Michael Kofler

»Aktuell zu Debian, CentOS, RHEL, Fedora, openSUSE und Ubuntu«

Linux

Das umfassende Handbuch

Der neue »Kofler«

- Das Standardwerk für Einsteiger und fortgeschrittene Anwender
- Für Desktops und Server: Installation, Konfiguration, Administration
- Mit zahlreichen Praxistipps und Raspberry-Pi-Kapitel

Inklusive E-Book zum Download

Galileo Computing

Liebe Leserin, lieber Leser,

dieses Handbuch – vielen einfach als »der Kofler« bekannt –, gilt bei seinen Lesern und Fans, in der Fachpresse und im Buchhandel seit Jahren als Standardwerk zu Linux. Erstmals erscheint es nun bei Galileo Press.

Egal, ob Sie das Buch schon aus früheren Auflagen kennen oder ob Sie es nun erstmals in Händen halten: Sie werden von den aktuellen und wertvollen Informationen profitieren. Als Einsteiger werden Sie schnell erfahren, weshalb dieses Buch seit vielen Jahren Kultstatus genießt: Sowohl die inhaltliche Tiefe, mit der die Fülle der Themen behandelt wird, als auch die ausgezeichnete Art der Erläuterung machen es einzigartig. Und als Kenner früherer Auflagen werden Sie zu schätzen wissen, wie sehr es am Puls der Zeit ist: Es berücksichtigt neben den aktuellen Ausgaben der wichtigsten Linux-Distributionen umfassend neue Technologien wie IPv6 oder den Minicomputer Raspberry Pi.

Zu Michael Kofler als einem der bekanntesten und erfolgreichsten deutschen IT-Fachbuchautoren ist bereits viel in der Fachpresse geschrieben worden. Deshalb hier nur so viel: Seine sorgfältige Planung der Neuauflage, sein schier unerschöpfliches Linux-Know-how, die Genauigkeit bei der Durchführung und nicht zuletzt sein Witz – all das werden Sie auf jeder Seite dieses Buches wiederfinden!

Übrigens: **Wenn Sie die gedruckte Ausgabe des Buches erworben haben, erhalten Sie das vollständige E-Book (PDF-Datei) kostenlos dazu.** Sie können es von der Webseite *www.galileo-press.de/bonusseite* herunterladen.

Und noch ein Wort in eigener Sache: Dieses Werk wurde mit großer Sorgfalt geschrieben, geprüft und produziert. Sollte dennoch einmal etwas nicht so funktionieren, wie Sie es erwarten, freue ich mich, wenn Sie sich mit mir in Verbindung setzen. Ihre Kritik und konstruktiven Anregungen sind uns jederzeit herzlich willkommen!

Ihr Sebastian Kestel
Lektorat Galileo Computing

Sebastian.Kestel@galileo-press.de
www.galileocomputing.de
Galileo Press · Rheinwerkallee 4 · 53227 Bonn

Auf einen Blick

Wir hoffen sehr, dass Ihnen dieses Buch gefallen hat. Bitte teilen Sie uns doch Ihre Meinung mit. Eine E-Mail mit Ihrem Lob oder Tadel senden Sie direkt an den Lektor des Buches: *sebastian.kestel@galileo-press.de*. Im Falle einer Reklamation steht Ihnen gerne unser Leserservice zur Verfügung: *service@galileo-press.de*. Informationen über Rezensions- und Schulungsexemplare erhalten Sie von: *britta.behrens@galileo-press.de*.

Informationen zum Verlag und weitere Kontaktmöglichkeiten finden Sie auf unserer Verlagswebsite *www.galileo-press.de*. Dort können Sie sich auch umfassend und aus erster Hand über unser aktuelles Verlagsprogramm informieren und alle unsere Bücher versandkostenfrei bestellen.

An diesem Buch haben viele mitgewirkt, insbesondere:

Lektorat Sebastian Kestel
Korrektorat Friederike Daenecke, Zülpich
Herstellung Norbert Englert
Layout Vera Brauner
Einbandgestaltung Mai Loan Nguyen Duy
Satz Michael Kofler
Druck und Bindung Beltz, Bad Langensalza

Dieses Buch wurde gesetzt aus der TheAntiquaB (9,35 pt/13,7 pt) mit LaTeX.
Gedruckt wurde es auf chlorfrei gebleichtem Offsetpapier (70 g/m^2).

Der Name Galileo Press geht auf den italienischen Mathematiker und Philosophen Galileo Galilei (1564–1642) zurück. Er gilt als Gründungsfigur der neuzeitlichen Wissenschaft und wurde berühmt als Verfechter des modernen, heliozentrischen Weltbilds. Legendär ist sein Ausspruch *Eppur si muove* (Und sie bewegt sich doch). Das Emblem von Galileo Press ist der Jupiter, umkreist von den vier Galileischen Monden. Galilei entdeckte die nach ihm benannten Monde 1610.

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

ISBN 978-3-8362-2591-5

1. Auflage 2014

Dieses Buch ist meiner Frau Heidi und
meinen Kindern Sebastian und Matthias gewidmet.

Inhalt

Vorwort

Linux erlebt momentan in Form von Android einen Siegeszug, den vor fünf Jahren niemand für möglich gehalten hätte. Viele Medien beobachteten damals den Wettstreit der Betriebssysteme ausschließlich auf der Desktop-Ebene – ein Schauplatz, auf dem Microsoft Windows bis heute überlegen dominiert.

Inzwischen ist aber allen klar geworden, dass Notebooks und Desktop-PCs nur *ein* Segment des IT-Markts sind. Andere Segmente sind Smartphones und Tablets, der Server-Bereich inklusive aller Cloud-Anwendungen und der Embedded-Bereich. Letzteres meint in sich abgeschlossene Geräte, vom ADSL-Router über den Industrie-Roboter bis zur Waschmaschine, die durch Minicomputer gesteuert werden.

Bemerkenswert ist, dass Linux mittlerweile in *allen* Segmenten präsent ist und einige sogar dominiert. Bei den Smartphones geht es längst nicht mehr um den Kampf von David/Linux gegen Goliath/Microsoft, sondern um Android versus iOS; Microsoft spielt hier eine vollkommen untergeordnete Rolle. Das moderne Internet (Schlagwort »Web 2.0«) würde es ohne Linux nicht geben.

Linux ist allgegenwärtig

Ironischerweise verwendet heute nahezu jeder *ständig* in irgendeiner Form Linux, freilich ohne es zu wissen:

- Die Basis von Android ist der Linux-Kernel – kombiniert mit einer schönen Benutzeroberfläche.
- Jede Google- oder Wikipedia-Frage wird von Servern beantwortet, die unter Linux laufen.
- Einkäufe bei Amazon und bei unzähligen anderen Webstores werden von Linux-Servern abgewickelt.
- Viele ADSL- und WLAN-Router, NAS-Geräte etc. laufen unter Linux.
- Die Infrastruktur vieler Telekom-Unternehmen basiert auf Linux. Wenn Sie telefonieren oder mit Ihrem Smartphone im Internet surfen, fließen die Datenpakete über Linux-Rechner.
- Große Server-Systeme, zu Neudeutsch die »Cloud«, verwenden häufig Linux. Beispielsweise befinden sich Ihre Dropbox-Dateien im Cloud-Service S3 von Amazon – und in letzter Konsequenz auf einem Linux-Server!

Dieses Buch

In diesem Buch stelle ich Ihnen Linux von Grund auf vor. Die Themenpalette reicht über die Installation von Linux auf einem Notebook oder PC über die Desktop-Anwendung bis hin zum Server-Einsatz und zur Virtualisierung. Ganz neu in dieser Auflage ist ein umfassendes Kapitel zum Minicomputer Raspberry Pi, der sich nicht nur für Elektronikbasteleien eignet, sondern einen kostengünstigen Einstieg in die Linux-Embedded-Welt gibt.

Besonders wichtig ist mir, dass Sie Linux nicht nur anwenden, sondern auch verstehen lernen: Ausführliche Grundlagenkapitel erklären, wie Sie Linux im Terminal bedienen, wie Sie Linux optimal konfigurieren und warum Linux so funktioniert. Nach der Lektüre dieser Kapitel kennen Sie nicht nur Linux an sich, sondern auch die Philosophie von Unix/Linux – also gewissermaßen *the Linux way to do it*.

Freilich gibt es nicht *ein* Linux, sondern viele Linux-Distributionen. Vereinfacht ausgedrückt: Eine Distribution ist eine Sammlung von Programmen rund um Linux. Zu den bekanntesten Distributionen zählen Debian, Red Hat, openSUSE und Ubuntu. Diese Vielfalt hat eine Menge Vorteile, aber natürlich auch einen entscheidenden Nachteil: Viele Details sind je nach Distribution unterschiedlich gelöst. Dieses Buch verfolgt so weit wie möglich einen distributionsunabhängigen Ansatz. Da ist es nicht zu vermeiden, hin und wieder auf verschiedene Varianten hinzuweisen – ganz nach dem Motto: Bei openSUSE funktioniert es auf die eine Weise, bei Debian auf die andere.

Viel Spaß!

Im Vergleich zu kommerziellen Produkten bietet Linux Ihnen die Möglichkeit, das Betriebssystem beinahe grenzenlos an Ihre eigenen Bedürfnisse und Vorlieben anzupassen – sei es zur Programmierung, für den Netzwerkeinsatz oder als Server. Für nahezu jede Aufgabe stehen mehrere Werkzeuge zur Wahl. Und je mehr Sie sich in die Linux-Welt einarbeiten, desto mehr wird Linux *Ihr* Betriebssystem. Ich wünsche Ihnen viel Freude beim Experimentieren, Kennenlernen und Arbeiten mit Linux!

Michael Kofler
http://kofler.info

PS: Dieses Buch ist in seinen ersten zwölf Auflagen über einen Zeitraum von 17 Jahren im Addison-Wesley Verlag erschienen. 2012 sah dessen Eigentümer Pearson keine Zukunft mehr für IT-Bücher; der deutsche Addison-Wesley Verlag ist damit Geschichte. Ich bin mehr als glücklich, dass ich bei Galileo Press eine neue verlegerische Heimat gefunden habe. Besonders bedanken möchte ich mich bei Judith Stevens-Lemoine und Sebastian Kestel, die mir den Wechsel zu Galileo Press leicht gemacht haben.

Konzeption

Das Buch ist in sieben Teile gegliedert:

- **Teil I** erklärt, was Linux eigentlich ist, und vermittelt das Grundlagenwissen, das Sie für eine optimale und sichere **Installation** brauchen. Hier finden Sie konkrete Installationsanleitungen für ein halbes Dutzend Distributionen: CentOS, Debian, Fedora, openSUSE, Ubuntu und Ubuntu Server.
- **Teil II** behandelt Linux auf dem **Desktop**. Hier lernen Sie verschiedene Desktop-Systeme kennen (Gnome, KDE, Unity, Xfce, LXDE). Außerdem stelle ich Ihnen die wichtigsten Programme vor, um im Web zu surfen, E-Mails und Fotos zu verwalten sowie Audio-Dateien und Filme abzuspielen. Ein umfassendes Kapitel zum Minicomputer Raspberry Pi beschreibt einen ganz neuen Weg, wie Sie Linux als Medien-Center oder als Plattform für Bastelprojekte einsetzen können.
- In **Teil III** lernen Sie das **Terminal** kennen. In mehreren Kapiteln lernen Sie, mit welchen Kommandos Sie das Dateisystem durchsuchen, wie Sie Dokumente und Bilder in andere Formate konvertieren, wie Sie mit den Editoren Emacs und Vi umgehen und den Kommandointerpreter `bash` nutzen.
- **Teil IV** widmet sich der **Konfiguration**. Egal, ob es gerade bei Ihrer Hardware Probleme gibt oder ob Sie ganz besondere Anforderungen stellen – hier erfahren Sie, wie Sie das Dateisystem administrieren, das Grafiksystem konfigurieren, Software-Pakete installieren und aktualisieren, den Systemstart konfigurieren sowie den Kernel und seine Module einrichten bzw. neu kompilieren.
- **Teil V** zeigt, wie Sie **Linux im lokalen Netzwerk** nutzen – vom Client (LAN, WLAN) bis zum Server (Internet-Gateway, DNS, NFS, Samba, AFP), wahlweise mit IPv4 oder mit IPv6.
- **Teil VI** behandelt **Root-Server**, also Server, die extern in einem Rechenzentrum laufen und direkten Internetzugang haben. Wenn Sie einen derartigen Server mieten, werden Sie dort wahrscheinlich Web-, Mail- und Datenbank-Server einrichten – und vielleicht sogar mit ownCloud Ihre eigene Mini-Cloud bilden.
- **Teil VII** hat verschiedene Aspekte der **Sicherheit** zum Thema. Dort erfahren Sie, wie Sie Backups durchführen, wie Sie Ihre Server durch Firewalls, SELinux oder AppArmor schützen und wie Sie mit KVM einzelne Server-Funktionen in getrennten virtuellen Maschinen voneinander isolieren.

Neu in dieser Auflage

Das Buch wurde für diese 13. Auflage vollständig aktualisiert und teilweise neu strukturiert. Ganz neu sind ein umfassendes Kapitel zum Raspberry Pi sowie die durchgängige Berücksichtigung von IPv6 bei der Netzwerk- und Server-Konfiguration. Die folgende Liste nennt in Stichpunkten einige weitere Neuerungen:

- Media-Center mit XBMC
- Account-Administration mit `chage`
- Grafik: Vorschau auf Mir und Wayland
- Systemd: neue Konfigurationsdateien, Journal
- EFI Secure Boot im Zusammenspiel mit GRUB
- Netzwerkkonfiguration mit `ip` (`ifconfig` und `route` sind obsolet)
- FirewallD
- MariaDB (eine MySQL-Alternative)
- STARTTLS bei Postfix/Dovecot

Formales

Kommandos

In diesem Buch sind die Teile eines Kommandos, die tatsächlich einzugeben sind, fett hervorgehoben. Im folgenden Beispiel müssen Sie also nur `ls *.tex` eingeben, um sich die Liste aller `*.tex`-Dateien im aktuellen Verzeichnis anzeigen zu lassen.

```
user$ ls *.tex
article.tex
...
```

Mehrzeilige Kommandos

Falls einzelne Kommandos so lang sind, dass sie nicht in einer Zeile Platz finden, werden sie mit dem Zeichen `\` auf zwei oder mehr Zeilen verteilt. In diesem Fall können Sie die Eingabe entweder in einer Zeile ohne `\` tippen oder sie wie im Buch auf mehrere Zeilen verteilen. `\` ist also ein unter Linux zulässiges Zeichen, um mehrzeilige Kommandoeingaben durchzuführen.

root

Manche Kommandos können nur vom Systemadministrator `root` ausgeführt werden. In diesem Fall wird der Kommandoprompt als `root#` dargestellt:

```
root# service nfs restart
```

sudo

Bei manchen Distributionen ist der Account für `root` gesperrt, z. B. bei Ubuntu. In diesem Fall müssen Sie Systemkommandos mit `sudo` ausführen (siehe auch Abschnitt 16.3):

```
user$ sudo service nfs restart
Password: ********
```

TEIL I

Installation

Kapitel 1
Was ist Linux?

Um die einleitende Frage zu beantworten, erkläre ich in diesem Kapitel zuerst einige wichtige Begriffe, die im gesamten Buch immer wieder verwendet werden: Betriebssystem, Unix, Distribution, Kernel etc. Ein knapper Überblick über die Merkmale von Linux und die verfügbaren Programme macht deutlich, wie weit die Anwendungsmöglichkeiten von Linux reichen. Es folgt ein kurzer Ausflug in die Geschichte von Linux: Sie erfahren, wie Linux entstanden ist und auf welchen Komponenten es basiert.

Von zentraler Bedeutung ist dabei natürlich die *General Public License* (kurz GPL), die angibt, unter welchen Bedingungen Linux weitergegeben werden darf. Erst die GPL macht Linux zu einem freien System, wobei »frei« mehr heißt als einfach »kostenlos«!

1.1 Einführung

Linux ist ein Unix-ähnliches Betriebssystem. Der wichtigste Unterschied gegenüber herkömmlichen Unix-Systemen besteht darin, dass Linux zusammen mit dem vollständigen Quellcode frei kopiert werden darf.

Betriebssystem

Ein Betriebssystem ist ein Bündel von Programmen, mit denen die grundlegendsten Funktionen eines Rechners realisiert werden: die Schnittstelle zwischen Mensch und Maschine (also konkret: die Verwaltung von Tastatur, Bildschirm etc.) und die Verwaltung der Systemressourcen (CPU-Zeit, Speicher etc.). Sie benötigen ein Betriebssystem, damit Sie ein Anwendungsprogramm überhaupt starten und eigene Daten in einer Datei speichern können. Populäre Betriebssysteme sind Windows, Linux, BSD, OS X und iOS.

Unix

Schon lange vor Windows, Linux oder OS X gab es Unix. Dieses Betriebssystem war von Anfang an mit Merkmalen ausgestattet, die von Microsoft erst sehr viel später in einer vergleichbaren Form angeboten wurden: echtes Multitasking, eine Trennung der Prozesse voneinander, klar definierte Zugriffsrechte für Dateien, ausgereifte Netzwerkfunktionen etc. Allerdings bot Unix anfänglich nur eine sparta-

nische Benutzeroberfläche und stellte hohe Hardware-Anforderungen. Das erklärt, warum Unix fast ausschließlich auf teuren Workstations im wissenschaftlichen und industriellen Bereich eingesetzt wurde.

Unix wird in diesem Buch als Oberbegriff für diverse vom ursprünglichen Unix abgeleitete Betriebssysteme verwendet. Die Namen dieser Betriebssysteme enden im Regelfall auf -ix (Irix, Xenix etc.) und sind zumeist geschützte Warenzeichen der jeweiligen Firmen. Auch UNIX selbst ist ein geschütztes Warenzeichen.

Linux

Linux ist eine Unix-Variante, bei der aber der Quelltext frei verfügbar ist. Große Teile des Internets (z. B. Google) werden heute von Linux getragen. Linux läuft nicht nur auf herkömmlichen Rechnern, sondern in Form von Android auf Smartphones und Tablets, auf Embedded Devices (z. B. ADSL-Routern, NAS-Festplatten) und in Supercomputern. Mehr als 90 Prozent der 500 schnellsten Rechner der Welt verwenden Linux (*http://www.top500.org/statistics/list*).

Kernel

Genau genommen bezeichnet der Begriff Linux nur den Kernel: Er ist der innerste Teil (Kern) eines Betriebssystems mit ganz elementaren Funktionen, wie Speicherverwaltung, Prozessverwaltung und Steuerung der Hardware. Die Informationen in diesem Buch beziehen sich auf den Kernel 3.*n*.

1.2 Hardware-Unterstützung

Linux unterstützt beinahe die gesamte gängige PC-Hardware und läuft darüber hinaus auch auf unzähligen anderen Hardware-Plattformen, z. B. auf Smartphones mit ARM-CPUs. Dennoch sollten Sie beim Kauf eines neuen Rechners ein wenig aufpassen. Es gibt einige Hardware-Komponenten, die im Zusammenspiel mit Linux oft Probleme machen:

- **EFI/UEFI:** Seit Herbst 2012 wendet sich die PC-Industrie unter dem Druck von Microsoft vom alten BIOS ab. Neue Rechner bzw. Mainboards werden nun fast ausschließlich durch das Extensible Firmware Interface (EFI) gestartet. Immer häufiger ist dabei auch die Zusatzfunktion UEFI Secure Boot im Einsatz.

  Grundsätzlich sind die meisten aktuellen Linux-Distributionen EFI-kompatibel, und auch UEFI Secure Boot wird immer häufiger unterstützt (siehe Tabelle 2.1). Das ändert aber nichts daran, dass EFI für den PC-Sektor eine neue Technologie ist, die noch unter vielen Kinderkrankheiten leidet und im Zusammenspiel mit Linux oft zickt. Kaum ein Hersteller macht sich die Mühe, die eigene EFI-Implementierung auch mit ein, zwei Linux-Distributionen zu testen.

- **Grafikkarten:** Fast alle am Markt vertretenen Grafikkarten bzw. in die CPU integrierten Grafik-Cores funktionieren unter Linux. Neue Grafikkarten von NVIDIA und ATI/AMD erfordern allerdings oft einen proprietären Zusatztreiber, damit die Karte perfekt genutzt werden kann (3D-Funktionen, Energiesparfunktionen, Audio via HDMI etc.). Die Installation dieser Treiber macht aber oft Probleme.

  Für viele Linux-Anwender ohne besondere Anforderungen an das Grafiksystem sind Intel-CPUs mit eingebautem Grafik-Code die optimale Lösung. Die erforderlichen Treiber liegen als Open-Source-Code vor und funktionieren ausgezeichnet. Die einzige Ausnahme sind die Grafikkerne GMA 500, 600, 3600 und 3650 (»Poulsbo«), die in manchen Netbooks zum Einsatz kamen und nach wie vor in einigen Atom-CPUs integriert sind.

  Problematisch sind schließlich Hybrid-Grafiksysteme, bei denen ein energiesparender interner Grafik-Core mit einer schnelleren externen Grafikkarte kombiniert wird. Mit geeigneten Windows- oder OS-X-Treibern wechselt das Betriebssystem im laufenden Betrieb zwischen dem Grafik-Code und der Grafikkarte. Unter Linux funktioniert das – wenn überhaupt – nur nach einer zeitaufwendigen, komplizierten Konfiguration.

  Umfassende Hintergrundinformationen zum Thema Grafik folgen in Kapitel 24. Dort wird auch der Umgang und die manuelle Konfiguration der wichtigsten Treiber beschrieben.

- **WLAN- und Netzwerk-Adapter:** WLAN- und LAN-Controller machen nur relativ selten Probleme. Nur ganz neue Modelle werden von Linux oft noch nicht unterstützt. Als Übergangslösung bis zum Erscheinen einer Linux-Distribution mit einem kompatiblen Linux-Kernel können Sie einen USB-Adapter einsetzen.

- **SSD-Cache:** Manche Notebooks kombinieren eine herkömmliche Festplatte mit einer kleinen SSD. In der Theorie erhalten Sie damit das Beste aus beiden Welten, also viel Speicherplatz und hohe Geschwindigkeit für wenig Geld. Die Praxis sieht zumeist schon unter Windows weit weniger rosig aus. Wenn dann auch noch Linux ins Spiel kommt, ist es mit den Vorteilen des SSD-Caches ganz vorbei. Im besten Fall ignoriert Linux den SSD-Cache ganz einfach und läuft so, als gäbe es nur eine herkömmliche Festplatte; im ungünstigsten Fall verursachen Sie ein defektes Dateisystem, wenn Sie unter Linux in eine Windows-Partition schreiben, deren Daten sich teilweise im SSD-Cache befinden. Investieren Sie ein paar Euro mehr in ein Notebook, das nur eine SSD enthält – es lohnt sich!

- **Windows-only-Hardware:** Vermeiden Sie Windows-spezifische Zusatz-Hardware, die keinen öffentlichen Standards entspricht und eigens für Windows entwickelte Treiber erfordert. Zum Glück werden solche Komponenten (z. B. GDI-Drucker) zunehmend seltener.

Stellen Sie also *vor* dem Kauf eines neuen Rechners bzw. einer Hardware-Erweiterung sicher, dass alle Komponenten von Linux unterstützt werden. Werfen Sie dazu eventuell einen Blick in die in Tabelle 1.1 aufgelisteten Webseiten. Auch eine Internetsuche nach *linux hardwarename* kann nicht schaden. Lesenswert sind schließlich Testberichte der Zeitschrift c't; deren Redakteure machen sich bei den meisten Geräten die Mühe, auch die Linux-Kompatibilität zu testen.

Distribution/Hardware	Link
Debian	*http://wiki.debian.org/Hardware*
Fedora	*http://fedoraproject.org/wiki/HCL*
openSUSE	*http://en.opensuse.org/Hardware*
Ubuntu	*http://wiki.ubuntuusers.de/Hardwaredatenbanken* *https://wiki.ubuntu.com/HardwareSupport*
Notebooks	*http://www.linux-on-laptops.com* *http://tuxmobil.org*
Grafikkarten	*http://wiki.x.org/wiki/Projects/Drivers*
Drucker	*http://www.openprinting.org/printers*
Scanner	*http://www.sane-project.org*

Tabelle 1.1 Webseiten zum Thema Linux-Hardware

Checkliste für das ideale Linux-Notebook bzw. den idealen Linux-PC

Wenn ich mir einen neuen Rechner kaufe, beachte ich zumeist die folgenden Punkte:

- **EFI:** Kann UEFI Secure Boot ausgeschaltet werden? Enthält das EFI Kompatibilitätsfunktionen, die es BIOS-kompatibel machen?
- **CPU und Grafik:** Es kommt nur eine in die 64-Bit-CPU integrierte Grafiklösung infrage, die mit Open-Source-Treibern gut funktioniert, momentan z. B. Intel Ivy Bridge oder Haswell.
- **Speicher:** Es muss eine SSD sein. Größere Datenmengen speichere ich extern auf einem NAS-Gerät, in einem Cloud-Speicher etc.
- **Kein Windows:** Nach Möglichkeit kaufe ich Geräte ohne vorinstalliertes Windows, auch wenn die Preisersparnis oft gering ist.
- **Lieber etwas älter:** Um ganz neue Geräte mache ich nach Möglichkeit einen großen Bogen, auch wenn die Spezifikationen noch so verlockend sind.

1.3 Distributionen

Noch immer ist die einleitende Frage – Was ist Linux? – nicht ganz beantwortet. Viele Anwender interessiert der Kernel nämlich herzlich wenig, sofern er nur läuft und die vorhandene Hardware unterstützt. Für sie umfasst der Begriff Linux, wie er umgangssprachlich verwendet wird, neben dem Kernel auch das riesige Bündel von Programmen, das mit Linux mitgeliefert wird: Dazu zählen neben unzähligen Kommandos die Desktop-Systeme KDE und Gnome, das Office-Paket LibreOffice bzw. OpenOffice, der Webbrowser Firefox, das Zeichenprogramm Gimp sowie zahllose Programmiersprachen und Server-Programme (Webserver, Mail-Server, File-Server etc.).

Als Linux-Distribution wird also die Einheit bezeichnet, die aus dem eigentlichen Betriebssystem (Kernel) und seinen Zusatzprogrammen besteht. Eine Distribution ermöglicht eine rasche und bequeme Installation von Linux. Die meisten Distributionen können kostenlos aus dem Internet heruntergeladen werden, lediglich einige kommerzielle Angebote sind kostenpflichtig.

Distributionen unterscheiden sich vor allem durch folgende Punkte voneinander:

- **Umfang, Aktualität:** Die Anzahl, Auswahl und Aktualität der mitgelieferten Programme und Bibliotheken variiert stark. Manche Distributionen setzen bewusst auf etwas ältere, stabile Versionen (z. B. Debian).
- **Installations- und Konfigurationswerkzeuge:** Die mitgelieferten Programme zur Installation, Konfiguration und Wartung des Systems helfen dabei, die Konfigurationsdateien einzustellen. Gut funktionierende Konfigurationswerkzeuge sparen viel Zeit.
- **Konfiguration des Desktops (KDE, Gnome):** Manche Distributionen lassen dem Anwender die Wahl zwischen KDE, Gnome und eventuell weiteren Window Managern. Es gibt aber auch Unterschiede in der Detailkonfiguration von KDE oder Gnome, die das Aussehen, die Menüanordnung etc. betreffen.
- **Hardware-Unterstützung:** Linux kommt mit den meisten PC-Hardware-Komponenten zurecht. Dennoch gibt es im Detail Unterschiede zwischen den Distributionen, insbesondere wenn es darum geht, Nicht-Open-Source-Treiber (z. B. für NVIDIA-Grafikkarten) in das System zu integrieren.
- **Paketsystem:** Das Paketsystem bestimmt, wie einfach die spätere Installation zusätzlicher Programme bzw. das Update vorhandener Programme ist. Zurzeit sind drei zueinander inkompatible Paketsysteme üblich: RPM (unter anderem bei Fedora, Red Hat, SUSE), DEB (Debian, Ubuntu) und TXZ (Slackware).

  Grundsätzlich gilt, dass Sie eine Linux-Distribution nur so lange sicher betreiben können, wie Sie Updates bekommen. Danach ist aus Sicherheitsgründen ein

Wechsel auf eine neue Version der Distribution erforderlich. Deswegen ist es bedeutsam, wie lange es für eine Distribution Updates gibt. Hier gilt meist die Grundregel: je teurer die Distribution, desto länger der Zeitraum. Einige Beispiele (Stand: Sommer 2013):

Fedora:	13 Monate
Ubuntu:	9 Monate, für LTS-Versionen 3 bis 5 Jahre
openSUSE:	18 Monate
Red Hat Enterprise Linux:	10 Jahre (mit Einschränkungen sogar 13 Jahre)
SUSE Enterprise Server:	7 bis 9 Jahre

- **Live-System:** Viele Distributionen ermöglichen den Linux-Betrieb direkt von einer CD oder DVD. Das ist zwar vergleichsweise langsam und unflexibel, ermöglicht aber ein einfaches Ausprobieren von Linux. Außerdem bieten Live-Systeme eine ideale Möglichkeit, um ein defektes Linux-System zu reparieren.
- **Zielplattform (CPU-Architektur):** Viele Distributionen sind nur für Intel- und AMD-kompatible Prozessoren erhältlich, in der Regel in einer 32- und in einer 64-Bit-Variante. Es gibt aber auch Distributionen für andere Prozessorplattformen, z. B. für ARM- oder für PowerPC-CPUs.
- **Dokumentation:** Große Unterschiede gibt es bei der Qualität und dem Umfang der Online-Dokumentation. Gedruckte Handbücher sind nur noch ganz vereinzelt zu bekommen.
- **Support:** Bei kommerziellen Distributionen bekommen Sie Hilfe bei der Installation (via E-Mail und/oder per Telefon).
- **Lizenz:** Die meisten Distributionen sind kostenlos erhältlich. Bei einigen Distributionen gibt es hier aber Einschränkungen: Beispielsweise ist bei den Enterprise-Distributionen von Red Hat und SUSE ein Zugriff auf das Update-System nur für registrierte Kunden möglich.

Kommerzielle Distributionen

Die Behauptung, Linux sei frei, steht scheinbar im krassen Widerspruch zu dem Preis für Enterprise-Distributionen für den Unternehmenseinsatz. Allerdings zahlen Sie bei kommerziellen Distributionen von Red Hat, SUSE oder anderen Anbietern nicht für die Software an sich, sondern für die dazugehörenden Zusatzleistungen: Update-Service, Support etc.

Freie Distributionen

Die populärsten Distributionen für den Privatbereich sind durchweg kostenlos: Debian, Fedora, openSUSE, Ubuntu etc. Bei diesen Distributionen können Sie ISO-Dateien aus dem Internet herunterladen und damit selbst die Installations-CDs oder -DVDs brennen bzw. einen USB-Stick zum Start der Installation erstellen.

Welche Distribution für welchen Zweck?

Die Frage, welche Distribution die beste sei, welche wem zu empfehlen sei etc., artet leicht zu einem Glaubenskrieg aus. Wer sich einmal für eine Distribution entschieden und sich an deren Eigenheiten gewöhnt hat, der steigt nicht so schnell

auf eine andere Distribution um. Ein Wechsel der Distribution ist nur durch eine Neuinstallation möglich, bereitet also einige Mühe.

Kriterien für die Auswahl einer Distribution sind die Aktualität ihrer Komponenten (achten Sie auf die Versionsnummer des Kernels und wichtiger Programme, etwa des C-Compilers), die Qualität der Installations- und Konfigurationstools, der angebotene Support, mitgelieferte Handbücher etc.

Linux Standard Base (LSB)

So belebend die Konkurrenz vieler Distributionen für deren Weiterentwicklung ist, so lästig ist sie bei der Installation von Programmen, die nicht mit der Distribution mitgeliefert werden – insbesondere bei kommerziellen Programmen. Eine fehlende oder veraltete Programmbibliothek ist oft die Ursache dafür, dass ein Programm nicht läuft. Die Problembehebung ist insbesondere für Linux-Einsteiger fast unmöglich. Abhilfe schafft das Linux-Standard-Base-Projekt (LSB): Die LSB-Spezifikation definiert Regeln, die einen gemeinsamen Nenner aller am LSB-Projekt beteiligten Distributionen sicherstellen:

http://www.linuxfoundation.org/collaborate/workgroups/lsb

Gängige Linux-Distributionen

Der folgende Überblick über die wichtigsten verfügbaren Distributionen (in alphabetischer Reihenfolge und ohne Anspruch auf Vollständigkeit!) soll eine erste Orientierungshilfe geben. Beachten Sie bitte, dass die Landschaft der Linux-Distributionen sich ständig verändert: Neue Distributionen entstehen und werden oft rasch beliebt (das ist beinahe wie mit Mode-Trends), andere verlieren ebenso rasch an Bedeutung oder werden ganz eingestellt. Dieser Abschnitt ist also nur eine – ohnedies subjektive – Momentaufnahme.

Android

Android ist eine von Google entwickelte Plattform für Mobilfunkgeräte und Tablets. Die Open-Source-Freiheiten stoßen bei Android allerdings rasch an ihre Grenzen: Viele Handy-Hersteller modifizieren Android und verhindern bzw. verbieten die manuelle Installation anderer Android-Versionen.

CentOS und Scientific Linux

CentOS und **Scientific Linux** sind zwei kostenlose Varianten zu Red Hat Enterprise Linux (RHEL). Beide Distributionen sind binärkompatibel zu RHEL, es fehlen aber alle Red-Hat-Markenzeichen, -Logos etc. Die Distributionen sind vor allem für Server-Betreiber interessant, die kompatibel zu RHEL sein möchten, sich die hohen RHEL-Kosten aber nicht leisten können und auf den Red-Hat-Support verzichten können.

Chrome OS

Das **Chrome OS** wird wie Android von Google entwickelt. Es ist für Notebooks optimiert und setzt zur Nutzung eine aktive Internetverbindung voraus. Die minimalistische Benutzeroberfläche basiert auf dem Google Chrome Webbrowser.

Debian

Debian ist die älteste vollkommen freie Distribution. Sie wird von engagierten Linux-Entwicklern zusammengestellt, wobei die Einhaltung der Spielregeln »freier« Software eine hohe Priorität genießt. Die strikte Auslegung dieser Philosophie hat in der Vergangenheit mehrfach zu Verzögerungen geführt.

Debian richtet sich an fortgeschrittene Linux-Anwender und hat einen großen Marktanteil bei Server-Installationen. Im Vergleich zu anderen Distributionen ist Debian stark auf maximale Stabilität hin optimiert und enthält deswegen oft relativ alte Programmversionen. Dafür steht Debian für elf Hardware-Plattformen zur Verfügung (unter anderem amd64, ARM, i386, IA64, Mips, Mipsel, PPC, S390 und Sparc). Es gibt zahlreiche Distributionen, die sich von Debian ableiten (z. B. Ubuntu).

Fedora

Fedora ist der kostenlose Entwicklungszweig von Red Hat Linux. Die Entwicklung wird von Red Hat unterstützt und gelenkt. Für Red Hat ist Fedora eine Art Spielwiese, auf der neue Funktionen ausprobiert werden können, ohne die Stabilität der Enterprise-Versionen zu gefährden. Programme, die sich unter Fedora bewähren, werden später in die Enterprise-Versionen integriert. Für technisch interessierte Linux-Fans ist Fedora interessant, weil diese Distribution oft eine Vorreiterrolle spielt: Neue Linux-Funktionen finden sich oft zuerst in Fedora und erst später in anderen Distributionen. Neue Fedora-Versionen erscheinen alle sechs Monate. Updates werden einen Monat nach dem Erscheinen der übernächsten Version eingestellt, d. h., die Lebensdauer ist mit 13 Monaten sehr kurz.

Gentoo

Gentoo richtet sich an Programmentwickler und an Anwender, die maximale Flexibilität und Kontrolle über ihre Distribution wünschen. Die Besonderheit von Gentoo besteht darin, dass jedes Programmpaket eigens kompiliert und so optimal an die jeweilige Hardware angepasst werden kann. Natürlich können Linux-Profis bei jeder Distribution ihre Programme selbst kompilieren. Aber Gentoo unterstützt diesen Prozess besonders gut durch entsprechende Konfigurationswerkzeuge.

Knoppix

Das auf Debian basierende **Knoppix** war vor einem Jahrzehnt eines der ersten und am besten funktionierenden Live-Systeme. Mittlerweile bietet nahezu jede Distribution auch eine Live-Variante an. Dementsprechend hat Knoppix an Popularität verloren.

openSUSE

openSUSE ist eine kostenlose Linux-Distribution, die gleichzeitig als Entwicklungs- und Testbasis für die Enterprise-Versionen von SUSE dient. openSUSE-Versionen erscheinen momentan in einem 8-Monatsrhythmus; es gibt aber Diskussionen, auf einen einjährigen Zyklus umzusteigen. Der Update-Zeitraum beträgt 18 Monate.

Oracle

Oracle bietet seit Herbst 2006 eine eigene Version von Red Hat Enterprise Linux (RHEL) an, anfänglich unter dem Namen »Oracle Unbreakable Linux«, mittlerweile einfach als **Oracle Linux**. Das ist aufgrund der Open-Source-Lizenzen eine zulässige

Vorgehensweise. Technisch gibt es nur wenige Unterschiede zu RHEL, die Oracle-Variante ist aber billiger und ohne Support sogar kostenlos verfügbar. Dennoch ist die Verbreitung von Oracles Linux-Variante bisher gering.

Red Hat

Red Hat ist die international bekannteste und erfolgreichste Linux-Firma. Red-Hat-Distributionen dominieren insbesondere den amerikanischen Markt. Die Paketverwaltung auf der Basis des RPM-Formats (einer Eigenentwicklung von Red Hat) wurde von vielen anderen Distributionen übernommen.

Red Hat ist überwiegend auf Unternehmenskunden ausgerichtet. Die Enterprise-Versionen (RHEL = **Red Hat Enterprise Linux**) sind vergleichsweise teuer. Sie zeichnen sich durch hohe Stabilität und einen zehnjährigen Update-Zeitraum aus. Für Linux-Enthusiasten und -Entwickler, die ein Red-Hat-ähnliches System zum Nulltarif suchen, bieten sich **CentOS**, **Scientific Linux** und **Fedora** an.

SUSE

Nachdem Novell 2010 von Attachmate übernommen wurde, werden die kommerziellen **SUSE**-Distributionen von der nun wieder selbstständigen SUSE GmbH entwickelt und verkauft. SUSE gilt weltweit als die Nummer zwei auf dem kommerziellen Linux-Markt. Ähnlich wie Red Hat fährt auch SUSE zweigleisig: Auf der einen Seite gibt es unter dem Namen SUSE diverse Enterprise-Distributionen für Firmenkunden. Auf der anderen Seite steht die freie Distribution openSUSE, die sich an private Linux-Anwender und -Entwickler richtet. Eine Kooperation mit Microsoft schützt SUSE vor Patentklagen. Allerdings wurde dieses noch von Novell ausgehandelte Übereinkommen von vielen Open-Source-Entwicklern als indirekte Anerkennung der Patentansprüche Microsofts kritisiert.

Ubuntu

Ubuntu ist die zurzeit populärste Distribution für Privatanwender. Ubuntu verwendet als Basis Debian, ist aber besser für Desktop-Anwender optimiert (Motto: *Linux for human beings*). Die kostenlose Distribution erscheint im Halbjahresrhythmus. Für gewöhnliche Versionen werden Updates über neun Monate zur Verfügung gestellt. Für die alle zwei Jahre erscheinenden LTS-Versionen gibt es sogar 3 bzw. 5 Jahre lang Updates (für Desktop- bzw. Server-Pakete).

Finanziell wird Ubuntu Linux durch die Firma Canonical unterstützt. Canonical arbeitet momentan auch an Ubuntu-Versionen für Smartphones, Tablets und TV-Geräte.

Zu Ubuntu gibt es diverse offizielle und inoffizielle Varianten: **Kubuntu**, **Xubuntu**, **Ubuntu Server**, **Linux Mint** etc.

Andere Distributionen

Neben den oben aufgezählten »großen« Distributionen gibt es im Internet zahlreiche Zusammenstellungen von Miniatursystemen (bis hin zum kompletten Linux-System auf einer einzigen Diskette!). Diese Distributionen basieren zumeist auf alten und daher kleineren Kernelversionen. Sie sind vor allem für Spezialaufgaben konzi-

piert, etwa für Wartungsarbeiten (Emergency-Systeme), oder um ein Linux-System ohne eigentliche Installation verwenden zu können (Live-Systeme). Populäre Vertreter dieser Linux-Gattung sind **Devil Linux**, **Damn Small Linux**, **Parted Magic**, **Puppy**, **SystemRescueCd**, **TinyCore** und **TinyMe**.

Einen ziemlich guten Überblick über alle momentan verfügbaren Linux-Distributionen (egal ob kommerziellen oder anderen Ursprungs) finden Sie im Internet auf den folgenden Seiten:

http://www.distrowatch.com
http://lwn.net/Distributions

Die Qual der Wahl

Eine Empfehlung für eine bestimmte Distribution ist schwierig. Für Linux-Einsteiger ist es zumeist von Vorteil, sich vorerst für eine weitverbreitete Distribution wie Fedora, openSUSE oder Ubuntu zu entscheiden. Zu diesen sind sowohl im Internet als auch im Buch- und Zeitschriftenhandel viele Informationen verfügbar. Bei Problemen ist es vergleichsweise leicht, Hilfe zu finden.

Kommerzielle Linux-Anwender bzw. Server-Administratoren müssen sich entscheiden, ob sie bereit sind, für professionellen Support Geld auszugeben. In diesem Fall spricht wenig gegen die Marktführer Red Hat und SUSE. Andernfalls sind CentOS, Debian und Ubuntu attraktive kostenlose Alternativen.

1.4 Traum und Wirklichkeit

Dieser Abschnitt nimmt zu einigen oft gehörten Behauptungen und Vorurteilen zu Linux Stellung. Mein Ziel ist es, Ihnen ein abgerundetes Bild von Linux zu präsentieren, ohne die Übertreibungen vieler begeisterter Linux-Fans, aber auch ohne die Schwarzmalerei der Linux-Gegner, die Linux oft nur deswegen schlechtmachen, weil sie ihre eigenen Software-Geschäfte in Gefahr sehen.

Linux ist schneller als Windows

Es lässt sich nicht allgemeingültig sagen, ob Windows oder Linux schneller bzw. effizienter läuft. Wenn einzelne Programme unter Linux oder unter Windows schneller ausgeführt werden, hat das zumeist damit zu tun, für welches Betriebssystem das Programm optimiert wurde, welche Linux- und Windows-Versionen miteinander verglichen werden, welche Hardware für den Vergleich verwendet wurde etc.

Linux benötigt weniger Ressourcen

Nach wie vor gibt es Linux-Distributionen, die auf einem uralten Pentium-PC mit einigen MByte RAM laufen – freilich nur im Textmodus und nicht mit dem Funktionsreichtum aktueller Betriebssysteme. Interessanter ist ein Vergleich zwischen einer aktuellen Linux-Distribution und Windows 7 oder 8: Für einen komfortablen Desktop-Einsatz benötigen Sie in beiden Fällen einen einigermaßen aktuellen Rechner. Linux stellt dabei etwas geringere Hardware-Anforderungen als Windows.

Linux ist sicherer als Windows

Alle gängigen Betriebssysteme leiden an Sicherheitsproblemen. Linux schneidet in den meisten Vergleichen relativ gut ab. Dennoch gibt es selbst in jahrzehntealten Netzwerkprogrammen immer wieder neue Sicherheitslücken. Letztlich hängt es vom Einsatzzweck ab, wie sicher Linux ist:

- In Desktop-Anwendungen ist Linux im Gegensatz zu Windows fast vollständig virensicher. Es hat bis jetzt keinen einzigen nennenswerten Virenbefall unter Linux gegeben. Gewöhnliche Benutzer können unter Linux kaum größere Schäden am System anrichten. Das liegt unter anderem daran, dass es unter Linux seit jeher unüblich war, gewöhnliche Programme mit Systemadministratorrechten auszuführen.
- Bei der Anwendung von Linux als Netzwerk- oder Internet-Server hängt die Sicherheit sehr stark von der Wartung des Systems ab. Beinahe zu allen Sicherheitsproblemen der vergangenen Jahre gab es bereits Updates, bevor diese Sicherheitsrisiken allgemein bekannt und von Hackern ausgenutzt wurden. Regelmäßige Updates sind also unverzichtbar!

Linux ist stabiler als Windows

Als Linux in den 90er-Jahren populär wurde, begann Microsoft Windows 95 gerade seinen Siegeszug. Die Aussage, dass Linux viel stabiler als Windows sei, war damals leicht zu untermauern. Mittlerweile hat Microsoft durchaus respektable und stabile Windows-Versionen zustande gebracht. In jedem Fall erfordern Aussagen zur Stabilität von Linux jetzt eine Differenzierung:

- Der Kernel an sich ist außerordentlich stabil. Ich arbeite nun schon seit vielen Jahren mit Linux, aber einen richtigen Absturz des gesamten Betriebssystems habe ich nur sehr selten erlebt; wenn doch, war meist defekte oder falsch konfigurierte Hardware schuld.
- Wenn Sie mit Linux aber das Gesamtsystem der mitgelieferten Software meinen (also eine ganze Distribution, inklusive Grafiksystem, KDE oder Gnome etc.), dann sieht es mit der Stabilität erheblich schlechter aus. Programme wie Firefox oder LibreOffice sind auch unter Linux nicht vor Abstürzen sicher.

Als wie stabil Sie Linux empfinden, hängt davon ab, wie Sie Linux einsetzen: Die besten Erfahrungen werden Sie machen, wenn Sie Linux primär als Netzwerk-Server, als Workstation für eher wissenschaftlich orientierte Arbeiten oder zum Programmieren einsetzen. Je stärker Sie sich aber anwendungsorientierten Programmen zuwenden und Linux als Desktop-System einsetzen, desto eher werden Sie auch die negativen Seiten kennenlernen.

Linux ist billiger als Windows

Linux ist kostenlos erhältlich. Microsoft weist deswegen gern darauf hin, dass auch Schulungskosten etc. berücksichtigt werden müssen. In solchen Rechenbeispielen wird Windows-Wissen meist als gottgegeben vorausgesetzt. Außerdem ist nicht jede Linux-Distribution tatsächlich kostenlos. Gerade Firmen greifen oft zu den kommer-

ziellen Angeboten von Red Hat oder SUSE, die Support, lange Update-Zeiträume etc. einschließen. Aber selbst bei Berücksichtigung dieser Faktoren ist der Kostenvorteil von Linux nicht zu leugnen.

Linux ist kompliziert zu installieren

Wenn man einen PC kauft, ist Windows meist schon vorinstalliert. Insofern stellt es natürlich einen Mehraufwand dar, Linux zusätzlich zu installieren. Wie Sie im nächsten Kapitel feststellen werden, ist eine Linux-Installation aber mittlerweile unkompliziert – und sicher nicht schwieriger als eine Windows-Installation. Aber wer installiert Windows schon selbst?

Problematisch ist lediglich die Unterstützung neuer Hardware, die unter Windows besser ist: Jeder Hersteller von Computer-Komponenten stellt selbstverständlich einen Windows-Treiber zur Verfügung. Vergleichbare Treiber für Linux müssen dagegen oft von der Open-Source-Gemeinschaft programmiert werden. Das dauert natürlich eine gewisse Zeit.

Linux ist kompliziert zu bedienen

Dieses Vorurteil ist alt, aber nicht mehr bzw. nur noch in einem sehr geringen Maß zutreffend. Linux ist anders zu bedienen als Windows, so wie auch Apples OS X anders zu bedienen ist. Wirklich schwieriger ist die Handhabung von Linux zumeist nicht, lediglich die Umgewöhnung von Windows kann manchmal mühsam sein.

Windows-Programme laufen nicht unter Linux

Viele Programme, wie Microsoft Office, Adobe Photoshop etc., stehen momentan nur für die Betriebssysteme Windows und Mac OS X zur Verfügung. Es gibt aber einige Auswege aus diesem Software-Dilemma:

- Für viele Anwendungen stehen unter Linux vergleichbare Programme zur Verfügung – beispielsweise OpenOffice/LibreOffice oder das Bildverarbeitungsprogramm Gimp.
- Manche Windows-Programme können mit der kostenlosen Laufzeitumgebung Wine (*Wine is not an emulator*) unter Linux ausgeführt werden. Wine bietet allerdings wenig Komfort und ist nur für fortgeschrittene Linux-Anwender geeignet.
- Einen höheren Grad an Kompatibilität bietet das kommerzielle Programm CrossOver, das auf Wine basiert. CrossOver erleichtert die Installation und Ausführung der meisten Microsoft-Office-Komponenten sowie einiger anderer Programme.
- Die Programme VMware, VirtualBox sowie diverse andere Virtualisierungslösungen gehen noch einen Schritt weiter: Sie emulieren gleich einen ganzen Rechner. Sie können darin eine Windows-Installation durchführen und Windows dann in einem Fenster ausführen. Das funktioniert hervorragend, ist aber teuer: Sie brauchen eine Lizenz für Windows; dazu kommen bei kommerziellen Virtualisierungsprogrammen noch deren Kosten.

1.5 Open-Source-Lizenzen (GPL & Co.)

Die Grundidee von »Open Source« besteht darin, dass der Quellcode von Programmen frei verfügbar ist und von jedem erweitert bzw. geändert werden darf. Allerdings ist damit auch eine Verpflichtung verbunden: Wer Open-Source-Code zur Entwicklung eigener Produkte verwendet, muss den gesamten Code ebenfalls wieder frei weitergeben.

Die Open-Source-Idee verbietet übrigens keinesfalls den Verkauf von Open-Source-Produkten. Auf den ersten Blick scheint das ein Widerspruch zu sein. Tatsächlich bezieht sich die Freiheit in »Open Source« mehr auf den Code als auf das fertige Produkt. Zudem regelt die freie Verfügbarkeit des Codes auch die Preisgestaltung von Open-Source-Produkten: Nur wer neben dem Kompilat eines Open-Source-Programms weitere Zusatzleistungen anbietet (Handbücher, Support etc.), wird überleben. Sobald der Preis in keinem vernünftigen Verhältnis zu den Leistungen steht, werden sich andere Firmen finden, die es günstiger machen.

General Public License (GPL)

Das Ziel der Open-Source-Entwickler ist es, ein System zu schaffen, dessen Quellen frei verfügbar sind und es auch bleiben. Um einen Missbrauch auszuschließen, sind viele Open-Source-Programme durch die *GNU General Public License* (kurz GPL) geschützt. Hinter der GPL steht die *Free Software Foundation* (FSF). Diese Organisation wurde von Richard Stallman gegründet, um hochwertige Software frei verfügbar zu machen. Richard Stallman ist übrigens auch der Autor des Editors Emacs, der in Kapitel 20 beschrieben wird.

Die Kernaussage der GPL besteht darin, dass zwar jeder den Code verändern und sogar die resultierenden Programme verkaufen darf, dass aber gleichzeitig der Anwender/Käufer das Recht auf den vollständigen Code hat und diesen ebenfalls verändern und wieder kostenlos weitergeben darf. Jedes GNU-Programm muss zusammen mit dem vollständigen GPL-Text weitergegeben werden. Die GPL schließt damit aus, dass jemand ein GPL-Programm weiterentwickeln und verkaufen kann, *ohne* die Veränderungen öffentlich verfügbar zu machen. Jede Weiterentwicklung ist somit ein Gewinn für *alle* Anwender. Den vollständigen Text der GPL finden Sie hier:

http://www.gnu.org/licenses/gpl.html

Die Grundidee der GPL ist recht einfach zu verstehen, im Detail treten aber immer wieder Fragen auf. Viele dieser Fragen werden hier beantwortet:

http://www.gnu.org/licenses/gpl-faq.html

Wenn Sie glauben, dass Sie alles verstanden haben, sollten Sie das GPL-Quiz ausprobieren:

http://www.gnu.org/cgi-bin/license-quiz.cgi

GPL-Versionen

Zurzeit sind drei GPL-Versionen gebräuchlich: GPL 1 (1985), GPL 2 (1991) und GPL 3 (2007). Zu den wichtigsten Neuerungen der GPL 3 zählen:

- **Internationalisierung:** Die GPL 3 ist mit den Rechtskonzepten vieler Länder kompatibel.
- **Software-Patente:** Wer Software unter der GPL 3 entwickelt bzw. weitergibt, darf die Nutzer der Software nicht aufgrund von Software-Patenten verklagen.
- **DRM (Digital Rights Management):** Die GPL 3 nimmt gegen DRM-Software Stellung und stellt fest, dass DRM fundamental inkompatibel mit den Ideen der GPL ist.

Die GPL 3 hat bisher keine so breite Anwendung gefunden wie die GPL 2. Beispielsweise haben sich namhafte Kernelentwickler, darunter Linus Torvalds, gegen eine Umstellung der Kernellizenz auf die GPL 3 ausgesprochen. Das wäre auch aus praktischen Gründen schwierig: Sämtliche Entwickler, die Code zum Kernel beigesteuert haben, müssten zustimmen.

Lesser General Public License (LGPL)

Neben der GPL existiert noch die Variante LGPL (Lesser GPL). Der wesentliche Unterschied zur GPL besteht darin, dass eine derart geschützte Bibliothek auch von kommerziellen Produkten genutzt werden darf, deren Code *nicht* frei verfügbar ist. Ohne die LGPL könnten GPL-Bibliotheken nur wieder für GPL-Programme genutzt werden, was in vielen Fällen eine unerwünschte Einschränkung für kommerzielle Programmierer wäre.

Andere Lizenzen

Durchaus nicht alle Teile einer Linux-Distribution unterliegen den gleichen Copyright-Bedingungen! Obwohl der Kernel und viele Tools der GPL unterliegen, gelten für manche Komponenten und Programme andere rechtliche Bedingungen:

- Beispielsweise gibt es für das X Window System eine eigene Lizenz. Das X Window System wurde ursprünglich von der amerikanischen Universität MIT entwickelt. Die jetzige Lizenz ist von einer früheren Lizenz des MIT abgeleitet.
- Für manche Netzwerk-Tools gilt die BSD-Lizenz. BSD ist wie Linux ein freies Unix-System. Die BSD-Lizenz ist insofern liberaler als die GPL, als die kommerzielle Nutzung ohne die Freigabe des Codes zulässig ist. Die Lizenz ist daher vor allem für kommerzielle Programmierer interessant, die Produkte entwickeln möchten, deren Code sie nicht veröffentlichen müssen.
- Für einige Programme gelten Doppellizenzen. Beispielsweise können Sie den Datenbank-Server MySQL für Open-Source-Projekte, auf einem eigenen Webserver bzw. für die innerbetriebliche Anwendung gemäß der GPL kostenlos einsetzen. Wenn Sie hingegen ein kommerzielles Produkt auf der Basis von MySQL entwickeln und samt MySQL verkaufen möchten, ohne Ihren Quellcode zur

Verfügung zu stellen, dann kommt die kommerzielle Lizenz zum Einsatz. Die Weitergabe von MySQL wird in diesem Fall kostenpflichtig.

- Andere Programme sind zwar kommerziell, es ist aber dennoch eine kostenlose Nutzung möglich. Ein bekanntes Beispiel ist der Adobe Reader zum Lesen von PDF-Dokumenten: Zwar ist das Programm unter Linux kostenlos erhältlich (und darf auch in Firmen kostenlos eingesetzt werden), aber der Quellcode zu diesem Programm ist nicht verfügbar.

Manche Distributionen kennzeichnen die Produkte, bei denen die Nutzung oder Weitergabe eventuell lizenzrechtliche Probleme verursachen könnte. Bei Debian befinden sich solche Programme in der Paketquelle *non-free*.

Das Dickicht der zahllosen, mehr oder weniger »freien« Lizenzen ist schwer zu durchschauen. Die Bandbreite zwischen der manchmal fundamentalistischen Auslegung von »frei« im Sinne der GPL und den verklausulierten Bestimmungen mancher Firmen, die ihr Software-Produkt zwar frei nennen möchten (weil dies gerade modern ist), in Wirklichkeit aber uneingeschränkte Kontrolle über den Code behalten möchten, ist groß. Eine gute Einführung in das Thema geben die beiden folgenden Websites. Das Ziel von *opensource.org* ist es, unabhängig von Einzel- oder Firmeninteressen die Idee (oder das Ideal) von Software mit frei verfügbarem Quellcode zu fördern. Dort finden Sie auch eine Liste von Lizenzen, die der Open-Source-Idee entsprechen.

http://heise.de/-221957
http://www.opensource.org

Lizenzkonflikte zwischen Open- und Closed-Source-Software

Open-Source-Lizenzen für Entwickler

Wenn Sie Programme entwickeln und diese zusammen mit Linux bzw. in Kombination mit Open-Source-Programmen oder -Bibliotheken verkaufen möchten, müssen Sie sich in die bisweilen verwirrende Problematik der unterschiedlichen Software-Lizenzen tiefer einarbeiten. Viele Open-Source-Lizenzen erlauben die Weitergabe nur, wenn auch Sie Ihren Quellcode im Rahmen einer Open-Source-Lizenz frei verfügbar machen. Auf je mehr Open-Source-Komponenten mit unterschiedlichen Lizenzen Ihr Programm basiert, desto komplizierter wird die Weitergabe.

Es gibt aber auch Ausnahmen, die die kommerzielle Nutzung von Open-Source-Komponenten erleichtern: Beispielsweise gilt für Apache und PHP sinngemäß, dass Sie diese Programme auch in Kombination mit einem Closed-Source-Programm frei weitergeben dürfen.

Die Einhaltung der Regeln der GPL kann zumindest in Deutschland gerichtlich erzwungen werden. Diverse Fälle, in denen Firmen Open-Source-Bibliotheken ein-

gesetzt haben, aber ihren eigenen Code nicht zur Verfügung stellen wollten, sind auf der folgenden Website dokumentiert. In den meisten Fällen konnte eine Einigung ohne Gerichtsverfahren erzielt werden.

http://gpl-violations.org

GPL-Probleme mit Hardware-Treibern

Manche proprietäre Treiber für Hardware-Komponenten z. B. für NVIDIA-Grafikkarten bestehen aus einem kleinen Kernelmodul (Open Source) und diversen externen Programmen oder Bibliotheken, deren Quellcode nicht verfügbar ist (Closed Source). Das Kernelmodul hat nur den Zweck, eine Verbindung zwischen dem Kernel und dem Closed-Source-Treiber herzustellen.

Diese Treiber sind aus Sicht vieler Linux-Anwender eine gute Sache: Sie sind kostenlos verfügbar und ermöglichen es, diverse Hardware-Komponenten zu nutzen, zu denen es entweder gar keine oder zumindest keine vollständigen Open-Source-Treiber für Linux gibt. Die Frage ist aber, ob bzw. in welchem Ausmaß die Closed-Source-Treiber wegen der engen Verzahnung mit dem Kernel, der ja der GPL untersteht, diese Lizenz verletzen. Viele Open-Source-Entwickler dulden die Treiber nur widerwillig. Eine direkte Weitergabe mit GPL-Produkten ist nicht zulässig, weswegen der Benutzer die Treiber in der Regel selbst herunterladen und installieren muss.

Die Frage ist allerdings, ob man der Open-Source-Idee mit dieser engen Auslegung der GPL-Regeln nützt oder schadet: Optimisten glauben, dass die Hardware-Firmen dadurch gezwungen wären, selbst Open-Source-Treiber zu entwickeln oder zumindest die erforderlichen Informationen an die Entwicklergemeinde freizugeben. Pessimisten befürchten, dass derartige Hardware dann unter Linux einfach nicht mehr nutzbar wäre, oft ohne gute Alternativen.

1.6 Die Geschichte von Linux

1982: GNU

Da Linux ein Unix-ähnliches Betriebssystem ist, müsste ich an dieser Stelle eigentlich mit der Geschichte von Unix beginnen – aber dazu fehlt hier der Platz. Stattdessen beginnt diese Geschichtsstunde mit der Gründung des GNU-Projekts durch Richard Stallman. GNU steht für *GNU is not Unix*. In diesem Projekt wurden seit 1982 Open-Source-Werkzeuge entwickelt. Dazu zählen der GNU-C-Compiler, der Texteditor Emacs sowie diverse GNU-Utilities wie `find` und `grep` etc.

1989: GPL

Erst sieben Jahre nach dem Start des GNU-Projekts war die Zeit reif für die erste Version der *General Public License*. Diese Lizenz stellt sicher, dass freier Code frei bleibt.

1991: Linux-Kernel 0.01

Die allerersten Teile des Linux-Kernels (Version 0.01) entwickelte Linus Torvalds, der den Programmcode im September 1991 über das Internet freigab. In kürzester Zeit fanden sich weltweit Programmierer, die an der Idee Interesse hatten und

Erweiterungen dazu programmierten. Sobald der Kernel von Linux so weit entwickelt worden war, dass der GNU-C-Compiler darauf lief, stand mit einem Schlag die gesamte Palette der GNU-Tools zur Verfügung. Aus dem bloßen Kernel wurde also ein vollständiges System. Weitere Komponenten waren das Dateisystem Minix, Netzwerk-Software von BSD-Unix, das X Window System des MIT und dessen Portierung XFree86 etc.

Damit sollte klar sein, dass Linux nicht allein Linus Torvalds zu verdanken ist. Hinter Linux stehen vielmehr eine Menge engagierter Menschen, die seit Jahren in ihrer Freizeit, im Rahmen ihres Informatikstudiums und zum Teil auch bezahlt von Firmen wie Google, IBM oder HP freie Software produzieren. Allein der Kernel von Linux umfasst mittlerweile viele Millionen Programmzeilen!

1994: Erste Distributionen

Informatik-Freaks an Universitäten konnten sich Linux und seine Komponenten selbst herunterladen, kompilieren und installieren. Eine breite Anwendung fand Linux aber erst mit Linux-Distributionen, die Linux und die darum entstandene Software auf Disketten bzw. CD-ROMs verpackten und mit einem Installationsprogramm versahen. Vier der zu dieser Zeit entstandenen Distributionen existieren heute noch: Debian, Red Hat, Slackware und SUSE.

1996: Pinguin

1996 wurde der Pinguin zum Linux-Logo.

1998: Microsoft nimmt Linux wahr

Mit dem rasanten Siegeszug des Internets stieg auch die Verbreitung von Linux, vor allem auf Servern. Gewissermaßen zum Ritterschlag für Linux wurde der legendäre Ausspruch von Steve Ballmer: *Microsoft is worried about free software* … Ein Jahr später ging Red Hat spektakulär an die Börse.

2002: Linux fürs Büro

Nachdem Sun StarOffice gekauft und den Quellcode veröffentlicht hatte, wurde 2002 schließlich OpenOffice 1.0 fertiggestellt. Ein komplettes Office-Paket, eingebettet in eine komfortable Benutzeroberfläche (KDE oder Gnome), machte Linux büro- und massentauglich. Damit gelang Linux der Schritt aus der Freak- und Server-Ecke heraus. 2003 entschied sich die Stadt München dafür, rund 14.000 Rechner von Windows auf Linux umzustellen. Diese Migration ist inzwischen abgeschlossen.

2009: Android

Die Android-Plattform von Google bringt Linux seit 2009 auf das Handy. Mittlerweile ist Android die nach Stückzahlen dominierende Plattform für Smartphones und Tablets.

2012: Raspberry Pi

2012 erobert der Minicomputer Raspberry Pi die Herzen von Elektronik-Bastlern. Für nur rund 40 EUR können Sie damit selbst Hardware-Experimente durchführen, in die Welt der Heimautomation einsteigen, ein Medien-Center oder einen Home-Server betreiben. Der Raspberry Pi macht Embedded Linux zu einem Massenphänomen.

1.7 Software-Patente und andere Ärgernisse

Vieles deutet darauf hin, dass Linux in Zukunft eine noch höhere Bedeutung und Verbreitung finden wird: Die Entwicklung schreitet auf allen Ebenen (Kernel, Server-Programme, Anwendungen) rasch voran, immer mehr Behörden und Firmen erkennen die Vorteile von Linux etc. Es gibt aber auch Stolpersteine, die das Thema dieses Abschnitts sind.

Software-Patente

Software-Patente schützen in den USA und einigen anderen Ländern Software-Ideen, -Konzepte und Algorithmen. Alles Mögliche und Unmögliche ist schon patentiert, bisweilen vollkommen triviale Dinge wie die Darstellung eines Fortschrittsbalkens oder die berühmte 1-Click-Bestellung (Amazon). Der Missbrauch derartiger Trivialpatente und die für die schnelllebige Software-Branche unsinnig langen Laufzeiten von 20 Jahren tragen zum Widerwillen gegen Software-Patente bei. Sie können davon ausgehen, dass jedes Programm mit einigen 100 Zeilen Code weltweit irgendwelche Patente verletzt ...

Die Entscheidung des Europäischen Patentamts gegen die Einführung von Software-Patenten in Europa im Sommer 2005 war einer der wenigen Lichtblicke. Da Linux aber auch außerhalb Europas eingesetzt wird, beschränken Software-Patente den Lieferumfang vieler Distributionen: Beispielsweise verzichten viele Distributionen aus Angst vor Klagen darauf, Bibliotheken zum Abspielen von MP3-Dateien mitzuliefern; die darin eingesetzten Algorithmen sind durch Patente geschützt. Es bleibt jedem Benutzer überlassen, entsprechende Bibliotheken selbst zu installieren.

Während Patente selten ein Risiko für einzelne Software-Entwickler sind, spielen sie im Kampf um Marktanteile eine immer größere Rolle, besonders im heiß umkämpften Smartphone- und Tablet-Markt. Jeder große Hersteller verklagt jeden anderen, mit ungewissem Ausgang, aber auf jeden Fall zur Freude der beteiligten Rechtsanwälte und Kanzleien. Besonders geschickt agiert Microsoft: In Form von Lizenzierungsverträgen für die Hersteller von Smartphones verdient die Firma am Verkauf von Android-Handys – ohne selbst eine Zeile Code dafür geschrieben zu haben und ohne bisher selbst eine relevante Rolle auf dem Smartphone-Markt zu spielen.

Patent-Pools der Open-Source-Gemeinde

Ganz aussichtslos ist die Lage freilich nicht. Das liegt vor allem daran, dass einige Linux nahestehende Firmen wie IBM selbst über riesige Patent-Pools verfügen. Gleichzeitig haben diverse Linux-Firmen damit begonnen, selbst Patente zu sammeln, die teilweise von anderen Firmen gleichsam für Open-Source-Zwecke »gespendet« wurden. Das Absurde der Situation besteht darin, dass ein verfehltes Patentrecht die Open-Source-Gemeinde dazu zwingt, selbst Patente einzusetzen, um sich gegen eventuelle Klagen zu schützen. Details über Patent-Tools der Open-Source-Gemeinde finden Sie hier:

http://www.openinventionnetwork.com

Multimedia

Ein weiteres Problemfeld ist der Multimedia-Markt. Schon jetzt können Sie unter Linux Ihre ganz legal erworbenen DVDs nicht abspielen. Diese Einschränkung ist juristischer Natur, nicht technischer. Die meisten DVDs sind durch ein ziemlich primitives Verschlüsselungsverfahren geschützt. Ähnlich sieht es bei Blu-ray Discs aus: Deren Schutzverfahren sind zwar technisch etwas ausgereifter als bei DVDs, mittlerweile aber ebenfalls geknackt.

Das ist aber noch keine echte Lösung für das Problem: Diverse Gesetze verbieten in vielen Ländern sowohl die Weitergabe der erforderlichen Bibliotheken als auch die bloße Beschreibung, wie diese zu installieren sind – z. B. das Urheberrechtsgesetz in Deutschland.

Digital Rights Management

Nicht besser sieht es mit online erworbenen Daten (Videos, eBooks etc.) aus, die durch DRM geschützt sind. DRM steht für *Digital Rights Management* und bezeichnet diverse Verfahren, um die Nutzung der Daten so einzuschränken, dass sie nur auf einem ganz bestimmten Rechner möglich ist. Sozusagen nebenbei werden Sie dadurch auf eine bestimmte Hardware (z. B. iPod oder iPhone) bzw. auf ein bestimmtes Betriebssystem (z. B. Windows, OS X) beschränkt. DRM-Gegner bezeichnen das System nicht umsonst als *Digital Restriction Management*. DRM und Open Source sind fundamental inkompatibel zueinander. Deswegen erfordert der legale Zugriff auf DRM-geschützte Inhalte kommerzielle Closed-Source-Programme, die für Linux aber selten verfügbar sind.

SCO

Ein Thema für sich war die SCO-Klage: Am 7. März 2003 reichte die Firma SCO eine Klage gegen die Firma IBM ein (Streitwert: eine Milliarde Dollar). SCO warf IBM unter anderem vor, dass IBM im Linux-Kernel durch Copyrights geschützten Unix-Code von SCO eingesetzt habe. Daraus folgerte SCO, dass jede Anwendung von Linux ab Kernel 2.4 illegal sei. Zur Legalisierung bot SCO Linux-Anwendern eine Weile eine spezielle Lizenz an, deren Preis aber ein Vielfaches dessen betrug, was eine Linux-Distribution üblicherweise kostet. SCO hat allerdings sämtliche Prozesse bzw. alle Instanzen verloren. 2011 wurde dieser sinnlose Rechtsstreit endgültig beigelegt.

Kapitel 2
Installationsgrundlagen

Dieses Kapitel gibt einen Überblick über die Installation eines Linux-Systems auf einem PC oder einem Notebook mit einem Intel-kompatiblen Prozessor. Das Kapitel bezieht sich nicht auf eine spezielle Distribution, sondern beschreibt wesentliche Installationsschritte, wie die Partitionierung der Festplatte, in allgemeiner Form und vermittelt das erforderliche Grundlagenwissen. Spezifische Details zur Installation einiger ausgewählter Distributionen folgen dann im nächsten Kapitel.

Die Installation ist in den vergangenen Jahren immer einfacher geworden. Im Idealfall – d. h., wenn Sie Standard-Hardware verwenden und ausreichend Platz für Linux vorhanden ist – sollten 30 Minuten ausreichen, um zu einem funktionierenden Linux-System zu gelangen. Schwierig wird die Installation zumeist nur deswegen, weil im Regelfall ein wechselweiser Betrieb von einem schon vorhandenen Windows-Betriebssystem und von Linux gewährleistet werden soll. Probleme kann es aber auch bei der Unterstützung ungewöhnlicher oder ganz neuer Hardware geben.

2.1 Voraussetzungen

Damit Sie Linux installieren können, müssen mehrere Voraussetzungen erfüllt sein:

- Sie benötigen einen PC bzw. ein Notebook mit einem Intel-kompatiblen Prozessor. Dazu zählen alle gängigen 32- und 64-Bit-Prozessoren von Intel oder AMD. Es gibt auch Linux-Distributionen für Systeme mit anderen Prozessor-Architekturen (z. B. ARM).
- Sie benötigen eine freie Partition mit ausreichend Platz auf Ihrer Festplatte. Wie viel »ausreichend« ist, hängt von der Distribution und davon ab, wie viele Programme Sie installieren und welche persönlichen Daten Sie speichern möchten (Fotos, Videos etc.). Meine Empfehlung lautet mindestens 15 GByte, um Linux einfach nur auszuprobieren.
- Sie benötigen Hardware-Komponenten, die von Linux erkannt und unterstützt werden. Gegenwärtig ist das bei einem Großteil der Standard-Hardware der Fall.

Probleme bereiten momentan vor allem EFI-Implementierungsfehler, ganz neue WLAN-Adapter, Hybrid-Grafiksysteme und SSD-Caches (siehe auch Abschnitt 1.2).

Distributionen für Uralt-PCs sowie Installationen in virtuellen Maschinen

Wie ich im vorigen Kapitel erwähnt habe, gibt es auch Minimal-Distributionen, die wesentlich geringere Hardware-Anforderungen stellen. In diesem Kapitel gehe ich aber davon aus, dass Sie eine gewöhnliche Distribution installieren – z. B. CentOS, Debian, Fedora, Kubuntu, RHEL, SUSE oder Ubuntu.

Wenn Sie Virtualisierungsprogramme wie VirtualBox oder VMware einsetzen, können Sie Linux auch innerhalb von Windows oder OS X in einer virtuellen Umgebung installieren und ausführen. Das vereinfacht die Installation, mindert aber auch die Funktionalität (limitierter Hardware-Zugriff, keine 3D-Grafik etc.). Tipps zum virtuellen Linux-Einstieg finden Sie am Ende dieses Kapitels in Abschnitt 2.16.

32 oder 64 Bit?

In fast allen gängigen PCs und Notebooks befinden sich 64-Bit-Prozessoren. Die einzige Ausnahme sind Netbooks mit dem Atom-Prozessor von Intel, der nicht 64-Bit-kompatibel ist. Der wesentliche Unterschied zwischen 32- und 64-Bit-Prozessoren besteht darin, dass mit 64-Bit-Prozessoren Speicherbereiche über 4 GByte direkt adressiert werden können.

64-Bit-Distributionen

Aus technischen Gründen werden die Vorteile der 64-Bit-Architektur nur wirksam, wenn die gesamte Distribution aus 64-Bit-Programmen und -Bibliotheken besteht. Aus diesem Grund gibt es von den meisten Distributionen zwei Ausführungen: eine 32-Bit-Version (übliche Kürzel sind i386, i586 oder i686, die sich auf Intel-Prozessorfamilien beziehen) und eine 64-Bit-Version (Kürzel x86_64 oder AMD64).

Gängige 64-Bit-Prozessoren sind vollständig abwärtskompatibel zu 32-Bit-Prozessoren. Aus diesem Grund ist es möglich, auf einem 64-Bit-Rechner auch eine 32-Bit-Distribution zu installieren. Diese Entscheidung ist endgültig: Ein späterer Wechsel von der 32- zur 64-Bit-Version ist nur durch eine Neuinstallation möglich.

In der Vergangenheit mussten sich Anwender von 64-Bit-Distributionen damit herumärgern, dass es diverse Nicht-Open-Source-Programme und -Treiber nur in 32-Bit-Versionen gab. Das hat sich mittlerweile zum Glück geändert.

Empfehlungen

Es gibt keinen Grund mehr, der *gegen* eine 64-Bit-Installation spricht. Aktuelle 64-Bit-Distributionen haben zudem den Vorteil, dass sie EFI-kompatibel sind. Während ich dieses Buch schrieb, habe ich ausschließlich mit 64-Bit-Distributionen gearbeitet.

2.2 BIOS- und EFI-Grundlagen

BIOS

Jahrzehntelang war für die Initialisierung von PCs und Notebooks das sogenannte BIOS (Basic Input/Output System) verantwortlich. Dabei handelt es sich um ein Programm, das unmittelbar nach dem Einschalten des Rechners ausgeführt wird. Das BIOS ist für die Erkennung der Hardware-Komponenten, für die Konfiguration der Hardware sowie für den Start des Betriebssystems verantwortlich. Der Begriff BIOS für diese Funktionen ist nun fast schon seit 40 Jahren gebräuchlich.

EFI und UEFI

Das traditionelle BIOS bringt eine Menge Altlasten mit sich. Deswegen begann Intel bereits 1998 mit der Entwicklung des BIOS-Nachfolgers EFI (Extensible Firmware Interface). Später beteiligten sich viele namhafte Firmen (AMD, Apple, Microsoft etc.) an der Weiterentwicklung, wobei die Software auch eine neue Abkürzung bekam: UEFI (Unified Extensible Firmware Interface). Die Kürzel EFI und UEFI werden seither oft synonym verwendet, auch in diesem Buch: Ist bei modernen Mainboards oder PCs von EFI die Rede, ist fast immer UEFI gemeint.

Während Apple schon früh auf den EFI-Zug aufsprang und seit vielen Jahren alle Macs mit einer EFI-Variante ausstattet, dauerte es in der PC-Welt wesentlich länger. Der Siegeszug von EFI hat erst 2012 mit der Markteinführung von Windows 8 begonnen. Seither kommt EFI auf nahezu allen neuen Notebooks und PCs zum Einsatz. Viele EFI-Implementierungen sind zudem BIOS-kompatibel.

Wozu EFI?

Aus technischer Sicht bietet EFI viele grundlegende Vorteile im Vergleich zum BIOS (höhere Initialisierungsgeschwindigkeit, Unterstützung der Parallelinstallation mehrerer Betriebssysteme etc.). Aus Anwendersicht reduzieren sich die Argumente für EFI aber zumeist auf zwei Punkte:

- EFI kommt mit Festplatten über 2 TByte zurecht. Für das herkömmliche BIOS gilt das nur mit Einschränkungen.
- EFI ist kompatibel zu den GUID Partition Tables (GPT). Das ist eine modernere Form zur Festplattenpartitionierung. Hintergrundinformationen zur Partitionierung und zur GPT folgen im weiteren Verlauf des Kapitels.

Linux und EFI

Die meisten aktuellen Linux-Distributionen sind EFI-kompatibel (siehe Tabelle 2.1, Stand: Sommer 2013): Das Installationsmedium startet direkt im EFI-Modus (nicht im BIOS-Modus) und richtet Linux so ein, dass es direkt durch EFI hochgefahren werden kann.

Manche Mainboards unterstützen sowohl den herkömmlichen BIOS-Start als auch EFI: Im Bootmenü erscheint das Installationsmedium dann möglicherweise doppelt, einmal mit der gewöhnlichen Bezeichnung und einmal mit dem vorangestellten Wort EFI oder UEFI. Sie müssen das Bootmedium unbedingt in der EFI-Variante starten, wenn Sie eine EFI-Installation durchführen möchten (siehe Abbildung 2.1).

Distribution	EFI-kompatibel ab	EFI Secure Boot ab
CentOS	Version 6.4	voraussichtlich Version 7
Debian	Version 7	voraussichtlich Version 8
Fedora	Version 16	Version 18
Linux Mint	Version 15	voraussichtlich Version 16
openSUSE	Version 12.3	voraussichtlich Version 13.1
RHEL	Version 6.2	voraussichtlich Version 7
Ubuntu	Version 11.10	Version 12.10

Tabelle 2.1 EFI-Kompatibilität der wichtigsten Linux-Distributionen

Abbildung 2.1 Für eine EFI-Installation müssen Sie den EFI-Eintrag auswählen!

Es mag paradox wirken, aber aus Linux-Sicht bringt EFI kaum nennenswerte Vorteile mit sich: Linux unterstützte schon bisher im Zusammenspiel mit den meisten BIOS-Versionen GPT-partitionierte Festplatten in beliebiger Größe, und Linux konnte mit dem Bootloader GRUB schon bisher beliebig viele parallel installierte Betriebssysteme starten.

Defektes Notebook nach EFI-Installation

Die EFI-Implementierungen der diversen Computer-Hersteller leiden noch an Kinderkrankheiten, und getestet wird natürlich primär mit Microsoft Windows. Im Januar 2013 wurde beispielsweise bekannt, dass einige Samsung-Notebooks aufgrund eines EFI-Fehlers im Rahmen einer Linux-Installation irreparabel beschädigt wurden.

Aus Sicherheitsgründen wurde daraufhin der Linux-Kernel so verändert, dass auf den betroffenen Geräten der Kerneltreiber `samsung-laptop` im EFI-Modus nicht mehr genutzt werden kann. Natürlich ist nicht ganz auszuschließen, dass in Zukunft bei anderen Rechnern ähnliche Probleme auftreten. Deswegen ist eine kurze Recherche im Internet zweckmäßig, bevor Sie eine EFI-Installation auf Ihrem brandneuen Gerät durchführen. Hintergrundinformationen können Sie hier nachlesen:

http://heise.de/-1793534
http://heise.de/-1794889

EFI-Unterstützung nur für 64-Bit-Distributionen

Bei den meisten Linux-Distributionen kommt nur die 64-Bit-Variante mit EFI zurecht! Diese Einschränkung gilt z. B. für Debian und Ubuntu. Zwar sind Notebooks mit 32-Bit-CPU *und* EFI sehr selten, aber es gibt sie. Vorsicht also beim Rechnerkauf: Auf einem derartigen Notebook ist es unmöglich, Linux zu installieren!

Windows und EFI

Microsoft Windows bietet seit Version 7 eine gute EFI-Unterstützung. Anders als Linux ist Windows allerdings unbedingt auf EFI angewiesen, wenn die Festplatte eine GUID Partition Table enthält!

Apple und EFI

Apple setzt EFI schon seit vielen Jahren ein. Das bringt es leider mit sich, dass die EFI-Version auf Macs inkompatibel zu den (U)EFI-Versionen auf PCs ist. Trotz EFI ist die Installation von Linux auf einem Mac daher häufig mit Problemen verbunden. Ubuntu geht sogar so weit, dass es speziell für Mac-Installationen eigene ISO-Images zum Download anbietet.

Aus meiner persönlichen Erfahrung rate ich Einsteigern von der Linux-Installation auf Macs ab: Dabei treten nahezu garantiert Probleme auf! Zwar gibt es für die meisten Mac-Modelle im Internet Installationsanleitungen; um diese zu verstehen brauchen Sie aber ein solides Linux-Grundwissen. In der Regel ist es zweckmäßiger, Linux auf dem Mac in einer virtuellen Maschine auszuführen.

EFI-Partition

Im Gegensatz zum BIOS sieht die EFI-Spezifikation die Parallelinstallation mehrerer Betriebssysteme sowie deren Auswahl während des Bootprozesses vor. Damit das funktioniert, muss es auf der Festplatte eine spezielle EFI-Partition geben, in der jedes Betriebssystem sein eigenes Startprogramm installiert (in der Fachsprache: seinen eigenen Bootloader).

Die EFI-Partition muss ein VFAT-Dateisystem enthalten, also ein Windows-95-kompatibles Dateisystem. Außerdem muss die Partition durch eine spezielle UID markiert sein. Microsoft empfiehlt, diese Partition als erste Partition auf der Festplatte einzurichten, obwohl der EFI-Standard dies nicht verlangt.

Die Partition muss nicht besonders groß sein, ca. 100 bis 200 MByte reichen. Die von mir getesteten Linux-Distributionen benötigen zur Speicherung des EFI-Bootloaders jeweils weniger als ein MByte. Deutlich mehr Platz beansprucht der Windows 8 Preview mit beachtlichen 30 MByte.

Bei der Installation von Linux müssen Sie darauf achten, dass eine bereits vorhandene EFI-Partition in das Verzeichnis `/boot/efi` eingebunden werden muss. Existiert noch keine EFI-Partition, muss sie angelegt werden. Die Installationsprogramme der meisten aktuellen Linux-Distributionen kümmern sich automatisch um diesen Schritt, sofern Sie sich nicht für eine manuelle Partitionierung entscheiden. In

diesem Fall ist Handarbeit und etwas Vorsicht angesagt! Auf keinen Fall darf eine vorhandene EFI-Partition formatiert werden, sonst kann keines der bereits installierten Betriebssysteme mehr gestartet werden!

UEFI Secure Boot

UEFI Secure Boot ist eine von Microsoft betriebene Erweiterung der EFI-Funktionen: Wenn Secure Boot aktiv ist, kann nur ein Betriebssystem gestartet werden, das mit dem auf dem Mainboard hinterlegten Schlüssel signiert ist. Auf diese Weise ist ausgeschlossen, dass Viren oder andere Schadsoftware bereits in den Bootvorgang eingreifen – was in der Praxis in den letzten Jahren aber ohnedies nur äußerst selten der Fall war.

Dennoch wird Secure Boot natürlich als Sicherheitsgewinn für Windows-Anwender verkauft. Aus Linux-Sicht verursacht diese Funktion hingegen Probleme: Bei aktivem Secure Boot kann Linux nur dann installiert und gestartet werden, wenn sein Startprogramm (exakt: sein Bootloader) mit einem auf dem Mainboard existierenden Schlüssel signiert ist. Auf den meisten Mainboards gibt es nur einen Schlüssel – den von Microsoft. Immerhin stellt Microsoft den Schlüssel auch Linux-Distributoren gegen eine geringe Gebühr zur Verfügung, dennoch hat sich die Unterstützung von Secure Boot als relativ schwierig erwiesen. Für Linux-Anwender gibt es gegenwärtig zwei Wege, um Linux auf Rechnern mit UEFI Secure Boot einsetzen zu können:

- Sie verwenden eine Linux-Distribution, die kompatibel zu UEFI Secure Boot ist (siehe Tabelle 2.1). Bei diesen Distributionen kommt ein mit dem Microsoft-Schlüssel signierter Bootloader zum Einsatz, zumeist das Programm Shim. Dieses startet in einem zweiten Schritt den gewöhnlichen Linux-Bootloader GRUB. Die weiteren Details sind distributionsabhängig. Fedora verlangt beim Secure-Boot-Vorgang z. B. auch einen signierten Kernel und signierte Kernelmodule.

  Debian 7 ist zwar EFI-kompatibel, unterstützt in der im Mai 2013 freigegebenen Version aber UEFI Secure Boot nicht. Vielleicht wird es schon vor der Freigabe von Debian 8 ein neues Installationsprogramm für Debian 7 geben, das mit UEFI Secure Boot zurechtkommt.

  openSUSE 12.3 enthält eine experimentelle Unterstützung für UEFI Secure Boot. Dazu muss die gut versteckte Option Enable Secure Boot Support in den Bootloader-Einstellungen aktiviert werden.

- Sie deaktivieren UEFI Secure Boot vor der Installation. Die EFI-Spezifikation sieht dies erfreulicherweise vor vor. Wie diese Deaktivierung konkret aussieht, ist allerdings auf jedem Rechner bzw. bei jedem Mainboard anders und erfordert mitunter langes Suchen.

Weiterführende Informationen

Weitere Details zu EFI können Sie auf den folgenden Webseiten nachlesen:

http://de.wikipedia.org/wiki/Extensible_Firmware_Interface
https://wiki.archlinux.org/index.php/Unified_Extensible_Firmware_Interface
https://help.ubuntu.com/community/UEFIBooting
http://www.rodsbooks.com/efi-bootloaders/index.html
http://mjg59.dreamwidth.org

2.3 Installationsvarianten

Bis vor wenigen Jahren verwendeten die meisten Distributionen dasselbe Installationsverfahren: Der Rechner wird neu gestartet, das auf der CD oder DVD befindliche Installationsprogramm wird ausgeführt, und Linux wird auf die Festplatte installiert. Dieses Verfahren ist nach wie vor populär, es gibt aber mittlerweile eine Menge Varianten, die ich Ihnen hier vorstelle.

Installationsmedium

Das gängigste Installationsmedium ist noch immer eine CD oder DVD. Soweit Sie den Datenträger nicht einer Zeitschrift oder einem Buch entnehmen, laden Sie die entsprechende ISO-Datei aus dem Internet herunter und brennen die CD oder DVD einfach selbst. Anschließend starten Sie Ihren Rechner neu und führen das auf der CD oder DVD befindliche Installationsprogramm aus.

Anstelle einer CD/DVD kann auch ein USB-Stick als Installationsmedium verwendet werden. Die ISO-Dateien der meisten Distributionen sind mittlerweile so konzipiert, dass sie direkt von USB-Datenträgern bootfähig sind. Wenn Sie schon mit Linux vertraut sind, können Sie derartige Image-Dateien im Terminal einfach mit dem Kommando `dd` auf den USB-Stick oder eine Speicherkarte kopieren:

```
user$  dd if=ubuntu.img of=/dev/sdc bs=4M
```

Passen Sie aber auf, dass Sie mit `of=...` das korrekte Gerät angeben! Wer sich das nicht zutraut, kann diesen Schritt komfortabler mit einer Benutzeroberfläche durchführen, unter Linux beispielsweise mit dem *USB-ImageWriter*, unter Windows mit dem *Universal USB Installer*. Anschließend starten Sie Ihren Rechner neu und booten das Linux-Installationsprogramm vom USB-Stick.

Schwieriger ist es, eine ISO-Datei als Grundlage für eine USB-Installation zu verwenden, wenn das ISO-Image *nicht* für den Einsatz auf USB-Sticks vorgesehen ist: In diesem Fall müssen Sie den Inhalt einer ISO-Datei auf dem USB-Medium auspacken und dort das Programm Syslinux installieren. Die manuelle Durchführung dieser Schritte ist schwierig und Linux-Profis vorbehalten.

Besser ist es, zum Beschreiben des USB-Sticks das Programm *UNetbootin* einzusetzen (siehe Abbildung 2.2), das Sie wahlweise unter Linux, Windows oder OS X

ausführen. Anschließend wählen Sie entweder eine Distribution zum Download aus oder geben den Speicherort einer bereits vorher heruntergeladenen ISO-Datei an. Außerdem müssen Sie einstellen, in welches Device bzw. Laufwerk die Daten kopiert werden sollen. Da die ISO-Datei in entpackter Form auf den USB-Datenträger geschrieben wird, muss dieser oftmals wesentlich größer als die ISO-Datei sein. Sie finden dieses ausgesprochen nützliche Programm hier zum Download:

http://unetbootin.sourceforge.net

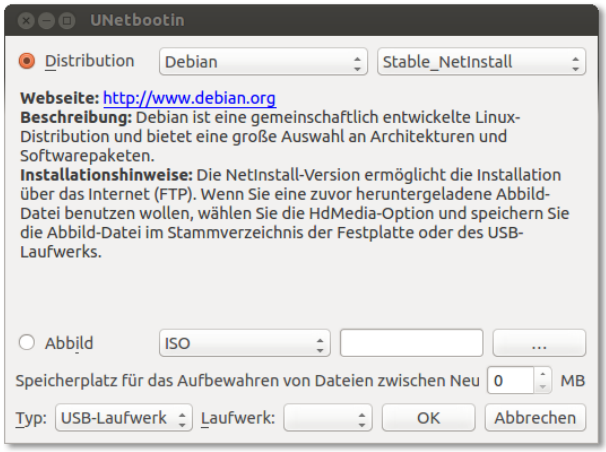


Abbildung 2.2 ISO-Datei auf USB-Medium übertragen

Probleme mit Installationen vom USB-Stick

Ich habe mit der Linux-Installation von USB-Sticks unzählige negative Erfahrungen gemacht: Bei manchen Rechnern funktioniert die Installation nur via USB 2 (nicht USB 3), bei manchen Distributionen gelingt der Installationsstart nur im BIOS-, aber nicht im EFI-Modus etc.

CDs/DVDs erscheinen aus heutiger Sicht altmodisch, funktionieren aber als Installationsmedium für Linux auf jeden Fall robuster. Wenn Ihr Rechner kein DVD-Laufwerk hat, sollten Sie bei Problemen den Einsatz eines externen USB-Laufwerks erwägen.

Installationsprogramm versus Live-System

Traditionell wird von der Installations-CD oder -DVD ein minimales Linux-System mit einem Installationsprogramm ausgeführt. Ein anderes Konzept besteht darin, vom Installationsmedium ein vollständiges Linux-System zu starten, ein sogenanntes Live-System. Das Installationsprogramm wird dann innerhalb dieses Live-Systems ausgeführt. Diese z. B. von Ubuntu gewählte Vorgehensweise hat den Vorteil, dass das Live-System auch für andere Zwecke verwendet werden kann – etwa um Linux auszuprobieren, um Reparaturarbeiten durchzuführen etc.

Einige Distributionen bieten für beide Installationsvarianten eigene ISO-Dateien an. Der Vorteil der Live-Variante ist vielfach ein geringerer Download-Bedarf. Allerdings bietet die Live-Variante in der Regel weniger Auswahl- und Konfigurationsmöglichkeiten. Außerdem werden vielfach nur englische Sprachpakete installiert. Eine positive Ausnahme ist in dieser Hinsicht Ubuntu, das sich auch bei einer Live-Installation um die korrekte Installation der Sprachpakete kümmert.

Wenn Sie die Wahl haben, sollten Sie das traditionelle Installationsverfahren vorziehen. Das gilt insbesondere dann, wenn Sie spezielle Konfigurationswünsche haben – LVM, RAID, Auswahl eines eigenen Dateisystemtyps etc.

Installation im Textmodus

Bei nahezu allen Distributionen erfolgt die Installation innerhalb einer grafischen Benutzeroberfläche. Optional kann die Installation zumeist auch im Textmodus durchgeführt werden, etwa wenn es Probleme bei der korrekten Erkennung der Grafikkarte gibt. Es gibt auch noch immer Distributionen, die *nur* im Textmodus installiert werden können, beispielsweise die Server-Variante von Ubuntu oder Arch Linux, Gentoo und Slackware.

Installation auf ein USB-Medium

USB-Medien werden nicht nur als Quellmedium für das Installationsprogramm immer beliebter, sondern auch als Ziel einer Installation: Einige Distributionen bieten die Möglichkeit, Linux auf einen USB-Stick zu installieren. Das ergibt dann ein »Linux zum Mitnehmen«, das unterwegs nahezu auf jedem beliebigen Rechner ausgeführt werden kann – sofern Ihnen nicht BIOS/EFI-Inkompatibiltitäten einen Strich durch die Rechnung machen.

Oft handelt es sich bei dieser Installationsvariante nicht um eine vollwertige Installation; vielmehr wird einfach ein Live-System auf den USB-Stick übertragen. Daraus ergeben sich diverse Einschränkungen, etwa was die Installation weiterer Programme oder die Durchführung von Updates betrifft. Ein Live-System – egal, ob auf einer CD oder auf einem USB-Stick – kann eine »richtige« Installation nie ersetzen.

Installation auf eine externe Festplatte

Sie können Linux auch auf eine externe Festplatte installieren. Diese Variante sieht auf den ersten Blick verlockend aus, insbesondere bei Notebooks, deren eingebaute Festplatte schon voll ist. Leider gibt es bei dieser Installationsvariante oft Probleme, das Linux-System anschließend zu starten. Deswegen ist diese Installationsform nur fortgeschrittenen Linux-Anwendern zu empfehlen.

Windows-Installation

Der irreführende Begriff »Windows-Installation« bedeutet, dass die Installation von Linux nicht mit einem Neustart des Rechners, sondern direkt unter Windows beginnt. Es gab in der Vergangenheit mehrfach den Versuch, die Hemmschwelle einer Linux-Installation auf diese Weise zu minimieren.

Der populärste Windows-Installer ist WUBI: Bei dieser besonders einfachen Installationsvariante für Ubuntu werden die Installationseinstellungen und Vorbereitungs-

arbeiten unter Windows durchgeführt. Anschließend ist aber auch bei WUBI ein Neustart des Rechners erforderlich. Die weitere Installation erfolgt automatisch. Leider ist WUBI inkompatibel zu Windows 8 und EFI, weswegen das Programm von Ubuntu nicht mehr offiziell unterstützt wird.

http://wubi-installer.org

Netzwerkinstallation

Bei einer Netzwerkinstallation werden die Installationsdateien nicht von einer CD/DVD oder einem USB-Stick gelesen, sondern aus dem Netzwerk. Dabei gibt es zwei Varianten, die sich darin unterscheiden, wie die Installation beginnt:

- **Installationsstart mit einem herkömmlichen Medium:** Hier startet die Installation von einer CD oder einem USB-Stick. Das Installationsprogramm hilft bei der Herstellung der Netzwerkverbindung und lädt dann alle weiteren Daten aus dem Netz. Besonders populär ist diese Installationsform bei Debian mit dem sogenannten *netinst*-Image.
- **Installationsstart via Netzwerk:** Diese »echte« Netzwerkinstallation setzt voraus, dass Ihr Rechner die Boot-Daten aus dem lokalen Netzwerk laden kann. Die meisten gängigen Mainboards sind dazu in der Lage, wenn das BIOS oder EFI korrekt eingestellt wird.

  Außerdem muss es im lokalen Netzwerk einen Server geben, der das Linux-Installationsprogramm in Form von Boot-Daten anbietet. Diese Vorgehensweise ist optimal, um viele Linux-Installationen auf einmal durchzuführen. Allerdings ist das Einrichten des Installations-Servers nicht ganz einfach. Nur ausgewählte Distributionen unterstützen dieses Installationsverfahren, unter anderem Red Hat und SUSE. Wenn Sie Debian auf mehreren Rechnern automatisch installieren möchten, werfen Sie einen Blick auf die folgende Seite:

  http://fai-project.org

Mehrere Distributionen auf einem PC

Um mehrere Distributionen auszuprobieren oder um eine neue Version Ihrer Distribution parallel zur vorhandenen Version zu testen, können Sie mehrere Distributionen nebeneinander auf Ihrer Festplatte installieren. Dazu benötigt jede Distribution ihre eigene Systempartition. Die wichtigste Voraussetzung besteht also darin, dass auf Ihrer Festplatte Platz für weitere Partitionen ist. Swap- und Datenpartitionen können von unterschiedlichen Distributionen gemeinsam genutzt werden.

Bei BIOS-Rechnern ist zudem die richtige Installation des Bootloaders entscheidend: Wenn Sie den Bootloader einfach in den Bootsektor der Festplatte installieren und das Installationsprogramm die bereits installierten Distributionen nicht erkennt, können Sie anschließend nur die neue, nicht aber die alte Distribution starten. In solchen Fällen ist später eine manuelle Korrektur der Konfiguration des Bootloaders notwendig, damit wieder beide Distributionen gestartet werden können.

2.4 Überblick über den Installationsprozess

Dieser Abschnitt fasst die Schritte einer gewöhnlichen Linux-Installation zusammen. »Gewöhnlich« bedeutet hier, dass auf dem Rechner bereits Microsoft Windows installiert ist. Wesentlich einfacher verläuft die Installation, wenn auf dem Rechner noch kein Betriebssystem installiert ist oder wenn dieses gelöscht werden darf. Nun aber zu den Installationsschritten, die ich in den weiteren Abschnitten im Detail beschreiben werde.

- **Linux-Installation starten:** Legen Sie die Installations-CD in das Laufwerk ein, und starten Sie den Rechner neu. Das Linux-Installationsprogramm sollte automatisch gestartet werden. Das Installationsprogramm sieht bei jeder Distribution ein wenig anders aus. Für die wichtigsten Distributionen folgen im nächsten Kapitel konkrete Tipps zur Bedienung des Installationsprogramms. Die ersten Fragen betreffen zumeist die Sprache der Benutzeroberfläche sowie die Konfiguration von Tastatur und Maus.

  Falls Sie als Installationsmedium einen USB-Stick oder eine Speicherkarte verwenden, müssen Sie während des Starts explizit angeben, dass Sie davon booten möchten. Die erforderlichen Tastenkombinationen hängen vom BIOS bzw. EFI Ihres Rechners ab.
- **Windows-Partition verkleinern:** Normalerweise füllt Windows die gesamte Festplatte oder SSD in einer einzigen, sehr großen Partition. Um Platz für Linux zu machen, muss diese Partition verkleinert werden. Bei den meisten Distributionen kümmert sich das Installationsprogramm um diesen Schritt. Nur wenn Ihre Distribution diese Möglichkeit nicht bietet oder wenn die Verkleinerung nicht klappt, müssen Sie Hand anlegen und die Windows-Partition vor dem Start der Linux-Installation selbst verkleinern.
- **Linux-Partitionen anlegen:** Ein wesentlicher Schritt jeder Installation ist das Anlegen von Linux-Partitionen auf der Festplatte. Wie das Partitionierprogramm aussieht, hängt stark von der jeweiligen Distribution ab.
- **Installationsumfang auswählen:** Bei vielen Distributionen können Sie auswählen, welche Teile der Linux-Distribution Sie installieren möchten. Bei einigen Distributionen entfällt dieser Schritt (z. B. bei Ubuntu). Stattdessen wird hier ein relativ kleines Grundsystem installiert. Weitere Programme fügen Sie dann später bei Bedarf im laufenden Betrieb hinzu.
- **Konfiguration:** Je nach Installationsprogramm folgen nun diverse Rückfragen zur Konfiguration – z. B. zum gewünschten Passwort für den Administrator `root`, zu den Netzwerkeinstellungen, zur Druckerkonfiguration etc.
- **Bootloader:** Ungeklärt ist jetzt nur noch eine Frage: Wie soll Linux in Zukunft gestartet werden? Dazu wird bei den meisten Distributionen das Programm

GRUB eingesetzt. Bei EFI-Installationen wird GRUB in ein Verzeichnis der EFI-Partition installiert. Damit können mühelos beliebig viele Betriebssysteme parallel installiert werden.

Bei BIOS-Rechnern wird GRUB wahlweise in den Bootsektor der Festplatte oder in den ersten Sektor einer Linux-Partition installiert. Komfortabler ist die erste Variante: In diesem Fall erscheint der Bootloader bei jedem Start, und Sie können auswählen, welches Betriebssystem Sie starten möchten. Der Nachteil besteht allerdings darin, dass die GRUB-Installation in seltenen Fällen Konflikte mit dem bisher installierten Bootloader verursacht.

Insgesamt wird die Erstinstallation von Linux vermutlich etwa eine Stunde in Anspruch nehmen. Mit etwas Übung und einem schnellen Rechner gelingt sie aber auch in 15 Minuten! Anschließend können Sie mit Linux zu arbeiten beginnen bzw. manuell weitere Konfigurationsschritte durchführen und Linux optimal an Ihre besonderen Ansprüche anpassen.

Vorsicht bei der Partitionierung und bei der Konfiguration des Bootloaders

Es gibt während einer Linux-Installation nur zwei kritische Phasen, in denen Sie unbeabsichtigt Daten anderer Betriebssysteme zerstören oder Ihren Rechner nicht mehr startbar machen können: bei der Partitionierung der Festplatte und bei der Installation des Bootloaders auf die Festplatte. Führen Sie diese Schritte also mit besonderer Vorsicht aus.

Festplatte oder SSD?

Aus Linux-Sicht ist es egal, ob sich in Ihrem Rechner eine herkömmliche Festplatte oder eine Solid State Disk (SSD) befindet. Wenn ich in diesem Buch also öfters einfach von der »Festplatte« schreibe, gilt dies gleichermaßen auch für SSDs. Ganz exakt wäre es, wenn ich jedes Mal »Datenträger« schreiben würde – aber dieser Begriff erschien mir zu sperrig.

Problematisch sind Notebooks, die eine zumeist sehr kleine SSD mit einer großen Festplatte kombinieren. Unter Windows kommen dann besondere Treiber zum Einsatz, die beide Speicherträger kombinieren. Unter Linux kann in solchen Fällen zumeist nur die herkömmliche Festplatte genutzt werden. Wenn möglich, sollten Sie den Kauf derartiger Notebooks vermeiden. Wenn es Ihr Budget zulässt, sollten Sie auf herkömmliche Festplatten ganz verzichten; der Geschwindigkeits- und Komfortgewinn eines reinen SSD-Systems ist den Aufpreis definitiv wert.

2.5 Start der Linux-Installation

Von einer CD/DVD starten

Sie beginnen die Installation damit, dass Sie die Installations-CD oder -DVD in Ihr CD/DVD-Laufwerk legen und den Rechner neu starten. Statt des üblichen Starts Ihres bereits installierten Betriebssystems sollte nun ein Linux-System bzw. das Linux-Installationsprogramm direkt von der CD starten.

Sollte dies nicht gelingen, ist Ihr BIOS bzw. EFI vermutlich so konfiguriert, dass ein Booten von einer CD/DVD nicht möglich ist. Um die BIOS/EFI-Einstellungen zu ändern, müssen Sie unmittelbar nach dem Einschalten des Rechners eine Taste drücken, häufig Entf oder F1. Falls diese Tasten unwirksam bleiben, müssen Sie im Handbuch Ihres Rechners bzw. Mainboards nachschauen bzw. im Internet danach suchen. Beachten Sie, dass während der BIOS-Einstellung meist das amerikanische Tastaturlayout gilt. Unter anderem sind Y und Z vertauscht!

Von einem USB-Stick starten

Auch wenn Sie als Installationsmedium einen USB-Stick oder eine Speicherkarte verwenden, müssen Sie den Rechner neu starten. Abermals sind BIOS bzw. EFI-Einstellungen dafür verantwortlich, ob ein Booten vom USB-Stick oder von der Speicherkarte gelingt.

Erste Einstellungen

Bei einigen Distributionen können Sie noch vor dem eigentlichen Start von Linux durch Funktionstasten die Sprache, das Tastaturlayout und eventuell einige weitere Parameter einstellen (siehe Abbildung 2.3). Bei anderen Distributionen erfolgen diese Einstellungen wenige Sekunden nach dem Start.

Abbildung 2.3 Sprachauswahl am Beginn einer SUSE-Installation

Was sind tote Tasten?

Bei manchen Distributionen können Sie ein Tastaturlayout mit oder ohne sogenannte *Dead Keys* auswählen. Damit sind beispielsweise ' und ~ gemeint. (De)aktiviert werden nicht die Tasten an sich, sondern das Zusammensetzen von Buchstaben mit diesen Tasten.

Bei einem Tastaturlayout mit Dead Keys können Sie beispielsweise den Buchstaben Ç in der Form ~, C eingeben. Wenn Sie die den Dead Keys zugeordneten Zeichen selbst eingeben möchten, müssen Sie die betreffende Taste und danach die Leerzeichentaste drücken – also ~, ␣ für ~. Beim Arbeiten im Terminal wird dieses Zeichen unter Linux häufig benötigt.

Bei einem Tastaturlayout ohne Dead Keys können Sie keine ausländischen Sonderzeichen zusammensetzen. Dafür ist jetzt die Eingabe der den Dead Keys zugeordneten Zeichen bequemer, weil das betreffende Zeichen sofort erscheint.

Interna

Das Installationsprogramm läuft selbst unter Linux. Dazu wird vom Installationsmedium zuerst der Linux-Kernel geladen. Der Kernel muss alle für die Installation relevanten Hardware-Komponenten richtig erkennen. Sollte das nicht gelingen, können Linux-Profis beim Start der Installation zusätzliche Kernelparameter angeben, um dem Kernel bei der Hardware-Erkennung auf die Sprünge zu helfen. Sobald der Kernel läuft, wird das eigentliche Installationsprogramm gestartet.

2.6 Grundlagen der Festplattenpartitionierung

Nach dem Start des Installationsprogramms und diversen elementaren Einstellungen ist die Partitionierung der Festplatte oder SSD der erste entscheidende Schritt der Installation. Zwar bieten viele Installationsprogramme an, diesen Schritt automatisch zu erledigen, dabei ist aber Vorsicht angebracht: Nicht immer entspricht das Resultat wirklich Ihren Bedürfnissen. Bevor der nächste Abschnitt konkrete Tipps zur Partitionierung gibt, erklärt dieser Abschnitt, was Partitionen sind und welche Regeln beim Anlegen von Partitionen zu beachten sind.

Was sind Partitionen?

Partitionen sind Abschnitte auf der Festplatte. Windows-Partitionen bekommen eigene Buchstaben (`C:`, `D:` etc.) und verhalten sich scheinbar wie selbstständige Festplatten.

Im einfachsten Fall gibt es nur eine einzige Partition, die einfach die gesamte Festplatte umfasst. Bei Windows-XP-Installationen war das der Regelfall. Seit Windows-7-PCs gibt es zumeist *zwei* Partitionen: eine winzige Partition, die Dateien für den Start von Windows enthält, und eine zweite Partition, die den Rest der Festplatte füllt und

Windows sowie alle persönlichen Daten enthält. Bei einem Rechner mit EFI sind es in der Regel sogar mindestens *drei* Partitionen, weil auch EFI eine kleine Partition zur Speicherung von Boot-Dateien benötigt. Mit Windows 8 ist diese Konfiguration zum Normalfall geworden.

Auf manchen Rechner gibt es darüber hinaus weitere Partitionen, die Dateien zur Wiederherstellung des Systems, Hardware-Treiber, Zusatz-Software etc. enthalten – alles Dinge, die früher oft mit einer DVD mitgeliefert wurden. Die Zeitschrift c't ist auf vorkonfigurierte Windows-Notebooks mit bis zu sechs Partitionen gestoßen.

Wozu noch mehr Partitionen?

Noch mehr Partitionen benötigen Sie, sobald Sie mehrere Betriebssysteme gleichzeitig auf Ihrem Rechner installieren möchten. Dafür gibt es zwei Gründe: Zum einen verwenden unterschiedliche Betriebssysteme oft auch unterschiedliche Dateisysteme, also unterschiedliche Verfahren, wie Dateien innerhalb der Partition abgelegt werden. Zum anderen vermeiden eigene Partitionen Doppelgleisigkeiten und Konflikte bei Verzeichnis- und Dateinamen.

Unter Linux kommt noch hinzu, dass es zumeist sinnvoll ist, für Linux selbst mehrere Partitionen vorzusehen – z. B. eine Partition für das Betriebssystem, eine weitere für Ihre eigenen Daten und eine dritte als sogenannte Swap-Partition. Dabei handelt es sich um das Gegenstück zur Auslagerungsdatei von Windows.

Für eine Linux-Installation kommt es also nicht darauf an, wie viel Platz auf Ihrer Festplatte unter Windows noch frei ist. Diesen Platz – innerhalb einer Windows-Partition – können Sie nämlich für Linux nicht nutzen. Sie benötigen für die Linux-Installation Platz *außerhalb* der Windows-Partition(en), um dort neue Linux-Partitionen anzulegen.

Vorsicht, wenn Windows nicht erkannt wird ...

Die Installationsprogramme der meisten Distributionen bieten eine halbautomatische Partitionierung an. Aufpassen müssen Sie dabei, was das Installationsprogramm mit den Windows-Partitionen machen möchte. Vorsicht: Wenn im Partitionierungsvorschlag keine Windows-Partitionen erscheinen, hat das Installationsprogramm diese vermutlich nicht erkannt. Das kann z. B. bei Rechnern mit SSD-Cache passieren, oder auf PCs mit mehreren Festplatten und Fake-RAID. Führen Sie in solchen Fällen unbedingt eine manuelle Partitionierung durch!

Partitionierungshilfen

Um die Aufteilung der Festplatte zu verändern, sieht jedes Betriebssystem eigene Werkzeuge vor. Unter Windows 9x/ME war das aus DOS-Zeiten bekannte Programm `FDISK` gebräuchlich. Seit Windows NT steht ein komfortableres Werkzeug mit grafischer Benutzeroberfläche zur Verfügung; der Aufruf ist allerdings bei jeder dieser Windows-Versionen ein wenig anders. Unter Windows 7 füh-

ren Sie Systemsteuerung • System und Sicherheit • Verwaltung • Computerverwaltung • Datenträgerverwaltung aus. Unter Linux stehen je nach Installationsprogramm diverse Partitionierungshilfen zur Verfügung. Sollte es damit Probleme geben, können Linux-Profis auch auf die Kommandos `fdisk` oder `parted` zurückgreifen.

Mehr Flexibilität mit LVM

Die Partitionierung der Festplatte lässt sich nachträglich nur mit großem Aufwand ändern. In vielen Fällen geht der Inhalt einer Partition verloren, wenn deren Größe verändert wird. Auch ein Verschieben von Partitionen ist nicht vorgesehen. Daher ist es empfehlenswert, die Partitionierung von Anfang an gut zu bedenken.

Linux-Profis können viele Einschränkungen umgehen, indem sie das System LVM einsetzen (siehe Abschnitt 2.7). Dabei handelt es sich um eine Zwischenschicht zwischen Partitionen und Dateisystemen.

MBR versus GPT

Es gibt aktuell zwei Verfahren zur Verwaltung der Partitionierungsinformationen auf der Festplatte:

- **MBR:** Die Partitionierungskonzepte auf Basis der MBR-Partitionstabellen reichen bis in die DOS-Zeit zurück, und entsprechend angestaubt wirken manche Regeln und Einschränkungen. Dennoch gelten sie für nahezu alle gängigen Festplatten, die bis 2012 in Linux- oder Windows-PCs eingesetzt wurden. Die Partitionierungstabelle wird in diesem Fall im Master Boot Record (MBR) gespeichert, also im ersten Sektor der Festplatte.
- **GPT:** Um die vielen MBR-Einschränkungen zu umgehen, wurde schon vor Jahren ein neuer Standard geschaffen: *GUID Partition Tables*. Apple ist schon 2005 auf GPT umgestiegen, der PC-Markt hat diesen Schritt erst im Herbst 2012 mit der Markteinführung von Windows 8 vollzogen. Aber auch viele ältere PCs sind GPT-kompatibel. EFI ist keine zwingende Voraussetzung für GPT!

MBR-Grundlagen

Partitionstypen

Bei Festplatten mit MBR-Partitionierung gibt es drei Typen von Festplattenpartitionen: primäre, erweiterte und logische Partitionen. Auf der Festplatte können maximal vier primäre Partitionen existieren. Außerdem besteht die Möglichkeit, statt einer dieser vier primären Partitionen eine erweiterte Partition zu definieren. Innerhalb der erweiterten Partition können dann mehrere logische Partitionen angelegt werden.

Der Sinn von erweiterten und logischen Partitionen besteht darin, das historisch vorgegebene Limit von nur vier primären Partitionen zu umgehen. Beachten Sie, dass manche Partitionierwerkzeuge an der Oberfläche nicht zwischen verschiedenen Partitionstypen unterscheiden und sich selbstständig darum kümmern, wie die Partitionen intern angelegt werden.

Eine erweiterte Partition dient nur als Container für logische Partitionen. Zur eigentlichen Speicherung von Daten sind nur primäre und logische Partitionen geeignet.

Der Begriff »Partitionstyp« wird auch in einem anderen Kontext verwendet: Zusammen mit jeder Partition wird eine Zusatzinformation (eine Kennzahl) gespeichert, die angibt, für welches Betriebssystem die Partition gedacht ist (z. B. Windows, Linux, Novell Netware, BSD) bzw. welche Aufgabe der Partition zugeteilt ist.

Maximalanzahl der Partitionen

Linux kann auf jeder Festplatte maximal 15 Partitionen ansprechen, davon maximal 11 logische Partitionen. Effektiv für Dateisysteme nutzbar sind im Idealfall 14 Partitionen, also 3 primäre und 11 logische Partitionen. Folglich ist es am besten, zuerst die drei primären Partitionen einzurichten, dann die erweiterte Partition, sodass diese die gesamte restliche Festplatte füllt, und schließlich darin die logischen Partitionen nach Bedarf.

Maximale Partitionsgröße

Die maximale Partitionsgröße beträgt 2 TByte. Zur Not können Sie selbst Festplatten bis zu 4 TByte mit MBR-Partitionierung nutzen: Dazu lassen Sie die letzte primäre Partition gerade noch innerhalb der ersten 2 TByte beginnen und machen diese beinahe 2 TByte groß. Damit kann sie noch vollständig angesprochen werden – z. B. als Physical Volume für ein LVM-System. Empfehlenswert ist dieser im c't-Magazin 4/2011 vorgeschlagene Weg aber nicht. Steigen Sie besser auf GTP um!

GPT-Grundlagen

GPT steht für *GUID Partition Table*. Jede Partition wird durch einen *Global Unique Identifier* (GUID) gekennzeichnet. In der GPT-Partitionstabelle ist Platz für 128 Partitionen, wobei Sie unter Linux aber nur die ersten 15 ansprechen können. Alle Partitionen sind gleichwertig, d. h., es gibt keine Unterscheidung zwischen primären, erweiterten und logischen Partitionen. Jede Partition kann bis zu 8 Zettabyte groß sein – also 2^{73} Byte, das sind ca. $9,4 * 10^{21}$ Byte oder rund eine Milliarde TByte! Das sollte für die nächste Zeit reichen.

Die Partitionstabelle befindet sich in den ersten 34 * 512 = 17.408 Byte der Festplatte. Eine Kopie dieser Informationen nimmt weitere 17 kByte am Ende der Festplatte in Anspruch. Aus Sicherheitsgründen beginnt die GPT-Partitionstabelle mit MBR-Partitionsinformationen, um MBR-kompatiblen Programmen den Eindruck zu ver-

mitteln, die gesamte Festplatte würde bereits von einer Partition genutzt, die die gesamte Festplatte füllt.

Beachten Sie, dass die Partitionsnummern nicht mit der tatsächlichen Reihenfolge der Partitionen übereinstimmen müssen. Nehmen Sie an, Sie erzeugen drei Partitionen mit jeweils 20 GByte. Nun verkleinern Sie die zweite Partition auf 10 GByte. Damit entsteht zwischen den Partitionen 2 und 3 eine Lücke, in der Sie eine neue Partition einrichten können. Diese bekommt die Nummer 4 und entsprechend unter Linux den Device-Namen `/dev/sda4`!

Kompatibilität

Grundsätzlich können GPT-Partitionstabellen auf *jeder* Festplatte verwendet werden. Allerdings kommen nur moderne Betriebssysteme mit diesen Partitionstabellen zurecht. Zu den GPT-kompatiblen Betriebssystemen zählen neben allen einigermaßen aktuellen Linux-Distributionen auch OS X ab Version 10.4 sowie alle 64-Bit-Versionen von Windows (ab Windows XP).

Einige 32-Bit-Versionen von Windows sind immerhin eingeschränkt GPT-kompatibel: Dazu zählen Windows Vista, Windows Server 2008 und Windows 7 und 8. Diese Windows-Versionen können allerdings nur dann von einer GPT-Festplatte starten, wenn statt des herkömmlichen BIOS das neuere EFI im Einsatz ist. Für Linux sowie für die 64-Bit-Versionen von Windows gilt diese Einschränkung nicht, d. h., ein traditionelles BIOS ist vollkommen ausreichend.

Umfassende Informationen zum Aufbau der GPT-Partitionstabelle sowie zur Kompatibilität mit diversen Betriebssystemversionen gibt die englische Wikipedia-Seite:

http://en.wikipedia.org/wiki/GUID_Partition_Table

Umstieg auf GPT

Die meisten Linux-Installationsprogramme kommen zwar mühelos mit GPT-partitionierten Festplatten zurecht. Erstaunlicherweise gibt es aber kaum Distributionen, die Ihnen bei der Partitionierung neuer Festplatten die Wahl zwischen MBR und GPT bieten.

Die Umstellung einer Festplatte von MBR auf GPT bzw. die Initialisierung einer noch vollkommen leeren Festplatte mit einer GPT ist momentan also nur von Hand möglich. Dazu verwenden Sie am besten ein Linux-Live-System. Anschließend führen Sie das Kommando `parted` aus und darin wiederum den Befehl `mklabel gpt`. Damit wird die Partitionstabelle im GPT-Format neu eingerichtet. Beachten Sie aber, dass die folgenden Kommandos mit dem Verlust aller Daten auf der Festplatte verbunden sind!

```
root#  parted /dev/sda
(parted)  mklabel gpt
(parted)  quit
```

MBR oder GPT?

Bei Festplatten bis zu 2 TByte gibt es keinen zwingenden Grund für GTP. Persönlich richte ich allerdings schon seit geraumer Zeit auf allen neuen Festplatten und SSDs eine GPT ein. Damit erspare ich mir das Theater mit primären, erweiterten und logischen Partitionen. Nachteile sind mir keine aufgefallen.

Festplatten mit 4-kByte-Sektoren

Neue Festplatten sowie Solid State Disks (SSDs) verwenden statt der jahrzehntelang üblichen 512-Byte-Sektoren längere Sektoren von 4096 Byte (4 kByte). Das hat viele Vorteile, unter anderem eine höhere Geschwindigkeit und eine höhere Festplattenkapazität. Aus Kompatibilitätsgründen melden aber auch Festplatten mit 4-kByte-Sektoren eine 512-Byte-Sektorgröße an das Betriebssystem.

Um Festplatten mit 4-kByte-Sektoren effizient zu nutzen, müssen Partitionen so eingerichtet werden, dass die Startposition jeder Partition ein Vielfaches von 4 kByte beträgt. Ist das nicht der Fall und will das Dateisystem einen 4-kByte-Bereich verändern, muss die Festplatte zwei 4-kByte-Sektoren lesen, modifizieren und schreiben. Das würde Schreibvorgänge massiv bremsen.

Die Installationsprogramme aller aktuellen Distributionen nehmen auf diesen Umstand mittlerweile Rücksicht. Aufpassen müssen nur Linux-Profis, die Festplatten mit Low-Level-Werkzeugen wie `fdisk` oder `parted` partitionieren. Diese beiden Kommandos werden in Kapitel 25 näher vorgestellt.

Solid State Disks (SSDs)

Linux kommt problemlos mit Solid State Disks zurecht. Damit SSDs auch bei langer, intensiver Benutzung schnell bleiben, ist es aber empfehlenswert, etwa fünf bis zehn Prozent der SSD nicht zu nutzen – am besten dadurch, dass Sie einen kleinen Teil der SSD unpartitioniert lassen.

Außerdem sollten Sie in Erwägung ziehen, die Trim-Funktion zu aktivieren (siehe Abschnitt 25.17). Damit teilt Linux der SSD mit, welche Speicherblöcke des Dateisystems nach dem Löschen einer Datei ungenutzt sind. Die SSD kann dann die interne Nutzung der Speicherzellen optimieren.

Dateisysteme

Durch das Partitionieren wird auf der Festplatte lediglich Platz reserviert. Bevor Sie in einer Partition Dateien speichern können, muss ein sogenanntes Dateisystem angelegt werden. Es enthält neben den eigentlichen Daten diverse Verwaltungsinformationen. Sowohl Windows als auch Linux kennen unterschiedliche Dateisystemtypen:

- Unter Windows sind VFAT (Windows 9x/ME) und NTFS (alle Versionen ab Windows NT) gebräuchlich. VFAT kommt darüber hinaus auch auf den meisten SD-Karten für Kameras, Smartphones etc. zum Einsatz.
- Unter Linux ist `ext4` der beliebteste Dateisystemtyp.

Das Anlegen eines Dateisystems in einer Partition wird auch Formatieren genannt. Unter Windows können Sie diese Operation über ein Kontextmenü im Explorer oder mit dem Programm `FORMAT` durchführen. Bei einer Linux-Installation kümmert sich das Installationsprogramm um die Formatierung, wobei hinter den Kulissen ein Kommando wie `mkfs.ext4` zum Einsatz kommt.

Achtung

Im Regelfall gehen sowohl durch die Partitionierung als auch durch das Formatieren alle in der betroffenen Partition gespeicherten Daten verloren! Die einzige Ausnahme sind spezielle Werkzeuge zur verlustfreien Größenänderung von Partitionen.

Partitionsnamen

Windows

Unter Windows werden Partitionen, die das Betriebssystem nutzen kann, mit Laufwerksbuchstaben bezeichnet. `A:` und `B:` sind für Disketten reserviert. Die weiteren Buchstaben bezeichnen die primären und logischen Partitionen der Festplatte. Erweiterte Partitionen erhalten keinen Laufwerksbuchstaben und sind somit unsichtbar.

Die verschiedenen Windows-Versionen gehen unterschiedlich mit dem Fall um, dass später neue Partitionen oder Laufwerke hinzukommen. Bei Windows 9x/ME bekommen zuerst die primären Partitionen aller Festplatten bzw. Laufwerke einen Buchstaben. Erst anschließend werden auch die logischen Partitionen benannt. Ab Windows NT ändern sich bereits genutzte Laufwerksbuchstaben dagegen nicht mehr. Neue Laufwerke bzw. Partitionen bekommen einfach den ersten freien Buchstaben. Außerdem können Sie Laufwerken einen freien Buchstaben fix zuordnen.

Partitionen mit fremden Dateisystemen (also z. B. Linux-Partitionen) bekommen keinen Laufwerksbuchstaben und sind daher in den meisten Programmen unsichtbar. Die Partitionen werden nur in Partitionierungsprogrammen angezeigt.

Linux

Unter Linux erfolgt der interne Zugriff auf Festplatten bzw. deren Partitionen über sogenannte Device-Dateien (siehe Tabelle 2.2). Die Festplatten erhalten der Reihe nach die Bezeichnung `/dev/sda`, `/dev/sdb`, `/dev/sdc` etc.

Device-Name	Bedeutung
`/dev/sda`	erste Festplatte
`/dev/sdb`	zweite Festplatte
...	
`/dev/sda1`	die erste primäre Partition der Festplatte `/dev/sda`
`/dev/sda2`	die zweite primäre Partition
`/dev/sda3`	die erweiterte Partition (nur MBR)
`/dev/sda5`	die erste logische Partition (nur MBR)
`/dev/sda8`	die vierte logische Partition (nur MBR)
...	

Tabelle 2.2 Device-Namen von Festplattenpartitionen

Um eine einzelne Partition und nicht die ganze Festplatte anzusprechen, wird der Name um die Partitionsnummer ergänzt. Bei der MBR-Partitionierung sind die Zahlen 1 bis 4 für primäre und erweiterte Partitionen reserviert. Logische Partitionen beginnen mit der Nummer 5, auch dann, wenn es weniger als vier primäre oder erweiterte Partitionen gibt. Bei der GPT-Partitionierung werden einfach alle Partitionen der Reihe nach durchnummeriert.

2.7 RAID, LVM und Verschlüsselung

Dieser Abschnitt führt in die Grundlagen von RAID und LVM ein und geht kurz auf das Thema Verschlüsselung ein. Wenn Sie vorhaben, eine ganz gewöhnliche Desktop-Installation auf einem Notebook bzw. Rechner mit nur einer Festplatte durchzuführen, können Sie diesen Abschnitt getrost überspringen. Wenn Sie aber eine Server-Installation planen, sollten Sie diesen Abschnitt in Ruhe lesen: Viele Linux-Installationsprogramme unterstützen alle drei Verfahren. Nur wenn Sie die zugrunde liegenden Techniken kennen, können Sie die Tragweite einer Entscheidung für oder wider den Einsatz von RAID, LVM und Verschlüsselungstechniken abschätzen.

Redundant Array of Independent Disks (RAID)

Die Grundidee von RAID besteht darin, Partitionen mehrerer Festplatten logisch miteinander zu verknüpfen. Das Ziel ist dabei, ein zuverlässigeres und/oder schnelleres Gesamtsystem zu schaffen:

- Durch RAID kann die Datenübertragung gesteigert werden, indem der Datenzugriff von mehreren Festplatten parallel erfolgt.
- Durch RAID kann aber auch die Sicherheit gesteigert werden, indem Daten redundant (mehrfach) gespeichert werden. Das ist allerdings mit Geschwindigkeitseinbußen verbunden und beansprucht zusätzlichen Speicherplatz.

Hardware- versus Software-RAID

Es gibt zwei grundsätzliche Möglichkeiten, RAID zu realisieren: durch Hardware (also durch einen Festplattencontroller, der die RAID-Logik selbst ausführt) oder durch Software, die von der CPU des Rechners ausgeführt wird. Hardware-RAID kommt vor allem in teuren Server-Systemen zum Einsatz. Seine größten Vorzüge bestehen darin, dass die CPU nicht durch RAID-Aufgaben belastet wird und dass der RAID-Controller unabhängig vom Betriebssystem agiert.

Bei Software-RAID wird zwischen verschiedenen Formen unterschieden, je nachdem, woher die Software kommt:

- **Fake-RAID:** Beim Fake-RAID realisiert das BIOS bzw. EFI in Kombination mit einem Betriebssystem-Treiber verschiedene RAID-Level. Der abfällige Begriff *Fake-RAID* erklärt sich daraus, dass viele RAID-Controller so angepriesen werden, als wären sie echte Hardware-RAID-Controller – und das ist unrichtig. In der Vergangenheit wurde Fake-RAID oft auch als BIOS-RAID bezeichnet, der analoge Begriff EFI-RAID hat sich aber nicht eingebürgert.
- **Linux-Software-RAID:** Linux kann durch den Multi Devices Driver Support mehrere Festplatten(partitionen) zu einem RAID verbinden. Das ist genauso schnell wie Fake-RAID, lässt sich aber wesentlich besser administrieren. Aus Linux-Sicht ist diese RAID-Variante vorzuziehen. Wenn in diesem Buch ohne weitere Erläuterungen von RAID die Rede ist, dann ist Linux-Software-RAID gemeint!
- **Windows-Software-RAID:** Auch Windows unterstützt seit Windows NT verschiedene RAID-Varianten in Form von Software-RAID. Derart eingerichtete Windows-Dateisysteme sind für Linux nicht lesbar.

Vermeiden Sie Fake-RAID!

Fake-RAID wird von vielen Distributionen nicht oder nur halbherzig unterstützt. Im schlimmsten Fall erkennt das Installationsprogramm ein vorhandenes Fake-RAID nicht und führt eine Neupartitionierung durch, was mit dem Verlust aller Daten einhergeht.

RAID-Level

Es gibt verschiedene Verfahren, um Festplattenpartitionen zu verbinden. Diese Varianten werden als »RAID-Level« bezeichnet:

- **RAID-0 (Striping):** Bei RAID-0 werden mehrere physikalische Partitionen zu einer größeren Partition vereint. Dabei werden die Daten parallel in kleinen Blöcken (z. B. 4 kByte) auf die einzelnen Partitionen verteilt, sodass die Daten beim Zugriff alternierend von allen Festplatten gelesen werden. Daraus ergibt sich im Idealfall eine Vervielfachung der Datenrate (d. h. bei drei Festplatten eine Verdreifachung). In der Praxis ist der Effekt meist kleiner als erhofft und kommt nur bei großen Dateien wirklich zum Tragen. Die Anzahl der Random-Access-Zugriffe pro Sekunde wird durch das Striping nicht verbessert. RAID-0 hat einen gravierenden Nachteil: Das Ausfallrisiko ist hoch, weil *eine* defekte Festplatte zum Verlust *aller* Daten führt.
- **RAID-1 (Mirroring):** Bei RAID-1 werden dieselben Daten in der Regel auf zwei Festplatten gespeichert (selten auch auf mehr Festplatten). Wenn eine Festplatte ausfällt, stehen alle Daten auf der anderen Festplatte zur Verfügung. Der Vorteil ist die höhere Sicherheit, der Nachteil die halbierte Kapazität. RAID-1 bietet keine Geschwindigkeitsvorteile, vielmehr werden insbesondere Schreibvorgänge sogar ein wenig langsamer ausgeführt als bei der einfachen Verwendung einer Festplatte.
- **RAID-10:** RAID-10 kombiniert RAID-1 und RAID-0 und setzt mindestens vier Festplatten bzw. Partitionen voraus: Die Festplatten 1 und 2 bilden einen RAID-1-Verbund, die Festplatten 3 und 4 einen weiteren RAID-1-Verbund. Auf der nächsten Ebene werden die beiden RAID-1-Verbunde zu einem RAID-0-Verbund kombiniert. Damit kombiniert RAID-10 die Vorteile von RAID-0 (Geschwindigkeit) und RAID-1 (Sicherheit).
- **RAID-5 (Parity Striping):** RAID-5 funktioniert im Prinzip wie RAID-0, allerdings werden zusätzlich in einer (für jeden Datenblock wechselnden) Partition Paritätsinformationen gespeichert. Wenn eine Festplatte ausfällt, können die gesamten Daten rekonstruiert werden. Der Ausfall von zwei oder mehr Festplatten führt allerdings zu einem kompletten Datenverlust. RAID-5 setzt zumindest drei Festplatten voraus.

  RAID-5 ist ebenso sicher wie RAID-1 und bei Lesezugriffen etwa so schnell wie RAID-0. Zudem hat RAID-5 den Vorteil, dass der für die Redundanz erforderliche Datenanteil mit der Anzahl der Festplatten kleiner wird: Bei RAID-1 beträgt der Kapazitätsverlust immer 50 Prozent; bei RAID-5 beträgt er nur 33 Prozent bei drei Festplatten, 25 Prozent bei vier, 20 Prozent bei fünf etc.

  RAID-5 hat gegenüber RAID-1 allerdings auch Nachteile: Zum einen sind Schreiboperationen langsamer als bei RAID-1, insbesondere wenn sich häufig kleine Datenmengen ändern. Der Grund ist, dass selbst bei kleinen Veränderungen

die Paritätsinformationen für einen ganzen Datenblock neu berechnet und gespeichert werden müssen.

Nach dem Austausch einer defekten Platte dauert die Rekonstruktion des RAID-5-Verbunds sehr lange, viel länger als bei RAID-1. Bei einem Software-RAID kann der RAID-Verbund während dieser Zeit nicht genutzt werden. Sollte während der Rekonstruktion eine weitere Platte ausfallen, sind alle Daten verloren.

- **RAID-6:** RAID-6 funktioniert wie RAID-5, ist aber doppelt redundant und erfordert zumindest vier Festplatten. Selbst beim Ausfall von zwei Festplatten kommt es zu keinem Datenverlust.

Weitere RAID-Level sowie viele interessante Details und Grundlagen zu RAID finden Sie im folgenden Wikipedia-Artikel:

http://de.wikipedia.org/wiki/RAID

Logical Volume Manager (LVM)

Der Logical Volume Manager setzt eine logische Schicht zwischen das Dateisystem und die Partitionen der Festplatte. Was zuerst sehr abstrakt klingt, hat in der Praxis durchaus handfeste Vorteile:

- Im Rahmen des von LVM verwalteten Festplattenbereichs können Sie im laufenden Betrieb ohne Rechnerneustart Partitionen anlegen, vergrößern und verkleinern. Den vorhandenen LVM-Speicherpool können Sie jederzeit durch den Einbau einer weiteren Festplatte vergrößern.
- Sie können dank LVM Bereiche mehrerer Festplatten zu einer einzigen, riesigen virtuellen Partition zusammenfassen.
- Sie können sehr einfach einen sogenannten Snapshot eines Dateisystems erstellen. Das ist ideal für Backups im laufenden Betrieb.
- LVM ist sehr schnell. Sie bezahlen für die höhere Flexibilität also nicht mit einer spürbar verringerten Geschwindigkeit. Der Geschwindigkeitsunterschied gegenüber dem direkten Ansprechen einer Festplattenpartition ist kaum messbar. Die CPU-Belastung ist nur geringfügig höher.

LVM kann mit RAID kombiniert werden, indem ein RAID-Verbund als Grundlage für LVM verwendet wird. In diesem Fall muss zuerst RAID und dann darauf aufbauend LVM konfiguriert werden.

Glossar

Die Fülle ähnlich lautender Begriffe und Abkürzungen erschwert den Einstieg in die LVM-Welt. Um die Konfusion nicht noch zu vergrößern, verzichte ich in diesem Abschnitt bewusst auf eine Übersetzung der Begriffe. Zwischen der Festplatte und

dem Dateisystem stehen drei Ebenen: Physical Volumes, Volume Groups und Logical Volumes:

- **Physical Volume (PV):** Ein PV ist im Regelfall eine von LVM verwaltete Partition der Festplatte. Es kann sich auch um eine ganze Festplatte oder um ein RAID-Device handeln. Entscheidend ist, dass die Partition, die Festplatte oder der RAID-Verbund als PV gekennzeichnet ist, damit die unterschiedlichen LVM-Kommandos funktionieren.
- **Volume Group (VG):** Ein oder mehrere Physical Volumes können zu einer Gruppe zusammengefasst werden. Auf diese Weise ist es möglich, Partitionen unterschiedlicher Festplatten quasi zusammenzuhängen, also einheitlich zu nutzen. Die Volume Group stellt eine Art Speicherpool dar, der alle zur Verfügung stehenden physikalischen Speichermedien vereint. Dieser Pool kann jederzeit um weitere Physical Volumes erweitert werden.
- **Logical Volume (LV):** Ein Logical Volume ist ein Teil der Volume Group. Für den Anwender wirkt ein Logical Volume wie eine virtuelle Partition. Im Logical Volume wird das Dateisystem angelegt. Das heißt, anstatt ein Dateisystem in `/dev/sda7` anzulegen, geben Sie jetzt den Device-Namen des Logical Volume an. Falls in der Volume Group noch Speicher verfügbar ist, können Logical Volumes jederzeit vergrößert werden.

In der LVM-Dokumentation kommen noch zwei weitere Begriffe häufig vor:

- **Physical Device (PD):** Dabei handelt es sich einfach um eine Festplatte. LVM kann die gesamte Festplatte oder auch Partitionen dieser Festplatte in Form von Physical Volumes nutzen.
- **Physical Extent (PE):** Bei Volume Groups und Logical Volumes kann nicht jedes einzelne Byte einzeln verwaltet werden. Die kleinste Dateneinheit ist vielmehr ein Physical Extent (standardmäßig 4 MByte). Die Anzahl der PEs ist unbegrenzt. Zu viele PEs machen aber die Verwaltung ineffizient, weswegen Sie für sehr große Logical Volumes die Größe von PEs hinaufsetzen sollten.

Beispiel

Das folgende Beispiel (siehe Abbildung 2.4) veranschaulicht die oben definierten Begriffe: Auf einem System dienen die beiden Partitionen `/dev/sda3` und `/dev/sdb1` als Physical Volumes für eine Volume Group eines LVM-Systems. `/dev/sda3` umfasst 400 GByte, `/dev/sdb1` umfasst 900 GByte. Der LVM-Speicherpool (also die Volume Group) ist somit 1,3 TByte groß. Darin befinden sich nun diverse Logical Volumes:

LV1 mit der Systempartition (50 GByte)
LV2 mit der Partition `/var` (200 GByte)
LV3 mit der Partition `/var/lib/mysql` (200 GByte)
LV4 mit der Partition `/home` (400 GByte)

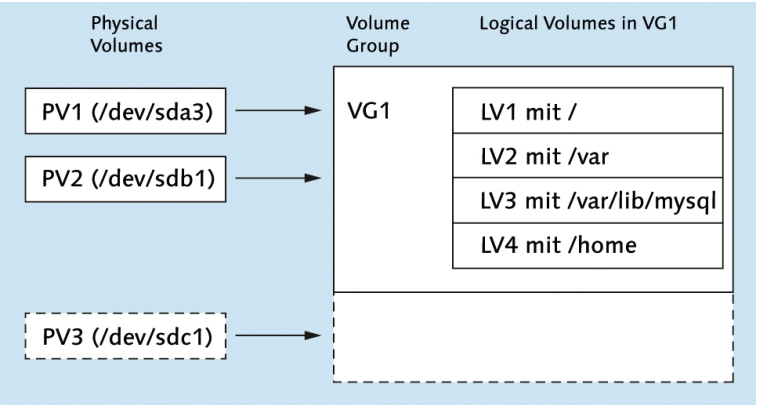


Abbildung 2.4 LVM-System

Insgesamt sind somit 850 GByte mit Partitionen belegt, und 450 GByte sind noch frei. Damit können Sie zu einem späteren Zeitpunkt vorhandene Partitionen vergrößern oder neue Partitionen anlegen. Sollte der gesamte LVM-Pool erschöpft sein, können vorhandene LVs/Dateisysteme verkleinert werden (wenn sich herausgestellt hat, dass sie ursprünglich zu großzügig dimensioniert wurden), um so Platz zur Vergrößerung anderer LVs/Dateisysteme zu schaffen. Reicht das nicht aus, fügen Sie eine weitere Festplatte hinzu und fügen eine Partition dieser Festplatte als drittes Physical Volume zur Volume Group hinzu.

Verschlüsselung

Viele Distributionen bieten die Möglichkeit, die Installation in verschlüsselten Partitionen durchzuführen bzw. zumindest die Partition für die persönlichen Daten verschlüsselt anzulegen. Beim Systemstart muss dann ein Passwort angegeben werden, bevor auf das Dateisystem zugegriffen werden kann. Sofern Sie ein ausreichend langes und nicht erratbares Passwort verwenden, schützt die Verschlüsselung Ihre Daten wirkungsvoll: Auch wenn Ihr Notebook in falsche Hände gelangt, kann niemand Ihre Dateien lesen.

Wahrscheinlich fragen Sie sich, was Verschlüsselung mit RAID und LVM zu tun hat: Die meisten Verschlüsselungssysteme beruhen darauf, dass das verschlüsselte Dateisystem nicht direkt angesprochen wird, sondern über eine Zwischenschicht, die für die Verschlüsselung verantwortlich ist. Technisch gesehen ist die Vorgehensweise ganz ähnlich wie bei LVM, und deswegen gelten auch dieselben Einschränkungen wie bei LVM.

Einschränkungen

Der Einsatz von RAID, LVM und Verschlüsselung hat nicht nur Vorteile, sondern ist auch mit diversen Einschränkungen bzw. Nachteilen verbunden:

- Der eigentlich veraltete Bootloader GRUB 0.97, der aber noch von einigen Enterprise-Distributionen eingesetzt wird, ist zu RAID, LVM und zu den meisten Verschlüsselungssystemen inkompatibel. Deswegen ist eine eigene Bootpartition erforderlich, deren Daten außerhalb des durch RAID oder LVM verwalteten bzw. außerhalb des verschlüsselten Bereichs liegen.

  Debian, Fedora, openSUSE und Ubuntu verwenden schon seit einigen Jahren GRUB 2.0, der mit RAID und LVM kompatibel ist. Diese Distributionen benötigen also keine eigene Bootpartition für LVM- und RAID-Konfigurationen.
- Vermeiden Sie Fake-RAID!
- Die Administration von LVM und RAID ist relativ kompliziert. Während der Installation unterstützt das Installationsprogramm Sie beim Einrichten von LVM, RAID bzw. der verschlüsselten Partition. Wenn Sie dann aber im laufenden Betrieb die Konfiguration verändern möchten, sind Sie bei den meisten Distributionen auf relativ sperrige Kommandos angewiesen. Ausführliche Informationen zum Umgang mit diesen Kommandos finden Sie in Kapitel 25.
- Wenn in einem RAID-Verbund ein Problem auftritt, wird die Fehlermeldung üblicherweise per E-Mail versandt. Das setzt voraus, dass auf dem Rechner ein E-Mail-Server läuft. Dessen sichere Konfiguration und Administration ist nicht ganz trivial. Gerade auf Privat-PCs gibt es normalerweise keinen Grund, einen eigenen E-Mail-Server zu betreiben.
- Swap-Partitionen sollten aus Performance-Gründen in gewöhnlichen Partitionen ohne die Verwendung von LVM oder RAID angelegt werden, idealerweise auf jeder Festplatte eine. Wenn Ihnen optimale Sicherheit wichtiger ist als maximale Geschwindigkeit, sollten Sie bei RAID-Systemen allerdings auch die Swap-Partition innerhalb des RAID-Verbunds einrichten. Das stellt sicher, dass auch bei einem Festplattenausfall keine Daten des Swap-Speichers verloren gehen.
- Wenn Sie ein verschlüsseltes Dateisystem einsetzen, um Ihre Daten zu schützen, sollte auch die Swap-Partition verschlüsselt werden. Noch besser ist es zumeist, auf die Swap-Partition gleich ganz zu verzichten. Was nützt es, wenn Ihr Dateisystem sicher ist, die Swap-Partition aber ausgelagerte Speicherblöcke mit unverschlüsselten kritischen Daten enthält?
- Während LVM und RAID die Geschwindigkeit Ihres Systems kaum beeinträchtigen und manche RAID-Level sogar zu einem besseren Datenumsatz führen können, kostet die Verschlüsselung viel CPU-Kapazität und verlangsamt Lese- und Schreiboperationen spürbar. Ein weiterer Nachteil besteht darin, dass das

Verschlüsselungspasswort bei jedem Rechnerstart manuell eingegeben werden muss. Prinzipbedingt ist die Verschlüsselung ganzer Dateisysteme somit ungeeignet für Server, die automatisch (neu) starten sollen.

Kurz und gut: Bei allen Vorteilen, die mit RAID, LVM und diversen Verschlüsselungstechniken verbunden sind, nimmt die Komplexität des Gesamtsystems doch sehr stark zu.

Empfehlung

Linux-Einsteigern rate ich, wegen der damit verbundenen Komplexität auf RAID, LVM und Verschlüsselung gleichermaßen zu verzichten. Das gilt insbesondere, wenn Sie RAID-1 oder RAID-5 einsetzen möchten, um eine höhere Datensicherheit zu erzielen! Sicherheit vor Datenverlusten haben Sie nur, wenn Sie nach dem Ausfall einer Festplatte auch in der Lage sind, die richtigen Kommandos auszuführen, um die defekte Platte zu deaktivieren und um dem RAID-Verbund eine neue Festplatte hinzuzufügen. Linux-Einsteiger sind damit sicherlich überfordert, vor allem, wenn sie aufgrund des drohenden Datenverlusts gerade unter Stress stehen. Aus diesem Grund sind einfache, aber konsequent durchgeführte Backups besser als eine technisch noch so hervorragende RAID-Konfiguration!

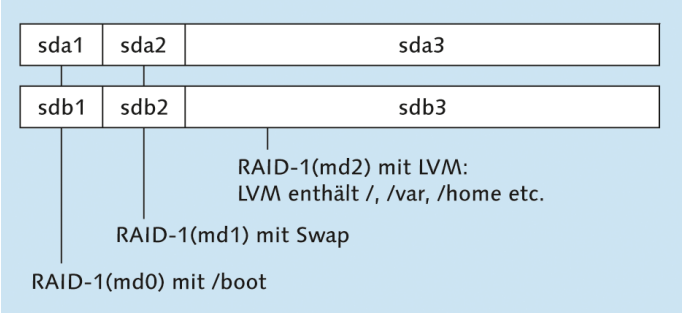


Abbildung 2.5 Server-Konfiguration mit RAID-1 und LVM auf zwei Festplatten

Beim Einrichten eines Servers sind RAID und LVM dagegen empfehlenswert, aber selbst da lautet die goldene Regel KISS (Keep it simple, stupid!, sinngemäß also: Mach's einfach, Dummkopf!). Persönlich bevorzuge ich in solchen Fällen den Einsatz zweier gleich großer Festplatten, auf denen ich jeweils drei Partitionen einrichte. Diese Partitionen verbinde ich zu drei RAID-1-Verbunden für die Boot-Partition, die Swap-Partition und für LVM (siehe Abbildung 2.5). Im LVM-Bereich richte ich dann nach Bedarf die Root- sowie diverse Datenpartitionen ein.

Zwei Hersteller sind sicherer als einer

Aus Sicherheitsgründen ist es bei RAID-Konfigurationen empfehlenswert, Festplatten unterschiedlicher Hersteller einzusetzen! Wenn Sie nämlich zwei baugleiche Festplatten kaufen (ich weiß, die Versuchung ist groß) und der Hersteller gerade Fertigungsprobleme hatte, kann es Ihnen passieren, dass beide Festplatten innerhalb weniger Tage ausfallen.

2.8 Partitionierung der Festplatte

Einer der wichtigsten Schritte während der Linux-Installation ist das Anlegen neuer Linux-Partitionen. Alle gängigen Installationsprogramme enthalten zu diesem Zweck einfach zu bedienende Partitionierungshilfen. Abbildung 2.6 zeigt exemplarisch den Partitionseditor von Ubuntu.

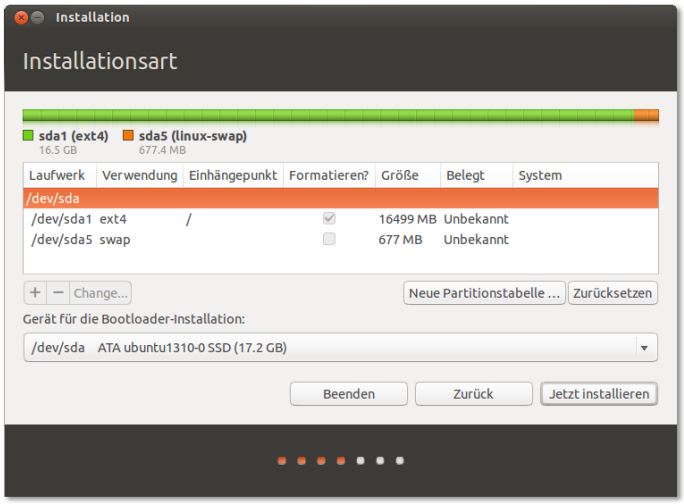


Abbildung 2.6 Ubuntu-Partitionseditor

An dieser Stelle geht es um grundsätzliche Fragen: Wie viele Partitionen sollten Sie für Linux einrichten? In welcher Größe? Welche Auswirkungen hat dies auf die Geschwindigkeit, auf die spätere Wartung und auf eine eventuelle Neuinstallation einer anderen oder aktualisierten Linux-Distribution?

Partitionierung im laufenden Betrieb ändern

Wenn Sie Linux bereits installiert haben und im laufenden Betrieb eine neue Partition anlegen möchten, brauchen Sie ein Partitionierwerkzeug, das unabhängig vom Installationsprogramm Ihrer Distribution funktioniert. Dazu zählen die Programme `fdisk`, `parted` und `gparted`, die ich Ihnen in Kapitel 25 näher vorstelle.

Achtung

Wie ich im vorigen Abschnitt erwähnt habe, sind viele Linux-Distributionen nicht Fake-RAID-kompatibel! Wenn das BIOS oder EFI Ihres Rechners mehrere Festplatten zu einem RAID-Verbund zusammenschließt, erscheinen diese Festplatten für Windows wie eine einzige, große Festplatte. Wenn das Partitionierungswerkzeug Ihrer Linux-Distribution hingegen mehrere Einzelfestplatten sieht, erkennt es das RAID-System nicht richtig. Brechen Sie die Installation ab! Sie riskieren den Verlust Ihrer gesamten Daten! Verwenden Sie eine Distribution mit besserer Fake-RAID-Unterstützung (z. B. Fedora) oder, noch besser, vermeiden Sie Fake-RAID ganz!

Windows-Partition verkleinern

Oft befindet sich das bereits installierte Windows in einer einzigen, sehr großen Partition, die die gesamte Festplatte ausfüllt. Dass innerhalb dieser Partition womöglich Hunderte GByte frei sind, nützt nichts: Linux braucht für die Installation eine oder besser gleich mehrere eigene Partitionen. Und bevor Sie diese Partitionen anlegen können, müssen Sie die Windows-Partition verkleinern – und das möglichst ohne Datenverlust!

Die radikalere und einfachere Lösung bestünde darin, die Windows-Partition(en) einfach zu löschen. Aber die meisten Linux-Umsteiger wollen Windows als alternatives Betriebssystem vorerst erhalten – beispielsweise zum Spielen oder zur Ausführung von Programmen, die es unter Linux nicht gibt. Deswegen gehe ich in diesem Buch davon aus, dass Windows bereits installiert ist und auch weiterhin genutzt werden soll.

Verkleinerung während der Installation

Bei den meisten Distributionen ist das Installationsprogramm selbst in der Lage, die Windows-Partition und das darin befindliche Dateisystem zu verkleinern. Je nach Distribution ändern Sie die Größe der Windows-Partition einfach im Partitionierungsprogramm oder rufen die entsprechende Verkleinerungsfunktion über ein Menü auf. Die Verkleinerung funktioniert sowohl für VFAT- als auch für NTFS-Dateisysteme.

Verkleinern vor der Installation

Wenn eine Verkleinerung der Windows-Partition durch das Linux-Installationsprogramm scheitert, können Sie diesen Schritt auch *vor* der Installation durch andere Werkzeuge vornehmen. Hier eine kleine Auswahl:

- **Direkt unter Windows:** Seit Windows Vista ist eine verlustfreie Verkleinerung von Windows-Partitionen im laufenden Betrieb möglich. Unter Windows 7 führen Sie dazu SYSTEMSTEUERUNG • SYSTEM UND SICHERHEIT • VERWALTUNG • COMPUTERVERWALTUNG • DATENTRÄGERVERWALTUNG aus, klicken die Windows-Partition mit der rechten Maustaste an und führen VOLUME VERKLEINERN AUS.

  Ältere Windows-Versionen bieten keine Möglichkeit, Partitionen zu verkleinern. Sie können Partitionen lediglich löschen und neu anlegen. Dabei verlieren Sie den gesamten Inhalt der Partition.

- **Mit einem Live-System:** Live-Systeme wie Knoppix, GParted oder SystemRescueCD enthalten verschiedene Kommandos bzw. Programme, um Windows-Partitionen zu verkleinern. Die Bedienung dieser Werkzeuge ist allerdings teilweise kompliziert.

- **Kommerzielle Programme:** Den größten Komfort bieten kommerzielle Partitionierungsprogramme, die aber leider relativ teuer sind:

  http://www.acronis.com/homecomputing/products/diskdirector

Windows und Linux neu installieren

Falls auf Ihrem Rechner noch gar kein Betriebssystem installiert ist und Sie vorhaben, sowohl Windows als auch Linux zu installieren, sollten Sie mit Windows beginnen. Auch während der Windows-Installation müssen Sie die Festplatte partitionieren. Geben Sie hier an, dass die Windows-Partition nicht die ganze Festplatte füllen soll, sondern nur so viele GByte, wie Sie unter Windows eben nutzen möchten (z. B. 100 GByte). Entscheiden Sie sich im Zweifelsfall lieber für einen kleineren Wert – es ist einfacher, später eine weitere Windows-Partition hinzuzufügen, als die vorhandene Partition zu verkleinern.

Zweier-Potenzen versus Zehner-Potenzen

In diesem Buch, im Großteil der sonstigen Linux-Dokumentation und für die meisten Linux-Werkzeuge werden kByte, MByte, GByte etc. mit Zweier-Potenzen gerechnet:

1 kByte = 2^{10} Byte = 1024 Byte
1 MByte = 2^{20} Byte = 1024^2 Byte = 1.048.576 Byte
1 GByte = 2^{30} Byte = 1024^3 Byte = 1.073.741.824 Byte
1 TByte = 2^{40} Byte = 1024^4 Byte = 1.099.511.627.776 Byte

Viele Festplattenhersteller und auch manche Dateimanager rechnen dagegen dezimal, also mit 10er-Potenzen: 1 TByte = 10^{12} Byte = 1.000.000.000.000 Byte. Damit hat eine Festplatte, die laut Hersteller ein TByte umfasst, gemäß den Konventionen in diesem Buch nur ca. 931 GByte.

Anzahl und Größe von Linux-Partitionen

Immer wieder wird mir die Frage gestellt, wie eine Festplatte mit *n* GByte am besten in Partitionen zerlegt werden soll. Leider gibt es darauf keine allgemeingültige Antwort. Dieser Abschnitt soll Ihnen aber zumindest ein paar Faustregeln für die richtige Anzahl und Größe von Partitionen vermitteln.

Möglicherweise überrascht Sie der Umstand, dass hier fast selbstverständlich von mehreren Partitionen die Rede ist. Wenn für Windows eine Partition ausreicht, sollte dies wohl auch für Linux gelten. Tatsächlich ist es so, dass Sie Linux mit einer einzigen Partition betreiben können – aber eben nicht optimal. Vielmehr bietet es sich an, den Platz auf die im Folgenden beschriebenen Partitionen zu verteilen.

Systempartition

Die Systempartition ist die einzige Partition, die Sie unbedingt benötigen. Sie nimmt das Linux-System mit all seinen Programmen auf. Diese Partition bekommt immer den Namen `/`. Dabei handelt es sich genau genommen um den Punkt, an dem die Partition in das Dateisystem eingebunden wird (den `mount`-Punkt). Wenn das System also einmal läuft, sprechen Sie diese Partition mit dem Pfad `/` an. `/` bezeichnet die Wurzel, also den Anfang des Dateisystems. Aus diesem Grund wird die Systempartition oft als Root-Partition bezeichnet.

Eine vernünftige Größe für die Installation und den Betrieb einer gängigen Distribution liegt bei rund 15 GByte. Dazu kommt natürlich noch der Platzbedarf für Ihre eigenen Daten – es sei denn, Sie speichern eigene Dateien in einer separaten Datenpartition.

Es ist übrigens durchaus möglich, mehrere Linux-Distributionen parallel auf einen Rechner zu installieren; auf meinen Testrechnern ist das der Regelfall. Dazu benötigen Sie für jede Distribution zumindest eine eigene Systempartition. Swap- und Datenpartitionen können gemeinsam genutzt werden. Wenn Sie den Bootloader richtig konfigurieren bzw. EFI verwenden, können Sie dann beim Rechnerstart zwischen Windows und allen installierten Linux-Distributionen wählen.

Bootpartition

Unter Umständen ist es erforderlich, eine eigene Bootpartition mit dem Namen `/boot` anzulegen. Diese Partition beherbergt lediglich die Daten, die während der ersten Phase des Rechnerstarts benötigt werden. Dabei handelt es sich insbesondere um die Kerneldatei `vmlinuz*`, die Initial-RAM-Disk-Datei `initrd*` sowie um einige kleinere Dateien des Bootloaders. Insgesamt enthält die Bootpartition selten mehr als 200 MByte Daten.

Sie brauchen nur dann eine eigene Bootpartition, wenn der Bootloader GRUB nicht in der Lage ist, Dateien aus der Systempartition zu lesen. Das ist dann der Fall, wenn das ganze Dateisystem verschlüsselt ist oder wenn Sie LVM, RAID oder `btrfs` in Kombination mit der alten GRUB-Version 0.97 einsetzen. Das betrifft insbesondere

RHEL 6 und CentOS 6! Die für den Bootprozess erforderlichen Dateien müssen dann in einer eigenen Bootpartition mit einem Standarddateisystem gespeichert werden – in der Regel `ext3` oder `ext4`.

Im Zweifelsfall schadet es nie, eine eigene Bootpartition zu verwenden. Viele Installationsprogramme schlagen deswegen die Einrichtung einer Bootpartition selbst dann vor, wenn diese nicht unbedingt erforderlich ist. Wenn Sie allerdings vorhaben, viele Linux-Distributionen parallel auf Ihre Festplatte zu installieren, führen getrennte Boot- und Systempartitionen zu einer unübersichtlichen Zersplitterung der Festplatte.

Home-Partition

Mit einer Datenpartition trennen Sie den Speicherort für die Systemdateien und für Ihre eigenen Dateien. Das hat einen wesentlichen Vorteil: Sie können später problemlos eine neue Distribution in die Systempartition installieren, ohne die davon getrennte Datenpartition mit Ihren eigenen Daten zu gefährden.

Bei der Datenpartition wird üblicherweise `/home` als Name bzw. `mount`-Punkt verwendet, weswegen oft von der Home-Partition die Rede ist. Es ist nicht möglich, eine Empfehlung für die Größe der Datenpartition zu geben – das hängt zu sehr davon ab, welche Aufgaben Sie mit Ihrem Linux-System erledigen möchten. Wenn Sie sich sicher sind, dass Sie auf Ihrem Rechner keine weiteren Betriebssysteme mehr installieren möchten, können Sie die Home-Partition so groß machen, dass sie den gesamten Rest der Festplatte bzw. SSD füllt.

Weitere Datenpartitionen

Die Aufteilung der Festplatte in Partitionen lässt sich noch weiter treiben. Wenn Sie den Linux-Rechner beispielsweise innerhalb eines größeren Netzwerks als speziellen Server für Netzwerk- oder Datenbank-Aufgaben einsetzen möchten, können Sie für die dabei anfallenden Daten eigene Partitionen vorsehen und ein für die Art des Datenzugriffs optimales Dateisystem auswählen. Diese Art der Optimierung ist allerdings nur für Linux-Experten zweckmäßig.

Sofern auf Ihrer Festplatte noch unpartitionierter Platz frei ist, stellt es kein Problem dar, ein laufendes System um weitere Partitionen zu erweitern und gegebenenfalls Daten von einer vorhandenen Partition in eine neue zu verschieben. Wenn Sie also unsicher sind, warten Sie mit der Partitionierung vorerst einfach noch ein wenig ab, und lassen Sie einen Teil der Festplatte ohne Partitionen.

Swap-Partition

Die Swap-Partition ist das Gegenstück zur Auslagerungsdatei von Windows: Wenn Linux zu wenig RAM hat, lagert es Teile des gerade nicht benötigten RAM-Inhalts dorthin aus. Die Verwendung einer eigenen Partition statt wie unter Windows einer gewöhnlichen Datei hat vor allem Geschwindigkeitsvorteile. Linux kann zwar ebenfalls so konfiguriert werden, dass es statt einer Swap-Partition eine Swap-Datei verwendet, das ist aber unüblich und langsam.

Im Gegensatz zu den anderen Partitionen bekommt die Swap-Partition keinen Namen (keinen `mount`-Punkt). Der Grund: Aus Effizienzgründen wird die Swap-Partition direkt und nicht über ein Dateisystem angesprochen.

Wenn Sie viel RAM haben, können Sie grundsätzlich ganz auf die Swap-Partition verzichten. Das ist aber nicht empfehlenswert: Wenn Linux – etwa wegen eines außer Kontrolle geratenen Programms – kein RAM mehr findet, muss es laufende Programme beenden. Welche das sind, ist nicht vorhersehbar und kann daher zum Absturz des Rechners führen. Wenn eine Swap-Partition existiert, wird Linux aufgrund der RAM-Auslagerung immer langsamer. Das ist zwar lästig, gibt Ihnen aber die Chance, dem Problem noch rechtzeitig auf den Grund zu gehen und das fehlerhafte Programm gezielt zu beenden. Die Swap-Partition dient damit weniger als RAM-Reserve, sondern als eine Art automatische Notbremse.

Eine Richtgröße für die Swap-Partition ist die ein- bis zweifache Größe Ihres RAMs, wobei bei einem großen RAM die einfache Größe mehr ausreicht. Bei einem Rechner mit 4 GByte RAM ist die Swap-Partition mit 2 bis 4 GByte gut bemessen. Wenn Sie bei Notebooks den Ruhezustand nutzen möchten, sollte die Swap-Partition zumindest eineinhalbmal so groß wie das RAM sein.

Die maximale Größe für Swap-Partitionen auf 32-Bit-Systemen beträgt 2 GByte. Wenn Sie mehr Swap-Speicher benötigen, richten Sie mehrere Swap-Partitionen ein. Das ist aber selten sinnvoll: Wenn Ihre Anwendungen tatsächlich so viel Speicher benötigen, ist Linux nur noch mit der Übertragung von Seiten zwischen der Swap-Partition und dem RAM beschäftigt und praktisch nicht mehr bedienbar. Abhilfe schaffen hier nicht größere bzw. mehr Swap-Partitionen, sondern eine 64-Bit-Distribution und mehr RAM.

BIOS-GRUB-Partition

Unter ganz bestimmten Umständen sollten Sie zusätzlich zu den bereits erwähnten Partitionen eine BIOS-GRUB-Partition vorsehen: Diese üblicherweise nur 1 MByte große Partition dient als Ort zur Installation des Bootloaders. Sie ist nur erforderlich, wenn die folgenden drei Bedingungen alle erfüllt sind: Ihr Rechner verwendet ein BIOS (und nicht EFI) zum Hochfahren, die darin enthaltene Festplatte hat eine GPT (also keine MBR-Partitionstabelle), und Ihre Distribution verwendet den Bootloader GRUB 2. Diese Partition muss nicht formatiert werden, es ist also kein Dateisystem erforderlich, es muss aber das Flag `bios_grub` gesetzt werden.

EFI-Partition

Auf EFI-Systemen muss es *eine* EFI-Partition geben. Diese Partition wird bei der Installation des ersten Betriebssystems standardmäßig eingerichtet, egal ob es sich um Windows oder Linux handelt. Wenn später weitere Betriebssysteme installiert werden, teilen sich alle Betriebssysteme die gemeinsame EFI-Partition und legen dort jeweils Dateien zum Start des Betriebssystems ab. Die EFI-Partition muss ein

VFAT-Dateisystem enthalten und wird unter Linux über das Verzeichnis `/boot/efi` angesprochen.

Fazit

Bei jeder Linux-Installation benötigen Sie eine Systempartition. Darüber hinaus ist eine Swap-Partition sehr zu empfehlen. Das Einrichten weiterer Partitionen ist optional, sehr stark von der geplanten Anwendung von Linux abhängig und auch eine Geschmacksfrage. Meine persönliche Empfehlung für eine Linux-Erstinstallation ist in Tabelle 2.3 zusammengefasst.

Verzeichnis	Verwendung
	BIOS-GRUB-Partition (1 MByte, nur für die Kombination BIOS + GPT + GRUB2)
`/boot/efi`	EFI-Partition (nur bei EFI-Systemen, ca. 200 MByte)
	Swap-Partition (ca. so groß wie das RAM)
`/`	Systempartition (ca. 15 GByte)
`/home`	Datenpartition (Größe je nach geplanter Nutzung)

Tabelle 2.3 Empfohlene Partitionen für den Desktop-Einsatz

Welches Dateisystem?

Linux unterstützt eine Menge unterschiedlicher Dateisysteme, unter anderem `ext2`, `ext3`, `ext4`, `btrfs`, `reiserfs` und `xfs`. Im Detail werden diese Dateisysteme in Kapitel 25 vorgestellt. Alle Dateisysteme mit der Ausnahme von `ext2` unterstützen Journaling-Funktionen, stellen also sicher, dass das Dateisystem auch bei einem unvorhergesehenen Absturz oder Stromausfall konsistent bleibt. (Die Journaling-Funktionen schützen allerdings *nicht* vor einem Datenverlust bei Dateien, die gerade geöffnet sind!)

ext4

Der populärste Dateisystemtyp für Linux ist `ext4`. Die Vorteile im Vergleich zur Vorgängerversion `ext3` sind die höhere maximale Dateisystemgröße, eine höhere Geschwindigkeit bei manchen Dateioperationen und insbesondere eine wesentlich schnellere Überprüfung des Dateisystems.

btrfs

Viele Linux-Dateisystementwickler betrachten `ext4` als Übergangslösung, bis das von Grund auf neu entwickelte Dateisystem `btrfs` fertiggestellt ist und stabil läuft. Das wird aber wohl noch ein, zwei Jahre dauern. (Dieser Satz steht nun leider schon seit einigen Auflagen in diesem Kapitel ...) Momentan ist der Einsatz von `btrfs` nur experimentierfreudigen Linux-Entwicklern zu empfehlen.

xfs Für große Server-Installationen können erfahrene Administratoren auch `xfs` in Erwägung ziehen. Dieses ursprünglich von SGI entwickelte Dateisystem gilt als robust und schnell, vor allem wenn sehr große Datenmengen im Spiel sind (viele TByte!). Unter RHEL 7 wird `xfs` voraussichtlich das Default-Dateisystem sein.

Swap-Partition In der Swap-Partition wird *kein* richtiges Dateisystem eingerichtet! Die Partition muss aber vor der ersten Verwendung durch `mkswap` formatiert werden. Alle Linux-Distributionen kümmern sich automatisch darum.

BIOS-GRUB-Partition Auch in der BIOS-GRUB-Partition wird *kein* richtiges Dateisystem eingerichtet! Die Partition muss aber mit dem Flag `bios_grub` gekennzeichnet werden.

Fazit Tabelle 2.4 fasst zusammen, welche Dateisysteme Sie am besten für welche Partitionen einsetzen. Die Empfehlungen gelten für eine gewöhnliche Installation als Desktop- oder Entwicklungssystem.

Partition	Verwendung
EFI-Partition	VFAT (Windows)
BIOS-GRUB-Partition	kein Dateisystem erforderlich
Swap-Partition	kein Dateisystem erforderlich
`/`	`ext4`
`/boot`	`ext3` **oder** `ext4`
`/home`	`ext4`

Tabelle 2.4 Empfohlene Dateisystemtypen für den Desktop-Einsatz

2.9 Installationsumfang festlegen (Paketauswahl)

Bei vielen Distributionen können Sie während der Installation auswählen, welche Komponenten, Programme bzw. Pakete installiert werden. Aus verschiedenen Gründen ist es selten sinnvoll, einfach alles zu installieren:

- Die riesige Anzahl der verfügbaren Software-Pakete überfordert Einsteiger. Erheblich übersichtlicher ist es, vorerst nur eine Grundinstallation durchzuführen und die benötigten Zusatzprogramme später bei Bedarf nachzuinstallieren.
- Es gibt Programme, die sich gegenseitig im Weg sind. So können Sie beispielsweise auf einem Rechner nicht zwei verschiedene E-Mail-Server gleichzeitig betreiben. Sie müssen sich für eine Variante entscheiden.

- Wenn Sie vorhaben, den Rechner als Netzwerk-Server einzusetzen, vergrößert jeder aktive Netzwerkdienst die potenziellen Sicherheitsrisiken. Pakete für Netzwerkfunktionen, die Sie nicht benötigen, sollten Sie gar nicht erst installieren.

Die Auswahl der Software-Pakete erfolgt oft in Form von vorkonfigurierten Gruppen. Es gibt auch Distributionen wie Ubuntu, bei denen Sie während der Installation gar keinen Einfluss auf die Paketauswahl haben: In diesem Fall wird einfach nur ein Grundsystem installiert. Auch bei den meisten Installationsprogrammen, die aus einem Live-System heraus gestartet werden, ist eine Paketauswahl unmöglich – es wird einfach das gesamte Live-System auf die Festplatte übertragen. In beiden Fällen installieren Sie alle weiteren Programme erst später bei Bedarf.

