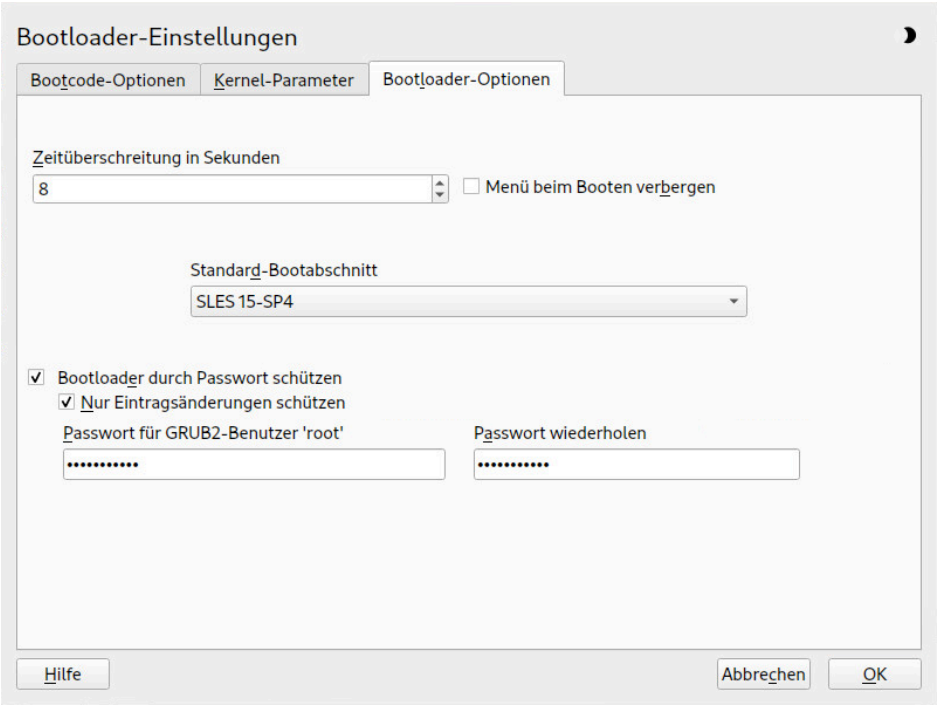


ABBILDUNG 18.3: BOOTLOADER-OPTIONEN

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 entsprechende 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. Details zur manuellen Konfiguration finden Sie in *Abschnitt 18.2.6, „Festlegen eines Bootpassworts“*. Das Bootpasswort muss bei jedem Booten eingegeben werden, wenn diese Option aktiviert ist. Das

System wird also nicht automatisch gebootet. Wenn Sie jedoch das Verhalten von GRUB 1 bevorzugen, aktivieren Sie zusätzlich *Nur Eintragsänderungen schützen*. Bei dieser Einstellung darf jeder eine Boot-Eingabe auswählen und das System booten. Das Passwort für den GRUB 2 `root`-Benutzer ist jedoch nur zum Ändern der Boot-Einträge erforderlich.

18.3.3.2 Registerkarte *Kernel-Parameter*

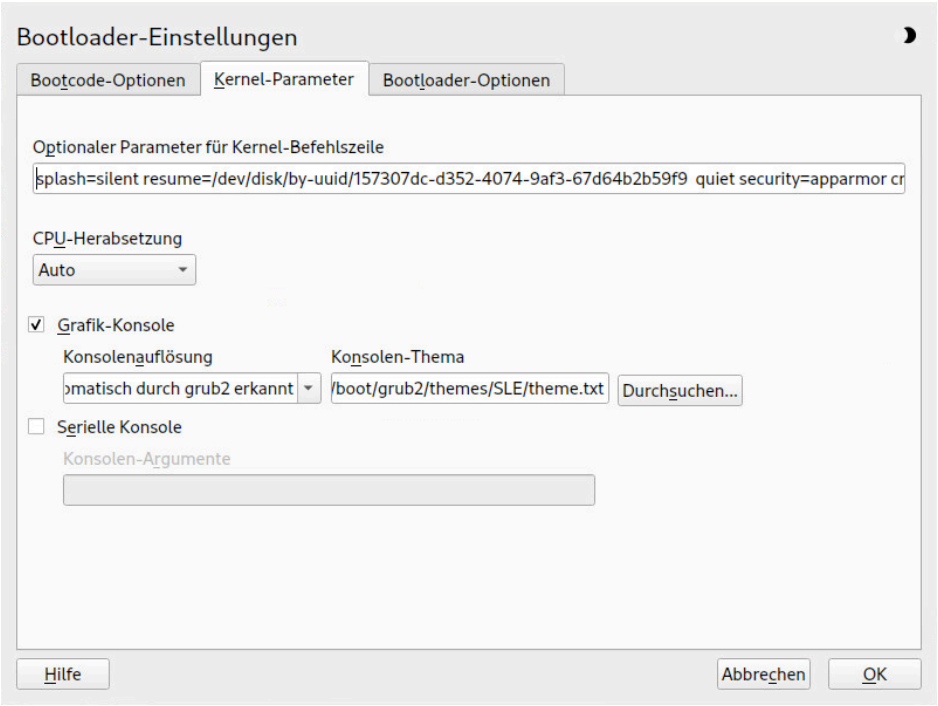


ABBILDUNG 18.4: KERNEL-PARAMETER

Optionaler Kernel-Befehlszeilenparameter

Geben Sie hier optionale Kernel-Parameter an, um Systemfunktionen zu aktivieren/deaktivieren, Treiber hinzuzufügen usw.

CPU-Mitigationen

SUSE hat mindestens einen Kernel-Boot-Befehlszeilenparameter für alle Software-Mitigationen veröffentlicht, die zur Vorbeugung von CPU-Seitenkanalangriffen bereitgestellt wurden. Einige Parameter führen unter Umständen zu Leistungseinbußen. Bringen Sie die Sicherheit und Leistung je nach Ihrer Situation mit einer der folgenden Optionen ins Gleichgewicht:

Automatisch. Aktiviert alle erforderlichen Mitigationen für Ihr CPU-Modell, schützt jedoch nicht vor CPU-übergreifenden Thread-Angriffen. Diese Einstellung kann die Leistung in gewissem Maße einschränken, je nach Auslastung.

Auto + kein SMT. Aktiviert alle verfügbaren Sicherheitsmitigationen. Aktiviert alle erforderlichen Mitigationen für Ihr CPU-Modell. Darüber hinaus wird Simultaneous Multithreading (SMT) deaktiviert, sodass Seitenkanalangriffe über mehrere CPU-Threads unterbunden werden. Diese Einstellung kann die Leistung weiter einschränken, je nach Auslastung.

Aus. Deaktiviert alle Mitigationen. Es sind Seitenkanalangriffe gegen die CPU möglich, je nach CPU-Modell. Diese Einstellung wirkt sich nicht auf die Leistung aus.

Manuell. Gibt keine Mitigationsstufe vor. Legen Sie die CPU-Mitigationen manuell über die Kernel-Befehlszeilenoptionen fest.

Grafik-Konsole benutzen

Wenn diese Option aktiviert ist, wird das Bootmenü nicht im Textmodus dargestellt, sondern in einem grafischen Begrüßungsbildschirm. Die Auflösung des Bootbildschirms wird standardmäßig automatisch festgelegt, doch Sie können diese manuell über *Konsolenauflösung* festlegen. Die Datei mit der Definition des Grafikthemas wird mit der *Konsolenthema*-Dateiauswahl angegeben. Ändern Sie diese Einstellung nur, wenn Sie ein eigenes benutzerdefiniertes Thema anwenden möchten.

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. Informationen finden Sie unter `info grub` oder https://www.gnu.org/software/grub/manual/grub.html#Serial-terminal

18.4 Nützliche Befehle in GRUB 2

`grub2-mkconfig`

Generiert eine neue Datei `/boot/grub2/grub.cfg` basierend auf `/etc/default/grub` und den Skripten von `/etc/grub.d/`.

BEISPIEL 18.1: 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 den folgenden Befehl:

```
# shim-install --config-file=/boot/grub2/grub.cfg
```

`grub2-mkrescue`

Hiermit wird ein bootfähiges Rettungs-Image der installierten GRUB 2-Konfiguration erstellt.

BEISPIEL 18.2: VERWENDUNG VON GRUB2-MKRESCUE

```
grub2-mkrescue -o save_path/name.iso iso
```

`grub2-script-check`

Hiermit prüfen Sie die angegebene Datei auf Syntaxfehler.

BEISPIEL 18.3: 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 18.4: VERWENDUNG VON GRUB2-ONCE

```
grub2-once number_of_the_boot_entry
```

Tipp: **`grub2-once`** help

Wenn Sie das Programm ohne Angabe von Optionen aufrufen, erhalten Sie eine vollständige Liste der zulässigen Optionen.

18.5 Rescue-Modus

Der *Rescue-Modus* ist eine spezielle `root`-Benutzersitzung zur Fehlerbehebung und Reparatur von Systemen, bei denen beim Booten ein Fehler auftritt. Er bietet eine Einzelbenutzerumgebung mit lokalen Dateisystemen und aktiven Kernsystemdiensten. Es sind keine Netzwerkschnittstellen aktiviert. Gehen Sie folgendermaßen vor, um in den Rescue-Modus zu gelangen.

VORGEHEN 18.3: AUFRUFEN DES RESCUE-MODUS

1. Booten Sie das System neu. Der Bootbildschirm wird mit dem GRUB 2-Startmenü angezeigt.
2. Wählen Sie den Menüeintrag zum Booten und drücken Sie `e`, um die Bootzeile zu bearbeiten.
3. Fügen Sie den folgenden Parameter an die Zeile mit den Kernel-Parametern an:

   ```
   systemd.unit=rescue.target
   ```

4. Drücken Sie `Strg` + `X`, um mit diesen Einstellungen zu booten.
5. Geben Sie das Passwort für `root` ein.

6. Nehmen Sie alle erforderlichen Änderungen vor.

7. Wechseln Sie wieder zum Ziel im normalen Betrieb, indem Sie an der Befehlszeile **`systemctl isolate multi-user.target`** oder **`systemctl isolate graphical.target`** eingeben.

18.6 Weitere Informationen

Umfassende Informationen zu GRUB 2 finden Sie unter https://www.gnu.org/software/grub/. Ausführliche Informationen finden Sie auch auf der Infoseite für den Befehl **`grub`**. Weitere Informationen zu bestimmten Themen erhalten Sie auch, wenn Sie „GRUB 2“ in der Suchfunktion für technische Informationen unter https://www.suse.com/support als Suchwort eingeben.

19 Der Daemon systemd

systemd initialisiert das System. Er hat die Prozess-ID 1. systemd wird direkt vom Kernel gestartet und widersteht dem Signal 1, das in der Regel Prozesse beendet. Alle anderen Programme werden direkt von systemd oder von einem seiner untergeordneten Prozesse gestartet. systemd ist ein Ersatz für den Daemon „System V-init“ und vollständig mit System V-init kompatibel (durch Unterstützung von init-Skripten).

Der wichtigste Vorteil von systemd ist der erheblich schnellere Systemstart durch die Parallelisierung der Dienststarts. 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 auch Kernel-Steuergruppen (cgroups), das Erstellen von Snapshots und das Wiederherstellen des Systemstatus. Weitere Informationen finden Sie unter https://www.freedesktop.org/wiki/Software/systemd/.

Tipp: systemd innerhalb des WSL

Das Windows-Subsystem für Linux (WSL) ermöglicht die Ausführung von Linux-Anwendungen und -Distributionen unter dem Betriebssystem Microsoft Windows. WSL verwendet seinen init-Prozess anstelle von systemd. Um systemd in SUSE Linux Enterprise Desktop zu aktivieren, das unter WSL ausgeführt wird, installieren Sie das wsl_systemd-Schema, das den Prozess automatisiert:

```
> sudo zypper in -t pattern wsl_systemd
```

Alternativ können Sie /etc/wsl.conf bearbeiten und die folgenden Zeilen manuell hinzufügen:

```
[boot]
systemd=true
```

Beachten Sie, dass die Unterstützung für systemd unter WSL teilweise ist – systemd-Unit-Dateien müssen ein angemessenes Prozessverwaltungsverhalten aufweisen.

19.1 Das Konzept von systemd

Im folgenden Abschnitt wird das Konzept hinter systemd erläutert.

`systemd` ist ein System- und Sitzungsmanager für Linux und mit System V- und LSB-init-Skripts kompatibel. Die wichtigsten Funktionen von `systemd`:

- Parallelisierungsfunktionen
- Starten von Diensten per Socket- und D-Bus-Aktivierung
- Starten der Daemons bei Bedarf
- Verfolgen von Prozessen mithilfe von Linux-cgroups
- Erstellen von Snapshots und Wiederherstellen des Systemstatus
- Einhängepunkte und Automount-Punkte
- Ausgereifte Dienststeuerlogik auf der Basis der Transaktionsabhängigkeiten

19.1.1 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 ein von `systemd` verwendeter generischer Term für Folgendes:

- **Service.** Informationen zu einem Prozess (z. B. Ausführung eines Daemon); Datei endet auf .service
- **Zielgruppen.** 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
- **Path.** Dient als Auslöser von anderen Units (z. B. Ausführen eines Diensts, 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-Dateien finden Sie in https://www.freedesktop.org/software/systemd/man/latest/systemd.unit.html

19.2 Grundlegende Verwendung

Im System V-init-System werden Dienste mit mehreren Befehlen verarbeitet – mit init-Skripten, **`insserv`**, **`telinit`** und anderen. `systemd` erleichtert die Verwaltung von Diensten, da es nur einen Befehl gibt, um die meisten dienstbezogenen Aufgaben zu erledigen: **`systemctl`**. Hierbei gilt die Syntax „Befehl plus Unterbefehl“ 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`-Befehle 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 Unterbefehls ein und drücken dann `→|` . Diese Funktion ist nur in der `bash`-Shell verfügbar und das Paket `bash-completion` muss installiert sein.

19.2.1 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 Dienstverwaltungsbefehle 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 einen einzigen Befehl aus, beispielsweise:

```
> sudo systemctl start MY_1ST_SERVICE MY_2ND_SERVICE
```

So rufen Sie eine Liste aller auf dem System verfügbaren Dienste ab:

```
> sudo systemctl list-unit-files --type=service
```

Die folgende Tabelle zeigt die wichtigsten Dienstverwaltungsbefehle für `systemd` und System V-init:

TABELLE 19.1: BEFEHLE ZUR DIENSTVERWALTUNG

Aufgabe	**`systemd`-Befehl**	**System V-init-Befehl**
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`

Aufgabe	`systemd`-Befehl	System V-init-Befehl
Neu laden. Weist die Dienste an, die Konfigurationsdateien neu zu laden ohne die laufenden Vorgänge zu unterbrechen. Anwendungsbeispiel: Weisen Sie Apache an, eine bearbeitete `httpd.conf`-Konfigurationsdatei neu zu laden. Nicht alle Dienste unterstützen das Neuladen.	`reload`	`reload`
Neu laden oder neu starten. Lädt Dienste neu, wenn das Neuladen unterstützt wird; ansonsten werden die Dienste neu gestartet. Wenn ein Dienst noch nicht ausgeführt wird, wird er gestartet.	`reload-or-restart`	`n/a`
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. Der Befehl `systemd` zeigt Details wie Beschreibung, ausführbare Datei, Status, cgroup und zuletzt durch den Dienst ausgegebene Meldungen (siehe *Abschnitt 19.6.9, „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`

19.2.2 Dienste dauerhaft aktivieren/deaktivieren

Mit den Dienstverwaltungsbefehlen im vorangegangenen Abschnitt können Sie die Dienste für die aktuelle Sitzung bearbeiten. Mit `systemd` können Sie Dienste außerdem dauerhaft aktivieren oder deaktivieren, sodass sie entweder automatisch bei Bedarf gestartet werden oder gar nicht verfügbar sind. Sie können dies mithilfe von YaST oder über die Befehlszeile tun.

19.2.2.1 Aktivieren/Deaktivieren von Diensten über die Befehlszeile

Die folgende Tabelle zeigt die wichtigsten Aktivierungs- und Deaktivierungsbefehle für `systemd` und System V-init:

Wichtig: Dienststart

Wenn ein Dienst über die Befehlszeile aktiviert wird, wird er nicht automatisch gestartet. Der Dienst wird beim nächsten Systemstart oder bei der nächsten Änderung des Runlevels/Ziels gestartet. Um einen Dienst sofort zu starten, nachdem Sie ihn aktiviert haben, führen Sie **`systemctl start`** *MY_SERVICE* oder **`rc`** *MY_SERVICE* **`start`** explizit aus.

TABELLE 19.2: BEFEHLE ZUM AKTIVIEREN UND DEAKTIVIEREN VON DIENSTEN

Aufgabe	`systemd`-Befehl	System V-init-Befehl
Aktivieren von.	**`systemctl enable`** *MY_SERVICE(S)*	**`insserv`** *MY_SERVICE(S)*, **`chkconfig -a`** *MY_SERVICE(S)*
Deaktivieren.	**`systemctl disable`** *MY_SERVICE(S)*`.service`	**`insserv -r`** *MY_SERVICE(S)*, **`chkconfig -d`** *MY_SERVICE(S)*
Überprüfen. Zeigt an, ob ein Dienst aktiviert ist oder nicht.	**`systemctl is-enabled`** *MY_SERVICE*	**`chkconfig`** *MY_SERVICE*
Erneut aktivieren. Ähnlich wie beim Neustarten eines Diensts, deaktiviert dieser	**`systemctl reenable`** *MY_SERVICE*	n/v

Aufgabe	`systemd`-Befehl	System V-init-Befehl
Befehl einen Dienst und aktiviert ihn dann wieder. Nützlich, wenn ein Dienst mit den Standardeinstellungen erneut aktiviert werden soll.		
Maskierung. Nach dem „Deaktivieren“ eines Dienstes kann er weiterhin manuell aktiviert werden. Soll ein Dienst deaktiviert werden, maskieren Sie ihn. Mit Vorsicht verwenden.	**`systemctl mask`** *MY_SERVICE*	n/v
Demaskieren. Ein maskierter Dienst kann erst dann wieder genutzt werden, wenn er demaskiert wurde.	**`systemctl unmask`** *MY_SERVICE*	n/v

19.3 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.

19.3.1 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 nummeriert. 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 dieser Befehl 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 19.4, „Verwalten von Diensten mit YaST“*). Soll das Ziel für eine einzige Sitzung geändert werden, geben Sie den Kernel-Parameter `systemd.unit=`*`MY_TARGET.target`* am Bootprompt ein.

`emergency.target`
: Startet eine minimale `root`-Notfall-Shell an der Konsole. Dieser Befehl 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 `root`-Einzelbenutzersystem ohne Netzwerk. Es stehen grundlegende Werkzeuge für die Systemadministration zur Verfügung. Das `rescue`-Ziel eignet sich zum Lösen mehrerer Systemprobleme, z. B. zum Beheben fehlerhafter Anmeldungen oder zum Beheben von Problemen mit einem Anzeigetreiber.

Damit die Kompatibilität mit dem Runlevel-System von System V-init gewährleistet bleibt, bietet `systemd` besondere Ziele mit der Bezeichnung `runlevel`*X*`.target`, denen die entsprechenden, mit *X* nummerierten Runlevels zugeordnet sind.

Verwenden Sie zum Prüfen des aktuellen Ziels den folgenden Befehl: **`systemctl get-default`**

TABELLE 19.3: 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 19.5.5, „Erstellen von benutzerdefinierten Zielen“*.

19.3.1.1 Befehle zum Ändern von Zielen

Mit den folgenden Befehlen arbeiten Sie mit den Ziel-Units:

Aufgabe	**`systemd`-Befehl**	**System V-init-Befehl**
Aktuelles Ziel/ Runlevel ändern	**`systemctl isolate`** *MY_TARGET*.Ziel	**`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 Befehl werden alle derzeit aktiven Ziele aufgelistet.	**`who -r`** oder **`runlevel`**
Standard-Runlevel dauerhaft ändern	Verwenden Sie die Dienste-Verwaltung, oder führen Sie den folgenden Befehl aus: **`ln -sf /usr/lib/systemd/system/`** *MY_TARGET*.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=`** *MY_TARGET*.Ziel	Geben Sie an der Boot-Eingabeaufforderung die gewünschte Runlevel-Nummer ein.

Aufgabe	`systemd`-Befehl	System V-init-Befehl
Abhängigkeiten für ein Ziel/Runlevel anzeigen	**`systemctl show -p "Requires"`** *MY_TARGET*.Ziel **`systemctl show -p "Wants"`** *MY_TARGET*.Ziel „Requires“ (Benötigt) zeigt eine Liste der harten Abhängigkeiten (die in jedem Fall aufgelöst werden müssen), „Wants“ (Erwünscht) dagegen eine Liste der weichen Abhängigkeiten (die nach Möglichkeit aufgelöst werden).	n/v

19.3.2 Fehlersuche beim Systemstart

`systemd` bietet eine Möglichkeit, den Systemstartvorgang zu analysieren. Sie können die Liste der Dienste mit dem jeweiligen Status prüfen (ohne durch `/var/log/` blättern zu müssen). Mit `systemd` können Sie zudem den Startvorgang scannen und so ermitteln, wie lang das Starten der einzelnen Dienste dauert.

19.3.2.1 Prüfen des Startvorgangs der Dienste

Mit dem Befehl **`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`** *MY_SERVICE* erhalten Sie weitere Informationen zu einem bestimmten Dienst.

BEISPIEL 19.1: LISTE DER AKTIVEN DIENSTE

```
# 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
chronyd.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 19.2: LISTE DER FEHLERHAFTEN DIENSTE

```
# 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

[...]
```

19.3.2.2 Fehlersuche für die Startzeit

Mit dem Befehl **`systemd-analyze`** in `systemd` 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

```
# systemd-analyze
Startup finished in 2666ms (kernel) + 21961ms (userspace) = 24628ms
```

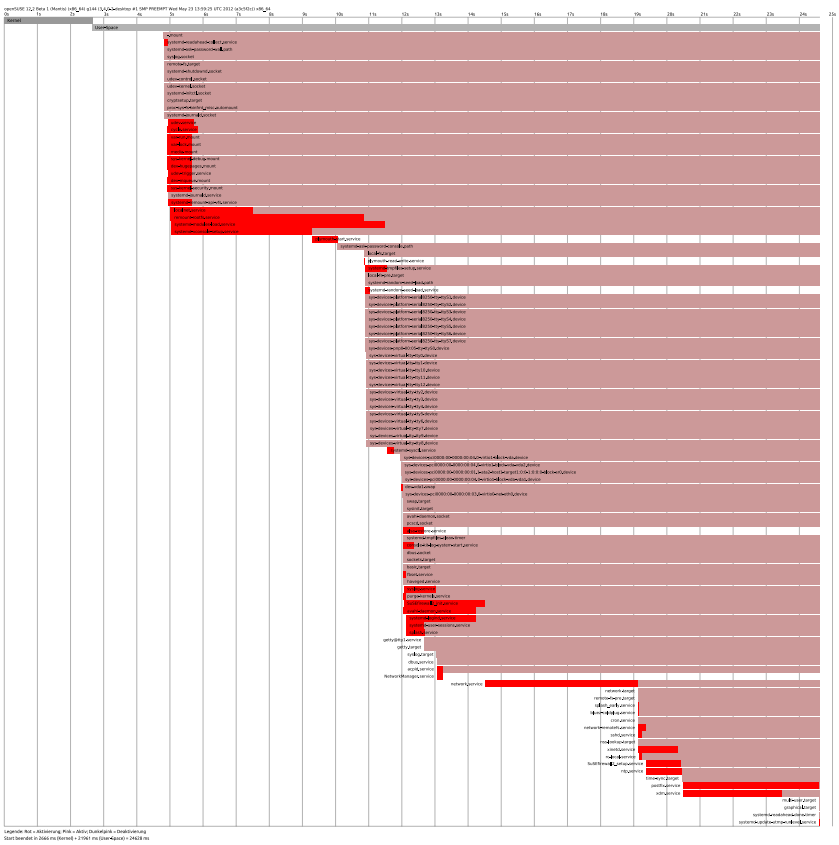
Auflisten der Startzeit der Dienste

```
# systemd-analyze blame
    15.000s backup-rpmdb.service
    14.879s mandb.service
     7.646s backup-sysconfig.service
     4.940s postfix.service
     4.921s logrotate.service
     4.640s libvirtd.service
```

```
     4.519s display-manager.service
     3.921s btrfsmaintenance-refresh.service
     3.466s lvm2-monitor.service
     2.774s plymouth-quit-wait.service
     2.591s firewalld.service
     2.137s initrd-switch-root.service
     1.954s ModemManager.service
     1.528s rsyslog.service
     1.378s apparmor.service
    [...]
```

Grafische Darstellung der Startzeit der Dienste

```
# systemd-analyze plot > jupiter.example.com-startup.svg
```



19.3.2.3 Prüfen des gesamten Startvorgangs

Die Befehle oben listen die gestarteten Dienste und ihre Startzeiten auf. Eine detailliertere Übersicht erhalten Sie, wenn Sie folgende Parameter an der Boot-Eingabeaufforderung angeben, damit `systemd` ein ausführliches Protokoll des gesamten Startvorgangs erstellt.

```
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
```

19.3.3 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 Dienst, 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 *`UPPERCASE LETTERS`* 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 `graphical.target`.

2. Starten Sie den Daemon mit **`systemctl start`** *`APPLICATION`*.

19.4 Verwalten von Diensten 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*.

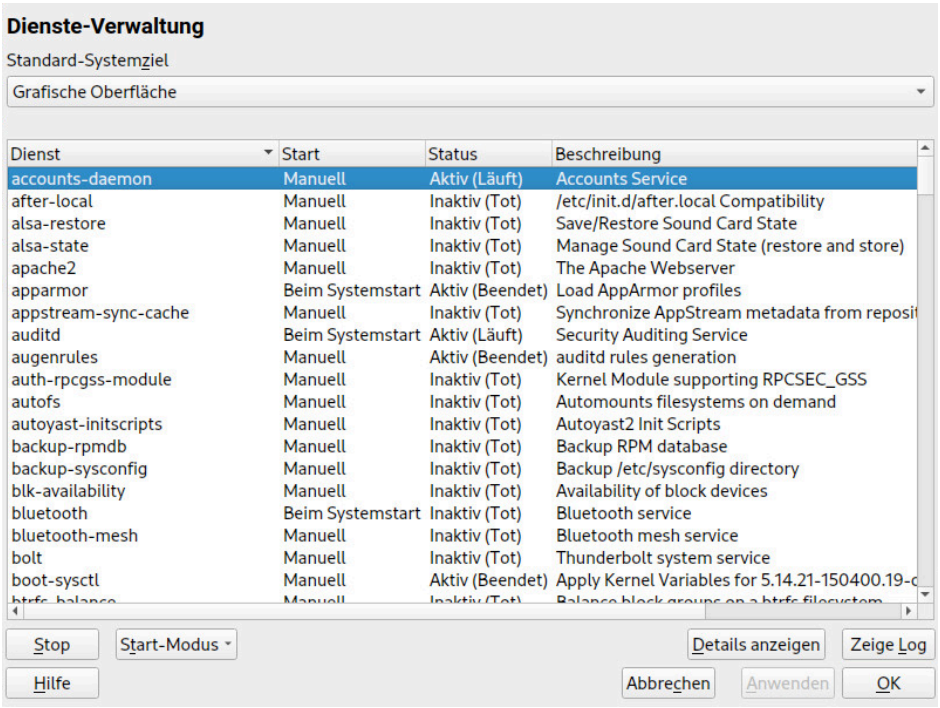


ABBILDUNG 19.1: DIENSTE-VERWALTUNG

Ändern des *Standard-Systemziels*

Zum Ändern des Ziels, in das das System gebootet wird, wählen Sie ein Ziel in der Dropdownliste *Standard Systemziel* aus. Die häufigsten Ziele sind *Grafische Oberfläche* (öffnet einen grafischen Anmeldebildschirm) und *Mehrbenutzer* (startet das System im Befehlszeilenmodus).

Starten oder Stoppen eines Dienstes

Wählen Sie einen Dienst in der Tabelle aus. Die Spalte *Status* zeigt, ob er derzeit ausgeführt wird (*Aktiv*) oder nicht (*Inaktiv*). Mit *Starten* bzw. *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.

Definieren des Verhaltens beim Starten von Diensten

Dienste können entweder automatisch bei Booten oder manuell gestartet werden. Wählen Sie einen Dienst in der Tabelle aus. Die Spalte *Start* zeigt, ob er derzeit gestartet ist: *Manuell* oder *Beim Booten*. Mit *Startmodus* schalten Sie den Status um.
Um den Status eines Dienstes in der aktuellen Sitzung zu ändern, müssen Sie ihn wie oben beschrieben 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` und dem Status *`MY_SERVICE`* identisch.

19.5 Anpassen `systemd`

In den folgenden Abschnitten wird beschrieben, wie `systemd`-Unit-Dateien angepasst werden.

19.5.1 Wo werden Unit-Dateien gespeichert?

Von SUSE bereitgestellte `systemd`-Unit-Dateien werden in `/usr/lib/systemd/` gespeichert. Benutzerdefinierte Unit-Dateien und *Drop-Ins* von Unit-Dateien werden in `/etc/systemd/` gespeichert.

Warnung: Verhindern des Überschreibens Ihrer Anpassung

Verwenden Sie beim Anpassen von `systemd` immer das Verzeichnis `/etc/systemd/` anstelle von `/usr/lib/systemd/`. Ansonsten werden Ihre Änderungen bei der nächsten Aktualisierung von `systemd` überschrieben.

19.5.2 Überschreiben mit Drop-In-Dateien

Drop-In-Dateien (oder *Drop-Ins*) sind teilweise Unit-Dateien, die nur bestimmte Einstellungen der Unit-Datei überschreiben. Drop-Ins haben Vorrang vor Hauptkonfigurationsdateien. Der Befehl **`systemctl edit`** *`SERVICE`* startet den Standardtexteditor und erstellt ein Verzeichnis mit einer leeren `override.conf`-Datei in `/etc/systemd/system/`*`NAME`*`.service.d/`. Der Befehl benachrichtigt außerdem den laufenden `systemd`-Vorgang über die Änderungen.

Um beispielsweise die Zeit zu ändern, die das System auf den Start von MariaDB wartet, führen Sie **`sudo systemctl edit mariadb.service`** aus und bearbeiten die geöffnete Datei so, dass nur die geänderten Zeilen eingefügt werden:

```
# Configures the time to wait for start-up/stop
TimeoutSec=300
```

Passen Sie den Wert `TimeoutSec` an und speichern Sie die Änderungen. Führen Sie zum Aktivieren der Änderungen **`sudo systemctl daemon-reload`** auf.

Weitere Informationen finden Sie auf den man-Seiten, die Sie mit dem Befehl **`man 1 systemctl`** aufrufen können.

Warnung: Erstellen einer Kopie einer vollständigen Unit-Datei

Wenn Sie die Option `--full` im Befehl **`systemctl edit --full`** *`SERVICE`* verwenden, wird eine Kopie der ursprünglichen Unit-Datei erstellt, in der Sie bestimmte Optionen ändern können. Eine solche Anpassung wird nicht empfohlen, da bei der Aktualisierung der Unit-Datei durch SUSE ihre Änderungen durch die angepasste Kopie im Verzeichnis `/etc/systemd/system/` überschrieben werden. Wenn SUSE Aktualisierungen für Distributions-Drop-Ins bereitstellt, überschreiben sie außerdem die Kopie der Unit-Datei, die mit `--full` wurde. Um diese Verwirrung zu vermeiden und damit Ihre Anpassung immer gültig bleibt, verwenden Sie Drop-Ins.

19.5.3 Manuelles Erstellen von Drop-in-Dateien

Neben der Verwendung des Befehls **`systemctl edit`** können Sie Drop-Ins manuell erstellen, um mehr Kontrolle über ihre Priorität zu haben. Mit solchen Drop-Ins können Sie sowohl Unit- als auch Daemon-Konfigurationsdateien erweitern, ohne die Dateien selbst bearbeiten oder überschreiben zu müssen. Sie werden in den folgenden Verzeichnissen gespeichert:

`/etc/systemd/*.conf.d/`, `/etc/systemd/system/*.service.d/`
: Drop-Ins, die von Systemadministratoren hinzugefügt und angepasst werden.

`/usr/lib/systemd/*.conf.d/`, `/usr/lib/systemd/system/*.service.d/`
: Drop-Ins, die von Anpassungspaketen installiert werden, um Upstream-Einstellungen zu überschreiben. SUSE stellt beispielsweise `systemd-default-settings` bereit.

Tipp

Auf der Manpage für **`man 5 systemd.unit`** finden Sie die vollständige Liste der Unit-Suchpfade.

Gehen Sie beispielsweise folgendermaßen vor, um die Ratenbegrenzung zu deaktivieren, die durch die Standardeinstellung von `systemd-journald` erzwungen wird:

1. Erstellen Sie ein Verzeichnis mit dem Namen `/etc/systemd/journald.conf.d`.

   ```
   > sudo mkdir /etc/systemd/journald.conf.d
   ```

   #### Anmerkung

   Der Verzeichnisname muss dem Dienstnamen folgen, den Sie mit der Drop-In-Datei patchen möchten.

2. Erstellen Sie in diesem Verzeichnis eine Datei mit der Option `/etc/systemd/journald.conf.d/60-rate-limit.conf`, die Sie überschreiben möchten, z. B.:

   ```
   > cat /etc/systemd/journald.conf.d/60-rate-limit.conf
   # Disable rate limiting
   RateLimitIntervalSec=0
   ```

3. Speichern Sie Ihre Änderungen und starten Sie den Dienst des entsprechenden Daemons `systemd` neu.

```
> sudo systemctl restart systemd-journald
```

Anmerkung: Vermeiden von Namenskonflikten

Damit Namenskonflikte zwischen Ihren Drop-Ins und von SUSE bereitgestellten Dateien vermieden werden, empfiehlt es sich, allen Drop-Ins eine zweistellige Nummer und einen Bindestrich voranzustellen, z. B. `80-override.conf`.

Die folgenden Bereiche sind reserviert:

- `0-19` ist für `systemd`-Upstream reserviert.
- `20-29` ist für `systemd` reserviert (von SUSE bereitgestellt).
- `30-39` ist für SUSE-Pakete reserviert (außer `systemd`).
- `40-49` ist für Pakete von Drittanbietern reserviert.
- `50` ist für Unit-Drop-In-Dateien reserviert, die mit **`systemctl set-property`** erstellt werden.

Geben Sie eine zweistellige Zahl oberhalb dieses Bereichs an, damit die von SUSE bereitgestellten Drop-Ins Ihre eigenen Drop-Ins nicht überschreiben können.

Tipp

Sie können mit **`systemctl cat $UNIT`** auflisten und überprüfen, welche Dateien in der Units-Konfiguration berücksichtigt werden.

Tipp

Da die Konfiguration von `systemd`-Komponenten auf verschiedene Stellen im Dateisystem verstreut sein kann, ist es möglicherweise schwierig, einen Gesamtüberblick zu erhalten. Verwenden Sie die folgenden Befehle, um die Konfiguration einer `systemd`-Komponente zu prüfen:

- **`systemctl cat`** *`UNIT_PATTERN`* druckt Konfigurationsdateien, die sich auf eine oder mehrere `systemd`-Units beziehen, z. B.:

```
> systemctl cat atd.service
```

- **`systemd-analyze cat-config`** *`DAEMON_NAME_OR_PATH`* kopiert den Inhalt einer Konfigurationsdatei und Drop-Ins für einen `systemd`-Daemon, z. B.:

```
> systemd-analyze cat-config systemd/journald.conf
```

19.5.4 Konvertieren von `xinetd`-Diensten in `systemd`

Seit der Version SUSE Linux Enterprise Desktop 15 wurde die `xinetd`-Infrastruktur entfernt. In diesem Abschnitt wird beschrieben, wie Sie vorhandene benutzerdefinierte `xinetd`-Dienstdateien in `systemd`-Sockets konvertieren.

Für jede `xinetd`-Dienstdatei benötigen Sie mindestens zwei `systemd`-Unit-Dateien: die Socket-Datei (`*.socket`) und eine zugehörige Dienstdatei (`*.service`). Die Socket-Datei weist `systemd` an, welcher Socket erstellt werden soll, und die Dienstdatei weist `systemd` an, welche ausführbare Datei gestartet werden soll.

Betrachten Sie das folgende Beispiel für eine `xinetd`-Dienstdatei:

```
# cat /etc/xinetd.d/example
service example
{
  socket_type = stream
  protocol = tcp
  port = 10085
  wait = no
  user = user
  group = users
  groups = yes
  server = /usr/libexec/example/exampled
```

```
  server_args = -auth=bsdtcp exampledump
  disable = no
}
```

Zum Konvertieren in `systemd` benötigen Sie die folgenden beiden Dateien:

```
# cat /usr/lib/systemd/system/example.socket
[Socket]
ListenStream=0.0.0.0:10085
Accept=false

[Install]
WantedBy=sockets.target
```

```
# cat /usr/lib/systemd/system/example.service
[Unit]
Description=example

[Service]
ExecStart=/usr/libexec/example/exampled -auth=bsdtcp exampledump
User=user
Group=users
StandardInput=socket
```

Eine vollständige Liste der `systemd` „Socket“- und „Dienst“-Dateioptionen finden Sie auf den Handbuchseiten für „systemd.socket“ und „systemd.service“ (**`man 5 systemd.socket`**, **`man 5 systemd.service`**).

19.5.5 Erstellen von benutzerdefinierten Zielen

Auf SUSE-Systemen mit System V-init wird Runlevel 4 nicht genutzt, sodass 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/`*`MY_TARGET`*`.target` und passen Sie sie entsprechend Ihrer Anforderungen an.
2. Die im vorangegangenen Schritt kopierte Konfigurationsdatei enthält bereits die erforderlichen („harten“) Abhängigkeiten für das Ziel. Um auch die gewünschten („weichen“) Abhängigkeiten abzudecken, erstellen Sie das Verzeichnis `/etc/systemd/system/`*`MY_TARGET`*`.target.wants`.

3. Erstellen Sie für jeden gewünschten Dienst einen symbolischen Link von `/usr/lib/systemd/system` nach `/etc/systemd/system/MY_TARGET.target.wants`.
4. Sobald Sie alle Einstellungen für das Ziel festgelegt haben, laden Sie die `systemd`-Konfiguration neu. Damit wird das neue Ziel verfügbar:

```
> sudo systemctl daemon-reload
```

19.6 Erweiterte Nutzung

In den nachfolgenden Abschnitten finden Sie weiterführende Themen für Systemadministratoren. Eine noch eingehendere Dokumentation zu `systemd` finden Sie in der Serie von Lennart Pöttering zu `systemd` für Administratoren unter https://0pointer.de/blog/projects/.

19.6.1 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` – für die Verwaltung temporärer Dateien verantwortlich – liest ihre Konfiguration aus den Dateien `/etc/tmpfiles.d/*.conf`, `/run/tmpfiles.d/*.conf` und `/usr/lib/tmpfiles.d/*.conf`. Die Konfiguration in `/etc/tmpfiles.d/*.conf` hat Vorrang vor ähnlichen Konfigurationen in den anderen beiden Verzeichnissen. (In `/usr/lib/tmpfiles.d/*.conf` werden die Konfigurationsdateien der Pakete gespeichert.)

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:

```
> sudo 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 2018-04-09 15:30:36 CEST; 1 weeks 6 days ago
   Docs: man:tmpfiles.d(5)
         man:systemd-tmpfiles(8)
```

```
Apr 09 15:30:36 jupiter systemd[1]: Starting Daily Cleanup of Temporary Directories.
Apr 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`**.

19.6.2 Systemprotokoll

In *Abschnitt 19.6.9, „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`**.

19.6.3 Aufnahmen

Mit dem Unterbefehl **`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

```
> sudo systemctl snapshot MY_SNAPSHOT.snapshot
```

Löschen eines Snapshots

```
> sudo systemctl delete MY_SNAPSHOT.snapshot
```

Anzeigen eines Snapshots

```
> sudo systemctl show MY_SNAPSHOT.snapshot
```

Aktivieren eines Snapshots

```
> sudo systemctl isolate MY_SNAPSHOT.snapshot
```

19.6.4 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 *`MODULE`*.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 zu `modules-load.d(5)`.

19.6.5 Ausführen von Aktionen vor dem Laden eines Dienstes

Bei System V mussten init-Aktionen, die vor dem Laden eines Dienstes 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 Vorlage:

```
[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 Befehle aus (als `root`):

```
> sudo systemctl daemon-reload
> sudo systemctl enable before
```

Bei jedem Bearbeiten der Dienstdatei müssen Sie Folgendes ausführen:

```
> sudo systemctl daemon-reload
```

19.6.6 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. Bestimmt 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. bestimmte 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. `systemd` benennt die cgroups dabei nach dem jeweiligen Dienst. 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 Befehl **`systemd-cgls`** erhalten Sie eine Liste aller Prozesse, die zu einem Dienst gehören, z. B.:

BEISPIEL 19.3: AUFLISTEN ALLER PROZESSE, DIE ZU EINEM DIENST GEHÖREN

```
# 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
  ├─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 im *Buch „System Analysis and Tuning Guide“, Kapitel 10 „Kernel control groups“*.

19.6.7 Beenden von Diensten (Senden von Signalen)

Wie in *Abschnitt 19.6.6, „Kernel-Steuergruppen (cgroups)“* erläutert, kann ein Prozess in einem System-V-init-System nicht immer eindeutig seinem übergeordneten Dienstprozess zugeordnet werden. Das erschwert das Anhalten eines Diensts und seiner untergeordneten Dienste. Untergeordnete Prozesse, die nicht ordnungsgemäß beendet wurden, bleiben als „Zombie-Prozesse“ zurück.

Durch das Konzept von `systemd`, mit dem jeder Dienst in einer eigenen cgroup abgegrenzt wird, können alle untergeordneten Prozesse eines Diensts 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.

```
> sudo systemctl kill MY_SERVICE
```

Senden von *`SIGNAL`* an einen Dienst

Mit der Option `-s` legen Sie das zu sendende Signal fest.

```
> sudo systemctl kill -s SIGNAL MY_SERVICE
```

Auswählen von Prozessen

Standardmäßig sendet der Befehl **`kill`** das Signal an alle (`all`) Prozesse der angegebenen cgroup. Sie können dies jedoch auf den Prozess `control` oder `main` beschränken. Damit können Sie beispielsweise das Neuladen der Konfiguration eines Diensts mit dem Signal `SIGHUP` erzwingen:

```
> sudo systemctl kill -s SIGHUP --kill-who=main MY_SERVICE
```

19.6.8 Wichtige Hinweise zum D-Bus-Dienst

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 Anhalten von `dbus` oder das Neustarten im laufenden System entspricht dem Versuch, PID 1 zu anzuhalten oder neu zu starten. Dadurch wird die Client/Server-Kommunikation von `systemd` unterbrochen und die meisten `systemd`-Funktionen werden unbrauchbar.

Das Beenden oder Neustarten von `dbus` wird daher weder empfohlen noch unterstützt.

Nach einer Aktualisierung von `dbus` oder `dbus`-Paketen fällt ein Neustart an. Wenn Sie sich nicht sicher sind, ob ein Neustart erforderlich ist, führen Sie den Befehl **`sudo zypper ps -s`** aus. Ist `dbus` unter den aufgelisteten Diensten zu finden, müssen Sie das System neu starten.

Beachten Sie, dass `dbus` selbst dann aktualisiert wird, wenn in der Konfiguration der automatischen Aktualisierungen festgelegt ist, dass die Pakete, die einen Neustart erfordern, übersprungen werden sollen.

19.6.9 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. **`systemctl status`** bietet jedoch eine Möglichkeit, den Start und Betrieb eines Diensts zu debuggen.

`systemd` umfasst einen Protokollierungsmechanismus („Journal“), mit dem die Systemmeldungen protokolliert werden. Auf diese Weise können Sie die Dienstmeldungen zusammen mit den Statusmeldungen abrufen. Der Befehl **`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`** *`MY_SERVICE`* eine ausführliche Fehlermeldung:

```
# systemctl start apache2
Job failed. See system journal and 'systemctl status' for details.
# systemctl status apache2
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled)
   Active: failed (Result: exit-code) since Mon, 04 Apr 2018 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

Apr 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 von Nachrichten fest:

```
> sudo systemctl status chronyd
> sudo systemctl --lines=20 status chronyd
```

Anzeigen von Dienstmeldungen im Anhängemodus

Mit der Option `--follow` erhalten Sie einen „Live-Stream“ mit Dienstmeldungen; diese Option entspricht **`tail`** `-f`:

```
> sudo systemctl --follow status chronyd
```

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.

19.7 systemd-Zeitgeber-Units

Ähnlich wie Cron bieten systemd-Zeitgeber-Units einen Mechanismus für die Planung von Aufträgen unter Linux. Die systemd-Zeitgeber-Units dienen zwar demselben Zweck wie Cron, eröffnen allerdings mehrere Vorteile.

- Aufträge, die mit einer Zeitgeber-Unit geplant werden, können von anderen systemd-Diensten abhängig sein.
- Zeitgeber-Units werden wie normale systemd-Dienste behandelt und können daher mit **systemctl** verwaltet werden.
- Timer können in Echtzeit und monoton vorliegen.
- Zeiteinheiten werden im systemd-Journal protokolliert, was die Überwachung und Fehlerbehebung vereinfacht.

systemd-Zeitgeber-Units sind mit der Dateinamenerweiterung .timer gekennzeichnet.

19.7.1 systemd-Zeitgebertypen

Timer-Einheiten können monotone und Echtzeit-Timer verwenden.

- Ähnlich wie Cronjobs werden Echtzeit-Zeitgeber durch Kalenderereignisse ausgelöst. Echtzeit-Zeitgeber werden mit der Option OnCalendar definiert.
- Monotone Zeitgeber werden ausgelöst, sobald ein angegebener Zeitraum nach einem bestimmten Startpunkt vergangen ist. Dies ist beispielsweise ein Systemstart-Ereignis oder ein System-Unit-Aktivierungsereignis. Für die Definition von monotonen Zeitgebern stehen mehrere Optionen zur Auswahl, einschließlich OnBootSec, OnUnitActiveSec und OnTypeSec. Monotone Timer sind nicht permanent und werden nach jedem Neustart zurückgesetzt.

19.7.2 systemd-Timer und Dienst-Units

Für jede Zeitgeber-Unit muss eine entsprechende systemd-Unit-Datei vorliegen, die durch die Zeitgeber-Unit gesteuert wird. Anders ausgedruckt aktiviert und verwaltet eine .timer-Datei die entsprechende .service-Datei. Wird eine .service-Datei mit einem Zeitgeber verwendet, muss die Datei keinen Abschnitt [Install] enthalten, da der Dienst durch den Zeitgeber verwaltet wird.

19.7.3 Beispiel aus der Praxis

Zur Veranschaulichung der Grundlagen von `systemd`-Zeitgeber-Units soll ein Zeitgeber eingerichtet werden, der das Shell-Skript `foo.sh` auslöst.

Im ersten Schritt erstellen Sie eine `systemd`-Dienst-Unit, die das Shell-Skript steuert. Öffnen Sie dazu eine neue Textdatei zur Bearbeitung und fügen Sie die folgende Dienst-Unit-Definition hinzu:

```
[Unit]
Description="Foo shell script"

[Service]
ExecStart=/usr/local/bin/foo.sh
```

Speichern Sie die Datei unter dem Namen `foo.service` im Verzeichnis `/etc/systemd/system/`.

Öffnen Sie als Nächstes eine neue Textdatei zur Bearbeitung und fügen Sie die folgende Timer-Definition hinzu:

```
[Unit]
Description="Run foo shell script"

[Timer]
OnBootSec=5min
OnUnitActiveSec=24h
Unit=foo.service

[Install]
WantedBy=multi-user.target
```

Der Abschnitt `[Timer]` im Beispiel oben gibt an, welcher Dienst (`foo.service`) ausgelöst werden soll und wann er ausgelöst werden soll. In diesem Fall gibt die Option `OnBootSec` einen monotonen Zeitgeber an, der den Dienst fünf Minuten nach Systemstart auslöst, während die Option `OnUnitActiveSec` den Dienst 24 Stunden nach Aktivierung des Diensts auslöst (der Zeitgeber löst den Dienst also einmal täglich aus). Die Option `WantedBy` gibt schließlich an, dass der Zeitgeber gestartet werden soll, sobald das System das Mehrbenutzerziel erreicht hat.

Anstelle eines monotonen Zeitgebers können Sie mit der Option `OnCalendar` einen Echtzeit-Zeitgeber angeben. Die folgende Echtzeit-Zeitgeberdefinition löst die zugehörige Dienst-Unit einmal wöchentlich aus, beginnend am Montag um 12:00 Uhr.