Installationsempfehlungen

Gnome oder KDE

Bei manchen Distributionen haben Sie die Wahl zwischen den Desktop-Systemen KDE und Gnome bzw. können sogar beide Systeme parallel installieren. Dabei handelt es sich um unterschiedliche Benutzeroberflächen zu Linux. Kurz gefasst: Gnome ist einfacher zu bedienen, dafür bietet KDE für technisch versierte Nutzer mehr Funktionen und Einstellmöglichkeiten. Bei einer Parallelinstallation haben Sie maximale Flexibilität und können bei jedem Login auswählen, ob Sie mit Gnome oder KDE arbeiten.

Netzwerkdienste (Server)

Für die Desktop-Anwendung von Linux brauchen Sie üblicherweise keinen Web-, Mail- oder Datenbank-Server. Es gibt allerdings drei Ausnahmen:

- Um Ihren Drucker verwenden zu können, brauchen Sie einen Drucker-Server. Bei den meisten Distributionen wird dazu CUPS standardmäßig installiert.
- Um Ihren Rechner über das Netzwerk steuern zu können, sollten Sie einen SSH-Server installieren.
- Wenn Sie eigene Verzeichnisse mit Windows-Rechnern im lokalen Netz teilen möchten, müssen Sie das Programm Samba installieren.

Entwicklungswerkzeuge und Kernel-Header

Gerade Linux-Einsteiger haben vermutlich wenig Ambitionen, den Linux-Kernel neu zu kompilieren. Dennoch ist die Installation der elementaren Entwicklungswerkzeuge (C-Compiler, `make` etc.) und der sogenannten Kernel-Header-Dateien empfehlenswert. Damit sind Sie in der Lage, selbst neue Kernelmodule zu kompilieren. Das ist erforderlich, wenn Sie zusätzliche Hardware-Treiber installieren möchten, die nicht vollständig als Open-Source-Code verfügbar sind, oder wenn Sie kommerzielle Virtualisierungsprogramme einsetzen möchten. Die Installation des vollständigen Kernelcodes ist dazu nicht erforderlich!

2.10 Grundkonfiguration

Dieser Abschnitt gibt einige Hintergrundinformationen zu den üblichen Schritten der Basiskonfiguration. Reihenfolge, Details und Umfang der Grundkonfiguration variieren stark je nach Distribution. Einige Distributionen beschränken die Konfiguration während der Installation auf ein Minimum. Die weitergehende Hardware-Konfiguration erfolgt dann erst im laufenden Grundsystem. Generell gilt: Nahezu alle Einstellungen können auch später durchgeführt werden. Verschieben Sie die Konfiguration von momentan nicht benötigten Komponenten einfach auf später!

Root-Passwort

Unter Linux ist in der Regel der Benutzer `root` für die Systemadministration zuständig. Dieser Benutzer hat uneingeschränkte Rechte, aber natürlich ist damit auch das Schadenspotenzial uneingeschränkt. Es ist daher unbedingt erforderlich, dass der Zugang zu `root` mit einem Passwort abgesichert wird.

Bei Ubuntu und einigen anderen Distributionen ist der Benutzer-Account `root` vollständig deaktiviert. Eine Passwortabsicherung für `root` ist daher nicht nötig. Administrative Aufgaben werden bei Ubuntu von dafür vorgesehenen Benutzern durchgeführt und erfordern die nochmalige Angabe des Benutzerpassworts.

Bei openSUSE erhalten `root` und der Standardbenutzer dasselbe Passwort. Wenn Sie das nicht wünschen, müssen Sie die leicht zu übersehende Option im Installationsprogramm deaktivieren.

Benutzerverwaltung

Es ist unter Linux unüblich, als `root` zu arbeiten – außer natürlich bei der Durchführung administrativer Aufgaben. Wenn Sie eine E-Mail schreiben, ein Programm kompilieren oder im Internet surfen, melden Sie sich als gewöhnlicher Benutzer an. Während der Installation haben Sie die Möglichkeit, einen oder mehrere derartige Benutzer samt Passwort einzurichten. Im laufenden Betrieb können Sie später weitere Benutzer hinzufügen, das Passwort vorhandener Benutzer verändern etc.

Linux-Benutzernamen sollten aus maximal acht Buchstaben und Ziffern bestehen. Verwenden Sie keine deutschen Sonderzeichen. Die funktionieren zwar meistens, aber nicht immer. Es ist üblich, nur Kleinbuchstaben zu verwenden.

Das Passwort sollte mindestens acht Zeichen lang sein. Idealerweise enthält es sowohl Groß- als auch Kleinbuchstaben sowie mindestens eine Ziffer. Auch diverse Sonderzeichen sind erlaubt, z. B. `+-*/_.,;:()[]`. Deutsche Sonderzeichen (äöüß) und andere Buchstaben, die nicht im ASCII-Zeichensatz definiert sind, sollten Sie hingegen vermeiden.

Netzwerkkonfiguration

Damit Sie Ihren Rechner in einem lokalen Netz einsetzen können, ist eine Netzwerkkonfiguration erforderlich. Die Konfiguration erfolgt vollautomatisch, wenn das Installationsprogramm im lokalen Netz einen sogenannten DHCP-Server erkennt.

Das ist ein Rechner, der allen anderen Rechnern im Netzwerk automatisch die Netzwerkparameter sendet. In diesem Fall reduziert sich die gesamte Netzwerkkonfiguration auf das Anklicken der entsprechenden Option und eventuell auf die Angabe des gewünschten Rechnernamens.

Bei einer manuellen Netzwerkkonfiguration werden Sie nach den folgenden Parametern gefragt. Hintergrundinformationen und Erklärungen zu den hier verwendeten Fachausdrücken finden Sie in Kapitel 29, in dem die Grundlagen der Netzwerkkonfiguration beschrieben sind.

- **Host- und Domainname:** Der Host- und der Domainname entsprechen unter Windows dem Rechnernamen und dem Workgroup-Namen. In einem lokalen Netz ist der Domainname meist vorgegeben. Der Hostname sollte eindeutig sein. Verwenden Sie als Hostnamen nicht `localhost`, dieser Name hat eine besondere Bedeutung!
- **IP-Adresse des Rechners:** Diese Zahl in der Form a.b.c.d (z. B. 192.168.27.35) dient zur internen Identifizierung des Rechners im Netz. Üblicherweise sind die drei ersten Zahlengruppen bereits durch das lokale Netz vorgegeben (z. B. 192.168.27); die vierte Zahl muss innerhalb des Netzes eindeutig sein.
- **Netzwerkmaske, Netzwerkadresse und Broadcast-Adresse:** Die Ausdehnung eines lokalen Netzes wird durch zwei oder drei Masken ausgedrückt, die hier ganz kurz anhand eines Beispiels erläutert werden: Wenn das lokale Netz alle Nummern 192.168.27.*n* umfasst, lautet die dazugehörige Netzwerkmaske 255.255.255.0 (der Regelfall für kleine, lokale Netze). Als Netzwerkadresse ergibt sich 192.168.27.0, als Broadcast-Adresse 192.168.27.255.
- **Gateway-Adresse:** Wenn es im lokalen Netz einen Rechner gibt, der für alle anderen Rechner den Internetzugang herstellt, dann geben Sie dessen IP-Adresse an.
- **Nameserver-Adresse:** Der sogenannte Nameserver (oft auch als DNS für Domain Name Server bezeichnet) ist für die Auflösung von Netzwerknamen in IP-Adressen zuständig. Der Nameserver ist also dafür verantwortlich, dass Sie in einem Webbrowser *http://www.google.de* eingeben können und der Rechner automatisch die dazugehörige IP-Adresse ermittelt. Beim Nameserver kann es sich wahlweise um einen Rechner im lokalen Netz handeln, der auch für die Auflösung lokaler Namen zuständig ist, oder um einen externen Rechner des Internet Service Providers.

Firewall

Die meisten Distributionen schützen den Netzwerk- bzw. Internetzugang standardmäßig durch eine Firewall. Diese Firewall lässt von Ihnen initiierte Verbindungen zu, blockiert aber von außen kommende Anfragen und erhöht so die Sicherheit erheblich. Falls Sie vorhaben, auf Ihrem Rechner selbst Netzwerkdienste anzubieten (z. B.

einen SSH- oder Webserver), können Sie für diese Dienste Ausnahmen definieren und externe Zugriffe zulassen.

SELinux, AppArmor

Manche Distributionen sehen über die Paketfilter-Firewall hinaus zusätzliche Schutzsysteme vor, die wichtige Programme gegen Fehlfunktionen schützen. Red Hat bzw. Fedora setzen hierfür SELinux ein, Ubuntu und SUSE das System AppArmor.

Solange Sie nur Programme Ihrer Distribution einsetzen, funktionieren SELinux bzw. AppArmor zumeist problemlos. Wenn Sie vorhaben, selbst kompilierte Netzwerkprogramme einzusetzen, oder sonst von elementaren Konfigurationsvorgaben Ihrer Distribution abweichen, führen SELinux bzw. AppArmor leider oft zu Problemen. Deren einfachste Lösung besteht darin, SELinux bzw. AppArmor einfach zu deaktivieren; das ist auch im laufenden Betrieb möglich.

Zeitzone

Damit die Uhrzeit korrekt eingestellt wird, muss das Installationsprogramm wissen, ob die CMOS-Uhr Ihres Rechners die lokale Uhrzeit oder die *Universal Coordinated Time* (UTC) enthält und in welcher Zeitzone Sie sich befinden. Falls Ihr Rechner ständigen Internetzugang hat, können Sie viele Distributionen auch so konfigurieren, dass die Uhrzeit mit einem Zeit-Server (NTP-Server) aus dem Internet synchronisiert wird.

Sprache

Standardmäßig wird Linux in der zu Beginn der Installation eingestellten Sprache installiert – für die Leser dieses Buchs also in der Regel in Deutsch. Standardmäßig werden auch die englischen Sprachdateien installiert. Das stellt sicher, dass zumindest englische Menü-, Dialog- und Hilfetexte zur Verfügung stehen, falls es keine deutsche Übersetzung gibt.

Wenn einzelne Benutzer Ihres Rechners Linux auch in anderen Sprachen nutzen möchten, müssen Sie zusätzlich entsprechende Sprachdateien installieren (in Form von sogenannten Lokalisierungspaketen). Sie können dann bei jedem Login die gewünschte Sprache wählen.

2.11 Installation des Bootloaders

Die letzte Frage ist nun noch, wie Linux in Zukunft gestartet werden soll. Dafür ist bei den meisten Distributionen das Programm GRUB verantwortlich. Es wird automatisch installiert; nur wenige Distributionen bieten bei diesem Punkt Konfigurationsmöglichkeiten. Hintergrundinformationen zur manuellen Installation, Konfiguration und Reparatur von GRUB finden Sie in Kapitel 26.

GRUB bei BIOS-Rechnern

Bei BIOS-Rechnern wird der Startcode von GRUB üblicherweise in den ersten Sektor der Festplatte installiert, den sogenannten Bootsektor bzw. Master Boot Record (MBR). Dadurch wird der bisher vorhandene Bootcode, der meist von Windows

stammt, überschrieben. Damit ist in Zukunft GRUB nicht nur für den Linux-Start verantwortlich, sondern auch für das richtige Verzweigen in den Windows-Bootloader. Beim Start des Rechners erscheint ein kleines Menü, in dem Sie zwischen Windows und Linux wählen (siehe Abbildung 2.7 mit dem grafischen GRUB-Menü von openSUSE).

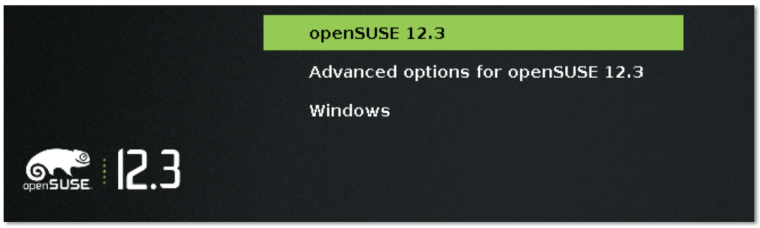


Abbildung 2.7 openSUSE oder Windows starten

Es ist möglich, GRUB nicht in den Bootsektor der Festplatte, sondern in den Bootsektor der Linux-Systempartition zu installieren. Das Handbuch des zurzeit populärsten Bootloaders GRUB 2 rät von dieser früher üblichen Vorgehensweise aber ab.

GRUB bei EFI-Rechnern

Bei EFI-Rechnern wird GRUB in eine Partition innerhalb der EFI-Partition installiert. Gleichzeitig wird GRUB zum Standard-Bootloader des Rechners. Wenn Sie anstelle von Linux Windows booten möchten, müssen Sie beim Rechnerstart mit einer Tastenkombination das EFI-Bootmenü einblenden und den gewünschten Eintrag auswählen.

Probleme

Die Installation des Bootloaders funktioniert mittlerweile bei nahezu allen Hard- und Software-Kombinationen – aber in ganz seltenen Fällen geht doch etwas schief. Sie können dann weder Windows noch Linux starten! Tipps, wie Sie mit dieser Situation fertig werden, folgen in den weiteren Abschnitten.

Erster Linux-Start

Je nach Distribution erscheint nach dem ersten Start des neuen Linux-Systems nochmals das Installationsprogramm. Anschließend beginnen Sie Ihre erste Erkundungsreise durch die Linux-Welt. Kapitel 4 gibt dazu einige Tipps.

2.12 Probleme während der Installation

Dieser Abschnitt geht auf einige typische Probleme ein, die während der Installation auftreten können. So weit möglich, finden Sie hier auch Lösungsansätze. Dieses Buch kann allerdings trotz seines großen Umfangs nicht das ganze Linux- und Hardware-Universum umfassen. Sie müssen daher lernen, sich selbst zu helfen – je früher, desto besser.

Hilfe zur Selbsthilfe

Was tun Sie, wenn es während der Installation Probleme gibt, der Rechner stehen bleibt, Hardware nicht oder falsch erkennt etc.? Der erste Tipp ist geradezu trivial: Lesen Sie vor Beginn der Installation auf jeden Fall die sogenannten Release-Notes im Internet oder auf der CD/DVD!

Ein weiterer guter Startpunkt sind natürlich die Homepages der jeweiligen Distributionen. Dort gibt es eigene Support-Bereiche, Foren und Wikis, in denen Sie Antworten zu häufigen Fragen bzw. Problemen finden.

Hardware-Probleme

Wenn Linux für die Installation wichtige Hardware-Komponenten nicht richtig erkennt oder bei deren Erkennung hängen bleibt, helfen eventuell Kernelparameter weiter. Dahinter verbirgt sich ein Mechanismus, dem Kernel beim Start Informationen zur besseren Hardware-Erkennung zu geben. Derartige Parameter geben Sie unmittelbar beim Installationsstart an. Weitere Informationen zu diesem Mechanismus und einen Überblick über einige wichtige bzw. häufig benötigte Parameter finden Sie in Abschnitt 28.4.

Partitionierungsprobleme

Die Partitionierhilfen des Linux-Installationsprogramms sollten dieselben Partitionen erkennen wie vergleichbare Windows-Werkzeuge, die Sie unter Windows 7 mit SYSTEMSTEUERUNG • SYSTEM UND SICHERHEIT • VERWALTUNG • COMPUTERVERWALTUNG • DATENTRÄGERVERWALTUNG starten. Wenn das nicht der Fall ist bzw. Linux statt einer Windows-Partition mehrere Einzelfestplatten sieht, haben Sie die Festplatten Ihres Rechners wahrscheinlich zu einem RAID-System verbunden, das Linux nicht richtig erkennt. Abhilfe schafft die Verwendung einer Linux-Distribution, die korrekt mit Fake-RAID umgehen kann (z. B. Fedora).

Tastaturprobleme

In den ersten Phasen der Installation kann es vorkommen, dass noch kein deutscher Tastaturtreiber installiert ist und daher das amerikanische Tastaturlayout gilt. Das trifft meistens auch während des Starts des Bootloaders zu.

Solange der Rechner glaubt, dass Sie mit einer US-Tastatur arbeiten, während tatsächlich aber ein deutsches Modell im Einsatz ist, sind Y und Z vertauscht; außerdem bereitet die Eingabe von Sonderzeichen Probleme.

Tabelle 2.5 zeigt, wie Sie diverse Sonderzeichen auf einer deutschen Tastatur trotz eines fehlenden Tastaturtreibers eingeben können. Dabei zeigt die erste Spalte die auf einer deutschen Tastatur erforderliche Tastenkombination, um das Zeichen in der zweiten Spalte zu erzeugen. Verwenden Sie auch den numerischen Tastaturblock – die dort befindlichen Sonderzeichen funktionieren mit Ausnahme des Kommas problemlos!

Falls es auch nach der Installation noch Tastaturprobleme gibt, finden Sie in Abschnitt 21.2 (Textmodus) bzw. 24.5 (Grafikmodus) eine Anleitung, wie Sie dieses Manko beheben können.

Kürzel	Ergebnis	Kürzel	Ergebnis	Kürzel	Ergebnis
Z	Y	Ö	;	⇧+9	(
Y	Z	⇧+Ö	:	⇧+0	)
-	/	⇧+-	?	Ü	[
#	\	⇧+Ä	"	+	]
ß	- (Bindestrich/Minus)	Ä	'	⇧+Ü	{
⇧+ß	_ (Unterstrich)	^	`	⇧++	}
'	=	⇧+^	~	⇧+,	<
⇧+'	+	⇧+2	@	⇧+.	>
⇧+8	*	⇧+3	#		
⇧+7	&	⇧+6	^		

Tabelle 2.5 Tastenkürzel zur Eingabe von Sonderzeichen für das US-Tastaturlayout

2.13 Probleme nach der Installation

Manchmal läuft eine Installation ohne Schwierigkeiten bis zum Ende. Erst beim nächsten Neustart treten Probleme auf. Dieser Abschnitt gibt einige Tipps zu häufigen Problemquellen.

Der Rechner kann nicht mehr gestartet werden

Der schlimmste Fall bei einer Linux-Installation besteht darin, dass der Rechner anschließend nicht mehr gestartet werden kann oder dass zumindest einzelne der installierten Betriebssysteme nicht mehr zugänglich sind. Dabei gibt es verschiedene Varianten, die im Folgenden erörtert werden. Wenn diese Informationen nicht weiterhelfen, werfen Sie auch einen Blick in das Stichwortverzeichnis, Eintrag *Notfall*!

- **Linux-Absturz (Hardware-Probleme):** Nach dem Neustart des Rechners erscheinen zuerst diverse Meldungen von Linux. Anschließend bleibt der Rechner stehen bzw. stürzt ab.

  Mögliche Ursache: Die wahrscheinlichste Ursache sind Hardware-Probleme.

  Abhilfe: Durch die Angabe von sogenannten Bootoptionen können Sie Linux bei der Erkennung der Hardware helfen (siehe Abschnitt 28.4). Bootoptionen werden direkt an den Kernel übergeben und werden deswegen auch Kernelparameter genannt. Die Eingabe derartiger Optionen erfolgt im Bootloader GRUB unmittelbar nach dem Rechnerstart. Dazu drücken Sie zuerst Esc, um in das

GRUB-Menü zu gelangen. Dann wählen Sie mit den Cursortasten die zu startende Linux-Distribution aus. Mit E gelangen Sie in den GRUB-Editor, der einige Zeilen anzeigt, die so ähnlich wie das folgende Muster aussehen:

```
kernel (hd0,5)/boot/vmlinuz root=/dev/sda6 splash=silent vga=normal
initrd (hd0,5)/boot/initrd
```

Wählen Sie mit den Cursortasten die `kernel`-Zeile aus, drücken Sie abermals E, um diese Zeile zu verändern, und fügen Sie an das Ende dieser Zeile die zusätzlichen Bootoptionen an. Mit ↵ bestätigen Sie die Änderung. Esc führt zurück zum Bootmenü, wo Sie Linux dann starten. Die Änderung an den Kernelparametern gilt nur für dieses eine Mal, sie wird also nicht bleibend gespeichert.

Hinweis

Bei Hardware-Problemen, die durch Kernelmodule verursacht werden, bleiben die Bootoptionen wirkungslos. Stattdessen muss eine der Dateien im Verzeichnis `/etc/modprobe.d` geändert werden. Dazu starten Sie ein Live-System oder ein sogenanntes Rescue-System (Rettungssystem, Notfallsystem), das sich bei vielen Distributionen auf der Installations-CD befindet. Der Umgang mit einem derartigen System erfordert allerdings einiges an Linux-Wissen und empfiehlt sich daher nicht für Linux-Einsteiger. Hintergrundinformationen zur Modulverwaltung und zu `modprobe.conf` finden Sie in Abschnitt 28.1.

- **Linux-Absturz (unable to mount root fs):** Der Start des Linux-Kernels hat geklappt, Linux konnte aber anschließend die Linux-Systempartition nicht finden.

  Mögliche Ursache: Es liegt ein Problem in der GRUB-Konfiguration vor. Der Fehler kann auch dann auftreten, wenn die Verkabelung von Festplatten geändert wurde.

  Abhilfe: Geben Sie beim Linux-Start die richtige Partition als Bootoption in der Form `root=/dev/sda6` an. Wenn der Start so gelingt, können Sie unter Linux GRUB neu konfigurieren (siehe Abschnitt 26.1). Unter Umständen müssen Sie auch die Datei `/etc/fstab` entsprechend anpassen (siehe Abschnitt 25.5).
- **Linux startet nicht (BIOS):** Nach dem Neustart des Rechners wird ohne Rückfrage einfach Windows gestartet. Von Linux ist keine Spur zu sehen.

  Mögliche Ursache: Die Installation von GRUB (oder eines anderen Bootloaders) auf die Festplatte hat aus irgendeinem Grund nicht funktioniert.

  Abhilfe: Starten Sie ein Rescue-System oder eine Live-CD, und installieren Sie GRUB neu (siehe Abschnitt 26.4).

- **Linux startet nicht (EFI):** Bei EFI-Rechnern kann es sein, dass die GRUB-Installation an sich zwar funktioniert hat und nur der Eintrag des Bootloaders in die Liste der EFI-Betriebssysteme gescheitert ist.

  Abhilfe: Werfen Sie in einem Live-System einen Blick in die EFI-Partition. Wenn Sie dort ein neues Verzeichnis mit dem Namen Ihrer Distribution entdecken, wurde GRUB dorthin installiert. Versuchen Sie, die GRUB- oder SHIM-Datei mit dem Kommando `efibootmgr` zur Liste der EFI-Booteinträge hinzuzufügen (siehe Abschnitt 26.3).

- **Linux startet nicht (EFI Secure Boot):** Beim Versuch, Linux zu starten, wird eine Fehlermeldung wie *secure boot violation* oder *invalid signature* angezeigt. Das deutet auf ein Problem mit EFI Secure Boot hin.

  Abhilfe: Die einfachste Lösung besteht darin, Secure Boot in den EFI-Einstellungen zu deaktivieren. Sofern Ihre Distribution EFI Secure Boot unterstützt, können Sie eine Neuinstallation versuchen; achten Sie dabei darauf, dass Secure Boot aktiviert ist. Bei manchen Installationsprogrammen gibt es hierfür eigene Optionen.

- **Windows startet nicht (BIOS):** Nach dem Neustart wird automatisch Linux gestartet. Windows scheint verschwunden zu sein.

  Mögliche Ursache: Wahrscheinlich hat die GRUB-Installation funktioniert. Sie können nun unmittelbar nach dem Rechnerstart auswählen, welches Betriebssystem gestartet werden soll. Tun Sie nichts, wird nach einer Weile automatisch Linux gestartet. Eventuell erscheint das Menü erst nach dem Drücken von Esc.

  Abhilfe: Falls ein Menü angezeigt wird, wählen Sie mit den Cursortasten `windows` aus und drücken ↵. Falls es kein Menü gibt, starten Sie Linux und fügen in die GRUB-Konfigurationsdatei einen zusätzlichen Eintrag zum Start von Windows ein (siehe Abschnitt 26.1).

- **Windows startet nicht (EFI):** Zu einem ähnlichen Problem kann es auch bei EFI-Installationen kommen. Durch die Linux-Installation gilt nun Linux als Default-Betriebssystem.
  Abhilfe: Um Windows zu starten, drücken Sie unmittelbar nach dem Rechnerstart eine Tastenkombination, um das EFI-Bootmenü anzuzeigen. Für die Tastenkombination gibt es leider keinen Standard, sie ist bei jedem Rechner bzw. Mainboard anders. Den EFI-Default-Booteintrag können Sie entweder im EFI oder mit dem Linux-Kommando `efibootmgr` einstellen (siehe Abschnitt 26.3).

- **Weder Linux noch Windows startet (BIOS):** Nach dem Rechnerstart wird GRUB ausgeführt, stürzt aber sofort ab bzw. zeigt eine endlose Liste von Fehlermeldungen an.

  Mögliche Ursache: Die GRUB-Installation ist fehlgeschlagen.

Abhilfe: Starten Sie ein Rescue-System oder eine Live-CD, und installieren Sie GRUB neu (siehe Abschnitt 26.4). Alternativ können Sie auch den früheren Zustand des Bootsektors (MBR) wiederherstellen (siehe Abschnitt 2.15). Wenn das gelingt, kann Windows anschließend wieder normal gestartet werden. Linux lässt sich allerdings weiterhin nicht starten.

Das Grafiksystem startet nicht

Es kann vorkommen, dass Linux nur im Textmodus startet. Das Grafiksystem X, das die Basis für die Desktop-Systeme KDE oder Gnome ist, funktioniert nicht.

X automatisch starten

Zuerst sollten Sie testen, ob sich X manuell starten lässt. Dazu loggen Sie sich mit Ihrem Benutzernamen und dem Passwort im Textmodus ein und führen dann das Kommando `startx` aus. Wenn das klappt, funktioniert das Grafiksystem prinzipiell. Es geht jetzt nur noch darum, das System so zu konfigurieren, dass das Grafiksystem automatisch gestartet wird. Die Vorgehensweise ist distributionsabhängig und wird im Detail in Abschnitt 24.2 beschrieben.

X manuell konfigurieren

Sollte `startx` nicht zum Erfolg führen, resultieren die Probleme wahrscheinlich aus einer falschen oder gar nicht erfolgten Konfiguration des X Window Systems bzw. seiner Treiber. Ausführliche Hintergrundinformationen zur richtigen X-Konfiguration finden Sie in Kapitel 24.

Die Tastatur funktioniert nicht

Tastaturprobleme äußern sich im Regelfall dadurch, dass statt der gewünschten Buchstaben andere Zeichen erscheinen. Die Ursache ist fast immer eine falsche Einstellung des Tastaturlayouts: Linux glaubt beispielsweise, Sie würden mit einer US-Tastatur arbeiten, in Wirklichkeit besitzen Sie aber ein deutsches Modell. Bei Gnome und KDE können Sie das gewünschte Tastaturlayout vor dem Login einstellen. Die Standardeinstellungen für die Tastatur erfolgen getrennt für den Text- und den Grafikmodus (siehe Abschnitt 21.2 bzw. 24.5).

Menüs erscheinen in der falschen Sprache

Alle Linux-Programme sind in der Lage, Fehlermeldungen, Menüs etc. in englischer Sprache auszugeben. Sehr viele Programme stellen darüber hinaus aber auch Menüs in vielen Landessprachen zur Verfügung. Informationen zur Einstellung der gewünschten Sprache finden Sie in Abschnitt 21.5. Unter Umständen müssen Sie vorher das richtige Sprachpaket installieren, das die Übersetzungen der Menüs und anderer Texte in Ihre Sprache enthält.

2.14 Systemveränderungen, Erweiterungen, Updates

Wenn Ihr Linux-System einmal stabil läuft, wollen Sie es zumeist nach Ihren eigenen Vorstellungen konfigurieren, erweitern, aktualisieren etc. Detaillierte Informationen zu diesen Themen sind über das gesamte Buch verteilt. Dieser Abschnitt dient daher primär als Referenz, um Ihnen die Sucharbeit so weit wie möglich zu ersparen.

Software-Installation, Paketverwaltung

Je nach Distribution existieren verschiedene Kommandos und Programme, mit denen Sie im laufenden Betrieb weitere Software-Pakete installieren, aktualisieren oder entfernen. Einführende Informationen zur unter Linux üblichen Paketverwaltung finden Sie in Kapitel 22.

Generell sollten Sie bei der Installation zusätzlicher Software nur die von Ihrer Distribution vorgesehenen Werkzeuge verwenden und nur zur Distribution passende Pakete verwenden. Wenn Sie hingegen eine SUSE-Distribution durch ein Red-Hat-Paket erweitern, können aufgrund unterschiedlicher Installationspfade oder unterschiedlicher Bibliotheksanforderungen Probleme auftreten.

Updates

Normale Updates

Alle Distributionen bieten Werkzeuge an, um die installierten Programme bzw. Pakete mit wenigen Mausklicks zu aktualisieren. Durch das Update-System werden gravierende Fehler behoben und Sicherheits-Updates durchgeführt. Das erste Update nach der Neuinstallation einer Distribution dauert oft sehr lange, bisweilen länger als die eigentliche Installation! Das liegt daran, dass damit sämtliche Updates installiert werden, die seit der Fertigstellung der Distribution freigegeben wurden. Alle weiteren Updates, die regelmäßig durchgeführt werden, betreffen dann nur noch wenige Pakete und erfolgen entsprechend schneller.

Distributions-Updates

Durch das Update-System werden Fehler und Sicherheitsmängel behoben, aber in der Regel keine grundlegend neuen Programmversionen installiert. Auf ein Update von LibreOffice 3.5 auf Version 3.6 werden Sie also vergeblich warten. Dazu müssen Sie vielmehr Ihre gesamte Distribution auf die nächste Version aktualisieren – daher die Bezeichnung »Distributions-Update«.

Es gibt zwei unterschiedliche Verfahren für Distributions-Updates: Entweder beginnen Sie die Installation von einem Datenträger und geben dann an, dass Sie eine vorhandene Distribution aktualisieren möchten, oder Sie führen das Update im laufenden Betrieb durch und müssen anschließend nur einen Neustart durchführen. Das zweite Verfahren ist wesentlich eleganter, weil es ohne Installationsmedien

durchgeführt werden kann. Die neuen Pakete werden einfach aus dem Internet heruntergeladen. Außerdem wird die Zeit minimiert, während der die Distribution nicht läuft bzw. während der ein Server offline ist. Tabelle 2.6 fasst zusammen, welche Distributionen welche Verfahren unterstützen.

	Update während der Installation	Update im laufenden Betrieb
Debian		•
Fedora	•	
openSUSE	•	•
Red Hat	•	
Ubuntu		•

Tabelle 2.6 Verfahren für Distributions-Updates

Was in der Theorie toll klingt, funktioniert in der Praxis leider oft schlecht. Nach dem Update funktionieren bisweilen Programme nicht mehr wie vorher, und die Suche nach den Fehlern kann zeitraubend sein. Ich selbst habe nach zahllosen Problemen den Glauben an Distributions-Updates verloren.

Persönlich tendiere ich dazu, nicht jedes Distributions-Update mitzumachen, sofern mich nicht die Arbeit an diesem Buch dazu zwingt. Stattdessen führe ich bei Bedarf – oft erst nach drei, vier Jahren – eine komplette Neuinstallation in eine eigene Systempartition durch, wobei ich die Datenpartition `/home` unverändert weiternutze.

Nun kann ich während einer Übergangsphase sowohl die alte als auch die neue Version nutzen. Diese Doppelgleisigkeit erleichtert auch die Neukonfiguration ganz erheblich, weil alle bisherigen Konfigurationsdateien weiterhin zur Verfügung stehen.

Rolling Releases

Rolling Releases sollen die Notwendigkeit von Distributions-Updates ganz eliminieren. Bei Distributionen, die dem Rolling-Release-Modell folgen, werden alle Pakete ständig auf die gerade aktuellste vorliegende Version aktualisiert – so wie dies bei vielen Webbrowsern gehandhabt wird.

Auch dieses Konzept klingt besser, als es tatsächlich funktioniert: Viele Neuerungen führen zwangsläufig zu Inkompatibilitäten oder Migrationsproblemen. Automatische Updates erfolgen unter Umständen zu einem ungünstigen Zeitpunkt, und der Benutzer wird plötzlich mit Programmen konfrontiert, die nicht mehr so funktionieren, wie bisher – oder gar nicht mehr.

Aus diesen Gründen haben sich Rolling-Release-Distributionen bisher nicht durchsetzen können bzw. richten sich ausschließlich an technisch versierte Linux-

Profis. Debian und openSUSE bieten solchen Nutzern durch die Aktivierung der Paketquellen *testing*, *unstable* bzw. *tumbleweed* eine Rolling-Release-Option an.

Konfiguration

Zwar gab es in der Vergangenheit immer wieder Bemühungen, die Konfiguration von Linux zu vereinheitlichen, tatsächlich unterscheiden sich die einzelnen Distributionen leider nach wie vor erheblich. Aus diesem Grund sollten Sie zur weiteren Konfiguration nach Möglichkeit die jeweils mitgelieferten Werkzeuge einsetzen.

Die Lösung mancher Konfigurationsprobleme erfordert freilich mehr als ein paar Mausklicks. Deswegen gehe ich in diesem Buch losgelöst von speziellen Distributionen ausführlich auf Grundlagen und Hintergründe verschiedener Soft- und Hardware-Komponenten ein.

Thema	Seite	Thema	Seite
Gnome	Abschnitt 5	X (Grafiksystem)	Abschnitt 24
KDE	Abschnitt 6	Systemstart	Abschnitt 26
E-Mail	Abschnitt 8	Kernel, Module	Abschnitt 28
Scanner, Digitalkamera	Abschnitt 9	Netzwerkkonfiguration	Abschnitt 29
Basiskonfiguration	Abschnitt 21	Server-Konfiguration	Abschnitt 30
Paketverwaltung	Abschnitt 22	Drucker	Abschnitt 33

Tabelle 2.7 Linux-Konfiguration

2.15 Linux wieder entfernen

Persönlich kann ich mir das zwar kaum vorstellen, aber vielleicht sind Sie von Linux nicht so begeistert wie ich und möchten es wieder entfernen. Am einfachsten geht das, indem Sie Windows auf dem Rechner neu installieren und während der Installation die Festplatte neu partitionieren und die gesamte Festplatte für Windows nutzen.

Wenn Sie eine Windows-Neuinstallation vermeiden möchten und einfach nur das auf der Festplatte vorhandene Windows weiternutzen möchten, müssen Sie sich um zwei Dinge kümmern:

- Löschen Sie alle Linux-Partitionen, damit Sie den Platz später wieder unter Windows nutzen können.

- Stellen Sie sicher, dass Windows beim Einschalten des Rechners automatisch gestartet wird. Die genaue Vorgehensweise hängt davon ab, ob Ihr Rechner durch ein herkömmliches BIOS oder durch ein EFI gesteuert wird.

Linux-Partitionen löschen

Es ist empfehlenswert, Partitionen eines bestimmten Betriebssystems möglichst nur mit den Werkzeugen dieses Betriebssystems zu ändern. Insofern sollten Sie zum Löschen der Linux-Partitionen idealerweise Linux-Werkzeuge einsetzen. Da es unmöglich ist, die Systempartition eines laufenden Linux-Systems direkt zu löschen, setzen Sie zum Löschen der Linux-Partitionen am besten ein Live-System ein.

Zum eigentlichen Löschen der Linux-Distributionen setzen Sie die Kommandos `fdisk` oder `parted` bzw. dessen grafische Variante `gparted` ein. Die Bedienung dieser Programme wird in Abschnitt 25.3 beschrieben.

Original-MBR wiederherstellen (BIOS-Rechner)

Bei einem BIOS-Rechner enthält der Master-Boot-Record (MBR) normalerweise Daten des Bootloaders GRUB. Um GRUB zu deaktivieren, stellen Sie den ursprünglichen Zustand des MBRs wieder her. Die Vorgehensweise variiert je nach Windows-Version:

- Bei Windows 2000/XP starten Sie den Rechner mit der Windows-Installations-CD und aktivieren mit R, K (Windows 2000) bzw. nur mit R (Windows XP) die sogenannte Wiederherstellungskonsole. Dort können Sie aus einer Liste Ihre Windows-Installation auswählen. Nach der Eingabe Ihres Administrator-Passworts führen Sie das Kommando `FIXMBR` aus. Anschließend starten Sie den Computer mit `EXIT` neu.
- Bei neueren Windows-Versionen starten Sie den Rechner mit der Installations-DVD. Nach der Sprach- und Tastatureinstellung klicken Sie auf den Eintrag Computerreparaturoptionen und wählen dann Ihre Windows-Version aus. Im Dialog Systemwiederherstellungsoptionen wählen Sie den Punkt Eingabeaufforderung und gelangen so in ein Konsolenfenster. Dort führen Sie das folgende Kommando aus:

  ```
  > BOOTREC /fixmbr
  Der Vorgang wurde abgeschlossen.
  ```

  Anschließend starten Sie den Rechner neu. Weitere Informationen zu `BOOTREC` finden Sie hier:

  http://support.microsoft.com/kb/927392/en-us

Windows zuerst booten (EFI-Rechner)

Bei EFI-Rechnern gibt es für jedes installierte Betriebssystem einen Eintrag in der EFI-internen Liste der Betriebssysteme. Als Defaulteintrag gilt üblicherweise das zuletzt installierte Betriebssystem, also Linux. Um zu erreichen, dass wieder Windows zum EFI-Defaultsystem wird, müssen Sie beim Rechnerstart die EFI-Konfigurationsdialoge starten. Dazu müssen Sie eine Tastenkombination drücken, die vom Rechner

bzw. Mainboard abhängig ist. Eine Internetsuche nach *computermodell start efi configuration* führt vermutlich rasch zum Ziel.

In den EFI-Konfigurationsdialogen suchen Sie nach der Liste aller Betriebssysteme. Dort verschieben Sie den Windows-Eintrag an die erste Stelle. Sofern das EFI eine entsprechende Möglichkeit gibt, können Sie die Linux-Einträge ganz löschen.

2.16 Linux in eine virtuelle Umgebung installieren

Virtualisierungsprogramme wie VirtualBox (siehe Abbildung 2.8), VMware Player bzw. VMware Fusion, Virtual PC sowie Parallels Desktop erfreuen sich großer Beliebtheit. Diese Programme emulieren einen kompletten PC. Damit können Sie innerhalb eines Betriebssystems ein zweites installieren und ausführen, also z. B. eine Linux-Installation innerhalb von Windows durchführen – oder umgekehrt! Kapitel 11 führt in die Grundlagen derartiger Virtualisierungssysteme ein und beschreibt detailliert den Einsatz des kostenlosen Programms VirtualBox.

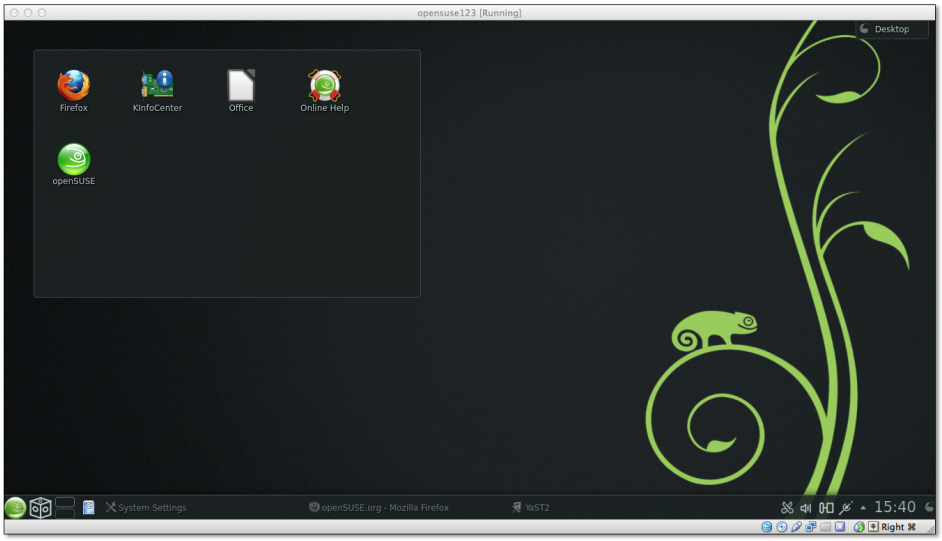


Abbildung 2.8 openSUSE mit VirtualBox unter OS X ausführen

Der größte Vorteil von Virtualisierungssystemen besteht darin, dass die Installation von Linux in eine virtuelle Umgebung einfacher ist als auf einem richtigen Rechner: Sie müssen keine Rücksicht auf das vorhandene System nehmen, die Partitionierung der Festplatte spielt keine Rolle, und es ist ausgeschlossen, dass sich Windows und Linux in die Quere kommen.

Dem stehen freilich auch Nachteile gegenüber: Linux läuft in der virtuellen Umgebung etwas langsamer. Auch die Nutzung diverser Hardware-Komponenten unterliegt Einschränkungen: In den meisten Virtualisierungssystemen können Sie weder DVDs brennen noch 3D-Grafikfunktionen nutzen. Je nach Virtualisierungssystem ist der Datenaustausch zwischen Linux und Windows bzw. OS X relativ umständlich.

Kapitel 3
Installationsanleitungen

Nachdem das vorige Kapitel ausführlich die Grundlagen einer Linux-Installation behandelt hat, folgen in diesem Kapitel konkrete Beispiele. Sie lernen hier einige ausgewählte Linux-Distributionen näher kennen und erfahren, welche Besonderheiten bei deren Installation zu beachten sind:

- CentOS
- Debian
- Fedora
- openSUSE
- Ubuntu und Ubuntu Server

Welche Distribution für welche Anwendung?

Für Linux-Einsteiger am besten geeignet sind momentan Ubuntu und openSUSE. Beide Distributionen sind für den Desktop-Einsatz optimiert und weit verbreitet, d. h., es gibt eine Menge Foren und Wikis, die bei Problemen weiterhelfen. Ubuntu-LTS-Versionen können Sie mit gutem Gewissen auch auf den Rechnern Ihrer Freunde und Verwandten installieren – sie genießen einen drei- bis fünfjährigen Update-Service.

Fedora ist ebenfalls eine Desktop-Distribution; sie richtet sich aber an fortgeschrittene Linux-Anwender. Red Hat betrachtet Fedora als Experimentierplattform. Insofern ist Fedora ideal geeignet, um die neuesten Entwicklungen aus der Linux-Welt kennenzulernen. Die Stabilität bleibt dabei leider oft auf der Strecke.

Für den Server-Einsatz ist ein langer Update-Zeitraum noch wichtiger als für Desktop-Anwendungen. openSUSE, Fedora sowie gewöhnliche Ubuntu-Versionen (ohne LTS) scheiden deswegen von vorneherein aus. Sehr empfehlenswert sind hingegen CentOS, Debian sowie Ubuntu LTS.

Außer den hier präsentierten Distributionen gibt es natürlich noch Hunderte andere. Einige davon werden Sie in speziell dazu passenden Kapiteln kurz kennenlernen – etwa Linux Mint in Kapitel 5, Kubuntu in Kapitel 6 oder Raspbian in Kapitel 12. Aktuelle Nachrichten zu den gerade populärsten Distributionen finden Sie hier:

http://distrowatch.com

3.1 CentOS

RHEL

Bevor ich die Besonderheiten von CentOS erklären kann, muss ich kurz Red Hat Enterprise Linux (kurz RHEL) beschreiben. RHEL ist die kommerziell erfolgreichste Linux-Distribution. Sie kommt beispielsweise in Banken, Versicherungen oder auf Großrechnern zum Einsatz – also immer dann, wenn Stabilität und professioneller Support höchste Priorität genießen. Neben dem Kernprodukt RHEL bietet Red Hat verschiedene RHEL-Erweiterungen und Spezialprodukte an, z. B. den Red Hat Storage Server, die JBoss Enterprise Middleware (Java) und das Red Hat Virtualization System.

Neue Versionen von Red Hat Enterprise Linux (RHEL) basieren grundsätzlich auf der zuletzt erschienenen Fedora-Version. Bei RHEL 6 war das Fedora 13. Es gibt aber natürlich grundlegende Unterschiede zwischen Fedora und RHEL: In die Enterprise-Version werden keine Funktionen eingebaut, die noch nicht vollkommen stabil und ausgereift sind. Der Support-Zeitraum für RHEL ist wesentlich länger und beträgt mindestens 5 Jahre. Und schließlich hilft das *Red Hat Network* (RHN) bei der zentralen Wartung mehrerer RHEL-Installationen.

Im Unterschied zu den anderen in diesem Buch vorgestellten Distributionen ist RHEL nicht frei erhältlich. Installationsmedien und Updates stehen nur zahlenden Kunden zur Verfügung. Aber selbstverständlich muss sich auch Red Hat an die Regeln der GPL halten und den Quellcode seiner Produkte zur Verfügung stellen.

CentOS

CentOS ist der seit vielen Jahren populärste Klon von RHEL. CentOS ist binärkompatibel zu RHEL, im Gegensatz zu diesem aber inklusive aller Updates kostenlos verfügbar. Abstriche müssen Sie aber naturgemäß beim kommerziellen Support machen – den gibt es nicht. Dennoch ist CentOS für Administratoren mit Red-Hat- oder Fedora-Erfahrung eine tolle Möglichkeit, bei Projekten mit kleinem Budget Red-Hat-kompatible Server einzusetzen.

https://www.centos.org

CentOS basiert auf dem originalen Quellcode von Red Hat – RHEL ist ja ein Open-Source-Produkt! CentOS kann den RHEL-Quellcode freilich nicht einfach unverändert übernehmen: »Red Hat« ist ein geschütztes Markenzeichen, deswegen müssen alle Pakete, die Red-Hat-spezifische Zeichenketten, Logos oder Bilder enthalten, modifiziert werden. Einige Red-Hat-spezifische Pakete, z. B. jene zum Zugriff auf das Red Hat Network, werden ganz entfernt. Die modifizierten Pakete müssen kompiliert, getestet und schließlich in Form von neuen Installationsmedien gebündelt werden.

All das kostet eine Menge Zeit und Mühe und erklärt, warum es nach der Freigabe einer neuen RHEL-Version oft Wochen oder Monate dauert, bis auch die entspre-

chende CentOS-Variante zur Verfügung steht. Diese Verzögerungen sind übrigens akribisch in der englischen Wikipedia notiert:

http://en.wikipedia.org/wiki/CentOS

Bei aller Begeisterung für CentOS muss Ihnen klar sein, dass diese Distribution natürlich kein vollwertiger Ersatz für RHEL ist:

- **Support:** Sie erhalten keinen kommerziellen Support. Bei Problemen sind Sie auf Foren, Mailinglisten und Selbsthilfe angewiesen.
- **CPU-Architekturen:** Während es einige RHEL-Versionen auch für ausgefallene CPU-Architekturen und Hardware-Plattformen gibt (IA-64, Alpha, s390, PowerPC, SPARC), konzentriert sich CentOS auf die 32- und 64-Bit-PC-Architektur.
- **Updates:** In der Regel dauert es immer einige Tage, bis von Red Hat freigegebene Sicherheits-Updates auch für CentOS zur Verfügung stehen. In der Vergangenheit betrug die Verzögerung aber mitunter auch mehrere Wochen!
- **Vertrauen:** Hinter CentOS steht ein winziges Team. Auch wenn das Projekt nun schon seit 2004 sehr erfolgreich ist, kann niemand garantieren, dass es CentOS auch in zwei Jahren noch geben wird oder dass es dem Projekt weiter gelingt, CentOS über die schier endlosen Wartungszeiträume zu pflegen: CentOS verspricht, Version 5 bis 2017 und Version 6 bis 2020 mit Sicherheits-Updates zu versorgen!

Scientific Linux

CentOS ist keineswegs der einzige RHEL-Klon. Ebenfalls weit verbreitet sind Scientific Linux und Oracle Linux (siehe unten). Während CentOS für den »gewöhnlichen« Server-Einsatz optimiert ist, hat Scientific Linux eine etwas andere Zielrichtung: Diese Distribution wird von Mitarbeitern der Forschungseinrichtungen Fermilab und CERN zusammengestellt und in unzähligen Universitäten und Forschungseinrichtungen verwendet. Nichtsdestotrotz ist auch Scientific Linux ein weitgehend unverändertes RHEL und ebenso gut für den Server-Alltag geeignet wie CentOS.

Oracle Linux

Auch Oracle ist 2006 in den Markt der RHEL-Klone eingestiegen – aber mit ganz anderen Konzepten: Zum einen ist Oracle Linux ein kommerzielles Angebot, zum anderen versucht Oracle Linux sich mit diversen Zusatzfunktionen von RHEL abzuheben: Dazu zählen ein neuerer Kernel mit diversen Zusatzfunktionen (im Marketing-Jargon: »Unbreakable Enterprise Kernel«), Ksplice-Kernel-Updates im laufenden Betrieb sowie eine bessere Unterstützung des neuen, von Oracle mitentwickelten Dateisystems `btrfs`.

Anfänglich war Oracle Linux wie RHEL ausschließlich für zahlende Kunden zugänglich, wenn auch zu deutlich günstigeren Preisen als bei RHEL. Seit März 2012 kann Oracle Linux inklusive aller Updates kostenlos bezogen werden und steht damit auf

einer Ebene mit CentOS und Scientific Linux. Einzig der kommerzielle Support ist weiterhin kostenpflichtig.

https://blogs.oracle.com/linux/entry/free_updates_and_errata_for

Zugleich hat Oracle damit begonnen, gezielt CentOS-Anwender von den Vorteilen eines Umstiegs auf Oracle Linux zu überzeugen: Mit einem einzigen Shell-Script kann eine vorhandene CentOS-Installation auf Oracle Linux umgestellt werden. Im Wesentlichen werden dabei die Paketquellen geändert und einige Pakete mit Oracle-spezifischen Änderungen ausgetauscht. Die Reaktion der Linux-Gemeinde ist sehr verhalten ausgefallen (fallweise beinahe schon aggressiv negativ), allerdings mag es CentOS-Anwendern durchaus ein Gefühl der Sicherheit geben, dass sie im Notfall in das Oracle-Lager wechseln können. Oracle macht freilich keinerlei Versprechungen, wie lange es kostenlose Updates geben wird.

http://linux.oracle.com/switch/centos
http://lwn.net/Articles/507312

Zielrichtung

Egal ob Original oder Klon – die Zielrichtung von RHEL ist ganz klar der Server-Einsatz bei maximaler Stabilität. Das erklärt auch, warum RHEL & Co. eine veraltete Desktop-Umgebung ausliefern (siehe Abbildung 3.1) und generell ausgereifte Versionen von Apache, Samba etc. vorziehen.

Versionsnummern

RHEL, CentOS und alle anderen Klone verwenden ein Versionsschema, das von denen anderer Distributionen abweicht. Circa alle drei Jahre gibt es eine »große« neue RHEL-Version (Major Release). Momentan ist RHEL 6 aktuell (vorgestellt im November 2010); nach wie vor gewartet wird RHEL 5 (vorgestellt im März 2007). RHEL 7 wird voraussichtlich gegen Ende 2013 erscheinen und in seinen Grundzügen auf Fedora 18 und 19 basieren.

Innerhalb jeder großen RHEL-Version gibt es über einen Zeitraum von sechs Jahren ungefähr zweimal im Jahr ein neues Minor Release (Version 6.1, 6.2, 6.3 etc.). Im Zuge derartiger Updates gibt es auch neue Installationsmedien, die kompatibel zu aktueller Hardware sind. Fundamental neue Funktionen werden dabei nur in Ausnahmefällen eingebaut, und wenn doch, dann meist unter der Bezeichnung »Technical Preview« (im Klartext: ohne offiziellen Support).

Die Besonderheit der Minor Releases besteht darin, dass diese *keine* Neuinstallation erfordern. Wenn Sie also beispielsweise CentOS 6.4 installieren und dann regelmäßig alle Updates durchführen, erhalten Sie nach und nach CentOS 6.5, CentOS 6.6 etc. Erst für den Umstieg auf das nächste Major Release ist eine Neuinstallation erforderlich.

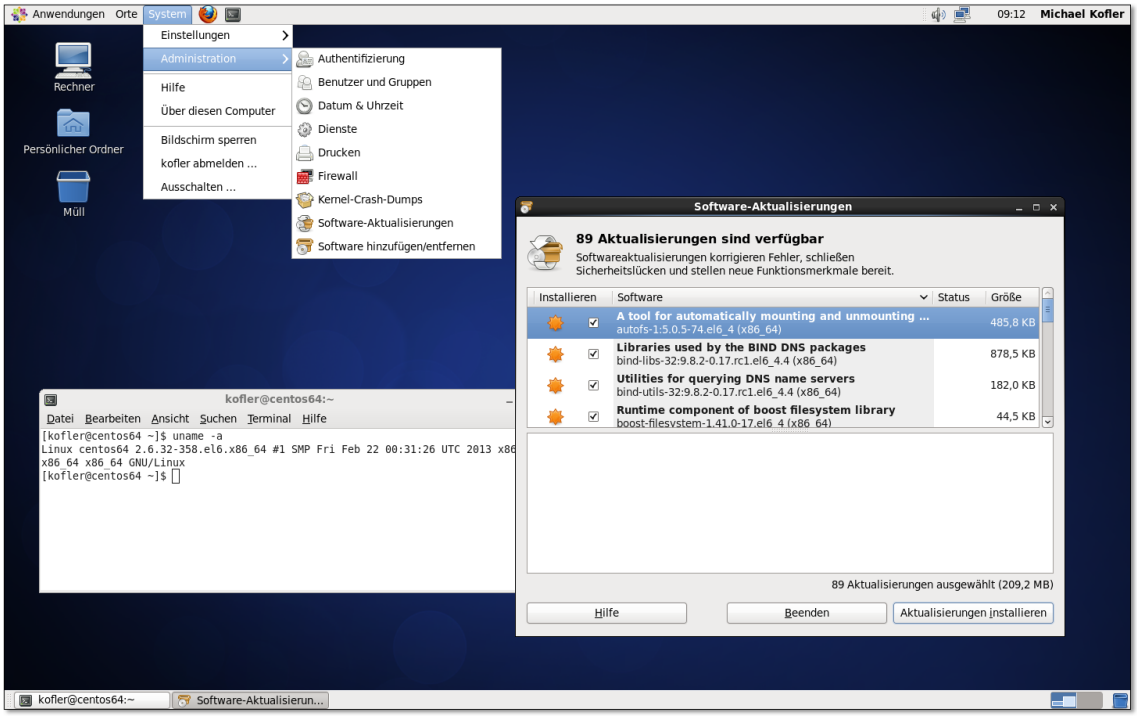


Abbildung 3.1 CentOS 6 mit einem schon etwas antiquiert wirkenden Gnome-Desktop

Update-Zeitraum

Red Hat garantiert ab RHEL 5 einen Wartungszeitraum von zehn Jahren, gerechnet vom Zeitpunkt der Freigabe des Major Release. Danach gibt es für drei weitere Jahre Updates für kritische Sicherheitsprobleme, aber nur noch beschränkten Support. Auf der folgenden Webseite sind die verschiedenen Phasen im Lebenszyklus einer RHEL-Version detailliert aufgeschlüsselt:

https://access.redhat.com/support/policy/updates/errata

Die entsprechenden CentOS-Daten können Sie hier nachlesen:

http://wiki.centos.org/About/Product

CentOS installieren

Installationsmedien

Zur Installation von CentOS müssen Sie die passenden ISO-Images von einem CentOS-Mirror-Server herunterladen, beispielsweise hier:

http://mirror.switch.ch/ftp/mirror/centos/6.4/isos/x86_64

Es stehen mehrere ISO-Images zur Auswahl:

- **DVD 1 und 2:** Für eine gewöhnliche Installation laden Sie nur die erste DVD herunter. Diese reicht für normale Installationen aus.
- **Netinstall:** Wenn Sie über eine schnelle Internetverbindung verfügen, können Sie auch das nur 200 MByte große Netinstall-Image herunterladen und auf eine CD brennen bzw. auf einen USB-Stick übertragen. Während der Installation werden dann alle weiteren Pakete direkt aus dem Internet geladen.
- **Minimal:** Eine weitere Option ist das Minimal-Image. Damit wird wirklich eine Minimal-Installation durchgeführt: CentOS kann danach nur im Textmodus genutzt werden, Sie müssen sich selbst um die Netzwerkkonfiguration kümmern, es sind keinerlei Server-Dienste installiert etc. Das klingt unbequem, eignet sich aber z. B. gut als Startpunkt für eine möglichst ressourcensparende virtuelle Maschine.

Anaconda

CentOS verwendet das grafische Installationsprogramm *Anaconda*. Es ist vielen Linux-Anwendern von Fedora vertraut, wo es bis Version 17 zum Einsatz kam. Anaconda erfordert zumindest 1 GByte RAM. Wenn in einer virtuellen Maschine weniger RAM zur Verfügung steht, müssen Sie die Installation im Textmodus durchführen.

Nachdem Sie das Installations-Image auf eine DVD gebrannt bzw. auf einen USB-Stick übertragen und dann einen Rechnerneustart durchgeführt haben, erscheint ein englischsprachiges Menü mit den folgenden Einträgen:

Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test

Für eine normale Installation im Grafikmodus wählen Sie den ersten Eintrag des Startmenüs mit ↵ aus. Die Variante Install system with basic video driver ist nur zweckmäßig, wenn die Initialisierung des Grafiksystems nicht gelingt. Das Installationsprogramm verwendet dann den VESA-Videotreiber, der eigentlich auf jedem Rechner funktionieren sollte.

Bootoptionen

Wenn das Installationsprogramm Probleme mit der korrekten Erkennung Ihrer Hardware hat, wählen Sie einen Menüeintrag aus und blenden dann mit ⇆ die dazugehörige Kommandozeile ein. Dort können Sie zusätzliche Kerneloptionen angeben. Gleichzeitig sollten Sie die Option `quiet` entfernen, damit Sie während des Bootprozesses die Kernelmeldungen auf dem Bildschirm lesen können. Leider gilt zu diesem Zeitpunkt noch das US-Tastaturlayout, was die Eingabe von Sonderzeichen erschwert.

Medium testen

Unmittelbar nach dem Start können Sie überprüfen, ob die DVD fehlerfrei ist. Dieser Vorgang dauert ziemlich lange – überspringen Sie diesen Schritt einfach mit SKIP. Nur wenn es bei der Installation Probleme gibt, lohnt sich dieser Test, um auf diese Weise zumindest eine Fehlerursache auszuschließen.

Grund-einstellungen

Erst jetzt wechselt das Installationsprogramm Anaconda in den Grafikmodus. Sie wählen nun die gewünschte Sprache und das Tastaturlayout aus. Danach fragt das Installationsprogramm, ob Sie spezielle Speichergeräte verwenden. Damit meint es SAN-Geräte (Storage Area Network) gemäß der Standards FCoE, iSCSI oder zFCP, die üblicherweise nur bei großen Unternehmens-Servern zum Einsatz kommen. In aller Regel ist die Option BASIS-SPEICHERGERÄTE zutreffend. Wenn Anaconda auf Ihren Festplatten eine ältere CentOS-Version erkennt, bietet es anschließend die Möglichkeit, diese Version zu aktualisieren.

Die Netzwerkkonfiguration beschränkt sich in der Regel auf die Angabe des gewünschten Hostnamens. Nur wenn Ihr Rechner nicht mit einem (ADSL- oder WLAN-) Router verbunden ist, können Sie mit dem Button NETZWERK KONFIGURIEREN eine statische Konfiguration durchführen. Nach der Auswahl der Zeitzone, in der der Rechner läuft, müssen Sie den root-Login durch ein Passwort absichern.

Partitionierung

Bei der Partitionierung der Festplatte haben Sie die Wahl zwischen fünf Varianten:

- GESAMTEN PLATZ VERWENDEN: Das Installationsprogramm löscht sämtliche Partitionen auf allen Festplatten und erstellt dann neue Partitionen für CentOS. Vorsicht: Nach einer Rückfrage verlieren Sie sämtliche Daten auf Ihren Festplatten.
- BESTEHENDES LINUX-SYSTEM ERSETZEN: Diese Variante zum obigen Punkt löscht nur vorhandene Linux-Partitionen, rührt aber Windows-Partitionen nicht an.
- AKTUELLES SYSTEM VERKLEINERN: Bei dieser Variante können Sie vorhandene Linux- oder Windows-Partitionen verkleinern. Im frei werdenden Platz werden dann die neuen Partitionen für CentOS angelegt.
- FREIEN PLATZ VERWENDEN: Bei dieser Variante nutzt das Installationsprogramm den freien Platz auf der Festplatte, um darin neue Partitionen anzulegen. Das funktioniert nur, wenn die Festplatte nicht partitionierte Bereiche enthält und darin genug Platz ist, um eine Boot- und eine LVM-Partition anzulegen.
- MASSGESCHNEIDERTES LAYOUT ERSTELLEN: Damit können Sie die Partitionierung selbst vornehmen.

Zusätzlich zu diesen Varianten gibt es noch zwei Optionen: SYSTEM VERSCHLÜSSELN verschlüsselt die Dateisysteme neuer Linux-Partitionen. Für den Server-Einsatz ist das aber selten zweckmäßig, weil dies die Eingabe des Schlüssels bei jedem Bootprozess erfordert. PARTITIONS-LAYOUT NOCHMALS ÜBERPRÜFEN gibt Ihnen die

Möglichkeit, die automatische Partitionierung von Anaconda bei den ersten vier der obigen Varianten zu kontrollieren und gegebenenfalls zu ändern. Bereits gelöschte Partitionen anderer Betriebssysteme lassen sich zu diesem Zeitpunkt aber nicht mehr retten.

Standardmäßig richtet das Installationsprogramm eine 500 MByte große Bootpartition (`ext4`) sowie eine LVM-Partition ein, die den Rest der Festplatte füllt. Die LVM-Partition erhält den Namen `vg_hostname`.

Innerhalb der LVM-Partition werden dann drei Logical Volumes für die Swap-, die Root- und die Home-Partition eingerichtet (`lv_swap` mit der doppelten RAM-Größe, `lv_root` mit maximal 50 GByte und `lv_home`). Die Root- und Home-Partitionen werden ebenfalls mit einem `ext4`-Dateisystem formatiert. Bei kleinen Festplatten, z. B. in virtuellen Maschinen, verzichtet das Installationsprogramm auf eine eigene Home-Partition.

EFI

Sofern Sie zur Installation die 64-Bit-Version von DVD 1 verwenden, kann CentOS auch im EFI-Modus installiert werden. In diesem Fall richtet das Installationsprogramm eine EFI-Partition mit einem VFAT-Dateisystem ein, falls diese noch nicht existiert. Achtung: Alle anderen Installationsmedien sind *nicht* EFI-kompatibel!

Manuelle Partitionierung

Wenn Sie sich für die Variante MASSGESCHNEIDERTES LAYOUT entscheiden, gelangen Sie in den Partitionseditor Disk Druid (siehe Abbildung 3.2). Sie können hier vorhandene Partitionen löschen, ändern (d. h., einen Mount-Point angeben) und neue Partitionen anlegen. Mit RÜCKSETZEN lesen Sie die Partitionstabelle neu ein. Alle durchgeführten Einstellungen gehen damit verloren, und Sie können mit der Partitionierung neu beginnen.

Abbildung 3.2 Festplatte mit dem Disk Druid einrichten

Im Dialog zum Anlegen einer neuen Partition müssen Sie drei Informationen angeben: den Einhängepunkt (d. h. den Punkt, an dem die Partition in das Dateisystem integriert wird, beispielsweise `/` für die Root-Partition), den Typ des Dateisystems (`ext4` oder `swap`) und die gewünschte Größe der Partition. Falls Sie mehrere Festplatten haben, auf denen noch freier Platz ist, müssen Sie angeben, auf welcher Festplatte die neue Partition erstellt werden soll.

Wenn es von einer früheren Linux- oder Windows-Installation schon Partitionen gibt, die Sie nutzen möchten, können Sie mit BEARBEITEN auch zu diesen Partitionen einen Mount-Point angeben.

Boot-Loader

Bei einer BIOS-Installation wird der Boot-Loader GRUB 2 in den MBR (Master Boot Record) der ersten Festplatte installiert. Wenn GRUB stattdessen in die Root-Partition installiert werden soll, klicken Sie im Bootloader-Dialog auf den Button DATENTRÄGER WECHSELN.

Bei einer EFI-Installation kommt hingegen eine EFI-kompatible Variante von GRUB 0.97 zum Einsatz. In diesem Fall werden die GRUB-Dateien in das Verzeichnis `/boot/efi/EFI/redhat` geschrieben.

Installationsumfang

Standardmäßig führt Anaconda lediglich eine Minimalinstallation durch. Sie können dann CentOS nach der Installation nur im Textmodus verwenden. Wenn Sie eine grafische Benutzeroberfläche zur Konfiguration von CentOS wünschen, müssen Sie den Eintrag DESKTOP oder MINIMAL DESKTOP auswählen (siehe Abbildung 3.3).

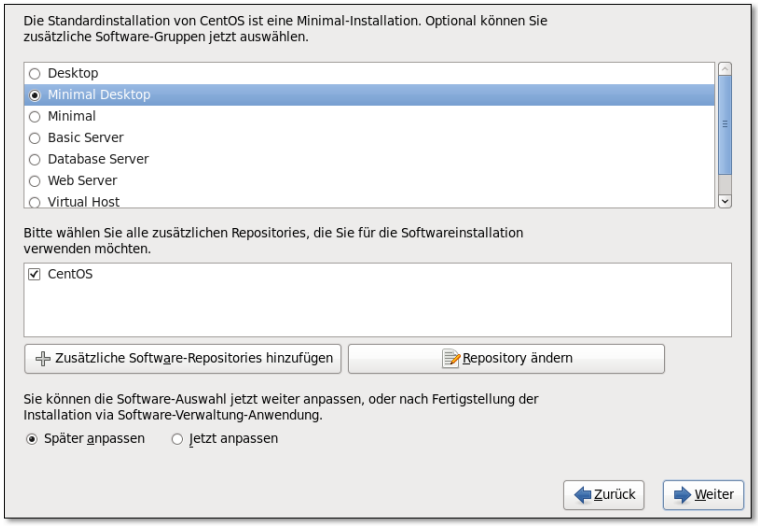


Abbildung 3.3 Paketauswahl

Das offizielle CentOS-Paketarchiv ist bereits vorkonfiguriert. Mit ZUSÄTZLICHE SOFTWARE-REPOSITORIES HINZUFÜGEN können Sie außerdem weitere Paketquellen einrichten – das ist aber ein Schritt, den Sie ebenso gut nach dem Ende der Installation durchführen können.

Nach der Auswahl der Pakete werden diese installiert, was einige Minuten dauert. Ein Protokoll aller installierten Pakete wird in die Datei `/root/install.log` geschrieben.

Abschließende Konfiguration

Anschließend wird der Rechner neu gestartet. Es erscheint automatisch ein Konfigurationsprogramm, in dem Sie die verbleibenden Einstellungen durchführen.

- LIZENZVEREINBARUNG: Ein kurzer Text weist auf die Rechte und Pflichten hin, die sich aus der GPL ergeben.
- ERSTELLE BENUTZER: Hier richten Sie einen Benutzer ein, damit Sie nur in Ausnahmefällen als `root` arbeiten müssen.
- DATUM UND UHRZEIT: In diesem Dialog zeigt das Konfigurationsprogramm die aktuelle Zeit an. Sie können die Zeit hier korrigieren bzw. NTP einrichten. In diesem Fall bezieht CentOS die aktuelle Uhrzeit aus dem Internet.
- KDUMP: Sofern ausreichend RAM zur Verfügung steht, können Sie Kdump aktivieren. Damit werden im Falle eines Absturzes Kernel-Informationen gespeichert.

Wenn Sie diese Einstellungen zu einem späteren Zeitpunkt nochmals durchführen möchten, müssen Sie als `root` unter X die folgenden Kommandos ausführen:

```
root#  rm /etc/sysconfig/firstboot
root#  firstboot
```

Kickstart-Installation

Anstatt die Installation manuell durchzuführen, können Sie diesen Vorgang auch automatisieren. Das ist dann zweckmäßig, wenn Sie Dutzende gleichartige Installationen durchführen müssen. Eine ausführliche Beschreibung dieses Verfahrens finden Sie in den offiziellen Red-Hat-Handbüchern:

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Installation_Guide/ch-kickstart2.html

Erste Schritte

Netzwerk automatisch aktivieren

Bei einer Desktop-Installation wird unverständlicherweise nicht automatisch eine Verbindung zum lokalen Netzwerk hergestellt. Abhilfe: Öffnen Sie das Kontextmenü des NetworkManagers, dessen Icon sich rechts oben in der Menüliste befindet. Mit VERBINDUNGEN BEARBEITEN gelangen Sie in den Konfigurationsdialog. Dort aktivieren Sie für die Verbindung `eth0` die Option AUTOMATISCH VERBINDEN.

Mit System • Software-Aktualisierungen bzw. mit `yum update` installieren Sie alle verfügbaren Updates.

Updates durchführen

Die CentOS-Paketquellen enthalten nur Pakete, die offiziell von Red Hat unterstützt werden. Deshalb ist die Paketauswahl wesentlich kleiner als bei Desktop-Distributionen wie Fedora oder Ubuntu. Abhilfe schafft das Einrichten der Paketquelle EPEL (*Extra Packages for Enterprise Linux*). Das ist eine Sammlung von oft benötigten Zusatzpaketen für RHEL und seine Klone.

EPEL-Paketquelle

http://fedoraproject.org/wiki/EPEL

Das Einrichten der Paketquelle ist umkompliziert: Sie laden von der obigen Webseite das Paket `epel-release-n.n.noarch.rpm` herunter und installieren es – fertig!

3.2 Debian

Keine Distribution steht so sehr für das »reine« Linux wie Debian – und das aus mehreren Gründen:

Debian – das »reine« Linux

- Die Entwicklung von Debian erfolgt ausschließlich durch eine freie Entwicklergemeinde. Hinter Debian stehen weder eine Firma noch kommerzielle Interessen, sondern laut Wikipedia über 1000 Entwickler, von denen die meisten ehrenamtlich für Debian arbeiten. In logischer Konsequenz ist sowohl Debian an sich als auch der Zugang zu Updates vollkommen frei.
- Zu den zentralen Zielen Debians zählt es, dass die Distribution wirklich »frei« im Sinne der Open-Source-Idee bleibt. Die Integration von Binärtreibern oder kommerzieller Software ohne frei verfügbaren Quellcode ist selbstverständlich tabu. Die Debian-Entwickler diskutieren aber auch darüber, ob es vertretbar ist, Firmware-Dateien für Hardware-Geräte mitzuliefern, wenn es dafür keinen Open-Source-Code gibt.
- Bei Debian sind Stabilität und Sicherheit wichtiger als neue Installationen. Deswegen hinkt eine gewöhnliche Debian-Installation dem aktuellen Entwicklungsstand bei nahezu allen wichtigen Komponenten (Kernel, Xorg, Gnome, KDE, Server-Komponenten etc.) immer ein bis zwei Versionsnummern hinterher. Wer aktuellere Versionen benötigt, kann diese aus den *testing*- oder *unstable*-Paketquellen installieren.
- Debian unterstützt wesentlich mehr Hardware-Plattformen als jede andere Distribution. Auch das ist ein Grund dafür, dass die Entwicklung einer neuen Debian-Version oft länger dauert als geplant.

- Die Leitung des Debian-Projekts erfolgt durch eine demokratische Organisation, deren Führungsmitglieder regelmäßig gewählt werden. Die Spielregeln sind in einem »Gesellschaftsvertrag« formuliert:

  http://www.debian.org/social_contract.de.html

  Dieser Gesellschaftsvertrag enthält auch »Richtlinien für Freie Software« (DFSG = *Debian Free Software Guidelines*). Diese Richtlinien formulieren Kriterien, die ein Software-Projekt erfüllen muss, damit es Teil der offiziellen Debian-Pakete werden kann.

Desktop- und Server-Einsatz

Debian hat im weltweiten Linux-Server-Segment laut einer Statistik von W3Techs einen Marktanteil von über 30 Prozent. Dafür gibt es mehrere Gründe: Debian hat sich einen Ruf als sicheres System erarbeitet, es ist kostenlos verfügbar, und es lässt sich dank des Debian-Paketsystems über viele Jahre ohne Neuinstallation immer wieder aktualisieren.

http://w3techs.com/technologies/details/os-debian/all/all

Im Desktop-Segment war Debian nie so stark präsent. Debian hat noch immer den Ruf, dass es schwieriger zu bedienen sei als andere Distributionen. Dieses Vorurteil stimmt schon lange nicht mehr. Fakt ist aber, dass die Installation umständlicher als bei anderen Distributionen ist und dass Sie mit Debian durchwegs ältere Software-Versionen erhalten als beispielsweise mit Ubuntu oder Fedora. Wenn Sie Wert auf neue Gnome-, KDE-, Gimp- oder LibreOffice-Versionen sowie auf aktuelle Hardware-Treiber legen, ist Debian die falsche Wahl.

Die Bedeutung von Debian reicht weit über das hinaus, was sich in Marktanteilen messen lässt: Debian ist ein wichtiges und unverzichtbares Fundament für zahlreiche andere Distributionen, allen voran für das gerade erwähnte Ubuntu. Viele Debian-Werkzeuge, angefangen bei der Paketverwaltung, haben Eingang in zahlreiche andere Distributionen gefunden.

Kritik

Allen Errungenschaften zum Trotz gibt es natürlich auch Kritik an Debian. Heiß umstritten sind insbesondere die oft jahrelangen Release-Zyklen, die durch interne Querelen um bisweilen fast schon philosophische Details regelmäßig noch größer werden als ursprünglich geplant. Ubuntu hat bewiesen, dass es auf der Basis der Debian-Pakete möglich ist, halbjährlich aktuelle Versionen zu veröffentlichen. Und gerade der große Erfolg von Ubuntu irritiert manche Debian-Entwickler, weil es den Anschein hat, als würde Ubuntu dank einer besseren Vermarktung gewissermaßen die Ernte Debians einfahren.

Versionen/ Varianten

Im Vergleich zu anderen Distributionen verzichtet Debian dankenswerterweise auf unzählige Distributionsvarianten. Es gibt nur ein Debian, das aus einem Pool von rund 35.000 Paketen besteht. Die genaue Anzahl variiert je nach CPU-Architektur. Je

nachdem, welches Installationsmedium Sie einsetzen, müssen Sie bei Bedarf mehr oder weniger Pakete aus dem Internet herunterladen.

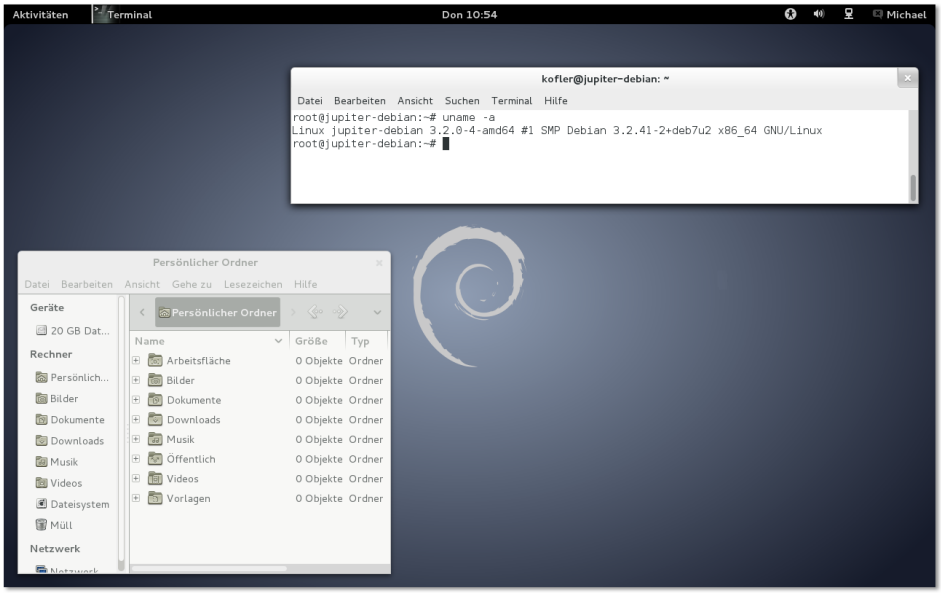


Abbildung 3.4 Debian verwendet standardmäßig Gnome als Desktop-System.

Die Installation des Grundsystems kann wahlweise von einer oder mehreren DVDs oder von einer Netzwerkinstallations-CD (`netinst`-Image, rund 170 MByte) erfolgen. Diese CD enthält nur das Installationsprogramm. Alle Pakete werden während der Installation aus dem Internet oder von einem lokalen Server heruntergeladen. Bei einer einmaligen Installation minimiert das `netinst`-Image den Ressourcen-Bedarf: Sie müssen nur eine CD brennen und nur die Pakete herunterladen, die Sie tatsächlich brauchen.

Beeindruckend ist die Hardware-Unterstützung: Während andere Distributionen zumeist nur zwei oder drei CPU-Plattformen unterstützen, sind es bei Debian 7 elf: Armel, Armhf, IA-64, Mips, Mipsel, PowerPC, S/390, S390x, SPARC, x86 und x86_64. Außerdem gibt es Debian-Varianten für x86-Systeme, die den BSD-Kernel anstelle von Linux verwenden. Für die x86-Linux-Varianten gibt es nicht nur Installations-, sondern auch Live-CDs.

Codenamen

Debian verwendet für jede Version einen Codenamen, der mit Figuren aus dem Film Toy Story übereinstimmt:

Squeeze = Debian 6
Wheezy = Debian 7
Jessie = Debian 8

Weitere Infos

Umfassende Informationen zu Debian finden Sie auf dessen Website:

http://www.debian.org

Werfen Sie auch einen Blick in das *Debian GNU/Linux Anwenderhandbuch* von Frank Ronneburg, das vollständig online verfügbar ist:

http://www.debiananwenderhandbuch.de

Debian installieren

Installationsmedien

ISO-Dateien zum Brennen einer CD/DVD bzw. zur Übertragung auf einen USB-Stick finden Sie hier zum kostenlosen Download:

http://www.debian.org/CD/http-ftp

Empfehlenswert ist in der Regel das DVD-Image für die Plattform amd64; es ist selbstverständlich auch für alle 64-Bit-Prozessoren von Intel geeignet!

Installation starten

Wie üblich beginnen Sie die Installation, indem Sie Ihren Rechner neu starten und die Debian-CD oder -DVD einlegen bzw. einen USB-Stick anstecken. Auf der Willkommensseite geben Sie an, welche Installationsvariante Sie nutzen möchten:

INSTALL	Standardinstallation im Textmodus
GRAPHICAL INSTALL	Standardinstallation im Grafikmodus
ADVANCED OPTIONS	Installation für Experten, KDE-Installation, Rescue-System
HELP	Hilfetexte (Drücken Sie F2 bis F10.)

Standardmäßig startet das Installationsprogramm im Textmodus. Diese Installationsform ist nahezu identisch mit der von Ubuntu-Server-CDs (siehe Abschnitt 3.6). Das ist kein Zufall – Ubuntu hat das Installationsprogramm mit wenigen Änderungen von Debian übernommen.

Mit GRAPHICAL INSTALL führen Sie die Installation im Grafikmodus aus. Diese Installationsvariante bietet zwar keine zusätzlichen Funktionen, sieht aber wesentlich ansprechender aus.

Wenn Sie Hardware-Probleme haben, führen Sie ADVANCED OPTIONS • EXPERT INSTALL aus. Sie können nun ganz genau Einfluss auf die einzelnen Installationsschritte und insbesondere auf das Laden von Kernelmodulen nehmen. Das setzt natürlich einiges Linux-Know-how voraus.

Gnome, KDE, Xfce oder LXDE?

Normalerweise wird Debian mit dem Gnome-Desktop installiert. Wenn Sie ein anderes Desktop-System wünschen, führen Sie ADVANCED OPTIONS • DESKTOP ENVIRONMENT MENU aus. Zur Wahl stehen KDE, LXDE und Xfce.

Im Folgenden gehe ich davon aus, dass Sie sich für eine Standardinstallation im Grafikmodus entschieden haben. Die ersten Schritte betreffen die Einstellung der Sprache und des Tastaturlayouts.

Fehlende Firmware-Dateien

Im Gegensatz zu den meisten anderen Linux-Distributionen enthält das Installations-Image keine Firmware-Dateien, deren Code nicht quelloffen zur Verfügung steht. Wenn das Installationsprogramm erkennt, dass eine für die Installation erforderliche Hardware-Komponente aufgrund fehlender Firmware nicht funktioniert, zeigt es eine entsprechende Warnung an (siehe Abbildung 3.5).

Abbildung 3.5 Eine Firmware-Datei fehlt und muss nachgeliefert werden.

In solchen Fällen müssen Sie sich auf die Suche nach den Firmware-Dateien machen. Die gängigsten Firmware-Dateien befinden sich in der Datei `firmware.zip` auf der folgenden Seite:

http://cdimage.debian.org/cdimage/unofficial/non-free/firmware

Die zu Ihrer Debian-Version passende Firmware-Datei finden Sie im Unterverzeichnis `codename/current`, für Debian 7 also in `wheezy/current`. Den Inhalt der Datei packen Sie aus und schreiben ihn auf eine CD oder auf einen USB-Stick. Die Treiberdateien

müssen sich auf diesem Datenträger im Unterverzeichnis `firmware` befinden. Der USB-Stick darf ein VFAT-Dateisystem enthalten. Der Platzbedarf für die Dateien beträgt nur einige MByte. Es ist nicht notwendig, den USB-Stick vorher zu formatieren. Nachdem Sie den USB-Stick angesteckt haben, können Sie fortsetzen. Das Installationsprogramm sucht sich selbst die Firmware-Datei vom Datenträger.

Netzwerkkonfiguration

Falls Ihr Rechner über mehrere Netzwerkschnittstellen verfügt, müssen Sie die richtige auswählen. Sofern Ihr Rechner an einen lokalen Server oder einen ADSL-Router mit DHCP-Server angeschlossen ist, erfolgt die weitere Netzwerkkonfiguration automatisch; Sie müssen nur den gewünschten Rechnernamen (Hostnamen) angeben.

root-Passwort, Benutzer

In den nächsten Dialogen geben Sie das Passwort für `root` ein und legen einen neuen Benutzer an.

Partitionierung der Festplatte

Das Installationsprogramm stellt Ihnen unter anderem die folgenden Möglichkeiten zur Partitionierung der Festplatte zur Wahl:

- Geführt – vollständige Festplatte verwenden: Das Installationsprogramm löscht alle Partitionen und verwendet dann die gesamte Festplatte für die Debian-Installation. In einem weiteren Dialog erscheint wenig später die Frage, ob Sie alle Daten in einer Partition speichern möchten, ob Sie eine getrennte Home-Partition wünschen (das ist empfehlenswert) oder ob auch für die Verzeichnisse `/usr`, `/var` und `/tmp` eigene Partitionen eingerichtet werden sollen; Letzteres ist selten zweckmäßig.
- Geführt – gesamte Platte verwenden und LVM einrichten: Wie oben, allerdings mit einem LVM-System, das bei späteren Änderungen mehr Flexibilität gibt.
- Geführt – gesamte Platte mit verschlüsseltem LVM: Wie oben, allerdings wird das LVM-System verschlüsselt. Der Schlüssel muss bei jedem Bootvorgang angegeben werden, d. h., diese Variante ist für Server-Installationen ungeeignet.
- Manuell: Dieser Punkt gibt Ihnen die Möglichkeit, die Partitionierung selbst durchzuführen. Sie können aber auch eine der obigen Varianten wählen und den Vorschlag des Installationsprogramms nach Ihren eigenen Vorstellungen ändern.

Falls die Festplatte bereits andere Betriebssysteme enthält, gibt es zusätzlich zum Eintrag gesamte Festplatte verwenden auch die Option den grössten freien Speicherbereich verwenden. Unabhängig davon, für welche Variante Sie sich entscheiden, müssen Sie den Partitionierungsplan nochmals explizit bestätigen. Es besteht also keine Gefahr, dass das Installationsprogramm die Partitionierung vorschnell und unwiderruflich vornimmt.

Bei der manuellen Partitionierung zeigt das Installationsprogramm eine Liste aller verfügbaren Partitionen an. Vorhandene Partitionen wählen Sie per Doppelklick aus. Neue Partitionen erstellen Sie, indem Sie den Punkt FREIER SPEICHER am Ende der Liste anklicken. Sie können auch vorhandene Windows- und Linux-Partitionen verkleinern, um so Platz für neue Linux-Partitionen zu schaffen.

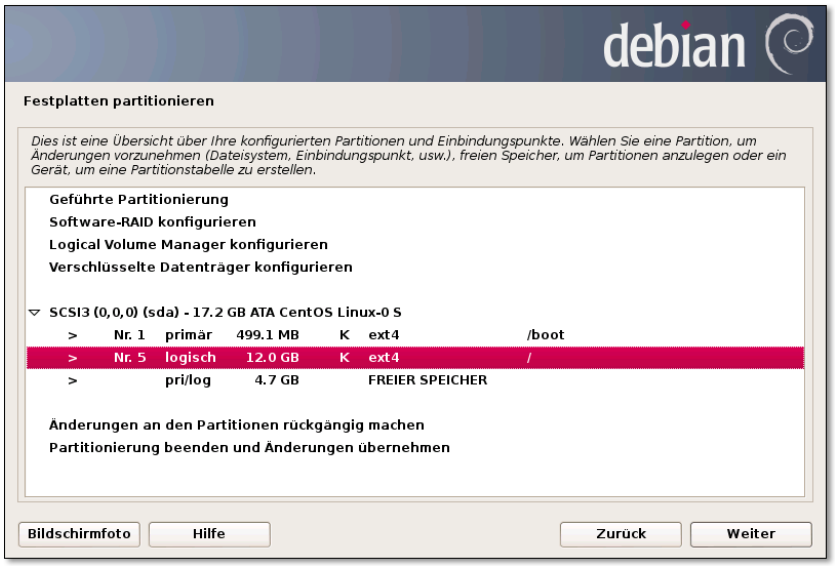


Abbildung 3.6 Partitionierung der Festplatte

Die verschachtelten Dialoge zur Bearbeitung der Partitionen sind leider unübersichtlich und machen von den Möglichkeiten einer grafischen Benutzeroberfläche wenig Gebrauch. Viele Texte in den Dialogen sind als Menükommandos zu interpretieren; sie führen beim Anklicken in weitere Dialoge. Beispielsweise öffnet ein Mausklick auf die Zeile BENUTZEN ALS: NICHT BENUTZEN eine Auswahlliste, in der Sie den gewünschten Dateisystemtyp angeben.

Mit ANLEGEN DER PARTITION BEENDEN speichern Sie die Einstellungen der zuletzt bearbeiteten Partition. Anschließend können Sie eine weitere Partition bearbeiten oder die PARTITIONIERUNG BEENDEN und alle durchgeführten ÄNDERUNGEN ÜBERNEHMEN. Das Installationsprogramm zeigt eine Zusammenfassung der geplanten Änderungen an der Festplattenpartitionierung an und führt diese nach einer weiteren Bestätigung schließlich aus.

Falls die Festplatte bisher unbenutzt war, muss vor der Partitionierung eine Partitionstabelle eingerichtet werden. Auf EFI-Rechnern entscheidet sich Debian für das GPT-Format, zeigt diesbezüglich aber keine Informationen an und bietet auch keine Wahlmöglichkeiten.

Paketmanager konfigurieren

Falls Sie mehrere Installations-CDs/DVDs gebrannt haben, können Sie diese nun einlesen. Im Regelfall werden Sie nur eine CD/DVD verwenden und die restlichen Pakete bei Bedarf aus dem Internet herunterladen; in diesem Fall beantworten Sie die entsprechende Frage mit NEIN.

Im nächsten Dialog fragt das Installationsprogramm, welchen »Netzwerkspiegel« es verwenden soll. Im Klartext heißt das: Sollen Pakete, die sich nicht auf den vorhandenen CDs/DVDs befinden, aus dem Internet von einem Mirror-Server heruntergeladen werden? Insbesondere bei einer Netzwerkinstallation (»netinst«-CD) ist dieser Punkt essenziell. Antworten Sie mit JA und wählen Sie im nächsten Schritt einen geografisch nahe gelegenen Server aus.

Nach der Installation einiger Pakete werden Sie gefragt, ob Ihre Paketauswahl an einen zentralen Server gemeldet werden soll, um so die populärsten Debian-Pakete zu ermitteln.

Im nächsten Dialog führen Sie eine erste Software-Auswahl durch: Dabei stehen die Paketgruppen DEBIAN DESKTOP ENVIRONMENT, WEB SERVER, PRINT SERVER, DNS SERVER, FILE SERVER, MAIL SERVER, SQL DATABASE, LAPTOP und STANDARD-SYSTEMWERKZEUGE zur Wahl.

Achten Sie darauf, dass der Punkt DEBIAN DESKTOP ENVIRONMENT aktiviert ist! Sie haben an dieser Stelle leider keinen Einfluss darauf, welche Desktop-Umgebung installiert wird (Gnome), welche SQL-Datenbank etc. Auch sonst müssen Sie mit der Installation weiterer Pakete warten, bis das Grundsystem läuft.

GRUB-Installation und EFI

Debian verwendet GRUB 2 als Bootloader. Das Installationsprogramm trägt in das GRUB-Menü automatisch alle anderen Betriebssysteme ein, die bereits installiert sind. Nach der GRUB-Installation wird der Rechner neu gestartet.

Die amd64-Version von Debian erlaubt seit Version 7 die Installationen im EFI-Modus. Dabei wird der Bootloader GRUB in die EFI-Partition installiert. Die automatische Partitionierung denkt auch an die EFI-Partition, falls diese noch nicht existiert. UEFI Secure Boot wird allerdings nicht unterstützt.

Screenshots

Während der Installation können Sie das aktuelle Aussehen des Installationsprogramms dank eines dafür vorgesehenen Buttons in Screenshots dokumentieren. Die Screenshots werden im Verzeichnis `/var/log` gespeichert, gehen aber beim Neustart des Rechners am Ende der Installation verloren. Um die Bilder zu archivieren, wechseln Sie vor dem Neustart in eine Textkonsole und kopieren die Dateien nach `/target/root` oder in ein anderes Verzeichnis Ihrer Wahl.

Erste Schritte

CD/DVD als Paketquelle deaktivieren

Standardmäßig greift Debian jedes Mal auf die Installations-CD/DVD zurück, wenn Sie ein neues Paket installieren möchten. Wenn es Ihnen lieber ist, dass Debian die Pakete aus dem Internet bezieht, öffnen Sie die Datei `/etc/apt/sources.list` mit einem Editor und stellen der Zeile `deb cdrom:xxx` das Kommentarzeichen # voran.

MP3 und Multimedia

Überraschenderweise kann Debian bereits nach einer Grundinstallation MP3-Dateien und die gängigsten Audio- und Video-Formate abspielen. Da Debian keinen kommerziellen Hintergrund hat, befürchten die Entwickler offensichtlich keine Patentprobleme.

Der MP3-Encoder `lame` steht dagegen nur in der Paketquelle *http://deb-multimedia.org* zur Verfügung. Wenn Sie diese Paketquelle nicht verwenden möchten, müssen Sie auf die offiziellen Pakete `toolame` und `twolame` ausweichen. Damit erzeugen Sie allerdings nur Dateien im Format MPEG-1 Layer 2 (statt Layer 3), also MP2 statt MP3. In der Praxis ergeben sich daraus nur selten Einschränkungen, weil die meisten MP3-Player auch mit MP2-Dateien zurechtkommen.

Inoffizielle Pakete mit weiteren Codecs, Multimedia-Bibliotheken und -Programmen finden Sie in von Debian unabhängigen Paketquellen, beispielsweise hier:

http://www.deb-multimedia.org

Proprietäre Grafiktreiber

Die binären Treiber für AMD/ATI- und NVIDIA-Grafikkarten stehen als *non-free*-Pakete zur Verfügung. Vor der Installation müssen Sie in `/etc/apt/sources.list` die Paketquellen *contrib* und *non-free* hinzufügen.

```
# in /etc/apt/sources.list
deb  http://http.debian.net/debian/ wheezy main contrib non-free
...
```

Zur Installation führen Sie die folgenden Kommandos aus. Dabei müssen Sie gegebenenfalls `amd64` durch Ihre Hardware-Architektur ersetzen.

```
root#  apt-get update
root#  apt-get install linux-headers-amd64
root#  apt-get fglrx-driver fglrx-control          (für AMD/ATI)
root#  apt-get nvidia-kernel-dkms nvidia-xconfig   (für NVIDIA)
```

Nun müssen Sie noch die Konfigurationsdatei `xorg.conf` anpassen. Die Konfiguration wird erst nach einem Neustart wirksam.

```
root#  aticonfig --inital                         (für AMD/ATI)
root#  nvidia-xconfig                             (für NVIDIA)
root#  reboot
```

Weitere Tipps zur ATI- und NVIDIA-Treiberinstallation finden Sie auf den beiden folgenden Websites. Dort wird auch die Installation älterer Versionen der beiden Treiber behandelt.

http://wiki.debian.org/ATIProprietary
http://wiki.debian.org/NvidiaGraphicsDrivers

3.3 Fedora

Fedora ist eine Variante von Red Hat Enterprise Linux (RHEL). Die Fedora-Entwicklung wird von Red Hat personell und finanziell unterstützt. Im Gegensatz zu RHEL sind sowohl Fedora an sich als auch alle Updates kostenlos verfügbar. Für Red Hat ist Fedora eine Art Testplattform, um neue Funktionen zu entwickeln und zu testen. Für viele Linux-Freaks ist Fedora hingegen die modernste verfügbare Linux-Distribution. Neue Linux-Konzepte und -Ideen finden sich oft zuerst in Fedora, bevor andere Distributionen nachziehen. Fedora ist üblicherweise auch die Linux-Distribution, mit der Sie die gerade aktuellste Gnome-Version zuerst ausprobieren können (siehe Abbildung 3.7).

Trotz der Experimentierfreudigkeit der Entwickler hat sich Fedora in den letzten Jahren als relativ stabile Distribution herausgestellt. Hier kommt ganz offensichtlich das Know-how der Red-Hat-Entwickler zum Tragen. Bei der Benutzerfreundlichkeit hat Fedora in den letzten Jahren große Fortschritte gemacht: Hatte Fedora früher den Nimbus »von Freaks für Freaks«, so ist die Distribution mittlerweile ebenso einfach zu installieren und zu nutzen wie Ubuntu.

Der größte Nachteil von Fedora ist die kurze Lebensdauer: Fedora-Updates werden für den Zyklus von zwei Versionen plus einem Monat gepflegt. Mit anderen Worten: Der Update-Zeitraum für Fedora 18 endet einen Monat, nachdem Fedora 20 fertiggestellt ist. Da ein Release-Zyklus von etwa sechs Monaten angepeilt wird, entspricht dies einer Update-Spanne von ca. 13 Monaten.

Varianten

Fedora steht in zwei Versionen für 32- und für 64-Bit-Prozessoren zur Auswahl. Außerdem gibt es noch sogenannte *Spins*. Das sind Fedora-Varianten mit einer vordefinierten Paketauswahl für einen bestimmten Verwendungszweck, z. B. mit Werkzeugen zur Sicherheitsanalyse oder mit dem Desktop LXDE.

http://spins.fedoraproject.org

Dokumentation

Weitere Informationen zu Fedora finden Sie auf den folgenden Webseiten:

http://fedoraproject.org
http://www.fedorawiki.de

http://www.fedoraforum.de
http://www.fedoraforum.org

Zu Fedora gibt es außer diversen Wikis nur wenig offizielle Dokumentation. Da Fedora aber viele Ähnlichkeiten zu RHEL aufweist, helfen die RHEL-Handbücher oft weiter:

http://docs.fedoraproject.org
http://www.redhat.com/docs/manuals/enterprise

Abbildung 3.7 Fedora-Desktop (Gnome)

Fedora installieren

Installationsmedien

Üblicherweise laden Sie als Installationsmedium das DVD-ISO-Image von der folgenden Website herunter. Diese Datei kann auch auf einen ausreichend großen USB-Stick übertragen werden.

http://fedoraproject.org/de/get-fedora-options#formats

Als Alternativen zu den recht großen DVD-Dateien (ca. 4 GByte) stehen auch Live-Images zur Auswahl. Offiziell unterstützt werden KDE und Gnome, außerdem gibt es Images für diverse Spins. Auch mit den Live-Systemen kann eine Installation durchgeführt werden. Diese Installationsform ist besonders einfach, bietet aber weniger Konfigurationsmöglichkeiten als eine herkömmliche Installation vom DVD-Image.

Zu guter Letzt können Sie auch das Netzwerk-Installationsmedium verwenden. Es hat mit rund 300 MByte den geringsten Download-Umfang und lässt sich auch auf eine CD brennen. Das Image enthält nur das eigentliche Installationsprogramm. Die eigentlichen Pakete werden während der Installation aus dem Internet heruntergeladen.

Startmenü

Wenn Sie das DVD-Image zur Installation verwenden, enthält das Startmenü drei Einträge:

INSTALL FEDORA
TEST THIS MEDIA AND INSTALL FEDORA
TROUBLESHOOTING

Die beiden ersten Einträge sind selbsterklärend, wobei ein Test des Installationsmediums nur sinnvoll ist, wenn damit zuvor Probleme aufgetreten sind. TROUBLESHOOTING führt in ein weiteres Menü:

INTALL FEDORA IN BASIC GRAPHICS MODE
RESCUE A FEDORA SYSTEM
RUN A MEMORY TEST
BOOT FROM LOCAL DRIVE

Grafisches Installationsprogramm

Beginnend mit Version 18 kommt ein vollkommen neu konzipiertes Installationsprogramm zum Einsatz. Nach der Einstellung der Sprache werden alle Konfigurationseinstellungen in einem einzigen Dialog zusammengefasst (siehe Abbildung 3.8). Normalerweise müssen Sie dann nur einen einzigen Punkt ändern, nämlich das INSTALLATIONSZIEL.

Partitionierung

Ein Klick auf das Icon INSTALLATIONSZIEL führt in einen Partitionseditor, der leider im Hinblick auf intuitive Bedienung keine Meisterleistung darstellt. Im ersten Dialog werden die gefundenen lokalen Festplatten und SSDs aufgelistet. Sie müssen nun die Festplatten mit einem Auswahlhäkchen versehen, auf denen Partitionen erstellt oder genutzt werden sollen. Der Button FERTIG schließt die Partitionierung keineswegs ab, sondern führt in den nächsten Dialog (siehe Abbildung 3.9). Dort können Sie zwischen drei grundsätzlichen Partitionierungsschemata auswählen:

- LVM: Das Installationsprogramm verwendet den Linux Volume Manager. Im Gegensatz zu anderen Distributionen müssen Sie sich nicht um die Details kümmern: Sie geben nur an, welche Logical Volumes Sie nutzen möchten. Das Installationsprogramm kümmert sich selbst darum, die entsprechenden Partitionen, Physical Volumes, Volume Groups und Logical Volumes einzurichten.
- STANDARD-PARTITIONEN: Das Installationsprogramm verwendet gewöhnliche Partitionen.
- BTRFS: Das Installationsprogramm verwendet gewöhnliche Partitionen, in denen btrfs-Dateisysteme eingerichtet werden. Das btrfs-Dateisystem ist allerdings noch nicht stabil, weswegen diese Option nur von Linux-Profis genutzt werden sollte, die wissen, worauf sie sich einlassen.

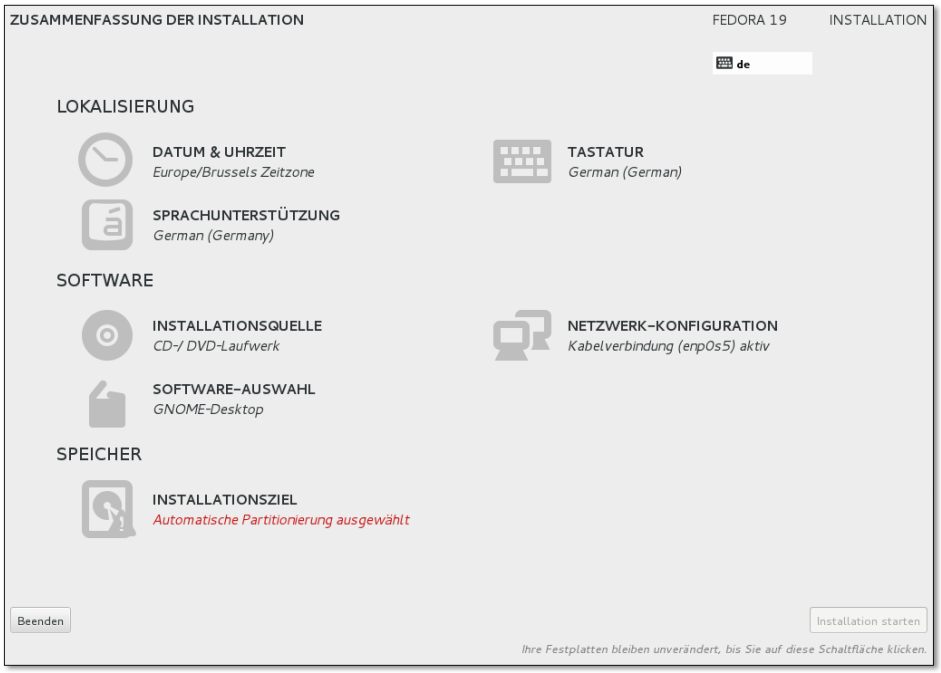


Abbildung 3.8 Überblick über die Installationseinstellungen

Losgelöst von diesen drei Varianten können Sie durch Optionen festlegen, ob Sie den Partitionierungsvorschlag überprüfen möchten und ob Ihre Daten verschlüsselt werden sollen. Falls sich auf der Festplatte bereits Partitionen befinden, werden im Dialog zwei weitere Buttons angezeigt: Mit SPEICHERPLATZ FESTLEGEN können Sie vorhandene Partitionen löschen oder verkleinern. ANGEPASSTE PARTITIONIERUNG führt in einen Editor zur manuellen Partitionierung.

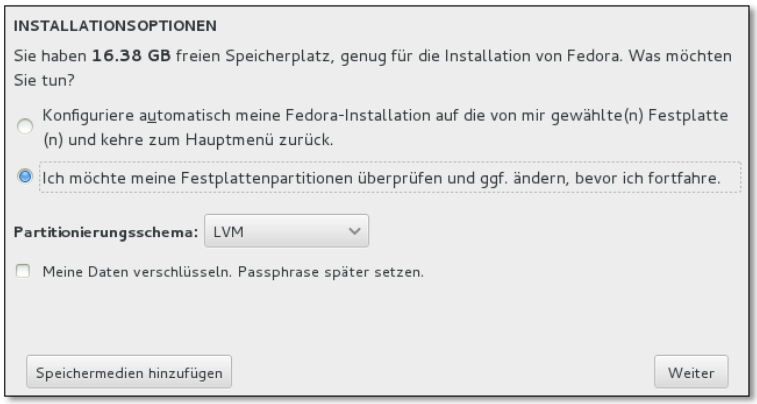


Abbildung 3.9 Auswahl des Partitionierungsverfahrens

Manuelle Partitionierung

Gänzlich ungewohnt verläuft hingegen die manuelle Partitionierung (siehe Abbildung 3.10): In der Leiste links werden alle auf den Festplatten vorhandenen und neu einzurichtenden Partitionen bzw. Dateisysteme aufgelistet. Die Partitionen sind gruppiert; die erste Gruppe beschreibt das neue Fedora-System, die weiteren Gruppen die auf den Festplatten erkannten, schon vorhandenen Windows- und Linux-Installationen. Dabei kann es durchaus vorkommen, dass ein- und dieselbe Partition in mehreren Gruppen angezeigt wird – z. B. eine Swap-Partition, die parallel von mehreren Linux-Distributionen genutzt wird.

Um neue Partitionen einzurichten, klicken Sie auf den Plus-Button und geben vorerst nur zwei Parameter an: das Mount-Verzeichnis bzw. die Bezeichnung SWAP sowie die gewünschte Größe in MB oder GB. Erst im zweiten Schritt wählen Sie den Datensystemtyp (in der Regel `ext4`) und geben an, ob das Dateisystem in einer gewöhnlichen Partition oder in einem Logical Volume eingerichtet werden soll.

Wenn Sie alle Partitionen wunschgemäß eingerichtet haben, schließen Sie den Vorgang mit dem Button FERTIG ab. Das Installationsprogramm zeigt nun eine Zusammenfassung der anstehenden Aktionen an, also z. B. welche Partitionen gelöscht oder neu erstellt werden. Mit der Bestätigung dieser Daten gelangen Sie zurück in den Zusammenfassungsdialog.

Software-Auswahl

Wesentlich übersichtlicher als die Dialoge zur manuellen Partitionierung ist die Einstellung der Software-Auswahl gelungen (siehe Abbildung 3.11). Dort können Sie in der linken Optionsliste zwischen sechs verschiedenen Desktop-Umgebungen (Gnome, KDE, Xfce, LXDE, Cinnamon und MATE), zwei Server-Konfigurationen (Web oder Infrastruktur, gemeint ist mit zweiterem ein LAN-Server) sowie einer Minimalinstallation wählen. Rechts können Sie das gewählte System um dazu passende Erweiterungen ergänzen.

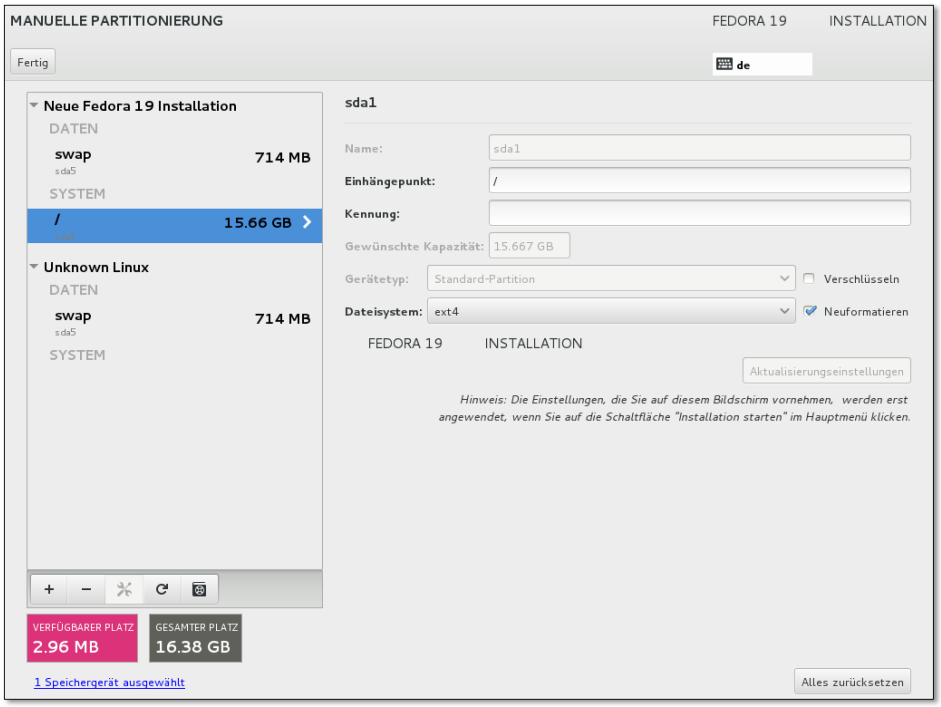


Abbildung 3.10 Manuelle Partitionierung

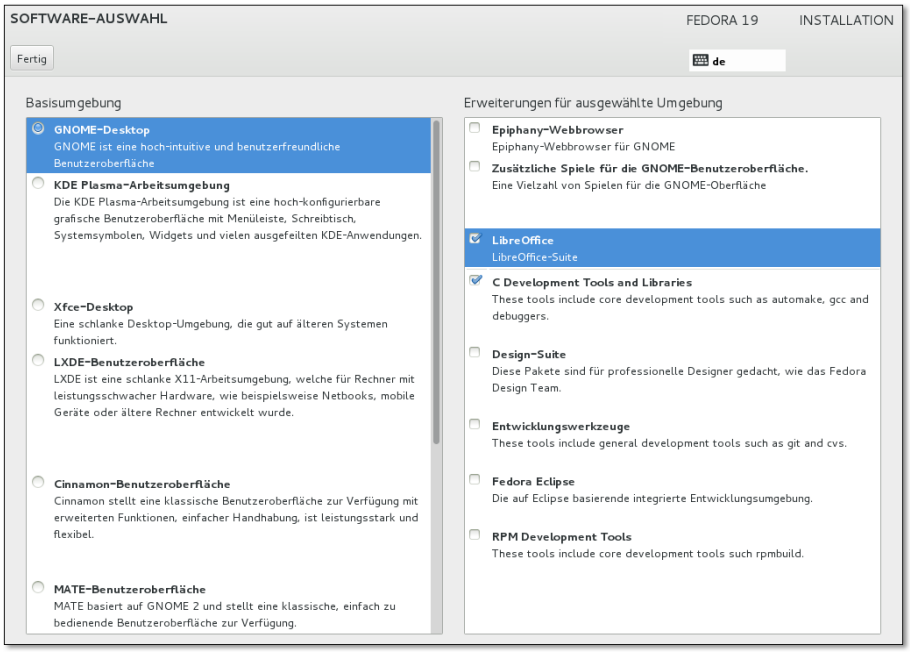


Abbildung 3.11 Auswahl des Desktop-Systems sowie wichtiger Erweiterungen

Root-Passwort, Benutzer einrichten

Sobald Sie den Zusammenfassungsdialog mit INSTALLATION STARTEN abschließen, beginnt die eigentliche Installation. Die Wartezeit bis zum Abschluss der Installation können Sie nutzen, um das Passwort für `root` einzustellen sowie um einen gewöhnlichen Benutzer einzurichten. Falls Sie dabei ein Passwort verwenden, das dem Installationsprogramm als zu einfach erscheint, müssen Sie zur Bestätigung *zweimal* den Button FERTIG anklicken.

Beim Einrichten des Benutzers können Sie diesen mit einer Option zum Administrator machen. Das bedeutet, dass der Benutzer zur Gruppe `wheel` hinzugefügt wird. Alle Benutzer dieser Gruppe dürfen `sudo` zur Durchführung von Administrationsarbeiten nutzen.

Installation aus dem Live-System

Neben der herkömmlichen Installation bietet Fedora auch eine Live-Installation an. Dazu starten Sie den Rechner mit einer Live-CD. Mit SYSTEM TOOLS • INSTALL TO HARD DISK starten Sie das Installationsprogramm. Es ist nahezu identisch mit dem der Installations-DVD, es bietet aber keine Upgrade-Möglichkeit für vorhandene Fedora-Installationen und keine Paketauswahl. Es werden einfach alle Dateien des Live-Systems installiert. Aus diesem Grund ist die Installation nach verblüffend kurzer Zeit fertig.

Nach dem ersten Start sollten Sie noch einige deutsche Sprachpakete installieren. Unter Umständen müssen Sie auch mit `system-config-language` die globalen Spracheinstellungen ändern.

```
root#  yum install autocorr-de hunspell-de hyphen-de system-config-language
root#  system-config-language
```

Installation auf einen USB-Stick

Mit dem Programm `liveusb-creator` können Sie das Fedora-Live-System direkt auf einen USB-Stick installieren. Das Programm kann wahlweise in einem laufenden Fedora-System (`yum install liveusb-creator`) oder unter Windows installiert werden:

https://fedorahosted.org/liveusb-creator

Nach dem Programmstart geben Sie an, wie viel Speicherplatz auf dem USB-Stick zur persistenten Speicherung von Einstellungen und eigenen Dateien reserviert werden soll. `liveusb-creator` lädt die gewünschte Fedora-Version direkt aus dem Internet herunter oder greift auf eine vorhandene Live-CD zurück.

Erfahrene Benutzer können ISO-Dateien von Installationsmedien auch einfach mit `dd` auf das Device des USB-Sticks übertragen.

Erste Schritte

Sofern Sie sich für den Gnome-Desktop entschieden haben, erscheint beim ersten Login dessen Willkommensassistent. Dort können Sie nochmals die gewünschte Sprache und das Tastaturlayout bestätigen bzw. verändern und Online-Konten einrichten. Das anschließende Einführungsvideo können Sie mit Esc abbrechen.

Erstes Update

Anschließend sollten Sie ein erstes Update durchführen – wahlweise mit dem Programm SOFTWARE-AKTUALISIERUNG oder im Terminal mit `yum update`. Dieses Update dauert oft ähnlich lange wie die Installation.

Zusätzliche Paketquellen einrichten

In den offiziellen Fedora-Paketen fehlen aus Lizenz- und Patentgründen eine Menge oft benötigter Pakete: Treiber für ATI- und NVIDIA-Grafikkarten, MP3-Unterstützung etc. Die größten alternativen Paketquellen, nämlich *Livna*, *Freshrpms* und *Dribble*, haben sich 2008 unter dem Namen *RPM Fusion* zusammengeschlossen. RPM Fusion ist somit die wichtigste inoffizielle Quelle für Fedora-Erweiterungen. Aus rechtlichen Gründen wurde ein traditionell von Livna angebotenes Paket nicht in RPM Fusion integriert. Die Livna-Paketquelle existiert deswegen weiterhin und bietet dieses eine Paket an. (Den Namen des Pakets mag ich hier – ebenfalls aus rechtlichen Gründen – nicht nennen.)

http://rpmfusion.org
http://rpm.livna.org

Um eine zusätzliche Paketquelle in YUM zu integrieren, müssen Sie eine neue Datei in `/etc/yum.repos.d` anlegen sowie einen Schlüssel für die Paketquelle einrichten. Die meisten Paketquellen erleichtern Ihnen diese Arbeit durch ein kleines RPM-Paket, das alle erforderlichen Dateien enthält. Dieses Paket installieren Sie mit `rpm -i`. Für RPM Fusion und Livna sehen die Kommandos wie folgt aus:

```
root#  rpm -ivh http://download1.rpmfusion.org/free/fedora/\
                rpmfusion-free-release-stable.noarch.rpm
root#  rpm -ivh http://download1.rpmfusion.org/nonfree/fedora/\
                rpmfusion-nonfree-release-stable.noarch.rpm
root#  rpm -ivh http://rpm.livna.org/livna-release.rpm
```

Die Webadressen müssen jeweils ohne Leerzeichen angegeben werden. RPM Fusion stellt eigentlich zwei Paketquellen zur Verfügung: `free` und `nonfree`. Der Unterschied besteht darin, dass `free`-Pakete Open-Source-Software enthalten, `nonfree`-Pakete dagegen kostenlose kommerzielle Software, etwa Grafiktreiber.

Bei der ersten Installation von Paketen aus der RPM-Fusion-Paketquelle müssen Sie die Schlüssel dieser Paketquelle importieren. Nach meinen Erfahrungen funktioniert das am besten, wenn Sie die Installation mit `yum` durchführen, nicht mit einem grafischen Paketverwaltungswerkzeug.

Multimedia-Pakete

Nachdem Sie die die RPM-Fusion-Paketquellen `free` und `nonfree` eingerichtet haben, installieren Sie so die wichtigsten Multimedia-Codecs:

```
root#  yum install gstreamer1-plugins-bad* gstreamer1-plugins-ugly* \
         gstreamer1-plugins-libav*
```

ATI/AMD-Treiber

Wenn Sie auf die binären Grafiktreiber von ATI/AMD oder NVIDIA angewiesen sind, treffen Sie mit Fedora keine gute Wahl. Etliche Xorg-Entwickler sind bei Red Hat angestellt und nutzen Fedora als Testplattform und Spielwiese. Fedora enthält grundsätzlich die allerneuesten Versionen des X-Servers, oft lange bevor deren Entwicklung ausgereift oder gar abgeschlossen ist. Das hat zur Folge, dass die Treiber von ATI/AMD bzw. NVIDIA häufig noch inkompatibel zum X-System sind.

Die einfachste Möglichkeit zur Installation des ATI-Treibers bietet in der Regel die RPM-Fusion-Paketquelle, die Sie zuerst aktivieren müssen. Anschließend installieren Sie den Treiber mit dem folgenden Kommando:

```
root#  yum install akmod-catalyst
```

NVIDIA-Treiber

Auf Rechnern mit NVIDIA-Grafikkarten kommt in Fedora standardmäßig der Nouveau-Grafiktreiber zum Einsatz. Dieser funktioniert mittlerweile gut. Der proprietäre NVIDA-Treiber verspricht aber zum Teil eine höhere Geschwindigkeit und einen geringeren Stromverbrauch. Fedora-kompatible Pakete dieses Treibers finden Sie mit etwas Glück in der RPM-Fusion-Paketquelle. Der NVIDIA-Treiber ist im Paket `akmod-nvidia` versteckt. Während der Installation wird automatisch `/etc/X11/xorg.conf` modifiziert, sodass der neue Treiber nach einem Neustart des Rechners automatisch zum Einsatz kommt.

alias-Einstellungen für root

Wenn Sie als `root` arbeiten, erscheinen bei der Ausführung von `mv` und `rm` ständig Sicherheitsabfragen, ob Sie die Operation wirklich durchführen möchten. Diese Sicherheitsabfragen hören auf, wenn Sie die `alias`-Anweisungen aus `/root/.bashrc` entfernen.

bash-completion

Die programmspezifische Erweiterung von Dateinamen in der `bash` funktioniert nur, wenn Sie das Paket `bash-completion` installieren.

3.4 openSUSE

openSUSE zählt zu den im deutschen Sprachraum am weitesten verbreiteten Linux-Distributionen. Das wesentliche Unterscheidungsmerkmal der diversen SUSE-Distributionen gegenüber der Konkurrenz ist das allumfassende Konfigurations- und Administrationswerkzeug YaST (*Yet another Setup Tool*). openSUSE gilt als die beste KDE-Distribution. openSUSE steht damit im Gegensatz zu den meisten anderen Distributoren, die sich primär auf Gnome konzentrieren.

Der Name SUSE

Die Abkürzung SUSE stand ursprünglich für »Gesellschaft für Software und Systementwicklung«. 2003 hat Novell SUSE gekauft. SUSE wurde damit Teil der Firma Novell. 2010 übernahm Attachmate Novell. Alle kommerziellen Linux-Produkte werden seither wieder unter dem Namen SUSE von der nun eigenständig agierenden SUSE Linux GmbH verkauft.

openSUSE

openSUSE ist eine kostenlose Variante zu den kommerziellen SUSE-Distributionen. Die Entwicklung wird zwar ebenfalls stark von SUSE-Mitarbeitern getragen, es gibt aber öffentliche Beta-Versionen, Mailinglisten, eine Bug-Datenbank und eine aktive Community, die an der Entwicklung teilnimmt und diese unterstützt. Damit spielt openSUSE für SUSE eine ähnliche Rolle wie Fedora für Red Hat.

openSUSE-Versionen erscheinen momentan in einem achtmonatigen Rhythmus: Version 13.1 im November 2013, Version 13.2 im August 2014 etc. Für jede Version gibt es 18 Monate lang kostenlose Updates.

SUSE-Varianten

Wenn in diesem Buch von *SUSE* die Rede ist, meine ich damit die zurzeit populärste SUSE-Linux-Variante, nämlich *openSUSE*. Auf der SUSE-Website finden Sie diverse andere Linux-Distributionen, beispielsweise den *SUSE Linux Enterprise Server*. Diese Varianten richten sich (auch bei der Preisgestaltung) an kommerzielle Anwender, denen maximale Stabilität, lange Support-Zeiträume sowie die Unterstützung zusätzlicher CPU-Plattformen wichtiger sind als die jeweils neueste Kernel-, KDE- bzw. Gnome-Version.

Links

Ausführliche Informationen zu openSUSE und SUSE sowie Handbücher im HTML- und PDF-Format finden Sie auf den folgenden Webseiten:

http://www.opensuse.org
http://en.opensuse.org/SDB:Official_documentation
http://www.suse.com

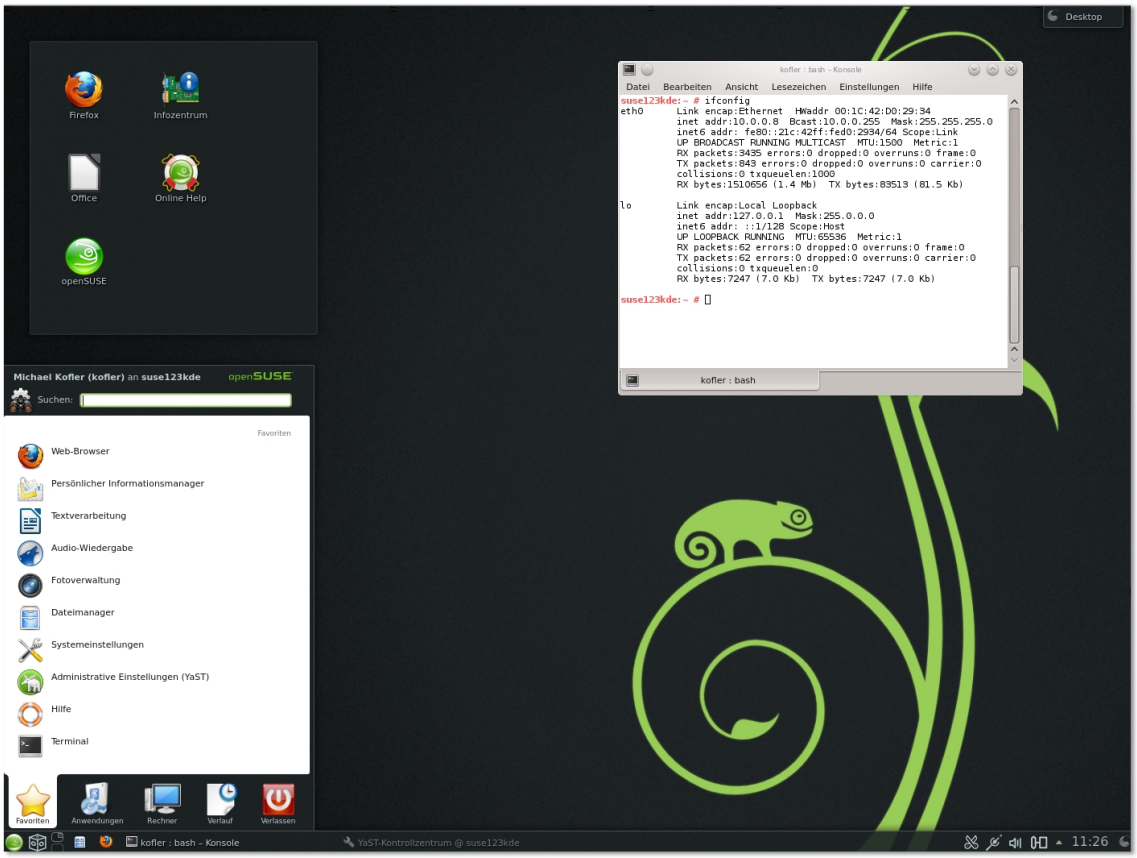


Abbildung 3.12 KDE-Desktop in openSUSE

openSUSE installieren

Installationsmedien

Auf der Website *http://software.opensuse.org* stehen mehrere ISO-Images zum Brennen eigener Installationsmedien zur Auswahl. Die ca. 4,7 GByte umfassende Komplett-DVD eignet sich zur Installation aller gängigen Desktop-Systeme: KDE, Gnome, XFCE oder LXDE. Aus den ehemaligen Live-CDs sind ebenfalls DVDs geworden; die ISO-Dateien sind knapp 1 GByte groß. Schließlich gibt es ein relativ kleines Image zur Netzwerkinstallation: Es enthält nur das Installationsprogramm; die Pakete werden während der Installation heruntergeladen.

Alle ISO-Images können nicht nur auf CDs bzw. DVDs gebrannt werden, sondern auch auf einen USB-Stick kopiert werden. Wenn Sie Zugang zu einem laufenden Linux-System haben, verwenden Sie dazu das Kommando `dd`. Dabei müssen Sie `/dev/sdc` durch das Device Ihres USB-Sticks ersetzen:

```
root#  dd if=datei.iso of=/dev/sdc
```

Installationseinstellungen

In diesem Abschnitt gehe ich davon aus, dass Sie die Komplett-DVD oder einen entsprechenden USB-Stick als Installationsmedium verwenden. Auf der Begrüßungsseite stellen Sie mit F2 die gewünschte Sprache ein. Falls notwendig, können Sie mit F3 die Auflösung des Grafiksystems während der Installation ändern. Falls das Grafiksystem Probleme bereitet, wählen Sie hier TEXTMODUS.

Mit F4 geben Sie an, aus welcher Quelle das Installationsprogramm die Pakete beziehen soll: standardmäßig natürlich von der Installations-DVD, alternativ besteht aber auch die Möglichkeit, die Pakete via HTTP/FTP/NFS/SMB oder SLP von einem Server herunterzuladen.

F5 steuert, welche Optionen an den Kernel übergeben werden. Von den Standardeinstellungen sollten Sie nur abweichen, wenn während des Kernelstarts Probleme auftreten. Mögliche Optionen sind KEIN ACPI, KEIN LOKALES APIC sowie SICHERE EINSTELLUNGEN, wodurch neben ACPI und APIC weitere Kernelfunktionen deaktiviert werden. (ACPI steht für *Advanced Configuration and Power Interface*. APIC steht für *Advanced Programmable Interrupt Controller* und bezeichnet ein Schema, um Hardware-Interrupts an die CPUs weiterzuleiten.)

Unabhängig von den durch F5 gewählten, aber leider nicht angezeigten Kerneloptionen können Sie in der Zeile BOOTOPTIONEN zusätzliche Kernelparameter eingeben (siehe auch Abschnitt 28.4). Vorher sollten Sie mit F2 das deutsche Tastaturlayout aktivieren. Falls während der Installation eine Update-Diskette, -CD oder -Datei berücksichtigt werden soll, drücken Sie schließlich noch auf F6.

Installationsmenü

Nach diesen Voreinstellungen wählen Sie einen Eintrag aus dem im Folgenden beschriebenen Menü aus (siehe Abbildung 3.13). Wenn Sie 10 Sekunden lang keine Cursortaste drücken, wird automatisch der erste Menüpunkt ausgewählt. Zur Installation ist aber normalerweise der zweite Punkt erforderlich!

- VON FESTPLATTE BOOTEN: Damit wird die Auto-Run-Funktion der CD beendet und stattdessen das momentan auf der Festplatte installierte Betriebssystem gestartet. Diese Variante gilt standardmäßig. Das ist dann praktisch, wenn Sie die CD oder DVD versehentlich im Laufwerk lassen. In diesem Fall wird bei einem Rechnerneustart nicht das SUSE-Installationsprogramm, sondern ganz normal das vorhandene Betriebssystem gestartet (sei es nun Windows, SUSE oder ein anderes Linux-System).
- INSTALLATION: Damit beginnt die normale Installation mit YaST.
- RETTUNGSSYSTEM: Im Rettungssystem können Sie versuchen, vorhandene Linux-Installationen zu reparieren.
- INSTALLATIONSMEDIUM ÜBERPRÜFEN: Damit kontrollieren Sie, ob die DVD frei von Fehlern ist.

- FIRMWARE-TEST: Dieser Menüpunkt startet ein von Intel entwickeltes Programm, das das BIOS auf seine Linux-Tauglichkeit überprüft. Dieses Programm kann bei aktueller Hardware Fehlermeldungen liefern, obwohl Linux sehr wohl läuft. Weitere Informationen finden Sie hier:

  http://www.linuxfirmwarekit.org

- SPEICHERTEST: Damit überprüfen Sie, ob Ihr RAM zuverlässig funktioniert.

Abbildung 3.13 openSUSE-Installationsmenü

Installation starten

Im ersten Dialog des Installationsprogramms stellen Sie die Sprache und Tastaturbelegung ein. Nach einer kurzen Systemanalyse können Sie sich im nächsten Dialog entscheiden, ob Sie SUSE neu installieren möchten oder ob Sie ein vorhandenes SUSE-System aktualisieren oder reparieren möchten. Dieser Dialog enthält die standardmäßig aktivierte Option AUTOMATISCHE KONFIGURATION. Sie bewirkt, dass das Installationsprogramm die Hardware-Konfiguration selbstständig vornimmt. Das betrifft unter anderem die Netzwerkschnittstellen, das Audio- und das Grafiksystem. Linux-Einsteiger sollten diese Option aktiviert lassen. Nur wenn Probleme auftreten bzw. wenn Sie ganz spezifische Konfigurationswünsche haben, deaktivieren Sie die Option.

Bei einer Neuinstallation bestätigen Sie als Nächstes Datum und Uhrzeit sowie Ihre Zeitzone. Dann wählen Sie, ob Sie als Benutzeroberfläche Gnome oder KDE nutzen möchten. Es ist zu diesem Zeitpunkt nicht möglich, beide Systeme auszuwählen. Sie können aber später im Punkt SOFTWARE-AUSWAHL die jeweils andere Benutzer-

oberfläche zusätzlich zur Installation markieren und in der Folge beim Login den gewünschten Desktop auswählen.

Partitionierung

Das Installationsprogramm macht nun einen Vorschlag für die Partitionierung der Festplatte: Standardmäßig richtet das Programm eine Swap-Partition mit circa der eineinhalbfachen RAM-Größe ein, außerdem eine Root-Partition und eine `/home`-Partition. Zudem werden alle Windows-Partitionen in das Dateisystem eingebunden. Wenn Sie mit dem Vorschlag einverstanden sind, klicken Sie einfach auf WEITER. Wenn Sie den Vorschlag an sich übernehmen, aber noch Details verändern möchten, entscheiden Sie sich für PARTITIONSAUFBAU BEARBEITEN. Wenn Sie die Partitionierung dagegen vollständig selbst vornehmen möchten, wählen Sie PARTITIONSAUFBAU ERSTELLEN und im nächsten Dialog BENUTZERDEFINIERTE PARTITIONIERUNG (FÜR EXPERTEN).

Damit gelangen Sie in den Partitionseditor (siehe Abbildung 3.14). Dieser Programmteil ermöglicht es Ihnen, neue Partitionen auf allen Festplatten anzulegen. Vorhandene Windows-Partitionen können mit dem Button GRÖSSE ÄNDERN verkleinert werden.

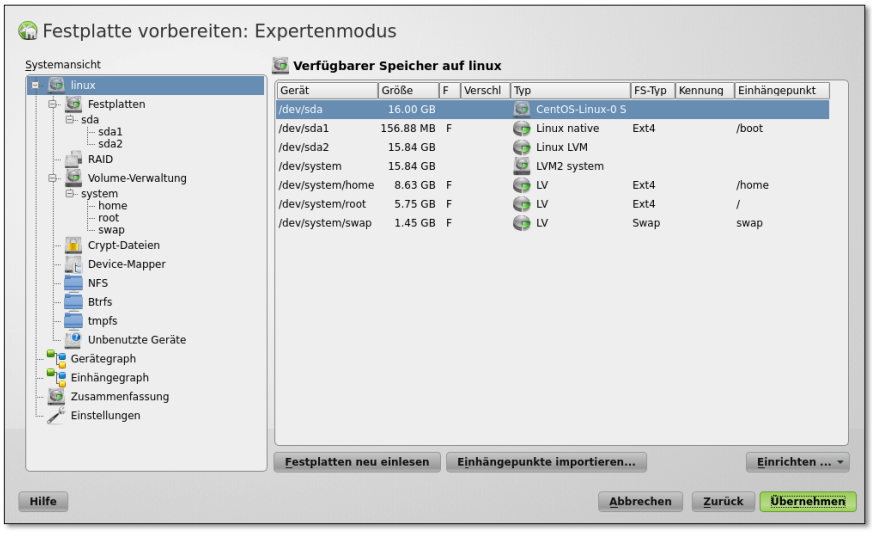


Abbildung 3.14 Partitionseditor

Sie können auch Partitionen löschen oder bereits vorhandene Partitionen nutzen. Führen Sie das Kontextmenükommando BEARBEITEN aus, und geben Sie den gewünschten Mount-Punkt an, z. B. `/`. Wahlweise können Sie die Partition auch formatieren – damit gehen alle darin enthaltenen Daten verloren. YaST unterstützt die Linux-Dateisysteme `ext2`, `ext3`, `ext4`, `btrfs`, `jfs`, `reiserfs` und `xfs`.

Für Linux-Profis bietet der Partitionseditor einige Besonderheiten: So ist es möglich, eine bereits vorhandene `/etc/fstab`-Datei zu nutzen oder ein LVM- bzw. ein RAID-System einzurichten.

Verschlüsselung

Es ist möglich, einzelne Datenpartitionen mit der Option GERÄTE-VERSCHLÜSSELUNG zu verschlüsseln. Zur Nutzung dieser Partitionen muss dann während des Startprozesses das Verschlüsselungspasswort angegeben werden.

Es ist auf diese Weise allerdings unmöglich, die Systempartition, die Bootpartition sowie die Partitionen für die Verzeichnisse `/usr` und `/var` zu verschlüsseln. Wenn Sie die gesamte Installation gegen eine unbefugte Nutzung absichern möchten, ist es am besten, LVM einzusetzen und die gesamte Volume Group zu verschlüsseln. Das Installationsprogramm bietet hierfür eine eigene Option an.

Benutzereinstellungen

Im nächsten Dialogblatt geben Sie in der Regel Ihren vollständigen Namen, den gewünschten Login-Namen sowie das Passwort an. Optional ist es auch möglich, mit ÄNDERN eine externe Authentifizierungsmethode auszuwählen, z. B. LDAP, NIS, Windows-Domäne oder Kerberos.

Etwas bedenklich ist der Umstand, dass das Benutzerpasswort standardmäßig auch für `root` gilt. Nur wenn Sie die diesbezügliche Option deaktivieren, haben Sie die Möglichkeit, im nächsten Dialog ein eigenes `root`-Passwort anzugeben. Die openSUSE-Entwickler begründen ihre Vorgehensweise damit, dass ohnedies mehr als 75 Prozent aller Benutzer für `root` dasselbe Passwort verwenden wie für den ersten Benutzeraccount. Das mag sein, aber vom Sicherheitsstandpunkt aus betrachtet ist das natürlich nicht ganz optimal ...

Zusammenfassung

Das Installationsprogramm zeigt nun eine Zusammenfassung aller Einstellungen an (siehe Abbildung 3.15). Wenn Sie damit einverstanden sind, klicken Sie einfach auf INSTALLIEREN, und los geht's. Sie sollten sich aber die Mühe machen, den Installationsvorschlag vorher in Ruhe durchzulesen! Oft ist es sinnvoll bzw. notwendig, Details zu verändern. Zur Änderung wählen Sie einfach den entsprechenden Punkt in der Zusammenfassung mit der Maus bzw. mit ⇆ aus.

Software-Auswahl

Wenn Sie sich für ein KDE-Standardsystem entschieden haben, beansprucht dieses bei einem `ext4`-Dateisystem ca. 4 GByte in der Systempartition. Optional können Sie nun ganze Software-Gruppen oder auch nur einzelne Pakete hinzufügen: Gnome, Server-Komponenten, Entwicklerwerkzeuge etc. YaST zeigt dabei an, wie viel Platz die Installation auf Ihrer Festplatte ungefähr beanspruchen wird. Wenn Sie ein bestimmtes Programm nicht finden, klicken Sie auf DETAILS und verwenden dann die Suchfunktion (FILTER SUCHE).

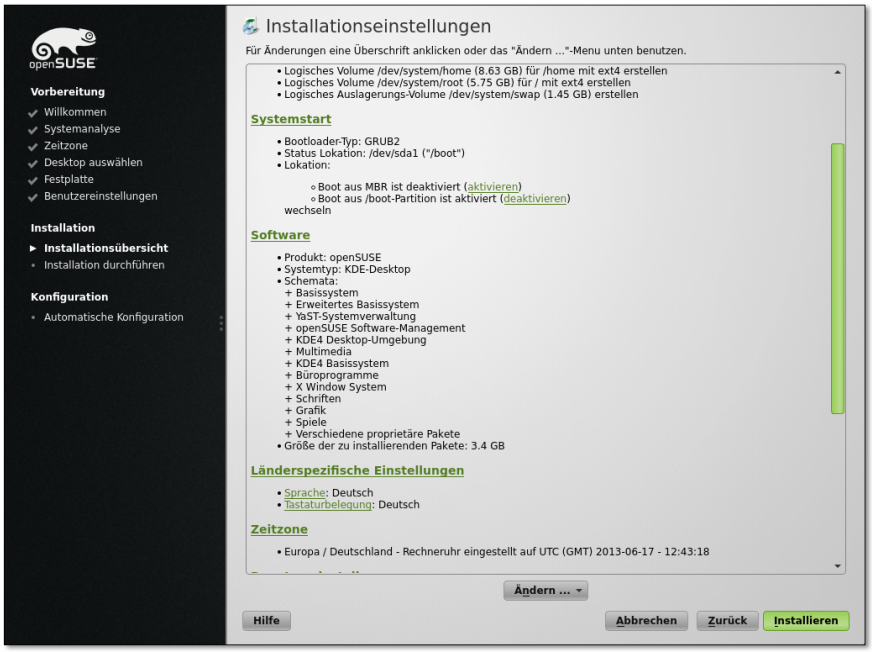


Abbildung 3.15 Installationseinstellungen

Systemstart bei BIOS-Rechnern

Die Details des Systemstarts hängen davon ab, ob openSUSE im BIOS- oder im EFI-Modus installiert wurde. In beiden Fällen verwendet openSUSE den Bootloader GRUB. Dabei werden im GRUB-Menü Einträge für alle auf der Festplatte erkannten Betriebssysteme eingebaut.

Im Gegensatz zu den meisten anderen Distributionen installiert openSUSE GRUB normalerweise *nicht* in den Master Boot Record der ersten Festplatte. Wenn es eine erweiterte Partition gibt, schlägt YaST vor, GRUB in deren Bootsektor zu installieren, andernfalls in den Bootsektor der System- oder Bootpartition. Die GRUB-Entwickler raten allerdings explizit von der Installation in einzelne Partitionen ab und empfehlen die Installation in den Bootsektor der Festplatte.

YaST markiert außerdem die Partition, in deren Bootsektor GRUB installiert wird, als *aktive* Partition – also als die Partition, von der gebootet werden soll. Schließlich überschreibt YaST den MBR mit einem Code, um den Bootloader der aktiven Partition zu laden. Diese relativ komplizierte Vorgehensweise soll ein möglichst konfliktfreies Zusammenspiel mit Windows garantieren.

Beachten Sie, dass openSUSE in der Standardkonfiguration eine bereits vorhandene GRUB-Installation einer anderen Linux-Distribution überschreibt. Wenn Sie das nicht möchten, klicken Sie im Dialogblatt BOOTLOADER-INSTALLATION den But-

ton Bootloader-Optionen an und deaktivieren dann die Option Generischen Bootcode in MBR schreiben (siehe Abbildung 3.16)!

Wenn Sie GRUB – wie von den GRUB-Entwicklern vorgesehen – in den Startsektor der Festplatte bzw. SSD installieren möchten, aktivieren Sie im Dialog Bootloader-Installation die Option Aus Master-Boot-Record starten und deaktivieren alle anderen Optionen.

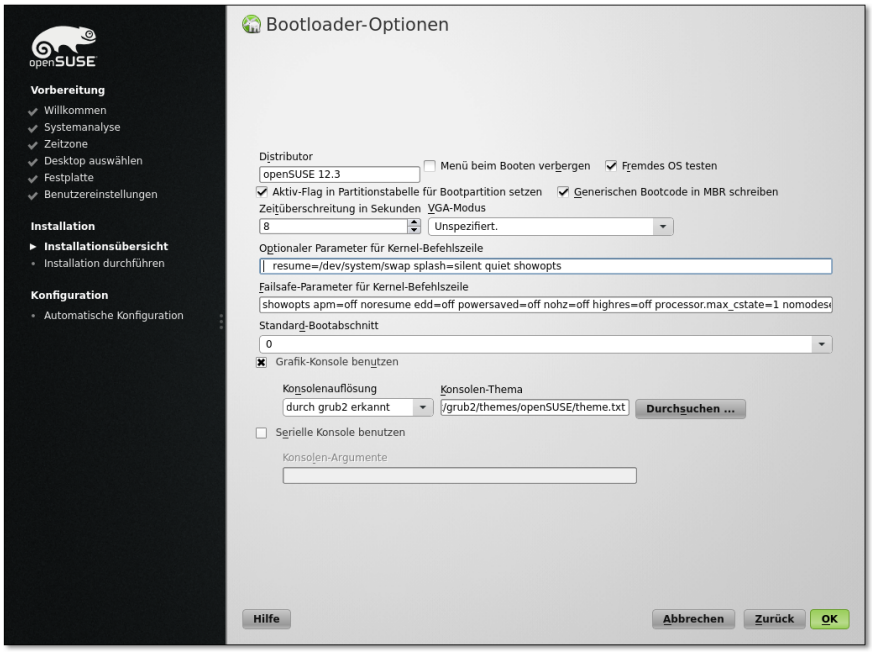


Abbildung 3.16 Es gibt unzählige Bootloader-Optionen.

Vorsicht bei der Bootloader-Konfiguration!

Ich kenne keine andere Distribution, bei der die Bootloader-Konfiguration so kompliziert und unübersichtlich ist wie bei openSUSE! Nur wenn auf Ihrem Rechner keine anderen Betriebssysteme installiert sind, können Sie die zahllosen Optionen bedenkenlos so lassen, wie sie sind. Ansonsten sollten Sie unbedingt einen genauen Blick auf sämtliche Bootloader-Optionen werfen.

Systemstart im EFI-Modus

Bei Rechnern mit EFI wird GRUB in das Verzeichnis `/boot/efi/EFI/opensuse` installiert. openSUSE 12.3 unterstützt UEFI Secure Boot erst experimentell. Wenn auf Ihrem Rechner Secure Boot aktiv ist, müssen Sie im Dialog Bootloader-Einstellungen die Option Enable Secure Boot Support aktivieren.

Installation durchführen

Sobald Sie mit allen Einstellungen einverstanden sind, klicken Sie den Button INSTALLIEREN an. Die Installation dauert einige Minuten. Sie können sich während dieser Wartezeit eine Diashow ansehen oder die Release-Notes lesen. Anschließend wird der Rechner neu gestartet.

Erste Schritte

Netzwerk konfigurieren

openSUSE fährt bei der Netzwerkkonfiguration zweigleisig: Auf Desktop-PCs kümmern sich YaST und dessen Scripts (`ifup`) um die Netzwerkkonfiguration, bei Notebooks hingegen sind der NetworkManager und dessen KDE- bzw. Gnome-Benutzeroberflächen zuständig. Wenn die Netzwerkeinstellungen zicken, wie dies bei openSUSE 12.3 häufig vorkam, starten Sie das Konfigurationsprogramm YaST und aktivieren dessen Modul NETZWERKGERÄTE • NETZWERKEINSTELLUNGEN. Im Dialogblatt GLOBALE OPTIONEN stehen die Varianten TRADITIONELLE METHODE MIT IFUP oder BENUTZERGESTEUERT MITHILFE VON NETWORKMANAGER zur Auswahl.

Hostname einstellen

Während der Installation besteht keine Möglichkeit, den Hostnamen einzustellen. openSUSE verwendet stattdessen eine Zufallszeichenkette wie `linux-q2uf`. Abhilfe: Starten Sie das YaST-Modul NETZWERKGERÄTE • NETZWERKEINSTELLUNGEN, wechseln Sie in das Dialogblatt HOSTNAME, und geben Sie dort den gewünschten Hostnamen an. Damit alle KDE- und Gnome-Programme diese Änderung nachvollziehen, müssen Sie sich ab- und neu anmelden.

Firewall einstellen

Unter openSUSE ist standardmäßig eine Firewall installiert und auch aktiv. Damit wird nahezu der gesamte nach außen gehende Netzwerkverkehr blockiert. Unter anderem ist es deswegen unmöglich, auf Windows- oder Samba-Netzwerkfreigaben zuzugreifen. Die Konfiguration erfolgt durch das YaST-Modul SICHERHEIT • FIREWALL, (siehe auch Kapitel 40). Wenn sich Ihr Rechner in einem sicheren lokalen Netz befindet, sollten Sie die Netzwerkschnittstelle der INTERNEN ZONE zuordnen.

Erstes Update

Das erste Update führen Sie wahlweise mit dem von KDE oder Gnome vorgeschlagenen Update-Tool oder in einem Terminal mit dem Kommando `zypper update` durch.

CD/DVD als Paketquelle deaktivieren

Nach der Installation von einer Komplett-DVD dient diese als Paketquelle für die Installation weiterer Pakete. Im Regelfall ist es aber wünschenswert, neue Pakete in der gerade aktuellen Version direkt aus dem Internet herunterzuladen. Dazu starten Sie das YaST-Modul SOFTWARE-REPOSITORIES und löschen die Paketquelle *URL cd:///xxx*.

Packman-Paketquelle einrichten

openSUSE liefert zwar von Haus aus diverse Audio- und Video-Player mit, dennoch ist die Multimedia-Unterstützung relativ schlecht: Viele Audio- und Video-Formate können nicht abgespielt werden. Ebenso wenig können kopiergeschützte DVDs ange-

sehen werden. Das hat nicht technische, sondern rechtliche Gründe: Diverse Codecs sind in manchen Ländern durch Patente geschützt. Deswegen ist die Weitergabe von Open-Source-Implementierungen nicht überall zulässig. Und da openSUSE international verbreitet wird, gilt eben der kleinste gemeinsame Nenner.

Die Lösung dieses Problems ist die Packman-Paketquelle. Um diese zu aktivieren, starten Sie das YaST-Modul Software-Repositories, führen dort Hinzufügen • Community/Gemeinschafts-Repositories aus und aktivieren die Packman-Paketquelle. Dabei müssen Sie den Schlüssel der Packman-Paketquelle als vertrauenswürdig bestätigen.

Danach starten Sie das YaST-Modul Software installieren und löschen, wählen mit Anzeigen • Installationsquellen die Packman-Paketquelle aus und klicken dann auf den Link Wechsel von Systempaketen. Wenn Sie unter Gnome arbeiten, hat in dessen YaST-Modul Software installieren der Button Installierte Pakete auf die Versionen in diesem Repository umstellen dieselbe Wirkung. Alternativ können Sie auch in einem Terminalfenster das Kommando `zypper dup` ausführen. In allen drei Fällen werden nun eine Menge openSUSE-Pakete durch äquivalente Packman-Pakete ersetzt.

Codecs installieren

Nachdem Sie die Packman-Paketquellen eingerichtet haben, installieren Sie so die wichtigsten Multimedia-Codecs:

```
root#  zypper install gstreamer-0_10-plugins-bad \
              gstreamer-0_10-plugins-ugly* gstreamer-0_10-plugins-ffmpeg
```

Auf der Website *http://opensuse-community.org* finden Sie 1-Click-Links zur Installation weiterer Codecs.

ATI/AMD-Grafiktreiber

Zur Installation des proprietären ATI/AMD-Treibers gibt es drei Möglichkeiten: Am einfachsten ist die Verwendung der inoffiziellen Paketquelle von Bruno Friedmann. Beinahe ebenso simpel ist die Ausführung des Installations-Scripts `makerpm-ati` von Sebastian Siebert, das den Treiber herunterlädt, kompiliert, in ein RPM-Paket verpackt und installiert. Und zu guter Letzt können Sie den Treiber natürlich auch manuell installieren (siehe Abschnitt 24.4). Details, Download-Links und Tipps finden Sie auf der folgenden Webseite:

http://de.opensuse.org/SDB:AMD/ATI-Grafiktreiber

NVIDIA-Grafiktreiber

Wenn Ihr Rechner eine NVIDIA-Grafikkarte enthält, kommt standardmäßig der `nouveau`-Treiber zum Einsatz. Der Treiber funktioniert mit nahezu allen Modellen gut, kann aber die Energiesparfunktionen der Grafikkarte nicht optimal nutzen.

Zum Glück ist die Installation des proprietären NVIDIA-Treibers ganz einfach: Dazu aktivieren Sie mit YaST die NVIDIA-Paketquelle und installieren dann das Paket `x11-video-nvidiaG02`.

Falls Probleme beim Einrichten des NVIDIA-Treibers auftreten sollten oder wenn Sie die aktuellste Version des Treibers manuell installieren möchten, finden Sie hier weitere Informationen:

http://de.opensuse.org/Proprietäre_NVIDIA-Grafiktreiber
http://www.suse.de/~sndirsch/nvidia-installer-HOWTO.html

3.5 Ubuntu

Ubuntu ist momentan die populärste und im Privatbereich am weitesten verbreitete Distribution. Das Motto von Ubuntu lautet *Linux for human beings* – also gewissermaßen »das menschliche Linux«. Das Zulu-Wort *ubuntu* steht denn auch für *Menschlichkeit gegenüber anderen* oder *achtsames Miteinander* oder auch *I am what I am because of who we all are*. Ubuntu Linux ist also nicht nur eine Menge Software-Technik, sondern eine ganze Philosophie.

Im Vergleich zu anderen Distributionen brilliert Ubuntu mit seiner guten Hardware-Unterstützung: Ubuntu war die erste große Distribution, die im EFI-Modus installiert werden konnte, und macht es seinen Anwendern besonders einfach, binäre Treiber für Grafikkarten (ATI und NVIDIA) sowie für WLAN-Karten zu installieren. Das Motto *it just works* stimmt natürlich nicht immer, aber es trifft für Ubuntu häufiger zu als bei jeder anderen Distribution.

Canonical

Hinter Ubuntu steht die Firma Canonical Ltd. des südafrikanischen Millionärs Mark Shuttleworth – ehemals Eigentümer von Thawte Consulting. Im Vergleich zu Red Hat hat Canonical aber wesentlich weniger Mitarbeiter. Dennoch tanzt Canonical momentan sprichwörtlich auf allen Hochzeiten und versucht neben dem klassischen Ubuntu für PCs auch Ubuntu-Versionen für Smartphones, Tablets und TV-Geräte fertigzustellen. Ob die ambitionierten Ziele von Canonical erreichbar sind, bleibt abzuwarten, zumal momentan kein plausibles Geschäftsmodell zu erkennen ist. Die Ubuntu-Website betont auf jeden Fall: *Ubuntu will always be free of charge.*

Versionen

Es gibt halbjährlich neue Ubuntu-Versionen, deren Versionsnummer das Datum der Fertigstellung widerspiegelt. Ubuntu 13.10 meint also die im Oktober 2013 fertiggestellte Ubuntu-Version. Außerdem hat jede Ubuntu-Version einen merkwürdigen Codenamen, für Version 13.10 lautet es z. B. *Saucy Salamander*. Diese Codenamen sind perfekt für Suchanfragen geeignet! Eine Suche nach *saucy nvidia* wird wesentlich spezifischere Ergebnisse liefern als eine Suche nach *ubuntu nvidia* oder gar nach *linux nvidia*.

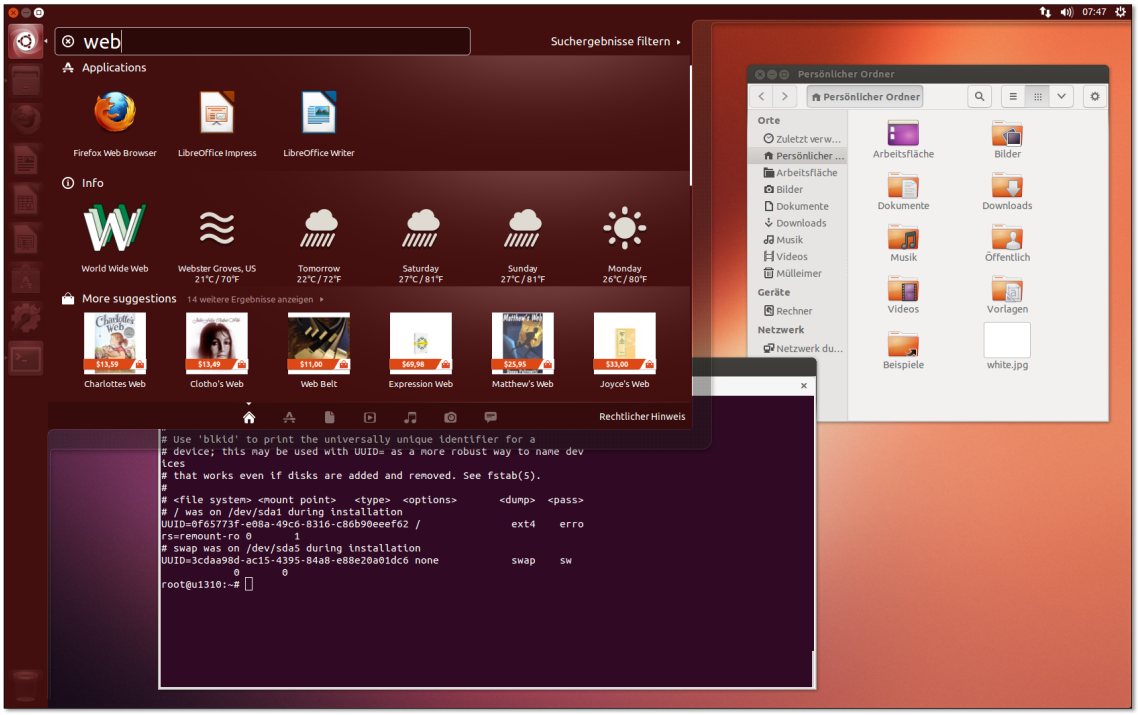


Abbildung 3.17 Der Ubuntu-Desktop mit dem Unity-spezifischen Startmenü

Long Time Support

Eine Sonderstellung innerhalb der vielen Ubuntu-Versionen nehmen die sogenannten LTS-Versionen ein (*Long Term Support*), deren Desktop-Pakete normalerweise für 3 Jahre, die Server-Pakete sogar für 5 Jahre gewartet werden. Keine andere kostenlose Linux-Distribution kann momentan mit derartig langen Update-Zeiträumen glänzen.

Varianten

Es gibt zahlreiche von Ubuntu abgeleitete Distributionen. Tabelle 3.1 fasst die wichtigsten offiziellen, also von Canonical unterstützten, sowie einige inoffizielle Varianten zusammen. Alle offiziellen Varianten greifen auf dieselben Paketquellen zurück und lassen sich daher beliebig erweitern. Sie können auch zuerst Xubuntu installieren und später die Gnome-Pakete von Ubuntu hinzufügen. Der Hauptunterschied zwischen den verschiedenen Ubuntu-Varianten besteht darin, welche Paketauswahl auf dem Datenträger mitgeliefert und erstmalig installiert wird.

Nachteile/Kritik

Ubuntu ist zwar sehr populär, hat aber wie jede andere Distribution Schwächen:

- Canonical geht mit Ubuntu viele eigene Wege und unterscheidet sich mittlerweile stark vom Linux-*Mainstream*. Insbesondere der Ubuntu-Desktop Unity hat viel Kritik und Emotionen geweckt; letztlich wurde der neue Desktop aber von den meisten Ubuntu-Anwendern positiv angenommen. Unbrauchbar ist Unity in

der aktuellen Version allerdings in virtuellen Maschinen: Dort laufen die vielen Unity-Animationseffekte quälend langsam ab.

- Einige Open-Source-Entwickler kritisieren, dass sich Ubuntu zwar großzügig im Open-Source-Supermarkt bedient, aber vergleichsweise wenig eigenen Code zurückgibt. Mark Shuttleworth hat diese Argumentation in einem langen Blog-Beitrag als einseitig zurückgewiesen und darauf verwiesen, dass Ubuntu einen nennenswerten Beitrag zur größeren Verbreitung von Linux leistet, gerade weil es sich auf andere Dinge, wie einfache Bedienung oder schönes Layout, konzentriert:

  http://www.markshuttleworth.com/archives/517

- Das pünktliche, halbjährliche Erscheinen neuer Ubuntu-Versionen geht mitunter auf Kosten der Stabilität.
- 2013 wurde der Update-Zeitraum für gewöhnliche Ubuntu-Versionen auf neun Monate reduziert. Damit sind diese Versionen eigentlich nur noch Linux-Profis zu empfehlen, die sich nicht an regelmäßigen Distributions-Updates stören. Für gewöhnliche Anwender sowie für den Server-Einsatz sind ausschließlich die LTS-Versionen geeignet, die alle zwei Jahre im April erscheinen – zuletzt Ubuntu 12.04 im April 2012, demnächst Ubuntu 14.04 im April 2014.
- Standardmäßig richtet Ubuntu keine Firewall ein.

Variante	Beschreibung
Kubuntu	Ubuntu mit KDE
Ubuntu Gnome	Ubuntu mit Gnome Shell statt Unity
Xubuntu	Ubuntu mit Xfce
Lubuntu	Ubuntu mit LXDE
Edubuntu	Ubuntu-Variante für Schule und Unterricht
Ubuntu Server	Ubuntu für den Server-Einsatz (ohne X)
Ubuntu Studio	Ubuntu für Multimedia-Anwender
Mythbuntu	Ubuntu als Media-Center mit Myth TV
Linux Mint	populäre Ubuntu-Variante ohne Unity (inoffiziell)
Zentyal (ehemals eBox)	kommerzielle Ubuntu-Server-Variante mit webbasierten Konfigurationswerkzeugen (inoffiziell)

Tabelle 3.1 Ubuntu-Varianten

Ubuntu installieren

Installationsmedien

Auf der Website *http://www.ubuntu.com/download/desktop* können Sie kostenlos Ubuntu-Installationsmedien herunterladen. Dabei haben Sie die Wahl zwischen einer 32- und einer 64-Bit-Variante.

In der Vergangenheit wurde darauf geachtet, dass sich die ISO-Datei auf eine CD brennen ließ, also nicht größer als ca. 700 MByte war. Mit Ubuntu 12.10 ist diese Grenze aber aus Platzgründen gefallen: Die ISO-Images müssen nun auf eine DVD gebrannt werden oder auf einen USB-Stick übertragen werden.

Alternative Ubuntu-Downloads

Auf der Website *http://cdimage.ubuntu.com* finden Sie diverse alternative Installationsmedien. Dazu zählen ein Image für die Installation auf Apple-Rechnern, Ubuntu-Varianten wie Kubuntu, Xubuntu oder Ubuntu Server sowie experimentelle Versionen für andere CPU-Plattformen. Auf dieser Website finden Sie auch die sogenannten Daily-Images der gerade in Entwicklung befindlichen nächsten Ubuntu-Version sowie ein kleines Netinstall-Image, das nur das Installationsprogramm enthält und die zu installierenden Pakete erst bei Bedarf aus dem Internet herunterlädt.

Die Netinstall-Image und Ubuntu Server unterscheiden sich insofern von den anderen Varianten, als hierbei ein textbasiertes Installationsprogramm zum Einsatz kommt. Eine ausführliche Beschreibung des Installationsverlaufes folgt in Abschnitt 3.6.

Standardinstallation starten

Um eine Ubuntu-Standardinstallation durchzuführen, starten Sie den Rechner mit der Ubuntu-DVD oder einem entsprechenden USB-Stick neu. Nach der Auswahl der gewünschten Sprache gelangen Sie in ein Live-System, in dem Sie Ubuntu ausprobieren und anschließend installieren können.

Grundeinstellungen

Nach dem Start des Installationsprogramms wählen Sie im ersten Schritt nochmals die gewünschte Sprache aus. Anschließend stellen Sie durch die Option AKTUALISIERUNG WÄHREND DER INSTALLATION HERUNTERLADEN (siehe Abbildung 3.18) ein, ob während der Installation Updates heruntergeladen werden sollen; das stellt sicher, dass Sie vom ersten Start an ein aktuelles System haben. Eine weitere Option steuert, ob auch Pakete von Drittanbietern installiert werden sollen; das betrifft z. B. das Adobe-Flash-Plugin sowie grundlegende Audio- und Video-Codecs. Diese Programme sind zwar kostenlos verfügbar, unterliegen aber nicht alle einer Open-Source-Lizenz. Ich verzichte normalerweise auf beide Optionen, da sie die Installationsdauer verlängern. Sowohl das Update als auch die Installation von MP3-Codecs können Sie auch später vornehmen.

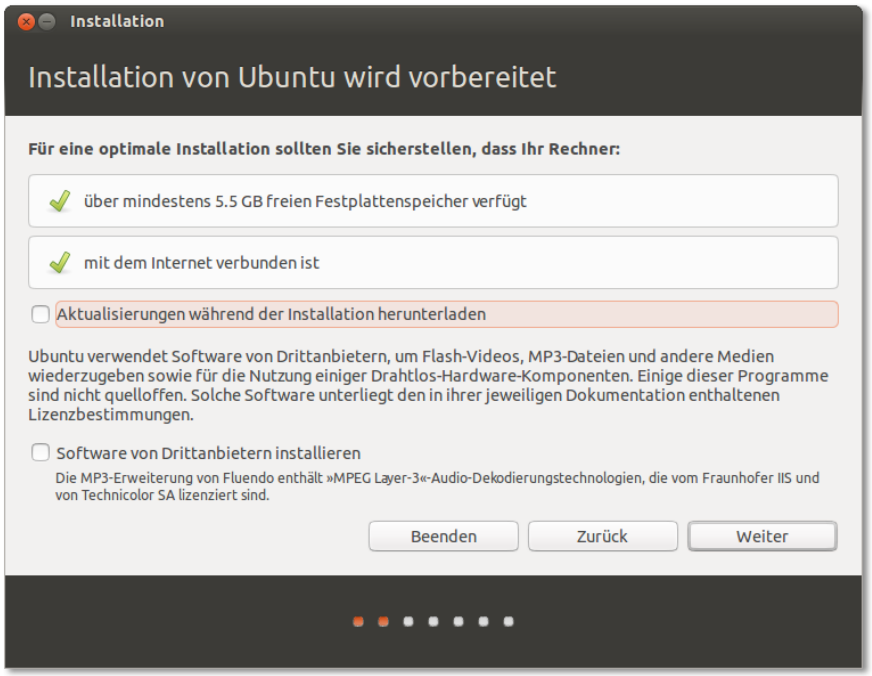


Abbildung 3.18 Grundeinstellungen im Ubuntu-Installationsprogramm

Partitionierung der Festplatte

Je nachdem, wie die Festplatte momentan partitioniert ist, können Sie zwischen mehreren Optionen wählen:

- UBUNTU NEBEN XXX INSTALLIEREN: Bei dieser Variante können Sie im nächsten Dialog eine vorhandene Partition von Windows oder einer bereits installierten Linux-Distribution verkleinern und den freien Platz für die Ubuntu-Installation nutzen. Mit dem Schieberegler zwischen den beiden Bereichen bestimmen Sie, wie viel Platz für die bisherige Partition und wie viel für Linux reserviert werden soll. Die Verkleinerung kann einige Minuten dauern. Haben Sie Geduld!
- XXX MIT UBUNTU ERSETZEN: Das Installationsprogramm löscht Ihr vorhandenes Windows- oder Linux-System und nutzt anschließend die gesamte Festplatte zur Installation von Ubuntu.
- UBUNTU AUF DIE VERSION NNN AKTUALISIEREN: Das Installationsprogramm aktualisiert eine bereits vorhandene Ubuntu-Installation. Dabei bleiben das `/home`-Verzeichnis und einige Grundeinstellungen des Systems erhalten. Allerdings funktioniert dieses Update nicht immer problemlos. Führen Sie nach Möglichkeit eine Neuinstallation durch.

- Ubuntu löschen und neu installieren: Damit wird eine vorhandene Ubuntu-Installation gelöscht. Auf dem so frei gewordenen Platz der Festplatte wird Ubuntu neu installiert.
- Festplatte löschen und Ubuntu installieren: Damit wird die gesamte Festplatte bzw. SSD gelöscht und anschließend neu partitioniert. Sie verlieren alle Daten auf der Festplatte. Diese Option wird unter anderem dann angezeigt, wenn die Festplatte noch leer ist und keine Partitionstabelle enthält.
- Etwas anderes: Hiermit führen Sie die Partitionierung selbst durch.

Sofern Sie sich nicht für Etwas anderes entscheiden, richtet das Installationsprogramm eine Swap-Partition (entspricht der Auslagerungsdatei) und eine Systempartition ein. Die Größe der Swap-Partition richtet sich nach der Größe des RAMs Ihres Rechners; die Swap-Partition wird je nachdem, wie viel Platz zur Verfügung steht, ein- bis zweimal so groß wie das RAM dimensioniert. Die Systempartition nutzt den gesamten Rest der Festplatte.

Wenn Sie die Größe der Partitionen selbst einstellen möchten, eine eigene `/home`-Partition wünschen etc., wählen Sie Etwas anderes. Um eine neue Partition zu erzeugen, klicken Sie zuerst den Eintrag Freier Speicherplatz und dann den Button Hinzufügen an. Im nun erscheinenden Dialog geben Sie den Typ der Partition, die Größe in MByte und das Dateisystem an. Falls es auf Ihrer Festplatte bereits eine geeignete Partition gibt, in die Sie Ubuntu installieren möchten, wählen Sie diese Partition aus, ändern mit Partition bearbeiten den Einhängepunkt und aktivieren das Auswahlhäkchen zur Neuformatierung der Partition (siehe Abbildung 3.19).

Sie beenden die Partitionierung mit dem Button Jetzt installieren. Das Installationsprogramm beginnt jetzt sofort mit der Installation. Vorsicht: Sie können die Installation nun nicht mehr stoppen! Der Bootloader GRUB wird im Verlauf der Installation ohne weitere Rückfrage in den Bootsektor (MBR) der ersten Festplatte installiert. Wenn Sie einen anderen Ort wünschen, müssen Sie die Installationsvariante Etwas anderes wählen und können die gewünschte Partition dann durch ein Listenfeld am unteren Rand des Partitionierungsdialogs einstellen.

Installation mit LVM und Verschlüsselung

Seit Version 12.10 unterstützt das grafische Installationsprogramm die LVM-Konfiguration sowie das Einrichten eines vollständig verschlüsselten Systems; dieses ist dann ebenfalls ein LVM-System, auch wenn das aus den Optionen nicht klar wird.

Den schnellsten Weg zu einer funktionierenden LVM-Konfiguration bietet die Option LVM für die neue Ubuntu-Installation benutzen im Dialog Installationsart (siehe Abbildung 3.20). Diese Option kann nur gewählt werden, wenn Sie die gesamte Festplatte für die Ubuntu-Installation verwenden und alle eventuell schon vorhandenen anderen Betriebssysteme löschen.

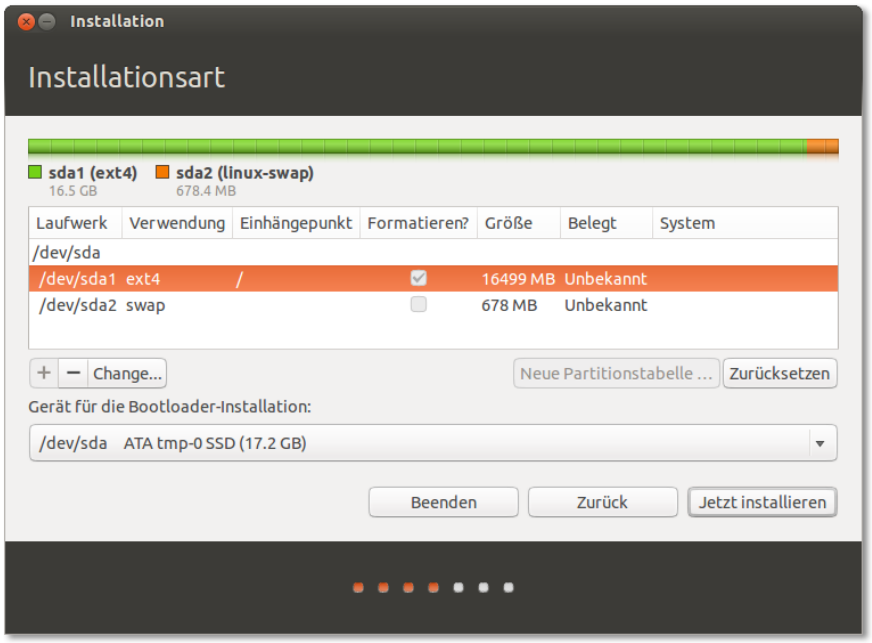


Abbildung 3.19 Manuelle Partitionierung

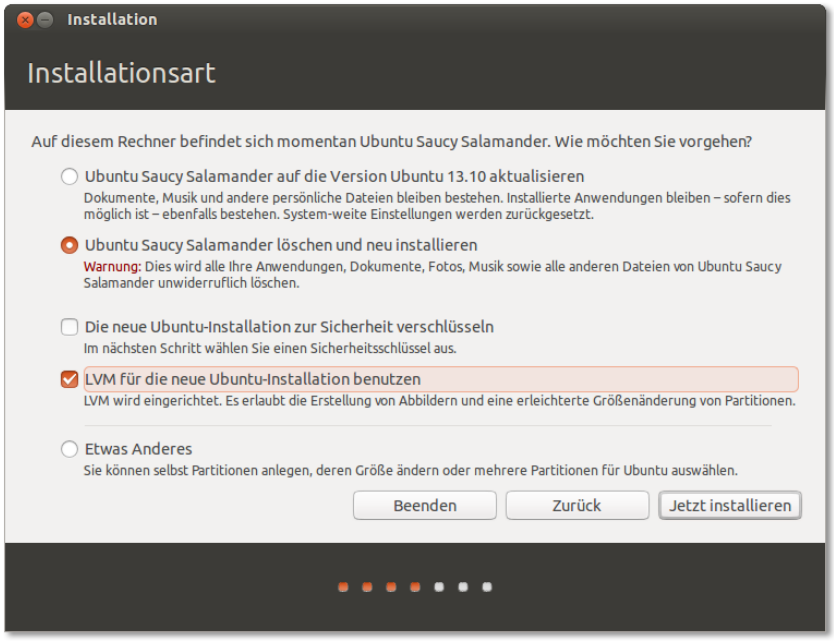


Abbildung 3.20 Die Verschlüsselungs- und LVM-Optionen im Ubuntu-Installationsprogramm

Das Installationsprogramm erstellt dann eine ca. 200 MByte große Boot-Partition und richtet darin ein ext2-Dateisystem ein. Im verbleibenden Speicherbereich wird eine große Partition eingerichtet, die als Physical Volume für eine Volume Group mit dem Namen *ubuntu* dient. Innerhalb dieser VG sieht das Installationsprogramm zwei Logical Volumes vor, die die Swap-Partition und die Systempartition aufnehmen.

Diese »LVM-Standardinstallation« funktioniert prinzipiell gut, bietet aber keinerlei Konfigurationsmöglichkeiten. Alle Versuche, mit der Option Etwas Anderes ein von einer früheren Installation bereits vorhandenes LVM-System zu modifizieren bzw. zu erweitern oder LVM manuell einzurichten, scheitern kläglich. Es ist nicht einmal möglich, die Reste einer zuvor durchgeführten LVM-Installation aufzuräumen und neu zu starten.

Das Ubuntu-Installationsprogramm kann in dieser Hinsicht nicht mit Fedora oder openSUSE mithalten. Wenn Sie eine individuelle LVM-Konfiguration wünschen, müssen Sie das textbasierte Installationsprogramm von Ubuntu Server oder des Netinstall-Images verwenden.

EFI-Installationen

Ubuntu unterstützt Installationen im EFI-Modus ausgezeichnet und kommt seit Ubuntu 12.10 auch mit *UEFI Secure Boot* zurecht. Auf einer leeren Festplatte oder SSD richtet Ubuntu selbstständig eine ca. 20 MByte große EFI-Partition ein und bindet diese unter `/boot/efi` in den Ubuntu-Verzeichnisbaum ein. Der Automatismus funktioniert gut, einzig die Sparsamkeit bei der Größe der Partition stimmt bedenklich: Während Linux-Distributionen in der EFI-Partition wenig Platz brauchen, sieht das unter Windows ganz anders aus.

Wenn Sie also vorhaben, später auch Windows zu installieren, sollten Sie die Partitionierung selbst vornehmen und die EFI-Partition lieber 200 MByte groß einrichten. Dazu sind Partitionsgrösse = 200 (in MByte) und Benutzen als = EFI-Boot-Partition geeignete Einstellungen.

Wenn auf der Festplatte bereits Betriebssysteme installiert sind und Sie eine manuelle Partitionierung durchführen (Etwas Anderes), müssen Sie die EFI-Partition als solche markieren. Dazu klicken Sie zuerst die schon existierende EFI-Partition und dann den Button Ändern an und stellen dann Benutzen als = EFI-Boot-Partition ein.

Zeitzone

Diverse noch ausstehende Einstellungen können Sie parallel zur Installation erledigen. Diese neue Abfolge der Installationsschritte spart Zeit. Als Erstes geben Sie die Zeitzone an, in der Sie sich befinden. Das Installationsprogramm nimmt an, dass die Uhr Ihres Rechners auf die lokale Uhrzeit eingestellt ist. Wenn das nicht der Fall ist, müssen Sie die Uhrzeit nach dem Ende der Installation korrigieren.

Tastatur

Damit sich die Tastatur so verhält, wie Sie es von Windows gewöhnt sind, müssen Sie das Layout Deutsch – Nur Grave- und Acute-Akzenttaste wählen. Das bedeutet, dass das Zeichen ~ direkt eingegeben werden kann, die Zeichen ` und ´ aber zur Komposition von Buchstaben aus Fremdsprachen dienen. ´, e ergibt daher é.

Benutzerdaten

Im nächsten Schritt geben Sie den Benutzernamen und das Passwort für den ersten Ubuntu-Nutzer an. Weitere Nutzer können Sie bei Bedarf später im laufenden Betrieb einrichten. Im Gegensatz zu anderen Linux-Installationsprogrammen müssen Sie kein `root`-Passwort angeben: Administrative Arbeiten werden unter Ubuntu von einem gewöhnlichen Benutzer mit `sudo` durchgeführt.

Sie haben an dieser Stelle die Wahl zwischen drei Sicherheitsoptionen: Automatisch anmelden bewirkt, dass Sie beim Rechnerstart automatisch eingeloggt werden. Das ist bequem, aber natürlich ein Sicherheitsmangel. Passwort zum Anmelden abfragen ist die Standardeinstellung und erfordert nach dem Rechnerstart einen gewöhnlichen Login.

Mehr Sicherheit durch Verschlüsselung?

Noch mehr Sicherheit verspricht die Option Meine persönlichen Dateien verschlüsseln. Damit wird Ihr gesamtes persönliches Verzeichnis verschlüsselt. Ein Zugriff auf die Daten ist nur nach einem Login möglich. Dieses Ubuntu-spezifische Verschlüsselungsverfahren ist aber auch mit Nachteilen verbunden! Insbesondere ist es sehr schwierig, die eigenen Daten zu retten, wenn sich das System aus irgendeinem Grund nicht mehr starten lässt. Ich rate Ihnen deswegen entschieden von dieser Option ab!

Verwenden Sie gegebenenfalls lieber die Option Die neue Ubuntu-Installation zur Sicherheit verschlüsseln im Dialog Installationsart (siehe Abbildung 3.20): Dann wird das gesamte LVM-System auf die gleiche Art und Weise wie bei den meisten anderen Distributionen verschlüsselt. Das vereinfacht die Wartung und verbessert die Chancen, dass sich Ihre Daten bei Problemen retten lassen.

Sprachpakete

Auf der CD fehlen aus Platzgründen deutsche Sprachpakete. Sofern es dem Installationsprogramm gelingt, eine Internetverbindung herzustellen, lädt es die fehlenden Pakete nun aus dem Internet herunter und installiert sie.

USB-Stick-Installation

Grundsätzlich bestehen zwei Möglichkeiten, Ubuntu auf einen USB-Stick oder auf eine externe Festplatte zu installieren: Entweder führen Sie eine gewöhnliche Installation in eine Partition eines USB-Datenträgers durch, oder Sie verwenden den Startmedienersteller (`usb-creator-gtk`, siehe Abbildung 3.21). Dieses Programm muss auf die Installations-CD oder eine entsprechende ISO-Datei zugreifen können.

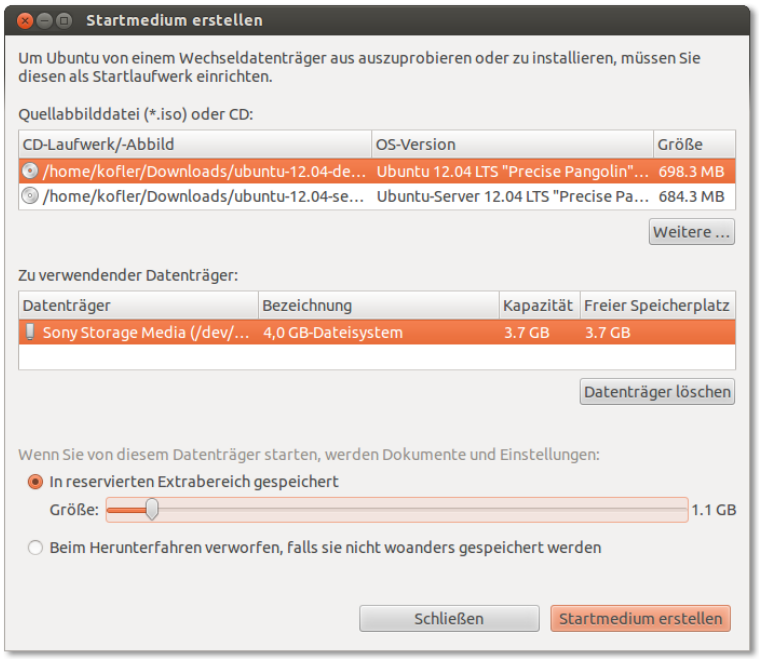


Abbildung 3.21 Ubuntu auf einen USB-Stick übertragen

Der externe Datenträger muss mindestens 2 GByte groß sein und muss in der Regel neu formatiert werden. Sie verlieren also alle darauf enthaltenen Daten! Sie können auf dem Datenträger einen reservierten Bereich vorsehen, um darin Systemeinstellungen und persönliche Daten zu speichern. Wenn Sie das nicht wollen, wählen Sie die Option BEIM HERUNTERFAHREN VERWORFEN, FALLS SIE NICHT WOANDERS GESPEICHERT WERDEN.

`usb-creator-gtk` führt keine echte Installation durch, sondern kopiert lediglich den Inhalt der Live-CD auf den USB-Stick. Im Vergleich zu einer richtigen Installation ist das Live-System nur bedingt modifizierbar und läuft langsamer. Es eignet sich als »Ubuntu zum Mitnehmen« oder zur Durchführung einer richtigen Ubuntu-Installation auf einem Computer ohne CD/DVD-Laufwerk, aber nicht für den Dauerbetrieb.

Erste Schritte

Updates durchführen

Um alle installierten Ubuntu-Pakete auf den aktuellsten Stand zu bringen, führen Sie in einem Terminal-Fenster das folgende Kommando aus:

```
user$  sudo apt-get update
user$  sudo apt-get dist-upgrade
```

ubuntu-restricted-extras

Das Paket `ubuntu-restricted-extras` macht Ihr Ubuntu-System multimediatauglich. Installiert werden unter anderem das Adobe-Flash-Plugin, Codecs für alle möglichen Audio- und Video-Formate inklusive MP3, die kostenlosen Microsoft-Web-Fonts etc.

```
user$  sudo apt-get install ubuntu-restricted-extras
```

Hardware-Treiber installieren

Ubuntu stellt für ATI- und NVIDIA-Grafikkarten sowie für einige WLAN-Adapter proprietäre Hardware-Treiber zur Verfügung. Um diese zu installieren, öffnen Sie im Startmenü das Programm SOFTWARE & AKTUALISIERUNG. Die für Ihr System passenden Treiber werden im Dialogblatt ZUSÄTZLICHE TREIBER aufgelistet. Zur Aktivierung müssen Sie den Rechner neu starten.

Werbung im Startmenü abstellen

Ubuntu darf für sich in Anspruch nehmen, das weltweit einzige Betriebssystem zu sein, das Werbung im Startmenü anzeigt. Abhilfe: Öffnen Sie im Systemmenü ganz rechts in der Menüleiste die Systemeinstellungen und dort das Modul PRIVATSPHÄRE. Dort deaktivieren Sie die Option AUCH ONLINE-SUCHERGEBNISSE VERARBEITEN.

Position der Fenster-Buttons ändern

Ubuntu zeigt wie OS X die Fenster-Buttons an der linken Seite an. Sollte Sie das irritieren, können Sie die Buttons unkompliziert auf die rechte Seite bringen. Das folgende Kommando gilt für Ubuntu-Versionen bis 12.10:

```
user$  gconftool-2 --set /apps/metacity/general/button_layout \
         --type string ':minimize,maximize,close'
```

Ab 13.04 lautet das korrekte Kommando hingegen:

```
user$  gsettings set org.gnome.desktop.wm.preferences \
         button-layout ':minimize,maximize,close'
```

Kein Zentralmenü

Standardmäßig zeigt Ubuntu das Menü der Programme in der Menüleiste des Desktops ganz oben auf dem Bildschirm an, und auch das nur, wenn Sie die Maus dorthin bewegen oder die Alt-Taste drücken. Auf kleinen Bildschirmen spart das Platz, vor allem, wenn Sie die Programme ohnedies alle maximiert ausführen. Auf großen Bildschirmen ist das Verhalten hingegen unpraktisch. Abhilfe:

```
user$  sudo apt-get remove indicator-appmenu
```

Anschließend loggen Sie sich aus und wieder ein.

Richtige Scrollbalken

Bei den meisten Ubuntu-Programmen kommen schmale Bildlaufleisten zum Einsatz. Sie sehen elegant aus und sparen Platz, sind mit der Maus aber weniger komfortabel zu bedienen als herkömmliche Bildlaufleisten. Wenn Ihnen die herkömmlichen Scrollbalken sympathischer sind, führen Sie eines der beiden folgenden Kommandos aus. Auch diese Änderung wird erst mit dem nächsten Login wirksam.

```
root#  sudo apt-get remove liboverlay-scrollbar*     (bis Ubuntu 12.10)
root#  sudo apt-get remove liboverlay-scrollbar*     (ab Ubuntu 13.04)
```

3.6 Ubuntu Server

Ubuntu Server ist eine für den Server-Betrieb optimierte Variante von Ubuntu. Vor allem die LTS-Versionen von Ubuntu Server zählen wegen des langen Support-Zeitraums von fünf Jahren mittlerweile neben CentOS und Debian zu den beliebtesten Linux-Server-Systemen im nicht-kommerziellen Bereich. Canonical versucht Ubuntu Server aber auch im kommerziellen Segment zu etablieren und bietet für zahlungswillige Kunden mit *Landscape* ein optionales Werkzeug zur Überwachung mehrerer Server-Installationen.

http://www.canonical.com/enterprise-services/ubuntu-advantage/landscape

Hinter den Kulissen unterscheidet sich Ubuntu Server eigentlich nicht vom gewöhnlichen Ubuntu, d. h., es verwendet dieselben Pakete und Paketquellen. Die Besonderheit von Ubuntu Server besteht vielmehr darin, dass es speziell für den Server-Einsatz ein eigenes, textbasiertes Installationsprogramm gibt. Im Unterschied zu dem im vorigen Abschnitt vorgestellten Desktop-Installationsprogramm kommt es gut mit LVM und Software-RAID zurecht.

Es installiert ein Grundsystem für den Server-Einsatz ohne grafische Benutzeroberfläche: Da viele Server-Systeme ohnedies via SSH administriert werden, ist eine Benutzeroberfläche zumeist nicht notwendig. Grundsätzlich ist es aber auch möglich, eine gewöhnliche Ubuntu-Installation für den Server-Einsatz zu verwenden und die entsprechenden Server-Pakete einfach nachträglich zu installieren.

Ubuntu Server installieren

Installationsmedien

Auf der Website *http://www.ubuntu.com/download/server* finden Sie ISO-Images zur Ubuntu-Server-Installation. In aller Regel sollten Sie sich für die 64-Bit-Variante der letzten LTS-Version entscheiden. Sie finden auf der Download-Seite auch Installationsmedien für Nicht-LTS-Versionen. Diese sind zwar aktueller, werden aber nur für neun Monate mit Updates versorgt. Für den Server-Einsatz ist das zu wenig!

Installation starten

Nachdem Sie die ISO-Datei auf eine CD gebrannt oder auf einen USB-Stick übertragen haben, starten Sie Ihren Rechner damit neu. Falls Ubuntu Probleme mit der richtigen Hardware-Erkennung hat, führt F1 zu einigen Hilfeseiten. Diese beschreiben unter anderem, wie Sie durch die zusätzliche Angabe von Optionen Hardware-Probleme umgehen können. Wenn Ubuntu beispielsweise Ihren SCSI-Controller nicht erkennt, müssen Sie eine entsprechende Option angeben. Um die Installation mit solchen Optionen zu starten, geben Sie ein Kommando wie im folgenden Beispiel an:

```
linux noapic nolapic
```

Grund-einstellungen

In den ersten Dialogen des Installationsprogramms wählen Sie die Sprache und Ihr Land oder Gebiet aus. Diese Information wird zur Auswahl des nächstgelegenen Mirror-Servers verwendet. Das Installationsprogramm kann das Tastaturlayout selbst erkennen. Wesentlich schneller ist es aber, das gewünschte Layout manuell einzustellen (wählen Sie Deutschland – Nur Grave- und Acute-Akzentzeichen).

Nach der Hardware-Erkennung versucht das Installationsprogramm, das Netzwerk automatisch zu konfigurieren. Das gelingt nur, wenn sich im lokalen Netzwerk ein Router bzw. DHCP-Server befindet. Andernfalls haben Sie die Wahl, auf die Netzwerkkonfiguration vorerst zu verzichten oder die wichtigsten Parameter manuell einzugeben. Dazu müssen Sie wissen, welche IP-Adresse Ihr Rechner haben soll und welche Netzwerkmaske gelten soll. Außerdem müssen Sie die IP-Adressen des Internet-Gateways und des DNS-Servers angeben.

Benutzerdaten

Im nächsten Schritt geben Sie den Namen und das Passwort eines Ubuntu-Benutzers an. Weitere Benutzer können Sie später im laufenden Betrieb hinzufügen. Das Installationsprogramm fragt nun, ob es Ihr persönliches Verzeichnis verschlüsseln soll. Für den Server-Einsatz ist dies nicht zweckmäßig.

Partitionierung der Festplatte

Die verschachtelten Dialoge zur Partitionierung der Festplatten sind leider sehr unübersichtlich. Im ersten Dialog stellt das Installationsprogramm verschiedene Kommandos zur Auswahl. Je nachdem, wie viele Festplatten Ihr Rechner hat und welche Partitionen sich darauf bereits befinden, kann das Auswahlmenü zusätzliche Kommandos aufweisen:

- Geführt – Partition n verkleinern und den freigewordenen Speicher nutzen: Diese Option erscheint nur, wenn (Windows-)Partitionen auf der Festplatte existieren. Mit dem Kommando können Sie deren Größe reduzieren, um so Platz für Linux-Partitionen zu machen.
- Geführt – vollständige Festplatte verwenden: Das Installationsprogramm erstellt einen Vorschlag, wie die gesamte Festplatte für Linux-Partitionen genutzt werden kann. Diesen Vorschlag können Sie bestätigen (Partitionierung beenden und Änderungen speichern) oder abbrechen (Änderungen rückgängig machen). Vorsicht: Mit dieser Option verlieren Sie alle bisher auf der Festplatte gespeicherten Daten!
- Geführt – den grössten freien Speicherbereich benutzen: Das Installationsprogramm erstellt einen Vorschlag, wie der freie Platz auf der Festplatte für Linux-Partitionen genutzt werden soll. Sie müssen diesen Vorschlag anschließend bestätigen. Wenn Sie das nicht tun (Antwort Nein), gelangen Sie in einen Dialog mit der Partitionstabelle (siehe Abbildung 3.22). Dort können Sie die Partitionen manuell verändern oder alle Änderungen rückgängig machen. Diese Option ist nur sinnvoll, wenn es auf der Festplatte partitionsfreien Platz gibt.

- GEFÜHRT – GESAMTE PLATTE VERWENDEN UND LVM EINRICHTEN: Auch mit dieser Option werden alle vorhandenen Daten der Festplatte gelöscht. Anschließend richtet das Installationsprogramm ein LVM-System ein.
- GEFÜHRT – GESAMTE PLATTE MIT VERSCHLÜSSELTEM LVM: Wie oben, allerdings wird das gesamte Dateisystem zusätzlich verschlüsselt. Für den Server-Einsatz ist diese Option ungeeignet, weil das Verschlüsselungspasswort bei jedem Start manuell eingegeben werden muss und die Verschlüsselung den Festplattenzugriff spürbar verlangsamt.
- MANUELL: Mit diesem Punkt können Sie neue Linux-Partitionen für die Ubuntu-Installation manuell anlegen.

Automatische Partitionierung

Bei allen Partitionierungsvarianten, deren Menüpunkt mit GEFÜHRT beginnt, überlassen Sie die Partitionierung dem Installationsprogramm. Dieses erzeugt eine kleine Swap-Partition und eine Systempartition, die den Rest der Festplatte füllt. Dieses Setup ist freilich nur selten optimal.

Manuelle Partitionierung

Das Menükommando MANUELL führt in einen neuen Dialog, der einige Menükommandos sowie eine Liste aller vorhandenen Festplatten bzw. Festplattenpartitionen enthält (siehe Abbildung 3.22).

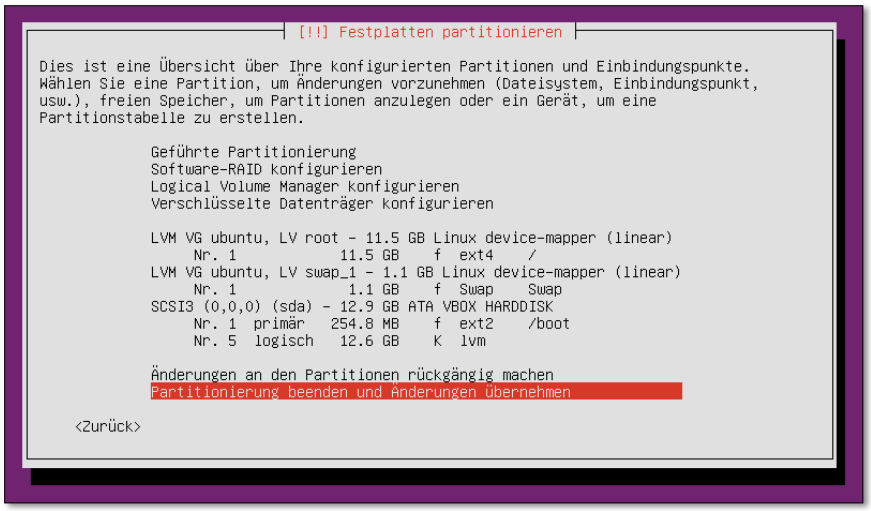


Abbildung 3.22 Die Partitionstabelle

In der Partitionstabelle wählen Sie den Eintrag FREIER SPEICHER aus. (Wenn es keinen freien Speicher gibt, müssen Sie eine vorhandene Partition löschen oder ändern.) Im nächsten Dialog entscheiden Sie sich für die Option EINE NEUE PARTITION ERSTELLEN. Anschließend geben Sie die gewünschte Partitionsgröße an und wählen den Partitionstyp. (Die erste Partition der Festplatte muss eine primäre Partition sein.

Oft befindet sich darin Windows. Für alle weiteren Partitionen wählen Sie LOGISCH.) Das Installationsprogramm zeigt nun eine Zusammenfassung der Einstellungen für diese Partition an (siehe Abbildung 3.23).

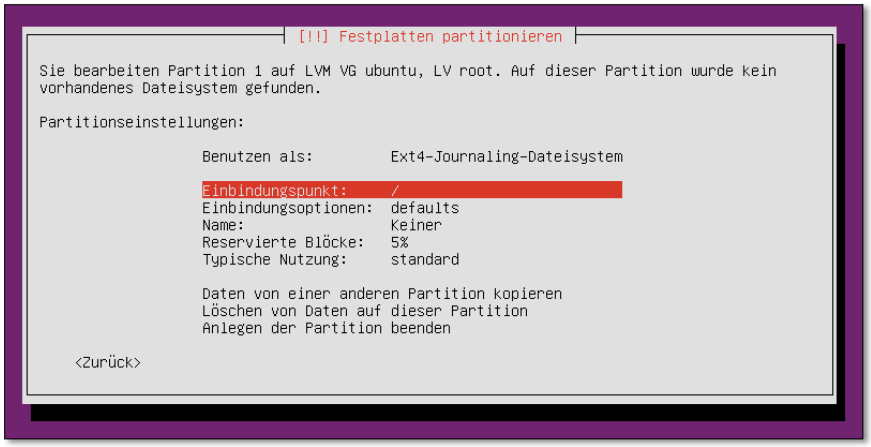


Abbildung 3.23 Die Einstellungen für die neue Partition

Für die Systempartition können Sie zumeist alle Einstellungen beibehalten und müssen diese nur noch durch ANLEGEN DER PARTITION BEENDEN bestätigen. Damit gelangen Sie zurück in die Partitionstabelle, die nun eine weitere Partition enthält.

Beim Anlegen der Swap-Partition müssen Sie in den Partitionseinstellungen eine Änderung vornehmen: Den Punkt BENUTZEN ALS stellen Sie auf AUSLAGERUNGSDATEI (SWAP). Auch beim Anlegen zusätzlicher Partitionen (`/home`, `/tmp` etc.) müssen Sie die Partitionseinstellungen ändern: Diesmal wählen Sie den Punkt EINHÄNGEPUNKT aus und stellen dann den gewünschten Verzeichnisnamen für die Partition ein.

Nach der Definition aller Partitionen führen Sie in der Partitionstabelle das Kommando PARTITIONIERUNG BEENDEN UND ÄNDERUNGEN ÜBERNEHMEN aus. Nach einer weiteren Rückfrage werden die Änderungen an der Festplatte tatsächlich durchgeführt. Anschließend kopiert das Installationsprogramm unzählige Dateien in die soeben angelegte Systempartition. Das dauert einige Minuten.

Automatische Updates

Wenn Sie möchten, installiert Ubuntu im laufenden Betrieb einmal täglich automatisch neue Updates, sobald diese verfügbar werden. Das ist praktisch, wenn Sie nicht regelmäßig kontrollieren möchten, ob es neue Sicherheits-Updates gibt.

Paketauswahl

Außer den Grundpaketen kann das Installationsprogramm auch gleich diverse Server-Pakete installieren (siehe Abbildung 3.24). Selbst wähle ich an dieser Stelle normalerweise nur den OpenSSH-Server aus und installiere die restlichen Server-Dienste dann nach und nach selbst. Mit der Installation ist es ja normalerweise nicht getan – die Server-Programme müssen ja auch konfiguriert werden.

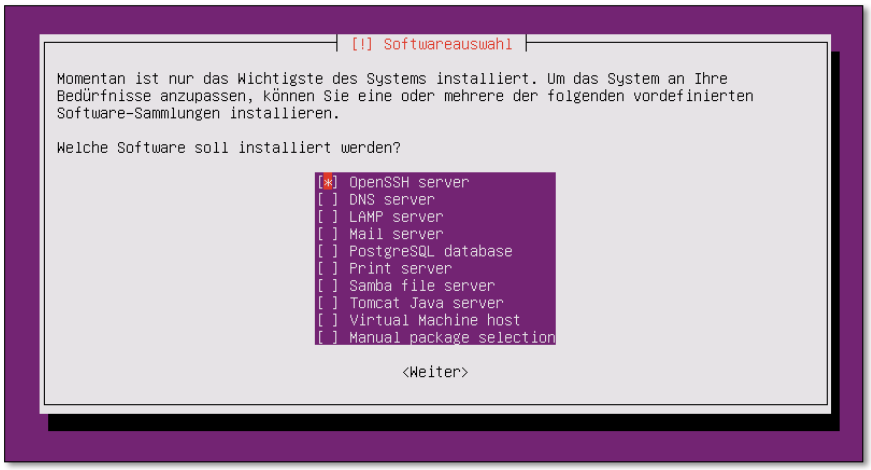


Abbildung 3.24 Paketauswahl

Bootloader

Bei EFI-Rechnern wird GRUB in der EFI-Partition eingerichtet. Bei BIOS-Rechnern erscheint eine Rückfrage, ob Sie GRUB in den Startsektor (MBR) der ersten Festplatte installieren möchten. Diesen Vorschlag bestätigen Sie in der Regel einfach durch ↵.

Kapitel 4
Linux-Schnelleinstieg

Dieses Kapitel hilft Ihnen bei den ersten Schritten unter Linux: einloggen, Programme ausführen, auf Dateien und Datenträger zugreifen, ausloggen bzw. Rechner herunterfahren etc. Das Kapitel vermittelt ein minimales Grundlagenwissen über die Dateiverwaltung von Linux und verrät, wo Sie im installierten System bzw. im Internet nach Online-Dokumentation suchen können.

Ein Grundproblem bei einer allgemeinen Beschreibung von Linux besteht darin, dass nahezu jede Funktion frei konfigurierbar ist. Daher sieht beispielsweise das Startmenü jeder Distribution ein wenig anders aus. Es kann also sein, dass eine bestimmte Tasten- oder Mauskombination unter Red Hat eine andere Reaktion hervorruft als unter SUSE. Aus diesem Grund gibt es in diesem Kapitel viele Formulierungen mit *meistens*, *gewöhnlich* etc. Das ist leider nicht zu ändern.

4.1 Linux starten und beenden

Um Linux zu starten, müssen Sie Ihren Rechner neu starten. Beim Neustart geben Sie in einem Menü an, dass Sie Linux und nicht Windows ausführen möchten. Es ist nicht möglich, Linux von Windows aus zu starten – es sei denn, Sie verwenden unter Windows ein Programm wie VirtualBox und führen Linux in einer virtuellen Umgebung aus.

Der Linux-Bootprozess dauert je nach Hardware ca. 15 Sekunden. Bei manchen Distributionen erscheint während dieser Zeit ein Fortschrittsbalken. Andere Distributionen zeigen hingegen unzählige Detailinformationen über den Systemstart an. Diese Informationen sind aber nur dann von Interesse, wenn irgendetwas nicht funktionieren sollte.

Login

Im Normalfall endet der Bootprozess mit dem Erscheinen einer grafischen Login-Box (siehe Abbildung 4.1). Dort melden Sie sich mit Ihrem Benutzernamen und dem Passwort an. Anschließend erscheint Ihre Arbeitsumgebung im Standard-Desktop-System Ihrer Distribution, üblicherweise Gnome, Unity oder KDE. Eine Einführung in diese Desktop-Systeme folgt in den beiden nächsten Kapiteln.

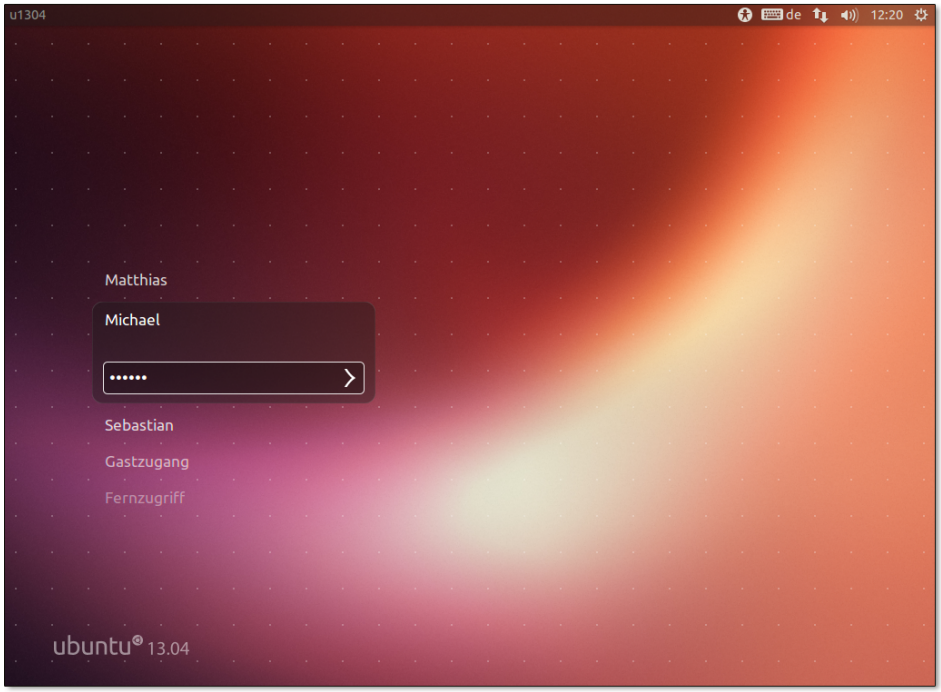


Abbildung 4.1 Login-Bildschirm bei Ubuntu

Melden Sie sich aber nicht als `root` an, sondern verwenden Sie einen gewöhnlichen Login! Der Benutzer `root` hat uneingeschränkte Rechte. Es ist unter Linux nicht üblich, mit `root`-Rechten zu arbeiten. Stattdessen werden für administrative Aufgaben nur einzelne Programme mit `root`-Rechten ausgeführt, wobei Sie diesen Vorgang durch die Eingabe des `root`-Passworts bzw. Ihres eigenen Passworts (Ubuntu) bestätigen müssen. Die Veränderung des Passworts für `root` und das Einrichten neuer Benutzer wird in Abschnitt 21.4 beschrieben.

Sofern Sie mehrere Desktop-Systeme parallel installiert haben (also Gnome *und* KDE), können Sie beim Login den gewünschten Desktop auswählen. Bei einigen Distributionen haben Sie beim Login auch die Möglichkeit, das Tastaturlayout und die Sprache einzustellen.

Auto-Login – bequem oder sicher?

Linux kann so konfiguriert werden, dass nach dem Rechnerstart ein automatischer Login erfolgt. Das ist zwar bequem, aber sicherheitstechnisch nicht optimal. Tipps zur Konfiguration der Auto-Login-Funktion finden Sie in Abschnitt 24.2.

Logout

Die KDE- bzw. Gnome-Menüs bzw. das Panel sehen jeweils ein Kommando zum Logout vor. Die genaue Bezeichnung des Menükommandos variiert je nach Distribution und lautet z. B. System • Benutzer abmelden. Damit werden sämtliche auf dem Desktop laufenden Programme beendet. Sichern Sie vorher alle noch offenen Dateien! Der Logout führt zurück zum Login-Bildschirm, in dem Sie sich nun neu einloggen oder den Rechner herunterfahren können.

Benutzerwechsel

Bei den meisten Desktop-Systemen ist für einen Benutzerwechsel kein Logout erforderlich. Stattdessen führen Sie im Systemmenü Benutzer wechseln oder einen vergleichbaren Eintrag aus. Beachten Sie, dass damit zwei Benutzer parallel eingeloggt sind und somit auch beide Benutzer Speicherplatz und CPU-Zeit beanspruchen.

Login und Logout im Textmodus

Viele Funktionen von Linux können auch im Textmodus genutzt werden. Gerade bei Server-Installationen wird manchmal ganz auf das Grafiksystem, also auf das sogenannte X Window System verzichtet. Zum Arbeiten führen Sie den Login in einer Textkonsole durch (siehe auch Kapitel 13). Zum Logout drücken Sie einfach Strg+D oder führen das Kommando `exit` aus.

Linux beenden (Shutdown)

Die grafischen Benutzeroberflächen sehen Menükommandos zum Herunterfahren des Rechners vor oder bieten eine entsprechende Option im Abmelde-Dialog. Im Textmodus erfolgt ein ordnungsgemäßes Herunterfahren des Systems mit dem Kommando `shutdown -h now`. Dieses Kommando darf allerdings nur von `root` ausgeführt werden.

Auf vielen Linux-Systemen gibt es eine bequemere Alternative zum `shutdown`-Kommando: Drücken Sie im Textmodus einfach die Tasten Strg+Alt+Entf. Falls Sie unter X arbeiten, müssen Sie vorher mit Strg+Alt+F2 in eine Textkonsole wechseln.

Sicherer Neustart ohne Root-Rechte

Wenn Linux auf Strg+Alt+Entf nicht reagiert und Sie kein `root`-Passwort besitzen, den Rechner aber dennoch neu starten müssen, sollten Sie vorher zumindest das Kommando `sync` ausführen. Damit werden alle gepufferten Schreibzugriffe auf die Festplatte ausgeführt. Unmittelbar danach schalten Sie Ihren Rechner aus. Das ist allerdings nur eine Notlösung zur Schadensminimierung.

4.2 Tastatur, Maus und Zwischenablage

Wichtige Tastenkürzel

Welche Tastenkürzel zur Verfügung stehen, hängt davon ab, ob Sie im Grafikmodus oder in einer Textkonsole arbeiten. Hier setze ich voraus, dass Sie den Grafikmodus nutzen. Die Tastenkürzel werden in drei Programmebenen definiert:

- Das X Window System ist für die elementaren Funktionen des Grafiksystems verantwortlich. Das X Window System stellt nur relativ wenige Tastenkürzel zur Verfügung (siehe Tabelle 4.1).
- Desktop-Systeme wie Gnome, KDE, Unity, Xfce oder LXDE bauen auf X auf. Auch durch sie werden einige Tastenkürzel definiert. Erfreulicherweise hat hier in den letzten Jahren eine Vereinheitlichung stattgefunden, sodass zumindest für die wichtigsten Operationen dieselben Tastenkürzel gelten (siehe Tabelle 4.2).
- Schließlich hängen die verfügbaren Tastenkürzel natürlich vom individuellen Programm ab, das gerade läuft. Je nachdem, ob Sie mit Firefox im Web surfen, mit LibreOffice einen Brief schreiben oder im Editor Emacs Programmcode ändern – in jedem Fall gelten andere Tastenkürzel, die in diesem Abschnitt natürlich nicht beschrieben werden können.

  Bei Programmen mit grafischer Benutzeroberfläche gelten für wichtige Operationen dieselben Kürzel wie unter Windows. Das betrifft beispielsweise das Kopieren von Text in die Zwischenablage mit Strg+C, das Einfügen des kopierten Texts mit Strg+V oder das Speichern einer Datei mit Strg+S.

  Für viele textorientierte Kommandos gelten andere Konventionen, die sich im Verlauf der Unix/Linux-Geschichte etabliert haben. Wichtige Tastenkürzel für derartige Programme sind in Abschnitt 13.1 zusammengefasst.

Leider gibt es keine Garantie, dass die hier zusammengefassten Tastenkürzel wirklich bei jeder Distribution gelten. Alle Tastenkürzel sind konfigurierbar, und manche Distributoren weichen von den üblichen Konventionen ab. Beispielsweise verwenden Fedora und Red Hat nicht die siebte, sondern die erste Konsole für den Grafikmodus. Die Tastenkombination Strg+Alt+← ist auf immer mehr Distributionen standardmäßig deaktiviert oder wird erst bei zweimaligem Drücken wirksam.

Kürzel	Bedeutung
Strg+Alt+←	beendet das Grafiksystem (das X Window System) gewaltsam. Unter SUSE muss diese Tastenkombination zweimal gedrückt werden. Bei einigen Distributionen ist die Tastenkombination auch ganz deaktiviert.
Strg+Alt+Fn	wechselt vom Grafiksystem in die Konsole *n*.
Strg+Alt+Fn	wechselt vom Textmodus in die Konsole *n*. Bei den meisten Distributionen führt Alt+F7 zurück in den Grafikmodus. Bei Fedora drücken Sie Alt+F1.

Tabelle 4.1 Tastenkürzel unter X

Kürzel	Bedeutung
Alt + ⇆	wechselt das aktive Fenster.
Alt + F1 oder ⊞	zeigt das Startmenü an.
Alt + F2	startet ein Programm.
Alt + F3	zeigt das Fenstermenü des aktuellen Fensters.
Alt + F4	schließt das Fenster bzw. beendet das Programm.

Tabelle 4.2 Wichtige Tastenkürzel des Desktops (Gnome, KDE, Unity)

Verwendung der Maus

Linux orientiert sich tendenziell immer mehr an den Konventionen der Windows- bzw. Mac-OS-Welt. Dennoch existieren je nach Desktop bzw. je nachdem, welches Programm Sie gerade einsetzen, einige Besonderheiten, die in diesem Abschnitt zusammengefasst sind.

Einfach- oder Doppelklick

Bei den meisten Desktop-Systemen ist wie unter Windows für viele Operationen – etwa das Öffnen einer Datei – ein Doppelklick erforderlich. In KDE werden dagegen viele Mausoperationen standardmäßig durch einen einfachen Mausklick ausgeführt. Wie Sie auch in KDE den Doppelklickmodus aktivieren, ist in Abschnitt 6 beschrieben.

Texte mit der Maus kopieren und einfügen

In fast allen Linux-Programmen können Sie mit der Maus Textausschnitte kopieren und an einer anderen Stelle oder in einem anderen Programm wieder einfügen. Zum Markieren von Textausschnitten bewegen Sie die Maus einfach mit gedrückter linker Maustaste über den Text. Der so markierte Text wird dabei automatisch in einen Puffer kopiert. Sobald Sie die mittlere Maustaste drücken, wird der Text dort eingefügt, wo der aktive Eingabecursor steht. Bei einzelnen Programmen können Sie auch die rechte Maustaste zum Einfügen verwenden, was besonders dann praktisch ist, wenn Sie eine Maus mit nur zwei Tasten verwenden.

Das Markieren und Kopieren erfolgt also allein mit der Maus, ohne Tastatur! Wenn Sie sich einmal an diese Methode gewöhnt haben, werden Sie sich immer wieder fragen, warum das unter Windows oder OS X nicht ebenso einfach funktioniert.

Eingabefokus

Bei manchen alten Programmen kann bei Dialogen nur dann Text in Eingabefelder eingegeben werden, wenn sich die Maus über diesem Feld befindet. Der Eingabefokus hängt also nicht nur davon ab, welches Programm gerade aktiv ist, sondern auch davon, wo sich die Maus befindet.

Dieses Verhalten kann bei einigen Desktop-Systemen auch für Fenster aktiviert werden (*focus follows mouse*): Dann ist es nicht mehr erforderlich, ein Fenster

anzuklicken, um darin Eingaben durchzuführen. Es reicht, die Maus richtig zu positionieren. Allerdings führt eine unbeabsichtigte Bewegung der Maus nun oft dazu, dass Texteingaben an das falsche Fenster oder Programm weitergeleitet werden. Aus diesem Grund ist der Modus *focus follows mouse* nicht gebräuchlich.

Maussteuerung per Tastatur

Wenn die Maus nicht funktioniert, können Sie den Mauszeiger bei einigen Distributionen zur Not auch mit der Tastatur steuern (siehe Tabelle 4.3). Dazu müssen Sie mit ⇧+Strg+Num einen speziellen Tastaturmodus aktivieren, der eine Tastatur mit eigenem Ziffernblock voraussetzt.

Kürzel	Bedeutung
4, 6	Maus nach links bzw. rechts bewegen
2, 8	Maus nach unten bzw. oben bewegen
5	linke Maustaste kurz drücken
+	Doppelklick
0	Maustaste bleibend drücken (5 löst die Taste wieder)
-	auf die rechte Maustaste umschalten (5, + und 0 gelten jetzt für die rechte Maustaste)
*	wieder auf die linke Maustaste umschalten

Tabelle 4.3 Tastenkürzel zur Maussteuerung durch den numerischen Ziffernblock

Zwischenablage

Wie gerade erwähnt wurde, landet jeder mit der Maus markierte Text in einer Art Ad-hoc-Zwischenablage. Solange die Markierung besteht, kann der markierte Text mit der mittleren Maustaste in ein anderes Programm eingefügt werden. Der Vorteil dieses Verfahrens besteht darin, dass es ohne Tastatur funktioniert. Das Verfahren hat aber auch Nachteile: Durch jede neue Markierung wird die bisherige Markierung (und damit die Ad-hoc-Zwischenablage) gelöscht, was oft lästig ist. Außerdem hat nicht jede Maus drei Tasten.

Deswegen bieten viele Programme, z. B. alle KDE- und Gnome-Programme sowie Firefox und LibreOffice, zusätzlich die Möglichkeit, wie unter Windows mit Strg+C den markierten Text in eine eigene Zwischenablage zu kopieren, die unabhängig von der aktuellen Markierung ist. Zum Einfügen dieser Zwischenablage verwenden Sie Strg+V.

4.3 Umgang mit Dateien, Zugriff auf externe Datenträger

Das Dateisystem beginnt mit dem Wurzelverzeichnis `/`. Auch wenn es mehrere Festplatten bzw. Festplattenpartitionen sowie CD- und DVD-Laufwerke gibt, sind alle Daten in den Verzeichnisbaum eingebunden. Beispielsweise kann der Inhalt eines CD-Laufwerks üblicherweise unter dem Verzeichnis `/media/cdrom` gelesen werden. Aus diesem Grund besteht unter Linux keine Notwendigkeit für die Laufwerksbuchstaben `A:`, `C:` etc., die unter Windows üblich sind.

Linux unterscheidet bei Datei- und Verzeichnisnamen zwischen Groß- und Kleinbuchstaben. `readme`, `Readme` und `README` bezeichnen drei verschiedene Dateien! Dateinamen dürfen bis zu 255 Zeichen lang sein.

Heimatverzeichnis

Nach dem Einloggen befinden Sie sich automatisch in einem Verzeichnis, das Ihnen gehört. Dieses Verzeichnis wird Heimat- oder Home-Verzeichnis genannt. Andere Benutzer dürfen diese Dateien weder verändern noch löschen, aber in der Regel lesen. Das Heimatverzeichnis wird mit der Tilde `~` abgekürzt. Bei gewöhnlichen Linux-Anwendern befindet sich das Heimatverzeichnis in `/home/name`. Bei `root` lautet der Speicherort dagegen `/root`.

CDs, DVDs, USB-Sticks

Im Idealfall funktioniert der Zugriff auf externe Datenträger weitgehend automatisch: Nach dem Einlegen bzw. Anstecken eines Datenträgers erscheint auf dem Desktop automatisch ein entsprechendes Icon oder ein Fenster des Datei-Managers.

Wenn das automatische Einbinden externer Datenträger nicht funktioniert bzw. wenn Sie in einer Textkonsole arbeiten, müssen Sie manuell das Kommando `mount` ausführen – und später `umount`, um den Datenträger wieder zu lösen. Die Vorgehensweise wird ausführlich in Kapitel 25 beschrieben.

Melden Sie USB-Sticks und externe Festplatten richtig ab!

Bevor Sie einen Datenträger mit Schreibzugriff entfernen bzw. das Kabel lösen, müssen Sie ihn explizit abmelden. Die Details hängen vom Desktop-System bzw. von der Distribution ab. In der Regel klicken Sie das Icon an und führen ein Kommando in der Art Datenträger lösen oder Datenträger sicher entfernen aus. Wenn Sie das vergessen, riskieren Sie ein inkonsistentes Dateisystem auf dem Datenträger und Datenverluste!

df

Mit dem Kommando `df` stellen Sie fest, welche Partitionen momentan in das Dateisystem eingebunden sind und wie viel Speicher dort noch frei ist. Die Option `-h` bewirkt, dass als Maßeinheit nicht starr kByte verwendet wird, sondern eine zur Größe der Partition passende Einheit (MByte, GByte etc.). Im folgenden Beispiel ist außer der Systempartition `/` noch die Datenpartition `/myhome` in das Dateisystem ein-

gebunden. `df` zählt außerdem einige virtuelle Dateisysteme auf, die nur zur internen Verwaltung von Linux relevant sind. Lassen Sie sich davon nicht irritieren!

```
user$  df -h
Dateisystem            Größe Benut  Verf Ben% Eingehängt auf
/dev/sdb6              9,2G  4,0G  4,8G  46% /
/dev/sdb5               14G  6,9G  6,2G  53% /myhome
tmpfs                  754M     0  754M   0% /lib/init/rw
varrun                 754M  332K  754M   1% /var/run
...
```

4.4 Dokumentation zu Linux

Zu Linux gibt es nahezu unendlich viel Dokumentation, die teilweise gleich mitgeliefert wird und ansonsten im Internet zu finden ist. Experten können zudem einen Blick in den Quellcode aller Programme werfen. Dieser Abschnitt gibt einen Überblick über die wichtigsten Informationsquellen.

So groß die Menge der Dokumentation ist, so schwierig ist es bisweilen, zu einem spezifischen Problem tatsächlich passende Informationen zu finden. Allzu oft geht der entscheidende Tipp in einer Fülle veralteter Informationen, versions- bzw. distributionsspezifischer Nebensächlichkeiten und wirren Diskussionen unter. Zudem gilt: Wer Englisch beherrscht, ist klar im Vorteil. Egal, ob es sich um die Online-Hilfe zu einem Programm oder um die technische Beschreibung eines Server-Dienstes handelt – deutsche Übersetzungen sind Mangelware und, soweit überhaupt vorhanden, oft unvollständig oder veraltet.

Formate

Der Großteil der Linux-Dokumentation befindet sich in einfachen Textdateien oder in HTML- bzw. PDF-Dokumenten. Vereinzelt werden Sie aber auch auf PostScript-Dateien stoßen. Zum Lesen solcher Dateien verwenden Sie einen PostScript-Viewer, beispielsweise Evince oder Okular. Normalerweise startet ein Doppelklick im Datei-Manager Ihres Desktop-Systems automatisch das richtige Programm.

Unter Umständen ist die Datei komprimiert. Das erkennen Sie an der Dateinamenserweiterung `.gz` oder `.bz2`. Zur Dekompression führen Sie `gunzip datei.gz` bzw. `bunzip2 datei.bz2` aus. Dadurch wird die komprimierte Datei durch eine entkomprimierte Version ersetzt.

Online-Hilfe

Bei fast allen Programmen mit grafischer Benutzeroberfläche führt F1 zur Online-Hilfe. Sollte das nicht funktionieren, stellen Sie sicher, dass die Hilfedateien installiert sind. Bei einigen großen Programmen, wie Gimp oder OpenOffice, befinden sich die umfangreichen Hilfedateien in eigenen Paketen, die manchmal nicht standardmäßig installiert werden.

man und info

Bei vielen textorientierten Kommandos führen `man` *name* oder `info` *name* zu einer genauen Beschreibung und Syntaxreferenz. Weitere Informationen zu `man` und `info` finden Sie in Abschnitt 13.3. `man`- und `info`-Texte können Sie auch in den Hilfesystemen von Gnome und KDE lesen.

Paketdokumentation

Unter Linux werden Programme in Form von Paketen installiert. Ein Paket enthält neben allen für ein Programm erforderlichen Dateien oft auch Dokumentationsdateien. Diese Dokumentation wird je nach Distribution in die folgenden Verzeichnisse installiert:

Debian, Fedora, Red Hat, Ubuntu:	`/usr/share/doc/`*paketname*
SUSE:	`/usr/share/doc/packages/`*paketname*

Was tun Sie, wenn Sie Zusatzdokumentation zu einem bestimmten Kommando suchen, aber nicht wissen, zu welchem Paket das Kommando gehört? Der erste Schritt besteht darin, den genauen Dateinamen des Kommandos festzustellen. Dazu führen Sie `which -a kommando` aus:

```
user$  which -a cp
/bin/cp
```

Im nächsten Schritt ermitteln Sie, zu welchem Paket diese Datei gehört. Die Vorgehensweise hängt davon ab, welches Paketformat Ihre Distribution verwendet (siehe auch Kapitel 22). Das folgende Kommando verrät, dass `cp` ein Teil des Pakets `coreutils` ist:

```
user$  rpm -qf /bin/cp       (Fedora, Red Hat, SUSE)
coreutils-6.4-10
user$   dpkg -S /bin/cp      (Debian, Ubuntu)
coreutils: /bin/cp
```

Linux-Foren und -Wikis im Internet

Im Internet gibt es unzählige Foren, Wikis und sonstige Websites von Linux-Firmen und -Enthusiasten. Eine Aufzählung erscheint hier sinnlos – eine kurze Suche nach *fedora forum* oder *ubuntu wiki* führt unweigerlich zu den richtigen Seiten. Bei distributionsspezifischen Fragen sind Sie im Vorteil, wenn Sie eine populäre Distribution einsetzen: Je größer die Verbreitung einer Distribution ist, desto reger ist der Informationsaustausch in den Foren. Ein leuchtendes Beispiel sind die Foren und Wikis zu Ubuntu.

Newsgroups

Die Bedeutung von Newsgroups zur Diskussion über Linux ist nicht mehr sehr groß. Linux-Einsteiger ziehen Foren und Wikis vor, Entwickler kommunizieren hingegen häufig über Mailing-Listen. Dennoch hilft das Archiv alter News-Beiträge mitunter bei der Lösung von Konfigurations- oder Hardware-Problemen. Die populärste Suchmaschine für Newsgroups ist Google:

http://groups.google.com

Das Linux Documentation Project

Das *Linux Documentation Project* (LDP) hat sich das Ziel gesetzt, eine möglichst umfassende und zentrale Sammlung frei verfügbarer Linux-Dokumentation zu schaffen. Tatsächlich ist die Informationsfülle auf der folgenden Seite beeindruckend:

http://www.tldp.org

Die Mehrzahl der Dokumente ist in einem von drei Formaten erschienen: als HOWTO-Text (grundlagenorientierte Anleitungen), als FAQ-Text (Fragen und Antworten) oder als Guide (Buchform). Beachten Sie aber, dass viele LDP-Texte nicht mehr gewartet werden bzw. veraltet sind. Immer mehr Linux-Projekte bzw. -Websites setzen zur Dokumentation stattdessen Wiki-Systeme ein, bei denen alle Anwender zur Dokumentation beitragen können.

Kerneldokumentation

Eine Menge hardware-spezifische Informationen finden Sie in der Kerneldokumentation. Sie ist Teil des Kernelcodes. Die Dokumentation des gerade aktuellen Linux-Kernels können Sie auch im Internet nachlesen:

http://www.kernel.org/doc/Documentation

RFCs

RFC steht für *Request For Comment*. Dahinter verbergen sich Dokumente, die diverse Protokolle (darunter z. B. TCP, IP, FTP, PPP etc.) im Detail beschreiben. Das etwas merkwürdige Kürzel RFC deutet auf die Entstehungsgeschichte dieser Protokolle hin: Sie wurden im Regelfall nicht durch eine Person, Organisation oder Firma diktiert, sondern sind aus einem oft langwierigen Diskussionsprozess entstanden. Die hier dargestellten Informationen sind sehr technischer Natur. RFCs finden Sie z. B. hier:

http://www.faqs.org/rfcs

TEIL II

Desktop-Nutzung

Kapitel 5
Gnome

Wenn Sie unter Windows oder Mac OS X arbeiten, gibt es *eine* Benutzeroberfläche, die Teil des Betriebssystems ist. Unter Linux ist das anders: Das Betriebssystem ist nur für die Grundfunktionen verantwortlich. Für die Benutzeroberfläche sind darauf aufbauende Programme zuständig. Aus unterschiedlichen Gründen sind im Laufe der Zeit mehrere Desktop-Systeme entstanden. In diesem Kapitel steht Gnome im Vordergrund, die folgenden zwei Kapitel gehen auf KDE, Unity, Xfce und LXDE ein.

Egal, welches Desktop-System Sie einsetzen, die Grundfunktionen sind dieselben. Dazu zählen

- die Darstellung von ein oder zwei Panels mit dem Startmenü, der Taskleiste und anderen Miniprogrammen,
- ein Window Manager, der für die Verwaltung der Fenster zuständig ist (aktives Fenster wechseln, Fenster verschieben etc.) sowie
- zahllose Anwendungs- und Konfigurationsprogramme.

Zusammen mit Gnome werden diverse Programme installiert, die sich in Funktionsweise und Aussehen in den Desktop einfügen. In diesem Kapitel stelle ich allerdings nur eine kleine Auswahl vor. Weitere Programme lernen Sie in themenspezifischen Kapiteln kennen – das Bildverwaltungsprogramm Shotwell beispielsweise in Kapitel 9 zum Umgang mit Digitalkameras.

Gnome 3

Mit dem seit 2011 verfügbaren Gnome 3 haben die Gnome-Entwickler ihren Desktop radikal umgestaltet. Eine zentrale Rolle spielt dabei die vollkommen neue »Gnome Shell«: Das ist jene Komponente von Gnome, die sich um den Start von Programmen und die Verwaltung von Fenstern kümmert. Das Ergebnis ist optisch sehr ansprechend: Meiner ganz subjektiven Ansicht nach bietet Gnome den momentan schönsten Desktop für Linux.

An der Funktionalität scheiden sich aber die Geister. Durch das Abrücken von bekannten Bedienungsmustern sowie wegen der fehlenden Konfigurierbarkeit hat sich das Gnome-Projekt den Unmut vieler Linux-Profis zugezogen. Die Gnome-Entwickler verteidigen sich damit, die Bedienung des Desktops für Einsteiger einfacher machen zu wollen.

Geben Sie Gnome eine Chance!

Lassen Sie sich von den kritischen Stimmen zu Gnome nicht beeindrucken! Viele Konzepte in Gnome 3 sind gut durchdacht und ermöglichen eine effiziente Bedienung, sobald man sich einmal daran gewöhnt hat. Außerdem lässt sich Gnome 3 außergewöhnlich einfach durch Erweiterungen modifizieren: Ein Webbrowser-Mausklick in der Gnome-Extension-Seite reicht oft aus, um Gnome zu neuen Funktionen zu verhelfen! Nicht zuletzt deswegen ist Gnome während der Arbeit an diesem Buch zu meinem persönlichen Lieblings-Desktop geworden und hat in dieser Rolle Ubuntus Unity abgelöst.

5.1 Der Aufbau des Desktops

Login und Logout

Bevor Sie unter Gnome arbeiten können, müssen Sie sich mit Ihrem Benutzernamen (Login-Namen) und dem Passwort anmelden. Falls auf Ihrem Rechner mehrere Desktop-Systeme installiert sind, können Sie in der Login-Box das gewünschte System auswählen.

Beim Abmelden wird es schon schwieriger: Je nach Gnome-Version und -Konfiguration sieht das Systemmenü, das Sie rechts oben im Gnome-Panel öffnen, entweder den Eintrag ABMELDEN oder AUSSCHALTEN vor, nicht aber beide Einträge! Aktuelle Gnome-Versionen folgen dabei der Logik, dass der Eintrag ABMELDEN nur notwendig ist, wenn es auf dem Rechner mehrere Benutzer gibt. Zur Not können Sie sich mit dem Kommando `gnome-session-quit` behelfen.

Bei allem Verständnis für ihr Vorhaben, die Oberfläche nicht mit unnötigen Einträgen zu überfrachten, sind die Gnome-Entwickler hier jedoch weit über das Ziel hinausgeschossen. Wenn Sie selbst entscheiden möchten, ob Sie sich nur abmelden oder den Rechner ganz ausschalten wollen, müssen Sie eine Gnome-Erweiterung installieren, z. B. das *Alternative Status Menu* (siehe Abschnitt 5.4).

Willkommens-Assistent

Ab Gnome 3.8 erscheint beim ersten Login ein Willkommens-Assistent. Dort können Sie die gewünschte Sprache für die Benutzeroberfläche sowie das Tastaturlayout (die EINGABEMETHODE) einstellen und Gnome mit einem Online-Konto verbinden, also z. B. mit Google oder ownCloud. Diesen Schritt können Sie aber ebensogut später in den Systemeinstellungen erledigen. Zuletzt erscheint ein kurzes Video, das elementare Funktionen des Gnome-Desktops erklärt. Das Video wird vom Webbrowser ausgeführt und lässt sich mit Esc beenden.

Benutzerwechsel

Wenn mehrere Benutzer einen Rechner verwenden, ist es nicht notwendig, dass sich der eine abmeldet, nur damit der andere rasch seine E-Mails lesen kann. Vielmehr

können sie im Systemmenü mit BENUTZER WECHSELN gewissermaßen einen fliegenden Wechsel durchführen. Intern wird für jeden Benutzer ein eigenes Grafiksystem ausgeführt. Mehrere parallele Logins erfordern daher eine Menge Ressourcen.

Panel

Das einzige Bedienungselement des Desktops ist das Panel, das unverrückbar am oberen Bildschirmrand angezeigt wird (siehe Abbildung 5.1). Es enthält den Button AKTIVITÄTEN, ein Icon für das gerade aktive Programm, die Uhrzeit sowie am rechten Rand diverse Status-Icons und -Menüs. Ganz rechts befindet sich das bereits erwähnte Systemmenü, über dessen Einträge Sie sich abmelden, die Systemeinstellungen verändern oder den aktiven Benutzer wechseln können. Der eigentliche Arbeitsbereich ist – wenn man von eventuell offenen Fenstern einmal absieht – vollkommen leer. Die Darstellung von Icons auf dem Desktop ist nicht mehr vorgesehen.

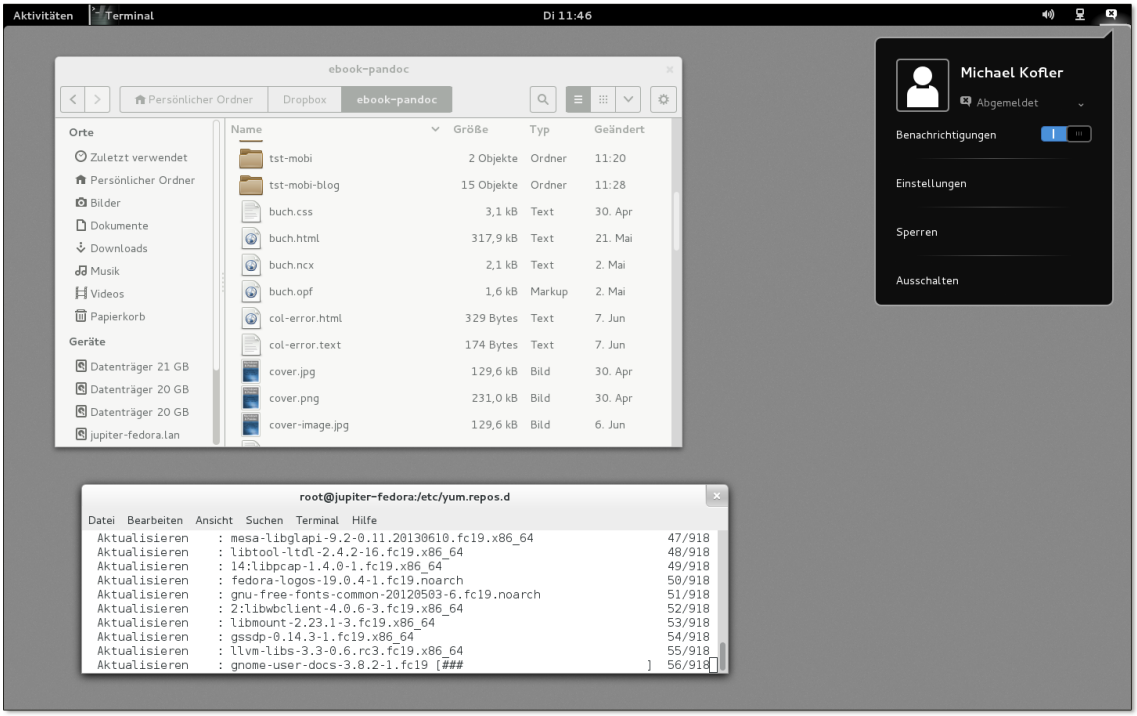


Abbildung 5.1 Der Gnome-Desktop

Applikationsmenü

Vereinzelte Gnome-Programme machen ihre wichtigsten Menükommandos auch über das sogenannte »Applikationsmenü« zugänglich (siehe Abbildung 5.2). In dieses Menü gelangen Sie, wenn Sie im Panel auf den Namen des gerade aktiven Programms klicken. Bei manchen Programmen ersetzt das Applikationsmenü sogar das herkömmliche Menü.

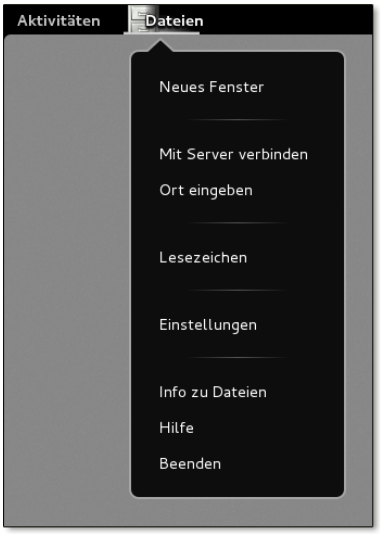


Abbildung 5.2 Das Applikationsmenü des Dateimanagers

Aktivitäten

Ein Mausklick auf den Button AKTIVITÄTEN, das Verschieben des Mauscursors in die linke obere Ecke des Bildschirms oder das Drücken der ⊞-Taste oder der Tasten Alt+F1 öffnet die Aktivitäten-Ansicht (siehe Abbildung 5.3). Standardmäßig zeigt diese Ansicht links ein Dock mit den Icons oft benötigter sowie aller laufenden Programme an, rechts eine Vorschau der aktiven Arbeitsflächen. Dazwischen werden in einer Art Exposé-Ansicht alle Fenster der Arbeitsfläche angezeigt. Nun können Sie beispielsweise Fenster in eine andere Arbeitsfläche verschieben, Icons von häufig benötigten Programmen in der Icon-Leiste am linken Bildschirmrand neu positionieren etc.

Suchfunktion

In der Aktivitäten-Ansicht ist ein Suchfeld aktiv. Sobald Sie per Tastatur einen Suchbegriff eingeben, ersetzt Gnome die Exposé-Ansicht aller Fenster durch die Suchergebnisse, wobei Programme, Systemeinstellungsmodule, Verzeichnisse, Kontakte sowie die zuletzt verwendeten Dateien berücksichtigt werden. Das gewünschte Objekt können Sie wahlweise mit der Maus oder mit den Cursortasten auswählen.

Die Suchfunktion ist zweifellos die beste Neuerung in Gnome 3.*n*. Wenn Sie beispielsweise rasch Gimp öffnen möchten, geben Sie einfach ⊞ gi ↵ ein. Sobald Sie sich daran gewöhnt haben und die Anfangsbuchstaben der wichtigsten Programme auswendig kennen, gelingt der Programmstart so äußerst schnell und effizient.

Beachten Sie, dass ⊞ xxx ↵ bereits laufende Programme aktiviert und nicht eine neue Instanz startet. Das ist meistens zweckmäßig, aber nicht immer: Wenn Sie beispielsweise nicht ein bereits laufendes Terminalfenster aktivieren möchten, son-

dern ein neues Terminalfenster öffnen möchten, müssen Sie Strg+↵ drücken bzw. das Terminal-Icon zusammen mit Strg anklicken.

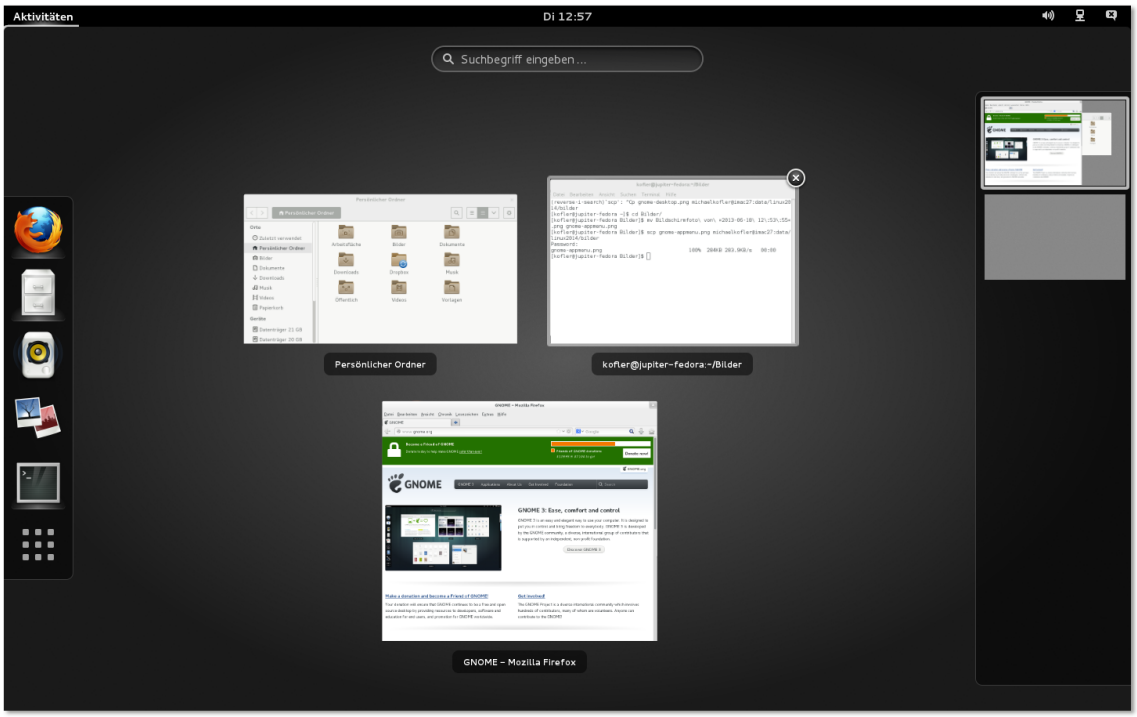


Abbildung 5.3 Aktivitäten-Ansicht

Programme starten

Um ein Programm zu starten, dessen Namen Sie nicht kennen, klicken Sie in der Aktivitäten-Ansicht auf den Button ANWENDUNGEN ANZEIGEN unten im Dock. Damit gelangen Sie in eine Icon-Übersicht, die anfänglich die zuletzt benutzten Programme zeigt. Um zwischen allen Programmen wählen zu können, klicken Sie auf den Button ALLE (siehe Abbildung 5.4). Nun werden alle installierten Programme angezeigt, wobei weniger häufig benötigte Programme in Gruppen wie HILFSPROGRAMME oder VERSCHIEDENES verborgen sind.

Das aktive Programm wechseln

Nicht besonders intuitiv ist die Bedienung von Gnome mit der Tastatur. Besonders irritierend ist anfänglich, dass Alt+⇆ nicht mehr zwischen Fenstern wechselt, sondern zwischen Programmen. Dieses Konzept verfolgt OS X schon lange, aber auch Apple hat mich nicht überzeugen können, dass das eine gute Idee ist.

Ist das richtige Programm einmal gefunden, kann das Fenster mit Alt und den Cursor-Tasten ausgewählt werden. Das erfordert aber Geduld! Einfacher ist es, zum Fensterwechsel Alt+Esc zu verwenden; dieses Tastenkürzel funktioniert im Wesentlichen so wie früher Alt+⇆. Ebenfalls praktisch: Alt+^ wechselt

zwischen den Fenstern des gerade aktiven Programms. Und so haben wir nun *drei* Tastenkürzel, um das zu tun, was bisher mit einem Tastenkürzel wunderbar funktionierte.

Abbildung 5.4 Programme starten

Dock

In Gnome 3.*n* gibt es keine ständig sichtbare Task- oder Fenster-Leiste. Diese Rolle übernimmt die vertikale Icon-Leiste am linken Rand der Aktivitäten-Ansicht. Die Gnome-Entwickler bezeichnen sie als *Dash*, ich bleibe in diesem Buch aber bei dem gebräuchlicheren Begriff *Dock*.

Das Dock enthält im oberen Bereich standardmäßig einige Programme, von denen die Gnome-Entwickler denken, dass Sie sie häufig benötigen werden. Der untere Bereich des Docks enthält Icons aller gerade laufenden Programme, soweit sich diese nicht sowieso im Dock befinden.

Laufende Programme werden durch einen Schatten hervorgehoben. Die Icon-Größe im Dock wird automatisch so angepasst, dass alle Icons angezeigt werden können. Wenn also viele Programme gleichzeitig laufen, schrumpfen die Icons entsprechend.

Um ein Icon aus dem Dock zu entfernen, führen Sie das Kontextmenükommando AUS FAVORITEN ENTFERNEN aus. Um dem Dock ein Programm hinzuzufügen, verschieben Sie das betreffende Programm per Drag&Drop aus der Ansicht ANWENDUNGEN in das Dock. Alternativ führen Sie bei einem bereits laufenden Programm das Kontextmenükommando ZU FAVORITEN HINZUFÜGEN aus.

Statusbereich

Der untere Rand des Bildschirms ist für Statusmeldungen und Benachrichtigungen reserviert. Der Statusbereich ist normalerweise ausgeblendet. Um dort enthaltene Informationen anzusehen, müssen Sie die Maus nachdrücklich in den unteren Rand des Bildschirms bewegen, d. h., Sie müssen die Maus- oder Trackpad-Bewegung fortsetzen, nachdem der Mauszeiger den unteren Bildschirmrand erreicht hat. Auf diese Weise soll ein unbeabsichtigtes Einblenden des Statusbereichs vermieden werden.

Fenster

In Gnome 3.*n* fehlen die Fensterbuttons MINIMIEREN und MAXIMIEREN. Um ein Fenster zu minimieren, klicken Sie die Fensterleiste mit der rechten Maustaste an und führen MINIMIEREN aus; um es zu maximieren, verschieben Sie es an den oberen Bildschirmrand oder doppelklicken auf die Fensterleiste. Am einfachsten gelangen Sie mit dem Gnome Tweak Tool wieder zu »normalen« Fensterbuttons (siehe Abschnitt 5.4).

Wie unter Windows können Sie ein Fenster in der linken oder rechten Bildschirmhälfte platzieren, indem Sie es an den linken oder rechten Fensterrand verschieben.

Arbeitsflächen

Arbeitsflächen ermöglichen es, die Fenster der laufenden Programme auf mehrere virtuelle Desktops zu verteilen und zwischen diesen Desktops zu wechseln. Das erleichtert die Arbeit und verbessert die Übersicht, wenn Sie sehr viele Fenster gleichzeitig öffnen. Beispielsweise können Sie das Bildverarbeitungsprogramm Gimp in einer eigenen Arbeitsfläche starten. Damit befinden sich die vielen Gimp-Fenster in einer Arbeitsfläche und alle anderen Fenster in einer zweiten Arbeitsfläche.

Arbeitsflächen werden in Gnome 3.*n* dynamisch verwaltet. Standardmäßig gibt es nur eine Arbeitsoberfläche. In der Aktivitätenansicht können Sie Fenster in eine zweite Arbeitsoberfläche verschieben. Sobald es zwei aktive Arbeitsflächen gibt, sieht Gnome eine dritte, vorerst leere Arbeitsfläche vor. Ganz egal, wie viele Arbeitsflächen Sie einsetzen – es gibt immer noch eine.

Für ständig benötigte Fenster besteht die Möglichkeit, diese so zu kennzeichnen, dass sie nicht auf einer, sondern auf allen Arbeitsflächen sichtbar sind. Dazu öffnen Sie mit der rechten Maustaste oder mit Alt+␣ das Fenstermenü und aktivieren die Option IMMER AUF DER SICHTBAREN ARBEITSFLÄCHE.

Um zwischen den Arbeitsflächen zu wechseln, können Sie die Aktivitätenansicht verwenden. Noch schneller klappt es mit den Tastenkürzeln Strg+Alt+↑ bzw. +↓.

Applets

Die im rechten Teil des Panels angezeigten Miniprogramme (Applets) sind nicht ohne Weiteres veränderlich. Es gibt keinen Dialog, um weitere Applets hinzuzufügen. Stattdessen können Sie über die Seite *https://extensions.gnome.org* Gnome-Erweiterungen herunterladen und aktivieren (siehe Abschnitt 5.4). Gnome-2.*n*-

Applets sind nicht kompatibel zu Gnome 3.*n* und können nicht mehr genutzt werden.

Tastenkürzel

Tabelle 5.1 fasst die wichtigsten Tastenkürzel von Gnome 3.*n* zusammen. Weitere Tastenkürzel finden Sie in den Systemeinstellungen, Modul TASTATUR, Dialogblatt TASTENKÜRZEL.

Tastenkürzel	Bedeutung
⊞ oder Alt+F1	wechselt zwischen der Standardansicht und der Desktop-Übersicht (Exposé-Ansicht). In diese Ansicht gelangen Sie auch, wenn Sie die Maus in die linke obere Ecke des Fensters bewegen. Sie können nun die Tastatur zur Eingabe von Suchtexten verwenden.
Alt+F2	startet das Programm, dessen Namen Sie angeben.
Alt+↹	wechselt zwischen Programmen (nicht Fenstern!).
Alt+Esc	wechselt zwischen allen Fenstern (so wie früher Alt+↹).
Alt+^	wechselt zwischen den Fenstern innerhalb des gerade aktiven Programms.
Strg+Alt+↹	bewegt in der Standardansicht den Eingabefokus in das Panel und ermöglicht so eine Bedienung der Panelelemente. In der Desktop-Übersicht wechselt Strg+Alt+↹ zwischen verschiedenen Desktop-Elementen, also dem Panel, der Seitenleiste (Dash), den Fenstern, den Arbeitsflächen etc.
Strg+Alt+↑/↓	wechselt zwischen den Arbeitsflächen.
⇧+Strg+Alt+↑/↓	verschiebt das aktuelle Fenster in die nächste Arbeitsfläche.

Tabelle 5.1 Wichtige Gnome-Tastenkürzel

5.2 Dateimanager

Das Programm *Dateien* ist der Dateimanager des Gnome-Desktops (siehe Abbildung 5.5). Es gewährt nicht nur den Zugriff auf Dateien und Verzeichnisse, sondern ermöglicht auch den Zugriff auf externe Datenträger und Netzwerkverzeichnisse. Dieser Abschnitt beschreibt die Bedienung des Dateimanagers, geht aber nicht im Detail auf die Besonderheiten der Dateiverwaltung unter Linux ein. Was Links sind, wie verborgene Dateien gekennzeichnet werden und wie Zugriffsrechte unter Linux funktionieren, erfahren Sie in Kapitel 15.

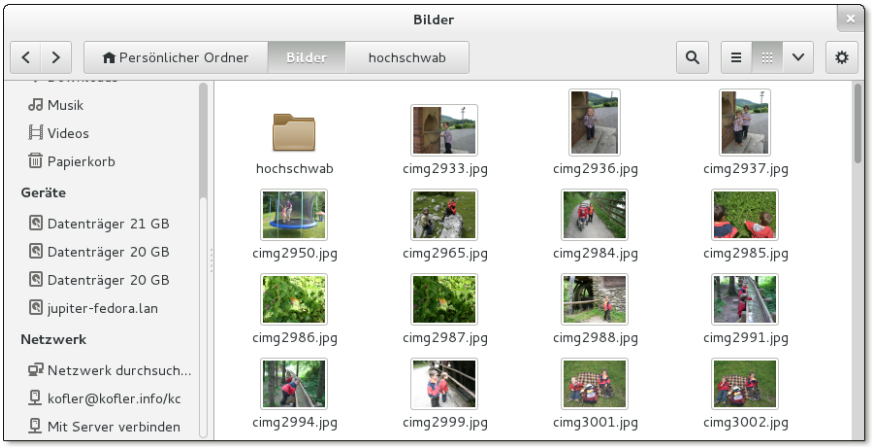


Abbildung 5.5 Der Gnome-Dateimanager

»Nautilus« versus »Dateien«

Bis einschließlich Version 3.4 hieß der Gnome-Dateimanager *Nautilus*. Seit Version 3.6 lautet der neue Name *Files* bzw. im Deutschen einfach *Dateien*. Da sich mit diesem selten blöden Namen keine vernünftigen Sätze bilden lassen (»Verwenden Sie *Dateien*, um Ihre Dateien zu verwalten ...«), bleibe ich in diesem Buch beim alten Namen Nautilus oder schreibe »Dateimanager«. Auch intern wird der Name Nautilus weiter verwendet, z. B. für die Programmdatei bzw. für den Paketnamen.

Abschied nehmen von praktischen Funktionen

Mit Version 3.6 hat sich freilich nicht nur der Name geändert, sondern auch das Aussehen und die Funktion des Dateimanagers. In typischer Gnome-Manier haben die Entwickler das Programm radikal vereinfacht. Das Ergebnis: Das Programm sieht sehr aufgeräumt aus und lässt sich gut bedienen, hat aber auch eine Menge essenzieller Funktionen verloren:

- Der Dateimanager hat kein reguläres Menü mehr, nur noch ein Werkzeugmenü und ein Applikationsmenü. Lesezeichen können nur über die Seitenleiste angesprochen werden.
- Die kompakte Dateiansicht gibt es nicht mehr.
- Die Parallelansicht zweier Verzeichnisse durch F3 wurde gestrichen.
- Standardmäßig werden Verzeichnisse nicht mehr vor Dateien sortiert. Dieser Unfug lässt sich zum Glück in den Programmeinstellungen ändern.

Von den Lesern der Website *http://omgubuntu.co.uk* sind gerade einmal 18 Prozent der Meinung, dass diese Änderungen gut sind. Die Entwickler der Distribution Linux Mint haben daraus die Konsequenzen gezogen und einen Fork des Dateimanagers unter dem Namen *Nemo* vorgestellt; aktuelle Versionen von Linux Mint verwenden

nun Nemo. Die meisten anderen Distributionen sind aber beim Original von Gnome geblieben, selbst Ubuntu, wo man vor Alleingängen sonst nicht zurückschreckt.

Dateien anzeigen

Den Dateimanager starten Sie am einfachsten durch einen Klick auf dessen Icon im Dock der Aktivitätenansicht. Der Dateimanager zeigt den Inhalt des ausgewählten Verzeichnisses standardmäßig in der Symbolansicht an. Jede Datei wird durch ein Icon dargestellt, das bei Bildern und einigen anderen Dateitypen gleichzeitig eine Vorschau auf den Inhalt gibt. Die Vorschau funktioniert standardmäßig nur bei lokalen Dateien bis zu 10 MByte. Damit die Vorschau auch in Netzwerkverzeichnissen sowie für größere Dateien funktioniert, verändern Sie die entsprechenden Optionen im Werkzeugmenü mit Bearbeiten • Einstellungen • Vorschau.

Mit Strg+1 und Strg+2 können Sie zwischen der Symbolansicht und der Detailansicht wechseln. Innerhalb der Symbolansicht können Sie mit Strg++ und Strg+- die Icon-Größe einstellen.

Damit die Vorschau nicht immer wieder neu erzeugt werden muss, speichert der Dateimanager die Bilder im Verzeichnis `.thumbnails`. Auch viele andere Gnome-Programme nutzen dieses Verzeichnis.

Ausklappbare Unterverzeichnisse

Beginnend mit Gnome 3.8 kann Nautilus in der Listenansicht die Ordner ausklappbar darstellen. Das ermöglicht eine einfachere Navigation durch den Verzeichnisbaum. Diese Funktion kann im Dialogblatt Anzeige der Programmeinstellungen aktiviert werden.

Seitenleiste

Der linke Fensterrand enthält normalerweise eine Seitenleiste, die einen raschen Wechsel zu wichtigen Verzeichnissen ermöglicht. Per Drag&Drop können Sie oft benötigte Verzeichnisse der Seitenleiste hinzufügen und auf diese Weise Lesezeichen definieren. F9 schaltet die Seitenleiste aus bzw. wieder ein.

Verzeichniswechsel

In der Symbolleiste befinden sich einige Buttons, mit denen Sie rasch in übergeordnete Verzeichnisse wechseln können. Aus den Buttons geht auch der aktuelle Verzeichnispfad hervor. Alternativ zeigt der Dateimanager an dieser Stelle mit Strg+L den kompletten Pfad an, was vor allem die rasche Eingabe eines anderen Verzeichnisses erleichtert.

Reiter

Mit Strg+T öffnen Sie ein neues Dialogblatt. Besonders praktisch sind Dialogblätter, wenn Sie Dateien von einem Verzeichnis in ein anderes kopieren oder verschieben möchten: Während Drag&Drop-Operationen können Sie das aktive Dialogblatt wechseln.

Dateien öffnen

Bei den meisten Dateitypen wird die Datei durch einen Doppelklick geöffnet. Der Dateimanager startet automatisch das geeignete Programm. Wenn der Dateityp dem Dateimanager nicht bekannt ist, klicken Sie die Datei mit der rechten Maustaste an und führen MIT ANDERER ANWENDUNG ÖFFNEN aus. Damit gelangen Sie in einen Dialog, der die meisten auf dem Rechner installierten Programme zur Auswahl anbietet.

Bei manchen Dateien sind mehrere Programme zur Bearbeitung geeignet. Beispielsweise können Sie Bilddateien wahlweise mit einem Bildbetrachter, mit Gimp oder mit Firefox öffnen. Eines dieser Programme gilt als Standardprogramm und wird per Doppelklick gestartet. Wenn Sie das Standardprogramm ändern möchten, klicken Sie die Datei mit der rechten Maustaste an, führen EIGENSCHAFTEN • ÖFFNEN MIT aus und wählen das gewünschte Programm. Die Einstellung gilt in Zukunft für alle Dateien mit derselben Endung, also beispielsweise für alle `*.png`-Dateien.

Dateien verschieben und kopieren

Zuvor markierte Dateien kopieren Sie mit Strg+C bzw. schneiden Sie mit Strg+X aus. Anschließend fügen Sie die betreffenden Dateien mit Strg+V am neuen Ort wieder ein. Die ausgeschnittenen Dateien werden erst jetzt am Ursprungsort entfernt.

Deutlich einfacher ist es, Dateien per Drag&Drop von einem Dateimanager-Fenster in ein zweites zu verschieben. Dabei werden die Dateien normalerweise verschoben, nicht kopiert! Eine Ausnahme von dieser Regel sind Drag&Drop-Operationen zwischen unterschiedlichen Datenträgern, also beispielsweise von der CD oder von einem Netzwerkverzeichnis in das lokale Dateisystem. Im Mauszeiger wird in solchen Fällen ein Plus-Symbol eingeblendet, sodass die Wirkung der Operation klar sein sollte.

Wenn Sie eine Datei gezielt kopieren statt verschieben möchten, drücken Sie während der Drag&Drop-Operation die Strg-Taste. Wenn Sie den Verschiebemodus selbst angeben möchten, drücken Sie die Alt-Taste. Nach dem Loslassen der Maus haben Sie die Möglichkeit, die Datei zu kopieren, zu verschieben oder eine Verknüpfung (einen Link) einzurichten.

Dateien suchen

Mit dem SUCHEN-Button können Sie im Adressfeld einen Suchbegriff eingeben. Der Dateimanager liefert dann eine Liste aller Dateien, die den Suchbegriff im Dateinamen enthalten. Im Anschluss an die Suche können Sie die Suchergebnisse auf einen bestimmten Dokumenttyp oder ein Verzeichnis einschränken (siehe Abbildung 5.6).

Verborgene Dateien

Unter Linux gelten alle Dateien und Verzeichnisse, deren Namen mit einem Punkt beginnen, als verborgen. Das bedeutet, dass sie im Dateimanager bzw. in Dateiauswahldialogen normalerweise nicht angezeigt werden. Verborgene Dateien enthalten

oft Konfigurationseinstellungen oder andere Daten, die nicht direkt verändert werden sollen. Eine direkte Bearbeitung versteckter Dateien und Verzeichnisse ist nur in Ausnahmefällen zweckmäßig (z. B. wenn Sie ein Backup Ihrer E-Mail-Verzeichnisse in `.thunderbird` durchführen möchten). Damit solche Dateien und Verzeichnisse im Dateimanager sichtbar werden, führen Sie Ansicht • Verborgene Dateien anzeigen aus oder drücken Strg+H.

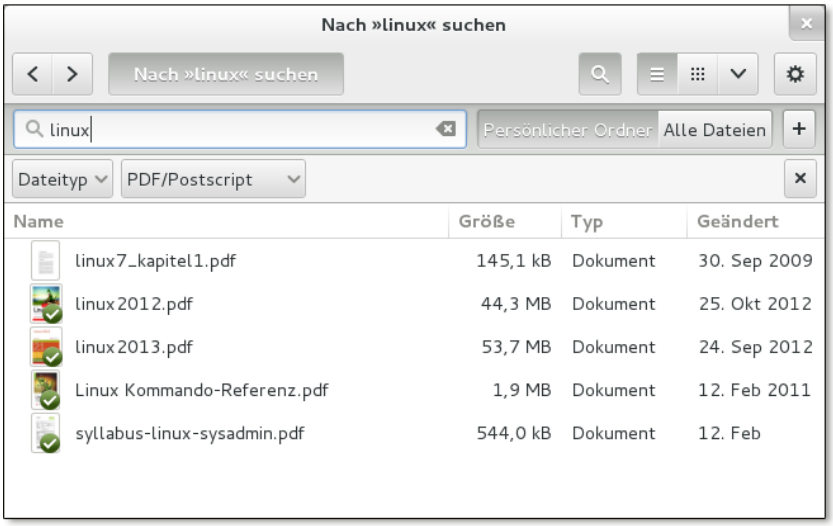


Abbildung 5.6 Nach Dateien suchen

Zugriffsrechte

Damit nicht jeder Benutzer alle Dateien und Verzeichnisse lesen bzw. verändern kann, speichert Linux zu jeder Datei und zu jedem Verzeichnis den Besitzer sowie die Zugriffsrechte. Das zugrunde liegende Konzept wird in Abschnitt 15.6 ausführlich beschrieben. Um den Besitzer oder die Zugriffsrechte zu ändern, klicken Sie die Datei mit der rechten Maustaste an und führen Eigenschaften • Zugriffsrechte aus.

Dateien löschen

Um Dateien zu löschen, müssen Sie Strg+Entf drücken. Die markierten Dateien und Verzeichnisse landen vorerst im Papierkorb. Den Inhalt des Papierkorbs sehen Sie durch einen Klick auf das Müll-Icon in der Seitenleiste des Dateimanagers. Erst wenn Sie den Papierkorb leeren, werden die Dateien endgültig gelöscht.

Eigene Tastenkürzel

Die Tastenkürzel für Nautilus sind in der Textdatei `.config/nautilus/accels` gespeichert. Wenn Sie also z. B. Dateien einfach mit Entf in den Papierkorb befördern möchten, fügen Sie die folgende Zeile in diese Datei ein:

```
(gtk_accel_path "<Actions>/DirViewActions/Trash" "Delete")
```

Die neuen Tastenkürzel werden nach einem Neustart des Dateimanagers wirksam.

Externe Datenträger

Beim Einlegen einer CD oder DVD bzw. beim Anstecken eines USB-, Firewire- oder eSATA-Laufwerks erscheint automatisch ein neues Dateimanager-Fenster mit dem Inhalt des Datenträgers. Die zugrunde liegenden Einstellungen finden Sie in den Systemeinstellungen im Modul DETAILS • WECHSELMEDIEN.

Denken Sie daran, dass Sie externe Festplatten oder USB-Sticks explizit abmelden müssen, bevor Sie das Kabel zum Computer lösen! Dazu klicken Sie auf den Auswerfen-Button in der Seitenleiste.

Netzwerkfunktionen

Windows-Freigaben

Der Eintrag NETZWERK DURCHSUCHEN in der Seitenleiste führt in eine Ansicht, die nach einigen Sekunden Icons für alle erkannten Netzwerke anzeigt. In der Praxis ist das oft nur ein WINDOWS-NETZWERK. Ein Doppelklick führt zur nächsten Ansicht mit allen erkannten Windows-Netzwerken. Ein weiterer Doppelklick zeigt alle in diesem Netz sichtbaren Rechner an. Noch ein Doppelklick, und Sie wissen, welche Ressourcen dieser Rechner anbietet.

Wenn das Netzwerkverzeichnis durch ein Passwort geschützt ist, müssen Sie den Login-Namen und das Passwort angeben. Dabei bekommen Sie die Möglichkeit, diese Daten bleibend in einer Gnome-Passwortdatenbank zu speichern. Damit Sie den relativ umständlichen Weg in ein Netzwerkverzeichnis nicht immer wieder neu beschreiten müssen, richten Sie mit Strg+D ein Lesezeichen ein.

Wenn der Dateimanager ein Netzwerkverzeichnis ohne Passwort nutzen kann, entscheidet er sich automatisch für diese Variante. Diese Vorgehensweise ist allerdings nicht immer ideal: Je nachdem, wie der Windows- oder Samba-Server konfiguriert ist, zeigt der Dateimanager anschließend nur ein leeres Verzeichnis. Über die Benutzeroberfläche besteht nun keine Möglichkeit mehr, sich namentlich anzumelden. Abhilfe: Drücken Sie Strg+L, und fügen Sie Ihren Login-Namen in den Pfad ein. Die korrekte Schreibweise lautet `smb://login@servername/verzeichnisname`.

Sollte der Dateimanager keine Windows-Server finden, ist die wahrscheinlichste Fehlerursache eine zu restriktive Firewall zwischen Ihrem Rechner und dem Windows-Rechner. Oft funktioniert auch nur die Namensauflösung nicht. Abhilfe: Drücken Sie Strg+L, und geben Sie die Adresse `smb://servername` ein.

Analog können Sie auch Verbindungen zu anderen Server-Diensten herstellen. Tabelle 5.2 fasst die wichtigsten Adressen bzw. Protokolle zusammen. In der Tabelle finden Sie auch die Spezialadressen `computer:` und `trash:`.

Adresse	Ergebnis
`computer:`	Liste aller Datenträger
`afp://user@hostname`	Zugriff auf AFP-Server (Apple)
`ftp://hostname`	Zugriff auf FTP-Server
`network:`	Verwendung als allgemeiner Netzwerk-Browser
`sftp://hostname`	Zugriff auf SFTP-Server (SSH-Protokoll)
`smb:`	Verwendung als Windows-Netzwerk-Browser
`smb://hostname`	Zugriff auf die Netzwerkverzeichnisse eines Windows-Rechners
`trash:`	Papierkorb (gelöschte Dateien)

Tabelle 5.2 Spezialadressen

GVFS

Für den Zugriff auf Netzwerkverzeichnisse ist das Gnome Virtual File System (GVFS) verwantwortlich. Es bindet externe Verzeichnisse als Unterverzeichnisse von `.gvfs` in den Verzeichnisbaum ein. Der Dateimanager sowie Gnome-Dateiauswahldialoge zeigen externe Netzwerkverzeichnisse in der Seitenleiste an (drücken Sie gegebenenfalls F9).

Selbst Verzeichnisse freigeben

Bei einigen Distributionen können Sie unkompliziert selbst Verzeichnisse im Netzwerk freigeben. Dazu klicken Sie das Verzeichnis mit der rechten Maustaste an und führen FREIGABEOPTIONEN aus. Dieses Kommando stammt vom Nautilus-Erweiterungspaket `nautilus-share`. Leider stellen nicht alle Distributionen dieses Paket zur Verfügung: Glück haben Sie mit Debian, openSUSE und Ubuntu, Pech mit Fedora oder RHEL.

Das Einrichten der Freigabe funktioniert nur dann auf Anhieb, wenn die lokale Firewall die Nutzung des Rechners als Samba-Server zulässt und wenn Sie die Option GASTZUGANG wählen, also auf eine Passwortabsicherung verzichten. Bei einigen Distributionen ist außerdem vorher eine Samba-Basiskonfiguration erforderlich, z. B. bei SUSE mit dem YaST-Modul NETZWERKDIENSTE • SAMBA-SERVER. Wenn Sie mit Fedora oder RHEL arbeiten, geben Sie Verzeichnisse am besten mit dem Programm `system-config-samba` frei. Tipps zur manuellen Freigabe von Netzwerkverzeichnisses sind in Abschnitt 31.4 im Samba-Kapitel zusammengefasst.

Plugins

Der Dateimanager kann durch Plugins erweitert werden. Die meisten Distributionen stellen Pakete für einige Plugins zur Verfügung, installieren diese aber nicht standardmäßig. Suchen Sie im Paketverwaltungsprogramm Ihrer Distribution nach *nautilus*, installieren Sie die gewünschten Pakete, und loggen Sie sich dann neu

in Gnome ein. Ich stelle Ihnen hier nur einige ausgewählte Pakete vor, wobei die Paketnamen für Debian und Ubuntu gelten.

- `nautilus-image-converter` und `nautilus-image-manipulator` (siehe Abbildung 5.7): Die beiden Plugins ermöglichen es, Bilder per Kontextmenü zu drehen bzw. ihre Größe zu verändern.
- `nautilus-compare`: Mit dem Plugin können Sie zwei oder mehrere zuvor markierte Textdateien vergleichen. Die Unterschiede zwischen den Dateien werden grafisch im Programm Meld dargestellt.
- `nautilus-open-terminal`: Dieses Plugin ermöglicht es, ein Terminal-Fenster zu öffnen, indem man mit der rechten Maustaste auf den Desktop klickt.
- `nautilus-pastebin`: Mit diesem Plugin können Sie Textdateien zu einem Pastebin-Service hochladen.
- `seahorse-nautilus`: Das Plugin hilft dabei, die ausgewählten Dateien per Kontextmenü zu verschlüsseln.
- `nautilus-dropbox`: Das Dropbox-Plugin hilft bei der Synchronisation des Verzeichnisses `Dropbox` mit Ihrem Dropbox-Konto (siehe auch Kapitel 8).

Abbildung 5.7 Die Bildgröße ändern mit dem nautilus-image-manipulator

CDs/DVDs brennen

Daten-CDs und -DVDs

Nichts ist einfacher, als einige Dateien oder ganze Verzeichnisse auf eine CD oder DVD zu brennen: Das Fenster CD/DVD-Ersteller erscheint automatisch, sobald Sie einen CD- oder DVD-Rohling einlegen. Sollte das nicht funktionieren, starten Sie das Programm *Brasero* und klicken auf den Button Daten-Projekt. Nun kopieren Sie von einem Dateimanager-Fenster die zu sichernden Dateien und Verzeichnisse per Drag&Drop in das Fenster des Brennprogramms (siehe Abbildung 5.8).

Brasero sollte eigentlich bei allen Verzeichnissen und Dateien deren Platzbedarf auf der CD anzeigen; bei meinem Test waren stattdessen nur schwarze Balken zu sehen. Der Button Brennen führt noch in einen Einstellungsdialog für die Brenngeschwindigkeit und einige weitere Optionen, dann geht's los!

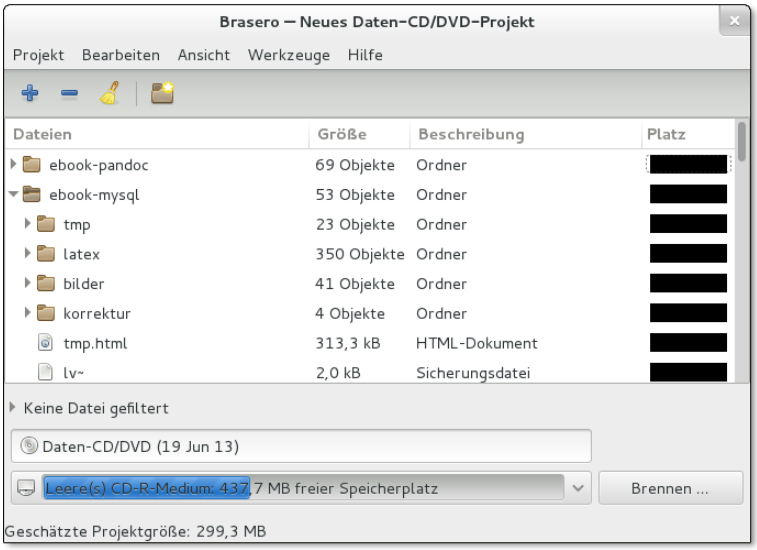


Abbildung 5.8 CDs und DVDs brennen mit Brasero

Nach dem Brennen überprüft Brasero automatisch, ob die neue CD oder DVD fehlerfrei ist. Wenn Sie das nicht wünschen, deaktivieren Sie in der Benutzeroberfläche von Brasero mit Bearbeiten • Plugins die Prüfsummen-Plugins.

CDs/DVDs kopieren

Um eine CD oder DVD zu kopieren, legen Sie diese in das Laufwerk, starten abermals das Programm Brasero und führen dort CD/DVD kopieren aus. Brasero schreibt den Inhalt der CD/DVD nun in eine ISO- oder TOC-Datei. Wenn das Auslesen der Daten abgeschlossen ist, können Sie diese Datei auf eine leere CD/DVD schreiben.

ISO- und TOC-Dateien

ISO- bzw. TOC-Dateien enthalten den gesamten Inhalt einer CD oder DVD. Um eine derartige Datei zu brennen, klicken Sie die Datei mit der rechten Maustaste an und führen Auf CD/DVD schreiben aus.

Übrigens können Sie vorher auch den Inhalt der ISO-Datei ansehen. Ein Doppelklick auf die Datei öffnet den Archivmanager, der die ISO-Datei ähnlich wie eine ZIP-Datei behandelt. Sie können den Inhalt der ISO-Datei allerdings nicht verändern.

Sie können ISO-Dateien auch selbst herstellen: Dazu gehen Sie wie beim Brennen einer Daten-CD bzw. -DVD vor, wählen aber als Zielmedium eine Abbilddatei.

Audio-CDs

Wenn Sie aus MP3- oder Ogg-Dateien eine Audio-CD machen möchten, die mit einem gewöhnlichen CD-Player angehört werden kann, starten Sie wiederum Brasero und beginnen dort ein neues AUDIO-PROJEKT. In dieses fügen Sie die gewünschten Audio-Dateien wahlweise per Drag&Drop, mit dem EINFÜGE-Button oder aus dem in die Seitenleiste (F7) integrierten Dateibrowser ein. Der Button BRENNEN startet den Brennvorgang. Der eigentliche Brennvorgang dauert nun ein wenig länger als üblich, weil die Audio-Dateien zuerst in das WAV-Format umgewandelt werden müssen.

5.3 Gnome-Standardprogramme

In diesem Abschnitt stelle ich Ihnen einige Programme vor, die üblicherweise zusammen mit dem Gnome-Desktop zur Verfügung stehen. Da das Gnome-Projekt zuletzt dazu übergegangen ist, die Programme entsprechend ihrer Funktion zu bezeichnen (z. B. *Web* für den Webbrowser), gebe ich in Klammern zusätzlich auch den ehemaligen Namen bzw. den internen Programmnamen an.

Boxes

Ab Gnome 3.8 ist das Programm *Boxes* integraler Bestandteil von Gnome. Boxes erlaubt das Einrichten und Ausführen virtueller Maschinen, wobei hinter den Kulissen KVM zum Einsatz kommt (siehe auch Kapitel 43). Boxes richtet sich an Linux-Anwender, die rasch und unkompliziert eine virtuelle Maschine mit Windows oder mit einer anderen Linux-Distribution einrichten möchten.

Boxes oder VirtualBox?

Wenn Sie keine Erfahrung mit Virtualisierung haben, ist das in Kapitel 11 vorgestellte Programm VirtualBox besser geeignet als Boxes. VirtualBox bietet mehr Funktionen und eine klarere Logik bei der Bedienung.

Dateiarchive (file-roller)

Zur Weitergabe von Dateien per E-Mail bzw. zum Anlegen von Sicherungskopien ist es oft zweckmäßig, mehrere Dateien oder den gesamten Inhalt eines Verzeichnisses zu komprimieren. Dabei hilft der sogenannte *Archivmanager* (siehe Abbildung 5.9). Das Programm starten Sie üblicherweise durch einen Doppelklick auf die Archivdatei. Sie können mit dem Archivmanager auch EPUB-, JAR- oder LibreOffice-Dateien inspizieren; all diese Dateiformate sind in Wirklichkeit vom ZIP-Format abgeleitet.

Der Archivmanager zeigt das Archiv so an, als wäre es ein ganz gewöhnliches Verzeichnis. Wenn Sie rasch einen Überblick über alle Dateien bekommen möchten, führen Sie ALLE DATEIEN ANZEIGEN im Applikationsmenü aus. Um das gesamte Archiv auszupacken, klicken Sie auf den Button ENTPACKEN. Um ein neues Archiv zu erstellen, führen Sie Alt+F2 `file-roller` aus. Sie können nun einfach per Drag&Drop Dateien bzw. ganze Verzeichnisse einfügen.

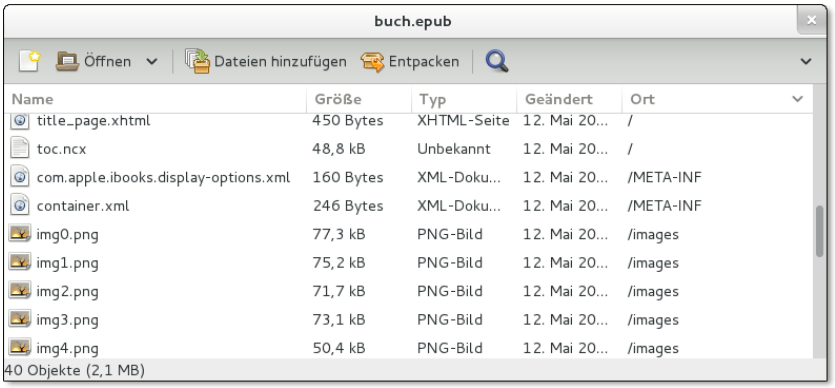


Abbildung 5.9 Dateiarchive bearbeiten

Dokumente (gnome-documents)

Das Programm *Dokumente* gibt einen Überblick über zuletzt bearbeitete Office- und PDF-Dateien. Sofern Sie im Modul ONLINE-KONTEN der Systemeinstellungen ein Google-Konto einrichten, können Sie auch Dateien aus Google Docs synchronisieren. Bei meinen Tests wirkte das Programm aber noch unausgegoren und ein wenig wie eine Antwort auf eine nicht gestellte Frage.

Fernwartung (vino-preferences)

Wenn Sie auf Ihrem Rechner ein Problem haben, z. B. weil ein Programm nicht richtig funktioniert, werden Sie üblicherweise per Telefon oder E-Mail Hilfe anfordern. Erfahrungsgemäß sind derartige Hilfsversuche aber recht umständlich: *Klick einfach auf den Button xy! – Wo ist dieser Button? – Du kannst auch das Menükommando* ABC • EFG *verwenden! – Bei welchem Programm?*

Für solche Fälle gibt es ein viel eleganteres Hilfsmittel: Per Fernwartung bekommt der Helfer für einige Zeit volle Kontrolle über Ihren Computer. Der Helfer sieht auf seinem Rechner in einem Fenster den gesamten Inhalt Ihres Bildschirms und kann per Maus und Tastatur alle Programme bedienen. Unter Gnome starten Sie die Fernwartung als Hilfesuche mit dem Programm *Freigabe der Arbeitsfläche* (Programmname `vino-preferences` aus dem Paket `vino`). Der Helfer kann einen beliebigen VNC-Client einsetzen, beispielsweise Vinagre, Remmina oder TightVNC (Paketname `tigervnc` unter Fedora/RHEL bzw. `xtightvncviewer` unter Debian/Ubuntu).

Leider funktioniert die Fernwartung nur, wenn sich beide Rechner in einem lokalen Netzwerk befinden oder eindeutige IP-Adressen haben. Sind die Rechner dagegen mit einem ADSL- oder WLAN-Router verbunden, scheitert die Gnome-Fernwartung. Abhilfe schaffen in solchen Fällen kommerzielle Programme. Gute Erfahrungen habe ich mit TeamViewer gemacht: Für dieses Programm gibt es eine Linux-Version, deren private Nutzung kostenlos ist:

http://www.teamviewer.com/de/index.aspx

Festplattennutzung (baobab)

Wenn Sie wissen möchten, in welchen Ihrer Verzeichnisse sich die größten Datenmengen befinden, ist das Programm *Festplattenbelegung analysieren* eine wertvolle Hilfe (Programmname baobab). Das Programm zeigt in einer anschaulichen Grafik an, welche Verzeichnisse und Unterverzeichnisse wie viele Daten enthalten (siehe Abbildung 5.10). Zur Erzeugung dieser Grafik müssen alle Unterverzeichnisse eingelesen werden. Dazu klicken Sie auf den Button PERSÖNLICHEN ORDNER EINLESEN oder DATEISYSTEM EINLESEN, wenn Sie das gesamte Dateisystem analysieren möchten (das kann eine ganze Weile dauern!).

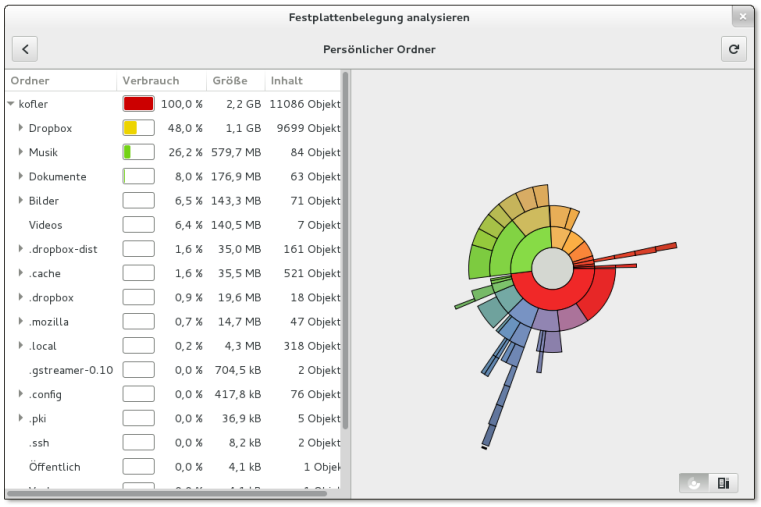


Abbildung 5.10 Platzbedarf von Verzeichnissen darstellen

Kontakte (gnome-contacts)

Mit dem Programm *Kontakte* können Sie ein lokales Adressbuch bzw. Online-Adressbücher von Google, Facebook, ownCloud oder Windows Live verwalten. Die Konfiguration des Adressbuchs erfolgt beim ersten Start des Programms bzw. in der Folge im Modul ONLINE-KONTEN der Systemeinstellungen. Die Adressdaten können auch von anderen Gnome-Programmen genutzt werden.

Schlüsselverwaltung (seahorse)

Diverse Gnome-Programme erfordern die Eingabe von Benutzerdaten und Passwörtern. Damit sich nicht jedes Programm selbst um die (möglichst sichere) Verwaltung der Passwörter kümmern muss, gibt es in Gnome eine zentrale Passwortverwaltung. Sie wird beispielsweise vom Dateimanager, dem Network Manager sowie von Evolution (einem E-Mail-Client) genutzt. Die Passwortdatenbank ist durch ein Master-Passwort abgesichert, das bei der ersten Nutzung des Programms abgefragt wird. Alle weiteren Datenbankzugriffe erfolgen dann aber ohne weitere Rückfragen.

Um gezielt einzelne Einträge aus der Datenbank zu entfernen, starten Sie das Programm *Passwörter und Verschlüsselung* (Programmname seahorse). Das Programm hilft auch bei der Verwaltung von GPG- und SSH-Schlüsseln. Derartige Schlüssel

brauchen Anwender zum Verschlüsseln oder Signieren ihrer E-Mails, Programmierer zum Signieren ihres Codes, Webentwickler zum Einloggen auf externen Rechnern etc.

PDF- und PostScript-Dateien (Evince)

Ein Doppelklick auf `*.pdf`- oder `*.ps`-Dateien startet das Programm Evince und zeigt das Dokument an. Sie können das Dokument nun durchsuchen, einzelne Seiten ausdrucken etc. Bei komplexen PDF-Dokumenten erzielen Sie mit dem Adobe Reader eine bessere Darstellung. Die Installation dieses kostenlosen, aber leider nicht als Open-Source-Code verfügbaren Programms ist in Abschnitt 8.2 beschrieben.

Terminalfenster (gnome-terminal)

Für Gnome-Terminalfenster ist das Programm `gnome-terminal` zuständig. Es zeichnet sich durch einige Besonderheiten aus:

- Webadressen werden automatisch unterstrichen, sobald Sie die Maus darüber bewegen. Mit der rechten Maustaste können Sie einen Webbrowser starten, um die Seite anzuzeigen.
- Wenn Sie Dateien oder Verzeichnisse vom Dateimanager per Drag&Drop in das Shell-Fenster bewegen, wird der vollständige Dateiname eingefügt.
- Mit Strg++ bzw. Strg+- ändern Sie rasch die Schriftgröße.
- Mit DATEI • NEUER REITER bzw. Strg+⇧+T öffnen Sie innerhalb des Fensters ein neues Terminal. Zwischen den Terminals können Sie per Mausklick oder mit Strg+Bild↑ bzw. Strg+Bild↓ wechseln.
- Tastenkürzel wie Alt+D führen in das Menü des Terminalfensters. Wenn Sie diese Tastenkürzel lieber zur Bearbeitung der Eingabezeile verwenden möchten, führen Sie BEARBEITEN • TASTENKOMBINATIONEN aus und aktivieren die Option ALLE MENÜKÜRZEL DEAKTIVIEREN.
- Eine Menge weiterer Konfigurationsmöglichkeiten bietet BEARBEITEN • PROFILE. Die Einstellungen können unterschiedlichen Profilen zugeordnet werden. Jedem Terminal kann dann sein eigenes Profil zugeordnet werden.

Texteditor (gedit)

Der Standardtexteditor von Gnome ist `gedit`. Das Programm ist leicht zu erlernen und für einfache Aufgaben vollkommen ausreichend. Profis werden aber bei Emacs oder Vi bleiben.

Web (Epiphany)

Seit Version 3.6 heißt der offizielle Webbrowser von Gnome nicht mehr Epiphany, sondern einfach *Web*. Freilich wird auch die gute Integration des Programms in den Gnome-Desktop nichts daran ändern, dass die meisten Anwender lieber eine aktuelle Version von Firefox oder Google Chrome einsetzen. Bei vielen Distributoren ist *Web* alias Epiphany deswegen nicht standardmäßig installiert. Wenn Sie das Programm ausprobieren möchten, müssen Sie das Paket `epiphany` bzw. `epiphany-browser` (Debian, Ubuntu) installieren.

5.4 Konfiguration und Interna

In Gnome 2.*n* waren die meisten Desktop-Elemente konfigurierbar: Panels konnten an allen vier Bildschirmrändern platziert werden, die darin enthaltenen Komponenten waren frei wählbar etc. Damit ist mit Gnome 3.*n* Schluss! Die Gnome-Systemeinstellungen sehen gerade einmal eine Veränderung des Bildschirmhintergrundbilds vor, im Übrigen in einem vollkommen verunglückten Dialog!

Als Entschädigung bietet Gnome 3 ein neues Erweiterungskonzept, das es ermöglicht, kleine, auf JavaScript basierende Erweiterungsprogramme mit einem Mausklick im Browser zu installieren. Nach ersten Startschwierigkeiten funktionieren die *gnome extensions* jetzt hervorragend und bilden das Fundament für unzählige nützliche Gnome-Erweiterungen und -Modifikationen.

Dieser Abschnitt stellt neben den Gnome-Systemeinstellungen und -Erweiterungen auch einige weitere Programme und Hilfsmittel vor, die bei der optimalen Konfiguration des Gnome-Desktops helfen. Bei dieser Gelegenheit lernen Sie gleich auch einige Gnome-Interna kennen.

Systemeinstellungen

In den Systemeinstellungen stellt Gnome eine ganze Palette von Werkzeugen zur Desktop- und Systemkonfiguration zur Verfügung. Am schnellsten starten Sie dieses Programm mit dem Menü Benutzername rechts oben im Panel.

Die Module der Systemeinstellungen helfen nicht nur bei den grundlegenden Einstellungen (Bildschirmhintergrund, Energiesparmodus, Spracheinstellungen etc.), sondern auch bei diversen Aufgaben der Systemadministration: Netzwerkeinstellungen, Bluetooth, Benutzerverwaltung, Zeiteinstellung etc. Wie alle Gnome-Werkzeuge beschränken sich auch die Systemeinstellungen auf das absolute Minimum. Beispielsweise können Sie mit dem Modul Benutzerkonten zwar neue Benutzer einrichten, aber keine Gruppen verwalten. Wenn Sie an die Grenzen der Gnome-Systemeinstellungen stoßen, müssen Sie auf Konsolenwerkzeuge oder auf die mitgelieferten Konfigurationsprogramme Ihrer Distribution zurückgreifen.

Versteckte Systemwerkzeuge

Nicht alle der früher über das System-Menü verfügbaren Werkzeuge sind in den Systemeinstellungen integriert. Weitere Einstellungsprogramme und Systemwerkzeuge können wie gewöhnliche Programme gestartet werden. Dazu aktivieren Sie die Aktivitätenansicht, klicken auf Anwendungen anzeigen und werfen einen Blick in die Programmgruppe Verschiedenes.

Drucker

Im Idealfall erfolgt die Druckerkonfiguration automatisch: Viele Distributionen erkennen die meisten USB-Drucker direkt beim Anstecken und führen die Konfiguration selbstständig durch. Das Gerät ist wenige Sekunden später bereit zum Drucken. Bequemer geht es nicht mehr!

Wenn dies nicht funktioniert bzw. wenn Sie einen Netzwerkdrucker besitzen, sollte bei der Konfiguration das Modul DRUCKER der Systemeinstellungen helfen. Bei meinen Tests konnte ich manche Netzwerkdrucker finden, andere aber nicht. Das Konfigurationswerkzeug kann aber nur Drucker konfigurieren, die es selbst im Netz erkennt. Eine manuelle Eingabe des Hostnamens oder der IP-Adresse des Druckers ist nicht vorgesehen.

Abhilfe schafft das bei den meisten Distributionen weiterhin mitgelieferte Programm `system-config-printer`. Dieses Programm ist zwar optisch weniger elegant als das DRUCKER-Modul der Systemeinstellungen, aber dafür ausgereift. HINZUFÜGEN • DRUCKER führt zu einem Assistenten, der eine Liste aller zur Auswahl stehenden Druckertypen anzeigt (inklusive eventuell erkannter Drucker, siehe Abbildung 5.11). Bei Netzwerkdruckern führt zumeist APPSOCKET/HP JETDIRECT zum Ziel. Nach der Auswahl des Druckertyps wählen Sie den Druckertreiber aus. Dabei geben Sie den Hersteller und das Modell an. Zuletzt müssen Sie dem Drucker noch einen Namen geben. Damit ist die Basiskonfiguration beendet. Alle weitergehenden Einstellungen und Druckeroptionen (Papiergröße, Duplex-Modus etc.) sind optional und erfolgen im Dialog EIGENSCHAFTEN.

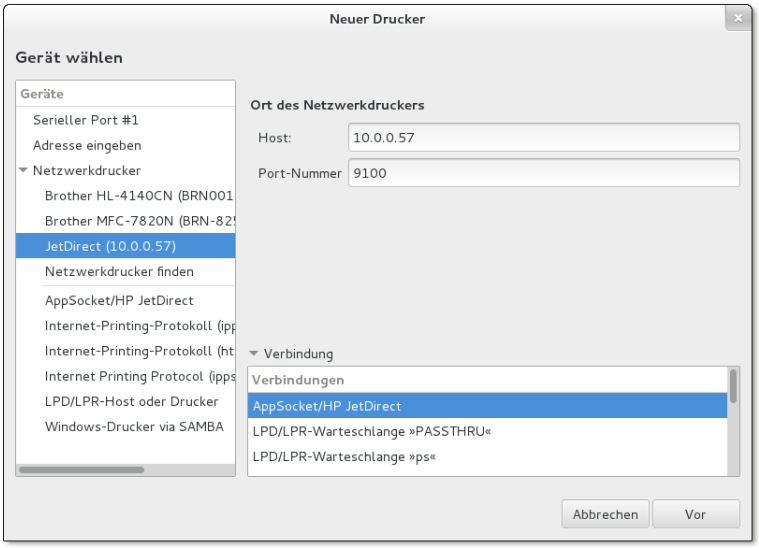


Abbildung 5.11 Druckerverwaltung mit system-config-printer

Online-Konten

Im Modul ONLINE-KONTEN können Sie die Login-Parameter diverser Online-Dienste angeben, darunter Google, Facebook, ownCloud und Windows Live (siehe Abbildung 5.12). Die Konten können dann in anderen Gnome-Anwendungen verwendet werden, z. B. in den Programmen *Kontakte* und *Evolution*.

Abbildung 5.12 Online-Konten einrichten

Standard-programme einstellen

Die meisten Distributionen mit Gnome als Basis verwenden Firefox als Webbrowser, Evolution oder Thunderbird als E-Mail-Programm etc. Wenn Sie möchten, dass Gnome beim Anklicken entsprechender Links andere Programme startet, finden Sie Einstellmöglichkeiten im Dialogblatt DETAILS • VORGABE-ANWENDUNGEN der Systemeinstellungen.

Welches Programm Gnome beim Einlegen einer Audio-CD, Video-DVD bzw. beim Anstecken eines MP3-Players starten soll, legen Sie im Dialogblatt WECHSELMEDIEN fest.

Tastatur

Die Tastatureinstellungen sind über zwei Module der Systemeinstellungen verteilt. Im Modul TASTATUR stellen Sie die Parameter der Tastenwiederholung sowie Tastaturkürzel ein. Einstellungen zum Tastaturlayout sind hingegen im Modul REGION UND SPRACHE • EINGABEQUELLEN gut versteckt.

Gnome Tweak Tool

Mit dem *Gnome Tweak Tool* (der Paketname lautet zumeist `gnome-tweak-tool`) können Sie einige Optionen des Gnome-Desktops verändern, für die in den offiziellen Systemeinstellungen Einstellmöglichkeiten fehlen. Mit dem Programm können Sie unter anderem einstellen,

- welche Buttons in der Fensterleiste dargestellt werden,
- welche Schrift auf dem Desktop verwendet werden soll,

- welches Fensterthema gelten soll,
- wie sich Notebooks beim Schließen des Deckels verhalten sollen,
- ob der Dateimanager auf dem Desktop Icons darstellen darf und
- ob das Uhrzeit-Applet auch das Datum anzeigen soll.

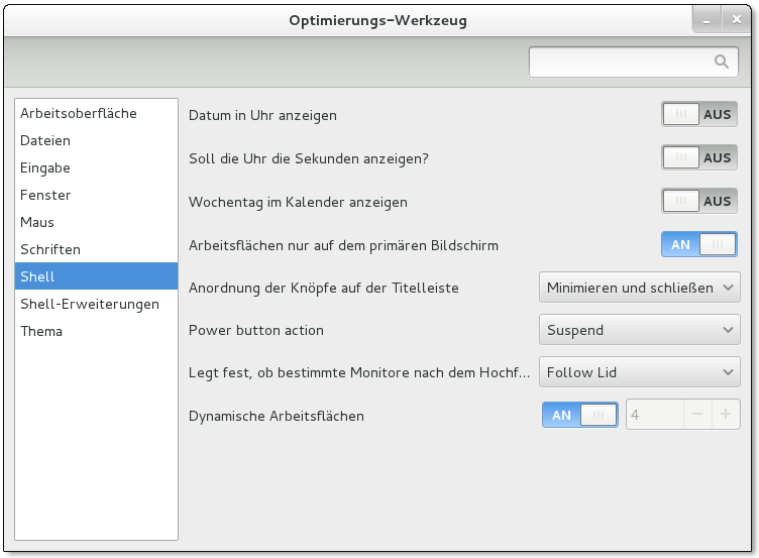


Abbildung 5.13 Gnome Tweak Tool

Manche Konfigurationsänderungen werden sofort wirksam, andere erst dann, wenn Sie die Gnome Shell mit Alt+F2 r ↵ neu starten bzw. sich aus- und neu einloggen.

Gnome Shell Extensions

Die Gnome Shell greift intern stark auf JavaScript zurück. Deswegen können Sie mit wenigen Zeilen JavaScript-Code umfassende Modifikationen am Desktop durchführen. Gnome sieht hierfür einen speziellen Extensions-Mechanismus vor. Seit Version 3.4 können derartige Erweiterungen unkompliziert im Webbrowser heruntergeladen, aktiviert und bei Missfallen auch gleich wieder deaktiviert werden (siehe Abbildung 5.14). Die folgende Website lädt wirklich zum Ausprobieren ein!

https://extensions.gnome.org

Die meisten Erweiterungen werden sofort wirksam, nur wenige erfordern einen Neustart der Gnome Shell oder einen neuerlichen Login. Offiziell trägt die Gnome-Extensions-Website noch ein Beta-Emblem. Nach meinen Erfahrungen funktioniert das System bereits ausgezeichnet. Das Problem sind aber Versionswechsel: Wenn Sie

ein Update auf eine neuere Gnome-Version durchführen, kann es vorkommen, dass einzelne Erweiterungen nicht mehr funktionieren.

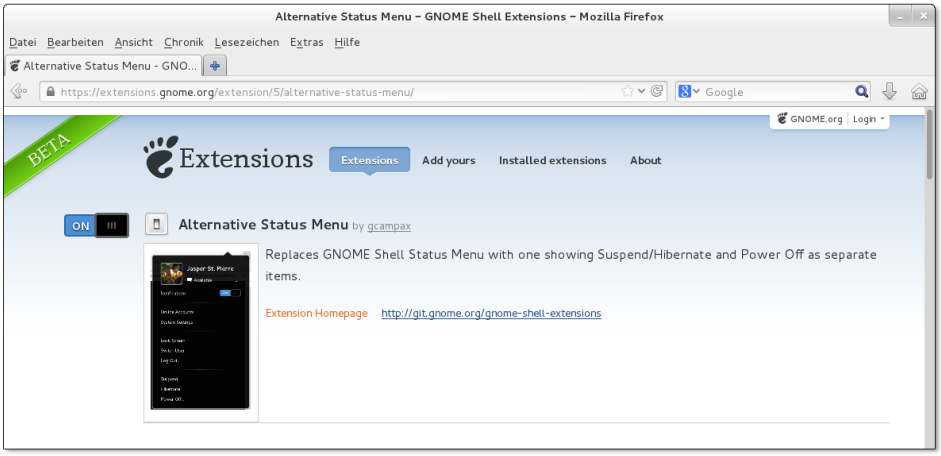


Abbildung 5.14 Installation einer Gnome-Shell-Erweiterung direkt im Webbrowser

Im Folgenden stelle ich Ihnen einige Erweiterungen vor, die bei meinen Tests zufriedenstellend funktioniert haben:

- **Alternative Status Menu:** Die Erweiterung bewirkt, dass das Menü ganz rechts im Panel außer ABMELDEN auch die Einträge BEREITSCHAFT, RUHEZUSTAND und AUSSCHALTEN enthält.
- **Alternate Tab:** Mit der Aktivierung dieser Erweiterung funktioniert Alt+⇆ wieder wie früher.
- **Application Menu:** Diese Erweiterung bildet das Gnome-2-Menü nach.
- **Media Player Indicator:** Diese Erweiterung ermöglicht die Steuerung der meisten Media-Player über ein Panel-Icon, wie dies z. B. auch unter Ubuntu üblich ist.
- **Remove Accessibility:** Wenn Sie diese Erweiterung aktivieren, verschwindet das Icon BARIERREFREIHEIT aus dem Panel.
- **Sensors:** Diese Erweiterung zeigt die CPU-Temperatur und andere Hardware-Daten im Panel an. Die Erweiterung erfordert je nach Distribution die Installation des Pakets `sensors` oder `lm_sensors`.
- **System Monitor:** Die Erweiterung bettet einen System-Monitor in das Panel ein und zeigt die CPU-Auslastung, Speichernutzung etc. an.

Gnome-Konfigurationsdateien

dconf-Datenbank

Parallel zu Gnome 3.0 wurde das neue `dconf`-System zur Speicherung von Programmeinstellungen entwickelt. Die `dconf`-Daten befinden sich in der binären Datenbankdatei `.config/dconf/user`. Allerdings verwenden noch nicht alle Gnome-Programme das `dconf`-System.

In Entwicklerkreisen war die Einführung des `dconf`-Formats nicht unumstritten. Kritiker befürchten, dass die binäre Datei auf lange Sicht ähnlich schwer zu warten ist wie die Windows-Registrierungsdatenbank. Zudem erscheint es riskant, Einstellungen zahlreicher Programme in einer einzigen binären Datei zu vereinen: Sollte diese Datei irrtümlich oder durch einen Dateisystemfehler zerstört werden, hätte das Auswirkungen auf große Teile des Desktops.

Der Vorteil von `dconf` gegenüber dem älteren `gconf`-System liegt in der wesentlich höheren Zugriffsgeschwindigkeit. Während des Starts von Gnome müssen unzählige Einstellungen gelesen werden. Das `dconf`-System beschleunigt den Gnome-Start spürbar.

Gnome-Programme greifen direkt über API-Funktionen (Application Programming Interface) auf die `dconf`-Datenbank zu. Wenn Sie `dconf`-Einstellungen von außen lesen oder ändern möchten, installieren Sie das Paket `dconf-tools` und starten das Programm `dconf-editor` (siehe Abbildung 5.15). Die Benutzeroberfläche zeigt links eine baumartige Struktur aller Einstellungsverzeichnisse, rechts die in diesem Verzeichnis enthaltenen Parameter.

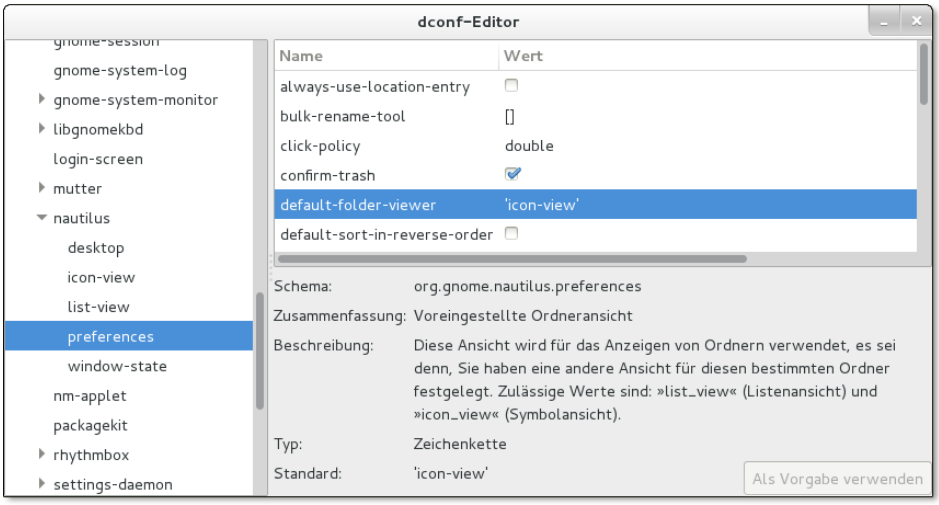


Abbildung 5.15 Einstellungen in der dconf-Datenbank verändern

Mit dem Kommando `gsettings` ist es möglich, die `dconf`-Einstellungen im Terminal oder durch ein Script zu verändern. Das folgende Kommando bewirkt, dass Nautilus standardmäßig die Listenansicht verwendet, nicht die Symbolansicht:

```
user$  gsettings set org.gnome.nautilus.preferences \
         default-folder-viewer 'list-view'
```

Falls Sie `gsettings` via SSH ausführen, müssen Sie den SSH-Client mit der Option `-x` starten. `gsettings` ist zwar selbst kein X-Programm, greift aber auf das Programm `dbus-launch` zurück. Und dieses wertet offensichtlich Umgebungsvariablen aus, die nur gesetzt sind, wenn SSH das X-Protokoll mitüberträgt.

gconf-Datenbank

Ältere bzw. noch nicht auf das `dconf`-System umgestellte Gnome-Programme speichern ihre Einstellungen zumeist in der `gconf`-Datenbank. Intern besteht diese Datenbank aus unzähligen kleinen XML-Dateien, die im Verzeichnis `.gconf` sowie in dessen Unterverzeichnissen gespeichert werden. Auch zur Veränderung von `gconf`-Einstellungen gibt es mit dem `gconf-editor` eine einfache Benutzeroberfläche. Sie sieht ganz ähnlich aus wie die des `dconf-editor`. Alternativ dazu können Sie die Einstellungen auch ohne Benutzeroberfläche mit dem Kommando `gconftool-2` verändern.

Interna

Hinter den Kulissen ist für die Verwaltung der Fenster sowie für den Start von Programmen (AKTIVITÄTEN) das Programm *Gnome Shell* (Kommando `gnome-shell`) verantwortlich, in das wiederum der neue Window Manager *Mutter* integriert ist. Mutter ist eine Weiterentwicklung des Window Managers *Metacity*, wobei die wichtigste Neuerung die Unterstützung von 3D-Effekten ist. Compiz ist deswegen für die Ausführung von Gnome 3.*n* nicht mehr erforderlich.

Autostart

Während des Starts von Gnome werden eine Menge Programme automatisch gestartet. Welche dies sind, steuern `*.desktop`-Dateien aus den folgenden Autostart-Verzeichnissen:

`~/.config/autostart/*.desktop`	(persönliche Autostart-Programme)
`/usr/share/gnome/autostart/*.desktop`	(globale Autostart-Programme für Gnome)
`/etc/xdg/autostart/*.desktop`	(globale Autostart-Programme für alle Desktops, also für Gnome und KDE)

In den Systemeinstellungen gibt es leider kein Modul, um den automatischen Start von Programmen zu steuern. Abhilfe schaffen Alt+F2 `gnome-session-properties`, die Gnome-Erweiterung *Startup Applications* oder die manuelle Konfiguration von `*.desktop`-Dateien. Der Aufbau solcher Dateien geht aus dem folgenden Beispiel hervor. Die Datei ist für das Abspielen des Login-Tons verantwortlich:

```
[Desktop Entry]
Type=Application
Name=GNOME Login Sound
Comment=Plays a sound whenever you log in
Exec=/usr/bin/canberra-gtk-play --id="desktop-login" --description="GNOME Login"
OnlyShowIn=GNOME;
AutostartCondition=GSettings org.gnome.desktop.sound event-sounds
X-GNOME-Autostart-Phase=Application
X-GNOME-Provides=login-sound
```

GDM

Für den Login bei auf Gnome basierenden Distributionen ist in der Regel der *Gnome Display Manager* (`gdm`) verantwortlich. Eine Ausnahme ist Ubuntu, das stattdessen den *Light Display Manager* (`lightdm`) verwendet.

Eine Beschreibung von GDM finden Sie in Abschnitt 24.2. Dort erfahren Sie auch, wie Sie die Konfigurationsdatei `/etc/gdm/custom.conf` einrichten, wenn Sie den Login während des Rechnerstarts automatisieren möchten. Nur unter openSUSE sollten Sie auf Veränderungen an `custom.conf` verzichten und den Auto-Login stattdessen mit YaST einrichten.

MIME

Wenn nach einem Doppelklick auf eine MP3-Datei in Nautilus automatisch Rhythmbox oder Banshee erscheint, dann sind hierfür die MIME-Einstellungen von Gnome verantwortlich. MIME steht für Multipurpose Internet Mail Extensions und ist eine Art Datenbank, die eine Zuordnung zwischen Dateitypen und Programmen herstellt.

Am einfachsten erfolgen Änderungen an der MIME-Konfiguration direkt im Dateimanager: Dort klicken Sie die betreffende Datei an, führen per Kontextmenü Eigenschaften • Öffnen mit aus und wählen das gewünschte Programm. Die Einstellung gilt in Zukunft für alle Dateien mit derselben Endung.

Individuelle Änderungen an der MIME-Konfiguration werden hier gespeichert:

```
~/.local/share/mime/*
~/.local/share/applications/mimeapps.list
```

Weitere Informationen zur MIME-Datenbank unter Gnome finden Sie hier:

http://standards.freedesktop.org/shared-mime-info-spec/shared-mime-info-spec-latest.html

XDG-Verzeichnisse und -Scripts

Vor einigen Jahren wurde im Rahmen des Portland-Projekts eine Reihe gemeinsamer Standards definiert. Sie helfen dabei, Programme unabhängig von Gnome oder KDE richtig in den Desktop zu integrieren. Später führte die X Desktop Group (XDG) diese Bemühungen fort, und heute ist es das Projekt freedesktop.org.

Standardverzeichnisse

Beim ersten Login werden im Heimatverzeichnis die Unterverzeichnisse `Bilder`, `Dokumente`, `Downloads`, `Musik`, `Öffentlich`, `Videos` und `Vorlagen` erzeugt. Wenn eine andere Sprache als Deutsch eingestellt ist, erhalten diese Verzeichnisse andere Namen. Hinter den Kulissen ist das Paket `xdg-user-dirs` für die Verzeichnisse verantwortlich.

Die Konfiguration erfolgt durch die Datei `user-dirs.dirs`. Dieses Verzeichnis stellt sicher, dass XDG-kompatible Programme die Verzeichnisse unabhängig von der eingestellten Sprache finden. Unter Gnome werden die Verzeichnisse, wenn die Sprache verändert wurde, nach einer Rückfrage sogar entsprechend umbenannt (Paket `xdg-user-dirs-gtk`).

Wenn Sie die Standardverzeichnisse nicht wünschen, löschen Sie die Verzeichnisse und legen die folgende neue Datei an:

```
# ~/.config/user-dirs.conf
enabled=False
```

Sie können diese Einstellung auch systemweit in `/etc/xdg/user-dirs.conf` vornehmen.

Konfigurationsverzeichnisse

Viele, wenn auch leider nicht alle Gnome- und KDE-Programme verwenden zum Speichern von Konfigurationseinstellungen und internen Daten speziell dafür vorgesehene Verzeichnisse. Die Verzeichnisnamen beginnen mit einem Punkt und gelten damit als »verborgen«. Die Verzeichnisse werden deswegen im Dateimanager standardmäßig nicht angezeigt.

- Das `.cache`-Verzeichnis ist zur Speicherung von temporären Dateien gedacht, die bei Bedarf neuerlich erzeugt werden können – also z. B. verkleinerte Bilder (Thumbnails), Suchindizes etc. Die Zwischenspeicherung dient dazu, häufig vorkommende Arbeitsabläufe zu beschleunigen.
- Das `.config`-Verzeichnis ist zur Speicherung von Programmeinstellungen vorgesehen, wobei jedes Programm ein eigenes Unterverzeichnis verwendet.
- Im `.local`-Verzeichnis werden Benutzerdaten gespeichert. Üblicherweise legt jedes Programm hierfür das Unterverzeichnis `share/programmname` an.

xdg-Scripts

Das Paket `xdg-utils` stellt die folgenden Scripts zur Verfügung. Eine genauere Beschreibung finden Sie in den `man`-Seiten der jeweiligen Kommandos.

- `xdg-desktop-menu` fügt dem Desktop-Menü einen neuen Eintrag hinzu.
- `xdg-desktop-icon` installiert ein neues Icon auf dem Desktop.
- `xdg-icon-resource` installiert Icon-Ressourcen.
- `xdg-mime` fragt die MIME-Datenbank ab bzw. richtet einen neuen MIME-Datentyp ein.

- `xdg-open` öffnet ein Dokument im Standardprogramm des Benutzers.
- `xdg-email` sendet eine E-Mail im Standard-E-Mail-Programm des Benutzers.
- `xdg-screensaver` steuert den Bildschirmschoner.

5.5 Gnome-Varianten

Mit der Fertigstellung von Gnome 3 ist die Gnome-Welt sehr inkohärent geworden: Manche Distributionen setzen noch auf Gnome 2 (z. B. RHEL 6) oder verwenden den Gnome 2-Fork MATE (Linux Mint MATE). Andere Distributionen nutzen zwar Kernkomponenten von Gnome 3, modifizieren die Funktion und das Erscheinungsbild des Desktops aber derart, dass man eigentlich nicht mehr von Gnome 3 sprechen kann (Ubuntu, Linux Mint Cinnamon). RHEL 7 wird zwar voraussichtlich Gnome 3 als Standarddesktop verwenden, aber nicht mit der in diesem Kapitel beschriebenen Gnome-Shell, sondern im sogenannten Klassik-Modus. Dieser Abschnitt gibt einen kurzen Überblick über die wichtigsten Gnome-Varianten mit der Ausnahme von Unity. Diesen Ubuntu-spezifischen Desktop stelle ich Ihnen in Kapitel 7 näher vor.

Gnome 2

In älteren Distributionen kommt häufig noch Gnome 2 zum Einsatz. Zentrale Merkmale von Gnome 2 sind zwei Panels. Üblicherweise enthält das obere Panel ein Startmenü sowie einige Applets, das untere Panel die Taskbar. Einträge des Startmenüs können Sie mit der rechten Maustaste Als Starter zum Panel hinzufügen. Ebenfalls mit der rechten Maustaste können Sie Panel-Elemente hinzufügen, verschieben und entfernen. Wenn Sie Platz sparen möchten, können Sie ein Panel löschen und die dort befindlichen Applets im anderen Panel unterbringen.

llvmpipe

Die Gnome-Shell setzt eine Grafikkarte mit 3D-Unterstützung sowie einen dazu passenden Treiber voraus. Sind die Hardware-Voraussetzungen nicht erfüllt, werden die fehlenden 3D-Funktionen bei aktuellen Distributionen durch die CPU emuliert. Für die Emulation verantwortlich ist die `llvmpipe`-Bibliothek. Die Geschwindigkeit von Gnome leidet unter dieser Emulation ein wenig, aber Gnome bleibt selbst in virtuellen Maschinen gut verwendbar – ganz im Gegensatz zu Ubuntu, dessen aktuellen Unity-Versionen in Virtualisierungssystemen unerträglich langsam sind. Wenn Sie herausfinden möchten, ob Ihr Grafiksystem die `llvmpipe`-Bibliothek verwendet, führen Sie `glxinfo | grep 'OpenGL render'` aus.

Fallback-Modus zu Gnome 3

Distributionen mit älteren Gnome-3-Versionen sind nicht `llvmpipe`-kompatibel. Das betrifft insbesondere Debian 7. Wenn Gnome erkennt, dass keine 3D-Funktionen zur Verfügung stehen, aktiviert es den Fallback-Modus. Damit sieht Gnome 3 so ähnlich aus wie Gnome 2. Gnome-2-Applets können allerdings auch im Fallback-Modus nicht verwendet werden.

Ein wesentlicher Unterschied zu Gnome 2 besteht darin, dass Sie für alle Veränderungen im Panel zusätzlich zur linken oder rechten Maustaste auch Alt drücken müssen. Auf diese Weise soll der Desktop vor ungewollten Veränderungen geschützt werden.

Klassik-Modus

Der Fallback-Modus war sowohl für die Anwender als auch für die Gnome-Entwickler ein ungeliebtes Stiefkind. Es wurde daher mit Gnome 3.8 durch den neuen Klassik-Modus ersetzt (siehe Abbildung 5.16). Dabei handelt es sich um eine vordefinierte Sammlung von Gnome-Erweiterungen (Extensions), mit denen Gnome 3 ähnlich aussieht wie Gnome 2: Es gibt ein traditionelles Startmenü, Icons auf dem Desktop und eine Task-Leiste am unteren Bildschirmrand.

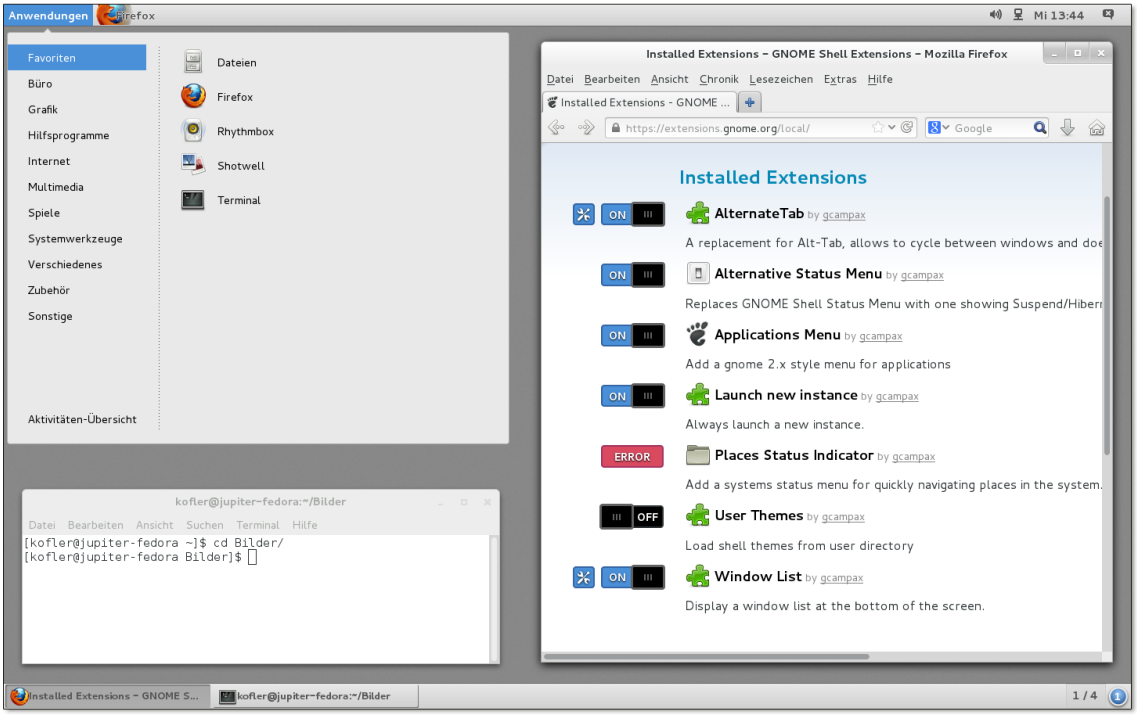


Abbildung 5.16 Im Klassik-Modus sieht Gnome 3 ähnlich aus wie Gnome 2.

Bei den meisten Distributionen müssen die Erweiterungspakete des Klassik-Modus extra installiert werden, unter Fedora z. B. mit `yum install gnome-classic-session`. Beim nächsten Login können Sie dann zwischen GNOME und GNOME CLASSIC wählen.

Gerade umgekehrt wird es voraussichtlich bei RHEL 7 sein: Um die konservativen Unternehmenskunden nicht mit zu viel Modernität zu überfordern, soll der Klassik-

modus dort standardmäßig zum Einsatz kommen. Wer will, kann selbst auf das »echte« Gnome umsteigen.

Bei meinen Tests unter Gnome 3.8 funktionierte der Klassik-Modus zufriedenstellend. Persönlich hätte ich mir noch konfigurierbare Schnellstart-Icons im Panel gewünscht; diese lassen sich bei Bedarf mit der Gnome-Extension *Frippery Panel Favorites* realisieren.

MATE

Seit der Fertigstellung von Gnome 3 wird Gnome 2 nicht mehr gewartet. Damit sind selbst Distributionen, die eigentlich gerne bei Gnome 2 bleiben würden, auf kurz oder lang zu einem Umstieg auf Gnome 3 gezwungen – wäre da nicht MATE!

http://mate-desktop.org

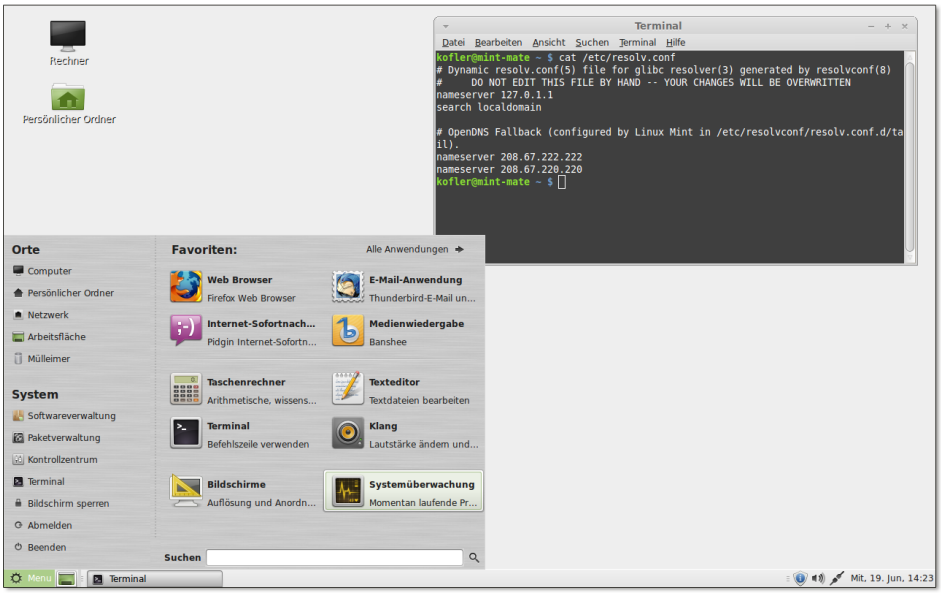


Abbildung 5.17 Linux Mint mit dem MATE-Desktop

MATE ist ein Fork von Gnome 2. Das MATE-Projekt hat also den Code von Gnome 2 übernommen, den einzelnen Komponenten neue Namen gegeben (um Konflikte mit dem Gnome-Projekt zu vermeiden) und kümmert sich um Fehlerkorrekturen. Größere Änderungen oder Neuerungen sind nicht geplant. Wie elegant ein Desktop auf der Basis von Gnome 2 alias MATE aussehen kann, beweist Linux Mint mit der auf MATE basierenden Distribution (siehe Abbildung 5.17).

Cinnamon

Der Cinnamon Desktop ist eine ebenfalls vom Linux-Mint-Team entwickelte Erweiterung zu Gnome 3. Cinnamon versucht, Gnome 3 so zu konfigurieren, dass es wie Gnome 2 zu bedienen ist – also mit herkömmlichen Panels, ohne Dock etc. Die Idee von Cinnamon ist somit dieselbe wie bei dem ab Gnome 3.8 verfügbaren Klassik-

Modus, auch wenn die Realisierung und die Grundkonfiguration vollkommen anders aussieht.

http://cinnamon.linuxmint.com

Ob der Weg zukunftsweisend ist, bleibt abzuwarten: Cinnamon-Anwender verzichten auf viele Neuerungen von Gnome 3, dennoch geht die Kompatibilität zu Gnome 2 verloren. Cinnamon verwendet eigene Applets und Erweiterungen, die inkompatibel zu Gnome 2, Gnome 3 und Unity sind. Wie populär das Konzept trotz seiner Nachteile ist, beweist einerseits die erstaunlich große Anzahl von Applets, Desklets und anderen Erweiterungen auf der Cinnamon-Website, andererseits die Beliebtheit von Linux Mint: Die Distribution ist nun schon seit mehreren Jahren auf Platz 1 des Zugriffs-Rankings auf *http://distrowatch.com*.

Kapitel 6
KDE

KDE ist eine populäre Alternative zu dem im vorigen Kapitel vorgestellten Gnome-Desktop. KDE erfüllt im Prinzip dieselben Aufgaben, sieht aber anders aus und verwendet intern andere Bibliotheken und Protokolle. Die Abkürzung KDE stand ursprünglich für *Kool Desktop Environment*, später wurde daraus das *K Desktop Environment*. KDE basiert auf Qt, einer Open-Source-Bibliothek, die ursprünglich von Troll Tech entwickelt wurde. Umfassende Informationen zu KDE gibt diese Website:

http://kde.org

Im Vergleich zu Gnome bietet KDE mehr Spezialfunktionen und Konfigurationsmöglichkeiten, die technisch versierten Linux-Benutzern entgegenkommen. Dem steht aber eine etwas schwierigere Bedienung gegenüber, weswegen viele Distributionen standardmäßig auf Gnome basieren.

Sofern Ihre Distribution entsprechende Pakete anbietet, spricht nichts gegen eine Parallelinstallation von Gnome und KDE. Sie können dann vor dem Login angeben (üblicherweise mit dem Button bzw. dem Menüpunkt SITZUNG), ob Sie KDE oder Gnome nutzen möchten.

Im Mittelpunkt dieses Kapitels stehen die Basisfunktionen von KDE. Freilich sieht KDE je nach Distribution ganz unterschiedlich aus: Der Aufbau des Login-Bildschirms, die Menüeinträge des Startmenüs, die optische Gestaltung des Desktops und die Auswahl der mitgelieferten Programme und Konfigurationshilfen variieren stark.

KDE und die Maus

Der vielleicht offensichtlichste Unterschied zwischen KDE und anderen Benutzeroberflächen ist der Umgang mit der Maus: Unter KDE reicht statt eines Doppelklicks ein einfacher Mausklick, um Dateien zu öffnen, Module zu starten oder vergleichbare Operationen durchzuführen. Das ist anfangs gewöhnungsbedürftig, ermöglicht aber ein effizientes und komfortables Arbeiten. Wenn Sie sich nicht umstellen wollen, können Sie natürlich auch KDE doppelklick-konform einrichten: Dazu starten Sie im KDE-Menü die SYSTEMEINSTELLUNGEN, wechseln in das Modul EINGABEGERÄTE • MAUS und aktivieren die Option DOPPELKLICK ZUM ÖFFNEN VON DATEIEN UND ORDNERN.

6.1 Aufbau des Desktops

Login und Logout

Bevor Sie unter KDE arbeiten können, müssen Sie sich mit Ihrem Login-Namen und dem Passwort anmelden. Wenn Sie außer KDE andere Desktop-Systeme oder Window Manager installiert haben, können Sie über ein Menü das gewünschte Desktop-System auswählen.

Um sich abzumelden oder den Rechner herunterzufahren, wählen Sie im KDE-Menü den Eintrag VERLASSEN • ABMELDEN bzw. VERLASSEN • HERUNTERFAHREN. Je nach Hardware besteht hier auch die Möglichkeit, den Rechner in einen Ruhe- oder Energiesparmodus zu versetzen.

Benutzerwechsel

Das KDE-Menü bietet mit dem Kommando VERLASSEN • BENUTZER WECHSELN die Möglichkeit, dass sich ein zweiter Benutzer anmeldet, ohne dass der aktuelle Benutzer alle seine Programme beenden muss. Intern wird für jeden Benutzer ein eigenes Grafiksystem (ein X-Server) gestartet. Mehrere parallele Logins erfordern daher eine Menge Ressourcen und funktionieren nur auf schnellen Rechnern zufriedenstellend. Zum raschen Wechsel zwischen den angemeldeten Benutzern gelten bei den meisten Distributionen die folgenden Tastenkürzel – nur bei Fedora ist dem ersten Benutzer das Tastenkürzel Strg+Alt+F1 zugeordnet:

Strg+Alt+F7	erster Benutzer
Strg+Alt+F8	zweiter Benutzer
Strg+Alt+F9	dritter Benutzer
...	...

Desktop

Abbildung 6.1 zeigt den Desktop eines KDE-Systems. Wie bereits erwähnt, hängt das Aussehen des Desktops stark von der Standardkonfiguration Ihrer Distribution ab. Der Desktop setzt sich standardmäßig aus einem Panel am unteren Bildschirmrand und dem eigentlichen Arbeitsbereich zusammen. Das Panel enthält das KDE-Menü, eventuell einige Icons zum raschen Start von Programmen, eine Task-Leiste mit Icons aller offenen Fenster sowie diverse Hilfsprogramme.

Plasma

Die vielleicht wichtigste KDE-Komponente heißt Plasma. Sie ermöglicht es, interaktive Objekte auf dem Desktop oder im Panel abzulegen und dort zu bedienen. Diese Funktion ist mit Apples Dashboard vergleichbar.

Plasmoids

Der eigentliche Arbeitsbereich (Desktop) ist anfänglich zumeist leer. Sie können direkt im Desktop oder im Panel Miniprogramme ausführen, die in der KDE-Nomenklatur *Plasmoids* heißen. Die Uhr rechts oben in Abbildung 6.1 ist ein Beispiel für ein Plasmoid. Über das Kontextmenükommando MINIPROGRAMME HINZUFÜGEN bzw. über den Button WERKZEUGKASTEN in der rechten oberen Ecke des Bildschirms fügen Sie Plasmoids in den Desktop ein (siehe Abbildung 6.2).

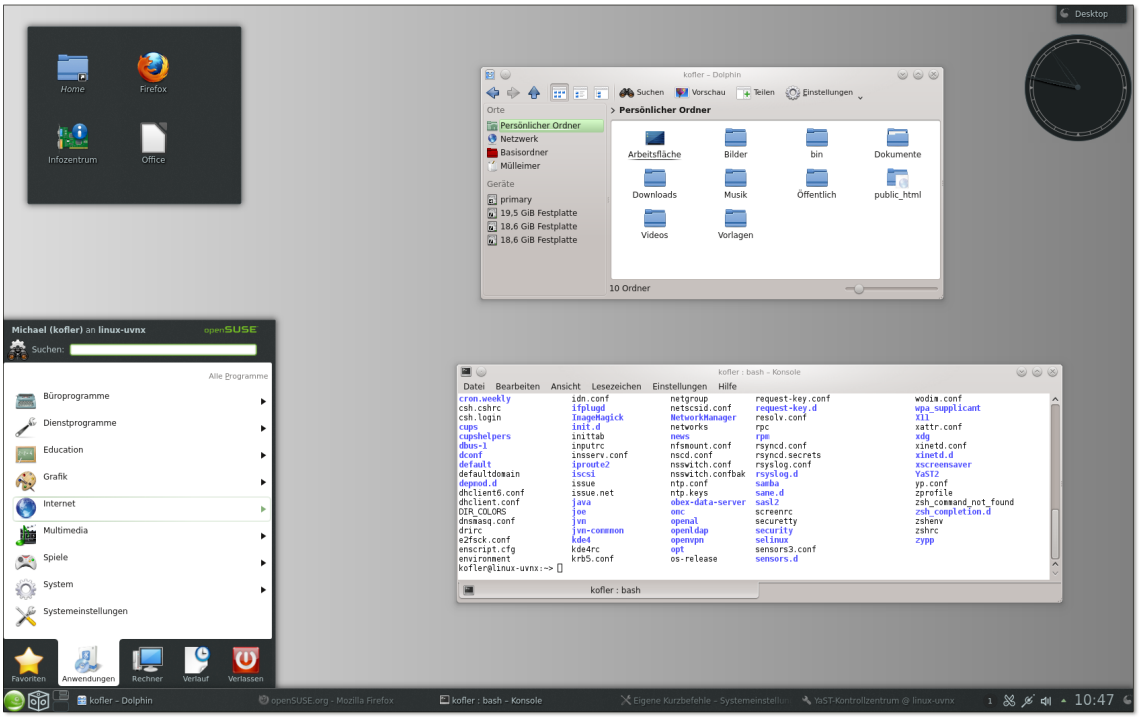


Abbildung 6.1 Der KDE-Desktop

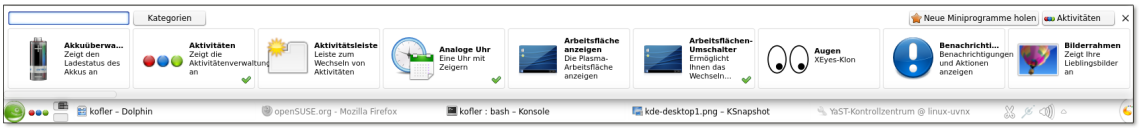


Abbildung 6.2 Miniprogramme (Plasmoids) einfügen

Leider ist die Plasmoid-Auswahl aus einer schmalen Liste sehr unübersichtlich. Immerhin ist es möglich, die Liste der Plasmoids nach Kategorien zu filtern.

Wie unter alten Windows-Versionen können Sie auch unter KDE Icons auf dem Desktop abzulegen. Die KDE-Entwickler empfehlen aber, auf Desktop-Icons zu verzichten und stattdessen das Plasmoid ORDNER-ANSICHT zu verwenden und damit das Verzeichnis `Desktop` mit den darin enthaltenen Icons in einer Art Plasma-Fenster anzuzeigen (links oben in Abbildung 6.1). Es handelt sich dabei um kein herkömmliches Fenster. Die ORDNER-ANSICHT befindet sich deswegen immer hinter allen regulären Fenstern und sieht auch optisch anders aus.

Alle Icons und Plasmoids in die erste Reihe, bitte!

Persönlich bin ich kein Freund von Icons, Miniprogrammen und anderen Desktop-Objekten: Bei mir verdecken in der Regel mehrere große Fenster den gesamten Arbeitsbereich. Wenn Sie gern Icons und Plasmoids verwenden, sollten Sie sich die Tastenkombination Strg+F12 merken: Sie rückt die Desktop-Elemente in den Vordergrund und stellt alle Fenster abgedunkelt in den Hintergrund. Nochmals Strg+F12 oder Esc stellt den bisherigen Desktop-Zustand wieder her.

Sobald Sie die Maus über ein Icon oder Plasmoid bewegen, erscheinen auf einer Seite einige Buttons, mit denen Sie die Größe und Konfiguration des Miniprogramms verändern können. Diese Einstellungen werden in der Datei `.kde4/share/config/plasma-desktop-appletsrc` gespeichert.

Panels

Ein Panel bzw. eine Kontrollleiste ist ein rechteckiger Bereich, der sich an einem Bildschirmrand befindet (standardmäßig unten). Das Panel an sich hat keine Funktion, sondern dient nur als Container für Miniprogramme. Auch so grundlegende Elemente wie das Menü und die Taskleiste sind in KDE 4 als Plasmoids implementiert! Deswegen ist es grundsätzlich möglich (wenngleich unüblich), auf ein Panel ganz zu verzichten und das Menü, die Taskleiste und andere typische Panel-Inhalte direkt auf dem Desktop abzulegen. Der größte Vorteil des Panels besteht darin, dass dieser Bereich nicht von Fenstern überdeckt werden kann. Außerdem spart die kompakte Anordnung mehrerer Plasmoids in einem Panel viel Platz.

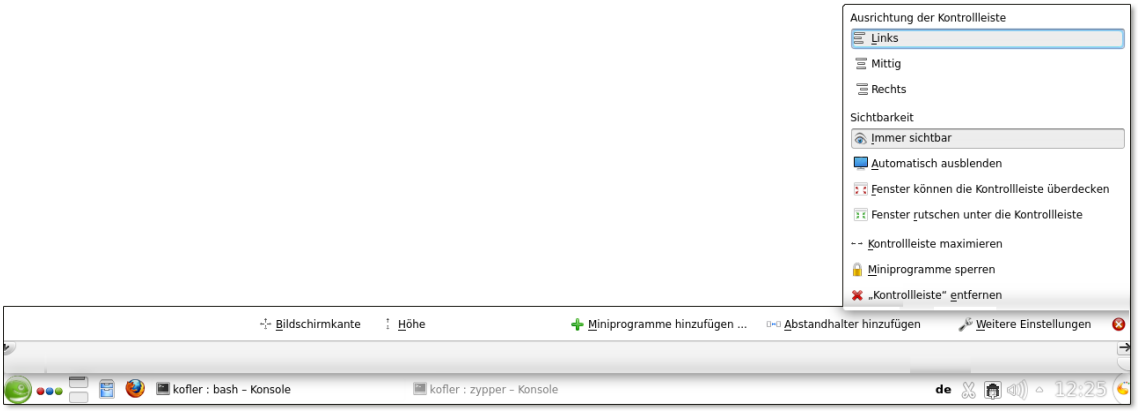


Abbildung 6.3 Panel-Konfiguration

Über das Kontextmenükommando Einstellungen für die Kontrollleiste können Sie Größe, Position und andere Eigenschaften des Panels verändern sowie Miniprogramme hinzufügen, verschieben und entfernen (siehe Abbildung 6.3). Dazu wird oberhalb bzw. neben dem Panel eine Art Menü eingeblendet. Die Farbe bzw.

Hintergrundgrafik des Panels ist übrigens durch das Desktop-Design vorgegeben und kann nur durch die Auswahl eines anderen Designs verändert werden (siehe Abschnitt 6.4).

Wichtige Miniprogramme (Plasmoids)

KDE-Menü (Kickstart)

Das wahrscheinlich wichtigste Plasmoid ist das KDE-Menü Kickstart (links unten in Abbildung 6.1). Es ist in fünf Kategorien gegliedert:

- Favoriten enthält die für den Benutzer wichtigsten Programme. Um ein Programm in diesen Bereich aufzunehmen, führen Sie in den anderen Menükategorien das Kontextmenükommando Zu Favoriten hinzufügen aus.
- Anwendungen führt in eine hierarchisch strukturierte Liste aller Programme.
- Rechner gibt Ihnen die Möglichkeit, Administrationsprogramme zu starten sowie wichtige Verzeichnisse zu öffnen.
- Verlauf enthält eine Liste der zuletzt gestarteten Programme bzw. zuletzt genutzten Dateien oder Verzeichnisse.
- Verlassen enthält Kommandos zum Abmelden, zum Benutzerwechsel sowie zum Herunterfahren des Rechners.

Losgelöst von den Kategorien enthält das KDE-Menü eine Suchfunktion. Sie eignet sich insbesondere dazu, um Programme rasch zu starten, ohne durch die Registerkarten des Menüs Programme zu navigieren. Sie können das Menü selbst modifizieren. Dazu klicken Sie den Menü-Startbutton mit der rechten Maustaste an und starten den Menü-Editor. Oft benötigte Programme können Sie per Drag&Drop in einen leeren Bereich des Panels oder Desktops verschieben. Sie erscheinen dort als Icons und ermöglichen so einen besonders schnellen Start.

Task-Leiste (Fensterleiste)

Das Miniprogramm Fensterleiste zeigt für jedes Fenster ein Icon an und entspricht so der aus Windows bekannten Task-Leiste. Über den Einstellungsdialog können Sie angeben, ob mehrere Fenster eines Programms zu einer Gruppe zusammengefasst werden sollen (z. B. alle Gimp-Fenster) und wie die Fenster sortiert werden sollen.

Die Fensterleiste kann ähnlich wie das Mac-OS-X-Dock bzw. wie unter Windows 7 auch dazu verwendet werden, um darin Start-Icons von gerade nicht laufenden Programmen abzulegen. Dazu führen Sie bei einem laufenden Programm das Kontextmenükommando Erweitert • Einen Starter für Programmname anzeigen, wenn es nicht läuft aus.

Arbeitsflächen

Arbeitsflächen ermöglichen es, die Fenster der laufenden Programme auf mehrere virtuelle Desktops zu verteilen und zwischen diesen Desktops zu wechseln. Das erleichtert die Arbeit und verbessert die Übersicht, wenn Sie sehr viele Fenster gleichzeitig öffnen. Für die Verwaltung der Arbeitsflächen ist das Plasmoid Arbeitsflächen-Umschalter verantwortlich. In dessen Einstellungsmenü stellen Sie die gewünschte Anzahl von Arbeitsflächen sowie diverse andere Optionen ein.

Für ständig benötigte Fenster besteht die Möglichkeit, diese so zu kennzeichnen, dass sie nicht auf einer, sondern auf allen Arbeitsflächen sichtbar sind. Dazu öffnen Sie mit der Maus oder mit Alt+ das Fenstermenü und aktivieren die Option Auf Arbeitsfläche • Alle Arbeitsflächen.

Aktivitäten

»Aktivitäten« verfolgen eine ähnliche Idee wie Arbeitsflächen. Über den durch drei farbige Punkte gekennzeichneten Aktivitäten-Button können Sie zwischen verschiedenen Desktops wechseln. Dabei startet der Pfeil-Button die Aktivität, der quadratische schwarze Button stoppt sie wieder.

Aktivitäten sind aber mehr als nur eine Neuimplementierung von Arbeitsflächen: Jede Aktivität kann einen eigenen Bildschirmhintergrund haben, eigene Programme und Plasmoids ausführen und eigene Energiespareinstellungen aufweisen (z. B. zur Deaktivierung des Bildschirmschoners und der Bildschirmsperre für die Aktivität *Vortrag*). Bei der erstmaligen Verwendung einer Aktivität können automatisch Programme gestartet werden, wenngleich ich hierfür keine Konfigurationsmöglichkeit gefunden habe.

Obwohl das Aktivitäten-Konzept interessant ist, erschweren die fehlende Dokumentation und die unübersichtliche Konfiguration eine effiziente Nutzung. Insofern verwundert das Ergebnis einer Umfrage auf der Website *http://pro-linux.de* nicht: Weniger als 10 Prozent der KDE-Nutzer gaben an, Aktivitäten regelmäßig zu nutzen.

Systemabschnitt

Wenn das Panel den sogenannten Systemabschnitt enthält, können Hintergrundprogramme im Panel dort auf sich aufmerksam machen – z. B. wenn neue Updates verfügbar sind oder eine neue E-Mail eingetroffen ist. Der Systemabschnitt befindet sich normalerweise am rechten oder unteren Ende des Panels. Er erfüllt für sich keine Funktion, sondern ist lediglich ein Platzhalter, in dem andere Programme Icons darstellen können. Diese Funktion scheint selbstverständlich zu sein, und tatsächlich werden Sie auf den Systemabschnitt wohl nur aufmerksam, wenn er aus irgendeinem Grund im Panel fehlt und Benachrichtigungen über E-Mails, Updates etc. ausbleiben.