```
[Timer]
OnCalendar=weekly
Persistent=true
```

Die Option `Persistent=true` gibt an, dass der Dienst sofort nach Aktivierung des Zeitgebers ausgelöst wird, falls der Zeitgeber die letzte Startzeit versäumt hat (z. B. weil das System ausgeschaltet war).

Mit der Option `OnCalendar` können außerdem bestimmte Zeitpunkte (Datum und Uhrzeit) für die Auslösung eines Dienstes im folgenden Format definiert werden: `DayOfWeek Year-Month-Day Hour:Minute:Second` Im folgenden Beispiel wird ein Dienst täglich um 5:00 Uhr gestartet:

```
OnCalendar=*-*-* 5:00:00
```

Sie können ein Sternchen verwenden, um einen beliebigen Wert anzugeben, und Kommas, um mögliche Werte aufzulisten. Zwei Werte, die durch zwei Punkte (..) getrennt sind, geben einen zusammenhängenden Bereich an. Im folgenden Beispiel wird ein Dienst an jedem Freitag im Monat um 18:00 Uhr gestartet:

```
OnCalendar=Fri *-*-1..7 18:00:00
```

Soll ein Dienst zu verschiedenen Zeiten ausgelöst werden, können Sie mehrere `OnCalendar`-Einträge angeben:

```
OnCalendar=Mon..Fri 10:00
OnCalendar=Sat,Sun 22:00
```

Im Beispiel oben wird ein Dienst an Wochentagen um 10 Uhr und am Wochenende um 22 Uhr ausgelöst.

Wenn Sie die Zeitgeber-Unit-Datei bearbeitet haben, speichern Sie sie unter dem Namen `foo.timer` im Verzeichnis `/etc/systemd/system/`. Prüfen Sie die erstellten Unit-Dateien mit folgendem Befehl:

```
> sudo  systemd-analyze verify /etc/systemd/system/foo.*
```

Wenn der Befehl keine Ausgabe zurückgibt, haben die Dateien die Überprüfung erfolgreich bestanden.

Starten Sie den Zeitgeber mit dem Befehl **`sudo systemctl start foo.timer`**. Soll der Zeitgeber beim Starten aktiviert werden, führen Sie den Befehl **`sudo systemctl enable foo.timer`** aus.

19.7.4 Verwalten von systemd-Zeitgebern

Da Zeitgeber wie normale systemd-Units behandelt werden, können Sie sie mit **systemctl** verwalten. Sie können einen Timer mit **systemctl start** starten, einen Timer mit **systemctl enable** aktivieren usw. Außerdem können Sie mit dem Befehl **systemctl list-timers** alle aktiven Zeitgeber auflisten. Mit dem Befehl **systemctl list-timers --all** werden alle Zeitgeber aufgelistet, auch wenn sie inaktiv sind.

19.8 Weitere Informationen

Weitere Informationen zu systemd finden Sie in folgenden Online-Quellen:

Startseite

https://systemd.io/

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 https://0pointer.de/blog/projects/ zu finden.

III System

20 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung 313

21 **`journalctl`**: Abfragen des `systemd`-Journals 315

22 **`update-alternatives`**: Verwalten mehrerer Befehls- und Dateiversionen 323

23 Grundlegendes zu Netzwerken 332

24 Druckerbetrieb 405

25 Über die grafische Benutzeroberfläche 421

26 Zugriff auf Dateisysteme mit FUSE 442

27 Installieren von mehreren Kernel-Versionen 444

28 Verwalten von Kernelmodulen 452

29 Gerätemanagement über dynamischen Kernel mithilfe von `udev` 456

30 Spezielle Systemfunktionen 470

31 Verwendung von NetworkManager 483

20 32-Bit- und 64-Bit-Anwendungen in einer 64-Bit-Systemumgebung

SUSE® Linux Enterprise Desktop ist für 64-Bit-Plattformen verfügbar. Die Entwickler haben nicht alle 32-Bit-Anwendungen auf 64-Bit-Systeme portiert. Dieses Kapitel bietet einen kurzen Überblick darüber, wie die 32-Bit-Unterstützung auf SUSE Linux Enterprise Desktop-64-Bit-Plattformen implementiert wird.

SUSE Linux Enterprise Desktop für die 64-Bit-Plattformen AMD64 und Intel 64 ist so konzipiert, dass bestehende 32-Bit-Anwendungen in der 64-Bit-Umgebung ausgeführt werden können – und zwar als „Sofortlösungen“. 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.

Anmerkung: Keine Unterstützung für die Erstellung von 32-Bit-Anwendungen

SUSE Linux Enterprise Desktop unterstützt nicht die Kompilierung von 32-Bit-Anwendungen. Laufzeitunterstützung wird nur für 32-Bit-Binärdateien angeboten.

20.1 Laufzeitunterstützung

Wichtig: Konflikte zwischen Anwendungsversionen

Sollte eine Anwendung sowohl für 32-Bit-Umgebungen als auch für 64-Bit-Umgebungen verfügbar sein, verursacht die Installation von beiden Versionen möglicherweise Probleme. Entscheiden Sie sich in diesem Fall für die Installation einer Version, um potenzielle Laufzeitprobleme zu vermeiden.

Eine Ausnahme von dieser Regel ist PAM (Pluggable Authentication Modules). Während des Authentifizierungsprozesses verwendet SUSE Linux Enterprise Desktop PAM (austauschbare Authentifizierungsmodule) als Schicht für die Vermittlung zwischen Benutzer und Anwendung. Installieren Sie immer beide PAM-Versionen auf 64-Bit-Betriebssystemen, die auch 32-Bit-Anwendungen ausführen.

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

32-Bit- und 64-Bit-Bibliotheken sind am selben Standort gespeichert, um die Kompatibilität mit 32-Bit-Versionen aufrechtzuerhalten. 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` befanden, befinden sich nun unter `/lib64` und `/usr/lib64`. Unter `/lib` und `/usr/lib` ist also Platz für die 32-Bit-Bibliotheken, sodass der Dateiname für beide Versionen unverändert bleiben kann.

Wenn Dateninhalte von 32-Bit-Unterverzeichnissen unter `/lib` nicht von der Wortgröße abhängig sind, werden sie nicht verschoben. Dieses Schema entspricht LSB (Linux Standards Base) und FHS (Filesystem Hierarchy Standard, Dateisystem-Hierarchiestandard).

20.2 Kernel-Spezifikationen

Die 64-Bit-Kernel für AMD64/Intel 64 bieten sowohl eine 64-Bit- als auch eine 32-Bit-Kernel-ABI (binäre Anwendungsschnittstelle). Letztere ist mit der ABI für den entsprechenden 32-Bit-Kernel identisch. Dies bedeutet, dass die Kommunikation zwischen 32-Bit- und 64-Bit-Anwendungen mit 64-Bit-Kernel identisch ist.

Die 32-Bit-Systemaufrufemulation für 64-Bit-Kernel unterstützt nicht alle APIs, die von Systemprogrammen verwendet werden. Dies hängt von der Plattform ab. Daher müssen einige Anwendungen wie **`lspci`** kompiliert werden.

Ein 64-Bit-Kernel kann nur 64-Bit-Kernel-Module laden. 64-Bit-Module müssen speziell für 64-Bit-Kernel kompiliert werden. Es ist nicht möglich, 32-Bit-Kernel-Module mit 64-Bit-Kernels zu verwenden.

Tipp: Kernel-ladbare Module

Für bestimmte Anwendungen sind separate, Kernel-ladbare Module erforderlich. Sollten Sie eine 32-Bit-Anwendung in einer 64-Bit-Systemumgebung verwenden wollen, kontaktieren Sie den Anwendungsanbieter und SUSE. Stellen Sie sicher, dass die 64-Bit-Version des Kernel-ladbaren Moduls und die kompilierte 32-Bit-Version der Kernel-API für dieses Modul verfügbar sind.

21 `journalctl`: Abfragen des `systemd`-Journals

`systemd` umfasst ein eigenes Protokollierungssystem, das als *Journal* bezeichnet wird. Alle Systemereignisse werden in das Journal geschrieben, so dass Sie keinen `syslog`-basierten Service 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:

```
> sudo 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
[...]
```

21.1 Festlegen des Journals als permanent

Das Journal speichert die Protokolldaten standardmäßig in `/run/log/journal/`. Das Verzeichnis `/run/` ist naturgemäß flüchtig, weshalb die Protokolldaten beim Neubooten verloren gehen. Damit die Protokolldaten permanent sind, erstellen Sie das Verzeichnis `/var/log/journal/` und stellen Sie sicher, dass es über die richtigen Zugriffsmodi und den richtigen Eigentümer verfügt, damit der Dienst „systemd-journald“ seine Daten speichern kann. Führen Sie die folgenden Befehle aus, um zur permanenten Protokollierung zu wechseln:

```
> sudo  mkdir /var/log/journal
> sudo  systemd-tmpfiles --create --prefix=/var/log/journal
> sudo  journalctl --flush
```

Alle Protokolldaten, die in `/run/log/journal/` gespeichert sind, werden in `/var/log/journal/` übertragen.

21.2 `journalctl`: Nützliche Schalter

In diesem Abschnitt finden Sie einige häufig verwendete, nützliche Optionen, mit denen Sie das Standardverhalten von **`journalctl`** optimieren. Alle Schalter sind auf der Manpage 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:

```
> sudo journalctl /usr/lib/systemd/systemd
```

-f

Zeigt lediglich die jüngsten Protokollmeldungen an und gibt neue Protokolleinträge aus, sobald sie zum Journal hinzugefügt werden.

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 21.3.3, „Filtern nach Feldern“*).

-u

Zeigt nur Meldungen für die angegebene `systemd`-Einheit an. Dies entspricht der Feldzuordnung `_SYSTEMD_UNIT=`*`UNIT`* (siehe *Abschnitt 21.3.3, „Filtern nach Feldern“*).

```
> sudo 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.
```

21.3 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.

21.3.1 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:

```
> sudo 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:

```
> sudo 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:

```
> sudo journalctl -b -1
```

Alternativ können Sie die Bootmeldungen nach der Boot-ID auflisten. Verwenden Sie hierzu das Feld _BOOT_ID:

```
> sudo journalctl _BOOT_ID=156019a44a774a0bb0148a92df4af81b
```

21.3.2 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 `yesterday`, `today` oder `tomorrow` angeben. Diese Wörter bezeichnen Mitternacht am Tag vor dem aktuellen Tag, am aktuellen Tag bzw. am Tag nach dem aktuellen Tag. Das Schlüsselwort `now` 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:

```
> sudo journalctl --since "now" -f
```

Alle Meldungen ab der letzten Mitternacht bis 3:20 Uhr anzeigen:

```
> sudo journalctl --since "today" --until "3:20"
```

21.3.3 Filtern nach Feldern

Sie können die Ausgabe des Journals nach bestimmten Feldern filtern. Die Syntax für ein abzugleichendes Feld lautet `FIELD_NAME=MATCHED_VALUE`, 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:

```
> sudo 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`**):

```
> sudo journalctl _TRANSPORT=kernel
```

Meldungen aus der Standard- oder Fehlerausgabe des Services anzeigen:

```
> sudo journalctl _TRANSPORT=stdout
```

Nur Meldungen anzeigen, die von einem bestimmten Service erzeugt wurden:

```
> sudo journalctl _SYSTEMD_UNIT=avahi-daemon.service
```

Wenn Sie zwei verschiedene Felder angeben, werden nur solche Einträge zurückgegeben, die beide Ausdrücke gleichzeitig erfüllen:

```
> sudo 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:

```
> sudo 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:

```
> sudo journalctl _SYSTEMD_UNIT=avahi-daemon.service _PID=1480 +
 _SYSTEMD_UNIT=dbus.service
```

21.4 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:

   ```
   > sudo 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:

   ```
   > sudo 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-Dienst und lassen Sie den Status ausgeben:

```
> sudo 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 [...]
```

21.5 Konfiguration von journald

Das Verhalten des systemd-journald-Service lässt sich durch Ändern von `/etc/systemd/journald.conf` anpassen. 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:

```
> sudo systemctl restart systemd-journald
```

21.5.1 Ändern der Größenbeschränkung für das Journal

Wenn die Journalprotokolldaten an einem permanenten Speicherort gespeichert werden (siehe *Abschnitt 21.1, „Festlegen des Journals als permanent“*), 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
```

21.5.2 Weiterleiten des Journals an `/dev/ttyX`

Sie können das Journal an ein Terminalgerät weiterleiten, sodass Sie an einem bevorzugten Terminalbildschirm (beispielsweise `/dev/tty12`) über Systemmeldungen informiert werden. Ändern Sie die folgenden journald-Optionen:

```
ForwardToConsole=yes
TTYPath=/dev/tty12
```

21.5.3 Weiterleiten des Journals an die Syslog-Funktion

journald ist abwärtskompatibel zu herkömmlichen syslog-Implementierungen wie `rsyslog`. Prüfen Sie Folgendes:

- rsyslog ist installiert.

  ```
  > sudo rpm -q rsyslog
  rsyslog-7.4.8-2.16.x86_64
  ```

- Der rsyslog-Service ist aktiviert.

  ```
  > sudo systemctl is-enabled rsyslog
  enabled
  ```

- Die Weiterleitung an syslog wird in `/etc/systemd/journald.conf` aktiviert.

  ```
  ForwardToSyslog=yes
  ```

21.6 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`**.

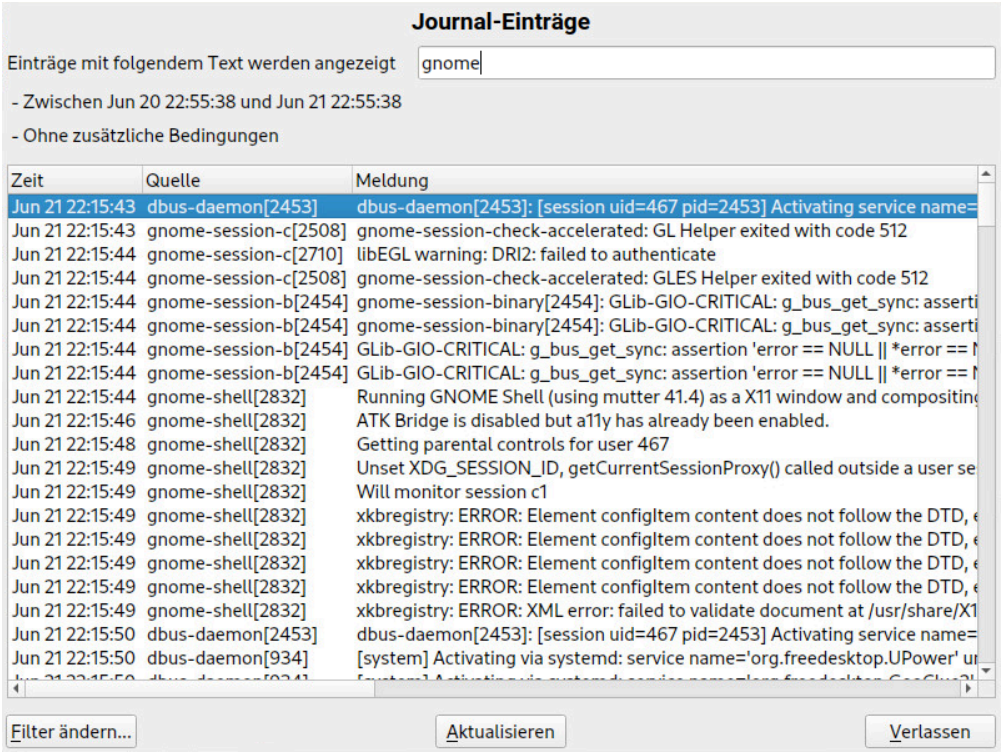


ABBILDUNG 21.1: YAST-SYSTEMD-JOURNAL

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.

21.7 Abrufen von Protokollen in GNOME

Sie können das Journal mit den *GNOME-Protokollen* abrufen. Starten Sie diesen Befehl über das Anwendungsmenü. Zum Abrufen von Systemprotokollmeldungen muss dieser Befehl als root ausgeführt werden, beispielsweise mit **`xdg-su gnome-logs`**. Dieser Befehl kann mit `Alt`–`F2` ausgeführt werden.

22 `update-alternatives`: Verwalten mehrerer Befehls- und Dateiversionen

Häufig sind gleich mehrere Versionen eines Werkzeugs auf einem System installiert. Mit dem Alternativen-System lassen sich diese Versionen konsistent verwalten. So können die Administratoren eine Auswahl treffen und es ist möglich, verschiedene Versionen nebeneinander zu installieren und zu nutzen.

22.1 Übersicht

Auf SUSE Linux Enterprise Desktop haben mehrere Programme identische oder ähnliche Aufgaben. Wenn beispielsweise sowohl Java 1.7 als auch Java 1.8 auf einem System installiert sind, wird das Skript des Alternativen-Systems (`update-alternatives`) aus dem RPM-Paket heraus aufgerufen. Standardmäßig verweist das Alternativen-System auf Version 1.8: Höhere Versionen besitzen auch eine höhere Priorität. Der Administrator kann jedoch die Standardeinstellung ändern, sodass der generische Name auf Version 1.7 verweist.

In diesem Kapitel gilt die folgende Terminologie:

TERMINOLOGIE

Administrationsverzeichnis

Das Standardverzeichnis `/var/lib/rpm/alternatives` enthält Informationen zum aktuellen Status der Alternativen.

Alternativ

Name einer bestimmten Datei im Dateisystem. Der Zugriff auf diese Datei erfolgt anhand eines generischen Namens über das Alternativen-System.

Alternativen-Verzeichnis

Standardverzeichnis `/etc/alternatives` mit symbolischen Links.

Generischer Name

Name (z. B. `/usr/bin/edit`), der auf eine von mehreren über das Alternativen-System verfügbaren Dateien verweist.

Link-Gruppe

Gruppe zusammengehöriger symbolischer Links, die als Gruppe aktualisiert werden können.

Master-Link
: Link in Link-Gruppe, der bestimmt, wie die anderen Links in der Gruppe konfiguriert werden.

Slave-Link
: Link in einer Link-Gruppe, der durch den Master-Link gesteuert wird.

Symbolischer Link (Symlink)
: Datei, die auf eine andere Datei in demselben Dateisystem verweist. Das Alternativen-System schaltet über symbolische Links im Alternativen-Verzeichnis zwischen den verschiedenen Versionen einer Datei um.
Der Administrator kann die symbolischen Links im Alternativen-Verzeichnis mit dem Befehl **`update-alternatives`** bearbeiten.

Mit dem Befehl **`update-alternatives`** im Alternativen-System lassen sich symbolische Links erstellen entfernen und pflegen sowie Informationen zu diesen Links abrufen. Diese symbolischen Links verweisen in der Regel auf Befehle, können allerdings auch auf JAR-Archive, man-Seiten und andere Dateien verweisen. Die Beispiele in diesem Kapitel zeigen Befehle und man-Seiten, gelten jedoch auch für andere Dateitypen.

Im Alternativen-Verzeichnis legt das Alternativen-System die Links zu möglichen Alternativen ab. Wenn ein neues Paket mit einer Alternative installiert wird, wird die neue Alternative in das System aufgenommen. Die Entscheidung, ob die Alternative des neuen Pakets als Standard festgelegt werden soll, ist abhängig von der Priorität des Pakets und vom ausgewählten Modus. Pakete mit einer höheren Version haben auch eine höhere Priorität. Das Alternativen-System bietet zwei Modi:

- **Automatischer Modus.** In diesem Modus sorgt das Alternativen-System dafür, dass die Links in der Gruppe auf die geeigneten Alternativen mit der höchsten Priorität für die Gruppe verweisen.
- **Manueller Modus.** In diesem Modus nimmt das Alternativen-System keine Änderungen an den Einstellungen des Systemadministrators vor.

Für das Kommando **`java`** gilt beispielsweise die folgende Link-Hierarchie im Alternativen-System:

BEISPIEL 22.1: ALTERNATIVEN-SYSTEM FÜR DEN BEFEHL `java`

```
/usr/bin/java ❶
```

```
 -> /etc/alternatives/java ❷
     -> /usr/lib64/jvm/jre-10-openjdk/bin/java ❸
```

❶ Generischer Name.

❷ Symbolischer Link im Alternativen-Verzeichnis.

❸ Eine der Alternativen.

22.2 Einsatzbereiche

Standardmäßig wird das Skript **`update-alternatives`** aus einem RPM-Paket heraus aufgerufen. Wenn ein Paket installiert oder entfernt wird, bearbeitet das Skript alle zugehörigen symbolischen Links. Sie können das Skript jedoch auch manuell über die Befehlszeile ausführen und so:

- die aktuellen Alternativen für einen generischen Namen abrufen.
- die Standardeinstellungen für eine Alternative ändern.
- eine Gruppe zusammengehöriger Dateien für eine Alternative erstellen.

22.3 Überblick über Alternativen

Die Namen aller konfigurierten Alternativen erhalten Sie mit:

```
> ls /var/lib/alternatives
```

Einen Überblick über alle konfigurierten Alternativen und deren Werte erhalten Sie mit

```
> sudo update-alternatives --get-selections
asadmin                        auto     /usr/bin/asadmin-2.7
awk                            auto     /usr/bin/gawk
chardetect                     auto     /usr/bin/chardetect-3.6
dbus-launch                    auto     /usr/bin/dbus-launch.x11
default-displaymanager         auto     /usr/lib/X11/displaymanagers/gdm
[...]
```

22.4 Anzeigen von Details zu spezifischen Alternativen

Am einfachsten überprüfen Sie die Alternativen, wenn Sie den symbolischen Links des Befehls folgen. Um beispielsweise herauszufinden, worauf sich der Befehl **java** bezieht, verwenden Sie den folgenden Befehl:

```
> readlink --canonicalize /usr/bin/java
/usr/lib64/jvm/jre-10-openjdk/bin/java
```

Falls jeweils derselbe Pfad angezeigt wird (in diesem Beispiel `/usr/bin/java`), stehen keine Alternativen für diesen Befehl zur Auswahl.

Mit der Option `--display` rufen Sie sämtliche Alternativen (mit Slaves) ab:

```
> sudo update-alternatives --display java
java - auto mode
  link best version is /usr/lib64/jvm/jre-1.8.0-openjdk/bin/java
  link currently points to /usr/lib64/jvm/jre-1.8.0-openjdk/bin/java
  link java is /usr/bin/java
  slave java.1.gz is /usr/share/man/man1/java.1.gz
  slave jre is /usr/lib64/jvm/jre
  slave jre_exports is /usr/lib64/jvm-exports/jre
  slave keytool is /usr/bin/keytool
  slave keytool.1.gz is /usr/share/man/man1/keytool.1.gz
  slave orbd is /usr/bin/orbd
  slave orbd.1.gz is /usr/share/man/man1/orbd.1.gz
[...]
```

22.5 Festlegen der Standardversion von Alternativen

Standardmäßig verweisen die Kommandos unter `/usr/bin` auf das Alternativen-Verzeichnis mit der höchsten Priorität. Der Befehl **java** gibt beispielsweise standardmäßig die folgende Versionsnummer zurück:

```
> java -version
openjdk version "10.0.1" 2018-04-17
OpenJDK Runtime Environment (build 10.0.1+10-suse-lp150.1.11-x8664)
OpenJDK 64-Bit Server VM (build 10.0.1+10-suse-lp150.1.11-x8664, mixed mode)
```

Ändern Sie die Standardeinstellung, sodass der Befehl **java** auf eine frühere Version verweist, mit dem folgenden Befehl:

```
> sudo update-alternatives --config java
root's password:
There are 2 choices for the alternative java (providing /usr/bin/java).

  Selection    Path                                          Priority   Status
------------------------------------------------------------
* 0            /usr/lib64/jvm/jre-10-openjdk/bin/java         2005      auto mode
  1            /usr/lib64/jvm/jre-1.8.0-openjdk/bin/java      1805      manual mode
  2            /usr/lib64/jvm/jre-10-openjdk/bin/java         2005      manual mode
  3            /usr/lib64/jvm/jre-11-openjdk/bin/java         0         manual mode

Press <enter> to keep the current choice[*], or type selection number:
```

Die genaue Java-Versionsnummer ist dabei abhängig von Ihrem System und von den installierten Versionen. Wenn Sie 1 ausgewählt haben, zeigt **java** die folgende Versionsnummer an:

```
> java -version
java version "1.8.0_171"
OpenJDK Runtime Environment (IcedTea 3.8.0) (build 1.8.0_171-b11 suse-lp150.2.3.1-x86_64)
OpenJDK 64-Bit Server VM (build 25.171-b11, mixed mode)
```

Beachten Sie auch die folgenden Punkte:

- Wenn Sie im manuellen Modus arbeiten und eine andere Java-Version installieren, behält das Alternativen-System sowohl die Links als auch den generischen Namen unverändert bei.
- Wenn Sie im automatischen Modus arbeiten und eine andere Java-Version installieren, ändert das Alternativen-System den Java-Master-Link und alle Slave-Links (siehe *Abschnitt 22.4, „Anzeigen von Details zu spezifischen Alternativen“*). Prüfen Sie die Master-Slave-Beziehungen mit dem folgenden Befehl:

  ```
  > sudo update-alternatives --display java
  ```

22.6 Installieren von benutzerdefinierten Alternativen

In diesem Abschnitt erfahren Sie, wie Sie benutzerdefinierte Alternativen in einem System einrichten.

Warnung: Keine benutzerdefinierten Alternativen für python3

Installieren Sie keine benutzerdefinierten Alternativen für python3. **`/usr/bin/python3`** hat keine Update-Alternativen und verweist immer auf bestimmte getestete Versionen. Das Erstellen einer benutzerdefinierten python3-Alternative, die auf eine andere Version verweist – z. B. python 3.11 – beschädigt abhängige Systemwerkzeuge.

Für das Beispiel gelten die folgenden Annahmen:

- Es gibt zwei Skripte – **`foo-2`** und **`foo-3`** – mit ähnlicher Funktionalität.
- Die Skripte sind im Verzeichnis `/usr/local/bin` gespeichert, sodass keine Konflikte mit den Systemwerkzeugen unter `/usr/bin` entstehen.
- Der Master-Link **`foo`** verweist entweder auf **`foo-2`** oder auf **`foo-3`**.

So richten Sie Alternativen im System ein:

1. Kopieren Sie die Skripte in das Verzeichnis `/usr/local/bin`.
2. Machen Sie die Skripte ausführbar:

```
> sudo chmod +x /usr/local/bin/foo-{2,3}
```

3. Führen Sie **`update-alternatives`** für beide Skripte aus:

```
> sudo update-alternatives --install \
   /usr/local/bin/foo ❶\
   foo ❷\
   /usr/local/bin/foo-2 ❸\
   200 ❹
> sudo update-alternatives --install \
   /usr/local/bin/foo ❶\
   foo ❷\
   /usr/local/bin/foo-3 ❸\
   300 ❹
```

   Die Optionen nach `--install` bedeuten:

   ❶ Generischer Name. Zur Bedeutung: Dies ist in der Regel der Skriptname ohne Versionsnummern.

   ❷ Name des Master-Links. Muss identisch sein.

❸ Der Pfad zu den ursprünglichen Skripten in `/usr/local/bin`.

❹ Die Priorität. **`foo-2`** erhält eine niedrigere Priorität als **`foo-3`**. Die Prioritäten sollten nach Möglichkeit deutlich unterschiedliche Zahlen erhalten. Beispiel: Priorität 200 für **`foo-2`** und 300 für **`foo-3`**.

4. Prüfen Sie den Master-Link:

```
> sudo update-alternatives --display foo
foo - auto mode
  link best version is /usr/local/bin/foo-3
  link currently points to /usr/local/bin/foo-3
  link foo is /usr/local/bin/foo
/usr/local/bin/foo-2 - priority 200
/usr/local/bin/foo-3 - priority 300
```

Sobald Sie die angegebenen Schritte erledigt haben, können Sie den Master-Link **`/usr/local/bin/foo`** verwenden.

Bei Bedarf können Sie weitere Alternativen installieren. Mit dem folgenden Befehl entfernen Sie eine Alternative:

```
> sudo update-alternatives --remove foo /usr/local/bin/foo-2
```

Sobald dieses Skript entfernt wurde, sieht das Alternativen-System für die foo-Gruppe wie folgt aus:

```
> sudo update-alternatives --display foo
foo - auto mode
  link best version is /usr/local/bin/foo-3
  link currently points to /usr/local/bin/foo-3
  link foo is /usr/local/bin/foo
/usr/local/bin/foo-3 - priority 300
```

22.7 Definieren von abhängigen Alternativen

Wenn Sie mit Alternativen arbeiten, reicht das Skript allein nicht aus. Die meisten Befehle sind nicht eigenständig, sondern umfassen zusätzliche Dateien wie Erweiterungen, Konfigurationen oder man-Seiten. Mit *Slave-Alternativen* erstellen Sie Alternativen, die von einem Master-Link abhängig sind.

Angenommen, das Beispiel in *Abschnitt 22.6, „Installieren von benutzerdefinierten Alternativen“* soll mit man-Seiten und Konfigurationsdateien erweitert werden:

- Zwei Manpages – `foo-2.1.gz` und `foo-3.1.gz` –, die im Verzeichnis `/usr/local/man/man1` gespeichert sind.
- Zwei Konfigurationsdateien – `foo-2.conf` und `foo-3.conf` –, die in `/etc` gespeichert sind.

So nehmen Sie die zusätzlichen Dateien in Ihre Alternativen auf:

1. Kopieren Sie die Konfigurationsdateien in `/etc`:

```
> sudo cp foo-{2,3}.conf /etc
```

2. Kopieren Sie die man-Seiten in das Verzeichnis `/usr/local/man/man1`:

```
> sudo cp foo-{2,3}.1.gz /usr/local/man/man1/
```

3. Tragen Sie die Slave-Links mit der Option `--slave` in die Hauptskripte ein:

```
> sudo update-alternatives --install \
   /usr/local/bin/foo foo /usr/local/bin/foo-2 200 \
   --slave /usr/local/man/man1/foo.1.gz \
   foo.1.gz \
   /usr/local/man/man1/foo-2.1.gz \
   --slave /etc/foo.conf \
   foo.conf \
   /etc/foo-2.conf
> sudo update-alternatives --install \
   /usr/local/bin/foo foo /usr/local/bin/foo-3 300 \
   --slave /usr/local/man/man1/foo.1.gz \
   foo.1.gz \
   /usr/local/man/man1/foo-3.1.gz \
   --slave /etc/foo.conf \
   foo.conf \
   /etc/foo-3.conf
```

4. Prüfen Sie den Master-Link:

```
foo - auto mode
  link best version is /usr/local/bin/foo-3
  link currently points to /usr/local/bin/foo-3
  link foo is /usr/local/bin/foo
  slave foo.1.gz is /usr/local/man/man1/foo.1.gz
  slave foo.conf is /etc/foo.conf
/usr/local/bin/foo-2 - priority 200
```

```
  slave foo.1.gz: /usr/local/man/man1/foo-2.1.gz
  slave foo.conf: /etc/foo-2.conf
/usr/local/bin/foo-3 - priority 300
  slave foo.1.gz: /usr/local/man/man1/foo-3.1.gz
  slave foo.conf: /etc/foo-3.conf
```

Wenn Sie die Links mit **`update-alternatives --config foo`** in **`foo-2`**ändern, werden auch alle Slave-Links geändert.

23 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 mehrere 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 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 https://datatracker.ietf.org/.

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 23.1, „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.

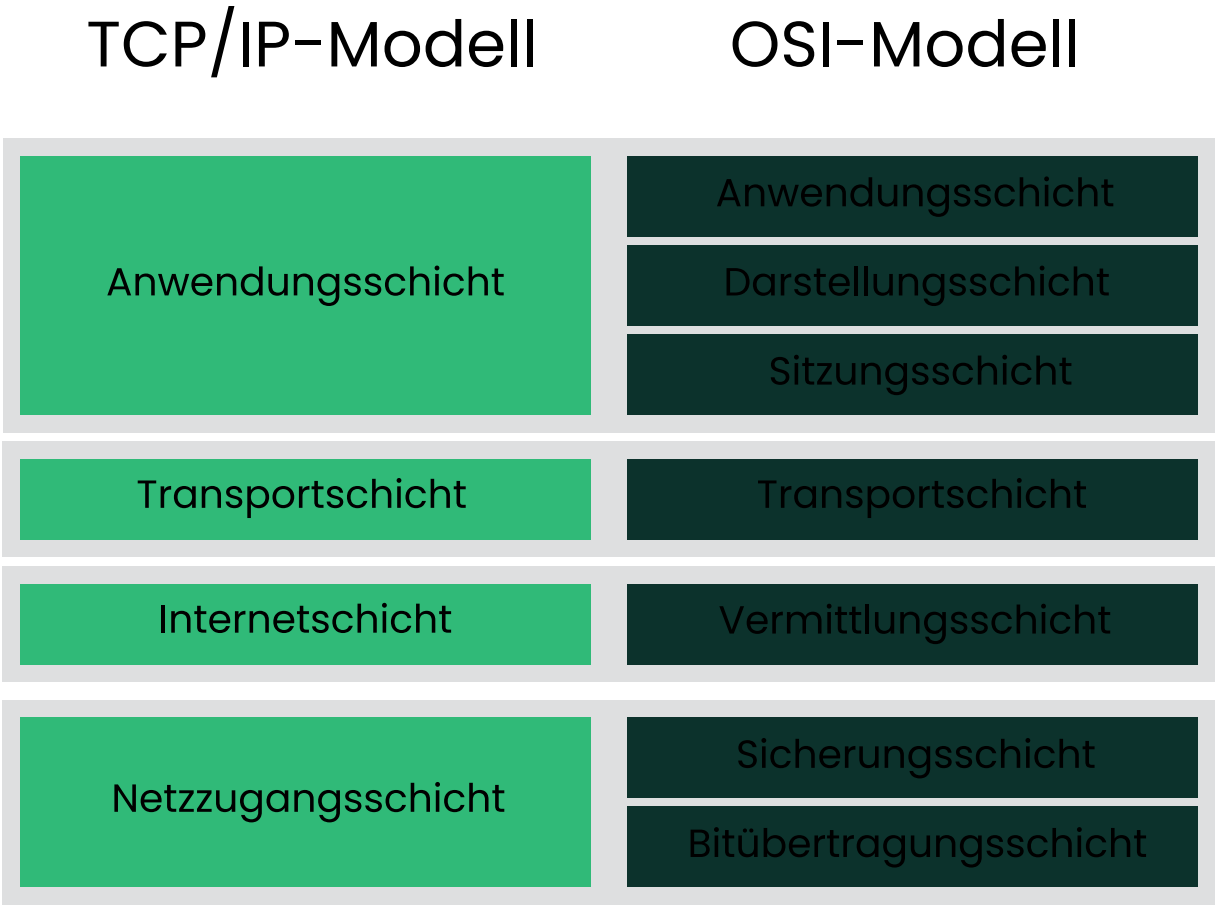


ABBILDUNG 23.1: VEREINFACHTES SCHICHTMODELL FÜR TCP/IP

Dieses Diagramm bietet für jede Schicht ein oder zwei Beispiele. Die Schichten sind nach *Abstraktionsstufen* sortiert. Die unterste Schicht ist 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 kleiner, da die Netzwerkhardware ein einschränkender Faktor sein kann. Die maximale Größe eines Datenpakets im Ethernet beträgt ca. 1500 Byte. Die Größe eines TCP/IP-Pakets ist auf diesen Wert begrenzt, wenn die Daten über 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 23.2, „TCP/IP-Ethernet-Paket“* dargestellt. Die Prüfsumme befindet sich am Ende des Pakets, nicht am Anfang. Dies erleichtert die Arbeit für die Netzwerkhardware.

ABBILDUNG 23.2: 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 bereitet die Daten zur Weitergabe an die nächste Schicht vor. 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 stellt die Daten den Anwendungen schließlich am Ziel zur Verfügung. Auf diese Weise kommuniziert eine Schicht nur mit der direkt darüber bzw. darunter liegenden Schicht. Für Anwendungen spielt es keine Rolle, ob Daten über eine drahtlose oder drahtgebundene Verbindung übertragen werden. Ähnlich spielt es für die Datenverbindung keine Rolle, welche Art von Daten übertragen wird, solange die Pakete das richtige Format haben.

23.1 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 23.2, „IPv6 – das Internet der nächsten Generation“*.

23.1.1 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 23.1, „IP-Adressen schreiben“* dargestellt geschrieben.

BEISPIEL 23.1: 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.

23.1.2 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 23.2, „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 23.2, „Verknüpfung von IP-Adressen mit der Netzmaske“* könnte das erste Netz mit 24 Bit auch als `192.168.0.0/24` geschrieben werden.

BEISPIEL 23.2: 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 auf sie kann direkt zugegriffen werden. 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 23.2, „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 Ergebnis im obigen Beispiel würde 192.168.0.255 lauten. Diese Adresse kann keinem Host zugewiesen werden.

Lokaler Host

Die Adresse `127.0.0.1` ist auf jedem Host dem „Loopback-Device“ zugewiesen. Mit dieser Adresse 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 23.1, „Private IP-Adressdomänen“* aufgelistet.

TABELLE 23.1: 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`

23.2 IPv6 – das Internet der nächsten Generation

Aufgrund der Entstehung des WWW (World Wide Web) hat das Internet in den letzten 15 Jahren ein explosives Wachstum mit einer immer größer werdenden Anzahl von Computern erfahren, die über TCP/IP kommunizieren. Seit Tim Berners-Lee bei CERN (https://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 manche IP-Adressen verloren, da sie aufgrund der Art, wie Netzwerke organisiert sind, 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. 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.

23.2.1 Vorteile

Die wichtigste und augenfälligste Verbesserung durch das IPv6-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 23.2.2, „Adresstypen und -struktur“*.

In der folgenden Liste werden andere Vorteile des IPv6-Protokolls aufgeführt:

Automatische Konfiguration

IPv6 macht das Netzwerk „Plug-and-Play“-fähig, d. h., ein neu konfiguriertes 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 Manpage `radvd.conf(5)` und im Artikel RFC 3315.

Mobilität

IPv6 ermöglicht es, einer Netzwerkschnittstelle gleichzeitig mehrere Adressen zuzuordnen. Dadurch können Benutzer problemlos auf mehrere Netzwerke zugreifen, was beispielsweise mit den von Mobilfunkunternehmen angebotenen internationalen Roaming-Diensten vergleichbar ist. Wenn Sie Ihr Mobiltelefon mit ins Ausland nehmen, meldet sich das Telefon automatisch bei dem fremden Dienst an, sobald Sie dessen Bereich betreten, sodass Sie überall unter Ihrer Rufnummer erreichbar sind und Anrufe genauso wie in Ihrem Heimatland tätigen können.

Sichere Kommunikation

Bei IPv4 ist die Netzwerksicherheit eine 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 in *Abschnitt 23.2.3, „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 unabhängig voneinander sind, sodass zwischen den beiden Protokollversionen keine Konflikte auftreten.

Bedarfsgerechte Dienste über Multicasting

Mit IPv4 müssen bestimmte 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 bestimmte vordefinierte Gruppen, mit denen beispielsweise alle Nameserver (die *Multicast-Gruppe „all name servers“*) oder alle Router (die *Multicast-Gruppe „all routers“*) angesprochen werden können.

23.2.2 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 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 23.3, „Beispiel einer IPv6-Adresse“* dargestellt, in dem alle drei Zeilen derselben Adresse entsprechen.

BEISPIEL 23.3: 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 23.4, „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 23.4: IPV6-ADRESSEN MIT ANGABE DER PRÄFIX-LÄNGE