Geräteüberwachung

Das Plasmoid Geräteüberwachung informiert über neu angeschlossene externe Datenträger und hilft dabei, deren Dateisystem zu öffnen bzw. wieder sicher aus dem Verzeichnisbaum zu lösen (`umount`).

Schnellzugriff

Das Miniprogramm SCHNELLZUGRIFF ermöglicht einen raschen Zugriff auf den Inhalt des Heimatverzeichnisses und aller darin befindlichen Unterverzeichnisse und Dateien. Durch das Anklicken einer Datei starten Sie das zugrunde liegende Programm. Um einzelne Verzeichnisse mit Dolphin anzusehen, wählen Sie mit der rechten Maustaste das Kontextmenükommando ÖFFNEN aus.

Fensterverwaltung

Die meisten Funktionen zur KDE-Fensterverwaltung sind Ihnen sicherlich aus anderen Betriebs- bzw. Desktop-Systemen vertraut: Sie können Fenster verschieben, maximieren, minimieren etc. KDE wartet darüber hinaus aber mit einigen Besonderheiten auf, die auf den ersten Blick nicht offensichtlich sind:

- **Fenster vertikal/horizontal maximieren:** Wenn Sie den Fenster-Button zum Maximieren des Fensters mit der mittleren bzw. rechten Maustaste anklicken, wird das Fenster nur vertikal bzw. horizontal maximiert.
- **Fenster in der linken/rechten Bildschirmhälfte platzieren:** Wenn Sie ein Fenster mit der Maus verschieben und die Maus dabei bis an den linken bzw. rechten Bildschirmrand bewegen, wird das Fenster so platziert, dass es die linke bzw. rechte Bildschirmhälfte bzw. ein Bildschirmviertel ausfüllt. Das ist vor allem bei großen Bildschirmen praktisch.
- **Fenster gruppieren:** Um mehrere inhaltlich zusammengehörende Fenster zu einer Gruppe zusammenzufassen, klicken Sie die Titelleiste des einen Fensters mit der rechten Maustaste an und führen ALS UNTERFENSTER ANHÄNGEN AN • PROGRAMMNAME aus. Damit wird das aktuelle Fenster in das Fenster des ausgewählten Programms integriert.

  Beide Fenster bzw. beide Programme sind nun als Dialogblätter in einem Fenster zusammengeführt und können gemeinsam minimiert, maximiert und verschoben werden. Durch eine Drehung des Mausrads über der Titelleiste eines geteilten Fensters wechseln Sie das gerade aktive Dialogblatt. Mit dem Kontextmenükommando AUS GRUPPE LÖSEN machen Sie aus dem Dialogblatt wieder ein eigenständiges Fenster.
- **Menü als Fensterbutton, Zentralmenü:** Im Systemeinstellungsmodul ERSCHEINUNGSBILD VON ANWENDUNGEN können Sie im Dialogblatt STIL • FEINEINSTELLUNG angeben, wo das Programmmenü angezeigt werden soll. Anstelle einer gewöhnlichen Menüleiste unterstützt KDE auch ein Zentralmenü wie bei OS X und Ubuntu sowie einen speziellen Menübutton in der Fensterleiste (siehe Abbildung 6.4). Wenn Sie ohnedies nur selten Menükommandos nutzen, spart diese Einstellung Platz.

Abbildung 6.4 Ein Terminal-Fenster mit einem Menübutton statt einer Menüleiste

6.2 Dolphin

In KDE 4 hat Dolphin das Universalprogramm Konqueror als Dateimanager abgelöst (siehe Abbildung 6.5). Dolphin hat im Vergleich zu Konqueror eine übersichtlichere Benutzeroberfläche. Konqueror-Fans können dieses Programm selbstverständlich weiterhin als Webbrowser und als Dateimanager verwenden.

Ansichten

Sie starten Dolphin im KDE-Menü mit FAVORITEN • DATEIMANAGER oder mit RECHNER • PERSÖNLICHER ORDNER. Die Grundfunktionen des Programms sind rasch erklärt: Im Zentrum des Fensters werden die Dateien angezeigt, wobei es drei Darstellungsmodi gibt: SYMBOLE, DETAILS und KOMPAKT, die Sie mit Strg+1 bis Strg+3 aktivieren.

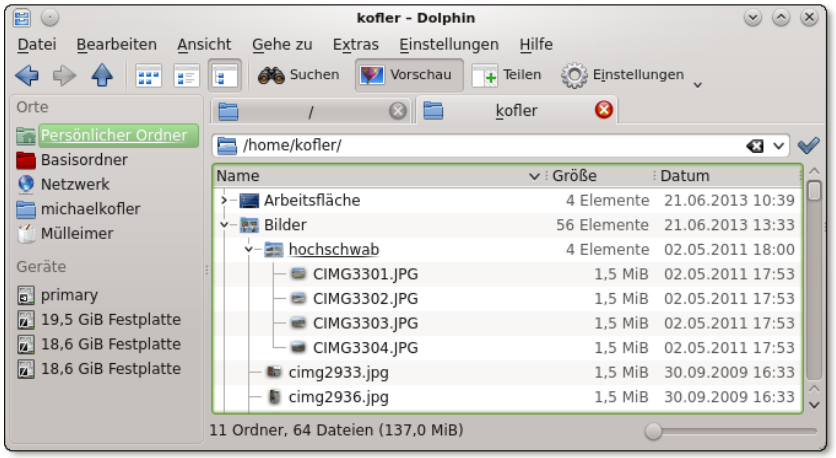


Abbildung 6.5 In der Detailansicht von Dolphin können Verzeichnisse baumartig ausgeklappt werden.

Sehr praktisch ist die Gruppierungsfunktion: ANSICHT • ELEMENTE GRUPPIEREN fasst Dateien mit demselben Typ bzw. nach Anfangsbuchstaben zu Gruppen zusammen.

Mit dem Button Vorschau aktivieren Sie unabhängig vom Darstellungsmodus bei Bildern und Dokumenten eine Vorschau. Die Größe der Vorschaubilder im Symbolmodus können Sie mit einem Schieberegler einstellen. Standardmäßig erstellt Dolphin keine Vorschau, wenn sich die Datei in einem Netzwerkverzeichnis befindet. Das Vorschauverhalten können Sie mit Einstellungen • Dolphin einrichten im Dialogblatt Allgemein • Vorschauen steuern.

Für Verschiebe- und Kopieroperationen kann der Innenbereich mit Ansicht teilen horizontal oder vertikal geteilt werden, um zwei Verzeichnisse im selben Fenster darzustellen.

Verzeichnispfad

Das aktuelle Verzeichnis wird in einer Navigationsleiste unterhalb des Menüs angezeigt. Strg+L schaltet zwischen zwei Ansichtsformen dieser Leiste um: Entweder werden die einzelnen Verzeichnisse als Buttons dargestellt, was einen raschen Verzeichniswechsel erlaubt; oder das Verzeichnis wird in Textform angezeigt, was eine schnelle Eingabe eines anderen Verzeichnisses ermöglicht. Unabhängig von der gerade aktiven Ansichtsform können Sie mit F6 ein neues Verzeichnis per Tastatur angeben.

Seitenleisten

Links, rechts und unterhalb des eigentlichen Fensterinhalts können Sie mit Ansicht Seitenleisten bzw. mit den Tasten F4, F7, F9 und F11 ein Terminal, die Verzeichnishierarchie, eine Liste häufig benötigter Orte sowie zusätzliche Informationen anzeigen. Zur Liste der Orte können Sie per Drag&Drop Lesezeichen für Verzeichnisse hinzufügen.

Menü

Je nach Konfiguration wird Dolphin ohne Menü angezeigt. Die scheinbar fehlenden Kommandos sind über den Button Einstellungen weiterhin verfügbar. Wenn Ihnen das herkömmliche Menü lieber ist, können Sie dieses mit Strg+M ein- und ausschalten.

Dateien markieren

Eine Besonderheit betrifft die Markierung von Dateien: In der KDE-Grundeinstellung ist dazu ein einfacher Mausklick nicht geeignet, weil damit die Datei angezeigt oder ausgeführt wird. Sie müssen deswegen gleichzeitig Strg (für Mehrfachmarkierungen) oder ⇧ (für Bereichsmarkierungen) drücken.

Noch eleganter ist ein weiterer Markierungsmodus: Wenn Sie den Mauszeiger eine Weile über einer Datei oder einem Verzeichnis ruhen lassen (*hover*), wird ein grünes Plus-Zeichen eingeblendet. Ein Mausklick auf dieses Symbol markiert die Datei. Bei bereits markierten Zeichen erscheint ein rotes Minus-Zeichen, mit dem Sie die Markierung wieder auflösen können.

Dateien suchen

Mit dem Button Suchen suchen Sie nach Dateien. Diese Suchfunktion ist allerdings ebenso simpel wie langsam. Wenn Sie eine effizientere Desktop-Suchfunktion benötigen, aktivieren Sie in den Systemeinstellungen im Modul Desktopsuche den

Nepomuk-Datei-Indexer. Meine persönlichen Erfahrungen mit der Desktop-Suche unter KDE waren bislang aber eher schlecht: großer Ressourcenverbrauch, mäßige Suchresultate. In den vergangenen Jahren war bei *jeder* Ankündigung einer neuen KDE-Version von Verbesserungen bei der Suchfunktion zu lesen; der endgültige Durchbruch steht weiterhin aus.

Dateien löschen

Wenn Sie Dateien und Verzeichnisse löschen, landen diese vorerst im Papierkorb. Um den Inhalt des Papierkorbs anzusehen, klicken Sie in der Seitenleiste ORTE (F9) den entsprechenden Eintrag an. Erst wenn Sie dort alle Objekte markieren und Entf drücken, werden die Dateien endgültig gelöscht. Um Dateien sofort unwiderruflich zu löschen, drücken Sie ⇧+Entf.

Mit EINSTELLUNGEN • DOLPHIN • PAPIERKORB können Sie den maximalen Speicherbedarf für den Papierkorb limitieren oder veranlassen, dass dort befindliche Dateien nach einer bestimmten Zeit endgültig gelöscht werden.

Verborgene Dateien

Unter Linux gelten alle Dateien und Verzeichnisse, deren Namen mit einem Punkt beginnen, als verborgen. Dolphin zeigt diese Dateien normalerweise nicht an, es sei denn, Sie führen im Werkzeugmenü VERSTECKTE DATEIEN ANZEIGEN aus. Noch schneller können Sie die Anzeige verborgener Dateien mit Alt+. ein- und wieder ausschalten.

Zugriffsrechte

Damit nicht jeder Benutzer alle Dateien und Verzeichnisse lesen bzw. verändern kann, speichert Linux zu jeder Datei und zu jedem Verzeichnis den Besitzer sowie Zugriffsrechte. Das zugrunde liegende Konzept wird in Kapitel 15 ausführlich beschrieben. Um den Besitzer oder die Zugriffsrechte zu ändern, klicken Sie die Datei mit der rechten Maustaste an und führen EIGENSCHAFTEN • BERECHTIGUNGEN aus.

Zugriff auf Datenträger

Die Seitenleiste ORTE (F9) enthält unter anderem eine Liste aller Festplattenpartitionen, die per Mausklick in das Dateisystem eingebunden werden können. Wenn Sie ein USB- oder Firewire-Laufwerk anschließen, erscheint im Panel ein entsprechender Hinweis. Ein Mausklick öffnet dann den Dateimanager und zeigt den Inhalt des Datenträgers an. Bevor Sie das Kabel vom Laufwerk lösen, müssen Sie entweder im KDE-Menü das Kontextmenükommando AUSWERFEN oder in Dolphin in der Seitenleiste ORTE das Kontextmenükommando EINBINDUNG LÖSEN ausführen. Nur so ist sichergestellt, dass alle noch offenen Dateien geschlossen werden und keine Dateifehler auftreten.

Audio-CDs

Sie können in Dolphin auch das Inhaltsverzeichnis von Audio-CDs betrachten. Dazu geben Sie als Adresse `audiocd:/` ein. Das Besondere an dieser Funktion besteht darin, dass alle Audio-Tracks scheinbar auch in Form von Audio-Dateien in den Formaten FLAC, MP3 (falls `lame` installiert ist) und Ogg Vorbis zugänglich sind. Wenn Sie die

Dateien nun per Drag&Drop in ein Verzeichnis kopieren, werden die Audio-Dateien eingelesen (gegrabbt) und automatisch in das entsprechende Format umgewandelt.

Im Systemeinstellungsmodul ERWEITERT • AUDIO-CDs können Sie einstellen, wie die CD ausgelesen werden soll, welche Parameter bei der Codierung der MP3- bzw. Ogg-Dateien gelten sollen etc. Wenn das Auslesen der CDs sehr lange dauert, können Sie im Dialogblatt ALLGEMEIN die Fehlerkorrektur deaktivieren. Das beschleunigt den Prozess oft um ein Vielfaches, reduziert bisweilen aber die Audio-Qualität hörbar.

Zugriff auf Netzwerkverzeichnisse

Über die Seitenleiste ORTE bzw. durch die Adressangabe `smb://` können Sie auf das lokale Netzwerk zugreifen. Um direkt auf ein bestimmtes Verzeichnis auf einem Samba- oder Windows-Server zuzugreifen, verwenden Sie die Schreibweise `smb://servername/sharename`. Diese Schreibweise ist auch dann notwendig, wenn Dolphin im Netzwerk keine Windows-Server erkennt, was je nach Firewall- und Netzwerkkonfiguration häufig vorkommt.

Hinweis

Wenn Dolphin Windows- oder Samba-Server im lokalen Netzwerk nicht findet, ist möglicherweise die Firewall Ihrer Distribution schuld. Sowohl bei Fedora als auch bei SUSE verhindern die Standardeinstellungen der Firewall die Nutzung von Windows-Netzwerkverzeichnissen. Abhilfe schafft die richtige Konfiguration der Firewall.

Passwortverwaltung

Dolphin fragt jetzt nach dem Benutzernamen und dem Passwort für den Verbindungsaufbau zum Windows-Rechner oder Samba-Server. Diese Daten werden von *KWallet* gespeichert, einem Programm zur Schlüsselverwaltung. Beim erstmaligen Start dieses Programms müssen Sie hierfür ein Zentralpasswort definieren. Das lohnt sich, weil KWallet auch Web- und Mail-Passwörter verwaltet.

FTP

Wenn die Adresse (URL) mit `ftp://` beginnt, wechselt Dolphin automatisch in den FTP-Modus. Die Oberfläche und Bedienung entsprechen dann beinahe der Verwendung des Programms als Dateimanager. Wenn Sie sich beim FTP-Server mit einem bestimmten Namen einloggen möchten (kein Anonymous-FTP), lautet die Schreibweise `ftp://name@adresse`. Sobald die Verbindung zum FTP-Server hergestellt worden ist, erscheint eine Login-Box zur Eingabe des Passworts.

SSH

Mit Dolphin können Sie auch über das sichere Protokoll SSH mit einem anderen Rechner kommunizieren und Dateien kopieren. Dazu geben Sie als Adresse `fish://username@rechnername/` ein. Nach dem Login zeigt Dolphin alle Dateien des externen Rechners an.

6.3 Konqueror und Rekonq

Das Programm Konqueror ist gleichermaßen Dateimanager für Fortgeschrittene, Webbrowser, Netzwerk-Client (FTP, SCP, Windows-Verzeichnisse etc.) und Dokument-Viewer (Bilder, Hilfedateien etc.). Die vielen Konqueror-Funktionen haben allerdings den Nachteil, dass das Menü vollkommen überladen und unübersichtlich ist. Davon einmal abgesehen, erfolgt die Bedienung von Konqueror ganz ähnlich wie bei Dolphin, weswegen ich im Folgenden nur noch auf die diversen Zusatzfunktionen eingehe. Weitere Informationen gibt die folgende Website:

http://www.konqueror.org

Verwendung als Dateimanager

Um Konqueror als Dateimanager zu verwenden, geben Sie in der Adressleiste das gewünschte Verzeichnis an. Im Menü ANSICHT können Sie nun dieselben drei Darstellungsmodi wie bei Dolphin wählen. Mit F9 können Sie einen seitlichen Navigationsbereich (Sidebar) ein- bzw. wieder ausblenden. Darin können Sie Lesezeichen, Geräte, einen Verzeichnisbaum, einen Netzwerk-Browser oder andere Navigationshilfen anzeigen.

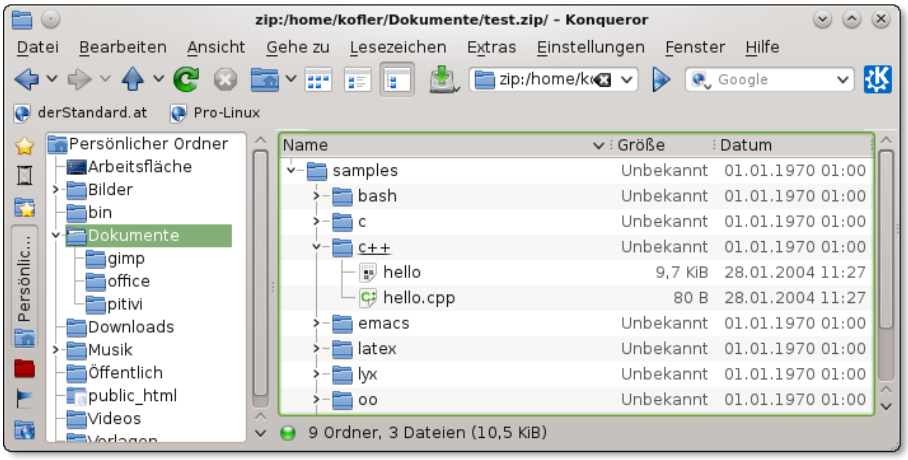


Abbildung 6.6 Konqueror als Dateimanager

Sehr elegant erfolgt der Zugriff auf Archive: Wenn Sie ein ZIP- oder TAR-Archiv anklicken (also z. B. `name.tar` oder `name.tgz` oder `name.zip`), wird der Inhalt dieses Archivs wie ein neues Verzeichnis direkt innerhalb von Konqueror angezeigt.

Festplatten-nutzung (fsview)

Wenn Sie wissen möchten, in welchen Ihrer Verzeichnisse sich die größten Datenmengen befinden, werden Sie den Konqueror-Anzeigemodus DATEIGRÖSSEN schätzen lernen. Konqueror erzeugt in diesem Modus eine Grafik aus in sich verschachtelten Rechtecken, deren Fläche die Größe von Dateien symbolisiert (siehe Abbildung 6.7). Falls dieser Modus bei Ihnen nicht zur Verfügung steht, müssen Sie eventuell das entsprechende Konqueror-Plugin-Paket installieren. Unter Ubuntu lautet der Paketname `konq-plugins`.

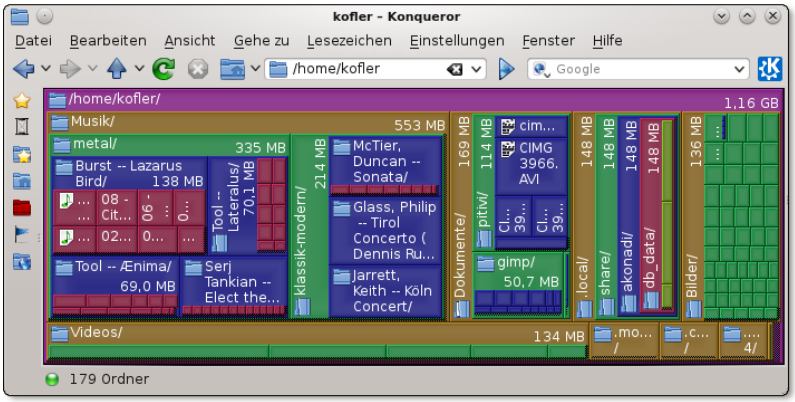


Abbildung 6.7 Festplattennutzung visualisieren

Farbgestaltung, Rekursionstiefe und andere Darstellungsdetails können Sie im ANSICHT-Menü einstellen. Per Mausklick können Sie in ein Unterverzeichnis wechseln, um so mehr Details über dessen Inhalt zu erfahren. Zur Dateigrößenansicht gelangen Sie auch, wenn Sie das Kommando `fsview` ausführen. In diesem Fall wird die Grafik ohne Konqueror-Menüs und anderes Beiwerk angezeigt.

KIO-Protokolle

In der Adressleiste von Konqueror und Dolphin können Sie Webadressen, Dateinamen etc. angeben. Konqueror zeigt grundsätzlich sämtliche Daten im Browser an, Dolphin öffnet dagegen bei einigen Protokollen ein externes Programm. Damit Konqueror und Dolphin wissen, wie sie die Adresse interpretieren sollen, muss der Adresse das Protokoll vorangestellt werden (siehe Tabelle 6.1). Beachten Sie bitte, dass manchmal gar kein, manchmal ein, manchmal aber auch zwei Schrägstriche erforderlich sind! Für die Verarbeitung dieser Protokolle sind Module zuständig, die in der KDE-Nomenklatur *KIO Slaves* heißen (KIO = KDE Input/Output).

Protokoll	Bedeutung
`file:/etc/fstab`	lokale Datei
`tar:/archivdatei`	Zugriff auf eine TAR-Datei

Tabelle 6.1 Die wichtigsten KIO-Protokolle

Protokoll	Bedeutung
audiocd:/	Zugriff auf eine Audio-CD
trash:/	gelöschte Dateien (Papierkorb)
http://www.kofler.info	Webseite
ftp://user@mars/verzeichnis	FTP-Server auf dem Rechner mars
sftp://user@mars/verzeichnis	SFTP-Server auf dem Rechner mars
fish://user@mars/verzeichnis	SSH-Zugriff auf den Rechner mars
smb://mars/myshare	Windows-Netzwerkverzeichnis
man:ls	man-Seite zum Kommando ls
info:emacs	info-Text zum Programm emacs
help:kmail	KDE-Hilfe zum Programm kmail
applications:/	Liste aller Programme
fonts:/	Liste aller Schriften
remote:/	allgemeiner Netzwerk-Browser
settings:/	Konfigurationsmodule des Kontrollzentrums

Tabelle 6.1 Die wichtigsten KIO-Protokolle (Forts.)

Verwendung als Webbrowser

KHTML versus Webkit

Die Darstellung von Webseiten in Konqueror kann je nach Konfiguration durch die KDE-eigene Rendering Engine KHTML oder durch WebKit erfolgen. Es fällt den KDE-Entwicklern zunehmend schwer, KHTML konform zu den ständig neuen HTML- und Webstandards zu halten. Um die Rendering Engine einzustellen, führen Sie in einer Konsole als gewöhnlicher Benutzer (nicht als root!) das folgende Kommando aus:

```
user$  keditfiletype text/html
```

Im Dialog Dateityp bearbeiten wechseln Sie in das Dialogblatt Einbetten, wählen das Dienstprogramm Webkit aus, schieben es in der Hierarchieliste ganz nach oben und bestätigen den Dialog mit OK. Nach einem Neustart greift Konqueror auf Webkit zurück und ist dann ACID3-konform. Unter openSUSE gilt diese Einstellung standardmäßig. Kubuntu setzt hingegen noch auf KTHML. Eine Umstellung auf Webkit gelingt nur, wenn Sie vorher das Paket kpart-webkit installieren.

Einstellungen

Es gibt wahrscheinlich keinen anderen Webbrowser mit derart vielen Konfigurationseinstellungen. Einstellungen • Konqueror einrichten führt in einen Dialog mit unzähligen Modulen, wobei manche Module wiederum aus mehreren Dialogblättern bestehen!

Neben der von anderen Webbrowsern bekannten Internetsuche können Sie die Suche auch direkt in der Adressleiste durchführen. Dazu sind spezielle Abkürzungen definiert. Wenn Sie beispielsweise als Adresse `gg:abc` eingeben, wird bei *http://www.google.com* eine Suche nach dem Begriff *abc* durchgeführt. Im Konfigurationsdialog WEBKÜRZEL können Sie die Abkürzungsliste durch eigene Kürzel ergänzen.

Plugins

Sofern das Programm `nspluginviewer` installiert ist, das sich üblicherweise im Paket `konqueror-nsplugins` befindet, kann Konqueror dieselben Plugins wie Firefox nutzen. Wenn die Plugins nicht funktionieren, werfen Sie einen Blick in den Konfigurationsdialog ERWEITERUNGEN: Dort können Sie nachsehen, welche Plugins Konqueror gefunden hat, und einstellen, welche Verzeichnisse nach Plugins durchsucht werden. Mit dem Button NACH NEUEN PLUGINS SUCHEN können Sie neu installierte Plugins in die Konqueror-Plugin-Liste aufnehmen.

Außer der Firefox-Plugin-Schnittstelle unterstützt Konqueror auch eigene, KDE-spezifische Plugins. Zu den populärsten Zusatzfunktionen zählen die Übersetzung von Webseiten, die Auto-Refresh-Funktion, um eine Website nach einer bestimmten Zeit neu zu laden, sowie der DOM-Viewer, um die HTML-Struktur einer Seite zu visualisieren. Diese Plugins müssen oft extra installiert werden. Bei den meisten Distributionen sind die Plugins im Paket `konq-plugins` gebündelt.

Java

Der Konqueror verwendet nicht direkt ein Java-Plugin, sondern den KJAS (KDE Java Applet Server, Datei `kjavaappletviewer.so`). KJAS wiederum startet den Java-Interpreter, also das Programm `java`. Falls Konqueror Probleme hat, diese Datei zu finden, ermitteln Sie deren vollständigen Dateinamen mit `which java` und tragen ihn im Konqueror-Konfigurationsdialog JAVA UND JAVASCRIPT ein.

Rekonq

Wenn Ihnen Konqueror zu überladen erscheint, bietet sich als KDE-affiner Browser das Programm Rekonq an. Es basiert standardmäßig auf Webkit. Wenn Sie parallel auch Konqueror einsetzen, werden Sie sich darüber freuen, dass die beiden Webbrowser dasselbe System zur Lesezeichenspeicherung verwenden. In Konqueror definierte Lesezeichen sind damit in Rekonq benutzbar und umgekehrt. Neue Lesezeichen definieren Sie mit Strg+B. Anstelle der Lesezeichenleiste können Sie mit ⇧+Strg+B eine vertikale Lesezeichenleiste ein- bzw. wieder ausschalten.

Eine weitere Gemeinsamkeit mit Konqueror ist die Unterstützung von Webkürzeln. Sie können also `wp:MBR` eingeben, um in der Wikipedia nach MBR (also dem Master Boot Record) zu suchen. Rekonq verfügt über einen integrierten Filter zum Ausblenden von Werbung, den Sie mit REKONQ EINRICHTEN • WERBEFILTER konfigurieren oder bei Bedarf auch deaktivieren können.

6.4 Konfiguration

Die diversen KDE-Konfigurationsmodule sind in der Systemsteuerung zusammengefasst (Kommando `systemsettings`, siehe Abbildung 6.8). Da es nicht immer ganz einfach ist, das richtige Modul zu finden, haben die KDE-Entwickler das Programm mit einer Suchfunktion ausgestattet, in der Sie nach Schlüsselwörtern (z. B. *Fenster*) suchen können. Von einem gerade aktiven Modul gelangen Sie mit dem Button ÜBERSICHT zurück in die Modulübersicht.

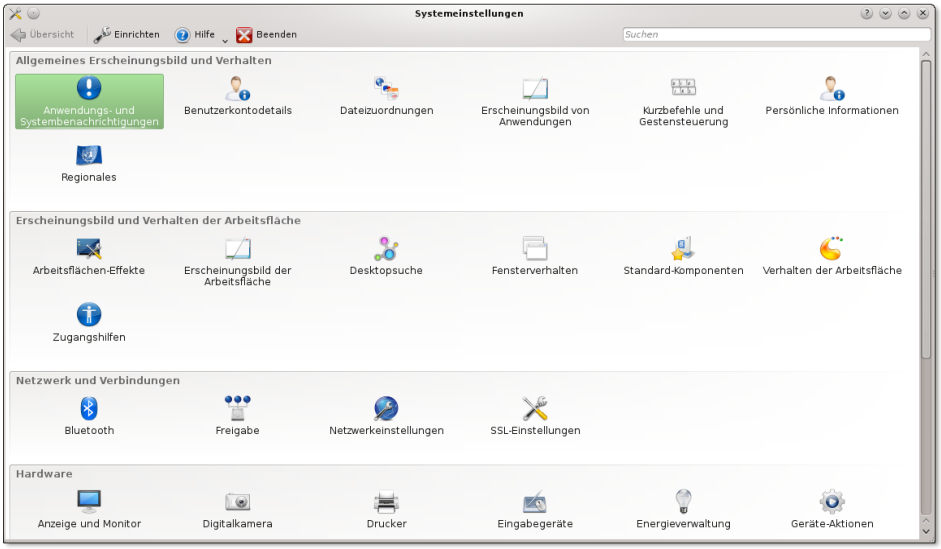


Abbildung 6.8 Das KDE-Kontrollzentrum

Einzelne Kontrollzentrumsmodule können auch in der Form `kcmshell4` *`modulname`* aufgerufen werden. Eine Liste aller zur Auswahl stehenden Module ermitteln Sie mit `kcmshell4 --list`. Beachten Sie bei der Bedienung der Module, dass geänderte Einstellungen erst wirksam werden, sobald sie durch den Button ANWENDEN bestätigt werden. In diesem Punkt unterscheidet sich KDE deutlich von Gnome, wo geänderte Einstellungen sofort aktiv sind.

KDE enthält auch Konfigurationsmodule, die nicht den Desktop betreffen, sondern Systemeinstellungen, also z. B. für die Netzwerkkonfiguration oder den Drucker. Diese Module sind bei solchen Distributionen sehr hilfreich, die keine eigenen Konfigurationswerkzeuge anbieten. Soweit verfügbar, sollten Sie aber immer distributionsspezifische Konfigurationsprogramme vorziehen. Eventuell müssen Sie bei Konfigurationsmodulen, die Systemeinstellungen betreffen, zuerst unter Angabe des `root`-Passworts in einen Administratormodus wechseln.

Konfigurationsverzeichnisse

Die meisten KDE-Programme speichern Ihre Einstellungen in Dateien des Verzeichnisses `.kde/` oder `.kde4/`. Darin existieren unter anderem die folgenden Unterverzeichnisse:

`~/.kde[4]/Autostart/`	(persönliche Autostart-Programme)
`~/.kde[4]/share/config/`	(Konfigurationseinstellungen)
`~/.kde[4]/share/apps/`	(sonstige programmspezifische Dateien)

Manche KDE-Programme sind konform zum XDG-Standard und verwenden die im vorigen Kapitel aufgelisteten XDG-Verzeichnisse:

`~/.cache/`	(Cache)
`~/.config/progname/`	(Konfigurationseinstellungen)
`~/.local/share/progname/`	(Benutzerdaten)

3D-Desktop-Effekte

Unter KDE ist der Window Manager KWin für die grafischen Effekte beim Fensterwechsel und bei anderen Operationen zuständig. Zur Konfiguration verwenden Sie das Systemeinstellungsmodul ARBEITSFLÄCHEN-EFFEKTE. In der Grundeinstellung sind nur relativ wenige Effekte aktiv, es gibt aber unzählige andere. Einige Effekte funktionieren nur, wenn ein 3D-tauglicher Grafiktreiber aktiv ist.

Auto-Login

Nach dem Start des Rechners müssen Sie sich einloggen, bevor Sie mit der Arbeit beginnen. Wenn Sie der einzige Benutzer des Rechners sind und keine Gefahr besteht, dass andere Personen Zugang zum Rechner haben, können Sie den ersten Login beim Rechnerstart automatisieren. Die Auto-Login-Funktion steuern Sie im Systemeinstellungsmodul ANMELDEBILDSCHIRM. Hinter den Kulissen ist normalerweise der KDE-Display-Manager (`kdm`) für den Login verantwortlich; Interna zu diesem Programm sind in Abschnitt 24.2 beschrieben. Davon abweichend verwendet Kubuntu den Display Manager LightDM.

Wenn auf Ihrem Rechner sowohl KDE als auch Gnome installiert ist, ist für den Login möglicherweise der Gnome-Display-Manager zuständig. Welcher Display Manager läuft, stellen Sie am einfachsten in einem Konsolenfenster mit dem folgenden Kommando fest:

```
user$  ps ax | egrep 'gdm|kdm|lightdm'
```

Bei SUSE-Distributionen erfolgt die Konfiguration der Auto-Login-Funktion desktop-unabhängig in der Datei `/etc/sysconfig/displaymanager`. Versuchen Sie nicht, den Auto-Login mit KDE- oder Gnome-Werkzeugen zu verändern: Ihre Einstellungen werden bei nächster Gelegenheit von YaST überschrieben!

Autostart

Bei jedem Logout werden alle laufenden Programme beendet. Beim nächsten Login bemüht sich KDE, die zuletzt laufenden Programme wieder zu starten, die letzte Sitzung also wiederherzustellen. Für KDE-Programme funktioniert das zumeist gut, für alle anderen Programme nur mit Einschränkungen oder gar nicht. Details zu diesem

Verhalten stellen Sie im Modul Starten und Beenden • Sitzungsverwaltung der Systemeinstellungen ein. Der zuletzt gültige Zustand der Sitzung wird in Dateien des Verzeichnisses `.kde[4]/share/config/session` gespeichert.

Unabhängig von der Sitzungsverwaltung können Sie im Verzeichnis `.kde[4]/Autostart` Programme angeben, die nach jedem Login gestartet werden sollen. KDE erwartet in diesem Verzeichnis `*.desktop`-Dateien, die das zu startende Programm beschreiben. Am einfachsten erzeugen Sie derartige Dateien, indem Sie das Verzeichnis `.kde/Autostart` mit dem Dateimanager Dolphin öffnen und das gewünschte Programm aus dem KDE-Menü per Drag&Drop dorthin kopieren. Alternativ können Sie zur Konfiguration auch das Systemsteuerungsmodul Starten und Beenden einsetzen.

Wenn Sie beide Mechanismen, also die Sitzungsverwaltung und Autostart-Verzeichnisse, parallel nutzen, kann es vorkommen, dass ein zuletzt laufendes Programm doppelt gestartet wird. Beachten Sie auch, dass KDE *mehrere* Autostart-Verzeichnisse berücksichtigt:

`~/.kde[4]/Autostart/`	(persönliche Autostart-Programme)
`/usr/share/autostart/`	(globale Autostart-Programme für KDE)
`/etc/xdg/autostart/`	(globale Autostart-Programme für Gnome und KDE)

Monitor-Konfiguration

Mit dem Modul Anzeige und Monitor stellen Sie ein, ob und wie mehrere Monitore bzw. Signalausgänge genutzt werden sollen und in welcher Auflösung Sie arbeiten möchten. Weitere Details zur Monitorkonfiguration finden Sie in Abschnitt 24.6.

Einstellungen bleibend speichern

Wenn Sie Anwenden anklicken, wird die Bildschirmauflösung zwar geändert, die neue Auflösung gilt allerdings nur bis zum nächsten Logout. Um die Einstellungen bleibend zu speichern, müssen Sie nach Abschluss der Konfiguration explizit den Button Als Standard speichern anklicken!

Desktop-Aussehen

Es gibt unzählige Möglichkeiten, auf das Aussehen (die Optik) des Desktops Einfluss zu nehmen. Wenn Sie Zeit und Lust haben, können Sie Stunden damit verbringen, den Desktop nach Ihren eigenen Vorstellungen zu gestalten.

- **Desktop-Hintergrund:** Zur Einstellung des Hintergrunds klicken Sie mit der rechten Maustaste auf den Desktop und führen Einstellungen für Desktop aus. Anschließend können Sie ein Hintergrundbild oder eine -farbe einstellen.
- **Desktop-Design:** Im Modul Erscheinungsbild der Arbeitsfläche können Sie im Dialogblatt Arbeitsflächendesign • Design das Thema für die Arbeitsfläche einstellen. Es bestimmt die Grundeinstellungen für das Aussehen des Panels, des KDE-Menüs, der Fensterdekoration etc. sowie der hierfür eingesetzten Farben.

Mit Neues Design herunterladen können Sie weitere Designs von der Website *http://kde-look.org* herunterladen; vergessen Sie nicht, das neue Design durch Anwenden auch zu aktivieren! Ansprechend ist meiner Ansicht nach das Design Caledonia. Die meisten Bildschirmabbildungen in diesem Kapitel nutzen das Design Air.

- **Gestaltung der Steuerelemente:** Im Systemeinstellungsmodul Erscheinungsbild von Anwendungen können Sie im Dialogblatt Stil zwischen mehreren Layoutvarianten für die optische Gestaltung von Buttons, Optionsfeldern, Bildlaufleisten etc. auswählen. Die meisten zur Auswahl stehenden Varianten sind allerdings uralt und sehen auch so aus.
- **Gestaltung der Fenster:** Im Systemeinstellungsmodul Erscheinungsbild der Arbeitsfläche können Sie im Dialogblatt Fensterdekoration zwischen mehreren Fensterlayouts wählen. Damit ändern Sie die Farbe und die Gestaltung des Fensterrahmens. Die Standardlayouts sind nicht übermäßig originell, aber Sie können mühelos weitere Dekorationsvarianten herunterladen und ausprobieren.

  Mit den Buttons Fensterdekoration einrichten und Knöpfe einrichten können Sie noch einige Details der aktiven Dekorationsvariante ändern: die Umrandung und den Schatten der Fenster, die Anordnung der Fenster-Buttons etc.
- **Farben:** Die Farben für die Fensterrahmen, das Menü, das Panel etc. werden durch das Desktop-Design/Thema und die Fensterdekorationsvariante vorgegeben. Das Systemeinstellungsmodul Erscheinungsbild von Anwendungen ermöglicht im Dialogblatt Farben davon abweichend die Einstellung eigener Farbschemata. Die vorgesehenen Dialogblätter sind leider unübersichtlich, und oft können Sie nur durch Ausprobieren feststellen, wie sich spezifische Veränderungen tatsächlich auswirken. Bequemer ist es, mit Neue Farbschemata herunterladen fertige Farbeinstellungen aus dem Internet zu beziehen.

Abbildung 6.9 zeigt ein Beispiel dafür, wie stark Sie das Aussehen des KDE-Desktops mit wenigen Optionen verändern können:

- Das Panel wurde wie bei Ubuntu am linken Bildschirmrand angeordnet, und die Panel-Elemente wurden auf das Minimum reduziert.
- Die Anzahl der Fensterbuttons wurde auf drei reduziert – ein vernünftiger Kompromiss zwischen übertriebenen *sechs* Buttons in den KDE-Standardeinstellungen und *einem* spärlichen Button bei Gnome. Durch die fette Schrift ist der Fenstertitel zudem besser lesbar
- Die Schatteneffekte der Fenster wurden dezenter eingestellt.
- Der Desktop wurde von allen Plasmoids befreit.

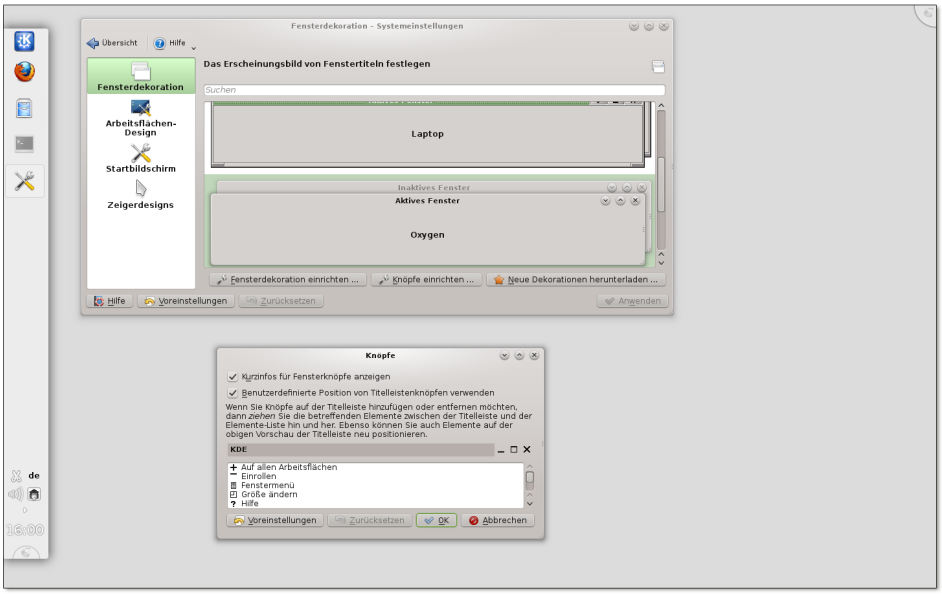


Abbildung 6.9 Reduzierte, klare KDE-Konfiguration nach dem Geschmack des Autors

Tastatur und Maus

Die Tastatureinstellungen sind im Systemeinstellungsmodul versteckt. Dort können Sie mehrere Tastaturlayouts zum raschen Wechseln einrichten, z. B., wenn Sie an mehrsprachigen Texten arbeiten. Sie können dort auch unzählige Optionen einstellen, die z. B. steuern, welche Funktionen die Tasten [⊞], [Alt] und [Strg] haben.

Auch die Optionen zur Konfiguration des Maus- bzw. Touchpad-Verhaltens finden Sie im Systemeinstellungsmodul EINGABEGERÄTE. Dort können Sie nicht nur das Doppelklickverhalten einstellen, sondern auch die Scrollrichtung angeben: normal oder umgekehrt, d. h. wie auf Smartphones bzw. unter OS X.

Drucker-konfiguration

Das KDE-Kontrollzentrum kann mit dem Modul DRUCKEINRICHTUNG auch zur Konfiguration von Druckern verwendet werden. Unter openSUSE verwenden Sie zur Druckerkonfiguration besser YaST. Das KDE-Modul zur Druckerkonfiguration erscheint aus diesem Grund nicht im Systemeinstellungsdialog, Sie können es aber mit `kcmshell printers` starten.

Den Assistenten zur Druckerkonfiguration starten Sie mit NEUER DRUCKER. Im ersten Schritt geben Sie Ihren Druckertyp (z. B. NETZWERKDRUCKER) an, im zweiten Schritt den Hersteller und das Modell. Zum Abschluss der Konfiguration müssen Sie dem Drucker einen Namen geben.

Alle Linux-Programme können nun die eingerichteten Drucker nutzen. Ist ein Drucker gerade nicht erreichbar oder stehen mehrere Druck-Jobs an, werden diese

in einer Warteschlange verwaltet. Hintergrundinformationen zum Linux-Drucksystem CUPS folgen in Kapitel 33.

Login-Icon

Je nach Konfiguration des Anmeldebildschirms wird dort zu jedem Benutzer ein kleines Bildchen angezeigt. Dieses Bild können Sie im Systemeinstellungsmodul Benutzerkontendetails einstellen bzw. ändern. In einem Konfigurationsdialog können Sie auch Ihr Passwort sowie diverse andere persönliche Einstellungen ändern. Das Login-Icon wird unter dem Namen `.face.icon` im PNG-Format gespeichert.

MIME

Wenn nach einem Doppelklick auf eine Ogg-Datei in Konqueror das Programm Amarok erscheint, dann sind hierfür die MIME-Einstellungen von KDE verantwortlich. MIME steht für Multipurpose Internet Mail Extensions und ist eine Datenbank, die eine Zuordnung zwischen Dateitypen und Programmen herstellt. Sie können die Liste der MIME-Dateitypen im Systemeinstellungsmodul Dateizuordnungen verändern. Einzelnen Dateitypen können mehrere Programme zugeordnet werden. Das in der Rangfolge am höchsten stehende Programm wird gestartet, wenn die Datei durch einen Mausklick geöffnet wird. Alle anderen Programme stehen zur Wahl, wenn Sie mit der rechten Maustaste Öffnen mit ausführen.

Schatten

Standardmäßig wird das aktive Fenster durch ein penetrantes blaues oder grünes Glühen hervorgehoben, und auch die gerade nicht aktiven Fenster haben einen sehr ausgeprägten Schatten. Natürlich ist in KDE auch die Schattengestaltung einstellbar, der entsprechende Dialog ist aber nicht ganz einfach zu finden: Im Modul Erscheinungsbild der Arbeitsfläche wählen Sie das Dialogblatt Fensterdekoration. Mit dem Button Fensterdekoration einrichten gelangen Sie in einen weiteren Dialog, dessen Dialogblatt Schatten die gesuchten Einstellungen enthält.

Standardprogramme einstellen

Standardmäßig verwendet KDE zumeist Konqueror als Webbrowser, KMail bzw. Kontact als E-Mail-Programm und `konsole` als Konsolenprogramm. Wenn Sie möchten, dass KDE beim Anklicken entsprechender Links andere Programme startet, finden Sie entsprechende Einstellmöglichkeiten im Modul Standard-Komponenten der Systemeinstellungen.

Window Manager

Für die Verwaltung der Fenster, also für das Verschieben, Vergrößern, Verkleinern etc., ist der Window Manager verantwortlich. Unter KDE kommt dafür standardmäßig das Programm KWin zum Einsatz. Unzählige Einstellungen können Sie im Modul Fensterverhalten der Systemeinstellungen ändern – etwa welche Funktionen die Maustasten in der Titelleiste des Fensters haben, nach welchen Kritierien neue Fenster platziert werden, ob und wie Fenster beim Verschieben einrasten etc.

Viele Fensteroperationen lassen sich auch mit der Tastatur erledigen. Die dafür vorgesehenen Kürzel können Sie im Systemeinstellungsmodul Kurzbefehle und Gestensteuerung (Dialogblatt Standard-Kurzbefehle) ansehen bzw. verändern.

6.5 CDs/DVDs brennen mit K3b

K3b ist das vielseitigste Brennprogramm, das momentan unter Linux verfügbar ist. Der Funktionsreichtum des Programms begeistert selbst eingefleischte Gnome-Anhänger. Ein wenig abschreckend sind nur die bisweilen unübersichtlichen Menüs und Einstellungsdialoge. Aber keine Angst! Für Standardaufgaben, also beispielsweise für das Erstellen einer Backup-CD, sind diese Optionen nicht wichtig und können getrost ignoriert werden. K3b entscheidet sich praktisch immer für vernünftige Defaulteinstellungen.

Daten-CDs und -DVDs brennen

Wenn Sie eine CD oder DVD brennen möchten, führen Sie nach dem Start DATEI • NEUES PROJEKT • NEUES DATENPROJEKT aus. Anschließend verschieben Sie die zu sichernden Verzeichnisse und Dateien aus dem Verzeichnisbaum (oben) in den CD/DVD-Bereich (unten). Der Statusbalken am unteren Fensterrand zeigt gleich an, wie viel Platz die ausgewählten Dateien beanspruchen.

Der Button BRENNEN unten im K3b-Fenster führt in einen komplexen Dialog (siehe Abbildung 6.10), in dem Sie noch diverse Einstellungen vornehmen können. Im Normalfall können Sie die Vorgaben einfach beibehalten und starten den Brennvorgang endgültig mit einem weiteren BRENNEN-Button. Während des Brennens zeigt ein Dialog den aktuellen Status an.

Abbildung 6.10 CDs/DVDs brennen mit K3b

Brennoptionen

Wenn Sie der CD bzw. DVD einen Namen geben möchten, können Sie dies im Dialogblatt DATEISYSTEM im Feld DATENTRÄGERNAME tun.

K3b speichert alle Dateien so auf der CD, dass später jeder Linux-Benutzer alle Dateien lesen kann. Wenn Sie möchten, dass die ursprünglichen Zugriffsrechte erhalten

bleiben, müssen Sie im Dialogblatt Dateisystem den Button Benutzerdefiniert und dann die Option Dateiberechtigungen erhalten anklicken.

Multi-Session-CDs/DVDs

Gewöhnliche CDs und DVDs können Sie nur einmal brennen. Zum Brennen von relativ kleinen Datenmengen gibt es das Multi-Session-Verfahren. Die Grundidee besteht darin, dass zwar keine vorhandenen Daten geändert werden können, aber im noch freien Bereich der CD/DVD neue Daten hinzugefügt werden können.

K3b unterstützt das Brennen von Multi-Session-CDs und -DVDs. Allerdings müssen Sie auf die richtige Einstellung der Optionen im Dialogblatt Einstellungen achten:

- Erste Session: Wenn Sie mit einer Multi-Session-CD/DVD beginnen, müssen Sie im Dialogblatt Verschiedenes die Einstellung Mehrfachsitzung starten auswählen.
- Weitere Sessions: Bei allen weiteren Sessions wählen Sie die Einstellung Mehrfachsitzung fortsetzen.
- Letzte Session: Um die CD bzw. DVD abzuschließen, wählen Sie die Einstellung Mehrfachsitzung abschliessen. Weitere Sessions sind nun nicht mehr möglich.

Wenn Sie die gleiche Datei in mehreren Sessions speichern, befindet sich die Datei mehrfach auf der CD bzw. DVD. Beim Lesen wird automatisch immer die neueste Version berücksichtigt, also die der letzten Session.

CDs/DVDs kopieren

Um eine CD oder DVD zu kopieren, egal, ob es sich um eine Daten- oder Audio-CD handelt, führen Sie Extras • Medium kopieren aus. Im Regelfall können Sie nun einfach auf Start klicken – K3b kümmert sich selbst um die richtigen Einstellungen. Nur in Sonderfällen sind Veränderungen an den Einstellungen notwendig. Beachten Sie, dass im temporären Verzeichnis genug Platz sein muss, um den gesamten Datenträger zwischenzuspeichern.

Bei CDs unterscheidet K3b zwischen zwei Kopiermodi: Normale Kopie und Klon-Kopie. Intern werden dabei unterschiedliche Programme eingesetzt. Im Regelfall liefert Normale Kopie gute Ergebnisse. Nur in Sonderfällen sollten Sie auf Klon-Kopie zurückgreifen.

ISO-Image brennen

Um ein ISO-Image zu brennen, führen Sie Extras • Abbild brennen aus. Im Brenndialog wählen Sie die zu brennende Datei aus, die normalerweise die Dateiendung `*.iso` hat. K3b errechnet nun automatisch eine MD5-Prüfsumme für die Datei. Die Prüfsumme wird normalerweise auch auf den Websites angegeben, die ISO-Images zum Download anbieten. Sie können damit überprüfen, ob Ihre heruntergeladene Datei wirklich exakt mit dem Original übereinstimmt.

6.6 KDE-Programme

Dieser Abschnitt stellt einige häufig eingesetzte KDE-Programme vor. Weitere KDE-Programme werden in themenspezifischen Kapiteln vorgestellt, etwa KMail und Kontact in Kapitel 8 zum Thema *Web, Mail & Co*.

Dateiarchive (Ark)

Konqueror eignet sich ausgezeichnet dazu, `*.tar.gz`-, `*.tgz`- und `*.zip`-Archive anzusehen bzw. Dateien daraus zu extrahieren. Sie können mit Konqueror aber keine neuen Archive erstellen oder vorhandene Archive verändern. Genau für diese Aufgabenstellung ist das Programm Ark gedacht, das ähnliche Funktionen bietet wie beispielsweise WinZip.

Fernwartung

Wenn Sie auf Ihrem Rechner ein Problem haben, z. B. weil ein Programm nicht richtig funktioniert, kann Ihnen ein Linux-kundiger Freund am besten via Fernwartung helfen. Dazu starten Sie eine VNC-Verbindung mit PROGRAMME • SYSTEM • ARBEITSFLÄCHE FREIGEBEN. Unter Kubuntu muss vorher das zugrunde liegende Programm `krfb` installiert werden.

Der Helfer kann einen beliebigen VNC-Client oder das KDE-Programm `krdc` einsetzen. Er sieht nun auf seinem Rechner in einem Fenster den gesamten Inhalt Ihres Bildschirms und kann per Maus und Tastatur alle Programme bedienen. Hintergründe zur Fernwartung sind in Abschnitt 24.9 beschrieben.

Konsole

Mit dem Programm *Konsole* können Sie eine oder mehrere Shells starten und in Textkonsolen darstellen. Zwischen den Shells wechseln Sie mit ⇧+← bzw. +→. Mit Strg+⇧+← bzw. +→ ändern Sie die Reihenfolge der Reiter, und mit einem Doppelklick können Sie die Reiter neu benennen. Ebenfalls sehr praktisch ist die Möglichkeit, Dateinamen von `konqueror` per Drag&Drop in das Konsolenfenster zu verschieben. Damit sparen Sie eine Menge Tipparbeit.

KRunner

Das Tastenkürzel Alt+F2 startet das winzige Programm KRunner, mit dem Sie wiederum ein anderes Programm starten können, indem Sie dessen Programmnamen eintippen. KRunner kann aber noch wesentlich mehr: Sie können damit z. B.

- einfache Berechnungen durchführen (Eingabe `= 2*3`),
- `man`-Seiten anzeigen (Eingabe `man:ls`),
- Konqueror-Webkürzel ausführen (Eingabe `gg:kde` für eine Google-Suche nach KDE),
- in eine andere Sitzung wechseln (`switch benutzername`) oder
- ein anderes Energieverwaltungsprofil aktivieren (`power profilname`).

PDF- und PostScript

Ein Klick auf `*.pdf`- oder `*.ps`-Dateien startet das Programm Okular und zeigt das Dokument an. Sie können das Dokument nun durchsuchen, einzelne Seiten ausdrucken etc.

Schlüsselverwaltung

Wenn Sie Ihre E-Mails signieren oder verschlüsseln oder andere Programme einsetzen, die PGP-Schlüssel nutzen, ist ein zentrales Werkzeug zur Schlüsselverwaltung hilfreich. In KDE übernimmt das Programm KGpg diese Aufgabe. Zur Verwaltung von S/MIME-Zertifikaten ist das Programm Kleopatra (ehemals KGpgCertmanager) vorgesehen, das bei vielen Distributionen im Paket `kdepim` enthalten ist.

Texteditoren (KEdit, KWrite, Kate)

Je nach Distribution werden zusammen mit KDE gleich drei Texteditoren installiert: KEdit, KWrite und Kate. KEdit und KWrite sind einfach zu bedienen, stellen aber nur Grundfunktionen zur Verfügung. Kate richtet sich eher an Programmierer bzw. fortgeschrittene Anwender. Sie können damit mehrere geöffnete Dateien zu einer »Sitzung« zusammenfassen, Codeteile (z. B. Funktionen oder Klassen) zusammenklappen etc.

Dateien umbenennen (KRename)

Mit dem Programm KRename können Sie Dateien effizient umbenennen, mit einer fortlaufenden Nummer ausstatten, das Datum in den Dateinamen einbauen etc. (siehe Abbildung 6.11). Zum Umbenennen sind sogar reguläre Ausdrücke erlaubt. Bevor die Dateien tatsächlich verändert werden, zeigt eine Vorschau die alten und neuen Dateinamen. KRename ist ein unentbehrliches Werkzeug, wenn Sie eine umfangreiche Sammlung von Audio- oder Bilddateien neu organisieren möchten! Bei vielen Distributionen müssen Sie das Programm vor der ersten Nutzung installieren (Paketname `krename`).

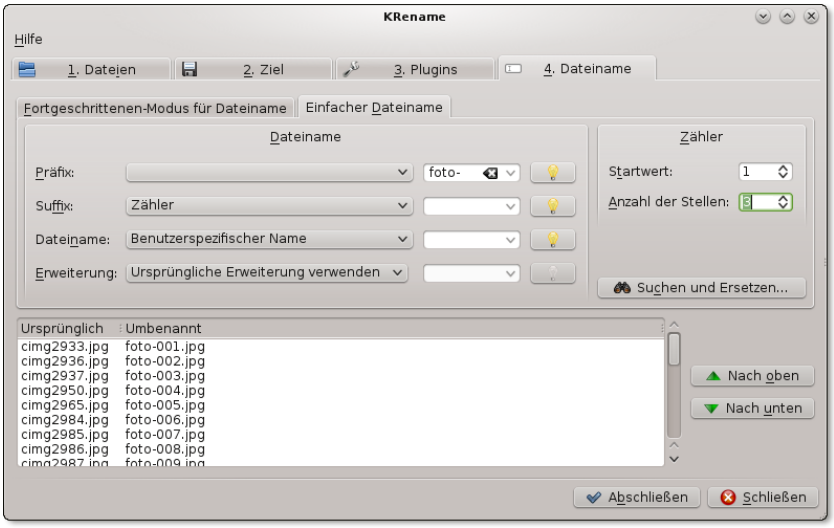


Abbildung 6.11 Dateien umbennenen mit Krename

Zwischenablage (Klipper)

Unter KDE läuft normalerweise das Programm Klipper, das sich in der Grundeinstellung die letzten sieben Einträge der Zwischenablage merkt. Per Mausklick im Systemabschnitt kann einer dieser Einträge wieder zum aktiven Inhalt der Zwischenablage gemacht werden, womit ältere Einträge auf einfache Weise nochmals genutzt werden können.

Optional können sogenannte Aktionen aktiviert werden: Dann analysiert Klipper alle neuen Einträge und führt automatisch dazu passende Operationen aus. Beispielsweise erscheint jedes Mal, wenn eine HTTP-Adresse markiert wurde, automatisch ein Konqueror-Fenster mit der entsprechenden Seite. Persönlich habe ich mit Klipper nie viel anfangen können und habe deswegen seinen automatischen Start deaktiviert (über den Menüeintrag BEENDEN).

Kapitel 7
Unity, Xfce und LXDE

Dieses Kapitel stellt die drei neben KDE und Gnome populärsten Desktop-Systeme vor:

- **Unity:** Unity ist eine von Canonical entwickelte Benutzeroberfläche, die standardmäßig in Ubuntu zum Einsatz kommt und daher eine sehr große Verbreitung hat. Genau genommen ist Unity kein komplett neuer Desktop; vielmehr basiert Unity auf Gnome. Canonical hat allerdings einige Komponenten von Gnome ausgetauscht, unter anderem die Gnome Shell und die Systemeinstellungen. Dazu gesellen sich sogenannte Indikatorprogramme und Web-Apps. Indikator-Programme sind Miniprogramme, die im Panel angezeigt werden; mit Web-Apps lassen sich Webseiten beinahe wie echte Programme ausführen.
- **Xfce:** Die Abkürzung Xfce stand ehemals für *XForms Common Environment*. Mittlerweile basiert Xfce aber nicht mehr auf der XForms-Bibliothek, sondern nutzt wie Gnome GTK-Bibliotheken. Die starken Ähnlichkeiten zu Gnome sind also kein Zufall! Die einmal eingeführte Abkürzung Xfce hat man dennoch beibehalten, auch wenn sie jetzt keine Bedeutung mehr hat.
- **LXDE:** Das Lightweight X11 Desktop Environment (LXDE) ist noch minimalistischer konzipiert als Xfce – ganz nach dem Motto: Weniger ist mehr! Davon abgesehen basiert aber auch LXDE auf den GTK-Bibliotheken. Andere Gnome-Bibliotheken kommen aber nicht zum Einsatz.

Warum Unity?

Unity ist für Canonical ein Mittel, um den eigenen Desktop optisch und funktionell von anderen Distributionen abzugrenzen. Für Canonical hat die Eigenentwicklung den Vorteil, dass man keine Rücksichten auf etablierte Meinungen und Entwicklungs-Teams nehmen muss und unkompliziert neue Wege beschreiten kann. Außerdem versucht Canonical mit Unity die Basis für eine Benutzeroberfläche zu schaffen, die nicht nur auf traditionellen Notebooks oder PCs funktioniert, sondern auch auf Smartphones, Tablets und TV-Geräten.

Auch wenn man über die Vor- und Nachteile von Unity im Vergleich zu KDE oder Gnome geteilter Meinung sein kann: Canonical ist mit Unity ein optisch sehr ansprechender und funktionell brauchbarer Desktop gelungen, den Millionen Ubuntu-

Anwender einsetzen. Auch wenn jede Neuerung anfänglich Kritik auslöste, sind die meisten Ubuntu-Anwender mit *Ihrem* Desktop durchaus zufrieden.

Warum Xfce oder LXDE?

Xfce und LXDE standen lange Zeit im Schatten von Gnome und KDE. Als Zielgruppe galten nur Nutzer von Uralt-Rechnern. Die seit einigen Jahren rapide steigende Popularität von Xfce und LXDE hat nichts damit zu tun, dass Linux-Anwender plötzlich ihre bereits ausrangierten Rechner wieder aus dem Keller holen. Andere Gründe spielen eine wichtigere Rolle:

- Xfce und LXDE können im Funktionsumfang und im Aussehen mittlerweile gut mit Gnome mithalten.
- Beide Desktop-Systeme zeichnen sich durch eine sehr einfache Bedienung aus, die – anders als Gnome 3 oder Unity – kein Umlernen verlangt.
- Weder Xfce noch LXDE setzen 3D-Grafikfunktionen voraus. Besonders praktisch ist das in Virtualisierungssystemen, wo Xfce und LXDE deutlich effizienter dargestellt werden als Gnome oder Unity.
- Auch der wesentlich geringere Ressourcenverbrauch spricht für Xfce und LXDE. Wenn Sie bei einem Server-System oder in einer virtuellen Maschine nicht ganz auf den Komfort einer grafischen Benutzeroberfläche verzichten, den Ballast von KDE oder Gnome aber vermeiden möchten, sind Xfce oder LXDE perfekte Kandidaten für das Desktop-System.

7.1 Unity

Seit Version 11.04 kümmert sich Unity unter Ubuntu um die Verwaltung der Fenster sowie um die Darstellung der Taskleiste (»Dock«) und des Startmenüs (»Dash«). Technisch gesehen ist Unity eine Erweiterung zum 3D-Window-Manager Compiz. Unity ersetzt in dieser Funktion die Gnome Shell, aber keinesfalls das gesamte Gnome-Projekt! Nahezu alle Anwendungsprogramme unter Ubuntu basieren weiterhin auf Gnome – unter anderem der Dateimanager, der Audio-Player, das Fotoverwaltungsprogrammm, das Terminal sowie unzählige Konfigurationswerkzeuge und sonstige Hilfsprogramme.

Außer Unity zeichnet sich der Ubuntu-Desktop durch weitere Ubuntu-spezifische Programme und Ergänzungen aus:

- **Web-Apps:** Web-Apps lassen einige im Webbrowser ausgeführte Seiten aussehen, als würde es sich um eigenständige Programme handeln.
- **Indikatoren:** Bei den Indikator-Programmen handelt es sich um Hintergrundprogramme, die durch ein Icon am rechten oberen Bildschirmrand dargestellt werden. Sie ersetzen Gnome-Applets bzw. KDE-Plasmoids.

- **Ubuntu One:** Ubuntu One ist ein Cloud-Dienst von Canonical. Ähnlich wie Dropbox hilft Ubuntu One bei der Speicherung von Dateien in der Cloud und bei der Synchronisierung dieser Dateien über verschiedene Geräte. Ubuntu-One-Clients existieren auch für Windows, OS X, Android und iOS.
- **Systemeinstellungen:** Um Ubuntu-spezifische Einstellungen besser in die Systemeinstellungen zu integrieren, hat Canonical die Gnome-Systemeinstellungen durch ein eigenes Programm ersetzt. Einige Einstellungsmodule wurden unverändert von Gnome übernommen, andere neu entwickelt.

Der Großteil der aufgezählten Programme bzw. Komponenten wird ebenfalls in diesem Kapitel kurz vorgestellt. Die einzige Ausnahme ist Ubuntu One, das ich zusammen mit Dropbox in Kapitel 8 (*Web, Mail & Co.*) näher beschreibe.

Startmenü (Dash)

In das Ubuntu-Startmenü, das in der englischen Dokumentation auch *Dash* genannt wird, gelangen Sie durch einen Mausklick auf das Ubuntu-Icon oder mit ⊞. Das Startmenü besteht aus mehreren Dialogblättern zur Auswahl von Programmen, Dateien und Ordnern, Musiktiteln und Videos (siehe Abbildung 7.1).

Abbildung 7.1 Programme im Ubuntu-Startmenü

Sie können im Startmenü nach Programmen oder Dateien suchen. Allerdings wird dann außer den Suchergebnissen auch Werbung angezeigt. Derart dreist hat sich bisher noch kein anderer Software-Hersteller verhalten, auch nicht die oft gescholtene Firma Microsoft. Wenn Sie nach *Terminal* suchen, schlägt das Startmenü beispielsweise den Kauf diverser Musikstücke vor, in deren Titel dieser Suchbegriff vorkommt. Abhilfe: Starten Sie im Systemmenü (rechts oben im Panel) die System-

Werbung

einstellungen. Im Modul PRIVATSPHÄRE deaktivieren Sie dann die Option AUCH ONLINE-SUCHERGEBNISSE VERARBEITEN.

Linsen (Lenses)

Die Dialogblätter im Startmenü ermöglichen gewissermaßen verschiedene Ansichten auf den Inhalt Ihres Computers und heißen deswegen »Linsen« (*Lenses*). Die Auswahl der Ansicht erfolgt wahlweise durch einen Mausklick auf die kleinen Icons am unteren Rand des Dash, mit Strg+⇆ bzw. mit den Cursortasten und ↵.

- Die Standardansicht (*home*) dient zum Start oft benötigter Programme. Hier werden die zuletzt am häufigsten eingesetzten Programme angezeigt, soweit sich diese nicht ohnehin im Dock befinden. Sobald Sie im Suchfeld einige Buchstaben eingeben, zeigt das Startmenü Programme mit den entsprechenden Anfangsbuchstaben an. Bei der Suche können Sie sowohl den Programm- bzw. Kommandonamen (z. B. `gnome-terminal`) als auch die deutsche Programmbezeichnung eingeben (z. B. *Terminal*). Zur Verfeinerung der Suchergebnisse gibt es diverse Filtermöglichkeiten.
- Die Ansicht ANWENDUNGEN hilft bei der Suche nach Programmen. Die Besonderheit dieser Ansicht besteht darin, dass in einer eigenen Gruppe noch gar nicht installierte Programme aufgelistet werden. Wenn Sie ein Icon aus dieser Gruppe auswählen, wird das Ubuntu Software-Center gestartet. Dort können Sie das gewünschte Programm dann herunterladen und installieren.
- Die Ansicht DATEIEN UND ORDNER hilft bei der gezielten Suche nach Dateien, die Sie in letzter Zeit bearbeitet haben. Durch Filter können Sie die Suche auf bestimmte Dateitypen, Dateigrößen oder Bearbeitungszeiträume eingrenzen, z. B. auf die letzten 30 Tage.
- In den Ansichten MUSIK, VIDEOS und FOTOS können Sie Ihre lokale Musik-, Video- und Fotosammlung durchsuchen. Außerdem bietet die Dash nun MP3-Dateien zum Kauf bzw. YouTube-Videos zum Ansehen an.
- In der Ansicht FREUNDE werden die neuesten Nachrichten aus Ihren sozialen Netzwerken angezeigt. Das erfordert eine entsprechende Konfiguration im Modul ONLINE-KONTEN in den Systemeinstellungen und funktioniert nur, wenn Sie nicht wie oben beschrieben die Werbung deaktiviert haben. Für die Dash gelten also auch Nachrichten aus Ihren sozialen Netzwerken als ONLINE-SUCHERGEBNISSE.

Dock (Seitenleiste, Launcher)

Die Seitenleiste am linken Bildschirmrand hat zwei Funktionen: Sie ermöglicht einerseits einen raschen Start häufig benötigter Programme und hilft andererseits beim Wechsel zwischen den laufenden Programmen. In der offiziellen englischen

Dokumentation wird die Seitenleiste *Launcher* genannt, gebräuchlicher ist aber der von Apple geprägte Begriff *Dock*.

Anfänglich enthält das Dock eine von den Ubuntu-Entwicklern vordefinierte Liste von Icons. Wenn Sie die Auswahl oder Reihenfolge der Icons verändern möchten, gehen Sie wie folgt vor:

- **Icon hinzufügen:** Um ein Icon hinzuzufügen, starten Sie zuerst das gewünschte Programm über das Startmenü. Das Icon erscheint nun im Dock, solange das Programm läuft. Damit das Icon im Dock bleibt, auch wenn das Programm nicht mehr läuft, klicken Sie es mit der rechten Maustaste an und wählen das Menükommando IM STARTER BEHALTEN aus. Es ist auch möglich, Icons aus dem Startmenü oder aus dem Dialog ANWENDUNGEN per Drag&Drop hinzuzufügen.
- **Icon entfernen:** Um ein selten benötigtes Icon zu entfernen, klicken Sie es mit der rechten Maustaste an und deaktivieren den Menüeintrag IM STARTER BEHALTEN. Eine andere Möglichkeit besteht darin, das Icon zuerst nach rechts aus dem Dock hinauszuziehen und es dann in den Mülleimer am unteren Ende des Docks zu bewegen.
- **Icon verschieben:** Um die Icon-Reihenfolge zu ändern, ziehen Sie das Icon nach rechts aus dem Dock hinaus und bewegen es dann an der gewünschten neuen Position wieder in das Dock hinein.

Bei laufenden Programmen geben weiße Dreiecke links neben dem Icon an, wie viele Fenster offen sind. (Beachten Sie aber, dass ein Programm auch laufen kann, obwohl kein Fenster offen ist – etwa beim Audio-Player. In diesem Fall ist im Dock nicht erkennbar, ob das Programm läuft oder nicht.) Das gerade aktive Programm ist im Dock durch ein weißes Dreieck rechts neben dem Icon gekennzeichnet. Wenn ein Programm Ihre Aufmerksamkeit erfordert, wird es im Dock durch einen blauen Indikator hervorgehoben.

Spezial-Icons

Das Dock enthält einige Spezial-Icons, die nicht entfernt werden können:

- **Arbeitsflächenumschalter:** Dieses Icon bewirkt, dass alle Arbeitsflächen in einem Exposé-Effekt nebeneinander angezeigt werden. In dieser Ansicht können Sie nicht nur die aktive Arbeitsfläche wechseln, sondern auch Fenster von einer Arbeitsfläche in eine andere verschieben. In aktuellen Ubuntu-Versionen wird dieses Icon standardmäßig nicht mehr angezeigt; Sie können es im Dialogblatt DARSTELLUNG • VERHALTEN in den Systemeinstellungen aktivieren.
- **Icons für externe Datenträger:** Das Dock enthält Icons für die eingelegte CD oder DVD sowie für jede aktive Partition von externen Festplatten und USB-Sticks.
- **Mülleimer:** Ein Mausklick auf dieses Icon zeigt den Inhalt des Mülleimers.

Menüleiste (Panel) mit Indikatoren

Panel

Unter Ubuntu gibt es ein Panel am oberen Bildschirmrand. Dieses Panel, das vielfach auch einfach als »Menüleiste« bezeichnet wird, enthält mehrere Elemente:

- **Programmname und Menüs:** Im linken Rand des Panels wird der Name des gerade aktiven Programms angezeigt. Diese reichlich überflüssige Information wird durch das Menü dieses Programms ersetzt, wenn Sie die Maus in das Panel bewegen oder Alt drücken. Ubuntu folgt in diesem Punkt also Apple, dessen Betriebssystem OS X ebenfalls keine Menüs in der Fensterleiste vorsieht und stattdessen das Menü des gerade aktiven Programms zentral links oben auf dem Bildschirm anzeigt.
- **Indikatoren:** Der rechte Rand des Panels ist den sogenannten Indikatoren vorbehalten. Diese Miniprogramme zeigen diverse Statusinformationen an: die Uhrzeit, die Netzwerkverbindung, die eingestellte Lautstärke etc. Alle Indikator-Anwendungen sind mit einem Menü ausgestattet, das zur Steuerung diverser Funktionen dient.

  Es ist nicht möglich, die Reihenfolge der Indikatoren zu verändern oder sie aus der Menüleiste zu entfernen. Wenn Sie einzelne Indikatoren nicht verwenden möchten, müssen Sie das betreffende Paket deinstallieren. Wenn Sie umgekehrt einen zusätzlichen Indikator wünschen, müssen Sie dessen Paket suchen, installieren und ausführen; die Auswahl ist allerdings klein. Herkömmliche Applets für das Panel, egal ob für Gnome 2 oder Gnome 3, können nicht mehr verwendet werden.

Indikatoren

Das Panel zeigt rechts unter anderem den Status der Netzwerkverbindung, die Lautstärke des Audio-Systems, den Zustand das Notebook-Akkus, den Bluetooth-Status, den Eingang neuer Nachrichten, die Uhrzeit und das Icon des Systemmenüs an (siehe Abbildung 7.2). Über die zugeordneten Menüs können Sie die Netzwerkverbindung konfigurieren, den Audio-Player steuern, Chat-, E-Mail- und Social-Messaging-Clients bedienen, Termine verwalten, Ihren Online-Status verändern, sich abmelden oder die Systemeinstellung starten.

Die für die Anzeige dieser Statusinformationen und Menüs verantwortlichen Programme heißen Indikator-Programme bzw. Indikator-Menüs. Ihre Anordnung kann nicht verändert werden. Das Panel bietet auch keine Möglichkeit, zusätzliche Indikator-Programme hinzuzufügen. Wenn Sie das möchten, müssen Sie zuerst ein entsprechendes Paket installieren und das darin enthaltene Programm dann starten. Dazu suchen Sie im Ubuntu Software-Center oder in Synaptic nach Paketen, die mit `indicator` beginnen. Technische Benutzer werden z. B. am Systemmonitor Gefallen finden (Paketname `indicator-multiload`).

Abbildung 7.2 Der Indikator-Bereich des Panels mit dem Audio-Indikator

Der einzige Weg, um nicht benötigte Indikatoren zu entfernen, ist die Deinstallation des betreffenden Pakets. Am ehesten besteht dieser Wunsch beim Messages-Menü, das den Mail- und Twitter-Status anzeigt. Das betreffende Paket heißt `indicator-messages`.

Tastatur, Maus, HUD-Menü

Tastatur

Zu den Stärken von Unity zählt die Möglichkeit, den Desktop vollständig per Tastatur zu steuern (siehe Tabelle 7.1). Das ermöglicht eine sehr effiziente Bedienung. Es ist nicht nötig, alle Tastenkürzel auswendig zu lernen! Drücken Sie einfach für zwei Sekunden ⊞, dann erscheint am Bildschirm eine Zusammenfassung der wichtigsten Kürzel. ⊞ wird dort als Super bezeichnet, das sollte Sie aber nicht weiter irritieren.

Tastenkürzel	Bedeutung
⊞	öffnet das Startmenü (Dash) zum Start von Programmen. Wenn Sie die Windows-Taste länger gedrückt halten, werden die Icons nummeriert.
⊞+1, 2 ...	aktiviert das erste, zweite ... Programm im Dock. Wenn Sie zusätzlich ⇧ drücken, wird eine neue Instanz eines bereits laufenden Programms gestartet.
⊞+A	öffnet das Dash-Fenster ANWENDUNGEN zum Start vorhandener bzw. zur Installation neuer Programme.
⊞+D	minimiert alle Fenster bzw. öffnet sie wieder.
⊞+F	öffnet das Dash-Fenster DATEIEN UND VERZEICHNISSE zur Auswahl zuletzt benutzter Dateien.
⊞+S	aktiviert den Arbeitsflächenumschalter.

Tabelle 7.1 Wichtige Unity-Tastenkürzel

Tastenkürzel	Bedeutung
⊞+T	öffnet den Papierkorb (Trash).
⊞+W	aktiviert die Exposé-Ansicht mit verkleinerten Darstellungen aller offenen Fenster.
Alt	zeigt im Panel das Menü des aktiven Programms an.
Alt+F1	bewegt den Eingabefokus in das Dock.
Alt+F2	öffnet einen Dialog zum raschen Start eines Programms, dessen Namen Sie per Tastatur eingeben.
Alt+F7	ermöglicht es, das aktuelle Fenster mit den Cursortasten nach links, rechts, oben oder unten zu verschieben.
Alt+F8	ermöglicht es, die Größe des aktuellen Fensters mit den Cursortasten zu verändern.
Alt+F9	minimiert das Fenster.
Alt+F10	maximiert das Fenster bzw. stellt seine bisherige Größe wieder her.
F10	bewegt den Eingabefokus in das Panel. Nun können Sie mit den Cursortasten durch alle Menüs sowie durch die im rechten Teil des Panels dargestellten Indikatoren blättern.
Strg+Alt+Cursortaste	wechselt in eine andere Arbeitsfläche.
⇧+Strg+Alt+Cursortaste	verschiebt das aktuelle Fenster in eine andere Arbeitsfläche.
Strg+Alt+T	öffnet ein Terminal-Fenster.

Tabelle 7.1 Wichtige Unity-Tastenkürzel (Forts.)

Maus

Innerhalb des Docks erfüllt die Maus diverse Zusatzfunktionen:

- Ein Mausklick auf ein Icon startet erwartungsgemäß das betreffende Programm.
- Ein Mausklick auf das Icon eines bereits laufenden Programms aktiviert dieses und bringt seine Fenster in den Vordergrund. Wenn das Programm bereits aktiv ist, bewirkt der Mausklick einen Exposé-Effekt, d. h., alle Fenster des Programms werden in Miniaturansicht nebeneinander dargestellt. Per Mausklick kann dann das gewünschte Fenster aktiviert werden.
- Mit der rechten Maustaste gelangen Sie in ein Kontextmenü des Icons. Darin können Sie das Programm beenden, die Verankerung im Dock einstellen und bei einigen Programmen auch diverse andere Kommandos ausführen.

- Um eine neue Instanz eines bereits laufenden Programms zu starten, also z. B. ein weiteres Webbrowser- oder Terminal-Fenster, klicken Sie das Icon mit der mittleren Maustaste an.
- Wenn der Platz im Dock nicht ausreicht, um alle Icons vollständig anzuzeigen, können Sie mit der Maus und besonders gut mit einem Mausrad durch die Icons scrollen. In solchen Fällen ist es zweckmäßig, die Icon-Größe im Modul DARSTELLUNG der Systemeinstellungen zu reduzieren.
- Bei manchen Programmen ist es möglich, Dateien aus dem Dateimanager per Drag&Drop in das jeweilige Icon zu verschieben, um diese Datei zu öffnen. Wenn Sie beispielsweise eine MP3-Datei über dem Icon des Audio-Players fallen lassen, wird die Datei abgespielt.

HUD-Menüs

Gewöhnliche Menüs werden in Ubuntu nicht in der Fensterleiste angezeigt, sondern im Panel – und auch dort nur, wenn Sie die Maus dorthin bewegen oder ca. eine Sekunde lang Alt drücken.

Daneben gibt es seit Ubuntu 12.04 die sogenannten HUD-Menüs: Wenn Sie kurz Alt drücken, erscheint an der Stelle des Startmenüs ein Eingabefeld (siehe Abbildung 7.3). Nach der Eingabe einiger Zeichen zeigt das Eingabefeld alle passenden Menükommandos an, aus denen Sie dann eines mit den Cursortasten auswählen können. Nach einer kurzen Gewöhnungszeit ist diese Art der Menübedienung äußerst effizient, zumal öfter genutzte Menükommandos in der Liste der Kommandos zuerst angezeigt werden.

Abbildung 7.3 HUD-Menüs

Die Abkürzung HUD steht für *Head-up Display* und bezieht sich auf den Umstand, dass das Menü losgelöst vom Programmfenster bedient wird. Das HUD-Menü-Konzept ist durchaus originell, kann das gewöhnliche Menü aber nicht vollständig ersetzen: Es gibt keine Möglichkeit, durch alle Menüeinträge zu navigieren und ein Menükommando zu suchen, dessen Name bzw. Position unbekannt ist.

Web-Apps

Seit Ubuntu 12.10 unterstützt Ubuntu die sogenannten Web-Apps. Damit können Sie ausgewählte Webseiten durch einen Button im Browser scheinbar zu einem eigenständigen Programm machen: Die Webseite bekommt dann ein eigenes Icon im Dock, manche Funktionen können über das HUD-Menü gesteuert werden, und einige Seiten integrieren sich sogar in das passende Audio- oder Nachrichten-Indikator-Menü im Panel.

Sobald Sie eine Website mit Web-App-Unterstützung öffnen, erscheint im Webbrowser unterhalb der Adressleiste ein kleiner Dialog, in dem Sie gefragt werden, ob Sie die zur Website passende Web-App-Erweiterung installieren möchten (siehe Abbildung 7.4). Wenn Sie das nicht wünschen, sollten Sie sich für die Option DON'T ASK AGAIN entscheiden – dann werden Sie nicht mehr mit dieser Rückfrage belästigt.

Abbildung 7.4 Twitter als Ubuntu-Web-App installieren

Die Installation erfolgt ohne visuelles Feedback. Nach rund 10 bis 15 Sekunden erscheint im Dock ein eigenes Icon der Web-App. Wenn Sie möchten, können Sie das Icon mit dem Kontextmenükommando IM STARTER BEHALTEN dort verankern – das geschieht nicht automatisch! Bei manchen Websites öffnet sich außerdem das Systemeinstellungsmodul ONLINE-KONTEN, um die Login-Daten zu erfassen und auch anderen Programmen zugänglich zu machen.

Ab dem nächsten Login, aber aus unerfindlichen Gründen nicht sofort nach der Installation, können Sie Web-Apps auch im Ubuntu-Startmenü öffnen. Der Unterschied zwischen einer »richtigen« Anwendung und einer Website verschwindet damit weitgehend.

Momentan werden ca. 30 Websites als Web-Apps unterstützt, darunter Google Mail und Google+, Yahoo Mail, Facebook, Twitter, YouTube und LinkedIn. Hinter den Kulissen ist für jede Web-App ein Paket mit dem Namen `unity-webapps-xxx` zuständig, für Twitter also beispielsweise `untiy-webapps-twitter`.

Web-Apps sind eine interessante Idee, überzeugen in der aktuellen Implementierung aber nicht restlos. Die browser-typische Darstellung der Web-Apps samt Adressleiste und dem Programmnamen »Firefox Webbrowser« im Unity-Panel lässt nie den Eindruck aufkommen, wirklich mit einem »richtigen« Programm zu arbeiten. Bei meinen Tests hat auch die Anzeige neuer Nachrichten im Nachrichten-Menü des Panels häufig versagt.

Web-Apps werden üblicherweise durch den Webbrowser Firefox ausgeführt. Wenn Sie Web-Apps in Kombination mit dem Webbrowser Chromium verwenden möchten, müssen Sie zusätzlich das Paket `unity-chromium-extension` installieren. Google Chrome wird leider nicht unterstützt.

Unity-Konfiguration

Systemeinstellungen

Ubuntu verwendet eine eigene Variante der Gnome-Systemeinstellungen (siehe Abbildung 7.5). Dort finden Sie neben einigen aus Gnome vertrauten Modulen auch einige weitere, die Ubuntu-spezifisch sind. Der schnellste Weg in die Systemeinstellungen führt über das gleichnamige Kommando im Systemmenü, das Sie durch einen Klick auf das Zahnrad-Icon ganz rechts im Panel öffnen.

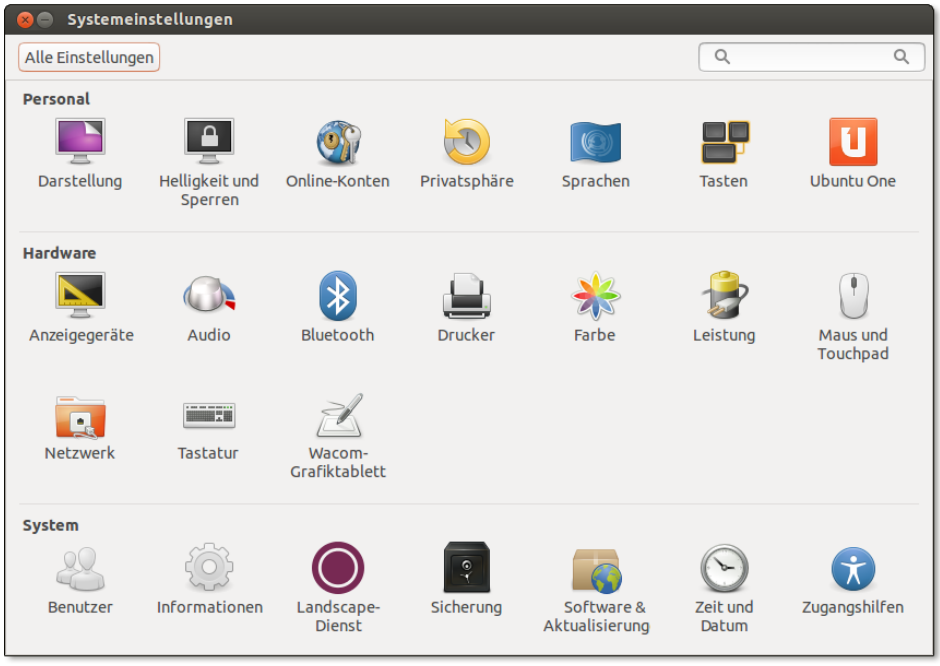


Abbildung 7.5 Ubuntu-Systemeinstellungen

Die wenigen Unity-spezifischen Einstellungen finden Sie im Modul DARSTELLUNG. Dort können Sie den Desktop-Hintergrund, die Gestaltung der Fensterrahmen (THEMA) und die Breite des Docks einstellen (GRÖSSE DER STARTERSYMBOLE). Im Dialogblatt VERHALTEN gibt es außerdem noch einige Optionen, mit denen Sie das Startmenü automatisch einblenden sowie mehrere Arbeitsflächen verwenden können.

Ubuntu Tweak

Sozusagen als Gegenmodell zu den simplen Systemeinstellungen bietet das Programm *Ubuntu Tweak* verwirrend viele Einstellmöglichkeiten und Funktionen: Sie können damit nicht nur diverse Optionen ändern, sondern auch nicht mehr benötigte Dateien und Pakete löschen, Zusatzprogramme installieren etc. (siehe Abbildung 7.6). Generell richtet sich das Programm eher an fortgeschrittene Ubuntu-Anwender.

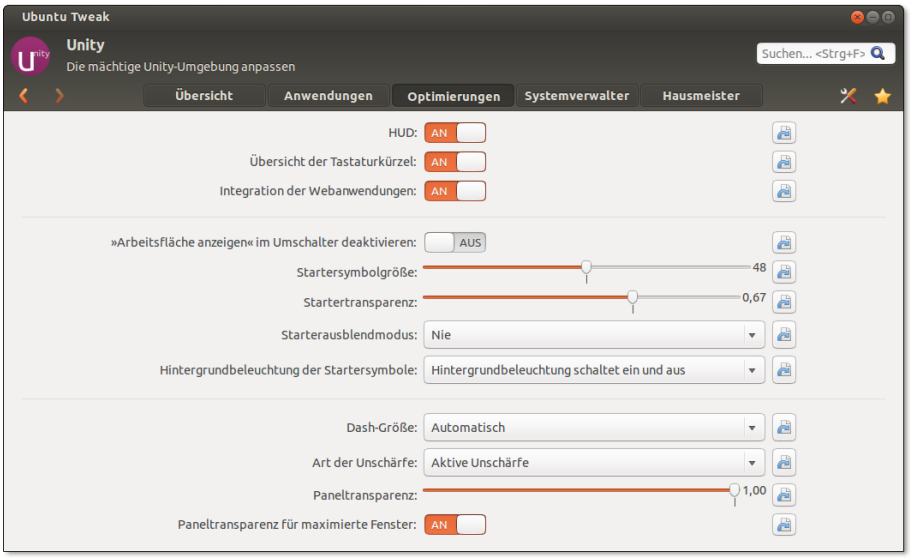


Abbildung 7.6 Unity-Einstellungen in Ubuntu Tweak

Ubuntu Tweak wird vom Ubuntu-Projekt nicht unterstützt. Um das Programm zu installieren, müssen Sie es von der Website *http://ubuntu-tweak.com* herunterladen und speichern. Zur Installation führen Sie in einem Terminal-Fenster diese Kommandos aus:

```
root#  apt-get install gdebi
root#  gdebi Downloads/ubuntu-tweaks*.deb
```

In der Testversion von Ubuntu 13.10 scheiterte die Installation an fehlenden abhängigen Paketen. Es ist aber zu hoffen, dass dieses Problem bis zur Fertigstellung von Ubuntu 13.10 gelöst wird.

Konfiguration im Textmodus

Einige oft benötigte Einstellungen lassen sich auch im Textmodus durchführen. Die folgenden Listings fassen die am häufigsten benötigten Kommandos zusammen. Ein Teil der Änderungen wird erst mit dem nächsten Login wirksam.

Unter Ubuntu sind die Fenster-Buttons wie unter OS X links in der Fensterleiste angeordnet. Wenn Sie die Fenster-Buttons lieber rechts haben, führen Sie das folgende Kommando aus:

```
user$  gconftool-2 --set /apps/metacity/general/button_layout \
         --type string ':minimize,maximize,close'              (bis Ubuntu 12.10)
user$  gsettings set org.gnome.desktop.wm.preferences \
         button-layout ':minimize,maximize,close'              (ab Ubuntu 13.04)
```

Wenn Sie sich mit dem Zentralmenü nicht anfreunden wollen, führen Sie das folgende Kommando aus:

```
user$  sudo apt-get remove indicator-appmenu
```

Gewöhnungsbedürftig sind auch die schmalen Scrollbalken. Abhilfe schafft eines der beiden folgenden Kommandos:

```
user$  sudo apt-get remove liboverlay-scrollbar*              (bis Ubuntu 12.10)
user$  sudo apt-get remove liboverlay-scrollbar*              (ab Ubuntu 13.04)
```

Autostart

In den Unity-Systemeinstellungen fehlt die Möglichkeit, Autostart-Programme einzurichten. Abhilfe: Führen Sie Alt+F2 `gnome-session-properties` aus!

7.2 Xfce

Das *XForms Common Environment* ist ein übersichtliches und schnelles Desktop-System. Es verwendet zum Teil dieselben Bibliotheken wie Gnome und hat auch optisch unverkennbare Ähnlichkeiten zu Gnome 2.

Die meisten gängigen Distributionen stellen Xfce-Pakete zur Verfügung. Bei Debian, Fedora und openSUSE besteht die Möglichkeit, Xfce bereits während der Installation als Desktop-System auszuwählen. Wenn Sie Xfce auf Ubuntu-Basis ausprobieren möchten, verwenden Sie dazu die eigene Xubuntu-Distribution. Debian hat für Version 7 sogar in Erwägung gezogen, Xfce als Default-Desktop zu verwenden; letztlich sind die Debian-Entwickler dann aber doch bei Gnome geblieben. Dafür verwendet Raspbian, die populärste Distribution für den Raspberry Pi, standardmäßig Xfce.

Aufbau des Desktops

Panels

Standardmäßig enthält der Xfce-Desktop zwei Panels. Das obere Panel ist ständig sichtbar. Auf seiner linken Seite führt ein Icon in das Anwendungs- und Einstellungsmenü. Der mittlere Bereich dient als Taskleiste zum Umschalten zwischen allen geöffneten Fenstern. Rechts geben diverse Status-Icons Informationen über den Zustand des Rechners (Uhrzeit, Netzwerkverbindung etc.). Außerdem können Sie im Arbeitsflächenumschalter zwischen mehreren virtuellen Desktops wechseln.

Das zweite Panel befindet sich am unteren Bildschirmrand und wird nur eingeblendet, wenn Sie den Mauscursor nach unten bewegen. Standardmäßig enthält dieses Panel nur ein OS X-ähnliches Dock (wenn auch ohne 3D-Effekte) zum Start häufig benötigter Programme.

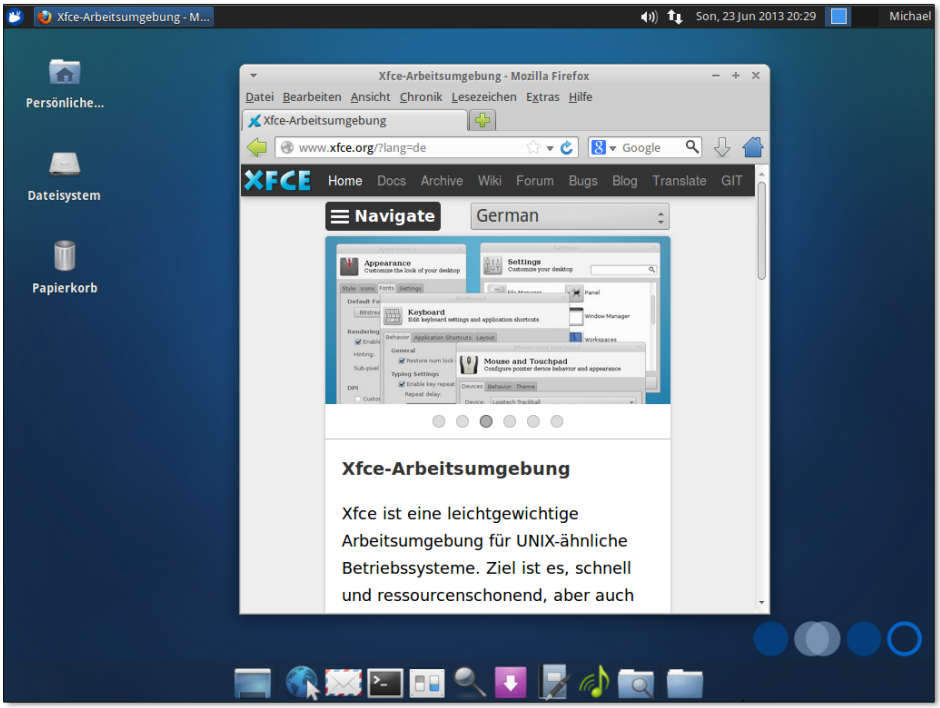


Abbildung 7.7 Der Xfce-Desktop mit den beiden Standard-Panels

Innerhalb der Panels können Sie mit der rechten Maustaste diverse Einstellungen vornehmen bzw. die darin enthaltenen Elemente verändern. Außerdem können Sie vorhandene Panels löschen und neue hinzufügen.

Mit LEISTE • LEISTENEINSTELLUNGEN gelangen Sie in einen Dialog, in dem Sie unter anderem die Ausrichtung des Panels zwischen HORIZONTAL und VERTIKAL ändern können. Eine vertikale Ausrichtung ist freilich nur bei Panels zweckmäßig, die aus-

schließlich Start-Icons enthalten! Die meisten anderen Panel-Elemente sind nur für die Darstellung in horizontalen Panels optimiert.

Tipp

Wenn Sie die Option Leiste sperren deaktivieren, werden an den Panel-Rändern angeraute Griffe eingeblendet, mit denen Sie die Panels beliebig auf dem Desktop positionieren können.

Leiste • Neue Elemente hinzufügen führt in einen Auswahldialog mit diversen Miniprogrammen, die in Panels ausgeführt werden können. Neben den bereits aktiven Panelelementen finden Sie dort z. B. Applets, mit denen Sie das aktuelle Tastaturlayout ändern, die Systemauslastung verfolgen oder den Wetterbericht für einen beliebigen Ort anzeigen können.

Wenn es Ihnen nur darum geht, ein Start-Icon für ein häufig benötigtes Programm in ein Panel einzufügen, erledigen Sie das am schnellsten per Drag&Drop aus dem Start-Menü. Achten Sie aber darauf, dass Sie das Programm nicht auf einem vorhandenen Icon fallen lassen, sondern in einem Freiraum im Panel. Sie können das Icon anschließend problemlos an die gewünschte Position verschieben.

Dateimanager

Als Dateimanager des Xfce-Desktops dient das Programm Thunar. Es weist optisch wie funktionell große Ähnlichkeiten zu seinem Gnome-Gegenstück Nautilus auf (siehe Abbildung 7.8).

Dateien umbenennen

Brillieren kann Thunar, wenn es darum geht, mehreren Dateien einen neuen Namen zu geben. Dazu markieren Sie die Dateien und drücken F2. Im Umbenennen-Dialog wählen Sie zuerst die gewünschte Verarbeitungsfunktion (z. B. Suchen und Ersetzen, Nummerieren oder Zeichen entfernen) und stellen dann die gewünschten Optionen ein. In komplizierten Fällen ist es nicht möglich, mit einem Schritt direkt zum gewünschten Ergebnis zu gelangen. Es spricht aber nichts dagegen, die Umbenennen-Funktion mehrfach auszuführen.

Dateien suchen

Thunar enthält leider keine Suchfunktionen. Um Dateien zu finden, verwenden Sie am besten das Programm Catfish, das auch auf den Index der Desktop-Suche Tracker zurückgreifen kann (`apt-get install tracker-utils`, siehe *http://wiki.ubuntuusers.de/Catfish*). Thunar lässt sich gut per Tastatur steuern. Die wichtigsten Tastenkürzel entnehmen Sie Tabelle 7.2.

Tastenkürzel	Bedeutung
Strg + 1	Icon-Ansicht
Strg + 2	Detailansicht
Strg + 3	mehrspaltige Listenansicht
Strg + B	Lesezeichen (*bookmarks*) in der Seitenleiste anzeigen
Strg + H	verborgene Dateien (*hidden files*) ein- bzw. ausblenden
Strg + L	Gehe-zu-Dialog anzeigen (*location bar*)
Strg + T	den Verzeichnisbaum (*tree*) in der Seitenleiste anzeigen
Strg + + / -	Ansicht vergrößern/verkleinern
Entf	Datei in den Papierkorb bewegen
⇧ + Entf	Datei endgültig löschen
F2	Dateien umbenennen
F9	Seitenleiste ein-/ausblenden

Tabelle 7.2 Wichtige Thunar-Tastenkürzel

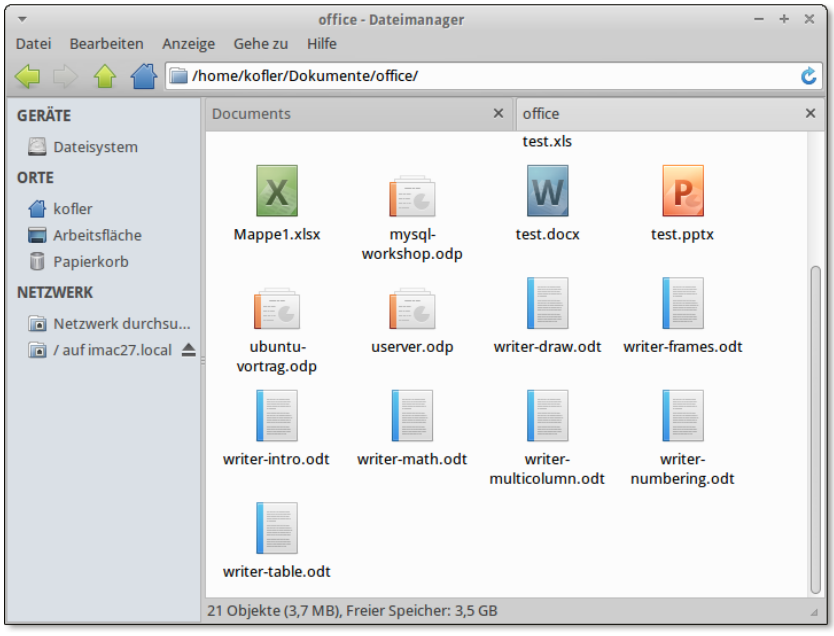


Abbildung 7.8 Der Xfce-Dateimanager Thunar

Netzwerkfunktionen

Thunar hilft nicht nur bei der Bearbeitung lokaler Dateien, sondern kann auch in diversen Protokollen (SMB, FTP, SFTP/SSH) auf Netzwerkverzeichnisse zugreifen. Die gewünschte Netzwerkadresse geben Sie am einfachsten direkt mit Strg+L an, z. B. `smb://hostname/`. Alternativ können Sie mit GEHE ZU • NETZWERK auch den Netzwerk-Browser verwenden.

Benutzerdefinierte Aktionen

Thunar kann durch selbst definierte Aktionen erweitert werden. Dazu markieren Sie eine oder mehrere Dateien und führen BEARBEITEN • BENUTZERDEFINIERTE AKTIONEN aus. Der nun erscheinende Dialog listet alle bekannten Aktionen auf und gibt Ihnen mit dem Plus-Button die Möglichkeit, eine neue Aktion zu definieren. Als »Aktion« gilt einfach ein Programm bzw. Script, an das Thunar die Dateinamen aller zuvor markierten Dateien übergibt. Eine ganze Reihe von Beispielen für eigene Aktionen gibt die folgende Webseite:

http://wiki.ubuntuusers.de/Thunar/Benutzerdefinierte_Aktionen

Terminal

Als Standardterminal unter Xfce dient das Programm `xfce4-terminal`. Es erfüllt seine Aufgaben unauffällig und problemlos. Mit BEARBEITEN • EINSTELLUNGEN können Sie das Aussehen, die Farbgestaltung und die Tastenkürzel einstellen (siehe Tabelle 7.3).

Tastenkürzel	Bedeutung
Strg+⇧+C / V	kopiert Text bzw. fügt Text ein.
Strg+⇧+T	öffnet einen neuen Tab.
Alt+1 bis Alt+9	wechselt in den Tab *n*.
Strg+Bild↑ / Bild↓	wechselt in den nächsten/vorigen Tab.

Tabelle 7.3 Wichtige Terminal-Tastenkürzel

Konfiguration

xfconf-Datenbank

Das Aussehen und die Funktion von Xfce können Sie in den Modulen der Systemeinstellungen konfigurieren (Programm `xfce4-settings-manager`, siehe Abbildung 7.9). Hinter den Kulissen werden die meisten Xfce-Einstellungen in der xfconf-Datenbank gespeichert. Dabei handelt es sich um eine Sammlung von XML-Dateien im Verzeichnis `.config/xfce4/xfconf`. In der Xfce-Nomenklatur gilt jede derartige Datei als Kanal (*channel*). Beispielsweise enthält die Datei `xfce4-panel.xml` alle Panel-Einstellungen.

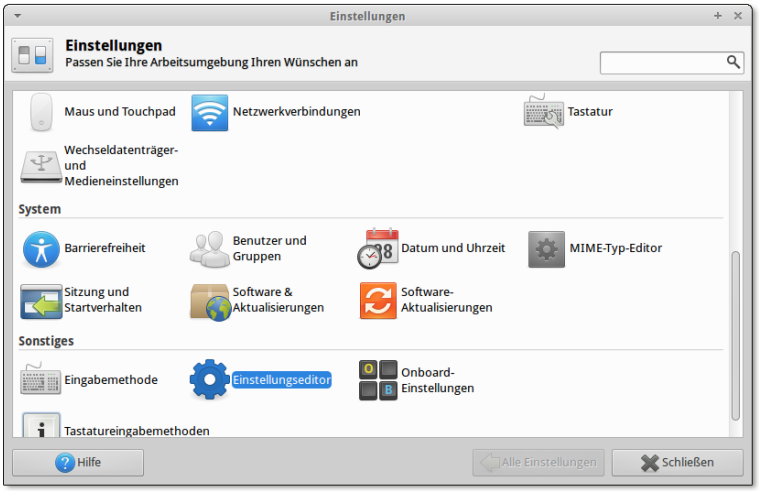


Abbildung 7.9 Xfce-Einstellungen

Am komfortabelsten stellen Sie die Xfce-Einstellungen in den dafür vorgesehenen Konfigurationsdialogen ein. Alternativ können Sie mit dem Programm `xfce4-settings-editor` durch alle Optionen blättern und Einstellungen verändern.

Das Kommando `xfconf-query` gibt Ihnen schließlich die Möglichkeit, Einstellungen in der Kommandozeile oder in einem Script auszulesen oder zu verändern. Das folgende Beispielkommando setzt die Größe für Icons auf dem Desktop mit 48 Pixel fest. Die Option `-c` wählt den richtigen Kanal aus, `-p` gibt den Namen des Parameters an und `-s` den neuen Wert:

```
user$ xfconf-query -c xfce4-desktop -p /desktop-icons/icon-size -s 48
```

7.3 LXDE

Das Lightweight X11 Desktop Environment (LXDE) ist noch minimalistischer konzipiert als Xfce – ganz nach dem Motto: Weniger ist mehr!

Panel

Standardmäßig gibt es nur ein Panel am unteren Bildschirmrand. Den Ort, das Erscheinungsbild und den Inhalt des Panels können Sie über den Kontextmenüeintrag PANEL-EINSTELLUNGEN konfigurieren. Eine vertikale Panelausrichtung ist zwar grundsätzlich möglich, aber nicht praktikabel.

Die Panelkonfiguration ist weniger intuitiv als unter Gnome oder Xfce. Insbesondere können Sie Panel-Elemente weder mit der Maus verschieben noch per Drag&Drop einfügen. Dies gilt auch für die ANWENDUNGSSTARTLEISTE, also jenes Panel-Element, das Start-Icons für häufig benötigte Programme enthält. Um die Icon-Liste zu ver-

ändern, müssen Sie per Kontextmenü dessen Konfigurationsdialog öffnen und die Liste der Programme bearbeiten.

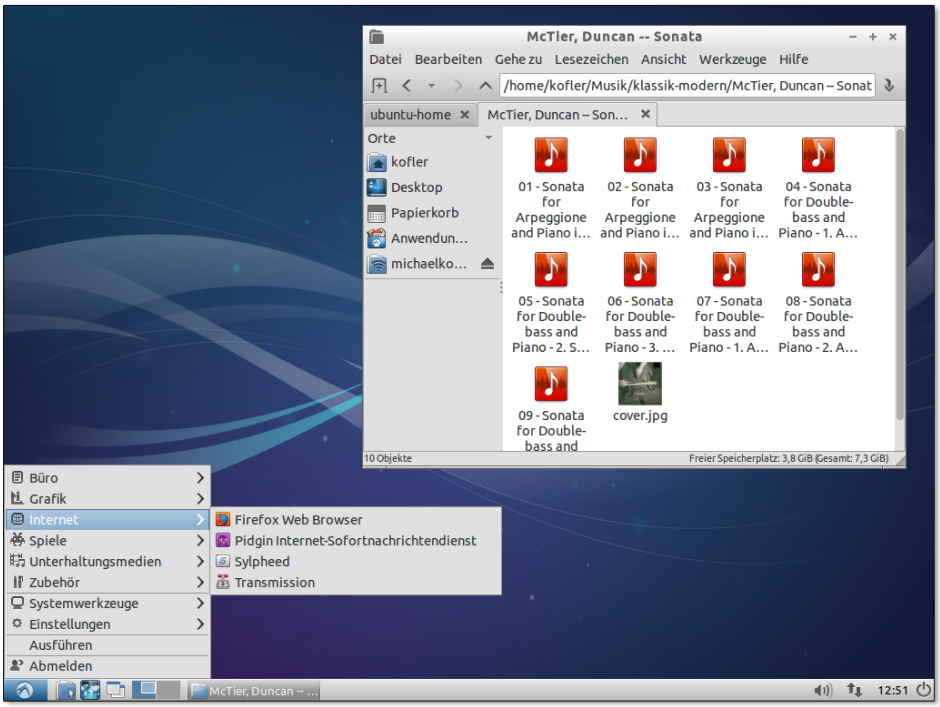


Abbildung 7.10 Der LXDE-Desktop

Dateimanager

Zum Verwalten Ihrer Dateien setzen Sie unter LXDE das Programm PCManFM ein, dessen Bedienung zum Glück weniger sperrig als sein Name ist. Das Programm kann auch als Netzwerk-Browser (für alle von gvfs unterstützten Protokolle, also SMB, FTP, SFTP etc.) sowie zum Starten von Programmen verwendet werden. Im Gegensatz zum Xfce-Dateimanager unterstützt PCManFM sogar Tabs. Einzig die Tastaturbedienung ist verbesserungsbedürfig. Der Entwickler hat sich vermutlich gedacht, wer Dateien ohne Maus verwalten will, verwendet dazu ohnedies das Terminal …

Bildvorschau

Die Vorschau von Bildern ist standardmäßig auf Dateien limitiert, die kleiner als 2 MByte sind. Fotos moderner Digitalkameras sind oft größer. Wenn Sie auch von diesen Bildern Miniaturen sehen möchten, müssen Sie den Grenzwert für die Vorschaufunktion im Dialogblatt BEARBEITEN • EINSTELLUNGEN • ANSICHT vergrößern. In diesem Dialogblatt können Sie auch die gewünschte Größe der Vorschaubilder

einstellen. Standardmäßig verwendet der Dateimanager je nach Ansicht zwischen 24×24 und 128×128 Pixel.

Terminal

Als Terminal kommt standardmäßig das Programm LXTerminal zum Einsatz. Wie die restlichen LXDE-Komponenten beschränken sich die Funktionen auf ein absolutes Minimum. Immerhin unterstützt das LXTerminal bereits Tabs, die Sie wie üblich mit Strg+⇧+T öffnen. Strg+Bild↓ bzw. Strg+Bild↑ wechseln zwischen den Tabs.

Konfiguration

Die Konfigurationswerkzeuge von LXDE sind nicht in einem Kontrollzentrum gesammelt, sondern werden über das Startmenü EINSTELLUNGEN aufgerufen. Die Einstellungen werden in einfachen Textdateien im Verzeichnis `.config/lx<name>` gestartet.

Standardschrift

Die Standardschrift für LXDE-Programme wird je nach Distribution durch eine der beiden folgenden Dateien mit dem Parameter `sGtk/FontName` eingestellt:

```
.config/lxsession/LXDE/desktop.conf
.config/lxsession/Lubuntu/desktop.conf
```

Kapitel 8
Web, Mail & Co.

Das Thema dieses Kapitels sind salopp gesagt »Internet-Programme«. Neben Webbrowsern und E-Mail-Clients behandelt dieses Kapitel auch Download-Manager, Twitter-Clients, Chat- und Telefonie-Programme sowie Cloud-Synchronisationswerkzeuge. Im Detail stelle ich Ihnen die folgenden Programme vor:

- Firefox und Google Chrome (Webbrowser)
- Thunderbird, Evolution, KMail und Mutt (Mail-Clients)
- Gwibber, Hotot (Twitter-Clients)
- Skype (Telefonie)
- Dropbox und Ubuntu One (Dateiaustausch und -synchronisation)
- Transmission und FileZilla (Download-Manager)

In das Kapitel sind zwei Grundlagenabschnitte zu den Themen »Webbrowser« und »E-Mail« eingebettet. Dort lernen Sie beispielsweise die E-Mail-Protokolle POP, IMAP und SMTP kennen, lernen etwas über Techniken zur E-Mail-Verschlüsselung und erfahren, welche Web- und Mail-Clients es abseits der in diesem Kapitel vorgestellten Programme noch gibt.

8.1 Webbrowser-Grundlagen

Im Prinzip sind alle Webbrowser gleich, möchte man meinen. Sie stellen eine Webseite dar und helfen bei der Verwaltung von Bookmarks. An der Oberfläche stimmt das, hinter den Kulissen gibt es aber erhebliche Unterschiede.

Gecko versus Webkit

Entscheidend für die Darstellung der Webseiten ist nicht die Benutzeroberfläche, die sogenannte Rendering Engine: Diese Software-Komponente (Bibliothek) ist für die Darstellung des HTML-Codes verantwortlich. Tabelle 8.1 fasst zusammen, welche Rendering Engine in welchem Browser momentan zum Einsatz kommt.

Rendering Engine	Webbrowser
Blink	Google Chrome, Chromium, Opera
Gecko	Firefox, Iceweasel
KHTML	alte Konqueror-Versionen
Trident	Internet Explorer (Microsoft)
WebKit	Arora, Epiphany, Konqueror, Midori, Rekonq, Safari (Apple) etc.

Tabelle 8.1 Rendering Engines

Interessant ist die Geschichte von WebKit: Apple hat für seinen Webbrowser Safari ursprünglich die Rendering Engine KHTML des KDE-Webbrowsers Konqueror eingesetzt. Aufgrund der umfangreichen Änderungen am Code bekam die Rendering Engine schließlich den neuen Namen WebKit und wurde dann auch von Google weiterentwickelt. Zuletzt hat WebKit zurück zu KDE gefunden und wird nun auch in Konqueror und Rekonq eingesetzt. Dafür hat sich Google von der Webkit-Entwicklung abgekoppelt und entwickelt den Code nun getrennt unter dem Namen Blink weiter.

JavaScript-Interpreter

Neben der Rendering Engine hat auch der JavaScript-Interpreter großen Einfluss darauf, wie schnell und zuverlässig der Webbrowser funktioniert, insbesondere bei modernen Web-2.0-Seiten. Je nach Webbrowser kommen abermals unterschiedliche Interpreter zum Einsatz, z. B. SpiderMonkey in Firefox, KJS in Konqueror, JavaScriptCore in vielen WebKit-Browsern, V8 in Google Chrome und Carakan in Opera.

Plugins

Plugins sind externe Erweiterungsprogramme mit Zusatzfunktionen für einen Webbrowser. Sie ermöglichen es beispielsweise, Multimedia-Inhalte abzuspielen (Adobe Flash) und PDF-Dokumente darzustellen. Zum Glück greifen die meisten gängigen Webbrowser auf das Mozilla-Plugin-System zurück. Einmal installierte Plugins sollten daher mit den meisten Linux-Webbrowsern funktionieren.

HTML5

HTML5 ist ein Standard zur Gestaltung von dynamischen Webseiten mit Multimedia-Inhalten. Flash-basierte Webseiten nehmen seit der Einführung von HTML5 langsam ab – eine aus Linux-Sicht durchaus erfreuliche Entwicklung.

HTML5 sieht unter anderem die Möglichkeit vor, Audio-Streams und Videos direkt im Webbrowser abzuspielen, also ohne zusätzliche Plugins. Das Problem dabei: Die am HTML5-Standard beteiligten Unternehmen konnten sich nicht auf einen Codec einigen.

Deswegen unterstützen verschiedene Webbrowser unterschiedliche Codecs: Der Internet Explorer und Safari setzen auf H.264. Dieser kommerzielle Codec ist für Open-Source-Software aber schlecht geeignet und kann nur über Umwege unter-

stützt werden (siehe auch Kapitel 10). Firefox und Google Chrome unterstützen deswegen die Open-Source-Codecs Ogg Theora und VP8 bzw. VP9. Ob Sie ein Video einer HTML5-Seite tatsächlich abspielen können, hängt also davon ab, welchen Codec die Website einsetzt – häufig leider H.264.

Updates

Von der Windows-Version von Firefox sind Ihnen vielleicht die automatischen Firefox-Updates bekannt. Unter Linux ist diese Art der Updates unüblich. Hier kümmert sich die zentrale Paketverwaltung um alle Updates, wobei die meisten Distributoren zwischen 2011 und 2012 dazu übergegangen sind, die Versions-Updates einfach direkt zu übernehmen. Solange es für eine Distribution Updates gibt, ist somit stets die aktuelle Version des Webbrowsers installiert.

Das war aber nicht immer so: In der Vergangenheit versuchten viele Distributionen, zwar Sicherheits-Updates einzupflegen, die Grundversion des Webbrowsers aber unverändert zu lassen. Das merken Sie vor allem bei Enterprise-Distributionen, auf denen teilweise noch uralte Browser-Versionen laufen.

Alternativen

Die meisten Distributionen verwenden Firefox oder Chromium als Default-Browser; viele Anwender installieren zudem selbst Google Chrome. Aber auch abseits des Mainstreams gibt es durchaus interessante Browser, die vor allem durch ihre perfekte Integration in das jeweilige Desktop-System brillieren. Ob das alleine als Grund für ihren Einsatz ausreicht, müssen Sie selbst entscheiden. Tabelle 8.2 zählt kurz die wichtigsten Vertreter auf.

Webbrowser	Beschreibung
Dillo	minimalistischer Browser ohne JavaScript
Konqueror	KDE-Standard-Browser
Midori	Xfce-Standard-Browser
Rekonq	schlanke Alternative zu Konqueror
Web	Gnome-Standard-Browser (ehemals Epiphany)
Lynx, ELinks, w3m	Textmodus-Browser

Tabelle 8.2 Alternative Webbrowser

Textmodus-Webbrowser

Wahrscheinlich fragen Sie sich, welchen Sinn ein Webbrowser für den Textmodus macht. Tatsächlich kommt es aber immer wieder vor, dass man in Linux in einer Textkonsole arbeitet und rasch eine Webseite besuchen oder ein HTML-Dokument lesen möchte. Dabei helfen Programme wie ELinks, Lynx oder w3m. Nebenbei können Sie mit diesen Programmen einfache HTML-Dokumente in reinen Text umwandeln. Alle drei Programme sind ähnlich zu bedienen. Zahlreiche Optionen sowie Tastenkürzel sind in den `man`-Seiten bzw. im integrierten Hilfesystem dokumentiert.

Aus Platzgründen stelle ich hier nur exemplarisch das bekannteste Programm Lynx näher vor.

Die Bedienung von Lynx ist einfach: Sie starten das Programm im Regelfall dadurch, dass Sie eine WWW-Adresse oder den Namen einer HTML-Datei als Parameter angeben. Lynx lädt das Dokument und zeigt die erste Seite an, wobei Überschriften und Links durch unterschiedliche Farben gekennzeichnet sind. Wenn Sie Lynx mit der Option `-use_mouse` starten, können Sie das Programm auch per Maus bedienen: Mit der linken Taste folgen Sie einem Link, die mittlere Taste zeigt ein Kontextmenü an, und die rechte Taste führt zur vorherigen Seite zurück.

Lynx verwendet zur Ausgabe standardmäßig den Latin-1-Zeichensatz. Damit Sonderzeichen in Unicode-Konsolen richtig dargestellt werden, geben Sie die Option `-display_charset=utf-8` an. Das folgende Kommando zeigt, wie Sie Lynx als Konverter von HTML in reinen Text einsetzen:

```
user$  lynx -dump quelle.html > ziel.txt
```

8.2 Firefox

Geschichte und Namen

Firefox ist der populärste Webbrowser für Linux. Firefox ist aus dem Netscape Navigator hervorgegangen, der ursprünglich auch einen E-Mail-Client und einen HTML-Editor enthielt. Später wurde der Code in Komponenten zerlegt – so entstanden Firefox und Thunderbird.

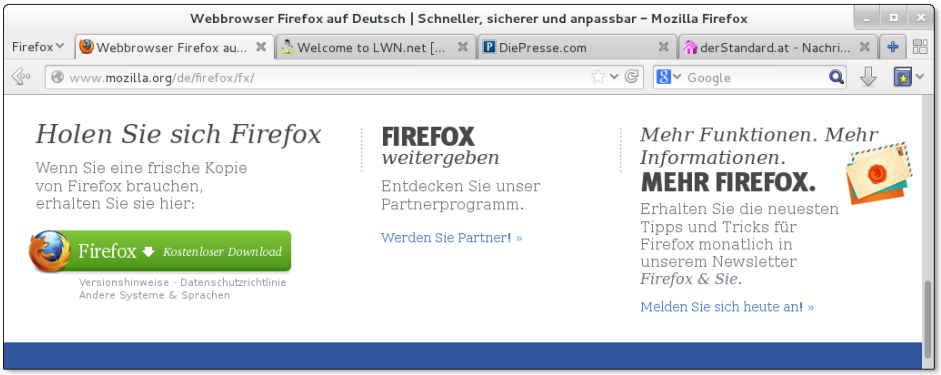


Abbildung 8.1 Der Webbrowser Firefox

Firefox und Debian

Obwohl Firefox aus Open-Source-Code besteht, darf ein Programm nur Firefox heißen, solange es ausschließlich »offiziellen« Code der Firefox-Entwickler enthält. Um unkompliziert Änderungen am Code vornehmen zu können, entschied sich Debian, den Webbrowser Firefox und den E-Mail-Client Thunderbird unter eigenen Namen

in seine Distribution zu integrieren. Aus diesem Grund heißt Firefox bei Debian »Iceweasel« und Thunderbird »Icedove«.

ESR-Versionen

Seit Mitte 2011 erscheint alle sechs Wochen eine neue Firefox-Version, die gleichermaßen Sicherheits-Updates und neue Features enthält. Ältere Firefox-Versionen werden nicht gewartet.

Neben den »gewöhnlichen« Firefox-Versionen gibt es auch spezielle ESR-Versionen (Extended Support Release) für den kommerziellen Einsatz. Der Vorteil von ESR-Versionen besteht darin, dass diese circa ein dreiviertel Jahr lang mit Sicherheits-Updates versorgt werden. Das erspart ESR-Anwendern ständig neue Firefox-Versionen. Die Firefox-ESR-Versionen kommen z. B. in Debian und in Enterprise-Distributionen wie RHEL 6 zum Einsatz.

Grundfunktionen

Tabs

Mit Strg+T sowie beim Anklicken von Links, die eine Webseite in einem neuen Fenster öffnen, erzeugt Firefox automatisch ein neues Dialogblatt (englisch *Tab*). Wer viel im Web surft, hat rasch 10, 20 Tabs offen, worunter die Übersichtlichkeit leidet. Firefox hilft mit zwei Funktionen bei der Organisation der Tabs:

- Mit dem Kontextmenü Tab anpinnen können Sie eine Seite in ein sogenanntes *App-Tab* umwandeln. App-Tabs werden vor allen anderen Tabs als Icons ohne Text angezeigt, um Platz zu sparen. App-Tabs bieten sich für Seiten an, die Sie ohnedies ständig offen haben – z. B. Facebook, Twitter, Google Mail etc.
- Der Button Tab-Gruppen ganz rechts in der Tab-Zeile verkleinert alle Tabs in Icons. Sie können die Tabs nun per Drag&Drop in Gruppen ordnen und diese Gruppen dann benennen. Per Mausklick aktivieren Sie dann den Tab, in dem Sie weiterarbeiten möchten. Die Tab-Zeile zeigt nun nur noch die Tabs der gerade aktuellen Gruppe an. Um in eine andere Gruppe zu wechseln, müssen Sie abermals den Button Tabs gruppieren anklicken. Falls der Button Tabs gruppieren fehlt, müssen Sie die Symbolleiste per Kontextmenü anpassen und den Button Tab-Gruppen hinzufügen.

Menüleiste

Wenn Sie ein platzsparendes Erscheinungsbild von Firefox wünschen, können Sie die Menüleiste mit Ansicht • Symbolleisten • Menüleiste deaktivieren. Die Menükommandos können weiter über ein kleines Dropdown-Menü links in der Tab-Leiste aufgerufen werden.

Textsuche

Mit Bearbeiten • Seite durchsuchen bzw. mit Strg+F öffnen Sie einen Suchdialog. Noch schneller gelangen Sie mit / A B C zum Text *abc*. Strg+G wiederholt diese Suche. Als Variante zu dieser Suchfunktion können Sie mit ' A B C nach Links suchen, die den Text *abc* enthalten.

Chronik (History)

Firefox merkt sich für einige Tage die Namen und Adressen aller besuchten Websites. Diese Surf-Chronik können Sie mit Strg+H (History) in der Sidebar chronologisch anzeigen und durchsuchen. Der Speicherzeitraum beträgt standardmäßig 90 Tage. Wenn Sie den Speicherzeitraum verkürzen möchten, wählen Sie im Dialogblatt Bearbeiten • Einstellungen • Datenschutz die Einstellung Firefox wird eine Chronik nach benutzerdefinierten Einstellungen anlegen. Im Dialog erscheinen nun diverse Optionen, die den Umgang mit der Seiten-Chronik, der Download-Chronik, den Formulardaten und Cookies steuern.

Privates Surfen

Normalerweise hinterlässt jeder Besuch einer Website Spuren auf Ihrem Computer: Die verwendeten Adressen erscheinen in der Chronik der besuchten Seiten, Cookies werden auf der Festplatte gespeichert, ebenso Bilder und HTML-Code im Seiten-Cache etc. Wenn Sie das nicht wollen, aktiviert Datei • Neues privates Fenster einen speziellen Modus, in dem Firefox diese Spuren beim Programmende bzw. bei der Deaktivierung des Modus löscht.

Spötter bezeichnen diese Funktion als »Porno-Modus«. Es gibt aber auch ernsthafte Anwendungen, etwa wenn Sie auf einem fremden Rechner Online-Banking durchführen oder auf andere sensitive Daten zugreifen möchten. Beachten Sie, dass Sie selbstverständlich auch im Privaten Modus Spuren im Netz hinterlassen – zwar nicht auf dem lokalen Rechner, wohl aber auf den Webservern der Seiten, die Sie besuchen, und eventuell auch auf Proxy-Servern, die sich zwischen Ihnen und dem Webserver befinden.

Downloads

Standardmäßig speichert Firefox Downloads im Verzeichnis `Downloads`. Wenn Sie den Speicherort bei jedem Download manuell angeben möchten, führen Sie Bearbeiten • Einstellungen • Allgemein aus und aktivieren die Option Jedes Mal nachfragen, wo eine Datei gespeichert werden soll.

IPv6

Sofern Ihr Computer über eine IPv6-Verbindung verfügt, können Sie mit Firefox natürlich auch auf IPv6-Webseiten zugreifen. Dabei geben Sie wie üblich den Hostnamen der Seite an, also z. B. *http://heise.de*. Nur in Ausnahmefällen bzw. bei einer Fehlkonfiguration ist es erforderlich, die IPv6-Adresse direkt anzugeben. Damit Firefox nicht mit den Doppelpunkten durcheinander kommt, geben Sie die Adresse in eckigen Klammern an. Die selten erforderliche Portnummer folgt außerhalb der eckigen Klammern. Der folgende Link führt zur Website *http://kofler.info*:

http://[2a01:4f8:161:107::3]:80

Passwörter

Wenn Sie Login-Formulare ausfüllen, z. B. um eine Webmail-Seite wie GMX zu nutzen, werden Ihre Login-Daten nach einer Rückfrage gespeichert. Das erspart bei einem neuerlichen Besuch der Website das wiederholte Ausfüllen.

Diese Bequemlichkeit hat natürlich ihren Preis: Wenn eine fremde Person Zugang zu Ihrem Rechner hat, öffnet Firefox auch den Zugang zu allen möglichen passwortgesicherten Websites. Deswegen können Sie sämtliche Passwörter selbst wiederum durch ein Master-Passwort schützen. Dieses Master-Passwort wird zur Verschlüsselung der anderen Passwörter eingesetzt. Sie müssen das Master-Passwort in Zukunft jeweils beim ersten Zugriff von Firefox auf die Passwortdatenbank angeben. Um ein Master-Passwort zu definieren, führen Sie BEARBEITEN • EINSTELLUNGEN • SICHERHEIT aus und aktivieren die Option MASTER-PASSWORT VERWENDEN.

Drucken

Vor dem Ausdruck wählen Sie mit DATEI • SEITE EINRICHTEN zwischen Hoch- und Querformat und geben die gewünschte Skalierung der Seite an (standardmäßig: Skalierung auf Seitenbreite). DATEI • DRUCKVORSCHAU liefert eine Seitenansicht des Drucks. DATEI • DRUCKEN startet den tatsächlichen Ausdruck.

Papiergröße einstellen

Bei vielen Distributionen verwendet Firefox die amerikanische Papiergröße *letter*, was in Europa je nach Drucker zu Problemen führen kann. Um die Standardgröße auf A4 umzustellen, öffnen Sie in Firefox die Seite *about:config*, suchen nach der Option `print.postscript.paper_size` und stellen diese per Doppelklick auf A4. Die neue Einstellung wird mit einem Neustart von Firefox wirksam.

Lesezeichen (Bookmarks)

Firefox zeigt Lesezeichen wahlweise an drei Orten an: im LESEZEICHEN-Menü, in einer Symbolleiste (ANSICHT • SYMBOLLEISTEN) und in der Seitenleiste, die Sie mit Strg+B (Bookmarks) ein- bzw. wieder ausschalten. Neue Lesezeichen speichern Sie wahlweise mit Strg+D oder indem Sie die aktuelle Adresse per Drag&Drop in die Symbol- oder Seitenleiste mit den Lesezeichen verschieben.

Zur Neuorganisation Ihrer Lesezeichen führen Sie LESEZEICHEN • LESEZEICHEN VERWALTEN aus. In einem eigenen Dialog können Sie nun Lesezeichen löschen, verschieben, umbenennen, sortieren, exportieren und importieren. Firefox-intern werden Lesezeichen in einer SQLite-Datenbank in der folgenden Datei gespeichert:

```
.mozilla/firefox/nnnn.default/places.sqlite
```

Firefox Sync

Um Lesezeichen zwischen mehreren Firefox-Installationen zu synchronisieren, können Sie die in Firefox integrierte Sync-Funktion nutzen. Die Konfiguration erfolgt mit BEARBEITEN • EINSTELLUNGEN • SYNC. Firefox Sync synchronisiert standardmäßig nicht nur Ihre Lesezeichen, sondern auch die Passwörter, Grundeinstellungen des Browsers, die Chronik sowie die offenen Tabs. Wenn Sie möchten, können Sie den Geltungsbereich von Firefox Sync aber einschränken.

Um die Sync-Funktion auf einem zweiten Rechner zu aktivieren, sollten Sie direkten Zugriff auf den ersten Rechner haben. Auf dem zweiten Rechner öffnen Sie das Dialogblatt SYNC im Firefox-Einstellungsdialog und führen FIREFOX-SYNC EINRICHTEN und VERBINDEN aus. Im Assistenten auf dem zweiten Rechner wird nun ein 12-stelliger Code angezeigt. Nun öffnen Sie den SYNC-Einstellungsdialog auf dem *ersten* Rechner, klicken auf den Link GERÄT VERBINDEN und geben den Code dort ein. Fertig!

Notieren Sie Ihren Synchronisationsschlüssel!

Die Sync-Funktion verwendet zur Verschlüsselung ein zufällig generiertes Passwort, das anfänglich *nur* auf dem Rechner gespeichert wird. Wenn Sie diesen Rechner verlieren und über keinen zweiten, ebenfalls synchronisierten Rechner verfügen, sind Ihre Lesezeichen und alle anderen Daten unwiederbringlich verloren! Abhilfe: Führen Sie im Dialogblatt EINSTELLUNGEN • SYNC das Menükommando BENUTZERKONTO VERWALTEN • MEIN WIEDERHERSTELLUNGSSCHLÜSSEL aus, und schreiben Sie den Schlüssel auf bzw. speichern Sie ihn an einem sicheren Ort.

Xmarks

Eine Alternative zur Firefox-Sync-Funktion ist das Add-on Xmarks. Der größte Vorteil von Xmarks besteht darin, dass das Add-on neben Firefox auch andere Webbrowser unterstützt und beispielsweise eine Synchronisation zwischen dem Internet Explorer, Safari und Firefox erlaubt. Xmarks ist allerdings weniger sicher als Firefox Sync.

Konfiguration und Interna

Menüleiste

Wenn Sie ein platzsparendes Erscheinungsbild von Firefox wünschen, können Sie die Menüleiste mit ANSICHT • SYMBOLLEISTEN • MENÜLEISTE deaktivieren. Die Menükommandos können weiter über ein kleines Dropdown-Menü links in der Tab-Leiste aufgerufen werden.

Konfigurationsdateien

Firefox erzeugt beim ersten Start das Verzeichnis `.mozilla/firefox/`*`profil`*`.default`, wobei *`profil`* eine zufällige Zeichenkette ist. In diesem Verzeichnis speichert Firefox alle Einstellungen, Bookmarks, den Cache etc.

Proxy

Falls Ihr Rechner an das Internet bzw. an das lokale Netzwerk angeschlossen ist, aber dennoch kein Webzugang möglich ist, verwendet Ihr lokales Netzwerk wahrscheinlich einen Proxy-Server. Das ist ein Rechner, der zwischen Ihrem PC und dem Internet steht. Er dient als Zwischenspeicher und beschleunigt den Zugriff auf häufig benötigte Seiten. Der Proxy kann aber auch dazu dienen, bestimmte Webseiten zu blockieren oder alle Webzugriffe zu protokollieren.

Damit Firefox den Proxy nutzt, öffnen Sie das Dialogblatt BEARBEITEN • EINSTELLUNGEN • ERWEITERT • NETZWERK • EINSTELLUNGEN und geben die erforderliche(n) Proxy-Adresse(n) an. Im Regelfall reicht es aus, die Felder für den HTTP- und FTP-Proxy auszufüllen. Die richtige Port-Nummer lautet zumeist 8080. Fragen Sie Ihren Systemadministrator, wenn Sie die Proxy-Adresse nicht kennen.

Lokaler Cache

Firefox verwaltet einen lokalen Zwischenspeicher, in dem zuletzt besuchte Webseiten, Bilder etc. gespeichert werden. Wenn dieselbe Seite später ein zweites Mal betrachtet wird und sich seither nicht geändert hat, kann sie aus dem Cache geladen werden, was natürlich schneller ist. Standardmäßig werden bis zu 50 MByte auf der Festplatte für den Cache reserviert. Mit BEARBEITEN • EINSTELLUNGEN • ERWEITERT • NETZWERK • OFFLINE-SPEICHER stellen Sie die Cache-Größe ein bzw. löschen den Cache. Im Hauptfenster führt die Adresse *about:cache* zu einer Liste aller Dateien, die momentan zwischengespeichert sind.

about:config

Die wichtigsten Konfigurationseinstellungen ändern Sie ganz komfortabel in den Dialogen von BEARBEITEN • EINSTELLUNGEN. Daneben gibt es unzählige weitere Optionen, die seltener benötigt werden. Eine alphabetische Liste dieser Optionen sowie deren aktuelle Einstellungen erhalten Sie, wenn Sie als Adresse *about:config* eingeben und dann ↵ drücken (siehe Abbildung 8.2). Im Textfeld SUCHEN können Sie die Optionsliste auf alle Einträge reduzieren, die den angegebenen Suchtext enthalten. Um eine Option zu verändern, führen Sie einen Doppelklick aus.

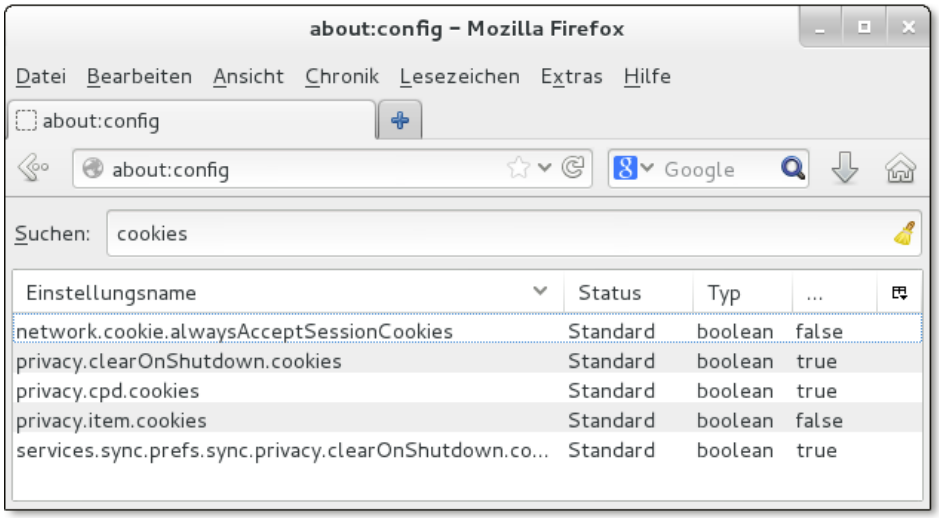


Abbildung 8.2 Firefox-Konfiguration

Textlinks bequem öffnen

Firefox enthält eine Funktion, mit der Sie in Textform angegebene Webadressen besonders schnell öffnen können. Dazu markieren Sie die Webadresse mit der Maus. Anschließend reicht ein einfacher Klick mit der mittleren Maustaste, um die in der Zwischenablage enthaltene Adresse zu öffnen. Bei einigen Distributionen, darunter Ubuntu, ist diese Funktion deaktiviert. Abhilfe: Suchen Sie auf der Seite *about:config* nach der Option `middlemouse.contentLoadURL` und stellen Sie diese auf *true*.

MIME

Die Abkürzung MIME steht für Multipurpose Internet Mail Extensions. MIME ist dafür verantwortlich, dass der Webbrowser weiß, welches Programm er starten soll, wenn Sie einen Link auf eine MP3- oder PDF-Datei anklicken. Firefox berücksichtigt die allgemeinen Linux-MIME-Einstellungen (siehe Abschnitt 15.3) sowie die MIME-Informationen aller installierten Browser-Plugins.

Den einfachsten Weg zu neuen bzw. geänderten MIME-Einstellungen bietet der ÖFFNEN-Dialog, der immer dann erscheint, wenn Firefox zwar einen MIME-Typ erkennt, aber kein Programm zuordnen kann. Sie haben nun die Möglichkeit, aus einer vorgegebenen Liste ein Programm auszuwählen oder selbst den vollständigen Dateinamen eines anderen Programms anzugeben. Unter Linux befinden sich die meisten Programme im Verzeichnis `/usr/bin`.

Einen Überblick über alle Firefox-spezifischen MIME-Einstellungen gibt BEARBEITEN • EINSTELLUNGEN • ANWENDUNGEN. Dort können Sie vorhandene Einstellungen ändern und löschen, aber leider keine neuen Einträge hinzufügen. Ihre Einstellungen speichert Firefox in der XML-Datei `.mozilla/firefox/`*`profil`*`/mimeTypes.rdf`.

Firefox-Erweiterungen (XPI-Dateien)

Der vermutlich wichtigste Faktor für den Erfolg von Firefox auch unter Windows und Mac OS X ist seine universelle Erweiterbarkeit durch XPI-Dateien. XPI steht für Cross Platform Installation. XPI-Dateien enthalten Firefox-Erweiterungen, wobei die Installationsdateien in einem Archiv samt JavaScript-Installationscode verpackt sind. Die Bandbreite der verfügbaren Erweiterungen reicht von Werbeblockern über Erweiterungen der Benutzeroberfläche, Download-Hilfen bis hin zu Werkzeugen für HTML-Entwickler (siehe auch Tabelle 8.3).

Das Dialogblatt EXTRAS • ADD-ONS • ADD-ONS SUCHEN hilft bei der Suche nach Erweiterungen. Zur Installation reicht ein einziger Mausklick auf den Link zur betreffenden XPI-Datei. Viele Erweiterungen werden allerdings erst nach einem Neustart von Firefox wirksam. EXTRAS • ADD-ONS • ERWEITERUNGEN gibt einen Überblick über installierte Extensions sowie die Möglichkeit zur Deaktivierung bzw. Deinstallation.

Erweiterung	Funktion
Adblock	blockiert die Anzeige von Werbe-Bitmaps und -Animationen.
Firebug	hilft Webentwicklern bei der Suche nach Fehlern im HTML-Code.
Flashblock	zeigt einen Button an, um Flash-Animationen zu starten.
Linkification	wandelt als Text angegebene Adressen in echte Links um.
NoScript	erlaubt JavaScript-Code nur auf vertrauenswürdigen Seiten.
Readability	hilft dabei, längere Texte komfortabler zu lesen.
ReloadEvery	lädt eine Website regelmäßig neu und verhindert so Auto-Logouts.
Screengrab	erzeugt Screenshots von mehrseitigen Webseiten.
WebDeveloper	enthält diverse Tools für Webentwickler.
WOT (Web of Trust)	warnt vor gefährlichen Seiten (ideal für Computer-Laien).
Xmarks	synchronisiert Bookmarks zwischen mehreren Browsern.

Tabelle 8.3 Populäre Firefox-Add-ons

Sicherheitsrisiko XPI

Bevor der XPI-Installationscode ausgeführt wird, warnt Firefox davor, dass XPI-Dateien auch bösartigen Code enthalten können. Nehmen Sie diese Warnung ernst. Von Firefox-Extensions können ähnliche Risiken ausgehen wie von ActiveX-Dateien für den Microsoft Internet Explorer! Installieren Sie keine Erweiterungen, von deren Notwendigkeit und Sicherheit Sie nicht überzeugt sind!

Browser-Plugins

Installation

Wenn Firefox auf eine Seite stößt, deren Inhalte ein nicht installiertes Plugin erfordern, zeigt es eine entsprechende Warnung sowie einen Installations-Button an. Allerdings funktioniert die Plugin-Installation aus Firefox heraus unter Linux häufig nicht! Zumeist ist eine manuelle Installation erforderlich, die Thema dieses Abschnitts ist.

Einen Überblick über alle momentan in Firefox verfügbaren Plugins samt der zugeordneten Dateiformate erhalten Sie, wenn Sie als Adresse `about:plugins` eingeben und ↵ drücken. Auch das Dialogblatt EXTRAS • ADD-ONS • PLUGINS liefert eine Liste aller Plugins. Dort können Sie einzelne Plugins deaktivieren.

Plugins generell deaktivieren

Firefox bietet die Möglichkeit, das Laden sämtlicher Plugins generell zu blockieren. Dazu suchen Sie auf der Seite *about:config* nach der Option `plugins.click_to_play` und aktivieren diese. Von nun an werden an der Stelle der Plugins in der Webseite nur noch Platzhalter angezeigt. Bei Bedarf können Sie das betreffende Plugin dann durch einen Mausklick aktivieren.

nspluginwrapper

Von manchen Plugins gibt es bis heute nur 32-Bit-Kompilate. Diese können nicht ohne Weiteres in einem Webbrowser ausgeführt werden, der als 64-Bit-Kompilat vorliegt. Um dieses Problem zu umgehen, wird häufig der `nsplugin-wrapper` eingesetzt. Diese Bibliothek erlaubt die Ausführung einiger 32-Bit-Plugins in 64-Bit-Linux-Distributionen. Außerdem müssen dann auch die grundlegenden 32-Bit-Bibliotheken installiert sein.

Verzeichnisse

Je nachdem, welche Distribution und Firefox-Version Sie einsetzen, werden die Plugin-Dateien an den folgenden Orten gesucht:

- im Verzeichnis `/usr/lib[64]/xulrunner/plugins`
- im Verzeichnis `/usr/lib[64]/xulrunner-addons/plugins`
- im Verzeichnis `/usr/lib[64]/mozilla/plugins`
- im Verzeichnis `/usr/lib[64]/firefox/plugins`
- im Verzeichnis `.mozilla/plugins`
- in allen Verzeichnissen, die die Umgebungsvariable `MOZ_PLUGIN_PATH` angibt

Die Vielzahl an Verzeichnissen führt dazu, dass Plugins bei vielen Rechnern nicht an einem einheitlichen Ort installiert werden, sondern quasi über die ganze Festplatte verteilt werden.

Flash-Plugin

Der Adobe Flash Player (ehemals Macromedia Flash) ermöglicht das Abspielen von Flash-Animationen im Webbrowser. Zwar verdrängt HTML5 Flash zunehmend, dennoch gibt es noch immer viele Webseiten, die Sie nur mit Flash benutzen können.

Das Adobe-Flash-Plugin ist kostenlos verfügbar. Allerdings hat Adobe entschieden, die Weitergabe des Flash-Plugins für Linux mit Version 11.2 zu beenden. Adobe verspricht zwar, diese Version noch bis 2017 mit Sicherheits-Updates zu versorgen, neuere Flash-Versionen für Linux werden aber nicht mehr frei verfügbar sein. Stattdessen haben Adobe und Google für den Webbrowser Chrome die neue Programmierschnittstelle »Pepper« entwickelt. Aktuelle Flash-Versionen nutzen diese Schnittstelle und sind direkt in Google Chrome integriert. Mit anderen Worten:

Flash-Seiten, die Flash 11.3 oder eine neuere Version voraussetzen, können unter Linux nur noch mit Google Chrome verwendet werden.

Installation von Version 11.2

Die Lizenzbedingungen von Adobe machen es den meisten Distributionen unmöglich, Pakete für Flash 11.2 selbst zur Verfügung zu stellen. Einige Distributionen liefern stattdessen Installations-Scripts aus, die sich um den Download und die Installation des Flash-Plugins kümmern:

Debian:	`flashplugin-nonfree` (`contrib`-Paketquelle)
openSUSE:	`pullin-flash-player`
Ubuntu:	`flashplugin-installer`

Wenn es für Ihre Distribution weder fertige Flash-Pakete noch ein Installations-Script gibt, müssen Sie Flash selbst installieren. Auf der folgenden Seite finden Sie das Flash-Plugin in Form von Debian- und RPM-Paketen, als YUM-Paketquelle sowie als TAR-Archiv. Falls Sie sich für die YUM-Paketquelle entscheiden, müssen Sie die eigentliche Plugin-Installation nach dem Einrichten der Paketquelle manuell starten (`yum install flash-plugin`).

http://get.adobe.com/de/flashplayer

Das TAR-Archiv enthält lediglich die Plugin-Datei `libflashplayer.so`. Diese Datei kopieren Sie in eines der vorhin angegebenen Plugin-Verzeichnisse. Anschließend starten Sie Ihren Webbrowser neu – fertig!

Flash testen

Nach einem Neustart von Firefox besuchen Sie die folgende Seite, um die Installation zu testen:

http://www.adobe.com/software/flash/about

Die Testseite zeigt animierte Werbung für diverse Adobe-Produkte an (willkommen in der Flash-Welt!) und gibt Auskunft darüber, welche Flash-Version gerade aktuell ist und welche auf Ihrem Rechner installiert ist.

FlashBlock

So toll Flash-Animationen sein können, so lästig ist ihre allgegenwärtige Präsenz für Werbezwecke. Die Firefox-Erweiterung FlashBlock schafft Abhilfe. Alle Flash-Objekte einer Seite erscheinen nun als Buttons. Die Animation beginnt erst, wenn dieser Button angeklickt wird. Anstelle von FlashBlock können Sie ab Firefox 14 auch die *about:config*-Option `click_to_play` aktivieren.

gnash, Lightspark und Shumway

Wichtige Programmkomponenten, die keiner freien Lizenz unterstehen, sind der Open-Source-Gemeinde immer ein Dorn im Auge. So verwundert es nicht, dass es auch zu Flash Open-Source-Alternativen gibt: den *GNU Flash Movie Player* (kurz `gnash`), das Lightspark-Projekt sowie das noch recht experimentelle Shumway-Projekt. Letzeres wurde in JavaScript entwickelt und kann als XPI-Erweiterung installiert werden.

Einen vollwertigen Ersatz kann leider keines der drei Projekte bieten. Sowohl bei der Kompatibilität als auch bei der Darstellungsqualität gibt es noch erhebliche Einschränkungen. Weitere Informationen finden Sie hier:

http://www.gnu.org/software/gnash
http://sourceforge.net/apps/trac/lightspark
https://github.com/mozilla/shumway

Adobe Reader

Adobe Reader ist ein Programm zur Darstellung von PDF-Seiten. Aktuelle Versionen von Firefox und Google Chrome enthalten zwar bereits einen PDF-Viewer, und auch die Programme Evince (Gnome) und Okular (KDE) können PDF-Dokumente darstellen, dennoch gibt es Argumente für den Adobe Reader:

- bessere Darstellungsqualität
- ausgereiftere Druckfunktionen
- Formularfunktionen

Gegen den Einsatz des Adobe Readers sprechen allerdings die seit Jahren andauernden Sicherheitsprobleme. Wenn Sie nur gelegentlich durch ein PDF-Dokument blättern möchten, sollten Sie bei den mit Linux bzw. Google Chrome mitgelieferten PDF-Viewern bleiben!

Der Adobe Reader ist kostenlos im Internet verfügbar, aus lizenzrechtlichen Gründen sind die meisten Distributionen aber nicht in der Lage, offizielle Adobe-Reader-Pakete in ihre Distribution zu integrieren. Aus diesem Grund müssen Sie das Programm von der Adobe-Website herunterladen und manuell installieren.

Manuelle Installation

Auf der folgenden Website finden Sie eine 32-Bit-Version des Adobe Readers als Debian- oder RPM-Paket, als TAR-Archiv (`*.tar.bz2`) oder als ausführbares Installationsprogramm (`*.bin`). Eine 64-Bit-Version existiert nicht.

http://get.adobe.com/de/reader

Die Debian- bzw. RPM-Pakete installieren Sie wie üblich mit `dpkg -i`, `rpm -i` oder `yum localinstall`. Wenn Sie bei Debian-basierten 64-Bit-Distributionen Warnungen erhalten, die besagen, dass die CPU-Architektur nicht stimmt, schafft die zusätzliche `dpkg`-Option `--force-architecture` Abhilfe.

Zur Installation des TAR-Archivs führen Sie in einer Konsole die folgenden Kommandos aus:

```
root#  tar xjf AdobeReader_ n.n.tar.bz2
root#  cd AdobeReader
root#  sh INSTALL
```

Falls Sie sich für die `.bin`-Variante entschieden haben, setzen Sie deren *Execute*-Bit und führen die Datei dann aus:

```
root#  chmod a+x AdobeReader_ n.n.bin
root#  ./AdobeReader_ n.n.bin
```

Im textbasierten Installationsprogramm bestätigen Sie durch ↵ das Installationsverzeichnis `/opt` und die automatische Installation des Mozilla-Plugins. Bei der Installation werden auch Startkommandos in die Gnome- und KDE-Menüs eingefügt.

Wenn Sie die Installation auf einem 64-Bit-Betriebssystem durchgeführt haben, brauchen Sie grundlegende 32-Bit-Bibliotheken, bevor Sie den Adobe Reader starten können. Unter Debian und Ubuntu installieren Sie dazu die Bibliothek `ia32-libs`. Bei Fedora sorgen die im RPM-Paket des Adobe Readers definierten Abhängigkeiten dafür, dass die erforderlichen Bibliotheken automatisch installiert werden.

Java-Plugin

Damit Sie Java-Applets im Webbrowser nutzen können, brauchen Sie ein Java-Plugin. Fast alle Distributionen stellen fertige Java-Plugin-Pakete auf der Basis von OpenJDK zur Verfügung, deren Installation ein Kinderspiel ist. Vom Plugin-Paket sind in der Regel eine Menge weiterer Pakete abhängig, die die eigentliche Java-Runtime enthalten.

Debian:	`icedtea-6-plugin` **oder** `icedtea-7-plugin`
Fedora, openSUSE, RHEL:	`icedtea-web`
Ubuntu:	`icedtea-plugin`

Test

Um sicherzustellen, dass alles funktioniert hat, öffnen Sie die folgende Webseite. Darin gibt ein Applet Auskunft über die installierte Java-Version.

http://www.java.com/de/download/testjava.jsp

Multimedia-Plugins

Aktuelle Versionen von Firefox und Google Chrome können von sich aus bereits Dateien bzw. Streams in mehreren Audio- und Video-Formaten abspielen. Viele Websites mit Multimedia-Angeboten setzen zudem auf Flash. Ein eigenes Multimedia-Plugin ist somit nur dann erforderlich, wenn Ihr Webbrowser die in eine Website integrierten Audio- und Video-Angebote nicht abspielen kann.

Die unter Linux verfügbaren Multimedia-Plugins basieren auf den Multimedia-Frameworks des jeweiligen Desktops bzw. auf den Video-Playern MPlayer, VLC oder Xine. Unter Ubuntu stehen momentan gleich vier Webbrowser-Plugins zur Auswahl, wobei standardmäßig das Totem-Plugin installiert ist:

`gecko-mediaplayer`	Plugin auf der Basis von MPlayer; löst `mozilla-mplayer` ab
`mozilla-plugin-vlc`	Plugin auf der Basis von VLC
`totem-mozilla`	Plugin auf der Basis von Totem (Gnome)
`xine-plugin`	Plugin auf der Basis von Xine

Für die meisten anderen Distributionen gibt es vergleichbare Pakete, die Paketnamen variieren aber. Es ist möglich, mehrere Multimedia-Player parallel zu installieren, aber Sie sollten sich für *ein* Webbrowser-Plugin entscheiden. Entscheidend ist in jedem Fall, dass Sie auch die erforderlichen Codec-Pakete installieren, die sich aus Lizenz- und Patentgründen oft *nicht* in den offiziellen Paketquellen befinden. Mehr Informationen zu diesem leidigen Thema finden Sie in Kapitel 10.

8.3 Google Chrome

In den vergangenen Jahren ist Google Chrome neben Firefox zum wichtigsten Webbrowser für Linux geworden. Was macht Chrome so attraktiv?

- Google Chrome ist ein vergleichsweise kleiner und schneller Webbrowser.
- Google Chrome ist im Hinblick auf größtmögliche Sicherheit optimiert und wird bei bekannten Sicherheitsmängeln schnell aktualisiert.
- Google Chrome enthält einen integrierten PDF-Viewer und die gerade aktuelle Version des Flash-Plugins. Weitere Plugins sind im Regelfall nicht erforderlich.
- Google Chrome richtet bei der Erstinstallation eine eigene Paketquelle ein, über die es Updates bezieht. Damit ist sichergestellt, dass jederzeit die gerade aktuellste stabile Version von Google Chrome installiert ist. Gerade bei älteren Distributionen, die sich noch nicht an den raschen Firefox-Release-Zyklus angepasst haben, bietet Google Chrome den oft einfachsten Weg hin zu einem modernen, standardkonformen Webbrowser.
- Jede Webseite (jedes Tab) wird von einem eigenen Prozess ausgeführt. Sollte eine Seite einen Absturz verursachen, so ist davon nur das entsprechende Dialogblatt betroffen. Der Webbrowser an sich läuft mit den anderen Seiten weiter.

Gegen Google Chrome sprechen eigentlich nur Datenschutzbedenken sowie der Umstand, dass das Angebot an Erweiterungen kleiner ist als für Firefox. Persönlich vermisse ich zudem eine vertikale Lesezeichenleiste (Strg+B bei Firefox).

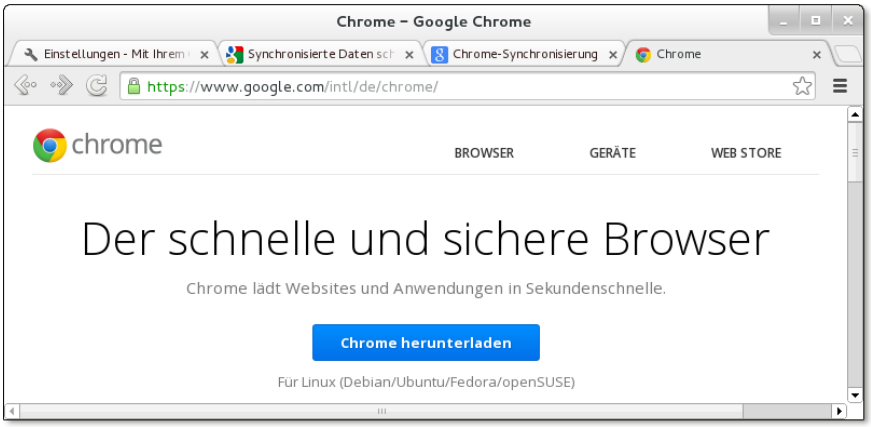


Abbildung 8.3 Google Chrome

Google Chrome versus Chromium

Google stellt Chrome zwar kostenlos zur Verfügung, die Binärpakete von *google.com* stehen aber nicht unter einer Open-Source-Lizenz zur Verfügung! Wenn Sie auf reinen Open-Source-Code Wert legen, müssen Sie statt Google Chrome dessen Open-Source-Basis Chromium installieren. Chromium steht bei vielen Distributionen als Paket zur Verfügung und kann mühelos installiert werden.

Es gibt nur wenige Unterschiede zwischen Google Chrome und Chromium: Bei Chromium fehlen das Google-Logo und das Google-Update-System. Stattdessen beziehen Sie Chromium-Updates über die Paketverwaltung Ihrer Distribution. Damit sind Sie darauf angewiesen, dass Ihre Distribution das Chromium-Paket gut wartet. In der Vergangenheit hat das leider nicht bei allen Distributionen gut geklappt! Auch auf die Integration der Plugins für Flash und PDF müssen Sie verzichten.

Installation

Sie finden RPM- und DEB-Installationspakete für Debian, Fedora, SUSE und Ubuntu in 32- und 64-Bit-Versionen auf der folgenden Seite zum Download:

http://www.google.com/chrome

Bei den meisten Distributionen wird nach dem Download automatisch ein geeignetes Paketinstallationsprogramm gestartet. Ist das nicht der Fall, installieren Sie das Paket manuell mit `zypper install`, `yum localinstall` `rpm -i` oder `dpkg -i`.

Während der Installation wird automatisch eine eigene Paketquelle eingerichtet: bei Debian/Ubuntu in der Datei `/etc/apt/sources.list.d/google-chrome.list`, bei Fedora in `/etc/yum.repos.d/google-chrome.repo` und bei openSUSE in `/etc/zypp/repos.d/google-chrome.repo`. Die Paketquelle stellt sicher, dass Sie in Zukunft über das Update-System neue Google-Chrome-Versionen erhalten.

Anmeldung

Beim ersten Start bietet Google Chrome Ihnen an, sich bei Ihrem Google-Konto anzumelden. Dieser Schritt ist natürlich freiwillig; wenn Sie aber ohnedies ein Google-Konto bzw. eine Gmail-Adresse haben, bietet die Verbindung des Webbrowsers zum Google-Konto eine Menge Vorteile: Ihre Lesezeichen, Online-Passwörter, offene Tabs, Google Apps etc. können nun über alle Ihre Geräte bzw. Webbrowser-Instanzen synchronisiert werden.

Im Detail steuern Sie mit EINSTELLUNGEN • ERWEITERTE SYNCHRONISIERUNGSEINSTELLUNGEN, welche Daten abgeglichen werden sollen und ob Ihre Daten mit einem eigenen Passwort verschlüsselt werden sollen. Um dem NSA und anderen Geheimdiensten den Zugriff auf Ihre persönlichen Daten nicht allzu leicht zu machen, ist Letzeres zu empfehlen – etwa nach dem Motto: »Wer meine Daten lesen will, muss sich zumindest anstrengen!«.

Bedienung

Die Benutzeroberfläche von Google Chrome ist minimalistisch. Es gibt kein reguläres Menü. Dafür führt ein Button ganz rechts in der Symbolleiste zu einem Menü mit diversen Einträgen, um die aktuelle Seite auszudrucken, diverse Optionen einzustellen etc.

Ebenso fehlt in Google Chrome ein eigenes Suchfeld. Stattdessen geben Sie die Suchbegriffe direkt im Adressfeld an. Die Suche wird standardmäßig natürlich mit Google durchgeführt, Sie können im Optionsdialog aber auch eine andere Suchmaschine einstellen.

Um im Web zu browsen, ohne Spuren auf dem lokalen Rechner zu hinterlassen, können Sie im Werkzeugmenü ein INKOGNITO-FENSTER öffnen.

Lesezeichen

Lesezeichen können nur in einer Symbolleiste dargestellt werden. Diese Lesezeichenleiste kann mit ⇧+Strg+B ein- und ausgeschaltet werden. Dafür enthält Google Chrome eine eingebaute Synchronisationsfunktion für Lesezeichen. Diese Funktion setzt voraus, dass Sie ein Google-Konto einrichten bzw. ein vorhandenes Konto angeben. Die Synchronisation erfolgt zwischen allen Google-Chrome-Installationen, die Sie mit dem Google-Konto verknüpft haben.

Plugins

Google Chrome wirbt damit, dass ein sicherer PDF-Reader sowie das gerade aktuellste Flash-Plugin direkt in den Browser integriert sind. Darüber hinaus ist die Plugin-Architektur von Google Chrome Firefox-kompatibel. Wenn Sie also andere Plugins für Firefox installiert haben, funktionieren diese Plugins in der Regel auch unter Chrome. Informationen über die verfügbaren Plugins liefert die Adresse *chrome://plugins*. Dort können Sie bei Bedarf einzelne Plugins deaktivieren.

Erweiterungen

Google Chrome kann wie Firefox um zusätzliche Funktionen erweitert werden. Darüber hinaus kann Chrome dazu verwendet werden, sogenannte Apps auszuführen, also gewissermaßen eigenständige Programme, die im Browser laufen. Erweiterungen und Apps (die meisten sind kostenlos!) finden Sie im Chrome Web Store:

https://chrome.google.com/webstore

Das Werkzeugmenü TOOLS • ERWEITERUNGEN listet alle installierten Erweiterungen auf und gibt Ihnen die Möglichkeit, einzelne Erweiterungen zu deaktivieren oder ganz zu entfernen.

8.4 Mail-Grundlagen

Aus Anwendersicht ist das Senden und Empfangen von E-Mails eine einfache Angelegenheit. Hinter den Kulissen sind die Vorgänge, die dabei stattfinden, aber nicht so trivial. Dieser Abschnitt gibt Ihnen daher einige Hintergrundinformationen zum Thema E-Mail. Noch mehr in die Tiefe geht Kapitel 37, wo es um die Konfiguration eines eigenen Mail-Servers geht.

Web-Mail versus Mail-Client

Wenn in diesem Kapitel von E-Mail-Clients die Rede ist, dann gehe ich davon, dass Sie Ihre E-Mails mit einem eigenen E-Mail-Programm bearbeiten möchten und nicht mit einer Weboberfläche (wie *http://gmx.net* oder *http://mail.google.com*). Beide Verfahren haben Vorteile, die sich sogar kombinieren lassen: Die Weboberfläche kann ja parallel zu einem Mail-Client verwendet werden, z. B. im Urlaub.

Die Qual der Wahl

In diesem Kapitel stelle ich Ihnen vier E-Mail-Clients näher vor – Thunderbird, Evolution (KDE), Kontact bzw. KMail (KDE) und Mutt. Daneben gibt es eine Reihe weiterer Programme. Für Rechner mit begrenzten Ressourcen bieten sich beispielsweise Claws Mail oder Slypheed an: Beide Programme bieten ansprechende Benutzeroberflächen, kommen aber mit vergleichsweise wenig RAM aus.

Im riesigen Mail-Client-Angebot unter Linux klafft eine offensichtliche Lücke: Ich kenne kein Programm, das für IT-Laien optimiert ist. Ein gemeinsames Merkmal aller in diesem Kapitel vorgestellten Programme ist eine überladene Oberfläche mit zahllosen Funktionen, die nur für Profis hilfreich sind. Vielleicht wird das Gnome-Programm Geary diese Lücke demnächst schließen. Die im Sommer 2013 verfügbare Version 0.3 besticht durch eine elegante, minimalistische Benutzeroberfläche, ist aber noch nicht alltagstauglich.

http://www.yorba.org/projects/geary

Konto/Account

Wenn Ihnen ein Mail-Anbieter eine E-Mail-Adresse zur Verfügung stellt, wird dieser Service auch als E-Mail-Konto oder -Account bezeichnet. Viele Leute besitzen mehrere E-Mail-Adressen, daher können die meisten E-Mail-Programme mehrere Konten verwalten. Damit Sie E-Mails von Ihrem Account lesen und neue Nachrichten versenden können, stellt Ihnen Ihr E-Mail-Provider Zugangsdaten zur Verfügung, die so ähnlich wie in Tabelle 8.4 aussehen:

Parameter	Beispiel
E-Mail-Adresse	kathrin.hofer@mailxxx.de
Postfach-Adresse für eingehende E-Mail (IMAP/POP)	imap.mailxxx.de **oder** pop.mailxxx.de
Server-Adresse für ausgehende E-Mail (SMTP)	smtp.mailxxx.de
Login-/Benutzername für das Postfach	khofer **oder** 12345678
Passwort	xxxxxxxx

Tabelle 8.4 Account-Zugangsdaten mit Beispielen

Mitunter wird als Login-Name für das Postfach auch die gesamte E-Mail-Adresse verwendet. Bei vorwiegend für die Benutzung über einen Webbrowser konzipierten E-Mail-Accounts (z. B. GMX, Google Mail) müssen Sie möglicherweise zuerst in der Weboberfläche einige Optionen ändern, bevor eine POP- oder IMAP-Nutzung möglich ist.

Protokolle

Die drei Abkürzungen POP, SMTP und IMAP bezeichnen verschiedene Protokolle zur Übertragung von E-Mails zwischen Ihrem Rechner und dem E-Mail-Provider:

- **POP:** Zur Übertragung von E-Mails vom Provider auf Ihren Rechner kommt häufig das Post Office Protocol (POP) zum Einsatz. Das Protokoll ist perfekt, wenn Sie nur *ein* E-Mail-Programm verwenden und die heruntergeladenen E-Mails auf Ihrem eigenen Rechner speichern. POP ist hingegen ungeeignet, wenn Sie parallel mehrere Mail-Clients benutzen.
- **IMAP:** Eine Alternative zu POP ist das Internet Message Access Protocol (IMAP). Der Hauptunterschied zu POP besteht darin, dass bei IMAP die E-Mails üblicherweise auf dem IMAP-Server bleiben und dort in mehreren Verzeichnissen (»Postfächern«) organisiert werden. Das E-Mail-Programm dient in diesem Fall also nur zur Kommunikation mit dem Server. IMAP ist dann optimal, wenn Sie Ihre E-Mails von unterschiedlichen Rechnern, Smartphones, Tablets etc. aus bearbeiten möchten. Wenn Sie auf der Suche nach einem neuen Mail-Account sind, sollten Sie unbedingt auf IMAP bestehen. Leider unterstützen manche kostenlose Mail-Provider nur POP.

- **SMTP:** Zum Versenden eigener E-Mails wird das Simple Mail Transfer Protocol (SMTP) verwendet. Zur Kommunikation mit dem SMTP-Server des Providers benötigt das E-Mail-Programm meist nur die Adresse des SMTP-Servers. Ob auch beim SMTP-Server eine Authentifizierung erforderlich ist, hängt vom Provider ab. Bei einigen Providern gilt eine vorherige POP-Authentifizierung automatisch auch für SMTP. Andere Provider verlangen eine eigene SMTP-Authentifizierung.

Während der Account-Konfiguration können Sie bei einigen E-Mail-Programmen Port-Nummern für POP, IMAP und SMTP angeben. Üblich sind die folgenden Ports:

POP: 110 (STARTTLS oder unverschlüsselt) bzw. 995 (SSL/TLS-verschlüsselt)
IMAP: 143 (STARTTLS oder unverschlüsselt) bzw. 993 (SSL/TLS-verschlüsselt)
SMTP: 25 (STARTTLS oder unverschlüsselt) bzw. 465 (SSL/TLS-verschlüsselt)

Die meisten Mail-Clients und Mail-Server unterstützen STARTTLS: Dabei beginnt die Kommunikation unverschlüsselt. Client und Server vereinbaren dann das bestmögliche Verschlüsselungsverfahren und setzen die Kommunikation am selben Port (also z. B. 25 bei SMTP) verschlüsselt fort.

Exchange-Server

Microsoft kocht bei E-Mails mit dem Exchange-Server sein eigenes Süppchen. Der Exchange-Server verwendet standardmäßig eigene Protokolle zur Kommunikation mit dem E-Mail-Client, weswegen die meisten Benutzer wohl oder übel Outlook verwenden. POP, IMAP und SMTP werden nur bei spezieller Konfiguration bzw. mit Zusatz-Software unterstützt. Das einzige Linux-Mail-Programm, das gut mit dem Exchange-Server kooperiert, ist Evolution.

Lokale E-Mails

Traditionell verwendet Unix bzw. Linux E-Mails auch als lokales Kommunikationsmedium. Manche Netzwerkdienste protokollieren Fehler daher nicht nur in einer Logging-Datei, sondern versenden auch eine E-Mail an `root`. Derartige E-Mails werden dann in einer lokalen Datei auf dem Rechner gespeichert, häufig in `/var/spool/mail/root`.

Die Gefahr ist groß, dass Sie derartige E-Mails nie zu sehen bekommen – und das gleich aus zweierlei Gründen: Erstens ignorieren die meisten grafischen E-Mail-Clients `/var/spool/mail/`*`loginname`*, und zweitens sind System-Mails meist an `root` adressiert, während Sie als gewöhnlicher Benutzer arbeiten.

Die Lösung für das erste Problem besteht darin, zum Lesen der lokalen E-Mails ein Programm zu verwenden, das `/var/spool/mail/`*`loginname`* berücksichtigt. Für diese Zwecke besonders gut geeignet ist das textbasierte Programm Mutt. Um die E-Mails zu lesen, loggen Sie sich vorübergehend als `root` ein (`su -l` oder `sudo -s`) und führen dann in einem Terminalfenster das Kommando `mutt` aus.

Noch eleganter ist es, alle an `root` adressierten E-Mails mit `/etc/aliases` in die Inbox des Benutzers umzuleiten, der normalerweise für die Administration des Rechners verantwortlich ist.

```
# am Ende von /etc/aliases
...
root:   kofler
```

Die geänderte Einstellung wird erst wirksam, wenn Sie das Kommando `newaliases` ausführen. Sie müssen aber weiterhin ein Programm verwenden, das die lokale Mailbox auswertet. Neben textbasierten Programmen wie `mutt` kommen hierfür auch Evolution und KMail infrage, wenn ein zusätzlicher Account entsprechend eingerichtet wird.

Mailbox-Formate

Alle E-Mail-Programme bieten die Möglichkeit, eingetroffene oder selbst verfasste E-Mails in Verzeichnissen zu speichern. Dabei kommt oft das mbox-Format zur Anwendung: Alle E-Mails eines Verzeichnisses werden einfach zu einer langen Textdatei verbunden. Zur Trennung zwischen den E-Mails dienen Zeilen, die mit `From` beginnen. Das Format ist im Internet dokumentiert, z. B. unter:

http://www.qmail.org/qmail-manual-html/man5/mbox.html

Die meisten E-Mail-Clients erzeugen neben den mbox-Dateien zusätzliche Indexdateien. Diese beschleunigen den Zugriff auf einzelne E-Mails, sind aber nicht zwischen den E-Mail-Programmen kompatibel.

Neben dem mbox-Format unterstützen manche E-Mail-Programme und die meisten E-Mail-Server auch das maildir-Format. Dabei wird jede einzelne E-Mail in einer eigenen Datei gespeichert. Eine Mailbox besteht aus allen Dateien innerhalb eines Verzeichnisses. Der offensichtliche Vorteil besteht darin, dass einzelne Nachrichten einfacher gelöscht werden können.

Lokale Mails von Windows zu Linux bringen

Unter Windows verwenden die meisten E-Mail-Clients jeweils ihr eigenes Format. Wenn Sie bisher unter Windows mit Microsoft Mail bzw. Outlook Express gearbeitet haben und nun unter Linux auf Thunderbird umsteigen möchten, sollten Sie einen Zwischenschritt einlegen und zuerst die Windows-Version von Thunderbird installieren. Damit können Sie nämlich Outlook-Express-E-Mails importieren. Anschließend kopieren Sie das gesamte E-Mail-Verzeichnis nach Linux. Alternativ können Sie Ihre lokalen E-Mails auch über ein ausreichend großes IMAP-Konto transferieren; bei großen E-Mail-Archiven ist das aber ein recht zeitaufwendiger Prozess.

Kontakte und Termine

Viele E-Mail-Programme enthalten auch Funktionen zur Adress- und Terminverwaltung. Das ist insbesondere praktisch, um E-Mail-Adressen und andere Kontaktdaten einheitlich zu erfassen und zu verwalten. Wenn diese Daten über mehrere Programme hinweg synchronisiert werden sollen, bieten sich hierfür Google oder eine eigene ownCloud-Installation an (siehe Kapitel 38).

Signierung und Verschlüsselung von E-Mails

E-Mails werden zwar viel schneller als gewöhnliche Post zugestellt, bedauerlicherweise ist es aber um die Sicherheit von E-Mails weniger gut bestellt: Für technisch versierte Personen ist es relativ einfach, E-Mails mit falschen Absenderadressen zu versenden oder von Ihnen an andere Personen versandte E-Mails zu lesen oder gar zu manipulieren. Aus diesem Grund sollten Sie niemals wirklich vertrauliche Daten in einer nicht verschlüsselten E-Mail versenden (z. B. eine Kreditkartennummer).

Durch die Signierung und Verschlüsselung können Sie Ihre E-Mail-Kommunikation wesentlich sicherer machen. Alle in diesem Kapitel vorgestellten E-Mail-Programme sind in der Lage, E-Mails zu signieren und zu verschlüsseln und können natürlich auch mit derart behandelten E-Mails umgehen.

Trotz der unbestrittenen Vorteile signierter bzw. verschlüsselter E-Mails werden Sie in der Praxis nur selten auf derartige E-Mails stoßen. Bequemlichkeit, die relativ komplexe Schlüsselverwaltung und zwei zueinander inkompatible Standards (PGP und S/MIME) stehen einer weiten Verbreitung im Wege.

Schlüssel

Zum Signieren bzw. Verschlüsseln werden sogenannte Schlüssel verwendet. Ein elektronischer Schlüssel ist einfach ein langer Zahlencode.

Geheimer und öffentlicher Schlüssel

Zum Signieren und Verschlüsseln von E-Mails werden die sogenannten asymmetrischen Verfahren eingesetzt. Jeder Schlüssel besteht daher aus zwei Teilen: aus einem geheimen Schlüssel, der normalerweise nur auf der Festplatte des Besitzers gespeichert ist, und aus einem öffentlichen Schlüssel, der z. B. im Internet publiziert wird. Das Besondere an den asymmetrischen Verfahren besteht darin, dass zum Signieren oder Verschlüsseln der eine Teil des Schlüssels verwendet wird, zur Kontrolle der Signatur bzw. zum Entschlüsseln dagegen der andere Teil des Schlüssels.

Signieren

Das Signieren einer E-Mail bedeutet, dass vor dem Versenden einer Nachricht eine Prüfsumme errechnet wird. Diese Prüfsumme wird verschlüsselt. Der Empfänger kann anhand der Prüfsumme sicherstellen, dass die E-Mail tatsächlich vom angegebenen Empfänger stammt und dass sie nach dem Versenden nicht manipuliert wurde.

Wenn Sie eine E-Mail signieren, verwendet das E-Mail-Programm dazu Ihren geheimen Schlüssel. Zur Kontrolle der Signatur reicht aber der öffentliche Schlüssel aus. Das bedeutet: Nur Sie selbst können Ihre E-Mails signieren (weil nur Sie Ihren geheimen Schlüssel besitzen). Es kann aber jeder Ihre signierte E-Mail kontrollieren, weil jeder über das Internet Zugang zu Ihrem öffentlichen Schlüssel hat.

Ihre signierte E-Mail kann jeder lesen, auch wenn der Empfänger Ihren öffentlichen Schlüssel nicht kennt oder ein E-Mail-Programm ohne Signaturfunktionen verwendet (z. B. ein Webmail-Interface). In solchen Fällen wird unterhalb der E-Mail der Signaturcode angezeigt. Dieser Code behindert das Lesen der eigentlichen Nachricht nicht. Ein Empfänger ohne Signaturmöglichkeiten kann aber nicht kontrollieren, ob die E-Mail tatsächlich von Ihnen stammt.

Verschlüsseln

Das Verschlüsseln einer E-Mail bedeutet, dass die E-Mail nicht im Klartext versendet wird, sondern in einer verschlüsselten Form. Niemand kann den Inhalt dieser E-Mail lesen, wenn er nicht den richtigen Schlüssel kennt, um die Verschlüsselung wieder aufzuheben.

Zum Verschlüsseln wird der öffentliche Schlüssel des Empfängers (!) verwendet. (Wenn Sie also eine verschlüsselte E-Mail an Gabi versenden möchten, müssen Sie sich zuerst den öffentlichen Schlüssel von Gabi besorgen.) Die verschlüsselte E-Mail kann anschließend nur noch durch den geheimen Schlüssel des Empfängers entschlüsselt werden. Diesen Schlüssel hat nur Gabi.

Ihre verschlüsselte E-Mail kann nur der Empfänger lesen, der den geheimen Teil des Schlüssels besitzt, dessen öffentlicher Teil zur Verschlüsselung eingesetzt wurde. Wenn der Empfänger seinen geheimen Schlüssel verloren oder irrtümlich gelöscht hat oder wenn er ein E-Mail-Programm ohne Verschlüsselungsfunktionen verwendet, sieht er nur eine lange Liste von Zahlen und Codes. Die Nachricht ist dann vollkommen wertlos.

PGP versus S/MIME

Es wäre zu einfach, wenn es zum Signieren, Verschlüsseln und zur Schlüsselverwaltung nur ein Verfahren gäbe! Etabliert haben sich vielmehr zwei Verfahren, die beide als sicher gelten:

- **PGP bzw. GPG bzw. OpenPGP:** Vorreiter in Sachen E-Mail-Verschlüsselung war das Software-Projekt PGP (Pretty Good Privacy). Als PGP zu einem kommerziellen Produkt wurde, schuf die Open-Source-Gemeinde das dazu weitgehend kompatible Projekt GPG (GNU Privacy Guard). OpenPGP ist schließlich ein öffentlicher Internet-Standard, dem sowohl PGP als auch GPG entsprechen.

  Standardmäßig wird durch PGP nur die eigentliche Nachricht signiert bzw. verschlüsselt. Wenn Sie auch Anhänge signieren bzw. verschlüsseln möchten, müssen Sie die Variante PGP/MIME nutzen.

Das aus Anwendersicht vielleicht wichtigste Merkmal von PGP besteht darin, dass es sehr einfach ist, die erforderlichen Schlüssel selbst zu erzeugen. Damit eignet sich PGP nicht nur für große Unternehmen, sondern auch für kleine Betriebe. Auch in der Linux- und Open-Source-Szene dominiert PGP. Sowohl Gnome als auch KDE bieten ausgereifte Werkzeuge zur Schlüsselverwaltung an. Leider unterstützen manche Windows-E-Mail-Clients PGP nicht bzw. erst nach der Installation von Erweiterungen oder Plugins.

- **S/MIME:** S/MIME (Secure Multipurpose Internet Mail Extension) basiert auf anderen Verschlüsselungsalgorithmen. Als S/MIME-Schlüssel müssen sogenannte X.509-Zertifikate verwendet werden.

  S/MIME-signierte bzw. -verschlüsselte Dokumente haben bei manchen öffentlichen Behörden denselben Wert wie eigenhändig unterschriebene Schriftstücke. Das gilt allerdings nur, wenn die eingesetzten X.509-Zertifikate von autorisierten Trustcentern (CA = Certificate Authority) nach der Kontrolle von Persönlichkeitsdaten (z. B. des Personalausweises) herausgegeben wurden. Derartige Zertifikate kosten aufgrund des hohen administrativen Aufwands relativ viel Geld, sind dafür aber vertrauenswürdiger als selbst erzeugte Schlüssel.

  S/MIME ist in der Windows-Welt weit verbreitet und wird auch unter Linux von den meisten E-Mail-Clients unterstützt – wenn auch zum Teil weniger gut als PGP. Die größte Hürde für Privatanwender besteht darin, sich einen S/MIME-Schlüssel zu beschaffen.

Leider sind die beiden Verfahren miteinander inkompatibel. Eine PGP-verschlüsselte E-Mail kann nicht mit den Mitteln von S/MIME gelesen werden und umgekehrt. Es gibt zwar E-Mail-Programme, die mit beiden Verschlüsselungsmechanismen zurechtkommen, aber in diesem Fall benötigen Sie für beide Verfahren jeweils eigene Schlüssel. Außerdem kann eine E-Mail immer nur mit einem Verfahren verschlüsselt werden, nicht mit beiden. Kurz und gut: PGP bietet nach dem aktuellen Wissensstand alles, um sicher und ohne zusätzliche Kosten miteinander zu kommunizieren. Der wesentliche Vorteil von S/MIME besteht darin, dass es bei der Verwendung von qualifizierten X.509-Zertifikaten einen verbindlicheren rechtlichen Charakter hat.

Schlüsselverwaltung

Die meisten E-Mail-Clients können die zum Senden und Empfangen erforderlichen Schlüssel selbst verwalten bzw. bei Bedarf einen neuen Schlüssel erzeugen. Da die Schlüssel aber oft auch für andere Aufgaben benötigt werden, ist es zweckmäßig, die Schlüsselverwaltung losgelöst vom E-Mail-Programm durchzuführen. Gnome unterstützt Sie bei dieser Aufgabe durch das Programm Seahorse, KDE durch KGpg und Kleopatra (für S/MIME).

Die primäre Aufgabe der Schlüsselverwaltung besteht darin, die öffentlichen Teile der Schlüssel Ihrer Kommunikationspartner in einem sogenannten Schlüsselbund zu sammeln. Beim Import neuer Schlüssel müssen Sie diese »signieren«. Das bedeutet, dass Sie davon überzeugt sind, dass der importierte Schlüssel tatsächlich von der richtigen Person stammt. Sofern Sie mit PGP-Schlüsseln arbeiten, befinden sich alle Verwaltungsdateien im Verzeichnis `.gnupg`.

8.5 Thunderbird

Das E-Mail-Programm Thunderbird ist wie Firefox aus dem ehemaligen Mozilla-Projekt hervorgegangen. Obwohl es für die meisten Distributionen Thunderbird-Pakete gibt, ist das Programm oft nicht installiert. Der Grund: Gnome und KDE sehen Evolution bzw. KMail als Standard-E-Mail-Client vor. Zu den wenigen Ausnahmen zählt Ubuntu, wo Thunderbird per Default vorinstalliert ist.

Thunderbird, Evolution oder KMail?

Die Entscheidung zwischen Thunderbird, Evolution oder KMail fällt schwer. Alle drei Programme bieten zahllose Funktionen und richten sich eher an fortgeschrittene Anwender. Persönlich bin ich ein Thunderbird-Fan. Für Evolution und KMail sprechen freilich die bessere Integration in Gnome und KDE, besonders bei der Kontakt- und Terminverwaltung.

Zukunft

Die Mozilla Foundation hat im Juni 2012 überraschend verkündet, die Weiterentwicklung von Thunderbird einzustellen. Im Herbst 2012 gab es mit Version 17 noch ein *Extended Support Release* (ESR). Seither kümmert sich die Mozilla Foundation nur noch um die Infrastruktur für das Projekt sowie um Sicherheits-Updates. Neue Funktionen wird Thunderbird nur erhalten, wenn diese von außen, also von der Community beigesteuert werden.

Icedove

Unter Debian werden Sie vergeblich nach einem Thunderbird-Paket suchen. Aufgrund der strengen Bestimmungen für die Benutzung der registrierten Marke »Thunderbird« benannten die Debian-Entwickler das Programm in Icedove um. Die Verwendung eines eigenen Namens erlaubt es Debian, das Programm um eigenen Code zu erweitern und eigene Icons einzusetzen.

Installation

Bei vielen Distributionen ist Thunderbird in mehrere Pakete aufgeteilt. Eines enthält die Grundfunktionen, und weitere Pakete enthalten die Menü- und Dialogtexte für verschiedene Sprachen. Vergessen Sie nicht, auch das deutsche Sprachpaket zu installieren! In Gnome bzw. KDE sollten Sie anschließend Thunderbird als Standard-E-Mail-Programm einrichten (siehe Abschnitt 5.4 bzw. 6.4).

Account-Konfiguration

Beim ersten Start erscheint automatisch der Konten-Assistent, der Ihnen die Einrichtung eines neuen E-Mail-Kontos anbietet. Im Regelfall werden Sie diesen Schritt überspringen und sich stattdessen für die Option MEINE EXISTIERENDE E-MAIL-ADRESSE VERWENDEN entscheiden.

Im Folgenden müssen Sie in der Regel nur drei Informationen angeben: Ihren Namen, Ihre E-Mail-Adresse und das Passwort für den E-Mail-Zugang. Thunderbird versucht die restlichen Parameter selbst zu erraten, was in vielen Fällen auch gelingt. Falls Ihr E-Mail-Server sowohl POP als auch IMAP unterstützt, entscheidet sich Thunderbird für IMAP. Bei Bedarf können Sie mit BEARBEITEN • KONTEN-EINSTELLUNGEN unzählige weitere Optionen einstellen und weitere Konten hinzufügen (siehe Abbildung 8.4).

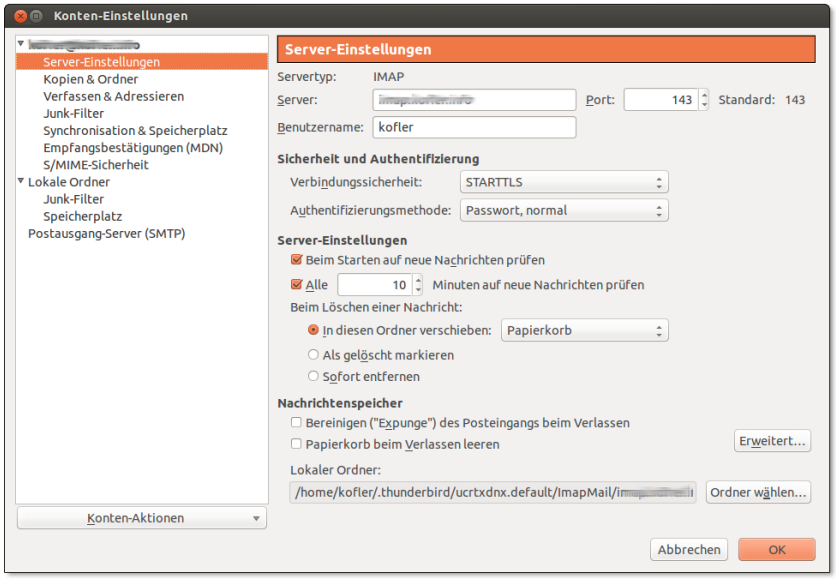


Abbildung 8.4 Account-Konfiguration in Thunderbird

Bei IMAP-Konten beginnt Thunderbird nach der Konfiguration, sämtliche E-Mails aus allen Verzeichnissen herunterzuladen. Die lokalen E-Mail-Kopien beschleunigen die Suchfunktionen, verursachen bei großen E-Mail-Konten aber eine Menge Download-Volumen und beanspruchen viel Platz auf der lokalen Festplatte oder SSD. Das können Sie vermeiden, indem Sie im Punkt SYNCHRONISATION & SPEICHERPLATZ die Synchronisation ganz abstellen, sie auf einzelne Postfächer limitieren oder pro Postfach nur ausgewählte Nachrichten synchronisieren, z. B. nur die aktuellsten E-Mails oder nur kleine E-Mails.

Grundfunktionen

Menüleiste

Um Platz zu sparen, zeigen aktuelle Thunderbird-Versionen keine Menüleiste mehr an. Das Menü ist nun hinter einem Button mit drei horizontalen Linien rechts oben im Fenster versteckt. Wenn Sie ein traditionelles Menü vorziehen, aktivieren Sie im Seitenmenü die Option EINSTELLUNGEN • MENÜLEISTE aus. Die folgenden Menükommandos beziehen sich auf die herkömmliche Menüleiste.

Posteingang

Neue E-Mails werden im Ordner POSTEINGANG gesammelt (siehe Abbildung 8.5). Unterhalb der Nachrichtenliste wird der Text der gerade ausgewählten E-Mail angezeigt. Mit einem Doppelklick innerhalb der Nachrichtenliste öffnen Sie ein eigenes E-Mail-Dialogblatt (Tab), das mehr Komfort und Platz zum Lesen umfangreicher E-Mails bietet. Wenn in HTML-Mails enthaltene Dateien und Bilder aus Sicherheitsgründen nicht geladen werden, schafft der Button EXTERNE INHALTE ANZEIGEN Abhilfe.

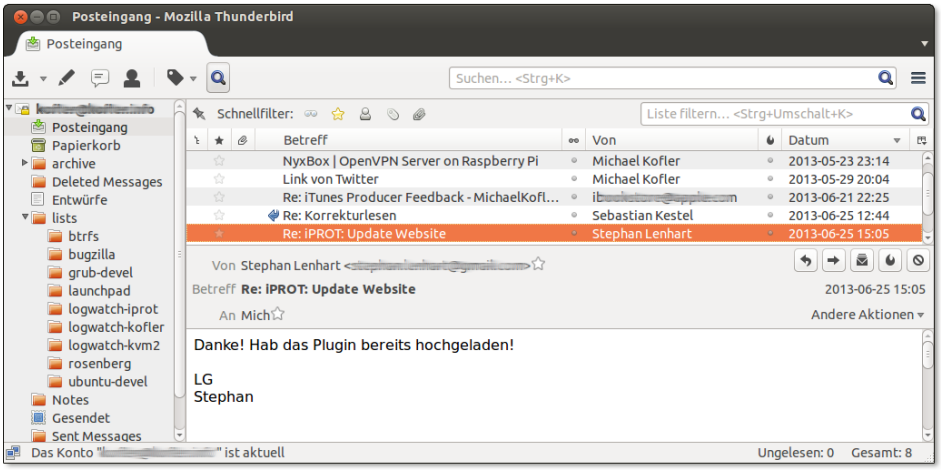


Abbildung 8.5 E-Mail-Verwaltung in Thunderbird

Ordneransichten

Im Menü ANSICHT • ORDNER können Sie zwischen verschiedenen Darstellungsformen wählen:

- Die Ansicht ALLE ORDNER ordnet alle Ordner dem jeweiligen Konto oder dem LOKALEN ORDNER zu. Der LOKALE ORDNER ist ein kontenunabhängiger Speicherort auf der Festplatte bzw. SSD. Der LOKALE ORDNER wird automatisch eingerichtet.
- Die Ansicht GRUPPIERTE ORDNER ist vor allem dann vorteilhaft, wenn Sie mehrere E-Mail-Konten eingerichtet haben. In diesem Fall werden Ordner aus verschiedenen Konten zusammengefasst. Damit sehen Sie alle neuen Nachrichten

in einem zentralen Posteingangsordner, alle gelöschten Nachrichten in einem zentralen Papierkorb etc.

- UNGELESENE ORDNER zeigt alle Ordner, die ungelesene E-Mails enthalten.
- FAVORITEN-ORDNER zeigt alle Ordner, die zuvor in einer anderen Ordneransicht per Kontextmenü als FAVORITEN deklariert wurden.
- LETZTE ORDNER zeigt die zuletzt aktiven Ordner.

E-Mails lesen und verfassen

Alle neuen E-Mails landen im Ordner POSTEINGANG. Dieser wird nach ein paar Tagen unübersichtlich. Deswegen sollten Sie E-Mails, die Sie nicht löschen möchten, in eigenen Ordnern archivieren. Am einfachsten drücken Sie dazu A. Thunderbird verschiebt die Nachricht dann in einen Ordner, dessen Name sich aus dem Kontonamen, Archiv und der aktuellen Jahreszahl ergibt, z. B. KONTO • ARCHIVE • 2013.

Alternativ können Sie natürlich selbst eigene Unterordner anlegen und E-Mails per Drag&Drop dorthin verschieben. Passen Sie aber auf, wo Sie die Unterordner erzeugen: Wenn Sie mit IMAP arbeiten und möchten, dass die E-Mail in einem neuen Ordner des Mail-Servers archiviert wird, müssen Sie den Ordner dort erzeugen, nicht innerhalb von LOKALER ORDNER!

Vorhandene E-Mails beantworten Sie mit Strg+R (*reply*) bzw. mit ⇧+Strg+R (*reply all*) bzw. mit den entsprechenden Kommandos des NACHRICHT-Menüs. Der Unterschied zwischen den beiden Varianten besteht darin, dass die Antwort im ersten Fall nur an den Versender geht, aber im zweiten Fall auch an alle Personen, die die ursprüngliche E-Mail ebenfalls empfangen haben.

Beim Verfassen neuer E-Mails verwendet Thunderbird automatisch das HTML-Format. Beachten Sie aber, dass sich nicht jeder Empfänger über diese Formatierung freut. Um eine einzelne E-Mail als reine Textnachricht zu verfassen, drücken Sie die ⇧-Taste, während Sie den Button VERFASSEN oder ANTWORTEN anklicken. Wenn Sie generell nur Text-Mails erstellen möchten, deaktivieren Sie im Konfigurationsdialog BEARBEITEN • KONTEN • VERFASSEN die Option NACHRICHTEN IM HTML-FORMAT VERFASSEN.

Anhänge

Thunderbird bietet die Möglichkeit, Anhänge nicht zusammen mit der E-Mail zu versenden; stattdessen werden die Dateien bei einem Online-Speicherdienst hochgeladen. Die E-Mail enthält dann nur einen Download-Link für den Anhang. Damit lässt sich vermeiden, dass zu große E-Mails vom Mail-Server zurückgewiesen werden.

Momentan werden die Dienste Box, YouSendIt und Ubuntu One unterstützt, DropBox und ownCloud aber leider nicht. Die Konfiguration dieser Funktion erfolgt in BEARBEITEN • EINSTELLUNGEN • ANHÄNGE. Sie benötigen ein Konto beim jeweiligen Speicherdienst. Auch nach der Konfiguration des Speicherdiensts bleibt die Funk-

tion optional: Sie können also vor dem Versenden jeder E-Mail festlegen, ob der Anhang in die E-Mail integriert wird oder ob er hochgeladen wird.

E-Mails suchen und filtern

Thunderbird bietet drei Möglichkeiten, um nach E-Mails zu suchen:

- **Globale Suche:** Um eine Suche in *allen* E-Mails durchzuführen, geben Sie die Suchbegriffe im Textfeld rechts oben im Thunderbird-Fenster ein. Nach wenigen Sekunden zeigt Thunderbird in einem Dialogblatt alle Suchergebnisse an. Sie können nun die Suchergebnisse einschränken und nur die E-Mails aus einer bestimmten Zeit, von oder an bestimmte Personen, aus einem bestimmten Ordner etc. anzeigen.
- **Filter:** Hier geben Sie die Suchbegriffe im Eingabefeld LISTE FILTERN ein und drücken ↵. Thunderbird reduziert nun die Liste der E-Mails im gerade aktuellen Verzeichnis auf alle E-Mails, die die Suchbegriffe im Absender-, Empfänger- oder Betreff-Feld enthalten. Optional können Sie die Suche auch auf den Nachrichteninhalt ausweiten.
- **Virtuelle Ordner:** Mit DATEI • NEU • VIRTUELLER ORDNER können Sie Suchkriterien formulieren. Diese Kriterien werden als virtueller Ordner gespeichert. Immer, wenn Sie diesen Ordner auswählen, werden darin alle E-Mails angezeigt, die den Suchkriterien entsprechen.

Adressbuch

Mit ⇧+Strg+B öffnen Sie das Adressbuch. Dort können Sie mehrere Adresslisten verwalten. Standardmäßig sind zwei Listen vorgesehen: PERSÖNLICHES ADRESSBUCH und GESAMMELTE ADRESSEN. Wenn Sie möchten, speichert Thunderbird automatisch alle Adressen, an die Sie E-Mails senden, in einem Adressbuch. Die entsprechende Option finden Sie im Dialogblatt BEARBEITEN • EINSTELLUNGEN • VERFASSEN • ADRESSIEREN.

Um E-Mail-Adressen manuell zu speichern, reicht ein einfacher Mausklick auf den Stern, der neben jeder E-Mail-Adresse in der Nachrichtenansicht angezeigt wird. Bei bereits bekannten Adressen wird dieser Stern gefüllt angezeigt, bei unbekannten Adressen als Kontur. Weitere Kontaktdaten können Sie anschließend im Adressbuchfenster hinzufügen. Mit EXTRAS • IMPORTIEREN können Sie zudem bereits vorhandene Adressbuchdateien in den verschiedensten Formaten einlesen.

Um das Thunderbird-Adressbuch mit dem Ihres Google-Kontos zu synchronisieren, müssen Sie auf ein Add-ons zurückgreifen, z. B. auf *google contacts*. Bis zur ersten Synchronisation sind aber gleich zwei Thunderbird-Neustarts erforderlich: einmal nach der Add-on-Installation und ein zweites Mal nach dem Einrichten des Google-Mail-Kontos innerhalb des Google-Contacts-Add-ons (EXTRAS • ADD-ONS • ERWEITERUNGEN).

Leider ist das Thunderbird-Adressbuch für andere Linux-Programme unzugänglich und somit eine Insellösung. Auch die minimalistische, listenförmige Darstellung des Adressbuchs löst wenig Begeisterung aus.

Spamfilter

In Thunderbird ist ein Spamfilter integriert. Alle spamverdächtigen E-Mails werden als Junk klassifiziert und in den gleichnamigen Ordner verschoben. Zur Verbesserung der Spamerkennung trainieren Sie den Spamfilter einige Tage lang. Während dieser Zeit klicken Sie bei jeder E-Mail, die Thunderbird falsch klassifiziert hat, auf den JUNK-Button.

Noch effizienter geht es per Tastatur: J klassifiziert zuvor markierte E-Mails als Spam, ⇧+J hebt eine irrtümliche Markierung als Spam auf. Weitere Optionen zur Spambekämpfung finden Sie im Konfigurationsdialog BEARBEITEN • EINSTELLUNGEN • SICHERHEIT.

Filter

Unabhängig vom Spamfilter können Sie mit EXTRAS • FILTER weitere Filterregeln definieren. Auf diese Weise können Sie alle eintreffenden E-Mails, die ein bestimmtes Kriterium erfüllen, markieren oder automatisch in einen beliebigen Ordner verschieben. Das ist insbesondere zur automatischen Verarbeitung von E-Mails aus Mailing-Listen praktisch.

Interna

Thunderbird speichert lokal heruntergeladene E-Mails sowie alle Konfigurationseinstellungen im Verzeichnis `.thunderbird/xxxxxxxx.default`, wobei `xxxxxxxx` eine zufällig generierte Zeichenkette ist. Die E-Mail-Ordner liegen im mbox-Format vor und befinden sich im Unterverzeichnis `Mail`.

Wenn Sie von Windows auf Linux umsteigen, können Sie Ihr `Mail`-Verzeichnis der Thunderbird-Installation unter Windows einfach in das betreffende Linux-Verzeichnis kopieren. Wenn Sie unter Windows mit einem anderen E-Mail-Client gearbeitet haben (z. B. Microsoft Mail), empfiehlt es sich, einen Zwischenschritt einzulegen: Die Windows-Version von Thunderbird bietet wesentlich bessere Import-Werkzeuge als die Linux-Version und hilft bei der Übertragung Ihrer E-Mail-Archive in ein Linux-kompatibles Format.

Beachten Sie, dass Thunderbird E-Mails normalerweise nicht physikalisch löscht. Die E-Mails werden nur als gelöscht markiert, verbleiben aber in der Datei. Deswegen beanspruchen Verzeichnisse für den Posteingang, für Spam-Mails sowie der Papierkorb oft unverhältnismäßig viel Platz. Abhilfe schafft das Kontextmenükommando KOMPRIMIEREN, das gelöschte E-Mails endgültig aus den mbox-Dateien entfernt.

Erweiterungen und Zusatzfunktionen

Add-ons

Ähnlich wie bei Firefox können auch bei Thunderbird mit Extras • Add-ons zusätzliche Funktionen in Form von Add-ons hinzugefügt werden. Erweiterungen werden erst nach einem Neustart von Thunderbird wirksam. Nach jedem Thunderbird-Update müssen in der Regel auch die Erweiterungen aktualisiert werden, was mitunter Probleme verursacht (z. B. wenn die Erweiterung nicht ebenfalls in einer aktualisierten Version zur Verfügung steht).

Um eine manuell heruntergeladene XPI-Datei mit einem Thunderbird-Add-on zu installieren, führen Sie Extras • Add-ons aus. Im Add-on-Dialog befindet sich am oberen Rand in der Mitte ein Werkzeug-Button, der in ein Menü führt. Dort haben die Thunderbird-Entwickler das Kommando Add-on aus Datei installieren versteckt.

E-Mails signieren/ verschlüsseln

In Thunderbird sind Kryptografiefunktionen für S/MIME bereits fix integriert. Sie finden alle erforderlichen Einstellungen im Dialogblatt Bearbeiten • Konten • S/MIME-Sicherheit. Der Button Zertifikate führt zu einem weiteren Dialog zur Verwaltung der X.509-Zertifikate, die bei S/MIME als Schlüssel dienen.

Damit Sie in Thunderbird PGP-signierte oder -verschlüsselte E-Mails lesen oder selbst verfassen können, müssen Sie das Add-on *Enigmail* installieren. Das Add-on setzt voraus, dass auf dem Rechner `gnupg` installiert ist. Das ist bei nahezu allen Distributionen der Fall. Alle Verschlüsselungsfunktionen sind über das OpenPGP-Menü im Hauptfenster und im Verfassen-Fenster zugänglich. Bei manchen Distributionen gibt es für Enigmail sogar ein eigenes Paket, das mit den Paketverwaltungswerkzeugen installiert werden kann.

Termin-verwaltung

Thunderbird enthält keine Funktionen zur Terminverwaltung. Abhilfe schafft das Add-on *Lightning* (siehe Abbildung 8.6). Es hilft bei der Synchronisation von Terminen mit externen Servern in den Formaten CalDAV oder WCAP und kann Termine im Format iCal importieren und exportieren.

http://www.mozilla.org/projects/calendar/lightning

Neue Kalender richten Sie mit Datei • Neu • Kalender bzw. im Minimenü mit Neue Nachricht • Kalender ein. Für den Google-Kalender müssen Sie dabei die folgende Adresse verwenden:

https://www.google.com/calendar/dav/ID/events

Dabei müssen Sie anstelle der *ID* für den Hauptkalender Ihre Google-E-Mail-Adresse angeben. Für die anderen Kalender ermitteln Sie die ID-Zeichenkette in der Google-Mail-Weboberfläche in den Einstellungen.

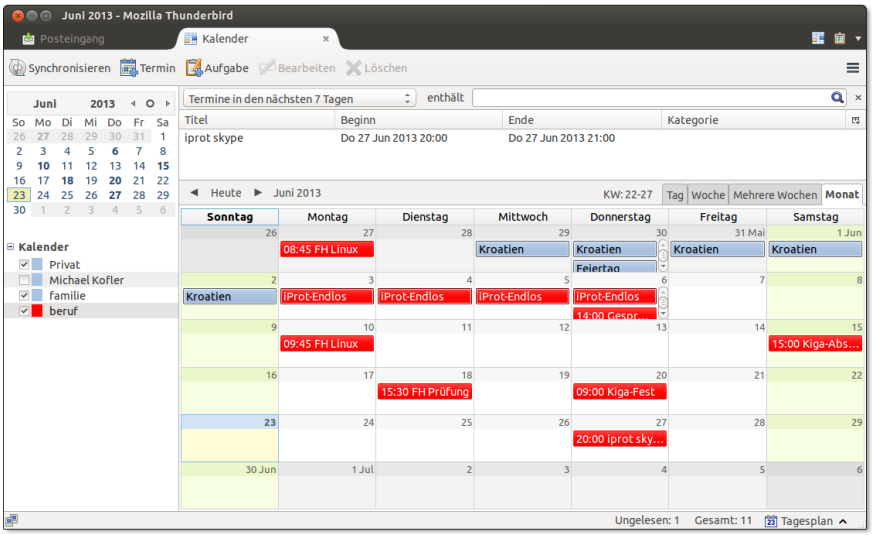


Abbildung 8.6 Die Lightning-Erweiterung zur Terminverwaltung

8.6 Evolution

Das Programm Evolution wurde ursprünglich von der Firma Ximian als Alternative zu Microsoft Outlook konzipiert. Später wurde Evolution das Standard-E-Mail-Programm des Gnome-Desktops. Evolution kann nicht nur zum Lesen und Schreiben von E-Mails verwendet werden, sondern enthält auch Funktionen zur Adress- und Terminverwaltung, zur Synchronisation dieser Daten mit dem Microsoft Exchange Server, zur Verschlüsselung von E-Mails mit PGP oder S/MIME etc.

Die vielen Funktionen führen leider zu einer unübersichtlichen Benutzeroberfläche und immer wieder zu Stabilitätsproblemen. Canonical hat deswegen Ubuntu mehrfach mit einer etwas älteren Evolution-Version ausgeliefert und ist schließlich auf Thunderbird als Default-E-Mail-Client umgestiegen. Die meisten anderen Gnome-basierten Distributionen verwenden aber weiterhin Evolution.

Account-Konfiguration

Beim ersten Start von Evolution erscheint ein Assistent zur Einrichtung des E-Mail-Accounts. Der Assistent muss vollständig ausgeführt werden, bevor Evolution genutzt werden kann.

Die Konfiguration beginnt mit der Angabe Ihres Namens und Ihrer E-Mail-Adresse. Im nächsten Dialog folgen die Daten des Mail-Servers, von dem Sie Ihre E-Mail holen: Hier geben Sie den Server-Typ (z. B. POP oder IMAP), die Adresse des Servers sowie

Ihren Login-Namen (Benutzernamen) an. Die unzähligen zur Auswahl stehenden Optionen belassen Sie auf den Vorgabeeinstellungen.

In einem weiteren Schritt konfigurieren Sie den Mail-Server (SMTP), an den Sie E-Mail senden. Sie müssen nicht nur den SMTP-Rechnernamen eingeben, sondern auch die Authentifizierungsoptionen einstellen. In den meisten Fällen lautet der richtige Legitimationstyp ANMELDEN. BENUTZERNAME bezeichnet nun den Login-Namen für SMTP. Nach dem Passwort werden Sie erst gefragt, wenn Sie zum ersten Mal E-Mails versenden.

Zuletzt müssen Sie dem Account noch einen Namen geben (standardmäßig einfach Ihre E-Mail-Adresse) und Ihre Zeitzone angeben, damit Evolution die Sendezeit korrekt eintragen kann. Nach dem Passwort werden Sie erst beim ersten Verbindungsaufbau gefragt, und zwar getrennt für das Empfangen und Senden von E-Mails.

Weitere Einstellungen können Sie später mit BEARBEITEN • EINSTELLUNGEN • E-MAIL-KONTEN vornehmen. Wenn Ihre E-Mails am Schluss immer denselben Text enthalten (z. B. *Mit freundlichen Grüßen* ...), können Sie hierfür im Dialogblatt IDENTITÄT eine Signatur angeben.

Grundfunktionen

Wenn Sie zum ersten Mal den Button VERSCHICKEN/ABRUFEN anklicken oder F9 drücken, um neue E-Mails zu laden, müssen Sie das Passwort für Ihr Postfach angeben. Das Passwort wird in der Gnome-Passwortverwaltung gespeichert. Evolution lädt bei HTML-Mails aus Sicherheitsgründen keine Dateien (auch keine Bilder), auf die die HTML-Nachricht verweist. Sie können dieses Verhalten im Konfigurationsdialog BEARBEITEN • EINSTELLUNGEN • E-MAIL-EINSTELLUNGEN • HTML-NACHRICHTEN ändern.

Neue E-Mails verfassen Sie mit Strg+N und versenden sie mit Strg+↵. Beim ersten Versenden fragt Evolution nach dem Passwort für den SMTP-Server, der ausgehende Nachrichten entgegennimmt. Standardmäßig erzeugt Evolution reine Text-Mails. Um eine HTML-Mail zu schreiben, führen Sie im VERFASSEN-Fenster FORMAT • HTML aus. Anschließend bieten diverse Buttons und die Menüs EINFÜGEN und FORMAT eine Menge Formatierungsmöglichkeiten. Wenn Sie E-Mails grundsätzlich als HTML-Mails schreiben möchten, führen Sie BEARBEITEN • EINSTELLUNGEN aus und aktivieren im Dialogblatt EDITOREINSTELLUNGEN • ALLGEMEIN die Option NACHRICHTEN IN HTML FORMATIEREN.

Evolution enthält direkt unterhalb der Symbolleiste ein Suchfeld, um rasch nach E-Mails zu suchen. Wenn Sie immer wieder dieselben Suchkriterien nutzen, lohnt

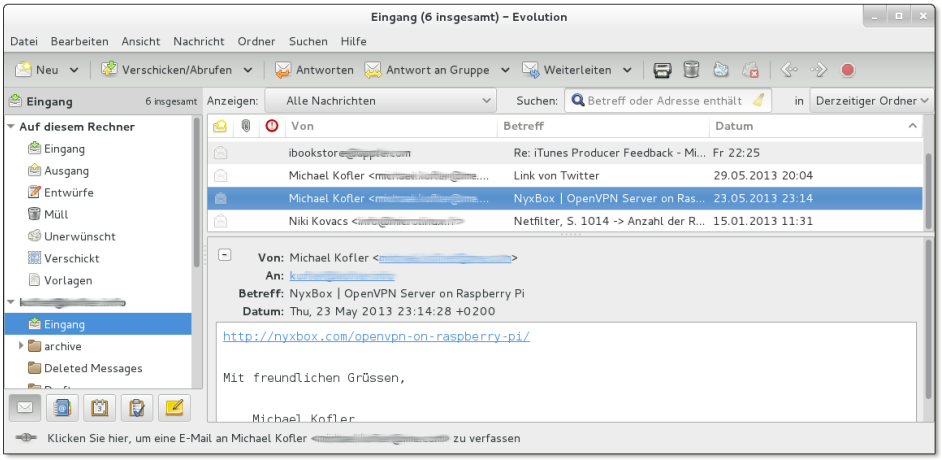


Abbildung 8.7 E-Mail-Verwaltung in Evolution

es sich, einen sogenannten Suchordner (ehemals »virtueller Ordner«) einzurichten. Darin werden alle E-Mails angezeigt, die bestimmten Suchkriterien entsprechen. Sie erstellen derartige Ordner mit BEARBEITEN • SUCHORDNER oder SUCHEN • SUCHORDNER AUS SUCHE ANLEGEN.

Spamfilter

Zur Erkennung unerwünschter E-Mails greift Evolution auf Bogofilter oder SpamAssassin zurück, je nachdem, welches Programm bereits installiert ist. Das gewünschte Programm wählen Sie mit BEARBEITEN • EINSTELLUNGEN • E-MAIL-EINSTELLUNGEN • UNERWÜNSCHT aus.

Um den Spamfilter auf die in einem Ordner bereits vorhandenen Nachrichten anzuwenden, markieren Sie alle Nachrichten mit Strg+A und führen dann NACHRICHT • ÜBERPRÜFUNG AUF UNERWÜNSCHTE NACHRICHT aus. Bei Verzeichnissen mit vielen E-Mails dauert dieser Vorgang recht lange. Als Spam erkannte Nachrichten werden in das Verzeichnis UNERWÜNSCHT verschoben.

In den ersten Wochen ist es häufig erforderlich, Nachrichten manuell als Spam zu kennzeichnen. Dazu markieren Sie die Nachrichten und klicken auf den Button UNERWÜNSCHT bzw. drücken Strg+J. Der Spamfilter versucht, Muster in den so markierten Nachrichten zu entdecken, die in der Folge bei der richtigen Klassifizierung weiterer E-Mails helfen.

Filter

Außer mit dem Spamfilter kann Evolution mit sogenannten Filterregeln eintreffende E-Mails automatisch in bestimmte Verzeichnisse verschieben oder auch gleich löschen. Das ist praktisch, wenn Sie sehr viele E-Mails erhalten und diese anhand von Mustern eindeutig zuzuordnen sind, z. B. anhand bestimmter Wörter in der Betreff-

zeile. Das ist typischerweise dann der Fall, wenn Sie in mehreren Mailing-Listen eingetragen sind.

Der einfachste Weg zur Definition einer neuen Filterregel besteht darin, die Nachricht zu markieren und dann NACHRICHT • REGEL ANLEGEN • FILTER ÜBER MAILINGLISTE auszuführen. Wenn Evolution die Filterregel nicht selbst richtig erkennt, können Sie sie ändern bzw. weitere Kriterien hinzufügen.

Interna

Evolution speichert E-Mails in `.local/share/evolution`, Konfigurationseinstellungen in `.config/evolution` und diverse Cache-Dateien in `.cache/evolution`. Für E-Mail-Ordner kommt das mbox-Format zur Anwendung, wobei Evolution zusätzliche Indexdateien anlegt.

Zusatzfunktionen

Adress- und Kontaktverwaltung

Das Evolution-Adressbuch ist eine vollständige Kontaktverwaltung, in der Sie neben Namen und E-Mail-Adressen unzählige weitere Daten speichern können. In das Adressbuch gelangen Sie mit ANSICHT • FENSTER • KONTAKTE oder einfach mit Strg+2. Mit DATEI • IMPORTIEREN • EINZELNE DATEI IMPORTIEREN können Sie Adressbuchdateien im Format LDIF (Lightweight Directory Interchange Format) importieren.

Mit DATEI • NEU • ADRESSBUCH können Sie neue Adressbücher einrichten, wobei als Datenquellen auch ein LDAP- oder WebDAV/CardDAV-Server sowie Google vorgesehen sind. Bei meinen Tests gelang auch der Adressabgleich mit ownCloud.

Stabilitätsprobleme

Beim Ausprobieren der Adresssynchronisation ist Evolution mehrfach abgestürzt. Wenn sich das Programm nach einem Absturz nicht mehr verwenden lässt, liegt das oft daran, dass die Hilfsdienste `evolution-calendar-factory` oder `evolution-addressbook-factory` nicht ordnungsgemäß beendet wurden. Öffnen Sie ein Terminalfenster, ermitteln Sie mit `ps ax` die Prozess-IDs der Hilfsdienste, und beenden Sie diese mit `kill`!

Kalender und Terminverwaltung

Das KALENDER-Modul hilft bei der Terminverwaltung. Vorhandene Termine können in unterschiedlichen Ansichten dargestellt werden: alle Termine eines Tags, einer Arbeitswoche, der gesamten Woche oder eines Monats. Viele Darstellungsdetails, z. B. die typische Arbeitszeit oder Schriftfarben, können Sie mit BEARBEITEN • EINSTELLUNGEN • KALENDER Ihren persönlichen Vorlieben anpassen.

Mit DATEI • NEU • KALENDER können Sie auch externe Kalender einrichten. Evolution unterstützt dabei die Protokolle WebCal und CalDAV sowie Google.

Aufgabenliste

Evolution enthält auch ein Modul zur Verwaltung von Aufgaben (also eine Art To-do-Liste). Die Aufgaben können wahlweise in einer eigenen Ansicht oder als Teilbereich der Kalenderansicht dargestellt werden.

Backups

Im DATEI-Menü können Sie ein vollständiges Backup aller Evolution-Daten anlegen. Eine derartige Sicherung ist auch dann praktisch, wenn Sie Ihr gesamtes Mail-Archiv inklusive aller Evolution-Einstellungen auf einen anderen Rechner übertragen möchten: Wenn Sie auf dem zweiten Rechner Evolution erstmalig starten, bietet das Programm Ihnen die Möglichkeit, die Daten aus einem Backup einzulesen.

Evolution Express

Für Gelegenheitsanwender, die nur einen simplen E-Mail-Client suchen, bietet Evolution zu viele Funktionen. Eine etwas schlankere Benutzeroberfläche erreichen Sie, wenn Sie Evolution mit der Option `--express` starten. Das Programm blendet dann die in diesem Abschnitt beschriebenen Zusatzfunktionen aus. Leider geht diese an sich gute Idee nicht weit genug: Sowohl dem Menü als auch den Konfigurationsdialogen würde eine Reduktion auf die Hälfte durchaus gut tun.

8.7 Kontact bzw. KMail

Kontact ist ein universelles Programm zur Verwaltung von E-Mails, Kontakten, Terminen, Aufgaben, Notizen sowie zur Anzeige von Nachrichten aus RSS-Feeds. Hinter den Kulissen ist Kontact eigentlich nur eine Benutzeroberfläche, um verschiedene KDE-Programme einheitlich zu bedienen. Beachten Sie, dass sich das Menü von Kontact verändert, je nachdem, welche Komponente gerade aktiv ist.

Für die E-Mail-Funktionen von Kontact ist KMail verantwortlich. Wenn Sie die restlichen Funktionen von Kontact nicht benötigen, können Sie KMail auch als eigenständiges Programm starten und ersparen sich so den durch Kontact bedingten Overhead. KMail ist stark technisch orientiert. Das Programm bietet zahllose Funktionen und lässt sich von Linux-Profis sehr effizient nutzen. Die Bedienung ist aber nicht immer intuitiv. Linux-Einsteigern ist das Programm daher nur eingeschränkt zu empfehlen.

Account-Konfiguration

Beim ersten Start erscheint ein Kontenassistent, in dem Sie drei Informationen angeben müssen: Ihren Namen, Ihre E-Mail-Adresse und das dazugehörende Passwort. In vielen Fällen reichen diese Angaben zur Account-Konfiguration aus. Kontact speichert die Passwörter in KWallet, einem KDE-Programm zur Verwaltung von Passwörtern und Schlüsseln. Wenn Sie KWallet bisher nicht verwendet haben, müssen Sie auch dieses Programm einrichten.

Nach der Erstkonfiguration laden Sie die E-Mails mit dem Button NACH E-MAILS SEHEN herunter. Im Dialogblatt EINSTELLUNGEN • KMAIL EINRICHTEN • ZUGÄNGE kön-

nen Sie weitere Konten einrichten. Irritierend ist dabei, dass POP-, IMAP- und SMTP-Server jeweils getrennt konfiguriert werden müssen. Wenn Sie also ein weiteres E-Mail-Konto hinzufügen möchten, müssen Sie *zwei* neue Zugänge einrichten: einen zum Empfang der Nachrichten (POP oder IMAP) und einen zweiten zum Versenden neuer E-Mails (SMTP). Diesem Ärgernis gehen Sie aus dem Weg, wenn Sie zum Einrichten neuer Konten EXTRAS • KONTEN-ASSISTENT ausführen.

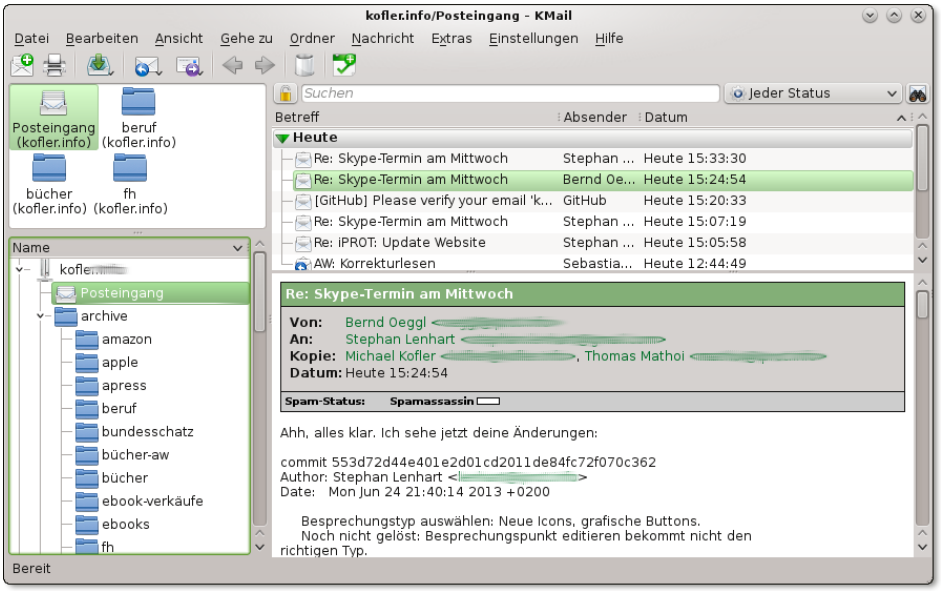


Abbildung 8.8 E-Mails verwalten mit KMail

E-Mails verfassen

Neue E-Mails sind standardmäßig reine Text-Mails. Wenn Sie eine HTML-Formatierung wünschen, führen Sie OPTIONEN • FORMATIERUNG (HTML) aus. Die fertige E-Mail versenden Sie mit Strg+↵.

KMail führt automatisch eine Rechtschreibprüfung durch und markiert alle nicht erkannten Wörter rot. Mit ANSICHT • WÖRTERBUCH können Sie zwischen verschiedenen Wörterbüchern wählen. Wenn die Rechtschreibprüfung nicht funktioniert, installieren Sie das Paket `aspell-de`.

Spam

KMail enthält keine integrierte Spamerkennung, kann diese Aufgabe aber an andere Programme delegieren. Bei der Konfiguration eines Spamfilters hilft das Kommando EXTRAS • ANTI-SPAM ASSISTENT. Sie müssen sich lediglich für eines der installierten Spamprogramme entscheiden – alles andere erledigt der Assistent. Als Spam erkannte E-Mails landen von nun an im Ordner MÜLLEIMER. Wie bei den anderen E-Mail-Programmen steigt die Trefferquote, wenn Sie falsch klassifizierte E-Mails manuell als Spam bzw. Nicht-Spam markieren.

Filter

Im Menü EINSTELLUNGEN können Sie Filter definieren, um E-Mails anhand verschiedener Kriterien in verschiedenen Verzeichnissen abzulegen oder auf andere Weise zu bearbeiten. KMail kennt sogar spezielle Filter für POP-Accounts, mit denen Sie unerwünschte E-Mails direkt auf dem Server löschen können, ohne diese vorher herunterzuladen.

Adressbuch und Kalender

Das in KMail bzw. Kontact integrierte Adressbuch kann auch Adressen von Online-Konten verwalten. Um ein neues Konto einzurichten, aktivieren Sie in Kontact das Adressbuch und führen DATEI • NEU • ADRESSBUCH HINZUFÜGEN aus. Sie haben nun die Wahl zwischen verschiedenen Adressbuchsystemen: DAV (z. B. für ownCloud, Zarafa oder Zimbra), Google Kontakte, Kolab, Open-Xchange etc. Bei meinen Tests gelang eine Synchronisation mit Google Mail auf Anhieb, der Zugriff auf das Adressbuch von ownCloud scheiterte aber ohne jede Fehlermeldungen.

Zur Kalenderkonfiguration führen Sie EINSTELLUNGEN • KALENDER EINRICHTEN • ALLGEMEIN • KALENDER aus. Sie haben die Wahl zwischen allen erdenklichen Arten von Online-Kalendern. Für ownCloud verwenden Sie den Typ DAV-GROUPWARE-RESSOURCE, wobei meine Tests diesmal auf Anhieb erfolgreich waren (siehe Abbildung 8.9).

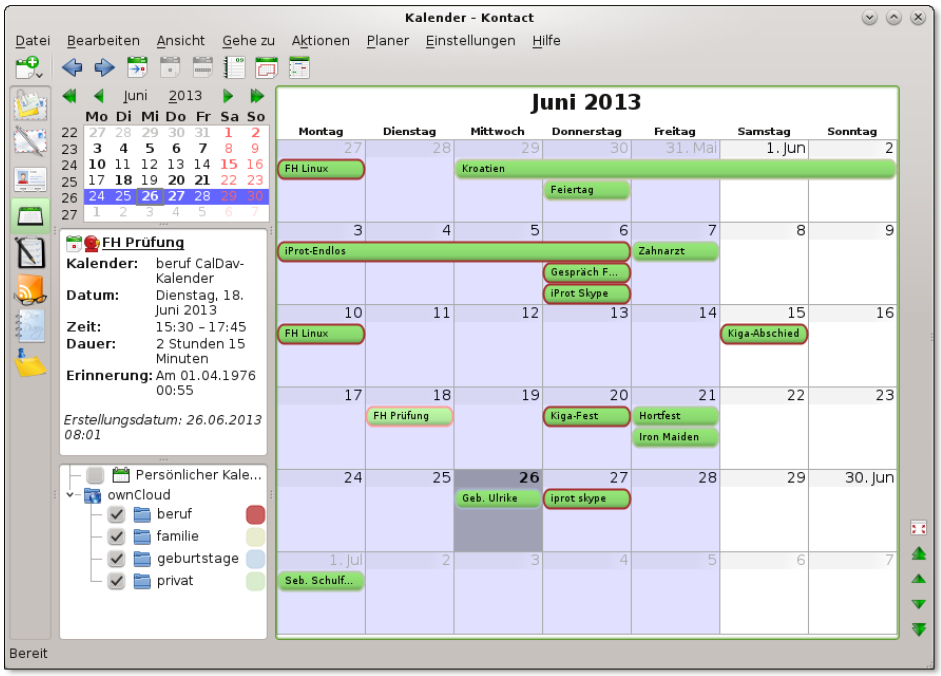


Abbildung 8.9 Die Kalenderansicht in Kontact

8.8 Mutt

Zum Lesen lokaler E-Mails bietet sich das textbasierte E-Mail-Programm Mutt an (siehe Abbildung 8.10). Vor dem ersten Einsatz muss das zumeist gleichnamige Paket installiert werden. In einem Konsolenfenster führen Sie zuerst `su -l` aus, um sich als `root` anzumelden, und starten das Programm dann mit dem Kommando `mutt`.

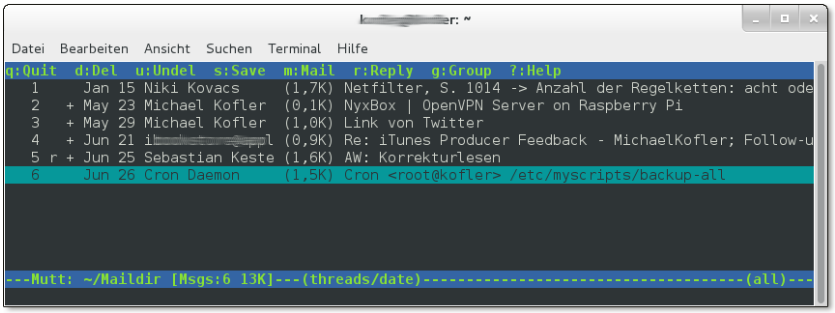


Abbildung 8.10 Lokale E-Mails mit Mutt lesen

Das Programm zeigt auf der Startseite die Titelzeilen aller E-Mails an. Wenn der aktive Benutzer noch keine einzige E-Mail empfangen hat, beklagt sich Mutt darüber, dass es die Datei `/var/mail/benutzer` noch nicht gibt. Diese Warnung können Sie ignorieren. Sie tritt nicht mehr auf, sobald die erste E-Mail eingetroffen ist.

Mit den Cursortasten bewegen Sie sich durch die Inbox. ↵ zeigt den Text der ausgewählten E-Mail an. Mit ␣ blättern Sie durch die Nachricht. J führt zur nächsten Nachricht, I zurück in die Inbox. ? zeigt einen Hilfetext mit allen wichtigen Tastenkürzeln an.

Um eine neue E-Mail zu verfassen, drücken Sie M und geben den Empfänger und die Subject-Zeile an. Anschließend startet Mutt den durch die Umgebungsvariable `$EDITOR` oder durch den Link `/etc/alternatives/editor` ausgewählten Editor. Dort schreiben Sie den Nachrichtentext, speichern ihn und verlassen den Editor. Anschließend versenden Sie die E-Mail in Mutt durch Y.

Q beendet das Programm. Beim Verlassen stellt Mutt zwei Fragen: Sollen mit D als gelöscht markierte E-Mails endgültig gelöscht werden? Und sollen gelesene Nachrichten nach `/home/`*`username`*`/mbox` verschoben werden? Wenn Sie vorhaben, die E-Mails später noch mit einem anderen Programm zu bearbeiten, sollten Sie beide Fragen mit N beantworten. Besonders die zweite Frage ist kritisch: In der lokalen `mbox`-Datei findet nur noch Mutt die E-Mails, nicht aber ein externes Programm wie z. B. der POP-Server Dovecot.

Konfiguration

Mutt funktioniert auf Anhieb, wenn sich Ihre E-Mail in einer mbox-Datei im Verzeichnis `/var/mail/name` befindet. Wenn Ihre E-Mails hingegen im Maildir-Format im Verzeichnis `Maildir` gespeichert werden, müssen Sie die Konfigurationsdatei `.muttrc` mit dem folgenden Inhalt einrichten:

```
# Datei .muttrc
set mbox_type=Maildir
set folder="~/Maildir"
set mask="!^\\.[^.]"
set mbox="~/Maildir"
set record="+.Sent"
set postponed="+.Drafts"
set spoolfile="~/Maildir"
```

Weitere Maildir-Konfigurationstipps für diverse Spezialfälle finden Sie hier:

http://wiki.mutt.org/?MuttFaq/Maildir
http://eising.wordpress.com/mutt-maildir-mini-howto

8.9 Social Networking, Twitter-Clients

An sich lassen sich Social-Networking-Dienste wie Facebook, Twitter und Google+ natürlich mit jedem Webbrowser bedienen. Aber nachdem Facebook-Apps sich zu den wichtigsten und am häufigsten eingesetzten Smartphone-Programmen entwickelt haben, darf natürlich auch Linux nicht zurückstehen und muss für diesen Zweck eigene Programme anbieten. Dieser Abschnitt stellt ganz kurz einige MicroBlogging-Clients vor, mit denen Sie Twitter- und Facebook-Nachrichten lesen bzw. selbst verfassen können.

Choqok

Der KDE-Microblogging-Client Choqok unterstützt die Dienste Twitter und Identi.ca. In typischer KDE-Manier umfasst der Konfigurationsdialog sechs Seiten – man würde es nicht für möglich halten, dass ein so einfaches Programm mit derart vielen Optionen ausgestattet ist. Wie auch immer: Einmal konfiguriert, funktioniert Choqok hervorragend.

Friends

Friends ist ein speziell für Ubuntu entwickeltes Social-Media-Programm (Paketname `friends-app`, siehe Abbildung 8.11). Es zeigt neue Nachrichten aus allen Social-Media-Kanälen, die im Modul ONLINE-KONTEN der Systemeinstellungen eingerichtet wurden. Im Sommer 2013 wirkte das Programm allerdings noch unausgereift.

Gwibber

Bis einschließlich Ubuntu 12.10 wurde unter Ubuntu standardmäßig das Programm Gwibber installiert. Es unterstützt die Nachrichtendienste von Twitter, Facebook, Flickr, Foursquare und Identi.ca. Wenn Sie mehrere Konten eingerichtet haben, kön-

nen Sie mit den Icons in der Statusleiste angeben, an welche Konten eine neue Nachricht gesendet werden soll.

Hotot

Eine gute Alternative zu Gwibber ist Hotot. Das Programm unterstützt zwar nur Twitter und Identi.ca, die wenigen Funktionen von Hotot bereiten aber weniger Probleme als der mitunter instabile bzw. langsame Gwibber.

Microblog-Plasmoid

Das KDE-Plasmoid *Microblog* ermöglicht es, Microblogging-Nachrichten von Twitter und Identi.ca direkt auf dem Desktop anzuzeigen. Persönlich finde ich die Desktop-Anzeige unpraktisch und ziehe ein eigenständiges Fenster vor, aber die Geschmäcker sind verschieden.

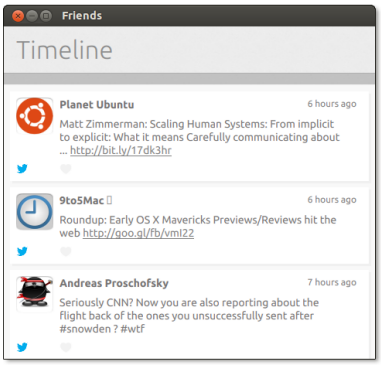


Abbildung 8.11 Social-Media-Nachrichten in Friends lesen

8.10 Skype

Skype ist ein kommerzielles Programm zur Internet-Telefonie. Unter Ubuntu steht es in der Canonical-Partner-Paketquelle zur Verfügung. Bei anderen Distributionen müssen Sie das Programm von der Skype-Website herunterladen und manuell installieren:

http://www.skype.com/intl/de/get-skype/other-downloads

Die Installation von Skype dauert geraume Zeit, weil in der Regel auch diverse zusätzliche Bibliotheken und andere Pakete heruntergeladen und eingerichtet werden müssen. Leider ist die Linux-Version von Skype stets um einige Versionen älter als die Versionen für Windows bzw. OS X. Zur Nutzung der Grundfunktionen reicht aber auch die Linux-Variante vollkommen aus.

Alternativen

Kein Linux-Fan installiert gerne ein kommerzielles Programm – noch dazu von Microsoft! –, wenn es Open-Source-Alternativen gibt. Tatsächlich herrscht an Telefonie-, Instant-Messaging und Chat-Programmen unter Linux durchaus kein Mangel (siehe Tabelle 8.5)! Google-Fans steht mit den Hangouts eine weitere, webbasierte Alternative zur Auswahl. Das Problem ist nur, dass sich beide Seiten auf ein Verfahren bzw. Protokoll einigen müssen – und da ist Skype häufig der kleinste gemeinsame Nenner.

Programmname	Website	Telefonie	Chat
Ekiga (Gnome)	*http://ekiga.org*	•	•
Empathy (Gnome)	*http://live.gnome.org/Empathy*	•	•
Konversation (KDE)	*http://konversation.kde.org*		•
Kopete (KDE)	*http://kopete.kde.org*	•	•
Pidgin (Gnome)	*http://pidgin.im*		•
Quassel (KDE)	*http://quassel-irc.org*	•	•
XChat	*http://www.xchat.org*		•

Tabelle 8.5 Telefonie- und Chat-Programme

8.11 Dropbox

Dropbox ermöglicht es, das lokale Verzeichnis `Dropbox` mit einem Online-Speicher zu synchronisieren. Auf diese Weise verfügen Sie nicht nur über ein Backup aller Dateien in diesem Verzeichnis, sondern können diese Dateien zudem unkompliziert über mehrere Rechner synchronisieren. Die Nutzung von Dropbox ist bis zu einem Datenvolumen von 2 GByte kostenlos.

Einige Distributionen stellen die Dropbox-Erweiterung für den Dateimanager Nautilus in fertigen Paketen zur Verfügung, z. B. `nautilus-dropbox` in Ubuntu. Für alle anderen Distributionen finden Sie den Dropbox-Client auf der Dropbox-Website zum Download:

https://www.dropbox.com/install?os=lnx

Nach der Installation führen Sie das Programm Dropbox oder das Kommando `dropbox start -i` aus und richten ein neues Dropbox-Konto ein bzw. melden sich bei Ihrem existierenden Konto an. Dabei wird automatisch das Verzeichnis `Dropbox` eingerichtet. Nach einem Neustart von Nautilus werden darin alle synchronisierten Dateien durch ein grünes OK-Häkchen gekennzeichnet.

Bei umfangreichen Änderungen im `Dropbox`-Verzeichnis dauert die Synchronisation eine Weile. Unter Ubuntu (Unity) gibt ein Panel-Icon Auskunft über den Status der Synchronisation. Unter Gnome 3 befindet sich ein entsprechendes Icon im Statusbereich, der nur angezeigt wird, wenn Sie die Maus nachdrücklich in den unteren Rand des Bildschirms bewegen.

Über das Dropbox-Menü können Sie diverse Dropbox-Einstellungen verändern. Insbesondere können Sie im Dialogblatt ERWEITERT mit dem Button SELEKTIVE SYNCHRONISATION einzelne Unterverzeichnisse innerhalb des `Dropbox`-Verzeichnisses von der Synchronisation ausschließen. Es gibt aber leider keine Möglichkeit, die Synchronisation für bestimmte Dateitypen zu deaktivieren.

Wie sicher sind Ihre Daten bei Dropbox?

Ihre Dateien werden auf den Dropbox-Servern zwar verschlüsselt, der Schlüssel ist allerdings von Dropbox vorgegeben und kann nicht individuell gewählt werden. Dieses Verfahren ist nur mäßig sicher. Persönliche bzw. unternehmenskritische Daten sollten daher nicht bzw. nur verschlüsselt im `Dropbox`-Verzeichnis gespeichert werden!

Alternativen

Sofern Sie über einen eigenen Server verfügen, können Sie mit ownCloud (siehe Kapitel 38) unbegrenzt große Verzeichnisse ohne zusätzliche Kosten synchronisieren. Ubuntu-Fans werden vielleicht den im nächsten Abschnitt beschriebenen Cloud-Service Ubuntu One in Erwägung ziehen. Daneben gibt es unzählige weitere Anbieter zur Synchronisation von Dateien in der Cloud: Google Drive, Microsoft SkyDrive, Apple iCloud, Box.net, Spideroak, SugarSync, Wuala, Pogoplug etc. Freilich stehen nicht für alle Cloud-Dienste Linux-Clients zur Verfügung. Außerdem gibt es wenige Dienste, die derart einfach und komfortabel zu nutzen sind wie Dropbox.

8.12 Ubuntu One

Ubuntu One ist ein von Canonical entwickelter Cloud-Dienst, um Daten von Ubuntu-Rechnern auf einem zentralen Server zu speichern und mit anderen Ubuntu-Rechnern auszutauschen bzw. zu synchronisieren. Ubuntu One ist auch die Basis für den Ubuntu One Music Store: Dort erworbene Audio-Dateien werden im Ubuntu One-Account gespeichert und können von dort auf Ihren Rechner heruntergeladen werden. Die Datenübertragung zwischen Ihrem Rechner und Ubuntu One erfolgt verschlüsselt, auf Ubuntu One werden Ihre Daten aber unverschlüsselt gespeichert. Für vertrauliche Daten ist Ubuntu One also ungeeignet.

Die Nutzung von Ubuntu One ist bis zu einem Speichervolumen von 5 GByte kostenlos, erfordert aber eine Registrierung bzw. einen Account auf *http://launchpad.net*. Wenn Sie mehr Speicherplatz wünschen, kosten je 20 weitere GByte ca. 25 EUR pro Jahr (Stand: Sommer 2013).

Vor der ersten Nutzung müssen Sie das Programm UBUNTU ONE installieren. Anschließend finden Sie das gleichnamige Modul in den Systemeinstellungen. Dort können Sie entweder einen neuen Account einrichten oder sich bei einem vorhandenen Account anmelden. Von nun an werden alle Dateien im Verzeichnis `Ubuntu One` automatisch synchronisiert. Ein kleines, wolkenförmiges Icon im Panel gibt den Synchronisationsstatus an.

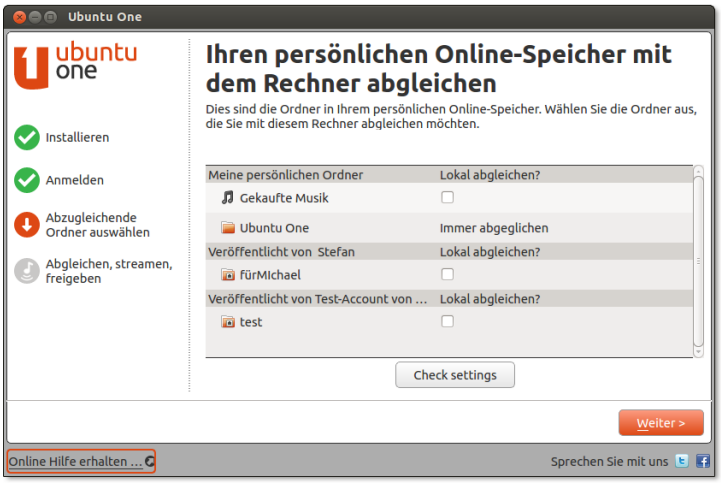


Abbildung 8.12 Ubuntu-One-Konfiguration

Auf die in Ubuntu One gespeicherten Daten können Sie auch mit Windows-, iOS- und Android-Versionen des Ubuntu-One-Clients zugreifen. Weitere Tipps und Anleitungen zur Nutzung von Ubuntu One finden Sie auf der folgenden Website:

https://one.ubuntu.com

8.13 Download-Manager

Anders als unter Windows gibt es für Linux nur wenige populäre FTP- und Download-Manager. Das hat zwei Gründe: Zum einen können Sie mit jedem Dateimanager FTP-Verzeichnisse genauso komfortabel wie lokale Verzeichnisse bearbeiten, und zum anderen gibt es unzählige Download-Kommandos (z. B. `wget`, `curl` und `mirror`), die sich perfekt zur Automatisierung von Downloads eignen.

FileZilla

Der beliebteste Download-Client mit grafischer Benutzeroberfläche ist FileZilla (siehe Abbildung 8.13). Dieses Programm unterstützt neben FTP auch die Protokolle SFTP und SSH, nicht aber HTTP.

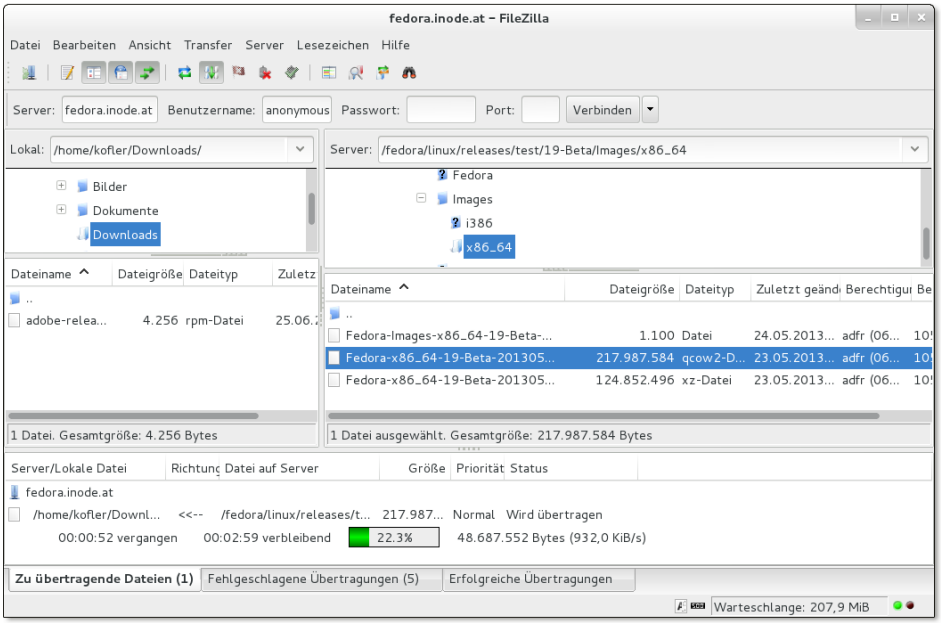


Abbildung 8.13 FileZilla

BitTorrent

BitTorrent ist ein Protokoll zum effizienten Download großer Dateien, die oft von vielen Benutzern gleichzeitig gewünscht werden. Die Grundidee ist einfach: Der Download erfolgt nicht von einem zentralen Server, sondern von allen im Netz verfügbaren Rechnern, auf denen zumindest Teile der Datei zur Verfügung stehen (also sogenanntes *Peer-to-Peer Networking*). Umgekehrt bedeutet das: Wenn Sie via BitTorrent eine große Datei herunterladen, stellen Sie diese Datei während dieser Zeit (und idealerweise auch danach) auch allen anderen BitTorrent-Benutzern im Netz zur Verfügung.

In der Linux-Praxis ist BitTorrent insofern interessant, als einige Distributionen DVD-Images als »Torrents« zur Verfügung stellen. Bei der Vorstellung einer neuen Version starten oft Tausende von Benutzern nahezu gleichzeitig den Download. Das überfordert jeden herkömmlichen FTP- oder HTTP-Server. Dank BitTorrent ist selbst in solchen Fällen ein Download in erträglicher Geschwindigkeit möglich. Weitere Informationen zu den Grundlagen und Techniken des BitTorrent-Verfahrens sind im folgenden Wikipedia-Artikel gut zusammengefasst:

http://de.wikipedia.org/wiki/BitTorrent

.torrent-Dateien

BitTorrent-Downloads werden durch `.torrent`-Dateien bekannt gegeben. Dabei handelt es sich um relativ kleine Binärdateien, die unter anderem Prüfsummen für zahllose Teilstücke der Datei enthalten. Das ermöglicht es, den Download nicht sequenziell, sondern in zufälliger Reihenfolge und parallel von mehreren im Netz verfügbaren BitTorrent-Quellen durchzuführen.

BitTorrent-Clients

BitTorrent-Clients sind Programme, die einerseits den Download durchführen und andererseits heruntergeladene Dateien anderen BitTorrent-Clients anbieten. Populäre Programme sind BitTorrent, KTorrent (KDE) sowie Transmission (Gnome), die alle eine ansprechende Oberfläche haben. Das KDE-Programm KTorrent zeigt an, welche Teile der Datei bereits heruntergeladen wurden (siehe Abbildung 8.14). Wenn Sie BitTorrent-Downloads interaktiv in einer Konsole oder automatisiert per Script ausführen möchten, sollten Sie einen Blick auf die BitTorrent-Varianten `bittorrent-curses` und `bittorent-console` werfen, die im `bittorrent`-Paket gleich mitgeliefert werden.

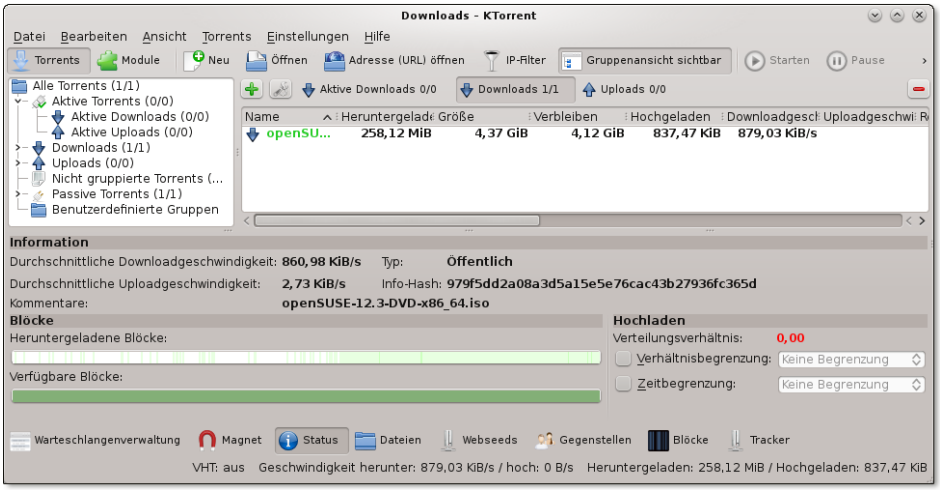


Abbildung 8.14 Downloads mit KTorrent

Kapitel 9
Fotos und Bilder

Dieses Kapitel stellt die wichtigsten Linux-Programme vor, um Fotos zu verwalten und weiterzuverarbeiten:

- **Shotwell:** Foto-Import und Bildverwaltung für Gnome
- **digiKam:** Foto-Import und Bildverwaltung für KDE
- **RawTherapee, Darktable:** RAW-Fotos optimieren
- **Gimp:** Bilder bearbeiten
- **Hugin:** Panoramas zusammensetzen
- **XSane**, **SimpleScan** und **Skanlite:** Scan-Programme
- Diverse Programme, um Screenshots zu erstellen

Beschränken Sie sich bei der Programmauswahl nicht auf das von Ihrem Desktop-System angebotene Standardprogramm! Es spricht nichts dagegen, unter Gnome ein KDE-Programm zum Scannen oder unter KDE das dem Gnome-Universum zugeordnete Programm Shotwell einzusetzen. Wesentlich problematischer ist der Umstand, dass Bildverwaltungsprogramme oft nur wenige Jahre gewartet werden. Was nützt es, wenn Sie viel Zeit in die Kategorisierung Ihrer Bilder investieren, das eingesetzte Programm aber plötzlich nicht mehr verfügbar ist? Insofern kann ich Ihnen leider keine Empfehlung für ein bestimmtes Programm geben – Hellsehen zählt nicht zu meinen Stärken.

Weitere Programme

Der Platz reicht hier nicht aus, um auf alle Programme zur Bildverarbeitung einzugehen. Tabelle 9.1 gibt einen Überblick über weitere Programme. Beachten Sie aber, dass bei einem Teil dieser Programme die Weiterentwicklung bereits eingestellt wurde.

Natürlich können Sie zur Verwaltung Ihrer Bilder auch einfach die Datei-Manager Nautilus bzw. Konqueror einsetzen. Diese Programme bieten aber wesentlich weniger Bearbeitungsfunktionen und Darstellungsoptionen.

Wenn Sie im Rahmen der Bildverwaltung mehr tun möchten, als nur den Kontrast zu optimieren oder die Bildgröße zu ändern, sollten Sie unbedingt Gimp kennenlernen. Dieses Open-Source-Programm bietet ähnliche Funktionen wie Adobe Photoshop.

Programm	Website	Beschreibung
eog	*http://projects.gnome.org/eog*	Gnome-Foto-Viewer, wenige Funktionen
F-Spot	*http://f-spot.org*	Gnome-Bildverwaltung
Gthumb	*http://live.gnome.org/gthumb*	Gnome-Bildverwaltung
Gwenview	*http://gwenview.sourceforge.net*	KDE-Foto-Viewer
KPhotoAlbum	*http://www.kphotoalbum.org*	KDE-Bildverwaltung
Mirage	*http://mirageiv.berlios.de*	Gnome-Foto-Viewer

Tabelle 9.1 Weitere Programme zur Verwaltung von Bildern

Wenn Ihnen der Sinn eher nach einer automatisierten Konvertierung oder Weiterverarbeitung vieler Bilder steht, ist schließlich der Abschnitt 17.1 zum Thema Grafik-Konverter lesenswert.

Digitalkameras

Wie kommen die Fotos von der Digitalkamera zum Computer? Fast alle Kameras sehen hierfür einen USB-Anschluss oder eine USB-Docking-Station vor. Uneins sind sich die Kamerahersteller allerdings über das Protokoll zum Datenaustausch:

- **USB-Datenträger:** Am einfachsten ist der Datentransport bei Kameras, die sich wie ein USB-Datenträger verhalten. In diesem Fall behandelt Linux die Kamera wie eine Festplatte mit USB-Anschluss bzw. wie einen USB-Memorystick.
- **PTP-Kameras:** Viele Kameras unterstützen auch das Picture Transfer Protocol (PTP). Dieses Protokoll sieht nicht nur Kommandos zur Übertragung von Bildern vor, sondern auch einfache Steuerungsfunktionen – z. B. um per Computersteuerung ein Foto zu erstellen.
- **Kameras mit herstellerspezifischem Protokoll:** Schließlich gibt es einige alte Kameramodelle aus der Anfangszeit digitaler Fotografie, die nur ein herstellerspezifisches Protokoll unterstützen. Linux unterstützt zwar viele dieser Kameramodelle, aber leider nicht alle.

  Sollte Ihr Kameramodell von Linux nicht erkannt werden, verwenden Sie einfach die SD-Karte zur Übertragung. Falls Ihr Computer keinen Karten-Slot hat, nutzen Sie ein externes USB-Lesegerät.

gphoto2

Zur Kommunikation mit PTP-Kameras bzw. mit Kameras mit einem herstellerspezifischen Protokoll stellt die Bibliothek `libgphoto2` die erforderlichen Funktionen zur Verfügung. Sie können diese Bibliothek direkt durch das Kommando `gphoto2` nutzen. Beispielsweise versucht `gphoto2 --auto-detect`, die angeschlossene Kamera

zu erkennen, und zeigt die entsprechenden Informationen an. `gphoto2 --get-all-thumbnails` überträgt verkleinerte Symbole aller auf der Kamera gespeicherten Bilder in das lokale Verzeichnis. Bemerkenswert ist, dass bei manchen Kameras mit `gphoto2 --capture-image` sogar per Kommando Fotos erstellt werden können, sodass die Kamera wie eine Webcam genutzt oder für Überwachungszwecke eingesetzt werden kann. Weitere Informationen zu `gphoto2` finden Sie auf der folgenden Website:

http://gphoto.sourceforge.net

In der Praxis ist die direkte Anwendung der `gphoto`-Funktionen unüblich. Nahezu alle Bildverarbeitungsprogramme enthalten komfortable Oberflächen zum Bildimport, wobei diese Programme hinter den Kulissen durchweg auf `libgphoto2` zurückgreifen.

9.1 Shotwell

Shotwell hat sich bei den meisten aktuellen Gnome-basierten Distributionen als Bildverwaltungsprogramm durchgesetzt und das früher populäre Programm F-Spot abgelöst. Shotwell bietet vergleichsweise wenige Funktionen; dafür ist es aber einfach zu bedienen und läuft schnell und stabil.

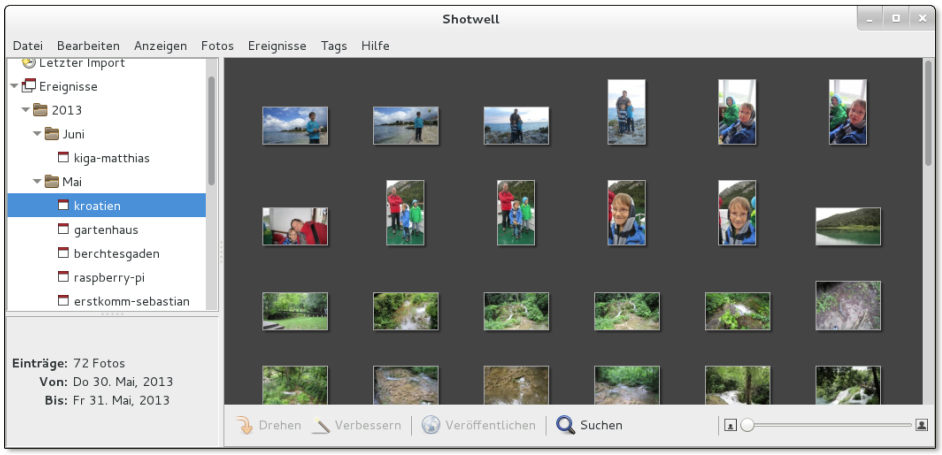


Abbildung 9.1 Bildverwaltung mit Shotwell

Bilder sofort ansehen

Shotwell kann auf zwei Arten verwendet werden: einerseits zum sofortigen Ansehen von Bildern in einem Verzeichnis, andererseits zum Organisieren großer Fotosammlungen. Das erfordert den vorherigen Import der Bilder.

Um Fotos ohne Import anzusehen, klicken Sie im Dateimanager auf ein Foto und führen ÖFFNEN MIT • SHOTWELL aus. Shotwell zeigt dann dieses Foto an und ermöglicht mit zwei Pfeil-Buttons das Vor- und Zurückblättern durch weitere Fotos im

aktuellen Verzeichnis. Auch grundlegende Bildbearbeitungsoperationen können durchgeführt werden, also Bild drehen, zuschneiden, ausrichten etc.

Import

Die Importfunktion erscheint bei vielen Distributionen automatisch, sobald Sie eine Kamera oder deren Speicherkarte mit dem Computer verbinden. Außerdem können Sie mit DATEI • AUS ORDNER IMPORTIEREN bereits Bilder und Filme aus einem Verzeichnis einlesen. Dabei haben Sie die Wahl, ob die Bild- und Videodateien an ihrem bisherigen Ort bleiben sollen oder ob sie in ein von Shotwell verwaltetes Verzeichnis kopiert werden sollen. Fotos können auch per Drag&Drop aus dem Dateimanager in Shotwell importiert werden.

Von F-Spot zu Shotwell

Shotwell kann auch bisher mit F-Spot verwaltete Fotos importieren. Die Bilddateien werden dabei nicht kopiert, sondern bleiben an ihrem bisherigen Ort. Shotwell benötigt zum Import Zugriff auf die F-Spot-Bilddatenbank `.config/f-spot/photos.db`. Leider gehen beim Import viele in F-Spot durchgeführte Bildmanipulationen verloren. Richtig gedrehte Bilder stehen also wieder auf dem Kopf etc. Immerhin bleiben die in F-Spot definierten Tags erhalten.

Ereignisse

Die Bilder werden beim Import automatisch »Ereignissen« zugeordnet, wobei jeder Tag, an dem Fotos entstanden sind, als Ereignis gilt. Ereignisse können mit F2 problemlos umbenannt werden. Um die Fotos mehrerer Tage zu einem Ereignis zu vereinen, markieren Sie die betreffenden Tage in der Monatsübersicht und führen dann das Kontextmenükommando EREIGNISSE ZUSAMMENFÜHREN aus. Leider ist dieser Vorgang bei vielen Bildern recht langsam. Um umgekehrt die Fotos eines Tages mehreren Ereignissen zuzuordnen, markieren Sie mehrere Fotos und führen dann Strg+N aus.

Sie können ein einzelnes Foto per Kontextmenü ZUM SCHLÜSSELFOTO FÜR DIESES EREIGNIS MACHEN. Das Bild wird dann in der Ereignisübersicht angezeigt.

Bilder organisieren

Mit Strg+T statten Sie Bilder mit sogenannten *Tags* aus, also mit Begriffen, nach denen Sie später suchen können. Für jedes Bild dürfen mehrere, nur durch Kommas getrennte Tags angegeben werden.

Mit den Tasten 1 bis 5 bewerten Sie ein Bild mit ein bis fünf Sternen. 0 entfernt die Bewertung, 9 kennzeichnet das Bild als ABGELEHNT. Mit ANZEIGEN • FOTOS FILTERN können Sie anschließend nur solche Bilder anzeigen, die positiv bewertet wurden. Noch mehr Suchmöglichkeiten bietet die Suchleiste, die Sie mit F8 ein- bzw. wieder ausblenden.

Bilder bearbeiten

Shotwell bietet einige simple Bearbeitungsfunktionen an: Die Bilder können in 90-Grad-Schritten gedreht (Strg+R) und beschnitten werden. Außerdem kann der Rote-Augen-Effekt behoben und der Kontrast der Bilder verbessert werden.

Sämtliche Bearbeitungsschritte werden nicht direkt an der Bilddatei durchgeführt, sondern in der Datenbank des Programms gespeichert und bei der Anzeige des Bilds angewendet. Mit dem Kontextmenükommando Zurück zum Original kann jedes veränderte Bild wiederhergestellt werden. Das sichert einerseits die Integrität der Originaldateien, erschwert aber andererseits einen späteren Wechsel auf ein anderes Programm.

Um ein Bild zu löschen, führen Sie Entf oder das Kontextmenükommando In den Müll verschieben aus. Damit wird das Bild innerhalb der Bilddatenbank in einen OpenShot-eigenen Papierkorb gelegt. Erst wenn Sie den Papierkorb explizit leeren, werden die Bilddateien nach einer Rückfrage endgültig gelöscht.

Sonstige Funktionen

Ausgewählte Bilder können mit Tags (Markierungen) versehen, in einer sehr einfachen Diaschau angezeigt, in ein Verzeichnis exportiert oder auf Facebook, Flickr oder Picasa veröffentlicht werden.

Interna

Standardmäßig verteilt Shotwell die importierten Bilder über die Verzeichnisse `Bilder/jahr/monat/tag`. Wenn Sie ein anderes Basisverzeichnis oder eine andere Organisationsstruktur wünschen, finden Sie entsprechende Optionen im Dialog Bearbeiten • Einstellungen.

Außer den Bilddateien speichert Shotwell im verborgenen Verzeichnis `.shotwell` eine Bilddatenbank mit Zusatzinformationen zu allen Bildern. Darüber hinaus befinden sich in diesem Verzeichnis verkleinerte Vorschaubilder zu allen Fotos. Diese Vorschaubilder sind entscheidend für die hohe Darstellungsgeschwindigkeit von Shotwell.

9.2 digiKam

digiKam ist ein sehr vielseitiges KDE-Programm zum Fotoimport von Digitalkameras, zur Verwaltung der Bilder und zur Durchführung einfacher Bearbeitungsschritte. digiKam ist durch ein Plugin-System erweiterbar. Dank derartiger Plugins kann es direkt mit RAW-Dateien umgehen, Farbprofile verwalten, diverse Filter auf Bilder anwenden etc. Wie viele andere KDE-Programme glänzt digiKam durch eine unvergleichliche Funktionsvielfalt; gleichzeitig ist aber die Benutzeroberfläche überladen und die Bedienung unübersichtlich.

Beim ersten Start des Programms durchlaufen Sie die Dialoge des Einrichtungsassistenten. Dort müssen Sie ein Basisverzeichnis für Ihre Bilder konfigurieren. Bei

allen weiteren Optionen können Sie jeweils die Vorgabeeinstellungen übernehmen. Bei Bedarf können Sie mit Einstellungen • digiKam einrichten • Alben sämtliche digiKam-Optionen in einem Dialog einstellen, der 18 Registerkarten umfasst.

Fotoimport

Wenn Linux Ihre Digitalkamera als USB-Speichermedium betrachtet, starten Sie den Import der dort befindlichen Bilder mit Importieren • USB-Speichergeräte. Alle anderen Kameras müssen Sie vor dem ersten Import konfigurieren: In den meisten Fällen ist es ausreichend, im Dialog Importieren • Kameras • Kamera manuell hinzufügen den Button Automatische Erkennung anzuklicken. Die Kamera wird von nun an im Kamera-Menü aufgelistet.

Den Import starten Sie dann mit Importieren • Kamera • Kameraname. In jedem Fall erscheint nun ein Dialog mit einer Vorschau aller Bilder. Der Button Ausgewählte herunterladen führt in einen Dialog zur Auswahl des Zielverzeichnisses. Anschließend werden die markierten Bilder dorthin kopiert.

Um ein bereits vorhandenes Fotoverzeichnis zu importieren, führen Sie Importieren • Ordner hinzufügen aus. Dieses Kommando kann nur verwendet werden, wenn Sie vorher in der Albenansicht ein Album (z. B. `/home/name/Bilder`) auswählen! Die Bilddateien werden beim Import kopiert.

Bildverwaltung

Jedes Verzeichnis innerhalb des Basisverzeichnisses bezeichnet digiKam als *Album*. Alternativ können Sie auch in der Datumsansicht nach den Bildern suchen (siehe Abbildung 9.2). Ein Mausklick auf das gerade aktuelle Bild vergrößert es, ein weiterer Klick führt zurück in die Albenansicht. Auf der rechten Fensterseite können Sie zusätzliche Bildeigenschaften, Kommentare und Stichwörter einblenden bzw. dort ändern. Diese zusätzlichen Daten, die bei der späteren Suche nach Bildern helfen, werden nicht direkt in den Bildern, sondern in der Datei `digikam4.db` im Basisverzeichnis gespeichert.

Bilder richtig drehen

Soweit die Kamera die Orientierung der Bilder in den EXIF-Daten vermerkt, dreht Bild • Automatisches Drehen/Spiegeln alle Bilder im aktuellen Verzeichnis richtig. Zum manuellen Rotieren sind die Tastenkürzel Strg+⇧+← bzw. + → vorgesehen, die bei meinen Tests aber nicht funktionierten. Abhilfe: Führen Sie in digiKam Einstellungen • Kurzbefehle festlegen aus, und geben Sie den Drehkommandos neue Kürzel.

Bilder bearbeiten

In der Ordneransicht können nur ganz elementare Bearbeitungsschritte durchgeführt werden, z. B. das Bild drehen. Weitergehende Operationen stehen zur Verfügung, wenn Sie per Kontextmenü Bearbeiten ausführen. digiKam zeigt das Bild dann in einem neuen Fenster an. Dort können Sie das Bild rahmen, beschriften, Farben und Helligkeit optimieren, weichzeichnen, schärfen, rote Augen korrigieren, die Größe ändern etc. Änderungen werden normalerweise direkt in der Originaldatei

gespeichert. Wenn Sie die nicht verlieren möchten, müssen Sie das veränderte Bild mit DATEI • SPEICHERN UNTER sichern.

Das Menü EXTRAS führt zu diversen Zusatzfunktionen. Zahlreiche digiKam-Funktionen sind als Plugins realisiert (KIPI = *KDE Image Plugin Interface*). Wenn einzelne digiKam-Funktionen bei Ihnen fehlen, stellen Sie sicher, dass die Plugins installiert und im Dialogblatt EINSTELLUNGEN • DIGIKAM EINRICHTEN • KIPI-MODULE auch aktiviert sind. Mit EXTRAS • STAPELVERARBEITUNG Sie können damit alle markierten Bilder gemeinsam konvertieren oder ändern.

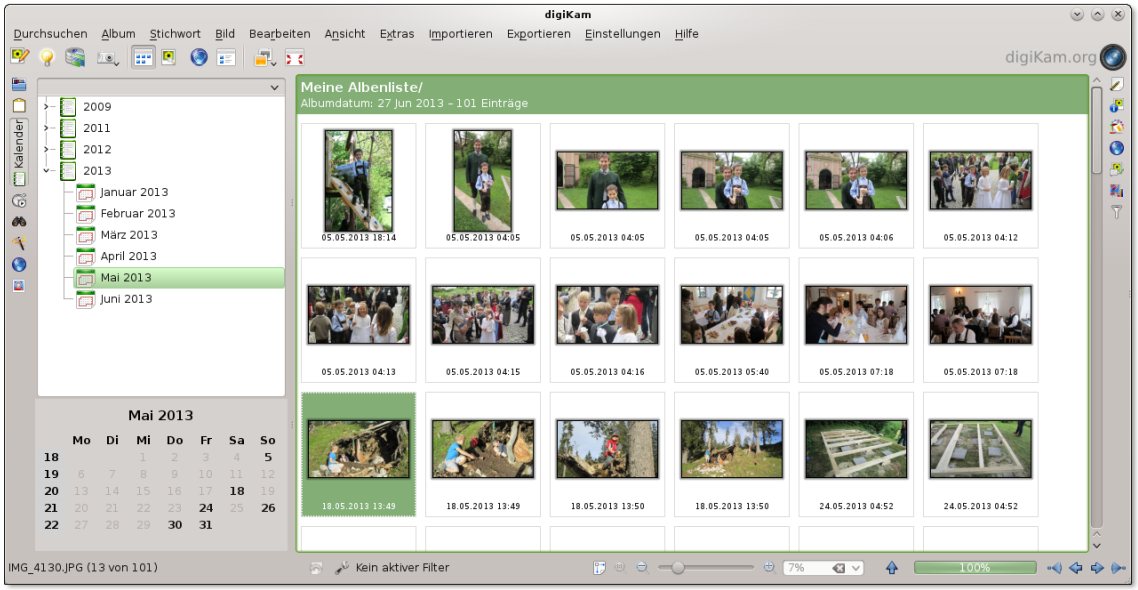


Abbildung 9.2 Bildverwaltung mit digiKam

Bilder ansehen und exportieren

ANSICHT • DIASCHAU • ALLE bzw. AUSWAHL präsentiert das aktuelle Album bzw. die gerade ausgewählten Bilder als Diaschau ohne besondere Effekte. Während die Präsentation aktiv ist, können Sie auch mit dem Mausrad vor- und zurückblättern. Das Zeitintervall für den Bildwechsel sowie einige andere Optionen können Sie mit EINSTELLUNGEN • DIGIKAM EINRICHTEN • DIASCHAU angeben.

Wenn Sie die Diaschau mit Überblendeffekten und Musikuntermalung durchführen möchten, verwenden Sie ANSICHT • DIASCHAU • ERWEITERTE DIASCHAU. In einem Dialog können Sie diverse Einstellungen vornehmen, die allerdings immer für alle Bilder gelten: Sie können also nicht einem bestimmten Bild einen Effekt zuordnen oder je nach Bild unterschiedliche Zeitintervalle für den Bildwechsel einstellen. Beachten Sie, dass die Auswahl der Bildeffekte variiert, je nachdem, ob Sie die Option OPENGL-ÜBERGÄNGE aktivieren oder nicht.

Das Menü EXPORTIEREN enthält ein ganzes Dutzend Kommandos, um die zuvor ausgewählten Bilder auf Facebook, Flickr, Picasa etc. zu exportieren, als HTML-Galerie zu speichern, in eine Flash-Präsentation umzuwandeln oder in ein beliebiges Verzeichnis auf dem lokalen Rechner oder einem Rechner im Netzwerk zu speichern (AUF FREMDRECHNER EXPORTIEREN).

Wenn Sie mehrere zuvor markierte Bilder als E-Mail versenden möchten, führen Sie BILD • BILDER PER E-MAIL VERSENDEN aus. Dabei können Sie zwischen verschiedenen E-Mail-Clients auswählen und wahlweise die maximale E-Mail-Größe oder die gewünschte Bildgröße (z. B. maximal 800 Pixel) vorgeben. digiKam skaliert die Bilder dann entsprechend. Den Exportdialog dürfen Sie erst schließen, nachdem Sie die E-Mail versandt haben – andernfalls findet das E-Mail-Programm die temporären Bilddateien nicht mehr!

9.3 RawTherapee, Darktable und Luminance (RAW- und HDR-Bilder)

Die meisten Digitalkameras speichern Bilder im JPEG-Format, das einen guten Kompromiss zwischen Bildgröße und Qualität bietet. Bessere Kameras bieten darüber hinaus die Möglichkeit, Bilder im sogenannten RAW-Format zu speichern. Dabei handelt es sich um herstellerspezifische Formate, die sicherstellen, dass keinerlei Bildinformationen verloren gehen. Allerdings sind RAW-Dateien zumeist sehr groß und können nur mit speziellen Programmen betrachtet werden. Unter Linux sind hierfür die Programme RawTherapee und Darktable geeignet. Diese Programme richten sich explizit an professionelle Fotografen, die das Optimum aus RAW-Fotodateien herauskitzeln möchten.

RawTherapee

Mit RawTherapee (siehe Abbildung 9.3) können Sie RAW-Bilddateien der meisten gängigen Kameras laden. Anschließend haben Sie unzählige Möglichkeiten, das Bild durch Filter und andere Funktionen zu optimieren und schließlich in einem anderen Bildformat zu speichern.

Darktable

Darktable (siehe Abbildung 9.4) versucht, den ganzen »Fotoworkflow« unter Linux abzubilden, vom Import der RAW-Daten bis hin zu den nachfolgenden Bildbearbeitungsfunktionen. Die Funktionen zur Verarbeitung der RAW-Daten sind ähnlich wie bei RawTherapee; darüber hinaus bietet Darktable auf dem sogenannten Leuchttisch aber auch Funktionen, um Bilder zu bewerten, mit Tags zu versehen etc. Die Bedienung von Darktable orientiert sich in Grundzügen an Adobe Photoshop Lightroom.

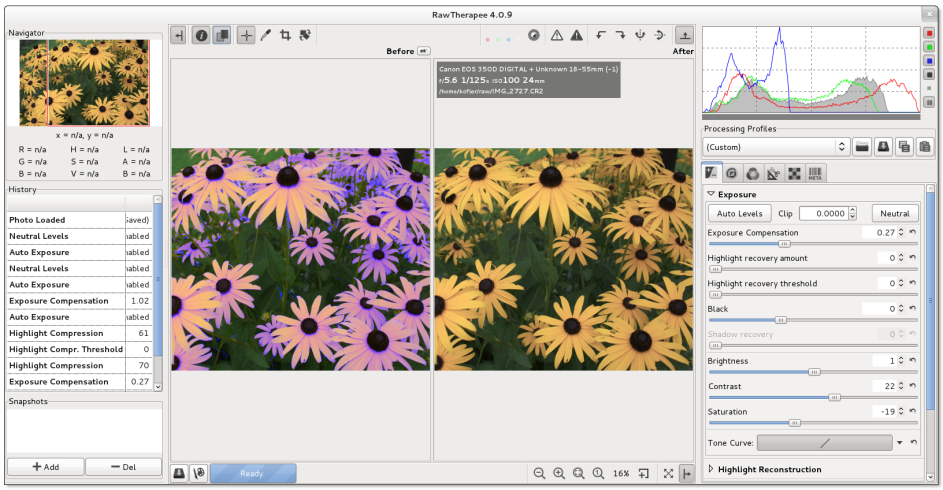


Abbildung 9.3 RawTherapee

Abbildung 9.4 Darktable

Auf Kommandoebene können Sie RAW-Dateien mit `dcraw` in andere Bildformate umwandeln. Wenn Sie mit Gimp arbeiten (siehe den folgenden Abschnitt), ermöglicht das Zusatzpaket `gimp-dcraw` den direkten Import von RAW-Dateien, ohne aber so viele Einstellmöglichkeiten wie RawTherapee oder Darktable zu bieten. Weitere Informationen zu `dcraw` finden Sie unter: dcraw

http://www.cybercom.net/~dcoffin/dcraw

Luminance HDR

HDR steht für *High Dynamic Range* und ist eine Technik, um auch bei extremen Helligkeitsunterschieden sowohl die dunklen als auch die hellen Teile des Bilds in guter Qualität darzustellen. Zur Erstellung von HDR-Bildern werden üblicherweise zwei Fotos mit unterschiedlicher Belichtung zusammengefügt. Unter Linux hilft dabei das Programm Luminance HDR. Einige Distributionen (darunter Ubuntu) bieten das Programm in den Standardpaketquellen an. Sollte das bei Ihrer Distribution nicht der Fall sein, können Sie das Programm hier herunterladen:

http://qtpfsgui.sourceforge.net

9.4 Gimp (Bildbearbeitung)

Gimp ist das Open-Source-Gegenstück zu Adobe Photoshop. Auch wenn Gimp nicht alle Funktionen von Photoshop aufweisen kann, so ist es doch ein unglaublich vielseitiges Werkzeug zur Bildbearbeitung. Sie können damit Fotos retuschieren, Bilder für Ihre Website optimieren, Plakate gestalten etc.

Leider ist die Bedienung von Gimp alles andere als einfach. Das Programm ist deswegen in erster Linie als Werkzeug für Bildverarbeitungsprofis geeignet; Gelegenheitsanwender werden mit ihm nicht glücklich werden. In diesem Abschnitt stelle ich lediglich einige Grundfunktionen des Programms vor.

Gimp 2.8

Aktuelle Linux-Distributionen enthalten die neue Gimp-Version 2.8. Deren größte Neuerung ist der Einzelfenster-Modus (siehe Abbildung 9.5), den Sie im FENSTER-Menü aktivieren müssen. Stark geändert hat sich auch das Speichern von Bildern: Mit DATEI • SPEICHERN bzw. Strg+S können Sie nur noch im Gimp-eigenen XCF-Format speichern. Um ein Bild in einem anderen Format zu speichern, müssen Sie DATEI • EXPORTIEREN bzw. Strg+E ausführen. Wenn Sie das Export-Format ändern möchten, führen Sie ⇧+Strg+E aus.

Bilder laden und bearbeiten

DATEI • ÖFFNEN führt zu einem Dateiauswahldialog samt Bildvorschau. Nach dem Öffnen wird die Bilddatei in einem neuen Bildfenster angezeigt. Wenn das Bildfenster leer war, ersetzt das neue Bildfenster das bisherige.

Solange das Bildfenster aktiv ist, können Sie mit + in das Bild hineinzoomen und mit - hinaus. 1 setzt den Zoomfaktor auf 1:1, das heißt, jedes Pixel des Bilds wird auf einem Bildschirmpixel abgebildet.

DATEI • SPEICHERN speichert die Bilddatei im XCF-Format (Kennung `*.xcf`). Der Vorteil dieses Formats besteht darin, dass nicht nur das Bild an sich gespeichert wird, sondern auch dessen Komposition sowie diverse Kontextinformationen und Gimp-Einstellungen. Wenn Sie dem Bild beispielsweise Text oder Ausschnitte anderer Bilder hinzugefügt haben, setzt sich das Bild aus mehreren Ebenen zusammen. Nur

im XCF-Format werden alle Ebenen gespeichert. Das XCF-Format hat somit den Vorteil, dass es viel bessere Voraussetzungen für eine spätere Weiterverarbeitung des Bilds bietet. Wenn Sie statt der Dateikennung `*.xcf` die Kennungen `*.xcf.gz` oder `*.xcf.bz2` verwenden, wird die Bilddatei zusätzlich komprimiert. Die Datei wird dadurch deutlich kleiner.

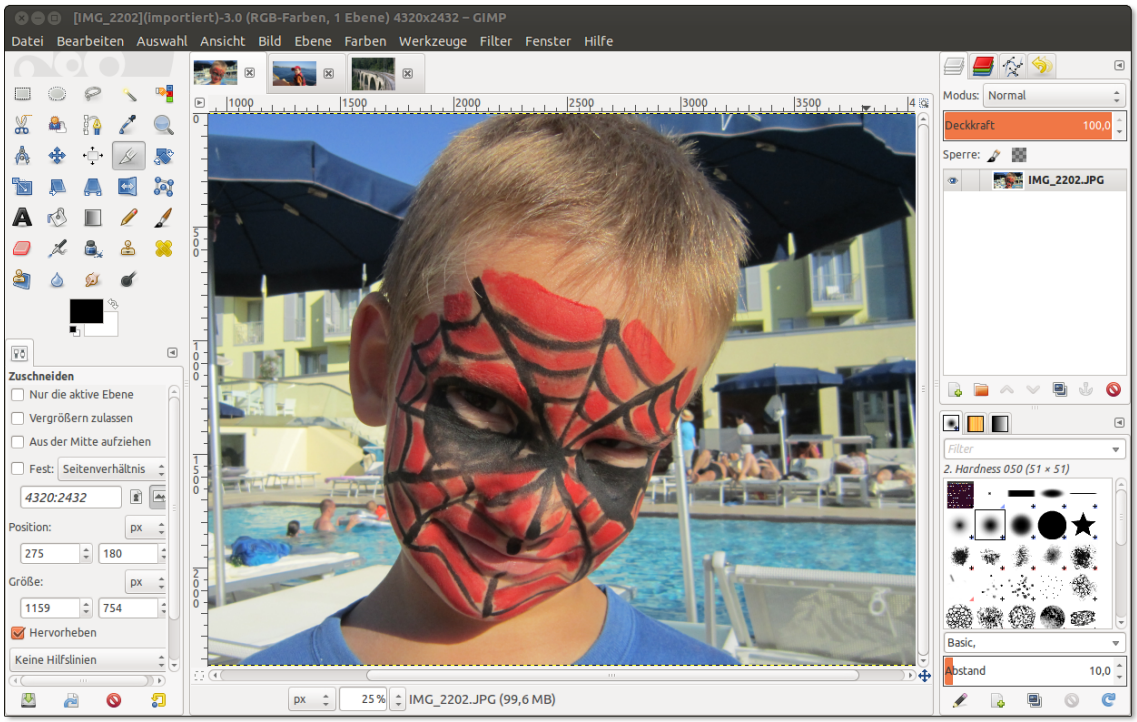


Abbildung 9.5 Gimp 2.8 im Einzelfenster-Modus

Bilder drehen, skalieren und ausschneiden

Mit BILD • TRANSFORMATIONEN drehen Sie das Bild um 90 Grad nach rechts oder links, stellen es auf den Kopf oder spiegeln es horizontal oder vertikal.

Mit BILD • BILD SKALIEREN gelangen Sie in den Skalierungsdialog. Dort geben Sie einfach die gewünschte Bildgröße in Pixel an. Alternativ kann die Größenangabe auch in Prozent erfolgen, z. B. um die Breite und Höhe des Bilds auf 25 Prozent seiner Größe zu verringern.

Um das Bild auf einen Ausschnitt zu verkleinern, aktivieren Sie in der Toolbox das Zuschneidewerkzeug (WERKZEUGE • TRANSFORMATIONEN • ZUSCHNEIDEN). Anschließend können Sie mit der Maus den gewünschten Bildausschnitt markieren. Ein Mausklick in den markierten Bereich schneidet das Bild aus.

Helligkeit, Kontrast und Farben ändern

Mit WERKZEUGE • FARBEN • HELLIGKEIT-KONTRAST gelangen Sie in einen einfachen Dialog, in dem Sie die Helligkeit und den Kontrast mit zwei Schiebereglern verändern können.

Fotos nutzen selten den gesamten Farbraum. Der hellste Punkt im Bild, der oft weiß sein sollte, ist meist nur ein flauer Grauton. Mit FARBEN • WERTE können Sie diesen Mangel beheben. Der WERTE-Dialog bietet eine Menge Bearbeitungsmöglichkeiten, von denen hier nur die wichtigsten erwähnt werden:

- Mit dem Button AUTOMATISCH führen Sie einen automatischen Weißabgleich durch. Das Ergebnis ist zwar mathematisch optimal, liefert aber oft eine zu extreme Helligkeits- bzw. Farbverteilung.
- Mit den drei Pipetten-Buttons markieren Sie jeweils einen Punkt im Bild, der schwarz, in einem mittleren Grau erscheinen bzw. weiß sein sollte.
- Im Dialogbereich QUELLWERTE können Sie die drei Dreiecke verschieben, um so den Weiß-, Grau- und Schwarzpunkt zu markieren. Das darüber angezeigte Histogramm gibt an, wie viele Punkte des Bilds eine bestimmte Helligkeit haben. Üblicherweise wird der Schwarzpunkt an den Beginn und der Weißpunkt an das Ende des Histogramms verschoben. Der Graupunkt sollte in der Mitte zwischen Weiß- und Schwarzpunkt liegen. Wenn Sie den Graupunkt verschieben, wird das Bild blasser (links) bzw. farbintensiver (rechts).

Bild schärfen oder weichzeichnen

Mit den folgenden Operationen können Sie die Wahrnehmungsqualität eines Bilds spürbar verbessern. Beachten Sie, dass alle hier beschriebenen Filter immer nur für den gerade markierten Bildbereich gelten. Führen Sie gegebenenfalls vorher Strg+A aus, um das gesamte Bild zu markieren!

- **Schärfen:** FILTER • VERBESSERN • SCHÄRFEN versucht das Bild zu schärfen, indem es Helligkeitsveränderungen betont. Relativ gut funktioniert das bei Nachtaufnahmen. Eine mögliche Alternative ist das Kommando FILTER • VERBESSERN • NL FILTER mit der Option KANTENVERSTÄRKUNG. Auch der Filter VERBESSERN • UNSCHARF MASKIEREN ist einen Versuch wert.
- **Weichzeichnen:** Die gegenteilige Wirkung haben die diversen Kommandos unter FILTER • WEICHZEICHNEN. Diese Filter mindern Helligkeitsübergänge. Das Bild wirkt dadurch weicher, aber auch etwas unschärfer. Relativ starke Effekte erzielen Sie mit dem GAUSSSCHEN WEICHZEICHNER.
- **Rauschen eliminieren:** Geradezu spektakuläre Verbesserungen bei verrauschten Bildern (auch bei schlecht eingescannten Fotos) erzielen Sie mit FILTER • WEICHZEICHNEN • SELEKTIVER GAUSSSCHER WEICHZEICHNER. Probieren Sie es beispielsweise mit einem Radius von 4 Pixeln und einem maximalen Deltawert von 10. Das bedeutet, dass der Weichzeichner nur dann zum Einsatz kommt, wenn der Farbunterschied nahe beieinander liegender Pixel gering ist (kleiner gleich 10).

Bei starken Farbunterschieden – z. B. entlang einer Hauskante – bleibt der Weichzeichner dagegen unwirksam, weswegen die Schärfe des Bilds weniger leidet als bei anderen Weichzeichnern.

Rote Augen entfernen

Der Rote-Augen-Effekt entsteht vor allem bei Porträtaufnahmen, wenn der Blitz nahe am Objekt ist: Die Pupillen sind weit geöffnet. Deswegen wird das Blitzlicht von der durchbluteten Netzhaut rot reflektiert.

Gimp enthält ein eigenes Werkzeug zur Eliminierung des Rote-Augen-Effekts. Bevor Sie es anwenden können, müssen Sie den roten Bereich der Augen markieren. Dazu verwenden Sie das Werkzeug ELLIPTISCHE AUSWAHL. Beim zweiten Auge drücken Sie zusätzlich Shift, um die bereits vorhandene Markierung zu ergänzen. Markieren Sie lieber ein bisschen zu viel als ein bisschen zu wenig!

FILTER • VERBESSERN • ROTE AUGEN ENTFERNEN ersetzt nun das Rot der Augen durch einen Grauton. Der Lichtreflex im Auge bleibt dabei erhalten. Den Schwellenwert für den Rot-Ton, ab dem die Farbe verändert wird, müssen Sie nur in Ausnahmefällen verändern.

9.5 Hugin (Panoramas)

Das Programm Hugin hilft dabei, mehrere einzelne Bilder zu einem großen Panoramabild zusammenzusetzen. Dieser Abschnitt gibt nur eine ganz kurze Einführung in das Programm. Wenn Sie mit Hugin arbeiten, werden Sie rasch feststellen, dass es unzählige weitere Optionen und Einstellmöglichkeiten gibt, deren korrekte Anwendung aber Kenntnisse der zugrunde liegenden optischen Begriffe und Verfahren voraussetzt – und die kann ich hier nicht vermitteln. Lesenswert sind auf jeden Fall die Tutorials auf der Hugin-Webseite sowie der folgende Bericht auf *http://lwn.net*, der unter anderem auf die Anwendung von Hugin zur Bearbeitung von Gruppenfotos eingeht:

http://hugin.sourceforge.net/tutorials
http://lwn.net/Articles/351053

Am einfachsten ist es, den Hugin-Assistenten zu nutzen und sich auf die Automatismen von Hugin zu verlassen. Im ersten Schritt laden Sie alle Bilder Ihres Panoramas. Mit AUSRICHTEN starten Sie einen Analyseprozess, der je nach Anzahl und Größe der Bilder und der CPU-Geschwindigkeit mehrere Minuten in Anspruch nimmt. Hugin versucht, übereinstimmende Merkmale auf den Bildern zu finden, anhand derer es die Bilder aneinanderfügen kann.

Sobald dieser Prozess abgeschlossen ist, erscheint ein Vorschaufenster (siehe Abbildung 9.6). Im Dialogblatt PROJEKTION können Sie das Projektionsverfahren ändern,

wobei Sie zumeist mit ZYLINDRISCH oder SPHÄRISCH die besten Ergebnisse erzielen. Im Dialogblatt BESCHNITT wird ein Auswahlrechteck über dem Bild eingeblendet. Sie können nun dessen Größe und Position einstellen. Das Reckteck gibt die Ausmaße des endgültigen Panoramabilds an. Wenn Sie mit dem Ergebnis zufrieden sind, schließen Sie das Vorschaufenster und starten im Hauptfenster die Panoramaerstellung. Die resultierende Datei wird im TIFF-Format gespeichert.

Nicht immer ist das Ergebnis so gut wie in Abbildung 9.7. Sie können nun versuchen, in den vielen Dialogblättern von Hugin manuell diverse Parameter zur Panoramaerstellung einzustellen. Nach meinen Erfahrungen führt das aber nur dann zum Erfolg, wenn Sie nicht auf gut Glück probieren, sondern ein fundiertes Wissen darüber haben, wie Hugin funktioniert.

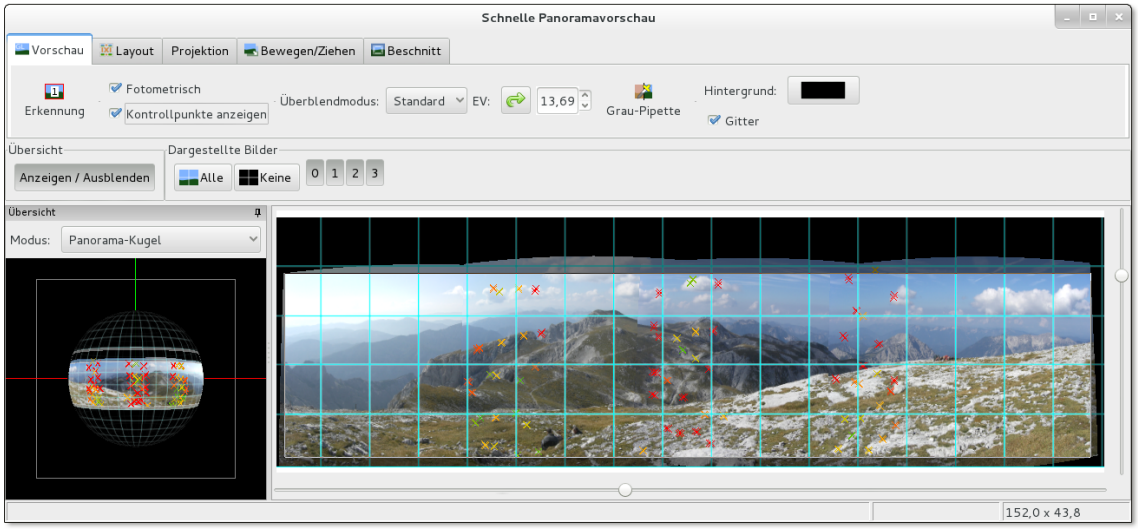


Abbildung 9.6 Panoramas mit Hugin zusammensetzen

Abbildung 9.7 Panoramaaufnahme im Hochschwabmassiv (Steiermark)

9.6 Bilder scannen

Seit Digitalkameras allgegenwärtig sind, hat die Bedeutung von Scannern abgenommen. Dennoch ist es bisweilen erforderlich, den Scanner aus dem Keller zu holen, um ein Bild in guter Qualität einzuscannen. Gängige Scanner werden an die USB-Schnittstelle angeschlossen. Grundsätzlich kommt Linux mit den meisten Scannern zurecht, es gibt aber natürlich auch Ausnahmen. Erkundigen Sie sich unbedingt vor dem Scanner-Kauf, ob das Gerät Linux-kompatibel ist:

http://www.sane-project.org/sane-supported-devices.html

SANE

Konfiguration

Für den Scanner-Zugriff ist das Programmpaket SANE verantwortlich (*Scanner Access Now Easy*). Zumeist wird Ihr Scanner sofort beim Anstecken erkannt, d. h., Scan-Programme wie XSane, Simple Scan oder Skanlite funktionieren auf Anhieb. Ist das nicht der Fall, müssen Sie SANE zuerst konfigurieren. Bei SUSE ist dies zwingend erforderlich; das YaST-Modul HARDWARE • SCANNER hilft Ihnen dabei.

Wenn ein derartiges Konfigurationsprogramm fehlt, müssen Sie die Konfigurationsdateien im Verzeichnis `/etc/sane.d/*` selbst modifizieren. Dieses Verzeichnis enthält für jeden Gerätehersteller eine Datei, in der sich normalerweise nur wenige Einträge befinden. Die folgenden drei Zeilen zeigen ein Beispiel für den Inhalt von `epson.conf`. Sie sind ausreichend, um alle unterstützten USB- und SCSI-Scanner von Epson zu erkennen.

```
# /etc/sane.d/epson.conf
usb
scsi EPSON
scsi "EPSON SC"
```

Probleme können ganz neue Geräte bereiten, deren ID-Nummern sich noch nicht in der USB-Datenbank der Linux-Hardware-Datenbank befinden. In solchen Fällen müssen Sie mit `lsusb` die ID-Nummer des Scanners herausfinden und wie im folgenden Beispiel eine zusätzliche Zeile in die betreffende Konfigurationsdatei einbauen:

```
user$  lsusb
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 002: ID  04b8:010b Seiko Epson Corp. Perfection 1240
...
# Ergänzung in /etc/sane.d/epson.conf
usb 0x04b8 0x010b
```

Sofern das Paket `sane-utils` installiert ist, sollten die Kommandos `sane-find-scanner` und `scanimage -L` den Scanner jetzt erkennen:

```
user$  sane-find-scanner
found USB scanner (vendor=0x04b8 [EPSON], product=0x010b [Perfection1240])
  at libusb:006:002
found USB scanner (vendor=0x0bda, product=0x8187) at libusb:001:002
...
```

SANE berücksichtigt nur die Herstellerdateien, die in `/etc/sane.d/dll.conf` angegeben sind. Wenn SANE Ihren Scanner nicht erkennt und Sie sich vergewissert haben, dass SANE diesen Scanner prinzipiell unterstützt, sollten Sie einen Blick in `dll.conf` werfen und sicherstellen, dass der Herstellername Ihres Scanners dort nicht auskommentiert ist.

Scannen mit SANE

Normalerweise werden Sie zum Scannen nicht direkt mit der SANE-Bibliothek kommunizieren, sondern eine der verfügbaren Benutzeroberflächen einsetzen. Am populärsten sind die in den folgenden Abschnitten vorgestellten Programme XSane, Simple Scan und Skanlite. Wenn Sie das Scannen durch ein Script automatisieren möchten, finden Sie im Paket `sane-utils` das Kommando `scanimage`. Wenn Sie mehrere Seiten effizient scannen und dann in ein PDF-Dokument umwandeln möchten, sollten Sie einen Blick auf `gscan2pdf` werfen.

XSane

XSane ist ein funktionsreiches Programm zum Scannen von Bildern (siehe Abbildung 9.8). Bevor Sie das erste Bild scannen, ändern Sie den Modus von SCHWARZWEISS in GRAUSTUFEN oder FARBE und wählen die gewünschte Auflösung. Standardmäßig verwendet XSane nur 72 DPI, also eine sehr grobe Auflösung.

Mit dem Button VORSCHAUSCAN im VORSCHAU-Fenster führen Sie einen ersten Scan durch. Mit dem Button SICHTBAREN BEREICH AUSWÄHLEN schränken Sie den Scanbereich auf die Größe Ihres Motivs ein. Wenn Sie gleich beim Scannen einen Weißabgleich durchführen möchten, markieren Sie mit den Pipetten WÄHLE WEISSEN PUNKT und WÄHLE SCHWARZEN PUNKT jeweils einen Punkt im Vorschaubild, der weiß bzw. schwarz ist. Scan-Profis können im Hauptfenster und auf Basis des Histogramms (FENSTER • ZEIGE HISTOGRAMM) weitere Korrektureinstellungen vornehmen.

Mit SCANNEN im Hauptfenster führen Sie den eigentlichen Scan in voller Auflösung durch. XSane zeigt das Scan-Ergebnis in einem neuen Fenster an. Dort können Sie das Bild drehen, weichzeichnen und skalieren. FILTER • ENTFLECKEN versucht, Scan-Fehler bzw. Staub aus dem Bild zu entfernen. Bei großen Scans dauert dieser Prozess relativ lange, führt nach meinen Erfahrungen aber nur selten zu einer merklichen Bildverbesserung. Zuletzt speichern Sie Ihren Scan mit DATEI • SPEICHERN.

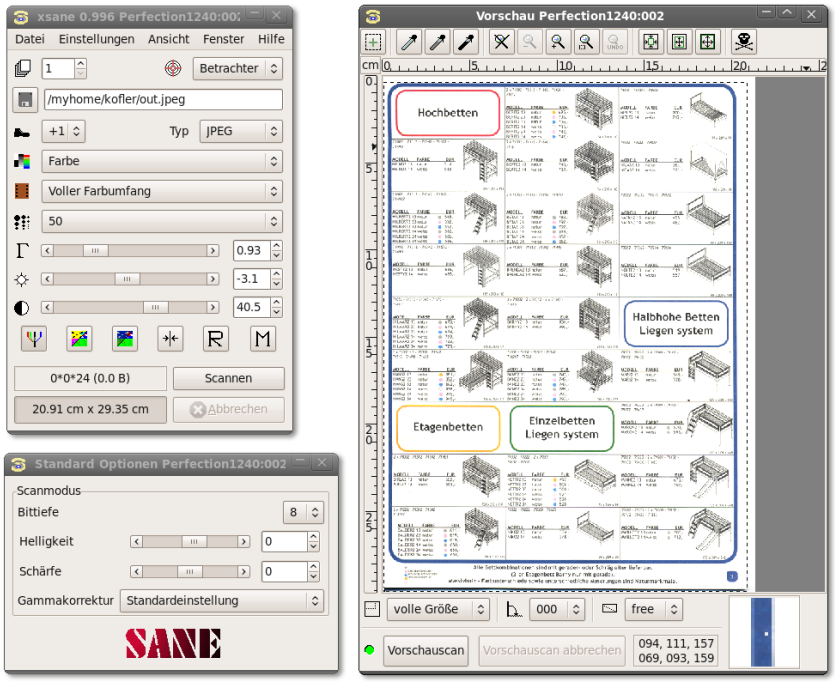


Abbildung 9.8 Scannen mit XSane

Scans optimieren

Es ist eine eigene Kunst, qualitativ hochwertige Scans zu erstellen. Noch schwieriger ist es, Scans in einer guten Qualität wieder auszudrucken. Meistens muss das eingescannte Bild dazu vorher mit einem Bildverarbeitungsprogramm wie Gimp optimiert werden. Wenn Sie Probleme mit Moiré-Mustern haben, versuchen Sie es einmal mit den Filtern WEICHZEICHNEN • GAUSSSCHER WEICHZEICHNER oder VERBESSERN • ENTFLACKERN!

Simple Scan und Skanlite

Simple Scan

Wesentlich einfacher zu bedienen als XSane ist das Gnome-Programm Simple Scan. Mit dem Button SCANNEN lesen Sie das gesamte Bild ein. Wenn nötig, können Sie das eingescannte Bild anschließend drehen und zuschneiden. ZUSCHNEIDEN markiert den Bereich des Bildes, den Sie anschließend speichern möchten. SPEICHERN öffnet schließlich einen Dialog, um das Bild zu speichern.

Standardmäßig scannt Simple Scan in einer Auflösung von ca. 300 DPI und in Farbe. Mit DOKUMENT • SCAN • TEXT können Sie die Auflösung auf 150 DPI reduzieren. DOKUMENT • EINSTELLUNGEN führt in einen einfachen Konfigurationsdialog, in dem Sie die DPI-Einstellungen und die Seitengröße verändern können.

Skanlite Das KDE-Gegenstück zu Simple Scan heißt Skanlite. Die eingescannten Bilder werden in einem eigenen Fenster angezeigt und können dann unter einem beliebigen Namen in den Formaten PNG, JPEG oder BMP gespeichert werden.

9.7 Screenshots erstellen

Ein Screenshot ist ein Abbild des aktuellen Bildschirm- oder Fensterinhalts in einer Grafikdatei. Die folgenden Sätze beschreiben ganz kurz einige Möglichkeiten, solche Screenshots zu erstellen.

Gnome Bei Gnome ist das Programm `gnome-panel-screenshot` direkt in den Desktop integriert. Wie unter Windows erstellt Druck einen Screenshot des gesamten Bildschirms und Alt+Druck eine Abbildung des gerade aktiven Fensters. Anschließend wird das Programmfenster sichtbar und bietet die Möglichkeit, die Abbildung zu speichern. Als einziges Format ist PNG vorgesehen. Das Tastenkürzel zum Erzeugen von Screenshots kann im Modul TASTATUR • TASTATURKÜRZEL der Systemeinstellungen eingestellt werden.

KDE Um unter KDE Bildschirmabbildungen zu erstellen, starten Sie das Programm `ksnapshot` und stellen den gewünschten Aufnahmemodus ein (VOLLBILD, FENSTER oder BEREICH). Mit dem Button NEUES BILDSCHIRMFOTO erstellen Sie den Screenshot. Beim Speichern wird je nach Dateikennung automatisch das entsprechende Format verwendet.

Gimp Auch mit dem Bildverarbeitungsprogramm Gimp können Sie mit DATEI • ERSTELLEN • SCREENSHOT eine Bildschirmabbildung erstellen. Das ist besonders dann praktisch, wenn Sie das Bild anschließend ohnedies mit Gimp weiterbearbeiten möchten.

Shutter Wenn Sie viele Screenshots erstellen, werden Sie vermutlich Shutter mögen: Dieses Programm bietet unzählige Zusatzfunktionen, um den gewünschten Bildausschnitt auszuwählen, das aufgenommene Bild mit Wasserzeichen zu versehen etc.

http://shutter-project.org

Kapitel 10
Audio und Video

Dieses Kapitel erklärt – zumindest so weit, wie es der Gesetzgeber zulässt –, wie Sie unter Linux Audio-Dateien anhören, CDs auslesen (rippen), MP3-Tags einstellen, Video-DVDs und -Dateien abspielen, Video-Dateien recodieren und Screencasts aufnehmen. Dabei setze ich voraus, dass das Audio- und Video-System Ihrer Distribution grundsätzlich funktioniert. Im Detail gehe ich auf die folgenden Programme ein:

- **Audio-Player:** Audacious, Amarok, Banshee, Musique, Rhythmbox, Spotify
- **Multimedia-Player:** Dragon Player, Kaffeine, MPlayer, Totem, VLC, xine
- **MP3- und Audio-Tools:** Audacity, EasyTAG, Sound Juicer
- **DVD-Tools:** DVD95, HandBrake, K9Copy, OGMrip
- **Screencasts:** Kazam

Zum Thema Multimedia ließe sich natürlich noch viel mehr schreiben, durchaus auch ein ganzes Buch! So viel Platz ist hier aber nicht. Der Grundlagenabschnitt, der dieses Kapitel einleitet, gibt Ihnen jedoch zumindest einen Überblick über eine Menge weiterer Multimedia-Programme, die Ihnen unter Linux zur Verfügung stehen.

10.1 Multimedia-Grundlagen

Encoder und Decoder

Encoder

Encoder wandeln unkomprimierte Audio- oder Video-Daten in ein komprimiertes Format um (z. B. MP3, Ogg oder MPEG-4). Die Aufgabe des Encoders ist es, die Daten einerseits möglichst stark zu komprimieren, andererseits aber für geringe Qualitätsverluste zu sorgen. Das ist ein rechenintensiver und daher verhältnismäßig langsamer Vorgang.

Decoder

Decoder sind für die umgekehrte Richtung zuständig, also für die Umwandlung der komprimierten Daten in ein Format, das an Soundkarten bzw. die Grafikkarte weitergegeben werden kann. Jeder Audio- oder Video-Player muss daher auf Decoder für

das jeweilige Format zurückgreifen. Decoder benötigen Sie aber auch, wenn Sie komprimierte Dateien in ein unkomprimiertes Format zurückverwandeln möchten (siehe auch Abschnitt 17.2). Das ist zweckmäßig, wenn Sie eine herkömmliche Audio-CD erzeugen möchten – denn dazu benötigen Sie unkomprimierte WAV-Dateien.

Manchmal besteht auch der Wunsch, Audio- oder Video-Dateien von einem Format in ein anderes umzuwandeln oder stärker zu komprimieren. Dieser Vorgang wird üblicherweise als *Recodieren* (Recoding) bezeichnet.

Codecs

Das dem Encoder/Decoder zugrunde liegende Verfahren wird als Codec bezeichnet. Umgangssprachlich meint Codec aber zumeist die Bibliothek bzw. das Modul/Plugin zur (De-)Codierung eines bestimmten Audio/Video-Formats.

Es existieren zahllose Codecs, wobei für Windows und Mac OS X der Decoder-Teil zumeist kostenlos verfügbar ist. Codec-Entwickler versuchen damit einen möglichst hohen Marktanteil ihres Formats zu erreichen. Etwas schwieriger ist die Situation unter Linux: Im Rahmen der Projekte FFmpeg und avconv gibt es zu vielen populären Codecs Open-Source-Implementierungen für den Decoder und zumeist auch für den Encoder. Allerdings ist der rechtliche Status dieser Programme bzw. Bibliotheken teilweise zweifelhaft, weil viele Codecs durch Patente und Lizenzen geschützt sind. Mangels besserer Alternativen greifen dennoch die meisten Audio- und Video-Player auf die Bibliotheken dieser Projekte zurück. Dies gilt z. B. für MPlayer, VLC, xine sowie für alle Programme, die auf GStreamer basieren.

Die andere Variante besteht darin, die für Windows gedachten Codecs unter Linux einzusetzen. Dazu sind viele der für Linux verfügbaren Audio- bzw. Video-Player in der Lage. Eine Zwischenschicht macht die für Windows gedachten Funktionen auch für Linux nutzbar. Allerdings kommt diese Variante nur für Linux-Rechner mit x86-kompatiblen Prozessoren infrage. Die Codecs sind üblicherweise in Paketen gesammelt, die je nach Distribution z. B. `w32codecs`, `w64codecs` oder `win32codecs` heißen. Aber natürlich gibt es auch hier rechtliche Bedenken: Obwohl die Codecs für Windows kostenlos verfügbar sind, ist eine freie Weitergabe bzw. die Nutzung unter Linux zumeist nicht vorgesehen.

Aufgrund der unklaren rechtlichen Situation, die auch von der nationalen Gesetzgebung abhängt, sind im Standardlieferumfang der meisten Linux-Distributionen nur wenige Codecs enthalten. Bei vielen Distributionen ist anfänglich nicht einmal eine MP3-Wiedergabe möglich. Abhilfe schaffen in der Regel inoffizielle Paketquellen (siehe Abschnitt 10.1). Ein anderer Ausweg aus dem rechtlichen Dilemma sind offiziell lizenzierte Codecs, die die Firma Fluendo zum kostenpflichtigen Download anbietet. Die Pakete sind allerdings nur für das GStreamer-Audio-System geeignet und damit inkompatibel zu vielen in diesem Kapitel vorgestellten Programmen.

http://www.fluendo.com

Streaming

Damit Sie live via Internet Radio hören oder fernsehen können, stellen viele Radio- und TV-Sender einen kontinuierlichen Datenstrom zur Verfügung. Dadurch kann die Wiedergabe sofort nach dem Start der Übertragung beginnen. Ein herkömmlicher Download ist nicht vorgesehen, oft auch aus Lizenzgründen. Manche Audio- und Video-Player bieten aber die Möglichkeit, den gerade abgespielten Datenstrom mitzuschneiden, also in eine Datei zu übertragen.

YouTube, der zurzeit sicherlich populärste Video-Anbieter, bietet die Videos wahlweise in Form von Flash-Dateien oder verpackt in HTML5-Seiten an. Das Abspielen von YouTube-Videos setzt also entweder einen Webbrowser mit Flash-Plugin voraus (siehe Abschnitt 8.2) oder einen HTML5-kompatiblen Browser samt der erforderlichen Codecs (siehe Abschnitt 8.1).

Wenn Sie selbst Streaming anbieten möchten, z. B. um diverse elektronische Geräte in Ihrem Haushalt mit Audio- oder Video-Streams zu versorgen, können Sie dazu unter anderen `ffserver` (Teil des FFmpeg-Projekts), Icecast (nur Audio), SHOUTcast oder VLC einsetzen.

Verschlüsselung, CSS, DRM

CSS

Nach der massenhaften Verbreitung von MP3-Dateien durch diverse Tauschbörsen wollte die Multimedia-Industrie ein vergleichbares Desaster im Video-Bereich vermeiden. Deswegen sind nahezu alle Video-DVDs durch das CSS (Content Scrambling System) verschlüsselt. Der dadurch erreichte Schutz hat sich freilich als gering erwiesen. Die Verschlüsselung ist ziemlich primitiv und wurde rasch geknackt.

Weit mehr Mühe als mit dem Verschlüsselungsalgorithmus hat sich die Medienindustrie gegeben, um jegliche Open-Source-Techniken zur Entschlüsselung zu kriminalisieren. Aus diesem Grund ist der Einsatz einer Entschlüsselungsbibliothek in vielen Ländern verboten.

In Deutschland ist es aufgrund des Urheberrechtsgesetzes sogar verboten, die Installation einer Bibliothek zur CSS-Entschlüsselung zu beschreiben. Auch wenn es im Internet unzählige Websites mit entsprechenden Anleitungen gibt, darf ich diese Informationen hier weder wiedergeben noch einen entsprechenden Link nennen. Die Grenzen der Pressefreiheit sind enger, als man denkt.

Damit Sie mich richtig verstehen: Es geht hier nicht um illegales Kopieren! Ich darf Ihnen nicht einmal erklären, wie Sie Ihre gerade in einem Geschäft erworbene DVD unter Linux ansehen können – etwas, was unter Windows eine Selbstverständlichkeit ist.

Sie sehen schon: Dem Video-Genuss unter Linux stehen weniger technische als vielmehr rechtliche Probleme im Weg. Den meisten Linux-Freaks wird es mit der Hilfe von Google dennoch gelingen, ihr System zufriedenstellend zu konfigurieren. Für Einsteiger ist es aber praktikabler, einen billigen DVD-Player an den Fernseher anzuschließen.

Blu-ray CSS war freilich nur der Anfang: Blu-ray Discs sehen wesentlich bessere Schutzmechanismen vor, die zum Teil direkt in der Hardware implementiert werden müssen, also beispielsweise in der Grafikkarte. Zwar wurden auch diese Schutzmaßnahmen bereits geknackt, die Vorgehensweise ist aber komplizierter geworden. Generell unternimmt die Medienindustrie momentan alles, um das Abspielen bzw. Auslesen von Video-Datenträgern am Computer zu erschweren. Der einzige Trost für Linux-Freunde besteht darin, dass mittlerweile auch Windows-Anwender zunehmend Probleme haben, eine Blu-ray Disc einfach anzusehen. Selbst die multimedia-affine Firma Apple macht aus diesen Gründen einen Bogen um Blu-ray.

DRM DRM steht für Digital Rights Management. Mit dieser Technik wird eine Audio- oder Video-Datei an eine bestimmte Hardware gebunden. Die Datei kann zwar mühelos kopiert, auf einem anderen Rechner aber nicht abgespielt werden. Lange Zeit waren alle Downloads von Apples iTunes-Shop durch DRM geschützt. Allerdings hat sich hier in den letzten Jahren eine Kursänderung abgezeichnet: Digitale Musik wird zunehmend DRM-frei verkauft – nicht zuletzt aufgrund des Drucks, den Apple auf die Musikindustrie ausgeübt hat.

Tot ist DRM aber leider noch lange nicht: Obwohl es bei Musik nicht funktioniert hat, versuchen Medienanbieter nun Videos, eBooks etc. DRM-geschützt zu verkaufen. Linux-Anwender sind von der legalen Nutzung DRM-geschützter Medien nahezu vollständig ausgeschlossen, und eine Besserung dieser Situation ist nicht in Sicht. Kaufen Sie nach Möglichkeit nur DRM-freie Musik bzw. Videos!

Audio- und Video-Formate

Es existieren unzählige Audio- und Video-Formate. Dieser Abschnitt macht gar nicht erst den Versuch, diese Formate vollständig aufzuzählen bzw. zu beschreiben. Vielmehr fasst er einige Linux-spezifische Informationen zu häufig eingesetzten Formaten zusammen. Einen guten Überblick über populäre Audio- und Video-Codecs gibt der folgende Wikipedia-Artikel:

http://de.wikipedia.org/wiki/Codec

Alle im Folgenden aufgezählten Formate werden in der einen oder anderen Form von Linux unterstützt. Aufgrund der bereits erwähnten rechtlichen Probleme können nur wenige Codecs offiziell in eine Distribution integriert werden.

WAV

WAV ist ein von Microsoft definiertes, sehr einfaches Audio-Format ohne Komprimierung. Die resultierenden Dateien sind frei von Qualitätsverlusten, aber leider riesig. WAV-Dateien können unter Linux problemlos erzeugt und abgespielt werden, es gibt weder Lizenz- noch Patentprobleme.

MP3

MP3 steht für *MPEG-1, Audio Layer 3*, wobei MPEG wiederum eine Abkürzung für *Moving Pictures Experts Group* ist. MP3 ist das bei Weitem populärste Dateiformat zur Komprimierung von Audio-Daten. Für Linux existieren diverse MP3-Decoder, sowohl in Form eigenständiger Kommandos oder Programme (`mpg123`) als auch als Bibliotheken. Bei MP3-Encodern zum Erzeugen von MP3-Dateien ist die Auswahl kleiner, in der Praxis kommt eigentlich nur noch `lame` zum Einsatz.

Obwohl das MP3-Verfahren überwiegend im Fraunhofer Institut entwickelt wurde, gibt es mehrere Firmen, die über MP3-Patente verfügen. Das bedeutet, dass MP3-Encoder lizenziert werden müssen – selbst dann, wenn sie kostenlos weitergegeben werden. Aus diesem Grund gibt es kaum noch eine Linux-Distribution, die MP3-Encoder direkt mitliefert.

Etwas besser sieht die Lage bei MP3-Decodern (MP3-Playern) aus: Zwar ist auch diese Technik patentiert, das Fraunhofer Institut und die Firma Thomson haben aber zum Ausdruck gebracht, dass Open-Source-Player bis auf Weiteres ohne Lizenz eingesetzt werden können:

http://mp3licensing.com

ID3-Tags

ID3-Tags sind Zusatzinformationen, die innerhalb der MP3-Datei gespeichert werden. Sie können unter anderem die folgenden Informationen umfassen: Titel, Interpret, Albumname, Komponist, ein Bild des CD-Covers etc. Es gibt zwei gängige Standards zur Speicherung der ID3-Informationen: ID3v1 und ID3v2 mit vielen zusätzlichen Textfeldern und Erweiterungsmöglichkeiten. Alle Audio-Player werten ID3-Tags aus, wobei die meisten Player kompatibel zu beiden Standards sind.

Die Informationen für die ID3-Tags werden in der Regel bereits beim Auslesen (Rippen) von Audio-Tracks ermittelt und gespeichert. Außerdem existieren zahllose Kommandos und Benutzeroberflächen, um die ID3-Informationen nachträglich zu vervollständigen, zu korrigieren bzw. von ID3v1 auf ID3v2 umzustellen (suchen Sie in Ihrem Paketmanager nach *id3*). Besonders komfortabel ist das Gnome-Programm EasyTAG; populäre Alternativen sind Ex Falso oder Kid3. Auch manche Audio-Player sind in der Lage, ID3-Tags zu verändern, beispielsweise Amarok.

Zur Suche nach CD-Cover-Dateien können Sie CoverFinder einsetzen. Zwar helfen auch Audio-Player wie Amarok oder Rhythmbox bei der Cover-Suche, diese Programme integrieren die Cover aber in eine interne Datenbank.

Ogg Vorbis Ogg Vorbis ist die Open-Source-Alternative zum MP3-Format. Ogg Vorbis bringt einen neuen Audio-Datentyp (Dateikennung `.ogg`) samt der Software zum Encodieren und Decodieren mit sich. Ogg Vorbis ist als Reaktion auf die Patent- und Lizenzschwierigkeiten mit dem MP3-Format entwickelt worden. Die Audio-Qualität ist so gut wie die von MP3. Das Ogg-Format unterstützt zwar keine ID3-Tags; Titel- und Meta-Informationen können aber in den Vorbis-Tags gespeichert werden. Detaillierte Informationen finden Sie unter:

http://www.vorbis.com

Leider hat sich das Ogg-Vorbis-Format nicht durchsetzen können. Im Internet werden Sie selten auf Ogg-Musikdateien stoßen, und auch Ogg-kompatible Audio-Player sind Mangelware. Deswegen ist das Ogg-Format eigentlich nur dann eine Option, wenn Sie Audio-Dateien nur am lokalen Computer anhören möchten, nicht aber auf externen Playern.

FLAC FLAC (*Free Lossless Audio Codec*) ermöglicht eine verlustfreie Kompression von Audiodaten. Das Format ist vor allem bei audiophilen Musikhörern beliebt.

WMA Windows Media Audio (WMA) ist ein weiterer, von Microsoft entwickelter Audio-Codec mit DRM-Unterstützung. Der Codec ist unter dem Namen VC-1 standardisiert und steht auch als Open-Source-Implementierung zur Verfügung, z. B. für den MPlayer bzw. im Rahmen der `ffmpeg`/`libavcodec0d`-Pakete.

AAC Advanced Audio Coding (AAC) ist eine Weiterentwicklung des MP3-Verfahrens, das im MPEG-2-Standard spezifiziert wird und ebenfalls DRM-Unterstützung bietet. AAC ist weit verbreitet und kommt unter anderem bei fast allen Audio-Dateien von Apple iTunes zum Einsatz. Mit `faac`/`faad` bzw. `libfacc`/`libfaad` existieren AAC-Encoder und -Decoder für Linux, die allerdings nur DRM-freie AAC-Dateien erzeugen bzw. verarbeiten können.

ATSC A/52 und AC-3 ATSC A/52 oder kurz AC-3 ist ein von Dolby Digital entwickeltes Mehrkanal-Audio-Format, das unter anderem für die Tonspur der meisten DVDs zum Einsatz kommt. Mit `liba52` existiert ein Open-Source-Decoder.

MPEG-1, -2 und -4 MPEG-1, -2 und -4 definieren diverse Formate zur Komprimierung von Audio- und Video-Daten. Wichtige Teile von MPEG-4 sind gleich in mehreren alternativen Codecs implementiert, die alle MPEG-4-kompatibel sind. Dazu zählen XviD und WebM (beide Open Source), DivX und H264.

WMV Unter dem Namen Windows Media Video (WMV) hat auch Microsoft eigene Video-Codecs entwickelt. Die WMV-Versionen 1 bis 3 (oft auch WMV7 bis -9 genannt, weil sie zusammen mit dem Windows Media Player 7 bis 9 ausgeliefert wurden) bieten ähnliche Eigenschaften wie MPEG-4, unterstützen aber zusätzlich DRM.

Theora

Theora ist das Video-Gegenstück zu Ogg -Vorbis. Auch der Theora-Codec bietet ähnliche Eigenschaften wie MPEG-4, basiert aber vollständig auf Open-Source-Code und ist damit frei verfügbar. Der Codec wird unter anderem vom Wikimedia-Projekt eingesetzt. Firefox kann ohne Installation irgendwelcher Plugins Theora-Videos abspielen.

http://www.theora.org

WebM (VP8, VP9)

Im Zuge der Entwicklung von HTML5 bestand für die Browser-Entwickler die Notwendigkeit, Audio- und Video-Codecs in ihre Webbrowser zu integrieren. Während Microsoft und Apple auf den proprietären Codec H264 setzen, kommt dieser für Open-Source-Software nicht infrage. Die Codecs Ogg und Theora wären eine Alternative, sind aber zu wenig verbreitet.

Diesen gordischen Konten versuchte Google zu durchschlagen, indem es den Codec-Entwickler On2 aufkaufte und den von dieser Firma entwickelten MPEG-4-Codec VP8 unter dem neuen Namen WebM als Open-Source-Code freigab. Wirklich umfassenden Erfolg hatte dieser Codec leider auch nicht, da es Zweifel gibt, dass der Codec frei von fremden Patenten ist. Google will 2013 einen verbesserten Nachfolger-Codec VP9 vorstellen; es bleibt abzuwarten, ob VP9 ein größerer Erfolg beschieden sein wird.

Video-Container

Ein Film besteht aus mehreren Komponenten, die intern voneinander getrennt sind: Zum eigentlichen Video ohne Ton kommen die Audio-Kanäle hinzu (oft in mehreren Sprachen, in Stereo und/oder in Mehrkanaltechnik wie Dolby Surround), bisweilen auch Untertitel (ebenfalls in mehreren Sprachen) und Metadaten, z. B. das DVD-Menü. Auf einer DVD liegen diese Komponenten in einzelnen Dateien vor. Soll ein Film aber in *einer* Datei verpackt werden, ist ein Container-Format erforderlich.

AVI, MOV und QT

Das populärste derartige Format ist AVI (Audio/Video Interleave): Sie kennen das Format sicher von vielen Digitalkameras, die selbst aufgenommene Videos so verpacken. Allerdings ist das AVI-Format relativ alt und mit vielen Einschränkungen verbunden. Beispielsweise können in AVI-Dateien keine Untertitel verpackt werden. Ebenfalls sehr weit verbreitet ist das von Apple definierte Container-Format QuickTime (QT oder MOV).

MKV, MP4 und OGM

In den letzten Jahren wurden zudem einige weitere Container-Formate entwickelt: Matroska (MKV), MP4 und OggMedia (OGM). Der größte Nachteil dieser Formate besteht darin, dass derartige Dateien in der Regel nur auf dem Computer abgespielt werden können, nicht aber auf DVD-Playern (schon gar nicht auf älteren Modellen). Dafür bieten diese Container-Formate eine Menge zusätzlicher Möglichkeiten. Falls

Sie die Wahl haben, sollten Sie das MKV-Format vorziehen, das momentan die meisten Funktionen bietet und sich bei video-begeisterten PC-Anwendern als eine Art inoffizieller Standard etabliert hat.

Das Container-Format hat nichts mit den Codecs zu tun!

Um es nochmals klarzustellen: Die hier vorgestellten Formate beschreiben lediglich den Container. Aus den Dateikennungen `*.avi`, `*.mkv`, `*.mp4`, `*.mov`, `*.ogm` bzw. `*.qt` geht *nicht* hervor, welche Audio- und Video-Codecs intern zum Einsatz kommen. Jedes Container-Format unterstützt diverse Codecs. Je nachdem, welche Codecs auf Ihrem Rechner installiert sind, kann es daher sein, dass Ihr Video-Player eine AVI-Datei abspielen kann, eine andere aber nicht.

Rechtliche Situation, Zusatzpakete

Ich habe nun bereits mehrfach erwähnt, dass je nach Ort, Gesetzgebung und der Reichweite bzw. Gültigkeit von Patenten eine standardmäßige Auslieferung diverser Codecs und Entschlüsselungs-Software unmöglich ist. Da Linux-Distributionen international heruntergeladen werden, müssen sie dem kleinsten gemeinsamen Nenner entsprechen.

Zu vielen Distributionen gibt es aber inoffizielle Paketquellen, in denen solche Pakete gesammelt sind (siehe Tabelle 10.1). Sie müssen diese Paketquellen zumeist selbst einrichten und können die gewünschten Pakete dann herunterladen. Auf den Websites der Paketquellen werden Sie oft einen Hinweis finden, dass Sie sich vor dem Download vergewissern müssen, dass die Verwendung der so zur Verfügung gestellten Software in Ihrem Land zulässig ist. Kurze Installationstipps zu den wichtigsten Multimedia-Paketquellen finden Sie auch in Kapitel 3, zu jeder Distribution jeweils im Abschnitt Erste Schritte.

Distribution	Multimedia-Website oder -Paketquelle
Debian	*http://deb-multimedia.org*
Fedora	*http://fedoraproject.org/wiki/Multimedia* *http://rpmfusion.org* *http://rpm.livna.org*
openSUSE	*http://en.opensuse.org/Restricted_formats* *http://packman.links2linux.de*
Ubuntu	*https://help.ubuntu.com/community/RestrictedFormats* *http://www.medibuntu.org*

Tabelle 10.1 Populäre Multimedia-Websites und -Paketquellen

10.2 Programmübersicht

Audio-Player

Das Programmangebot zum Abspielen von Audio-Dateien ist nahezu unüberschaubar. In Abschnitt 10.3 stelle ich Ihnen exemplarisch die Programme Amarok, Audacious, Banshee, Musique, Rhythmbox und Spotify vor. Nicht mehr gewartet und kaum noch verbreitet ist das WinAmp-ähnliche Programm XMMS. Ebenfalls obsolet sind die Linux-Version des RealPlayers und dessen Open-Source-Variante Helix-Player.

Multimedia-Player

Die sogenannten Multimedia-Player sind primär zum Abspielen von Video-Dateien konzipiert, kommen in der Regel aber auch mit Video-Streams und DVDs zurecht und können teilweise sogar zum Fernsehen verwendet werden. Sozusagen nebenbei können Multimedia-Player auch einzelne Audio-Dateien abspielen, ohne sich aber um die Verwaltung Ihrer MP3-Sammlung zu kümmern. Die wichtigsten Vertreter dieser Gruppe sind Dragon Player und Kaffeine (beide KDE), MPlayer, Totem (Gnome), VLC und xine. Details zu diesen Programmen folgen in Abschnitt 10.4.

DVDs ansehen

Damit Sie unter Linux eine nicht-kommerzielle DVD ansehen können, brauchen Sie einen Multimedia-Player sowie Codecs für AC-3 (Ton) und MPEG-2 (Bild). Außerdem sollte der Treiber für Ihre Grafikkarte die `XVideo`-Erweiterung (kurz `XV`) unterstützen. Grundsätzlich ist eine Video-Wiedergabe auch ohne XVideo möglich, beansprucht dann aber zusätzliche CPU-Leistung.

Zum Ansehen kommerzieller, durch CSS verschlüsselter DVDs brauchen Sie eine zusätzliche Bibliothek, die diese Schutzmaßnahme umgeht. In vielen Ländern ist es nicht zulässig, diese Bibliothek zu installieren. Eine rechtlich wasserdichte Alternative ist der Fluendo DVD Player, der momentan allerdings ca. 20 EUR kostet (siehe *http://www.fluendo.com*).

Kommandos

Wer es gern spartanisch hat, kann Audio-Dateien auch per Kommando abspielen. Diese Kommandos sind trotz des fehlenden Komforts wichtig, weil vielfach andere Programme darauf zurückgreifen, anstatt selbst einen entsprechenden Audio-Decoder zu implementieren. `mpg123` ist das klassische Kommando zum Abspielen von MP3-Dateien. Mit `mpg123 -w out.wav in.mp3` können Sie auch MP3-Dateien in WAV-Dateien umwandeln.

`madplayer` ist eine Alternative zu `mpg123`. Es basiert auf der `libmad`-Bibliothek. Das Programm kann MP3-Dateien in eine ganze Reihe anderer Formate umwandeln. `mad` und `libmad` unterstehen der GPL, was bei `mpg123` nicht der Fall ist. `mpg321` ist eine weitere Alternative zu `mpg123` und greift ebenfalls auf `libmad` zurück. `ogg123` spielt Ogg-Dateien ab. Das Kommando ist Teil des `vorbis-tools`-Pakets und setzt die Bibliotheken `libogg` und `libvorbis` voraus. Mit `vorbiscomment` können Sie die Kommentare (Meta-Tags) von Ogg-Dateien lesen und verändern.

CDs spielen und auslesen

Das direkte Abspielen einer CD ist insofern ein Sonderfall, als die Player-Software nur relativ triviale Aufgaben zu erledigen hat: Das Programm muss das Inhaltsverzeichnis einer Audio-CD einlesen und die Audio-Tracks dann abspielen. Das Programm überlässt dabei dem CD-Laufwerk die meiste Arbeit, also das Auslesen der Daten, die Fehlerkorrektur etc.

Es bestehen zwei Möglichkeiten, wie die Audio-Daten zur Sound-Karte kommen: Wenn es ein Audio-Kabel vom CD/DVD-Laufwerk zur Audio-Karte gibt, wird das Audio-Signal direkt in die Audio-Karte eingespeist. Fehlt dieses Kabel bzw. verwenden Sie ein externes Laufwerk (USB/Firewire), werden die digitalen Audio-Daten ausgelesen. Das Audio-System ist dafür verantwortlich, daraus Audio-Signale zu machen. Im Gegensatz zu Daten-CDs werden Audio-CDs nicht in das Dateisystem eingebunden. Der Zugriff auf die CD erfolgt normalerweise direkt über die Device-Datei, z. B. `/dev/cdrom` oder `/dev/scd0`.

Die meisten vorhin aufgezählten Audio- und Multimedia-Player können quasi nebenbei auch CDs abspielen. Reine CD-Player sind die Ausnahme geworden. Zu den wenigen Vertretern zählen die Kommandos `cdcd` und `tcd`.

CDDB und freedb

Die meisten CD-Player nehmen Kontakt mit einem CDDB-Server auf (CD Database), in der Regel mit *http://www.freedb.org*. Auf diesem Server befindet sich eine Datenbank, die zu allen dort registrierten CDs den Titel, die Gruppe bzw. die Interpreten sowie das Inhaltsverzeichnis in Textform speichert. Wenn Ihre CD bei `freedb.org` bekannt ist, zeigt der CD-Player also nicht mehr einfach die Track-Nummer an, sondern vielleicht »Led Zeppelin: Dazed and Confused«. Die Erkennung der CD basiert auf einem ID-Wert, der sich aus den Längen der Tracks der CD errechnet.

Für die Kommunikation mit dem CDDB-Server gelten in der Regel diese Parameter:

Adresse: `freedb.freedb.org`
IP-Port: 8880 (cddbp)

`freedb.freedb.org` leitet die Anfragen automatisch an einen von mehreren Mirror-Servern weiter. Falls der IP-Port 8880 durch eine Firewall blockiert ist, können Sie `freedb.org` auch über HTTP ansprechen. In diesem Fall sind folgende Angaben erforderlich:

Adresse: `freedb.freedb.org`
IP-Port: 80
CGI-Script: `~cddb/cddb.cgi`

Unter KDE können Sie die CDDB-Parameter für alle Programme im Systemeinstellungsmodul ERWEITERT • CDDB einstellen.

CD-Ripper

Sogenannte Ripper oder Grabber lesen Musik-Tracks einer Audio-CD in digitaler Form. Das ist schwieriger, als es auf den ersten Blick klingt. Die Audio-Tracks liegen zwar in digitaler Form vor, aber in einer anderen Form als bei einer Daten-CD. Wenn es beim Auslesen der Daten Probleme gibt, ist es für das CD-Laufwerk schwierig, exakt die Stelle zu finden, an der das Auslesen fortgesetzt werden soll. Sowohl die Auslesegeschwindigkeit als auch die Qualität der Audio-Dateien bei verkratzten oder schmutzigen CDs hängt stark vom CD/DVD-Laufwerk ab. Ripper liefern als Ergebnis üblicherweise WAV-Dateien.

Zum Auslesen von Audio-CDs und zur anschließenden Umwandlung der WAV-Dateien in ein besser geeignetes Format (MP3 oder Ogg) werden Sie in der Regel eine grafische Benutzeroberfläche verwenden. Unter Gnome können Sie dazu Sound Juicer oder Rhythmbox verwenden, unter KDE Amarok, Dolphin oder Konqueror. Wenn Sie den Prozess per Script automatisieren möchten, werden Sie an den Kommandowerkzeugen `icedax` und `cdparanoia` Freude finden (siehe Abschnitt 17.2).

Fernsehen am Computer

Neben speziellen Video-Angeboten für Computer (also YouTube und Co.) ist es auch möglich, herkömmliche Fernsehkanäle zu empfangen, am Computer anzusehen und aufzunehmen. Linux wird damit zum digitalen Videorecorder. Voraussetzung ist ein DVB-T-Empfänger, üblicherweise mit USB-Anschluss. Nicht alle Geräte sind Linux-kompatibel – recherchieren Sie also vor dem Kauf im Internet!

Ist der DVB-T-Empfänger einmal eingerichtet, können Sie nahezu jeden Linux-Multimedia-Player zum Fernsehen verwenden. Darüber hinaus gibt es spezielle TV-Benutzeroberflächen, die noch viel mehr Möglichkeiten bieten: Anzeige des TV-Programms, Aufnahme von Sendungen, zeitversetztes Fernsehen, Streaming etc. Die Programme können oft auch als Audio- und Video-Player sowie zum Ansehen von Fotos verwendet werden. All diese Funktionen sind in eine Benutzeroberfläche verpackt, die eine einfache Bedienung des *Home Theater PC* (HTPC) erlaubt.

Am populärsten ist momentan das Programm XBMC, das ich Ihnen in Kapitel 12 als Medien-Player für den Raspberry Pi näher vorstelle. Selbstverständlich können Sie XBMC auch auf jedem Linux-PC ausführen! Alternativen zu XBMC sind Boxee, MythTV, Freevo, MMS, Moovida sowie VDR bzw. deren Kompilation durch die Zeitschrift c't (c't-VDR).

Dem selbst gebauten Media-Center auf Linux-Basis steht also scheinbar nichts mehr im Wege. Ganz so toll, wie es hier klingt, ist es in der Praxis leider nicht: Die Konfiguration der Programme ist oft haarsträubend kompliziert. Viele Programme sind für den amerikanischen Markt optimiert und scheitern im deutschen Sprachraum beim Sendersuchlauf oder bei der Anzeige von Programminformationen. Bastler finden hier eine Spielwiese für Wochen. Kurz und gut: Erwarten Sie keine Lösungen, die nach der Installation quasi auf Knopfdruck funktionieren!

Fernbedienung

Falls Ihr Computer einen Infrarot-Empfänger hat oder ein Empfänger in der TV-Karte bzw. im DVB-T-Empfänger integriert ist, können Sie die TV-Funktionen auch per Fernbedienung steuern. Für die Verarbeitung der Signale ist das Paket `lirc` verantwortlich (Linux Infrared Remote Control), allerdings ist je nach Fernbedienung erst eine aufwendige Konfiguration erforderlich. Tipps dazu finden Sie im Raspberry-Pi-Kapitel in Abschnitt 12.3.

Audio- und Videoschnitt

Wenn Sie digitale Medien nicht nur konsumieren, sondern selbst erzeugen bzw. bearbeiten wollen, brauchen Sie Werkzeuge zum Audio- und Video-Schnitt, zur Recodierung von Dateien, zur Erzeugung von DVD-Menüs (DVD-Authoring) etc. Tabelle 10.2 gibt einen Überblick über die populärsten derartigen Programme. Programme bzw. Programmpakete ohne grafische Benutzeroberfläche sind darin als »Kommando« gekennzeichnet.

Beachten Sie, dass ein Teil der in Tabelle 10.2 aufgezählten Programme nicht mehr aktiv gewartet wird. Vielfach ist eine manuelle Installation erforderlich. Für multimedia-begeisterte Linux-Anwender gibt es übrigens auch eigene Distributionen, z. B. 64 Studio und Ubuntu Studio. Ein guter Startpunkt für die Suche nach weiteren Multimedia-Tools ist einmal mehr das deutsche Ubuntu-Wiki:

http://wiki.ubuntuusers.de/Multimedia

Eine kompakte Einführung zum Thema DVD-Authoring gibt der folgende, schon etwas ältere Artikel (2006):

http://www.kraus.tk/publications/DVDauthoring-Artikel/dvdauthoring.html

Eine etwas aktuellere Übersicht der verfügbaren Programme gibt eine dreiteilige Grumpy-Editor-Serie auf *lwn.net*:

http://lwn.net/Articles/261820 (Teil 1: Analog-Videos einlesen)
http://lwn.net/Articles/262985 (Teil 2: Video-Schnitt)
http://lwn.net/Articles/263387 (Teil 3: DVD-Struktur erzeugen)

Schließlich hat die Website Tom's Hardware 2011 das ganze Spektrum der Linux-Audio-Software unter die Lupe genommen:

http://www.tomshardware.com/reviews/ubuntu-linux-audio-software,2856.html
http://www.tomshardware.com/reviews/audio-production-software-linux-ubuntu,2860.html

DVDs kopieren und rippen

Nichtkommerzielle DVDs dürfen Sie kopieren bzw. auslesen und als Filmdatei auf Ihrer Festplatte speichern. Dabei helfen die Programme AcidRip, DVD::rip, DVD95, Handbrake, K9Copy und OGMrip. Einige dieser Programme stelle ich in Abschnitt 10.6 näher vor.

Programm	Funktion
Ardour	Mehrspur-Audio-Recorder
Audacity	Audio-Editor
Avidemux	Video-Schnitt und -Konvertierung
Bombono	DVD-Authoring (siehe auch *http://lwn.net/Articles/421786*)
Cinelerra CV	Video-Editor für Profis
DeVeDe	einfaches DVD-Authoring
DVBcut	DVB-T-Stream speichern
`dvdauthor`	DVD-Authoring (Kommando)
DVDStyler	DVD-Authoring
FFmpeg	Audio- und Video-Konverter (Kommando)
Gnome Sound Recorder	einfacher Audio-Recorder (Gnome, Paket `gnome-media[-apps]`)
Handbrake	Video-Konverter
Kdenlive	Video- und DVD-Menü-Editor (KDE)
KHdRecord	einfacher Audio-Recorder (KDE 3)
Kino	Video-Editor, Video-Schnitt
kMediaFactory	einfaches DVD-Authoring (KDE)
LiVES	Live-Video-Schnitt
ManDVD	DVD-Authoring
Mencoder	Audio- und Video-Konverter (Kommando, basiert auf MPlayer)
Open Movie Editor	einfacher Video-Editor
OpenShot	Video-Schnitt
PiTiVi	Video-Schnitt
PhotoFilmStrip	erzeugt aus Fotos einen Film (mit Ken-Burns-Effekt)
QDVDAuthor	DVD-Authoring
Rosegarden	Audio- und Midi-Sequenzer (vergleichbar mit Cubase)
SoundConverter	Audio-Konverter (Gnome-Benutzeroberfläche)
Steamripper	Ripper für Audio-Streams (Kommando)
traGtor	Audio- und Video-Konverter (KDE, basiert auf FFmpeg)
Transcode	Video-Konverter (Kommando)

Tabelle 10.2 Werkzeuge zum Audio- und Video-Schnitt und zum DVD-Authoring

10.3 Audio-Player (Amarok, Audacious, Banshee, Musique, Rhythmbox, Spotify)

Dieser Abschnitt stellt in alphabetischer Reihenfolge die wichtigsten Audio-Player für Linux vor. Die hier präsentierten Programme kümmern sich außerdem um die Verwaltung Ihrer MP3-Kollektion, sodass es einfach ist, ein bestimmtes Album auszuwählen und abzuspielen. Dazu müssen Sie beim ersten Start des Players das Musik-Verzeichnis angeben, das dann erfasst wird. Dieser Vorgang beansprucht bei großen MP3-Kollektionen beim ersten Mal relativ viel Zeit. Als Grundlage für die Kategorisierung dienen die ID3-Tags der MP3-Dateien. Wenn diese Daten fehlen oder nicht stimmen, macht keines der im Folgenden vorgestellten Programme Spaß!

Beachten Sie, dass die Player nur für die Benutzeroberfläche zuständig sind. Welche Audio-Formate die Programme abspielen können, hängt davon ab, welche zum Player passenden Codec-Bibliotheken installiert sind!

Einige der hier vorgestellten Programme können Ihre MP3-Sammlung mit traditionellen MP3-Playern und vielfach auch mit Android-Handys synchronisieren. Probleme bereiten aber die meisten neueren Apple-Geräte (iPhones, iPads etc.), deren Synchronisationsmechanismen sich ständig ändern. Bei älteren iPods können Sie das Programm gtkPod zu Hilfe nehmen; es unterstützt allerdings nur Geräte ohne iOS bzw. bis zur iOS-Version 4.*n*.

Amarok

Amarok (siehe Abbildung 10.1) ist das populärste und ausgereifteste KDE-Programm zum Abspielen von Audio-Dateien und zur Verwaltung großer Audio-Bibliotheken. Amarok greift zur Audio-Wiedergabe auf das KDE-Sound-System Phonon zurück.