```
fe80::10:1000:1a4/64
```

IPv6 kennt mehrere vordefinierte Präfixtypen. Einige sind unter *IPv6-Präfixe* angegeben.

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 die MAC-Adresse weltweit nur einmal vorhanden und zugleich vom Hardwarehersteller fest vorgegeben ist, vereinfacht sich die Konfiguration auf diese Weise. 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 auch, Geräten ohne MAC-Adresse (z. B. solchen, die auf dem Point-to-Point-Protokoll (PPP) basieren), 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 23.2.3, „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 spezielles Präfix (`fe80::/10`) und die Schnittstellen-ID der Netzwerkkarte aus. Der Mittelteil der Adresse besteht aus Null-Bytes. Diese Art Adresse wird von den Autokonfigurationsmethoden verwendet, um Hosts im selben Subnetz anzusprechen.

  site-local
  : Pakete mit diesem Adresstyp 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 neue Funktion: Einer Netzwerkschnittstelle werden in der Regel mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere Netzwerke über dieselbe Schnittstelle zugänglich sind. Eines dieser Netzwerke kann mit der MAC-Adresse und einem bekannten Präfix automatisch 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 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. Diese Pakete, die als Zieladresse die Care-of-Adresse tragen, können ohne Umweg über den Home-Agenten zugestellt werden.

23.2.3 Koexistenz von IPv4 und IPv6

Die Migration aller mit dem Internet verbundenen Hosts von IPv4 auf IPv6 wird nicht auf einen Schlag geschehen. Vielmehr können das alte und das neue Protokoll noch eine Weile nebeneinander 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 23.2.2, „Adresstypen und -struktur“*) sind hier die besten Lösungen.

Einzelne IPv6-Hosts im (weltweiten) IPv4-Netz tauschen ihre Daten über Tunnel aus. Beim Tunneling werden IPv6-Pakete in IPv4-Pakete verpackt, um sie über ein IPv4-Netzwerk transportieren zu können. Ein *Tunnel* ist definiert als die Verbindung zwischen zwei IPv4-Endpunkten.

Hierbei müssen die Pakete die IPv6-Zieladresse (oder das entsprechende Präfix) und die IPv4-Adresse des entfernten Hosts am Tunnelendpunkt enthalten. Einfache Tunnel können von den Administratoren zwischen ihren Netzwerken manuell und nach Absprache konfiguriert werden. Ein solches Tunneling wird *statisches Tunneling* genannt.

Trotzdem reicht manuelles Tunneling oft nicht aus, um die Menge der zum täglichen vernetzten Arbeiten nötigen Tunnel aufzubauen und zu verwalten. Aus diesem Grund wurden für IPv6 drei verschiedene Verfahren entwickelt, die das *dynamische Tunneling* erlauben:

6over4

IPv6-Pakete werden automatisch in IPv4-Pakete verpackt und über ein IPv4-Netzwerk versandt, in dem Multicasting aktiviert ist. IPv6 wird vorgespiegelt, das gesamte Netzwerk (Internet) sei ein einziges 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.

23.2.4 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 der Registerkarte *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 FRR (weitere Informationen hierzu finden Sie unter https://frrouting.org/) automatisch konfigurieren.

Weitere Informationen zum Einrichten verschiedener Tunnels mit den Dateien in `/etc/sysconfig/network` finden Sie auf der man-Seite zu `ifcfg-tunnel` (**`man ifcfg-tunnel`**).

23.2.5 Weitere Informationen

Das komplexe IPv6-Konzept wird im obigen Überblick nicht vollständig abgedeckt. Weitere ausführliche Informationen zu dem neueren Protokoll finden Sie in den folgenden Online-Dokumentationen und -Büchern:

https://pulse.internetsociety.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.

https://www.bieringer.de/linux/IPv6/

Der Beitrag „Linux IPv6 HOWTO“ und viele verwandte Links zum Thema.

RFC 2460

Die grundlegenden IPv6-Spezifikationen finden Sie unter https://www.rfc-editor.org/rfc/rfc2460.

IPv6 Essentials

Ein Buch, in dem alle wichtigen Aspekte zum Thema enthalten sind, ist *IPv6 Essentials* von Silvia Hagen (ISBN 0-596-00125-8).

23.3 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 in der Regel durch eine spezielle Software namens bind. Der Computer, der diese Umwandlung dann erledigt, nennt sich *Nameserver*. Dabei bilden die Namen wieder ein hierarchisches System, in dem die einzelnen Namensbestandteile durch Punkte getrennt sind. Die Namenshierarchie ist aber unabhängig von der oben beschriebenen Hierarchie der IP-Adressen.

Schauen wir uns einmal einen vollständigen Namen an, z. B. `jupiter.example.com`, geschrieben im Format `hostname.domain`. Ein vollständiger Name, der als *Fully Qualified Domain Name* oder kurz als FQDN bezeichnet wird, besteht aus einem Host- und einem Domänennamen (`example.com`). Ein Bestandteil des Domänennamens ist die *Top Level Domain* oder TLD (`com`).

Aus historischen Gründen ist die Zuteilung der TLDs ziemlich verwirrend. So werden in den USA traditionell dreibuchstabige TLDs verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen. Zusätzlich stehen seit 2000 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) wurden die Namen aller im Internet vertretenen Rechner in der Datei `/etc/hosts` gespeichert. 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, ähnlich wie der Nameserver, enthält also nicht die Daten aller Computer im Internet, sondern kann Anfragen an ihm nachgeschaltete, andere Nameserver weitersenden.

An der Spitze der Hierarchie befinden sich die *root-Nameserver*. Die root-Namenserver verwalten die Domänen der obersten Ebene (Top Level Domains) und werden vom Network Information Center (NIC) verwaltet. Der root-Nameserver kennt die jeweils für eine Top Level Domain zuständigen Nameserver. Weitere Informationen zu TLD-NICs finden Sie unter https://www.internic.net.

Der DNS bietet viel mehr Möglichkeiten als die bloße Namensauflösung. Der Nameserver 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.

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 zu `host.conf`.

Soll MDNS während der Installation ausgeschaltet werden, verwenden Sie `nomdns=1` als Bootparameter.

Weitere Informationen zum Multicast-DNS finden Sie unter http://www.multicastdns.org.

23.4 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 23.6, „Manuelle Netzwerkkonfiguration“*.

In SUSE Linux Enterprise Desktop mit standardmäßig aktivem NetworkManager sind alle Netzwerkkarten konfiguriert. Wenn NetworkManager nicht aktiv ist, wird nur die erste Schnittstelle mit Link-Up (einem angeschlossenen Netzwerkkabel) 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 Desktop unterstützten Netzwerkverbindungen beschrieben.

23.4.1 Konfigurieren der Netzwerkkarte mit YaST

Zur Konfiguration verkabelter oder drahtloser Netzwerkkarten in YaST wählen Sie *System* › *Netzwerkeinstellungen*. Nach Starten des Moduls zeigt YaST das Dialogfeld *Netzwerkeinstellungen* mit vier Karteireitern an: *Globale Optionen*, *Übersicht*, *Hostname/DNS* und *Routing*.

Auf dem Karteireiter *Globale Optionen* können allgemeine Netzwerkoptionen wie die Netzwerkeinrichtungsmethode, IPv6 und allgemeine DHCP-Optionen festgelegt werden. Weitere Informationen finden Sie in *Abschnitt 23.4.1.1, „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 23.4.1.3, „Konfigurieren einer unerkannten Netzwerkkarte“*. Informationen zum Ändern der Konfiguration einer bereits konfigurierten Karte finden Sie unter *Abschnitt 23.4.1.2, „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 in *Abschnitt 23.4.1.4, „Konfigurieren des Hostnamens und des DNS“*.

Der Karteireiter *Routing* wird zur Konfiguration des Routings verwendet. Weitere Informationen zu diesem Thema finden Sie in *Abschnitt 23.4.1.5, „Konfigurieren des Routings“*.

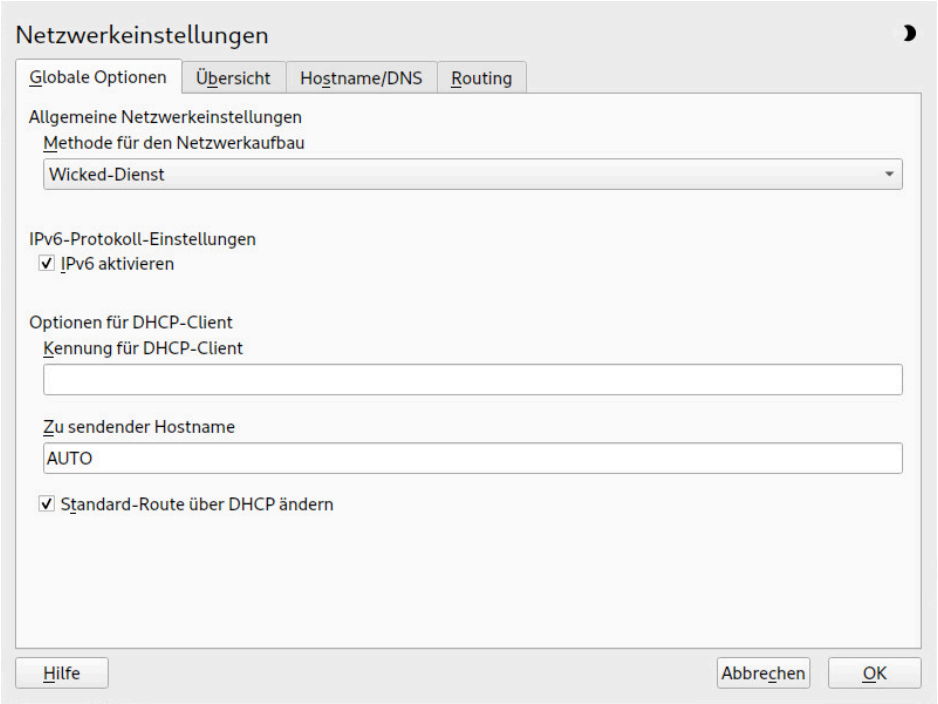


ABBILDUNG 23.3: KONFIGURIEREN DER NETZWERKEINSTELLUNGEN

23.4.1.1 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.

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 *Kapitel 31, Verwendung von NetworkManager*.

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*.

23.4.1.2 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.

23.4.1.2.1 IP-Adressen konfigurieren

Die IP-Adresse der Netzwerkkarte oder die Art der Festlegung dieser IP-Adresse kann auf der Registerkarte *Adresse* im Dialogfeld *Netzwerkkarten-Setup* 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 *Nur 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. In SUSE Linux Enterprise Desktop mit standardmäßig aktivem NetworkManager sind alle Netzwerkkarten konfiguriert.

DHCP sollten Sie auch verwenden, wenn Sie eine DSL-Leitung verwenden, Ihr ISP (Internet Service Provider) Ihnen aber keine statische IP-Adresse zugewiesen hat. Wenn Sie DHCP verwenden möchten, konfigurieren Sie dessen Einstellungen im Dialogfeld *Netzwerkeinstellungen* des YaST-Konfigurationsmoduls für Netzwerkkarten auf der Registerkarte *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 der Registerkarte *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 23.6.2.5, „`/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 Nameservern finden Sie unter *Abschnitt 23.4.1.4, „Konfigurieren des Hostnamens und des DNS“*. Informationen zur Konfiguration eines Gateways finden Sie unter *Abschnitt 23.4.1.5, „Konfigurieren des Routings“*.

23.4.1.2.2 Konfigurieren mehrerer Adressen

Ein einzelnes Netzwerkgerät kann mehrere IP-Adressen aufweisen, die als Aliasse oder Kennungen bezeichnet werden.

Anmerkung: Aliasse stellen eine Kompatibilitätsfunktion dar

Aliasse oder Kennungen können nur mit IPv4 verwendet werden. Bei **`iproute2`**-Netzwerkschnittstellen sind eine oder mehrere Adressen möglich.

So legen Sie zusätzliche Adressen für die Netzwerkkarte über YaST 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. Klicken Sie auf dem Karteireiter *Adresse* › *Zusätzliche Adressen* auf *Hinzufügen*.
3. Geben Sie die *IPv4-Adresskennung*, die *IP-Adresse* und die *Netzmaske* ein. Beachten Sie, dass IP-Aliasse mit der Netzmaske `/32` hinzugefügt werden müssen. Nehmen Sie den Schnittstellennamen nicht in den Aliasnamen auf.
4. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

23.4.1.2.3 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 *Allgemein*. 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.

23.4.1.2.4 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 `=` *`=VALUE`* ein. Wenn mehrere Optionen verwendet werden, sollten sie durch Leerzeichen getrennt sein.
4. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

23.4.1.2.5 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. Wählen Sie auf dem Karteireiter *Allgemein* den gewünschten Eintrag unter *Geräteaktivierung*.
   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 Systemstart*, allerdings fährt der Befehl **`systemctl stop network`** die Schnittstelle bei dieser Einstel-

lung 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 23.4.1.2.5, „Aktivieren des Netzwerkgeräts“* und wählen Sie unter *Geräteaktivierung* die Option *Bei NFSroot*.

23.4.1.2.6 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 auf dem Karteireiter *Allgemein* den gewünschten Eintrag aus der Liste *Set MTU* (MTU festlegen).

3. Zum Aktivieren der Konfiguration bestätigen Sie die Einstellungen.

23.4.1.2.7 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.

23.4.1.2.8 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`.

23.4.1.2.9 Konfigurieren der Firewall

Sie müssen nicht die genaue Firewall-Konfiguration durchführen, wie im *Buch „Security and Hardening Guide“, Kapitel 23 „Masquerading and firewalls“, Abschnitt 23.4 „*`firewalld`*“* beschrieben. Sie können die grundlegende Firewall-Konfiguration für Ihr Gerät als Teil der Gerätekonfiguration 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. Folgende Optionen sind verfügbar:

   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 any 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.

23.4.1.3 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 auf dem Karteireiter *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 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 INTERFACE_NAME rx on`), wird das zweite Wort der Zeichenkette durch den aktuellen Schnittstellennamen ersetzt. Andernfalls (beispielsweise bei `autoneg off speed 10`) fügt **`ifup`** am Anfang `-s INTERFACE_NAME` hinzu.

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 23.4.1.2, „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.

23.4.1.4 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* ein. Der Hostname ist global und gilt für alle eingerichteten Netzwerkschnittstellen.
   Wenn Sie zum Abrufen einer IP-Adresse DHCP verwenden, wird der Hostname Ihres Computers automatisch durch den DHCP-Server 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*.

3. Legen Sie unter *DNS-Konfiguration ändern* fest, wie die DNS-Konfiguration (Nameserver, Suchliste, Inhalt der Datei `/run/netconfig/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 `/run/netconfig/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 Liste *Domänensuche* aus. Nameserver müssen in der IP-Adresse angegeben werden (z. B. 192.168.1.116), nicht im Hostnamen. Namen, die auf dem Karteireiter *Domänensuche* angegeben werden, sind Namen zum Auflösen von Hostnamen ohne angegebene Domäne. Wenn mehr als eine *Domänensuche* 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 Befehlszeile 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 den folgenden Befehl aus:

```
# yast dns edit hostname=HOSTNAME
```

Zum Ändern der Nameserver führen Sie die folgenden Befehle 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
```

23.4.1.5 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 `- metric` *`NUMBER`* unter *Optionen* ein. Die kleinste mögliche Metrik ist 0. Die Route mit der niedrigsten Metrik hat die höchste Priorität und wird als Standard verwendet. Wenn das Netzwerkgerät getrennt wird, wird seine Route entfernt und die nächste verwendet.

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.

23.5 NetworkManager

NetworkManager ist die ideale Lösung für Notebooks und andere portable Computer. Wenn Sie viel unterwegs sind und den NetworkManager verwenden, brauchen Sie keine Gedanken mehr an die Konfiguration von Netzwerkschnittstellen und den Wechsel zwischen Netzwerken zu verschwenden.

Wichtig: Support-Abdeckung

NetworkManager wird von SUSE nur für Desktop-Arbeitslasten mit SLED oder der Arbeitsplatzrechner-Erweiterung unterstützt. Alle Serverzertifikate werden mit **`wicked`** als Netzwerkkonfigurationstool durchgeführt, und die Verwendung von NetworkManager kann diese ungültig machen. NetworkManager wird von SUSE nicht für Server-Arbeitslasten unterstützt.

23.5.1 NetworkManager und `wicked`

NetworkManager ist jedoch nicht in jedem Fall eine passende Lösung, daher können Sie immer noch zwischen der kontrollierten Methode **`wicked`** zur Verwaltung von Netzwerkverbindungen und NetworkManager wählen. Wenn Ihre Netzwerkverbindung mit NetworkManager verwaltet werden soll, aktivieren Sie NetworkManager im Netzwerkeinstellungsmodul von YaST wie in *Abschnitt 31.2, „Aktivieren oder Deaktivieren von NetworkManager“* beschrieben, und konfigurieren Sie Ihre Netzwerkverbindungen mit NetworkManager. Eine Liste der Anwendungsfälle sowie eine detaillierte Beschreibung zur Konfiguration und Verwendung von NetworkManager finden Sie in *Kapitel 31, Verwendung von NetworkManager*.

Einige Unterschiede zwischen wicked und NetworkManager sind:

`root`-Berechtigungen

Wenn Sie den NetworkManager für die Netzwerkeinrichtung verwenden, können Sie mithilfe eines Applets von Ihrer Desktop-Umgebung aus Ihre Netzwerkverbindung jederzeit auf einfache Weise wechseln, stoppen oder starten. Der NetworkManager ermöglicht zudem die Änderung und Konfiguration drahtloser Kartenverbindungen ohne `root`-Berechtigungen. Aus diesem Grund ist der NetworkManager die ideale Lösung für eine mobile Arbeitsstation.

`wicked` bietet auch einige Methoden zum Wechseln, Stoppen oder Starten der Verbindung mit oder ohne Eingreifen des Benutzers, wie zum Beispiel benutzerverwaltete Geräte. Dazu sind jedoch immer `root`-Berechtigungen erforderlich, um ein Netzwerkgerät ändern oder konfigurieren zu können. Dies stellt häufig ein Problem bei der mobilen Computernutzung dar, bei der es nicht möglich ist, alle Verbindungsmöglichkeiten vorzukonfigurieren.

Typen von Netzwerkverbindungen

Sowohl **`wicked`** als auch der NetworkManager ermöglichen Netzwerkverbindungen mit einem drahtlosen Netzwerk (mit WEP-, WPA-PSK- und WPA-Enterprise-Zugriff) und verkabelten Netzwerken mithilfe von DHCP oder der statischen Konfiguration. Diese unterstützen auch eine Verbindung über Einwahl und VPN. Mit NetworkManager können Sie auch ein Modem für mobiles Breitband (3G) anschließen oder eine DSL-Verbindung einrichten, was mit der herkömmlichen Konfiguration nicht möglich ist.

Der NetworkManager versucht, Ihren Computer fortlaufend mit der besten verfügbaren Verbindung im Netzwerk zu halten. Wurde das Netzwerkkabel versehentlich ausgesteckt, wird erneut versucht, eine Verbindung herzustellen. Der NetworkManager sucht in der Lis-

te Ihrer drahtlosen Verbindungen nach dem Netzwerk mit dem stärksten Signal und stellt automatisch eine Verbindung her. Wenn Sie dieselbe Funktionalität mit **wicked** erhalten möchten, ist ein höherer Konfigurationsaufwand erforderlich.

23.5.2 NetworkManager-Funktionalität und Konfigurationsdateien

Die mit NetworkManager erstellten individuellen Einstellungen für Netzwerkverbindungen werden in Konfigurationsprofilen gespeichert. Die mit NetworkManager oder YaST konfigurierten *System*-Verbindungen werden in `/etc/NetworkManager/system-connections/*` oder in `/etc/sysconfig/network/ifcfg-*` gespeichert. Bei GNOME sind alle benutzerdefinierten Verbindungen in GConf gespeichert.

Falls kein Profil konfiguriert wurde, erstellt NetworkManager es automatisch und nennt es `Auto $INTERFACE-NAME`. Damit versucht man, in möglichst vielen Fällen (auf sichere Weise) ohne Konfiguration zu arbeiten. Falls die automatisch erstellten Profile nicht Ihren Anforderungen entsprechen, verwenden Sie die von GNOME zur Verfügung gestellten Dialogfelder zur Konfiguration der Netzwerkverbindung, um die Profile wunschgemäß zu bearbeiten. Weitere Informationen finden Sie in *Abschnitt 31.3, „Konfigurieren von Netzwerkverbindungen“*.

23.5.3 Steuern und Sperren von NetworkManager-Funktionen

Auf zentral verwalteten Computern können bestimmte NetworkManager-Funktionen mit Polkit gesteuert oder deaktiviert werden, zum Beispiel, wenn ein Benutzer administratordefinierte Verbindungen bearbeiten oder ein Benutzer eigene Netzwerkkonfigurationen definieren darf. Starten Sie zum Anzeigen oder Ändern der entsprechenden NetworkManager-Richtlinien das grafische Werkzeug *Zugriffsberechtigungen* für Polkit. Im Baum auf der linken Seite finden Sie diese unterhalb des Eintrags *network-manager-settings*. Eine Einführung zu Polkit und detaillierte Informationen zur Verwendung finden Sie unter *Buch „Security and Hardening Guide“, Kapitel 18 „The Polkit authentication framework“*.

23.6 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.

23.6.1 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 `/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 `wickedd` 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.Network.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.

23.6.1.1 Architektur und Funktionen von `wicked`

Der `wicked`-Dienst umfasst mehrere Teile, wie in *Abbildung 23.4, „`wicked`-Architektur“* dargestellt.

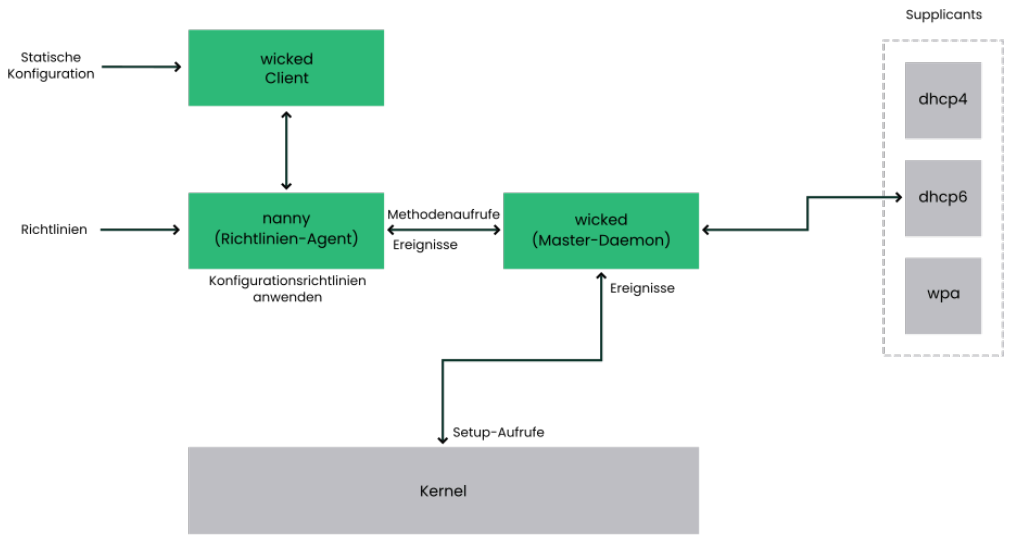


ABBILDUNG 23.4: `wicked`-ARCHITEKTUR

`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 zu diesem Thema finden Sie in *Abschnitt 23.6.1.3, „Nanny“*.
- `wicked` wurde als eine Gruppe von DBus-Diensten implementiert, die mit systemd integriert sind. Daher sind die üblichen **`systemctl`**-Befehle auch für `wicked` gültig.

23.6.1.2 Verwenden 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:

```
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-Dienste 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 **`wickedd`** (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.service`-Alias:

```
systemctl start network
```

Bei diesen Befehlen 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`**.

23.6.1.3 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 `wickedd` 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).

23.6.1.4 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 die 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.) separat aufgeführt werden müssen.

So fahren Sie mehrere Schnittstellen mit einem einzigen Befehl hoch:

```
wicked ifup bond0 br0 br1 br2
```

Oder auch alle Schnittstellen:

```
wicked ifup all
```

23.6.1.5 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 hierzu finden Sie in **`man 5 ifcfg-tunnel`**.

23.6.1.6 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.

23.6.1.7 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 einen Start- und Stopp-Befehl, 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 dem Tag `<dbus-service>` zugeordnet und definiert Befehle für die Aktionen dieser Schnittstelle. In der Deklaration können außerdem Umgebungsvariablen, die an die Aktion übergeben werden sollen, definiert und initialisiert werden.

23.6.1.8 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>
```

Wenn ein Update `wickedd` erreicht, analysieren die Systemaktualisierungsroutinen das Lease und rufen die entsprechenden Befehle (`backup`, `install` usw.) im Resolver-Skript auf. Hiermit werden wiederum die DNS-Einstellungen über **`/sbin/netconfig`** konfiguriert; als Fallback muss die Datei `/run/netconfig/resolv.conf` manuell geschrieben werden.

23.6.2 Konfigurationsdateien

Dieser Abschnitt bietet einen Überblick über die Netzwerkkonfigurationsdateien und erklärt ihren Zweck sowie das verwendete Format.

23.6.2.1 `/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 Feh-

lerbehebung 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 Dienstwickedd.serviceneu und führen Sie anschließend den folgenden Befehl aus, um alle Konfigurationen und Richtlinien anzuwenden:

```
> sudo 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.

23.6.2.2 /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 in 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.

23.6.2.3 /etc/wicked/client.xml

Die Datei /etc/wicked/client.xml wird vom Befehl **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.

23.6.2.4 `/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.

23.6.2.5 `/etc/sysconfig/network/ifcfg-*`

Diese Dateien enthalten die herkömmlichen Konfigurationsdaten für Netzwerkschnittstellen.

Anmerkung: `wicked` und die `ifcfg-*`-Dateien

`wicked` liest diese Dateien, wenn Sie das Präfix `compat:` angeben. Gemäß der Standardkonfiguration von SUSE Linux Enterprise Desktop 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 der `dhcp`- und `wireless`-Datei 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.

Informationen zur Konfiguration von `macvlan`- und `macvtab`-Schnittstellen finden Sie in den Manpages `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 23.6.2.6, „/etc/sysconfig/network/config, /etc/sysconfig/network/dhcp und /etc/sysconfig/network/wireless“*.

23.6.2.6 /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 Einstellungen für DHCP und `wireless` für WLAN-Karten. Die Variablen in allen drei Konfigurationsdateien sind kommentiert. Einige der Variablen 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 ist die die Variable `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, 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
```

23.6.2.7 `/etc/sysconfig/network/routes` und `/etc/sysconfig/network/ifroute-*`

Das statische Routing von TCP/IP-Paketen wird durch die `/etc/sysconfig/network/routes`- und `/etc/sysconfig/network/ifroute-*`-Dateien 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, für die ein separates Routing erforderlich ist, eine zusätzliche Konfigurationsdatei: `/etc/sysconfig/network/ifroute-*`. Ersetzen Sie das Platzhalterzeichen (`*`) durch den Namen der Schnittstelle. Die Einträge in der Routing-Konfigurationsdatei sehen wie folgt aus:

```
# 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, 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 23.5: 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
```

23.6.2.8 /var/run/netconfig/resolv.conf

In `/var/run/netconfig/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 23.6, „/var/run/netconfig/resolv.conf“*.

Jedoch sollte `/etc/resolv.conf` nicht manuell bearbeitet werden. Es wird vom **`netconfig`**-Skript generiert und ist ein symbolischer Link zu `/run/netconfig/resolv.conf`. 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`

Beliebige Optionen, die in `/var/run/netconfig/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 23.6: `/var/run/netconfig/resolv.conf`

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

23.6.2.9 `/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 Befehle **netconfig modify** und **netconfig remove** werden von Daemons wie DHCP oder PPP verwendet, um Einstellungen für netconfig hinzuzufügen oder zu entfernen. Nur der Befehl **netconfig update** steht dem Benutzer zur Verfügung:

modify

Der Befehl **netconfig modify** ändert die aktuelle Schnittstellen- und Dienst-spezifischen dynamischen Einstellungen und aktualisiert die Netzwerkkonfiguration. Netconfig liest Einstellungen aus der Standardeingabe oder einer Datei, die mit der Option `--lease-file` *FILENAME* 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` *INTERFACE_NAME* angegeben. Der Dienst wird durch den Parameter `-s` *SERVICE_NAME* angegeben.

remove

Der Befehl **netconfig remove** entfernt die dynamischen Einstellungen, die von einer Bearbeitungsaktion für die angegebene Schnittstellen- und Dienst-Kombination bereitgestellt wurden, und aktualisiert die Netzwerkkonfiguration. Die Schnittstelle wird durch den Parameter `-i` *INTERFACE_NAME* angegeben. Der Dienst wird durch den Parameter `-s` *SERVICE_NAME* angegeben.

update

Der Befehl **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 zu **netconfig** finden Sie unter **man 8 netconfig**.

23.6.2.10 /etc/hosts

In dieser Datei werden, wie in *Beispiel 23.7, „/etc/hosts“* gezeigt, IP-Adressen zu Hostnamen zugewiesen. Wenn kein Nameserver 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 23.7: /etc/hosts

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

23.6.2.11 /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 im *Beispiel 23.8, „/etc/networks“*.

BEISPIEL 23.8: /etc/networks

```
loopback    127.0.0.0
localnet    192.168.0.0
```

23.6.2.12 /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 23.2, „Parameter für /etc/host.conf“* aufgeführt. Ein Beispiel für `/etc/host.conf` ist in *Beispiel 23.9, „/etc/host.conf“* dargestellt.

TABELLE 23.2: 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 Nameserver 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 Nameservers, 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 23.9: `/etc/host.conf`

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

23.6.2.13 /etc/nsswitch.conf

Mit der GNU C Library 2.0 wurde *Name Service Switch* (NSS) eingeführt. Weitere Informationen hierzu finden Sie auf der Manpage 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 23.10, „/etc/nsswitch.conf“* dargestellt. Kommentaren werden #-Zeichen vorangestellt. Der Eintrag unter der `hosts`-Datenbank in diesem Beispiel bedeutet, dass Anfragen an `/etc/hosts` (`files`) über DNS gesendet werden.

BEISPIEL 23.10: /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 23.3, „Über /etc/nsswitch.conf verfügbare Datenbanken“* aufgelistet. Die Konfigurationsoptionen für NSS-Datenbanken sind in *Tabelle 23.4, „Konfigurationsoptionen für NSS-„Datenbanken““* aufgelistet.

TABELLE 23.3: ÜBER /ETC/NSSWITCH.CONF VERFÜGBARE DATENBANKEN

`aliases`	Mail-Aliasse, die von `sendmail` implementiert werden. Siehe **`man`** `5 aliases`.
`ethers`	Ethernet-Adressen

`netmasks`	Liste von Netzwerken und ihrer Teilnetzmasken. Wird nur benötigt, wenn Sie Subnetting nutzen.
`group`	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 Manpage 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 23.4: KONFIGURATIONSOPTIONEN FÜR NSS-„DATENBANKEN“

`files`	Direkter Dateizugriff, z. B. `/etc/aliases`
`db`	Zugriff über eine Datenbank
`nis`, `nisplus`	NIS, siehe auch *Buch „Security and Hardening Guide“, Kapitel 3 „Using NIS“*
`dns`	Nur bei `hosts` und `networks` als Erweiterung verwendbar
`compat`	Nur bei `passwd`, `shadow` und `group` als Erweiterung verwendbar

23.6.2.14 `/etc/nscd.conf`

Mit dieser Datei wird nscd (Name Service Cache Daemon) konfiguriert. Informationen finden Sie auf den Manpages für `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:

```
> sudo systemctl restart nscd
```

23.6.2.15 `/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.

23.6.3 Testen Sie die 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.

23.6.3.1 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. Die übliche Syntax lautet **`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 Befehl angegeben, wird der Standardbefehl verwendet (normalerweise **`list`**).

Ändern Sie den Gerätestatus mit dem Befehl:

```
> sudo ip link set DEV_NAME
```

Wenn Sie beispielsweise das Gerät eth0 deaktivieren möchten, geben Sie Folgendes ein:

```
> sudo ip link set eth0 down
```

Zur erneuten Aktivierung verwenden Sie

```
> sudo ip link set eth0 up
```

Tipp: Trennen des NIC-Geräts

Wenn Sie ein Gerät mit

```
> sudo ip link set DEV_NAME down
```

deaktivieren, wird die Netzwerkschnittstelle auf einer Softwareebene deaktiviert.

Wenn Sie simulieren möchten, dass die Verbindung getrennt wird, so als ob ein Ethernetkabel gezogen oder der Verbindungsschalter ausgeschaltet wird, führen Sie folgenden Befehl aus:

```
> sudo ip link set DEV_NAME carrier off
```

Während mit **`ip link set`** *DEV_NAME* **`down`** beispielsweise alle Routen mit *DEV_NAME* verworfen werden, ist dies bei **`ip link set DEV carrier off`** nicht der Fall. Beachten Sie, dass **`carrier off`** vom Netzwerkgerätetreiber unterstützt werden muss.

Führen Sie zur erneuten Verbindung mit dem physischen Netzwerk folgenden Befehl aus:

```
> sudo ip link set DEV_NAME carrier on
```

Nach dem Aktivieren eines Geräts können Sie es konfigurieren. Die IP-Adresse legen Sie fest mit

```
> sudo ip addr add IP_ADDRESS + dev DEV_NAME
```

Wenn Sie beispielsweise die Adresse der Schnittstelle eth0 auf 192.168.12.154/30 mit standardmäßigem Broadcast (Option `brd`) setzen möchten, geben Sie Folgendes ein:

```
> sudo ip addr add 192.168.12.154/30 brd + dev eth0
```

Damit die Verbindung funktioniert, müssen Sie außerdem das Standard-Gateway konfigurieren. Geben Sie zum Festlegen eines Gateways für Ihr System Folgendes ein:

```
> sudo ip route add default via gateway_ip_address
```

Zum Anzeigen aller Geräte verwenden Sie

```
> sudo ip link ls
```

Wenn Sie nur die aktiven Schnittstellen abrufen möchten, verwenden Sie

```
> sudo ip link ls up
```

Zum Drucken von Schnittstellenstatistiken für ein Gerät geben Sie Folgendes ein:

```
> sudo ip -s link ls DEV_NAME
```

Zum Anzeigen weiterer nützlicher Informationen, insbesondere über virtuelle Netzwerkgeräte, geben Sie Folgendes ein:

```
> sudo ip -d link ls DEV_NAME
```

Zur Anzeige der Adressen der Netzwerkschicht (IPv4, IPv6) Ihrer Geräte geben Sie Folgendes ein:

```
> sudo ip addr
```

In der Ausgabe finden Sie Informationen über die MAC-Adressen Ihrer Geräte. Wenn Sie alle Routen anzeigen möchten, wählen Sie

```
> sudo ip route show
```

Weitere Informationen zur Verwendung von **ip** erhalten Sie, indem Sie **ip** `help` eingeben oder die man-Seite **man 8 ip** aufrufen. Die Option `help` ist zudem für alle **ip**-Unterbefehle verfügbar, wie:

```
> sudo ip addr help
```

Weitere Informationen zu **ip** finden Sie in `/usr/share/doc/packages/iproute2/ip-cref.pdf`.

23.6.3.2 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 23.11, „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 z. B. einen Hostnamen oder eine IP-Adresse verwenden, beispielsweise **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 23.11: 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 der ping-Befehl die Option `-i`. Wenn beispielsweise das Ping-Intervall auf zehn Sekunden erhöht werden soll, geben Sie **`ping`** `-i 10 example.com` ein.

In einem System mit mehreren Netzwerkgeräten ist es manchmal nützlich, wenn das ping-Kommando über eine spezifische Schnittstellenadresse gesendet wird. Das legen Sie mit der `-I`-Option und dem Namen des ausgewählten Geräts fest, beispielsweise **`ping`** `-I wlan1 example.com`.

Genauere Optionen und Informationen zur Verwendung von ping erhalten Sie, indem Sie **`ping`** `-h` eingeben oder auf der Manpage für `ping (8)`.

Tipp: Ping-Ermittlung für IPv6-Adressen

Verwenden Sie für IPv6-Adressen den Befehl **`ping6`**. Hinweis: Zur Ping-Ermittlung für Link-Local-Adressen müssen Sie die Schnittstelle mit `-I` angeben. Der folgende Befehl funktioniert, wenn die Adresse über `eth1` erreichbar ist:

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

23.6.4 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 19, Der Daemon* `systemd`; weitere Informationen zu den `systemd`-Zielen finden Sie auf der Manseite für `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 in https://www.freedesktop.org/wiki/Software/systemd/NetworkTarget/.

`multi-user.target`

`multi-user.target` ist das systemd-Ziel für ein Mehrbenutzersystem mit allen erforderlichen Netzwerkdiensten.

`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.

23.7 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 der aktive Bond-Port ausfällt, wird also ein anderer Bond-Port aktiviert. Die folgenden Bonding-Modi sind verfügbar:

***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 Desktop. Bietet Fehlertoleranz.

2 (balance-xor)

Der Datenverkehr wird auf alle verfügbaren Schnittstellen aufgeteilt, je nach der Anzahl der Geräte im Bonding. 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

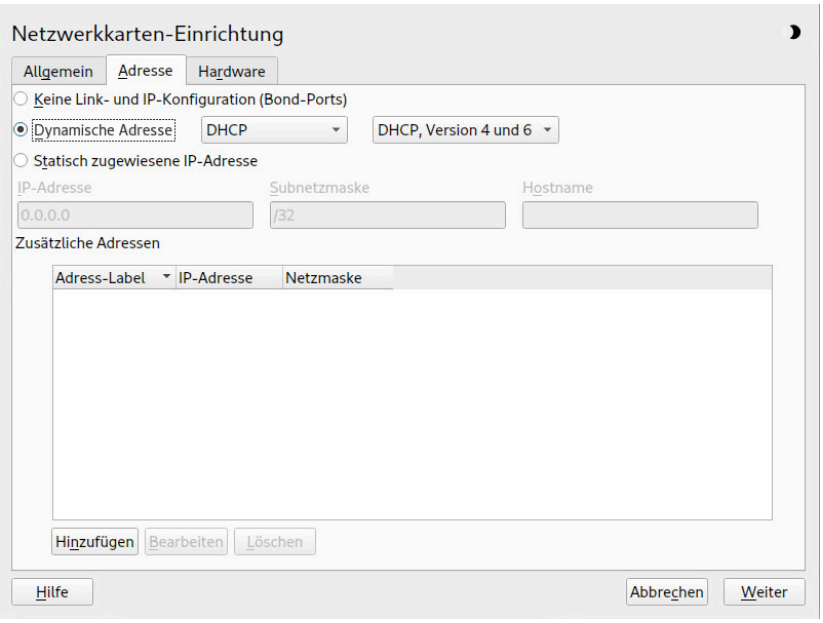
Der Einsatz von Bonding-Geräten empfiehlt sich nur für Computer, in denen mehrere physische Netzwerkkarten eingebaut sind. Bei den meisten Konstellationen sollten Sie die Bonding-Konfiguration daher lediglich in Dom0 verwenden. Die Bond-Einrichtung in einem VM-Gast-System ist dabei nur dann sinnvoll, wenn dem VM-Gast mehrere Netzwerkkarten zugewiesen sind.

Anmerkung: IBM POWER: Bonding-Modi 5 und 6 (balance-tlb / balance-alb) werden von ibmveth nicht mehr unterstützt

Es besteht ein Konflikt zwischen der tlb/alb-Bonding-Konfiguration und der Power-Firmware. Kurz gesagt, der Bonding-Treiber im tlb/alb-Modus sendet Ethernet-Loopback-Pakete mit den Ursprungs- und Ziel-MAC-Adressen, die als virtuelle Ethernet-MAC-Adressen aufgelistet sind. Diese Pakete werden von der Power-Firmware nicht unterstützt. Daher werden die Bonding-Modi 5 und 6 von ibmveth nicht mehr unterstützt.

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 der Registerkarte *Bond-Ports* 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.

23.7.1 Hot-Plugging der Bond-Ports

In bestimmten Netzwerkumgebungen (z. B. High Availability) muss eine Bond-Port-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 Bond-Ports.

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 Bond-Ports 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 Bond-Port-Schnittstelle durch das Bond-Gerät gesteuert wird.

Bei `STARTMODE=hotplug` wird die Bond-Port-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 Bond-Ports 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-Bond-Ports einsatzbereit sind, sondern es wird die Bereitschaft des gesamten Bonds abgewartet, wofür mindestens ein verfügbarer Bond-Port erforderlich ist. Wenn eine Bond-Port-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), 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 Bond-Ports um und ruft **ifup** für die Karte auf. Mit dem **ifup**-Aufruf tritt die Karte automatisch in den Bond ein.

23.7.2 Vorhersehbares Benennungsschema

Es gibt eine Einschränkung im Zusammenhang mit dem Generator für persistente Netzwerknamen und dem Bonding. Wenn einem Bond eine Schnittstelle untergeordnet ist, wird die MAC-Adresse vorübergehend überschrieben und so eingestellt, dass sie mit der MAC-Adresse der Bond-Schnittstelle übereinstimmt. Es führt zu Inkonsistenzen in der 70-persistent-net.rules-Datei, wenn die Regeln für untergeordnete Schnittstellen auf MAC-Adressen basieren.

Wenn für eine untergeordnete NIC mit einer aktualisierten MAC-Adresse ein uevent auftritt, versucht udev möglicherweise, diese mithilfe des Namens der ersten untergeordneten Schnittstelle umzubenennen, was zu einem temporären Namen wie rename4 führt. Eine Änderung am Generator für permanente Netzwerknamen zur Vermeidung MAC-basierter Regeln ist aufgrund des hohen Regressionsrisikos und der Notwendigkeit einer MAC-Filterung in bestimmten Fällen nicht möglich. Der Generator für permanente Netzwerknamen ist veraltet und wurde durch das vorhersehbare Benennungsschema ersetzt, das mehr Konfigurationsmöglichkeiten bietet und die

Abhängigkeit von MAC-Adressen vermeidet. Wir empfehlen Ihnen, das vorhersehbare Namensschema zu aktivieren, indem Sie bei einer neuen Systeminstallation `net.ifnames=1'` an die `Boot Options`-Eingabeaufforderung anhängen.

VORGEHEN 23.1: AKTIVIEREN DES BENENNUNGSSCHEMAS AUF EINEM BEREITS INSTALLIERTEN SYSTEM

1. Wenn das Paket `biosdevname` installiert ist, deinstallieren Sie es.

```
> sudo zypper rm biosdevname
```

2. Erstellen Sie eine Sicherungskopie der vorhandenen Benennungsregeln aus `/etc/udev/rules.d`, sofern vorhanden. Beispiel:

```
> sudo cp /etc/udev/rules.d/70-persistent-net.rules /backup
```

Anmerkung

Entfernen Sie die Datei `/etc/udev/rules.d/70-persistent-net.rules`, sofern vorhanden, um vorhersehbare Netzwerkschnittstellennamen zu ermöglichen.

3. Generieren Sie initrd erneut.

```
> sudo dracut -f
```

4. Starten Sie das YaST-Bootloadermodul und hängen Sie `net.ifnames=1` an die Kernel-Befehlszeile an. Bestätigen Sie mit *OK* und starten Sie das System neu.

5. Wenn das System Wicked als Netzwerkmanager verwendet, passen Sie die Konfiguration der Netzwerkschnittstellen an. Sie können das **`yast lan`**-Modul verwenden oder die Dateien unter `/etc/sysconfig/network/ifcfg-*` entsprechend umbenennen. Starten Sie Wicked dann neu.

```
> sudo systemctl restart wicked.service
```

23.8 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 finden Sie die Begriffe „Kanal-Teaming“, „Ethernet-Bonding“, „Port Truncating“ usw., die Synonyme sind und sich auf dasselbe Konzept beziehen.

Dieses Konzept ist allgemein bekannt als „Bonding“ und wurde ursprünglich in den Linux-Kernel integriert (Informationen zur ursprünglichen Implementierung finden Sie in *Abschnitt 23.7, „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 23.5, „Funktionsvergleich zwischen Bonding und Team“*.

TABELLE 23.5: 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	limited	Ja
VLAN-Unterstützung	Ja	Ja
Stapeln mehrerer Geräte	Ja	Ja
Quelle: https://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:

VORGEHEN 23.2: ALLGEMEINES VERFAHREN

1. Installieren Sie das Paket `libteam-tools`:

   ```
   > sudo zypper in libteam-tools
   ```

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 Manpages 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:

   ```
   > sudo wicked show-config
   ```

5. Starten Sie das Netzwerk-Teaming-Gerät `team0`:

   ```
   > sudo wicked ifup team0
   ```

   Falls Sie zusätzliche Informationen zum Debuggen benötigen, verwenden Sie die Option `--debug all` nach dem Unterbefehl **`all`**.

6. Überprüfen Sie den Status des Netzwerk-Teaming-Geräts. Führen Sie hierzu die folgenden Befehle aus:

   - Status der teamd-Instanz von Wicked abrufen:

     ```
     > sudo wicked ifstatus --verbose team0
     ```

   - Status der gesamten Instanz abrufen:

     ```
     > sudo teamdctl team0 state
     ```

   - systemd-Status der teamd-Instanz abrufen:

     ```
     > sudo systemctl status teamd@team0
     ```

   Jeder Befehl 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 Befehl neu:

   ```
   > sudo wicked ifreload team0
   ```

Verwenden Sie *nicht* **`systemctl`** zum Starten oder Stoppen des Teaming-Geräts! Verwenden Sie stattdessen den Befehl **`wicked`**, wie oben gezeigt.

So entfernen Sie das Teaming-Gerät vollständig:

VORGEHEN 23.3: ENTFERNEN EINES TEAMGERÄTS

1. Halten Sie das Netzwerk-Teaming-Gerät `team0` an:

   ```
   > sudo wicked ifdown team0
   ```

2. Benennen Sie die Datei `/etc/sysconfig/network/ifcfg-team0`, um in `/etc/sysconfig/network/.ifcfg-team0`. 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:

   ```
   > sudo wicked ifreload all
   ```

23.8.1 Anwendungsfall: Lastausgleich bei Netzwerk-Teaming

Der Lastausgleich erhöht die Bandbreite. Verwenden Sie die folgende Konfigurationsdatei zum Erstellen eines Netzwerk-Teaming-Geräts mit Funktionen für den Lastenausgleich. Fahren Sie mit *Prozedur 23.2, „Allgemeines Verfahren“* fort, um das Gerät einzurichten. Überprüfen Sie die Ausgabe mit **`teamdctl`**.

BEISPIEL 23.12: KONFIGURATION FÜR LASTAUSGLEICH BEI 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 `STARTMODE` auf `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 Stellt `TEAM_RUNNER` auf `loadbalance` ein und aktiviert damit den Lastausgleichsmodus.

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-Signale an einen beliebigen Host gesendet (in der Variablen `TEAM_LW_ARP_PING_TARGET_HOST` konfiguriert). Das Netzwerk-Teaming-Gerät gilt nur dann als funktionsfähig, wenn Antworten empfangen werden.

❻ Definiert die Verzögerung in Millisekunden zwischen dem Verbindungsaufbau (oder -abbau) und der Benachrichtigung des Runner.

23.8.2 Anwendungsfall: Failover bei 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 23.2, „Allgemeines Verfahren“* fort, um das Gerät einzurichten. Überprüfen Sie die Ausgabe mit **`teamdctl`**.

BEISPIEL 23.13: 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 `STARTMODE` auf `manual` fest.

❷ 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`.

❸ Stellt `TEAM_RUNNER` auf `activebackup` ein und aktiviert damit den Failover-Modus.

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-Signale an einen beliebigen Host gesendet (in der Variablen `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.

23.8.3 Anwendungsfall: VLAN zusätzlich zu 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 zusätzlich zu einem Teamgerät 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 Lastausgleich für das Teaming-Gerät vorgenommen werden, 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 Lastausgleich oder ein Failover für das Teamgerät verwendet werden soll. Richten Sie das Teamgerät gemäß den Anweisungen unter *Abschnitt 23.8.1, „Anwendungsfall: Lastausgleich bei Netzwerk-Teaming“* oder *Abschnitt 23.8.2, „Anwendungsfall: Failover bei 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. Vorzugsweise entsprechen der Dateiname und die `VLAN_ID` dem Namen `ifcfg-vlan`*`VLAN_ID`*. In diesem Fall ist `VLAN_ID` gleich `0`, sodass der Dateiname `ifcfg-vlan0` entsteht.

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:

```
# wicked ifup vlan0 vlan1
```

6. Prüfen Sie die Ausgabe von **`ifconfig`**:

```
# 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)
```

24 Druckerbetrieb

SUSE® Linux Enterprise Desktop unterstützt zahlreiche Druckermodelle (auch entfernte Netzwerkdrucker). Drucker können manuell oder mit YaST konfiguriert werden. Anleitungen zur Konfiguration finden Sie in *Kapitel 34, Einrichten eines Druckers*. Grafische Dienstprogramme und Dienstprogramme an der Befehlszeile sind verfügbar, um Druckaufträge zu starten und zu verwalten. Wenn Ihr Drucker nicht wie erwartet verwendet werden kann, lesen Sie die Informationen unter *Abschnitt 24.8, „Fehlersuche“*.

Das Standarddrucksystem in SUSE Linux Enterprise Desktop 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 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, 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 zu diesem Thema finden Sie in *Abschnitt 24.8.1, „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:

https://www.openprinting.org/printers

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 Desktop-Version nicht aufgewiesen hat. Die Datenbank gibt daher nicht notwendigerweise den richtigen Status, sondern nur eine Annäherung an diesen an.

https://www.ghostscript.com

Die Ghostscript-Website

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

Liste inbegriffener Ghostscript-Treiber.

24.1 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 Druckanwendung generierten Daten (gewöhnlich PostScript oder PDF, aber auch ASCII, JPEG usw.) in die druckerspezifischen Daten (PostScript, PCL, ESC/P usw). Die Funktionen des Druckers sind in den PPD-Dateien beschrieben. Eine PPD-Datei ent-

hält 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.

24.2 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 https://en.opensuse.org/SDB:CUPS_in_a_Nutshell.

Warnung: Ändern der Anschlüsse bei einem laufenden System

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

24.3 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 Druckeroptionen in CUPS erforderlich. Ohne eine PPD-Datei würden die Druckdaten in einem „rohen“ Zustand an den Drucker weitergeleitet werden, was 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 24.7.3, „PPD-Dateien in mehreren Paketen“* und *Abschnitt 24.8.2, „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 *Abschnitt 34.1.1, „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 Desktop. Außerdem funktionieren die Druckerbefehle unter Umständen anders und das System kann möglicherweise keine Geräte anderer Hersteller mehr adressieren. Aus diesem Grund wird das Installieren von Herstellersoftware nicht empfohlen.

24.4 Netzwerkdrucker

Ein Netzwerkdrucker kann mehrere Protokolle unterstützen. Die meisten unterstützten Protokolle sind standardisiert, und doch versuchen bestimmte Hersteller, diesen Standard abzuändern. Die Hersteller stellen dann nur noch Treiber für wenige Betriebssysteme zur Verfügung und Linux-Treiber werden selten bereitgestellt. 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 und `socket`, `LPD`, `IPP` und `smb`.

socket

Socket bezeichnet eine Verbindung, über die die einfachen Druckdaten direkt an einen TCP-Socket gesendet werden. Die am häufigsten verwendeten Socket-Ports sind `9100` oder `35`. Die Syntax der Geräte-URI (Uniform Resource Identifier) ist: socket://*`IP.OF.THE.PRINTER`*:*`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 fle-

xibel genug, um beliebige Namen als Druckerwarteschlange 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 basiert auf dem HTTP-Protokoll. 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 Druckerwarteschlange erforderlich. Die Portnummer für IPP lautet `631`. Beispiele für Geräte-URIs sind `ipp://192.168.2.202/ps` und `ipp://192.168.2.202/printers/ps`.

SMB (Windows-Freigabe)

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

Das vom Drucker unterstützte Protokoll muss vor der Konfiguration ermittelt werden. Wenn der Hersteller die erforderlichen Informationen nicht zur Verfügung stellt, können Sie das Protokoll mit dem Befehl **`nmap`** ermitteln, 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
```

24.5 Konfigurieren von CUPS mit Befehlszeilenwerkzeugen

CUPS kann mit Befehlszeilenwerkzeugen wie **`lpinfo`**, **`lpadmin`** und **`lpoptions`** konfiguriert werden. 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 den Befehl **`lpinfo -v | grep ":/"`**:

```
> sudo 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 Druckerwarteschlange hinzuzufügen:

```
> sudo lpadmin -p QUEUE -v DEVICE-URI -P PPD-FILE -E
```

Das Gerät (`-v`) ist anschließend als *QUEUE* (`-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:

```
> sudo lpadmin -p ps -v usb://ACME/FunPrinter%20XL -P \
/usr/share/cups/model/Postscript.ppd.gz -E
```

Im folgenden Beispiel wird ein Netzwerkdrucker konfiguriert:

```
> sudo 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-Seite 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 Befehlszeilenwerkzeuge wie folgt fest:

1. Zeigen Sie zunächst alle Optionen an:

   ```
   > sudo 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**:

   ```
   > sudo lpadmin -p QUEUE -o Resolution=600dpi
   ```

3. Prüfen Sie die neue Einstellung:

```
> sudo 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 `/etc/cups/lpoptions` geschrieben.

24.6 Drucken über die Befehlszeile

Um von der Befehlszeile aus zu drucken, geben Sie **lp -d***QUEUENAMEFILENAME* ein und ersetzen Sie die entsprechenden Namen durch *QUEUENAME* und *FILENAME*.

Verschiedene Anwendungen erfordern für den Druckvorgang den Befehl **lp**. Geben Sie in diesem Fall den richtigen Befehl in das Druckdialogfeld der Anwendung ohne Angabe von *FILENAME* ein, z. B. **lp -d** *QUEUENAME*.

24.7 Besondere Funktionen in SUSE Linux Enterprise Desktop

Mehrere CUPS-Funktionen wurden für SUSE Linux Enterprise Desktop angepasst. Die wichtigsten Änderungen werden im Folgenden beschrieben.

24.7.1 CUPS und Firewall

Nach einer Standardinstallation von SUSE Linux Enterprise Desktop ist `firewalld` aktiv und die Netzwerkschnittstellen werden so konfiguriert, dass sie sich in der `public`-Zone befinden, die eingehenden Datenverkehr blockiert.

Wenn `firewalld` aktiv ist, müssen Sie sie möglicherweise konfigurieren, damit Clients die Netzwerkdrucker durchsuchen können. Aktivieren Sie dazu `mdns` und `ipp` über die interne Netzwerkzone. Die öffentliche Zone sollte niemals Druckerwarteschlangen offenlegen.

(Weitere Informationen zur `firewalld`-Konfiguration finden Sie in *Buch „Security and Hardening Guide“, Kapitel 23 „Masquerading and firewalls“, Abschnitt 23.4 „*`firewalld`*“* und unter https://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings.)

24.7.1.1 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 `Internal Zone` zu konfigurieren, damit der Arbeitsplatzrechner innerhalb des Netzwerks erreichbar ist.

24.7.1.2 CUPS-Server

Wenn der CUPS-Server Teil der durch eine Firewall geschützten verbürgten Netzwerkumgebung ist, sollte die Netzwerkschnittstelle in der `Internal 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.

24.7.2 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 zu aktivieren, 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 die CUPS-Server die Netzwerkdrucker-Warteschlangen über Bonjour/DNS-SD bekannt. In diesem Fall müssen Sie zusätzlich das Paket `avahi` und den zugehörigen Dienst mit **`sudo systemctl start avahi-daemon`** auf allen Clients starten.

In *Abschnitt 24.7.1, „CUPS und Firewall“* finden Sie Informationen, wie das Durchsuchen von Druckern über `firewalld` zugelassen wird.

24.7.3 PPD-Dateien in mehreren 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 (sofern 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

24.8 Fehlersuche

In den folgenden Abschnitten werden die 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.

24.8.1 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 bestimmter 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. Bestimmte Modelle erfordern zum Umschalten eine spezielle Windows-Software. Beispielsweise kann der Windows-Druckertreiber den Drucker beim Drucken unter Windows immer wieder zurück in den GDI-Modus versetzen. Für andere GDI-Drucker sind Erweiterungsmodule für eine Standarddruckersprache erhältlich.

Verschiedene 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 mehrere 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.

24.8.2 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 (`.exe`) zur Verfügung gestellt wird, entpacken Sie sie mit **`unzip`**. Lesen Sie zunächst die Lizenzvereinbarung für die PPD-Datei. Prüfen Sie anschließend mit dem Dienstprogramm **`cupstestppd`**, ob die PPD-Datei der „Adobe PostScript-PDF-Format-Spezifikation Version 4.3“ entspricht. Wenn das Dienstprogramm „FAIL“ zurückgibt, sind die Fehler in den PPD-Dateien schwerwiegend und verursachen größere Probleme. Die von **`cupstestppd`** protokollierten Problempunkte müssen behoben werden. Fordern Sie beim Druckerhersteller ggf. eine geeignete PPD-Datei an.

24.8.3 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 *`QUEUE`* 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 24.1, „Fehlermeldung von* **lpd**“ gezeigt, wird das Problem durch den entfernten **lpd** verursacht.

BEISPIEL 24.1: 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 Befehl getestet werden, ob im Netzwerk ein CUPS-Netzwerkserver mit aktivem Broadcast vorhanden ist. Stoppen Sie unbedingt Ihren lokalen CUPS-Daemon, bevor Sie den Befehl 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 24.2, „Broadcast vom CUPS-Netzwerkserver“* dargestellt.

BEISPIEL 24.2: BROADCAST VOM CUPS-NETZWERKSERVER

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

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

```
> netcat -z HOST 631 && echo ok || echo failed
```

Wenn die Verbindung zu **cupsd** nicht hergestellt werden kann, ist **cupsd** entweder nicht aktiv oder es liegen grundlegende Netzwerkprobleme vor. **lpstat -h** *HOST* -l -t gibt einen 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 *QUEUE* auf dem *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. Weitere Informationen hierzu finden Sie in *Abschnitt 24.4, „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 eine bestimmte Zeit eingeschaltet ist. Beispiel: **nmap** *IP-address* 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** *FROM_PORT TO_PORT IP_ADDRESS*. Weitere Informationen finden Sie auf der man-Seite zu **nmap**.

Geben Sie einen Befehl ein wie

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

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

24.8.4 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.

24.8.5 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 Befehl **`cupsenable`** wieder aktivieren.

24.8.6 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 Befehl wie **`lpstat -h cups.example.com -o`**. Hierbei wird vorausgesetzt, dass der Server den Druckauftrag noch nicht erledigt, indem er ihn an den Drucker sendet. So löschen Sie den Druckauftrag anhand der abgerufenen Auftragsnummer auf dem Server:

```
> cancel -h cups.example.com QUEUE-JOBNUMBER
```

24.8.7 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 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`** *`QUEUE-JOBNUMBER`* oder **`cancel -h cups.example.com`** *`QUEUE-JOBNUMBER`*.
3. Auch wenn der Druckauftrag aus der Warteschlange gelöscht wurde, werden bestimmte Daten weiter an den Drucker gesendet. Prüfen Sie, ob ein CUPS-Backend-Prozess für die entsprechende Warteschlange ausgeführt wird und wenn ja, halten Sie ihn an.
4. Setzen Sie den Drucker zurück, indem Sie ihn eine Weile ausschalten. Legen Sie anschließend Papier ein und schalten Sie den Drucker wieder ein.

24.8.8 Fehlersuche für CUPS

Suchen Sie Probleme in CUPS mithilfe des folgenden generischen Verfahrens:

1. Legen Sie **`LogLevel debug`** in `/etc/cups/cupsd.conf` fest.
2. Stoppen **`cupsd`**.
3. Entfernen Sie `/var/log/cups/error_log*`, um das Durchsuchen 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.

24.8.9 Weitere Informationen

Ausführliche Informationen zum Drucken unter SUSE Linux Enterprise Desktop finden Sie in der openSUSE-Supportdatenbank unter https://en.opensuse.org/Portal:Printing. Lösungen zu vielen spezifischen Problemen finden Sie in der SUSE Knowledgebase (https://www.suse.com/support/). Die relevanten Themen finden Sie am schnellsten mittels einer Textsuche nach `CUPS`.

25 Über die grafische Benutzeroberfläche

SUSE Linux Enterprise Desktop umfasst den X.org-Server, Wayland und den GNOME-Desktop. In diesem Kapitel wird die Konfiguration der grafischen Benutzeroberfläche für alle Benutzer beschrieben.

25.1 X Window System

Der X.org-Server ist die allgemeine Norm für die Implementierung des X11-Protokolls. 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.

Das X Window System muss in den meisten Fällen 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.

In SUSE Linux Enterprise Desktop 15 SP7 ist Wayland als Alternative zum X.org-Server enthalten. Dies kann während der Installation ausgewählt werden.

Installieren Sie das `xorg-docs`-Paket, 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 https://www.x.org.

Die Treiber befinden sich in `xf86-video-*`-Paketen, beispielsweise `xf86-video-ati`. Viele der Treiber, die mit diesen Paketen geliefert werden, sind ausführlich in der zugehörigen man-Seite beschrieben. Wenn Sie beispielsweise den `ati`-Treiber verwenden, erhalten Sie weitere Informationen auf der man-Seite **`man 4 ati`**.

Informationen über Treiber von Drittanbietern finden Sie unter `/usr/share/doc/packages/<package_name>`. Beispielsweise ist die Dokumentation von `x11-video-nvidiaG03` nach der Installation des Pakets in `/usr/share/doc/packages/x11-video-nvidiaG04` verfügbar.

Installieren Sie das Paket `xrdp` auf einem Server und verwenden Sie die RDP-Clientsoftware, um über das Remote-Desktop-Protokoll auf den Server zuzugreifen.

25.2 Installation und Konfiguration von Schriften

Schriften in Linux lassen sich in zwei Gruppen gliedern:

Outline- 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 (https://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 (https://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 sowie andere höhere Textverarbeitung erfolgt mit Harfbuzz (https://harfbuzz.github.io/) oder Pango (https://www.pango.org/).

25.2.1 Anzeigen der installierten Schriften

Mit dem Befehl **`rpm`** oder **`fc-list`** erhalten Sie einen Überblick über die Schriften, die auf dem System installiert sind. Beide Befehle 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 der Befehl 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: Befehl **`fc-list`**

Der Befehl **`fc-list`** ist eine Erweiterung zur Fontconfig-Bibliothek. Aus Fontconfig – oder genauer gesagt, aus dem Cache – lassen sich zahlreiche interessante Informationen ermitteln. Weitere Einzelheiten finden Sie im **`man 1 fc-list`**.

25.2.2 Anzeigen von Schriften

Mit dem Befehl **ftview** (Paket ft2demos) sowie unter https://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 https://fontinfo.opensuse.org/ erfahren Sie, welche Schriftschnitte (normal, fett, kursiv etc.) und Sprachen unterstützt werden.

25.2.3 Abfragen von Schriften

Mit dem Befehl **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:

```
> 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:

```
> fc-match 'Foo Family'
DejaVuSans.ttf: "DejaVu Sans" "Book"
```

Fontconfig unterstützt *Aliasse*: 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:

```
> 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.

25.2.4 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 25.2.5.2, „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 (https://download.opensuse.org/repositories/M17N:/fonts/). Fügen Sie das Repository mit dem nachfolgenden Befehl in die Liste ein. So fügen Sie beispielsweise ein Repository für SUSE Linux Enterprise Desktop 15 SP7 hinzu:

   ```
   > sudo zypper ar
       https://download.opensuse.org/repositories/M17N:/fonts/SLE_15/
   ```

   `FONT_FAMILY_NAME` ermitteln Sie mit dem folgenden Befehl:

   ```
   > zypper se 'FONT_FAMILY_NAME*fonts'
   ```

25.2.5 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.

Mit Fontconfig können Sie den Rendering-Algorithmus für einzelne Schriften oder auch für eine Gruppe von Schriften gleichzeitig auswählen.

25.2.5.1 Konfigurieren von Schriften mit `sysconfig`

SUSE Linux Enterprise Desktop 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. Ausführliche 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

Berücksichtigen Sie `FORCE_HINTSTYLE`, `FORCE_AUTOHINT`, `FORCE_BW`, `FORCE_BW_MONOSPACE`, `USE_EMBEDDED_BITMAPS` und `EMBEDDED_BITMAP_LANGAGES`.

Präferenzliste generischer Aliasse

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

Mit den Variablen `PREFER_*_FAMILIES` können Sie Bitmap-Schriften den Vorzug geben. 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* (BCI) 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.

25.2.5.2 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. Details und andere Inspirationen finden Sie in **`man 5 fonts-conf`** oder in `/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 `~/.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 25.1, „Festlegen von Rendering-Algorithmen“*):

BEISPIEL 25.1: 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 25.2: 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 25.2, „Aliase und Ersetzungen von Familiennamen“* wird eine *priorisierte Familienliste* (PFL) erzeugt. Je nach Element werden verschiedene Aktionen ausgeführt:

`<default>` **Von** ***Regel 1***

Mit dieser Regel wird ein `serif`-Familienname *an das Ende* der PFL angehängt.

`<prefer>` **Von** ***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>` Von *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 25.1, „Erzeugen einer PFL aus Fontconfig-Regeln“* dargestellt erzeugt.

TABELLE 25.1: 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 25.2, „Ergebnisse beim Erzeugen der PFL aus Fontconfig-Regeln mit anderer Reihenfolge“*).

TABELLE 25.2: 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 in PFL, kein Ersatz
Regel 3	`Alegreya SC`	`serif` nicht in PFL, kein Ersatz

Reihenfolge	Aktuelle PFL	Hinweis
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 komplexeres Beispiel finden Sie in `/usr/share/fontconfig/conf.avail/30-metric-aliases.conf`.

Mit dem nachfolgenden Fontconfig-Snippet in *Beispiel 25.3, „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 25.3: 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 `<prefer>`-Aliasse verwendet werden.

Beispiel 25.2, „Aliase und Ersetzungen von Familiennamen“ wird durch *Beispiel 25.4, „Aliase und Ersetzungen von Familiennamen“* ergänzt.

BEISPIEL 25.4: 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 25.4, „Aliase und Ersetzungen von Familiennamen“* würde die folgende PFL-Entwicklung bewirken:

TABELLE 25.3: 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`

Reihenfolge	Aktuelle PFL
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 nach Möglichkeit `<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, `<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.

25.3 GNOME-Konfiguration für Administratoren

25.3.1 Das `dconf`-System

Die Konfiguration des GNOME-Desktops wird mit `dconf` verwaltet. Dabei handelt es sich um eine hierarchisch strukturierte Datenbank oder eine Registrierung, über die Benutzer persönliche Einstellungen bearbeiten können. Administratoren können darüber standardmäßige oder obligatorische Werte für alle Benutzer festlegen. `dconf` ersetzt das `gconf`-System von GNOME 2.

Mit **dconf-editor** werden die dconf-Optionen in einer grafischen Benutzeroberfläche angezeigt. Mit **dconf** können Sie über die Befehlszeile auf die Konfigurationsoptionen zugreifen und diese Optionen bearbeiten.

Das GNOME-Tool Tweaks bietet eine unkomplizierte Benutzeroberfläche mit zusätzlichen Konfigurationsoptionen, die über die normale GNOME-Konfiguration hinausgehen. Das Werkzeug lässt sich wahlweise über das GNOME-Anwendungsmenü oder auch über die Befehlszeile mit dem Befehl **gnome-tweak-tool** starten.

25.3.2 Systemweite Konfiguration

Globale dconf-Konfigurationsparameter können im Verzeichnis /etc/dconf/db/ festgelegt werden. Hierzu gehört beispielsweise die Konfiguration für GDM oder das Sperren bestimmter Konfigurationsoptionen für die Benutzer.

So erstellen Sie eine systemweite Konfiguration (Beispiel):

1. Erstellen Sie unter /etc/dconf/db/ ein neues Verzeichnis, das auf .d endet. Dieses Verzeichnis kann beliebig viele Textdateien mit Konfigurationsoptionen enthalten. Für dieses Beispiel erstellen Sie die Datei /etc/dconf/db/network.d/00-proxy mit dem folgenden Inhalt:

   ```
   # This is a comment
   [system/proxy/http]
   host='10.0.0.1'
   enabled=true
   ```

2. Parsen Sie die neuen Konfigurationsdirektiven in das dconf-Datenbankformat:

   ```
   > sudo dconf update
   ```

3. Tragen Sie die neue network-Konfigurationsdatenbank in das Standard-Benutzerprofil ein. Erstellen Sie hierzu die Datei /etc/dconf/profile/user. Fügen Sie dann den folgenden Inhalt ein:

   ```
   system-db:network
   ```

   Die Datei /etc/dconf/profile/user ist ein GNOME-Standard. Andere Profile können in der Umgebungsvariablen DCONF_PROFILE definiert werden.

4. Optional: Wenn die Proxy-Konfiguration für die Benutzer gesperrt werden soll, erstellen Sie die Datei `/etc/dconf/db/network/locks/proxy`. Fügen Sie dann eine Zeile mit den Schlüsseln, die nicht geändert werden dürfen, in diese Datei ein:

```
/system/proxy/http/host
/system/proxy/http/enabled
```

Mit dem grafischen **`dconf-editor`** können Sie ein Profil mit einem einzelnen Benutzer erstellen und dann mit **`dconf dump /`** eine Liste aller Konfigurationsoptionen abrufen. Die Konfigurationsoptionen können dann in einem globalen Profil gespeichert werden.

Eine ausführliche Beschreibung der globalen Konfiguration finden Sie unter https://wiki.gnome.org/Projects/dconf/SystemAdministrators.

25.3.3 Verwalten von Kachelfenstern auf Wayland

Wenn Sie den GNOME-Desktop auf Wayland ausführen und Ihre Fenster nebeneinander anordnen möchten, empfehlen wir die Verwendung der GNOME-Erweiterung *gTile*. Sie können beispielsweise sechs Terminals starten und sie in 3 Zeilen und 2 Spalten anordnen, sodass sie den gesamten Desktop-Bereich nutzen.

25.3.3.1 Installieren von „gTile“

Wichtig

Um die GNOME-Erweiterung gTile verwenden zu können, müssen Sie den GNOME-Desktop ausführen und das Paket `chrome-gnome-shell` (für SLED 15 SP4 und älter) oder `gnome-browser-connector` (für SLED 15 SP5 und neuer) installiert haben.

1. Geben Sie im Browser https://extensions.gnome.org/extension/28/gtile/ ein, um die Webseite der Erweiterung „gTile“ aufzurufen. Wenn Sie eine Warnung über eine fehlende Browsererweiterung sehen, klicken Sie auf den Link und befolgen Sie die Anweisungen Ihres Webbrowsers zum Installieren und Aktivieren der GNOME-Shell-Erweiterung.

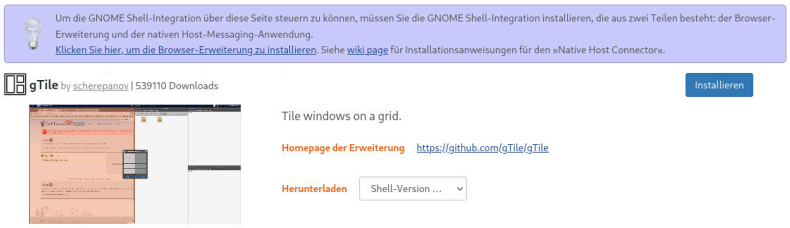


ABBILDUNG 25.1: WARNUNG ÜBER EINE FEHLENDE GNOME-SHELL-ERWEITERUNG

2. Nachdem die GNOME-Shell-Erweiterung in Ihrem Webbrowser installiert ist, sehen Sie oben rechts auf der gTile-Webseite die Schaltfläche *OFF* (AUS). Zum Aktivieren der Erweiterung „gTile“ klicken Sie auf diese Schaltfläche, damit sich der Status in *ON* (EIN) ändert.

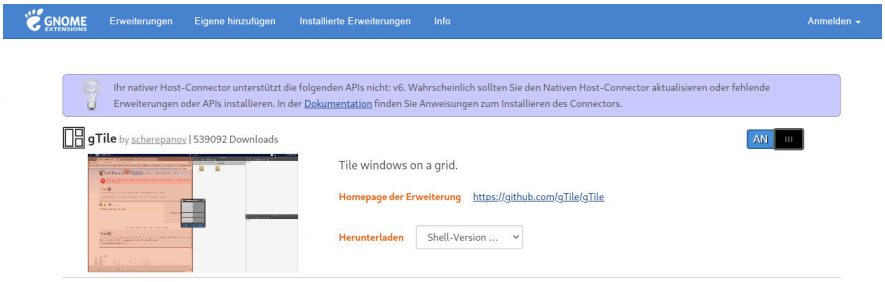


ABBILDUNG 25.2: AKTIVIERTE GNOME-ERWEITERUNG „GTILE“

3. Ein gTile-Symbol wird im GNOME-Abschnitt auf der rechten Seite der GNOME-Kontrollleiste angezeigt. Damit können Sie gTile-Fensterlayouts aktivieren.

ABBILDUNG 25.3: GTILE-KONTROLLLEISTENSYMBOL

25.3.3.2 Arbeiten mit der Erweiterung „gTile“

VORGEHEN 25.1: ANORDNEN DER FENSTER

1. Zum Öffnen von gTile für das aktuell fokussierte Fenster drücken Sie `Meta` – `Eingabetaste` .
2. Zum Festlegen der Spaltenanzahl für die Anordnung der Fenster drücken Sie eine Zahlentaste.

3. Um die Fenster automatisch entsprechend der Einstellung *Automatische Kachelgrößen im Hauptfenster* anzuordnen, drücken Sie die Taste `M`. Wenn Sie die Taste `M` zum ersten Mal drücken, wird das aktuelle Fenster standardmäßig auf der einen Hälfte des Bildschirms angezeigt und alle anderen Fenster als Kacheln in einer Spalte auf der anderen Hälfte des Bildschirms. Sie können die Taste `M` mehrmals drücken, um zwischen verschiedenen Varianten zu wechseln. Dies ist hilfreich, wenn Sie ein großes Hauptfenster und mehrere kleinere Nebenfenster nutzen möchten.

4. Um das aktuelle Fenster innerhalb der vordefinierten Kachelanordnung des Bildschirms zu verschieben, verwenden Sie die Pfeiltasten.
   Um die Anzahl der Kacheln in dem Fenster zu verkleinern oder zu vergrößern, verwenden Sie `Umschalttaste` und eine Pfeiltaste.

5. Um ein Fenster an den Rändern der benachbarten Fenster und des Desktops einzurasten, drücken Sie `Strg` – `Alt` – `S`.

6. Um das gTile-Fenster zu schließen, drücken Sie `Esc`.

VORGEHEN 25.2: ERWEITERTE KONFIGURATION

1. Um die gTile-Einstellungen zu öffnen, führen Sie folgendes Kommando aus: **`gnome-extensions-app`**.

2. Wählen Sie gTile aus und klicken Sie auf *Einstellungen*.

3. Definieren Sie eine Voreinstellung und eine Tastenkombination, um einfach zwischen häufig verwendeten Fensterlayouts zu wechseln.
   Details zur Konfiguration der Erweiterung „gTile“ finden Sie unter https://github.com/gTile/gTile.

25.3.4 Weitere Informationen

Weitere Informationen finden Sie in https://help.gnome.org/admin/.

25.4 Umschalten zwischen Intel- und NVIDIA Optimus-GPUs mit SUSE Prime

SUSE Prime ist ein Werkzeug zum Umschalten zwischen integrierten Intel-Grafikprozessoren (GPUs) und NVIDIA-GPUs, die mit der umschaltbaren Optimus-Grafiktechnologie von NVIDIA ausgestattet sind. Optimus bietet einen Mechanismus zum einfachen Umschalten zwischen einer integrierten Intel-GPU und einer diskreten NVIDIA-GPU. Dies ist für den Betrieb eines Laptops im Energiesparmodus oder mit maximaler Leistung ausgelegt: Verwenden Sie die Intel-GPU, um Energie zu sparen, und die NVIDIA-GPU für 3D-Anwendungen.

SUSE Prime ist in der SUSE Linux Enterprise Workstation-Erweiterung für SUSE Linux Enterprise 15 SP7 enthalten.

SUSE Prime ist nur auf Systemen mit X11 nutzbar, nicht auf Systemen mit Wayland. Wenn auf Ihrem System Wayland ausgeführt wird, müssen Sie es deaktivieren und auf X11 zurückgreifen, um SUSE Prime verwenden zu können (siehe *Abschnitt 25.4.1, „Voraussetzungen“*).

25.4.1 Voraussetzungen

Sie müssen über eine konfigurierte und funktionierende NVIDIA Optimus-GPU verfügen, die die in SUSE Linux Enterprise 15 SP7 enthaltenen NVIDIA-Treiber verwendet (siehe *Abschnitt 25.4.3, „Installieren von NVIDIA-Treibern“*), sowie über eine integrierte Intel-GPU. Bumblebee, das ältere Umschaltprogramm für NVIDIA Optimus, darf nicht installiert werden.

Es dürfen keine Datei `/etc/X11/xorg.conf` und keine Konfigurationsdateien mit aktiven Abschnitten `ServerLayout`, `Device` oder `Screen` im Verzeichnis `/etc/X11/xorg.conf.d` vorhanden sein.

SUSE Prime ist nur unter X11 nutzbar. Prüfen Sie mit dem Befehl **`loginctl`**, ob Ihr System X11 oder Wayland verwendet:

```
> loginctl
   SESSION        UID USER             SEAT            TTY
         2       1000 tux              seat0
> loginctl show-session 2|grep Type
Type=x11
```

Wenn Ihr System Wayland verwendet, deaktivieren Sie es, indem Sie `/etc/gdm/custom.conf` bearbeiten und die Auskommentierung für `WaylandEnable=false` aufheben. Starten Sie dann neu.

25.4.2 Installieren und Verwenden von SUSE Prime

Ihre NVIDIA-Grafikkarte sollte bereits installiert und funktionsfähig sein. Andernfalls finden Sie weitere Informationen hierzu unter *Abschnitt 25.4.3, „Installieren von NVIDIA-Treibern“*.

Installieren Sie das Paket `suse-prime`:

```
> sudo zypper install suse-prime
```

Um die GPU zu wechseln, führen Sie einen der folgenden Befehle aus, melden Sie sich dann ab und wieder an:

```
> sudo prime-select intel
> sudo prime-select intel2
> sudo prime-select nvidia
```

Verwenden Sie den **`intel`**-Treiber, wenn dies der Modesetting-Treiber ist. **`intel2`** ist für Systeme gedacht, die den `xf86-video-intel`-Treiber verwenden. Sie können diese Informationen erhalten, indem Sie sie `inxi` installieren und ausführen.

```
> inxi -G
Graphics: Device-1: Intel Xeon E3-1200 v3/4th Gen Core Processor Integrated Graphics
 Controller
          Display Server: x11(X.org 1.20.1 ) drivers: modesetting (unloaded: fbdev, vesa)
          Resolution: 1920x1080@60.00hz
          OpenGL: renderer: Mesa DRI Intel Haswell Desktop version: 4.5 Mesa 18.2.8
```

Welche GPU ist derzeit aktiv?

```
> sudo /usr/sbin/prime-select get-current
Driver configured: intel
```

25.4.3 Installieren von NVIDIA-Treibern

Wenn Sie Ihre NVIDIA-Karte identifizieren müssen, damit Sie den zu verwendenden Treiber ermitteln können, führen Sie folgenden Befehl aus:

```
> /sbin/lspci | grep VGA
```

Installieren Sie die Treiber anhand dieser Schritte mit Zypper.

Listen Sie die verfügbaren Treiberpakete auf:

```
> sudo zypper se nvidia
```

Installieren Sie dann die Treiber für Ihre NVIDIA-Grafikkarte:

```
> sudo zypper se packagename
```

26 Zugriff auf Dateisysteme mit FUSE

FUSE ist das Akronym für *File System in Userspace* (Dateisystem im Benutzerraum). 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 Plugins kann FUSE auf nahezu alle Dateisysteme wie SSH-Fernverbindungen, ISO-Images und mehr erweitert werden.

26.1 Konfigurieren von FUSE

Bevor Sie FUSE nutzen 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.

26.2 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. Das Einhängen von NTFS-Partitionen wird nur bei SUSE Linux Enterprise Server und SUSE Linux Enterprise Desktop mit SUSE Linux Enterprise Workstation Extension unterstützt.

1. Werden Sie `root`-Benutzer 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. Werden Sie alternativ ein `root`-Benutzer und führen Sie **`/sbin/fdisk -l`** aus. 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-ID (UID) und Gruppen-ID (GID) ein. Sollen die Schreibberechtigungen für einen anderen Benutzer festgelegt 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`*.

26.3 Weitere Informationen

Weitere Informationen finden Sie auf der Homepage von FUSE unter https://github.com/libfuse/libfuse.

27 Installieren von mehreren Kernel-Versionen

SUSE Linux Enterprise Desktop unterstützt die parallele Installation von mehreren Kernel-Versionen. Beim Installieren eines zweiten Kernels werden automatisch ein Boot-Eintrag und ein initrd erstellt; es sind also keine weiteren manuellen Konfigurationsschritte erforderlich. Beim Neustarten des Rechners wird der hinzugefügte Kernel als zusätzlicher Boot-Parameter angeboten.

Mithilfe dieser Funktion können Sie Kernel-Aktualisierungen zunächst auf sichere Weise testen, wobei Sie jederzeit ein Fallback auf den bisherigen (einwandfrei funktionsfähigen) Kernel vornehmen können. Verwenden Sie hierzu nicht die Aktualisierungswerkzeuge (wie YaST-Online-Update oder das Aktualisierungsmodul), sondern befolgen Sie die Anweisungen in diesem Kapitel.

Warnung: Supportberechtigung

Es ist zu beachten, dass Ihre gesamte Supportberechtigung für den Rechner erlischt, sobald Sie einen selbst kompilierten Kernel oder einen Kernel von Drittanbietern installieren. Es werden nur solche Kernels unterstützt, die zum Lieferumfang von SUSE Linux Enterprise Desktop gehören oder über die offiziellen Aktualisierungskanäle für SUSE Linux Enterprise Desktop bezogen werden.

Tipp: Prüfen der Bootloader-Konfiguration

Nach dem Installieren eines weiteren Kernels wird empfohlen, die Bootloader-Konfiguration zu prüfen und den gewünschten Standard-Booteintrag festzulegen. Weitere Informationen zu diesem Thema finden Sie in *Abschnitt 18.3, „Konfigurieren des Bootloaders mit YaST“*.

27.1 Aktivieren und Konfigurieren der Multiversions-Unterstützung

Die Unterstützung für die Installation mehrerer Versionen eines Softwarepakets (Multiversions-Unterstützung) ist bei SUSE Linux Enterprise Server 12 und neueren Versionen standardmäßig aktiviert. Diese Einstellung können Sie wie folgt überprüfen:

1. Öffnen Sie `/etc/zypp/zypp.conf` als `root` in einem Editor Ihrer Wahl.
2. Suchen Sie die Zeichenkette `multiversion`. Wenn „multiversion“ für alle Kernel-Pakete aktiviert ist, die diese Funktion unterstützen, wird folgende Zeile ohne Kommentare angezeigt:

   ```
   multiversion = provides:multiversion(kernel)
   ```

3. Soll die Multiversions-Unterstützung auf bestimmte Kernel-Varianten beschränkt werden, fügen Sie die Paketnamen in einer durch Kommas getrennten Liste an die Option `multiversion` in `/etc/zypp/zypp.conf` an, beispielsweise

   ```
   multiversion = kernel-default,kernel-default-base,kernel-source
   ```

4. Speichern Sie die Änderungen.

Warnung: Kernel-Modul-Pakete (KMP)

Stellen Sie sicher, dass die erforderlichen, vom Hersteller bereitgestellten Kernel-Module (Kernel-Modul-Pakete) auch für den neuen, aktualisierten Kernel installiert werden. Während der Aktualisierung des Kernels erhalten Sie keine Warnung zu fehlenden Kernel-Modulen, da die Paketanforderungen noch vom alten, auf dem System beibehaltenen Kernel erfüllt werden.

27.1.1 Automatisches Löschen nicht verwendeter Kernel

Wenn Sie häufig neue Kernel mit aktivierter Multiversions-Unterstützung testen, wird das Bootmenü rasch unübersichtlich. Da eine `/boot`-Partition normalerweise nur über einen begrenzten Speicherplatz verfügt, kann es zu Problemen kommen, wenn die `/boot`-Partition überläuft. Sie können die nicht verwendeten Kernel-Versionen durchaus manuell mit YaST oder Zypper

entfernen (Anweisungen siehe unten) oder auch alternativ `libzypp` so konfigurieren, dass alle nicht mehr genutzten Kernel automatisch gelöscht werden. Standardmäßig werden keine Kernel gelöscht.

1. Öffnen Sie `/etc/zypp/zypp.conf` als `root` in einem Editor Ihrer Wahl.
2. Suchen Sie die Zeichenkette `multiversion.kernels` und aktivieren Sie die Option, indem Sie die Auskommentierung der Zeile aufheben. Diese Option erfordert eine durch Komma getrennte Liste der folgenden Werte:

   `5.3.18-53.3`: Kernel mit angegebener Versionsnummer beibehalten

   `latest`: Kernel mit höchster Versionsnummer beibehalten

   `latest-N`: Kernel mit n-höchster Versionsnummer beibehalten

   `running`: Derzeit ausgeführten Kernel beibehalten

   `oldest`: Kernel mit niedrigster Versionsnummer beibehalten (also den Kernel, der aus dem ursprünglichen Lieferumfang von SUSE Linux Enterprise Desktop stammt)

   `oldest+N`. Kernel mit n-niedrigster Versionsnummer beibehalten
   Im Folgenden finden Sie einige Beispiele.

   `multiversion.kernels = latest,running`
   : Behält den jüngsten Kernel und den derzeit ausgeführten Kernel bei. Dies entspricht nahezu dem Nichtaktivieren der Multiversionsfunktion, mit der Ausnahme, dass der alte Kernel nicht direkt nach der Installation entfernt wird, sondern erst *nach dem nächsten Neubooten*.

   `multiversion.kernels = latest,latest-1,running`
   : Behält die beiden jüngsten Kernel und den derzeit ausgeführten Kernel bei.

   `multiversion.kernels = latest,running,5.3.18-53.3`
   : Behält den jüngsten Kernel, den derzeit ausgeführten Kernel und *`5.3.18-53.3`* bei.

Tipp: Derzeit ausgeführten Kernel beibehalten

Wenn Sie nicht mit einer besonderen Einrichtung arbeiten, behalten Sie den derzeit als `running` markierten Kernel bei.

> Falls Sie den derzeit ausgeführten Kernel nicht beibehalten, wird dieser Kernel bei einer Kernel-Aktualisierung gelöscht. Dies bedeutet wiederum, dass auch alle Module des derzeit ausgeführten Kernels gelöscht werden und nicht mehr geladen werden können.
>
> Wenn Sie sich entscheiden, den derzeit ausgeführten Kernel tatsächlich nicht beizubehalten, booten Sie nach einer Kernel-Aktualisierung stets unmittelbar neu, damit keine Probleme mit den Modulen auftreten.

27.1.2 Anwendungsfall: Löschen eines alten Kernels erst nach dem Neustart

Ein alter Kernel soll erst dann gelöscht werden, wenn das System fehlerfrei mit dem neuen Kernel gebootet wurde.

Ändern Sie die folgende Zeile in `/etc/zypp/zypp.conf`:

```
multiversion.kernels = latest,running
```

Die Parameter weisen das System an, den aktuellen Kernel und den ausgeführten Kernel nur dann beizubehalten, wenn sie nicht identisch sind.

27.1.3 Anwendungsfall: Beibehalten alter Kernels als Fallback

Mindestens eine Kernel-Version soll als „Ersatz“-Kernel beibehalten werden.

Dies kann von Nutzen sein, wenn Sie mehrere Kernel zu Testzwecken beibehalten möchten. Sollte ein Problem eintreten (beispielsweise weil der Computer nicht bootet), können Sie dennoch auf mindestens eine bekanntermaßen funktionsfähige Kernel-Version zurückgreifen.

Ändern Sie die folgende Zeile in `/etc/zypp/zypp.conf`:

```
multiversion.kernels = latest,latest-1,latest-2,running
```

Wenn Sie das System nach dem Installieren eines neuen Kernels neu booten, behält das System drei Kernel bei: den aktuellen Kernel (als `latest,running` konfiguriert) und die beiden unmittelbaren Vorgänger (als `latest-1` und `latest-2` konfiguriert).

27.1.4 Anwendungsfall: Beibehalten einer bestimmten Kernel-Version

Sie nehmen regelmäßige Systemaktualisierungen vor und installieren neue Kernel-Versionen. Daneben kompilieren Sie eine eigene Kernel-Version, die im System beibehalten werden soll.

Ändern Sie die folgende Zeile in `/etc/zypp/zypp.conf`:

```
multiversion.kernels = latest,5.3.18-53.3,running
```

Wenn Sie das System nach der Installation eines neuen Kernels neu booten, behält das System zwei Kernel bei: den neuen und ausgeführten Kernel (als `latest,running` konfiguriert) und den selbst kompilierten Kernel (als `5.3.18-53.3` konfiguriert).

27.2 Installieren/Entfernen von mehreren Kernel-Versionen mit YaST

Mit YaST können Sie mehrere Kernel installieren oder entfernen:

1. Starten Sie YaST, und öffnen Sie den Software-Manager mit *Software* › *Software installieren oder löschen*.
2. Wählen Sie *Ansicht* › *Package Classification (Paketklassifikation)* › *Multiversions-Pakete*. Eine Liste aller Pakete, die mehrere Versionen bieten, wird angezeigt.

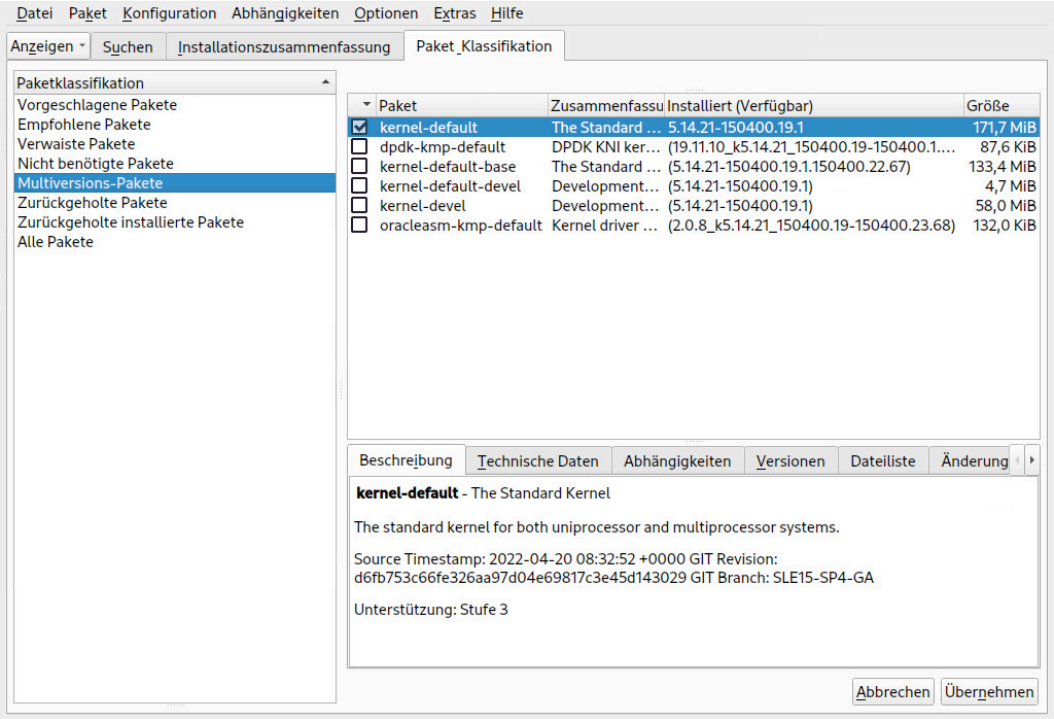


ABBILDUNG 27.1: DER YAST-SOFTWARE-MANAGER: MULTIVERSIONSANZEIGE

3. Wählen Sie ein Paket aus, und öffnen Sie den Karteireiter *Version* im unteren linken Bereich.

4. Zum Installieren eines Pakets klicken Sie auf das Kontrollkästchen neben dem Paket. Ein grünes Häkchen zeigt, dass das betreffende Paket zur Installation ausgewählt wurde.
   Soll ein bereits installiertes Paket (mit einem weißen Häkchen markiert) entfernt werden, klicken Sie auf das zugehörige Kontrollkästchen, bis ein rotes X sichtbar ist. Dies bedeutet, dass das Paket zum Entfernen ausgewählt wurde.

5. Klicken Sie auf *Übernehmen*, um mit der Installation zu beginnen.

27.3 Installieren/Entfernen von mehreren Kernel-Versionen mit Zypper

Mit **`zypper`** können Sie mehrere Kernel installieren oder entfernen:

1. Rufen Sie mit dem Befehl **`zypper se -s 'kernel*'`** eine Liste aller verfügbaren Kernel-Pakete ab:

```
S  | Name                | Type    | Version           | Arch   | Repository
```

```
---+---------------------+---------+------------------+--------
+-----------------------------------------------------
i+ | kernel-default                          | package | 6.4.0-150600.9.2              | x86_64 | SLE-
Module-Basesystem15-SP6-Pool
   | kernel-default-base                     | package | 6.4.0-150600.9.2.150600.10.40 | x86_64 | SLE-
Module-Basesystem15-SP6-Pool
   | kernel-default-devel                    | package | 6.4.0-150600.9.2              | x86_64 | SLE-
Module-Basesystem15-SP6-Pool
   | kernel-devel                            | package | 6.4.0-150600.9.2              | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-all                     | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-amdgpu                  | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-ath10k                  | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-ath11k                  | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-ath12k                  | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-atheros                 | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-bluetooth               | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-bnx2                    | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-brcm                    | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-chelsio                 | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-dpaa2                   | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-i915                    | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-intel                   | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-iwlwifi                 | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-liquidio                | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-marvell                 | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-media                   | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-mediatek                | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-mellanox                | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-mwifiex                 | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-network                 | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-nfp                     | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-nvidia                  | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
```

```
   | kernel-firmware-nvidia-gsp-G06          | package | 525.116.04-150500.1.1         | x86_64 | SLE-
Module-Basesystem15-SP6-Pool
   | kernel-firmware-nvidia-gspx-G06         | package | 550.54.14-150600.1.1          | x86_64 | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-platform                | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-prestera                | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-qcom                    | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-qlogic                  | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-radeon                  | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-realtek                 | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-serial                  | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-sound                   | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-ti                      | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-ueagle                  | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
i  | kernel-firmware-usb-network             | package | 20240201-150600.1.1           | noarch | SLE-
Module-Basesystem15-SP6-Pool
   | kernel-macros                           | package | 6.4.0-150600.9.2              | noarch | SLE-
Module-Basesystem15-SP6-Pool
```

2. Geben Sie beim Installieren die genaue Version an:

```
> sudo zypper in kernel-default-6.4.0-150600.9.2
```

3. Wenn Sie einen Kernel deinstallieren, verwenden Sie den Befehl **`zypper se -si 'kernel*'`**, um alle installierten Kernel aufzulisten, und den Befehl **`zypper rm`** *PACKAGENAME-VERSION*, um das Paket zu entfernen.

28 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.

28.1 Auflisten der geladenen Module mit lsmod und modinfo

Der Befehl **`lsmod`** zeigt die derzeit geladenen Kernelmodule. Dieser Befehl liefert beispielsweise die folgende Ausgabe:

```
> 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 `Module` enthält den Namen der geladenen Module, die Spalte `Size` entsprechend die Größe der einzelnen Module. Aus der Spalte `Used by` gehen die Anzahl und der Name der verweisenden Module hervor. Diese Liste ist möglicherweise unvollständig.

Ausführliche Informationen zu einem bestimmten Kernelmodul erhalten Sie mit dem Befehl **`modinfo`** *`MODULE_NAME`*, wobei *`MODULE_NAME`* für den Namen des gewünschten Kernelmoduls steht. Die **`modinfo`**-Binärdatei befindet sich im Verzeichnis `/sbin`, das nicht in der PATH-Umgebungsvariablen des Benutzers enthalten ist. Wenn Sie den Befehl **`modinfo`** als normaler Benutzer ausführen, müssen Sie daher den vollständigen Pfad zur Binärdatei angeben:

```
> /sbin/modinfo kvm
filename:       /lib/modules/6.4.0-150700.38-default/kernel/arch/x86/kvm/kvm.ko.zst
license:        GPL
author:         Qumranet
```

```
suserelease:    SLE15-SP7
srcversion:     9DACE73AC65F98D556DAD60
depends:        irqbypass
supported:      yes
retpoline:      Y
intree:         Y
name:           kvm
vermagic:       6.4.0-150700.38-default SMP mod_unload modversions
```

28.2 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 Sperrlisten.

Wenn Sie keine Parameter angeben, wird mit dem Befehl `modprobe` ein angegebenes Kernelmodul installiert. `modprobe` muss mit root-Berechtigungen ausgeführt werden:

```
> sudo modprobe acpi
```

Zum Entfernen eines Kernelmoduls geben Sie den Parameter `-r` an:

```
> sudo modprobe -r acpi
```

28.2.1 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` aufweisen. 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.

28.2.2 Eintragen von Kernelmodulen in Sperrlisten mit modprobe

Wenn ein Kernelmodul in eine Sperrliste 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 Sperrliste stehen, dennoch manuell laden.