Beim ersten Start fragt das Programm, wo sich Ihre Audio-Dateien befinden, und erstellt eine Bibliothek aller verfügbaren Titel. Amarok speichert diese Informationen in einer Datenbank, wobei der Datenbank-Server in Amarok integriert ist (Embedded MySQL). Über das Kontextmenükommando METADATEN BEARBEITEN können Sie die ID3-Tags eines einzelnen Titels oder eines ganzen Albums ändern.

Ihre Audio-Sammlung können Sie in der linken Seitenleiste LOKALE SAMMLUNG anzeigen und nach verschiedenen Kriterien ordnen. Ein Doppelklick auf ein Genre oder Album fügt alle entsprechenden Tracks der Wiedergabeliste (rechts) hinzu. Im mittleren Teil des Fensters können Sie Informationen zum gerade gespielten Titel einblenden, z. B. den Liedtext oder die Wikipedia-Seite der Band.

Wenn Sie eine CD eingelegt haben, können Sie die darauf enthaltenen Titel auslesen (rippen), in das MP3- oder Ogg-Format umwandeln und Ihrer Musiksammlung hinzufügen. Dazu klicken Sie in der linken Seitenleiste den Eintrag AUDIO-CD mit der rechten Maustaste an und führen ZUR SAMMLUNG KOPIEREN • LOKALE SAMMLUNG aus. In mehreren Dialogen können Sie nun das Audio-Format, den Aufbau der

Dateinamen, die Codierqualität etc. einstellen. In typischer KDE-Manier haben diese Dialoge mehr Optionen, als Sie es für möglich halten würden. Das Erzeugen von MP3-Dateien setzt voraus, dass `lame` installiert ist!

Abbildung 10.1 Audio-Dateien mit Amarok anhören

Audacious

Audacious zählt zu den schlanken Audio-Playern und eignet sich besonders gut dazu, einfach die Audio-Dateien eines Verzeichnisses abzuspielen. Wie die anderen in diesem Abschnitt vorgestellten Player kann aber auch Audacious eine Musiksammlung erfassen und im Dialogblatt SAMMLUNG nach Künstlern und Genres geordnet darstellen.

Banshee

Der Audio-Player Banshee basiert auf der Mono-Bibliothek. Das Programm ist durch Plugins erweiterbar (BEARBEITEN • EINSTELLUNGEN • ERWEITERUNGEN). Mit den Plugins können Sie unkompliziert Audio-CDs rippen und der Audio-Bibliothek hinzufügen, Platten-Cover aus dem Internet herunterladen, Ihre Audio-Sammlung mit einem MP3-Player synchronisieren, MP3-Dateien bei Amazon kaufen und herunterladen etc.

Die zu verwaltenden Audio-Dateien müssen zuerst »importiert« werden (MEDIEN • MEDIEN IMPORTIEREN • LOKALER ORDNER). Die Eigenschaften werden in der Datenbank `.config/banshee-1/banshee.db` gespeichert. In der Folge können Sie Titel nach verschiedenen Kriterien auswählen, in Listen organisieren, bewerten etc. Wenn Sie Ihre Audio-Sammlung nach Genres gruppieren möchten, führen Sie ANSICHT • BROWSERINHALT • GENRE-FILTER aus.

Musique

Musique (ehemals Minitunes) ist ein minimalistischer Audio-Player mit einer schlanken und eleganten Benutzeroberfläche. Das Programm zeigt alle Künstler, Alben oder Ordner in Form von Icons an. Die Ordneransicht ist besonders attraktiv, wenn Sie Ihre Musik in Form von Verzeichnissen organisiert haben. Mit einem Button fügen Sie alle Titel des gerade ausgewählten Objekts in die Liste der abzuspielenden Stücke ein. INFO zeigt soweit verfügbar den Wikipedia-Text der Band sowie den Liedtext an. Sonstige Zusatzfunktionen fehlen (leider auch die Genre-Ansicht).

Rhythmbox

Rhythmbox bzw. einfach *Musik*, wie sich das Programm in aktuellen Versionen nennt, ist der Standard-Audio-Player der meisten Gnome-basierten Distributionen sowie von Ubuntu (siehe Abbildung 10.2). Auch bei diesem Programm müssen Sie zuerst Ihre Musiksammlung mit MUSIK HINZUFÜGEN erfassen. Rhythmbox überwacht diesen Ordner nun auf Veränderungen; die entsprechende Option finden Sie in EINSTELLUNGEN • MUSIK.

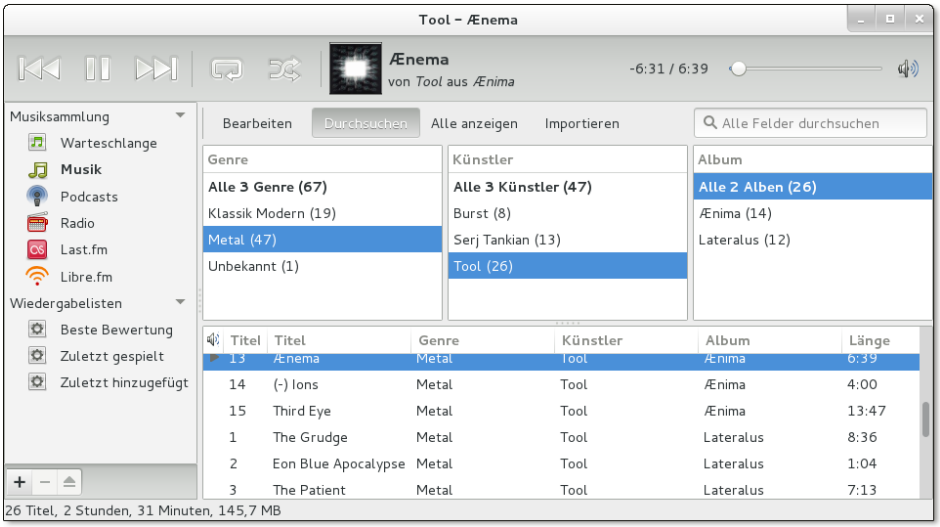


Abbildung 10.2 Audio-Dateien mit dem Gnome-Programm Rhythmbox anhören

Wenn Sie Ihre Audio-Verzeichnisse grundlegend ändern, ist es das Beste, in Rhythmbox alle Titel zu markieren, per Kontextmenü zu entfernen und anschließend neu zu importieren. Verwenden Sie zum Löschen von Titeln aus der Datenbank aber auf keinen Fall das Kommando IN DEN PAPIERKORB VERSCHIEBEN! Dieses Kommando betrifft nicht die Rhythmbox-Musikdatenbank, sondern es löscht Ihre MP3-Dateien! Rhythmbox speichert die Musikdatenbank in der Datei `.local/share/rhythmbox/rhythmdb.xml`.

Die Bedienung von Rhythmbox ist einfach: Sie wählen ein Genre, einen Interpreten und/oder ein Album aus und klicken auf den Button WIEDERGABE. Rhythmbox spielt

nun alle in der Liste angezeigten Titel. Die Genre-Auswahlliste wird standardmäßig nicht angezeigt. Um die Liste einzublenden, führen Sie EINSTELLUNGEN • ALLGEMEIN aus und wählen die Browser-Ansicht GENRES, KÜNSTLER UND ALBEN.

Eigene Wiedergabelisten erzeugen Sie in der Seitenleiste mit dem Plus-Button. Anschließend fügen Sie die gewünschten Titel per Drag&Drop in die neue Liste ein. Es ist auch möglich, ganze Genres, Interpreten oder Alben einzufügen.

Die Funktionen von Rhythmbox können durch Plugins erweitert werden. Unter anderem gibt es Plugins für den Online-Radio-Service LastFM und zum Einkauf von MP3-Dateien bei Amazon. Ubuntu installiert zusammen mit Rhythmbox ein Plugin, das es ermöglicht, MP3-Dateien im *Ubuntu One Music Shop* (U1MS) zu kaufen. U1MS setzt einen Account im Ubuntu-One-Cloud-Service voraus.

Spotify

Spotify (siehe Abbildung 10.3) ist ein kommerzielles Musik-Streaming-Angebot. Um es zu nutzen, ist die Installation des Spotify-Players erforderlich. Für Linux gibt es momentan erst eine Vorversion für Debian und Ubuntu. Eine Installationsanleitung finden Sie hier:

http://www.spotify.com/at/download/previews

Zur Nutzung von Spotify benötigen Sie ein Spotify- oder Facebook-Konto. Nach dem ersten Login sollten Sie die Sprache von Spotify auf DEUTSCH umstellen. Die entsprechende Auswahlliste finden Sie im Einstellungsdialog, den Sie mit EDIT • PREFERENCES erreichen. Wenn Sie nicht möchten, dass alle Ihre Facebook-Freunde genau mitverfolgen können, wann Sie welche Musik hören, sollten Sie außerdem alle entsprechenden Optionen (AKTIVITÄTEN TEILEN, PROFIL) deaktivieren.

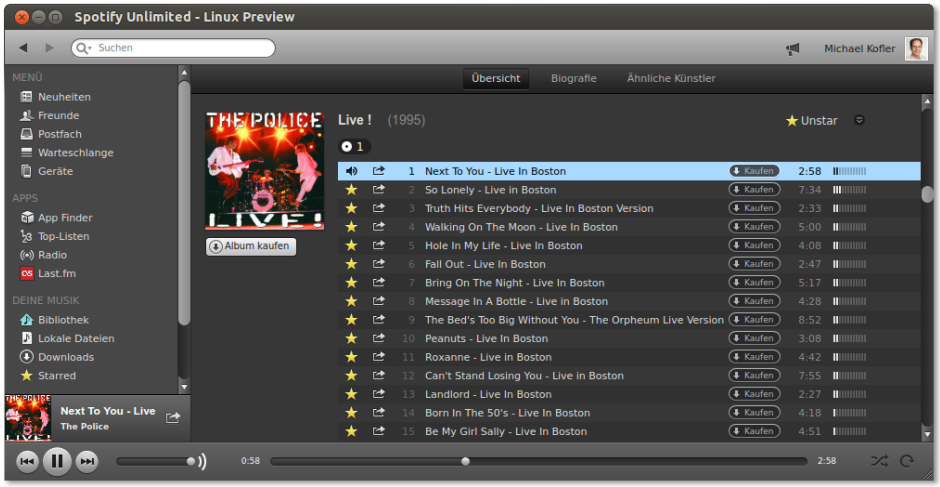


Abbildung 10.3 Spotify

Bei meinen Tests hat die Spotify-Vorversion problemlos und stabil funktioniert. Unter Ubuntu integriert sich das Programm sogar in das Audio-Menü im Panel und kann auch dort gesteuert werden, wenn das Spotify-Fenster geschlossen ist. Weniger erfreulich ist der verhältnismäßig hohe CPU- und Speicherbedarf.

10.4 Multimedia-Player (Dragon Player, Kaffeine, MPlayer, Totem, VLC, xine)

Die in diesem Abschnitt vorgestellten Multimedia-Player sind primär zum Abspielen von Video-Dateien oder -Streams und DVDs konzipiert. Die meisten Programme eignen sich zudem auch zum Fernsehen sowie zur Wiedergabe einzelner Audiodateien, ohne dass gleich die ganze Musik-Sammlung neu erfasst werden muss. Zu den meisten im Folgenden vorgestellten Playern gibt es auch Web-Plugins, die das komfortable Abspielen von Multimedia-Dateien direkt im Browser ermöglichen (siehe Abschnitt 8.2).

Dragon Player

Dragon Player ist ein minimalistischer Video-Player für KDE. Das Programm kommt unter anderem in Kubuntu zum Einsatz, wo es den KDE-Standard-Player Kaffeine ersetzt. Die Bedienung des Programms beschränkt sich auf das absolute Minimum. Die wichtigsten Kommandos können auch per Tastatur durchgeführt werden: F aktiviert bzw. deaktiviert den Vollbildmodus, M schaltet den Ton ein/aus (Mute), R zeigt das DVD-Menü an, ␣ unterbricht die Wiedergabe bzw. nimmt sie wieder auf, S beendet die Wiedergabe endgültig.

Kaffeine

Kaffeine (siehe Abbildung 10.4) ist der Standard-Player des KDE-Desktops. Die Benutzeroberfläche ist schnörkellos. Zu den attraktivsten Features zählt die Unterstützung des Mausrads, dessen Drehung das Video um 15 Sekunden vor bzw. zurück bewegt. Kaffeine nutzt die KDE-Multimedia-Bibliothek Phonon, wobei Phonon je nach Konfiguration bzw. Distribution wiederum auf xine, GStreamer oder VLC als Backend zurückgreift. Aktuelle openSUSE-Versionen verwenden standardmäßig die GStreamer-Bibliotheken.

MPlayer

MPlayer war im vorigen Jahrzehnt der beste und populärste Multimedia-Player für Linux. Diesen Status hat das Programm aber mittlerweile verloren: Im Vergleich zu den anderen hier vorgestellten Programmen ist MPlayer sperrig in der Bedienung und schwierig bei der Konfiguration (Video-Backend, CD/DVD-Device etc.). Lästig ist auch, dass das Programm als einziger der hier vorgestellten Player keine DVD-Navigationsmenüs anzeigen kann. Zur Auswahl der Sprache, der Untertitel etc. müssen Sie das Kontextmenü verwenden.

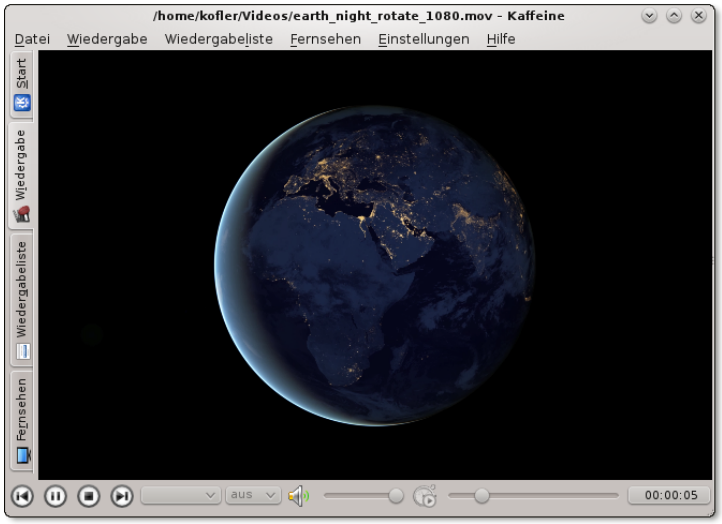


Abbildung 10.4 Kaffeine

Nach der Installation von MPlayer stehen gleich zwei Varianten des Programms zur Verfügung: `mplayer` *adresse* startet die minimalistische Version ohne Benutzeroberfläche, `gmplayer` *adresse* die ansprechendere Variante mit einer einfachen Benutzeroberfläche. Bei einigen Distributionen befindet sich `gmplayer` in einem eigenen Paket, das zumeist den Namen `mplayer-gui` hat. Falls Ihre Grafikkarte nicht XVideo-kompatibel ist, müssen Sie beim Start die Option `-vo x11` angeben. Mplayer benötigt dann aber mehr Rechenleistung.

Es gibt diverse Tastenkürzel zur Bedienung des Programms, die in der Datei `/etc/mplayer/input.conf` definiert und in `man mplayer` dokumentiert sind. Die wichtigsten sind P (Pause) und Q (Quit). Mit den Cursortasten bewegen Sie sich im Film vor bzw. zurück.

Beim Start von MPlayer können unzählige Optionen übergeben werden, die in `man mplayer` ausführlich dokumentiert sind. Hier werden nur einige ganz wichtige Optionen kurz vorgestellt:

- `-ao` *treiber* gibt den gewünschten Audio-Ausgabe-Treiber an (z. B. `oss`, `sdl`). `-ao help` zeigt eine Liste der verfügbaren Treiber an.
- `-fs` startet das Programm im Full-Screen-Modus.
- `-framedrop` überspringt einzelne Bilder, wenn die CPU-Leistung nicht für die Berechnung aller Bilder ausreicht. Der Vorteil dieser radikalen Maßnahme besteht darin, dass Audio- und Video-Informationen synchron bleiben.

- `-vo` *`treiber`* gibt den gewünschten Video-Ausgabe-Treiber an (z. B. `x11`, `xv`). `-vo help` zeigt eine Liste der verfügbaren Treiber an.

Die Optionen können auch in `~/.mplayer/config` bzw. in `/etc/mplayer/mplayer.conf` eingestellt werden. Jede Option wird in einer eigenen Zeile in der Form `vo=x11` eingetragen.

Totem

Totem (siehe Abbildung 10.5) ist der Standard-Player des Gnome-Desktops. Totem erfüllt diese Aufgabe zufriedenstellend, wenn auch ohne jegliche Zusatzfunktionen. Immerhin können Sie mit Strg+H unkompliziert das Menü, die Statuszeile und alle anderen Bedienelemente aus- und bei Bedarf wieder einblenden. Noch besser ist, Sie aktivieren mit F11 den Vollbildmodus.

Aktuelle Totem-Versionen basieren auf GStreamer; in der Vergangenheit gab es auch Totem-Versionen, die die xine-Bibliotheken nutzten. Wenn eine zur Wiedergabe erforderliche Codec-Bibliothek fehlt, bietet Totem an, in der Paketverwaltung danach zu suchen. Erfolgreich ist diese Suche bei den meisten Distributionen aber nur dann, wenn Sie vorher zusätzliche Multimedia-Paketquellen eingerichtet haben, also z. B. RPM Fusion für Fedora oder Packman für openSUSE.

Wenn Totem zum Abspielen von Audio-Dateien eingesetzt wird, nervt es mit der Anzeige psychedelischer Muster. Diese Grafikeffekte unterbinden Sie bei Bedarf mit Bearbeiten • Einstellungen • Anzeige.

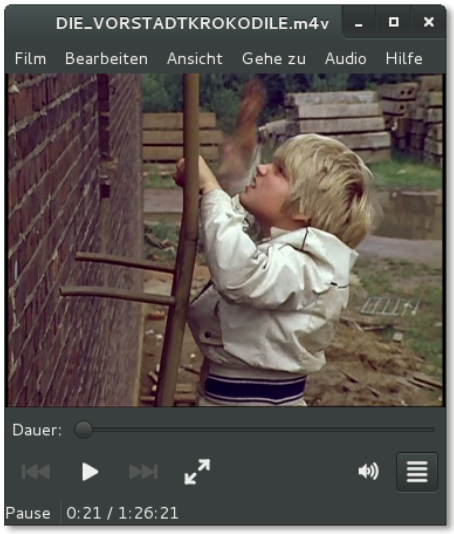


Abbildung 10.5 Totem, der Standard-Video-Player von Gnome

VLC

Der Multimedia-Player VLC (ehemals *VideoLan Client*, siehe Abbildung 10.6) ist momentan der modernste Multimedia-Player für Linux und bietet technisch versierten Anwendern eine herrliche Spielwiese. Die Stärken von VLC liegen in der Streaming-Anwendung, VLC kann aber selbstverständlich auch DVDs und Video-Dateien abspielen. VLC greift auf externe Codec-Bibliotheken zurück (z. B. FFmpeg, libmpeg2 und x264), und die Benutzeroberfläche basiert auf der Qt-Bibliothek. Eine Besonderheit des Programms besteht darin, dass Filtereffekte in Echtzeit angewendet werden können. Das ermöglicht es z. B., ein mit einer Digitalkamera hochkant aufgenommenes Video beim Abspielen richtig zu drehen.

Installieren Sie auch vlc-codecs!

Bei aktuellen Versionen von VLC sind die Pakete für den eigentlichen Player und dessen Codecs getrennt. Stellen Sie sicher, dass auch das Paket `vlc-codecs` installiert ist! Wenn VLC eine Codec-Bibliothek nicht findet, liefert es die Fehlermeldung: *VLC unterstützt das Audio- oder Videoformat xxx nicht. Leider können Sie daran nichts ändern.*

Lassen Sie sich davon nicht entmutigen! Sie müssen lediglich sicherstellen, dass `vlc-codecs` sowie einige andere Codec-Pakete installiert sind. Wenn Sie unter openSUSE arbeiten, finden Sie auf der Website *http://opensuse-community.org* 1-Click-Links zur Installation aller relevanten Pakete.

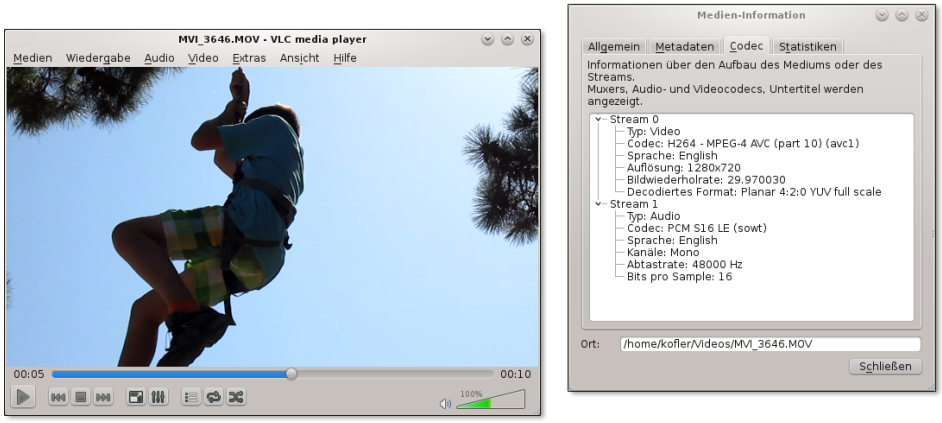


Abbildung 10.6 Der VLC-Player mit detaillierten Codec-Informationen

xine

Die Stärken von xine liegen in der Unterstützung zahlloser Audio- und Video-Formate. Das Programm kann weitestgehend über die Tastatur gesteuert werden. xine ist für Linux auch deswegen von großer Bedeutung, weil die xine-Benutzeroberfläche vollständig von den zugrunde liegenden Bibliotheken getrennt ist. Das ermöglicht es anderen Programmen, auf die xine-Bibliotheken zurückzugreifen.

Zum Start des Players führen Sie einfach `xine` aus. Wenn das Kommando nicht zur Verfügung steht, haben Sie wahrscheinlich nur die xine-Bibliotheken, aber nicht die Benutzeroberfläche installiert. Sie benötigen noch das Paket `xine-ui`.

Die Steuerung der Grundfunktionen des Programms erfolgt durch ein Bedienfeld (siehe Abbildung 10.7). Wenn dieses nicht angezeigt wird, müssen Sie es mit dem `xine`-Kontextmenükommando BEDIENPULT ANZEIGEN bzw. mit G einblenden. Die Navigations-Buttons, die in etwa den Knöpfen einer Fernbedienung für einen DVD-Player entsprechen, aktivieren Sie mit MENÜS • NAVIGATION bzw. mit Alt+E. Die DVD-Wiedergabe beginnen Sie mit dem gleichnamigen Button, oder Sie starten das Programm gleich in der Form `xine dvd:/`.

Abbildung 10.7 xine

EINSTELLUNGEN • EINSTELLUNGEN bzw. Alt+S führt in einen komplexen Konfigurationsdialog, der mehr Einstellmöglichkeiten bietet, als Sie sich vorstellen können. Das gilt insbesondere, wenn Sie im Dialogblatt GUI Ihre xine-Erfahrung von BEGINNER auf ADVANCED oder EXPERT stellen. Diese Änderung müssen Sie mit ANWENDEN quittieren, damit sie wirksam wird. Die Konfiguration wird in `.xine` gespeichert. Beachten Sie, dass diese Konfigurationsdatei für alle Player gültig ist, die auf die xine-Bibliotheken zurückgreifen. Weitere Konfigurationstipps sowie Informationen zu xine finden Sie auf der folgenden umfassenden Website:

http://xine-project.org

10.5 Audio- und MP3-Tools (Audacity, EasyTAG, Sound Juicer)

Dieser Abschnitt stellt einige Programme vor, die beim Erzeugen und Verwalten von Audio- und MP3-Dateien helfen: Audacity hilft beim Aufnehmen und Schneiden von Audio-Dateien, EasyTAG erlaubt das Einstellen bzw. Ändern der ID3-Tags von MP3-Dateien, und Sound Juicer liest Audio-CDs aus und erzeugt Ogg- oder MP3-Dateien.

Audacity

Audacity ist ein sehr vielseitiges, aber deswegen auch komplexes Programm: Sie können damit mehrere Audio-Spuren aufnehmen, bearbeiten, schneiden, übereinanderlegen, mit Effekten verändern etc. (siehe Abbildung 10.8). Ich stelle hier aber nur wenige, ganz elementare Funktionen vor, um Audio-Aufnahmen durchzuführen und Teile aus einer Audio-Datei herauszuschneiden.

Es mag übertrieben erscheinen, für solche Aufgaben Audacity einzusetzen, aber das Programm erledigt nach einer kurzen Einarbeitung auch derart triviale Tätigkeiten effizienter und zuverlässiger als vorgeblich einfachere Audio-Tools. Wenn es Ihnen nur darum geht, einen Audio-Kanal aufzunehmen und das Ergebnis gleich als MP3- oder Ogg-Datei zu speichern, bietet sich unter Gnome der Einsatz des Programms `gnome-sound-recorder` (Paket `gnome-media[-apps]`) an.

Aufnehmen

Um eine Aufnahme zu starten, stellen Sie in dem neben dem Mikrofonsymbol dargestellten Listenfeld das gewünschte Input-Device ein und klicken auf den roten Aufnahme-Button. Audacity erzeugt eine Stereo-Audio-Spur und beginnt unverzüglich mit der Aufnahme. Die aufgenommenen Daten werden unkomprimiert im Verzeichnis `.audacity`*n*`-name/project`*n* gespeichert. Stellen Sie sicher, dass in diesem Verzeichnis ausreichend Platz ist!

Standardmäßig können Sie die laufende Aufnahme nicht mithören. Wenn Sie das möchten, müssen Sie vor Beginn der Aufnahme Transport • Software Playthrough bzw. Transport • Software Playback aktivieren. Diese Funktion wird in den Audacity-FAQs aber zu Recht als *clunky* beschrieben und führte bei meinen Tests zu einer hohen CPU-Last und einem Abbruch der Aufnahme. Besser ist es, im Audio-Mixer, zur Not einfach mit `alsamixer` in einer Konsole, den Line- oder Mikrofon-Eingang zu aktivieren. Sie können die Wiedergabelautstärke dieses Kanals verändern, ohne die Aufnahme zu beeinflussen.

Schneiden

Nach Abschluss der Aufnahme können Sie diese anhören und bei Bedarf verändern, also Teile herausschneiden oder bei leisen Aufnahmen die Lautstärke durch Effekte • Normalisieren anheben. Dazu müssen Sie den gewünschten Bereich zuerst markieren. Am einfachsten geht das mit der Maus, Audacity bietet aber unzählige weitere Möglichkeiten, um Beginn und Ende der Markierung exakt festzulegen.

Speichern/ Exportieren

DATEI • EXPORTIEREN speichert den markierten Bereich in einer Audio-Datei beliebigen Formats, BEARBEITEN • TRIMMEN löscht alles außer der Markierung, Entf löscht den markierten Bereich.

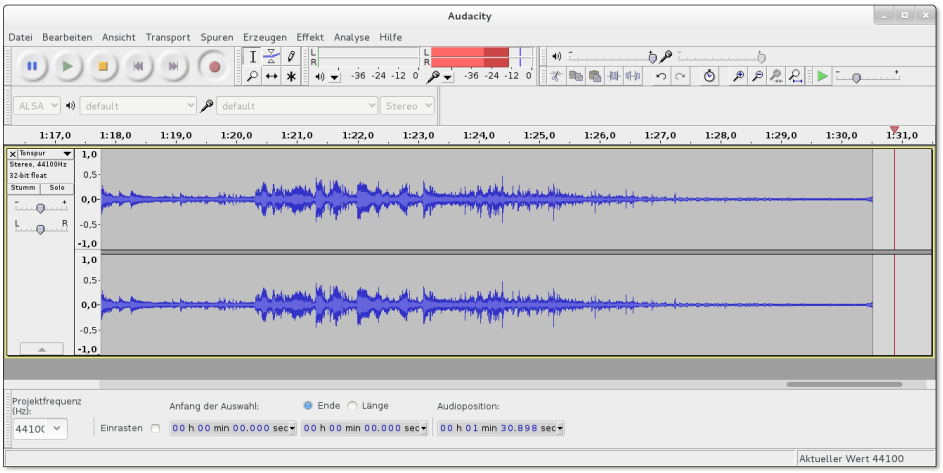


Abbildung 10.8 Audio-Tracks mit Audacity aufnehmen und schneiden

Wenn Sie ein Audacity-Projekt sichern, werden neben einer relativ kleinen Projektdatei alle Kanäle in einem eigenen, verlustfreien Format gespeichert, das in einem eigenen Verzeichnis `name_data` sehr viel Platz beansprucht. Um die Audio-Dateien problemlos mit einem anderen Programm anzuhören, exportieren Sie das Projekt im WAV-, Ogg- oder MP3-Format. Letzteres erfordert die Installation von `lame`. Wenn Sie bereits vorhandene MP3-Dateien oder andere Audio-Dateien bearbeiten möchten, laden Sie diese einfach in ein leeres Audacity-Projekt. Sobald der Import erledigt ist, haben Sie dieselben Bearbeitungsmöglichkeiten wie bei einer Aufnahme.

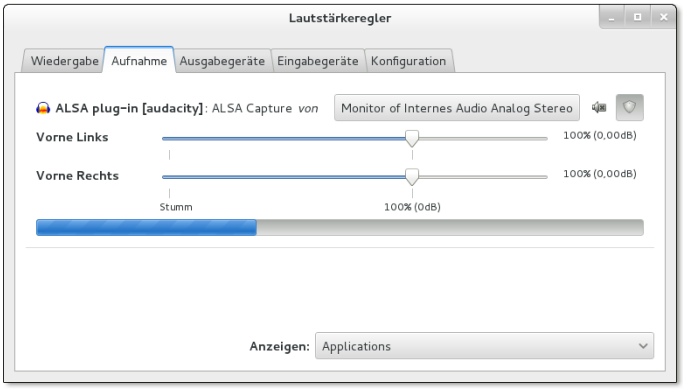


Abbildung 10.9 PulseAudio-Einstellungen, um die aktuelle Tonausgabe mitzuschneiden

Die aktuelle Tonausgabe mitschneiden

Je nach Audio-Konfiguration bzw. -Hardware scheint es für Audacity unmöglich zu sein, die aktuelle Tonausgabe aufzunehmen, also das, was Sie über den Lautsprecher des Computers gerade hören. Das wäre mitunter praktisch, beispielsweise, um den Ton eines Flash-Videos oder eines Internet-Radio-Senders mitzuschneiden.

Falls Sie PulseAudio als Audio-System einsetzen, können Sie diese Einschränkung umgehen: Dazu starten Sie Audacity und das Programm, das als Audio-Quelle dienen soll, z. B. ein Webbrowser. In Audacity müssen Sie die Aufnahme starten!

Nun starten Sie das Programm `pavucontrol`. Dieses Programm dient zur Steuerung von PulseAudio und muss oft extra installiert werden. In `pavucontrol` wechseln Sie in das Dialogblatt AUFNAHME und stellen dort beim Punkt ALSA PLUG-IN (AUDACITY) als Aufnahmequelle MONITOR OF INTERNES AUDIO ANALOG STEREO ein (siehe Abbildung 10.9).

EasyTAG

Wer selbst eine größere MP3-Sammlung pflegt, der weiß, dass die richtige Einstellung der MP3-Tags viel Zeit und Mühe macht: Die ID3-Daten von gekauften oder selbst gerippten MP3-Dateien entsprechen selten den eigenen Vorstellungen, Cover-Informationen fehlen etc. Es gibt unzählige Programme, die dabei helfen, ID3-Parameter effizient einzustellen bzw. zu verändern (suchen Sie in Ihrem Paketmanager nach *id3*). Persönlich ist mir das Programm EasyTAG am liebsten. Es erlaubt es, schnell alle MP3-Dateien eines Verzeichnisses gemeinsam zu bearbeiten.

Die Bedienung des Programms ist allerdings gewöhnungsbedürftig. Nach dem Start wählen Sie das Verzeichnis aus, in dem sich die MP3-Dateien befinden. EasyTAG liest nun alle MP3-Dateien in diesem Verzeichnis *und* in allen Unterverzeichnissen ein. Sie können dann eine einzelne MP3-Datei auswählen und deren ID3-Tags verändern (siehe Abbildung 10.10). Zur Einstellung gemeinsamer Eigenschaften ist es allerdings effizienter, mehrere bzw. mit Strg+A alle MP3-Dateien des aktuellen Verzeichnisses zu markieren und dann das Album, den Komponisten etc. neu einzustellen. Aus Sicherheitsgründen müssen Sie nun jede Änderung durch einen Klick auf den winzigen Button rechts vom Einstellungsfeld bestätigen – andernfalls gelten die Änderungen nur für die gerade aktive Datei, nicht für alle markierten Dateien. Anfangs werden Sie diesen zusätzlichen Mausklick sicher hin und wieder vergessen.

Um in MP3-Dateien das Bild des CD-Covers zu speichern, markieren Sie alle betreffenden Dateien, wechseln in EasyTAG in das Dialogblatt BILDER, laden mit dem Plus-Button eine neue Bilddatei (JPEG oder PNG) und wählen das geladene Bild aus. EasyTAG sucht die Bilddatei standardmäßig im selben Verzeichnis, in dem sich auch

die gerade bearbeiteten MP3-Dateien befinden. Vergessen Sie nun nicht, auf den winzigen Bestätigungs-Button zu klicken, damit das Bild in *allen* ausgewählten MP3-Dateien gespeichert wird! Anders als die meisten Audio-Player bietet EasyTAG leider keine Funktion, um nach Covern im Internet zu suchen – das müssen Sie selbst erledigen. Besonders komfortabel gelingt das mit dem Programm Coverfinder.

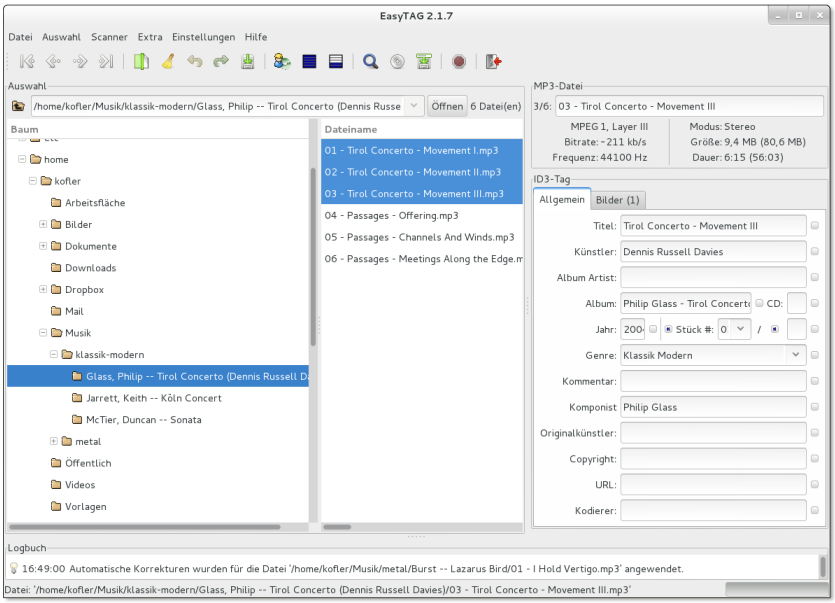


Abbildung 10.10 ID3-Tags neu einstellen

Im Einstellungsdialog können Sie angeben, in welcher ID3-Version die Tags geschrieben werden sollen, welcher Zeichensatz zur Anwendung kommen soll etc.

CD-Ripper

Sound Juicer

Das Gnome-Programm Sound Juicer spielt Audio-CDs ab bzw. liest die Tracks der CDs aus und speichert sie als Dateien im MP3-, Ogg-Vorbis- oder in einem anderen Format. Sound Juicer greift beim Erstellen der Audio-Dateien über das GStreamer-System auf externe Programme zurück, beispielsweise auf `oggenc` für Ogg-Dateien, `lame` für MP3-Dateien, `faac` für AAC-Dateien (`*.m4a`) etc. Standardmäßig erzeugt Sound Juicer Ogg-Dateien, deren Namen sich so zusammensetzen:

`Musik/`*`Gruppe/CD-Name/nn - Track-Titel`*`.ogg`

Die Verzeichnishierarchie und das Audio-Format stellen Sie mit BEARBEITEN • EINSTELLEN ein. Wenn Ihr gewünschtes Audio-Format nicht zur Auswahl steht, müssen Sie dafür ein neues Profil erstellen. Entscheidend ist die Zeile im Eingabe-

feld GStreamer-Weiterleitung. Das folgende Kommando erzeugt mit `lame` MP3-Dateien und kann als Muster dienen. Sämtliche Optionen müssen in einer einzigen Zeile angegeben werden!

```
audio/x-raw-int,rate=44100,channels=2 ! lame name=enc mode=0
  vbr-quality=6 ! id3v2mux
```

KDE-CD-Ripper

Unter KDE gibt es keinen eigenen CD-Ripper mehr. Das ehemals für diesen Zweck konzipierte Programm KAudioCreator wird nicht mehr gewartet. Das heißt aber nicht, dass Sie keine Audio-CDs rippen können, ganz im Gegenteil! Sie können Audio-CDs direkt mit Amarok Ihrer Musiksammlung hinzufügen bzw. Dolphin oder Konqueror verwenden, um WAV-, Ogg- oder MP3-Dateien zu erzeugen: Dazu klicken Sie in der Seitenleiste des Dateimanagers die Audio-CD an. Der Dateimanager zeigt nun mehrere virtuelle Verzeichnisse an, die scheinbar bereits MP3-, Ogg-Vorbis- oder Flac-Dateien enthalten (siehe Abbildung 10.11). Tatsächlich werden diese Dateien erst erzeugt, wenn Sie sie per Drag&Drop in ein Verzeichnis der Festplatte kopieren.

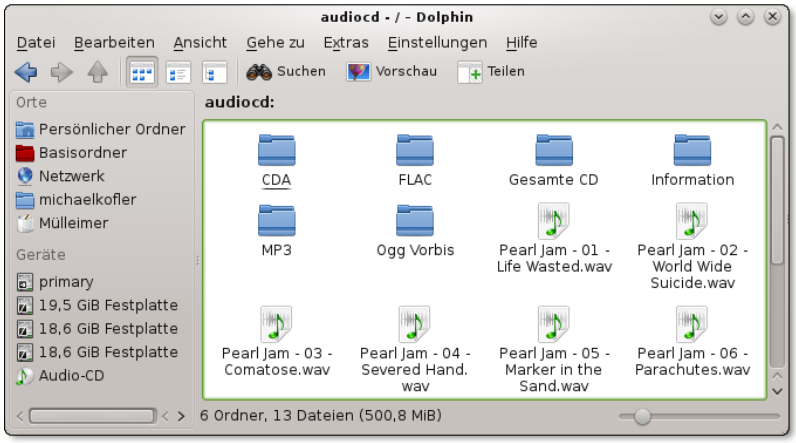


Abbildung 10.11 Virtuelle Audio-Verzeichnisse im KDE-Dateimanager

10.6 DVDs rippen und kopieren

Dieser Abschnitt stellt einige Programme vor, um DVDs zu rippen und zu kopieren. Dazu vorweg eine Leseempfehlung: *Brother Johns Encodingwissen* fasst fachlich fundiert und sprachlich unterhaltsam zusammen, was man wissen sollte, wenn man DVDs auslesen und daraus MPEG-4-Video-Dateien erzeugen möchte, also umgangssprachlich DVD-Ripping betreibt:

http://encodingwissen.de

Hinweis

Die hier vorgestellten Programme lesen DVDs aus. Das ist natürlich nur für DVDs zulässig, die keinen fremden Copyrights unterliegen – also z. B. für Ihre nicht verschlüsselte DVD mit einem Hochzeits- oder Kinder-Video (»Leos erste Schritte«). Keinesfalls dürfen Sie diese Werkzeuge verwenden, um irgendwelche Blockbuster zu kopieren oder der Video-Sammlung Ihres privaten Media-Centers hinzuzufügen. Welcher meiner Leser würde auf derart verwerfliche Ideen kommen? Lesen Sie lieber ein Buch!

Grundlagen

Wenn Sie eine DVD unterwegs ansehen möchten, Ihr Notebook aber kein DVD-Laufwerk besitzt, übertragen Sie den Film am besten auf die Festplatte. Um Platz zu sparen, erzeugen Sie dabei eine neue Filmdatei, die die Video- und Audio-Daten enthält. Dieser Vorgang wird als DVD-Ripping bezeichnet. Es gibt schier unendlich viele Varianten, wie das Ripping durchgeführt wird. Wichtige Parameter sind:

- der Audio-Codec (z. B. MP3, Ogg Vorbis, AAC, AC-3)
- der MPEG-4-Codec (z. B. DivX, H264, Ogg Theora, WebM, Xvid)
- das Container-Format (z. B. AVI, MKV, MOV, MP4, OGM)
- das Untertitel-Format (z. B. SRT, VobSub)
- Qualitätsfaktoren und Komprimierung

Anders als bei einer DVD, wo die Audio-Kanäle und Untertitel oft in mehreren Sprachen parallel zur Verfügung stehen, müssen Sie sich bei der Erstellung einer Filmdatei zumeist für *eine* Sprache entscheiden. Um Platz zu sparen, ist es zumeist auch zweckmäßig, auf Zusatzmaterial (Bonus-Kapitel, Trailer etc.) zu verzichten.

Bleibt noch die Qualitätsfrage: Wie groß darf die resultierende Datei maximal werden? Manche Programme sind dahingehend voreingestellt, 700 MByte nicht zu überschreiten, damit der Film auf einer CD Platz findet. Das war vielleicht vor zehn Jahren sinnvoll, ist aber im Zeitalter von Terabyte-Festplatten übertrieben. Sie verlieren so spürbar an Bildqualität! Wenn Sie die Originalqualität einer DVD erhalten wollen, müssen Sie bis zu 1 GByte pro Stunde Filmlänge veranschlagen. Wenn es sich dagegen um eine TV-Sendung handelt, die Sie vor 15 Jahren auf ein VHS-Band aufgenommen und vor 5 Jahren auf eine DVD überspielt haben, reichen auch rund 300 MByte/h vollkommen aus, um die ohnedies schon geringe Ausgangsqualität zu erhalten.

Wenn der resultierende Film eine hohe Qualität haben soll, müssen Sie für das Ripping oft wesentlich mehr Zeit veranschlagen, als der Film lang ist. Ein Rechner mit einer schnellen CPU ist hier definitiv zweckmäßig!

DVDs rippen

OGMrip

DVD-Ripping per Kommandozeile ist nur etwas für hartgesottene Linux-Anwender. Die Mühe lohnt nicht, zumal gleich eine ganze Palette von Benutzeroberflächen zur Auswahl steht, um bei der Einstellung der Parameter zu helfen. Mein persönlicher Favorit ist OGMrip mit einer minimalistischen Benutzeroberfläche: Sie wählen aus, welchen Titel der DVD Sie rippen möchten (in der Regel einfach den längsten), welche Sprachen für die Tonspur und die Untertitel verwendet werden sollen und welche Kapitel des Films berücksichtigt werden sollen (zumeist alle).

Mit AUSLÖSEN starten Sie die Filmproduktion, wobei Sie die Wahl zwischen verschiedenen Qualitätsstufen haben (siehe Abbildung 10.12). Mit BEARBEITEN • PROFILES können Sie die vorhandenen Qualitätsstufen verändern oder neue definieren.

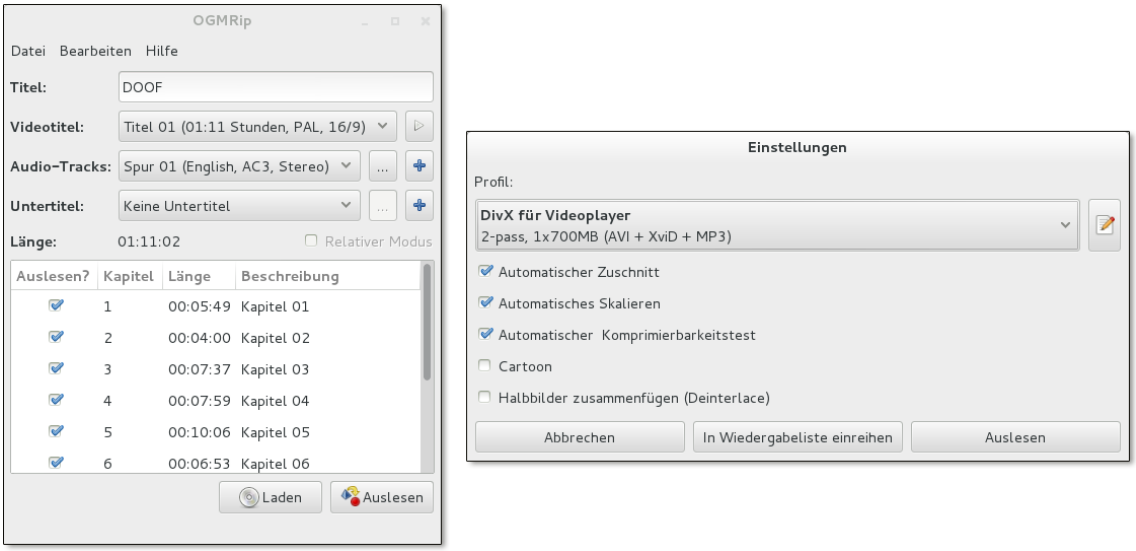


Abbildung 10.12 DVDs auslesen mit OGMrip

Wenn Sie mit OGMrip eine ISO-Datei verarbeiten möchten, müssen Sie diese zuerst in das Dateisystem einbinden (`mount -o loop datei.iso verzeichnis`) und das Verzeichnis dann mit DATEI • ÖFFNEN laden.

AcidRip

Populäre Alternativen zu OGMrip sind AcidRip und dvd::rip. Wer schon etwas Erfahrung mit DVD-Ripping hat, der wird mit AcidRip rasch ans Ziel kommen. Die technisch orientierte Benutzeroberfläche bietet viele Einstellmöglichkeiten, wirkt allerdings anfänglich unübersichtlich. Praktisch ist die Vorschaumöglichkeit, sodass Sie überprüfen können, welcher Titel der DVD was enthält.

dvd::rip

Sehr gewöhnungsbedürftig ist dvd::rip: Dieses Programm ist eindeutig für fortgeschrittene Ripping-Anwender konzipiert und entsprechend unübersichtlich zu bedienen. Dafür setzt sich das Programm in zwei Punkten von der Konkurrenz ab: Sie haben detaillierten Einfluss auf die Cropping-Funktionen, also auf das Ausschneiden des sichtbaren Teils des Films, und können die zeitraubende Erzeugung der Video-Dateien auf mehrere Rechner verteilen.

HandBrake

Das Programm HandBrake ist momentan unter Mac-OS-X-Anwendern bekannter als unter Linux – aber das wird sich möglicherweise in Zukunft ändern: Die Linux-Version dieses Programms kann durchaus überzeugen. Sie stellt unter anderem einige vordefinierte Konvertierungsprofile zur Auswahl, die für das Abspielen der Filme auf verschiedenen Apple-Geräten optimiert sind. Für meine Tests habe ich das Programm aus einem PPA (Personal Package Archive) für Ubuntu installiert:

```
root#  add-apt-repository ppa:stebbins/handbrake-releases
root#  apt-get update && apt-get install handbrake-gtk
```

Die Bedienung ist einfach: Sie geben eine Filmquelle (DVD, Film- oder ISO-Datei) an, legen fest, unter welchem Dateinamen der recodierte Film gespeichert werden soll, und wählen ein vordefiniertes Einstellungsprofil aus. Mit dem START-Button beginnen Sie dann die Recodierung.

DVDs kopieren

DVD95 und K9Copy

DVDs können Sie nicht auf Dateisystemebene kopieren, weil sich ein Teil der DVD-Daten außerhalb des Dateisystems befindet. Ein gangbarer Weg besteht hingegen darin, durch direktes Auslesen ein exaktes Abbild der DVD zu erzeugen und diese dann auf eine leere DVD zu brennen. Allerdings sind viele DVDs aus Platzgründen zweilagig (DVD9 oder DVD-DL).

Wenn das Video auf einer gewöhnlichen DVD Platz finden soll, werfen Sie einen Blick auf DVD95 (Gnome) oder K9Copy (KDE): Diese Programme erstellen eine DVD-Kopie, wobei sie den Datenumfang bei Bedarf so weit reduzieren, dass der Film auf einer DVD5 Platz findet. Dazu können einzelne DVD-Tracks und Audio-Spuren weggelassen werden. Wenn das nicht reicht, werden die Video-Tracks mit einer stärkeren Komprimierung recodiert, was aber je nach der Gesamtlänge des Videos und der Art des Films sichtbare Qualitätsverluste mit sich bringen kann. Besonders gut funktioniert die Komprimierung übrigens bei Zeichentrickfilmen, deren Bildqualität nahezu unverändert bleibt.

Obwohl beide Programme prinzipiell dieselben Funktionen bieten, ziehe ich auch unter Gnome K9Copy wegen der wesentlich einfacheren Bedienung vor.

10.7 Screencasts aufnehmen

Als »Screencast« bezeichnet man den Video-Mitschnitt des Bildschirminhalts. In der Regel kann auch ein Audio-Kanal mit aufgezeichnet werden. Screencasts eignen sich hervorragend, um Programmfunktionen zu dokumentieren. Unter Linux herrscht kein Mangel an Programmen zur Aufnahme von Screencasts, ganz im Gegenteil: Es gibt zu viele! Die folgende Seite zählt gleich neun verschiedene Programme bzw. Scripts auf:

http://wiki.ubuntuusers.de/Screencasts

Aber wenn man sich die Programme näher ansieht, bemerkt man rasch, dass die große Auswahl nicht wirklich weiterhilft. Viele Programme sind uralt und werden nicht mehr gewartet; die Grafikeffekte der Gnome Shell oder von Unity können nicht aufgezeichnet werden, in der resultierenden Video-Datei sind Bild und Ton nicht synchron etc. Kurzum, das Testen ist eine frustrierende Angelegenheit.

Screencasts unter Gnome

Bei aktuellen Gnome-Versionen ist eine Screencast-Funktion direkt in die Gnome Shell eingebaut. ⇧+Strg+Alt+R startet die Aufnahme. Wird diese Tastenkombination ein zweites Mal gedrückt wird, endet die Aufzeichnung. Die resultierende Datei im WebM-Format wird im Verzeichnis `Videos` gespeichert.

Leider gibt es zu dieser Screencast-Funktion keinerlei Konfigurationsmöglichkeiten. Standardmäßig wird kein Audio-Signal mitaufgezeichnet. Das lässt sich nur durch eine direkte Veränderung der dconf-Einstellungen für `org.gnome.shell.recorder` beheben. Details können Sie hier nachlesen:

http://askubuntu.com/questions/112473

recordMyDesktop

Das bekannteste Screencasting-Programm ist recordMyDesktop. Es kann auf den meisten Distributionen installiert werden und funktioniert im Wesentlichen zufriedenstellend. Der größte Mangel ist der Umstand, dass das Programm ausschließlich freie Formate unterstützt (Ogg-Container, Theora-Video-Codec, Vorbis-Audio-Codec). An sich ist das natürlich lobenswert, aber wenn die Aufnahme später in einem kommerziellen Umfeld weiterverarbeitet werden muss (sprich unter Windows oder OS X), macht man sich mit diesen Codecs wenig Freunde. Gegen recordMyDesktop spricht auch der Umstand, dass die aktuelle Version aus dem Jahr 2008 stammt. Das Programm wird zwar anscheinend noch gewartet, aber nicht mehr weiterentwickelt.

Kazam

Kazam ist im Gegensatz zu recordMyDesktop ein relativ neues Screencasting-Programm, das aktiv entwickelt wird. Kurz die wichtigsten Features:

- Kazam kommt mit 3D-Desktops zurecht.
- Kazam unterstützt die Aufnahmeformate H264/MP4, VP8/WebM und RAW/AVI.

- Es können zwei Audio-Kanäle aufgezeichnet werden.
- Die Framerate ist frei einstellbar (standardmäßig 15 Bilder/Sekunde).
- Der aufzuzeichnende Bildschirmbereich ist frei einstellbar. Bei einer Dual-Screen-Konfiguration ist es problemlos möglich, nur den Inhalt eines Monitors aufzuzeichnen.

Leider steht das Programm momentan nur unter Ubuntu standardmäßig als Paket zur Verfügung. Wer mit anderen Distributionen arbeitet, muss sich mit einer manuellen Installation plagen.

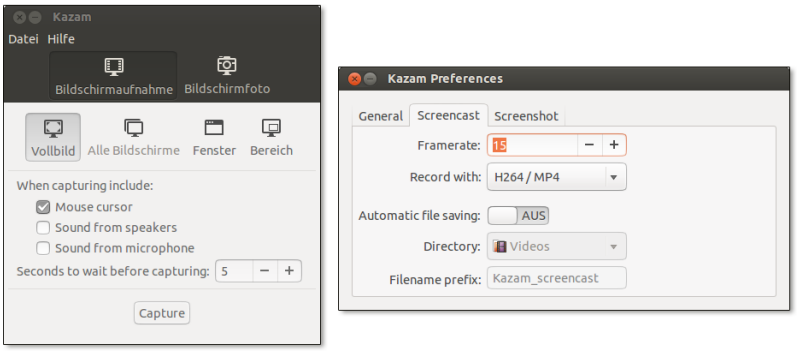


Abbildung 10.13 Aufnahmeeinstellungen in Kazam

Kapitel 11
VirtualBox

Virtualisierung macht es möglich, auf einem Rechner mehrere Betriebssysteme parallel auszuführen. Daraus ergeben sich unzählige Anwendungen: Sie können Linux unter Windows ausprobieren, Windows unter Linux ausführen, eine neue Alpha-Version der Distribution xyz gefahrlos testen, ohne die vorhandene Linux-Installation zu gefährden, Server-Funktionen sicher voneinander trennen etc.

Dieses Kapitel gibt einen Überblick über Virtualisierungsgrundlagen und -programme und konzentriert sich dann ganz auf VirtualBox. Zur Server-Virtualisierung ist KVM besser geeignet (siehe Kapitel 43).

11.1 Virtualisierungsgrundlagen

Dieser Abschnitt erklärt, warum es so viele unterschiedliche Virtualisierungsprogramme gibt, auf welchen Techniken sie basieren und welches Programm für welchen Zweck geeignet ist. Wenn es Ihnen primär darum geht, rasch eine virtuelle Windows-Maschine unter Linux einzurichten oder Linux unter Windows auszuführen, überspringen Sie diesen Grundlagenabschnitt und lesen in Abschnitt 11.2 weiter.

Virtualisierungstechniken

Gast und Wirt

Bei der Beschreibung von Virtualisierungssystemen hat es sich eingebürgert, das Grundsystem als Wirt (*Host*) und die darauf laufenden virtuellen Maschinen als Gäste (*Guests*) zu bezeichnen.

Virtualisierungstechniken

Zur Virtualisierung von Betriebssystemen existieren verschiedene Verfahren. Die folgende Liste fasst die gängigsten Virtualisierungstechniken zusammen und nennt einige populäre Programme bzw. Firmen, die diese Techniken nutzen.

- **Vollvirtualisierung (virtuelle Maschinen, Emulation):** Hier simuliert ein Programm virtuelle Hardware, also einen Rechner, der aus CPU, RAM, Festplatte, Netzwerkkarte etc. besteht. Für die Gastsysteme sieht es so aus, als würde die

virtuelle Hardware real existieren. Damit das funktioniert, muss das Virtualisierungsprogramm des Wirts den Code des Gasts überwachen und bestimmte Anweisungen durch anderen Code ersetzen. Diese Aufgabe übernimmt der sogenannte *Hypervisor*. Der Hypervisor ist aber auch für die Speicher- und Prozessverwaltung und andere hardware-nahe Funktionen verantwortlich.

Vorteile: Nahezu jedes Betriebssystem kann innerhalb der virtuellen Maschine ausgeführt werden. Das Betriebssystem muss dazu nicht verändert werden.

Nachteile: Relativ langsam.

Programme/Firmen: QEMU, VMware, VirtualBox etc.

- **Virtualisierung mit Hardware-Unterstützung:** Moderne CPUs von Intel und AMD enthalten hardware-seitig Funktionen zur Vereinfachung von Virtualisierungstechniken. Intel nennt diese Technik *Intel-VT* (ehemals *Vanderpool*), AMD taufte seine Funktionen *AMD-V* (ehemals *Pacifica*).

  Vorteile: Deutlich effizienter.

  Nachteile: Erfordert spezielle Prozessoren.

  Programme/Firmen: KVM, VMware, VirtualBox etc.

- **Paravirtualisierung mit Treibern:** Auch hier stellt der Wirt virtuelle Maschinen zur Verfügung, in denen die Gäste laufen. Der Unterschied besteht darin, dass das Gastbetriebssystem für die Virtualisierung modifiziert sein muss und über spezielle Treiber direkt mit dem VMM kommuniziert. Man könnte also sagen: Das Gastsystem hilft bei der Virtualisierung mit.

  Vorteile: Effizient.

  Nachteile: Erfordert speziell für das Virtualisierungssystem modifizierte Gäste. Das ist für Open-Source-Systeme wie Linux kein großes Problem; bei kommerziellen Betriebssystemen ist aber eine gute Kooperation zwischen dem Betriebssystemhersteller und dem Hersteller des Virtualisierungsprogramms erforderlich.

  Programme/Firmen: KVM, Xen/Citrix, UML (User-mode Linux)

- **Virtualisierung auf Betriebssystemebene (Containers):** Dieses Verfahren verzichtet auf richtige virtuelle Maschinen. Die Gastsysteme nutzen vielmehr den gemeinsamen Kernel und Teile des Dateisystems des Wirts. Zu den wichtigsten Aufgaben des Virtualisierungssystems zählt es, den Wirt von seinen Gästen zu isolieren, um jede Art von Sicherheitsrisiken zu vermeiden.

  Vorteile: Sehr effizient, spart Ressourcen (RAM, Festplatte etc.).

  Nachteile: Nur geeignet, wenn der Wirt und seine Gäste jeweils exakt dasselbe Betriebssystem bzw. exakt dieselbe Kernelversion nutzen. Das Betriebssystem muss entsprechend modifiziert werden.

Programme/Firmen: OpenVZ, Virtuozzo, Linux-VServer

CPU-Unterstützung

Um festzustellen, ob Ihre CPU bei der Hardware-Virtualisierung hilft (Intel-VT oder AMD-V), führen Sie das folgende `egrep`-Kommando aus. Das hier gezeigte Ergebnis stammt von einer Intel-i7-CPU.

```
user$  egrep '^flags.*(vmx|svm)' /proc/cpuinfo
flags : fpu vme de pse tsc msr pae mce cx8 apic mtrr pge mca cmov pat pse36
        clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx rdtscp lm
        constant_tsc arch_perfmon pebs bts rep_good xtopology nonstop_tsc
        aperfmperf pni pclmulqdq dtes64 monitor ds_cpl  vmx est tm2 ssse3 cx16
        xtpr pdcm sse4_1 sse4_2 popcnt aes xsave avx lahf_lm ida arat epb xsaveopt
        pln pts dts tpr_shadow vnmi flexpriority ept vpid
...
```

Hardware-Virtualisierung im BIOS/EFI aktivieren

Selbst wenn `/proc/cpuinfo` das Flag `vmx` bzw. `svm` aufweist, kann es sein, dass die Virtualisierungsfunktionen der CPU ungenutzt bleiben – dann nämlich, wenn das BIOS bzw. EFI diese deaktiviert. Aus unerfindlichen Gründen ist das erstaunlich oft der Fall. Starten Sie also Ihren Rechner neu, und suchen Sie in den BIOS/EFI-Dialogen nach der entsprechenden Option. Auf dem Mainboard eines meiner Rechner heißt die Option Advanced • Intel Virtualization Technology.

Virtuelle Hardware

Die Emulierung virtueller Hardware ist naturgemäß ein komplexer Prozess. Je nach Virtualisierungsverfahren bzw. je nach Implementierung werden Sie in der Praxis früher oder später an Grenzen stoßen.

RAM

Der Speicher in Ihrem Rechner muss größer sein als die Summe der Anforderungen für das Wirtssystem und alle laufenden Gäste. Je mehr Systeme zugleich laufen sollen, desto mehr RAM brauchen Sie.

Festplatte

Die meisten Virtualisierungssysteme speichern das Dateisystem des Gasts in einer großen Datei des Wirtssystems. Die Gäste greifen somit nicht direkt auf die Festplatte zu, sondern indirekt über das Virtualisierungssystem auf eine Datei. Datenzugriffe im Gast sind deswegen wesentlich langsamer als auf dem Wirtssystem, oft um einen Faktor zwischen zwei und drei.

CD/DVD-Laufwerke

CD- und DVD-Laufwerke werden vom Wirt an den Gast durchgereicht. Der Zugriff ist allerdings oft read-only. Nur wenige Virtualisierungssysteme lassen das Brennen von CDs/DVDs durch das Gastsystem zu.

Die meisten Virtualisierungsprogramme bieten dafür die Möglichkeit an, dem virtuellen CD/DVD-Laufwerk eine ISO-Datei zuzuordnen. Anstatt das reale Laufwerk zu

nutzen, greift der Gast nun auf die ISO-Datei zu. Gerade für wiederholte Installationen ist das außerordentlich praktisch, effizient und leise. Bei Bedarf können Sie eine ISO-Datei ganz einfach selbst aus einer CD/DVD extrahieren:

```
root# dd if=/dev/scd0 of=datei.iso bs=2048
```

Grafikkarte

Um die Grafikfunktionen einigermaßen effizient zu nutzen, muss auf jedem Gastsystem ein spezieller Treiber installiert werden, der auf die Virtualisierungssoftware des Wirts abgestimmt ist. Einschränkungen gibt es bei vielen Virtualisierungssystem bei der Nutzung von 3D-Funktionen. Das führt dazu, dass moderne Desktop-Systeme wie die Gnome Shell oder Unity gar nicht oder nur sehr langsam ausgeführt werden.

Audio-Funktionen

Die meisten Virtualisierungsprogramme stellen dem Gast eine virtuelle Audio-Karte zur Verfügung und leiten Audio-Ausgaben an das Audio-System des Wirts weiter. Solange Sie keine besonderen Ansprüche an das Audio-System stellen (Surround-Effekte etc.), funktioniert das gut.

USB-Geräte, externe Hardware

Tastatur- und Mauseingaben werden vom Wirt an den Gast übertragen. Welchen Zugriff Gäste auf sonstige externe Geräte haben, variiert sehr stark je nach Virtualisierungssystem. USB-Geräte werden leider von vielen Virtualisierungssystemen nicht oder nur mit großen Einschränkungen unterstützt; z. B. ist häufig kein Zugriff auf USB-Datenträger möglich.

Uhrzeit

Obwohl es trivial erscheint, haben manche Virtualisierungssysteme Probleme mit der Synchronisierung der Uhrzeit. Das Problem besteht darin, dass zumeist CPU-Taktzyklen zur Messung der Zeit verwendet werden. Der virtuellen Maschine fehlt aber oft die Information, mit welcher Taktfrequenz die *echte* CPU läuft. Außerdem können virtuelle Maschinen natürlich angehalten werden. Abhilfe schaffen spezielle Uhrzeittreiber, die die Zeit von Host und Gast abgleichen.

Netzwerkanbindung der virtuellen Maschinen

Das Virtualisierungssystem stellt seinen Gästen die Netzwerkinfrastruktur des Wirts zur Verfügung, normalerweise in Form einer virtuellen Netzwerkkarte. Es existieren unterschiedliche Verfahren, wie der Netzwerkverkehr von der virtuellen Netzwerkkarte in das reale Netzwerk geleitet wird. Sie können auch mehrere virtuelle Netzwerkadapter definieren, die über unterschiedliche Verfahren kommunizieren – gerade so, wie auch ein echter Rechner mehrere Netzwerkadapter haben kann, z. B. für LAN und WLAN.

Im Folgenden verwende ich die Nomenklatur von VirtualBox. Beachten Sie, dass nicht jedes Virtualisierungsprogramm alle Varianten kennt bzw. diese bisweilen anders bezeichnet.

- **Netzwerkbrücke:** Beim Bridged Networking erscheint der Gast als zusätzlicher Client im lokalen Netz. Diese Variante ist optimal, wenn es im lokalen Netzwerk einen DHCP-Server gibt bzw. wenn der Wirtsrechner mit einem ADSL- oder WLAN-Router verbunden ist. Die virtuellen Gäste beziehen ihre Netzwerkkonfiguration dann über diesen Server/Router und können sowohl auf das lokale Netzwerk als auch auf das Internet zugreifen. Wenn Ihr Wirtsrechner mehrere Netzwerkschnittstellen besitzt, müssen Sie angeben, welche Schnittstelle die Verbindung zum LAN herstellt.
- **NAT:** Bei der NAT-Variante fungiert das Virtualisierungssystem für seine Gäste selbst als DHCP-Server und führt Masquerading-Funktionen aus (siehe auch Kapitel 30). Auf diese Weise können die Gäste den Internetzugang des Wirtssystems nutzen. Ein Zugang zum lokalen Netzwerk ist wegen der unterschiedlichen Adressbereiche für das lokale Netz und das virtuelle NAT-Netz des Virtualisierungssystems unmöglich.
- **Host-only Networking:** Beim Host-only Networking kann der Gast über die Netzwerkfunktionen nur mit dem Wirt kommunizieren, nicht aber mit anderen Rechnern im lokalen Netzwerk oder mit dem Internet. Diese Variante ist dann zweckmäßig, wenn Sie ein von außen nicht zugängliches Testsystem aus mehreren virtuellen Maschinen aufbauen möchten.
- **Internes Netzwerk:** Das Virtualisierungsprogramm bildet ein virtuelles Netzwerk, in dem ausschließlich virtuelle Maschinen kommunizieren können. Sie haben bei dieser Variante weder Zugriff auf das lokale Netzwerk noch auf das Internet.

Datenaustausch zwischen Wirt und Gast

Grundsätzlich gilt: Ein Gast darf nicht direkt auf eine Festplatte zugreifen, die vom Wirt genutzt wird. Es kann nicht sein, dass zwei Betriebssysteme gleichzeitig den Festplatten-Controller steuern – Datenverluste wären unausweichlich. Deswegen simuliert die Virtualisierungssoftware auf dem Wirt für den Gast eine Festplatte und kümmert sich selbst darum, diese virtuelle Festplatte in Dateien des Wirtssystems abzubilden. Das bedeutet aber: Der Wirt kann nicht direkt auf das Dateisystem des Gasts zugreifen und umgekehrt.

Netzwerkverzeichnisse

Der schnellste Weg zum Datenaustausch führt deswegen über Netzwerkverzeichnisse. Am einfachsten ist es, wenn auf dem Wirt oder auf einem externen Rechner, der sowohl vom Wirt als auch von den Gästen via Netzwerk erreichbar ist, ein NFS- oder

Samba-Server läuft. Manche Virtualisierungsprogramme bieten derartige Funktionen selbst (Shared Folders etc.), was meinen Erfahrungen nach aber wenig Vorteile bietet und die Konfiguration komplizierter als notwendig macht.

Zwischenablage

Viele Virtualisierungsprogramme erlauben den Austausch markierten Texts über die Zwischenablage. Leider funktioniert das oft eher schlecht als recht. Schuld ist teilweise das Grafiksystem X, das zwischen der Ad-hoc-Zwischenablage für den gerade markierten Text und der Zwischenablage für den zuletzt mit Strg+C kopierten Text unterscheidet. Bisweilen ist unklar, welche dieser Zwischenablagen für das Virtualisierungssystem Gültigkeit hat. Außerdem beschränkt sich die Funktion der Zwischenablage auf reinen Text. Wer rasch ein Excel-Diagramm aus einem Windows-Gast in ein OpenOffice-Writer-Dokument auf dem Wirtsrechner kopieren will, der wird enttäuscht sein.

Virtualisierungsprogramme

Das Angebot an Virtualisierungsprodukten, sowohl im kommerziellen als auch im Open-Source-Segment, ist unübersichtlich groß. Die folgende Aufzählung nennt ganz kurz die wichtigsten Mitstreiter im Virtualisierungsmarkt. In Klammern ist jeweils angegeben, ob es sich um Open-Source-Software oder um kommerzielle Produkte handelt und welche Firma die Entwicklung vorantreibt bzw. die resultierenden Produkte vertreibt.

- **VMware (kommerziell, EMC):** Die Firma VMware ist unumstrittener Marktführer im kommerziellen Virtualisierungsmarkt. Die Palette der Virtualisierungsprodukte deckt sowohl den Desktop- als auch den Server-Bereich ab. Einzelne Programme sind zwar kostenlos verfügbar, aber nicht als Open-Source-Code. Als Wirtssystem werden Linux, Windows und vereinzelt Mac OS X unterstützt.
- **VirtualBox (teilweise Open Source, Oracle):** Das Programm VirtualBox bietet ähnliche Funktionen wie VMware Workstation, eignet sich also zur Desktop-Virtualisierung. Als Wirtssystem werden Linux, Windows und Mac OS X unterstützt. VirtualBox ist für Privatanwender kostenlos; außerdem gibt es eine Open-Source-Version, die im Rahmen der GPL auch kommerziell genutzt werden kann. VirtualBox harmonisiert zumeist gut mit den jeweils neuesten Kernel- und X-Versionen.
- **KVM/QEMU (Open Source, Red Hat):** KVM ist eigentlich nur ein Kernelmodul, das die bis dahin sehr langsame Emulationssoftware QEMU auf modernen CPUs enorm beschleunigt. Seit KVM offiziell in den Kernel integriert ist und Red Hat die KVM-Firma Qumranet gekauft hat, gewinnt KVM enorm an Bedeutung und gilt als Standard-Virtualisierungslösung für Fedora, Ubuntu und natürlich für die Version 6 von Red Hat Enterprise Linux. KVM ist besonders gut für die Server-

Anwendung geeignet. Als Wirtssystem wird nur Linux unterstützt. Detaillierte Informationen zu KVM finden Sie in Kapitel 43.

- **Xen (teilweise Open Source, Citrix):** Xen ist ein Hypervisor, der ohne Betriebssystem ausgeführt wird. Die virtualisierten Gäste laufen in sogenannten Domänen (`domU`), wobei die erste Domäne (`dom0`) besondere Privilegien hat und in gewisser Weise mit dem Wirtssystem bei anderen Virtualisierungsprodukten vergleichbar ist. Wie KVM ist Xen für die Server-Virtualisierung optimiert und setzt ein Linux-Wirtssystem voraus.
- **OpenVZ und Virtuozzo (teilweise Open Source, Parallels) sowie Linux-VServer (Open Source):** OpenVZ, das darauf basierende kommerzielle Produkt Virtuozzo und die technisch ähnliche Virtualisierungslösung VServer ermöglichen es, mehrere isolierte Umgebungen auf der Basis einer Linux-Distribution auszuführen. OpenVZ bzw. Virtuozzo gehen davon aus, dass es sich beim Wirt und seinen Gästen um dieselbe Linux-Version handelt. Dieses Konzept eignet sich dazu, mehrere (viele!) gleichartige Server zu virtualisieren. Es wird teilweise von Internet-Hosting-Providern genutzt, um kostengünstig virtuelle Root-Server anzubieten.
- **Hyper-V (kommerziell, Microsoft):** Microsoft ist recht spät in den Virtualisierungsmarkt eingestiegen. Hyper-V setzt ein Windows-Server-System als Wirtssystem voraus, unterstützt Linux aber immerhin als Gastsystem und hat dafür sogar eigene Linux-Kerneltreiber als Open-Source-Code entwickelt – ein Schritt, der Microsoft sicher schwergefallen ist.

Kompatibilität zwischen den Systemen

Grundsätzlich müssen Sie leider davon ausgehen, dass Virtualisierungssysteme zueinander inkompatibel sind. Ein Gastsystem, das Sie unter VMware installiert haben, können Sie daher nicht mit Xen nutzen. Zu dieser Inkompatibilität führen zwei Faktoren: Die Formate der virtuellen Festplatten sind unterschiedlich, und je nach Virtualisierungssystem sind im Gastsystem unterschiedliche Zusatztreiber, Kernelerweiterungen etc. erforderlich.

Empfehlungen

Mein persönlicher Favorit für die einfache Desktop-Virtualisierung ist VirtualBox. Das Programm läuft unter Linux, Windows und OS X, ist kostenlos verfügbar und einfach zu bedienen. Was will man mehr?

In den vergangenen Jahren habe ich Virtualisierung vermehrt auch im Server-Bereich eingesetzt. Auch hier bin ich natürlich bei einer Open-Source-Lösung gelandet: KVM. Meine Erfahrungen mit KVM habe ich zuerst in einem eBook und später zusammen mit Ralf Spenneberg in dem Buch *KVM für die Server-Virtualisierung* dokumentiert (Addison Wesley 2012, ISBN 978-3-8273-3149-6).

11.2 VirtualBox auf einem Linux-Host installieren

VirtualBox ist ein Desktop-Virtualisierungssystem, das unter Linux, Windows, Solaris und Mac OS X läuft. Als Gastsystem werden nahezu alle gängigen Betriebssysteme für x86-Hardware unterstützt, unter anderem auch Windows 8, Solaris und OpenBSD.

Hinter VirtualBox stand ursprünglich die Firma InnoTek. 2008 übernahm Sun InnoTek, und 2010 kaufte Oracle Sun. Damit ist nun Oracle der Eigentümer von VirtualBox. Umfassende Dokumentation zu VirtualBox finden Sie unter:

http://www.virtualbox.org

Licht ...

VirtualBox kann den Gästen mehrere Cores/CPUs weiterreichen, unterstützt in manchen Konfigurationsvarianten 3D-Funktionen im Gast, kann Snapshots durchführen etc. Die größten Stärken von VirtualBox gegenüber anderen Open-Source-Virtualisierungsprogrammen (KVM, Xen etc.) sind die relativ einfache Benutzeroberfläche und die gut organisierte Dokumentation. Das macht gerade Einsteigern das Leben leicht.

... und Schatten

Trotz aller Vorzüge ist leider auch VirtualBox nicht frei von Problemen: Die Stabilität des Programms könnte besser sein. Abstürze virtueller Maschinen kommen leider immer wieder vor. Besonders verärgert sind die Kernelentwickler über VirtualBox: Sie betrachten die Kernelmodule von VirtualBox als besonders fehleranfällig und bezeichnen sie wörtlich als *crap*:

http://www.phoronix.com/vr.php?view=OTk5Mw
https://lkml.org/lkml/2011/10/6/317

VirtualBox-Pakete Ihrer Distribution

VirtualBox unter Linux installieren

Die meisten Distributionen bieten fertige VirtualBox-Pakete an. Bei Fedora müssen Sie auf die `rpmfusion`-Paketquelle zurückgreifen. Bei openSUSE befinden sich die Kernfunktionen und die Benutzeroberfläche in getrennten Paketen, deswegen müssen Sie auch das Paket `virtualbox-qt` installieren.

VirtualBox-Kernelmodule

VirtualBox greift auf dem Wirtssystem auf die drei Kernelmodule `vboxdrv`, `vboxnetadp` und `vboxnetflt` zurück. Manche Distributionen stellen diese Module in binärer Form durch ein eigenes Paket zur Verfügung, das bei jedem Kernel-Update aktualisiert wird. Bei Fedora lautet der Paketname `kmod-VirtualBox`, bei openSUSE `virtualbox-host-kmp-desktop`.

Fehlt ein derartiges Paket, wird einfach der Quellcode der VirtualBox-Pakete installiert. Vor der ersten Verwendung von VirtualBox sowie nach jedem Kernel-

Update auf dem Host müssen Sie die VirtualBox-Module neu kompilieren. Je nach Distribution sieht das erforderliche Kommando z. B. so aus:

```
root#  service vboxdrv setup
```

Der Quellcode für die Kernelmodule wird zusammen mit VirtualBox installiert. Zum Kompilieren sind aber auch der C-Compiler `gcc` sowie die Kernel-Header-Dateien erforderlich. Bei Ubuntu sind diese Voraussetzungen standardmäßig erfüllt, bei anderen Distributionen müssen Sie die entsprechenden Pakete installieren (siehe Abschnitt 28.1).

VirtualBox-Pakete von Oracle

Statt der mit Ihrer Distribution mitgelieferten VirtualBox-Pakete können Sie auch die von Oracle zum Download angebotene Version installieren. Das ist vor allem dann zweckmäßig, wenn Oracle eine neuere VirtualBox-Version anbietet als Ihre Distribution.

http://www.virtualbox.org/wiki/Linux_Downloads

Auf der obigen Website finden Sie VirtualBox in verschiedenen Formaten: als RPM- und Debian-Paket für diverse Distributionen sowie als Universal-Installer, den Sie wie folgt starten:

```
root#  chmod u+x VirtualBox_nnn.run install
root#  ./VirtualBox_nnn.run install
```

Um das Kompilieren der Kernelmodule müssen Sie sich selbst kümmern:

```
root#  service vboxdrv setup
```

Nach Möglichkeit sollten Sie vor VirtualBox das `dkms`-Paket installieren. In diesem Fall verwaltet DKMS die VirtualBox-Module und kümmert sich bei Kernel-Updates automatisch um eine Neukompilierung (siehe Abschnitt 28.1). Bei meinen VirtualBox-Installationen hat das allerdings nicht immer zuverlässig funktioniert.

Oracle-APT-Paketquelle

Für Ubuntu- und Debian-Anwender gibt es eine eigene APT-Paketquelle, die automatische Updates innerhalb der gewählten Major-Version sicherstellt. Dazu fügen Sie zu `/etc/apt/sources.list` eine der folgenden Zeilen hinzu:

```
deb http://download.virtualbox.org/virtualbox/debian precise contrib
deb http://download.virtualbox.org/virtualbox/debian quantal contrib
deb http://download.virtualbox.org/virtualbox/debian raring  contrib
```

Außerdem führen Sie diese beiden Kommandos aus, um den Schlüssel der Paketquelle zu installieren:

```
root#  wget -q http://download.virtualbox.org/virtualbox/debian/oracle_vbox.asc
root#  apt-key add oracle_vbox.asc
```

Anschließend installieren Sie VirtualBox mit `apt-get` oder `aptitude`:

```
root#  apt-get update
root#  apt-get install virtualbox-4.1
```

Oracle-Yum-Paketquelle

Anwender von Yum-kompatiblen Distributionen (Fedora, openSUSE etc.) können eine Yum-Paketquelle einrichten:

```
root#  wget -q http://download.virtualbox.org/virtualbox/debian/oracle_vbox.asc
root#  rpm --import sun_vbox.asc
```

Anschließend laden Sie die entsprechende `*.repo`-Datei von der VirtualBox-Download-Seite herunter und kopieren sie in das Verzeichnis `/etc/yum.repos.d`:

```
[virtualbox]
name=VirtualBox
baseurl=http://download.virtualbox.org/virtualbox/rpm/fedora/$releasever
enabled=1
gpgcheck=1
```

Die VirtualBox-Installation führen Sie nun mit `yum install` oder `zypper install` durch.

Installation unter Windows und Mac OS X

Für Privatanwender ist die VirtualBox-Installation auch unter den aktuellen Versionen von Windows und Mac OS X ein Kinderspiel: Sie laden die gerade aktuelle Binärversion von *virtualbox.org* herunter, führen das Installationsprogramm aus und starten Windows neu – fertig!

Vorbereitungsarbeiten

vboxusers-Gruppe

Unabhängig davon, aus welcher Quelle Ihre VirtualBox-Installation stammt, wurde die Gruppe `vboxusers` eingerichtet. Nur Benutzer, die dieser Gruppe angehören, können virtuelle Maschinen ohne Einschränkungen ausführen. Deswegen müssen Sie vor dem ersten Start von VirtualBox Ihren Account der Gruppe `vboxusers` hinzufügen. Ersetzen Sie beim folgenden Kommando `kofler` durch Ihren Login-Namen!

```
root#  usermod -a -G vboxusers kofler
```

Damit die geänderte Gruppenzuordnung wirksam wird, müssen Sie sich aus- und neu einloggen. Anschließend starten Sie die Benutzeroberfläche von VirtualBox über das KDE- oder Gnome-Menü bzw. mit dem Kommando `VirtualBox`.

Speicherort für virtuelle Maschinen

VirtualBox richtet für jede virtuelle Maschine ein Unterverzeichnis innerhalb von `VirtualBox VMs` ein. In mehreren Dateien werden dort die Einstellungen der virtuellen Maschine sowie die virtuelle Festplatte gespeichert. Mit DATEI • GLOBALE EINSTELLUNGEN können Sie gegebenenfalls einen anderen Speicherort einstellen.

Extension Pack

Oracle bietet auf seiner Website ein sogenanntes Extension Pack zum Download an. Beim Download des Extension Packs schlägt der Webbrowser vor, die Datei direkt mit VirtualBox zu öffnen. Diesem Vorschlag folgen Sie einfach.

Das Extension Pack ergänzt VirtualBox um einige Zusatzfunktionen: Unter anderem können Sie dann in den virtuellen Maschinen auf USB-2-Geräte und iSCSI-Server zugreifen und die virtuellen Maschinen via RDP (Remote Display Protocol) auf einem anderen Rechner im Netzwerk steuern. Diese Erweiterungen werden nur in Binärform vertrieben, es handelt sich also nicht um Open-Source-Code. Die kommerzielle Nutzung dieser Erweiterungen erfordert eine Lizenz von Oracle!

11.3 VirtualBox-Maschinen einrichten

Eine virtuelle Maschine mit Linux einrichten

Dieser Abschnitt beschreibt, wie Sie innerhalb von VirtualBox eine virtuelle Maschine mit Linux einrichten. Dabei spielt es keine Rolle, ob VirtualBox unter Linux, Windows oder Mac OS X läuft.

Beim Einrichten einer neuen virtuellen Maschine unterstützt Sie ein Assistent. Als Betriebssystemtyp stehen neben Windows diverse Linux-Distributionen Linux zur Auswahl. Wenn Ihre Distribution nicht vertreten ist, wählen Sie LINUX MIT KERNEL 2.6; diese Einstellung gilt auch für 3.*n*-Kernelversionen. Achten Sie darauf, dass es für jedes Betriebssystem *zwei* Versionen gibt: VirtualBox geht davon aus, dass Sie eine 32-Bit-Version installieren. Für 64-Bit-Distributionen müssen Sie explizit den passenden 64-Bit-Eintrag auswählen!

Beim Einrichten der virtuellen Festplatte stehen verschiedene Formate zur Auswahl. Im Regelfall sollten Sie beim VirtualBox-eigenen Format VDI bleiben. Schließlich zeigt VirtualBox eine Zusammenfassung aller Hardware-Komponenten an. Dort können Sie bei Bedarf weitere Einstellungen durchführen, z. B. den Netzwerkzugang verändern oder eine ISO-Datei als Datenquelle für das CD/DVD-Laufwerk angeben.

Wenn Sie mit der Konfiguration fertig sind, starten Sie die virtuelle Maschine. VirtualBox zeigt die virtuelle Maschine in einem eigenen Fenster an. Dort installieren Sie Linux wie auf einem realen Rechner.

Mögliche Fehlermeldungen beim ersten Start einer virtuellen Maschine

VirtualBox testet erst mit dem Start einer virtuellen Maschine, ob die VirtualBox-Kernelmodule geladen sind und ob Hardware-Virtualisierungsfunktionen zur Verfügung stehen. Ist eine dieser Voraussetzungen nicht erfüllt, wird eine Fehlermeldung oder Warnung angezeigt. Bei den Kernelmodulen müssen Sie sicherstellen, dass diese installiert sind. Wenn Sie VirtualBox frisch installiert haben, hilft oft `service vboxdrv start`. Die Hardware-Virtualisierungsfunktionen müssen eventuell im BIOS oder EFI aktiviert werden. VirtualBox ist auf diese Funktionen nicht angewiesen, die Virtualisierung kann damit aber wesentlich effizienter durchgeführt werden!

Die Netzwerkverbindung zwischen Wirt und Gast erfolgt standardmäßig per NAT. Das Gastsystem hat dann zwar Internetzugang, kann aber keine Daten mit dem lokalen Netzwerk austauschen. In Abschnitt 11.1 sind die anderen von VirtualBox unterstützten Netzwerkvarianten beschrieben. Bei meinem privaten Setup ist der Wirtsrechner mit einem ADSL-Router verbunden. Zur Netzwerkkonfiguration meiner virtuellen Maschinen verwende ich zumeist NETZWERKBRÜCKE. Damit sind alle virtuellen Maschinen Mitglieder des lokalen Netzwerks, was den Datenaustausch zwischen dem Wirtssystem und seinen Gästen sehr erleichtert (SSH, NFS, Samba etc.).

Die virtuelle Maschine erhält automatisch den Tastatur- und Mausfokus, sobald Sie eine Taste drücken. Standardmäßig lösen Sie den Fokus mit der rechten Strg-Taste. Im VirtualBox-Hauptfenster können Sie mit DATEI • GLOBALE EINSTELLUNGEN • EINGABE eine andere »Host«-Taste einstellen. Einige weitere Tastenkürzel finden Sie im MASCHINE-Menü des VirtualBox-Fensters.

Tastenkürzel	Bedeutung
Host + F	Vollbildmodus (de)aktivieren
Host + Entf	Strg + Alt + Entf an das Gastsystem senden
Host + ←	Strg + Alt + ← an das Gastsystem senden
Host + Fn	Strg + Alt + Fn an das Gastsystem senden
Host + S	Snapshot der virtuellen Maschine erstellen
Host + H	virtuelle Maschine per ACPI ausschalten
Host + R	virtuelle Maschine sofort ausschalten (Reset, Vorsicht!)

Tabelle 11.1 VirtualBox-Tastenkürzel

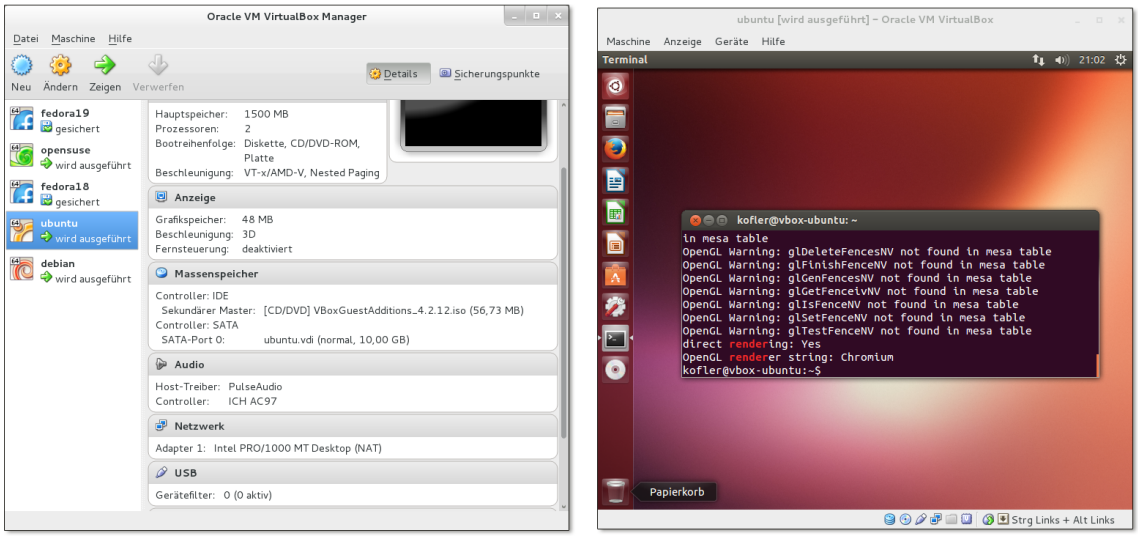


Abbildung 11.1 Links der Virtual Machine Manager, rechts eine virtuelle Ubuntu-Maschine

Gasterweiterungen installieren

Nachdem die eigentliche Installation abgeschlossen ist, sollten Sie in der virtuellen Maschine noch die sogenannten Guest Additions installieren. Sie stellen dem Gastsystem zusätzliche Treiber zur Verfügung und verbessern das Zusammenspiel mit dem Wirt: Die Maus kann nun aus der virtuellen Maschine herausbewegt werden, die virtuelle Bildschirmauflösung des Gasts passt sich automatisch an die Fenstergröße an, der Datenaustausch mit dem Wirtssystem kann über Shared Folders erfolgen, Text kann über die Zwischenablage kopiert werden etc.

Manche Distributionen liefern fertige Pakete mit den VirtualBox-Gasterweiterungen mit, und bei openSUSE werden sie sogar gleich automatisch installiert:

openSUSE: `virtualbox-guest-*`
Ubuntu: `virtualbox-guest-utils`, `virtualbox-guest-x11`, `virtualbox-guest-dkms`

Bei anderen Distributionen bzw. dann, wenn Sie die neueste Version der Gasterweiterungen benötigen, müssen Sie eine manuelle Installation durchführen. Dazu werfen Sie eine eventuell eingebundene CD/DVD aus und führen dann im VirtualBox-Fenster GERÄTE • GASTERWEITERUNGEN INSTALLIEREN aus. Im Regelfall erscheint nach einigen Sekunden in der virtuellen Maschine ein Dateimanagerfenster, in dem Sie `autorun.sh` starten. Sollte das nicht funktionieren, helfen die folgenden Kommandos weiter:

```
root#  mkdir /media/cdrom
root#  mount /dev/sr0 /media/cdrom
root#  sh /media/cdrom/autorun.sh
```

Das Installationsprogramm richtet nun die drei neuen Kernelmodule `vboxadd`, `vboxvideo` und `vboxvfs` sowie einen neuen X-Treiber ein und fügt einige Init-Scripts hinzu, damit diese Gasterweiterungen beim nächsten Start der virtuellen Maschine auch verwendet werden.

Unter gängigen Ubuntu-Versionen bis 13.04 funktioniert die Installation der Gasterweiterungen auf Anhieb. Da Ubuntu mit Version 13.10 auf das Grafiksystem Mir/Xmir umsteigt, war Mitte 2013 noch nicht absehbar, welche Auswirkungen das auf den Betrieb virtueller Maschinen haben wird.

Bei den meisten anderen Linux-Distributionen müssen Sie vor der Installation der Gasterweiterungen diverse Pakete installieren, die den C-Compiler und die Kernel-Header-Dateien enthalten. Führen Sie vorher ein Update aus, um sicherzustellen, dass die installierte Kernelversion und die Version der Kernel-Header-Dateien zusammenpassen!

```
root#  apt-get install gcc make linux-headers-platform          (Debian)
root#  yum install gcc make kernel-headers kernel-devel         (Fedora)
root#  zypper install gcc make kernel-source kernel-syms        (openSUSE)
```

3D-Grafik

Im Idealfall stehen innerhalb der virtuellen Maschine sogar 3D-Funktionen zur Verfügung. Dazu müssen auf jeden Fall die Gasterweiterungen aktiv sein, außerdem müssen die 3D-Funktionen in den Eigenschaften der virtuellen Maschine aktiviert sein (Dialogblatt ANZEIGE, Option 3D-BESCHLEUNIGUNG). Das alleine ist aber nicht in jedem Fall ausreichend – ob 3D-Funktionen an den Gast weitergereicht werden können, hängt auch davon ab, welches Host-Betriebssystem und welchen Grafiktreiber Sie verwenden. Sehr gute Erfahrungen habe ich mit Linux-Hosts in Kombination mit dem Intel-Grafiktreiber gemacht.

Wenn Sie sich vergewissern möchten, ob alles funktioniert, installieren Sie in der virtuellen Maschine je nach Distribution das Paket `mesa-utils`, `glx-utils` oder `Mesa-demo-x` und führen dann `glxinfo` aus. Das Ergebnis sollte wie im folgenden Listing aussehen:

```
user$  glxinfo | grep render
...
OpenGL renderer string: Chromium
```

Wenn der `OpenGL renderer string` hingegen `llvmpipe` enthält, dann werden die 3D-Funktionen durch die CPU emuliert, was deutlich langsamer ist.

Eine virtuelle Maschine mit Windows einrichten

Sofern Sie über eine Installations-CD/DVD bzw. die entsprechende ISO-Datei sowie eine gültige Lizenz und den dazugehörenden Schlüssel verfügen, können Sie in VirtualBox auch Windows installieren. Die Installation von Windows und der VirtualBox-Gasterweiterungen verlief bei meinen Tests mit Windows XP und Windows 7 problemlos. Allerdings stehen unter Windows keine 3D-Effekte (»Aero Glass«) zur Verfügung. Generell sind Sie aus Performance-Gründen mit älteren Windows-Versionen oft besser beraten.

Warten Sie mit der Online-Registrierung so lange ab, bis Sie mit der Leistung zufrieden sind. Wenn Sie später in den Einstellungen der virtuellen Maschine das RAM vergrößern oder andere virtuelle Hardware-Parameter ändern, müssen Sie die Registrierung wiederholen!

Windows 8.1

Ich habe während der Arbeit an diesem Kapitel auch die damals gerade ganz neue Preview-Version von Windows 8.1 ausprobiert (siehe Abbildung 11.2). Die Festplattengröße sollten Sie mit zumindest 20 GByte wählen. Davon sind nach der Installation innerhalb der virtuellen Maschine noch rund 10 GByte frei.

Die Installation versagte anfänglich mit dem Fehlercode 0x000000C4. Eine kurze Internet-Recherche erbrachte, dass vor der Installation ein CPU-Parameter verändert werden muss:

```
user$  vboxmanage setextradata "windows81" VBoxInternal/CPUM/CMPXCHG16B 1
```

Beim obigen Kommando müssen Sie `windows81` durch den Namen Ihrer virtuellen Maschine ersetzen. Welche Namen es gibt, können Sie gegebenenfalls mit `vboxmanage list vms` feststellen. `vboxmanage` ist ein Kommandozeilenwerkzeug, das im Vergleich zur grafischen Benutzeroberfläche von Virtual Box einige Zusatzfunktionen bietet. Es ist anzunehmen, dass die CPU-Option `CMPXCHG16B` in künftigen VirtualBox-Versionen für Windows-8-Installationen automatisch aktiviert wird.

VirtualBox-Zusatzfunktionen

Shared Folder einrichten

Um den Datenaustausch zwischen Wirt und Gast zu erleichtern, können Sie auf dem Wirt ein Verzeichnis als sogenannten Shared Folder einrichten. Das Verzeichnis gilt spezifisch für eine bestimmte virtuelle Maschine. Die virtuelle Maschine darf während des Einrichtens nicht laufen. Zur Konfiguration öffnen Sie mit Ändern den Einstellungsdialog, wechseln in das Dialogblatt Gemeinsame Ordner, wählen dann ein lokales Verzeichnis auf dem Wirtssystem aus und geben dem Ordner einen Namen (z. B. `myshare`).

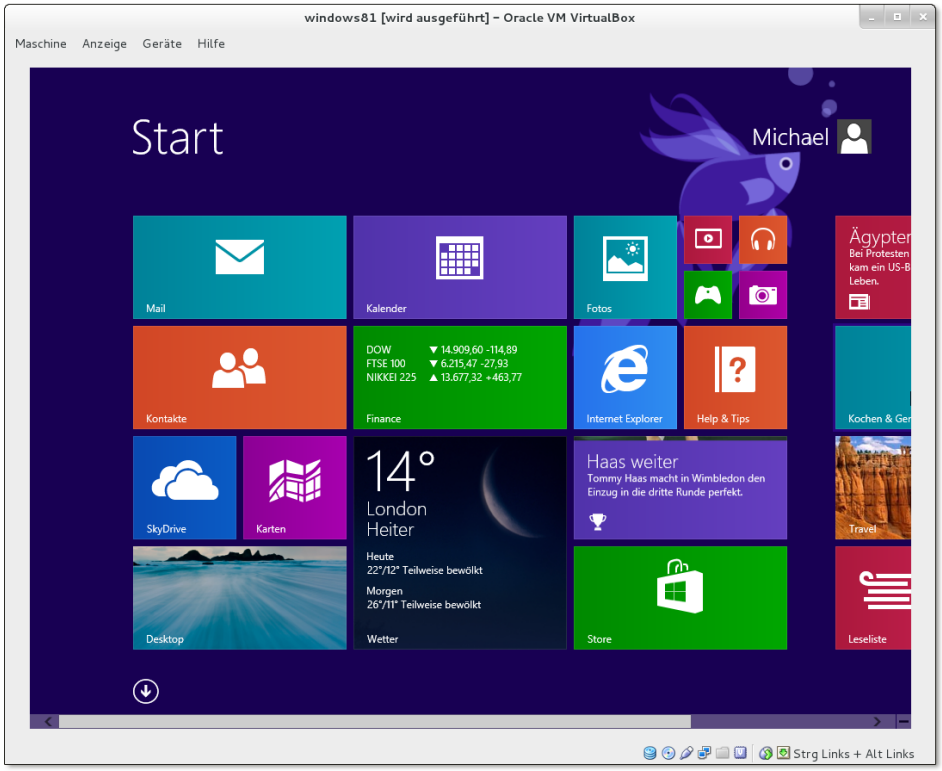


Abbildung 11.2 Windows 8.1 in einer virtuellen Maschine unter Linux ausprobieren

Auf dem Gastsystem ist ein manuelles `mount`-Kommando erforderlich, um auf das gemeinsame Verzeichnis zugreifen zu können. Dabei müssen Sie `myshare` durch den Namen ersetzen, den Sie bei der Konfiguration verwendet haben.

```
root@gast#  mkdir /media/vbox-share
root@gast#  mount -t vboxsf myshare /media/vbox-share
```

Shared Folders sind auch für Windows als Gastsystem vorgesehen, sofern darin die Gasterweiterungen installiert sind. Starten Sie unter Windows den Explorer, und führen Sie darin EXTRAS • NETZWERKLAUFWERK VERBINDEN aus. Der Zugriff auf den gemeinsamen Ordner erfolgt über das Netzwerkverzeichnis `\\vboxsrv\myshare`.

USB-Geräte in virtuellen Maschinen

Sofern Sie das VirtualBox Extension Pack installiert haben, können Sie USB-Geräte auch in virtuellen Maschinen nutzen. Das funktioniert nur, wenn das USB-Gerät im Wirtssystem *nicht* verwendet wird. USB-Datenträger werden im Wirtssystem normalerweise automatisch in das Dateisystem eingebunden; Sie müssen sie daraus wieder lösen.

Eine weitere Voraussetzung besteht darin, dass der Benutzer, der VirtualBox ausführt, Mitglied der Gruppe `vboxusers` ist. Schließlich müssen Sie darauf achten, dass der USB-2.0-Controller bei den Einstellungen der virtuellen Maschine im Dialogblatt USB aktiviert ist. In diesem Dialogblatt können Sie auch einen Filter definieren, um ein USB-Gerät direkt einer virtuellen Maschine zuzuordnen. Das ist aber keine zwingende Voraussetzung. Sie können das USB-Gerät nach dem Einschalten auch dynamisch in der VirtualBox-Statusleiste beim USB-Icon der virtuellen Maschine zuordnen.

Generell funktionierten die von mir getesteten USB-Geräte (ein Scanner und eine Digitalkamera) in den virtuellen Maschinen anstandslos, wenn auch langsamer als im Wirtssystem.

Export/Import virtueller Maschinen

Um eine virtuelle Maschine auf einen anderen Rechner zu migrieren, erzeugen Sie mit Datei • Appliance exportieren eine sogenannte Virtual Appliance, also eine zur Weitergabe bestimmte virtuelle Maschine, die üblicherweise aus zwei Dateien besteht: `*.ovf` enthält eine Beschreibung der virtuellen Maschine, `*.vmdk` das Festplatten-Image in komprimierter Form. Diese virtuelle Maschine können Sie nun bei einer anderen VirtualBox-Installation mit Datei • Appliance importieren wieder einrichten. Obwohl das Format für Virtual Appliances standardisiert ist, ist ein Wechsel von VMware zu VirtualBox oder umgekehrt leider nicht möglich. Ein Grund besteht darin, dass jedes Virtualisierungssystem andere virtuelle Hardware verwendet.

Geschwindigkeitsoptimierung

Mit zwei Optionen bei der Einstellung der virtuellen Hardware können Sie ein klein wenig mehr Geschwindigkeit aus Ihren virtuellen Maschinen herauskitzeln:

- **Host-Caching für die virtuelle Festplatte:** Im Dialogblatt Massenspeicher der virtuellen Maschine können Sie für den SATA-Controller die Option Host-I/O-Cache verwenden aktivieren. Sie erreichen damit, dass Schreibzugriffe zwischengespeichert werden, was die Geschwindigkeit I/O-lastiger Vorgänge stark vergrößern kann. Der Nachteil: Sollte der Host-Rechner abstürzen, riskieren Sie ein beschädigtes Dateisystem in der virtuellen Maschine.
- **Paravirtualisierte Netzwerktreiber:** Sofern es sich bei der virtuellen Maschine um eine Linux-Distribution handelt, können Sie im Dialogblatt Netzwerk bei den erweiterten Einstellungen die Option Paravirtualisiertes Netzwerk (virtio-net) aktivieren. VirtualBox spielt der virtuellen Maschine nun nicht mehr die Logik eines Netzwerkadapters vor, sondern spricht direkt mit dem `virtio-net`-Treiber des Linux-Kernels. Das ist deutlich effizienter.

Virtuelle Festplatten vergrößern

Die Benutzeroberfläche von VirtualBox gibt Ihnen leider keine Möglichkeit, eine virtuelle Festplatte nachträglich zu vergrößern. Wo die Benutzeroberfläche versagt, hilft oft auch ein Kommando weiter – so auch in diesem Fall. Bevor Sie loslegen, müssen Sie Ihre virtuelle Maschine herunterfahren. Ein vollständiges Backup ist sehr zu empfehlen!

Anschließend suchen Sie die `*.vdi`-Datei der virtuellen Festplatte und wenden darauf das Kommando `vboxmanage` an. Mit der Option `--resize` geben Sie die gewünschte neue Größe in MByte an. Im Regelfall wird das Kommando blitzschnell ausgeführt.

```
root#  vboxmanage modifyhd debian.vdi --resize 60000
```

Das ist aber erst die halbe Miete. Die virtuelle Maschine weiß nämlich noch nichts davon, dass ihre Festplatte größer geworden ist. Wenn es sich bei der virtuellen Maschine um eine Linux-Distribution handelt, binden Sie nun ein ISO-Image einer Linux-Live-CD in das virtuelle CD/DVD-Laufwerk ein und starten innerhalb der virtuellen Maschine ein Live-System. Darin führen Sie `parted /dev/sda` aus und können nun die Größe der letzten Partition vergrößern. Anschließend müssen Sie auch das darin enthaltene Dateisystem mit `resize2fs` vergrößern. Diese Eingriffe sind natürlich nicht ganz ungefährlich. Lesen Sie vorher die relevanten Abschnitte aus Kapitel 25!

Analog kann auch ein Windows-Dateisystem vergrößert werden, erstaunlicherweise sogar im laufenden Betrieb. Als ich zuletzt in die Verlegenheit kam, eine Windows-7-Installation zu vergrößern, habe ich ein Eingabeaufforderungsfenster mit Administratorrechten geöffnet und dort die folgenden Kommandos ausgeführt:

```
>  Diskpart
list disk
select disk 0
list partition
select partition 2
extend
```

`list disk` liefert eine Liste aller virtuellen Festplatten. Normalerweise muss die erste mit dem Index 0 ausgewählt werden. Nun ermittelt `list partition` die Partitionen. Abermals muss mit `select` eine Partition zur weiteren Bearbeitung ausgewählt werden – im Regelfall die letzte. Mit `extend` wird diese nun auf die maximale Größe erweitert.

Kapitel 12
Raspberry Pi

Der Raspberry Pi ist kein Himbeerkuchen, sondern ein winziger Computer. Die Grundfläche des Geräts ist etwas größer als eine Kreditkarte; in ein Gehäuse verpackt hat der Computer das Volumen von zwei Smartphones. Das eigentliche Grundgerät kostet je nach Händler rund 40 EUR; zusätzlich brauchen Sie in der Regel ein Netzteil, ein Gehäuse, eine SD-Speicherkarte und eventuell ein paar Kabel. Die Gesamtinvestition liegt also deutlich unter 100 EUR.

Dafür erhalten Sie einen vollwertigen, Linux-basierten Computer mit einer ARM-CPU, den Sie zur Steuerung elektrischer Geräte, für Versuchsaufbauten, als Mini-Server z. B. für den VPN-Zugang zu Ihrem Netzwerk zuhause oder als kleines Multimedia-Center in der Art des Apple TV einsetzen können.

Dieses Kapitel beschreibt, worauf Sie bei der Inbetriebnahme des Raspberry Pi achten müssen, gibt Konfigurationstipps und umreißt einige Anwendungsfälle. Natürlich ist zu erwarten, dass es in naher Zukunft eine größere Auswahl derartiger Minicomputer geben wird. Erste Ankündigungen für Raspberry-Pi-Alternativen mit einer schnelleren CPU und mehr Speicher gibt es schon, und angesichts des riesigen Erfolgs wird wohl auch die Version 2 des originalen Raspberry Pi nicht lange auf sich warten lassen. Deswegen habe ich mich in diesem Kapitel bemüht, die Grundprinzipien derartiger Minicomputer möglichst allgemeingültig zu beschreiben, sodass Ihnen dieser Text auch beim Betrieb anderer vergleichbarer Computer hilft.

Ich gehe in diesem Kapitel davon aus, dass Sie bereits über grundlegende Linux-Kenntnisse verfügen. Das ist auch der Grund dafür, dass sich dieses Kapitel erst an dieser Stelle im Buch befindet. Generell arbeiten Sie mit dem Raspberry Pi oft deutlich systemnäher, als dies auf einem Notebook oder PC mit einer typischen Distribution der Fall ist. Deswegen werden Sie sich mit dem Raspberry Pi umso rascher anfreunden, je mehr Linux-Erfahrung Sie bereits haben.

Zur Inbetriebnahme des Raspberry Pi benötigen Sie einen »richtigen« Computer. Damit beschreiben Sie die SD-Karte mit einer Linux-Distribution für den Raspberry Pi. Grundsätzlich können Sie das auch mit einem Windows- oder Apple-Computer tun, aber in diesem Buch nehme ich natürlich an, dass Sie unter Linux arbeiten.

Hinweis

Es gibt viele Möglichkeiten des Raspberry Pi zu nutzen: als Mini-PC, als Medien-Center, als Steuerungs- und Bastel-Plattform, als Server etc. Insofern ist die Einordnung dieses Kapitels in das Buch schwierig. Linux-Einsteiger werden feststellen, dass dieses Kapitel teilweise Know-how voraussetzt, das ich erst in späteren Kapiteln vermittle. Insofern müsste dieses Kapitel eigentlich am *Ende* des Buchs stehen. Das erschien mir aber nicht wünschenswert.

12.1 Grundlagen

Hardware

Der Minicomputer Raspberry Pi besteht aus einer einzigen Platine in der Größe einer Kreditkarte. Darauf sind enthalten (für das Modell B):

- ein Broadcom BCM2835 System-on-a-Chip (SoC), das aus einem CPU-Core in ARMv6-Architektur mit 700 MHz sowie einem Broadcom Video-Core IV mit H.264 Encoder/Decoder besteht
- 512 MByte RAM
- ein Micro-USB-Anschluss zur Stromversorgung (5V, 700 mA, ergibt 3,5 Watt)
- zwei USB-Anschlüsse für Tastatur, Maus und andere USB-Geräte mit einem maximalen Ausgangsstrom von 100 mA
- ein HDMI-Ausgang für Bild und Ton, Auflösung bis zu 1920*1200 Pixel
- ein Audio-Ausgang für einen 3,5-mm-Klinkenstecker
- ein Video-Ausgang (Composite Video, PAL oder NTSC)
- ein SD-Karten-Slot (SDHC/SDXC)
- ein Ethernet-Anschluss (10/100 MBit)
- eine Steckerleiste mit 26 Pins für allgemeine Input/Output-Zwecke (General Purpose Input/Output inklusive UART, I2C-Bus, SPI-Bus, I2S-Audio)

Der Raspberry Pi weist damit ähnliche Eckdaten auf wie ein Mittelklasse-Smartphone; natürlich fehlen die Telefonfunktionen und das Display, dafür bekommen Sie aber Netzwerk-, Monitor- sowie allgemeine I/O-Anschlüsse. Es existiert auch ein Modell A mit nur 256 MByte RAM, nur einem USB-Anschluss und ohne Ethernet-Anschluss; dieses Modell ist aber wenig verbreitet und nicht empfehlenswert, wenn Sie auf Ihrem Raspberry Pi Linux mit einer grafischen Benutzeroberfläche ausführen möchten. Entscheiden Sie sich unbedingt für das Modell B, der Preisunterschied ist nicht groß!

Vielleicht fragen Sie sich, warum der Raspberry Pi (Modell B) keinen Gigabit-Ethernet-Anschluss hat. Das liegt daran, dass der Ethernet-Adapter intern als USB-2-Device realisiert ist. USB 2 ist aber zu langsam, um die Datenmengen eines Gigabit-Netzwerks zu verarbeiten.

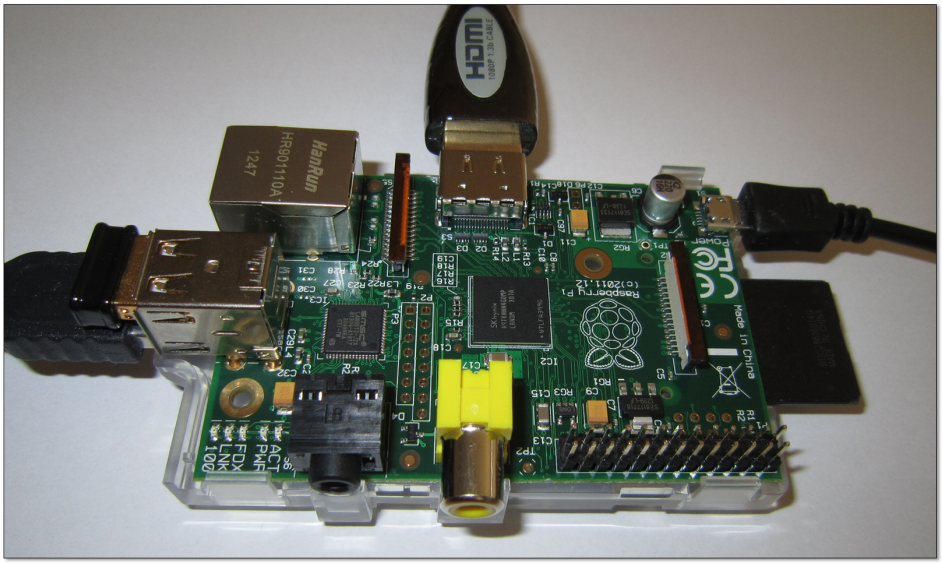


Abbildung 12.1 Versuchsaufbau des Raspberry Pi (Modell B)

Zubehör

Bevor Sie den Raspberry Pi erwerben, sollten Sie sich darüber klar werden, was Sie alles sonst noch brauchen:

- ein Netzteil
- eventuell ein Gehäuse
- eventuell einen USB-WLAN- oder USB-Bluetooth-Stecker
- eventuell einen Infrarot-Empfänger (direkter Anschluss an GPIO-Pins)
- eine SD-Speicherkarte mit zumindest 2 GByte
- Tastatur, Maus, Kabel, Monitor oder Fernseher etc.

Über ein HDMI-Kabel können Sie den Raspberry Pi an jeden gängigen Fernseher sowie an viele Computer-Monitore anschließen, sofern diese über einen HDMI-Eingang verfügen. Über ein HDMI-zu-DVI-Kabel können Sie auch einen Monitor mit DVI-Eingang anschließen. Schwieriger ist die Verwendung eines VGA-Monitors: Zwar gibt es HDMI-zu-VGA-Konverter, die kosten aber beinahe so viel wie ein ganzer Raspberry Pi.

Das Netzteil ist entscheidend für die Stabilität

Achten Sie beim Kauf des Netzteils darauf, dass dieses ausreichend leistungsstark ist. Typische Handy-Netzteile sind ungeeignet! Das Netzteil muss zumindest 5 Watt Leistung liefern können, damit der Raspberry Pi im Dauerbetrieb stabil läuft.

Vermeiden Sie auch den direkten Anschluss von USB-Geräten mit hohem Energiebedarf an den Raspberry Pi. Die Raspberry-Pi-Spezifikation erlaubt nur USB-Geräte mit einem Strombedarf von maximal 100 mA. Eine moderne, energieeffiziente Tastatur und eine Maus oder ein USB-WLAN-Stecker können zumeist so betrieben werden, aber externe Festplatten brauchen unbedingt eine eigene Energieversorgung, entweder durch ein zweites Netzteil oder über einen USB-Hub mit Stromversorgung!

Gehäuse

Falls Sie den Raspberry Pi in ein Gehäuse verpacken, sollten Sie darauf achten, dass es Belüftungsschlitze hat. Der Raspberry Pi läuft mangels Lüfter und anderer bewegter Teile vollkommen lautlos, produziert aber durchaus Abwärme. In einem Gehäuse ohne Luftzirkulation riskieren Sie ein vorzeitiges Ableben Ihres neuen Gadgets!

Uhr

Der Raspberry Pi enthält keine integrierte Uhr. Die Uhrzeit muss deswegen nach jedem Start neu gestellt werden, idealerweise über eine Netzwerkverbindung mit NTP.

Software

Der Raspberry Pi enthält anfangs (fast) gar keine Software. Wenn Sie den Minirechner mit der Stromversorgung und einem Monitor verbinden, erhalten Sie nicht einmal ein Bild! Es gibt kein BIOS, EFI oder eine vergleichbare eingebaute Software, die verrät, ob der Raspberry Pi prinzipiell funktioniert.

Um den Raspberry Pi ausprobieren zu können, müssen Sie zuerst ein Betriebssystem auf eine SD-Karte schreiben. Wie Sie dabei im Detail vorgehen müssen, wird etwas weiter unten beschrieben.

Geeignete Betriebssysteme für den Raspberry Pi müssen vor allem zwei Voraussetzungen erfüllen: Sie müssen für die ARMv6-CPU-Architektur kompiliert sein, und sie müssen in zwei getrennten Partitionen auf die SD-Karte geschrieben werden. Die erste Partition im FAT-Format enthält den Boot-Code, die Konfigurationsdatei `config.txt` und den Kernel; die zweite Partition enthält das eigentliche Betriebssystem.

Im Internet finden Sie neben mehreren Linux-Distributionen auch RISC OS für den Raspberry Pi zum Download:

- **Raspbian:** Das ist die von den Raspberry-Pi-Entwicklern empfohlene Linux-Distribution. Sie basiert auf Debian 7 und enthält ein komplettes Desktop-System (Xfce).
- **Arch Linux ARM:** Die ARM-Version von Arch Linux ist vor allem für Linux-Profis interessant. Die minimale Anfangskonfiguration im Textmodus startet sehr schnell und kann dann an die eigenen Ansprüche angepasst werden.
- **Pidora (Fedora Remix):** Red-Hat- und Fedora-Freunde müssen auf Ihre Lieblingsdistribution auch auf dem Raspberry Pi nicht verzichten. Pidora ist eine speziell für den Raspberry Pi optimierte und kompilierte Version von Fedora.
- **XBMC:** Wenn Sie Ihren Raspberry Pi als Multimedia-Center einsetzen möchten, gibt es gleich drei verschiedene Linux-Distributionen speziell für diesen Zweck: Raspbmc, OpenELEC und XBian. Am populärsten ist Raspbmc.
- **RISC OS:** Dieses Betriebssystem hat nichts mit Linux zu tun. RISC OS wurde 1987 für den Acorn Computer entwickelt. Für den praktischen Einsatz ist es nicht wirklich geeignet, aber wer gerne einen historischen Blick zurück in die Anfangszeiten des PCs werfen möchte, kann dies mit RISC OS ohne jedes Risiko tun.

Einen Vergleich zwischen sechs Raspberry-Pi-Distributionen können Sie hier nachlesen:

http://www.linuxuser.co.uk/reviews/distro-super-test-pi-edition

Vielleicht überrascht es Sie, dass es Ubuntu nicht für den Raspberry Pi gibt. Das liegt daran, dass Ubuntu zwar prinzipiell die ARM-Architektur unterstützt, nicht aber die relativ alte ARM-Version (ARMv6) der CPU des Raspberry Pi.

Für erste Experimente empfehle ich Ihnen Raspbian. Diese Distribution ist auch für Linux-Einsteiger gut handhabbar; außerdem ist ihre Bedienung und Konfiguration auf unzähligen Seiten im Internet umfassend dokumentiert.

Raspberry Pi versus Notebook/PC

Im Prinzip ist ein Raspberry Pi in Kombination mit einer geeigneten Linux-Distribution ein vollwertiger Computer mit grafischer Benutzeroberfläche, Webbrowser etc. Kann der Raspberry Pi also Ihren Desktop-PC ersetzen? In aller Regel: nein, noch nicht!

Im Vergleich zu einem Desktop-PC verfügt der Raspberry Pi über zu wenig Arbeitsspeicher, die CPU und der Grafikprozessor sind zu langsam, außerdem fehlt eine echte Festplatte. Stattdessen befinden sich sowohl das Betriebssystem als auch Ihre Daten auf einer SD-Speicherkarte; das funktioniert an sich zufriedenstellend, aber

eben deutlich langsamer, als Sie es von einem Notebook mit einer echten Festplatte oder gar mit einer SSD gewohnt sind. Auch ist die Zuverlässigkeit von SD-Karten mitunter deutlich geringer als die einer Festplatte. Von der Geschwindigkeit abgesehen, machen auch so triviale Dinge wie die fehlende eingebaute Uhr oder der nicht existente Ein/Aus-Schalter den Desktop-Betrieb des Raspberry Pi unpraktisch.

Es erscheint aber durchaus denkbar, dass es in wenigen Jahren mit dem Raspberry Pi vergleichbare Geräte gibt, deren Leistungsfähigkeit und Funktionsumfang mit einem Desktop-PC bzw. mit einem Notebook (minus Bildschirm) mithalten kann.

Raspberry Pi versus Arduino

Der Minicomputer Raspberry Pi wird oft in einem Atemzug mit Arduino genannt. Das ist eine andere sehr erfolgreiche Plattform für Elektronikprojekte mit Open-Source-Wurzeln. Ein besonderes Merkmal von Arduino besteht darin, dass auch die Hardware im Sinne der Open-Source-Idee frei zugänglich ist – also die Schaltpläne, der Code des Mikrocontrollers etc.

Der gemeinsame Nenner des Raspberry Pi und der Arduino-Komponenten besteht darin, dass beide Geräte häufig zur Steuerung elektrischer bzw. elektronischer Geräte eingesetzt werden. Bastler, (Hoch-)Schulen und Museen greifen gleichermaßen auf Raspberry Pi oder Arduino-Komponenten zurück, um Versuchsaufbauten durchzuführen, Begeisterung für die Elektronik zu vermitteln oder die Heizung intelligenter zu steuern.

Wo sind nun die Unterschiede zwischen diesen beiden Geräten bzw. Produktkategorien? Der Raspberry Pi ist ein vollwertiger Computer im Sinne eines PCs: Er kann an einen Monitor angeschlossen werden, über Tastatur und Maus bedient werden, verfügt über eine Netzwerkverbindung und hat eine ähnliche Leistungsfähigkeit wie ein typischer PC vor ein paar Jahren. Auf dem Raspberry Pi läuft eine komplette Linux-Distribution wie auf einem Desktop-PC oder Notebook.

Arduino-Boards sind auch Computer, aber eher im Sinne eines Mikrocontrollers zur Steuerung einer Waschmaschine. Die Entwicklung eines Programms für ein Arduino-Board erfolgt extern auf einem gewöhnlichen PC. Das fertige Programm wird dann auf das Arduino-Board übertragen und ermöglicht es diesem, bestimmte Aufgaben zu erfüllen – z. B. beim Unterschreiten einer bestimmten Temperaturschwelle die Heizung einzuschalten. Von Haus aus gibt es aber keine Möglichkeit, ein Arduino-Board an einen Monitor oder an ein Netzwerk anzuschließen. Die Rechenleistung ist viel geringer als beim Raspberry Pi. Auf einem Arduino-Board läuft kein vollwertiges Betriebssystem in der Art von Linux.

Daraus sollten Sie nun aber nicht die Schlussfolgerung ziehen, ein Raspberry Pi sei *besser* als ein Arduino-Board – das wäre ein Vergleich zwischen Äpfeln und Birnen! Beide Geräte sind für ganz unterschiedliche Dinge konzipiert. Zu den Stärken von Arduino-Geräten zählt beispielsweise ein viel geringerer Stromverbrauch. Diese sind damit viel besser für einen Batterie- oder Akkubetrieb geeignet als der Raspberry Pi.

Weiterführende Informationen

Zum Raspberry Pi existieren mittlerweile unzählige Websites. Anbei einige Links zu den wichtigsten Seiten, auf denen Sie über dieses Kapitel hinausgehende Informationen finden:

http://www.raspberrypi.org (die offizielle Website)
http://raspberrycenter.de
http://elinux.org/RPi_Hub

Alternativen zum Raspberry Pi

Der Raspberry Pi ist zwar momentan der erfolgreichste, aber keineswegs der einzige Linux-taugliche Minicomputer. Schon seit vielen Jahren gibt es diverse Embedded-Linux-Systeme, die aber deutlich teurer und primär für den industriellen Einsatz gedacht sind. Eine Menge Informationen zu diesem Thema finden Sie auf der schon erwähnten Website *http://elinux.org*.

Für Bastler mit kleinem Budget geeignet sind z. B. das BeagleBone Black, das Cubieboard oder der Via Android PC (Via APC).

http://beagleboard.org/Products/BeagleBone
http://cubieboard.org
http://apc.io

Wenn es Ihnen primär um Multimedia-Anwendungen und weniger um Bastel- und Steuerungsprojekte geht, können Sie auch die immer populäreren Android-HDMI-Sticks in Erwägung ziehen. Geräte wie das Google Chromecast, Cotton Candy, rikomagic MK802 oder Dell Ophelia sind nochmals deutlich kleiner als der Raspberry Pi und beanspruchen nicht mehr Platz als ein USB-Stick.

Bei der Auswahl eines Geräts sollten Sie freilich nicht nur auf den Preis und die technischen Daten achten. Das momentan wichtigste Argument für den Raspberry Pi sind die riesige Community und die unzähligen im Web verfügbaren Foren, Tipps und Anleitungen.

12.2 Raspbian installieren und konfigurieren

SD-Karte vorbereiten

Die »Installation« einer Linux-Distribution auf einem Raspberry Pi sieht vollkommen anders aus als die Installation einer gewöhnlichen Linux-Distribution auf ein Notebook. Genau genommen installieren Sie nämlich gar nichts, sondern kopieren ein vorkonfiguriertes Image auf eine SD-Karte. Dazu benötigen Sie einen Computer mit einem SD-Slot oder mit einem externen SD-Kartenleser.

Die richtige SD-Karte

Der Raspberry Pi erwartet eine SD-Karte im Standardformat. Mini- oder Micro-SD-Karten können nur mit einem Adapter verwendet werden. Die SD-Karte muss dem SDHC-Standard entsprechen. Der neuere SDXC-Standard wird offiziell nicht unterstützt; es gibt allerdings Forenberichte, dass auch derartige Karten funktionieren. Wenn Sie Wert auf einen schnellen Start des Raspberry Pi legen bzw. häufig größere Datenmengen lesen oder schreiben möchten, sollten Sie eine möglichst schnelle SD-Karte verwenden (z. B. Class 10).

Die SD-Karte muss zumindest 2 GByte Speicherplatz bieten. Die obere Grenze beträgt laut der Raspberry Pi-FAQ 32 GByte, aber in manchen Forenberichten heißt es, dass der Minicomputer auch mehr Speicherplatz adressieren kann.

Nicht funktionierende SD-Karten zählen zu den häufigsten Fehlerursachen im Betrieb des Raspberry Pi. Vermeiden Sie Billigprodukte. Verzichten Sie außerdem auf die Übertaktung der CPU Ihres Raspberry Pi! Werfen Sie bei Problemen auch einen Blick auf die folgende Seite:

http://elinux.org/RPi_SD_cards

Bei der Raspbian-Distribution handelt es sich im Wesentlichen um ein vorkonfiguriertes Debian-7-System für ARM. In Raspbian kommt allerdings ein aktuellerer Kernel als im originalen Debian zur Anwendung. Sie können die gerade aktuelle Raspbian-Version hier als ZIP-Archiv herunterladen:

http://www.raspberrypi.org/downloads

ZIP-Archiv überprüfen und auspacken

Die weiteren Arbeitsschritte erledigen Sie in einem Terminalfenster auf einem Linux-Rechner. Zuerst überprüfen Sie anhand der SHA1-Prüfsumme, ob die ZIP-Datei korrekt ist, danach packen Sie das Archiv mit `unzip` aus:

```
user$  sha1sum 2013-nn-nn-wheezy-raspbian.zip
  b4375dc9d140e6e48e0406f96dead3601fac6c81  2013-nn-nn-wheezy-raspbian.zip
user$  unzip 2013-xx-xx-wheezy-raspbian.zip
Archive:  2013-nn-nn-wheezy-raspbian.zip
  inflating: 2013-nn-nn-wheezy-raspbian.img
```

Device der SD-Karte feststellen

Als Nächstes kopieren Sie die Image-Datei auf die SD-Karte. Der gesamte bisherige Inhalt der SD-Karte – auch deren Formatierung – geht dabei verloren. Um den Device-Namen der SD-Karte festzustellen, führen Sie zuerst `lsblk` aus; danach schieben Sie die SD-Karte in den SD-Slot, und schließlich wiederholen Sie `lsblk`.

```
user$  lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda      8:0    0 119,2G  0 disk
  sda1   8:1    0 143,1M  0 part /boot/efi
  sda2   8:2    0   2,8G  0 part [SWAP]
  sda3   8:3    0  93,1G  0 part /
... (SD-Karte einschieben)
user$  lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda      8:0    0 119,2G  0 disk
  sda1   8:1    0 143,1M  0 part /boot/efi
  sda2   8:2    0   2,8G  0 part [SWAP]
  sda3   8:3    0  93,1G  0 part /
sdb      8:16   1   7,4G  0 disk
  sdb1   8:17   1    56M  0 part /media/xxxx
  sdb2   8:18   1   7,4G  0 part /media/yyyy
```

Die SD-Karte wird also über die Device-Datei `/dev/sdb` angesprochen. Die meisten Linux-Distributionen binden beim Verbinden externer Datenträger automatisch alle dort gefundenen Partitionen ein. Es ist ganz wichtig, dass Sie alle Partitionen der SD-Karte mit `umount` aus dem Verzeichnisbaum lösen! Mit `lsblk` können Sie sich vergewissern, dass es für `/dev/sdb?` nun keinen Mountpoint mehr gibt.

```
root#  umount /dev/sdb?
user$  lsblk /dev/sdb
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sdb      8:16   1   7,4G  0 disk
  sdb1   8:17   1    56M  0 part
  sdb2   8:18   1   7,4G  0 part
```

Verwenden Sie nicht »Sicher auswerfen«!

Wenn Sie unter Linux mit einer grafischen Benutzeroberfläche arbeiten, liegt es nahe, anstelle von `umount /dev/sdb?` den Button Sicher auswerfen oder Sicher entfernen Ihres Datei-Managers zu verwenden. Damit wird die betreffende Partition aber nicht nur aus dem Verzeichnisbaum gelöst, manche Datei-Manager deaktivieren die SD-Karte bei der Gelegenheit gleich ganz. Das gilt z. B. für aktuelle Versionen des Gnome-Dateimanagers Nautilus. Die SD-Karte kann dann überhaupt nicht mehr angesprochen werden, die Device-Datei `/dev/sdb` existiert nicht. Abhilfe: Entfernen Sie die SD-Karte aus dem Slot, fügen Sie sie neuerlich ein und verwenden Sie dann `umount`!

Image-Datei kopieren

Der letzte Schritt besteht jetzt darin, die Image-Datei auf die SD-Karte zu kopieren. Das geht am einfachsten mit dem Kommando `dd`, das Sie mit root-Rechten ausführen müssen. Achten Sie darauf, dass Sie den richtigen Device-Namen angeben! Wenn Sie hier irrtümlich `/dev/sda` angeben, sind alle Daten auf Ihrer Festplatte bzw. SSD unwiderruflich zerstört!

```
root#  dd if=2013-nn-nn-wheezy-raspbian.img of=/dev/sdb bs=4M
```

`dd` gibt leider kein optisches Feedback zum Kopiervorgang, der je nach Geschwindigkeit der SD-Karte mehrere Minuten dauert. Mehr Komfort bietet in dieser Hinsicht das Kommando `dcfldd`, das Sie aber zumeist extra installieren müssen. Eine wirklich präzise Fortschrittsanzeige kann aber auch `dcfldd` nicht bieten, weil die Ergebnisse durch das I/O-Caching verfälscht werden: Zuerst scheint alles ganz schnell zu gehen, dann dauert es aber doch recht lange, bis der Vorgang abgeschlossen ist.

```
root#  dcfldd if=2013-02-09-wheezy-raspbian.img of=/dev/sdb bs=4M \
         statusinterval=10
```

Um zu überprüfen, ob alles funktioniert hat, müssen Sie die SD-Karte entfernen und neu einfügen. Die Karte sollte nun zwei Partitionen enthalten: eine kleine FAT-Bootpartition und eine knapp 2 GByte große Systempartition (siehe Abbildung 12.2).

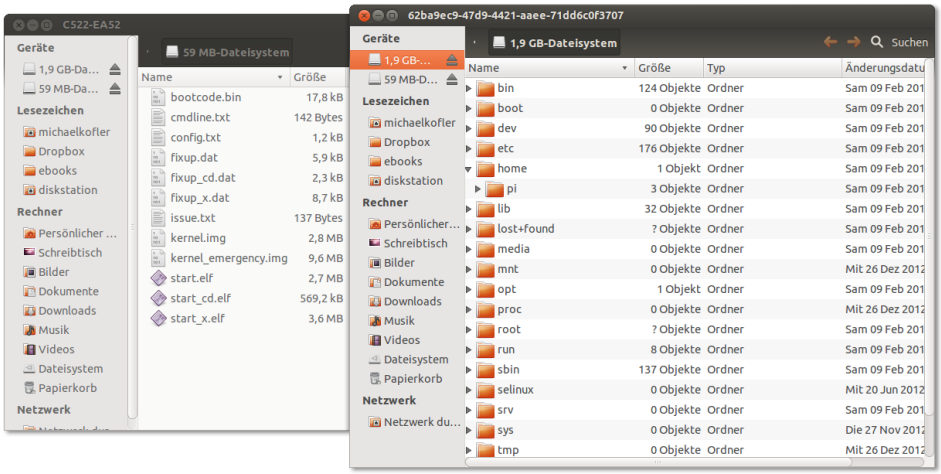


Abbildung 12.2 Inhalt der beiden Partitionen auf der SD-Karte

Den Raspberry Pi erstmalig starten

Nachdem Sie die Partitionen der SD-Karte aus dem Dateisystem Ihres Computers gelöst haben, entfernen Sie die Karte und stecken sie in den Raspberry Pi. Sobald Sie das Gerät nun an die Stromversorgung anschließen, beginnt der Bootprozess,

den Sie auf dem angeschlossenen HDMI-Monitor oder Fernseher verfolgen können. Nach etwa einer halben Minute sollte der Textdialog `raspi-config` auf dem Bildschirm erscheinen. Damit können Sie die Basiskonfiguration Ihres Raspberry Pi durchführen.

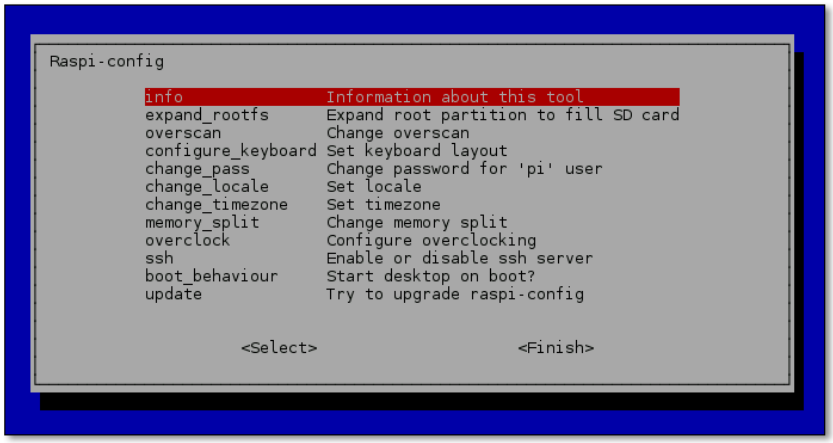


Abbildung 12.3 Das Raspi-config-Programm

- `expand_rootfs`: Vergrößert die Systempartition, sodass diese den gesamten zur Verfügung stehenden Platz der SD-Karte füllt. Standardmäßig ist diese Partition nur knapp 2 GByte groß, ganz egal, wie viel Speicherplatz die SD-Karte bietet. Die Größenanpassung wird erst beim nächsten Neustart des Raspberry Pi wirksam.
- `overscan`: Dieser Punkt gibt Ihnen die Möglichkeit, im normalerweisen schwarzen Randbereich eines analogen Monitors ebenfalls eine Farbe darzustellen. Bei einem HDMI-Monitor bzw. -Fernseher belassen Sie die Option auf `disable`.
- `configure_keyboard`: Hier stellen Sie das Tastaturlayout ein, üblicherweise zuerst `Generic 105-key Intl PC`, dann `German`. Alle weiteren Optionen können Sie auf der vorgeschlagenen Defaulteinstellung belassen. Die Einstellung gilt gleichermaßen für den Text- und den Grafikmodus.
- `change_pass`: Standardmäßig ist in Raspbian der Benutzer `pi` mit dem Passwort `raspberry` eingestellt. Dieses Passwort sollten Sie unbedingt ändern!
- `change_locale`: Hier stellen Sie die Systemsprache ein, üblicherweise `de_DE.UTF-8`.
- `change_timezone`: Hier stellen Sie die Zeitzone ein, üblicherweise `Europe/Berlin`. Beachten Sie, dass der Raspberry Pi keine batteriegepufferte Uhrzeit hat und deswegen bei jedem Neustart mit derselben Zeit beginnt. Wenn das Sie stört, schließen Sie den Raspberry Pi an ein Netzwerk an, über das der Rechner die aktuelle Uhrzeit via NTP beziehen kann.

- `memory_split`: Gibt an, wie viel Speicher für das Grafiksystem und wie viel für das Betriebssystem reserviert wird. Hintergrundinformationen zu dieser Einstellung finden Sie in Abschnitt 12.5.
- `overclock`: Die CPU des Raspberry Pi läuft standardmäßig mit 700 MHz. Mit diesem Menüpunkt können Sie die Frequenz auf bis zu 1 GHz erhöhen. Viele Raspberry Pi-Benutzer haben damit aber schlechte Erfahrungen gemacht: Abstürze, defekte Dateisysteme etc. waren die Folge. Vermeiden Sie Overclocking!
- `ssh`: Hier können Sie den SSH-Server aktivieren. Ändern Sie unbedingt vorher das Default-Passwort des Benutzers `pi`!
- `boot_behaviour`: Soll der Raspberry Pi im Text- oder im Grafikmodus starten? Beachten Sie, dass standardmäßig keine Login-Box erscheint. Jeder, der Zugang zum Minirechner hat, kann also damit arbeiten!
- `update`: Aktualisiert das Paket des Konfigurationsprogramms. Das funktioniert nur, wenn der Raspberry Pi über ein Ethernet-Kabel mit einem lokalen Netzwerk mit DHCP-Server verbunden ist.

Ein Teil der Einstellungen wird erst nach einem Neustart des Minicomputers wirksam. Das Konfigurationsprogramm erscheint nur beim ersten Start des Raspberry Pi automatisch, es kann aber bei Bedarf jederzeit mit dem Kommando `sudo raspi-config` neuerlich ausgeführt werden.

Erste Schritte

Sofern Sie im Konfigurationsprogramm den Grafikmodus aktiviert haben, erscheint beim nächsten Neustart direkt der Xfce-Desktop (siehe auch Abbildung 12.4 sowie Abschnitt 7.2). In Textkonsolen müssen Sie sich mit dem Login-Namen `pi` und Ihrem Passwort einloggen. Wenn Sie das Passwort nicht im Rahmen der Erstkonfiguration verändert haben, lautet es `raspberry`. Wenn Sie das Booten im Grafikmodus aktiviert haben, können Sie dort ohne Login als Benutzer `pi` arbeiten.

sudo

Administratorarbeiten führen Sie mit `sudo` aus (siehe auch Abschnitt 16.3). Der Benutzer `pi` darf `sudo` ohne Passwort benutzen. Wenn Sie `sudo`-Aktivitäten durch ein Passwort absichern möchten, stellen Sie mit einem Editor der letzten Zeile von `/etc/sudoers` ein Kommentarzeichen # voran. Wegen der weiter oben enthaltenen Regel für die Gruppe `sudo` kann `pi` weiterhin `sudo` nutzen, allerdings muss nun nochmals das eigene Passwort angegeben werden.

```
# /etc/sudoers
...
%sudo   ALL=(ALL:ALL) ALL
...
# pi ALL=(ALL) NOPASSWD: ALL
```

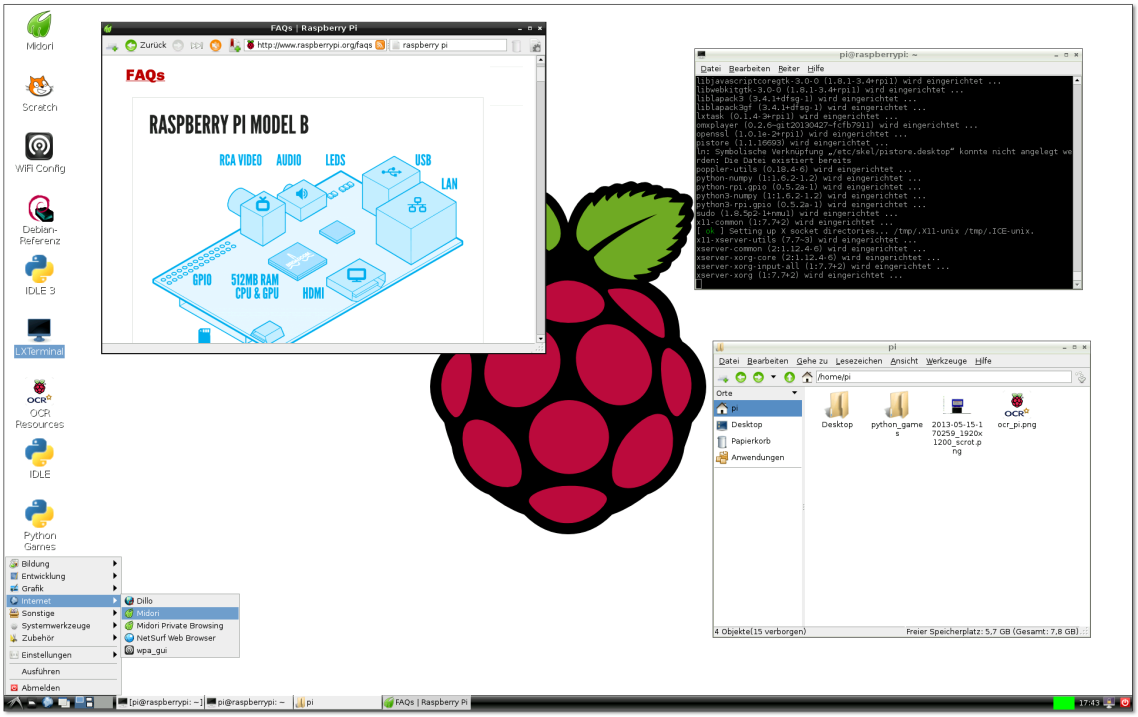


Abbildung 12.4 Der Xfce-Desktop von Raspbian

Ein- und ausschalten

Der Raspberry Pi ist für den Dauerbetrieb gedacht – es gibt keinen Schalter zum Ein- und Ausschalten. Um das Gerät sicher auszuschalten, müssen Sie es zuerst herunterfahren. Dazu führen Sie im Xfce-Menü ABMELDEN • AUSSCHALTEN oder im Textmodus `sudo halt` aus. Sobald das Bild auf dem Bildschirm verschwindet und keine der LEDs des Geräts mehr blinkt, können Sie das Kabel zur Stromversorgung lösen. Sobald Sie das Gerät wieder anstecken, wird es automatisch neu gestartet.

Achtung

Vermeiden Sie es, einfach im laufenden Betrieb die Stromversorgung zu trennen! Ihr Raspberry Pi kann dann das Dateisystem nicht ordentlich herunterfahren. Normalerweise passiert nichts, aber Sie riskieren nicht nur einzelne defekte Dateien, sondern sogar ein inkonsistentes Dateisystem auf der SD-Karte. Im schlimmsten Fall müssen Sie Raspbian oder eine andere Linux-Distribution neu auf die SD-Karte schreiben und verlieren alle Ihre Daten!

Update

Sobald Sie eine Netzwerkverbindung hergestellt haben, sollten Sie ein Update von Rasbian durchführen:

```
user$  sudo apt-get update
user$  sudo apt-get dist-upgrade
```

Sie werden feststellen, dass das Update im Vergleich zu einem Notebook relativ lange dauert. Das hat zwei Gründe: Einerseits braucht die relativ leistungsschwache CPU viel länger zum Dekomprimieren der Paketdateien, andererseits sind selbst schnelle SD-Karten deutlich langsamer als herkömmliche Festplatten.

Das Update ist aber in jedem Fall ein guter Stabilitätstest für Ihr frisch installiertes System. Es beansprucht alle Komponenten des Computers. Wenn das Update fehlerfrei abgeschlossen wird, können Sie zuversichtlich sein, dass Ihr Minicomputer stabil läuft.

Auto-Login

Standardmäßig gilt für die grafische Benutzeroberfläche ein Auto-Login ohne Angabe eines Passworts. Wenn Sie den Desktop durch eine Login-Box absichern möchten, deaktivieren Sie den Auto-Login, indem Sie in `/etc/lightdm.conf` der Zeile `autologin-user=pi` ein Kommentarzeichen voranstellen. Gleichzeitig sollten Sie auch die Einstellung für `greeter-hide-users` von `true` auf `false` stellen:

```
/etc/lightdm/lightdm.conf
...
greeter-hide-users=false
# autologin-user=pi
```

Automatischer Start des Grafiksystems

Den automatischen Start des Grafiksystems können Sie mit `raspi-config` oder mit dem Kommando `insserv` aktivieren bzw. deaktivieren:

```
root#  insserv    lightdm    (Grafiksystem automatisch starten)
root#  insserv -r lightdm    (Grafiksystem nicht starten)
```

Screenshots

Standardmäßig gibt es in Raspbian kein Programm, um Screenshots zu erstellen. Abhilfe: Installieren Sie mit `sudo apt-get install scrot` das winzige Programm `scrot`. Dieses starten Sie in einem Terminalfenster, wobei Sie mit der Option `-d` angeben, nach wie vielen Sekunden ein Screenshot des gesamten Bildschirms erstellt werden soll.

```
user$  scrot -d 5
```

`scrot` speichert die resultierende PNG-Datei im aktuellen Verzeichnis, wobei sich der Dateiname aus dem Datum, der Uhrzeit und der Bildschirmauflösung ergibt.

WLAN-Verbindung herstellen

Sofern Ihr Raspberry Pi über ein Netzwerkkabel mit einem lokalen Netzwerk verbunden ist, stellt der Minicomputer automatisch eine Netzwerkverbindung her. Die Konfiguration einer WLAN-Verbindung erfordert nicht nur einen USB-WLAN-Dongle, sondern auch ein wenig Arbeit. Vor dem Kauf eines USB-WLAN-Steckers sollten Sie ein wenig recherchieren, damit Sie ein Modell erhalten, das von Raspbian auf Anhieb unterstützt wird. Das trifft z. B. für die weit verbreiteten USB-Stecker mit RTL81xx-Chips zu. Ich habe für meine Tests das Modell EDIMAX-7811 verwendet, das keinerlei Probleme bereitete.

WLAN-Treiber

Nachdem Sie den USB-WLAN-Adapter angesteckt haben, stellen Sie mit `lsusb` das Modell fest:

```
user$  lsusb
...
Bus 001 Device 004: ID 7392:7811 Edimax Technology Co.,
  Ltd EW-7811Un 802.11n Wireless Adapter [Realtek RTL8188CUS]
```

Alle erforderlichen Treiber für die RTL81xx-Chipfamilie sind standardmäßig installiert, und das zuständige Kernelmodul `8192cu` wird automatisch geladen. Davon können Sie sich mit `lsmod` überzeugen:

```
root#  lsmod
Module                  Size  Used by
...
8192cu                490305  0
```

Bei anderen WLAN-Adaptern kann es sein, dass Sie ein zusätzliches Paket mit dem Treiber installieren bzw. eine Firmware-Datei aus dem Internet herunterladen müssen. Anleitungen für unzählige WLAN-Stecker finden Sie hier:

http://elinux.org/RPi_VerifiedPeripherals#USB_Wi-Fi_Adapters

Konfiguration

Zur Konfiguration des WLAN-Zugangs starten Sie im Grafikmodus das Programm `wpa_gui` (siehe Abbildung 12.5). Dort wählen Sie im Listenfeld ADAPTER die WLAN-Schnittstelle aus. Normalerweise ist das `wlan0`. Der Button SCAN führt in einen Dialog, der alle in Reichweite befindlichen WLAN-Netze auflistet. Ein Doppelklick auf das gewünschte Netz führt in einen weiterem Konfigurationsdialog, in dem Sie das Passwort für die WLAN-Verbindung angeben können. Bei WPA-verschlüsselten Netzen verwenden Sie dazu das Eingabefeld PSK.

Mit dem Button ADD fügen Sie die neue Verbindung zur Liste der bekannten Netzwerke hinzu. Die Verbindungsdaten werden in der Datei `/etc/wpa_supplicant/wpa_supplicant.conf` gespeichert (mit dem WLAN-Passwort im Klartext!). Zu diesem Netzwerk wird von nun an automatisch eine Verbindung hergestellt, auch dann, wenn der Raspberry Pi im Textmodus gestartet wird.

Den Raspberry Pi als WLAN-Access-Point einsetzen

Wenn Sie Ihren Raspberry Pi als Access-Point verwenden möchten, brauchen Sie einen WLAN-Adapter, der den Access-Point-Modus unterstützt. Das ist nicht bei allen Modellen der Fall! Außerdem müssen Sie das Paket `hostapd` installieren und konfigurieren. Ausführliche Anleitungen finden Sie beispielsweise hier:

http://elinux.org/RPI-Wireless-Hotspot
http://www.tacticalcode.de/2013/02/
raspberry-pi-als-accesspoint-oder-wlan-bridge.html

Es gibt für diese Art der Anwendung sogar ein eigenes Linux-Image:

http://www.pi-point.co.uk

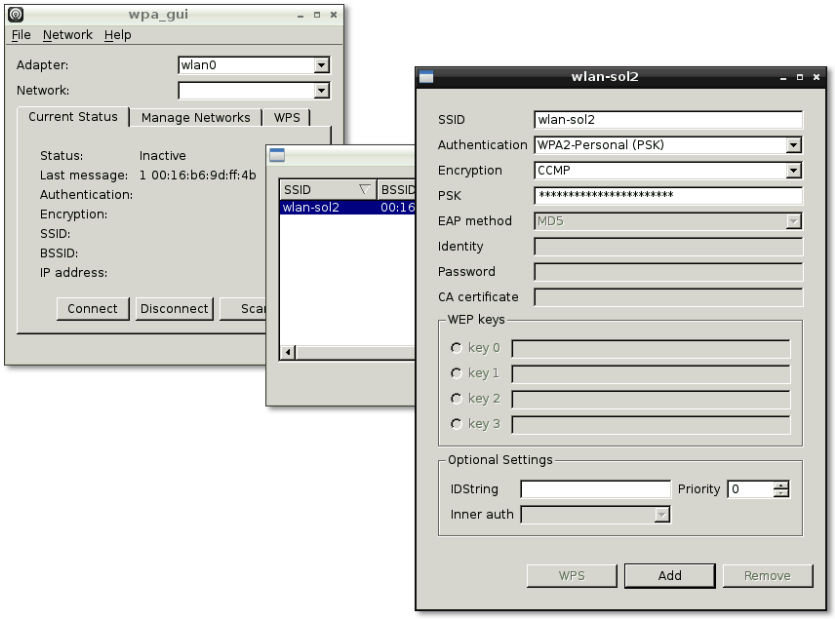


Abbildung 12.5 WLAN-Konfiguration

Bluetooth

Damit Sie Ihren Raspberry Pi mit Bluetooth-Geräten bedienen können, benötigen Sie einen USB-Bluetooth-Stecker, den Sie für wenige Euro bei jedem Computer-Händler erwerben können. Die meisten Modelle funktionieren auf Anhieb – recherchieren Sie dennoch *vor* dem Kauf!

http://elinux.org/RPi_VerifiedPeripherals#USB_Bluetooth_adapters

Hardware ...

Ob Ihr Bluetooth-Dongle richtig erkannt wird, stellen Sie am einfachsten mit `lsusb`, `lsmod` und `dmesg` fest. Mein Testkandidat von MSI funktioniert zum Glück ohne jede Konfiguration.

```
user$  lsusb
...
Bus 001 Device 008: ID 0a12:0001 Cambridge Silicon Radio, Ltd
  Bluetooth Dongle (HCI mode)
user$  lsmod | grep -i blue
bluetooth             193568  2 btusb
rfkill                 18202  1 bluetooth
user$  dmesg | grep -i bluetooth
[    9.182653] Bluetooth: Core ver 2.16
[    9.362510] Bluetooth: HCI device and connection manager initialized
[    9.512513] Bluetooth: HCI socket layer initialized
[    9.632518] Bluetooth: L2CAP socket layer initialized
[    9.662557] Bluetooth: SCO socket layer initialized
```

... und Software

Der Kerneltreiber für den Bluetooth-Dongle ist freilich erst die halbe Miete. Sie brauchen auch Software, die beim Verbindungsaufbau mit Bluetooth-Geräten hilft und sich um die eigentlichen Kommunikation kümmert. Die Installation der folgenden drei Pakete dauert wegen vieler Abhängigkeiten recht lange: So werden unter anderem unzählige Druckerpakete (CUPS) installiert. Der zusätzliche Platzbedarf auf der SD-Karte beträgt fast 100 MByte. Wenn Ihre SD-Karte nur 2 GByte groß ist, wird der Platz knapp.

```
root#  apt-get install bluetooth bluez-utils blueman
```

Im Einstellungsmenü des Xfce-Desktops können Sie nun den Bluetooth-Manager starten (siehe Abbildung 12.6). SUCHE liefert eine Liste aller in Funkreichweite befindlichen Bluetooth-Geräte. Per Kontextmenü können Sie nun eine Verbindung zu den Geräten herstellen bzw. diese als Eingabegeräte (Tastatur, Maus) verwenden. Letzteres funktionierte bei meinen Tests problemlos, an der Übertragung einer Datei zwischen dem Raspberry Pi und meinem Smartphone bin ich aber gescheitert.

Abbildung 12.6 Der Bluetooth-Manager

12.3 Einsatz als Multimedia-Center

Das XBMC Media Center (ehemals XBox Media Center, daher die Abkürzung XBMC) ist eine Sammlung von Open-Source-Programmen zur Verwendung eines Linux-Computers als Multimedia-Center. Je nach Hardware-Voraussetzungen können Sie damit Folgendes machen:

- auf lokalen Datenträgern oder im lokalen Netzwerk verfügbare Audio- und Video-Dateien abspielen (SMB, NFS, DNLS)
- CDs und DVDs abspielen (erfordert ein externes Laufwerk)
- Live fernsehen (erfordert eine Karte zum TV-Empfang)
- TV-Sendungen aufzeichnen
- YouTube, diverse Mediatheken, Internet-Radios und -Fernsehstationen nutzen (erfordert die Installation von Add-ons)
- Video-Streams und Bilder von iOS-Geräten anzeigen (AirPlay)
- Fotos ansehen
- den Wetterbericht lesen

Das Abspielen von CDs/DVDs sowie der Empfang traditioneller Fernsehprogramme ist auf einem Raspberry Pi aufgrund der fehlenden Hardware-Voraussetzungen nicht möglich. Üblicherweise wird ein Raspberry Pi primär zum Abspielen von Audio- und Video-Dateien oder Streams verwendet, die im Internet oder im lokalen Netzwerk zur Verfügung stehen. Ideal lässt sich XBMC in Kombination mit einem NAS-Gerät nutzen, das die Foto-, Audio- und Video-Sammlung des Haushalts enthält.

Die Bedienung des Geräts kann wie bei einem Computer mit Tastatur und Maus, aber auch durch eine IR-Fernbedienung oder durch ein Smartphone erfolgen.

Ich konzentriere mich in diesem Kapitel auf die Raspberry-Pi-spezifischen Besonderheiten von XBMC. Auf die eigentliche Bedienung von XBMC gehe ich hingegen nur kurz ein – die lässt sich rasch durch Ausprobieren erlernen. Außerdem gibt es ein umfassendes, als Wiki organisiertes Handbuch:

http://wiki.xbmc.org

XBMC-Distributionen für den Raspberry Pi

Speziell für den Raspberry Pi gibt es gleich drei Distributionen, die den Minicomputer zum Medien-Center machen:

- Raspbmc: *http://www.raspbmc.com*
- XBian: *http://xbian.org*
- OpenELEC: *http://openelec.tv*

Natürlich gibt es geteilte Meinungen darüber, welches nun die beste XBMC-Variante ist. OpenELEC ist das kleinste System; es geht sparsam mit dem Speicherplatz auf Ihrer SD-Karte und den Leistungsressourcen der CPU um. XBian und Raspbmc basieren beide auf Debian und bieten mehr Funktionen und Erweiterungsoptionen. Für die Arbeit an diesem Kapitel habe ich mich für Raspbmc entschieden.

Persönliche Einschätzung von XBMC auf dem Raspberry Pi

Der Raspberry Pi wird häufig als Media-Center eingesetzt. Mich selbst hat diese Art der Anwendung aber nicht restlos begeistern können: Die Bedienung von XBMC ist mitunter unübersichtlich und nicht wirklich wohnzimmertauglich. Die Konfiguration ist aufwendig, viele Zusatzfunktionen erfordern oft stundenlange Basteleien. Schließlich strapaziert XBMC die Hardware des Raspberry Pi bis an die Grenzen; XBMC reagiert deswegen oft träge und mit deutlichen Verzögerungen auf Eingaben.

Vorsicht – Overclocking!

Raspbian und XBian verwenden standardmäßig ein leichtes Overclocking. Das lässt diese XBMC-Varianten etwas schneller erscheinen. Die Entwickler von Raspbian und XBian argumentieren, dass das Overclocking moderat sei (800 bzw. 850 MHz statt 700 MHz) und gemäß offizieller Angaben (*http://www.raspberrypi.org/archives/2008*) weder die Stabilität noch die Lebensdauer des Raspberry Pi gefährden würde.

Sie können das Overclocking bei allen Distributionen in der Datei `config.txt` in der Boot-Partition steuern bzw. abschalten. Die Overclocking-Verlockung ist groß, weil der Raspberry Pi für den XBMC-Einsatz an der Grenze seiner Leistungsfähigkeit läuft. Allen Beteuerungen zum Trotz riskieren Sie damit aber sehr wohl Stabilitätsprobleme und ein vorzeitiges Ableben Ihres Minicomputers.

Raspbmc installieren

Sofern Sie Ihren Raspberry Pi über ein Ethernet-Kabel an das lokale Netzwerk anschließen können, sieht die empfohlene Installationsweise für Raspbmc so aus: Sie laden von der Raspbmc-Download-Seite das Network-Image herunter, dekomprimieren die Datei und schreiben sie mit `dd` auf die SD-Karte. Die folgenden Kommandos gehen wieder davon aus, dass die SD-Karte das Device `/dev/sdb` hat – das kann bei Ihnen anders sein!

```
user$  gunzip installer.img.gz
root#  umount /dev/sdb?
root#  dd if=installer.img of=/dev/sdb bs=4M
```

Die Image-Datei ist mit ca. 80 MByte erstaunlich klein. Das liegt daran, dass sie nur ein Installationsprogramm enthält, das beim ersten Start auf Ihrem Raspberry Pi ausgeführt wird und dann über die Netzwerkverbindung alle weiteren Pakete direkt aus dem Internet herunterlädt und die eigentliche Installation durchführt. Diese dauert – abhängig von der Geschwindigkeit Ihres Internetzugangs – etwa eine viertel Stunde. Danach füllt Raspbmc circa 1 GByte Ihrer SD-Karte.

Nach einem automatischen Neustart und einigen weiteren Vorbereitungsarbeiten erscheint schließlich erstmalig die grafische Benutzeroberfläche von XBMC. Sie müssen nun die gewünschte Sprache einstellen. Anschließend wird der Minicomputer ein weiteres Mal neu gestartet.

Raspbmc konfigurieren

Raspbmc Settings

In der grafischen Benutzeroberfläche von XBMC sollten Sie als Erstes zum Hauptmenüpunkt PROGRAMME navigieren und dort das Raspbmc-eigene Konfigurationsprogramm RASPBMC SETTINGS starten (siehe Abbildung 12.7). Dort können Sie einige Grundeinstellungen der Raspbmc-Konfiguration verändern. Dazu zählen:

- die Netzwerkkonfiguration (inklusive WLAN)
- automatische Updates
- das Passwort für den Benutzer *pi*
- die IR-Fernbedienung

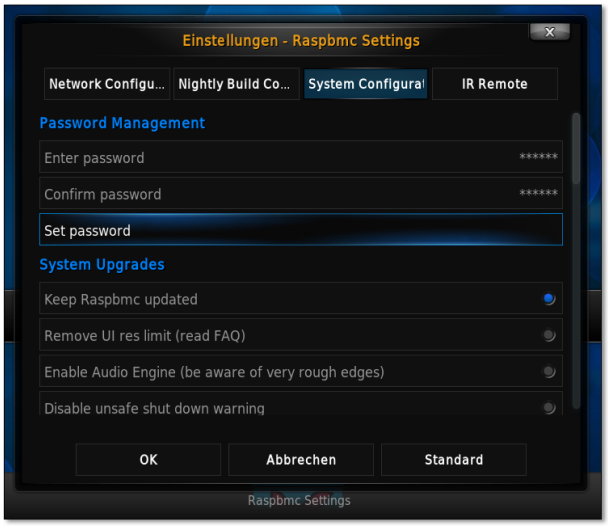


Abbildung 12.7 Raspbmc Settings

Passwort ändern

Aus Sicherheitsgründen sollten Sie im Programm RASPBMC SETTINGS unbedingt das Passwort des Benutzers *pi* verändern. Beachten Sie, dass dabei das US-Tastaturlayout gilt. Wie Sie das Tastaturlayout ändern, erfahren Sie im nächsten Abschnitt *Eingabegeräte*.

Sicherheitsrisiko SSH-Server

In Raspbmc ist standardmäßig ein SSH-Server aktiv. Jeder Benutzer im lokalen Netzwerk kann sich mit dem Benutzernamen *pi* und dem Default-Passwort *raspberry* einloggen. Daraus ergeben sich natürlich massive Sicherheitsrisiken. Ändern Sie also unbedingt das Passwort!

Netzwerkkonfiguration und WLAN

Raspbmc bezieht die Netzwerkkonfiguration via DHCP, sofern das Gerät über ein Ethernet-Kabel mit einem lokalen Netzwerk verbunden ist. Eine statische IP-Konfiguration können Sie im Dialog NETWORK CONFIGURATION in den RASPBMC SETTINGS durchführen.

Dieser Dialog ist auch für die WLAN-Konfiguration zuständig. Dazu stellen Sie zuerst den NETWORK MODE auf WIRELESS NETWORK um und geben dann im Feld WIFI SSID den Namen Ihres WLAN-Netzwerks ein. Leider gibt es hierfür keine Scan-Funktion samt Auswahl aus einer Dropdown-Liste. Im Listenfeld WIFI SECURITY können Sie zwischen verschiedenen WLAN-Verschlüsselungssystemen wählen; am gängigsten ist WPA/WPA2. Außerdem müssen Sie im Feld WIFI KEY Ihr WLAN-Passwort angeben. Wenn Sie das US-Tastaturlayout nicht im Kopf haben, sollten Sie vor der WLAN-Konfiguration das Tastaturlayout ändern, wie dies im Abschnitt *Eingabegeräte* beschrieben ist.

Nach Abschluss der Konfiguration sind in der Raspbmc-Oberfläche kurze Statusnachrichten zu sehen. Wenn Sie der Sache nicht trauen, öffnen Sie das Dialogblatt SYSTEM • SYSTEMINFO • NETZWERK, das die Eckdaten der Netzwerkverbindung anzeigt.

MPEG-2- und VC-1-Hardware-Decoding

Der Grafikprozessor des Raspberry Pi kann zur Hardware-Decodierung mancher Video-Codecs eingesetzt werden. Wenn Sie MPEG-2- oder VC-1-Videos auf Ihrem Raspberry Pi ansehen möchten, sind diese Schlüssel *zwingend* erforderlich. Ohne die Schlüssel macht Raspbmc aufgrund der unzureichenden CPU-Leistung nicht einmal den Versuch einer Decodierung und spielt nur den Ton ab.

Die Hardware-Decodierung muss durch einen Lizenzschlüssel freigeschaltet werden. Diese Schlüssel können Sie auf der Website *http://www.raspberrypi.com* erwerben, wobei momentan nur die Codecs MPEG-2 und VC-1 unterstützt werden. Der VC-1-Codec wird von Blu-ray-Discs und in WMV-Dateien verwendet.

Beim Kauf müssen Sie die Seriennummer Ihres Raspberry Pi angeben. Diese können Sie der Datei `/proc/cpuinfo` entnehmen oder im Dialogblatt SYSTEM • SYSTEMINFO • HARDWARE finden.

```
pi$  grep Serial /proc/cpuinfo
Serial          : 0000000013579bdf
```

Beide Schlüssel zusammen kosten momentan etwas mehr als 4 EUR. Zum Bezahlen müssen Sie PayPal verwenden. Sie erhalten den Freischaltcode nach einer Weile per E-Mail. Der Raspberry Pi Store verspricht eine Zusendung innerhalb von 72 Stunden, bei mir hat es aber nur eine Stunde gedauert. Der Code ist mit der Seriennummer verknüpft und gilt somit nur für Ihren Raspberry Pi.

Sobald Sie den bzw. die Schlüssel erhalten haben, können Sie diese im Dialogblatt SYSTEM CONFIGURATION im Programm RASPBMC SETTINGS angeben (inklusive des vorangestellten Codes `0x` zur Kennzeichnung als hexadezimale Zahl). Alternativ können Sie die Schlüssel auch direkt in die Datei `/boot/config.txt` eintragen:

```
# Datei /boot/config.txt
...
decode_MPG2=0x12345678
decode_WVC1=0x9abcedf0
```

Die Einstellungen werden nach dem nächsten Neustart des Raspberry Pi wirksam. Ob alles funktioniert hat, können Sie in der Konsole oder via SSH (siehe etwas weiter unten) wie folgt verifizieren:

```
pi$  vcgencmd codec_enabled MPG2
MPG2=enabled
pi$  vcgencmd codec_enabled WVC1
WVC1=enabled
```

Wechsel in die Konsole

Über den Einschaltknopf links unten können Sie XBMC verlassen und sich dann in einer Konsole einloggen. Dabei verwenden Sie den Benutzernamen `pi` und Ihr Passwort. Falls Sie das Standardpasswort *raspberry* noch nicht geändert haben, ist jetzt der richtige Zeitpunkt!

Administrationsarbeiten erledigen Sie mit `sudo`, wobei keine weitere Passworteingabe erforderlich ist. Nach dem Logout erscheint automatisch wieder XBMC.

SSH

Raspbmc aktiviert standardmäßig einen SSH-Server. Jeder, der Netzwerkzugriff auf den Raspberry Pi hat, kann sich einloggen.

Screenshots

Mit der auf vielen PC-Tastaturen vorgesehenen Taste Druck können Sie Screenshots erstellen. Wo diese gespeichert werden, stellen Sie mit SYSTEM • EINSTELLUNGEN • SYSTEM • DEBUGGING ein.

Wenn Sie an Ihren Raspberry Pi keine Tastatur mit der Taste Druck angeschlossen haben, können Sie Screenshots auch via SSH zu erstellen. Dazu installieren Sie zuerst das Paket `xbmc-eventclients-xbmc-send`. Mit `xbmc-send` können Sie nun das Screenshot-Kommando auslösen:

```
pi$  xbmc-send --host=127.0.0.1 -a "TakeScreenshot"
```

Eingabegeräte

Normalerweise gibt es im Betrieb eines Raspberry Pi als Medien-Center zwei Phasen: In der ersten Phase konfigurieren Sie das Gerät. Während dieser Phase sind Tastatur und Maus natürlich praktisch.

Ist die Konfiguration abgeschlossen, beginnt Phase zwei – die Nutzung des Geräts: Im einfachsten Fall reicht hierfür die Fernbedienung Ihres Fernsehgeräts aus. Dessen Signale werden nämlich bei modernen TV-Geräten via HDMI an den Raspberry Pi weitergeleitet. Alternative Steuerungsgeräte sind eine eigene Fernbedienung für den Raspberry Pi (erfordert einen zusätzlichen IR-Empfänger für den Raspberry Pi) oder die Bedienung durch eine XBMC-App auf dem Smartphone oder Tablet. Dieser Abschnitt gibt Tipps zur Konfiguration und Anwendung verschiedener Eingabegeräte.

Tastatur und Maus

Die Konfigurationsphase meistern Sie am einfachsten mit einer USB-Tastatur und einer USB-Maus.

Deutsches Tastaturlayout

Für alle Tastatureingaben gilt das US-Tastaturlayout. Abhilfe: Loggen Sie sich in einer Textkonsole oder via SSH ein, öffnen Sie mit dem Editor `vi` oder `nano` die Datei `/etc/default/keyboard`, und führen Sie folgende Änderung durch:

```
# /etc/default/keyboard
XKBLAYOUT="de"
```

Anschließend führen Sie diese Kommandos aus:

```
root#  setupcon
root#  udevadm trigger --subsystem-match=input --action=change
root#  reboot
```

Die Eingabe der meisten Zeichen funktioniert nun problemlos. Die Eingabe der Buchstaben äöüß ist leider weiterhin unmöglich.

Bluetooth-Geräte

Die Verwendung von Bluetooth-Eingabegeräten unter Raspbmc ist problematisch. Die erstmalige Konfiguration muss in einer Konsole oder mit SSH erfolgen. Eine gute Beschreibung finden Sie hier:

http://rienajouter.blogspot.co.at/2013/02/using-raspbmc-with-bluetooth-keyboard.html

Das eigentliche Problem ist aber, dass XBMC nur die Bluetooth-Geräte nutzt, zu denen beim Start von XBMC eine aktive Verbindung besteht. Um später hinzugekommene Geräte verwenden zu können, muss XBMC neu gestartet werden (z.B. via SSH mit `service xbmc restart`). Mir ist es bei meinen Tests nicht gelungen, eine Bluetooth-Tastatur und -Maus zuverlässig und stabil in ein Raspbmc-System zu integrieren.