Soll ein Modul in eine Sperrliste eingetragen werden, erstellen Sie eine Datei mit dem Namen `/etc/modprobe.d/60-blacklist-`*`MODULE_NAME`*`.conf` und dem folgenden Inhalt:

```
blacklist MODULE_NAME
```

Führen Sie den Befehl **`dracut`** als root-Benutzer aus, um ein neues `initrd`-Image zu generieren, und starten Sie dann Ihren Computer neu (ersetzen Sie *`NAME`* durch den Namen der aktuellen initrd und *`KERNELVERSION`* durch den aktuell ausgeführten Kernel):

```
> su
echo "blacklist nouveau" >> /etc/modprobe.d/60-blacklist-nouveau.conf
/usr/bin/dracut --logfile /var/log/YaST2/mkinitrd.log --force /boot/$initrd-NAME
 $KERNELVERSION
reboot
```

Soll ein Kernel-Modul nur vorübergehend deaktiviert werden, tragen Sie es direkt beim Booten in die Sperrliste 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=*MODULE_NAME*** 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.

Um ein Kernelmodul über GRUB dauerhaft auf die Sperrliste zu setzen, öffnen Sie die Datei `/etc/default/grub` zur Bearbeitung und fügen Sie dem Befehl **GRUB_CMDLINE_LINUX** die Option **modprobe.blacklist=*MODULE_NAME*** hinzu. Führen Sie dann den Befehl **sudo grub2-mkconfig -o /boot/grub2/grub.cfg** aus, damit die Änderungen in Kraft treten.

29 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. Benutzer eines bestimmten Geräts müssen über sämtliche erkannten Statusänderungen des entsprechenden Geräts informiert werden. `udev` bietet die erforderliche Infrastruktur, um die Geräteknotendateien und symbolische Links im `/dev`-Verzeichnis dynamisch zu warten. Mithilfe von `udev`-Regeln können externe Werkzeuge in die Ereignisverarbeitung des Kernel-Geräts eingebunden werden. Auf diese Weise können Sie die `udev`-Gerätebehandlung anpassen, 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.

29.1 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 wider. 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 befinden sich in `/usr/lib/tmpfiles.d/` und `/etc/tmpfiles.d/`. Weitere Informationen finden Sie auf der Manpage für `systemd-tmpfiles(8)`.

29.2 uevents und udev des Kernels

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 udev uevent, um über die Änderung zu informieren. Der Daemon udev liest und analysiert beim Starten alle Regeln aus den /usr/lib/udev/rules.d/*.rules- und /etc/udev/rules.d/*.rules-Dateien und behält sie im Speicher bei. 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 29.6, „Einflussnahme auf die Behandlung von Geräteereignissen durch den Kernel und 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.

29.3 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. Diese IDs bestehen 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.

29.4 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.

29.5 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 Daemons kann mit **`udevadm control --log_priority=`***`LEVEL/NUMBER`* geändert werden.

29.6 Einflussnahme auf die Behandlung von Geräteereignissen durch den Kernel und 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. Ereignis-

se werden mit allen Regeln abgeglichen, die in den Verzeichnissen `/usr/lib/udev/rules.d/` (für Standardregeln) und `/etc/udev/rules.d` (systemspezifische Konfiguration) bereitgestellt werden.

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 Manpage für `udev` beschrieben. Nachfolgend finden Sie einige Beispielregeln, die Sie in die grundlegende Regelsyntax von `udev` einführen. Sämtliche Beispielregeln stammen aus dem `udev`-Standardregelsatz `/usr/lib/udev/rules.d/50-udev-default.rules`.

BEISPIEL 29.1: 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 `console`-Regel besteht aus drei Schlüsseln: einer Übereinstimmungsschlüssel (`KERNEL`) und zwei Zuweisungsschlüssel (`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 Schemas, die die Schemas *, ? und [] abgleichen.
- udev-Regeln unterstützen Ersetzungen.

29.6.1 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.

29.6.2 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 für `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.

29.6.3 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{`*`FILENAME`*`}`
: `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{`*`FILENAME`*`}`
: Weist `udev` an, den Gerätepfad aufwärts nach einem Gerät mit übereinstimmenden `sysfs`-Attributwerten zu durchsuchen.

`ENV{KEY}`

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.

29.6.4 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{KEY}`

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{KEY}`

Weist `udev` an, eine Umgebungsvariable zu exportieren. Wenn der Operator `==` verwendet wird, überprüft dieser Schlüssel, ob der Wert einer Umgebungsvariablen mit dem angegebenen Wert übereinstimmt.

`RUN`

Weist `udev` an, der Liste der für dieses Gerät auszuführenden Programme ein Programm hinzuzufügen. Sie sollten hier nur 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 vom Schlüssel `GOTO` angegebene Bezeichnung enthält.

`IMPORT{TYPE}`

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. `WAIT_FOR_SYSFS="ioerr_cnt"` weist `udev` beispielsweise an, zu warten, bis die Datei `ioerr_cnt` erstellt wurde.

`OPTIONS`

Der Schlüssel `OPTION` kann mehrere Werte haben:

- `last_rule` weist `udev` an, alle nachfolgenden Regeln zu ignorieren.
- `ignore_device` weist `udev` an, dieses Ereignis 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.

29.7 Dauerhafte Benennung von Geräten

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
```

29.8 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 Manpage für `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 dürfen Sie 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/` **und** `/etc/tmpfiles.d/`

Verantwortlich für statische `/dev`-Inhalte.

29.9 Weitere 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 `udevz` u kontrollieren, Kernel-Ereignisse abzurufen, die Ereigniswarteschlange zu verwalten und einfache Methoden zur Fehlersuche bereitzustellen.

`udevd`

Informationen zum `udev`-Ereignisverwaltungs-Daemon.

30 Spezielle Systemfunktionen

In diesem Kapitel erhalten Sie zunächst Informationen zu den speziellen 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).

30.1 Informationen zu speziellen Softwarepaketen

Das folgende Kapitel enthält grundlegende Informationen zu den folgenden Werkzeugen: `bash`, `cron`, `logrotate`, `locate`, `ulimit` und `free`.

30.1.1 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.

30.1.2 Das cron-Paket

Mit `cron` lassen Sie automatisch Befehle im Hintergrund zu bestimmten Zeitpunkten 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 30.1, „Eintrag in /etc/crontab“*, wird `root` eingegeben. Die paketspezifischen Tabellen in `/etc/cron.d` weisen alle dasselbe Format auf. Siehe die man-Seite zu **`cron`** (**`man cron`**).

BEISPIEL 30.1: 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.

Mehrere Pakete installieren Shell-Skripte in den Verzeichnissen `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly`, deren Ausführung durch `/usr/lib/cron/run-crons` gesteuert wird. `/usr/lib/cron/run-crons` wird alle 15 Minuten von der Haupttabelle (`/etc/crontab`) ausgeführt. Hiermit wird gewährleistet, dass vernachlässigte Prozesse zum richtigen Zeitpunkt ausgeführt werden können.

Um die Skripte `hourly`, `daily` oder andere Skripte für regelmäßige Wartungsarbeiten zu benutzerdefinierten Zeiten auszuführen, entfernen Sie regelmäßig die Zeitstempeldateien mit `/etc/crontab`-Einträgen (siehe *Beispiel 30.2, „/etc/crontab: Entfernen der Zeitstempeldateien“*. Dadurch wird `hourly` vor jeder vollen Stunde und `daily` einmal täglich um 2:14 Uhr entfernt usw.).

BEISPIEL 30.2: /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.

30.1.3 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.

30.1.4 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. Diese 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 „System log files“, Abschnitt 3.3 „Managing log files with* **`logrotate`**“.

30.1.5 Das Kommando `locate`

`locate`, ein Befehl 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 bzw. etwa 15 Minuten nach dem Booten des Systems gestartet.

30.1.6 Das Kommando `ulimit`

Mit dem Befehl **`ulimit`** (*user limits*) können Grenzwerte für die Verwendung der Systemressourcen festgelegt und angezeigt werden. **`ulimit`** ist insbesondere für die Begrenzung des für Anwendungen verfügbaren Speichers hilfreich. 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 30.1, „`ulimit`: Einstellen von Ressourcen für Benutzer“* aufgeführten Optionen.

TABELLE 30.1: **`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 einem Systemupgrade überschrieben werden. Mit `/etc/profile.local` können Sie die systemweiten Profileinstellungen anpassen. Benutzerspezifische Einstellungen sind unter `~USER/.profile` vorzunehmen.

BEISPIEL 30.3: **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 hierzu finden Sie in **man bash**.

Wichtig: **ulimit** Support

ulimit-Direktiven werden nicht von allen Shells unterstützt. PAM (z. B. `pam_limits`) bietet umfassende Anpassungsfunktionen als Alternative zu **ulimit**.

30.1.7 Das Kommando **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`.

30.1.8 Manpages 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 Infoseiten zu erhalten, auf denen Sie detailliertere Anweisungen erhalten. Die Infoseiten befinden sich im Hypertextsystem von GNU. Eine Einführung in dieses System erhalten Sie, wenn Sie **`info`** `info` eingeben. Infoseiten können mit Emacs angezeigt werden, indem 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.

30.1.9 Auswählen von man-Seiten über den Befehl **`man`**

Geben Sie **`man`** *`MAN_PAGE`* ein, um die 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.

30.1.10 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 finden Sie unter https://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`. Um das Programm anzupassen, kopieren Sie `.gnu-emacs` (mit **`cp /etc/skel/.gnu-emacs ~/.gnu-emacs`**) in das Home-Verzeichnis und nehmen dort die gewünschten Einstellungen vor.

`.gnu-emacs` legt die Datei `~/.gnu-emacs-custom` als `custom-file` fest. Wenn Benutzer in Emacs Einstellungen mit den `customize`-Optionen vornehmen, werden die Einstellungen in `~/.gnu-emacs-custom` gespeichert.

Bei SUSE Linux Enterprise Desktop 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 befinden sich auch in `/usr/share/emacs/site-lisp` und beginnen immer mit `suse-start-`. Der lokale Systemadministrator kann systemweite Einstellungen in `default.el` festlegen.

Weitere Informationen zu diesen Dateien finden Sie in der Info-Datei zu Emacs unter *Init File*: `info:/emacs/InitFile`. Informationen zum Deaktivieren des Ladens dieser Dateien (sofern erforderlich) stehen dort ebenfalls zur Verfügung.

Die Komponenten von Emacs sind in mehrere Pakete unterteilt:

- Das Basispaket `emacs`.
- `emacs-x11` (in der Regel installiert): das Programm *mit* X11-Unterstützung.
- `emacs-nox`: das Programm *ohne* X11-Unterstützung.
- `emacs-info`: Onlinedokumentation im Info-Format.
- `emacs-el`: Die nicht kompilierten Bibliotheksdateien in Emacs Lisp. Sie sind während der Laufzeit nicht erforderlich.
- Falls erforderlich, können mehrere Zusatzpakete installiert werden: `emacs-auctex` (LaTeX), `psgml` (SGML und XML), `gnuserv` (Client- und Serverbetrieb) und andere.

30.2 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.

30.3 Tastaturbelegung

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 möglich mit der X-Tastaturerweiterung (XKB)

Tipp: Weitere Informationen

Informationen zu XKB finden Sie in den Dokumenten, die unter `/usr/share/doc/packages/xkeyboard-config` (Teil des Pakets `xkeyboard-config`) aufgelistet sind.

30.4 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`**).

LISTE DER VARIABLEN

`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`

Diese Variable kann auf `yes` oder `ctype` (Standardwert) festgelegt werden. Wenn sie auf `yes` festgelegt ist, verwendet `root` Spracheinstellungen und länderspezifische Einstellungen. Andernfalls arbeitet der Systemadministrator immer in einer 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>]]
```

30.4.1 Systemweite Locale-Einstellungen

`systemd` liest `/etc/locale.conf` im frühen Bootvorgang aus. Die in dieser Datei konfigurierten Locale-Einstellungen werden von jedem Service oder Benutzer übernommen, falls keine individuellen Einstellungen vorgenommen wurden.

Anmerkung: Verhalten älterer Konfigurationsdateien unter SUSE Linux Enterprise DesktopSUSE Linux Enterprise Desktop

Frühere Versionen von SUSE Linux Enterprise Desktop lesen Gebietsschemaeinstellungen aus `/etc/sysconfig/language`, `/etc/sysconfig/keyboard` und `/etc/sysconfig/console`. Ab SUSE Linux Enterprise Server 15 GA gelten diese Dateien als veraltet. `systemd` liest aus diesen Dateien keine Einstellungen mehr. `systemd` liest stattdessen `/etc/locale.conf`.

Variablen, die in `/etc/sysconfig/language` definiert sind, werden jedoch weiterhin verwendet: Sie überschreiben das systemweite Gebietsschema und können verwendet werden, um verschiedene Gebietsschemaeinstellungen für Benutzer-Shells zu definieren (siehe *Abschnitt 30.4.2, „Einige Beispiele“*).

Zum Festlegen der systemweiten Locale gehen Sie folgendermaßen vor:

- Schreiben Sie die Einstellungen in `/etc/locale.conf`. Jede Zeile ist eine umgebungsartige Variablenzuweisung (eine Liste von Variablen finden Sie in **`man 5 locale.conf`**):

  ```
  LANG=de_DE.UTF-8
  ```

  Zur Feinabstimmung der Einstellungen können Sie weitere Variablen hinzufügen, jeweils eine Variable pro Zeile.

- Verwenden Sie den Befehl **`localectl`**:

  ```
  # localectl set-locale LANG=de_DE.UTF-8
  ```

  Auch hier können Sie nach dem Befehl **`localectl set-locale`** weitere Variablen angeben.

Zum Zweck der Rückwärtskompatibilität mit älteren Systemen bei der Aktualisierung des systemd-Pakets werden alle genannten Variablen von sysconfig zu den endgültigen Zielen migriert, falls sie dort nicht bereits definiert sind.

30.4.2 Einige Beispiele

Sprach- und Ländercode sollten immer gleichzeitig eingestellt werden. Die Spracheinstellungen entsprechen der Norm ISO 639, die unter https://www.evertype.com/standards/iso639/iso639-en.html und https://www.loc.gov/standards/iso639-2/ verfügbar ist. Die Ländercodes sind in ISO 3166 aufgeführt (siehe https://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 die tcsh: Bei der Anmeldung liest `/etc/csh.login` die Datei `/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.

30.4.3 Locale-Einstellungen in ~/.i18n

Wenn Sie mit den Locale-Systemstandardwerten nicht zufrieden sind, können Sie die Einstellungen in ~/.i18n ändern. Achten Sie dabei jedoch auf die Einhaltung der Bash-Scripting-Syntax. Die Einträge in ~/.i18n setzen die Systemstandardwerte aus /etc/sysconfig/language außer Kraft. Verwenden Sie dieselben Variablennamen, jedoch ohne die RC_-Namespace-Präfixe. Nutzen Sie beispielsweise LANG anstatt RC_LANG:

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

30.4.4 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 LANG auf en_US festlegen und die Meldungsdatei in /usr/share/locale/en_US/LC_MESSAGES nicht vorhanden ist, erfolgt ein Fallback auf /usr/share/locale/en/LC_MESSAGES.

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"

Bei Norwegisch wird auch LC_TIME anders behandelt.

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.

30.4.5 Weitere Informationen

- *The GNU C Library Reference Manual*, Kapitel „Locales and Internationalization“. Es befindet sich im Paket `glibc-info`.
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, momentan verfügbar unter https://www.cl.cam.ac.uk/~mgk25/unicode.html.

31 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.

Wichtig: Support-Abdeckung

NetworkManager wird von SUSE nur für Desktop-Arbeitslasten mit SLED oder der Arbeitsplatzrechner-Erweiterung unterstützt. Alle Serverzertifikate werden mit **`wicked`** als Netzwerkkonfigurationstool durchgeführt, und die Verwendung von NetworkManager kann diese ungültig machen. NetworkManager wird von SUSE nicht für Server-Arbeitslasten unterstützt.

31.1 Anwendungsfälle 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.

31.2 Aktivieren oder Deaktivieren von NetworkManager

Auf Desktop- und Notebook-Computern ist NetworkManager standardmäßig aktiviert. Sie können es jederzeit über das Modul „Netzwerkeinstellungen“ in YaST deaktivieren und aktivieren.

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 31.3, „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 externen IP-Adresse ein.
    Eine ausführliche Beschreibung der Netzwerkkonfiguration mit YaST finden Sie in *Abschnitt 23.4, „Konfigurieren von Netzwerkverbindungen mit YaST“*.

31.3 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 bestimmte Verbindungen nicht konfigurieren. In einer abgesicherten Umgebung sind möglicherweise bestimmte Optionen gesperrt oder erfordern eine `root`-Berechtigung. Erfragen Sie Einzelheiten bei Ihrem Systemadministrator.

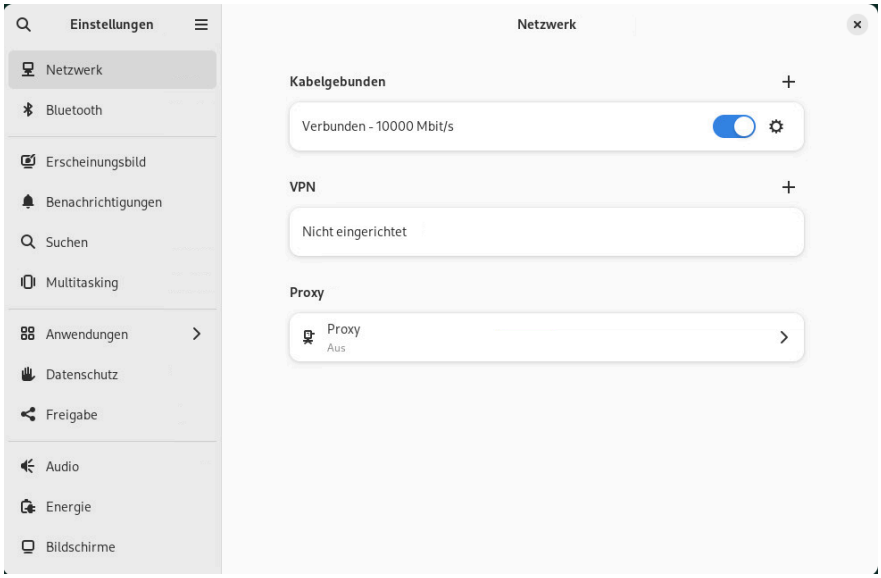


ABBILDUNG 31.1: DIALOGFELD „NETZWERKVERBINDUNGEN“ IN GNOME

VORGEHEN 31.1: HINZUFÜGEN UND BEARBEITEN VON VERBINDUNGEN

1. Öffnen Sie das Statusmenü, klicken Sie auf das Zahnradsymbol, um *Einstellungen* zu öffnen, und klicken Sie im linken Menü auf *Netzwerk*.

2. So fügen Sie eine Verbindung hinzu:

    a. Klicken Sie auf das Symbol + neben der Registerkarte mit dem Verbindungstyp, den Sie hinzufügen möchten.

    b. Füllen Sie je nach Verbindungstyp die erforderlichen Felder im entsprechenden Dialogfeld aus.

    c. Wenn Sie fertig sind, klicken Sie auf *Hinzufügen*.

    d. Nach Bestätigen der Änderungen wird die neu konfigurierte Netzwerkverbindung in der Liste der verfügbaren Netzwerke im Statusmenü angezeigt.

3. So bearbeiten Sie eine Verbindung:

    a. Klicken Sie auf der rechten Seite der Registerkarte mit dem Verbindungstyp, den Sie bearbeiten möchten, auf das Zahnradsymbol.

    b. Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf *Anwenden*, um diese zu speichern.

    c. Wenn die Verbindung als Systemverbindung zur Verfügung stehen soll, wechseln Sie zur Registerkarte *Details* und aktivieren Sie dort das Kontrollkästchen *Anderen Benutzern zur Verfügung stellen*. Weitere Informationen zu Benutzer- und Systemverbindungen finden Sie unter *Abschnitt 31.4.1, „Benutzer- und Systemverbindungen“*.

31.3.1 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 es auszuschalten, oder klicken Sie auf den entsprechenden Pfeil nach rechts, um die Verbindungsdetails zu ändern.

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*.

31.3.2 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.

VORGEHEN 31.2: 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.

VORGEHEN 31.3: 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 ausgewählt wurde, wird so lange wie möglich aufrecht erhalten. Wenn dabei ein Netzwerkkabel angeschlossen ist, werden alle Verbindungen, für die *Stay connected when possible* (Wenn möglich, verbunden bleiben) festgelegt wurde, hergestellt, während die drahtlose Verbindung bestehen bleibt.

31.3.3 Aktivieren der Captive Portal-Erkennung beim Wireless-Betrieb

Bei der erstmaligen Verbindung zwingen viele öffentliche Wireless-Hotspots die Benutzer, eine Landeseite (das *Captive Portal*) zu besuchen. Vor Ihrer Anmeldung oder Zustimmung zu den Bestimmungen und Bedingungen werden alle Ihre HTTP-Anforderungen an das Captive Portal des Anbieters umgeleitet.

Wenn Sie sich mit einem drahtlosen Netzwerk verbinden, das über ein Captive Portal verfügt, blenden NetworkManager und GNOME als Teil des Verbindungsvorgangs automatisch die Anmeldeseite ein. So wissen Sie stets, wann Sie verbunden sind, und Sie können schnellstmöglich loslegen, ohne den Browser für die Anmeldung verwenden zu müssen.

Um diese Funktion zu aktivieren, installieren Sie das Paket `NetworkManager-branding-SLE` und starten Sie NetworkManager neu mit:

```
> sudo systemctl restart network
```

Sobald Sie sich mit einem Netzwerk verbinden, das über ein Captive Portal verfügt, öffnet NetworkManager (oder GNOME) die Captive Portal-Anmeldeseite für Sie. Melden Sie sich mit Ihren Berechtigungsnachweisen an, um Zugang zum Internet zu erhalten.

31.3.4 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.

31.3.5 NetworkManager und VPN

NetworkManager unterstützt verschiedene Technologien für virtuelle private Netzwerke (VPN). Für jede Technologie bietet SUSE Linux Enterprise Desktop 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`

OpenConnect

Installieren Sie zur Verwendung dieser VPN-Technik:

- `NetworkManager-openconnect`
- `NetworkManager-openconnect-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.

VORGEHEN 31.4: 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 für *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
Benutzername	Der Benutzer (nur verfügbar, wenn Sie *Password with Certificates (TLS)* ausgewählt haben)
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`
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*.

31.4 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 Verbindungen 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.

31.4.1 Benutzer- und Systemverbindungen

NetworkManager kennt zwei Verbindungsarten: `user`- und `system`-Verbindungen.

Für Benutzerverbindungen müssen alle Benutzer im NetworkManager authentifiziert werden. Darin werden die Berechtigungsnachweise der Benutzer in deren lokalen GNOME-Schlüsselbunden gespeichert. Benutzer müssen sie daher nicht mehr erneut eingeben, wenn sie sich verbinden.

Systemverbindungen sind automatisch für alle Benutzer verfügbar. Der erste Benutzer, der die Verbindung herstellt, gibt die erforderliche Berechtigung ein. Danach haben alle anderen Benutzer Zugriff, ohne die Berechtigung kennen zu müssen. Die Konfiguration einer Benutzerverbindung unterscheidet sich von der Konfiguration einer Systemverbindung nur durch ein Kontrollkästchen: *Anderen Benutzern zur Verfügung stellen*. Informationen zum Konfigurieren von Benutzer- oder Systemverbindungen mit NetworkManager finden Sie unter *Abschnitt 31.3, „Konfigurieren von Netzwerkverbindungen“*.

31.4.2 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.

31.4.3 Firewall-Zonen

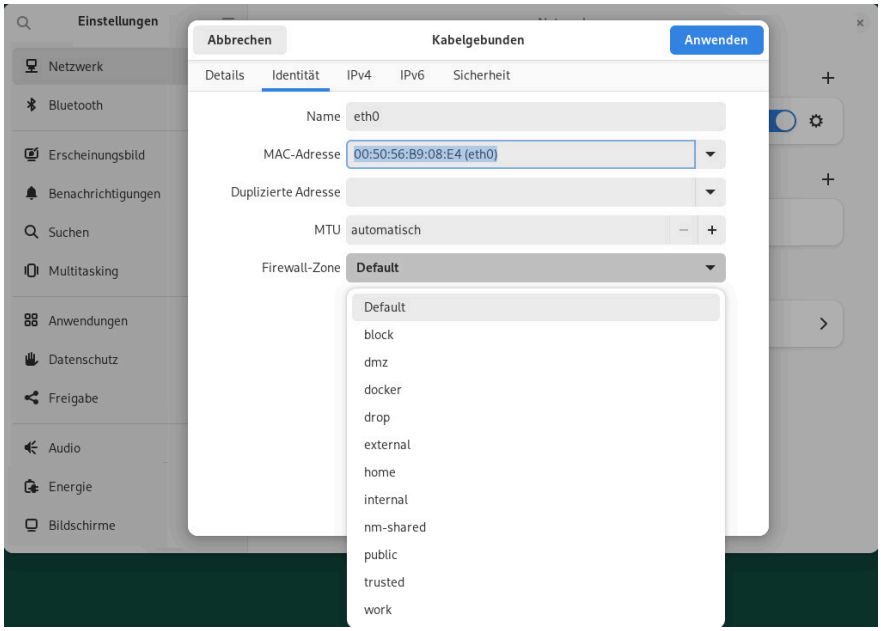


ABBILDUNG 31.2: `firewalld`-ZONEN IN NETWORKMANAGER

Die Firewall-Zonen legen allgemeine Regeln zu den zulässigen Netzwerkverbindungen fest. Zum Konfigurieren der *firewalld*-Zone für eine verkabelte Verbindung öffnen Sie die Registerkarte *Identität* der Verbindungseinstellungen. Zum Konfigurieren der *firewalld*-Zone für eine WLAN-Verbindung öffnen Sie die Registerkarte *Sicherheit* der Verbindungseinstellungen.

Wenn Sie sich in Ihrem Heimatnetz befinden, verwenden Sie die Zone `home`. Bei öffentlichen kabellosen Netzwerken wechseln Sie zu `public`. Wenn Sie sich in einer sicheren Umgebung befinden und alle Verbindungen zulassen möchten, verwenden Sie die Zone `trusted`.

Details zu firewalld finden Sie im *Buch „Security and Hardening Guide“, Kapitel 23 „Masquerading and firewalls“, Abschnitt 23.4 „`firewalld`“.*

31.5 Häufig gestellte Fragen

Nachfolgend finden Sie verschiedene häufig gestellte Fragen zum Konfigurieren spezieller Netzwerkoptionen mit NetworkManager.

5. *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 Befehlszeilenwerkzeugen 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.

6. *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 für die Konfiguration von Netzwerkverbindungen wie in *Abschnitt 31.3, „Konfigurieren von Netzwerkverbindungen“* beschrieben. Wählen Sie die drahtlose Verbindung, die Sie ändern möchten, und klicken Sie auf *Bearbeiten*. Geben Sie auf der Registerkarte *Drahtlos* die BSSID ein.

7. *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 für die Konfiguration von Netzwerkverbindungen wie in *Abschnitt 31.3, „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 in der Dropdownliste *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 DHCP-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* aus. Wechseln Sie zur Kategorie *Erlaubte Dienste*. Wenn *DHCP-Server* nicht bereits als *Erlaubter Dienst* angezeigt ist, wählen Sie *DHCP-Server* aus unter *Services to Allow* (Erlaubte Dienste) und klicken Sie auf *Hinzufügen*. Bestätigen Sie Ihre Änderungen in YaST.

8. *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 für die Konfiguration von Netzwerkverbindungen wie in *Abschnitt 31.3, „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.

9. *Wie kann NetworkManager dazu veranlasst werden, eine Verbindung zu passwortgeschützten Netzwerken aufzubauen, bevor sich ein Benutzer anmeldet?*

   Definieren Sie eine `system connection`, die für solche Zwecke verwendet werden kann. Weitere Informationen hierzu finden Sie in *Abschnitt 31.4.1, „Benutzer- und Systemverbindungen“*.

31.6 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 31.2, „Aktivieren oder Deaktivieren von NetworkManager“*). Überprüfen Sie dann, ob das NetworkManager-gnome-Paket installiert ist.

Wenn das Desktop-Miniprogramm installiert ist, aber nicht ausgeführt wird, starten Sie es manuell über den Befehl **`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 in *Abschnitt 31.3.5, „NetworkManager und VPN“*.

Keine Netzwerkverbindung verfügbar

Wenn Sie Ihre Netzwerkverbindung ordnungsgemäß konfiguriert haben und alle anderen Komponenten für die Netzwerkverbindung (Router usw.) ebenfalls funktionieren, hilft es manchmal, die Netzwerkschnittstellen auf Ihrem Computer neu zu starten. Melden Sie sich dazu bei einer Befehlszeile als `root` an und führen Sie einen **`systemctl restart wickeds`** aus.

31.7 Weitere Informationen

Weitere Informationen zu NetworkManager finden Sie auf den folgenden Websites und in folgenden Verzeichnissen:

Projektseite des NetworkManagers

https://gitlab.freedesktop.org/NetworkManager/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/`.

IV Hardwarekonfiguration

32 Einrichten der Systemtastaturbelegung 497

33 Einrichten von Soundkarten 498

34 Einrichten eines Druckers 502

35 Einrichten eines Scanners 509

36 Energieverwaltung 511

37 Permanenter Speicher 518

32 Einrichten der Systemtastaturbelegung

Mit dem YaST-Modul *Systemtastaturbelegung* definieren Sie die Standard-Tastaturbelegung für das System (auch für die Konsole verwendet). Die Benutzer können die Tastaturbelegung in den jeweiligen X-Sitzungen mithilfe der Desktop-Werkzeuge bearbeiten.

1. Öffnen Sie das YaST-Dialogfeld *Konfiguration der Systemtastatur*. Klicken Sie hierzu in YaST auf *Hardware* › *Systemtastaturbelegung*. Alternativ starten Sie das Modul von der Befehlszeile aus mit dem Befehl **`sudo yast2 keyboard`**.
2. Wählen Sie die gewünschte *Tastaturbelegung* aus der Liste aus.
3. Im Textfeld *Test* können Sie die ausgewählte Tastaturbelegung ausprobieren.
4. Wenn das Ergebnis Ihren Vorstellungen entspricht, bestätigen Sie Ihre Änderungen, und schließen Sie das Dialogfeld.
5. Das Ergebnis wird in den Dateien von Typ `/etc/vconsole.conf` (für Textkonsolen) und `/etc/X11/xorg.conf.d/00-keyboard.conf` (für X11) gespeichert.
6. Erweiterte Tastatureinstellungen werden unter *System* › *Sysconfig Editor* › *Hardware* › *Tastatur* konfiguriert. Hier können Sie den Tastatursatz und die Verzögerungseinstellungen angeben und Num-, Feststell- und Rollen-Taste aktivieren oder deaktivieren. Diese Einstellungen werden in `/etc/sysconfig/keyboard` gespeichert.

33 Einrichten von Soundkarten

YaST erkennt die meisten Soundkarten automatisch und konfiguriert sie mit den entsprechenden Werten. Wenn die Standardeinstellungen geändert werden sollen oder wenn eine Soundkarte eingerichtet werden soll, die nicht automatisch konfiguriert werden kann, verwenden Sie das YaST-Soundmodul. Damit können Sie auch weitere Soundkarten einrichten oder deren Reihenfolge ändern.

Warnung

Wenn Sie nicht alle Details zur Einrichtung Ihres Soundsystems kennen, ändern Sie die Einstellungen nicht manuell. Lassen Sie sie stattdessen von Ihrem Sound-Subsystem – PipeWire oder PulseAudio – für Sie konfigurieren. Verwenden Sie eine dedizierte Desktop-Anwendung, um zwischen Audiogeräten zu wechseln. Verwenden Sie als Fallback die grafische Anwendung **`pavucontrol`**.

Starten Sie YaST, um das Soundmodul zu starten, und klicken Sie auf *Hardware* › *Sound*. Starten Sie alternativ das Dialogfeld *Soundkonfiguration* direkt, indem Sie **`yast2 sound &`** als `root`-Benutzer von einer Befehlszeile aus ausführen. Wenn das Audiomodul nicht verfügbar ist, müssen Sie es mit dem Befehl **`sudo zypper install yast2-sound`** installieren.

VORGEHEN 33.1: KONFIGURIEREN VON SOUNDKARTEN

Wenn Sie eine neue Soundkarte hinzugefügt haben oder wenn YaST eine vorhandene Soundkarte nicht automatisch konfigurieren konnte, dann führen Sie die folgenden Schritte aus. Für die Konfiguration einer neuen Soundkarte müssen Sie den Hersteller und das Modell Ihrer Soundkarte kennen. Wenn Sie sich nicht sicher sind, finden Sie die erforderlichen Informationen in der Dokumentation zu Ihrer Soundkarte. Eine Referenzliste der von ALSA unterstützten Soundkarten mit ihren zugehörigen Soundmodulen finden Sie unter https://www.alsa-project.org/main/index.php/Matrix:Main.

Bei der Konfiguration können Sie zwischen den folgenden Einrichtungsoptionen wählen:

Schnelles automatisches Setup

Sie müssen keine der weiteren Konfigurationsschritte ausführen – die Soundkarte wird automatisch konfiguriert. Sie können die Lautstärke oder zu ändernde Optionen später festlegen.

Normales Setup

Ermöglicht Ihnen die Anpassung der Ausgabelautstärke und das Abspielen eines Testsounds bei der Konfiguration.

Erweitertes Setup mit der Möglichkeit, Optionen zu ändern

Nur für Experten. Ermöglicht Ihnen die Anpassung aller Parameter der Soundkarte.

Wichtig: Erweiterte Konfiguration

Wählen Sie diese Option nur, wenn Sie genau wissen, was Sie tun. Lassen Sie die Parameter andernfalls unverändert und verwenden Sie die normalen oder automatischen Setup-Optionen.

1. Starten Sie das YaST-Soundmodul.
2. Wählen Sie für die Konfiguration einer erkannten, aber *nicht konfigurierten* Soundkarte den entsprechenden Eintrag in der Liste aus und klicken Sie auf *Bearbeiten*.
   Klicken Sie für die Konfiguration einer neuen Soundkarte auf *Hinzufügen*. Wählen Sie den Anbieter und das Modell Ihrer Soundkarte aus und klicken Sie auf *Weiter*.
3. Wählen Sie eine der Einrichtungsoptionen aus und klicken Sie auf *Weiter*.
4. Wenn Sie *Normales Setup* gewählt haben, können Sie Ihre Soundkonfiguration nun *Testen* und die Lautstärke anpassen. Sie sollten bei ungefähr 10 Prozent Lautstärke beginnen, um Hörschäden und eine Beschädigung der Lautsprecher zu vermeiden.
5. Wenn Sie alle Optionen nach Ihren Wünschen festgelegt haben, klicken Sie auf *Weiter*.
   Im Dialogfeld *Soundkonfiguration* wird die neu konfigurierte oder bearbeitete Soundkarte angezeigt.
6. Zum Entfernen einer nicht mehr benötigten Soundkarten-Konfiguration wählen Sie den entsprechenden Eintrag aus und klicken Sie auf *Löschen*.
7. Klicken Sie auf *OK*, um die Änderungen zu speichern und das YaST-Soundmodul zu verlassen.

VORGEHEN 33.2: BEARBEITEN VON SOUNDKARTEN-KONFIGURATIONEN

1. Wählen Sie zum Ändern der Konfiguration einer einzelnen Soundkarte (nur durch Experten!) den Soundkarteneintrag im Dialogfeld *Soundkonfiguration* aus und klicken Sie auf *Bearbeiten*.

Dadurch gelangen Sie zu *Erweiterte Optionen für die Soundkarte*, wo Sie eine Reihe von Parametern feinabstimmen können. Weitere Informationen erhalten Sie durch Klicken auf *Hilfe*.

2. Wählen Sie zum Anpassen der Lautstärke einer bereits konfigurierten Soundkarte oder zum Testen der Soundkarte den entsprechenden Soundkarteneintrag im Dialogfeld *Soundkonfiguration* aus und klicken Sie auf *Weitere*. Wählen Sie den entsprechenden Menüeintrag aus.

   ### Anmerkung: YaST-Mixer

   Die YaST-Mixer-Einstellungen bieten nur grundlegende Optionen. Sie dienen zur Fehlerbehebung (wenn z. B. kein Textsound hörbar ist). Greifen Sie über *Weitere* › *Lautstärke* auf die YaST-Mixereinstellungen zu. Nutzen Sie für den täglichen Einsatz und die Feineinstellung der Soundoptionen das Mixer-Applet Ihres Desktops oder das Befehlszeilenwerkzeug **`alsasound`**.

3. Wählen Sie zur Wiedergabe von MIDI-Dateien die Optionen *Weitere* › *Sequenzer starten* aus.

4. Wenn eine unterstützte Soundkarte erkannt wird, können Sie SoundFonts für die Wiedergabe von MIDI-Dateien installieren:

   a. Legen Sie die Original-Treiber-CD-ROM in Ihr CD- oder DVD-Laufwerk ein.

   b. Wählen Sie *Weitere* › *Soundfonts installieren* aus, um SF2 SoundFonts™ auf Ihre Festplatte zu kopieren. Die SoundFonts werden im Verzeichnis `/usr/share/sfbank/creative/` gespeichert.

5. Wenn Sie in Ihrem System mehr als eine Soundkarte konfiguriert haben, können Sie die Reihenfolge Ihrer Soundkarten konfigurieren. Um eine Soundkarte als primäres Gerät festzulegen, wählen Sie die betreffende Soundkarte unter *Soundkonfiguration* aus und klicken Sie auf *Weitere* › *Als primäre Karte festlegen*. Das Audiogerät mit Index `0` ist das Standardgerät, das vom System und den Anwendungen verwendet wird.

6. Standardmäßig wird in SUSE Linux Enterprise Desktop das PulseAudio-Soundsystem genutzt. Dies ist eine Abstraktionsschicht, die Ihnen hilft, mehrere Audiostreams zu mischen, indem alle eventuell vorhandenen Hardwarerestriktionen umgangen werden. Klicken Sie zum Aktivieren oder Deaktivieren des PulseAudio-Soundsystems auf *Weitere* › *PulseAudio-Konfiguration*. Wenn diese Option aktiviert ist, wird der PulseAudio-Daemon zur Audiowiedergabe verwendet. Deaktivieren Sie die *PulseAudio-Unterstützung*, wenn Sie systemweit eine andere Option verwenden möchten.

Die Lautstärke und die Konfiguration aller installierten Soundkarten werden gespeichert, wenn Sie auf *OK* klicken und das YaST-Soundmodul verlassen. Die Mixereinstellungen werden in der Datei `/etc/asound.state` gespeichert. Die ALSA-Konfigurationsdaten werden an das Ende der Datei `/etc/modprobe.d/sound` angehängt und in `/etc/sysconfig/sound` geschrieben.

34 Einrichten eines Druckers

YaST kann zum Konfigurieren von lokalen Druckern und Netzwerkdruckern verwendet werden. Weitere Informationen zum Drucken (allgemeine Informationen, technische Details und Fehlerbehebung) finden Sie unter *Kapitel 24, Druckerbetrieb*.

Klicken Sie in YaST auf *Hardware* › *Drucker*, um das Druckermodul zu starten. Es wird standardmäßig in der Ansicht *Druckerkonfigurationen* geöffnet, die eine Liste aller verfügbaren und konfigurierten Drucker enthält. Diese Ansicht ist besonders dann nützlich, wenn Ihnen im Netzwerk sehr viele Drucker zur Verfügung stehen. Aus dieser Ansicht können Sie auch eine *Testseite drucken* und Drucker konfigurieren.

Anmerkung: Starten von CUPS

Damit Sie den an Ihr Gerät angeschlossenen Drucker verwenden können, muss CUPS auf Ihrem System installiert sein und ausgeführt werden. Wenn CUPS nicht ausgeführt wird, werden Sie aufgefordert, es zu starten. Falls CUPS beim Booten nicht gestartet wird, werden Sie außerdem aufgefordert, es zu aktivieren (empfohlen).

34.1 Konfigurieren von Druckern

Normalerweise werden USB-Drucker automatisch erkannt. Ist dies nicht der Fall, überprüfen Sie, ob der Drucker eingeschaltet und mit dem Gerät verbunden ist.

Die Konfiguration eines Druckers erfolgt in drei Schritten: Geben Sie die Verbindungsart ein, wählen Sie einen Treiber und nennen Sie die Druckwarteschlange für diese Einrichtung.

Für viele Druckermodelle sind mehrere Treiber verfügbar. Bei der Konfiguration des Druckers wählt YaST standardmäßig die mit `recommended` markierten aus. In der Regel muss der Treiber nicht geändert werden. Wenn jedoch ein Farbdrucker beispielsweise nur Schwarzweiß drucken soll, können Sie einen Treiber verwenden, der keinen Farbdruck unterstützt. Wenn bei der Grafikausgabe mit einem PostScript-Drucker Leistungsprobleme auftreten, wechseln Sie probeweise von einem PostScript-Treiber zu einem PCL-Treiber (vorausgesetzt Ihr Drucker unterstützt PCL).

Wenn in der Liste kein Treiber für Ihren Drucker aufgeführt ist, versuchen Sie, einen generischen Treiber mit der passenden Standardsprache auszuwählen. Welche Sprache (Befehlssatz, durch den der Drucker gesteuert wird) Ihr Drucker unterstützt, erfahren Sie in der Dokumentation Ihres Druckers. Alternative Lösungen finden Sie unter *Abschnitt 34.1.1, „Hinzufügen von Treibern mit YaST“*.

Ein Drucker wird immer über eine Druckwarteschlange verwendet. Dadurch wird sichergestellt, dass mehrere gleichzeitig gestartete Druckaufträge in eine Warteschlange gestellt und nacheinander ausgeführt werden. Jede Druckwarteschlange ist einem bestimmten Treiber zugewiesen; ein Drucker kann zudem auch über mehrere Warteschlangen verfügen. Sie haben dadurch zum Beispiel die Möglichkeit, für einen Farbdrucker eine zweite Druckwarteschlange für reine Schwarzweißdrucke einzurichten. Weitere Informationen zu Druckerwarteschlangen erhalten Sie unter *Abschnitt 24.1, „Der CUPS-Workflow“*.

VORGEHEN 34.1: HINZUFÜGEN EINES NEUEN DRUCKERS

1. Starten Sie das YaST-Druckermodul mit *Hardware* › *Drucker*.
2. Klicken Sie im Bildschirm *Druckerkonfigurationen* auf *Hinzufügen*.
3. Wenn Ihr Drucker bereits unter `Specify the Connection` aufgeführt ist, fahren Sie mit dem nächsten Schritt fort. Versuchen Sie es andernfalls mit der Option *Weitere erkennen* oder starten Sie den *Verbindungsassistenten*.
4. Geben Sie im Textfeld unter `Find and Assign a Driver` den Namen des Anbieters und den Modellnamen ein und klicken Sie auf *Suchen nach*.
5. Wählen Sie den richtigen Treiber für den Drucker aus. Es wird empfohlen, den zuerst aufgeführten Treiber auszuwählen. Wenn kein geeigneter Treiber angezeigt wird, versuchen Sie Folgendes.
    a. Überprüfen Sie den Suchbegriff.
    b. Erweitern Sie die Suche, indem Sie auf *Mehr finden* klicken.
    c. Fügen Sie einen Treiber hinzu, wie unter *Abschnitt 34.1.1, „Hinzufügen von Treibern mit YaST“* beschrieben.
6. Geben Sie für `Default paper size` das Standardpapierformat an.
7. Geben Sie im Feld *Beliebigen Namen festlegen* einen eindeutigen Namen für die Druckerwarteschlange ein.
8. Für den Drucker sind nun die Standardeinstellungen konfiguriert; er ist damit betriebsbereit. Klicken Sie auf *OK*, um zur Ansicht *Druckerkonfigurationen* zurückzukehren. Der neu konfigurierte Drucker wird nun in der Liste der Drucker angezeigt.

34.1.1 Hinzufügen von Treibern mit YaST

Nicht alle Druckertreiber, die für SUSE Linux Enterprise Desktop verfügbar sind, werden auch standardmäßig installiert. Wenn beim Hinzufügen eines Druckers im Dialogfeld *Treiber suchen und zuweisen* kein geeigneter Treiber verfügbar ist, installieren Sie ein Treiberpaket mit Treibern für den Drucker:

VORGEHEN 34.2: INSTALLIEREN VON ZUSÄTZLICHEN TREIBERPAKETEN

1. Starten Sie das YaST-Druckermodul mit *Hardware* › *Drucker*.
2. Klicken Sie im Bildschirm *Druckerkonfigurationen* auf *Hinzufügen*.
3. Klicken Sie im Abschnitt `Find and Assign a Driver` auf *Treiberpakete*.
4. Wählen Sie ein oder mehrere geeignete Treiberpakete in der Liste aus. Geben Sie *nicht* den Pfad zu einer Druckerbeschreibungsdatei an.
5. Wählen Sie *OK* und bestätigen Sie die Paketinstallation.
6. Sollen diese Treiber direkt verwendet werden, gehen Sie gemäß den Anweisungen in *Prozedur 34.1, „Hinzufügen eines neuen Druckers“* vor.

Für PostScript-Drucker ist keine Druckertreiber-Software erforderlich. Für PostScript-Drucker benötigen Sie lediglich die richtige PostScript-Druckerbeschreibungsdatei (PPD-Datei) für das Druckermodell. Weitere PPD-Dateien erhalten Sie beim Druckerhersteller.

Wenn beim Hinzufügen eines neuen Druckers im Dialogfeld *Treiber suchen und zuweisen* keine passende PPD-Datei vorhanden ist, installieren Sie eine PPD-Datei für Ihren Drucker:

Es gibt mehrere Quellen für PPD-Dateien. Es wird empfohlen, zunächst die weiteren Treiberpakete zu nutzen, die in SUSE Linux Enterprise Desktop inbegriffen sind, jedoch nicht standardmäßig installiert werden (Installationsanweisungen siehe unten). Falls diese Pakete keine geeigneten Dateien für Ihren Drucker enthalten, erhalten Sie die PPD-Dateien direkt vom Druckerhersteller oder von der Treiber-CD eines PostScript-Druckers. Weitere Informationen finden Sie in *Abschnitt 24.8.2, „Für einen PostScript-Drucker ist keine geeignete PPD-Datei verfügbar“*. PPD-Dateien können Sie auch unter https://www.openprinting.org/printers, der „Druckerdatenbank von OpenPrinting.org“, suchen. Beachten Sie bei der Verwendung der PPD-Dateien von OpenPrinting, dass diese möglicherweise nicht von SUSE Linux Enterprise Desktop unterstützt werden.

VORGEHEN 34.3: HINZUFÜGEN EINER PPD-DATEI FÜR POSTSCRIPT-DRUCKER

1. Starten Sie das YaST-Druckermodul mit *Hardware* › *Drucker*.

2. Klicken Sie im Bildschirm *Druckerkonfigurationen* auf *Hinzufügen*.
3. Klicken Sie im Abschnitt `Find and Assign a Driver` auf *Treiberpakete*.
4. Geben Sie den vollständigen Pfad zur PPD-Datei in das Textfeld unter `Make a Printer Description File Available` ein.
5. Klicken Sie auf *OK*, um zum Bildschirm `Add New Printer Configuration` zurückzukehren.
6. Gehen Sie wie unter *Prozedur 34.1, „Hinzufügen eines neuen Druckers“* beschrieben vor, um diese PPD-Datei direkt zu verwenden.

34.1.2 Anpassen einer lokalen Druckerkonfiguration

Sie können die vorhandene Konfiguration für einen Drucker bearbeiten und damit grundlegende Einstellungen wie den Verbindungstyp und den Treiber ändern. Außerdem können Sie die Standardeinstellungen für Papierformat, Auflösung, Medienquelle und vieles mehr anpassen. Sie können die Kennungen für den Drucker ändern, indem Sie die Druckerbeschreibung oder den Druckerort ändern.

1. Starten Sie das YaST-Druckermodul mit *Hardware* › *Drucker*.
2. Wählen Sie im Bildschirm *Druckerkonfigurationen* die Konfiguration für einen lokalen Drucker in der Liste aus und klicken Sie auf *Bearbeiten*.
3. Ändern Sie die Verbindungsart oder den Treiber wie unter *Prozedur 34.1, „Hinzufügen eines neuen Druckers“* beschrieben. Dies sollte jedoch nur erforderlich sein, wenn Sie Probleme mit der aktuellen Konfiguration haben.
4. Optional: Legen Sie diesen Drucker als Standarddrucker fest, indem Sie die Option *Standarddrucker* aktivieren.
5. Passen Sie die Standardeinstellungen an, indem Sie auf *Alle Optionen für den aktuellen Treiber* klicken. Erweitern Sie zum Ändern einer Einstellung die Liste der Optionen, indem Sie auf das entsprechende Pluszeichen (+) klicken. Ändern Sie die Standardeinstellung, indem Sie auf eine Option klicken. Übernehmen Sie die Änderungen mit *OK*.

34.2 Konfigurieren des Netzwerkdrucks in YaST

Netzwerkdrucker werden nicht automatisch erkannt. Sie müssen manuell konfiguriert werden. Hierfür verwenden Sie das Druckermodul von YaST. Je nach der Einrichtung Ihres Netzwerks können Sie auf einen Druckserver (CUPS, LPD, SMB oder IPX) oder direkt auf einen Netzwerkdrucker (vorzugsweise über TCP) drucken. Das Fenster für die Konfiguration des Netzwerkdrucks öffnen Sie über die Option *Über Netzwerk drucken* auf der linken Seite des Druckermoduls von YaST.

34.2.1 Verwenden von CUPS

In einer Linux-Umgebung wird für den Netzwerkdruck CUPS verwendet. Bei der einfachsten Konfiguration erfolgt der Ausdruck über einen einzigen CUPS-Server, auf den alle Clients zugreifen können. Zum Drucken über mehr als einen CUPS-Server ist ein aktivierter lokaler CUPS-Daemon erforderlich, der mit den entfernten CUPS-Servern kommuniziert.

Wichtig: Durchsuchen der Netzwerkdrucker-Warteschlangen

Die CUPS-Server geben ihre Druckerwarteschlangen entweder über das herkömmliche CUPS-Browsing-Protokoll oder über Bonjour/DND-SD im Netzwerk bekannt. Die Clients müssen diese Listen durchsuchen können, damit die Benutzer bestimmte Drucker auswählen können, an die sie die Druckaufträge senden. Um Netzwerkdruckerwarteschlangen durchsuchen zu können, muss der Dienst `cups-browsed` aus dem Paket `cups-filters-cups-browsed` auf allen Clients ausgeführt werden, die über CUPS-Server drucken. `cups-browsed` wird automatisch gestartet, sobald Sie den Netzwerkdruck mit YaST konfigurieren.

Falls das Durchsuchen nach dem Starten von `cups-browsed` nicht funktioniert, geben die CUPS-Server die Netzwerkdruckerwarteschlangen möglicherweise über Bonjour/DNS-SD bekannt. In diesem Fall müssen Sie zusätzlich das Paket `avahi` und den zugehörigen Dienst mit **`sudo systemctl start avahi-daemon`** auf allen Clients starten.

VORGEHEN 34.4: DRUCKEN ÜBER EINEN EINZELNEN CUPS-SERVER

1. Starten Sie das YaST-Druckermodul mit *Hardware* › *Drucker*.
2. Wählen Sie im linken Bereich die Option *Über Netzwerk drucken*.

3. Aktivieren Sie *Alle Druckaufträge direkt über einen einzelnen CUPS-Server ausführen* und geben Sie den Namen oder die IP-Adresse des Servers an.
4. Klicken Sie auf *Server testen*, um sicherzustellen, dass Sie den richtigen Namen bzw. die richtige IP-Adresse angegeben haben.
5. Klicken Sie auf *OK*, um zum Bildschirm *Druckerkonfigurationen* zurückzukehren. Alle Drucker, die über den CUPS-Server verfügbar sind, werden nun aufgelistet.

VORGEHEN 34.5: DRUCKEN ÜBER MEHRERE CUPS-SERVER

1. Starten Sie das YaST-Druckermodul mit *Hardware* › *Drucker*.
2. Wählen Sie im linken Bereich die Option *Über Netzwerk drucken*.
3. Aktivieren Sie *Druckerankündigungen von CUPS-Servern akzeptieren*.
4. Geben Sie unter `General Settings` an, welche Server verwendet werden müssen. Sie können Verbindungen von allen verfügbaren Netzwerken oder von bestimmten Hosts akzeptieren. Wenn Sie letztere Option wählen, müssen Sie die Hostnamen oder IP-Adressen angeben.
5. Wenn Sie aufgefordert werden, einen lokalen CUPS-Server zu starten, klicken Sie auf *OK* und dann auf *Ja*. Nachdem der Server gestartet wurde, kehrt YaST zum Bildschirm *Druckerkonfigurationen* zurück. Klicken Sie auf *Liste aktualisieren*, um die bislang erkannten Drucker anzuzeigen.

34.2.2 Verwenden von Nicht-CUPS-Druckservern

Wenn Ihr Netzwerk Druckservices über Druckserver anbietet, die keine CUPS-Server sind, starten Sie das YaST-Druckermodul mit *Hardware* › *Drucker* und wählen Sie im linken Bereich *Über Netzwerk drucken* aus. Starten Sie den *Verbindungsassistenten* und wählen Sie die entsprechende *Verbindungsart* aus. Ihr Netzwerkadministrator stellt Ihnen weitere Informationen zur Konfiguration eines Netzwerkdruckers in Ihrer Umgebung zur Verfügung.

34.3 Freigeben von Druckern im Netzwerk

Drucker, die von einem lokalen CUPS-Daemon verwaltet werden, können über das Netzwerk freigegeben werden, wodurch Ihr Rechner zu einem CUPS-Server wird. In der Regel wird ein Drucker durch Aktivierung des sogenannten „Browsing-Modus“ in CUPS freigegeben. Wenn

Browsing aktiviert ist, stehen die lokalen Druckerwarteschlangen den entfernten CUPS-Daemonen zur Überwachung im Netzwerk zur Verfügung. Es kann aber auch ein dedizierter CUPS-Server eingerichtet werden, der alle Druckwarteschlangen verwaltet und für die entfernten Clients direkt zugänglich ist. In diesem Fall ist die Aktivierung des Browsing-Modus nicht erforderlich.

VORGEHEN 34.6: FREIGEBEN VON DRUCKERN

1. Starten Sie das YaST-Druckermodul mit *Hardware* › *Drucker*.
2. Wählen Sie *Drucker freigeben* im linken Bereich aus.
3. Wählen Sie *Entfernten Zugriff zulassen* aus. Aktivieren Sie auch die Option *Für Computer im lokalen Netzwerk* und aktivieren Sie den Browsing-Modus, indem Sie außerdem die Option *Drucker standardmäßig im lokalen Netzwerk veröffentlichen* aktivieren.
4. Klicken Sie auf *OK*, um den CUPS-Server neu zu starten, und kehren Sie zum Bildschirm *Druckerkonfigurationen* zurück.
5. Informationen zu CUPS- und Firewall-Einstellungen finden Sie unter https://en.opensuse.org/SDB:CUPS_and_SANE_Firewall_settings.

35 Einrichten eines Scanners

Sie können einen USB- oder SCSI-Scanner mit YaST konfigurieren. Das Paket `sane-backends` enthält Hardwaretreiber und andere erforderliche Objekte für den Einsatz eines Scanners. Wenn Sie ein HP-All-in-One-Gerät verwenden, siehe *Abschnitt 35.1, „Konfigurieren eines HP All-In-One-Geräts“*. Anleitungen zur Konfiguration eines Netzwerkscanners finden Sie unter *Abschnitt 35.3, „Scannen über das Netzwerk“*.

VORGEHEN 35.1: KONFIGURIEREN EINES USB- ODER SCSI-SCANNERS

1. Schließen Sie Ihren USB- oder SCSI-Scanner an Ihren Computer an und schalten Sie ihn ein.
2. Starten Sie YaST und wählen Sie *Hardware* › *Scanner* aus. YaST erstellt die Scanner-Datenbank und versucht, Ihr Scannermodell automatisch zu erkennen.
   Wenn ein USB- oder SCSI-Scanner nicht korrekt erkannt wird, versuchen Sie es zunächst mit *Weitere* › *Erkennung neu starten*.
3. Wählen Sie den Scanner zur Aktivierung aus der Liste der erkannten Scanner aus und klicken Sie auf *Bearbeiten*.
4. Wählen Sie Ihr Modell aus der Liste aus und klicken Sie auf *Weiter* und *Fertig stellen*.
5. Verwenden Sie *Weitere* › *Testen*, um sicherzustellen, dass Sie den korrekten Treiber gewählt haben.
6. Verlassen Sie den Konfigurationsbildschirm mit *OK*.

35.1 Konfigurieren eines HP All-In-One-Geräts

Ein HP-All-in-One-Gerät kann mit YaST konfiguriert werden, selbst wenn es über das Netzwerk bereitgestellt wird. Wenn Sie ein USB-HP-Kompaktgerät besitzen, beginnen Sie mit der Konfiguration wie unter *Prozedur 35.1, „Konfigurieren eines USB- oder SCSI-Scanners“* beschrieben. Wenn es korrekt erkannt wird und der *Test* erfolgreich ist, ist es einsatzbereit.

Wenn Ihr USB-Gerät nicht ordnungsgemäß erkannt wird oder wenn Ihr HP-Kompaktgerät an das Netzwerk angeschlossen ist, führen Sie den HP-Gerätemanager aus:

1. Starten Sie YaST und wählen Sie *Hardware* › *Scanner* aus. YaST lädt die Scanner-Datenbank.

2. Starten Sie den HP-Gerätemanager mit *Weitere* › *hp-setup ausführen* und folgen Sie den Anweisungen am Bildschirm. Nach dem Beenden des HP Gerätemanagers startet das YaST-Scannermodul die automatische Erkennung neu.
3. Testen Sie ihn, indem Sie *Weitere* › *Testen* wählen.
4. Verlassen Sie den Konfigurationsbildschirm mit *OK*.

35.2 Gemeinsame Nutzung eines Scanners über das Netzwerk

SUSE Linux Enterprise Desktop ermöglicht die Freigabe eines Scanners über das Netzwerk. Konfigurieren Sie hierfür Ihren Scanner wie folgt:

1. Konfigurieren Sie den Scanner wie unter *Kapitel 35, Einrichten eines Scanners* beschrieben.
2. Wählen Sie *Weitere* › *Scannen via Netzwerk*.
3. Geben Sie unter *Servereinstellungen* › *Zulässige Clients für saned* durch ein Komma getrennt die Hostnamen der Clients ein, die den Scanner verwenden dürfen, und schließen Sie das Konfigurationsdialogfeld mit *OK*.

35.3 Scannen über das Netzwerk

Gehen Sie folgendermaßen vor, um einen im Netzwerk freigegebenen Scanner zu verwenden:

1. Starten Sie YaST und wählen Sie *Hardware* › *Scanner* aus.
2. Öffnen Sie das Menü zur Konfiguration des Netzwerkscanners mit *Weitere* › *Scannen via Netzwerk*.
3. Geben Sie unter *Client-Einstellungen* › *Für net-Metadriver verwendete Scanner* den Hostnamen des Computers an, an den der Scanner angeschlossen ist.
4. Beenden Sie das Dialogfeld mit *OK*. Der Netzwerkscanner wird nun im Fenster „Konfiguration des Scanners“ aufgelistet und ist einsatzbereit.

36 Energieverwaltung

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.

36.1 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. Verschiedene Hersteller bieten Hybridvarianten dieses Modus an, beispielsweise RediSafe bei IBM Thinkpads. Der entsprechende ACPI-Zustand ist S4. In Linux wird „suspend to disk“ über Kernel-Routinen durchgeführt, die von ACPI unabhängig sind.

Anmerkung: Geänderte UUID für Swap-Partitionen bei Formatierung über `mkswap`

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. Führen Sie die Neuformatierung entweder über YaST aus (`/etc/fstab` wird dabei aktualisiert) oder passen Sie `/etc/fstab` manuell an.

Akkuüberwachung

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.

36.2 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 21, `journalctl`: Abfragen des `systemd`-Journals*. Weitere Informationen zur Fehlersuche bei ACPI-Problemen finden Sie in *Abschnitt 36.2.2, „Fehlersuche“*.

36.2.1 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. Es empfiehlt sich, die dynamische Frequenzskalierung mit Steuerung durch den On-Demand-Governor im Kernel zu verwenden.

Drosselung sollte nur als letzter Ausweg verwendet werden, um die Betriebsdauer des Akkus trotz hoher Systemlast zu verlängern. Bestimmte 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 im *Buch „System Analysis and Tuning Guide“, Kapitel 12 „Power management“*.

36.2.2 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 Sperrliste 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

Bestimmte 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 36.4, „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.

36.2.2.1 Weitere Informationen

- https://tldp.org/HOWTO/ACPI-HOWTO/ (detailliertes ACPI HOWTO, enthält DSDT-Patches)
- https://uefi.org/specifications (technische Daten zur Advanced Configuration & Power Interface)

36.3 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 die folgenden Verfahren mit dem Befehl **`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 einem bestimmten Inaktivitätszeitraum abgeschaltet wird. Ersetzen Sie *`X`* wie folgt: `0` deaktiviert diesen Mechanismus, sodass die Festplatte kontinuierlich ausgeführt wird. Werte von `1` bis `240` werden mit 5 Sekunden multipliziert. Werte von `241` bis `251` entsprechen 1- bis 11-mal 30 Minuten.

Die internen Energiesparoptionen der Festplatte lassen sich über die Option `-B` steuern. Wählen Sie einen Wert `0` (maximale Energieeinsparung) bis `255` (maximaler Durchsatz). Das Ergebnis hängt von der verwendeten Festplatte ab und ist schwer einzuschätzen. Die Geräuschentwicklung einer Festplatte können Sie mit der Option `-M` reduzieren. Wählen Sie einen Wert von `128` (ruhig) bis `254` (schnell).

Häufig ist es nicht so einfach, die Festplatte in den Ruhezustand zu versetzen. Bei Linux führen mehrere 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 geschrieben werden sollte. Der Standardwert ist `3000`, was 30 Sekunden bedeutet.

`/proc/sys/vm/dirty_background_ratio`
: Maximaler Prozentsatz an schlechten Seiten, bis pdflush damit beginnt, sie zu schreiben. Der Standardwert ist `5`%.

`/proc/sys/vm/dirty_ratio`
: Wenn die schlechten Seiten diesen Prozentsatz des gesamten Arbeitsspeichers überschreiten, werden Prozesse gezwungen, während ihres Zeitabschnitts Puffer mit schlechten Seiten anstelle von weiteren Daten zu schreiben.

Warnung: Datenintegritätsrisiko

Änderungen an den Einstellungen für den `pdflush`-Aktualisierungs-Daemon können die Datenintegrität beeinträchtigen.

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. Um dies zu vermeiden, wurde eine spezielle Kernel-Erweiterung für mobile Geräte entwickelt. Um die Erweiterung zu verwenden, installieren Sie das Paket `laptop-mode-tools`. Weitere Informationen finden Sie unter `/usr/src/linux/Documentation/laptops/laptop-mode.txt`.

Ein weiterer wichtiger Faktor ist die Art und Weise, wie sich die Programme verhalten. Gute Editoren beispielsweise schreiben regelmäßig verborgene Sicherungskopien der aktuell bearbeiteten Datei auf die Festplatte, wodurch die Festplatte wieder aktiviert wird. Derartige Funktionen können auf Kosten der Datenintegrität deaktiviert werden.

In dieser Verbindung verwendet der Mail-Daemon postfix die Variable `POSTFIX_LAPTOP`. Wenn diese Variable auf `yes` (ja) gesetzt wird, greift postfix wesentlich seltener auf die Festplatte zu.

In SUSE Linux Enterprise Desktop werden diese Technologien von `laptop-mode-tools` gesteuert.

36.4 Fehlersuche

Alle Fehler- und Alarmmeldungen werden im Systemjournal gespeichert, das Sie mit dem Befehl **`journalctl`** abrufen können (weitere Informationen siehe *Kapitel 21, `journalctl`: Abfragen des `systemd`-Journals*). In den folgenden Abschnitten werden die häufigsten Probleme behandelt.

36.4.1 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 Permanenter Speicher

Dieses Kapitel enthält weitere Informationen zur Verwendung von SUSE Linux Enterprise Desktop mit nicht flüchtigem Hauptspeicher, auch als *permanenter Speicher* bekannt, der aus einem oder mehreren NVDIMMs besteht.

37.1 Einführung

Ein permanenter Speicher ist eine neue Art von Speicherung am Rechner. Er kombiniert annähernd so hohe Geschwindigkeiten wie bei dynamischen RAMs (DRAMs) mit der Byte-für-Byte-Adressierbarkeit des RAM und der Permanenz von Solid-State Drives (SSDs).

SUSE unterstützt aktuell die Verwendung eines permanenten Speichers mit SUSE Linux Enterprise Desktop auf Rechnern mit AMD64/Intel 64- und POWER-Architekturen.

Wie bei herkömmlichen RAMs wird der permanente Speicher direkt am Speichersteckplatz der Hauptplatine installiert. Damit wird er im selben physischen Formfaktor bereitgestellt wie RAM – als DIMMs. Man nennt sie NVDIMMs: Non-Volatile Dual Inline Memory Modules.

Im Unterschied zu RAM ist ein permanenter Speicher in vielerlei Hinsicht Flash-basierten SSDs ähnlich. Beide basieren auf unterschiedliche Weise auf dem Stromkreis von Festkörperspeichern, bieten aber unabhängig davon einen nicht flüchtigen Speicher. Dies bedeutet, dass ihre Inhalte beibehalten werden, wenn das System heruntergefahren oder neu gestartet wird. Bei beiden Varianten geht das Schreiben von Daten langsamer von statten als das Lesen und beide unterstützen eine begrenzte Anzahl von Neuschreibungszyklen. Wie bei SSDs ist der Zugriff auf Sektorebene des permanenten Speichers möglich, sollte dies für eine bestimmte Anwendung erforderlich sein.

Die unterschiedlichen Modelle verwenden verschiedene Arten von elektronischen Speichermedien, wie Intel 3D XPoint oder eine Kombination aus NAND-Flash und DRAM. Neue Arten von nicht flüchtigen RAMs werden derzeit entwickelt. Verschiedene Anbieter und Modelle von NVDIMMs bieten unterschiedliche Eigenschaften für Leistung und Langlebigkeit.

Da sich die entsprechenden Speichertechnologien noch in der frühen Entwicklungsphase befinden, ist bei der Hardware verschiedener Anbieter möglicherweise mit unterschiedlichen Einschränkungen zu rechnen. Daher sind die folgenden Aussagen als Verallgemeinerungen zu betrachten.

Ein permanenter Speicher ist bis zu zehn mal langsamer als DRAM, doch in etwa tausend mal schneller als Flash-Speicher. Im Gegensatz zum Vorgang des Auslöschens und Neuschreibens des gesamten Sektors beim Flash-Speicher kann der permanente Speicher auf Byte-zu-Byte-Basis neu geschrieben werden. Da die Neuschreibungszyklen begrenzt sind, können permanente Speicher schließlich Millionen von Neuschreibungen verarbeiten, verglichen mit Tausenden von Zyklen des Flash-Speichers.

Das hat zwei erhebliche Folgen:

- Beim aktuellen Stand der Technik ist es nicht möglich, ein System nur mit permanentem Speicher auszuführen und dadurch einen nicht flüchtigen Hauptspeicher zu erzielen. Sie müssen einen herkömmlichen RAM mit NVDIMMs kombinieren. Das Betriebssystem und die Anwendungen werden am herkömmlichen RAM ausgeführt und NVDIMMs bieten eine schnelle ergänzende Speichermöglichkeit.
- Aufgrund der Leistungsmerkmale der permanenten Speicher von verschiedenen Anbietern müssen Programmierer möglicherweise die Hardwarespezifikationen der NVDIMMs an einem bestimmten Server berücksichtigen, einschließlich deren Anzahl und belegten Speichersteckplätze. Dies wirkt sich auf die Verwendung des Hypervisors aus sowie auf die Migration von Software zwischen verschiedenen Host-Rechnern usw.

Dieses neue Speicher-Untersystem ist in Version 6 des ACPI-Standards definiert. `libnvdimm` unterstützt jedoch NVDIMMs, die den Standard noch nicht erfüllen, wodurch diese auf gleiche Weise verwendet werden können.

Tipp: Permanenter Intel Optane DC-Speicher

Intel Optane-DIMM-Speicher kann in verschiedenen Modi verwendet werden:

- Im *App-Direct-Modus* wird der Intel Optane-Speicher als schneller permanenter Speicher verwendet – eine Alternative zu SSDs und NVMe-Geräten. Daten in diesem Modus bleiben erhalten, wenn das System ausgeschaltet wird.
  Der App-Direct-Modus wird seit SLES 12 SP4 unterstützt.
- Im *Speichermodus* bietet der Intel Optane-Speicher eine kostengünstige Alternative zu DRAM mit hoher Speicherkapazität. In diesem Modus werden separate DRAM DIMMs als Cache für die Daten, auf die am häufigsten zugegriffen wird, verwendet, während der Optane-DIMM-Speicher für eine hohe Speicherkapazität sorgt. Verglichen mit reinen DRAM-Systemen ist dieser Modus jedoch bei Arbeitslasten mit wahlfreiem Zugriff langsamer. Wenn Sie Anwendungen ohne die Optane-spezifischen

Erweiterungen ausführen, die diesen Modus nutzen, kann sich die Speicherleistung verringern. Daten in diesem Modus gehen verloren, wenn das System ausgeschaltet wird.
Der Speichermodus wird seit SLES 15 SP1 unterstützt.

- Im *gemischten Modus* wird der Intel Optane-Speicher partitioniert, sodass er in beiden Modi gleichzeitig verwendet werden kann.
  Der gemischte Modus wird seit SLES 15 SP1 unterstützt.

37.2 Begriffe

Region

Eine *Region* ist ein Block des permanenten Speichers, der in einen oder mehrere *Namespaces* unterteilt werden kann. Der Zugriff auf den permanenten Speicher einer Region ist erst nach dessen Zuordnung zu einem Namespace möglich.

Namespace

Ein einzelner zusammenhängend adressierter Bereich eines nicht flüchtigen Speichers, vergleichbar mit NVM Express SSD-Namespaces oder SCSI Logical Units (LUNs). Namespaces werden im `/dev`-Verzeichnis des Servers als separate Blockgeräte angezeigt. Abhängig von der erforderlichen Zugriffsmethode können Namespaces entweder Speicherplatz von verschiedenen NVDIMMs in größere Volumes zusammenfassen oder dessen Partitionierung in kleinere Volumes zulassen.

Modus

Jeder Namespace weist auch einen *Modus* auf, der definiert, welche NVDIMM-Funktionen für diesen Namespace aktiviert sind. Gleichgeordnete Namespaces der gleichen übergeordneten Region sind im Typ immer gleich, werden jedoch möglicherweise mit verschiedenen Modi konfiguriert. Namespace-Modi:

devdax

Geräte-DAX-Modus. Erstellt eine Einzelzeichen-Gerätedatei (`/dev/daxX.Y`). Die Erstellung eines Dateisystems ist *nicht* erforderlich.

fsdax

Dateisystem-DAX-Modus. Standardmodus, falls kein anderer Modus angegeben wird. Erstellt ein Blockgerät (`/dev/pmemX [.Y]`), das DAX für `ext4` oder `XFS` unterstützt.

sector

Für veraltete Dateisysteme, die keine Checksumme für Metadaten erstellen. Geeignet für kleine Boot-Volumes. Kompatibel mit anderen Betriebssystemen.

raw

Ein Speicherdatenträger ohne Kennung oder Metadaten. Keine Unterstützung von DAX. Kompatibel mit anderen Betriebssystemen.

Anmerkung

Der `raw`-Modus wird von SUSE nicht unterstützt. Es ist nicht möglich, Dateisysteme auf `raw`-Namespaces einzuhängen.

Typ

Jeder Namespace und jede Region weist einen *Typ* auf, der definiert, wie auf den permanenten Speicher, der mit diesem Namespace oder dieser Region verknüpft ist, zugegriffen wird. Ein Namespace hat immer denselben Typ wie dessen übergeordnete Region. Zwei verschiedene Typen stehen zur Verfügung: Permanenter Speicher, der auf zwei verschiedene Arten konfiguriert werden kann, sowie der veraltete Block-Modus.

Permanenter Speicher (PMEM)

Der PMEM-Speicher bietet Zugriff auf Byte-Ebene, ähnlich wie RAM. Mit PMEM kann ein einzelner Namespace mehrere überlappende NVDIMMs enthalten und alle können als Einzelgerät verwendet werden.
Ein PMEM-Namespace kann auf zwei Arten konfiguriert werden.

PMEM mit DAX

Ein für den Direktzugriff (DAX) konfigurierter Namespace bedeutet, dass beim Zugreifen auf den Arbeitsspeicher der Seiten-Cache des Kernels umgangen und direkt auf das Medium zugegriffen wird. Die Software kann jedes Byte des Namespace separat lesen oder schreiben.

PMEM mit BTT (Block Translation Table)

Wie bei einem herkömmlichen Festplattenlaufwerk wird auf einen für den Betrieb im BTT-Modus konfigurierten PMEM-Namespace Sektor für Sektor zugegriffen, im Unterschied zu dem eher RAM-ähnlichen Byte-adressierbaren Modell. Durch einen Übersetzungstabellen-Mechanismus werden die Zugriffe in Einheiten von Sektorgröße eingeteilt.

Der Vorteil von BTT ist der Datenschutz. Das Speicher-Untersystem sorgt dafür, dass jeder Sektor vollständig auf das zugrunde liegende Medium geschrieben wird. Wenn ein Sektor nicht vollständig geschrieben wird (also wenn der Schreibvorgang aus jeglichen Gründen fehlschlägt), wird ein Rollback des gesamten Sektors auf den ursprünglichen Status vorgenommen. Daher kann ein Sektor nicht teilweise geschrieben werden.
Der Zugriff auf BTT-Namespaces wird zudem vom Kernel im Cache gespeichert. Der Nachteil ist, dass kein Direktzugriff auf BTT-Namespaces möglich ist.

Block-Modus (BLK)

Beim Speichern im Block-Modus wird jeder NVDIMM als separates Gerät adressiert. Dieser Modus ist inzwischen veraltet und wird nicht mehr unterstützt.

Abgesehen von `devdax`-Namespaces müssen alle anderen Typen mit einem Dateisystem formatiert werden, genau wie bei einem herkömmlichen Laufwerk. SUSE Linux Enterprise Desktop unterstützt dazu die Dateisysteme `ext2`, `ext4` und `XFS`.

Direktzugriff (Direct Access, DAX)

Durch DAX kann ein permanenter Speicher direkt im Adressbereich eines Prozesses zugeordnet werden, beispielsweise über den Systemaufruf `mmap`.

Physikalische DIMM-Adresse (DPA)

Eine Speicheradresse als Offset in den Speicher eines einzelnen DIMMs, das heißt beginnend bei Null als niedrigstem adressierbaren Byte in diesem DIMM.

Kennung

Im NVDIMM gespeicherte Metadaten wie beispielsweise Namespace-Definitionen. Der Zugriff ist über DSM möglich.

Gerätespezifische Methode (Device-specific method, DSM)

ACPI-Methode für den Zugriff auf die Firmware eines NVDIMM.

37.3 Einsatzbereiche

37.3.1 PMEM mit DAX

Diese Form des Speicherzugriffs ist *nicht* transaktional. Im Fall eines Stromausfalls oder eines anderen Systemfehlers werden die Daten möglicherweise nicht in den Speicher geschrieben. Ein PMEM ist nur für Anwendungen geeignet, die teilweise geschriebene Daten verarbeiten können.

37.3.1.1 Anwendungen, die von einem großen Byte-adressierbaren Speicher profitieren

Wenn am Server eine Anwendung gehostet wird, die direkt einen großen Teil eines schnellen Speichers Byte für Byte verwendet, kann der Programmierer mit dem Systemaufruf `mmap` Blöcke des permanenten Speichers direkt in den Adressbereich der Anwendung stellen, ohne auf zusätzlichen System-RAM zurückgreifen zu müssen.

37.3.1.2 Vermeiden des Kernel-Seiten-Caches

Vermeiden Sie den Kernel-Seiten-Cache, um den RAM für den Seiten-Cache aufzusparen und ihn stattdessen anderen Anwendungen zuzuweisen. Dieser könnte beispielsweise zum Speichern von VM-Images vorgesehen werden. Diese Images würden nicht in den Cache gestellt werden, was die Cache-Auslastung am Host reduzieren und mehr VMs pro Host zulassen würde.

37.3.2 PMEM mit BTT

Diese Variante ist nützlich, wenn Sie den permanenten Speicher auf einigen NVDIMMs als einen datenträgerähnlichen Pool von schnellen Speichern verwenden möchten. Wird beispielsweise das Dateisystemjournal auf PMEM mit BTT platziert, erhöht sich dadurch die Zuverlässigkeit der Dateisystemwiederherstellung nach Stromausfall oder sonstiger plötzlicher Unterbrechung (siehe *Abschnitt 37.5.3, „Erstellen eines PMEM-Namespace mit BTT“*).

Anwendungen halten diese Geräte für schnelle SSDs, die wie jedes andere Speichergerät verwendet werden. LVM kann beispielsweise auf den permanenten Speicher aufgesetzt werden und funktioniert normal.

BTT hat den Vorteil, dass die Unteilbarkeit beim Schreiben in den Sektor gewährleistet ist. Somit bleiben sogar sehr anspruchsvolle und von Datenintegrität abhängige Anwendungen funktionsfähig. Die Erstellung von Fehlerberichten funktioniert über standardmäßige Kanäle zur Fehlerberichterstellung.

37.4 Tools zur Verwaltung eines permanenten Speichers

Zur Verwaltung eines permanenten Speichers muss das Paket `ndctl` installiert werden. Dadurch wird auch das Paket `libndctl` installiert. Es enthält einige Benutzerbereich-Bibliotheken zum Konfigurieren von NVDIMMs.

Diese Tools arbeiten mit der Bibliothek `libnvdimm`, die drei Typen von NVDIMM unterstützt:

- PMEM
- BLK
- PMEM und BLK gleichzeitig

Das **`ndctl`**-Dienstprogramm enthält einige nützliche **`man`**-Seiten, auf die mit dem folgenden Befehl zugegriffen wird:

```
> ndctl help subcommand
```

Eine Liste der verfügbaren Unterbefehle erhalten Sie mit:

```
> ndctl --list-cmds
```

Folgende Unterbefehle stehen zur Verfügung:

version
: Zeigt die aktuelle Version der NVDIMM-Unterstützungstools an.

enable-namespace
: Stellt den angegebenen Namespace zur Verfügung.

disable-namespace
: Verhindert die Verwendung des angegebenen Namespace.

create-namespace

Erstellt einen neuen Namespace aus den angegebenen Speichergeräten.

destroy-namespace

Entfernt den angegebenen Namespace.

enable-region

Stellt die angegebene Region zur Verfügung.

disable-region

Verhindert die Verwendung der angegebenen Region.

zero-labels

Löscht die Metadaten von einem Gerät.

read-labels

Ruft die Metadaten vom angegebenen Gerät ab.

list

Zeigt verfügbare Geräte an.

help

Zeigt Informationen zur Verwendung des Tools an.

37.5 Einrichten eines permanenten Speichers

37.5.1 Anzeigen des verfügbaren NVDIMM-Speichers

Mit dem Befehl **`ndctl`** `list` werden alle verfügbaren NVDIMMs in einem System aufgelistet.

Im folgenden Beispiel hat das System drei NVDIMMs, die sich in einem einzelnen, dreikanaligen überlappenden Set befinden.

```
# ndctl list --dimms

[
 {
  "dev":"nmem2",
  "id":"8089-00-0000-12325476"
 },
 {
```

```
  "dev":"nmem1",
  "id":"8089-00-0000-11325476"
 },
 {
  "dev":"nmem0",
  "id":"8089-00-0000-10325476"
 }
]
```

Mit einem anderen Parameter listet **ndctl** `list` auch die verfügbaren Regionen auf.

Anmerkung

Regionen erscheinen möglicherweise nicht in numerischer Reihenfolge.

Beachten Sie, dass zwar nur drei NVDIMMs vorhanden sind, doch vier Regionen angezeigt werden.

```
# ndctl list --regions

[
 {
  "dev":"region1",
  "size":68182605824,
  "available_size":68182605824,
  "type":"blk"
 },
 {
  "dev":"region3",
  "size":202937204736,
  "available_size":202937204736,
  "type":"pmem",
  "iset_id":5903239628671731251
  },
  {
   "dev":"region0",
   "size":68182605824,
   "available_size":68182605824,
   "type":"blk"
  },
  {
   "dev":"region2",
   "size":68182605824,
   "available_size":68182605824,
   "type":"blk"
```

```
  }
]
```

Der Speicherplatz ist auf zwei verschiedene Arten verfügbar: entweder als drei separate 64 GB-Regionen vom Typ BLK oder als eine kombinierte 189 GB-Region vom Typ PMEM, die den gesamten Speicherplatz auf den drei überlappenden NVDIMMs als ein einziges Volume darstellt.

Beachten Sie, dass der angezeigte Wert für `available_size` identisch ist mit dem Wert für `size`. Dies bedeutet, dass noch kein Speicherplatz zugeordnet wurde.

37.5.2 Konfigurieren des Speichers als einzelnen PMEM-Namespace mit DAX

Im ersten Beispiel konfigurieren wir unsere drei NVDIMMs in einem einzelnen PMEM-Namespace mit Direktzugriff (DAX).

Im ersten Schritt erstellen wir einen neuen Namespace.

```
# ndctl create-namespace --type=pmem --mode=fsdax --map=memory
{
 "dev":"namespace3.0",
 "mode":"memory",
 "size":199764213760,
 "uuid":"dc8ebb84-c564-4248-9e8d-e18543c39b69",
 "blockdev":"pmem3"
}
```

Dadurch wird ein Blockgerät `/dev/pmem3` erstellt, das DAX unterstützt. Die `3` im Gerätenamen wird von der Nummer der übergeordneten übernommen, in diesem Fall `region3`region.

Die Option `--map=memory` reserviert einen Teil des PMEM-Speicherplatzes auf den NVDIMMs für die Zuordnung interner Kernel-Datenstrukturen namens `struct pages`. Dadurch kann der neue PMEM-Namespace mit Funktionen wie `O_DIRECT I/O` und `RDMA` verwendet werden.

Aufgrund der Reservierung eines Teils des permanenten Speichers für Kernel-Datenstrukturen hat der resultierende PMEM-Namespace eine geringere Kapazität als die übergeordnete PMEM-Region.

Als nächstes überprüfen wir, ob das neue Blockgerät für das Betriebssystem verfügbar ist:

```
# fdisk -l /dev/pmem3
Disk /dev/pmem3: 186 GiB, 199764213760 bytes, 390164480 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
```

```
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
```

Bevor es verwendet werden kann, muss es wie jedes andere Gerät formatiert werden. In diesem Beispiel formatieren wir es mit XFS:

```
# mkfs.xfs /dev/pmem3
meta-data=/dev/pmem3      isize=256    agcount=4, agsize=12192640 blks
         =                sectsz=4096  attr=2, projid32bit=1
         =                crc=0        finobt=0, sparse=0
data     =                bsize=4096   blocks=48770560, imaxpct=25
         =                sunit=0      swidth=0 blks
naming   =version 2       bsize=4096   ascii-ci=0 ftype=1
log      =internal log    bsize=4096   blocks=23813, version=2
         =                sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none            extsz=4096   blocks=0, rtextents=0
```

Danach können wir das neue Laufwerk in ein Verzeichnis einhängen:

```
# mount -o dax /dev/pmem3 /mnt/pmem3
```

Dann überprüfen wir, ob wir nun über ein DAX-fähiges Gerät verfügen:

```
# mount | grep dax
/dev/pmem3 on /mnt/pmem3 type xfs (rw,relatime,attr2,dax,inode64,noquota)
```

Das Ergebnis ist ein PMEM-Namespace, der mit dem XFS-Dateisystem formatiert und mit DAX eingehängt ist.

`mmap()`-Aufrufe von Dateien in diesem Dateisystem geben virtuelle Adressen zurück, die direkt dem permanenten Speicher auf unseren NVDIMMs zugeordnet werden. Der Seiten-Cache wird dabei umgangen.

`fsync`- oder `msync`-Aufrufe von Dateien in diesem Dateisystem stellen weiterhin sicher, dass geänderte Daten vollständig in die NVDIMMs geschrieben werden. Diese Aufrufe löschen die Zeilen des Prozessor-Cache, die mit Seiten verknüpft sind, die im Benutzerbereich über `mmap`-Zuordnungen geändert wurden.

37.5.2.1 Entfernen eines Namespace

Bevor wir einen anderen Volume-Typ erstellen, der den selben Speicher verwendet, müssen wir das PMEM-Volume aushängen und dann entfernen.

Hängen Sie es zunächst aus:

```
# umount /mnt/pmem3
```

Deaktivieren Sie dann den Namespace:

```
# ndctl disable-namespace namespace3.0
disabled 1 namespace
```

Löschen Sie es nun:

```
# ndctl destroy-namespace namespace3.0
destroyed 1 namespace
```

37.5.3 Erstellen eines PMEM-Namespace mit BTT

BTT sorgt für Unteilbarkeit beim Schreiben in den Sektor, was es zu einer guten Wahl macht, wenn Datenschutz erforderlich ist, zum Beispiel für Ext4- und XFS-Journale. Bei Stromausfall sind die Journale geschützt und sollten wiederherstellbar sein. Die folgenden Beispiele zeigen, wie ein PMEM-Namespace mit BTT im Sektormodus erstellt und wie das Dateisystemjournal in diesem Namespace platziert wird.

```
# ndctl create-namespace --type=pmem --mode=sector
{
 "dev":"namespace3.0",
 "mode":"sector",
 "uuid":"51ab652d-7f20-44ea-b51d-5670454f8b9b",
 "sector_size":4096,
 "blockdev":"pmem3s"
}
```

Überprüfen Sie als Nächstes, ob das Gerät vorhanden ist:

```
# fdisk -l /dev/pmem3s
Disk /dev/pmem3s: 188.8 GiB, 202738135040 bytes, 49496615 sectors
Units: sectors of 1 * 4096 = 4096 bytes
Sector size (logical/physical): 4096 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
```

Wie der vorher konfigurierte DAX-fähige PMEM-Namespace verbraucht dieser BTT-fähige Namespace den gesamten verfügbaren Speicherplatz auf den NVDIMMs.

Anmerkung

Das angehängte `s` am Ende des Gerätenamens (`/dev/pmem3s`) steht für `sector`. Damit lassen sich Namespaces, die zur Verwendung von BTT konfiguriert wurden, leicht unterscheiden.

Das Volume wird wie im vorigen Beispiel formatiert und eingehängt.

Der hier gezeigte PMEM-Namespace kann DAX nicht verwenden. Stattdessen verwendet er BTT für die *Unteilbarkeit beim Schreiben des Sektors*. Bei jedem Schreiben des Sektors über den PMEM-Blocktreiber ordnet BTT einen neuen Sektor zu, um neue Daten zu empfangen. BTT aktualisiert ungeteilt die internen Zuordnungsstrukturen, nachdem alle neuen Daten vollständig geschrieben sind, sodass die neu geschriebenen Daten den Anwendungen zur Verfügung stehen. Wenn zu irgendeinem Zeitpunkt dieses Vorgangs der Strom ausfällt, sind alle geschriebenen Daten verloren und die Anwendung hat Zugriff auf die alten Daten, die noch intakt sind. Dadurch wird der Zustand der sogenannten „zerrissenen Sektoren“ verhindert.

Dieser BTT-fähige PMEM-Namespace wird wie ein Dateisystem formatiert und verwendet, genau wie jedes andere Standard-Blockgerät. Die Verwendung mit DAX ist nicht möglich. `mmap`-Zuordnungen für Dateien auf diesem Blockgerät verwenden jedoch den Seiten-Cache.

37.5.4 Platzieren des Dateisystemjournals auf PMEM/BTT

Wird das Dateisystemjournal auf einem separaten Gerät platziert, muss es dieselbe Dateisystem-Blockgröße wie das Dateisystem verwenden. Sie beträgt höchstwahrscheinlich 4096 und Sie finden die Blockgröße mit diesem Befehl:

```
# blockdev --getbsz /dev/sda3
```

Im folgenden Beispiel wird ein neues Ext4-Journal auf einem separaten NVDIMM-Gerät erstellt und das Dateisystem auf einem SATA-Gerät. Dann wird das neue Dateisystem an das Journal angehängt:

```
# mke2fs -b 4096 -O journal_dev /dev/pmem3s
# mkfs.ext4 -J device=/dev/pmem3s /dev/sda3
```

Im folgenden Beispiel wird ein neues XFS-Dateisystem auf einem SATA-Laufwerk erstellt und das Journal auf einem separaten NVDIMM-Gerät:

```
# mkfs.xfs -l logdev=/dev/pmem3s  /dev/sda3
```

Detaillierte Informationen zu den Optionen finden Sie unter **`man 8 mkfs.ext4`** und **`man 8 mkfs.ext4`**.

37.6 Weitere Informationen

Für weitere Informationen zu diesem Thema siehe die folgende Liste:

- Permanenter Speicher – Wiki (https://nvdimm.wiki.kernel.org/)
  Enthält Anweisungen zum Konfigurieren von NVDIMM-Systemen, Informationen zu Tests sowie Links zu Spezifikationen für die Aktivierung von NVDIMMs. Diese Site wird im Zuge der NVDIMM-Unterstützung in Linux entwickelt.

- Permanenter Speicher – Programmierung (https://pmem.io/)
  Informationen zum Konfigurieren, Verwenden und Programmieren von Systemen mit nicht flüchtigem Speicher unter Linux und anderen Betriebssystemen. Behandelt die NVM-Bibliothek (NVML), die nützliche APIs zum Programmieren mit permanentem Speicher im Benutzerbereich bereitstellt.

- LIBNVDIMM: Nicht flüchtige Geräte (https://www.kernel.org/doc/Documentation/nvdimm/nvdimm.txt)
  Für Kernel-Entwickler gedacht und Teil des Dokumentationsverzeichnisses im aktuellen Linux-Kernel-Baum. Es beschreibt die verschiedenen Kernel-Module, die an der NVDIMM-Aktivierung beteiligt sind, gibt technische Details zur Kernel-Implementierung und erläutert die `sysfs`-Schnittstelle zum Kernel, die vom **`ndctl`**-Tool verwendet wird.

- GitHub: pmem/ndctl (https://github.com/pmem/ndctl)
  Dienstprogramm-Bibliothek zur Verwaltung des **`libnvdimm`**-Untersystems im Linux-Kernel. Enthält zudem Benutzerbereich-Bibliotheken sowie Einheitentests und eine Dokumentation.

V Services

38 Serviceverwaltung mit YaST 533

39 Zeitsynchronisierung mit NTP 535

38 Serviceverwaltung mit YaST

YaST umfasst einen Service-Manager zum Steuern des standardmäßigen Systemziels und der Services, zum Anzeigen des Servicestatus und Lesen der Protokolldatei. Neu in SUSE Linux Enterprise Desktop 15 SP7 ist die YaST-Unterstützung für die Aktivierung des Socket-basierten Service mit `systemd`. Dadurch werden die Services so konfiguriert, dass sie auf Abruf starten.

`systemd` unterstützt das Starten von Services mit Socket-basierter Aktivierung auf Abruf. Diese Services weisen zwei Arten von Einheiten auf: Service und Socket. Beispielsweise wird CUPS mit `cups.service` und `cups.socket` gesteuert. YaST ermöglicht Ihnen die Auswahl des gewünschten Servicestarts.

In *Abbildung 38.1, „YaST Service-Manager“* sehen Sie die Optionen im Dropdownfeld „Startmodus“: *Beim Booten*, *Auf Abruf* und *Manuell*. Wählen Sie für die Socket-basierte Aktivierung die Option *Auf Abruf* aus. Damit wird ein Netzwerk-Socket zur Überwachung geöffnet und der Service startet nach einer Anforderung.