Fernbedienung

CEC-Fernbedienung

Im Idealfall können Sie XBMC direkt mit der Fernbedienung Ihres TV-Geräts bedienen. Die meisten modernen Fernseher leiten Signale der Fernbedienung, die nicht für das TV-Gerät bestimmt sind, über das HDMI-Kabel via CEC (Consumer Electronics Control) an den Raspberry Pi weiter. Dieser verarbeitet dann die Signale. Laut Forenberichten funktioniert dieses Verfahren bei vielen Fernsehern auf Anhieb. Meine eigenen Erfahrungen mit einem ca. vier Jahre alten Sony-Bravia-Fernseher waren aber negativ: obwohl das Gerät CEC an sich unter dem Sony-Markennamen »Bravia Sync« unterstützt, erkannte es den Raspberry Pi nicht als CEC-taugliches HDMI-Gerät.

GPIO-IR-Empfänger

Wenn die TV-Fernbedienung somit nicht funktioniert und Sie auch nicht ein Smartphone zur Bedienung verwenden möchten (siehe unten), können Sie Ihren Raspberry Pi wie in Abschnitt 12.4 beschrieben selbst um einen IR-Empfänger erweitern. Das ist nicht schwierig, selbst Elektronik-Einsteiger werden dabei nicht überfordert.

LIRC-Konfiguration

Wesentlich schwieriger ist leider die Konfiguration: Dazu starten Sie das Programm Raspbmc Settings und aktivieren im Dialogblatt IR-Remote die Option Enable GPIO TSOP IR Receiver. Mit sehr viel Glück finden Sie im Punkt GPIO IR Remote Profile Ihr Fernbedienungsmodell und wählen es aus. Die Einstellungen werden als Link (Datei `/etc/lirc/lircd.conf`) gespeichert. Allerdings sind momentan mehrere Tausend unterschiedliche IR-Fernbedienungsmodelle im Umlauf, *Raspbmc Settings* kennt aber gerade acht! Und selbst wenn Sie eines davon besitzen, heißt das noch lange nicht, dass nun alles auf Anhieb funktioniert. Ich habe meine Tests mit der Fernbedienung eines Apple-TV-Geräts durchgeführt. Diese Fernbedienung zählt zu den wenigen von Raspbmc unterstützten Geräten – und funktionierte dennoch nicht!

In aller Regel ist somit Handarbeit erforderlich. Die folgenden Arbeiten führen Sie entweder in einer Konsole oder via SSH durch. Damit Sie die Low-Level-Konfiguration durchführen können, müssen Sie den LIRC-Dämon stoppen. LIRC steht für *Linux Infrared Remote Control* und ist ein Paket von Programmen, das IR-Signalen verarbeitet.

```
root#  service lirc stop
```

Nun können Sie das Programm `irrecord` starten. Es erzeugt die neue Konfigurationsdatei `/home/pi/lircd.conf`. Während das Programm läuft, müssen Sie zuerst wahllos 160-Mal eine Taste Ihrer Fernbedienung drücken. Jede Taste sollte mindestens einmal gedrückt werden.

```
root#  irrecord -d /dev/lirc0 /home/pi/lircd.conf
  irrecord -  application for recording IR-codes for usage with lirc
  ...
  Now start pressing buttons on your remote control. Don't stop pressing
  buttons until two lines of dots (2x80) have been generated.
  ...
```

In der zweiten Phase müssen Sie jeweils zuerst einen LIRC-Tastennamen angeben und dann die entsprechende Taste auf Ihrer Fernbedienung drücken. Mit ↵ schließen Sie diese überaus mühsame Konfiguration schließlich ab.

```
  Now enter the names for the buttons.
  Please enter the name for the next button (press <ENTER> to finish recording)
   KEY_UP
  Now hold down button "KEY_UP".
   <Pfeil hinauf der Fernbedienung>

  Please enter the name for the next button (press <ENTER> to finish recording)
   KEY_DOWN
  Now hold down button "KEY_DOWN".
   <Pfeil hinunter der Fernbedienung>
  ...
```

Welche LIRC-Tastennamen es gibt, ermitteln Sie am besten im Voraus mit `irrecord -l`:

```
root#  irrecord -l | grep KEY
KEY_0
KEY_102ND
KEY_1
KEY_2
...
```

Wenn die Konfiguration abgeschlossen ist, richten Sie einen Link auf Ihre Konfigurationsdatei ein und starten den LIRC-Dämon neu.

```
root#  cd /etc/lirc
root#  mv lircd.conf lircd.conf.bak
root#  ln -s /home/pi/lircd.conf .
root#  service lirc start
```

Sie können nun mit dem Kommando `irw` testen, ob die Signale Ihrer Fernbedienung richtig weiterverarbeitet werden. `irw` kommuniziert mit dem LIRC-Dämon und zeigt jede erkannte Taste an:

```
root#  irw
0000000077e1d030 00 KEY_UP lircd.conf
0000000077e11030 00 KEY_LEFT lircd.conf
0000000077e1b030 00 KEY_DOWN lircd.conf
0000000077e1e030 00 KEY_RIGHT lircd.conf
...
<Strg>+<C>
```

Nach einem Neustart sollte auch XBMC auf Ihre Fernbedienung reagieren. Weitere Tipps und Hilfe bei der Konfiguration von Fernbedienungen finden Sie hier:

http://wiki.xbmc.org/index.php?title=HOW-TO:Setup_Lirc
http://forum.stmlabs.com/showthread.php?tid=6201
http://forum.stmlabs.com/showthread.php?tid=5549

XBMC-Apps

Anstelle einer IR-Fernbedienung können Sie zur Steuerung des Media-Centers auch eine XBMC-App für Android- oder iOS-Geräte verwenden (siehe Abbildung 12.8). Entsprechende Apps sind kostenlos im Google PlayStore oder im AppStore von Apple erhältlich.

Damit XBMC Signale der Apps verarbeitet, müssen Sie in XBMC im Dialogblatt System • Einstellungen • Dienste • Fernsteuerung die Option Steuerung über entfernte Programme zulassen aktivieren.

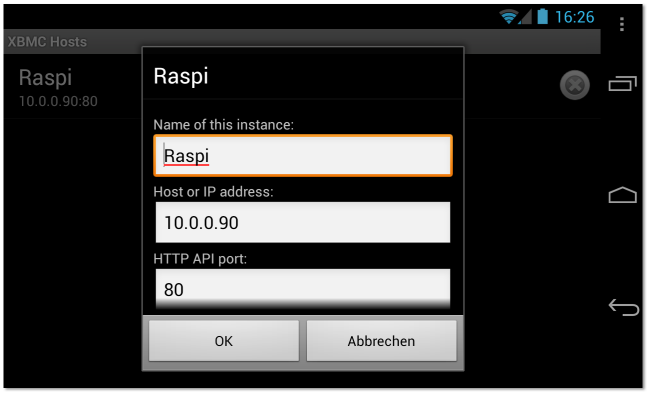


Abbildung 12.8 Konfiguration der XBMC-App auf einem Android-Smartphone

Die XBMC-Steuerung durch das Smartphone oder Tablet erfolgt über WLAN. Bei der Konfiguration der XBMC-App müssen Sie den Hostnamen oder die IP-Adresse Ihres Raspberry Pi angeben. Beachten Sie, dass der XBMC-Webserver von Raspbmc standardmäßig den Port 80 verwendet. Viele Apps sind hingegen für den Port 8080 vorkonfiguriert.

XBMC-Konfiguration

Losgelöst von der Raspbmc-spezifischen Konfiguration sieht auch XBMC selbst unzählige Einstellungen vor. Den Großteil davon verändern Sie im Programm System • Einstellungen (siehe Abbildung 12.9). Ausgehend von einem Hauptmenü gelangen Sie in weitere Einstellungsdialoge.

Abbildung 12.9 XBMC-Einstellungen

Darstellung

Sogenannte *skins* steuern den Hintergrund der XBMC-Benutzeroberfläche und ihrer Dialoge. Im Dialog Darstellung können Sie ergänzend zum XBMC-Defaultskin Confluence weitere Skins herunterladen und aktivieren. Beachten Sie aber, dass manche Skins große Anforderungen an das Grafiksystem stellen und für den Raspberry Pi deswegen ungeeignet sind. Die XBMC-FAQ für den Raspberry Pi empfiehlt neben Confluence unter anderem die Skins Metropolis, Quartz und Quartz Reloaded. Persönlich hat mir auch Ace gut gefallen.

Dienste

Im Dialog Dienste können Sie die AirPlay-Funktionen von XBMC aktivieren und steuern, ob die Funktionen von XBMC auch über einen Webbrowser genutzt werden können (das ist standardmäßig der Fall), ob dieser Zugriff durch ein Passwort abgesichert werden soll (das ist standardmäßig nicht der Fall), ob Raspbmc durch externe Geräte wie Smartphones im Netz ferngesteuert werden darf etc. Die meisten Einstellungen richten sich an fortgeschrittene XBMC-Anwender.

Audio-Einstellungen und Grafiksystem

Der Dialog System hilft bei der Konfiguration der Audio- und Video-Einstellungen sowie anderer Hardware-Optionen. Die Audio-Ausgabe erfolgt standardmäßig über das HDMI-Kabel. Alternativ können Sie das Audio-Signal auch an den Kopfhöreranschluss des Raspberry Pi leiten. Eine Lautstärkeregelung ist nicht vorgesehen. Sie müssen die gewünschte Lautstärke bei Ihrem Fernseher bzw. Monitor einstellen.

Im Dialogblatt VIDEO-HARDWARE können Sie die Auflösung des Grafiksystems verändern. Diese entspricht standardmäßig der Auflösung des Monitors bzw. Fernsehers. Eine Reduktion der Auflösung, z. B. auf 1280*720 Pixel, erhöht die Geschwindigkeit von XBMC.

GUI-Auflösung versus Video-Auflösung

Standardmäßig werden Videos in Full-HD-Auflösung wiedergegeben (1080p); die Benutzeroberfläche von Raspbmc verwendet hingegen aus Performance-Gründen nur die HD-Auflösung 720p und wird vom Grafikprozessor auf 1080p hochskaliert.

Wenn auch die Benutzeroberfläche die volle HD-Auflösung nutzen soll, aktivieren Sie die Option REMOVE UI RES LIMIT im Dialogblatt SYSTEM CONFIGURATION des Programms RASPBMC SETTINGS. Nach einem Neustart von XBMC sieht die Benutzeroberfläche nun spürbar schärfer aus, zumindest wenn Sie direkt vor Ihrem TV-Gerät sitzen. Angesichts der ohnedies knappen Rechenleistung ist diese Einstellung aber nicht empfehlenswert.

Im Dialogblatt AUDIO-AUSGABE geben Sie an, über welchen Ausgang die Audiosignale übertragen werden sollen. Zur Wahl stehen HDMI und ANALOG, also der Kopfhörer-Ausgang des Raspberry Pi. Leider ist es unmöglich, *beide* Ausgänge gleichzeitig zu nutzen. Die Audio-Ausgabe über USB wird nicht unterstützt.

XBMC-Grundfunktionen

Nachdem ich nun seitenlang alle möglichen Konfigurationsdetails beschrieben habe, wird es Zeit für die eigentliche Anwendung von XBMC – also für das Anhören von Musik und das Abspielen von Video-Dateien. Anfänglich führen die Menüs VIDEOS, MUSIK und BILDER ins Leere. Das liegt daran, dass es im lokalen Dateisystem von XBMC noch keine Multimedia-Dateien gibt und XBMC auch keine Netzwerkquellen für derartige Dateien kennt.

Lokale Videos abspielen

Für erste Experimente ist es am einfachsten, im Verzeichnis `/home/pi` ein Unterverzeichnis einzurichten und dorthin – z. B. via SSH – einige Video-Dateien zu kopieren.

Damit XBMC diese Dateien abspielen kann, führen Sie im Hauptmenü VIDEO • DATEIEN aus und wählen den Eintrag VIDEOS HINZUFÜGEN. Der nächste Dialog, QUELLE FÜR VIDEO HINZUFÜGEN, ist recht unübersichtlich; zudem ist in der deutschen Übersetzung von einem DIASHOW-ORDNER die Rede, obwohl ein simples Verzeichnis mit Mediendateien gemeint ist. Mit SUCHEN wechseln Sie in einen Dateiauswahldialog. Dort wählen Sie zuerst den HOME-ORDNER und dann das dort befindliche Unterverzeichnis mit Ihren Video-Dateien aus.

Nach der Verzeichnisauswahl erscheint ein weiterer Dialog: INHALT FESTLEGEN. Dort geben Sie an, welche Art von Dateien das Verzeichnis enthält – Filme, TV-Serien oder Musik-Videos. XBMC versucht nun, die Video-Dateien mit frei zugänglichen Datenbanken abzugleichen, damit es ein Titelbild sowie diverse Metadaten anzeigen kann (Schauspieler etc.) Dieser Datenabgleich kann einige Zeit beanspruchen.

Sind diese Vorbereitungsarbeiten erst einmal abgeschlossen, können Sie in den gerade eingerichteten Ordner wechseln. XBMC zeigt eine Liste der dort enthaltenen Video-Dateien an (siehe Abbildung 12.10). Über ein Menü am linken Bildschirmrand können Sie zwischen verschiedenen Darstellungsformen wechseln, z. B. LISTE, THUMBNAIL oder POSTER. Mit der Maus oder einer Fernbedienung wählen Sie den gewünschten Film aus und starten ihn. Sollte die Wiedergabe nicht funktionieren, vergewissern Sie sich, dass Sie die Lizenzschlüssel zur Hardware-Decodierung der Formate MPEG-2 und VC-1 korrekt eingerichtet haben. Grundsätzlich kann XBMC keine DRM-geschützten Video-Dateien abspielen.

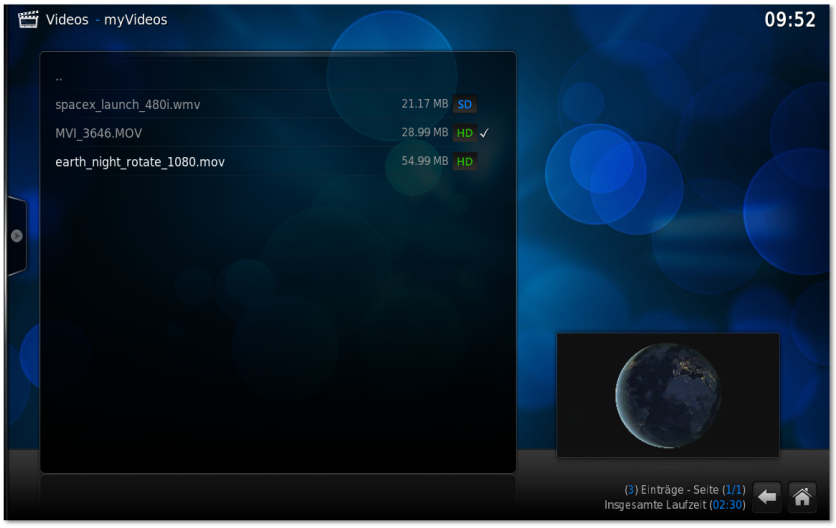


Abbildung 12.10 Auswahl von Video-Dateien im Listenmodus

Video-Dateien im lokalen Netzwerk

Die SD-Speicherkarte in Ihrem Raspberry Pi ist ein guter Ort für erste Experimente, aber zur Speicherung der lokalen Mediathek ist sie zu klein und zu langsam. Eine mögliche Alternative ist eine externe Festplatte, die Sie über ein USB-Kabel mit dem Raspberry Pi verbinden. Deutlich eleganter ist es, über das lokale Netzwerk oder WLAN auf Audio- und Video-Dateien zuzugreifen, die ein Linux-Server oder NAS-Gerät bereithält.

XBMC unterstützt die meisten gängigen Protokolle für Netzwerkverzeichnisse, also SMB (Windows/Samba), NFS, AFP (Apple), DLNA etc. Um Video-Dateien aus

einem SMB-Verzeichnis zu lesen, führen Sie VIDEOS • DATEIEN • VIDEOS HINZUFÜGEN • SUCHEN aus. Im Dialog NACH EINER NEUEN QUELLE SUCHEN finden Sie in der Liste der vordefinierten Medienquellen den Eintrag WINDOWS-NETZWERK. Damit können Sie Windows-Server in der Arbeitsgruppe WORKSTATION auswählen.

Sollte Ihr NAS-Gerät oder LAN-Server dort nicht erscheinen, verwenden Sie stattdessen den Eintrag NETZWERKFREIGABE HINZUFÜGEN. Der Dialog NETZWERKFREIGABE erlaubt den Zugriff auf alle erdenklichen Arten von Netzwerkdiensten (siehe Abbildung 12.11). Nach Abschluss der Konfiguration erscheint ein neuer `smb://xxx`-Eintrag in der Liste der Medienquellen und kann dort ausgewählt werden.

Abbildung 12.11 Zugriff auf ein SMB-Verzeichnis einrichten

Sofern XBMC neu hinzukommende Video-Dateien identifizieren kann (also Titel, Genre, Erscheinungsjahr etc.), zeigt es diese Filme im Hauptmenü in der neuen Rubrik FILME an. Das ermöglicht eine besonders komfortable Auswahl, funktioniert aber naturgemäß nicht für selbst produzierte Familien-Videos.

Videos aus dem Internet

VIDEOS • ADD-ONS • MEHR ... führt in eine Liste von Add-ons, mit denen Sie Filme aus diversen Internet-Angeboten auf Ihrem Media-Center ansehen können. Unter anderem gibt es Add-ons für Apple iTunes-Podcasts, die ARD Mediathek, Arte.TV, Netzkino.de, die ORF TVthek, Spiegel Online, YouTube sowie für die ZDF Mediathek. Die Installation eines Add-ons dauert typischerweise weniger als eine Minute. Alle installierten Add-ons werden je nach Einstellung als Liste oder in Bildform angezeigt (siehe Abbildung 12.12) und können nun bequem gestartet werden.

Audio

Das Abspielen von Musik folgt demselben Muster wie die Wiedergabe von Videos: Sie müssen zuerst eine Musikquelle definieren (ein lokales Verzeichnis, ein Netzwerkverzeichnis, einen DLNA-Server etc.) und können dann einen Titel zur Wiedergabe auswählen.

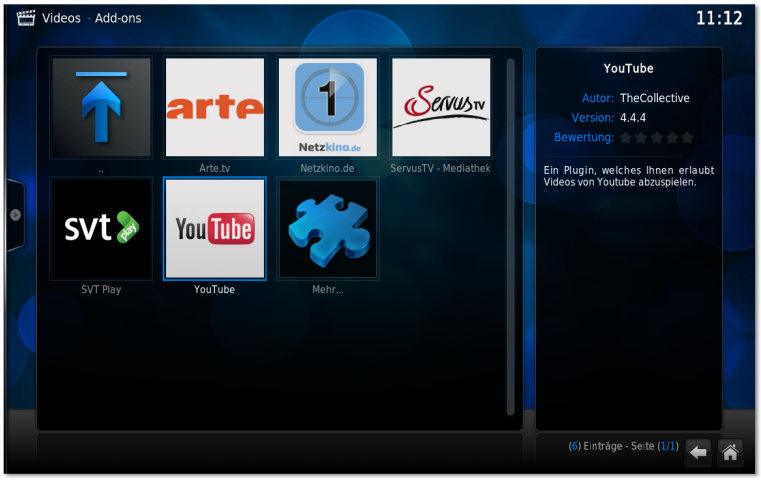


Abbildung 12.12 Installierte Video-Add-ons

Standardmäßig wird die Musik von einer 3D-Spektrumsanalyse begleitet. Um diesen Unfug abzustellen, aktivieren Sie die Vollbildansicht und klicken dann auf den zweiten Button der rechten Button-Gruppe. Das Button-Icon hat die Form eines Bergs mit Wolke und führt in den Dialog VISUALISIERUNG. Dort wählen Sie den Eintrag KEINE.

Sofern die Audio-Dateien mit MP3-Tags ausgestattet sind, kann XBMC alle Titel in einer Datenbank erfassen. Das ermöglicht eine Suche nach Genres, Künstler etc. Außerdem werden neue Alben nun als Icons im Hauptmenü angezeigt (siehe Abbildung 12.13). Den Datenbank-Scan starten Sie, indem Sie im Kontextmenü einer Musikquelle den Eintrag IN DATENBANK AUFNEHMEN wählen. In das Kontextmenü gelangen Sie mit der Taste C, mit der rechten Maustaste oder mit der TITLE-Taste der Fernbedienung.

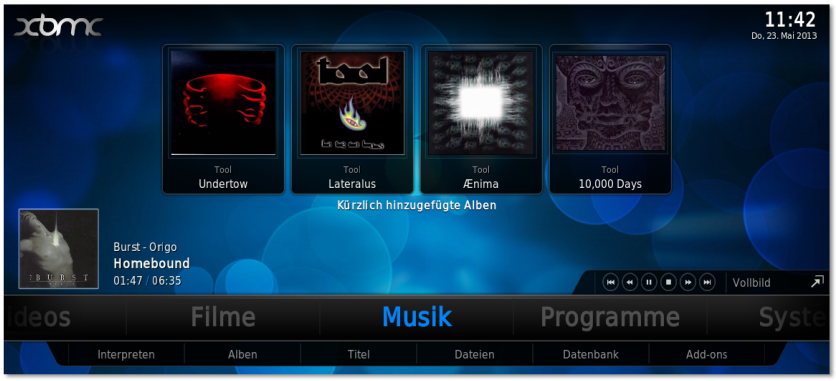


Abbildung 12.13 XBMC als Audio-Player

Spotify

Diverse Audio-Add-ons ermöglichen es, unzählige Internet-Radio-Stationen anzuhören und Dienste wie Last.fm zu nutzen. Das Spotify-Add-on `spotimc` lag Mitte 2013 nur in einer Beta-Version vor. Zum Download des Add-ons loggen Sie sich mit SSH in Ihren Raspberry Pi ein:

```
pi$ wget http://azkotoki.org/download-file/28/script-audio-spotimc-1-0-beta4.zip
```

Anschließend führen Sie in XBMC System • Einstellungen • Add-ons • Aus ZIP-Datei installieren aus und wählen die ZIP-Datei aus. Nach der Installation finden Sie das neue Add-on unter Musik • Add-ons. Bei der ersten Verwendung müssen Sie sich anmelden. Beachten Sie, dass das Add-on einen Spotify-Premium-Account voraussetzt.

AirPlay

XMBC kann auch Audio- und Video-Streams abspielen, deren Adresse über ein iPhone oder ein iPad zur Verfügung gestellt wird. Apple nennt diese Funktion »AirPlay«. Auch Bilder können so vom iOS-Gerät auf den Fernseher »gebeamt« werden.

XBMC-seitig ist die Konfiguration von AirPlay erfreulich einfach: In den Systemeinstellungen öffnen Sie den Dialog Dienste • AirPlay und aktivieren die Option AirPlay-Inhalte empfangen. Fertig! Wenn Sie nun auf Ihrem iPhone oder iPad das AirPlay-Menü öffnen, wird XBMC als möglicher AirPlay-Empfänger aufgelistet. Voraussetzung ist natürlich, dass beide Geräte WLAN-Zugang haben, also sowohl der Raspberry Pi mit XBMC als auch Ihr Smartphone bzw. Tablet.

Bei meinen Tests hat AirPlay zumeist problemlos funktioniert. Probleme gibt es nur, wenn Video-Streams in einem Format vorliegen, das XBMC nicht decodieren kann – dann versagt die Funktion, und das leider ohne irgendwelche Hinweise auf die Fehlerursache. Miracast, das Android-Gegenstück zu AirPlay, wird von XBMC leider noch nicht unterstützt.

12.4 Hardware-Basteleien

Die eigentliche Besonderheit des Raspberry Pi ist weder seine winzige Größe noch sein Preis – die riesige Faszination für den Raspberry Pi geht vielmehr von 26 Pins (elektrischen Kontakten) aus, die zur Messung und Steuerung elektronischer Geräte verwendet werden können. Sowohl Elektronik-Bastler als auch Embedded-Linux-Profis bekommen mit dem Raspberry Pi ein Spielzeug bzw. Werkzeug in die Hand, das die Entwicklung computergesteuerter Geräte so einfach wie selten zuvor macht.

Dieser Abschnitt gibt hierzu eine Einführung und präsentiert einige Beispiele. Im Internet sowie in Raspberry-Pi-Büchern und -Zeitschriften finden Sie unzählige weitere Anleitungen für anspruchsvollere Projekte.

Zerstören Sie Ihren Raspberry Pi nicht durch Unachtsamkeit!

Auch wenn ich mich in diesem Abschnitt an Elektronikeinsteiger und nicht an Embedded-Linux-Profis wende, gehe ich im Weiteren davon aus, dass Sie elementare Grundregeln im Umgang mit elektronischen Komponenten kennen:

- Durch elektrostatische Ladungen können Sie Ihren Raspberry Pi durch bloßes Berühren eines elektrischen Kontakts zerstören! Verwenden Sie ein Antistatikband (ESD-Armband).
- Auch versehentliche Kurzschlüsse, die falsche Beschaltung von Pins und dergleichen können Ihrem Minicomputer den Garaus machen.
- Schalten Sie Ihren Raspberry Pi immer aus, wenn Sie Veränderungen an der Schaltung durchführen.
- Beachten Sie schließlich, dass die meisten GPIO-Pins eine maximale Spannung von 3,3 Volt erwarten. Die für viele andere elektronische Bauteile üblichen 5 Volt sind zu hoch und können den Raspberry Pi ebenfalls kaputt machen.

Das Layout der 26-Pin-Steckerleiste

Die Platine des Raspberry Pi enthält in einer Ecke eine Steckerleiste mit 2*13 Kontakten in einem Rasterabstand von 2,54 mm. Diese Steckerleiste stellt neben einigen allgemein verwendbaren Kontakten (General Purpose Input/Output = GPIO) auch zwei Versorgungsspannungen (3,3 V bzw. 5 V) sowie die Masse (also 0 V) zur Verfügung. Die Nummerierung der 26 Pins geht aus Abbildung 12.14 hervor.

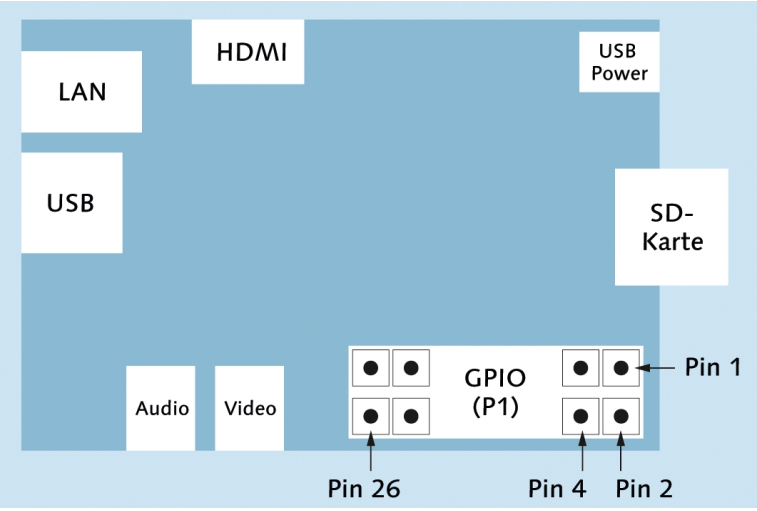


Abbildung 12.14 Schematischer Plan des Raspberry Pi mit Pin-Nummerierung

Häufig werden alle 26 Pins als GPIO-Pins bezeichnet. Genau genommen ist das aber falsch: Vielmehr bilden die 26 Pins den sogenannten P1-Header; nur ein Teil der P1-Kontakte sind tatsächlich GPIO-Pins. Dafür gibt es an anderen Stellen der Platine weitere GPIO-Kontaktpunkte (insbesondere im P5-Header, siehe unten).

Revision 1 versus Revision 2

Es gibt zwei Varianten der Raspberry-Pi-Platine: Revision 1 sowie Revision 2, die seit September 2012 ausgeliefert wird. Mit Revision 2 hat sich die Funktion der Pins 3, 5 und 13 verändert. In diesem Kapitel beziehe ich mich auf Revision 2!

Um festzustellen, welche Revision Sie besitzen, werfen Sie einen Blick in die Datei `/proc/cpuinfo`. Die Zeile `Revision` liefert einen hexadezimalen Code. Relevant ist dabei nur die letzte Ziffer, also gewissermaßen die Einerstelle, im folgenden Beispiel `d`. Ist diese Ziffer größer als 3, dann haben Sie eine Revision-2-Platine.

```
pi$  cat /proc/cpuinfo
...
Hardware        : BCM2708
Revision        : 000d
Serial          : 00000000d0c24d4b
```

Die Unterschiede zwischen Revision 1 und Revision 2 sowie die Funktionsabweichungen der Pins sind ausführlich auf den beiden folgenden Seiten dokumentiert:

http://elinux.org/RPi_Low-level_peripherals
http://www.raspberrypi.org/archives/1929

Pin-Belegung

Tabelle 12.1 fasst die Belegung der 26 Pins des P1-Headers zusammen (Quelle: *http://elinux.org/RPi_Low-level_peripherals*, ohne Gewähr!). Die Namen der Pins, deren Funktion sich mit Revision 2 geändert hat, sind fett hervorgehoben.

Viele Pins erfüllen je nach Programmierung alternative Funktionen. Beispielsweise können die Pins 3 und 5 nicht nur als GPIO-Kontakte verwendet werden, sondern auch zum Anschluss einer elektronischen Komponente mit I^2C-Bus.

Tabelle 12.2 erklärt die wichtigsten Abkürzungen, die in Tabelle 12.1 verwendet wurden. Eine detaillierte Beschreibung jedes einzelnen GPIO-Kontakts inklusive aller alternativen Belegungen finden Sie unter:

http://elinux.org/RPi_BCM2835_GPIOs

Diese Seite enthält vielmehr eine umfassende Beschreibung aller GPIO-Pins des Broadcom BCM2835 System-on-a-Chip. Dieser Bauteil, der auch die CPU und die GPU enthält, ist das Kernstück der Raspberry Pi-Platine.

Pin	Name	alternative Funktion	Pin	Name	alternative Funktion
1	3.3V		2	5V0	
3	**GPIO 2**	**I²C1_SDA**	4	5V0	
5	**GPIO 3**	**I²C1_SCL**	6	GND	
7	GPIO 4	GPCLK0, ARM_TDI	8	GPIO 14	UART_TXD
9	GND		10	GPIO 14	UART_RXD
11	GPIO 17	UART_RTS, SPI1_CE1_N	12	GPIO 18	PCM_CLK, SPI1_CE0_N, PWM
13	**GPIO 27**	**SD1_DAT3, ARM_TMS**	14	GND	
15	GPIO 22	SD1_CLK, ARM_TRST	16	GPIO 23	SD1_CMD, ARM_RTCK
17	3.3V		18	GPIO 24	SD1_DAT0, ARM_TDO
19	GPIO 10	SPI0_MOSI	20	GND	
21	GPIO 9	SPI0_MISO	22	GPIO 25	SD1_DAT1, ARM_TCK
23	GPIO 11	SPI0_SCLK	24	GPIO 8	SPI0_CE0_N
25	GND		26	GPIO 7	SPI0_CE1_N

Tabelle 12.1 Belegung der 26 Pins des P1-Headers

Abkürzung	Bedeutung
GND	Ground (Masse, also 0 V)
GPIO	General Purpose Input Output
GPCLK	General Purpose Clock (einstellbarer Taktgeber)
I²S	Inter-IC Sound Interface (Übertragung von Audio-Daten)
I²C	Inter-Integrated Circuit (serieller Datenbus)
PWM	Pulse Width Modulation (für SPI)
SD1	Secondary memory Data bus
SPI	Serial Peripheral Interface (serieller Datenbus)
SPI-MOSI	Master out, Slave in (für SPI)
SPI-MISO	Master in, Slave out (für SPI)
SPI-SCLK	Serial Clock (für SPI)
UART	Universal Asynchronous Receiver Transmitter (serielle Schnittstelle)

Tabelle 12.2 Abkürzungen

Maximaler Ausgangsstrom

Pin 1 und 17 dürfen *zusammen* maximal mit 50 mA belastet werden. Pin 2 und 4 werden über eine selbstrückstellende Sicherung (poly fuse) geleitet. Fließt hier zu viel Strom, schaltet sich der Raspberry Pi für eine Weile ab. Mit etwas Glück kommt es zu keinen bleibenden Schäden.

Wenn Sie GPIO-Kontakte zur Steuerung verwenden (Konfiguration als Output) und auf `HIGH` stellen, beträgt die Spannung am betreffenden GPIO-Pin 3,3 V. Der Steuerungsstrom pro Pin sollte 8 mA nicht überschreiten (bzw. 50 mA für *alle* GPIOs sowie Pin 1 und 17). Verwenden Sie also geeignete Vorwiderstände! Wirklich klare Angaben zum maximal erlaubten GPIO-Strom habe ich nicht gefunden. Aus Experimenten von Raspberry-Pi-Anwendern geht hervor, dass das Gerät auch bei einem etwas höheren Strom nicht gleich beschädigt wird bzw. dass die Ausgangsspannung dann entsprechend absinkt, um die Leistung zu begrenzen. Noch mehr Details können Sie der folgende Diskussion entnehmen:

http://www.raspberrypi.org/phpBB3/viewtopic.php?f=44&t=12248

Welcher GPIO für welchen Zweck?

Vor jedem Projekt müssen Sie sich die Frage stellen: Welche der vielen GPIO-Pins setzen Sie ein? Solange es nur darum geht, erste Experimente durchzuführen und ein paar Leuchtdioden ein- und auszuschalten, können Sie dazu jeden der 17 GPIO-*n*-Pins verwenden. Diverse Spezialfunktionen stehen allerdings auf ausgewählten Pins zur Verfügung. Ein kurzer Überblick, wobei sich die Pin-Nummern auf den P1-Header des Raspberry Pi beziehen (Revision 2):

- **Pin 3 und 5** sind erforderlich für I^2C-Komponenten. Die beiden Pins sind mit einem 1,8 kΩ-Pull-up-Widerstand verbunden und eignen sich auch gut als Signaleingänge (z. B. für Schalter/Taster). Vorsicht: unterschiedliche Funktion je nach Revision 1 oder 2!
- **Pin 7** wird vom 1-Wire-Kerneltreiber verwendet oder kann als Taktgeber eingesetzt werden.
- **Pin 8 und 10** Pins werden beim Booten des Raspberry Pi standardmäßig als serielle Schnittstelle konfiguriert. Dort werden normalerweise die Kernelmeldungen ausgegeben. Wenn Sie die Pins für allgemeine I/O-Aufgaben nutzen möchten, müssen Sie diese umprogrammieren, z. B. mit dem Kommando `gpio` aus der WiringPi-Bibliothek.
- **Pin 11, 12 und 13** können zum Anschluss von SPI-Komponenten verwendet werden (SPI-Kanal 1). Vorsicht: Pin 13 hat eine unterschiedliche Funktion je nach Revision 1 oder 2.
- **Pin 12** wird standardmäßig vom LIRC-Kerneltreiber verwendet und eignet sich daher gut als Signaleingang für einen IR-Empfänger. Dieser Pin kann auch als PWM-Ausgang verwendet werden. Vorsicht: Wenn Sie Audiosignale über den

Kopfhörerausgang ausgeben, wird automatisch ein Audio-Kanal als PWM-Signal über Pin 12 geleitet.

- **Pin 19, 21, 23, 24 und 26** können zum Anschluss von SPI-Komponenten verwendet werden (SPI-Kanal 0).

Noch mehr Informationen finden Sie auf den beiden folgenden Seiten, die sich allerdings *nicht* auf die Pin-Nummern des P1-Headers beziehen, sondern die Pin-Nummerierung der BCM2835-Chips verwenden:

http://wiringpi.com/pins/special-pin-functions
http://elinux.org/RPi_BCM2835_GPIOs

Kontakt zu GPIO-Pins herstellen

Bevor Sie Ihr erstes Bastelprojekt beginnen, müssen Sie sich überlegen, wie Sie den elektronischen Kontakt zu einem der 26 Pins herstellen. Für kleine Versuchsaufbauten auf einem Steckboard sind kurze Kabel mit Stecker und Buchse ideal (siehe Abbildung 12.15). Fertige Kabel sind in Deutschland schwer zu bekommen (suchen Sie z. B. in eBay nach *breadboard jumper wire male female*), werden aber in diversen Raspberry-Pi-Shops angeboten, oft auch zusammen mit einem Steckboard als Starter-Kit.

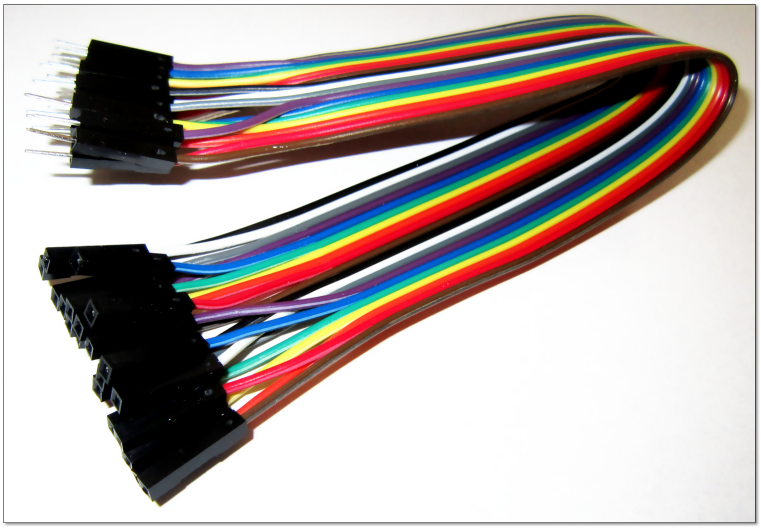


Abbildung 12.15 Steckboard-Kabel

Mit ein wenig Erfahrung im Löten und einer Buchsenleiste im 2,54-mm-Raster (erhältlich in jedem Elektronikmarkt) können Sie sich selbst passende Stecker machen. Eine andere Alternative ist ein 26-Pin-Stecker mit einem Flachbandkabel, deren Drähte Sie dann trennen. Manche Raspberry-Pi-Händler bieten auch spezielle *Cobbler* an, um alle 26 Pins des P1-Headers über ein Flachbandkabel mit den Kontaktreihen eines Steckboards zu verbinden.

Löten Sie auf keinen Fall die Kabel direkt an die Steckerpins. Die unvermeidlichen Lötreste machen es nahezu unmöglich, später einen Flachbandstecker zu verwenden.

Noch mehr Kontakte/GPIOs (P2, P3, P5, P6)

In Ergänzung zu den 26 Pins des P1-Headers enthält die Platine des Raspberry Pi einige weitere Kontaktstellen – die P2-, P3-, P5- und P6-Header. Diese Kontaktstellen sind nicht mit Steckern verbunden. Wenn Sie diese Kontakte nutzen möchten, müssen Sie Ihre elektronischen Bauteile, Kabel oder Stecker dort anlöten.

P5 und P6 stehen erst ab Revision 2 zur Verfügung. Die acht Kontakte des P5-Headers auf der Rückseite (!) der Platine stellen unter anderem die Kontakte GPIO28 bis -31 zur Verfügung. Diese können als zweite I2C- oder als I2S-Schnittstelle verwendet werden. Die beiden Kontakte des P6-Headers bieten die Möglichkeit eines Hardware-Resets. Eine Verbindung der beiden Kontakte startet die CPU des Raspberry Pi neu.

Vielleicht vermissen Sie den P4-Header: Dessen Kontakte sind beim Modell B mit der Ethernet-Buchse verbunden und stehen daher nicht mehr für andere Aufgaben zur Verfügung.

Im weiteren Verlauf dieses Kapitels beziehe ich mich ausschließlich auf die 26 Pins des P1-Headers! Eine vollständige Hardware-Beschreibung des Raspberry Pi finden Sie hier:

http://elinux.org/RPi_Hardware

LEDs ein- und ausschalten

LED im Dauerbetrieb

Sozusagen als *Hello World!*-Projekt zeige ich Ihnen, wie Sie mit Ihrem Raspberry Pi eine Leuchtdiode (LED) ein- und ausschalten. Die erste Variante besteht darin, die LED direkt an die 3,3-V-Spannungsversorgung anzuschließen. Sie leuchtet dann immer.

Im Datenblatt Ihrer LED lesen Sie nach, wie groß der Spannungsabfall an der Diode ist und welchen Strom die Diode erwartet – z. B. 2 V und 10 mA. Die Größe des erforderlichen Vorwiderstands ergibt sich aus der Restspannung 3,3 V - 2 V = 1,3 V und der Formel R = U / I = 1,3 V / 10 mA mit 130 Ω. Wenn Sie den nächstgrößeren Widerstand verwenden, den Sie finden, kann nichts passieren. Die LED leuchtet dann entsprechend weniger hell.

Da derselbe Schaltungsaufbau später über einen GPIO-Pin mit einem maximalen Ausgangsstrom von 8 mA gesteuert werden soll, ist es besser, den Widerstand gleich entsprechend größer zu dimensionieren (1,3 V / 8mA = 163 Ω). Ich habe für meine Experimente mit 330-Ω-Widerständen gearbeitet, womit sich ein Strom von 4 mA ergibt.

Auf einem Steckboard bauen Sie nun die Schaltung gemäß Abbildung 12.16 auf und verbinden die Schaltung mit den Pins 1 (3,3V) und 25 (GND) des Raspberry Pi. Achten Sie auf die richtige Polung der LED. Der längere Draht der LED verbindet die Anode (Plus), der kürzere die Kathode (Minus).

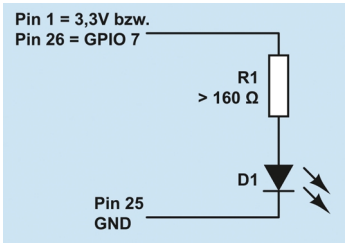


Abbildung 12.16 Simple LED-Schaltung

LED manuell ein- und ausschalten

Nachdem Sie sich überzeugt haben, dass die obige Schaltung prinzipiell funktioniert, verwenden Sie nun anstelle von Pin 1 (3,3V) einen GPIO-Kontakt, z. B. Pin 26 für GPIO 7.

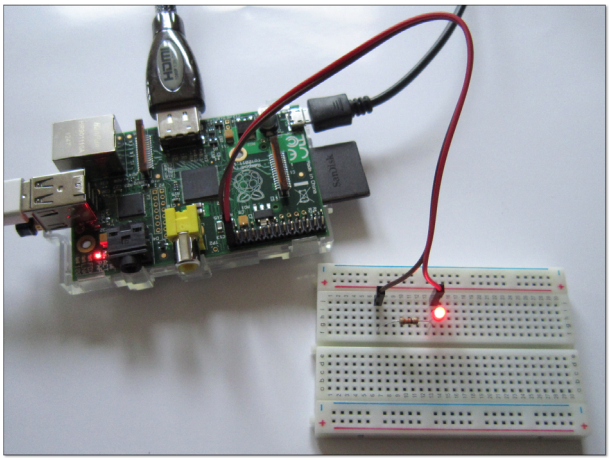


Abbildung 12.17 Versuchsaufbau zur LED-Steuerung

Tipp

GPIO-Pins sind zur Steuerung, nicht zur Stromversorgung gedacht. Wenn Sie ein elektronisches Bauteil mit mehr als 8 mA bei 3,3 V versorgen möchten, verwenden Sie zur Stromversorgung Pin 2 oder 4 (5 V) und steuern den Stromfluss durch einen GPIO-Ausgang über einen Transistor. Einen entspechenden Schaltungsaufbau finden Sie hier:

http://www.raspberrypi-spy.co.uk/2012/06/control-led-using-gpio-output-pin

Beim Einschalten des Raspberry Pi wird die LED nun nicht mehr leuchten. Vielmehr können Sie die LED jetzt durch ein Python-Programm steuern. Den erforderlichen Quellcode geben Sie mit einem Editor ein:

```
#!/usr/bin/python
# coding=utf-8
import RPi.GPIO as GPIO
import time

# Pin-Nummern verwenden (nicht GPIO-Nummern!)
GPIO.setmode(GPIO.BOARD)

# Pin 26 (= GPIO 7) zur Datenausgabe verwenden
GPIO.setup(26, GPIO.OUT)

# Pin 26 einschalten
GPIO.output(26, GPIO.HIGH)

# Pin 26 nach fünf Sekunden wieder ausschalten
time.sleep(5)
GPIO.output(26, GPIO.LOW)

# alle vom Script benutzten GPIOs/Pins wieder freigeben
GPIO.cleanup()
```

Der Programmcode sollte auch ohne Python-Erfahrung auf Anhieb verständlich sein. `chmod` macht die Script-Datei ausführbar. Nur `root` darf GPIO-Funktionen steuern, daher muss das Script mit `sudo` ausgeführt werden.

```
pi$  chmod a+x led1.py
pi$  sudo ./led1.py
```

Natürlich ist Python nicht die einzige Programmiersprache, die Sie zur GPIO-Steuerung einsetzen können. Python ist aber das populärste Werkzeug für diesen Zweck und steht bei den meisten Raspberry-Pi-Distributionen inklusive der GPIO-Bibliothek standardmäßig zur Verfügung. Eine kurze Einführung in die GPIO-Bibliothek für Python sowie einen Überblick, wie Sie GPIO-Pins mit anderen Programmiersprachen steuern, finden Sie hier:

http://code.google.com/p/raspberry-gpio-python/wiki/BasicUsage
http://elinux.org/RPi_Low-level_peripherals#GPIO_Code_examples

GPIO-Steuerung im Terminal (WiringPi)

Nicht immer ist es praktisch, für jede Veränderung eines GPIO-Pins gleich ein Python-Script zu verfassen. Das Projekt WiringPi stellt das Kommando `gpio` zur Verfügung, mit dem Sie einzelne GPIO-Pins direkt im Terminal manipulieren können. Die Installation von WiringPi aus einem Git-Repository ist in wenigen Minuten erledigt:

```
pi$  sudo apt-get install git-core
pi$  git clone git://git.drogon.net/wiringPi
pi$  cd wiringPi
pi$  ./build
```

Mit dem Kommando `gpio` können Sie nun ebenfalls die LED ein- und ausschalten. Das Kommando erfordert keine `root`-Rechte. Die Option `-1` (eins, nicht L) bewirkt dabei, das `gpio` physische Pin-Nummern des P1-Headern als Parameter erwartet.

```
pi$  gpio -1 mode 26 out
pi$  gpio -1 write 26 1     (LED ein)
pi$  gpio -1 write 26 0     (LED aus)
```

`gpio readall` verrät den aktuellen Status aller GPIO-Pins. Dabei gibt die erste Spalte die WiringPi-Nummer der Pins an, die zweite Spalte die am Raspberry Pi üblichen GPIO-Nummern und die dritte Spalte die Pin-Nummer des P1-Headers. Beachten Sie, dass Spalte 4 die Nomenklatur der Broadcom-CPU BCM2835 verwendet. Tabelle 12.1 verwendet hingegen die üblichen Raspberry-Pi-Bezeichnungen mit einem anderen Nummerierungsschema!

```
pi$  gpio readall
+----------+-Rev2-+------+--------+------+-------+
| wiringPi | GPIO | Phys | Name   | Mode | Value |
+----------+------+------+--------+------+-------+
|      0   |  17  |  11  | GPIO 0 | IN   | Low   |
|      1   |  18  |  12  | GPIO 1 | IN   | Low   |
|      2   |  27  |  13  | GPIO 2 | IN   | Low   |
|      3   |  22  |  15  | GPIO 3 | IN   | Low   |
|      4   |  23  |  16  | GPIO 4 | IN   | Low   |
|      5   |  24  |  18  | GPIO 5 | IN   | Low   |
|      6   |  25  |  22  | GPIO 6 | IN   | Low   |
|      7   |   4  |   7  | GPIO 7 | IN   | Low   |
|      8   |   2  |   3  | SDA    | IN   | High  |
|      9   |   3  |   5  | SCL    | IN   | High  |
|     10   |   8  |  24  | CE0    | IN   | Low   |
|     11   |   7  |  26  | CE1    | OUT  | Low   |
|     12   |  10  |  19  | MOSI   | IN   | Low   |
|     13   |   9  |  21  | MISO   | IN   | Low   |
|    ...   |      |      |        |      |       |
+----------+------+------+--------+------+-------+
```

LED-Überwachung der CPU-Temperatur

Um das Beispiel ein wenig interessanter zu machen, zeigt Abbildung 12.18 eine Schaltung mit nunmehr drei Dioden (grün, gelb und rot), die durch die GPIOs 7, 8 und 25 gesteuert werden (Pin 26, 24 und 22). Das Ziel besteht darin, die LEDs in Abhängigkeit von der CPU-Temperatur ein- und auszuschalten: Die grüne LED soll leuchten, wenn die CPU-Temperatur zwischen 30 und 45 Grad beträgt, die gelbe LED bei Temperaturen zwischen 45 und 60 Grad und die rote LED bei Temperaturen darüber.

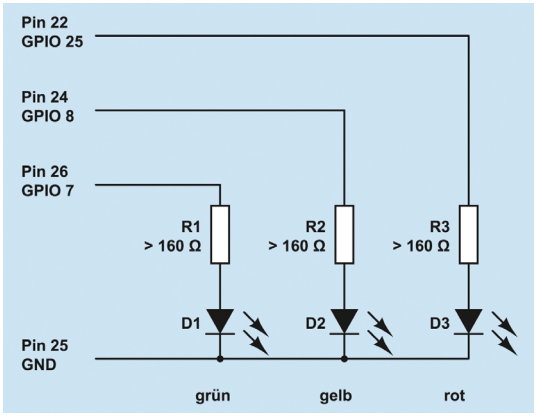


Abbildung 12.18 LED-Anzeige der CPU-Temperatur

Nachdem Sie die Schaltung aufgebaut haben, testen Sie, ob alle drei LEDs funktionieren:

```
pi$  sudo -s
pi$  gpio -1 mode 26 out
pi$  gpio -1 write 26 1     (grüne LED ein)
pi$  gpio -1 write 26 0     (grüne LED aus)
pi$  gpio -1 mode 24 out
pi$  gpio -1 write 24 1     (gelbe LED ein)
pi$  gpio -1 write 24 0     (gelbe LED aus)
pi$  gpio -1 mode 22 out
pi$  gpio -1 write 22 1     (rote LED ein)
pi$  gpio -1 write 22 0     (rote LED aus)
```

Ein Shell-Script zum Ein- und Ausschalten der drei LEDs in Abhängigkeit von der CPU-Temperatur ist rasch geschrieben. Wenn Ihnen Python lieber ist, können Sie den Code natürlich ebenso gut damit formulieren.

```
#!/bin/bash
# Datei /home/pi/cpu-led
greenpin=26
yellowpin=24
redpin=22
gpio -1 mode $greenpin  out
gpio -1 mode $yellowpin out
gpio -1 mode $redpin    out

# CPU-Temperatur
temp=$(cat /sys/class/thermal/thermal_zone0/temp)
echo $temp
```

```
# grüne LED ansteuern
if [[ "$temp" -ge 30000 &&  "$temp" -le 45000 ]]; then
  gpio -1 write $greenpin 1
else
  gpio -1 write $greenpin 0
fi

# gelbe LED ansteuern
if [[ "$temp" -ge 45000 &&  "$temp" -le 60000 ]]; then
  gpio -1 write $yellowpin 1
else
  gpio -1 write $yellowpin 0
fi

# rote LED ansteuern
if [[ "$temp" -ge 60000 ]]; then
  gpio -1 write $redpin 1
else
  gpio -1 write $redpin 0
fi
```

Diese Datei muss ausführbar sein!

```
root#  chmod a+x /home/pi/cpu-led
```

Jetzt geht es nur noch darum, dieses Script einmal pro Minute aufzurufen. Dazu legen Sie im Verzeichnis `/etc/cron.d` die folgende Datei an (siehe auch Abschnitt 16.6):

```
# Datei /etc/cron.d/cpu-temp
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
*/1 * * * *  root  /home/pi/cpu-led
```

Von nun an werden die drei LEDs minütlich je nach CPU-Temperatur ein- und ausgeschaltet. Vergessen Sie nicht, `/etc/cron.d/cpu-led` zu löschen, wenn Sie die Pins 22, 24 und 26 später für eine andere Schaltung verwenden möchten!

Eine LED mit einem Taster ein- und ausschalten

Die einfachste Form, an den Raspberry Pi *Eingaben* weiterzuleiten, ist ein simpler Taster, der den Stromkreis schließt, solange er gedrückt ist. Während umgangssprachlich oft alles, worauf man drücken kann, ein »Schalter« ist, unterscheidet die Elektrotechnik zwischen Schaltern, die den Zustand beibehalten (wie ein Lichtschalter) und Tastern, die zurückspringen, wenn man sie loslässt (wie bei Ihrer Tastatur). Für dieses Beispiel benötigen Sie also einen Taster. Wenn Sie zum Testaufbau ein Steckboard verwenden, fragen Sie in Ihrem Elektronikgeschäft nach einem *print-taster*.

Das Ziel dieses Abschnitts ist eine Schaltung, bei der Sie durch einen kurzen Druck auf eine Taste eine LED einschalten. Drücken Sie nochmals, soll die LED wieder ausgehen. Die Aufgabenstellung klingt erdenklich trivial, aber Sie werden sehen, dass dieser Eindruck täuscht.

GPIO-Input

Bevor Sie den Taster aber mit einem GPIO-Pin verbinden, müssen Sie sich Gedanken darüber machen, wie der Raspberry Pi Eingaben verarbeitet. Es ist möglich, einen GPIO-Pin als *Input* zu konfigurieren. Die Ausgangsspannung dieses Pins ist damit undefiniert. Wenn von außen eine Spannung nahe 0 V angelegt wird, wird das als *low* = 0 interpretiert. Ist die angelegte Spannung hingegen nahe 3,3 V, wird das Signal als *high* = 1 interpretiert. Als Input verwendete GPIOs können nicht zwischen anderen Zuständen unterscheiden und können somit nicht zur Messung der angelegten Spannung verwendet werden.

Pull-up- und Pull-down-Widerstände

Ein Input-Pin soll nie unbeschaltet sein, weil seine Spannung dann undefiniert ist (*floating*). Gleichzeitig ist es nicht empfehlenswert, den Pin direkt mit der Masse oder mit der Versorgungsspannung (3,3 V) zu verbinden: Sollte der GPIO-Pin irrtümlich als Output-Pin programmiert sein, würden unter Umständen große Ströme fließen, die Ihren Raspberry Pi mit etwas Pech zerstören. Die Lösung für dieses Problem sind Pull-up- oder Pull-down-Widerstände in der Größenordnung von circa 1 kΩ bis 10 kΩ, um den Signaleingang für beide möglichen Zustände des Tasters mit der Masse bzw. mit 3,3 V zu verbinden. Hintergrundinformationen zu Pull-up- und Pull-down-Widerständen können Sie in der Wikipedia nachlesen:

http://de.wikipedia.org/wiki/Open_circuit#Beschaltung_der_Signalleitungen

Bei der Beschaltung des Raspberry Pi können Sie sich Pull-up- und Pull-down-Widerstände unter Umständen sparen: Zum einen sind die Pins 3 und 5 des P1-Headers standardmäßig mit 1,8 kΩ externen Pull-up-Widerständen verbunden; zum anderen lassen sich alle GPIOs im Input-Modus so programmieren, dass CPU-interne Pull-up- oder Pull-down-Widerstände aktiviert werden. Der interne Schaltungsaufbau ist auf der folgenden Seite gut beschrieben:

http://www.mosaic-industries.com/embedded-systems/microcontroller-projects/raspberry-pi/gpio-pin-electrical-specifications

Dennoch ist es empfehlenswert, Signaleingänge grundsätzlich mit einem externen Pull-up- oder Pull-down-Widerstand zu versehen. Sie vermeiden damit Probleme, wenn ein GPIO-Pin versehentlich falsch konfiguriert ist oder während der Initialisierung des Raspberry Pi einen anderen Zustand einnimmt, als Ihre Schaltung voraussetzt. Gefahrlos auf Pull-up-Widerstände können Sie nur verzichten, wenn Sie Ihren Taster mit den Pins 3 oder 5 verbinden. Diese beiden Pins stehen aber nur zur freien Verfügung, wenn Ihre Schaltung keine I^2S-Komponenten enthält.

Schaltung

Abbildung 12.19 zeigt den Aufbau der Schaltung. Soweit es die Leuchtdiode betrifft, gibt es keine Veränderung im Vergleich zum vorigen Abschnitt – wenn man einmal davon absieht, dass diesmal Pin 23 zur Ansteuerung verwendet wird.

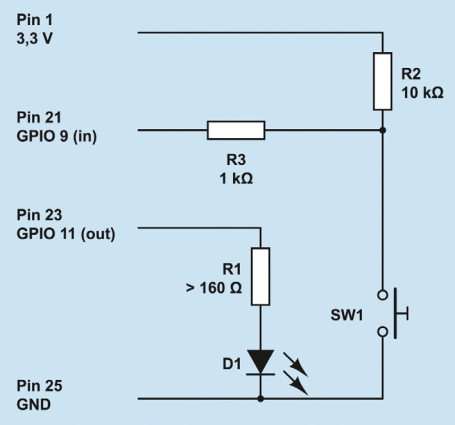


Abbildung 12.19 LED-Steuerung per Taster mit Pull-up-Widerstand

Der Taster ist direkt mit der Masse und über den Pull-up-Widerstand R2 mit der Versorgungsspannung 3,3 V verbunden. Im Normalzustand lautet der Signalzustand an Pin 21 also High, beim Drücken Low. Der Widerstand R3 ist eine zusätzliche Sicherheitsmaßnahme. Er verhindert einen Kurzschluss für den zugegebenermaßen unwahrscheinlichen Fall, dass Pin 21 irrtümlich als Output programmiert wird, auf High gestellt und gleichzeitig der Taster gedrückt ist. Ohne R3 gäbe es dann eine direkte Verbindung zwischen 3,3 V an Pin 21 und der Masse; es würde mehr Strom fließen, als der Raspberry Pi liefern kann. Dank R3 ist der Strom selbst in diesem Fall auf 3,3 mA begrenzt.

Test

Bevor Sie sich an die Programmierung machen, sollten Sie kurz überprüfen, ob der Schaltungsaufbau funktioniert. Zuerst schalten Sie versuchsweise die LED ein/aus:

```
pi$  gpio -1 mode 23 out
pi$  gpio -1 write 23 1      (LED ein)
pi$  gpio -1 write 23 0      (LED aus)
```

Dann testen Sie den Signaleingang an Pin 21, wobei Sie einmal die Taste gedrückt halten:

```
pi$  gpio -1 mode 21 in
pi$  gpio -1 read 21      (Normalzustand)
1
pi$  gpio -1 read 21      (Taste gedrückt)
0
```

Wenn Sie ein direktes Feedback wünschen, können Sie Pin 21 mit einem kleinen Python-Script kontinuierlich abfragen:

```
#!/usr/bin/python
# coding=utf-8
import RPi.GPIO as GPIO
import time

# Pin-Nummern verwenden (nicht GPIO-Nummern!)
GPIO.setmode(GPIO.BOARD)

# GPIO 21 = Input
GPIO.setup(21, GPIO.IN)

while True:
  input = GPIO.input(21)
  print("Zustand: " + str(input))
  time.sleep(0.01)
```

Sobald Sie dieses Programm starten, gibt es den aktuellen Signaleingang von Pin 21 regelmäßig im Terminal aus – bis Sie das Programm mit Strg+C wieder stoppen.

Signalüberwachung durch Events

Die Überwachung von Signalzuständen durch eine Schleife ist selten ein optimales Konzept. Wenn die `sleep`-Zeit kurz ist, verursacht das Programm eine Menge unnötige CPU-Last; verwenden Sie eine längere Zeit, steigt die Reaktionszeit des Programms, und im ungünstigsten Fall übersieht es einen kurzen Impuls ganz. Wesentlich intelligenter ist es, das Python-Programm so zu formulieren, dass es einfach auf einen Signalwechsel wartet und erst dann durch ein Event aktiv wird.

Das folgende Python-Programm demonstriert diese Vorgehensweise: Mit `def` wird eine Callback-Funktion definiert, die immer dann aufgerufen werden soll, wenn die Taste gedrückt wird. Genau darum kümmert sich `add_event_detect`: Damit wird Pin 23 überwacht; immer, wenn dessen Signalpegel von High auf Low fällt, wird die Funktion `switch_on` aufgerufen.

Das Programm soll laufen, bis es durch Strg+C beendet wird. Das ist der Zweck der Endlosschleife am Ende des Programms.

```
#!/usr/bin/python
# coding=utf-8
import RPi.GPIO as GPIO
import time, sys

# Pin-Nummern verwenden (nicht GPIO-Nummern!)
GPIO.setmode(GPIO.BOARD)
ledStatus = 0
```

```
# GPIO 21 = Input, 23 = Ouptput
GPIO.setup(21, GPIO.IN)
GPIO.setup(23, GPIO.OUT)
GPIO.output(23, ledStatus)

# Funktion definieren, um bei Tastendruck den LED-Zustand zu ändern
def switch_on( pin ):
  global ledStatus
  ledStatus = not ledStatus
  GPIO.output(23, ledStatus)
  return

# switch_on-Funktion aufrufen, wenn Signal von HIGH auf LOW wechselt
GPIO.add_event_detect(21, GPIO.FALLING, callback=switch_on)

# mit minimaler CPU-Belastung auf das Programmende durch Strg+C warten
try:
  while True:
    time.sleep(5)
except KeyboardInterrupt:
  GPIO.cleanup()
  sys.exit()
```

Taster entprellen

Wenn Sie Schaltung und Programm nun ausprobieren, werden Sie feststellen, dass das Ein- und Ausschalten recht unzuverlässig funktioniert. Schuld daran ist ein Verhalten aller mechanischer Taster und Schalter: Diese prellen, d. h., ein Metallblättchen schlägt *mehrfach* gegen einen Kontaktpunkt und löst deswegen ganz rasch hintereinander *mehrere* Pegelwechsel am Input-Pin aus.

Für das Problem gibt es zwei einfache Lösungen: Entweder bauen Sie in Ihre Schaltung einen Kondensator ein, der während seiner Ladezeit das Prellen verhindert, oder Sie entscheiden sich für eine Software-Lösung und warten nach jedem Input-Event 200 ms, bevor Sie wieder Eingaben entgegennehmen. Die Software-Lösung ist in der GPIO-Bibliothek für Python bereits vorgesehen. Sie geben einfach als zusätzlichen Parameter bei `add_event_detect` die gewünschte Entprellzeit in Millisekunden an:

```
GPIO.add_event_detect(21, GPIO.FALLING, callback=switch_on, bouncetime=200)
```

Bei meinen Tests mit Version 0.5.2a des Pakets `python-rpi.gpio` hat das leider nicht funktioniert. Eine entsprechende Funktion lässt sich mit wenig Aufwand selbst programmieren: Bei jedem Tastendruck merken Sie sich in `switch_on` die gerade aktuelle Zeit (Variable `lastTime`). Die nächste Veränderung des LED-Zustands führen Sie erst durch, wenn zumindest 200 ms vergangen sind.

```
# Änderungen im Programmcode
import datetime, time, sys
lastTime=datetime.datetime.now()
...
# bei Tastendruck LED-Zustand ändern
def switch_on( pin ):
  global ledStatus, lastTime
  now = datetime.datetime.now()
  if(now-lastTime > datetime.timedelta(microseconds=200000)):
    ledStatus = not ledStatus
    GPIO.output(23, ledStatus)
    lastTime = now
  return
```

Temperatur messen

Das Ziel dieses Abschnitts ist die Messung der Umgebungstemperatur mit einem Temperatursensor. Der Raspberry Pi verfügt über keine Analog-Eingänge, an denen die Spannung mit einem Analog/Digital-Wandler gemessen werden kann. Alle GPIO-Inputs sind digitale Eingänge, die nur zwischen 0 und 1 unterscheiden können. Deswegen empfiehlt es sich, zur einfachen Temperaturmessung ein Bauelement mit einem integrierten A/D-Wandler zu verwenden.

DS1820

Bewährt hat sich für diese Aufgabe das Bauelement DS1820, das oft auch als 1-Wire-Thermometer angepriesen wird. Dieser Name ergibt sich daraus, dass diese Komponente nur über drei Anschlüsse verfügt: Zwei dienen zur Stromversorgung und der dritte dient zur Signalübertragung in Form eines binären Datenstroms. Der DS1820 kann sogar ohne explizite Versorgungsspannung betrieben werden und bezieht den Strom dann über die Signalleitung; auf diese Schaltungsvariante gehe ich hier aber nicht ein.

Der DS1820 misst Temperaturen in einem Messbereich zwischen -55 °C und +125 °C. Die Temperatur wird als 9- oder 12-Bit-Zahl übertragen. Da jeder DS1820 mit einer eindeutigen Seriennummer ausgestattet ist, können mehrere Elemente parallel geschaltet und getrennt ausgewertet werden (über einen einzigen GPIO-Pin!). Beim Auslesen der Thermometer hilft ein eigenes Linux-Kernelmodul.

Es existieren verschiedene Varianten zum originalen DS1820: Am leichtesten erhältlich ist zumeist das Bauteil DS18S20, das fast vollständig kompatibel zum Original ist und als Grundlage für diesen Abschnitt diente. Ebenfalls populär ist die Variante DS18B20, bei dem die gewünschte Messgenauigkeit über ein Register programmiert werden kann. Eine kleinere Genauigkeit ermöglicht schnellere Messungen und reduziert den Stromverbrauch. Einige DS1820-Varianten werden zudem in einer wasserdichten Ausführung angeboten, die aber dieselben elektrischen Eigenschaften

aufweist. Ein ausführliches Datenblatt sowie eine Beschreibung der Unterschiede zwischen den verschiedenen Varianten finden Sie hier:

http://datasheets.maximintegrated.com/en/ds/DS18S20.pdf
http://www.maximintegrated.com/app-notes/index.mvp/id/4377

Schaltung

Abbildung 12.20 zeigt den Schaltungsaufbau. Ähnlich wie bei mechanischen Schaltern muss auch beim DS1820 ein Pull-up-Widerstand verwendet werden. Beachten Sie, dass Sie – im Gegensatz zu den bisherigen Schaltungen – den Signaleingang nicht frei wählen können. Sie müssen Pin 7 = GPIO 4 verwenden, weil der 1-Wire-Kerneltreiber ausschließlich diesen Signaleingang benutzt!

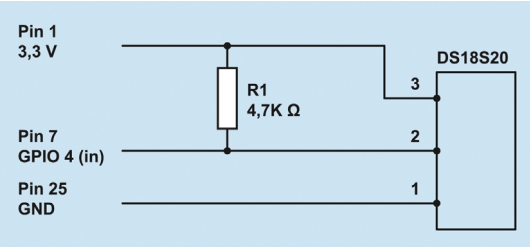


Abbildung 12.20 Schaltungsaufbau zur Messung der Umgebungstemperatur

Welcher Pin des DS1820 ist Pin 1?

Die Belegung der Pins des DS1820 geht aus dem Datenblatt hervor. Dabei müssen Sie beachten, dass das Bauelement in der Sicht von unten (*bottom view*) dargestellt ist!

Temperatur auslesen

Bevor Sie die Temperatur auslesen können, müssen Sie Pin 7 als Signaleingang konfigurieren und zwei Kernelmodule laden:

```
root#  gpio -1 mode 7 in
root#  modprobe w1_gpio
root#  modprobe w1_therm
```

Wenn Sie möchten, dass diese Kernelmodule immer geladen werden, fügen Sie deren Namen der Datei `/etc/modules` hinzu. Der Datei `/sys/devices/w1_bus_master1/w1_master_slaves` können Sie nun die IDs aller angeschlossenen DS1820-Sensoren entnehmen. In diesem Beispiel gibt es nur einen Sensor:

```
pi$  cat /sys/devices/w1_bus_master1/w1_master_slaves
10-000802ae1551
```

Die Messdaten jedes Sensors liegen in einer Textdatei vor. Interessant ist die zweite Zeile: `t=nnn` gibt die Temperatur in Tausendstel Grad an, auch wenn die Messgenauigkeit geringer ist. Zum Messzeitpunkt betrug die Umgebungstemperatur also ca. 20,6 °C.

```
pi$  cat /sys/devices/w1_bus_master1/10-000802ae1551/w1_slave
29 00 4b 46 ff ff 02 10 0c : crc=0c YES
29 00 4b 46 ff ff 02 10 0c t=20625
```

IR-Empfänger

Wenn Sie Ihren Raspberry Pi als Media-Center verwenden und dieses mit einer IR-Fernbedienung steuern möchten, benötigen Sie einen IR-Empfänger. Das gängigste Bauteil hierfür hat die Bezeichnung TSOP4838. DEs ist Mitglied einer ganzen Familie von IR-Empfängern, die für unterschiedliche Frequenzen optimiert sind. Das Bauteil TSOP4838 ist auf 38 kHz abgestimmt, also auf den Frequenzbereich typischer TV-Fernbedienungen. Technische Details können Sie im Datenblatt nachlesen. Beachten Sie, dass die Belegung der Pins je nach TSOP-Variante unterschiedlich ist!

http://www.vishay.com/docs/82459/tsop48.pdf

Schaltung

Die Schaltung in Abbildung 12.21 entspricht dem Vorschlag aus dem Datenblatt. Sowohl der Widerstand als auch der Kondensator sind optional; sie verbessern lediglich die elektrische Stabilität der Schaltung. Sie können also auch direkt die Pins 1, 2 und 3 des TSOP4838 mit den Pins 25 (GND), 12 und 1 (3,3 V) des P1-Headers des Raspberry Pi verbinden. Warum dient gerade Pin 12 als Signaleingang? Weil der mit ihm verbundene Eingang GPIO 18 standardmäßig vom `lirc`-Kerneltreiber verwendet wird.

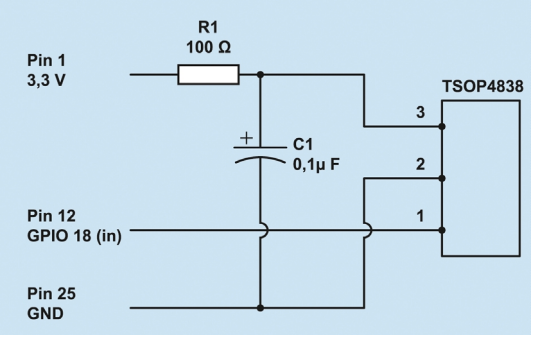


Abbildung 12.21 Ein einfacher IR-Empfänger

IR-Signale verarbeiten

Um den IR-Empfänger auszuprobieren, benötigen Sie das Kernelmodul `lirc_rpi` und das Kommando `mode2` aus dem Paket `lirc`. Damit können Sie im Textmodus Signale der Device-Datei der IR-Schnittstelle auslesen. Jetzt brauchen Sie nur noch eine Fernbedienung auf den IR-Empfänger richten und einige Tasten drücken.

```
root#  apt-get install lirc
root#  modprobe lirc_rpi
```

```
root#  dmesg | grep lirc
lirc_dev: IR Remote Control driver registered, major 251
lirc_rpi: module is from the staging directory, the quality is unknown,
  you have been warned.
lirc_rpi lirc_rpi.0: lirc_dev: driver lirc_rpi registered at minor = 0
lirc_rpi: driver registered!
input: lircd as /devices/virtual/input/input3
lirc_rpi: auto-detected active low receiver on GPIO pin 18
root#  mode2 -d /dev/lirc0
space 1613
pulse 584
space 537
pulse 593
space 524
pulse 603
space 530
...
<Strg>+<C>
```

Hinweis

Sollte auf Ihrem Raspberry Pi der Dämon `lircd` laufen, müssen Sie diesen vor dem Test der Fernbedienung durch `mode2` beenden: `kill $(pidof lircd)`

`mode2` ist nur dazu gedacht, die Fernbedienung auszuprobieren. In aller Regel werden Sie den IR-Empfänger in Kombination mit XBMC und dem Hintergrundprogramm `lircd` verwenden. Tipps zur richtigen Konfiguration Ihrer Fernbedienung finden Sie in Abschnitt 12.3.

12.5 Interna und Backups

Der Inhalt der Boot-Partition

Damit der Boot-Prozess des Raspberry Pi funktioniert, muss die erste Partition der SD-Karte eine VFAT-Partition sein und mehrere Dateien enthalten, deren Inhalt in Tabelle 12.3 zusammengefasst ist. Im laufenden Betrieb finden Sie diese Dateien im Verzeichnis `/boot`. Normalerweise sollten Sie diese Dateien nicht anrühren. Die einzige Ausnahme ist die Datei `config.txt`, die im nächsten Abschnitt näher beschrieben wird. Sollten Sie aus irgendeinem Grund aktuellere Versionen dieser Dateien benötigen, finden Sie diese im folgenden GitHub-Repository:

https://github.com/raspberrypi/firmware

Datei	Inhalt
config.txt	Textdatei zur Hardware-Konfiguration
bootcode.bin	der Bootloader
start.elf	die Firmware des Grafikprozessors
kernel.img	der Linux-Kernel
cmdline.txt	Textdatei mit Parametern, die an den Kernel übergeben werden

Tabelle 12.3 Die Boot-Dateien des Raspberry Pi

Boot-Prozess

Der Boot-Vorgang verläuft auf dem Raspberry Pi vollkommen anders als auf einem gewöhnlichen PC. Es gibt kein BIOS, kein EFI und keinen GRUB. Wenn der Raspberry Pi eingeschaltet wird, ist vorerst nur der GPU-Core aktiv, also der Grafikteil der CPU. Die GPU lädt den ersten Teil des Bootloaders aus einem ROM (1st stage bootloader). Mit diesem Miniprogramm kann die CPU auf die SD-Karte zugreifen und dort `bootcode.bin` in den Cache der CPU lesen. Diese Datei enthält den restlichen Bootloader (2nd stage bootloader). Der Bootloader lädt nun `start.elf`. Das darin enthaltene Programm wertet `config.txt` aus, liest `cmdline.txt` und `kernel.img` und startet schließlich den Kernel.

Die Konfigurationsdatei »config.txt«

Unabhängig davon, welches Betriebssystem Sie auf Ihrem Raspberry Pi installiert haben, bestimmt die Datei `config.txt` in der ersten Partition der SD-Karte viele Eckdaten der Konfiguration. Die Datei wird direkt beim Booten des Raspberry Pi ausgewertet. Dieser Abschnitt fasst die wichtigsten Einstellmöglichkeiten dieser Datei zusammen. Noch mehr `config.txt`-Details können Sie hier nachlesen:

http://elinux.org/RPi_config.txt

Parameter auslesen

Veränderungen an `config.txt` werden erst mit dem nächsten Neustart wirksam. Viele `config.txt`-Parameter können Sie im laufenden Betrieb mit `vcgencmd get_config` auslesen (siehe den folgenden Abschnitt).

Speicher für das Grafiksystem

Der Raspberry Pi (Modell B) verfügt insgesamt über 512 MByte RAM. Das RAM wird zwischen der CPU und dem Grafikprozessor geteilt. Bei Raspberry-Pi-Modellen mit aktueller Firmware (verfügbar seit November 2012) und einer Distribution mit aktuellem Kernel erfolgt die Teilung dynamisch je nach Bedarf.

Bei älteren Modellen muss die Aufteilung hingegen bereits beim Start des Geräts endgültig festgelegt werden, wobei Sie dem Grafiksystem 16, 64, 128 oder 256 MByte zuweisen können. 16 MByte sind für den normalen Betrieb ausreichend. Für grafik-

intensive Anwendungen (3D-Grafik, HD-Filme abspielen etc.) benötigt das Grafiksystem hingegen 128 MByte Speicher. Wie viel Speicher für das Grafiksystem reserviert werden soll, geben Sie mit dem Parameter `gpu_mem` in MByte an.

```
gpu_mem=128
```

HDMI-Einstellungen

Normalerweise funktioniert die Grafik via HDMI ohne weitere Konfiguration. Nur wenn es Probleme gibt, können Sie mit diversen `hdmi_xxx`-Parametern bestimmte Einstellungen erzwingen. Das folgende Listing gibt hierfür einige Beispiele:

```
# HDMI-Ausgang verwenden, auch wenn kein Monitor erkannt wird
hdmi_force_hotplug=1

# HDMI-Auflösung 1400*1050 @ 60 Hz
# alle zulässigen hdmi_mode-Werte: siehe http://elinux.org/RPi_config.txt
hdmi_group=2
hdmi_mode=42

# Display-Drehung korrigieren
# 1 = 90 Grad, 2 = 180 Grad, 3 = 270 Grad
display_rotate=1

# HDMI-Signalstärke
# 0 = normal, 7 = maximal (Vorsicht!)
config_hdmi_boost=4
```

Wenn Sie nicht wissen, welche Video-Modi Ihr Monitor unterstützt, führen Sie das Kommando `tvservice` aus. Die aufgelisteten Modi mit der Option `-m CEA` gelten für `hdmi_group=1`, die Modi mit der Option `-m DMT` für `hdmi_group=2`. Die folgenden Ergebnisse sind auf einem Monitor mit einer Auflösung von 1920*1200 Pixel entstanden:

```
pi$  vservice -m CEA
Group CEA has 7 modes:
           mode 1: 640x480 @ 60Hz 4:3, clock:25MHz progressive
           mode 2: 720x480 @ 60Hz 4:3, clock:27MHz progressive
           ...
  (native) mode 16: 1920x1080 @ 60Hz 16:9, clock:148MHz progressive
pi$  tvservice -m DMT
Group DMT has 13 modes:
           mode 4: 640x480 @ 60Hz 4:3, clock:25MHz progressive
           ...
           mode 68: 1920x1200 @ 60Hz 16:10, clock:154MHz progressive
```

Overclocking

Overclocking ermöglicht es, Ihren Raspberry Pi schneller zu takten als vorgesehen. Gerade für CPU- oder GPU-intensive Aufgaben, z. B. für die HD-Wiedergabe von Videos, ist Overclocking natürlich eine willkommene Hilfe, um den Raspberry Pi schneller zu machen.

Laut offiziellen Angaben auf der Raspberry-Pi-Website (*http://www.raspberrypi.org/archives/2008*) ist moderates Overclocking sicher. Das heißt, es sind weder Stabilitätsprobleme noch ein vorzeitiger Hitzetod zu erwarten, sofern die CPU-Temperatur 85 Grad Celsius nicht überschreitet. Dem widersprechen aber viele Foren-Berichte mit negativen Erfahrungen von Raspberry-Pi-Besitzern. Zudem führt der Einsatz von Overclocking in Kombination mit schnellen SD-Karten (Class 6 oder Class 10) häufig zu Speicherfehlern. Letztlich müssen Sie also selbst entscheiden, ob Ihnen mehr Performance das damit verbundene Risiko wert ist. Ich rate Ihnen davon ab.

Aus technischer Sicht ist das Overclocking unkompliziert. Sie müssen lediglich einige Zeilen in `config.txt` ändern und Ihren Raspberry Pi neu starten:

```
# Taktfrequenz der CPU in MHz. Default 700 MHz.
arm_freq=800

# Taktfrequenzen der Grafik- und Encoding-Cores. Default 250 MHz.
# GPU = Graphics Processing Unit.
gpu_freq=300

# RAM-Taktfrequenz. Default 400 MHz.
sdram_freq=450

# Immer die angegebene Taktfrequenz verwenden, keine dynamische
# Absenkung in Ruhepausen.
force_turbo=1

# Die Spannung um n*0.025 V anheben. Nur bei starkem Overclocking erforderlich.
# Maximal 6 mit force_turbo=0 (entspricht 0.150 V),
# maximal 8 mit force_turbe=1 (entspricht 0.2V).
over_voltage=0
over_voltage_sdram=0

# Limitiert die CPU-Temperatur (in Grad Celsius).
# Beim Erreichen der Temperatur werden Taktfrequenz und
# Spannung auf die Defaulteinstellung zurückgesetzt.
temp_limit = 85
```

Das Overclocking erfolgt normalerweise dynamisch, d. h. nur dann, wenn die CPU- oder GPU-Leistung tatsächlich benötigt wird. In den Ruhezeiten laufen CPU und GPU in den Defaulttaktfrequenzen. `force_turbo=1` verhindert die Taktabsenkung und bewirkt, dass die CPU/GPU immer mit der angegebenen Frequenz getaktet wird. Das ist stabiler, die CPU/GPU wird aber schneller heiß. Die gerade aktuelle CPU-Frequenz können Sie wie folgt auslesen (in kHz):

```
pi$  cat /sys/devices/system/cpu/cpu0/cpufreq/scaling_cur_freq
700000
```

`gpu_freq` verändert gleichermaßen die Taktfrequenz des Grafik-Cores sowie diverser anderer Video- und Encoding-Komponenten. Mit den Parametern `core_freq`, `h264_freq`, `isp_freq` und `v3d_freq` können für diese Komponenten auch jeweils eigene Taktfrequenzen eingestellt werden.

Der gerade aktuelle Temperatur können Sie aus der Datei `/sys/class/thermal/thermal_zone0/temp` auslesen (in Milligrad, d. h., 46540 entspricht 46,5 Grad) oder direkt mit dem Kommando `vcgencmd measure_temp` ermitteln.

Video-Codecs

Die Encoding-Komponenten der GPU können die Video-Decodierung unterstützen. Für manche Codecs ist das standardmäßig der Fall, für andere muss diese Funktion mit einem kostenpflichtigen Lizenzschlüssel freigeschaltet werden. Momentan sind zwei derartige Schlüssel vorgesehen: je einer für den MPG-2- und für den VC-1-Decoder. Die folgenden Werte sind natürlich nur Muster. Die Schlüssel müssen zur ID Ihrer CPU passen.

```
decode_MPG2=0x12345678
decode_WVC1=0x9abcedf0
```

Bootvorgang

Die folgenden Parameter modifizieren den Bootvorgang:

```
# Parameter für den Kernel (anstelle der Datei cmdline.txt)
cmdline=xxx

# Name der Kernel-Datei (default: kernel.img)
kernel=filename

# Wartezeit, bevor der Kernel geladen wird (in Sekunden, default 1).
boot_delay=2
```

Das Kommando »vcgencmd«

Mit dem Kommando `vcgencmd` können Sie diverse Statusinformationen der CPU auslesen. `vcgencmd commands` liefert eine Liste aller bekannten Kommandos. Die folgenden Beispiele zeigen einige Anwendungen:

```
pi$ vcgencmd measure_clock arm          (CPU-Frequenz)
frequency(45)=700072000
pi$ vcgencmd measure_clock core         (Frequenz der Grafik-Cores)
frequency(1)=250000000
pi$ vcgencmd measure_volts core         (Spannung der Grafik-Cores)
volt=1.20V
pi$ vcgencmd measure_temp               (CPU-Temperatur)
temp=47.1'C
pi$ vcgencmd codec_enabled H264         (Steht Codec xy zur Verfügung?)
H264=enabled
```

```
pi$  vcgencmd get_config int          (Liste aller aktiven Integer-Optionen)
disable_overscan=1
temp_limit=85
force_pwm_open=1
pi$  vcgencmd get_config str          (Liste aller aktiven String-Optionen)
```

Noch mehr Anwendungsbeispiele finden Sie hier:

http://elinux.org/RPI_vcgencmd_usage

Backups

Grundsätzlich gelten für den laufenden Betrieb eines Minicomputers dieselben Backup-Strategien wie für einen gewöhnlichen Computer (siehe Kapitel 39): Wenn Sie auf Ihrem Minicomputer veränderliche Daten speichern, sollten Sie diese regelmäßig sichern. Im Idealfall hat der Minicomputer eine Verbindung zu einem NAS-Gerät; dann bietet sich die Programmierung eines kleinen Backup-Scripts an, das einmal täglich alle relevanten Daten in einem Netzwerkverzeichnis sichert.

SD-Karte sichern

Davon losgelöst ist es zweckmäßig, hin und wieder eine Sicherungskopie der ganzen SD-Karte zu erstellen. Dieses Backup kann dann jederzeit auf eine neue, zumindest gleich große SD-Karte übertragen werden. Die folgenden Beispiele gehen wieder davon aus, dass das Device der SD-Karte `/dev/sdb` lautet. Passen Sie die Device-Angaben entsprechend an!

```
root#  umount /dev/sdb?
root#  dd if=/dev/sdb of=backup.img bs=4M
```

Das Auslesen großer SD-Karten dauert leider ziemlich lange. Wenn Sie in dieser Zeit ein Feedback wünschen, setzen Sie statt `dd` das Kommando `dcfldd` ein. Optional können Sie die zu sichernden Daten auch gleich komprimieren:

```
root#  dd if=/dev/sdb bs=4M | gzip > backup.img.gz
```

Riesen-Backup, obwohl die SD-Karte halb leer ist?

Die Backup-Datei wird möglicherweise trotz Komprimierung größer ausfallen als erwartet – auch dann, wenn nur ein kleiner Teil der SD-Karte tatsächlich mit Daten gefüllt ist. Das liegt daran, dass in jedem Fall der gesamte Datenträger blockweise ausgelesen wird, egal ob diese Blöcke vom Dateisystem genutzt sind oder nicht. Oft enthalten die Blöcke Zufallsdaten, z. B. Überreste einer früheren Nutzung der Karte in einer Digitalkamera, die schwer zu komprimieren sind.

In die umgekehrte Richtung sehen die Kommandos wie folgt aus. Beachten Sie, dass dabei der gesamte Inhalt des Datenträgers `/dev/sdb` überschrieben wird!

SD-Karte wiederherstellen

```
root#  umount /dev/sdb?
root#  dd if=backup.img of=/dev/sdb bs=4M
```

Wenn Sie das Backup-Image komprimiert haben, gehen Sie so vor:

```
root#  gunzip -c backup.img.gz | dd of=/dev/sdb bs=4M
```

12.6 Wenn es Probleme gibt

Nicht immer klappt alles auf Anhieb. Wenn Sie Pech haben, stürzt Ihr Raspberry Pi nach wenigen Sekunden ab, bleibt hängen, zeigt unverständliche Fehlermeldungen an oder – was sicherlich der unangenehmste Fall ist – liefert am Bildschirm überhaupt kein Bild. Dann ist eine Diagnose natürlich besonders schwierig. Dieser Abschnitt fasst einige Tipps zusammen, was Sie in solchen Fällen tun können.

Stromversorgung

Wenn man Forenberichten glauben darf, ist eine unzureichende Stromversorgung die bei Weitem häufigste Fehlerursache. Der Raspberry Pi benötigt laut Spezifikation an sich bereits 750 mA Strom – das ist wesentlich mehr, als typische Handy-Netzteile mit Micro-USB-Kabel liefern können. Sparen Sie daher nicht beim Netzteil, sondern kaufen Sie eines, das zumindest 1 A Strom liefern kann (also 5 Watt Leistung bei einer Ausgangsspannung von 5 V).

Auch mit einem ausreichend dimensionierten Netzteil ist der Raspberry Pi nicht in der Lage, eine Menge USB-Geräte mit Strom zu versorgen! Wenn Sie mehr als Tastatur und Maus anschließen wollen, brauchen Sie unter Umständen bereits einen USB-Hub mit eigener Stromversorgung. Bei meinen Tests funktionierten auch eine Tastatur, eine Maus und ein WLAN-Stecker noch problemlos, wobei in diesem Fall die Maus an die Tastatur angeschlossen war.

Wenn Sie also Stabilitätsprobleme haben oder Ihr Raspberry Pi immer wieder unmotiviert neu startet: Versuchen Sie es mit einem besseren Netzteil, verwenden Sie einen aktiven USB-Hub bzw. lösen Sie alle Verbindungen zu USB-Peripheriegeräten, die Sie nicht unbedingt brauchen. Deaktivieren Sie gegebenenfalls auch das Overclocking, von dem ich Ihnen generell abrate.

SD-Karte

An zweiter Stelle in der Hitliste der Probleme mit dem Raspberry Pi stehen SD-Karten. Es gibt Modelle, die nicht zum Raspberry Pi kompatibel sind, auch wenn diese Karten in einer Kamera oder im Kartenslot eines Notebooks problemlos funktionieren. Versuchen Sie es einfach mit einem anderen Modell, und werfen Sie vor dem Kauf einen Blick auf die folgende Seite der Embedded Linux Wikis:

http://elinux.org/RPi_SD_cards

Nicht immer ist die Karte an sich schuld. Eine mögliche Fehlerursache kann auch sein, dass Sie das Linux-Image nicht fehlerfrei auf die SD-Karte übertragen haben. Das Problem äußert sich in der Regel dadurch, dass der Boot-Prozess von diversen *Authentication*-Warnungen unterbrochen wird und schließlich ganz stoppt.

Abhilfe: Kopieren Sie die Image-Datei nochmals auf die SD-Karte. Vergleichen Sie vorher die SHA1-Prüfsumme der ZIP-Datei mit dem auf der Download-Seite angegebenen Wert. Achten Sie unbedingt darauf, dass keine Partition der SD-Karte in den Verzeichnisbaum eingebunden ist! Wenn die SD-Karte den Device-Namen `/dev/sdb` hat, müssen Sie also vor dem `dd`-Kommando `umount /dev/sdb?` ausführen.

SD-Karten sind keine Festplatten!

Generell sind SD-Karten – unabhängig von ihrem Preis – leider oft Billigprodukte, deren Lebensdauer und Stabilität selten mit Festplatten oder SSDs mithalten kann. Überlegen Sie sich eine Backup-Strategie, vermeiden Sie nach Möglichkeit stark I/O-lastige Anwendungen, bzw. speichern Sie Ihre Daten auf einem NAS-Speichergerät.

Display-Probleme

Besonders schwierig ist die Fehlersuche, wenn Ihr Monitor oder Fernseher gar kein Bild zeigt. Klären Sie zuerst die naheliegenden Fragen: Funktioniert die Stromversorgung? Wenn im Raspberry Pi nicht zumindest eine rote Diode leuchtet, bekommt der Computer keinen bzw. zu wenig Strom. Ist das Kabel oder der Bildschirm schuld? Wenn möglich, versuchen Sie es mit einem anderen HDMI-Kabel bzw. mit einem anderen Monitor/Fernseher.

Wenn das alles nichts hilft, sollten Sie versuchen, in der Datei `config.txt` auf der ersten Partition der SD-Karte Veränderungen vorzunehmen. Diese Datei wird vom Raspberry Pi unmittelbar nach dem Start gelesen und enthält unter anderem einige Parameter, die das HDMI-Signal und die Grafikauflösung betreffen. Standardmäßig enthält diese Datei nur eine einzige für das Grafiksystem relevante Anweisung:

```
# Datei config.txt (Default-Einstellung)
disable_overscan=1
```

Bei Display-Problemen sollten Sie es mit dieser Einstellung versuchen:

```
# Datei config.txt
hdmi_force_hotplug=1
config_hdmi_boost=4
hdmi_group=2
hdmi_mode=4
disable_overscan=0
```

Ihr Raspberry Pi verwendet nun eine Auflösung von nur 640*480 Pixel, wobei der tatsächlich nutzbare Bereich wegen eines schwarzen Overscan-Bereichs an den Rändern noch etwas kleiner ist. Wirklich zufriedenstellend arbeiten können Sie so nicht,

aber immerhin lässt sich auf diese Weise sicherstellen, dass Ihr Minicomputer an sich funktioniert.

config.txt sicher ändern

Zur Veränderung der Datei `config.txt` unterbrechen Sie die Stromversorgung zum Raspberry Pi und stecken die SD-Karte in den Slot Ihres regulären Computers. Dort können Sie die Datei `config.txt` mit einem beliebigen Editor ändern. Speichern Sie die Veränderungen, werfen Sie die SD-Karte im Dateimanager aus, stecken Sie sie wieder in den Raspberry Pi, und stellen Sie dessen Stromversorgung wieder her.

Sobald Ihr Raspberry Pi läuft, können Sie `config.txt` auch im laufenden Betrieb ändern. Sie finden die Datei im `/boot`-Verzeichnis. Änderungen werden erst nach einem Neustart wirksam.

Wenn am Monitor nach dem Einschalten des Raspberry Pi nur ein buntes Farbmuster zu sehen ist (links oben Rot, rechts unten Hellblau), deutet das darauf hin, dass die Datei `start.elf` von der ersten Partition der SD-Karte gelesen werden konnte, dass aber der Linux-Kernel aus der Datei `kernel.img` nicht gelesen oder ausgeführt werden kann.

Status-LEDS

Im Raspberry Pi befindet sich zwischen den beiden USB-Buchsen und dem Audio-Ausgang eine Gruppe von fünf Leuchtdioden. Die LEDs geben Auskunft über den Status des Minicomputers:

- **Erste LED** (gelb, am äußeren Rand): gibt die Geschwindigkeit der Ethernet-Verbindung an. An: 100 Mbp/s. Aus: 10 Mbp/s oder keine Verbindung.
- **Zweite LED** (grün): leuchtet, wenn eine Ethernet-Netzwerkverbindung besteht.
- **Dritte LED** (grün): leuchtet, wenn über die Ethernet-Schnittstelle Daten in beide Richtungen übertragen werden (Full Duplex Mode).
- **Vierte LED** (rot): leuchtet, wenn der Raspberry Pi mit der Stromversorgung verbunden ist.
- **Fünfte LED** (grün, nahe dem Audio-Ausgang): leuchtet, wenn Daten von oder zur SD-Karte übertragen werden. Falls diese LED nach dem Einschalten nur schwach leuchtet, findet der Raspberry Pi auf der SD-Karte die zum Booten erforderlichen Dateien nicht bzw. kann überhaupt nicht mit der SD-Karte kommunizieren.

  Wenn der Raspberry Pi nur einen Teil der Boot-Dateien lesen kann, blinkt die grüne LED in einem speziellen Muster:

  Dreimal Blinken bedeutet, dass die Datei `start.elf` nicht gefunden wurde.
  Viermal Blinken bedeutet, dass `start.elf` nicht ausgeführt werden kann.
  Siebenmal Blinken bedeutet, dass `kernel.img` nicht gefunden wurde.

Wenn Sie den Raspberry Pi mit der Stromversorgung verbinden, sollte sofort die rote LED zu leuchten beginnen. Wenn alles klappt, beginnt nach ein, zwei Sekunden die grüne LED unregelmäßig zu blinken. Das bedeutet, dass die Boot-Dateien von der SD-Karte gelesen werden.

Andere Probleme

Als *die* ultimative Referenz bei Hardware-Problemen mit dem Raspberry Pi gilt die folgende Website:

http://elinux.org/R-Pi_Troubleshooting

TEIL III

Arbeiten im Terminal

Kapitel 13
Terminalfenster und Konsolen

Vom Desktop ins Terminal

Bis jetzt habe ich Ihnen Linux in erster Linie als Desktop-System präsentiert. Sie haben diverse Internet- und Büroprogramme kennengelernt, die vielleicht ein wenig anders aussehen als unter Windows oder OS X, aber letztlich denselben Zweck erfüllen und ähnlich zu bedienen sind. Der Umgang mit Linux endet allerdings nicht an dieser Stelle. Es gibt quasi noch eine andere Seite von Linux, die auf den ersten Blick abschreckend wirken mag: Erfahrene Linux-Anwender führen in Terminalfenstern bzw. Textkonsolen Kommandos aus und erhalten die Resultate wiederum in Textform. Die Maus spielt nur noch eine Nebenrolle, grafische Benutzeroberflächen sind passé.

Wenn Sie einmal gelernt haben, in einem Terminalfenster zu arbeiten, können Sie dort viele Aufgaben effizient ausführen. Sie können Linux-Kommandos miteinander verknüpfen, im Hintergrund ausführen, automatisch ausführen, in kleinen Programmen (Scripts) automatisieren etc. All diese Möglichkeiten stehen Ihnen auch dann zur Verfügung, wenn Sie nicht lokal am Rechner sitzen, sondern nur über eine Netzwerkverbindung verfügen.

Reine Büroanwender werden für Terminalfenster seltener Verwendung finden als Programmierer oder Netzwerkadministratoren. Auf jeden Fall aber gehört die Arbeit im Terminal zum elementaren Handwerkszeug jedes Anwenders, der Linux richtig kennenlernen will. Das merken Sie spätestens dann zum ersten Mal, wenn das Grafiksystem wegen einer Fehlkonfiguration nicht funktioniert oder wenn Sie Ihren externen Root-Server administrieren möchten.

Querverweise

Dieses Kapitel gibt lediglich einen ersten Überblick über Arbeitstechniken in Terminalfenstern bzw. Konsolen. Für die Ausführung der Programme im Terminal ist eine sogenannte Shell verantwortlich. Unter Linux stehen mehrere Shells zur Auswahl. Am häufigsten kommt die `bash` zum Einsatz, deren Grundfunktionen Thema des nächsten Kapitels sind.

Die weiteren Kapitel stellen dann diverse Linux-Kommandos näher vor. Diese dienen beispielsweise zur Verwaltung des Dateisystems (`ls`, `cp`, `mv`, `ln`, `rm` etc.), zur Suche nach Dateien (`find`, `grep`, `locate`), zur Steuerung von Netzwerkfunktionen (`ping`, `ip`, `ssh`) etc. Nebenbei werden Sie eine Menge Linux-Grundlagen lernen.

13.1 Textkonsolen und Terminalfenster

Textkonsolen

Microsoft Windows können Sie ausschließlich im Grafikmodus verwenden. Linux können Sie dagegen auch in sogenannten Textkonsolen nutzen. Bei den meisten Distributionen stehen sechs Textkonsolen zur Verfügung. Der Wechsel zwischen diesen Textkonsolen erfolgt mit Alt+F1 für die erste Konsole, Alt+F2 für die zweite etc. Wenn der Rechner bereits im Grafikmodus läuft, führt Strg+Alt+F1 in die erste Textkonsole und Alt+F7 zurück in den Grafikmodus. Bei einigen Distributionen, unter anderem Fedora, ist die erste Konsole für den Grafikmodus reserviert.

Bevor Sie in einer Textkonsole arbeiten können, müssen Sie sich einloggen. Wenn Sie mit der Arbeit fertig sind oder wenn Sie sich unter einem anderen Namen anmelden möchten, müssen Sie sich wieder ausloggen. Dazu drücken Sie einfach Strg+D.

Sie können in der einen Konsole ein Kommando starten, und während dieses Kommando läuft, können Sie in der zweiten Konsole etwas anderes erledigen. Sie können sich auch in einer Konsole als `root` anmelden, um administrative Aufgaben zu erledigen, während Sie in der anderen Konsole unter Ihrem normalen Login-Namen eine Datei editieren. Jede Konsole läuft also vollkommen unabhängig von den anderen.

Tastenkürzel	Funktion
Strg+Alt+Fn	vom Grafikmodus in die Textkonsole *n* wechseln
Alt+Fn	von einer Textkonsole in eine andere Textkonsole *n* wechseln
Alt+F7	zurück in den Grafikmodus wechseln (Alt+F1 bei Fedora, Alt+F5 bei Knoppix)
Alt+→/+←	in die vorige/nächste Textkonsole wechseln
⇧+Bild↑/Bild↓	vorwärts/rückwärts blättern
Strg+Alt+Entf	Linux beenden (nur in Textkonsolen, führt `shutdown` aus, Vorsicht!)

Tabelle 13.1 Tastenkürzel zum Aktivieren von Textkonsolen

Mit ⇧+Bild↑ und ⇧+Bild↓ scrollen Sie den Bildschirminhalt einer Textkonsole auf und ab. Auf diese Weise können Sie die Ergebnisse der zuletzt ausgeführten Programme nochmals ansehen, auch wenn sie bereits aus dem sichtbaren Bildschirmbereich hinausgeschoben wurden.

Terminalfenster (Shell-Fenster)

Natürlich müssen Sie aus dem Grafikmodus nicht in eine Textkonsole wechseln, nur um Kommandos auszuführen. Für diesen Zweck reicht ein in einem Fenster ausgeführtes Terminalprogramm vollkommen aus (siehe Abbildung 13.1). Zur

Bezeichnung eines Terminals sind mitunter auch die Begriffe »Konsolenfenster« oder »Shell-Fenster« gebräuchlich.

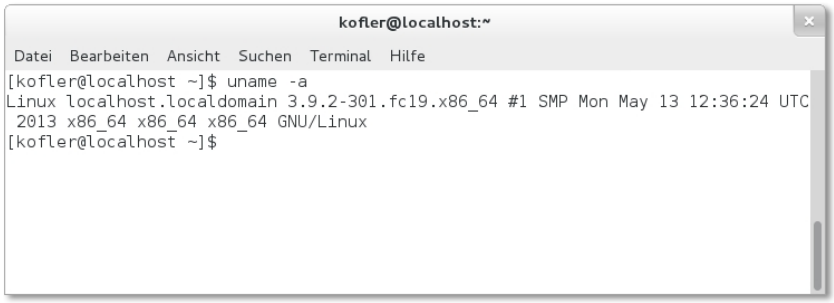


Abbildung 13.1 Ein Terminalfenster

Je nach Distribution und Desktop-System stehen unterschiedliche Terminalfenster zur Auswahl, beispielsweise `gnome-terminal` (Gnome), `konsole` (KDE) oder `xterm` (X). Auch das Menükommando zum Starten eines Terminalfensters variiert je nach Distribution – hier ein paar Beispiele:

Fedora (Gnome 3): ⊞ `terminal`
openSUSE (KDE): Anwendungen • System • Terminal
RHEL 6 (Gnome): Anwendungen • Systemwerkzeuge • Terminal
Ubuntu (Unity): ⊞ `terminal`

Bei manchen Gnome-Versionen kann ein Terminalfenster noch bequemer durch ein Kontextmenükommando im Desktop geöffnet werden. Dazu muss das Zusatzpaket `nautilus-open-terminal` installiert sein.

In Terminalfenstern können Sie wie in einer Textkonsole arbeiten. Der einzige Unterschied besteht darin, dass Sie dank einer Bildlaufleiste bequemer durch die bisherigen Ausgaben scrollen können.

Wichtige Tastenkürzel

Innerhalb von Textkonsolen bzw. Terminalfenstern helfen diverse Tastenkürzel bei der effizienten Eingabe von Kommandos. Tabelle 13.2 fasst die wichtigsten Kürzel zusammen. Sie gelten nur, wenn Sie die bash in der Standardkonfiguration als Shell verwenden, was bei den meisten Distributionen der Fall ist. Wenn Sie unter Gnome in einem Terminalfenster arbeiten, sollten Sie Bearbeiten • Tastenkombinationen ausführen und die Option Alle Menükürzelbuchstaben aktivieren deaktivieren.

Insbesondere die Kommandoerweiterung mit ⇆ spart eine Menge Tipparbeit. Sie brauchen nur die ersten Buchstaben eines Kommandos oder einer Datei angeben. Anschließend drücken Sie ⇆. Wenn der Dateiname bereits eindeutig erkennbar ist, wird er vollständig ergänzt, sonst nur so weit, bis sich mehrere Möglichkeiten ergeben. Ein zweimaliges Drücken von ⇆ bewirkt, dass eine Liste aller Dateinamen

Tastenkürzel	Funktion
Strg+A	Cursor an den Zeilenanfang (wie Pos1)
Strg+C	Programm abbrechen
Strg+E	Cursor an das Ende der Zeile (wie Ende)
Strg+K	Zeile ab Cursor löschen
Strg+Y	zuletzt gelöschten Text wieder einfügen
Strg+Z	Programm unterbrechen (Fortsetzung mit fg oder bg)
⇆	Datei- und Kommandonamen vervollständigen
↑ / ↓	durch die bisher ausgeführten Kommandos blättern

Tabelle 13.2 Tastenkürzel zur Kommandoeingabe in der bash

angezeigt wird, die mit den bereits eingegebenen Anfangsbuchstaben beginnen. Im Detail ist dieser Mechanismus in Abschnitt 14.3 beschrieben.

Maus

Die Maus spielt in Textkonsolen bzw. in Terminalfenstern nur eine untergeordnete Rolle. Sie können sie *nicht* dazu verwenden, um die aktuelle Cursorposition zu verändern! Ihre einzige Funktion beschränkt sich darauf, mit der linken Maustaste Text zu kopieren und diesen dann mit der mittleren Maustaste an der aktuellen Cursorposition wieder einzufügen. Damit die Maus in Textkonsolen funktioniert, also beim Arbeiten *ohne* grafische Benutzeroberfläche, muss das Programm `gpm` laufen.

Kommandos ausführen

Zum Ausführen von Kommandos geben Sie in der Textkonsole oder im Shell-Fenster einfach den Kommandonamen, eventuell einige Parameter und schließlich ↵ ein. Das Kommando `ls` liefert eine Liste der Dateien und Unterverzeichnisse im aktuellen Verzeichnis.

```
user$  ls -l
-rw-------  1 user users 17708403 19. Mai 10:35 20060519_DN.pdf
-rw-------  1 user users   506614 29. Jun 12:11 angebot-katzbauer.pdf
drwxrwxr-x  3 user users     4096 13. Apr 11:31 bak
drwxrwxr-x  2 user users     4096 18. Jul 15:03 bin
-rw-r--r--  1 user users   243571  3. Jul 09:14 DB20078.jpg
drwxr-xr-x  2 user users     4096  7. Apr 10:59 Desktop
...
```

Aus dem obigen Beispiel geht auch hervor, wie in diesem Buch die Kommandoeingabe und das Ergebnis dargestellt wird: `user$` am Beginn der ersten Zeile bedeutet, dass das Kommando von einem gewöhnlichen Benutzer ausgeführt wurde. Wenn in der ersten Textspalte stattdessen `root#` angegeben ist, wurde das Kommando hingegen von `root` ausgeführt (also vom Systemadministrator). `user$` bzw. `root#` gilt als

Eingabeprompt. Diese Zeichen werden am Beginn jeder Eingabezeile automatisch angezeigt. Sie dürfen diese Zeichen *nicht* mit eingeben! Generell gilt, dass nur die fett hervorgehobenen Zeichen einzugeben sind! Auf Ihrem Rechner wird statt `user$` bzw. `root#` möglicherweise ein anderer Text angezeigt, der oft das aktuelle Verzeichnis und/oder den Rechnernamen enthält. Auf diese Angaben verzichte ich in diesem Buch aus Gründen der Übersichtlichkeit.

Manchmal reicht der Platz in diesem Buch nicht aus, um ein Kommando in einer einzigen Zeile abzudrucken. In solchen Fällen wird das Kommando über mehrere Zeilen verteilt, die durch das Zeichen `\` getrennt sind. Das sieht dann beispielsweise so aus:

```
user$  gconftool-2 --set "/apps/panel/toplevels/top_panel_screen0/monitor" \
                   --type integer "0"
```

Sie können dieses Kommando nun ebenfalls zweizeilig eingeben – dann müssen Sie die erste Zeile wie im Buch mit `\` abschließen. Sie können die zwei Zeilen aber auch einfach zusammenziehen: Dann entfällt das Zeichen `\`!

Kommandos im Hintergrund ausführen

Sie können Kommandos auch im Hintergrund ausführen. Das bedeutet, dass Sie nicht auf das Programmende zu warten brauchen, sondern sofort weiterarbeiten können. Dazu geben Sie am Ende der Kommandozeile das Zeichen `&` an. Diese Vorgehensweise empfiehlt sich vor allem, wenn Sie aus einer Konsole heraus ein Programm mit grafischer Benutzeroberfläche starten (z. B. `firefox &`).

Arbeiten als root

Es ist unter Linux unüblich, als `root` (also mit Systemadministratorrechten) zu arbeiten. Auch wenn Sie als gewöhnlicher Benutzer eingeloggt sind, gibt es verschiedene Wege, Kommandos als `root` auszuführen. Bei vielen Distributionen führen Sie im Terminalfenster einfach `su -l` aus. Damit loggen Sie sich als `root` ein. (Dazu müssen Sie natürlich das `root`-Passwort kennen.) Nun können Sie als `root` textorientierte Kommandos ausführen. `exit` oder Strg+D führt wieder zum ursprünglichen User zurück. (Bei Ubuntu kommt statt `su` das Kommando `sudo` zum Einsatz.)

Tipps dazu, wie Sie die Kommandoausführung vom Vordergrund in den Hintergrund verschieben, wie Sie eine Liste aller aktiven Kommandos (Prozesse) ermitteln etc., folgen in Kapitel 16, »Prozessverwaltung«.

13.2 Textdateien anzeigen und editieren

less

Unter KDE oder Gnome können Sie Textdateien direkt im Dateimanager lesen. Mit der rechten Maustaste können Sie die Datei auch in einem komfortablen Editor öffnen. Wenn Sie hingegen in einer Textkonsole oder in einem Terminalfenster arbeiten, verwenden Sie zum Betrachten von Dateien am besten das Kommando

`less`. Sie können das Kommando auch hinter andere Kommandos stellen, um deren oft sehr lange Ausgaben in Ruhe seitenweise zu lesen:

```
user$ less datei        (seitenweise Anzeige der Datei)
user$ ls -l | less      (seitenweise Anzeige des Dateiverzeichnisses)
```

Auf manchen Mini-Linux-Systemen, z. B. in Embedded-Geräten wie NAS-Festplatten, fehlt das Kommando `less`. Möglicherweise ist stattdessen der `less`-Vorgänger `more` installiert. Andernfalls können Sie mit `cat` den gesamten Inhalt einer Textdatei ausgeben, also ohne seitenweises Blättern. Wenn Sie nur die letzten Zeilen lesen möchten, z. B. bei einer Logging-Datei, verwenden Sie `tail`.

Das Terminal zeigt nur noch merkwürdige Zeichen ...

Wenn Sie in einer Textkonsole eine Datei anzeigen, die statt Text binäre Daten enthält, kann es passieren, dass die Daten als Sonderzeichen interpretiert werden und die Konsole dabei durcheinanderkommt. In diesem Fall werden nur noch seltsame Zeichen am Bildschirm angezeigt, d. h., die Zuordnung des Zeichensatzes stimmt nicht mehr. Abhilfe schafft zumeist das Kommando `reset`.

Tastenkürzel	Funktion
Cursortasten	Text nach oben oder unten verschieben
Pos1, Ende	an den Beginn/das Ende des Textes springen
G, ⇧+G	an den Beginn/das Ende des Textes springen
/ muster ↵	vorwärts suchen
? muster ↵	rückwärts suchen
N	Suche vorwärts wiederholen (*next*)
⇧+N	Suche rückwärts wiederholen
Q	beenden (*quit*)
H	Hilfetext mit weiteren Tastenkürzeln anzeigen

Tabelle 13.3 less-Tastenkürzel

Präprozessor

Bei den meisten Distributionen kann `less` nicht nur einfache Textdateien anzeigen, sondern auch komprimierte Dateien, den Inhalt von `tar`-Archiven etc. Damit das funktioniert, analysiert ein Präprozessor die zu verarbeitenden Dateien und leitet das Ergebnis an `less` weiter. Im Detail ist die Vorgehensweise distributionsabhängig:

- Bei Fedora und Red Hat ist die Umgebungsvariable `LESSOPEN` so voreingestellt, dass `less` zuerst das Script `/usr/bin/lesspipe.sh` ausführt und dessen Ergebnis anzeigt. Bei SUSE verweist `LESSOPEN` auf das Script `/usr/bin/lessopen.sh`.

- Bei Debian und Ubuntu sind auch vergleichbare Scripts bzw. Kommandos installiert (`lessfile` und `lesspipe.sh`). Der Unterschied zwischen den beiden Varianten besteht darin, dass `lesspipe` seine Ergebnisse sofort an `less` weiterleitet, während `lessfile` eine temporäre Datei erzeugt. Das ist langsamer, hat aber den Vorteil, dass `less` sofort die Anzahl der Zeilen und die prozentuale Position im Text kennt. Bei Ubuntu ist `lesspipe` standardmäßig aktiv, bei Debian ist eine entsprechende Zeile in `.bashrc` zwar ebenfalls vorgesehen, aber auskommentiert.

Texteditoren

Unter KDE oder Gnome stehen mit `kate` oder `gedit` komfortable Texteditoren mit intuitiver Bedienung zur Verfügung. In einer Textkonsole sind diese Programme aber nicht verwendbar – Sie brauchen einen Editor, der komplett im Textmodus läuft. Dieser Abschnitt stellt die populärsten Vertreter dieser Zunft vor. Welcher der Editoren bei Ihnen standardmäßig installiert ist, hängt von Ihrer Distribution ab.

Emacs, Jove, Jed, Jmacs

Eine Sonderrolle unter den Editoren nimmt der GNU Emacs ein (Start mit `emacs`). Dieser Editor enthält unglaublich viele Funktionen und ersetzt für viele Programmierer eine ganze Entwicklungsumgebung. Daher habe ich Kapitel 20 ausschließlich diesem Editor gewidmet. Tabelle 13.4 fasst nur die elementaren Kommandos zusammen. Die Kommandos gelten auch für die Editoren `jove`, `jed` und `jmacs`. Dabei handelt es sich um Minimalversionen des Emacs, die in den Grundfunktionen kompatibel sind.

Tastenkürzel	Funktion
Strg+X, Strg+F	lädt eine neue Datei.
Strg+X, Strg+S	speichert die aktuelle Datei.
Strg+X, Strg+W	speichert die Datei unter einem neuen Namen.
Strg+G	bricht die Eingabe eines Kommandos ab.
Strg+K	löscht eine Zeile.
Strg+X, U	macht das Löschen rückgängig (Undo).
Strg+X, Strg+C	beendet den Emacs (mit Rückfrage zum Speichern).

Tabelle 13.4 Emacs-Tastenkürzel

Vi, Vim und Elvis

Ebenfalls ein Urgestein der Unix-Geschichte ist der Editor Vi, der unter Linux zumeist durch das dazu kompatible Programm Vim vertreten ist, seltener durch den ebenfalls kompatiblen Editor Elvis. Der Original-Vi ist aus urheberrechtlichen Gründen nicht Teil von Linux. Das Kommando `vi` kann aber dennoch ausgeführt werden und führt dann zum Start von Vim oder Elvis.

Der Vi bietet fast genauso viele Funktionen wie der Emacs, die Bedienung ist aber noch schwieriger zu erlernen. Dafür ist der Vi vergleichsweise kompakt und steht zumeist auch auf Notfallsystemen zur Verfügung. Außerdem werden Sie den Vi auf praktisch allen anderen Unix-Systemen vorfinden. Das Programm stellt insofern einen inoffiziellen Unix/Linux-Standard dar und wird von diversen Programmen automatisch als Editor aufgerufen.

Der wichtigste fundamentale Unterschied zu anderen Editoren besteht darin, dass der Vi zwischen verschiedenen Modi unterscheidet. Die Texteingabe ist nur im Insert-Modus möglich (siehe Tabelle 13.5). Die Eingabe der meisten Kommandos erfolgt im Complex-Command-Modus, der mit [:] aktiviert wird (siehe Tabelle 13.6). Vorher muss gegebenenfalls der Insert-Modus durch [Esc] verlassen werden. Die Cursorbewegung ist natürlich auch mit den Cursortasten möglich. Dem Vi in seiner Erscheinungsform Vim ist Kapitel 19 gewidmet.

Tastenkürzel	Funktion
[I]	wechselt in den Insert-Modus.
[Esc]	beendet den Insert-Modus.
[H] / [L]	bewegt den Cursor nach links/rechts.
[J] / [K]	bewegt den Cursor ab/auf.
[X]	löscht ein Zeichen.
[D] [D]	löscht die aktuelle Zeile.
[P]	fügt die gelöschte Zeile an der Cursorposition wieder ein.
[U]	macht die letzte Änderung rückgängig (Undo).
[:]	wechselt in den Complex-Command-Modus.

Tabelle 13.5 Vi-Tastenkürzel

Tastenkürzel	Funktion
:w *name*	speichert den Text unter einem neuen Namen.
:wq	speichert und beendet den Vi.
:q!	beendet den Vi, ohne zu speichern.
:help	startet die Online-Hilfe.

Tabelle 13.6 Vi-Kommandos im Complex-Command-Modus

Joe

`joe` ist ein sehr einfacher Editor. Die Tastenkürzel sind dem Textverarbeitungsprogramm Wordstar nachempfunden (siehe Tabelle 13.7). Eine umfassende Beschreibung aller Kommandos erhalten Sie, wenn Sie in einer Konsole `man joe` ausführen.

Das Programm kann auch unter den Namen `jmacs` oder `jpico` gestartet werden. Es gelten dann andere Tastenkürzel, die zum Emacs bzw. zu Pico kompatibel sind.

Tastenkürzel	Funktion
Strg+K, H	blendet das Hilfefenster ein/aus.
Strg+K, E	lädt eine neue Datei.
Strg+K, D	speichert die Datei (wahlweise unter neuem Namen).
Strg+Y	löscht eine Zeile.
Strg+⇧+-	macht das Löschen rückgängig (Undo).
Strg+C	beendet `joe` (mit Rückfrage zum Speichern).

Tabelle 13.7 joe-Tastenkürzel

nano, pico

Ebenfalls bescheiden im Befehlsumfang, aber dafür einfach zu bedienen, ist `nano` bzw. `pico`. Bei diesem Editor geben die beiden unteren Bildschirmzeilen eine Übersicht der zur Verfügung stehenden Kommandos (siehe Abbildung 13.2). Bei den meisten aktuellen Distributionen ist lediglich `nano` installiert. `pico` war früher stärker verbreitet; seine nicht vollständig Open-Source-kompatible Lizenz hat aber dazu geführt, dass der Editor nun unter Linux nicht mehr zum Einsatz kommt. `nano` ist zu `pico` kompatibel, leidet aber nicht unter Lizenzproblemen.

Abbildung 13.2 Der Editor nano in einem KDE-Terminalfenster

Standardeditor einstellen

Einige Programme starten zum Ansehen oder Editieren von Dateien selbstständig einen Editor, standardmäßig zumeist den Editor Vi. Wenn Sie einen anderen Editor wünschen, müssen Sie in `/etc/profile` oder `.profile` die Umgebungsvariablen `EDITOR` und `VISUAL` einstellen:

```
# Ergänzung in /etc/profile oder ~/.profile
export EDITOR=/usr/bin/jmacs
export VISUAL=$EDITOR
```

13.3 Online-Hilfe

Kommandos wie `ls`, `cp` oder `top`, die Sie üblicherweise in einem Terminalfenster ausführen, reagieren weder auf F1 noch verfügen sie über ein HILFE-Menü. Es gibt aber natürlich auch für diese Kommandos Hilfetexte, die durch verschiedene Kommandos gelesen werden können:

- `kommando -help` liefert bei sehr vielen Kommandos eine Liste aller Optionen samt einer kurzen Erklärung zu ihrer Bedeutung.
- `man kommando` zeigt bei vielen Kommandos den `man`-Hilfetext an. Durch den meist mehrseitigen Text können Sie mit den Cursortasten blättern. Q beendet die Hilfe.
- `help kommando` funktioniert nur bei sogenannten Shell-Kommandos, z. B. `cd` oder `alias`.
- `info kommando` ist eine Alternative zu `man`. Das `info`-System eignet sich vor allem für sehr umfangreiche Hilfetexte. Ob der Hilfetext im `man`- oder `info`-System vorliegt, hängt ganz einfach davon ab, für welches Hilfesystem sich die Programmentwickler entschieden haben. `man` ist aber deutlich populärer.

man

`man` ist ein Kommando zur Anzeige der Dokumentation vieler elementarer Kommandos wie `ls` oder `cp`. `man` wird in der Form `man kommando` aufgerufen, um den Hilfetext zu `kommando` zu lesen.

Die optionale Angabe eines Bereichs (`man bereich kommando`) schränkt die Suche nach `man`-Texten auf einen Themenbereich ein. Beispielsweise liefert `man 3 printf` die Syntax der C-Funktion *printf*. Diese Einschränkung ist dann notwendig, wenn mehrere gleichnamige `man`-Texte in unterschiedlichen Themenbereichen existieren. `man` zeigt in diesem Fall nur den ersten gefundenen `man`-Text an.

Wenn Sie alle gleichnamigen `man`-Texte aus allen Bereichen lesen möchten, müssen Sie `man` mit der Option `-a` verwenden. Sobald Sie den Text gelesen haben und `man` mit Q beenden, erscheint der `man`-Text zum nächsten Abschnitt.

In vielen Unix- und Linux-Büchern werden zusammen mit den Kommandos gleich die `man`-Nummern angegeben – etwa `find(1)`. Damit wissen Sie sofort, wie Sie `man` aufrufen müssen. `man` kennt üblicherweise die Themenbereiche 1 bis 9 und n (siehe Tabelle 13.8). Manchmal werden die Kommandos von Programmiersprachen in zusätzlichen Bereichen mit anderen Buchstaben eingeordnet.

Die Darstellung der Hilfetexte erfolgt intern durch das Programm `less`. Deswegen gelten für die Navigation im Hilfetext die in Tabelle 13.3 zusammengefassten Tastenkürzel. Aus welchen Verzeichnissen `man` die Hilfetexte liest, kann wahlweise durch

die Steuerungsdatei /etc/manpath.config oder durch die Umgebungsvariable MANPATH eingestellt werden.

	Thema		Thema
1	Benutzerkommandos	6	Spiele
2	Systemaufrufe	7	Diverses
3	Funktionen der Programmiersprache C	8	Kommandos zur Systemadministration
4	Dateiformate, Device-Dateien	9	Kernelfunktionen
5	Konfigurationsdateien	n	neue Kommandos

Tabelle 13.8 man-Themengruppen

Unter KDE und Gnome können Sie man-Texte auch mit den jeweiligen Help- oder Webbrowsern lesen. Die folgenden Beispiele zeigen, wie Sie die man-Seite zu ls und ein Inhaltsverzeichnis aller man-Seiten anzeigen können:

```
user$ gnome-help man:ls
user$ khelpcenter man:ls
user$ khelpcenter 'man:(index)'
```

help

Zu manchen Kommandos erhalten Sie Hilfe nicht mit man, sondern mit help. Das betrifft alle Kommandos, die direkt von der Shell ausgeführt werden. (Die Shell ist der Kommandointerpreter, der Ihre Eingaben entgegennimmt. Ausführliche Informationen zur Linux-Standard-Shell bash finden Sie im nächsten Kapitel.)

info

man-Hilfetexte haben den Nachteil, dass sie nur schwer strukturierbar sind. Das alternative info-Format bietet hier deutlich bessere Möglichkeiten, weswegen vor allem umfangreiche Hilfetexte häufig nur in diesem Format vorliegen.

info wird üblicherweise in der Form info kommando aufgerufen. Wird das Kommando ohne Parameter gestartet, zeigt das Programm eine Übersicht der verfügbaren Hilfethemen an.

Leider erweist sich der Vorteil der klareren Strukturierung rasch als Nachteil: Die Navigation in info-Texten ist unübersichtlich, außerdem fehlt ein Suchmechanismus, der über die gerade aktuelle Seite hinausreicht.

Statt info können Sie auch den Editor Emacs starten und mit Alt+X info ↵ oder mit Strg+H, I in den info-Modus wechseln. Dort werden alle Querverweise farbig hervorgehoben und können durch einen Klick mit der mittleren Maustaste bequem verfolgt werden. Eine andere komfortable Alternative zu info ist das Programm pinfo. Unter KDE bzw. Gnome lesen Sie info-Texte am besten mit dem jeweiligen Hilfesystem.

Tastenkürzel	Funktion
[Leertaste]	Text nach unten scrollen
[←]	Text nach oben scrollen
[B], [E]	zum Anfang/Ende der Info-Einheit springen (*beginning/end*)
[⇆]	Cursor zum nächsten Querverweis bewegen
[↵]	Querverweis zu anderer Info-Einheit verfolgen
[N]	nächste Info-Einheit derselben Hierarchiestufe (*next*)
[P]	vorige Info-Einheit derselben Hierarchiestufe (*previous*)
[U]	eine Hierarchieebene nach oben (*up*)
[L]	zurück zum zuletzt angezeigten Text (*last*)
[H]	ausführliche Bedienungsanleitung (*help*)
[?]	Kommandoübersicht
[Q]	beendet `info` (*quit*).

Tabelle 13.9 info-Tastenkürzel

Kapitel 14
bash (Shell)

Im Mittelpunkt dieses Kapitels steht die Bourne Again Shell (kurz bash). Dieses Programm ermöglicht die Ausführung von Kommandos in einem Terminalfenster bzw. in einer Textkonsole. Eine Shell ist also ein Kommandointerpreter, der eine Menge Zusatzfunktionen bietet, z. B. die Kombination mehrerer Kommandos oder die Speicherung der Ergebnisse eines Kommandos in einer Datei. Gleichzeitig enthält die bash eine eigene Programmiersprache, die zur Erstellung von Shell-Programmen (Shell-Scripts) verwendet werden kann.

Dieses Kapitel behandelt die Verwendung der bash sowohl als Kommandointerpreter als auch zur Programmierung. Wesentliche Themen dieses Kapitels sind eine Einführung in den Umgang mit der bash, die Ein- und Ausgabeumleitung, die Kommunikation zwischen mehreren Prozessen (Pipes, Kommandosubstitution) und die Verwaltung von Shell-Variablen. Wenn Sie sich für die bash-Programmierung interessieren, finden Sie in Abschnitt 14.8 einen Überblick über die wichtigsten Sprachelemente und diverse Beispiele. Das Kapitel endet mit einer Tabelle aller Sonderzeichen der bash.

14.1 Was ist eine Shell?

Bourne Again Shell ist ein englisches Wortspiel: Die bash ist somit die wiedergeborene Bourne-Shell, die neben der Korn-Shell und der C-Shell zu den drei klassischen Unix-Shells zählt. Unter Linux sind alle drei Shells und noch einige weitere verfügbar, standardmäßig wird aber zumeist die bash eingerichtet.

Was ist nun eine Shell? In erster Linie wird die Shell zum Aufruf von Linux-Kommandos und Programmen eingesetzt. Sie stellt damit eine Art Kommandointerpreter dar, vergleichbar in etwa mit cmd.exe aus der Windows-Welt. Eine Shell wird in jedem Terminalfenster und in jeder Textkonsole nach dem Login ausgeführt. Gleichzeitig stellt die Shell eine Programmiersprache zur Verfügung, mit der Arbeitsabläufe automatisiert werden können. Mit speziellen Shell-Kommandos können Sie innerhalb dieser Programme Variablen verwenden, Abfragen und Schleifen bilden etc. Die resultierenden Programme werden je nach den Präferenzen des Autors

als Stapeldateien, Batch-Dateien, Scripts, Shell-Prozeduren oder so ähnlich bezeichnet. In jedem Fall handelt es sich dabei um einfache Textdateien, die von der Shell ausgeführt (interpretiert) werden.

Version

Dieses Kapitel beschreibt die `bash`-Version 4.*n*, wobei die meisten Informationen auch auf Version 3.*n* zutreffen. Viele Neuerungen von Version 4 sind standardmäßig gar nicht aktiv und müssen explizit aktiviert werden, z. B. durch `shopt -s name` in `/etc/bashrc`. Wenn Sie nicht wissen, mit welcher Shell(-Version) Sie arbeiten, führen Sie die folgenden Kommandos aus:

```
user$  echo $0
-bash
user$  bash --version
GNU bash, Version 4.2.42(1)-release
```

Dokumentation

Zur `bash` existieren ein umfangreicher `man`-Text und eine ebenso umfangreiche `info`-Datei. Denselben Text können Sie auch im Webbrowser lesen:

http://www.gnu.org/software/bash/manual/bash.html

Andere Shells

Die `bash` gilt bei nahezu allen Linux-Distributionen als Standard-Shell für die Arbeit in Konsolen oder Terminal-Fenstern. Mit dem Paketverwaltungssystem Ihrer Distribution können Sie unzählige weitere Shells installieren. Bei Linux-Profis ist insbesondere die Z-Shell `zsh` beliebt. Andere Varianten sind die Korn-Shell (`ksh` oder `pdksh`) und die C-Chell (`csh` oder `tcsh`). Um eine dieser Shells nach der Installation auszuprobieren, starten Sie ein Terminalfenster und führen darin den jeweiligen Shell-Namen aus. `exit` führt zurück in die zuletzt aktive Shell.

```
user$  zsh
hostname%  ls       (Kommandos in der zsh ausführen)
...
hostname%  exit     (zurück zur vorigen Shell)
user$
```

Standard-Shell verändern

Für jeden Linux-Benutzer ist eine eigene Standard-Shell vorgesehen. Diese Shell wird ausgeführt, wenn Sie ein Terminalfenster öffnen bzw. wenn Sie sich in einer Textkonsole anmelden. Die Standard-Shell ist in der Datei `/etc/passwd` gespeichert. Die Shell wird als letzter Eintrag in der Zeile jedes Anwenders genannt. Um eine andere Standard-Shell einzustellen, führen Sie das Kommando `chsh` (*change shell*) aus. Die Shell-Programme sind im Verzeichnis `/bin` gespeichert. Sie müssen also beispielsweise `chsh /bin/csh` angeben, wenn Sie in Zukunft mit der C-Shell arbeiten möchten. Eine Liste der verwendbaren Shells befindet sich in `/etc/shells`.

Die meisten Scripts beginnen mit dem Code `#!/bin/sh`. Die Zeichenkette gibt an, dass das Script durch die Shell `/bin/sh` ausgeführt werden soll (siehe auch Abschnitt 14.8). In der Vergangenheit war `/bin/sh` fast immer ein Link auf die `bash`.

/bin/sh

```
user$  ls -l /bin/sh
... /bin/sh -> dash
```

Da die `bash` – nicht zuletzt wegen ihrer vielen Funktionen – als relativ langsam gilt und viel Speicher beansprucht, verwenden einige Distributionen statt der `bash` eine effizientere Shell zur Ausführung von Scripts. Unter Ubuntu kommt beispielsweise die Debian-Almquist-Shell (`dash`) zum Einsatz. Sie ist fast, aber nicht ganz mit der `bash` kompatibel. Wenn Sie bei der Programmierung `bash`-spezifische Funktionen verwenden, müssen Sie in der ersten Zeile explizit `#!/bin/bash` angeben.

14.2 Basiskonfiguration

Die Tastaturkonfiguration der `bash` wird global in der Datei `/etc/inputrc` bzw. individuell durch `~/.inputrc` eingestellt. Falls Sie keine deutschen Sonderzeichen eingeben können oder die Tasten Entf, Pos1 und Ende nicht wie erwartet funktionieren, müssen Sie `inputrc` wie folgt einstellen. Alle gängigen Distributionen sind standardmäßig so konfiguriert, wobei es oft noch diverse weitere Einstellungen gibt.

Funktionstasten in der bash

```
# Datei /etc/inputrc bzw. ~/.inputrc
set meta-flag on
set convert-meta off
set output-meta on
"\e[1~": beginning-of-line
"\e[3~": delete-char
"\e[4~": end-of-line
```

Diese Datei steuert die Funktion `readline`, die `bash`-intern zur Verarbeitung von Tastatureingaben verwendet wird. Durch die drei ersten Anweisungen wird erreicht, dass erstens 8-Bit-Zeichen bei der Eingabe erkannt werden, dass sie zweitens nicht in andere Zeichen konvertiert werden und dass sie drittens auch tatsächlich ausgegeben werden. Die nächsten drei Zeilen steuern die Reaktion auf das Drücken der Tasten Pos1, Entf und Ende.

Die Veränderungen werden erst nach einem Neustart der Shell wirksam. In einer Textkonsole loggen Sie sich aus und dann wieder ein. In Desktop-Systemen starten Sie ein neues Terminalfenster.

In der Shell wird am Beginn jeder Eingabezeile je nach Distribution der Name des Rechners, des Benutzers und/oder des aktuellen Verzeichnisses angezeigt. Die Zeichenkette endet üblicherweise mit `$`, `~` oder `>` (bei gewöhnlichen Benutzern) bzw. mit `#` (für `root`).

Eingabe-Prompt

Die Grundkonfiguration der Umgebungsvariablen `PS1`, die das Aussehen des Prompts steuert, erfolgt zumeist in `/etc/bash.bashrc`, bei Red Hat/Fedora in `/etc/bashrc`. Ohne Konfiguration gilt `PS1="\s-\v\$"`. In diesem Fall zeigt die `bash` den Namen der Shell und die Versionsnummer an. Um die Variable `PS1` individuell einzustellen, ändern Sie die Datei `.profile`. (Hintergründe zur Einstellung von Umgebungsvariablen werden in Abschnitt 14.7 behandelt.) Die folgende Zeile bewirkt, dass als Prompt einfach das aktuelle Verzeichnis angezeigt wird:

```
# Veränderung in ~/.profile
PS1="\w \$ "
```

Dabei ist `\u` ein Platzhalter für den Benutzernamen, `\h` für den Hostnamen, `\w` für das gesamte aktuelle Verzeichnis, `\W` für den letzten Teil des aktuellen Verzeichnisses und `\$` für den Promptabschluss (`$` oder `#`). Außerdem können Sie mit `\[\e[0;nnm\]` die Farbe einstellen. Eine umfassende Anleitung zur Prompt-Konfiguration inklusive einer Auflistung aller ANSI-Farbcodes finden Sie im folgenden HOWTO-Dokument:

http://tldp.org/HOWTO/Bash-Prompt-HOWTO

Auf meinen Rechnern verwende ich die folgende Einstellung:

```
PS1='\[\e[0;34m\]\u@\h:\W\$\[\e[0;39m\] '
```

Damit wird ein blauer Prompt in der Form `benutzername@rechnername:verzeichnis` angezeigt. Außerdem enthält der Prompt nicht den gesamten Pfad, sondern nur den letzten Teil, also z. B. `nautilus`, wenn das aktuelle Verzeichnis `/usr/lib/nautilus` lautet. Das spart Platz, wenn Sie sich in einem mehrteiligen Verzeichnis befinden.

In Ergänzung oder als Alternative zu `PS1` kann auch die Variable `PROMPT_COMMAND` eingestellt werden. Diese Variable enthält ein Kommando, das jedes Mal ausgeführt wird, bevor `PS1` angezeigt wird.

14.3 Kommandoeingabe

Normalerweise nutzen Sie die `bash` einfach durch die Eingabe ganz gewöhnlicher Kommandos. Die `bash` unterstützt Sie dabei durch eine Menge praktischer Tastenkürzel und Sondertasten. Insbesondere können Sie mit den Cursortasten ↑ und ↓ die zuletzt eingegebenen Kommandos wieder bearbeiten, was eine Menge Tipparbeit spart. Beim Ausloggen aus einer Shell werden die zuletzt eingegebenen Kommandos in einer Datei `~/.bash_history` gespeichert und stehen so auch nach dem nächsten Einloggen wieder zur Verfügung.

Kommandozeilen können wie in einem Texteditor verändert werden, das heißt, Sie können an beliebigen Stellen Zeichen einfügen und löschen. Die Tastaturbelegung der bash ist praktisch vollständig konfigurierbar. Außerdem können Sie zwischen dem emacs- und dem vi-Modus umschalten. Damit gelten für alle grundlegenden Edit-Kommandos dieselben Tastenkürzel wie im jeweils ausgewählten Editor. Die Standardeinstellung ist in der Regel der emacs-Modus. In diesem Kapitel werden alle Tastenkürzel ebenfalls für diesen Modus angegeben.

Expansion von Kommando- und Dateinamen

Mit der automatischen Expansion von Kommando- und Dateinamen hilft die bash Ihnen, den Tippaufwand zu minimieren. Dazu geben Sie zuerst die Anfangsbuchstaben des Kommandos oder des Dateinamens ein und drücken dann ↹. Wenn der Name bereits eindeutig identifizierbar ist, wird er vollständig ergänzt. Wenn es mehrere Namen gibt, die mit den gleichen Buchstaben beginnen, wird der Name nur so weit erweitert, wie die Namen übereinstimmen. Außerdem erklingt in diesem Fall ein Signalton, der darauf hinweist, dass der Dateiname möglicherweise noch nicht vollständig ist.

Am leichtesten ist die Expansion von Dateinamen anhand eines Beispiels zu verstehen. Die Eingabe

```
user$ em ↹ ba ↹
```

wird auf meinem Rechner automatisch zu

```
user$ emacs bash.tex
```

erweitert. Dabei ist emacs der Name meines Lieblingseditors und bash.tex der Dateiname der LaTeX-Datei dieses Kapitels. Zur Vervollständigung von em durchsucht bash alle in der PATH-Variablen angegebenen Verzeichnisse nach ausführbaren Programmen. Zur Vervollständigung des Dateinamens wird dagegen nur das aktuelle Verzeichnis berücksichtigt.

Die Expansion funktioniert auch bei Dateinamen, denen mehrere Verzeichnisse vorangestellt sind. Wenn Sie

```
user$ ls /usr/sh ↹
```

eingeben, erweitert bash diese Eingabe zu:

```
user$ ls /usr/share/
```

Wenn eine eindeutige Erweiterung nicht möglich ist (Signalton), können Sie einfach nochmals ↹ drücken. bash zeigt dann in den Zeilen unterhalb der aktuellen Eingabezeile alle möglichen Ergänzungen an. Die Eingabe

```
user$ e ↹ ↹
```

führt zur Ausgabe einer fast endlosen Liste aller Kommandos und Programme, die mit dem Buchstaben e beginnen. Anschließend kann die Eingabe fortgesetzt werden.

Programme bzw. Scripts im lokalen Verzeichnis starten

Programme und Kommandos im gerade aktuellen Verzeichnis werden bei der Kommandoexpansion nur dann berücksichtigt, wenn das aktuelle Verzeichnis in der PATH-Variablen enthalten ist. Den Inhalt von PATH können Sie sich mit echo $PATH ansehen. Das aktuelle Verzeichnis wird durch ».« abgekürzt.

Bei allen gängigen Linux-Distributionen fehlt aus Sicherheitsgründen das aktuelle Verzeichnis in PATH. Um Programme aus dem aktuellen Verzeichnis auszuführen, müssen Sie daher ./name eingeben.

Pfad zum Programm ermitteln

Die automatische Kommandoexpansion verschleiert, wo sich ein Programm nun wirklich befindet. Um das herauszufinden, gibt es mehrere Möglichkeiten:

- whereis name durchsucht alle Standardverzeichnisse.
- which name durchsucht alle in PATH enthaltenen Verzeichnisse und ermittelt das Programm, das bei der Eingabe des Kommandos ohne Pfad ausgeführt würde. which ist dann interessant, wenn es mehrere Versionen eines Programms gibt, die sich in unterschiedlichen Verzeichnissen befinden.
- type name funktioniert ähnlich wie which, berücksichtigt aber auch Kommandos, die in der bash integriert sind oder als Alias definiert sind (siehe Abschnitt 14.3).

Die bash bietet analoge Expansionsmechanismen auch für die Namen von Heimatverzeichnissen und für Variablennamen an: ~ko ↹ liefert auf meinem Rechner ~kofler/, $PAT ↹ ergibt $PATH.

Programmspezifische Expansion

Bei der Ausführung des Kommandos latex name.tex kommen als mögliche Dateien nur solche infrage, die mit *.tex enden. Wenn Sie man name ausführen, sind nur Einträge relevant, zu denen tatsächlich man-Texte existieren. Analog gibt es zahlreiche weitere Kommandos und Programme, bei denen die Auswahl der möglichen Dateien oder Parameter von vornherein eingeschränkt ist. Da ist es natürlich praktisch, wenn bei der Expansion nur solche Dateien bzw. Parameter berücksichtigt werden, die zum Kommando passen.

Genau darum kümmert sich das bash-Kommando complete. Viele Distributionen sind mit einer umfangreichen complete-Konfiguration ausgestattet, die aber teilweise extra installiert werden muss, unter Fedora beispielsweise mit dem Paket bash-completion. Die Konfiguration erfolgt in der Regel durch eine der folgenden Dateien:

```
/etc/bash_completion
/etc/bash_completion.d/*
/etc/profile.d/complete.bash
/etc/profile.d/bash_completion.sh
```

Zur Definition eigener Expansionsregeln müssen Sie sich in die recht unübersichtliche Syntax von complete einarbeiten. Eine knappe Beschreibung geben help complete und man bash (suchen Sie nach *Programmable Completion*). Weitere Tipps zur Konfiguration des Expansionsmechanismus finden Sie unter:

http://www.pl-berichte.de/t_system/bash-completion.html

Wichtige Tastenkürzel

Tabelle 14.1 fasst die wichtigsten Tastenkürzel der bash zusammen. Die Tabelle geht davon aus, dass bash für den emacs-Modus konfiguriert ist. Das ist bei nahezu allen Distributionen der Fall. Wenn manche Tasten auf Ihrem Rechner eine andere Reaktion hervorrufen, lesen Sie bitte die Konfigurationshinweise in Abschnitt 14.2. Unter Gnome sollten Sie im Terminalfenster Bearbeiten • Tastenkombinationen ausführen und die Option Alle Menükürzelbuchstaben aktivieren deaktivieren.

Letzten Parameter einfügen

Die Funktion des Tastenkürzels Alt+. ist nur anhand eines Beispiels zu verstehen. Nehmen wir an, Sie haben gerade eine Datei kopiert (cp name1 name2). Nun wollen Sie im nächsten Kommando die Kopie wieder löschen. Statt rm name2 geben Sie rm und dann Alt+. ein. bash fügt automatisch den zuletzt verwendeten Befehlsparameter ein. Durch das mehrfache Drücken von Alt+. können Sie auch auf alle weiteren Parameter zurückgreifen, also auf name1 durch zweimaliges Drücken.

Kommandosuche

Auch das Tastenkürzel Strg+R bedarf einer ausführlicheren Erklärung: Damit ist es möglich, bereits eingegebene Kommandos zu suchen: Drücken Sie am Beginn der Zeile Strg+R, und geben Sie dann die ersten Zeichen der gesuchten Kommandozeile ein. bash zeigt daraufhin automatisch das zuletzt verwendete Kommando mit diesen Anfangsbuchstaben an. Mehrmaliges Drücken von Strg+R wechselt zwischen verschiedenen passenden Möglichkeiten. Strg+S funktioniert wie Strg+R, durchläuft die Liste passender Kommandos aber in umgekehrter Richtung. ↵, ⇆ und die Cursortasten brechen die Suche ab und führen das gefundene Kommando aus bzw. ermöglichen das Editieren der gefundenen Zeile.

Kürzel	Bedeutung
↑, ↓	durch die zuletzt eingegebenen Kommandos scrollen
←, →	Cursor zurück- bzw. vorbewegen
Pos1, Ende	Cursor an den Beginn bzw. an das Ende der Zeile bewegen
Strg+A, Strg+E	wie oben, falls Pos1 oder Ende nicht funktioniert
Alt+B, Alt+F	Cursor um ein Wort rückwärts bzw. vorwärts bewegen
←, Entf	Zeichen rückwärts bzw. vorwärts löschen
Alt+D	Wort löschen
Strg+K	bis zum Ende der Zeile löschen
Strg+Y	zuletzt gelöschten Text wieder einfügen
Strg+T	die beiden vorangehenden Zeichen vertauschen
Alt+T	die beiden vorangehenden Wörter vertauschen
↹	Expansion des Kommando- oder Dateinamens
Strg+L	den Bildschirm löschen
Strg+R	Suche nach früher eingegebenen Kommandos
Alt+.	den zuletzt verwendeten Parameter einfügen
Strg+_	letzte Änderung rückgängig machen (Undo)

Tabelle 14.1 bash-Tastenkürzel

Manche Konsolen betrachten Strg+S als Anweisung, die Ausgabe vorübergehend zu stoppen. Erst Strg+Q setzt die Ausgabe wieder fort. Wenn Ihre Konsole so auf Strg+S reagiert, können Sie die Kommandosuche nur mit Strg+R durchführen.

Die `bash`-Tastenkürzel stammen eigentlich von der `readline`-Bibliothek, die von `bash` zur Verarbeitung von Eingaben genutzt wird. Noch mehr Kürzel finden Sie mit `man readline`.

Alias-Abkürzungen

Mit dem Kommando `alias` können Sie sich bei der Eingabe von Kommandos in der Shell einige Tipparbeit ersparen. Mit diesem Kommando werden Abkürzungen definiert. Bei der Verarbeitung der Kommandozeile wird überprüft, ob das erste Wort eine Abkürzung enthält. Wenn das der Fall ist, wird die Abkürzung durch den vollständigen Text ersetzt.

Abkürzungen für eine bestimmte Kombination von Optionen oder für Dateinamen sind nicht möglich, weil die bash die weiteren Parameter eines Kommandos nicht nach Abkürzungen durchsucht. Die bash erkennt aber Sonderfälle, bei denen in einer Kommandozeile mehrere Programme genannt werden (Pipes, Kommandosubstitution, sequenzielle Ausführung von Kommandos mit »;«), und durchsucht alle vorkommenden Kommandonamen auf Abkürzungen.

```
user$ alias cdb='cd ~kofler/linuxbuch'
```

Durch das obige Kommando wird die Abkürzung cdb definiert, mit der ich rasch in das von mir oft benötigte Verzeichnis ~kofler/linuxbuch wechseln kann.

alias-Aufrufe können auch verschachtelt eingesetzt werden. Beachten Sie, dass alias-Abkürzungen Vorrang gegenüber gleichnamigen Kommandos haben. Das kann dazu genutzt werden, um den unerwünschten Aufruf eines Kommandos zu vermeiden:

```
user$ alias more=less
```

Von nun an führt jeder Versuch, das Kommando more aufzurufen, zum Start des leistungsfähigeren Programms less. Sollten Sie aus irgendeinem Grund dennoch more benötigen, müssen Sie den gesamten Pfadnamen angeben (/bin/more) oder einen Backslash voranstellen (\more). Der Backslash verhindert in diesem Fall die Alias-Auswertung.

alias-Abkürzungen können mit unalias wieder gelöscht werden. Ansonsten gelten sie bis zum Verlassen der Shell (also spätestens bis zum Logout). Wenn Sie bestimmte Abkürzungen immer wieder benötigen, sollten Sie die alias-Anweisungen in die Dateien /etc/bashrc oder .bashrc in Ihrem Heimatverzeichnis aufnehmen.

Bei vielen Distributionen sind diverse alias-Abkürzungen vordefiniert. Wenn also beispielsweise rm ständig fragt, ob die Datei wirklich gelöscht werden soll, ist meist der vordefinierte Alias rm=rm -i schuld. Eine Liste mit allen gerade gültigen Abkürzungen liefert das Kommando alias. Die folgenden Zeilen geben an, an welchen Orten Debian, Fedora, SUSE und Ubuntu alias-Definitionen berücksichtigen.

Debian, Fedora, Ubuntu:	/etc/bashrc /etc/profile.d/*.sh ~/.bashrc
SUSE:	/etc/bash.bashrc /etc/profile.d/*.sh ~/.bashrc ~/.alias

Eine ähnliche Wirkung wie Abkürzungen können auch Shell-Programme haben. Shell-Scripts haben zudem den Vorteil, dass sie mit Parametern ($1, $2 etc.) zurechtkommen und flexibler eingesetzt werden können.

14.4 Ein- und Ausgabeumleitung

Bei der Ausführung von Kommandos in der bash existieren drei sogenannte Standarddateien. Der Begriff »Datei« stiftet dabei ein wenig Verwirrung: Es handelt sich eigentlich nicht um richtige Dateien, sondern um Dateideskriptoren, die auf Betriebssystemebene wie Dateien behandelt werden.

- **Standardeingabe:** Das gerade ausgeführte Programm, z. B. die bash oder ein beliebiges von dort gestartetes Kommando, liest alle Eingaben von der Standardeingabe. Als Standardeingabequelle gilt normalerweise die Tastatur.
- **Standardausgabe:** Dorthin werden alle Ausgaben des Programms geleitet – etwa die Auflistung aller Dateien durch ls. Als Standardausgabe gilt normalerweise das Terminalfenster.
- **Standardfehler:** Auch Fehlermeldungen werden üblicherweise im aktuellen Terminal angezeigt.

An sich ist das alles selbstverständlich – woher sonst als von der Tastatur sollten die Eingaben kommen, wo sonst als auf dem Bildschirm sollten Ergebnisse oder Fehler angezeigt werden? Bemerkenswert ist aber die Möglichkeit, die Standardeingabe oder -ausgabe umzuleiten.

Beispielsweise kann der Fall auftreten, dass das Inhaltsverzeichnis des aktuellen Verzeichnisses nicht auf dem Bildschirm angezeigt, sondern in einer Datei gespeichert werden soll. Die Standardausgabe soll also in eine echte Datei umgeleitet werden. Das erfolgt in der bash durch das Zeichen >:

```
user$  ls *.tex > inhalt
```

In der Textdatei inhalt befindet sich jetzt eine Liste aller *.tex-Dateien im aktuellen Verzeichnis. Diese Form der Ausgabeumleitung ist sicherlich die häufigste Anwendung. Daneben existieren aber viele weitere Varianten: 2> datei leitet alle Fehlermeldungen in die angegebene Datei. >& datei bzw. &> datei leiten sowohl die Standardausgabe als auch alle Fehlermeldungen in die angegebene Datei. Wenn statt > die Verdoppelung >> verwendet wird, dann werden die jeweiligen Ausgaben an das Ende einer bereits bestehenden Datei angehängt.

Eine Eingabeumleitung erfolgt mit < datei: Kommandos, die Eingaben von der Tastatur erwarten, lesen diese damit aus der angegebenen Datei.

Achtung

Es ist nicht möglich, eine Datei zu bearbeiten und gleichzeitig das Ergebnis wieder in diese Datei zu schreiben!

`sort dat > dat` oder auch `sort < dat > dat` führt dazu, dass `dat` gelöscht wird!

Kommando	Funktion
`kommando > datei`	leitet Standardausgaben zur angegebenen Datei.
`kommando < datei`	liest Eingaben aus der angegebenen Datei.
`kommando 2> datei`	leitet Fehlermeldungen zur angegebenen Datei.
`kommando >\tblcol datei`	leitet Ausgaben *und* Fehler um.
`kommando \tblcol> datei`	leitet ebenfalls Ausgaben *und* Fehler um.
`kommando >> datei`	hängt Standardausgaben an die vorhandene Datei an.
`kommando \tblcol>> datei`	hängt Ausgaben und Fehler an die Datei an (ab `bash` 4.0).
`kommando1 | kommando2`	leitet Ausgaben von Kommando 1 an Kommando 2 weiter.
`komm | tee datei`	zeigt die Ausgaben an und speichert zugleich eine Kopie.

Tabelle 14.2 Ein- und Ausgabeumleitung

Pipes

Pipes werden mit dem Zeichen | gebildet. Dabei wird die Ausgabe des ersten Kommandos als Eingabe für das zweite Kommando verwendet. In der Praxis werden Sie Pipes oft zusammen mit dem Kommando `less` bilden, wenn Sie längere Ausgaben seitenweise betrachten möchten.

```
user$ ls -l | less
```

Durch das obige Kommando wird das Inhaltsverzeichnis des aktuellen Verzeichnisses ermittelt und in eine Pipe geschrieben. Von dort liest das parallel ausgeführte Kommando `less` seine Eingaben und zeigt sie auf dem Bildschirm an.

Pipes eignen sich auch hervorragend dazu, unterschiedliche Kommandos zu kombinieren. So liefert das folgende Kommando eine sortierte Liste aller installierten RPM-Pakete:

```
user$ rpm -qa | sort
```

Statt Pipes können zur Ein- und Ausgabeumleitung auch sogenannte FIFO-Dateien verwendet werden. FIFO steht für *First In First Out* und realisiert die Idee einer Pipe in Form einer Datei. FIFOs sind bei der Eingabe viel umständlicher als Pipes, sie machen aber deutlich, was das Zeichen | eigentlich bewirkt. In der Praxis werden sie verwendet, damit zwei voneinander unabhängige Programme miteinander kommunizieren können.

```
user$  mkfifo fifo
user$  ls -l > fifo &
user$  less < fifo
```

Durch die drei obigen Kommandos wird zuerst eine FIFO-Datei eingerichtet. Anschließend wird `ls` als Hintergrundprozess gestartet. Er schreibt seine Ausgaben in die Datei. Von dort liest `less` die Daten wieder aus und zeigt sie auf dem Bildschirm an.

Zur Formulierung einer Pipe eignen sich nur solche Kommandos, die die zu verarbeitenden Kommandos aus dem Standardeingabekanal lesen. Wenn das nicht der Fall ist, können Sie ähnliche Effekte durch eine Kommandosubstitution oder durch das Kommando `xargs` erzielen (siehe Abschnitt 14.6).

Ausgabevervielfachung mit »tee«

Gelegentlich kommt es vor, dass die Ausgaben eines Programms zwar in einer Datei gespeichert werden sollen, dass Sie aber dennoch parallel am Bildschirm den Programmverlauf verfolgen wollen. In diesem Fall ist eine Verdoppelung der Ausgabe erforderlich, wobei eine Kopie auf dem Bildschirm angezeigt und die zweite Kopie in einer Datei gespeichert wird. Diese Aufgabe übernimmt das Kommando `tee`:

```
user$  ls | tee inhalt
```

Das Inhaltsverzeichnis des aktuellen Verzeichnisses wird auf dem Bildschirm angezeigt und gleichzeitig in der Datei `inhalt` gespeichert. Dabei erfolgt zuerst eine Weiterleitung der Standardausgabe an das Kommando `tee`. Dieses Kommando zeigt standardmäßig die Standardausgabe auf dem Terminal an und speichert die Kopie davon in der angegebenen Datei. Dass es sich wirklich um eine Vervielfachung der Ausgabe handelt, bemerken Sie, wenn Sie auch die Standardausgabe von `tee` in eine Datei weiterleiten:

```
user$  ls | tee inhalt1 > inhalt2
```

Das Ergebnis sind zwei identische Dateien, `inhalt1` und `inhalt2`. Das obige Kommando hat reinen Beispielcharakter. Etwas schwieriger zu verstehen, dafür aber sinnvoller, ist das folgende Beispiel:

```
user$  ls -l | tee inhalt1 | sort +4 > inhalt2
```

In `inhalt1` befindet sich wiederum das »normale« Inhaltsverzeichnis, das von `ls` automatisch nach Dateinamen sortiert wurde. Die Kopie dieser Ausgabe wurde an `sort` weitergegeben, dort nach der Dateigröße (fünfte Spalte, also Option +4) sortiert und in `inhalt2` gespeichert.

14.5 Kommandos ausführen

Üblicherweise starten Sie Kommandos einfach durch die Eingabe des Kommandonamens. Daneben gibt es aber einige Möglichkeiten, um mehrere Kommandos hintereinander auszuführen (siehe Tabelle 14.3).

Kommando	Funktion
`kommando1; kommando2`	führt die Kommandos nacheinander aus.
`kommando1 && kommando2`	führt Kommando 2 aus, wenn Kommando 1 erfolgreich war.
`kommando1 || kommando2`	führt Kommando 2 aus, wenn Kommando 1 einen Fehler liefert.
`kommando &`	startet das Kommando im Hintergrund.
`kommando1 & kommando2`	startet Kommando 1 im Hinter-, Kommando 2 im Vordergrund.
`(kommando1 ; kommando2)`	führt beide Kommandos in der gleichen Shell aus.

Tabelle 14.3 Kommandoausführung

Hintergrundprozesse

Das wichtigste und am häufigsten benötigte Sonderzeichen ist `&`. Wenn es am Ende der Kommandozeile eingegeben wird, startet `bash` dieses Programm im Hintergrund. Das ist vor allem bei zeitaufwendigen Programmen sinnvoll, weil sofort weitergearbeitet werden kann.

```
user$  find / -name '*sh' > ergebnis &
[1] 3345
```

Das obige Kommando durchsucht das gesamte Dateisystem nach Dateien, die mit den Buchstaben »sh« enden. Die Liste der Dateien wird in die Datei `ergebnis` geschrieben. Da das Kommando im Hintergrund ausgeführt wird, kann sofort weitergearbeitet werden. Die Ausgabe `[1] 3345` bedeutet, dass der Hintergrundprozess die PID-Nummer 3345 hat. PID steht dabei für »Prozessidentifikation«. Die PID-Nummer ist dann von Interesse, wenn der Prozess vorzeitig durch `kill` beendet werden soll. Die Nummer in eckigen Klammern gibt die Nummer des Hintergrundprozesses an, der in `bash` gestartet wurde, und ist im Regelfall nicht von Interesse.

Wenn Sie beim Start eines Kommandos das `&`-Zeichen vergessen, brauchen Sie weder zu warten noch müssen Sie das Programm mit Strg+C gewaltsam stoppen. Vielmehr sollten Sie das Programm mit Strg+Z unterbrechen und mit `bg` als Hintergrundprozess fortsetzen.

Ausführung mehrerer Kommandos

Nach dem &-Zeichen kann auch ein weiteres Kommando angegeben werden. In diesem Fall wird das erste Kommando im Hintergrund, das zweite dagegen im Vordergrund ausgeführt. Im folgenden Beispiel wird nochmals das obige find-Kommando im Hintergrund gestartet. Gleichzeitig wird aber mit ls das aktuelle Inhaltsverzeichnis ausgegeben:

```
user$ find / -name '*sh' > ergebnis & ls
```

Wenn statt des &-Zeichens ein Semikolon angegeben wird, führt bash die Kommandos nacheinander und im Vordergrund aus:

```
user$ ls; date
```

Das obige Kommando zeigt zuerst das aktuelle Inhaltsverzeichnis an und gibt anschließend das aktuelle Datum aus. Wenn die Gesamtheit dieser Informationen mit > in eine Datei umgeleitet werden soll, müssen beide Kommandos in runde Klammern gestellt werden. Dadurch werden beide Kommandos von ein und derselben Shell ausgeführt.

```
user$ (ls; date) > inhalt
```

In der Datei inhalt befinden sich nun die von ls erstellte Dateiliste sowie das mit date ermittelte aktuelle Datum. Die runden Klammern bewirken, dass die beiden Kommandos innerhalb derselben Shell ausgeführt werden und daher auch ein gemeinsames Ergebnis liefern. (Normalerweise wird bei der Ausführung jedes Kommandos eine neue Shell gestartet.)

Mit den Zeichenkombinationen && und || können Sie Kommandos bedingt ausführen, d. h. in Abhängigkeit vom Ergebnis eines anderen Kommandos:

```
user$ kommando1 && kommando2
```

führt Kommando 1 aus. Nur wenn dieses Kommando erfolgreich war (kein Fehler, Rückgabewert 0), wird anschließend auch Kommando 2 ausgeführt.

```
user$ kommando1 || kommando2
```

führt Kommando 1 aus. Nur wenn bei der Ausführung dieses Kommandos ein Fehler auftritt (Rückgabewert ungleich 0), wird anschließend auch Kommando 2 ausgeführt.

Weitere Möglichkeiten zur Bildung von Bedingungen und Verzweigungen bietet das Shell-Kommando if, das allerdings nur für die Shell-Programmierung von Interesse ist.

14.6 Substitutionsmechanismen

Der Begriff *Substitutionsmechanismus* klingt abstrakt und kompliziert. Die Grundidee besteht darin, dass mit Sonderzeichen gebildete Kommandos durch ihre Ergebnisse ersetzt werden. Im einfachsten Fall bedeutet das, dass bei der Auswertung des Kommandos `ls *.tex` die Zeichenkombination `*.tex` durch die Liste der passenden Dateien – etwa `buch.tex command.tex` – ersetzt wird. Das Kommando `ls` bekommt also nicht `*.tex` zu sehen, sondern eine Liste mit realen Dateinamen.

Kommando	Funktion
`?`	genau ein beliebiges Zeichen
`*`	beliebig viele (auch null) beliebige Zeichen (aber keine .*-Dateien!)
`**`	alle Dateien und Verzeichnisse, auch aus allen Unterverzeichnissen (ab `bash` 4.0 mit `shopt -s globstar`)
`[abc]`	eines der angegebenen Zeichen
`[a-f]`	ein Zeichen aus dem angegebenen Bereich
`[!abc]`	keines der angegebenen Zeichen
`[^abc]`	wie oben
`~`	Abkürzung für das Heimatverzeichnis
`.`	aktuelles Verzeichnis
`..`	übergeordnetes Verzeichnis
`ab{1,2,3}`	liefert `ab1 ab2 ab3`.
`a{1..4}`	liefert `a1 a2 a3 a4`.
`$[3*4]`	arithmetische Berechnungen
`` `kommando` ``	ersetzt das Kommando durch sein Ergebnis.
`$(kommando)`	wie oben, alternative Schreibweise
`kommando "zeichen"`	verhindert die Auswertung aller Sonderzeichen außer $.
`kommando 'zeichen'`	wie oben, aber noch restriktiver (keine Variablensubstitution)

Tabelle 14.4 Substitutionsmechanismen

Das Ziel dieses Abschnitts ist es, die wichtigsten Mechanismen bei der Interpretation der Kommandozeile vorzustellen (siehe auch die Zusammenfassung in Tabelle 14.4): Jokerzeichen dienen zur Bildung von Dateinamen, geschweifte Klammern zum Zusammensetzen von Zeichenketten, eckige Klammern zur Berechnung arithmetischer Klammern, umgekehrte Apostrophe zur Kommandosubstitution etc.

Ein Substitutionsmechanismus wird an dieser Stelle unterschlagen, nämlich die sogenannte Parametersubstitution. Damit können Sie in Variablen gespeicherte Zeichenketten analysieren und verändern. Die generelle Syntax lautet `${var__text}`, wobei `var` der Name einer Variablen ist, `__` für ein oder zwei Sonderzeichen steht und `text` das Suchmuster oder eine Defaulteinstellung enthält. Details zu diesem Substitutionsmechanismus finden Sie in Abschnitt 14.10.

Dateinamenbildung mit * und ?

Wenn Sie `rm *.bak` eingeben und das Kommando `rm` tatsächlich alle Dateien löscht, die mit `.bak` enden, dann ist dafür die `bash` verantwortlich. Die Shell durchsucht das aktuelle Verzeichnis nach passenden Dateien und ersetzt `*.bak` durch die entsprechenden Dateinamen.

Als Jokerzeichen sind `?` (genau ein beliebiges Zeichen) und `*` (beliebig viele (auch null) beliebige Zeichen) erlaubt. Die Zeichenkette `[a,b,e-h]*` steht für Dateinamen, die mit einem der Zeichen `a`, `b`, `e`, `f`, `g` oder `h` beginnen. Wenn als erstes Zeichen innerhalb der eckigen Klammern `^` oder `!` angegeben wird, dann sind alle Zeichen außer den angegebenen Zeichen zulässig. `~` kann als Abkürzung für das Heimatverzeichnis verwendet werden.

Die Funktion von Sonderzeichen können Sie einfach mit dem folgenden `echo`-Kommando testen. Das erste Kommando liefert alle Dateien und Verzeichnisse im Wurzelverzeichnis. Das zweite Kommando schränkt die Ausgabe auf Dateien und Verzeichnisse ein, die mit den Buchstaben `a-f` beginnen:

```
user$  echo /*
/bin /boot /dev /etc /home /lib /lost+found /media /misc /mnt /net /opt
/proc /root /sbin /selinux /srv /sys /tmp  /usr /var
user$  echo /[a-f]*
/bin /boot /dev /etc
```

Da die Bildung der Dateinamen nicht durch das jeweilige Programm, sondern durch die `bash` erfolgt, sehen die Resultate manchmal anders aus, als Sie es wahrscheinlich erwarten würden. So kann `ls *` zu einer schier endlosen Liste von Dateien führen, auch wenn sich im aktuellen Verzeichnis nur wenige Dateien befinden. Dem Kommando `ls` wird nach der Expansion von `*` eine Liste aller Dateien und Verzeichnisse übergeben.

`ls` wiederum zeigt bei Verzeichnissen nicht einfach deren Namen, sondern den ganzen Inhalt dieser Verzeichnisse an! Wenn Sie nur eine einfache Liste aller Dateien und Verzeichnisse haben möchten, müssen Sie die Option `-d` verwenden. Sie verhindert, dass der Inhalt der in der Parameterzeile angegebenen Verzeichnisse angezeigt wird.

Wenn Sie ein Feedback haben möchten, wie die bash intern funktioniert, können Sie set -x ausführen. Die bash zeigt dann vor der Ausführung jedes weiteren Kommandos an, wie die Kommandozeile ausgewertet wird (mit allen eventuell voreingestellten Optionen und mit den expandierten Dateinamen).

Standardmäßig berücksichtigt * keine Dateien oder Verzeichnisse, die mit einem Punkt beginnen (also »verborgen« sind). Wenn Sie diese auch erfassen möchten, müssen Sie mit shopt die bash-Option dotglob setzen:

```
user$  shopt -s dotglob
user$  echo *
...
user$  shopt -u dotglob     (dotglob wieder deaktivieren)
```

Dateinamenbildung mit **

Ab Version 4.0 erfasst die Zeichenkombination ** rekursiv alle Dateien und Verzeichnisse. Aus Kompatibilitätsgründen ist diese neue Funktion standardmäßig nicht aktiv. Wenn Sie sie nutzen möchten (z. B. in einem Script), müssen Sie mit shopt -s die bash-Option globstar setzen.

```
user$  shopt -s globstar
user$  echo **
...
```

Zeichenkettenbildung mit {}

bash setzt aus Zeichenketten, die in geschweiften Klammern angegeben werden, alle denkbaren Zeichenkettenkombinationen zusammen. Die offizielle Bezeichnung für diesen Substitutionsmechanismus lautet *Klammererweiterung* (Brace Expansion). Aus teil{1,2a,2b} wird teil1 teil2a teil2b. Klammererweiterungen können den Tippaufwand beim Zugriff auf mehrere ähnliche Dateinamen oder Verzeichnisse reduzieren. Gegenüber Jokerzeichen wie * und ? haben sie den Vorteil, dass auch noch nicht existierende Dateinamen gebildet werden können (etwa für mkdir).

```
user$  echo {a,b}{1,2,3}
a1 a2 a3 b1 b2 b3

user$  echo {ab,cd}{123,456,789}-{I,II}
ab123-I ab123-II ab456-I ab456-II ab789-I ab789-II
cd123-I cd123-II cd456-I cd456-II cd789-I cd789-II
```

Aufzählungen können Sie elegant in der Schreibweise {a..b} formulieren, wobei *a* und *b* wahlweise Zahlen oder Buchstaben sein dürfen. Die folgenden Beispiele erklären die Funktionsweise besser als jede Beschreibung:

```
user$  echo {1..5}
1 2 3 4 5

user$  echo {z..t}
z y x w v u t
```

Berechnung arithmetischer Ausdrücke mit []

bash ist normalerweise nicht in der Lage, Berechnungen auszuführen. Wenn Sie 2+3 eingeben, weiß die Shell nicht, was sie mit diesem Ausdruck anfangen soll. Wenn Sie innerhalb der Shell eine Berechnung ausführen möchten, müssen Sie den Ausdruck in eckige Klammern setzen und ein $-Zeichen voranstellen:

```
user$  echo $[2+3]
5
```

Innerhalb der eckigen Klammern sind die meisten aus der Programmiersprache C bekannten Operatoren erlaubt: + - * / für die vier Grundrechenarten, % für Modulo-Berechnungen, == != < <= > und >= für Vergleiche, << und >> für Bitverschiebungen, ! && und || für logisches NICHT, UND und ODER etc. Alle Berechnungen werden für 32-Bit-Integerzahlen ausgeführt (Zahlenbereich zwischen +/-2147483648). Wenn einzelne Werte aus Variablen entnommen werden sollen, muss ein $-Zeichen vorangestellt werden.

Eine alternative Möglichkeit, Berechnungen durchzuführen, bietet das Kommando expr. Dabei handelt es sich um ein eigenständiges Linux-Kommando, das unabhängig von bash funktioniert.

Kommando-substitution

Die Kommandosubstitution ermöglicht es, ein Kommando innerhalb der Kommandozeile durch dessen Ergebnis zu ersetzen. Dazu muss dieses Kommando zwischen zwei `-Zeichen eingeschlossen werden. Eine alternative Schreibweise lautet $(kommando). Diese Schreibweise ist vorzuziehen, weil sie erstens die Verwirrung durch die Verwendung von drei verschiedenen Anführungszeichen mindert (", ' und `) und zweitens verschachtelt werden kann.