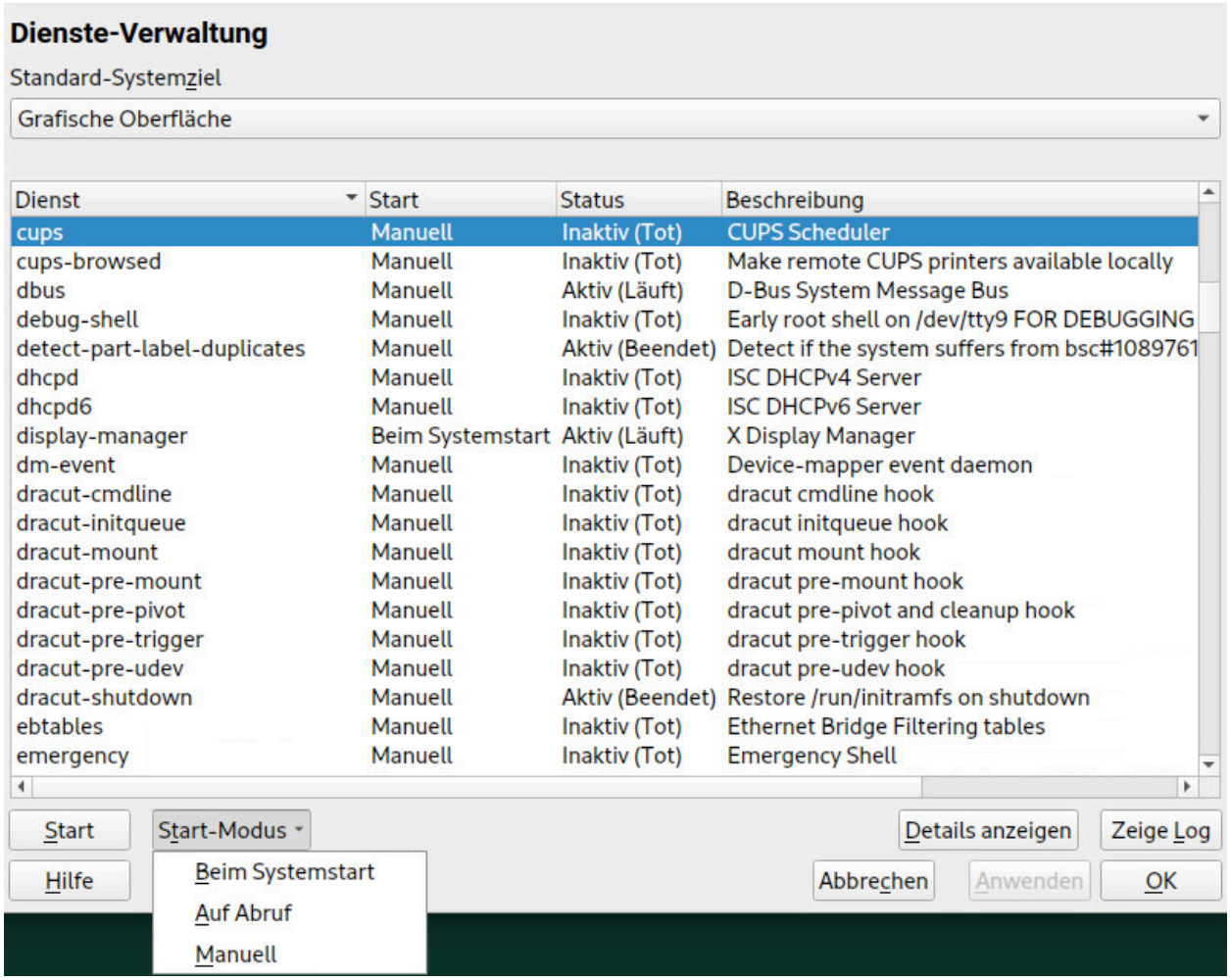


ABBILDUNG 38.1: YAST SERVICE-MANAGER

Die Option *Auf Abruf* ist nur für Services sichtbar, die diese Option unterstützen. Aktuell sind dies nur einige wenige Services wie CUPS, dbus, iscsid, iscsiuio, multipathd, pcscd, rpcbind, TFTP, virtlockd und virtlogd. Detaillierte Informationen zur Funktionsweise der Socket-Aktivierung finden Sie in `man 5 systemd.socket`.

39 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.

Ab SUSE Linux Enterprise Desktop 15 ist `chrony` die Standardimplementation von NTP. `chrony` besteht aus zwei Teilen: `chronyd` ist ein Daemon, der beim Booten gestartet werden kann, und mit dem Befehlszeilenschnittstellenprogramm **`chronyc`** ist es möglich, die Leistung von `chronyd` zu überwachen und Betriebsparameter zur Laufzeit zu ändern.

Ab SUSE Linux Enterprise Desktop 15.2 konfiguriert das YaST-Modul für die NTP-Client-Konfiguration den systemd-timer anstelle des Cron-Daemon, um `chrony` auszuführen, wenn es nicht zur Ausführung als Daemon konfiguriert ist.

Anmerkung

Befolgen Sie die Anweisungen unter *Buch „Security and Hardening Guide“, Kapitel 7 „Active Directory support“, Abschnitt 7.3.3 „Joining Active Directory using Windows domain membership“, Joining an Active Directory domain using Windows domain membership*, um die Zeitsynchronisierung über Active Directory zu aktivieren.

39.1 Konfigurieren eines NTP-Clients mit YaST

Der NTP-Daemon (`chronyd`) im `chrony`-Paket ist so voreingestellt, dass die Hardware-Uhr des lokalen Computers als Zeitreferenz verwendet wird. Die Präzision einer Hardware-Uhr ist stark von der Zeitquelle abhängig. Eine Atomuhr oder ein GPS-Empfänger ist beispielsweise eine genaue Zeitquelle, ein normaler RTC-Chip ist dagegen keine zuverlässige Zeitquelle. YaST erleichtert die Konfiguration von NTP-Clients.

Im Fenster für die YaST-NTP-Client-Konfiguration (*Netzwerkdienste* › *NTP-Konfiguration*) können Sie den Zeitpunkt für den Start des NTP-Daemons sowie den Typ der Konfigurationsquelle angeben und benutzerdefinierte Zeitserver einfügen.

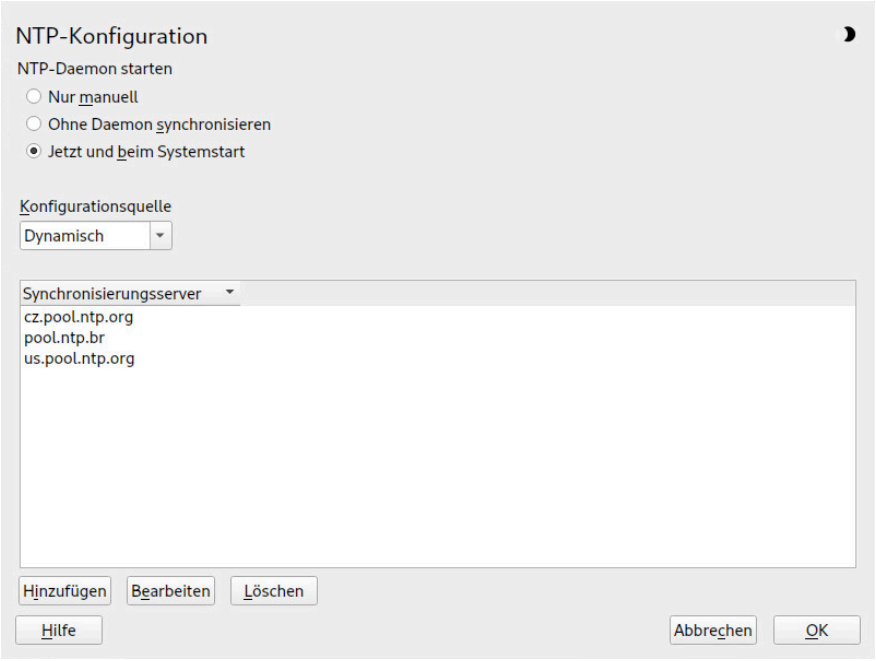


ABBILDUNG 39.1: FENSTER „NTP-KONFIGURATION“

39.1.1 Start des NTP-Daemons

Zum Starten des NTP-Daemons stehen drei Optionen zur Auswahl:

Nur manuell

Wählen Sie *Nur manuell*, um den `chrony`-Daemon manuell zu starten.

Ohne Daemon synchronisieren

Wählen Sie *Ohne Daemon synchronisieren* aus, um die Systemzeit regelmäßig festzulegen, ohne dass `chrony` ständig ausgeführt wird. Sie können das *Synchronisierungsintervall in Minuten* festlegen.

Jetzt und beim Booten

Wählen Sie *Jetzt und beim Booten* aus, um `chronyd` automatisch beim Booten des Systems zu starten. Diese Einstellung wird empfohlen.

39.1.2 Typ der Konfigurationsquelle

Wählen Sie im Dropdown-Feld *Konfigurationsquelle* entweder die Option *Dynamisch* oder *Statisch*. Verwenden Sie *Statisch*, wenn Ihr Server nur mit einer bestimmten Gruppe (öffentlicher) NTP-Server arbeitet, und *Dynamisch*, wenn Ihr internes Netzwerk NTP-Server über DHCP anbietet.

39.1.3 Konfigurieren von Zeitservern

Im unteren Bereich des Fensters *NTP-Konfiguration* werden die Zeitserver aufgelistet, die der Client abfragen kann. Bearbeiten Sie diese Liste nach Bedarf mithilfe der Optionen *Hinzufügen*, *Bearbeiten* und *Löschen*.

Klicken Sie auf *Hinzufügen*, um einen neuen Zeitserver hinzuzufügen:

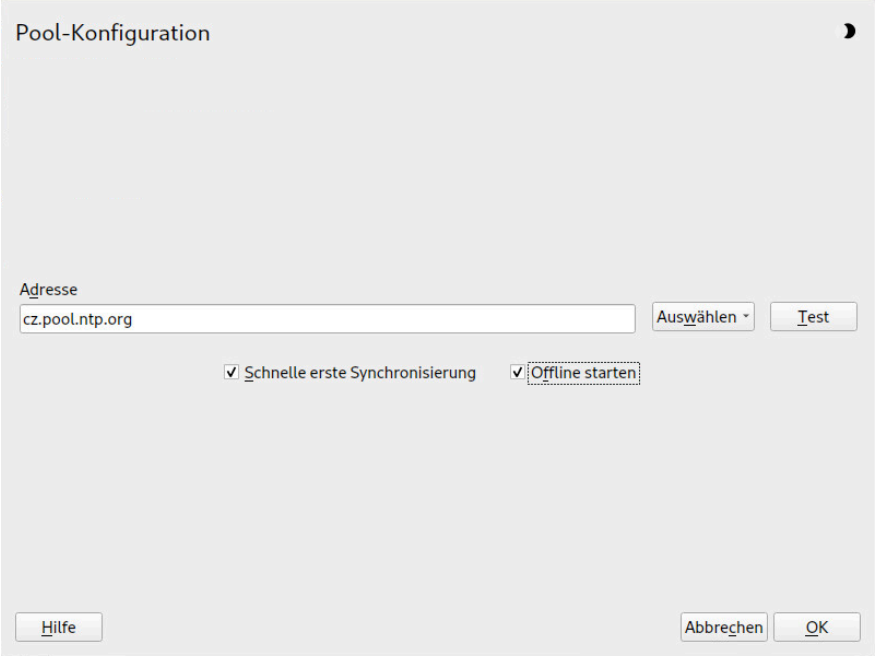


ABBILDUNG 39.2: HINZUFÜGEN EINES ZEITSERVERS

1. Geben Sie in das Feld *Adresse* die URL des Zeitservers oder des Zeitserver-Pools ein, mit dem die Computerzeit synchronisiert werden soll. Prüfen Sie mit *Test*, ob die eingegebene URL auf eine gültige Zeitquelle verweist.

2. Mit *Schnelle erste Synchronisierung* wird eine größere Anzahl von Anfragen beim Start des `chronyd`-Daemons gesendet, sodass die Zeitsynchronisierung beschleunigt wird.

3. Mit *Offline starten* beschleunigen Sie den Bootvorgang auf Systemen, auf denen der `chronyd`-Daemon automatisch gestartet wird und die beim Booten keine Internetverbindung besitzen. Diese Option eignet sich beispielsweise für Laptops, deren Netzwerkverbindungen über NetworkManager verwaltet werden.

4. Bestätigen Sie Ihre Auswahl mit *OK*.

39.2 Manuelle Konfiguration von NTP im Netzwerk

`chrony` liest die Konfiguration aus der Datei `/etc/chrony.conf` aus. Damit die Computeruhr synchronisiert bleibt, müssen Sie die zu verwendenden Zeitserver in `chrony` festlegen. Hierbei können Sie spezielle Servernamen oder IP-Adressen angeben, beispielsweise:

```
0.suse.pool.ntp.org
1.suse.pool.ntp.org
2.suse.pool.ntp.org
3.suse.pool.ntp.org
```

Sie können auch den Namen für einen *Pool* angeben. Der Poolname wird in mehrere IP-Adressen aufgelöst:

```
pool pool.ntp.org
```

Tipp: Computer im selben Netzwerk

Soll die Zeit auf mehreren Computern in demselben Netzwerk synchronisiert werden, sollten Sie nicht alle Computer mit einem externen Server synchronisieren. Ein bewährtes Verfahren besteht darin, einen Computer als Zeitserver, der mit einem externen Zeitserver synchronisiert wird, und die anderen Computer als die Clients dieses Computers festzulegen. Fügen Sie eine `local`-Direktive zur Datei `/etc/chrony.conf` des Servers hinzu, sodass dieser Server von einem autoritativen Zeitserver unterschieden wird:

```
local stratum 10
```

Starten Sie `chrony` mit dem folgenden Befehl:

```
systemctl start chronyd.service
```

Nach der Initialisierung von `chronyd` dauert es eine gewisse Zeit, bis die Zeit sich stabilisiert und die Drift-Datei zum 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.

Aktivieren Sie den Dienst, sodass `chrony` automatisch beim Booten gestartet wird, mit dem folgenden Befehl:

```
systemctl enable chronyd.service
```

Warnung: Konflikt mit dem Dienst `yast-timesync.service`

Neben dem Dienst `chronyd.service` umfasst SUSE Linux Enterprise Desktop auch `yast-timesync.service`. `yast-timesync.service` wird alle 5 Minuten durch einen Zeitgeber ausgelöst. Der Dienst führt `chronyd` mit der Option `-q` aus, um die Systemzeit festzulegen, und wird anschließend beendet. Da immer nur eine Instanz von `chronyd` ausgeführt werden kann, sollten Sie nicht beide `chronyd`-bezogenen Dienste gleichzeitig aktivieren oder starten.

39.3 Konfigurieren von NTS

Das Network Time Protocol (NTP) ist ein Protokoll, das zum Synchronisieren und Aufrechterhalten der genauen Systemzeit eines oder mehrerer Hosts im Netzwerk verwendet wird. In diesem Artikel wird beschrieben, wie Sie Sicherheit von NTP mittels Network Time Security (NTS) sicherstellen können.

Das NTP-Protokoll bietet keinen Sicherheitsmechanismus, der die Kommunikation zwischen dem Zeitserver und dem Client authentifiziert und verschlüsselt. Network Time Security (NTS) ist eine Erweiterung, die die Sicherheit von NTP verbessert. `chrony` unterstützt NTS und kann Zeitquellen authentifizieren und vor bestimmten Netzwerkangriffen schützen.

Im Folgenden wird beschrieben, wie Sie den Zeitserver und den Client-Rechner für eine sichere Zeitsynchronisation konfigurieren.

VORGEHEN 39.1: KONFIGURIEREN DES NTS-ZEITSERVERS

1. *(Optional)* Es ist ratsam, den Zeitserver so zu konfigurieren, dass er seine Uhrzeit über NTS aktualisiert. Dies gewährleistet eine sichere Zeitsynchronisierung ab dem Beginn der Synchronisierungskette. Kommentieren Sie alle in `/etc/chrony.conf` vorhandenen Zeitquellen aus, die NTS nicht unterstützen, und fügen Sie mindestens eine Zeitquelle hinzu, die NTS unterstützt. Beispiel:

```
server time.cloudflare.com iburst nts
```

Tipp

Die Option `nts` fordert eine NTS-Verbindung an, wenn diese verfügbar ist. Wenn NTS nicht verfügbar ist, findet ein Fallback auf NTP statt.

2. Starten Sie den `chronyd`-Dienst neu.

```
> sudo systemctl restart chronyd.srvice
```

3. Überprüfen Sie die konfigurierten Zeitquellen.

```
> chronyc sources -v
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^? time.cloudflare.com           3   6     1     2   -947ms[ -947ms] +/-   12ms
^? pyrrha.fi.muni.cz             2   6     1     1   -948ms[ -948ms] +/-   39ms
^* whitesoft-intex16.c.cbsn>     1   6     1     2   -948ms[ -948ms] +/- 5444us
^? mail.combatostrich.dev        2   6     1     1   -948ms[ -948ms] +/-   28ms
```

Anmerkung

In der mit `^*` beginnenden Zeile steht die Zeitquelle, die als beste Quelle ausgewählt wurde.

Überprüfen Sie, ob die konfigurierte Zeitquelle den NTS-Modus verwendet.

```
> chronyc -N authdata
Name/IP address             Mode KeyID Type KLen Last Atmp  NAK Cook CLen
=========================================================================
[...]
time.cloudflare.com          NTS     1   15  256    3    0    0    8   96
```

4. Vergewissern Sie sich, dass die Serverkonfiguration die Option `allow` enthält, mit der festgelegt wird, welche Clients die Zeit mit dem Zeitserver synchronisieren können. Beispiel:

```
allow 192.168.1.0/24
```

5. *(Optional)* Wenn der Zeitserver hinter einer Firewall ausgeführt wird, erlauben Sie die Kommunikation über die Ports für NTP und NTS. Standardmäßig sind dies die Ports 123 und 4460.

6. Besorgen Sie sich ein TLS-Zertifikat und einen entsprechenden privaten Schlüssel und kopieren Sie diese in `/var/lib/chrony/`. Stellen Sie sicher, dass sie von `chrony` gelesen werden können, z. B.:

```
> sudo install -m 0440 -o chrony -g chrony nts.key /var/lib/chrony/
> sudo install -m 0440 -o chrony -g chrony nts.crt /var/lib/chrony/
```

Tipp

Ausführliche Informationen zu TLS-Zertifikaten finden Sie in einem Artikel zum Thema (https://documentation.suse.com/smart/security/html/tls-certificates/index.html).

7. Bearbeiten Sie `/etc/chrony.conf` und stellen Sie sicher, dass die Option `ntsdumpdir /var/lib/chrony` aktiviert ist. Hängen Sie dann die Pfade an den TLS-Schlüssel und das Zertifikat an.

```
ntsdumpdir /var/lib/chrony
ntsserverkey /var/lib/chrony/nts.key
ntsservercert /var/lib/chrony/nts.crt
```

8. Starten Sie den `chronyd`-Dienst neu.

```
> sudo systemctl restart chronyd.service
```

VORGEHEN 39.2: KONFIGURIEREN VON NTS-CLIENTS

1. Deaktivieren Sie vorhandene NTP-Quellen. Beispiel:

```
#server 192.168.1.1 iburst
```

   Die Konfigurationen der Quellen befinden sich in `/etc/chrony.conf` oder in Dateien unter `/etc/chrony.d/`.

2. Der Client-Host muss der Root-CA vertrauen, die das TLS-Zertifikat signiert hat. Weitere Informationen zur Verwaltung des CA-Zertifikatspeichers finden Sie in einem Artikel zum Thema (https://documentation.suse.com/smart/security/html/tls-certificates/index.html#tls-certificates-store).

3. Fügen Sie die Quelle des NTS-Zeitservers, die Sie in *Prozedur 39.1, „Konfigurieren des NTS-Zeitservers“* konfiguriert haben, zur Konfiguration des Clients `chrony` in `/etc/chrony.conf` hinzu. Beispiel:

```
server nts1.example.com iburst nts
```

4. Starten Sie den `chronyd`-Dienst neu.

```
> sudo systemctl restart chronyd.service
```

5. Überprüfen Sie die konfigurierten Zeitquellen auf dem Client und stellen Sie sicher, dass die Verbindung authentifiziert ist.

```
> sudo chronyc sources -v
> sudo chronyc -N authdata
```

6. Überprüfen Sie auf dem NTS-Zeitserver die Client-Statistiken im Hinblick auf NTS-Verbindungen.

```
> sudo chronyc -N clients -k
```

39.4 Konfigurieren von `chronyd` zur Laufzeit mit `chronyc`

Mit **`chronyc`** können Sie das Verhalten von `chronyd` zur Laufzeit verändern. Hiermit werden außerdem Statusberichte zum Betrieb von `chronyd` erzeugt.

Sie können **`chronyc`** wahlweise im interaktiven oder im nicht interaktiven Modus ausführen. Soll **`chronyc`** interaktiv ausgeführt werden, geben Sie **`chronyc`** in die Befehlszeile ein. Eine Eingabeaufforderung wird angezeigt und das System wartet auf Ihre Kommandoeingabe. Mit dem folgenden Befehl prüfen Sie beispielsweise, wie viele NTP-Quellen online oder offline sind:

```
# chronyc
chronyc> activity
200 OK
4 sources online
2 sources offline
1 sources doing burst (return to online)
1 sources doing burst (return to offline)
0 sources with unknown address
```

Mit **`quit`** oder **`exit`** schließen Sie die **`chronyc`**-Eingabeaufforderung.

Falls Sie keine interaktive Eingabeaufforderung benötigen, geben Sie den Befehl direkt ein:

```
# chronyc activity
```

Anmerkung: Temporäre Änderungen

Die mit **chronyc** vorgenommenen Änderungen sind nicht dauerhaft. Sie gehen nach dem nächsten Neustart von chronyd verloren. Sollen dauerhafte Änderungen erfolgen, bearbeiten Sie /etc/chrony.conf.

Eine vollständige Liste der **chronyc**-Befehle finden Sie auf der Man-Seite (**man 1 chronyc**).

39.5 Dynamische Zeitsynchronisierung während der Laufzeit

chronyd wird zwar auf einem System, das ohne Netzwerkverbindung bootet, normal ausgeführt, kann jedoch nicht die DNS-Namen der in der Konfigurationsdatei angegebenen Zeitserver auflösen.

chronyd versucht in immer größeren Zeitabständen, die in den server-, pool- und peer-Direktiven angegebenen Zeitservernamen aufzulösen, bis die Auflösung erfolgreich ist.

Falls der Zeitserver beim Starten von chronyd nicht erreichbar sein wird, können Sie die Option offline angeben:

```
server server_address offline
```

Hiermit ruft chronyd den Server erst nach Aktivierung mit dem folgenden Kommando ab:

```
# chronyc online server_address
```

Wenn die Option auto_offline eingestellt ist, nimmt chronyd an, dass der Zeitserver offline geschaltet wurde, sobald zwei Anfragen ohne Antwort gesendet wurden. Mit dieser Option müssen Sie nicht mehr den Befehl offline über **chronyc** ausführen, wenn Sie die Netzwerkverbindung trennen.

39.6 Einrichten einer lokalen Referenzuhr

Das Software-Paket chrony greift auf andere Programme (z. B. gpsd) zurück, die die Zeitgebungsdaten über den SHM- oder SOCK-Treiber abrufen. Geben Sie mit der refclock-Direktive in /etc/chrony.conf eine Hardware-Referenzuhr als Zeitquelle an. Hierbei sind zwei Parameter

obligatorisch, zum einen der Treibername und zum anderen ein treiberspezifischer Parameter. Nach den beiden Parametern können bei Bedarf noch `refclock`-Optionen angegeben werden. `chronyd` umfasst folgende Treiber:

- PPS – Treiber für die Kernel-API `pulse per second`. Beispiel:

```
refclock PPS /dev/pps0 lock NMEA refid GPS
```

- SHM – Treiber für den gemeinsam genutzten NTP-Speicher. Beispiel:

```
refclock SHM 0 poll 3 refid GPS1
refclock SHM 1:perm=0644 refid GPS2
```

- SOCK – Treiber für den Unix-Domänen-Socket. Beispiel:

```
refclock SOCK /var/run/chrony.ttyS0.sock
```

- PHC – Treiber für die PTP-Hardware-Uhr. Beispiel:

```
refclock PHC /dev/ptp0 poll 0 dpoll -2 offset -37
refclock PHC /dev/ptp1:nocrossts poll 3 pps
```

Weitere Informationen zu den Optionen der einzelnen Treiber finden Sie auf der man-Seite **`man 8 chrony.conf`**.

39.7 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 Befehle als `root` aus:

```
echo 1 > /sys/devices/system/etr/etr0/online
```

```
echo 1 > /sys/devices/system/etr/etr1/online
```

VI Fehlersuche

40 Hilfe und Dokumentation 548

41 Erfassen der Systeminformationen für den Support 553

42 Häufige Probleme und deren Lösung 586

40 Hilfe und Dokumentation

Im Lieferumfang von SUSE® Linux Enterprise Desktop sind verschiedene Informationen und Dokumentationen enthalten, die online verfügbar oder in Ihr installiertes System integriert sind.

Produktdokumentation

Eine ausführliche Dokumentation für SUSE Linux Enterprise Desktop finden Sie unter https://documentation.suse.com/#sled. Die behandelten Themen reichen unter anderem von Bereitstellung, Upgrade und Systemadministration bis hin zu Virtualisierung, Systemoptimierung und Sicherheit.

Dokumentation in `/usr/share/doc`

Dieses Verzeichnis enthält Versionshinweise für Ihr System (im Unterverzeichnis `release-notes`). Außerdem enthält es Informationen über die im Unterverzeichnis `packages` installierten Pakete. Weitere Informationen finden Sie unter *Abschnitt 40.1, „Dokumentationsverzeichnis“*.

man-Seiten und Infoseiten für Shell-Befehle

Wenn Sie mit der Shell arbeiten, brauchen Sie die Optionen der Befehle nicht auswendig zu kennen. Die Shell bietet normalerweise eine integrierte Hilfefunktion mit man-Seiten und Infoseiten. Weitere Informationen dazu finden Sie unter *Abschnitt 40.2, „Man Pages“* und *Abschnitt 40.3, „Infoseiten“*.

Desktop-Hilfezentrum

Das Hilfezentrum des GNOME-Desktops (Hilfe) bietet zentralen Zugriff auf die GNOME-Desktop-Dokumentation.

Separate Hilfepakete für bestimmte 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 bestimmte Anwendungen, beispielsweise GIMP, über andere Online-Hilfepakete verfügen, die separat mit YaST installiert werden können und nicht in die Hilfe integriert werden.

40.1 Dokumentationsverzeichnis

Das traditionelle Verzeichnis zum Suchen von Dokumentationen in Ihrem installierten Linux-System finden Sie unter `/usr/share/doc`. Das Verzeichnis enthält die Versionshinweise und Informationen zu den auf Ihrem System installierten Paketen sowie Handbücher und mehr.

Anmerkung: Inhalte sind 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/doc` 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.

40.1.1 Versionshinweise

Wir bieten HTML-, PDF-, RTF- und Textversionen der Versionshinweise zu SUSE Linux Enterprise Desktop. Sie stehen auf Ihrem installierten System unter `/usr/share/doc/release-notes/` oder online auf Ihrer produktspezifischen Webseite unter https://www.suse.com/release-notes/index.html zur Verfügung.

40.1.2 Dokumentation zu den einzelnen Paketen

Im Verzeichnis `packages` befindet sich die Dokumentation zu den auf Ihrem System installierten Software-Paketen. Für jedes Paket wird ein Unterverzeichnis mit dem Namen `/usr/share/doc/packages/`*`PACKAGENAME`* 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 nur einige davon.

`AUTHORS`
: 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. Sie ist für Entwickler interessant, weil sie detaillierte Angaben enthält.

`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. Zum Beispiel, zu welchem Zweck und wie sie verwendet wird.

`TODO`
: Für die Zukunft geplante Funktionen.

`MANIFEST`
: Diese Datei enthält eine Übersicht über die im Paket enthaltenen Dateien.

`NEWS`
: Beschreibung der Neuerungen in dieser Version.

40.2 Man Pages

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. Mit `Q` schließen Sie die Manpages. Weitere Informationen über den Befehl **`man`** erhalten Sie durch Eingabe von **`man man`**. man-Seiten sind in Kategorien unterteilt, wie in *Tabelle 40.1, „Manpages – Kategorien und Beschreibungen“* gezeigt (diese Einteilung wurde direkt von der man-Seite für den Befehl „man“ übernommen).

TABELLE 40.1: MANPAGES – 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 (gewöhnlich nur für `root`)
9	Nicht standardgemäße Kernel-Routinen

Jede Manpage besteht aus verschiedenen Teilen, die als *NAME*, *SYNOPSIS*, *DESCRIPTION*, *SEE ALSO*, *LICENSING* und *AUTHOR* bezeichnet werden. Je nach Befehlstyp stehen möglicherweise auch weitere Abschnitte zur Verfügung.

40.3 Infoseiten

Eine weitere wichtige Informationsquelle sind Infoseiten. Diese sind in der Regel ausführlicher als Manpages. Hier finden Sie nicht nur die Befehlszeilenoptionen, 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 jeden Befehl gibt es eine Infoseite und umgekehrt.

40.4 Online-Ressourcen

Eine Übersicht über alle Dokumentationen für SUSE Linux Enterprise Desktop erhalten Sie auf den produktspezifischen Dokumentations-Webseiten unter https://documentation.suse.com/.

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 https://www.suse.com/support/ bereit.

Benutzer-Community

SUSE und Rancher Community (https://www.rancher.com/community)

SUSE-Blog

Im SUSE-Blog finden Sie Artikel, Tipps sowie Fragen und Antworten: https://www.suse.com/c/blog/

GNOME-Dokumentation

Dokumentation für GNOME-Benutzer, -Administratoren und -Entwickler finden Sie unter https://help.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 https://tldp.org/). Es ist eine umfassende 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 Desktop verfügbar.

41 Erfassen der Systeminformationen für den Support

Das Paket `hostinfo` in SUSE Linux Enterprise Desktop 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 hochladen. 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 Desktop bietet hierzu eine Anwendung und ein Kommandozeilenwerkzeug für die `Supportconfig Analysis` (SCA).

41.1 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 41.1: AUSGABE VON **`hostinfo`** BEIM ANMELDEN ALS `root`

```
Welcome to SUSE Linux Enterprise Server 15 SP2 Snapshot8 (x86_64) - Kernel \r (\l).


Distribution:             SUSE Linux Enterprise Server 15 SP7
Current As Of:            Mon 11 March 2024 10:11:51 AM CET
Hostname:                 localhost
Kernel Version:           6.4.0-150700.38-default
```

```
 Architecture:            x86_64
 Installed:               Fri 08 March 2024 04:45:50 PM CET
 Status:                  Not Tainted
Last Installed Package:   Mon 11 March 2024 10:02:13 AM CET
 Patches Needed:          0
 Security:                0
 3rd Party Packages:      6
Network Interfaces
 eth0:                    192.168.2/24 2002:c0a8:20a::/64
Memory
 Total/Free/Avail:        7.4Gi/6.4Gi/6.8Gi (91% Avail)
CPU Load Average:         7 (3%) with 2 CPUs
```

Wenn die Ausgabe auf den Kernel-Status `tainted` (unbrauchbar) hinweist, finden Sie weitere Details in *Abschnitt 41.6, „Unterstützung für Kernelmodule“*.

41.2 Erfassen von Systeminformationen mit supportconfig

Ein TAR-Archiv mit ausführlichen Systeminformationen, die Sie an den globalen technischen Support übertragen können, erstellen Sie entweder:

- mit dem Befehl **`supportconfig`** oder
- mit dem YaST-*Support*-Modul.

Das Befehlszeilenwerkzeug wird im Paket `supportutils` bereitgestellt, das standardmäßig installiert ist. Das YaST-*Support*-Modul baut zudem auf dem Kommandozeilenwerkzeug auf.

Bestimmte Pakete integrieren Supportconfig-Plugins. Beim Ausführen von Supportconfig werden auch alle Plugins ausgeführt, wobei mindestens eine Ergebnisdatei für das Archiv erstellt wird. Der Vorteil ist, dass nur Themen mit einem bestimmten Plugin geprüft werden. Die Supportconfig-Plugins werden im Verzeichnis `/usr/lib/supportconfig/plugins/` gespeichert.

41.2.1 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 zum Support hochladen zu können.

Zum Erstellen einer Service-Anforderung, wechseln Sie zu https://scc.suse.com/support/requests, und befolgen Sie die Anweisungen auf dem Bildschirm. Notieren Sie die Serviceanforderungsnummer.

Anmerkung: Datenschutzerklärung

SUSE behandelt Systemberichte als vertrauliche Daten. Weitere Informationen zum Datenschutz finden Sie unter https://www.suse.com/company/policies/privacy/.

41.2.2 Upload-Ziele

Sobald Sie eine Service-Anforderungs-Nummer erstellt haben, können Sie Ihre Supportconfig-Archive gemäß den Anweisungen in *Prozedur 41.1, „Übertragen von Informationen an den Support mithilfe von YaST“* oder *Prozedur 41.2, „Übertragen von Informationen an den Support über die Befehlszeile“* an den globalen technischen Support hochladen. Verwenden Sie eines der folgenden Upload-Ziele:

- Nordamerika: FTP ftp://support-ftp.us.suse.com/incoming/
- EMEA (Europa, Nahost und Afrika): FTP ftp://support-ftp.emea.suse.com/incoming

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.

41.2.3 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.

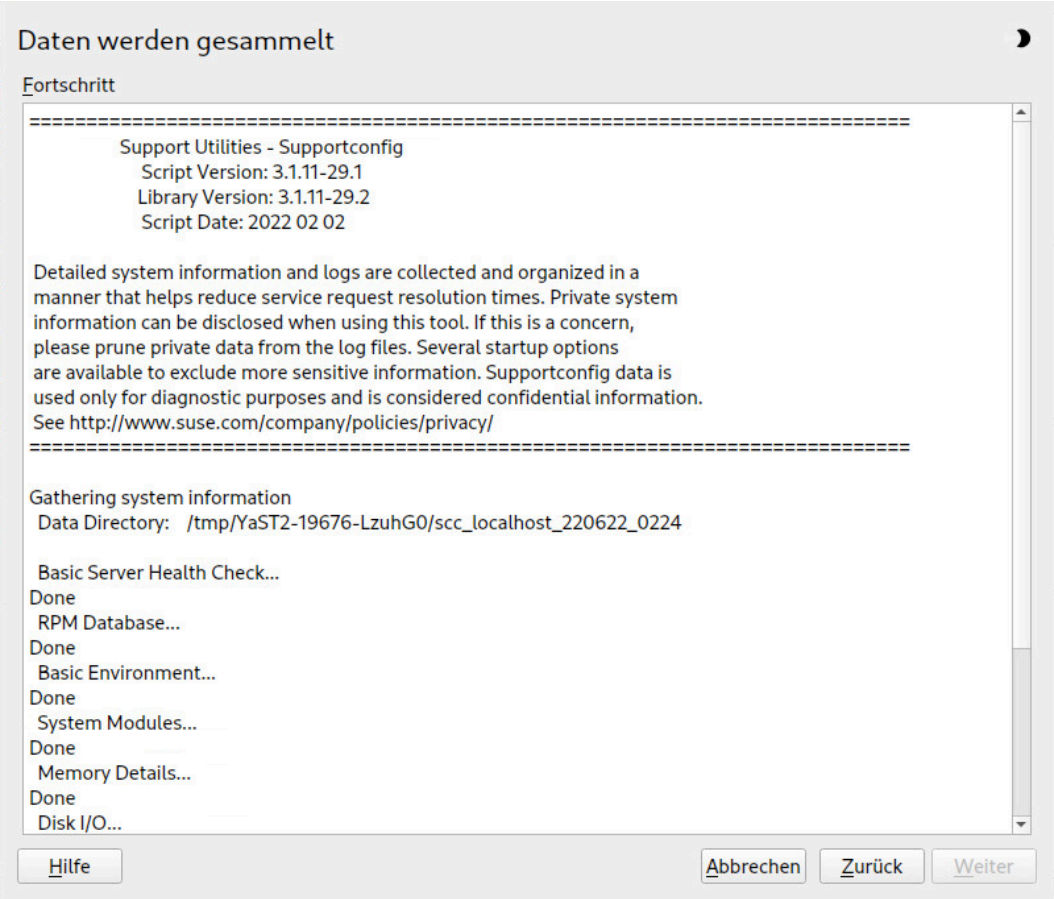
2. Klicken Sie auf *Berichts-Tarball erstellen*.

3. Wählen Sie im nächsten Fenster eine der Supportconfig-Optionen in der Optionsliste aus. Die Option *Benutzerdefinierte Einstellungen (für Experten) verwenden* ist standardmäßig aktiviert. Um die Berichtfunktion zuerst zu testen, verwenden Sie *Nur eine minimale Anzahl von Informationen sammeln*. Zusätzliche Informationen zu den weiteren Optionen finden Sie auf der man-Seite zu **`supportconfig`**.
   Klicken Sie auf *Weiter*.

4. Geben Sie Ihre Kontaktdaten ein. Sie sind in der Datei `basic-environment.txt` gespeichert und im erstellten Archiv enthalten.

5. Geben Sie zum Senden des Archivs an den globalen technischen Support die erforderlichen *Upload-Informationen* an. YaST schlägt automatisch einen Upload-Server vor. Falls Sie einen anderen verwenden möchten, finden Sie detaillierte Informationen zu den verfügbaren Upload-Servern in *Abschnitt 41.2.2, „Upload-Ziele“*.
   Lassen Sie das Feld für *Upload-Informationen* leer, falls Sie das Archiv später senden möchten.

6. Klicken Sie zum Starten des Vorgangs der Informationserfassung auf *Weiter*.



Klicken Sie nach Ende des Vorgangs auf *Weiter*.

7. Wählen Sie zum Prüfen der erfassten Daten die gewünschte Datei unter *Dateiname* aus, um den Inhalt in YaST anzuzeigen. Mit der Option *Aus Daten entfernen* entfernen Sie eine Datei aus dem TAR-Archiv, bevor Sie es an den Support senden. Klicken Sie auf *Weiter*.

8. Speichern Sie das TAR-Archiv. Wenn Sie das YaST-Modul als `root`-Benutzer gestartet haben, fordert YaST Sie standardmäßig dazu auf, das Archiv unter `/var/log` zu speichern (ansonsten in Ihrem Basisverzeichnis). Der Dateiname hat das Format `scc_HOST_DATE_TIME.tbz`.

9. Zum Heraufladen des Archivs direkt an den Support muss die Option *Protokolldatei-Tarball an URL hochladen* aktiviert sein. Hier ist das *Upload-Ziel* angegeben, das YaST in *Schritt 5* vorgeschlagen hat. Prüfen Sie in *Abschnitt 41.2.2, „Upload-Ziele“*, welche Upload-Server verfügbar sind, bevor Sie das Upload-Ziel ändern.

10. Deaktivieren Sie die Option *Protokolldatei-Tarball zu URL hochladen*, um den Upload zu überspringen.

11. Bestätigen Sie die Änderungen, um das YaST-Modul zu schließen.

41.2.4 Erstellen eines supportconfig-Archivs über die Befehlszeile

Mit dem nachstehenden Verfahren erstellen Sie ein Supportconfig-Archiv, ohne das Archiv direkt an den Support zu übertragen. Zum Heraufladen müssen Sie daen entsprechenden Befehl mit den zugehörigen Optionen ausführen (siehe *Prozedur 41.2, „Übertragen von Informationen an den Support über die Befehlszeile“*).

1. Öffnen Sie eine Shell und melden Sie sich als `root` an.
2. Führen Sie **`supportconfig`**. Es reicht aus, dieses Werkzeug ohne Optionen auszuführen. Die gängigsten Optionen werden jedoch in der folgenden Liste aufgeführt:

   `-E` *`MAIL`*,
   `-N` *`NAME`*,
   `-O` *`COMPANY`*,
   `-P` *`PHONE`*
   : Legt Ihre Kontaktangaben fest: Email-Adresse (`-E`), Unternehmensname (`-O`), Ihr Name (`-N`) und Ihre Telefonnummer (`-P`).

   `-i` *`KEYWORDS`*,
   `-F`
   : Schränkt die zu überprüfenden Funktionen ein. Der Platzhalter *`KEYWORDS`* steht für eine Liste von Schlüsselwörtern, die jeweils durch Komma voneinander getrennt werden müssen und bei denen zwischen Groß- und Kleinschreibung unterschieden wird. Mit **`supportconfig -F`** erhalten Sie eine Liste aller Schlüsselwörter.

   `-r` *`SRNUMBER`*
   : Definiert die Nummer Ihrer Service-Anforderung, wenn Sie das erzeugte TAR-Archiv hochladen.

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 `scc_`*`HOST_DATE_TIME`*`.tbz`.

41.2.5 Informationen zur Ausgabe von `supportconfig`

`supportconfig` gibt eine Zusammenfassung der erledigten Aktionen zurück, unabhängig davon, ob Sie das Skript über YaST oder direkt ausführen.

```
                     Support Utilities - Supportconfig
                          Script Version: 3.0-98
                          Script Date: 2017 06 01
[...]
Gathering system information
  Data Directory:    /var/log/scc_d251_180201_1525 ❶

  Basic Server Health Check...                 Done ❷
  RPM Database...                              Done ❷
  Basic Environment...                         Done ❷
  System Modules...                            Done ❷
[...]
  File System List...                          Skipped ❸
[...]
  Command History...                           Excluded ❹
[...]
  Supportconfig Plugins:                       1 ❺
    Plugin: pstree...                          Done
[...]
Creating Tar Ball

==[ DONE ]=====================================================================
  Log file tar ball: /var/log/scc_d251_180201_1525.txz ❻
  Log file size:     732K
  Log file md5sum:   bf23e0e15e9382c49f92cbce46000d8b
================================================================================
```

❶ Das temporäre Verzeichnis, in dem die Ergebnisse gespeichert werden. Dieses Verzeichnis wird als tar-Datei archiviert (siehe ❻).

❷ Die Funktion wurde (standardmäßig oder manuell) aktiviert und wurde erfolgreich ausgeführt. Das Ergebnis wird in einer Datei gespeichert (siehe *Tabelle 41.1, „Vergleich der Funktionen und Dateinamen im TAR-Archiv“*).

❸ Die Funktion wurde übersprungen, weil Dateien in mindestens einem RPM-Paket geändert wurden.

❹ Die Funktion wurde ausgeschlossen, weil ihre Auswahl mit der Option `-x` aufgehoben wurde.

5. Das Skript hat ein Plugin gefunden und führt das Plugin **`pstree`** aus. Das Plugin wurde im Verzeichnis `/usr/lib/supportconfig/plugins/` gefunden. Weitere Informationen hierzu finden Sie auf der man-Seite.
6. Der tar-Dateiname des Archivs, das standardmäßig mit **`xz`** komprimiert wird.

41.2.6 Allgemeine Optionen für Supportconfig

Das Dienstprogramm **`supportconfig`** wird in der Regel ohne Optionen aufgerufen. Zeigen Sie eine Liste aller Optionen mit **`supportconfig`** `-h` an oder lesen Sie die Manpage. Die folgende Liste enthält eine kurze Übersicht gängiger Fälle:

Vermindern des Umfangs der erfassten Informationen

Verwenden Sie die Minimal-Option (`-m`):

```
> sudo supportconfig -m
```

Begrenzen der Informationen auf ein bestimmtes Thema

Wenn Sie bereits ein Problem festgestellt haben, das auf einen bestimmten Bereich oder eine bestimmte Funktionsgruppe beschränkt ist, sollten Sie die erfassten Informationen beim nächsten Ausführen von **`supportconfig`** auf diesen Bereich begrenzen. Sie haben beispielsweise Probleme mit LVM festgestellt und möchten nun eine Änderung testen, die Sie kürzlich an der LVM-Konfiguration vorgenommen haben. In diesem Fall sollten Sie nur die mindestens erforderlichen Supportconfig-Informationen zu LVM zusammenstellen:

```
> sudo supportconfig -i LVM
```

Zusätzliche Schlüsselwörter können jeweils durch Komma getrennt werden. Beispielsweise ein zusätzlicher Festplattentest:

```
> sudo supportconfig -i LVM,DISK
```

Eine vollständige Liste der Funktionsschlüsselwörter, mit denen Sie die erfassten Informationen auf einen bestimmten Bereich begrenzen, erhalten Sie mit dem:

```
> sudo supportconfig -F
```

Aufnehmen zusätzlicher Kontaktinformationen in die Ausgabe:

```
> sudo supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

(alle in einer Zeile)

Sammeln von bereits rotierten Protokolldateien

```
> sudo supportconfig -l
```

Nützlich ist dies insbesondere in Umgebungen mit hohem Protokollierungsaufkommen sowie nach einem Kernel-Crash, wenn syslog die Protokolldateien nach dem Neustart rotiert.

41.2.7 Überblick über den Archivinhalt

Das TAR-Archiv enthält alle Ergebnisse der Funktionen. Der Funktionssatz kann mit der Option `-i` eingeschränkt werden (siehe *Abschnitt 41.2.6, „Allgemeine Optionen für Supportconfig“*).

Mit dem folgenden **`tar`**-Befehl rufen Sie eine Liste des Archivinhalts ab:

```
# tar xf /var/log/scc_earth_180131_1545.tbz
```

Die folgenden Dateinamen sind stets im TAR-Archiv verfügbar:

MINDESTENS IM ARCHIV ENTHALTENE DATEIEN

`basic-environment.txt`
: Datum, an dem dieses Skript ausgeführt wurde, sowie Systeminformationen wie die Version der Distribution, Hypervisor-Informationen und vieles mehr.

`basic-health-check.txt`
: Grundlegende Integritätsprüfungen, z. B. Betriebszeit, Statistiken zum virtuellen Speicher, freier Arbeits- und Festplattenspeicher, Prüfungen auf „Zombie-Prozesse“ und vieles mehr.

`hardware.txt`
: Grundlegende Hardware-Prüfungen, z. B. Informationen zur CPU-Active Directory, Liste der gesamten angeschlossenen Hardware, Interrupts, E/A-Ports, Kernel-Bootmeldungen und vieles mehr.

`messages.txt`
: Enthält Protokollmeldungen vom Systemjournal.

`rpm.txt`
: Liste aller installierten RPM-Pakete mit Name, Ursprung und Version.

`summary.xml`
: Informationen im XML-Format, z. B. Distribution, Version und produktspezifische Fragmente.

`supportconfig.txt`

Informationen zum Skript **`supportconfig`** selbst.

`y2log.txt`

YaST-spezifische Informationen, z. B. spezielle Pakete, Konfigurationsdateien und Protokolldateien.

Tabelle 41.1, „Vergleich der Funktionen und Dateinamen im TAR-Archiv“ zeigt eine Liste aller verfügbaren Funktionen und ihrer Dateinamen. Weitere Service Packs und Plugins können die Liste noch erweitern.

TABELLE 41.1: VERGLEICH DER FUNKTIONEN UND DATEINAMEN IM TAR-ARCHIV

Funktion	Dateiname
APPARMOR	security-apparmor.txt
AUDIT	security-audit.txt
AUTOFS	fs-autofs.txt
BOOT	boot.txt
BTRFS	fs-btrfs.txt
DAEMONS	systemd.txt
CIMOM	cimom.txt
CRASH	crash.txt
CRON	cron.txt
DHCP	dhcp.txt
DISK	fs-diskio.txt
DNS	dns.txt
DOCKER	docker.txt
DRBD	drbd.txt
ENV	env.txt
ETC	etc.txt

Funktion	Dateiname
HA	ha.txt
HAPROXY	haproxy.txt
HISTORY	shell_history.txt
IB	ib.txt
IMAN	novell-iman.txt
ISCSI	fs-iscsi.txt
LDAP	ldap.txt
LIVEPATCH	kernel-livepatch.txt
LVM	lvm.txt
MEM	memory.txt
MOD	modules.txt
MPIO	mpio.txt
NET	network-*.txt
NFS	nfs.txt
NTP	ntp.txt
NVME	nvme.txt
OCFS2	ocfs2.txt
OFILES	open-files.txt
PRINT	print.txt
PROC	proc.txt
SAR	sar.txt
SLERT	slert.txt
SLP	slp.txt

Funktion	Dateiname
SMT	smt.txt
SMART	fs-smartmon.txt
SMB	samba.txt
SRAID	fs-softraid.txt
SSH	ssh.txt
SSSD	sssd.txt
SYSCONFIG	sysconfig.txt
SYSFS	sysfs.txt
TRANSACTIONAL	transactional-update.txt
TUNED	tuned.txt
UDEV	udev.txt
UFILES	fs-files-additional.txt
UP	updates.txt
WEB	web.txt
X	x.txt

41.3 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 Kommandozeilenprogramm **supportconfig**. Falls Serverprobleme auftreten und Sie Hilfe benötigen, müssen Sie zunächst eine Serviceanforderung öffnen. Weitere Informationen finden Sie in *Abschnitt 41.2.1, „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 41.2.1, „Erstellen einer Serviceanforderungsnummer“* erstellt haben.

VORGEHEN 41.1: ÜBERTRAGEN VON INFORMATIONEN AN DEN SUPPORT MITHILFE VON YAST

Im nachfolgenden Verfahren wird angenommen, dass Sie bereits ein Supportconfig-Archiv erstellt, jedoch noch nicht hochgeladen haben. Nehmen Sie in jedem Fall Ihre Kontaktdaten in das Archiv auf (siehe *Abschnitt 41.2.3, „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 41.2.3, „Erstellen eines supportconfig-Archivs mit YaST“*.

1. Starten Sie YaST und öffnen Sie das *Support*-Modul.
2. Klicken Sie auf *Hochladen*.
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. Falls Sie einen anderen verwenden möchten, finden Sie detaillierte Informationen zu den verfügbaren Upload-Servern in *Abschnitt 41.2.2, „Upload-Ziele“*.

Fahren Sie mit *Weiter* fort.

5. Klicken Sie auf *Finish* (Fertigstellen).

VORGEHEN 41.2: ÜBERTRAGEN VON INFORMATIONEN AN DEN SUPPORT ÜBER DIE BEFEHLSZEILE

Im nachfolgenden Verfahren wird angenommen, dass Sie bereits ein Supportconfig-Archiv erstellt, jedoch noch nicht hochgeladen haben. Weitere Anweisungen zum Erzeugen und Übertragen eines Supportconfig-Archivs in einem einzigen Arbeitsgang finden Sie in *Abschnitt 41.2.3, „Erstellen eines supportconfig-Archivs mit YaST“*.

1. Server mit Internetkonnektivität:

   a. Führen Sie den folgenden Befehl aus, um das Standard-Uploadziel zu verwenden:

   ```
   > sudo supportconfig -ur 12345678901
   ```

   b. Verwenden Sie das folgende sichere Upload-Ziel:

   ```
   > sudo supportconfig -ar 12345678901
   ```

2. Server *ohne* Internetkonnektivität

   a. Führen Sie Folgendes aus:

   ```
   > sudo supportconfig -r 12345678901
   ```

   b. Laden Sie das Archiv `/var/log/scc_SR12345678901*tbz` manuell auf einen unserer FTP-Server hoch. Der richtige Server ist abhängig von Ihrem Standort. Einen Überblick finden Sie unter *Abschnitt 41.2.2, „Upload-Ziele“*.

3. Sobald das TAR-Archiv im Eingangsverzeichnis unseres FTP-Servers eingeht, wird es automatisch an Ihre Service-Anforderung angehängt.

41.4 Analysieren von Systeminformationen

Die mit **`supportconfig`** erstellten Systemberichte können auf bekannte Probleme hin analysiert werden, sodass die Fehlerbehebung noch beschleunigt wird. SUSE Linux Enterprise Desktop bietet hierzu eine Anwendung und ein Kommandozeilenwerkzeug für die `Supportconfig Analysis` (SCA). Die SCA-Appliance ist ein serverseitiges, nicht interaktives Werkzeug. Das SCA-Werk-

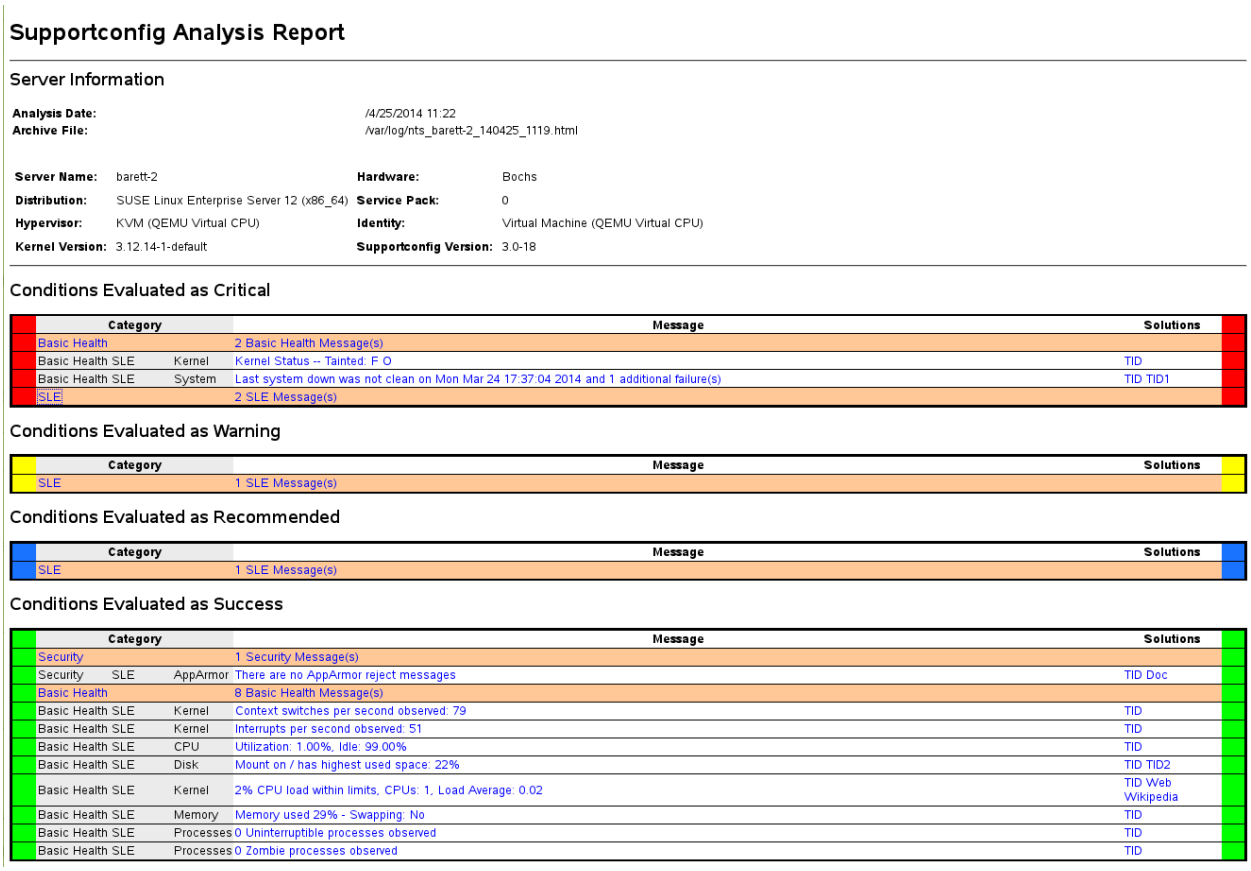
zeug (**scatool**, durch das Paket sca-server-report bereitgestellt) wird auf der Client-Seite über die Befehlszeile ausgeführt. Beide Werkzeuge analysieren die Supportconfig-Archive von betroffenen Servern. Die erste Serveranalyse erfolgt in der SCA-Appliance oder auf dem Arbeitsplatzrechner, auf dem **scatool** ausgeführt wird. Auf dem Produktionsserver werden keine Analysezyklen durchgeführt.

Sowohl für die Appliance als auch für das Befehlszeilenwerkzeug 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.

Sie können außerdem eigene Schemata entwickeln (kurze Beschreibung siehe *Abschnitt 41.4.3, „Entwickeln von benutzerdefinierten Analyseschemata“*).

41.4.1 SCA-Befehlszeilenwerkzeug

Mithilfe des SCA-Befehlszeilenwerkzeugs 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 41.1, „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 41.1: MIT DEM SCA-WERKZEUG ERSTELLTER HTML-BERICHT

Der Befehl **`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 der Befehl **`scatool`** ausgeführt werden soll.

Führen Sie den Befehl **`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 generieren und im gleichen Arbeitsgang analysieren. Das Werkzeug bietet außerdem eine interaktive Konsole zum Ausfüllen der Registerkarten. Sie können **`supportconfig`** auf einem externen Computer und die nachfolgende Analyse dann auf dem lokalen Computer ausführen.

Nachfolgend finden Sie einige Beispielbefehle:

`sudo scatool``-s`

Ruft **`supportconfig`** auf und generiert 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 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` *`PATH_TO_TARBALL_OR_DIR`*

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 dem 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 Befehle drücken Sie zweimal `↹` .

Führen Sie für weitere Optionen und Informationen den Befehl **`sudo scatool -h`** aus oder sehen Sie auf der **`scatool`**-Man-Seite nach.

41.4.2 SCA-Appliance

Wenn Sie die Supportconfig-Archive mit der SCA-Appliance analysieren, konfigurieren Sie einen dedizierten Server (oder einen dedizierten virtuellen Computer) als SCA-Appliance-Server. 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-Archi-

ve 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 in *Abschnitt 41.4.2.5.4, „Senden von SCA-Berichten per Email“*.

41.4.2.1 Kurzanleitung zur Installation

Zum schnellen Installieren und Einrichten der SCA-Appliance über die Befehlszeile führen Sie die folgenden Anweisungen aus. Das Verfahren richtet sich an fortgeschrittene Benutzer und umfasst lediglich die reinen Installations- und Einrichtungsbefehle. Weitere Informationen finden Sie in der detaillierteren Beschreibung in *Abschnitt 41.4.2.2, „Voraussetzungen“* bis *Abschnitt 41.4.2.3, „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.

VORGEHEN 41.3: 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 die folgenden Befehle aus (stellen Sie sicher, dass Sie die empfohlenen Pakete akzeptieren):

```
> sudo zypper install sca-appliance-* sca-patterns-* \
vsftpd yast2 yast2-ftp-server
> sudo systemctl enable apache2
> sudo systemctl start apache2
```

```
> sudo systemctl enable vsftpd
> sudo systemctl start vsftpd
> sudo 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:

```
> sudo systemctl enable mysql
> sudo systemctl start mysql
> sudo mysql_secure_installation
> sudo setup-sca -f
```

Bei der sicheren MySQL-Erstellung (mysql_secure_installation) wird ein `root`-Passwort für MariaDB erstellt.

VORGEHEN 41.4: 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:

```
> sudo zypper install sca-appliance-* sca-patterns-*
> sudo systemctl enable apache2
> sudo systemctl start apache2
> sudo sudo systemctl enable mysql
> sudo systemctl start mysql
> sudo mysql_secure_installation
> sudo setup-sca
```

41.4.2.2 Voraussetzungen

Zum Ausführen eines Appliance-Servers müssen folgende Voraussetzungen erfüllt sein:

- Alle Pakete `sca-appliance-*`.
- Das 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)

41.4.2.3 Installation und grundlegende Einrichtung

Wie in *Abschnitt 41.4.2.2, „Voraussetzungen“* beschrieben, bestehen mehrere Abhängigkeiten der SCA-Appliance von anderen Paketen. Daher müssen Sie vorbereitende Schritte ausführen, bevor Sie den SCA-Appliance-Server installieren und einrichten:

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).
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 41.5, „Installieren und Konfigurieren der SCA-Appliance“* installieren und einrichten.

VORGEHEN 41.5: 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 12 und SUSE Linux Enterprise 15 in Ihrer Umgebung befinden, installieren Sie sowohl das Paket `sca-patterns-sle12` als auch das Paket `sca-patterns-sle15`.
   So installieren Sie alle verfügbaren Pakete:

   ```
   > sudo 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 hochgeladen 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. Befolgen Sie die Anweisungen auf dem Bildschirm:

     ```
     > sudo setup-sca -f
     ```

     ### Anmerkung: FTP-Server mit anderem Verzeichnis

     Wenn Ihr FTP-Server ein anderes Verzeichnis als `/srv/ftp/upload` verwendet, passen Sie zuerst die folgenden Konfigurationsdateien an, damit sie auf das richtige Verzeichnis verweisen: `/etc/sca/sdagent.conf` und `/etc/sca/sdbroker.conf`

   - Sollen Supportconfig-Dateien mit `/tmp` in das Verzeichnis **`scp`** des SCA-Appliance-Servers hochgeladen werden, rufen Sie das Einrichtungsskript ohne Parameter auf. Befolgen Sie die Anweisungen auf dem Bildschirm:

     ```
     > sudo 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. Es wird in `/srv/www/htdocs/sca/web-config.php` geschrieben und als Passwort für den Benutzer `scdiag` festgelegt. Sowohl der Benutzername als auch das Passwort können jederzeit geändert werden (siehe *Abschnitt 41.4.2.5.1, „Passwort für die Webschnittstelle“*).

Nach erfolgter Installation und Einrichtung ist die SCA-Appliance einsatzbereit (siehe *Abschnitt 41.4.2.4, „Verwenden der SCA-Appliance“*). Sie sollten jedoch einige 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 41.4.2.5, „Anpassen der SCA-Appliance“*.

Warnung: Schutz der Daten

Die Berichte auf dem SCA-Appliance-Server enthalten sicherheitsrelevante Informationen, weshalb die Daten auf dem SCA-Appliance-Server vor unbefugtem Zugriff geschützt werden müssen.

41.4.2.4 Verwenden der SCA-Appliance

Sie können vorhandene Supportconfig-Archive manuell an die SCA-Appliance heraufladen oder neue Supportconfig-Archive erstellen und im gleichen Arbeitsgang analysieren an 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 41.5, „Installieren und Konfigurieren der SCA-Appliance“*).

41.4.2.4.1 Hochladen von supportconfig-Archiven an die SCA-Appliance

- So können Sie ein Supportconfig-Archiv erstellen und über einen (anonymen) FTP-Zugang hochladen:

```
> sudo supportconfig -U “ftp://SCA-APPLIANCE.COMPANY.COM/upload”
```

- So können Sie ein Supportconfig-Archiv erstellen und über SCP hochladen:

```
> 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 Hochladen von einem oder mehreren Archiven kopieren Sie die vorhandenen Archivdateien (unter `/var/log/scc_*.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).

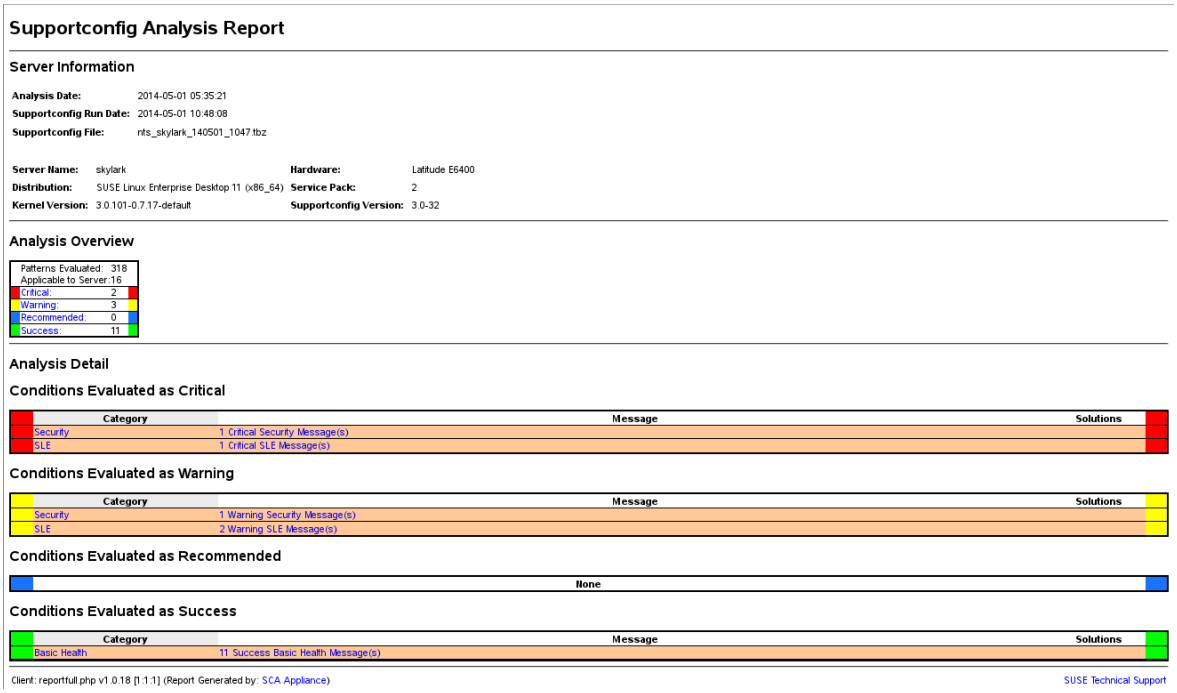
41.4.2.4.2 Anzeigen von SCA-Berichten

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 41.2: MIT DEM SCA-WERKZEUG 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 (https://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.

41.4.2.5 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.

41.4.2.5.1 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 `linux` (sofern nicht anders festgelegt, siehe *Prozedur 41.5, „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.

VORGEHEN 41.6: 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 Texteditor.
3. Ändern Sie bei Bedarf die Werte von `$username` und `$password`.
4. Speichern und schließen Sie die Datei.

41.4.2.5.2 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 15 SP7 installiert. Bei Bedarf können Sie die Quelle der Aktualisierungen in einen RMT-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 RMT-Server befindet, werden die Pakete von diesem Server abgerufen.

VORGEHEN 41.7: 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 Texteditor.
3. Ändern Sie den Eintrag

   ```
   UPDATE_FROM_PATTERN_REPO=1
   ```

   zu

   ```
   UPDATE_FROM_PATTERN_REPO=0
   ```
4. Speichern und schließen Sie die Datei. Die Änderung tritt ohne Neustart des Rechners in Kraft.

41.4.2.5.3 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.

VORGEHEN 41.8: 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 Texteditor.
3. Ändern Sie den Eintrag

   ```
   ARCHIVE_MODE=0
   ```

   zu

   ```
   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.

41.4.2.5.4 Senden von SCA-Berichten per Email

Die SCA-Appliance kann für jede analysierte Supportconfig-Datei einen HTML-Bericht per Email schicken. Diese Funktion ist standardmäßig deaktiviert. Wenn Sie dies aktivieren, können Sie eine Liste der Email-Adressen definieren, an die die Berichte gesendet werden sollen. Definieren Sie die Statusebene, die das Senden von Berichten auslösen soll (`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.

VORGEHEN 41.9: 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 Texteditor.
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 Statusnachrichtenebene, ab der die Email-Berichte gesendet werden sollen, beispielsweise:

   ```
   STATUS_NOTIFY_LEVEL=$STATUS_SUCCESS
   ```

   Weitere Informationen finden Sie im *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.

41.4.2.6 Sichern und Wiederherstellen der Datenbank

Mit dem Befehl **`scadb`** können Sie die MariaDB-Datenbank, in der die SCA-Berichte gespeichert werden, sichern und wiederherstellen. **`scadb`** wird im Paket `sca-appliance-broker` bereitgestellt.

VORGEHEN 41.10: 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 Befehl 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 41.4.3, „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
```

VORGEHEN 41.11: 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 neuesten und TAR-Archive `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 Befehl 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
```

41.4.3 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 https://www.suse.com/c/sca-pattern-development/.

41.5 Sammeln von Informationen bei der Installation

Während der Installation ist **`supportconfig`** nicht verfügbar. Sie können Protokolldateien von YaST jedoch mithilfe von **`save_y2logs`** sammeln. Dieser Befehl 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 kleiner Befehl, der 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.

41.6 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 Program` bereitgestellt werden, sind als „external“ gekennzeichnet.
- Wenn das Flag `supported` nicht gesetzt ist, wird der Kernel beim Laden dieses Moduls unbrauchbar. Unbrauchbare Kernel werden nicht unterstützt. Die nicht unterstützten Kernel-Module befinden sich in einem separaten RPM-Paket (`kernel-`*`FLAVOR`*`-extra`). Dieses Paket ist lediglich für SUSE Linux Enterprise Desktop und SUSE Linux Enterprise Workstation Extension verfügbar. Diese Kernel werden standardmäßig nicht geladen (*`FLAVOR`* = `default`|`xen`|...). Darüber hinaus sind diese nicht unterstützten Module im Installationsprogramm nicht verfügbar und das Paket `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. Details finden Sie im Status von `/proc/sys/kernel/tainted`

41.6.1 Technischer Hintergrund

- Linux-Kernel: Der Standardwert von `/proc/sys/kernel/unsupported` ist `2` in SUSE Linux Enterprise 15 SP7 (`do not warn in syslog when loading unsupported modules`). Dieser Standardwert wird im Installationsprogramm und im installierten System verwendet.

- **`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 41.6.2, „Arbeiten mit nicht unterstützten Modulen“*.

Anmerkung: Support

SUSE bietet im Allgemeinen keine Unterstützung für das Entfernen von Speichermodulen mit **`modprobe -r`**.

41.6.2 Arbeiten mit nicht unterstützten Modulen

Auch wenn die allgemeine Unterstützung wichtig ist, können Situationen auftreten, in denen das Laden eines nicht unterstützten Moduls erforderlich ist. Zum Beispiel zu Testzwecken oder für die Fehlersuche oder wenn Ihr Hardwarehersteller ein Hotfix zur Verfügung stellt.

- Um die Standardeinstellung zu überschreiben, kopieren Sie `/lib/modprobe.d/10-unsupported-modules.conf` nach `/etc/modprobe.d/10-unsupported-modules.conf` und ändern Sie den Wert der Variablen `allow_unsupported_modules` von `0` in `1`. Bearbeiten Sie `/lib/modprobe.d/10-unsupported-modules.conf` nicht direkt. Alle Änderungen werden bei der nächsten Aktualisierung des `suse-module-tools`-Pakets überschrieben.
  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 in den Kommentaren in `/lib/modprobe.d/10-unsupported-modules.conf` und in der Man-Page 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, verwen-

den Sie die Kernel-Befehlszeilenoption `oem-modules`. Während der Installation und Initialisierung 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 unterstützten 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.

41.7 Weitere Informationen

- **`man supportconfig`** – man-Seite **`supportconfig`**.
- **`man supportconfig.conf`** – man-Seite zur Supportconfig-Konfigurationsdatei.
- **`man scatool`** – man-Seite **`scatool`**.
- **`man scadb`** – man-Seite **`scadb`**.
- **`man setup-sca`** – man-Seite **`setup-sca`**.
- https://mariadb.com/kb/en/ – Dokumentation zur MariaDB.
- https://www.suse.com/c/sca-pattern-development/ – Anweisungen zum Erstellen (und Testen) benutzerdefinierter SCA-Schemata.
- https://community.microfocus.com/img/gw/groupwise/w/tips/34308/create-your-own-supportconfig-plugin – Erstellen eines eigenen supportconfig-Plugins.
- https://www.suse.com/c/creating-a-central-supportconfig-repository/ – Erstellen eines zentralen supportconfig-Repositorys.

42 Häufige Probleme und deren Lösung

In diesem Kapitel werden mögliche Probleme und deren Lösungen beschrieben. Auch wenn Ihre Situation nicht genau auf die beschriebenen Probleme zutreffen mag, finden Sie vielleicht einen ähnlichen Fall, der Ihnen Hinweise zur Lösung Ihres Problems liefert.

42.1 Suchen und Sammeln von Informationen

Linux gibt äußerst detailliert Aufschluss über die Vorgänge in Ihrem System. Bei Problemen mit Ihrem System gibt es mehrere Stellen, an denen Sie nachsehen können. Die meisten von ihnen sind standardmäßig für Linux-Systeme und einige sind für SUSE Linux Enterprise Desktop-Systeme relevant. Die meisten Protokolldateien können mit YaST angezeigt werden (*Verschiedenes* › *Startprotokoll anzeigen*).

YaST bietet die Möglichkeit, alle erforderlichen Systeminformationen für das Supportteam zusammenzustellen. 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 42.1: PROTOKOLLDATEIEN

Protokolldatei	Beschreibung
`~/.xsession-errors`	Meldungen von den zurzeit ausgeführten Desktop-Anwendungen.
`/var/log/apparmor/`	Protokolldateien von AppArmor (Detailinformationen finden Sie im *Buch „Security and Hardening 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 im *Buch „Security and Hardening 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`	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. Siehe *Tabelle 42.2: Systeminformationen mit dem `/proc`-Dateisystem*

TABELLE 42.2: SYSTEMINFORMATIONEN MIT DEM `/proc`-DATEISYSTEM

Datei	Beschreibung
`/proc/cpuinfo`	Enthält Prozessorinformationen wie Typ, Fabrikat, Modell und Leistung.
`/proc/dma`	Zeigt die aktuell verwendeten DMA-Kanäle an.

Datei	Beschreibung
/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 in Abschnitt *Kapitel 29, Gerätemanagement über dynamischen Kernel mithilfe von* udev. *Tabelle 42.3* enthält einen Überblick über die am häufigsten verwendeten Verzeichnisse unter /sys.

TABELLE 42.3: 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. Im *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.

42.2 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.

42.2.1 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 42.5.2, „Verwenden des Rettungssystems“* beschrieben und den Anweisungen in *Abschnitt 42.5.2.4, „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.

42.2.2 Es wird keine Anmeldemaske oder Eingabeaufforderung angezeigt

Dieses Verhalten tritt normalerweise nach einem nicht erfolgreichen Kernelupgrade auf und ist nach der Art von Fehler auf der Systemkonsole, der zuweilen im Endstadium des Vorgangs auftritt, als *Kernelpanik* bekannt. Wenn der Computer tatsächlich soeben nach einer Softwareaktualisierung neu gebootet wurde, sollte er zunächst mithilfe der alten, bewährten Version des Linux-Kernels und der zugehörigen Dateien erneut gebootet werden. Gehen Sie dazu während des Bootvorgangs am Bildschirm des GRUB 2-Bootloaders wie folgt vor:

1. Booten Sie den Computer mithilfe der Schaltfläche zum Zurücksetzen neu oder schalten Sie ihn aus und wieder an.
2. Wenn der GRUB 2-Bootbildschirm angezeigt wird, wählen Sie den Eintrag *Erweiterte Optionen* aus und wählen Sie den vorherigen Kernel aus dem Menü aus. Der Computer sollte nun mithilfe der früheren Version des Kernels und der zugehörigen Dateien gebootet werden.
3. Entfernen Sie nach Abschluss des Bootvorgangs den neu installierten Kernel und legen Sie, falls nötig, anhand des YaST *Boot Loader*-Moduls den Standard-Boot-Eintrag auf den alten Kernel fest. Weitere Informationen hierzu finden Sie in *Abschnitt 18.3, „Konfigurieren des*

Bootloaders mit YaST“. Eine Aktualisierung dieser Datei ist jedoch nicht erforderlich, da sie normalerweise während des Rollback-Vorgangs von den automatischen Aktualisierungswerkzeugen bearbeitet wird.

4. Booten Sie den Computer neu.

Falls dadurch das Problem nicht behoben wird, booten Sie den Computer anhand der Installationsmedien. Fahren Sie nach dem Booten des Computers mit *Schritt 3* und fort.

42.2.3 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 System mit Problemen rechnen. Zum Prüfen des aktuellen systemd-Standardziels führen Sie den Befehl **`sudo systemctl get-default`** aus. Wenn *nicht* der Wert `graphical.target` zurückgegeben wird, führen Sie den Befehl **`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 *Standard-Systemziel* den Wert *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. Untersuchen Sie die Protokolldateien unter `/var/log/Xorg.*.log` nach detaillierten Meldungen vom X-Server beim Startversuch. Wenn beim Starten des Desktops ein Fehler auftritt, werden möglicherweise Fehlermeldungen im Systemjournal protokolliert, die Sie mit dem Befehl **`journalctl`** abfragen können (weitere Informationen finden Sie in *Kapitel 21, `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.

42.2.4 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.

42.2.5 Erzwingen der Prüfung von root-Partitionen

Wenn die Root-Partition beschädigt ist, verwenden Sie den Parameter `forcefsck` an der Boot-Eingabeaufforderung. Hierdurch wird die Option `-f` (force = zwingen) an den Befehl **`fsck`** übergeben.

42.2.6 Auslagerungsgerät zum Booten deaktivieren

Wenn kein Auslagerungsgerät verfügbar ist und das System es beim Booten nicht aktivieren kann, schlägt der Bootvorgang womöglich fehl. Versuchen Sie, alle Auslagerungsgeräte zu deaktivieren, indem Sie auf der Kernel-Befehlszeile die folgenden Optionen hinzufügen:

```
systemd.device_wants_unit=off systemd.mask=swap.target
```

Sie können auch versuchen, bestimmte Auslagerungsgeräte zu deaktivieren:

```
systemd.mask=dev-sda1.swap
```

42.2.7 Fehler bei GRUB 2 beim Neustarten auf einem Dual-Boot-System

Wenn bei GRUB 2 ein Fehler beim Neustarten auftritt, deaktivieren Sie die Einstellung `Fast Boot` (Schnelles Booten) im BIOS.

42.3 Probleme bei der Anmeldung

Anmeldeprobleme treten auf, wenn Ihr System den Benutzernamen und das Passwort nicht akzeptiert oder beides akzeptiert, dann aber beispielsweise den grafischen Desktop nicht startet, Fehler erzeugt oder in eine Befehlszeile wechselt.

42.3.1 Fehler trotz gültiger Kombination aus Benutzername und Passwort

Dieser Fall tritt oft ein, wenn das System zur Verwendung von Netzwerkauthentifizierung oder Verzeichnisdiensten konfiguriert wurde und 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 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 42.4, „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 langsam reagiert. Weitere Informationen zu diesem Thema finden Sie in *Abschnitt 42.4, „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 im *Buch „Security and Hardening Guide“, Kapitel 2 „Authentication with PAM“*.
- Die Home-Partition ist verschlüsselt. Weitere Informationen zu diesem Thema finden Sie in *Abschnitt 42.3.3, „Anmeldung bei verschlüsselter Home-Partition fehlgeschlagen“*.

In Fällen, bei denen es nicht um externe Netzwerkprobleme geht, besteht die Lösung darin, sich als `root`-Benutzer anzumelden und die Konfiguration zu reparieren. Wenn Sie sich nicht beim ausgeführten System anmelden können, booten Sie es wie unter *Prozedur 18.3, „Aufrufen des Rescue-Modus“* beschrieben im Rescue-Modus neu.

42.3.2 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 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 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 42.3.4, „Probleme mit dem 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 42.3.4, „Probleme mit dem 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 42.3.4, „Probleme mit dem 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 42.3.4, „Probleme mit dem GNOME-Desktop“* fort.

42.3.3 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, liegt es vielleicht daran, dass Ihre Partition nicht entsperrt werden konnte.

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.

42.3.4 Probleme mit dem GNOME-Desktop

Wenn Probleme mit dem GNOME-Desktop auftreten, stehen mehrere Möglichkeiten zur Fehlerbehebung der problembehafteten grafischen Desktop-Umgebung zur Auswahl. Das unten beschriebene empfohlene Verfahren ist die sicherste Option zum Reparieren eines beschädigten GNOME-Desktops.

VORGEHEN 42.1: FEHLERBEHEBUNG FÜR GNOME

1. Starten Sie YaST und wechseln Sie zu *Sicherheit und Benutzer*.
2. Öffnen Sie das Dialogfeld *Verwaltung von Benutzern und Gruppen* und klicken Sie auf *Hinzufügen*.
3. Füllen Sie die erforderlichen Felder aus und klicken Sie auf *OK*, um einen neuen Benutzer zu erstellen.
4. Melden Sie sich ab und melden Sie sich als neuer Benutzer an. So erhalten Sie eine frische GNOME-Umgebung.
5. Kopieren Sie einzelne Unterverzeichnisse aus den Verzeichnissen `~/.local/` und `~/.config/` des alten Benutzerkontos in die jeweiligen Verzeichnisse des neuen Benutzerkontos. Melden Sie sich nach jedem Kopiervorgang ab und als neuer Benutzer wieder an, um zu überprüfen, ob GNOME noch ordnungsgemäß funktioniert.
6. Wiederholen Sie den letzten Schritt, bis Sie die Konfigurationsdatei finden, die den Fehler in GNOME verursacht hat.

7. Melden Sie sich als alter Benutzer an und verschieben Sie die fehlerhafte Konfigurationsdatei an einen anderen Speicherort. Melden Sie sich ab und als alter Benutzer wieder an.

8. Löschen Sie den zuvor erstellten Benutzer.

42.4 Probleme mit dem Netzwerk

Viele Probleme Ihres Systems beziehen sich möglicherweise auf das Netzwerk, obwohl die Symptome unterschiedlich aussehen. 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.

VORGEHEN 42.2: 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 die 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 Desktop-System hinsichtlich der Bereitstellung der Benutzerdaten von einem fehlerhaften NIS-Server abhängig ist, können sich Benutzer nicht bei diesem Rechner anmelden.

LDAP (Benutzerverwaltung)

Wenn Ihr SUSE Linux Enterprise Desktop-System hinsichtlich der Bereitstellung der Benutzerdaten von einem fehlerhaften LDAP-Server abhängig ist, können sich Benutzer nicht bei diesem Rechner 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: Nutzungsbeschränkungen

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_ADDRESS/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 dieser Befehl 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 address`* oder *`YOUR_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, ordnungsgemäß in eine IP-Adresse übersetzt wird (und umgekehrt). Wenn bei diesem Befehl die IP-Adresse dieses Host zurückgegeben wird, ist der Namendienst aktiv. Wenn bei diesem **`host`**-Befehl ein Fehler auftritt, überprüfen Sie alle Netzwerkkonfigurationsdateien, die für die Namen- und Adressauflösung auf Ihrem Host relevant sind:

`/var/run/netconfig/resolv.conf`

Mithilfe dieser Datei wissen Sie stets, welchen Nameserver und welche Domäne Sie zurzeit verwenden. Sie ist ein symbolischer Link zu `/run/netconfig/resolv.conf` und wird in der Regel von YaST oder DHCP automatisch angepasst. Stellen Sie 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 Nameserver 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 Nameserver 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. 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 Befehl **`ip addr show`** *`NETWORK_DEVICE`*, 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 bestimmten externen Netzwerkverbindungen jedoch nach wie vor lange Zeitüberschreitungen auftreten bzw. der Verbindungsaufbau überhaupt nicht möglich ist, können Sie mit **`traceroute`** *`FULLY_QUALIFIED_DOMAIN_NAME`* (Ausführung als `root`) die Netzwerkroute dieser Anforderungen überwachen. Mit diesem Befehl werden sämtliche Gateways (Sprünge) aufgelistet, die eine Anforderung von Ihrem Computer auf ihrem Weg zu ihrem Ziel passiert. Mit ihm wird die Antwortzeit der einzelnen Sprünge (Hops) aufgelistet und es wird ersichtlich, ob dieser Sprung 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.

42.4.1 Probleme mit NetworkManager

Grenzen Sie Probleme mit der Netzwerkkonnektivität wie unter *Prozedur 42.2, „Erkennen von Netzwerkproblemen“* beschrieben ein. Wenn NetworkManager verdächtig aussieht, gehen Sie wie folgt vor, um Protokolle zu erhalten, die Hinweise darauf geben, warum bei NetworkManager ein Fehler auftritt:

1. Öffnen Sie eine Shell und melden Sie sich als `root` an.
2. Starten Sie NetworkManager neu.

   ```
   > sudo systemctl restart NetworkManager
   ```

3. Öffnen Sie eine Website, beispielsweise https://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 31, Verwendung von NetworkManager*.

42.5 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.

42.5.1 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.

VORGEHEN 42.3: SICHERN UND WIEDERHERSTELLEN VON FESTPLATTEN

1. Starten Sie eine Shell als `root`-Benutzer.

2. Wählen Sie das Quellgerät aus. Typischerweise ist dies `/dev/sda` oder etwas Ähnliches (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 Befehle zur Erstellung einer komprimierten Image-Datei aus:

```
# dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
```

5. Stellen Sie die Festplatte mithilfe der folgenden Befehle wieder her:

```
# gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
```

Wenn Sie eine Partition nur sichern müssen, ersetzen Sie den Platzhalter *SOURCE* durch Ihre entsprechende Partition. In diesem Fall kann sich Ihre Image-Datei auf derselben Festplatte befinden, allerdings in einer anderen Partition.

42.5.2 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 Desktop 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-Befehls verändert werden. Weitere Informationen zu diesem Werkzeug finden Sie auf der Website von GNU Parted (https://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.

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 `root` an der Eingabeaufforderung `Rescue:` 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-Start-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 *`PROTOCOL`* für eines der unterstützten Netzwerkprotokolle (NFS, HTTP, FTP usw.) und *`INSTSOURCE`* für den Pfad zur Netzwerkinstallationsquelle.
2. Booten Sie das System mit „Wake on LAN“, wie in *Buch „Installationshandbuch“, Kapitel 14 „Vorbereiten der Netzwerk-Boot-Umgebung“, Abschnitt 14.5 „Verwenden von Wake-on-LAN für Fernaktivierungen“* erläutert.
3. Geben Sie `root` an der Eingabeaufforderung `Rescue:` 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. Dieses Verzeichnis enthält auch die wichtigsten Binärdateien für die Systemwartung wie **`fdisk`**, **`mkfs`**, **`mkswap`**, **`mount`** und **`shutdown`**, **`ip`** und **`ss`** zum Warten des Netzwerks. Das Verzeichnis `/usr/bin` enthält den vi-Editor, find, less sowie SSH.

Die Systemmeldungen können über den Befehl **`dmesg`** angezeigt werden; mit **`journalctl`** rufen Sie das Systemprotokoll ab.

42.5.2.1 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 folgenden Befehl:

   ```
   > sudo mount /dev/sda6 /mnt
   ```

   Sämtliche Verzeichnisse des Systems befinden sich nun unter `/mnt`
3. Wechseln Sie in das eingehängte root -Dateisystem:

   ```
   > sudo 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:

   ```
   > sudo umount /mnt
   ```
6. Den Computer neu booten.

42.5.2.2 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 das **`fsck`**-Dienstprogramm zum Überprüfen und Reparieren mehrerer Dateisystemtypen wie `ext2`, `ext3`, `ext4`, `msdos` und `vfat`. Verwenden Sie die Option `-t`, um anzugeben, welches Dateisystem überprüft werden soll.

Der folgende Befehl überprüft alle in der Spezifikation `/etc/fstab` gefundenen `ext4`-Dateisysteme:

```
> sudo fsck -t ext4 -A
```

Tipp

Für Btrfs können Sie den Befehl **`btrfs check`** im Paket `btrfsprogs` verwenden.

Themen zum Btrfs-Dateisystem finden Sie an den folgenden Stellen:

- Der Storage Administration Guide enthält die Abschnitte https://documentation.suse.com/sles/html/SLES-all/cha-filesystems.html#sec-filesystems-major-btrfs und https://documentation.suse.com/sles/html/SLES-all/cha-resize-fs.html#sec-resize-fs-btrfs.
- Im folgenden Artikel wird beschrieben, wie Sie die Wiederherstellung nach Btrfs-Fehlern vornehmen: https://www.suse.com/support/kb/doc/?id=000018769.
- Der folgende Artikel enthält Links zu mehreren auf Btrfs bezogenen Themen: https://www.suse.com/support/kb/doc/?id=000018779.
- Die Manpage für **`man 8 btrfs-check`** enthält alle Optionen des Befehls **`btrfs check`**.

42.5.2.3 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 „Installationshandbuch“, Kapitel 7 „Festplatte vorbereiten: Expertenmodus“, Abschnitt 7.3 „LVM-Konfiguration“*), 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:

   ```
   > sudo mount /dev/sda2 /mnt
   ```

3. Hängen Sie die Partitionen `/proc`, `/dev` und `/sys` ein.

   ```
   > sudo mount -t proc none /mnt/proc
   > sudo mount --rbind /dev /mnt/dev
   > sudo 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: Nutzungsbeschränkungen

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.

42.5.2.4 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 42.5.2.3, „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:

```
> sudo grub2-install /dev/sda
```

3. Prüfen Sie, ob die nachfolgend angegebenen Dateien gemäß den in *Kapitel 18, 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`
   - `/boot/grub2/grub.cfg` (diese Datei wird automatisch generiert; nicht bearbeiten)
   - `/etc/sysconfig/bootloader`

4. Installieren Sie den Bootloader mit folgender Befehlssequenz neu:

```
> sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. Hängen Sie die Partitionen aus, melden Sie sich bei der „change-root“-Umgebung ab und führen Sie den Reboot des Systems durch:

```
> umount -a
exit
reboot
```

42.5.2.5 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 der Aktualisierung

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
```

in die Datei `/etc/zypp/zypp.conf`. Weitere Informationen zu diesem Thema finden Sie in *Kapitel 27, Installieren von mehreren Kernel-Versionen*.

Ähnlich verhält es sich, wenn Sie einen defekten Treiber für ein nicht durch SUSE Linux Enterprise Desktop 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 Desktop-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 `root` an der Eingabeaufforderung `Rescue:` 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 in *Abschnitt 42.5.2.3, „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-Gerät 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/`**.

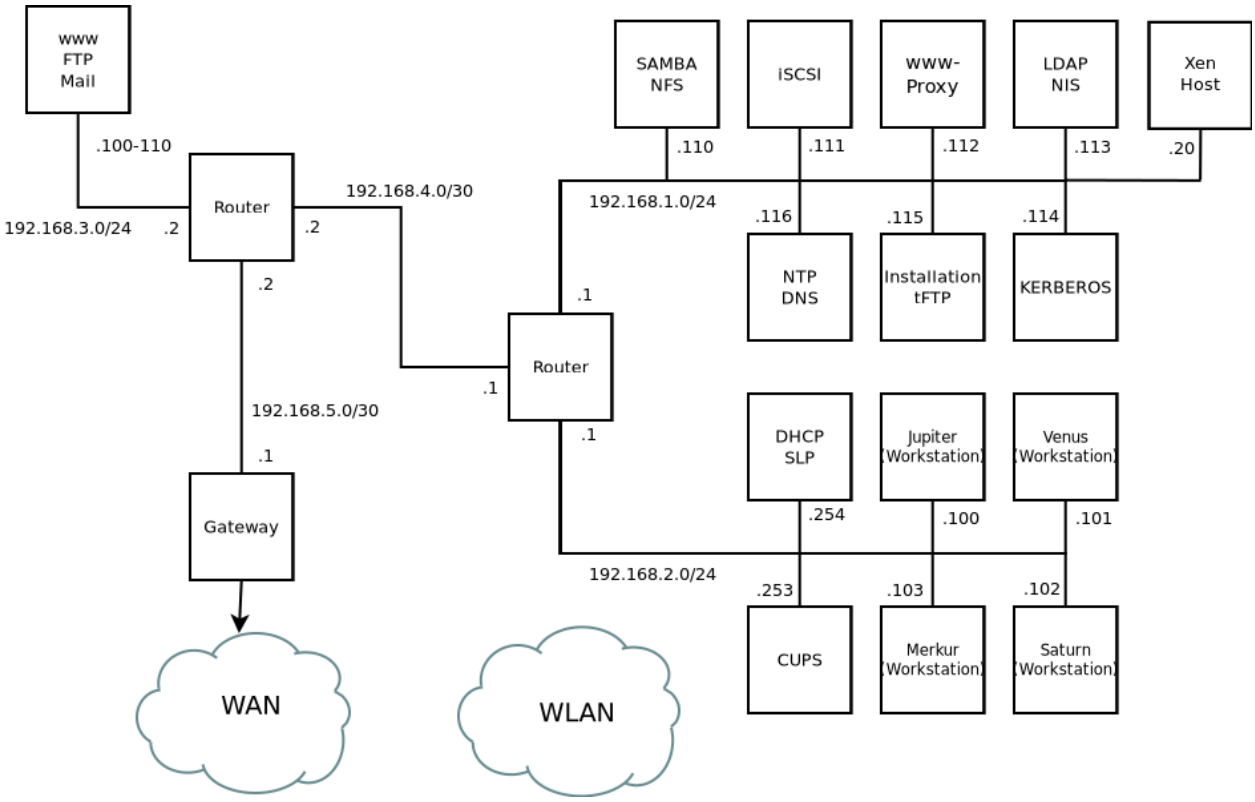
   c. Installieren Sie die erforderlichen und Pakete `kernel-*`, `kernel-*-base` und `kernel-*-extra`, die Sie bevorzugen, mit dem Befehl **`rpm -i`**.

7. Aktualisieren Sie Konfigurationsdateien und initialisieren Sie den Bootloader gegebenenfalls neu. Weitere Informationen finden Sie in *Abschnitt 42.5.2.4, „Bearbeiten und erneutes Installieren des Bootloaders“*.

8. Entfernen Sie alle bootbaren Medien aus dem Systemlaufwerk und booten Sie neu.

A Ein Beispielnetzwerk

Dieses Beispielnetzwerk wird in allen Kapiteln über das Netzwerk in der Dokumentation zu SUSE® Linux Enterprise Desktop herangezogen.



B GNU licenses

Versionsgeschichte

2023-02-03

This appendix contains the 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 https://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.