Das so gekennzeichnete Kommando wird also durch sein Ergebnis ersetzt. Diese Substitution ermöglicht den verschachtelten Aufruf mehrerer Kommandos, wobei ein Kommando sein Ergebnis an das andere Kommando übergibt. Die beiden folgenden, gleichwertigen Kommandos verdeutlichen diesen sehr leistungsfähigen Mechanismus:

```
user$  ls -lgo `find /usr/share -name '*README*'`
user$  ls -lgo $(find /usr/share -name '*README*')
```

Durch das obige Kommando wird zuerst find /usr/share -name '*README*' ausgeführt. Das Ergebnis dieses Kommandos ist eine Liste aller Dateien im Verzeichnis /usr/share, in denen die Zeichenkette README vorkommt. Diese Liste wird nun anstelle des find-Kommandos in die Kommandozeile eingesetzt. Die Kommandozeile lautet dann beispielsweise:

```
user$  ls -lgo /usr/share/a2ps/ppd/README \
    >  /usr/share/a2ps/README ...
```

Dieses Kommando führt zum folgenden Ergebnis:

```
-rw-r--r-- 1    301 15. Feb 12:30 /usr/share/a2ps/ppd/README
-rw-r--r-- 1   1029 15. Feb 12:30 /usr/share/a2ps/README
...
```

Dieses Ergebnis wäre durch eine einfache Pipe mit dem |-Zeichen nicht möglich. `ls` erwartet keine Eingaben über die Standardeingabe und ignoriert daher auch die Informationen, die `find` über die Pipe liefert. Das folgende Kommando zeigt daher nur einfach den Inhalt des aktuellen Verzeichnisses an. Die Ergebnisse von `find` werden nicht angezeigt!

```
user$ find /usr/share -name '*README*' | ls -l   (funktioniert nicht!)
```

xargs

Es gibt aber eine andere Lösung, die ohne Kommandosubstitution auskommt: Durch die Zuhilfenahme des Kommandos `xargs` werden Daten aus der Standardeingabe an das nach `xargs` angegebene Kommando weitergeleitet:

```
user$ find /usr/share -name '*README*' | xargs ls -l
```

Ein wesentlicher Vorteil von `xargs` besteht darin, dass es kein Größenlimit für die zu verarbeitenden Daten gibt. Gegebenenfalls ruft `xargs` das Kommando mehrfach auf und übergibt die aus der Standardeingabe kommenden Daten in mehreren Schritten. Die Kommandosubstitution ist hingegen durch die maximale Größe einer Kommandozeile – üblicherweise mehrere Tausend Zeichen – begrenzt.

Die Weitergabe von Dateinamen führt zu Problemen, wenn die Dateinamen Leerzeichen enthalten. Diese Probleme können Sie umgehen, indem Sie an `find` die Option `-print0` übergeben und an `xargs` die Option `-null`. Das folgende Kommando setzt bei allen Verzeichnissen das *execute*-Bit:

```
user$ find -type d -print0 | xargs --null chmod a+x
```

Sonderzeichen in Zeichenketten

Da in der `bash` praktisch jedes Zeichen mit Ausnahme der Buchstaben und Ziffern irgendeine besondere Bedeutung hat, scheint es so gut wie unmöglich zu sein, diese Zeichen in Zeichenketten oder Dateinamen zu verwenden. Das Problem kann auf zwei Arten gelöst werden: Entweder wird dem Sonderzeichen ein Backslash \ vorangestellt, oder die gesamte Zeichenkette wird in Apostrophe oder Anführungszeichen gestellt. Durch die Angabe von Apostrophen können Sie also beispielsweise eine Datei mit dem Dateinamen `ab* $cd` löschen:

```
user$ rm 'ab* $cd'
```

Beachten Sie bitte den Unterschied zwischen ' zur Kennzeichnung von Zeichenketten und ` zur Kommandosubstitution!

Anführungszeichen haben eine ähnliche Wirkung wie Apostrophe. Sie sind allerdings weniger restriktiv und ermöglichen die Interpretation einiger Sonderzeichen wie $ \ und `. In Zeichenketten, die in Anführungszeichen gestellt sind, werden daher Shell-Variablen mit vorangestelltem $-Zeichen ausgewertet:

```
user$  echo "Das ist der Zugriffspfad: $PATH"
```

Das Kommando liefert als Ergebnis die Zeichenkette »Das ist der Zugriffspfad:«, gefolgt vom Inhalt der Shell-Variablen PATH. Wenn statt der Anführungszeichen einfache Apostrophe verwendet werden, wird die gesamte Zeichenkette unverändert durch echo ausgegeben.

14.7 Shell-Variablen

Die Funktionalität der bash und die vieler anderer Linux-Programme wird durch den Zustand sogenannter Shell-Variablen gesteuert. Shell-Variablen sind mit Variablen einer Programmiersprache vergleichbar, können allerdings nur Zeichenketten speichern. Die Zuweisung von Shell-Variablen erfolgt durch den Zuweisungsoperator =. Der Inhalt einer Shell-Variablen kann am einfachsten durch echo angezeigt werden, wobei dem Variablennamen ein $-Zeichen vorangestellt werden muss:

```
user$  var=abc
user$  echo $var
abc
```

Bei Variablenzuweisungen dürfen Sie zwischen dem Variablennamen und dem Zuweisungsoperator = kein Leerzeichen angeben. var = abc ist syntaktisch falsch und funktioniert nicht!

Wenn Shell-Variablen Leerzeichen oder andere Sonderzeichen enthalten sollen, muss bei der Zuweisung die gesamte Zeichenkette in einfache oder doppelte Hochkommata gestellt werden:

```
user$  var='abc efg'
```

Bei der Zuweisung können mehrere Zeichenketten unmittelbar aneinandergereiht werden. Im folgenden Beispiel wird der Variablen a eine neue Zeichenkette zugewiesen, die aus ihrem alten Inhalt, der Zeichenkette »xxx« und nochmals dem ursprünglichen Inhalt besteht:

```
user$  a=3
user$  a=$a'xxx'$a
user$  echo $a
3xxx3
```

Im folgenden Beispiel wird die vorhandene Variable PATH mit einer Liste aller Verzeichnisse, die nach ausführbaren Programmen durchsucht werden, um das bin-Verzeichnis im Heimatverzeichnis ergänzt. Damit können nun auch alle Kommandos ausgeführt werden, die sich in diesem Verzeichnis befinden, ohne den Pfad vollständig anzugeben.

```
user$  echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
user$  PATH=$PATH':/home/kofler/bin'
user$  echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/home/kofler/bin
```

Berechnungen mit Variablen können in der bereits vorgestellten Schreibweise mit eckigen Klammern durchgeführt werden:

```
user$  a=3
user$  a=$[$a*4]
user$  echo $a
12
```

Wenn das Ergebnis eines Kommandos in einer Variablen gespeichert werden soll, muss die ebenfalls bereits beschriebene Kommandosubstitution mit $(kommando) durchgeführt werden. Im folgenden Beispiel wird das aktuelle Verzeichnis in a gespeichert:

```
user$  a=$(pwd)
user$  echo $a
/home/kofler
```

Die Inhalte von Variablen werden nur innerhalb der Shell gespeichert. Sie gehen beim Verlassen der Shell wieder verloren. Wenn bestimmte Variablen immer wieder benötigt werden, sollten die Zuweisungen in der Datei /etc/profile bzw. in .profile im Heimatverzeichnis durchgeführt werden. Diese beiden Dateien werden (sofern vorhanden) beim Start der bash automatisch ausgeführt.

Wenn Sie den Inhalt einer Variablen in einer Datei speichern möchten, führen Sie am einfachsten echo mit einer Ausgabeumleitung durch:

```
user$  echo $var > datei
```

Lokale und globale Variablen (Umgebungsvariablen)

Die Begriffe »lokal« und »global« zur Beschreibung von Variablen sind aus der Welt der Programmiersprachen entlehnt. Bei Shell-Variablen gilt eine Variable dann als global, wenn sie beim Start eines Kommandos oder eines Shell-Programms weitergegeben wird. Globale Variablen werden oft auch als Umgebungsvariablen (*Environment Variables*) bezeichnet.

Beachten Sie bitte, dass alle durch eine einfache Zuweisung entstandenen Variablen nur als lokal gelten! Um eine globale Variable zu definieren, müssen Sie `export` oder `declare -x` aufrufen.

Zur Variablenverwaltung innerhalb der Shell existieren zahlreiche Kommandos, wobei es funktionelle Überlappungen gibt. Zur Definition einer globalen Variablen können Sie beispielsweise sowohl `export` als auch `declare -x` verwenden. Die folgenden Beispiele versuchen, die Verwirrung durch ähnliche Kommandos ein wenig zu mindern:

`a=3`	Kurzschreibweise für `let`, `a` ist lokal.
`declare a=3`	weist der lokalen Variablen `a` einen Wert zu (wie `let`).
`declare -x a=3`	weist der globalen Variablen `a` einen Wert zu (wie `export`).
`export`	zeigt alle globalen Variablen an.
`export a`	macht `a` zu einer globalen Variablen.
`export a=3`	weist der globalen Variablen `a` einen Wert zu.
`let a=3`	weist der lokalen Variablen `a` einen Wert zu.
`local a=3`	definiert `a` als lokal (nur in Shell-Funktionen).
`printenv`	zeigt wie `export` alle globalen Variablen an.
`set`	zeigt *alle* Variablen an (lokale und globale).
`unset a`	löscht die Variable `a`.

Wenn Sie Variablen einrichten, die das Verhalten von anderen Linux-Kommandos steuern sollen, müssen diese Variablen immer global sein! Damit Sie einerseits die Substitutionsmechanismen der Shell ausnutzen und andererseits globale Variablen definieren können, sollten Sie Variablen zuerst mit `x=...` zuweisen und anschließend mit `export x` als global definieren.

Variablenzuweisungen gelten immer nur für *eine* Shell. Wenn Sie in mehreren Terminals bzw. Terminalfenstern arbeiten, laufen darin jeweils eigenständige und voneinander unabhängige Shells. Die Veränderung einer Variablen in einer Shell hat keinerlei Einfluss auf die anderen Shells. Sie können aber oft benötigte Variablenzuweisungen in der Datei `.profile` festlegen, die automatisch beim Start jeder Shell ausgeführt wird.

Wichtige Shell-Variablen

Prinzipiell können Sie beliebig viele neue Variablen einführen und nach Gutdünken benennen und verwenden. Dabei sollten Sie aber versuchen, bereits vorhandene Variablen zu vermeiden, da diese zumeist von der `bash` und häufig auch von anderen Linux-Kommandos ausgewertet werden. Eine unkontrollierte Veränderung dieser Variablen kann zur Folge haben, dass die Verarbeitung von Kommandos nicht mehr

richtig funktioniert, dass Linux plötzlich Dateien nicht mehr findet etc. Dieser Abschnitt beschreibt die wichtigsten Shell-Variablen in alphabetischer Reihenfolge:

BASH
enthält den Dateinamen der `bash`.

HOME
enthält den Pfad des Heimatverzeichnisses, beispielsweise `/home/mk`.

LOGNAME
enthält den Login-Namen (User-Namen).

HOSTNAME
enthält den Hostnamen (Rechnernamen).

MAIL
enthält den Pfad des Verzeichnisses, in dem ankommende Mail gespeichert wird (nur, wenn ein lokaler Mail-Server installiert ist).

OLDPWD
enthält den Pfad des zuletzt aktiven Verzeichnisses.

PATH
enthält eine Liste von Verzeichnissen. Wenn die `bash` ein Kommando ausführen soll, durchsucht sie alle in `PATH` aufgezählten Verzeichnisse nach dem Kommando. Die Verzeichnisse sind durch Doppelpunkte voneinander getrennt.

Die Einstellung von `PATH` erfolgt distributionsspezifisch an verschiedenen Stellen während des Startprozesses (Init-V, Upstart). Der beste Ort, um eigene Änderungen durchzuführen, ist `/etc/profile` bzw. (wenn Ihre Distribution dies vorsieht) eine Datei im Verzeichnis `/etc/profile.d`. Dort fügen Sie ein Kommando nach dem folgenden Muster ein:

```
# Ergänzung in /etc/profile oder in /etc/profile.d/myown.sh
PATH=$PATH:/myown/bin
```

Aus Sicherheitsgründen (um das unbeabsichtigte Ausführen von Programmen im aktuellen Verzeichnis zu vermeiden) fehlt in `PATH` das lokale Verzeichnis. Wenn Sie Programme im gerade aktuellen Verzeichnis ohne vorangestelltes `./` ausführen möchten, müssen Sie `PATH` um `.` erweitern.

PROMPT_COMMAND
kann ein Kommando enthalten, das jedes Mal ausgeführt wird, bevor die `bash` den Kommandoprompt anzeigt.

PS1
enthält eine Zeichenkette, deren Inhalt am Beginn jeder Eingabezeile angezeigt wird (Prompt). Innerhalb dieser Zeichenkette sind unter anderem folgende Zeichenkombinationen vorgesehen: `\t` für die aktuelle Zeit, `\d` für das Datum, `\w` für das aktuelle Verzeichnis, `\W` für den letzten Teil des aktuellen Verzeichnisses (also `X11` für `/usr/bin/X11`), `\u` für den User-Namen, `\h` für den Hostnamen (Rechnernamen) sowie `\$` für das Promptzeichen (`$` für normale Anwender, `#` für `root`).

PS2
wie `PS1`, allerdings wird die Zeichenkette nur bei mehrzeiligen Eingaben angezeigt, also wenn die erste Zeile mit `\` abgeschlossen wurde. Eine typische Einstellung lautet `">"`.

PWD
enthält den Pfad des aktuellen Verzeichnisses.

Neben den hier beschriebenen Variablen sind normalerweise zahlreiche weitere Umgebungsvariablen definiert, die Funktionen der Shell sowie diverser anderer Programme steuern. Eine Liste aller definierten Variablen erhalten Sie mit `printenv | sort`.

14.8 bash-Script-Beispiele

Shell-Programme sind einfache Textdateien mit einigen Linux- und/oder `bash`-Kommandos. Nach dem Start eines Shell-Programms werden diese Kommandos der Reihe nach ausgeführt. Dem Shell-Programm können Parameter wie einem normalen Kommando übergeben werden. Diese Parameter können innerhalb des Programms ausgewertet werden.

Da die einfache sequenzielle Ausführung einiger Kommandos keinen allzu großen Spielraum für komplexe Aufgabenstellungen lässt, unterstützt die `bash` die Shell-Programmierung durch Kommandos zur Bildung von Verzweigungen und Schleifen. Damit steht Ihnen eine echte Programmiersprache zur Verfügung, für die Sie weder einen Compiler noch C-Kenntnisse benötigen. Zugegebenermaßen hinkt der Vergleich: C-Programme sind ungleich schneller in der Ausführung, unterstützen mehrere Variablentypen, kennen zahlreiche Spezialfunktionen etc. Dennoch reichen die Möglichkeiten der `bash` für überraschend viele Problemstellungen vollkommen aus.

Typische Anwendungen für Shell-Programme sind die Automatisierung von oft benötigten Kommandofolgen zur Installation von Programmen, zur Administration des Systems, zur Durchführung von Backups, zur Konfiguration und Ausführung einzelner Programme etc.

Die folgenden Seiten geben nur eine erste Einführung in die Programmierung mit der bash. Unzählige weitere Informationen und Beispiele finden Sie auf der ausgezeichneten Website *http://bash-hackers.org*.

dash

Aus Geschwindigkeitsgründen kommt bei Ubuntu für die Ausführung von Scripts standardmäßig die dash statt der bash zum Einsatz:

```
user$  ls -l /bin/sh
lrwxrwxrwx 1 root root ...  /bin/sh -> dash
```

Die dash ist zwar in vielen Fällen effizienter als die bash, ist aber nicht zu 100 Prozent kompatibel. Wenn Sie möchten, dass Ihr Script mit der bash ausgeführt wird, müssen Sie in der ersten Zeile des Scripts statt /bin/sh explizit /bin/bash angeben:

```
#!/bin/bash
```

Scripts suchen

Unter Linux wimmelt es nur so von Beispielen für die bash-Programmierung, auch wenn Sie bisher möglicherweise nichts davon bemerkt haben. Viele Kommandos, die Sie während der Installation, Konfiguration und Administration von Linux ausführen, sind in Wirklichkeit bash-Programme.

Das folgende find/grep-Kommando durchsucht das Verzeichnis /etc/ nach shell-Programmen. Dabei werden alle Dateien erkannt, die als ausführbar gekennzeichnet sind und die die Zeichenkette \#! ... sh enthalten. Die Ausführung des Kommandos nimmt einige Zeit in Anspruch, weil das gesamte Dateisystem durchsucht wird.

```
user$  find /etc -type f -perm +111 -exec grep -q '#!.*sh' {} \; -print
```

Beispiel 1: grepall

Angenommen, Sie verwenden häufig die Kommandos grep und find, um im gerade aktuellen Verzeichnis und allen Unterverzeichnissen nach Dateien zu suchen, die eine bestimmte Zeichenkette enthalten. Das richtige Kommando sieht so aus:

```
user$  find . -type f -exec grep -q suchtext {}  \; -print
```

Wenn Sie wie ich jedes Mal neu rätseln, welche Kombination der Optionen dazu erforderlich ist, liegt es nahe, das neue Kommando grepall zu definieren, das eben diese Aufgabe übernimmt. Dazu starten Sie Ihren Lieblingseditor, um die Textdatei grepall zu schreiben. Die Datei besteht aus nur zwei Zeilen, wobei die erste den Programmnamen des Interpreters angibt, der die Script-Datei ausführen soll.

```
#!/bin/sh
find . -type f -exec grep -q $1 {}  \; -print
```

Kleine Textdateien ohne Editor erstellen

Wenn Sie sich den Editoraufruf sparen möchten, können Sie die Datei auch mit `cat` erstellen: Geben Sie das Kommando `cat > grepall` ein. Das Kommando erwartet jetzt Daten aus der Standardeingabe (Tastatur) und schreibt diese in die Datei `grepall`. Geben Sie nun das Kommando mit all seinen Optionen ein. Anschließend beenden Sie `cat` mit Strg+D (das entspricht EOF, also *end of file*). Die resultierende Datei können Sie mit `cat grepall` ansehen.

Der Versuch, die gerade erstellte Datei `grepall` auszuführen, endet mit der Fehlermeldung *permission denied*. Der Grund für diese Meldung besteht darin, dass bei neuen Dateien generell die Zugriffsbits (x) zum Ausführen der Datei deaktiviert sind. Das können Sie aber rasch mit `chmod` ändern. `grepall abc` liefert jetzt die gewünschte Liste aller Dateien, die die Zeichenkette »abc« enthalten:

```
user$  ./grepall abc
bash: ./grepall: Permission denied
user$  chmod a+x grepall
user$  ./grepall abc
./bashprg.tex
```

Damit Sie das Kommando `grepall` unabhängig vom aktuellen Verzeichnis einfach durch `grepall` (ohne vorangestelltes Verzeichnis) ausführen können, müssen Sie es in ein Verzeichnis kopieren, das in `$PATH` enthalten ist. Wenn das Kommando allen Benutzern zugänglich sein soll, bietet sich `/usr/local/bin` an:

```
root#  cp grepall /usr/local/bin
```

Beispiel 2: stripcomments

Auch das zweite Beispiel ist ein Einzeiler. Sie übergeben an das Kommando `stripcomments` eine Textdatei. Die drei verschachtelten `grep`-Kommandos eliminieren nun alle Zeilen, die mit den Zeichen # oder ; beginnen bzw. ganz leer sind. Kommentare werden auch dann entfernt, wenn sich vor den Zeichen # oder ; Leer- oder Tabulatorzeichen befinden. Das Kommando eignet sich ausgezeichnet dazu, um bei Konfigurationsdateien alle Kommentarzeilen zu entfernen und nur die tatsächlich gültigen Einstellungen anzuzeigen.

```
#!/bin/sh
grep -Ev '^[[:space:]]*#|^[[:space:]]*;|^$' $1
```

Kurz zur Erklärung: Das Muster `^[[:space:]]*\#` findet Zeilen, die mit # beginnen, wobei zwischen dem Zeilenanfang (^) und # beliebig viele Leer- und Tabulatorzeichen sein dürfen. Analog erfasst der Ausdruck `^[[:space:]]*;` alle Zeilen, die mit

; beginnen. Das dritte Muster gilt für leere Zeilen, die nur aus Zeilenanfang und Zeilenende ($) bestehen.

Die Option `-v` invertiert die übliche Funktion von `grep`: Statt die gefundenen Zeilen zu extrahieren, liefert `grep` nun alle Zeilen, auf die das Muster *nicht* zutrifft. Die Option `-E` aktiviert die erweiterte `grep`-Syntax, die die Kombination mehrerer Suchausdrücke mit dem Zeichen | erlaubt.

Beispiel 3: applysedfile

Die beiden obigen Beispiele zeigen zwar gut, wie Sie sich etwas Tipp- und Denkarbeit ersparen können, deuten die weitreichenden Möglichkeiten der Script-Programmierung aber noch nicht einmal an. Schon mehr bietet in dieser Hinsicht das nächste Beispiel: Nehmen Sie an, Sie stehen vor der Aufgabe, in einem ganzen Bündel von Dateien eine Reihe gleichartiger Suchen-und-Ersetzen-Läufe durchzuführen. Das kommt immer wieder vor, wenn Sie in einem über mehrere Dateien verteilten Programmcode einen Variablen- oder Prozedurnamen verändern möchten. Ich stand bei der Überarbeitung dieses Buchs für die fünfte Auflage aufgrund der neuen Rechtschreibung vor einem ähnlichen Problem: In Dutzenden von `*.tex`-Dateien sollte »daß« durch »dass«, »muß« durch »muss« etc. ersetzt werden.

Das Script-Programm `applysedfile` hilft bei derartigen Aufgaben. Der Aufruf dieses Scripts sieht folgendermaßen aus:

```
user$  applysedfile *.tex
```

Das Programm erstellt nun von allen `*.tex`-Dateien eine Sicherheitskopie `*.bak`. Anschließend wird das Unix-Kommando `sed` verwendet, um eine ganze Liste von Kommandos für jede `*.tex`-Datei auszuführen. Diese Kommandos müssen sich in der Datei `./sedfile` befinden, die von `applysedfile` automatisch benutzt wird. Der Code von `applysedfile` sieht folgendermaßen aus:

```
#! /bin/bash
# Beispiel applysedfile
# Verwendung: applysedfile *.tex
#             wendet ./sedfile auf die Liste der übergebenen Dateien an
for i in $*
do
  echo "process $i"
  # make a backup of old file
  cp $i ${i%.*}.bak
  # build new file
  sed -f ./sedfile < ${i%.*}.bak > $i
done
```

Kurz einige Anmerkungen zur Funktion dieses kleinen Programms: Bei den vier ersten Zeilen handelt es sich um Kommentare, die mit dem Zeichen # eingeleitet werden.

for leitet eine Schleife ein. Für jeden Schleifendurchgang wird ein Dateiname in die Variable i eingesetzt. Die Liste der Dateinamen stammt aus $*. Diese Zeichenkombination ist ein Platzhalter für alle an das Programm übergebenen Parameter und Dateinamen.

Der Schleifenkörper gibt den Namen jeder Datei aus. Mit cp wird eine Sicherungskopie der Datei erstellt. (Dabei werden zuerst alle Zeichen ab dem ersten Punkt im Dateinamen gelöscht. Anschließend wird .bak angehängt.) Schließlich wird das Kommando sed für die Datei ausgeführt, wobei die Steuerungsdatei sedfile aus dem lokalen Verzeichnis verwendet wird.

Für die Umstellung auf die neue Rechtschreibung sahen die ersten Zeilen dieser Datei wie folgt aus:

```
s.daß.dass.g
s.muß.muss.g
s.paßt.passt.g
s.läßt.lässt.g
```

Dabei handelt es sich bei jeder Zeile um ein sed-Kommando, das die erste Zeichenkette durch die zweite ersetzt (Kommando s). Der nachgestellte Buchstabe g bedeutet, dass das Kommando auch mehrfach innerhalb einer Zeile ausgeführt werden soll (falls »daß« oder »muß« mehrere Male innerhalb einer Zeile auftreten sollte).

Beispiel 4: Backup-Script

Das folgende Script wird jede Nacht automatisch auf meinem root-Server ausgeführt. Als Erstes wird die Variable m initialisiert, die den aktuellen Monat als Zahl enthält. Das Kommando date liefert das aktuelle Datum samt Uhrzeit. Die Formatzeichenkette +%m extrahiert daraus den Monat.

Nun erstellt tar ein Backup des Verzeichnisses /var/www. Das Archiv wird nicht direkt in einer Datei gespeichert, sondern mittels | an das Kommando curl weitergeleitet. curl überträgt die Daten auf einen FTP-Server (Benutzername kofler, Passwort xxxx, IP-Adresse 1.2.3.4). Auf dem FTP-Server wird das Backup unter dem Namen www-*monat*.tgz gespeichert.

Auf diese Weise entstehen über den Verlauf eines Jahres monatliche Backup-Versionen, sodass ich zur Not auch einen alten Zustand meiner Website rekonstruieren kann, sollte das erforderlich sein. Gleichzeitig ist der Platzbedarf der Backup-

Dateien gering. Zu jedem Zeitpunkt gibt es maximal 12 Versionen, also `www-01.tgz` bis `www-12.tgz`.

Das Kommando `mysqldump` erstellt ein Backup der MySQL-Datenbank `cms`, in der das Content-Management-System (CMS) meiner Website alle Seiten und unzählige andere Daten speichert. Abermals wird das Backup mittels `|` an `curl` weitergegeben und auf meinem FTP-Server gespeichert.

```
#!/bin/sh
m=$(date "+%m")
cd /var
tar czf - www | curl -T - -u kofler:xxxx ftp://1.2.3.4/www-$m.tgz
mysqldump -u cms -pxxxx cms | curl -T - -u kofler:xxxx ftp://1.2.3.4/cms-$m.sql
```

Das gesamte Script habe ich unter dem Dateinamen `/etc/myscripts/backup` gespeichert. Um den täglichen Aufruf kümmert sich Cron (siehe Abschnitt 16.6). Die dazu passende Konfigurationsdatei `/etc/cron.d/backup` sieht so aus:

```
# jeden Sonntag um 3:15
15 3 * * 0 root /etc/myscripts/backup
```

Beispiel 5: Thumbnails erzeugen

Als »Thumbnails« werden verkleinerte Versionen von Bilddateien bezeichnet. Das folgende Script wird in der Form `makethumbs *.jpg` aufgerufen. Es erzeugt das Unterverzeichnis `400x400` und speichert dort verkleinerte Kopien der ursprünglichen Bilder. Die Maximalgröße der neuen Bilder beträgt 400*400 Pixel, wobei die Proportionen des Originalbilds erhalten bleiben. Bilder, die kleiner sind, bleiben unverändert und werden also nicht vergrößert.

Das Script wendet das `convert`-Kommando aus dem Paket Image Magick an. Für die Verkleinerung ist die Option `-resize` verantwortlich. `-size` bewirkt lediglich eine schnellere Verarbeitung.

```
#!/bin/sh
# Verwendung: makethumbs *.jpg
if [ ! -d 400x400 ]; then     # Unterverzeichnis erzeugen
  mkdir 400x400
fi
for filename do               # alle Dateien verarbeiten
  echo "processing $filename"
  convert -size 400x400 -resize 400x400 $filename 400x400/$filename
done
```

14.9 bash-Script-Syntax

Shell-Scripts sollten mit einer Zeile beginnen, die aus den Zeichen `#!` und dem gewünschten Shell-Namen zusammengesetzt ist. In diesem Fall wird zur Ausführung der Datei automatisch die gewünschte Shell gestartet. Für die meisten Shell-Scripts ist `#!/bin/sh` die richtige Wahl. Nur wenn Sie `bash`-spezifische Funktionen einsetzen, sollten Sie explizit `#!/bin/bash` angeben.

Shell-Scripts können nur ausgeführt werden, wenn die Zugriffsbits für den Lesezugriff (r) und die Ausführung (x) gesetzt sind (`chmod ug+rx datei`). Falls sich Scripts auf externen Datenträgern bzw. Partitionen befinden, müssen Sie sicherstellen, dass das Dateisystem mit der `exec`-Option in den Verzeichnisbaum eingebunden ist.

Vorsicht mit Sonderzeichen

In der ersten Zeile eines Scripts dürfen keine deutschen Sonderzeichen verwendet werden, auch nicht in Kommentaren. Die `bash` weigert sich sonst, die Datei auszuführen, und liefert die Meldung *cannot execute binary file*.

In Shell-Script-Dateien dürfen die Zeilen nicht durch die Windows-typische Kombination aus Carriage Return und Linefeed getrennt sein. Das kann z. B. passieren, wenn die Dateien unter Windows erstellt und dann nach Linux kopiert wurden. In diesem Fall liefert `bash` die wenig aussagekräftige Fehlermeldung *bad interpreter*. Bei Unicode-Dateien (UTF8) sorgt das folgende Kommando für die richtige Zeilentrennung:

```
recode u8/cr-lf..u8 < windowsdatei > \ linuxdatei
```

Wenn Sie eine Sammlung eigener Shell-Script-Programme für den täglichen Gebrauch schreiben, ist es sinnvoll, diese an einem zentralen Ort zu speichern. Als Verzeichnis bietet sich `~/bin` an. Wenn Sie anschließend folgende Änderung in `.profile` vornehmen, können diese Script-Programme ohne eine komplette Pfadangabe ausgeführt werden. (Bei manchen Distributionen ist das gar nicht notwendig, dort ist `~/bin` immer Bestandteil von `PATH`.)

```
# Ergänzung in ~/.profile bzw. in ~/.bashrc
PATH=$PATH':~/bin'
```

14.10 Variablen in bash-Scripts

Einleitende Informationen zum Umgang mit Variablen habe ich bereits in Abschnitt 14.7 gegeben. Dort ist unter anderem der Unterschied zwischen normalen Shell-Variablen und Umgebungsvariablen beschrieben. In diesem Abschnitt werden weitere Aspekte der Variablenverwaltung behandelt, die besonders für die Shell-Programmierung relevant sind. Im Detail geht es um den Gültigkeitsbereich von

Variablen, um einige in der bash vordefinierte Variablen (z. B. $* oder $?), um den Mechanismus der Parametersubstitution zur Analyse und Verarbeitung von Zeichenketten in Variablen und schließlich um die Eingabe von Variablen in Shell-Programmen.

Gültigkeitsbereich von Variablen

Um die Feinheiten der Variablenverwaltung bei der Ausführung von Shell-Programmen zu verstehen, sind Grundkenntnisse über die Mechanismen beim Start von Kommandos und Shell-Programmen erforderlich.

Zur Ausführung eines Kommandos oder eines Programms erzeugt die bash einen neuen Prozess mit einer eigenen PID-Nummer. Das ist eine Linux-interne Nummer zur Identifizierung und Verwaltung des Prozesses. Von den Shell-Variablen werden nur jene an den neuen Prozess weitergegeben, die als Umgebungsvariablen deklariert wurden (export oder declare -x). Wenn ein Kommando im Vordergrund gestartet wird, tritt die bash während der Ausführung in den Hintergrund und wartet auf das Ende des Kommandos. Andernfalls laufen beide Programme parallel, also die bash und das im Hintergrund gestartete Programm.

Einen Sonderfall stellt der Start eines Shell-Programms dar. Die Abarbeitung des Shell-Programms erfolgt nämlich nicht in der laufenden Shell, sondern in einer eigens dazu gestarteten Subshell. Es laufen nun also zwei Instanzen der bash – die eine als ihr Kommandointerpreter und die zweite zur Ausführung des Shell-Programms. Wenn innerhalb dieses Programms ein weiteres Shell-Programm gestartet wird, wird dazu eine dritte bash-Instanz gestartet usw. Die Ausführung eigener Subshells für Shell-Programme ist erforderlich, damit mehrere Shell-Programme parallel und ohne gegenseitige Beeinflussung gegebenenfalls auch im Hintergrund ausgeführt werden können.

Das Konzept der Subshells wirkt sich insofern auf die Variablenverwaltung aus, als jede (Sub-)Shell ihren eigenen Satz an Variablen besitzt. Der Subshell werden wie beim Start jedes beliebigen anderen Programms nur die Variablen der interaktiven Shell übergegeben, die als Umgebungsvariablen deklariert waren. Anschließend sind die Variablen in den beiden Shells vollkommen unabhängig voneinander, d. h., die Veränderung von Variablen in der einen Shell hat keinerlei Einfluss auf Variablen der anderen Shell.

Manchmal möchte man mit einem Shell-Programm neue Variablen deklarieren bzw. vorhandene Variablen bleibend verändern. Um das zu ermöglichen, können Sie Shell-Programme auch innerhalb der aktuellen bash, also ohne den automatischen Start einer Subshell ausführen. Dazu müssen Sie vor den Dateinamen

des Shell-Programms einen Punkt und ein Leerzeichen stellen. Das entspricht der Kurzschreibweise des Shell-Kommandos `source`.

Dazu ein Beispiel: Sie möchten ein Shell-Programm schreiben, das die `PATH`-Variable um den Pfad des gerade aktuellen Verzeichnisses erweitert. Das erforderliche Programm `addpwd` ist ganz einfach:

```
#! /bin/sh
# Shell-Programm addpwd ergänzt den Pfad um das aktuelle Verzeichnis
#
PATH=$PATH":"$(pwd)
```

In der Variablen `PATH` werden also der bisherige Inhalt dieser Variablen, ein Doppelpunkt und schließlich via Kommandosubstitution das Ergebnis des Kommandos `pwd` gespeichert. Der folgende Testlauf beweist, dass sich der Inhalt der `PATH`-Variablen in der aktuellen Shell erst dann ändert, wenn `addpwd` mit einem vorangestellten Punkt gestartet wird. Innerhalb der Subshell, die beim ersten Aufruf von `addpwd` gestartet wurde, wird `PATH` natürlich auch geändert – aber diese Änderung gilt nur, solange `addpwd` läuft.

```
user$  echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
user$  addpwd
user$  echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
user$  . addpwd
user$  echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/home/user
```

Durch die Shell vordefinierte Variablen

Innerhalb von Shell-Programmen kann auf einige von der `bash` vordefinierte Variablen zugegriffen werden. Diese Variablen können nicht durch Zuweisungen verändert, sondern nur gelesen werden. Der Name der Variablen wird durch verschiedene Sonderzeichen gebildet. In Tabelle 14.5 werden die Variablen gleich mit dem vorangestellten `$`-Zeichen angegeben.

Noch einige Anmerkungen zur Anwendung dieser Variablen: `$0` bis `$9`, `$#` und `$*` dienen zur Auswertung der Parameter, die dem Batch-Programm übergeben wurden. Beinahe jedes Script-Beispiel in diesem Kapitel zeigt dafür Anwendungsmöglichkeiten.

Im Zusammenhang mit der Auswertung von Parametern ist das `bash`-Kommando `shift` interessant. Dieses Kommando schiebt die übergebenen Parameter quasi durch die neun Variablen `$0` bis `$9`. Wenn Sie `shift 9` ausführen, gehen die ersten neun dem Programm übergebenen Parameter verloren, dafür können jetzt aber

die nächsten neun bequem angesprochen werden. `shift` ohne weitere Angaben verschiebt die Parameterliste um einen Parameter.

Variable	Bedeutung
`$?`	Rückgabewert des letzten Kommandos
`$!`	PID des zuletzt gestarteten Hintergrundprozesses
`$$`	PID der aktuellen Shell
`$0`	Dateiname des gerade ausgeführten Shell-Scripts (oder des symbolischen Links, der auf die Datei zeigt)
`$#`	Anzahl der dem Shell-Programm übergebenen Parameter
`$1` bis `$9`	Parameter 1 bis 9
`$*` oder `$@`	Gesamtheit aller übergebenen Parameter

Tabelle 14.5 $-Variablen

`$?` kann zur Bildung von Bedingungen verwendet werden, um den weiteren Programmverlauf vom Ergebnis des letzten Kommandos abhängig zu machen. Prinzipiell ist es auch möglich, ein Kommando direkt als Bedingung in `if` anzugeben. Die Variable `$?` hat den Vorteil, dass allzu lange und unübersichtliche Anweisungen vermieden werden können.

Die Variable `$$` enthält die PID (*Process Identification Number*). Dieser Zahlenwert wird Linux-intern zur Verwaltung der Prozesse verwendet. Die PID ist eindeutig, d. h., im ganzen System existiert mit Sicherheit kein zweiter Prozess mit derselben Nummer. Deswegen eignet sich dieser Wert hervorragend zur Bildung einer temporären Datei. Beispielsweise speichern Sie mit `ls > tmp.$$` eine Liste aller Dateien in der Datei `tmp.`*`nnn`*. Selbst wenn dieselbe Stapeldatei gleichzeitig in einem anderen Terminal läuft, wird es wegen der unterschiedlichen PIDs der beiden Shells mit Sicherheit zu keinem Namenskonflikt kommen.

Felder

Neben einfachen Variablen kennt die `bash` auch Felder. Bis einschließlich Version 3 muss der Index eine Zahl sein. Beachten Sie die von C abweichende Syntax `${feld[n]}` für den Zugriff auf das n-te Element.

```
x=()                        # Definition eines leeren Arrays
x[0]='a'                    # Array-Elemente zuweisen
x[1]='b'
x[2]='c'
x=('a' 'b' 'c')             # Kurzschreibweise für die obigen vier Zeilen
```

```
echo ${x[1]}                # ein Array-Element lesen
echo ${x[@]}                # alle Array-Elemente lesen
```

Die für Programmierer wahrscheinlich wichtigste Neuerung in bash 4.0 ist die Unterstützung assoziativer Arrays. Dazu müssen Sie die Feldvariable explizit mit declare -A als assoziativ deklarieren! Andernfalls wird die Variable als normales Feld betrachtet. Die im Index verwendeten Zeichenketten werden zu 0 ausgewertet, und Sie bekommen ein gewöhnliches Array, das aus nur einem einzigen Element besteht (Index 0).

```
declare -A y                # Definition eines leeren assoziativen Arrays
y[abc] = 123                # Element eines assoziativen Arrays zuweisen
y[efg] = xxx
y=( [abc]=123 [efg]=xxx )   # Kurzschreibweise für die obigen zwei Zeilen
echo ${y[abc]}              # ein Array-Element lesen
```

Eine weitere Neuerung in Version 4 besteht darin, dass Sie mit mapfile eine Textdatei zeilenweise in die Elemente eines gewöhnlichen Arrays einlesen können:

```
mapfile z < textdatei
```

Parametersubstitution

Die bash stellt unter dem Begriff Parametersubstitution einige Kommandos zur Verfügung, mit denen in Variablen gespeicherte Zeichenketten bearbeitet werden können. Beachten Sie, dass der Variablenname *ohne* vorangestelltes $-Zeichen angegeben wird. Wenn hingegen das Vergleichsmuster aus einer Variablen gelesen werden soll, muss dort ein $-Zeichen verwendet werden.

${var:-default}
Wenn die Variable leer ist, liefert die Konstruktion die Defaulteinstellung als Ergebnis, andernfalls den Inhalt der Variablen. Die Variable wird nicht geändert.

${var:=default}
Wie oben, es wird aber gleichzeitig der Inhalt der Variablen geändert, wenn diese bisher leer war.

${var:+neu}
Wenn die Variable leer ist, bleibt sie leer. Wenn die Variable dagegen bereits belegt ist, wird der bisherige Inhalt durch eine neue Einstellung ersetzt. Die Konstruktion liefert den neuen Inhalt der Variablen.

${var:?fehlermeldung}
Wenn die Variable leer ist, werden der Variablenname und die Fehlermeldung ausgegeben, und das Shell-Programm wird anschließend beendet. Andernfalls liefert die Konstruktion den Inhalt der Variablen.

${#var}
liefert die Anzahl der in der Variablen gespeicherten Zeichen als Ergebnis (0, falls die Variable leer ist). Die Variable wird nicht geändert.

${var#muster}
vergleicht den Anfang der Variablen mit dem angegebenen Muster. Wenn das Muster erkannt wird, liefert die Konstruktion den Inhalt der Variablen abzüglich des kürzestmöglichen Textes, der dem Suchmuster entspricht. Wird das Muster dagegen nicht gefunden, wird der ganze Inhalt der Variablen zurückgegeben. Im Suchmuster können die zur Bildung von Dateinamen bekannten Joker-Zeichen verwendet werden (`* ? [abc]`). Die Variable wird in keinem Fall verändert:

```
user$  dat=/home/mk/buch/buch.tar.gz
user$  echo ${dat#*/}
home/mk/buch/buch.tar.gz
user$  echo ${dat#*.}
tar.gz
```

${var##muster}
Wie oben, allerdings wird jetzt die größtmögliche Zeichenkette, die dem Muster entspricht, eliminiert:

```
user$  dat=/home/mk/buch/buch.tar.gz
user$  echo ${dat##*/}
buch.tar.gz
user$  echo ${dat##*.}
gz
```

${var%muster}
Wie `${var#muster}`, allerdings erfolgt der Mustervergleich jetzt am Ende des Variableninhalts. Es wird die kürzestmögliche Zeichenkette vom Ende der Variablen eliminiert. Die Variable selbst bleibt unverändert:

```
user$  dat=/home/mk/buch/buch.tar.gz
user$  echo ${dat%/*}
/home/mk/buch
user$  echo ${dat%.*}
/home/mk/buch/buch.tar
```

${var%%muster}
Wie oben, allerdings wird die größtmögliche Zeichenkette eliminiert:

```
user$  dat=/home/mk/buch/buch.tar.gz
user$  echo ${dat%%/*}
     -- keine Ausgabe --
user$  echo ${dat%%.*}
/home/mk/buch/buch
```

${var/find/replace}
ersetzt das erste Auftreten des Musters `find` durch `replace`:

```
user$  x='abcdeab12ab'
user$  echo echo ${x/ab/xy}
xycdeab12ab
```

${var//find/replace}
ersetzt jedes Auftreten des Musters `find` durch `replace`:

```
user$  x='abcdeab12ab'
user$  echo echo ${x//ab/xy}
xycdexy12xy
```

${!var}
liefert den Inhalt der Variablen, deren Name in `var` als Zeichenkette enthalten ist:

```
user$  abc="123"
user$  efg=abc
user$  echo ${!efg}
123
```

Variablen mit »read« einlesen

Mit dem `bash`-Kommando `read` können Sie Benutzereingaben verarbeiten. In der Regel geben Sie dazu zuerst mit `echo` einen kurzen Text aus, in dem Sie den Anwender darüber informieren, welche Eingabe Sie erwarten, beispielsweise y/n, einen numerischen Wert etc. Dabei ist die Option `-n` sinnvoll, damit die Eingabe unmittelbar hinter dem `echo`-Text und nicht in der nächsten Zeile erfolgt. Bei der Ausführung des anschließenden `read`-Kommandos wartet die `bash` so lange, bis der Anwender eine Zeile eingibt und diese mit ↵ abschließt.

Im folgenden Beispielprogramm wird die `while`-Schleife so lange ausgeführt, bis die Zeichenkette in der Variablen `a` nicht mehr leer ist. Ein Testlauf demonstriert die Funktion des kleinen Programms:

```
user$  readvar
Geben Sie eine Zahl ein:  a
Ungültige Eingabe, bitte Eingabe wiederholen
Geben Sie eine Zahl ein:  12
12
```

Nach der Eingabe durch `read` wird der gesamte Inhalt der Variablen via Parametersubstitution gelöscht, wenn darin irgendein Zeichen außer einer Ziffer, einem Minuszeichen oder einem Leerzeichen vorkommt. Diese Kontrolle ist zwar nicht vollkommen (die Zeichenketten `"12-34-5"` und `"12 34"` sind demnach beide gültig), aber schon recht wirkungsvoll. Informationen zu `while` finden Sie in Abschnitt 14.11.

```
#! /bin/sh
# Beispiel readvar: numerischen Wert einlesen
a=                          # a löschen
while [ -z "$a" ]; do
  echo -n "Geben Sie eine Zahl ein: "
  read a
  a=${a##*[^0-9,' ',-]*}  # Zeichenketten eliminieren, die
                          # irgendwelche Zeichen außer 0-9, dem
                          # Minuszeichen und dem Leerzeichen
                          # enthalten
  if [ -z "$a" ]; then
    echo "Ungültige Eingabe, bitte Eingabe wiederholen"
  fi
done
echo $a
```

14.11 Verzweigungen und Schleifen in bash-Scripts

Verzweigungen in Shell-Programmen können mit den Kommandos `if` und `case` gebildet werden. Während sich `if` eher für einfache Fallunterscheidungen eignet, ist `case` für die Analyse von Zeichenketten prädestiniert (Mustervergleich).

if-Verzweigungen

In der Shell-Datei `iftst` wird durch eine `if`-Abfrage getestet, ob zwei Parameter übergeben wurden. Wenn das nicht der Fall ist, wird eine Fehlermeldung ausgegeben. Das Programm wird durch `exit` mit einem Rückgabewert ungleich 0 (Indikator für Fehler) beendet. Andernfalls wird der Inhalt der beiden Parameter auf dem Bildschirm angezeigt.

```
#! /bin/sh
# Beispiel iftst
if test $# -ne 2; then
  echo "Dem Kommando müssen genau zwei Parameter übergeben werden!"
  exit 1
else
  echo "Parameter 1: $1, Parameter 2: $2"
fi
```

Ein kurzer Testlauf demonstriert das Verhalten des Programms:

```
user$  iftst a
Dem Kommando müssen genau zwei Parameter übergeben werden!
user$  iftst a b
Parameter 1: a, Parameter 2: b
```

Als Kriterium für die Verzweigung gilt der Rückgabewert des letzten Kommandos vor then. Die Bedingung ist erfüllt, wenn dieses Kommando den Rückgabewert 0 liefert. Wenn then noch in derselben Zeile angegeben wird (und nicht erst in der nächsten), dann muss das Kommando mit einem Semikolon abgeschlossen werden.

Verkehrte Logik

Beachten Sie, dass in der bash die Wahrheitswerte für wahr (0) und falsch (ungleich 0) genau umgekehrt definiert sind als in den meisten anderen Programmiersprachen! Kommandos, die ordnungsgemäß beendet werden, liefern den Rückgabewert 0. Jeder Wert ungleich 0 deutet auf einen Fehler hin. Manche Kommandos liefern je nach Fehlertyp unterschiedliche Fehlerwerte.

Im obigen Beispiel wurde die Bedingung unter Zuhilfenahme des bash-Kommandos test gebildet. Der Operator -ne steht dabei für ungleich (*not equal*). test kommt immer dann zum Einsatz, wenn zwei Zeichenketten oder Zahlen miteinander verglichen werden sollen, wenn getestet werden soll, ob eine Datei existiert etc. Das Kommando wird im nächsten Abschnitt beschrieben.

Das obige Programm könnte auch anders formuliert werden: Statt des test-Kommandos kann eine Kurzschreibweise in eckigen Klammern verwendet werden. Dabei muss nach [und vor] jeweils ein Leerzeichen angegeben werden!

Außerdem kann das zweite echo-Kommando aus der if-Struktur herausgelöst werden, weil wegen der exit-Anweisungen alle Zeilen nach fi nur dann ausgeführt werden, wenn die Bedingung erfüllt ist.

```
#! /bin/sh
# Beispiel iftst, 2. Variante
if [ $# -ne 2 ]; then
  echo "Dem Kommando müssen genau zwei Parameter übergeben werden!"
  exit 1
fi
echo "Parameter 1: $1, Parameter 2: $2"
```

Formulierung von Bedingungen mit »test«

In der bash ist es nicht möglich, Bedingungen – etwa den Vergleich einer Variablen mit einem Wert – direkt anzugeben. Zum einen basiert die ganze Konzeption der bash darauf, dass alle Aktionen über ein einheitliches Kommandokonzept durchgeführt werden, zum anderen sind Sonderzeichen wie > und < bereits für andere Zwecke vergeben. Aus diesem Grund müssen Sie zur Formulierung von Bedingungen in Schleifen und Verzweigungen das bash-Kommando test verwenden. (test existiert übrigens auch als eigenständiges Kommando außerhalb der bash. Es wur-

de aber auch in die bash integriert, um eine höhere Verarbeitungsgeschwindigkeit zu erzielen.)

test liefert als Rückgabewert 0 (wahr), wenn die Bedingung erfüllt ist, oder 1 (falsch), wenn die Bedingung nicht erfüllt ist. Um den Schreibaufwand zu verringern, ist eine Kurzschreibweise in eckigen Klammern vorgesehen.

Zahlen, Zeichenketten, Dateien

test wird in drei Aufgabenbereichen eingesetzt: zum Vergleich zweier Zahlen, zum Vergleich von Zeichenketten und zum Test, ob eine Datei existiert und bestimmte Eigenschaften aufweist. Die folgenden Beispiele zeigen einige mögliche Anwendungsfälle:

`test "$x"`
überprüft, ob x belegt ist. Das Ergebnis ist falsch, wenn die Zeichenkette 0 Zeichen aufweist, andernfalls ist es wahr.

`test $x -gt 5`
testet, ob die Variable x einen Zahlenwert größer 5 enthält. Wenn x keine Zahl enthält, kommt es zu einer Fehlermeldung. Statt -gt (greater than) können auch die folgenden Vergleichsoperatoren verwendet werden: -eq (equal), -ne (not equal), -lt (less than), -le (less equal) und -ge (greater equal).

`test -f $x`
testet, ob eine Datei mit dem in x angegebenen Namen existiert.

Wenn test interaktiv in der Shell ausgeführt werden soll, muss nach dem test-Kommando die Variable $? (Rückgabewert des letzten Kommandos) mit echo gelesen werden:

```
user$  a=20
user$  test $a -eq 20; echo $?
0
user$  test $a -gt 20; echo $?
1
```

case-Verzweigungen

case-Konstruktionen werden mit dem Schlüsselwort case eingeleitet, dem der zu analysierende Parameter zumeist in einer Variablen folgt. Nach dem Schlüsselwort in können dann mehrere mögliche Musterzeichenketten angegeben werden, mit denen der Parameter verglichen wird. Dabei sind die gleichen Jokerzeichen wie bei Dateinamen erlaubt. Das Muster wird mit einer runden Klammer) abgeschlossen, also etwa mit --*) zur Erkennung von Zeichenketten, die mit zwei Minuszeichen beginnen. Mehrere Muster können durch | voneinander getrennt werden. In diesem Fall werden beide Muster getestet. Beispielsweise dient *.c|*.h) zur Erkennung von *.c- und *.h-Dateien im selben Zweig.

Die der Klammer folgenden Kommandos müssen durch zwei Semikola abgeschlossen werden. Wenn ein `else`-Zweig benötigt wird, dann muss als letztes Muster `*` angegeben werden – alle Zeichenketten entsprechen diesem Muster. Bei der Abarbeitung einer `case`-Konstruktion wird nur der erste Zweig berücksichtigt, bei dem der Parameter dem angegebenen Muster entspricht.

Beispiel Das folgende Beispiel `casetst` zeigt die Anwendung von `case` zur Klassifizierung der übergebenen Parameter in Dateinamen und Optionen. Die Schleife für die Variable `i` wird für alle der Shell-Datei übergebenen Parameter ausgeführt. Innerhalb dieser Schleife wird jeder einzelne Parameter mit `case` analysiert. Wenn der Parameter mit einem Bindestrich beginnt, wird der Parameter an das Ende der Variablen `opt` angefügt, andernfalls an das Ende von `dat`.

```
#!/bin/bash
# Beispiel casetst
for i do    # Schleife für alle übergebenen Parameter
  case "$i" in
    -* ) opt="$opt $i";;
    *  ) dat="$dat $i";;
  esac
done        # Ende der Schleife
echo "Optionen: $opt"
echo "Dateien:  $dat"
```

Ein Beispiellauf der Shell-Datei beweist die Wirkungsweise dieser einfachen Fallunterscheidung. Die in ihrer Reihenfolge wahllos übergebenen Parameter werden in Optionen und Dateinamen untergliedert:

```
user$  casetst -x -y dat1 dat2 -z dat3
Optionen:  -x -y -z
Dateien:   dat1 dat2 dat3
```

Nach demselben Schema können `case`-Verzweigungen auch zur Klassifizierung von bestimmten Dateikennungen verwendet werden, indem im Suchmuster `*.abc` angegeben wird. Wenn Sie sich eingehender mit `case`-Analysen beschäftigen möchten, sollten Sie sich die Shell-Datei `/usr/bin/gnroff` ansehen. Die Datei bereitet die in der Syntax von `nroff` übergebenen Parameter so auf, dass das verwandte Kommando `groff` damit zurechtkommt.

for-Schleifen

Die `bash` kennt drei Kommandos zur Bildung von Schleifen: `for` führt eine Schleife für alle Elemente einer angegebenen Liste aus. `while` führt eine Schleife so lange aus, bis die angegebene Bedingung nicht mehr erfüllt ist, `until` führt sie dagegen so lange aus, bis die Bedingung zum ersten Mal erfüllt ist. Alle drei Schleifen können mit `break`

vorzeitig verlassen werden. `continue` überspringt den restlichen Schleifenkörper und setzt die Schleife mit dem nächsten Schleifendurchlauf fort.

Im ersten Beispiel werden der Variablen `i` der Reihe nach die Zeichenketten a, b und c zugewiesen. Im Schleifenkörper wird zwischen `do` und `done` der Inhalt der Variablen ausgegeben. Beachten Sie, dass sowohl am Ende der Liste als auch am Ende des `echo`-Kommandos ein Strichpunkt erforderlich ist. Auf diese Strichpunkte kann nur verzichtet werden, wenn die Eingabe auf mehrere Zeilen verteilt wird (was in Script-Dateien häufig der Fall ist).

```
user$  for i in a b c; do echo $i; done
a
b
c
```

Die äquivalente mehrzeilige Formulierung des obigen Kommandos in einer Script-Datei würde so aussehen:

```
#! /bin/sh
for i in a b c; do
  echo $i
done
```

Schleife über Dateien

Die Liste für `for` kann auch mit Jokerzeichen für Dateinamen oder mit {..}-Konstruktionen zur Bildung von Zeichenketten gebildet werden. Im folgenden Beispiel werden alle `*.tex`-Dateien in `*.tex~`-Dateien kopiert. Das Zeichen `~` am Ende eines Dateinamens bezeichnet unter Unix/Linux üblicherweise eine Backup-Datei. Beim `cp`-Kommando ist `$file` jeweils in Anführungszeichen gestellt, damit auch Dateinamen mit Leerzeichen korrekt behandelt werden.

```
user$  for file in *.tex; do cp "$file" "$file~"; done
```

Schleife über alle Zeilen einer Textdatei

Oft benötigen Sie Schleifen, um eine Textdatei Zeile für Zeile abzuarbeiten. Kein Problem: Übergeben Sie an das Schlüsselwort `in` einfach das Ergebnis von `cat datei`! Das folgende Miniprogramm erstellt für alle Datenbanken, die in der Datei `dbs.txt` zeilenweise genannt sind, ein komprimiertes Backup in der Datei `dbname.sql.gz`.

```
#!/bin/bash
# Schleife über
for db in $(cat dbs.txt); do
  mysqldump $db | gzip -c > $db.sql.gz
done
```

Schleife über alle Parameter

Wenn `for`-Schleifen ohne `in ...` gebildet werden, dann werden der Schleifenvariablen der Reihe nach alle beim Aufruf übergebenen Parameter übergeben (das entspricht also `in $*`). Ein Beispiel für so eine Schleife finden Sie bei der Beschreibung von `case`.

Wenn an das case-Beispiel Dateinamen mit Leerzeichen übergeben werden, kommt es allerdings zu Problemen: Die bash interpretiert das Leerzeichen als Trennzeichen und verarbeitet die Teile des Dateinamens getrennt. Abhilfe schafft die folgende Konstruktion:

```
#!/bin/bash
# Schleife über alle Parameter, kommt mit Leerzeichen in den Dateinamen zurecht
for i in "$@"; do
  ls -l "$i"
done
```

while-Schleifen

Im folgenden Beispiel wird der Variablen i der Wert 1 zugewiesen. Anschließend wird die Variable im Schleifenkörper zwischen do und done so oft um 1 erhöht, bis der Wert 5 überschritten wird. Beachten Sie, dass Bedingungen wie bei if-Verzweigungen mit dem Kommando test bzw. mit dessen Kurzschreibweise in eckigen Klammern angegeben werden müssen.

```
user$  i=1; while [ $i -le 5 ]; do echo $i; i=$[$i+1]; done
1
2
3
4
5
```

Die folgende Schleife verarbeitet alle Dateinamen, die sich aus dem Kommando ls *.jpg ergeben:

```
ls *.jpg | while read file
do
  echo "$file"
done
```

until-Schleifen

Der einzige Unterschied zwischen until-Schleifen und while-Schleifen besteht darin, dass die Bedingung logisch negiert formuliert wird. Das folgende Kommando ist daher zur obigen while-Schleife äquivalent. Dabei wird -gt zur Formulierung der Bedingung i>5 (*greater than*) verwendet.

```
user$  i=1; until [ $i -gt 5 ]; do echo $i; i=$[$i+1]; done
1
2
3
4
5
```

14.12 Referenz wichtiger bash-Sonderzeichen

Sowohl bei der Eingabe von Kommandos als auch bei der Shell-Programmierung können Sie eine unüberschaubare Fülle von Sonderzeichen für diverse Aktionen verwenden. Tabelle 14.6 fasst alle Sonderzeichen zusammen, die in diesem Kapitel behandelt wurden.

Zeichen	Bedeutung
;	trennt mehrere Kommandos.
:	Shell-Kommando, das nichts tut
.	Shell-Code hier einfügen (`. datei` entspricht `source datei`)
#	leitet einen Kommentar ein.
#!/bin/sh	identifiziert die gewünschte Shell für das Shell-Programm.
&	führt das Kommando im Hintergrund aus (`kom &`).
&&	bedingte Kommandoausführung (`kom1 && kom2`)
&>	Umleitung von Standardausgabe und -fehler (entspricht >&)
|	bildet Pipes (`kom1 | kom2`).
||	bedingte Kommandoausführung (`kom1 || kom2`)
*	Jokerzeichen für Dateinamen (beliebig viele Zeichen)
?	Jokerzeichen für Dateinamen (ein beliebiges Zeichen)
[abc]	Jokerzeichen für Dateinamen (ein Zeichen aus `abc`)
[ausdruck]	Kurzschreibweise für `test ausdruck`
(...)	Kommandos in derselben Shell ausführen (`(kom1; kom2)`)
{...}	Kommandos gruppieren
{ , , }	Zeichenketten zusammensetzen (`a{1,2,3}` → `a1 a2 a3`)
{a..b}	Zeichenketten zusammensetzen (`b{4..6}` → `b4 b5 b6`)
~	Abkürzung für das Heimatverzeichnis
>	Ausgabeumleitung in eine Datei (`kom > dat`)
>>	Ausgabeumleitung; an vorhandene Datei anhängen
>&	Umleitung von Standardausgabe und -fehler (entspricht &>)
2>	Umleitung der Standardfehlerausgabe

Tabelle 14.6 bash-Sonderzeichen

Zeichen	Bedeutung
<	Eingabeumleitung aus einer Datei (kom < dat)
<< ende	Eingabeumleitung aus der aktiven Datei bis zu ende
$	Kennzeichnung von Variablen (echo $var)
$!	PID des zuletzt gestarteten Hintergrundprozesses
$$	PID der aktuellen Shell
$0	Dateiname des gerade ausgeführten Shell-Scripts
$1 bis $9	die ersten neun dem Kommando übergebenen Parameter
$#	Anzahl der dem Shell-Programm übergebenen Parameter
$* oder $@	Gesamtheit aller übergebenen Parameter
$?	Rückgabewert des letzten Kommandos (0 = OK oder Fehlernummer)
$(...)	Kommandosubstitution (echo $(ls))
${...}	diverse Spezialfunktionen zur Bearbeitung von Zeichenketten
$[...]	arithmetische Auswertung (echo $[2+3])
"..."	Auswertung der meisten Sonderzeichen verhindern
'...'	Auswertung aller Sonderzeichen verhindern
`...`	Kommandosubstitution (echo `ls`)

Tabelle 14.6 bash-Sonderzeichen (Forts.)

Kapitel 15
Dateiverwaltung

Dieses Kapitel beschreibt, wie Sie mit Dateien umgehen. Im Detail werden die folgenden Themen behandelt:

- Dateien, Verzeichnisse und Links
- Dateien kopieren, verschieben, löschen und suchen
- CDs und DVDs brennen
- Zugriffsrechte von Dateien (inklusive ACLs)
- Linux-Verzeichnisstruktur
- Device-Dateien

Administration des Dateisystems

Gewissermaßen als Fortsetzung behandelt Kapitel 25 die Administration des Dateisystems. Dort geht es dann um Fragen, die weniger für Anwender und mehr für Systemadministratoren interessant sind: Welche Dateisysteme gibt es? Wie werden sie in das Dateisystem integriert (`/etc/fstab`, `mount`-Optionen)? Wie kann die Partitionierung einer Festplatte oder SSD verändert werden? Wie kann ein Software-RAID-System eingesetzt werden? Was ist LVM? Wie kann ein ganzes Dateisystem verschlüsselt werden?

Backup

Das Thema Backups behandele ich in Kapitel 39. Dort stelle ich Ihnen nicht nur Benutzeroberflächen zur Durchführung von Backups vor, sondern auch eine breite Palette von Kommandos, mit denen Sie Dateien komprimieren, in Archive bündeln, synchronisieren, verschlüsseln etc.

15.1 Umgang mit Dateien und Verzeichnissen

Ganz kurz die wichtigsten Fakten zu Dateinamen:

- Unter Linux sind Dateinamen mit einer Länge bis zu 255 Zeichen zulässig.
- Es wird zwischen Groß- und Kleinschreibung unterschieden!
- Internationale Zeichen im Dateinamen sind zulässig, können aber zu Problemen führen, wenn unterschiedliche Zeichensätze zum Einsatz kommen, z. B. in einem

Netzwerk. Alle gängigen Linux-Distributionen verwenden Unicode UTF-8 als Standardzeichensatz. Aus der Sicht des Linux-Kernels ist der Dateiname einfach eine Bytefolge, in der lediglich das Zeichen / und der Code 0 nicht vorkommen dürfen. Wie diese Bytefolge interpretiert wird, hängt vom gerade gültigen Zeichensatz ab.

- Dateinamen dürfen beliebig viele Punkte enthalten. `README.bootutils.gz` ist ein ganz normaler Dateiname, der andeutet, dass es sich um eine komprimierte README-Datei zum Thema Boot-Utilities handelt.
- Dateien, die mit einem Punkt beginnen, gelten als versteckte Dateien. Versteckte Dateien werden durch `ls` bzw. durch diverse Dateimanager normalerweise nicht angezeigt.
- Dateinamen, die bei der Eingabe von Kommandos nicht eindeutig als solche erkennbar sind, müssen in Hochkommata gestellt werden. Das gilt z. B. für Dateinamen mit Leerzeichen: `"a b"`.

Die Größe von Dateien ist bei aktuellen Linux-Distributionen nahezu unbeschränkt und liegt je nach Dateisystem zumeist im TByte-Bereich.

Verzeichnisse

Verzeichnisbaum

Der Verzeichnisbaum von Linux beginnt im Wurzelverzeichnis /. Laufwerksangaben wie `C:` sind unter Linux nicht möglich. Innerhalb dieses Buchs gelten alle weiteren Verzeichnisse als *untergeordnet*: Das Wurzelverzeichnis steht also – bildlich gesehen – ganz oben. In manchen Büchern ist die Nomenklatur gerade umgekehrt, was zwar dem Baumbild (Wurzel unten, Verästelung oben) besser entspricht, aber nicht mit dem üblichen Sprachgebrauch übereinstimmt.

Linux-Einsteiger tun sich oft schwer, Dateien im weit verästelten Verzeichnissystem zu finden. Abhilfe: Lesen Sie die Abschnitte 15.4 und 15.8! Dort lernen Sie einerseits diverse Suchwerkzeuge kennen und erfahren andererseits, wie der Verzeichnisbaum von Linux strukturiert ist.

Heimatverzeichnis

In Textkonsolen bzw. Terminalfenstern ist anfänglich automatisch das sogenannte Heimat- oder Home-Verzeichnis aktiv. Alle darin enthaltenen Dateien und Unterverzeichnisse gehören Ihnen. Andere Benutzer mit der Ausnahme von `root` dürfen diese Dateien weder verändern noch löschen, und je nach Einstellung der Zugriffsrechte nicht einmal lesen.

Das Heimatverzeichnis befindet sich im Linux-Verzeichnisbaum üblicherweise an der Stelle `/home/loginname/`. Nur bei `root` heißt das Heimatverzeichnis `/root`. Da es zu umständlich wäre, `/home/loginname` immer auszuschreiben, wird das eigene Heimat-

verzeichnis mit der Tilde ~ abgekürzt. Für den Zugriff auf die Heimatverzeichnisse anderer Benutzer ist außerdem die Schreibweise `~loginname` möglich.

Die Verzeichnisse . und ..

In jedem Verzeichnis existieren zwei besondere Unterverzeichnisse, die zur formalen Verwaltung der Verzeichnishierarchie dienen: Das Verzeichnis mit dem Namen `.` ist ein Verweis auf das aktuelle Verzeichnis, das Verzeichnis `..` ein Verweis auf das übergeordnete Verzeichnis.

Die beiden folgenden Kopierkommandos zeigen, wie Sie diese Verzeichnisse nutzen. Das erste Kommando kopiert die Datei `/etc/fstab` in das gerade aktuelle Verzeichnis. Wenn das aktuelle Verzeichnis `/home/name` lautet, dann hat die neue Datei den Namen `/home/name/fstab`.

```
user$  cp /etc/fstab .
```

Das zweite Beispiel aktiviert zuerst mit `cd` das Verzeichnis `~/linuxbuch`. Das Kopierkommando `cp` erstellt dann eine Sicherheitskopie der Datei `fileuse.tex`, die den Text dieses Kapitels enthält. Die Sicherheitskopie hat den Namen `~/fileuse.tex.bak`.

```
user$  cd ~/linuxbuch
user$  cp fileuse.tex ../fileuse.tex.bak
```

Wenn das Heimatverzeichnis `/home/name` lautet, dann haben Sie also gerade eine Kopie von `/home/name/linuxbuch/fileuse.tex` erstellt. Die Sicherheitskopie hat den vollständigen Namen `/home/name/fileuse.tex.bak`. Weitere `cp`-Beispiele folgen im nächsten Abschnitt.

Zeichen	Bedeutung
~	Heimatverzeichnis
.	aktuelles Verzeichnis
..	übergeordnetes Verzeichnis zum aktuellen Verzeichnis

Tabelle 15.1 Sonderzeichen für Verzeichnisse

Elementare Kommandos zur Bearbeitung von Dateien und Verzeichnissen

Obwohl unter KDE und Gnome moderne Dateimanager zur Verfügung stehen, verwenden erfahrene Linux-Anwender gerne textorientierte Kommandos. Tabelle 15.2 fasst nur die allerwichtigsten Kommandos zusammen.

Verzeichnis mit cd wechseln

Mit dem Kommando `cd` wechseln Sie in ein anderes Verzeichnis. `cd -` wechselt zurück in das zuletzt aktive Verzeichnis, `cd ..` wechselt in das Unterverzeichnis, `cd` ohne weitere Parameter wechselt in das Heimatverzeichnis.

```
user$  cd /etc/samba
```

Kommando	Funktion
cd	wechselt das aktuelle Verzeichnis.
cp	kopiert Dateien.
j	wechselt in ein zuletzt verwendetes Verzeichnis.
less	zeigt Textdateien seitenweise an.
ls	zeigt alle Dateien eines Verzeichnisses an.
mkdir	erzeugt ein neues Verzeichnis.
mv	verschiebt Dateien bzw. ändert ihren Namen.
rm	löscht Dateien.
rmdir	löscht Verzeichnisse.

Tabelle 15.2 Elementare Kommandos zum Umgang mit Dateien und Verzeichnissen

Verzeichnis mit j wechseln

Bei einigen Distributionen können Sie zum Verzeichniswechsel auch das Kommando `j` aus dem Paket `autojump` verwenden. In der Regel müssen Sie dieses Paket zuerst installieren. Anschließend merkt sich Autojump, in welchen Verzeichnissen Sie am häufigsten arbeiten. `jumpstats` liefert Ihnen bei Bedarf die dazugehörenden statistischen Daten.

Wenn Sie nun in ein schon früher genutztes Verzeichnis wechseln möchten, führen Sie `j abc` aus, wobei `abc` die ersten Buchstaben des Verzeichnisnamens sind. Die Eingabe des oft langen Pfads zum Verzeichnis ist nicht erforderlich! Sofern es mehrere passende Verzeichnisse gibt, wechselt `j` in das Verzeichnis, das Sie zuletzt am häufigsten verwendet haben. Zudem können Sie mit ↹ zwischen den zur Auswahl stehenden Verzeichnissen wählen.

Die Autojump-Website bezeichnet `j` als ein mitlernendes `cd`-Kommando – durchaus eine zutreffende Beschreibung. Es dauert nur kurze Zeit, sich an `j` zu gewöhnen; danach möchte man das Kommando nicht mehr missen.

https://github.com/joelthelion/autojump/wiki

`j` kann `cd` allerdings nicht ersetzen, sondern nur ergänzen: Die Vervollständigung des Pfadnamens durch ↹ funktioniert nur für Verzeichnisse, die sich bereits in der Autojump-Datenbank befinden. Wenn Sie also `cd /e` ↹ eingeben, wird `/e` in der Regel zu `/etc/` ergänzt. Die analoge Vervollständigung von `j /e` ↹ funktioniert hingegen erst, wenn sich `/etc` bereits in der Autojump-Datenbank befindet. Mit anderen Worten: Um in ein Verzeichnis zu wechseln, das Autojump nicht kennt, ist es weiterhin besser, `cd` zu verwenden. (Sie gelangen auch mit `j` in das gewünschte Verzeichnis – aber dann müssen Sie den ganzen Verzeichnisnamen eintippen.) Schade – noch eleganter wäre es, wenn `j` als vollständiger `cd`-Ersatz verwendet werden könnte!

Dateien auflisten

`ls` liefert eine Liste aller Dateien im aktuellen Verzeichnis. Wenn Sie auch verborgene Dateien sehen möchten, geben Sie zusätzlich die Option `-a` an. Wenn Sie sich nicht nur für den Dateinamen, sondern auch für die Dateigröße, den Besitzer und andere Details interessieren, hilft Ihnen die Option `-l` weiter. Standardmäßig ist die Ausgabe von `ls` alphabetisch geordnet. Um die Dateiliste nach dem Zeitpunkt der letzten Änderung, der Dateigröße bzw. der Dateikennung zu sortieren, verwenden Sie die Optionen `-t`, `-S` bzw. `-X`. `-r` dreht die Sortierordnung um. Das folgende Kommando zeigt alle `*.tex`-Dateien im Verzeichnis `linuxbuch`, geordnet nach ihrer Größe (die größte Datei zuerst).

```
user$  ls -l -S linuxbuch/*.tex
...
-rw-r--r-- 1 kofler kofler  30113 2012-05-11 09:09 linuxbuch/intro.tex
-rw-r--r-- 1 kofler kofler  63173 2012-01-29 08:05 linuxbuch/kde.tex
-rw-r--r-- 1 kofler kofler  76498 2012-06-08 15:43 linuxbuch/kernel.tex
...
```

Kurz einige Anmerkungen zur Interpretation des `ls`-Ergebnisses: Die zehn Zeichen am Beginn der Zeile geben den Dateityp und die Zugriffsbits an. Als Dateityp kommen infrage: der Bindestrich `-` für eine normale Datei, `d` für ein Verzeichnis (Directory), `b` oder `c` für eine Device-Datei (Block oder Char) oder `l` für einen symbolischen Link. Die nächsten drei Zeichen (rwx) geben an, ob der Besitzer die Datei lesen, schreiben und ausführen darf. Analoge Informationen folgen für die Mitglieder der Gruppe sowie für alle anderen Systembenutzer.

Die Zahl im Anschluss an die zehn Typ- und Zugriffszeichen gibt an, wie viele Hard-Links auf die Datei verweisen. (Was Links sind, wird in Abschnitt 15.2 beschrieben. Details zur Zugriffsverwaltung von Linux-Dateien folgen in Abschnitt 15.6.) Die weiteren Spalten geben den Besitzer und die Gruppe der Datei an (hier jeweils `kofler`), die Größe der Datei, das Datum und die Uhrzeit der letzten Änderung und zuletzt den Dateinamen.

Bei den meisten Distributionen ist `ls` so konfiguriert, dass es Dateien und Verzeichnisse je nach Typ in unterschiedlichen Farben darstellt. Sollte das bei Ihrer Distribution nicht der Fall sein, erzielen Sie diesen Effekt mit der zusätzlichen Option `--color`.

`ls` berücksichtigt normalerweise nur die Dateien des gerade aktuellen Verzeichnisses. Wenn Sie auch die Dateien aus Unterverzeichnissen einschließen möchten, verwenden Sie die Option `-R`. Diese Option steht übrigens auch bei vielen anderen Kommandos zur Verfügung. Das folgende Kommando listet sämtliche Dateien in allen Unterverzeichnissen auf. Diese Liste wird normalerweise recht lang. Daher leitet `| less` das Resultat von `ls` an `less` weiter, sodass Sie durch das Ergebnis blättern können.

```
user$  ls -lR | less
```

Dateien kopieren

`cp name1 name2` kopiert die Datei `name1`. Die Kopie hat den Namen `name2`. Um mehrere Dateien zu kopieren, rufen Sie das Kommando in der Form `cp name1 name2 ... zielverzeichnis` auf. Die folgenden Kommandos machen `linuxbuch` zum aktiven Verzeichnis, erzeugen `bak` als Unterverzeichnis und kopieren alle `*.tex`-Dateien dorthin.

```
user$  cd linuxbuch
user$  mkdir bak
user$  cp *.tex bak/
```

Verzeichnisse kopieren

Um ganze Verzeichnisse samt ihrem Inhalt zu kopieren, verwenden Sie `cp -r`. Die Option `-r` bewirkt, dass der gesamte Inhalt des Quellverzeichnisses rekursiv verarbeitet wird (inklusive versteckter Dateien). Wenn Sie möchten, dass beim Kopieren die Zugriffsrechte und -zeiten erhalten bleiben, verwenden Sie statt `-r` die Option `-a`.

Etwas diffizil ist die Frage, ob das Quellverzeichnis selbst oder nur sein Inhalt kopiert wird. Wenn es das Zielverzeichnis bereits gibt, wird darin das neue Unterverzeichnis `quellverzeichnis` erzeugt und der gesamte Inhalt des Quellverzeichnisses dorthin kopiert. Wenn es das Zielverzeichnis hingegen noch nicht gibt, wird es erzeugt; in diesem Fall wird nur der *Inhalt* des Quellverzeichnisses in das neu erzeugte Zielverzeichnis kopiert, nicht aber das Quellverzeichnis selbst. Die folgenden Beispiele verdeutlichen den Unterschied:

```
user$  mkdir test
user$  touch test/a
user$  mkdir test/b
user$  touch test/b/c
user$  mkdir ziel1
user$  cp -r test ziel1          (Das Verzeichnis ziel1/ existiert schon.)
user$  ls ziel1
test
user$  cp -r test ziel2          (Das Verzeichnis ziel2/ existiert noch nicht.)
user$  ls ziel2
a  b
```

Dateien und Verzeichnisse löschen

`rm datei` löscht die angegebene Datei unwiderruflich. `rm` kann normalerweise nur für Dateien, nicht aber für Verzeichnisse verwendet werden. Für Verzeichnisse ist das Kommando `rmdir verzeichnis` vorgesehen, das allerdings nur funktioniert, wenn das Verzeichnis leer ist. In der Praxis werden Sie zum Löschen von Verzeichnissen oft `rm` mit der Option `-rf` verwenden. Das bedeutet, dass rekursiv alle Unterverzeichnisse und Dateien ohne Rückfrage gelöscht werden. Es sollte Ihnen klar sein, dass `rm -rf` ein sehr gefährliches Kommando ist!

```
user$  rm -rf linuxbuch-bak/     (Backup-Verzeichnis löschen)
```

Platzbedarf von Dateien und Verzeichnissen ermitteln

`ls -l` verrät Ihnen zwar, wie groß eine Datei ist. Oft wollen Sie aber wissen, wie viel Platz die Dateien im gesamten Verzeichnis beanspruchen, wie viel Platz auf der Festplatte noch frei ist etc. Dabei helfen die beiden Kommandos `df` und `du`.

Freie Festplattenkapazität ermitteln

`df` zeigt für alle in das Dateisystem eingebundenen Partitionen bzw. Datenträger an, wie viel Speicher insgesamt zur Verfügung steht und wie viel davon noch frei ist.

Im folgenden Beispiel liefert `df` Ergebnisse für vier Partitionen bzw. Datenträger. Die Option `-h` bewirkt, dass sämtliche Kapazitätsangaben in lesbaren Zahlen in kByte, MByte bzw. GByte angegeben werden, nicht standardmäßig in 1-kByte-Blöcken. `df` zeigt auch diverse Dateisysteme an, die nur zur internen Verwaltung dienen und nicht zum Speichern regulärer Dateien gedacht sind.

```
user$  df -h
Dateisystem          Größe Benut  Verf Ben% Eingehängt auf
/dev/sda3              14G  4,7G  8,5G  36% /
/dev/sda2             942M   47M  849M   6% /boot
/dev/sda6              28G  7,7G   19G  30% /home
...
```

Mit `df` können Sie auch feststellen, in welcher Partition sich ein Verzeichnis physikalisch befindet. Im folgenden Beispiel befindet sich das Verzeichnis `/home/kofler` in der Partition `/dev/sda6`, die an der Stelle `/home` in den Verzeichnisbaum eingebunden ist.

```
user$  df -h /home/kofler/
/dev/sda6              28G  7,7G   19G  30% /home
```

Verzeichnisgröße ermitteln

`du` ermittelt den Platzbedarf für das aktuelle Verzeichnis sowie für alle darin enthaltenen Unterverzeichnisse. Die Option `-h` bewirkt wiederum, dass das Ergebnis in lesbarer Form (nicht in kByte-Blöcken) angezeigt wird. Es gibt keine Optionen, um die `du`-Ergebnisse zu sortieren. Unter Gnome können Sie die Größe von Verzeichnissen mit dem Programm `baobag` grafisch veranschaulichen; bei KDE ist eine vergleichbare Ansicht in den Dateimanager Konqueror integriert.

```
user$  du -h fotos/2013
74M     fotos/2013/2013-03-ostern
162M    fotos/2013/2013-08-korsika
66M     fotos/2013/2013-11-diverse
...
2,0G    fotos/2013
```

Jokerzeichen

Im täglichen Umgang mit Dateien werden Sie häufig ganze Gruppen von Dateien bearbeiten – etwa alle Dateien mit der Endung `.tex`. Um das zu ermöglichen, sind bei der Eingabe von Linux-Kommandos sogenannte Jokerzeichen vorgesehen.

Zeichen	Bedeutung
`?`	genau ein beliebiges Zeichen
`*`	beliebig viele (auch null) beliebige Zeichen
`[abc]`	genau eines der angegebenen Zeichen
`[a-f]`	ein Zeichen aus dem angegebenen Bereich
`[!abc]` oder `[^abc]`	keines der angegebenen Zeichen

Tabelle 15.3 Jokerzeichen für Dateinamen

*** und ?** `?` dient zur Spezifikation *eines* beliebigen Zeichens, und `*` dient zur Spezifikation beliebig vieler (auch null) Zeichen. Wer sich noch mit DOS auskennt, wird auf den ersten Blick keinen Unterschied erkennen. Dieser Eindruck täuscht aber:

- `*` erfasst fast alle Zeichen, also auch Punkte, sofern diese nicht am Beginn des Dateinamens stehen. Wenn Sie alle Dateien bearbeiten möchten, heißt es unter Linux `*` und nicht `*.*`! (Anmerkungen zu versteckten Dateien folgen weiter unten.)
- Auch mehrere Jokerzeichen bringen Linux nicht aus dem Gleichgewicht. Sie können beispielsweise mit `*graf*` alle Dateien suchen, die `graf` in ihrem Namen enthalten – also etwa `grafik.doc`, `apfelgraf` und `README.graf`.

[ ] und [!] Wenn Ihnen die Jokerzeichen `?` und `*` zu allgemein sind, können Sie eine stärkere Einschränkung durch die Angabe eckiger Klammern erreichen. `[abc]` steht als Platzhalter für einen der drei Buchstaben `a`, `b` oder `c`. Wenn innerhalb der eckigen Klammern ein Bindestrich zwischen zwei Buchstaben oder Ziffern angegeben wird, dann ist ein Zeichen dazwischen gemeint:

- `[a-f]*` erfasst demnach alle Dateien, die mit einem Buchstaben zwischen `a` und `f` beginnen.
- `*[_.-]*` meint alle Dateien, die irgendwo in ihrem Dateinamen zumindest einen Punkt, Unterstrich oder Bindestrich enthalten.
- Durch ein Ausrufezeichen kann der Ausdruck negiert werden: `[!a-z]*` meint alle Dateien, die mit einem Großbuchstaben oder mit einem Sonderzeichen beginnen.
- `*.[hc]` erfasst alle Dateien, die mit `.c` oder `.h` enden.

Die Jokerzeichen können auch für Verzeichnisse verwendet werden. `*/*.tex` erfasst alle `*.tex`-Dateien, die sich in Unterverzeichnissen des aktuellen Verzeichnisses befinden (nur eine Ebene darunter, also nicht auch Dateien in Unter-Unterverzeichnissen). `/usr/*bin/*` erfasst alle Dateien in den Verzeichnissen `/usr/bin` und `/usr/sbin`.

* für Verzeichnisse

Für die Auswertung der Jokerzeichen ist nicht das jeweils aufgerufene Kommando zuständig, sondern die Shell, aus der das Kommando aufgerufen wird. `bash`, die unter Linux gebräuchlichste Shell, kennt neben den gerade beschriebenen Jokerzeichen eine Menge weiterer Sonderzeichen, die bei der Ausführung eines Kommandos eine besondere Wirkung haben (siehe Abschnitt 14.6).

Das folgende Kommando kopiert alle `*.c`-Dateien aus dem Verzeichnis `project` in das aktuelle Verzeichnis:

Beispiel

```
user$  cp projekt/*.c .
```

Komplikationen bei der Verwendung von Jokerzeichen

Der Umgang mit Jokerzeichen sieht auf den ersten Blick einfacher aus, als er in Wirklichkeit ist. Wenn Sie Schwierigkeiten mit Jokerzeichen haben, sollten Sie einfach einige Experimente mit `echo jokerzeichen` durchführen. Dieses Kommando zeigt einfach alle durch eine Jokerzeichen-Kombination erfassten Dateinamen auf dem Bildschirm an, ohne die Dateinamen zu verändern.

Ein Problem besteht darin, dass `*` nicht nur Dateien, sondern auch Verzeichnisse erfasst. `ls *` zeigt aus diesem Grund nicht nur alle Dateien im aktuellen Verzeichnis an, sondern auch den Inhalt aller Unterverzeichnisse, die über `*` erfasst werden. Beim Kommando `ls` kann dieses Problem durch die Option `-d` umgangen werden; bei anderen Kommandos steht diese Option aber nicht zur Verfügung.

Wenn Sie alle Verzeichnisse, nicht aber normale Dateien bearbeiten möchten, hilft die Jokerzeichenkombination `*/.` weiter: Mit ihr werden alle »Dateien« erfasst, die als Unterverzeichnis einen Verweis auf sich selbst enthalten, und das ist eben nur bei Verzeichnissen der Fall. (Verzeichnisse gelten intern als eine Sonderform einer Datei – daher die Anführungszeichen.)

Verzeichnisse mit */. bearbeiten

```
user$  echo */.
```

Die Tatsache, dass nicht das jeweilige Programm, sondern schon die Shell für die Verarbeitung der Jokerzeichen zuständig ist, hat nicht nur Vorteile. So ist es etwa unmöglich, mit `ls -R *.tex` nach `*.tex`-Dateien auch in Unterverzeichnissen zu suchen. Die Option `-R` für das Kommando `ls` bewirkt eigentlich ein rekursives Durchsuchen von Unterverzeichnissen.

Probleme mit *.endung

Der Grund dafür ist einfach: Die Shell erweitert das Muster `*.tex` für das *aktuelle* Verzeichnis und übergibt die Liste der gefundenen Dateien an `ls`. Das Kommando zeigt Informationen zu diesen Dateien an. Wenn Sie keine Verzeichnisse mit der Endung `.tex` haben, ist `ls` damit am Ende – auch die Option `-R` kann daran nichts mehr ändern. Rekursiv durchsucht werden nämlich nur die Verzeichnisse, die als Parameter übergeben werden.

Zum Suchen nach Dateien stellt Linux deshalb das sehr viel flexiblere Kommando `find` zur Verfügung. Im Beispiel unten wird eine Liste aller `*.tex`-Dateien im aktuellen und in allen untergeordneten Verzeichnissen angezeigt. Grundlagen und weitere Beispiele zu `find` folgen auf in Abschnitt 15.4.

```
user$  find . -name '*.tex'
```

Dateien umbenennen

Leider ist es in Linux nicht möglich, mit dem Kommando `mv *.x *.y` alle `*.x`-Dateien in `*.y`-Dateien umzubenennen. Der Grund für diese Einschränkung ist wieder derselbe wie oben beschrieben: Die Shell ersetzt `*.x` durch die Liste aller Dateien, die diesem Muster entsprechen. Für `*.y` gibt es keine gültigen Dateinamen. An das Kommando `mv` werden daher eine Liste mehrerer Dateien und der Ausdruck `*.y` übergeben – und `mv` weiß dann nicht, was es mit diesen Argumenten tun soll.

Dazu ein konkretes Beispiel: Angenommen, im aktuellen Verzeichnis befinden sich nur die Dateien `markus.x`, `peter.x` und `ulrike.x`. Wenn Sie `mv *.x *.y` ausführen, ersetzt die Shell das Muster `*.x` durch die drei genannten Dateien. Die Shell findet keine passenden Dateien für `*.y` und übergibt das Muster so, wie es ist. Erst jetzt wird das Kommando `mv` gestartet. Es bekommt folgende Parameter, mit denen es erwartungsgemäß nichts anfangen kann:

```
user$  mv markus.x peter.x ulrike.x *.y
```

Selbst wenn an `mv` als Parameterliste `markus.x peter.x ulrike.x markus.y peter.y ulrike.y` übergeben würde, wäre die Wirkung nicht die erwünschte. `mv` ist prinzipiell nicht in der Lage, mehrere Dateien umzubenennen. Entweder werden *mehrere* Dateien in ein anderes Verzeichnis verschoben, oder es wird nur *eine* Datei umbenannt.

Umbenennen mit sed und for

Unix-Experten haben natürlich auch für dieses Problem eine Lösung gefunden: Sie verwenden den Streameditor `sed`. Wegen der eher komplizierten Bedienung von `sed` eignen sich Beispiele wie das folgende eigentlich nur zur Shell-Programmierung.

Kurz zur Funktionsweise: `ls` liefert die Liste der Dateien, die umbenannt werden sollen, und gibt sie an `sed` weiter. `sed` bildet daraus mit dem Kommando `s` (reguläres Suchen und Ersetzen) eine Liste von `cp`-Kommandos und gibt diese wiederum an eine neue Shell `sh` weiter, die die Kommandos schließlich ausführt. Durch die Zeile unten werden alle `*.xxx`-Dateien in `*.yyy`-Dateien kopiert.

```
user$  ls *.xxx | sed 's/\(.*\)\.xxx$/cp & \1.yyy/' | sh
```

Eine andere Lösung besteht darin, eine kleine Schleife zu formulieren. Das folgende Kommando bildet zu allen `*.tex`-Dateien Backup-Kopien mit der Endung `tex~`. (Die Endung ~ wird häufig zur Kennzeichnung von Sicherheitskopien verwendet.)

```
user$  for i in *.tex; do cp $i $i~; done
```

Versteckte Dateien

Unter Linux gelten Dateien, deren Name mit einem Punkt beginnt, als versteckte Dateien. * berücksichtigt deswegen nicht wirklich alle Dateien in einem Verzeichnis: Dateien, die mit einem Punkt beginnen (häufig Konfigurationsdateien, die unsichtbar sein sollen), werden ignoriert.

Wenn Sie nun glauben, Sie könnten unsichtbare Dateien mit `.*` erfassen, wird alles noch schlimmer: Damit sind nämlich nicht nur unsichtbare Dateien gemeint, die mit . beginnen, sondern auch die Verzeichnisse . und .. (also das aktuelle und das übergeordnete Verzeichnis). Wenn das jeweilige Kommando in der Lage ist, ganze Verzeichnisse zu bearbeiten, können die Folgen fatal sein.

Das Problem kann mit dem Suchmuster `.[!.]*` umgangen werden. Damit werden alle Dateinamen erfasst, deren erstes Zeichen ein Punkt ist, die mindestens ein weiteres Zeichen aufweisen, das kein Punkt ist, und die beliebig viele (auch null) weitere Zeichen haben.

```
user$  echo .[!.]*
```

Beim Kommando `ls` kann die Option `-a` verwendet werden. Sie führt dazu, dass alle Dateien angezeigt werden, auch unsichtbare. Allerdings dürfen bei dieser Verwendung von `ls` keine Masken (etwa *rc*) angegeben werden. `-a` funktioniert nur dann, wenn `ls` sich die Dateien selbst suchen darf und nicht die Shell diese Aufgabe übernimmt.

Wirklich universell funktioniert auch in diesem Fall nur `find`. Das folgende Kommando findet alle versteckten Dateien im aktuellen Verzeichnis:

```
user$  find -maxdepth 1 -type f -name '.*'
```

Sonderformen von Dateien (Links, Devices etc.)

Neben gewöhnlichen Dateien kennt Linux eine Reihe von Sonderformen, z. B. Verzeichnisse, Links sowie Device-Dateien zum Zugriff auf Hardware-Komponenten. `ls -F` kennzeichnet derartige Sonderformen durch ein zusätzliches Zeichen.

```
user$  ls -lF
... 13. Apr 11:31 bak/
... 11. Apr 12:21 grepalltex*
...
```

Links lernen Sie im nächsten Abschnitt näher kennen, Device-Dateien in Abschnitt 15.9. FIFO-Dateien ermöglichen es, dass ein Prozess in die Datei schreibt und ein zweiter Prozess die Daten von dort wieder ausliest.

Zeichen	Bedeutung
/	Verzeichnis
*	ausführbare Datei
@	symbolischer Link
-	zeichenorientiertes Gerät (Character Device)
+	blockorientiertes Gerät (Block Device)
=	Pipe, First In First Out (FIFO)

Tabelle 15.4 Identifizierung von Spezialdateien

15.2 Links

Links sind Verweise auf Dateien. Durch Links können Sie von verschiedenen Orten in der Verzeichnisstruktur auf ein- und dieselbe Datei zugreifen, ohne dass diese Datei physikalisch mehrfach gespeichert werden muss. Links sind damit ein wichtiges Hilfsmittel zur Vermeidung von Redundanzen. Im Linux-Dateisystem kommen Links besonders häufig in `/bin`- und `/lib`-Verzeichnissen vor. (Sehen Sie sich beispielsweise `/usr/bin` oder `/usr/lib` mit `ls -l` genauer an!)

Am einfachsten sind Links anhand eines Beispiels zu verstehen: Angenommen, im Verzeichnis `test` befindet sich die Datei `abc`; durch das Kommando `ln abc xyz` wird scheinbar eine neue Datei `xyz` erstellt. In Wahrheit sind aber `abc` und `xyz` nur zwei Verweise auf ein und dieselbe Datei. Die einzige Möglichkeit, das zu überprüfen, bietet das Kommando `ls` mit der Option `-l`. Es gibt in der zweiten Spalte an, wie viele Links auf eine bestimmte Datei zeigen – im vorliegenden Beispiel also 2. Wenn zusätzlich die Option `-i` verwendet wird, gibt `ls` auch den Inode der Datei an, der bei Links identisch ist. Inodes sind interne Identifikationsnummern des Dateisystems.

```
user$  ls -li
 59293 -rw-r--r--   1 root     root    1004 Oct  4 16:40 abc
user$  ln abc xyz
user$  ls -li
 59293 -rw-r--r--   2 root     root    1004 Oct  4 16:40 abc
 59293 -rw-r--r--   2 root     root    1004 Oct  4 16:40 xyz
```

Wenn Sie nun eine der beiden Dateien verändern (egal welche), ändert sich automatisch auch die andere Datei – weil es ja in Wirklichkeit nur eine einzige Datei gibt!

Wenn Sie eine der beiden Dateien löschen, reduzieren Sie dadurch nur die Anzahl der Links.

Backup-Dateien von verlinkten Dateien sind problematisch

Wenn Sie fest verlinkte Dateien mit einem Texteditor bearbeiten, treten bisweilen seltsame Ergebnisse auf: Der Link zeigt nach dem ersten Speichern auf die Backup-Datei und beim zweiten Speichern ins Leere.

Der Grund: Manche Editoren erzeugen beim Speichern eine Backup-Datei, indem sie die vorhandene Datei umbenennen, also beispielsweise `abc` in `abc~`. Die geänderte Datei wird vollkommen neu angelegt, erhält einen neuen Inode und ist damit frei von Links. Abhilfe: Verwenden Sie symbolische Links.

Symbolische Links

Linux kennt zwei Formen von Links. Das obige Beispiel hat feste Links (Hardlinks) vorgestellt, wie sie standardmäßig durch das Kommando `ln` erzeugt werden. Wird `ln` dagegen mit der Option `-s` verwendet, erzeugt das Kommando symbolische Links. Symbolische Links werden manchmal auch weiche Links oder Softlinks genannt. Sie haben den Vorteil, dass sie innerhalb des Dateisystems von einer physikalischen Festplatte auf eine andere verweisen können und dass sie nicht nur auf Dateien, sondern auch auf Verzeichnisse angewandt werden können. Beides ist mit festen Links normalerweise nicht möglich. Einen Sonderfall stellen feste Links auf Verzeichnisse dar, die zwar möglich sind, aber nur von `root` erstellt werden können.

Durch `ls` wird bei symbolischen Links angezeigt, wo sich die Ursprungsdatei befindet. Es wird allerdings kein Zähler verwaltet, der angibt, von wie vielen Stellen auf die Ursprungsdatei verwiesen wird.

Intern besteht der Unterschied zwischen festen und symbolischen Links darin, dass im einen Fall der Inode, im anderen Fall der Dateiname oder (bei Links über ein Verzeichnis hinaus) die Pfadangabe gespeichert wird.

```
user$  ln -s abc efg
user$  ls -li
 59293 -rw-r--r--   2 root     root    1004 Oct  4 16:40 abc
 59310 lrwxrwxrwx   1 root     root       3 Oct  4 16:52 efg -> abc
 59293 -rw-r--r--   2 root     root    1004 Oct  4 16:40 xyz
```

Tipp

Bevor Sie einen symbolischen Link einrichten, sollten Sie immer in das Verzeichnis wechseln, das den Link enthalten wird. Andernfalls kann es passieren, dass der Link nicht dorthin zeigt, wohin Sie es erwarten.

Symbolische Links verhalten sich ein wenig anders als feste Links. Das Löschen der Ursprungsdatei (also z. B. `abc` aus dem vorigen Beispiel) verändert den Link auf diese Datei nicht, `efg` verweist jetzt aber auf eine gar nicht vorhandene Datei. Wird dagegen der symbolische Link gelöscht, hat das keinen Einfluss auf die Ursprungsdatei.

Symbolische Links können nicht nur für Dateien, sondern auch für Verzeichnisse erstellt werden. Das kann einige Verwirrung stiften, weil durch einen symbolischen Link ganze Verzeichnisbäume scheinbar verdoppelt werden. In Wirklichkeit stellt der Verzeichnis-Link aber nur einen zusätzlichen Pfad zu denselben Dateien und Unterverzeichnissen dar.

Generell sollten Sie versuchen, möglichst keine absoluten, sondern nur relative Pfadangaben in Links zu verwenden. Damit vermeiden Sie Probleme, die sich beim Mounten von Verzeichnissen per NFS oder beim Verschieben von Verzeichnissen ergeben können.

Feste Links versus symbolische Links

Sowohl symbolische als auch feste Links haben Vorteile. Symbolische Links sind einfacher in der Handhabung. Dafür verbrauchen feste Links weniger Speicher und sind schneller.

15.3 Dateitypen (MIME)

Sie klicken in einem Webbrowser oder Dateimanager auf einen Link, der auf eine MP3-Datei verweist – und die MP3-Datei wird automatisch in einem Audio-Player abgespielt. Wenn das funktioniert, ist MIME korrekt konfiguriert.

MIME

MIME steht für Multipurpose Internet Mail Extensions. Ursprünglich bezog sich MIME auf E-Mail-Attachments. Wenn mit einer E-Mail beispielsweise eine PDF- oder JPEG-Datei mitgesandt wird, dann sollte der E-Mail-Client wissen, mit welchem Programm diese Datei betrachtet bzw. bearbeitet werden kann. Damit das funktioniert, ist die MIME-Konfiguration erforderlich.

Mittlerweile reicht die Anwendung von MIME aber viel weiter: Wenn Sie im Dateimanager oder Webbrowser einen Link auf eine Datendatei verfolgen, sollte auch dieses Programm wissen, wie es mit diesen Daten umgehen soll. Die Bedeutung einer korrekten MIME-Konfiguration erstreckt sich also auf alle Programme, die mit unterschiedlichen Datentypen zurechtkommen müssen.

MIME-Konfiguration

Linux wäre nicht Linux (oder Unix), wenn es *einen* zentralen Ort für die MIME-Konfiguration gäbe. Stattdessen gibt es eine ganze Menge. Die MIME-Daten für KDE-Programme, Gnome-Programme, diverse Webbrowser, für das Drucksystem CUPS etc. werden jeweils separat verwaltet. Außerdem gibt es noch eine zentrale MIME-Konfiguration für alle Programme, die keine eigenen MIME-Konfigurationsdateien verwalten.

Die Aufteilung der MIME-Konfiguration auf mehrere Orte hat natürlich gute Gründe: Sowohl KDE als auch Gnome verwenden ein Konzept, das Komponenten zur Bearbeitung verschiedener Datentypen vorsieht. Wenn im KDE-Dateimanager eine PNG-Bilddatei angezeigt werden soll, wird einfach die entsprechende Komponente geladen und ausgeführt. Da die KDE- und Gnome-Bibliotheken in der Regel zueinander inkompatibel sind, wäre es fatal, wenn der KDE-Dateimanager versuchen würde, eine Gnome-Komponente auszuführen (oder umgekehrt). Um das zu vermeiden, verwenden KDE und Gnome jeweils ihre eigene MIME-Datenbank. Ähnlich ist die Argumentation auch bei allen anderen Programmen mit eigener MIME-Konfiguration.

Bei vielen MIME-Konfigurationsdateien muss darüber hinaus zwischen der globalen und der individuellen Konfiguration unterschieden werden, also zwischen der Grundeinstellung für alle Anwender und den benutzerspezifischen Einstellungen. Im Folgenden wird nur die MIME-Grundkonfiguration von Linux präsentiert. Anwendungsspezifische MIME-Details sind in anderen Kapiteln beschrieben: die KDE-MIME-Konfiguration also im KDE-Kapitel etc.

Allgemeine MIME-Konfiguration

Die allgemeinen MIME-Konfigurationsdateien werden nur von den Programmen berücksichtigt, die keine eigenen MIME-Dateien verwalten. Die Einstellungen sind auf zwei Dateien verteilt, von denen es jeweils eine globale und eine benutzerspezifische Version gibt (siehe Tabelle 15.5).

Datei	Bedeutung
`/etc/mime.types`	globale Konfiguration für Dateitypen
`/etc/mailcap`	globale Konfiguration für Programme
`.mime.types`	lokale Konfiguration für Dateitypen
`.mailcap`	lokale Konfiguration für Programme

Tabelle 15.5 MIME-Konfigurationsdateien

`mime.types` enthält eine Liste, die die Zuordnung zwischen Dateitypen (erste Spalte) und Dateikennungen (alle weiteren Spalten) herstellt. Die erste Beispielzeile ordnet dem Typ *application/pdf* die Kennung `*.pdf` zu. In `mime.types` wird zum Teil

zwischen Text- und X-Applikationen unterschieden, weswegen Sie Dateitypen wie *application/x-name* finden werden.

```
# in /etc/mime.types
...
application/pdf     pdf
```

`mailcap` gibt an, welches Programm zur Anzeige bzw. Bearbeitung eines bestimmten Dateityps verwendet werden soll. Die folgende Zeile besagt, dass zur Anzeige von PDF-Dateien das Programm `evince` verwendet werden soll. Im Gegensatz zu `mime.types` müssen die Spalten in `mailcap` durch Semikola getrennt werden. `%s` ist ein Platzhalter für den Dateinamen.

```
# in /etc/mailcap
application/pdf; evince %s
```

Magic-Dateien zur Erkennung des Dateityps

MIME ist für die Zuordnung zwischen dem Dateityp und den dazu passenden Programmen zuständig. Aber wie wird der Dateityp überhaupt festgestellt? Der Normalfall besteht darin, dass die Dateikennung den Dateityp angibt. Die Dateikennung `*.ps` deutet also beispielsweise auf eine PostScript-Datei hin.

Bei Dateien ohne Kennung versuchen das Programm `file` bzw. entsprechende KDE- oder Gnome-Äquivalente den Dateityp aus dem Inhalt der ersten Bytes bzw. anhand in der Datei enthaltener charakteristischer Zeichenketten zu erkennen. Das Erkennungsverfahren basiert auf in das Kommando `file` einkompilierten Informationen darüber, welche Byte- und Zeichenmuster eine Datei enthalten kann. Bei einigen Distributionen kann die Standardkonfiguration durch die Dateien `/etc/magic` bzw. in `.magic` verändert werden.

15.4 Dateien suchen (find, grep, locate)

Linux bietet eine Menge Möglichkeiten, um nach Dateien zu suchen (siehe Tabelle 15.6). Welches Kommando am besten geeignet ist, hängt davon ab, um welche Art von Datei es sich handelt (Textdatei, Programm etc.) und welche Informationen bekannt sind – z. B. Teile des Dateinamens oder Suchbegriffe für den Inhalt.

which und whereis

`which` sucht nach dem angegebenen Kommando. Es liefert den vollständigen Namen des Kommandos, das ausgeführt werden würde, wenn der Kommandoname ohne Pfadinformationen aufgerufen würde.

`which` durchsucht lediglich die in `PATH` angegebenen Verzeichnisse und arbeitet daher außerordentlich schnell. `PATH` enthält eine Liste von Verzeichnissen, in denen sich

Kommando	Funktion
grep	sucht Text in einer Textdatei.
find	sucht Dateien nach Name, Datum, Größe etc.
locate	sucht Dateien nach ihrem Namen.
whereis	sucht Dateien in vordefinierten Verzeichnissen.
which	sucht Programme in PATH-Verzeichnissen.

Tabelle 15.6 Kommandos zur Dateisuche

Programme befinden. Beachten Sie aber, dass PATH für root mehr Verzeichnisse enthält als für gewöhnliche Benutzer. Wenn Sie also Systemkommandos suchen, müssen Sie sich als root einloggen.

```
user$  which emacs
/usr/bin/emacs
```

whereis durchsucht alle üblichen Pfade für Binärdateien, Konfigurationsdateien, man-Seiten und Quellcode nach dem angegebenen Dateinamen. whereis erfasst damit mehr Verzeichnisse als which und beschränkt sich nicht nur auf Programme. Es versagt allerdings für Dateien, die sich nicht in den für whereis vordefinierten Verzeichnissen befinden (siehe man whereis).

```
user$  whereis fstab
fstab: /etc/fstab /usr/include/fstab.h /usr/share/man/man5/fstab.5.gz
```

locate

locate muster findet Dateien, bei denen das angegebene Suchmuster im vollständigen Dateinamen vorkommt, also im Pfad plus Dateinamen. Die Suche ist sehr schnell: locate durchsucht nämlich nicht das Dateisystem, sondern greift auf eine Datenbank zurück, die eine Liste aller Dateinamen des Dateisystems enthält. Je nach Distribution zeigt locate nur solche Dateien an, auf die der Benutzer tatsächlich Zugriff hat. Führen Sie locate gegebenenfalls als root aus, wenn Sie nach Systemdateien suchen. locate kann nur benutzt werden, wenn das entsprechende Paket installiert ist, was nicht bei allen Distributionen standardmäßig der Fall ist.

Das folgende Kommando sucht die X-Konfigurationsdatei xorg.conf: **Beispiele**

```
user$  locate xorg.conf
/etc/X11/xorg.conf
/etc/X11/xorg.conf.backup
/etc/X11/xorg.conf~
/usr/share/man/man5/xorg.conf.5x.gz
```

Die Suche nach `dvips` liefert (sofern dieses Paket sowie LaTeX installiert ist) sehr viele Treffer, weil der Suchbegriff in mehreren Verzeichnisnamen vorkommt. Anstatt alle Suchergebnisse anzuzeigen, werden diese mit `wc` gezählt.

```
user$  locate dvips | wc -l
    421
```

Die Anzahl der Ergebnisse wird wesentlich kleiner, wenn Sie nur nach Dateien suchen, die mit `dvips` enden:

```
user$  locate '*dvips'
/usr/bin/dvips
/usr/bin/odvips
/usr/bin/opdvips
/usr/bin/pdvips
/usr/local/texmf/dvips
/usr/local/texmf/fonts/map/dvips
...
```

updatedb

Die Qualität der Suchergebnisse steht und fällt mit der Aktualität der Datenbank für `locate`. Bei den meisten Distributionen wird die `locate`-Datenbank einmal täglich durch das Kommando `updatedb` aktualisiert. `updatedb` kann natürlich jederzeit auch manuell ausgeführt werden. Das erfordert aber `root`-Rechte.

Distributionsspezifische Details

Je nach Distribution sind `locate` und `updatedb` unterschiedlich implementiert. Bei Debian, Fedora und Ubuntu stellt das standardmäßig installierte Paket `mlocate` die Kommandos `locate` und `updatedb` zur Verfügung. Die Dateidatenbank befindet sich in der Datei `/var/lib/mlocate/mlocate.db` und wird einmal täglich durch den Cron-Job `/etc/cron.daily/mlocate` aktualisiert. Die Konfigurationsdatei `/etc/updatedb.conf` bestimmt, welche Verzeichnisse und Dateisysteme nicht berücksichtigt werden (z. B. CDs, DVDs, diverse Spool-Verzeichnisse).

Bei openSUSE steht `locate` standardmäßig nicht zur Verfügung. Bevor Sie das Suchkommando nutzen können, müssen Sie das Paket `findutils-locate` installieren und als `root` einmalig `updatedb` ausführen. In Zukunft wird das Kommando einmal täglich durch den Cron-Job `/etc/cron.daily/suse.de-updatedb` aktualisiert. Die Konfiguration erfolgt durch `/etc/sysconfig/locate`.

find und grep

`find` ist ein ebenso leistungsfähiges wie komplexes Kommando zur Suche nach Dateien. Es berücksichtigt verschiedene Suchkriterien: ein Muster für den Dateinamen, die Dateigröße, das Datum der Erstellung oder des letzten Zugriffs etc. Eine vollständige Referenz aller Optionen gibt `man find`. Die folgenden Beispiele führen

aber wohl am besten in den Umgang mit `find` ein. Beachten Sie, dass `find` ein vergleichsweise langsames Kommando ist, weil es das Dateisystem Verzeichnis für Verzeichnis durchsucht.

Ohne weitere Parameter liefert `find` eine Liste aller Dateien im aktuellen Verzeichnis und in allen Unterverzeichnissen: find

```
user$  find
...
```

Das folgende Kommando sucht alle Dateien im aktuellen Verzeichnis und in allen Unterverzeichnissen, die mit `.e` beginnen:

```
user$  find -name '.e*'
./.evolution
./.emacs
./.emacs~
./.esd_auth
...
```

`find` sucht ausgehend vom Verzeichnis `/usr/share/texmf` alle `*.tex`-Dateien in einem Verzeichnis, das mit `latex` endet:

```
user$  find /usr/share/texmf -path '*latex/*.tex'
/usr/share/texmf/ptex/platex/base/plnews03.tex
/usr/share/texmf/ptex/platex/base/kinsoku.tex
...
```

Im nächsten Beispiel sucht `find` alle Verzeichnisse innerhalb von `/etc/`. Gewöhnliche Dateien in `/etc` werden dagegen nicht angezeigt. Die Ergebnisliste wird durch `sort` alphabetisch geordnet, was standardmäßig nicht der Fall ist.

```
root#  find /etc -type d | sort
/etc
/etc/acpi
/etc/acpi/actions
...
```

Im Folgenden sucht `find` alle Dateien in den (Unter-)Verzeichnissen von `/home`, die Benutzern der Gruppe `users` gehören und deren Inhalt in den letzten fünf Tagen in irgendeiner Form verändert wurden:

```
root#  find /home -group users -mtime -5
...
```

`find -mtime +5` findet Dateien, die vor *mehr* als fünf Tagen verändert wurden, und `-mtime 5` liefert solche Dateien, die vor *genau* fünf Tagen verändert wurden. `find` rechnet dabei in Vielfachen von 24 Stunden vom aktuellen Zeitpunkt aus. Wenn Sie statt

-mtime die Option -ctime verwenden, gilt die *inode change time* als Änderungszeitpunkt. Dieser Zeitpunkt verändert sich beispielsweise auch dann, wenn nicht der Inhalt, sondern z. B. die Zugriffsrechte verändert werden.

Das folgende Kommando löscht alle Backup-Dateien im aktuellen Verzeichnis und in allen Unterverzeichnissen. Dabei wird die Liste aller infrage kommenden Dateien mit find gebildet und durch Kommandosubstitution ($(kommando)) an rm weitergeleitet.

```
user$ rm $(find . -name '*~')
```

Falls es sich um *sehr* viele Dateien handelt, tritt bei der Ausführung des obigen Kommandos ein Fehler auf: Die Kommandozeile mit allen *~-Dateien wird so lang, dass sie die maximale Kommandozeilenlänge überschreitet. In solchen Fällen müssen Sie entweder die -exec-Option des find-Kommandos oder das Kommando xargs zu Hilfe nehmen.

grep Das Kommando grep durchsucht eine Textdatei nach einem Suchmuster. Je nach Einstellung der Optionen zeigt das Kommando anschließend die gefundenen Textpassagen an oder gibt einfach nur an, in wie vielen Zeilen das Suchmuster gefunden wurde. Das Suchmuster ist ein sogenannter regulärer Ausdruck.

Das folgende Kommando durchsucht alle *.tex-Dateien des aktuellen Verzeichnisses nach der Zeichenkette »emacs«. Die Liste aller gefundenen Zeilen, denen jeweils der Dateiname vorangestellt ist, wird im Terminal angezeigt.

```
user$ grep emacs *.tex
...
```

grep ermittelt hier, wie oft die Funktion arctan in den angegebenen *.c-Dateien verwendet wird:

```
user$ grep -c arctan\(.*\) *.c
```

grep -v liefert als Ergebnis alle Zeilen, die das Suchmuster nicht enthalten. Im folgenden Beispiel entfernt grep aus configfile alle Zeilen, die mit dem Zeichen # beginnen – also alle Kommentare. Das nachgestellte cat-Kommando eliminiert außerdem alle leeren Zeilen. Das Endergebnis wird in der Datei nocomments gespeichert. Die Anweisung ist praktisch, wenn wenige Konfigurationszeilen in Hunderten oder Tausenden von Kommentarzeilen untergehen.

```
user$ grep -v '^#' configfile | cat -s > nocomments
```

find und grep kombinieren

Sie können `find` und `grep` auch kombinieren, um besonders wirkungsvolle Suchen durchzuführen. Im folgenden Beispiel durchsucht `find` alle `*.tex`-Dateien daraufhin, ob in ihnen die Zeichenkette »emacs« vorkommt. Wenn das der Fall ist, wird der Dateiname auf dem Bildschirm ausgegeben. Beachten Sie, dass die Option `-print` nicht vor `-exec` angegeben werden darf. Im Gegensatz zum obigen Beispiel `grep emacs *.tex` berücksichtigt dieses Beispiel auch `*.tex`-Dateien in beliebig tief verschachtelten Unterverzeichnissen.

```
user$  find -name '*.tex' -type f -exec grep -q emacs {}  \; -print
...
```

Das folgende Kommando durchsucht alle Dateien im aktuellen Verzeichnis, die kleiner als 10 kByte sind, nach dem regulären Ausdruck `case.*in`. Die Liste der gefundenen Dateien wird in der Datei `ergebnis` gespeichert. Durch die Einschränkung der Dateigröße auf 10 kByte wird versucht, die zumeist erheblich größeren binären Dateien aus der Suche auszuschließen.

```
user$  find -name '*' -maxdepth 1 -size -10k -exec grep -q \
    >  case.*in {} \; -print > ergebnis
```

15.5 CDs und DVDs brennen

Die wichtigsten Benutzeroberflächen zum Brennen von CDs und DVDs habe ich Ihnen in den Gnome- und KDE-Kapiteln bereits vorgestellt: Brasero und K3B. Solange Sie nur gelegentlich eine CD oder DVD brennen, bieten diese Programme ausreichend Funktionen und sind zudem einfach zu bedienen. Wenn Sie eine Benutzeroberfläche für die Textkonsole suchen, werden Sie beim Kommando `burncdda` fündig.

Dieser Abschnitt stellt hingegen Kommandos vor, die hinter den Kulissen dieser Benutzeroberflächen zum Einsatz kommen. Das ist beispielsweise dann interessant, wenn Sie durch ein Script das Erzeugen von Backup-CDs automatisieren möchten. Wie so oft verhilft die Kenntnis der zugrunde liegenden Kommandos auch zu einem besseren Verständnis, wie Linux funktioniert.

Device-Namen

Bevor Sie die im Folgenden beschriebenen Kommandos einsetzen können, müssen Sie wissen, unter welchem Device-Namen Sie Ihr Laufwerk ansprechen. In der Regel lautet der richtige Device-Name `/dev/scd0`, `/dev/scd1` etc. oder `/dev/sr0`, `/dev/sr1` etc.

Vereinzelt gibt es auch Kommandos, die die Device-Angabe für SCSI-Geräte in der Form eines Zahlentripels erwarten, z. B. `dev=3,0,0`. Die drei Zahlen geben die SCSI-Bus-Nummer an (meistens 0), die SCSI-ID des Gerätes und schließlich die Logical Unit Number (kurz LUN, ebenfalls meist 0). Die richtige Zahlenkombination für Ihr Laufwerk ermitteln Sie am einfachsten mit `readcd -scanbus`.

CDs und DVDs müssen vor dem Brennen aus dem Dateisystem gelöst werden

Egal, ob Sie CDs oder DVDs brennen: Stellen Sie sicher, dass Ihre Linux-Distribution den Datenträger nicht in den Verzeichnisbaum einbindet oder sonstwie darauf zugreift, und lösen Sie die CD/DVD gegebenenfalls mit `umount` aus dem Verzeichnisbaum!

ISO-Images erzeugen und testen

Bevor Sie eine Daten-CD oder eine DVD brennen können, brauchen Sie ein sogenanntes ISO-Image. Diese Datei enthält die zu brennenden Daten im internen Format des optischen Datenträgers. In der Regel werden Sie zum Erzeugen von ISO-Dateien `genisoimage` einsetzen (ehemals `mkisofs`).

genisoimage

Mit dem Kommando `genisoimage` schreiben Sie alle Dateien eines oder mehrerer Verzeichnisse in eine ISO-Datei. Das für CDs vorgesehene Format ISO-9660 verwendet einen eigenen, sehr limitierten Zeichensatz, der nur wenige Nicht-ASCII-Zeichen zulässt. Um diesen Mangel zu umgehen, gibt es mehrere Erweiterungen zum ISO-Standard, von denen die folgenden beiden weit verbreitet sind und von `genisoimage` unterstützt werden:

- Die für Unix/Linux-Systeme übliche Rockridge-Extension erlaubt die Speicherung langer Dateinamen in Form beliebiger, nullterminierter Zeichenketten. Außerdem erlaubt diese Erweiterung die Speicherung von Zugriffsrechten (UID, GID, Zugriffsbits).

  Allerdings enthalten Rockridge-CDs keine Information darüber, in welchem Zeichensatz das ISO-Image erstellt wurde. Das kann zu Problemen führen, wenn der Datenträger später auf einem Rechner mit einem anderen Zeichensatz verwendet wird. Am einfachsten ist das anhand eines Beispiels zu verstehen: Vor ein paar Jahren war unter Linux noch der Latin-1-Zeichensatz üblich. Eine zu diesem Zeitpunkt mit der Rockridge-Extension erzeugte Daten-CD verwendet daher ebenfalls diesen Zeichensatz. Wenn Sie die CD auf einer heute aktuellen Distribution mit aktivem Unicode-Zeichensatz (UTF-8) nutzen, werden Nicht-ASCII-Zeichen in den Dateinamen falsch interpretiert. Wenn bereits beim Vorbereiten eines ISO-Images klar ist, dass die CD später auf einem Rechner mit einem anderen Zeichensatz genutzt werden soll, kann der gewünschte Zielzeichensatz durch die Option `-output-charset` eingestellt werden.
- Die für Windows-Systeme übliche Joliet-Extension erlaubt ebenfalls die Speicherung langer Dateinamen, wobei als Zeichensatz Unicode (UTF-16) zum Einsatz kommt.

Beispiele

Das folgende Kommando schreibt alle Dateien innerhalb des `/master`-Verzeichnisses in die Datei `/tmp/master.iso`. Das Verzeichnis `master` ist selbst *kein* Verzeichnis im ISO-Image. Das ISO-Image nutzt sowohl die Rockridge-Extension (Option `-r`) als auch die Joliet-Extension (Option `-J`) und bekommt den Namen `Linux` (Option `-V`). Wenn Sie aus dem ISO-Image eine CD brennen, gilt diese Zeichenkette als CD-Name.

```
user$ genisoimage -o /tmp/master.iso -r -J -V Linux /master
```

Das zweite Beispiel ist dem ersten ähnlich, allerdings wird diesmal eine bootfähige CD erstellt:

```
user$ genisoimage -o /tmp/master.iso -r -J /master -b images/boot.img \
        -c boot.catalog
```

Im dritten Beispiel ist das Verzeichnis `master` nun selbst ein Verzeichnis im ISO-Image (Option `-graft-points`):

```
user$ genisoimage -o /tmp/master.iso -r -graft-points /master=/master
```

Tipp

Falls Sie die Option `-r` nicht verwenden, sollten Sie darauf achten, dass alle Dateien im `master`-Verzeichnis `root` gehören und von allen lesbar sind!

```
user$ chown -R root.root /master
user$ chmod -R a+r /master
```

xorriso

Eine Alternative zu `genisoimage` ist das Kommando `xorriso` aus dem gleichnamigen Paket. Mit dem Kommando können Sie ISO-Dateien erzeugen, veränden und auf eine CD oder DVD brennen. Eine Menge Anwendungsbeispiele finden Sie auf der Projektseite:

http://www.gnu.org/software/xorriso

dd

Wenn Sie eine Daten-CD oder -DVD (keine Audio-CD!) unverändert kopieren möchten, reicht ein einziges `dd`-Kommando aus, um die erforderliche ISO-Datei zu erzeugen. Statt `/dev/cdrom` müssen Sie den Device-Namen Ihres CD- oder DVD-Laufwerks angeben, der je nach Distribution variiert.

```
user$ dd if=/dev/cdrom of=/usr/local/iso.img bs=2048
```

readcd

Eine Variante zu `dd` ist das Kommando `readcd` bzw. dessen Variante `readom`. Es verwendet SCSI-Kommandos zum Auslesen der CD und sollte zum gleichen Ergebnis kommen wie `dd`. Bei meinen Tests auf zwei unterschiedlichen Rechnern lieferte `readcd` allerdings zahllose Fehlermeldungen. Anders als bei `dd` müssen Sie Ihr CD- oder DVD-Laufwerk durch ein Zahlentripel angeben. Die richtige Zahlenkombination für Ihr Laufwerk ermitteln Sie mit `readcd -scanbus`.

```
user$  readcd dev=0,0,0 f=iso.img
```

Der Vorteil von readcd besteht darin, dass es auch eine TOC-Datei erstellen kann (bei Audio-CDs mit der Option -clone) und dass das Programm je nach Optionen auf unterschiedliche Weise mit Lesefehlern umgehen kann (Optionen -noerror und -noclone, siehe man cdread). Mit -w kann readcd auch zum Schreiben von CDs verwendet werden.

ISO-Image testen

Mit dem sogenannten Loopback-Device des Linux-Kernels können Sie eine Datei als Dateisystem betrachten und mit mount in den Verzeichnisbaum einbinden. Die Loopback-Funktion ist im Kernelmodul loop versteckt. Falls das Modul nicht automatisch geladen wird, müssen Sie eventuell mit modprobe nachhelfen. Das folgende Kommando bindet das in der Datei master.iso enthaltene ISO-Dateisystem im Read-Only-Modus in den Verzeichnisbaum ein:

```
root#  mkdir /iso-test
root#  mount -t iso9660 -o loop,ro /tmp/master.iso /iso-test/
```

Über das Verzeichnis iso-test können Sie jetzt den Inhalt der zukünftigen CD-ROM überprüfen.

CDs brennen

cdrecord und wodim

Mehr als ein Jahrzehnt lang war cdrecord das Standardprogramm zum Schreiben von CDs. Seit Sommer 2006 verwendet der cdrecord-Entwickler Jörg Schilling allerdings für einige Teile des cdrecord-Pakets die von Sun entworfene Lizenz CDDL. Andere Entwickler betrachten diese Lizenz als inkompatibel zur GPL. Aus diesem Grund kam es zu einem sogenannten »Fork«, also zu einer Spaltung des Projekts: Die letzte GPL-konforme cdrecord-Version diente als Basis für das neue Kommando wodim (Write Data to Optical Disk Media), das Teil des neuen cdrkit-Projekts ist. Parallel zu cdrecord gibt es auch Forks für zwei weitere Kommandos: aus mkisofs wurde genisoimage, und aus cdda2wav wurde icedax.

Alle aktuellen Distributionen verwenden nun wodim, genisoimage und icedax. Aus Kompatibilitätsgründen kann cdrecord aber vielfach weiterhin über den bisher üblichen Namen cdrecord aufgerufen werden. /usr/bin/cdrecord ist aber nur ein Link auf wodim.

Bevor Sie eine Daten-CD brennen können, brauchen Sie ein ISO-Image, das Sie normalerweise mit genisoimage erzeugen (siehe den vorigen Abschnitt). Mit den beiden folgenden Kommandos wird zuerst das Brennen einer Daten-CD simuliert (-dummy) und dann tatsächlich durchgeführt:

```
root#  wodim -dummy -v speed=16 dev=/dev/scd0 iso.img
root#  wodim -v speed=16 dev=/dev/scd0 iso.img
```

Auf schnellen Rechnern können Sie `genisoimage` und `wodim` mit einer Pipe verbinden. Dadurch sparen Sie den Platz für das ISO-Image:

```
root#  genisoimage -r /master | wodim -v speed=16 dev=/dev/scd0 -
```

Das folgende Kommando erzeugt eine Audio-CD. Die Ausgangsdaten liegen als `*.wav`-Dateien vor. Die Dateien werden in alphabetischer Reihenfolge verarbeitet. Wenn Sie eine andere Reihenfolge wünschen, müssen Sie die Dateien der Reihe nach angeben.

```
root#  wodim -v speed=16 dev=0,5,0 -pad -dao -audio *.wav
```

cdrdao

Das Kommando `cdrdao` ist eine Alternative zu `wodim`. `cdrdao` ist zwar nicht so vielseitig, bietet dafür aber wesentlich mehr Optionen zum Lesen und Schreiben von Audio-CDs. Seinen Namen verdankt `cdrdao` dem Schreibmodus *Disk at Once* (kurz DAO).

In der Praxis besteht die gebräuchlichste Anwendung von `cdrdao` darin, Audio-CDs zu kopieren. Das erste `cdrdao`-Kommando erzeugt die Dateien `data.bin` (Inhalt der CD) und `data.toc` (Inhaltsverzeichnis). Das zweite Kommando schreibt diese Daten auf eine CD:

```
user$  cdrdao read-cd --device /dev/sg0 data.toc
user$  cdrdao write   --device /dev/sg0 --buffers 64 data.toc
```

Daten-CD verifizieren

Das folgende Kommando vergleicht den Inhalt der CD-ROM mit dem des `master`-Verzeichnisses Datei für Datei und Byte für Byte. Sämtliche Unterschiede werden in die Datei `diff.log` im Heimatverzeichnis geschrieben. Statt `/media/cdrom` müssen Sie das Verzeichnis angeben, an dem die CD in Ihren Verzeichnisbaum eingebunden ist.

```
root#  diff -qrd /master /media/cdrom/  >& ~/diff.log
```

In einem zweiten Fenster bzw. in einer zweiten Konsole können Sie mit `tail` das Entstehen von `diff.log` verfolgen. Dabei sind Fehlermeldungen aufgrund von symbolischen Links zu erwarten, die auf der CD nicht mehr an den richtigen Ort verweisen. Ein echtes Warnsignal ist es hingegen, wenn einzelne Dateien gar nicht gelesen werden können (I/O-Error) oder wenn der Inhalt von Dateien abweicht und Sie sicher sind, dass sich die Datei seither nicht verändert hat.

```
root#  tail -f ~/diff.log
```

Wenn Sie nur testen möchten, ob alle Datenblöcke der CD gelesen werden können (ganz egal, welchen Inhalt sie haben), führen Sie das folgende Kommando aus. Dieser Test ist beispielsweise dann sinnvoll, wenn Sie eine CD bekommen haben, von der Sie vermuten, dass sie defekt ist.

```
root#  dd if=/dev/cdrom of=/dev/null
```

DVDs brennen (dvd+rw-tools)

Auch beim Brennen von DVDs haben Sie die Wahl zwischen mehreren Kommandos bzw. Paketen:

- Am populärsten sind die Kommandos der `dvd+rw-tools`, die ich Ihnen in diesem Abschnitt kurz vorstelle.
- Sollten Sie damit Probleme haben, können Sie Ihr Glück auch mit `wodim` versuchen. Das Kommando eignet sich zum Schreiben einfacher DVD-Rs und DVD+Rs, wobei sich die Syntax nicht vom Schreiben von CDs unterscheidet. `wodim` bietet allerdings weniger Optionen beim Beschreiben von DVD+RW- bzw. DVD-RW-Medien.

dvd+rw-tools

Alle im weiteren Verlauf dieses Abschnitts vorgestellten Kommandos sind Teil des `dvd+rw-tools`-Pakets. Ursprünglich unterstützte dieses Paket nur die Formate DVD+R und DVD+RW (daher auch der Name). Mittlerweile können Sie damit aber auch DVD-Rs und DVD-RWs sowie Blu-ray Discs brennen (was ich aber nicht getestet habe). Das `dvd+rw-tool` wird mit nahezu allen gängigen Distributionen standardmäßig installiert. Weitere Informationen finden Sie unter:

http://fy.chalmers.se/~appro/linux/DVD+RW

growisofs

Das zentrale Kommando des `dvd+rw-tools`-Pakets ist `growisofs`. Es schreibt DVD+Rs, DVD+RWs, DVD-Rs, DVD-RWs und Blu-ray-Discs. Vorweg einige allgemeine Informationen zu den unterschiedlichen Medientypen:

- DVD+R, DVD-R: Dem Datenträger können Daten wie bei Multi-Session-CDs hinzugefügt werden. Bei der ersten Session verwenden Sie `growisofs -Z`, bei allen weiteren Sessions `growisofs -M`. Einmal gespeicherte Daten können aber nicht gelöscht werden. Eine Formatierung ist nicht möglich.
- DVD+RW, DVD-RW: Der Datenträger muss vor der ersten Verwendung mit `dvd+rw-format` formatiert werden (siehe unten). Anschließend können Sie wie bei einer DVD+R/DVD-R in mehreren Schritten Daten hinzufügen. Wenn Sie vorhandene Daten überschreiben möchten, starten Sie den Session-Zyklus einfach mit `growisofs -Z` neu. Anders als bei CD-RWs ist es in diesem Fall nicht notwendig, die DVD neu zu formatieren!

  Bei DVD-RWs werden je nach Formatierung die Modi *Incremental Sequential* und *Restricted Overwrite* unterstützt.

Da `growisofs` auf `genisoimage` zurückgreift, sind die meisten Optionen mit diesem Kommando identisch. Das folgende Kommando speichert den Inhalt des Verzeichnisses `daten` auf einer DVD. Die `genisoimage`-Optionen `-r` und `-J` bewirken, dass die DVD lange Dateinamen entsprechend den Rockridge- und Joliet-Erweiterungen auf-

weist. Statt des Device-Namens `/dev/srn` müssen Sie je nach Distribution `/dev/scdn` angeben.

```
user$  growisofs -r -J -Z /dev/sr0 daten/
```

Eine zweite Session fügen Sie so hinzu (Option `-M` statt `-Z`):

```
user$  growisofs -r -J -M /dev/sr0 nochmehrdaten/
```

Tipps zu Multi-Session-DVDs

Beachten Sie, dass Sie die DVD auswerfen und neu in das Laufwerk einführen müssen, bevor Sie eine weitere Session hinzufügen können!

Multi-Session-DVDs können beim Lesen in manchen Laufwerken Probleme bereiten. Bei DVD-RWs sollten Sie den Modus *Restricted Overwrite* nutzen (siehe `dvd+rw-format`).

Normalerweise übergibt `growisofs` alle Optionen außer `-Z` bzw. `-M` an `genisoimage` und schreibt das Ergebnis von `genisoimage` dann direkt auf die DVD. Wenn Sie ein bereits existierendes ISO-Image schreiben möchten, lautet die Syntax `-Z device=isodatei`:

```
user$  growisofs -Z /dev/sr0=daten.iso
```

dvd+rw-format

DVD+RWs und DVD-RWs im *Restricted Overwrite* Modus müssen vor der ersten Verwendung formatiert werden. Diese Aufgabe übernimmt `dvd+rw-format`:

```
user$  dvd+rw-format /dev/sr0
```

Was beim Formatieren im Detail passiert, hängt vom Medientyp ab:

- **DVD+RWs:** Hier wird nur der Anfangsbereich des Rohlings formatiert. Wie weit dieser reicht, hängt vom Brenner ab. Wenn der Formatiervorgang also bei 11,5 Prozent (oder irgendeiner anderen Prozentzahl kleiner 100) endet, ist dies kein Fehler! Die Formatierung über den Anfangsbereich hinaus erfolgt automatisch durch das Laufwerk, sobald die DVD über den vorformatierten Bereich hinaus beschrieben wird.
- **DVD-RWs:** DVD-RWs werden von `dvd+rw-format` standardmäßig für den Modus *Restricted Overwrite* formatiert. Dieser Modus ermöglicht es, bereits beschriebene Bereiche der DVD neu zu beschreiben. Es ist daher nicht erforderlich, DVD-RWs vor jedem Schreiben neu zu formatieren!

  DVD-RWs können Sie mit der Option `-blank` auch für den Modus *Incremental Sequential* formatieren. Fabrikneue DVD-RWs sind in der Regel bereits in diesem Modus formatiert. Dieser Modus eignet sich besonders für Video-DVDs und erhöht die Kompatibilität mit manchen Abspielgeräten. Allerdings ist `growisofs` in diesem Modus nicht in der Lage, Daten zu überschreiben. Dazu muss die DVD jedes Mal neu formatiert werden, was sehr lange dauert.

> Fazit: Für die optimale Zusammenarbeit mit `growisofs` sollten Sie DVD-RWs unbedingt vorher mit `dvd+rw-format` und ohne die Option `-blank` formatieren!

Die Formatierung löscht die Daten nicht physikalisch. Falls Sie dies aus Datenschutzgründen wünschen, führen Sie besser `growisofs -Z device=/dev/zero` aus. Damit wird das gesamte Medium mit Nullen vollgeschrieben.

dvd+rw-mediainfo

Wenn Sie eine DVD erhalten und nicht wissen, um welchen DVD-Typ es sich handelt, ob die DVD schon beschrieben ist und wenn ja, in welchem Modus und mit wie vielen Sessions, ermitteln Sie diese Informationen mit `dvd+rw-mediainfo`:

```
user$  dvd+rw-mediainfo /dev/sr0
INQUIRY:                [_NEC    ][DVD_RW ND-1300A ][1.07]
GET [CURRENT] CONFIGURATION:
 Mounted Media:         1Ah, DVD+RW
GET PERFORMANCE:
 Speed Descriptor#0:    00/221280 Reading@7.8x Writing@2.3x
READ DVD STRUCTURE[#0h]:
 Media Book Type:       92h, DVD+RW book [revision 2]
 Media ID:              RICOHJPN/W01
 Legacy lead-out at:    221280*2KB=453181440
...
```

15.6 Zugriffsrechte, Benutzer und Gruppenzugehörigkeit

Linux ist als Multiuser-System konzipiert und benötigt daher Mechanismen, die steuern, wer auf welche Dateien zugreifen darf, wer sie ändern darf etc. Die Basis des Zugriffssystems stellt die Verwaltung von Benutzern und Gruppen dar, die in Abschnitt 21.4 beschrieben wird.

Zugriffsrechte für Dateien

Zugriffsrechte pro Datei

Mit jeder Datei bzw. mit jedem Verzeichnis werden folgende Informationen gespeichert:

- der Besitzer (Owner) der Datei
- eine Gruppe, der die Datei zuzuordnen ist
- neun Zugriffsbits (`rwxrwxrwx` für Read/Write/Execute für den Besitzer, für alle Gruppenmitglieder und für den Rest der Welt)
- einige weitere Zusatzbits für Spezialfunktionen

Der Besitzer (Owner) einer Datei ist in der Regel die Person, die die Datei erzeugt hat. Als Gruppe wird normalerweise die primäre Gruppe des Besitzers verwendet.

Die Zugriffsinformationen `r`, `w` und `x` steuern, wer die Datei lesen, schreiben (verändern) und ausführen darf. Diese Informationen werden getrennt für den Besitzer, für die Gruppe und für alle anderen Benutzer gespeichert. Das ermöglicht es, dem Besitzer mehr Rechte zu geben als anderen Benutzern. Die Informationen werden meist Zugriffsbits genannt, weil sie intern als Zahl mit bitweiser Codierung gespeichert werden.

Wer darf eine Datei löschen?

Die Zugriffsrechte einer Datei haben Einfluss darauf, wer eine Datei löschen darf. Darüber entscheidet einzig und allein, wer Zugriff auf das *Verzeichnis* hat, in dem sich die Datei befindet! Eine Datei darf löschen, wer für das Verzeichnis die Rechte w und x hat. Mehr Informationen zu den Zugriffsrechten für Verzeichnisse folgen im nächsten Abschnitt.

Die Zugriffsbits, der Besitzer sowie die Gruppenzugehörigkeit einer Datei können mit `ls -l` betrachtet werden. Für eine typische Textdatei liefert `ls` das folgende Ergebnis:

```
michael$  ls -l datei.txt
-rw-r-----   1 michael  users        3529 Oct  4 15:43 datei.txt
```

Kurz die Interpretation: Das erste Zeichen gibt den Dateityp an. Das Zeichen `-` bedeutet, dass es sich um eine normale Datei handelt. Andere Möglichkeiten sind `d` für ein Verzeichnis (Directory), `l` für einen symbolischen Link etc.

Die drei Zeichen `rw-` geben an, dass die Datei vom Besitzer `michael` gelesen und verändert werden kann. Da es sich um eine Textdatei handelt, ist das erste x-Bit deaktiviert, die Datei kann also nicht ausgeführt werden.

Die folgenden drei Zeichen `r--` geben an, dass alle Mitglieder der Gruppe `users` die Datei lesen, aber nicht verändern dürfen.

Aus den letzten drei Zeichen `---` geht hervor, dass andere Benutzer, die also weder `michael` noch Mitglieder der Gruppe `user` sind, die Datei weder lesen noch verändern dürfen.

Wenn `michael` möchte, dass diese Datei von allen Anwendern gelesen werden kann, dann muss er das letzte `r`-Bit aktivieren. Dazu verwendet er das Kommando `chmod o+r`:

```
michael$  chmod o+r datei.txt
michael$  ls datei.txt -l
-rw-r--r--   1 michael  users        3529 Oct  4 15:43 datei.txt
```

Manchmal sollen *zwei* oder mehr Benutzer die Möglichkeit bekommen, die Datei zu verändern. Dazu kann eine neue Gruppe gebildet werden, der diese Benut-

zer angehören. Wenn michael und kathrin das Dokumentationsteam einer Firma bilden, wäre als Gruppenname etwa dokuteam sinnvoll. Anschließend wird die Gruppenzugehörigkeit mit chgrp geändert:

```
michael$  chgrp dokuteam datei.txt
michael$  chmod g+rw datei.txt
michael$  ls datei.txt -l
-rw-rw-r--   1 michael  dokuteam     3529 Oct  4 15:43 datei.txt
```

Tatsächlich ist die gemeinsame Bearbeitung von Dateien noch ein wenig diffiziler: Es muss auch sichergestellt werden, dass alle Benutzer Zugriff auf das *Verzeichnis* haben, in dem sich die Dateien befinden. Mehr Details zu diesem Thema folgen gleich.

Oktale Schreibweise

Statt in der Schreibweise rwxrwxrwx werden die neun Zugriffsbits sowie drei weitere Spezialbits oft auch oktal dargestellt. Das ist wahrscheinlich die populärste Anwendung, die dieses Zahlensystem auf der Basis der Zahl 8 bis heute hat.

Den Zugriffsbits für den Benutzer, die Gruppe und alle anderen ist jeweils eine Ziffer zugeordnet (siehe Tabelle 15.7). Jede Ziffer ist aus den Werten 4, 2 und 1 für r, w und x zusammengesetzt. 660 bedeutet daher rw-rw----, 777 steht für rwxrwxrwx. Die in Abschnitt 15.6 vorgestellten Spezialbits setuid, setgid und sticky haben die Oktalwerte 4000, 2000 und 1000.

Code	Bedeutung
4000 = s = setiud 2000 = s = setgid 1000 = t = sticky	Spezialbits
400 = r = read 200 = w = write 100 = x = execute	Zugriffsbits für den Besitzer (u = user in chmod)
40 = r 20 = w 10 = x	Zugriffsbits für Gruppenmitglieder (g = group)
4 = r 2 = w 1 = x	Zugriffsbits für alle anderen (o = others)

Tabelle 15.7 Oktalcodes für die Zugriffsbits

Mit dem Kommando chmod können Sie die Zugriffsbits auch oktal einstellen, was viele erfahrene Benutzer wegen des geringeren Tippaufwands vorziehen:

```
user$  chmod 640 datei.txt
```

Erstaunlicherweise ist `ls` aber nicht in der Lage, die Zugriffsbits oktal darzustellen. Abhilfe schafft das Kommando `stat`:

```
user$  stat -c "%a %n" *
755 php53-beispiele
550 Private
755 samples
...
```

Zugriffsrechte auf Devices

Der Zugriff auf diverse Hardware-Komponenten wie Festplatten, CD- und DVD-Laufwerke, Schnittstellen etc. erfolgt in Linux über sogenannte Devices (siehe Abschnitt 15.9). Um gezielt steuern zu können, welcher Benutzer auf welche Devices zugreifen darf, sind den Devices unterschiedliche Benutzergruppen zugeordnet. Beispielsweise sind die Devices `/dev/ttyS*` für die seriellen Schnittstellen unter Debian und Ubuntu der Gruppe `dialout` zugeordnet:

```
root#  ls -l /dev/ttyS1
crw-rw----   1 root     dialout       5,  65 Jul 18  /dev/ttyS1
```

Wenn der Systemadministrator möchte, dass der User `hubert` die serielle Schnittstelle nutzen darf, fügt er `hubert` zur Gruppe `dialout` hinzu:

```
root#  usermod -a -G dialout hubert
```

Zugriffsrechte für Verzeichnisse

r-, w- und x-Zugriff auf Verzeichnisse

Die neun Zugriffsbits haben im Prinzip auch bei Verzeichnissen Gültigkeit, allerdings besitzen sie dort eine etwas abweichende Bedeutung: Das `r`-Bit erlaubt einem Anwender, die Liste der Dateinamen zu ermitteln (Kommando `ls`). Mit dem `x`-Bit können Sie in ein Verzeichnis wechseln (Kommando `cd`); Sie können aber nur auf Dateien zugreifen, deren Namen Sie kennen. Erst die Kombination `rx` ermöglicht es, ein Verzeichnis richtig zu bearbeiten, also z. B. mit `ls -l` eine Liste aller Dateinamen samt detaillierter Informationen zu jeder Datei zu ermitteln. Wenn sowohl `x` als auch `w` gesetzt sind, dürfen im Verzeichnis neue Dateien erzeugt werden.

Die ein wenig merkwürdige Interpretation der `r`- und `x`-Zugriffsrechte hat damit zu tun, dass Verzeichnisse vom Dateisystem als ein Sonderfall einer Datei betrachtet werden; der Inhalt der Verzeichnis-»Datei« ist eine Auflistung der Namen der Dateien, die sich im Verzeichnis befinden, sowie von deren Inode-Nummern.

Wer darf was?

Tabelle 15.8 fasst zusammen, welche Zugriffsrechte für ein Verzeichnis und die darin enthaltene Datei erforderlich sind, um bestimmte Aktionen durchzuführen. Das Zeichen – in der Spalte *Datei* gibt an, dass die Zugriffsrechte auf die Datei nicht relevant sind. Wie üblich gelten diese Regeln nur für gewöhnliche Benutzer. `root` darf unabhängig von den eingestellten Zugriffsrechten alles!

Aktion	Kommando	Datei	Verzeichnis
in Verzeichnis wechseln	`cd verzeichnis`	–	x
Liste der Dateien ermitteln	`ls verzeichnis/*`	–	r
Dateiinformationen lesen	`ls -l verzeichnis/*`	–	rx
neue Datei erzeugen	`touch verzeichnis/neuedatei`	–	wx
Datei lesen	`less verzeichnis/datei`	r	x
vorhandene Datei ändern	`cat >> verzeichnis/datei`	w	x
Datei löschen	`rm verzeichnis/datei`	–	wx
Programm ausführen	`verzeichnis/programm`	x	x
Script-Datei ausführen	`verzeichnis/script`	rx	x

Tabelle 15.8 Erforderliche Zugriffsrechte für Standardaktionen

Verschachtelte Verzeichnisse

Bei verschachtelten Verzeichnissen ist für die Basisverzeichnisse vor allem das `x`-Bit entscheidend. Ist dieses nicht gesetzt, können die Unterverzeichnisse nicht genutzt werden. In der Praxis ist es zumeist zweckmäßig, für Basisverzeichnisse auch das `r`-Bit zu setzen. Fehlt das Leserecht, muss der Anwender den Namen des Unterverzeichnisses wissen.

Welche Operationen im Unterverzeichnis erlaubt sind, hängt ausschließlich von den `rwx`-Bits dieses Verzeichnisses ab. Wenn für das Unterverzeichnis die Rechte `rwx` gesetzt sind, können somit Dateien gelesen, erzeugt, verändert und gelöscht werden – selbst dann, wenn in den Basisverzeichnissen die Rechte `r` und `w` fehlen!

Betrachten Sie zum besseren Verständnis das Verzeichnis `/`, das Verzeichnis `/home` und ein darin enthaltenes Benutzerverzeichnis:

```
root#  ls -ld /
drwxr-xr-x ... root root ... /home/
root#  ls -ld /home/
drwxr-xr-x ... root root ... /home/
root#  ls -ld /home/kofler/     (unter Debian, Ubuntu)
drwxr-xr-x ... kofler kofler ... /home/kofler/
```

Für `/` und `/home` gilt: Jeder darf die Namen der in diesem Verzeichnis enthaltenen Dateien und Unterverzeichnisse ermitteln sowie detaillierte Informationen darüber abfragen, also `ls -l /home` ausführen. Aber nur `root` darf mit `mkdir /home/neuerBenutzer` neue Heimatverzeichnisse einrichten.

Für `/home/kofler` gilt: Nur der Benutzer `kofler` darf in diesem Verzeichnis neue Dateien anlegen. Alle anderen Benutzer dürfen in das Verzeichnis reinsehen (`ls -l`), aber nichts verändern. Es bleibt dem Besitzer des Heimatverzeichnisses überlas-

sen, die Zugriffsrechte für eigene Dateien und Unterverzeichnisse gegebenenfalls so einzustellen, dass auch ein Lesezugriff unmöglich ist.

Beachten Sie, dass `kofler` selbstverständlich in seinem Heimatverzeichnis Dateien anlegen, verändern und löschen darf, obwohl er keine Schreibrechte in `/` und `/home` hat!

Einige Linux-Distributionen, wie Fedora oder Red Hat, stellen die Zugriffsrechte für die Heimatverzeichnisse restriktiver ein und erlauben wirklich nur dem Besitzer einen Blick in das Verzeichnis:

```
root#  ls -ld /home/kofler/      (unter Fedora, RHEL, CentOS)
drwx------ ... kofler kofler ... /home/kofler/
```

Verzeichnisse gemeinsam benutzen

Die gerade erwähnten Heimatverzeichnisse sind ein Beispiel für Verzeichnisse, die nur für einen bestimmten Benutzer gedacht sind. Wie aber richten Sie Verzeichnisse ein, die mehrere Benutzer gemeinsam nutzen können – z. B. ein Projektverzeichnis für die Benutzer `sebastian` und `matthias`, sodass beide in dem Verzeichnis Dateien lesen *und* verändern dürfen?

Die Lösung für derartige Probleme sind Gruppen: Sie legen eine neue Gruppe `projektxy` an und ordnen `sebastian` und `matthias` dieser Gruppe zu. Nun brauchen Sie noch ein Projektverzeichnis, das dieser Gruppe zugeordnet ist:

```
root#  addgroup projektxy
root#  usermod -a -G projektxy sebastian
root#  usermod -a -G projektxy matthias
root#  mkdir -p /projekte/xy
root#  chgrp projektxy /projekte/xy
root#  chmod 755 /projekte
root#  chmod 2770 /projekte/xy
root#  ls -ld /projekte/xy
drwxrws--- ... root projektxy ... /projekte/xy
```

Die Einstellung der Zugriffsrechte für `/projekte` ist wie für das `/home`-Verzeichnis: Nur `root` darf darin neue Dateien und Verzeichnisse anlegen. Alle anderen dürfen die Verzeichnisse benutzen.

Im Verzeichnis `/projekte/xy` haben alle Mitglieder der Gruppe `projektxy` Schreib- und Leserechte, also in diesem Beispiel `sebastian` und `matthias`.

Die einzige Besonderheit ist das Setgid-Bit für dieses Verzeichnis (Oktalcode 2000). Es bewirkt, dass in diesem Verzeichnis eingerichtete Dateien und Verzeichnisse automatisch der Gruppe `projektxy` zugeordnet werden, nicht der Gruppe desjenigen Benutzers, der die Datei erzeugt. Damit wird der Fall vermieden, dass `sebastian` eine neue Datei erzeugt und `matthias` diese zwar sieht und lesen, aber nicht verändern kann. Hintergrundinformationen zum Setgid-Bit folgen im nächsten Abschnitt.

Spezialbits (Setuid, Setgid und Sticky)

Die Bedeutung der drei mal drei Zugriffsbits `rwxrwxrwx` ist leicht zu verstehen. Darüber hinaus können bei den Zugriffsinformationen von Dateien und Verzeichnissen noch drei weitere Informationen gespeichert werden: das Setuid-Bit, das Setgid-Bit und das Sticky-Bit. Im Regelfall müssen nur Systemadministratoren diese Spezialbits kennen.

Setuid-Bit (Suid-Bit)

Das Setuid-Bit wird oft verkürzt Suid-Bit genannt. Es bewirkt, dass Programme immer so ausgeführt werden, als hätte der Besitzer selbst das Programm gestartet. Oft ist der Besitzer von Programmen `root`; dann kann jeder das Programm ausführen, als wäre er selbst `root`. Intern wird für die Ausführung des Programms die User-Identifikationsnummer des Besitzers der Datei und nicht die UID des aktuellen Benutzers verwendet.

Das Bit wird eingesetzt, um gewöhnlichen Besitzern zusätzliche Rechte zu geben, die nur bei der Ausführung dieses Programms gelten. Ein Beispiel für die Anwendung des Setuid-Bits ist das Kommando `/usr/bin/passwd`. Es ermöglicht jedem Benutzer, sein eigenes Passwort zu verändern. Die Passwörter werden aber in der Datei `/etc/shadow` gespeichert, auf die nur `root` Lese- und Schreibzugriff hat. Daher muss `passwd` mit `root`-Rechten ausgeführt werden.

`ls -l` zeigt bei derartigen Programmen bei den Benutzer-Zugriffsbits, also in der ersten `rwx`-Gruppe, den Buchstaben `s` oder `S` statt des `x` an: ein kleines `s`, wenn das Execute-Bit auch gesetzt ist (der Normalfall), ein großes `S`, wenn nur das Setuid-Bit, nicht aber das Execute-Bit gesetzt ist. Der Oktalwert dieses Bits für `chmod` beträgt 4000.

```
root#  ls -l /bin/mount
-rwsr-xr-x    1 root   root    68508 Feb 25  01:11 /bin/mount
root#  ls -l /usr/bin/passwd
-rwsr-xr-x ... root root ... /usr/bin/passwd
```

Achtung, Sicherheitsrisiko!

Das Setuid-Bit kann leicht zu einem Sicherheitsrisiko werden – insbesondere dann, wenn während der Ausführung des Programms weitere Programme gestartet werden. Aus diesem Grund wird die Anwendung des Setuid-Bits nach Möglichkeit vermieden, insbesondere bei Script-Dateien.

Setgid-Bit für Dateien

Das Setgit-Bit hat bei Programmen eine ähnliche Wirkung wie Setuid. Allerdings wird nun während der Ausführung des Programms die Gruppen-Identifikationsnummer der Datei verwendet, nicht die GID des aktuellen Benutzers.

`ls -l` zeigt bei derartigen Programmen für die Gruppen-Zugriffsbits, also in der zweiten `rwx`-Gruppe, den Buchstaben `s` oder `S` anstelle des `x`) an. Der Oktalwert dieses Bits beträgt 2000.

Setgid-Bit für Verzeichnisse

Bei Verzeichnissen hat das Setgid-Bit eine ganz andere Bedeutung: Wenn es gesetzt ist, wird neu erzeugten Dateien innerhalb dieses Verzeichnisses die Gruppe des Verzeichnisses zugeordnet – anstatt, wie sonst üblich, die Gruppe desjenigen, der die Datei erzeugt.

In der Praxis wird das Setgid-Bit eingesetzt, wenn mehrere Benutzer ein Verzeichnis gemeinsam benutzen sollen: Dann ist es nämlich zweckmäßig, dass neue Dateien der gemeinsamen Gruppe zugeordnet werden und nicht der gerade aktiven Gruppe desjenigen Benutzers, der die Datei erzeugt. Aus diesem Grund wurde das Setgid-Bit im vorigen Abschnitt für das Verzeichnis `/projekte/xy` verwendet.

Sticky-Bit für Verzeichnisse

Das Sticky-Bit bewirkt bei Verzeichnissen, in denen alle die Dateien ändern dürfen, dass jeder nur seine *eigenen* Dateien löschen darf und nicht auch Dateien anderer Benutzer. Das Bit ist beispielsweise beim `/tmp`-Verzeichnis gesetzt. In diesem Verzeichnis darf jeder Benutzer temporäre Dateien anlegen. Es soll aber vermieden werden, dass auch jeder Benutzer nach Belieben fremde Dateien umbenennen oder löschen kann.

`ls -l` zeigt bei derartigen Programmen für alle gültigen Zugriffsbits den Buchstaben `t` an anstelle des `x` an. Der Oktalwert dieses Bits beträgt 1000. Die Bedeutung des Sticky-Bits ist Linux-spezifisch! Bei anderen Unix-Varianten kann das Bit eine andere oder gar keine Bedeutung haben.

```
user$  ls -ld /tmp/
drwxrwxrwt  ... root root ... /tmp/
```

Veränderung der Spezialbits durch chmod

Am einfachsten gelingt die Einstellung der Spezialbits durch `chmod`, wenn Sie mit Oktalcodes arbeiten – also z. B. `chmod 2770 verzeichnis`. Aber natürlich ist auch eine Veränderung in der `chmod`-üblichen Syntax `owner+-bit` möglich:

```
root#  chmod u+s datei   (setzt das Setuid-Bit)
root#  chmod u-s datei   (löscht das Setuid-Bit)
root#  chmod g+s datei   (setzt das Setgid-Bit)
root#  chmod g-s datei   (löscht das Setgid-Bit)
root#  chmod +t  datei   (setzt das Sticky-Bit)
root#  chmod -t  datei   (löscht das Sticky-Bit)
```

Darstellung der Spezialbits durch ls

Die Interpretation der Ergebnisse von `ls -l` ist nicht ganz einfach:

- Das Setuid-Bit wird durch die Buchstaben `s`/`S` anstelle des `x` in der ersten `rwx`-Gruppe angezeigt.
- Das Setgid-Bit wird durch die Buchstaben `s`/`S` anstelle des `x` in der zweiten `rwx`-Gruppe angezeigt.
- Das Sticky-Bit wird durch die Buchstaben `t`/`T` anstelle des `x` in der dritten `rwx`-Gruppe angezeigt.

Die Großbuchstaben `S` und `T` kommen nur zur Anwendung, wenn das entsprechende Execute-Bit *nicht* gesetzt ist. In der Regel ist das ein Hinweis darauf, dass die Spezialbits falsch verwendet werden.

Dateifunktion bzw. -typ

Linux-intern werden zusammen mit den Zugriffsbits und den Spezialbits auch die Informationen darüber gespeichert, welche Funktion eine Datei hat. Es kann sich beispielsweise um eine normale Datei handeln, um ein Verzeichnis, um einen Link, um ein Block-Device etc.

Die meisten Programme zur Dateiverwaltung verbergen diese Zusatzinformation. Es gibt aber einige wenige Programme, die diese Information als Zahlenwert anzeigen. Bei einer gewöhnlichen Datei lautet die komplette Spezifikation dann `100000` (Kennzeichnung für eine gewöhnliche Datei) plus *x*`000` (Spezialbits) plus *xxx* (Zugriffsbits), also beispielsweise `100760`. Die Zahlencodes für die Dateitypen erhalten Sie mit `man 2 stat`.

Besitzer, Gruppe und Zugriffsbits neuer Dateien

Dieser Abschnitt beschäftigt sich mit der Frage, welche Faktoren die Zugriffsinformationen *neuer* Dateien bestimmen. Um das einfach auszuprobieren, verwenden Sie das Kommando `touch`. Dieses Kommando erzeugt eine neue, leere Datei, falls die angegebene Datei noch nicht existiert.

Beispiel

Der Benutzer `michael` erzeugt die neue Datei `myFile1`. Es sollte nicht überraschen, dass diese Datei wieder dem Benutzer `michael` gehört – er hat sie ja gerade selbst erzeugt. Als Gruppenzugehörigkeit wurde automatisch `michael` verwendet. `michael` ist die primäre Gruppe des Benutzers `michael`. (Manche Distributionen weisen nicht jedem Benutzer eine eigene Gruppe zu, sondern allen Benutzern die Gruppe `users`.)

```
michael$  touch myFile1
michael$  ls -l myFile1
-rw-r--r--    1 michael   michael          0 Jun 14 16:45 myFile1
```

michael gehört einer Reihe weiterer Gruppen an (Kommando groups). Um eine Datei zu erzeugen, die nicht der primären Gruppe angehört, muss zuerst die aktive Gruppe gewechselt werden (Kommando newgrp):

```
michael$  groups
michael adm admin cdrom dokuteam dialout lpadmin plugdev sambashare
michael$  newgrp dokuteam
michael$  touch myFile2
michael$  ls -l myFile2
-rw-r--r--    1 michael   dokuteam           0 Jun 14 17:02 myFile2
```

Natürlich hätte myFile2 auch ohne vorheriges newgrp erzeugt werden können. Dann hätte die Gruppenzugehörigkeit nachträglich mit chgrp verändert werden müssen. newgrp ist dann praktisch, wenn mehrere neue Dateien erzeugt werden, die automatisch einer bestimmten Gruppe angehören sollen.

Besitzer und Gruppenzugehörigkeit

Aus den zwei Beispielen oben geht hervor, dass neue Dateien automatisch dem Benutzer gehören, der sie erzeugt. Als Gruppenzugehörigkeit wird normalerweise die primäre Gruppe des Benutzers verwendet. Allerdings gibt es hier zwei Ausnahmen:

- Wenn der Benutzer mit newgrp eine andere seiner Gruppen zur aktuellen Gruppe gemacht hat, gehört die neue Datei dieser Gruppe.
- Wenn in einem Verzeichnis das Setgid-Bit gesetzt ist (siehe den vorigen Abschnitt), dann erhalten darin erzeugte Dateien automatisch dieselbe Gruppe wie das Verzeichnis. Die aktive Gruppe des Benutzers wird nicht berücksichtigt.

Zugriffsbits

Bei den Zugriffsbits ist die Sache etwas komplizierter. Linux sieht eigentlich vor, dass neue Dateien die Zugriffsbits rw-rw-rw (oktal 666) bekommen, also von jedem gelesen und verändert werden dürfen. Neue Verzeichnisse und Programmdateien, die von einem Compiler erzeugt werden, bekommen automatisch die Zugriffsbits rwxrwxrwx (777), können also auch von jedem ausgeführt werden.

umask-Arithmetik

Für die praktische Arbeit mit mehreren Benutzern wäre diese Grundeinstellung allerdings zu freizügig. Deswegen sehen alle Linux-Shells die sogenannte umask-Einstellung vor. Dabei handelt es sich um einen Zahlenwert, der die Bits angibt, die von den Standardzugriffsbits abgezogen werden. Die aktuelle Einstellung des umask-Werts können Sie mit dem gleichnamigen Kommando feststellen und bei Bedarf auch verändern:

```
michael$   umask    (Debian, openSUSE, Ubuntu)
0022
michael$   umask    (Fedora, RHEL)
0002
```

Viele Linux-Distributionen verwenden also den umask-Wert 022 (----w--w-). Daher bekommen neue Dateien die Zugriffsbits 666 - 022 = 644 (rw-r--r--), neue Verzeichnisse und Programme die Zugriffsbits 777 - 022 = 755 (rwxr-xr-x).

Der bei Fedora und Red Hat übliche umask-Wert 002 ist liberaler: Neue Dateien erhalten die Zugriffsbits 666 - 002 = 664 (rw-rw-r--), neue Verzeichnisse 777 - 002 = 775 (rwxrwxr-x).

Oft lautet die Frage umgekehrt: Wie muss umask eingestellt werden, damit neue Dateien die Zugriffsrechte rw-r----- = 640 erhalten, neue Verzeichnisse rwxr-x--- = 750? Die Antwort ergibt sich aus der Subtraktion von 777 minus dem oktalen Zielwert für Verzeichnisse: 777 - 750 = 027.

```
michael$  umask 27
michael$  touch neue-datei
michael$  mkdir neues-verzeichnis
michael$  ls -ld neu*
-rw-r----- ... michael michael ... neue-datei
drwxr-x--- ... michael michael ... neues-verzeichnis
```

umask-Konfigurationsdateien

Die Einstellung des umask-Werts erfolgt in den Konfigurationsdateien der Shells. Für die Bash wird umask meist in /etc/profile oder /etc/bashrc eingestellt.

Bei neueren Distributionen kümmert sich PAM (siehe Abschnitt 21.4) um die Einstellung von umask. Das PAM-Modul pam_umask wertet unter anderen den optionalen Eintrag ulimit=xxx in der dritten Spalte (GECOS) von /etc/passwd aus. Außerdem werden die Einstellungen aus /etc/default/login und /etc/login.defs berücksichtigt. Die letztere Datei enthält z. B. unter Ubuntu die umask-Defaulteinstellung.

Einzelne Benutzer können bei den meisten Distributionen eine davon abweichende Einstellung in der Datei ~/.bashrc vornehmen. Wenn Sie beispielsweise möchten, dass von Ihnen erzeugte Dateien nur von den Gruppenmitgliedern, nicht aber von anderen Benutzern gelesen bzw. ausgeführt werden dürfen, verwenden Sie folgende Einstellung:

```
# in ~/.bashrc
umask 027
```

Wer darf Zugriffsinformationen ändern?

Bei einer einmal erzeugten Datei werden weder der Besitzer noch die Zugriffsbits geändert, wenn sie von einem anderen Benutzer bearbeitet wird. Nur der Besitzer darf die Gruppenzugehörigkeit und Zugriffsbits ändern. Und nur root darf den Besitzer einer Datei verändern. Damit ist es also nicht möglich, dass der Besitzer einer Datei diese einem anderen gleichsam schenkt.

15.7 Access Control Lists und Extended Attributes

Access Control Lists (ACLs)

Die Unix-typische Verwaltung von Benutzern und Gruppen sowie die darauf aufbauenden Zugriffsrechte für Verzeichnisse und Dateien haben sich seit Jahrzehnten bewährt. Das Konzept ist so einfach, dass man es nach ein paar Stunden versteht. Es gibt allerdings Fälle, in denen dieses einfache System unzureichend ist.

Aus diesem Grund wurde ein feinmaschigeres System zur Verwaltung von Zugriffsrechten entwickelt, das auf sogenannten Access Control Lists (ACLs) basiert. ACLs ermöglichen es, für jede Datei bzw. für jedes Verzeichnis beliebig viele Regeln aufzustellen, welche Benutzer und Gruppen die Datei bzw. das Verzeichnis lesen oder verändern dürfen und wer das – abweichend von den Unix-Zugriffsrechten – *nicht* darf. ACLs wirken also ergänzend zu den Standardzugriffsrechten und können zusätzliche Rechte einräumen oder vorhandene Rechte entziehen.

ACLs stehen unter Linux ab Kernel 2.6 standardmäßig zur Verfügung. Für frühere Kernelversionen gab es entsprechende Patches. Bei den Dateisystemen `btrfs`, `jfs` und `xfs` sind ACLs in jedem Fall aktiv. Bei den `ext`-Dateisystemen muss dagegen die `mount`-Option `acl` verwendet werden, um ACLs zu aktivieren.

Der Datei-Server Samba ist das bei Weitem wichtigste Programm, das wirklich von ACLs profitiert. Es ist dank ACLs in der Lage, Windows-Zugriffsrechte unter Linux nachzubilden.

Einschränkungen

Nur weil ACLs mehr Möglichkeiten bieten, lösen sie die herkömmliche Rechteverwaltung keineswegs ab! Für erfahrene Administratoren großer Netzwerke mögen ACLs zusätzliche Sicherheit bringen oder zumindest die Verwaltung vereinfachen, für die meisten Linux-Anwender ist die gewöhnliche Rechteverwaltung aber absolut ausreichend. Wer das komplexe ACL-System nicht korrekt anwendet, wird womöglich zusätzliche Sicherheitslöcher aufreißen. Daher gibt es momentan kaum Distributionen, die ACLs standardmäßig nutzen.

Ein zentrales Problem besteht darin, dass viele Linux-Kommandos und -Programme ACLs nicht korrekt verarbeiten. Da kann es schon einmal passieren, dass einer kopierten Datei plötzlich die ACL-Informationen des Originals fehlen. Auch die meisten Dateimanager können ACLs weder richtig anzeigen noch verändern. Der KDE-Dateimanager Dolphin ist eine positive Ausnahme.

Extended Attributes (EAs)

Eng verwandt mit ACLs sind Extended Attributes (EAs). Sie ermöglichen es, zu jeder Datei zusätzliche Attribut-Wert-Paare zu speichern. Sie können einer Textdatei also beispielsweise das Attribut `charset` mit der Einstellung `utf8` zuordnen, um so den benutzten Zeichensatz zu speichern. Das bringt freilich nur dann Vorteile mit sich, wenn es auch Programme gibt, die diese Informationen auswerten. Je nachdem, welches Dateisystem Sie einsetzen, müssen auch EAs durch eine entspre-

chende mount-Option aktiviert werden, beim ext-Dateisystem beispielsweise durch user_xattr.

Weitere Hintergrundinformationen und Details zur Anwendung von ACLs und EAs finden Sie in den man-Seiten zu acl, getfacl, setfacl, attr(5), getfattr und getsattr sowie unter:

http://acl.bestbits.at
http://turing.suse.de/~agruen
http://www.vanemery.com/Linux/ACL/linux-acl.html

Voraussetzungen

In den folgenden Beispielen gehe ich davon aus, dass das Paket attr mit den Kommandos attr, getfattr und setfattr installiert ist und dass Sie mit einem Dateisystem arbeiten, in dem ACLs und EAs aktiviert sind. Wenn es sich um ein ext4-Dateisystem handelt, sollte das Ergebnis von mount so aussehen:

```
user$  mount
...
/dev/sdc5 on /test type ext4 (rw,acl,user_xattr)
...
```

Sollte das nicht der Fall sein, erhalten Sie bei den folgenden Beispielen Fehler der Art *Operation wird nicht unterstützt*. Abhilfe schafft die Veränderung der mount-Optionen in /etc/fstab und ein Neueinbinden des Dateisystems. Werfen Sie gegebenenfalls einen Blick in Kapitel 25 über die Administration des Dateisystems. Informationen speziell zur Veränderung der mount-Optionen in /etc/fstab finden Sie in Abschnitt 25.5.

Access Control Lists

getfacl

Auch bei einem Dateisystem mit ACLs gelten normalerweise die Standardzugriffsrechte, die oft auch als minimale ACL bezeichnet werden. getfacl zeigt diese Rechte in ACL-Form an:

```
user$  touch datei1
user$  getfacl datei1
# file: datei1
# owner: kofler
# group: kofler
user::rw-
group::r--
other::r--
user$  ls -l datei1
-rw-r--r-- 1 kofler kofler ...  datei2
```

setfacl

Mit `setfacl` definieren Sie nun zusätzliche Zugriffsregeln. Die folgenden Kommandos geben der Benutzerin `gabi` sowie allen Mitgliedern der Gruppe `docuteam` Schreib- und Lesezugriff auf die Datei, verbieten aber der Benutzerin `kathrin` jeglichen Zugriff:

```
user$  setfacl -m gabi:rw datei1
user$  setfacl -m g:docuteam:rw datei1
user$  setfacl -m kathrin:- datei1
```

Die Rechteliste von `getfacl` ist nun schon etwas länger. `ls` zeigt nun bei den Zugriffsrechten für Gruppenmitglieder die ACL-Maske an. Den Zugriffsbuchstaben folgt das Zeichen `+`, um darauf hinzuweisen, dass es ACL-Regeln gibt.

```
user$  getfacl datei1
# file: datei1
# owner: kofler
# group: kofler
user::rw-
user:gabi:rw-
user:kathrin:---
group::r--
group:docuteam:rw-
mask::rw-
other::r--
user$  ls -l datei1
-rw-rw-r--+ 1 kofler kofler ... datei1
```

Eine typische Anwendung von ACLs besteht darin, dass Sie einem bestimmten Benutzer Zugriff auf Ihre Dateien geben möchten, ohne die Dateien aber gleich allen anderen Benutzern (einer bestimmten Gruppe) zugänglich zu machen. Normalerweise müssten Sie nun den Administrator bitten, dass er eine neue Gruppe einrichtet, der Sie und der oder die weiteren Benutzer angehören, mit denen Sie die Dateien gemeinsam bearbeiten möchten. Mit ACL führen Sie einfach `setfacl -m benutzer:rw datei` aus.

ACL-Maske

Die ACL-Maske limitiert die Rechte, die durch ACL-Regeln gegeben werden. Wenn Sie die ACL-Maske beispielsweise auf `r` stellen, kann keine ACL-Regel einem Benutzer Schreib- oder Ausführrechte geben. Die ACL-Maske hat also Vorrang gegenüber den ACL-Regeln. Sie hat allerdings keinen Einfluss auf die Rechte, die sich durch die herkömmlichen Zugriffsrechte für den Besitzer der Datei bzw. für Gruppenmitglieder der Datei ergeben.

Bei jeder Änderung einer ACL-Regel durch `setfacl` wird die Maske automatisch so neu berechnet, dass alle anderen ACL-Regeln erfüllt werden können. Diese Maske wird von `getfacl` angezeigt und auch bei `ls -l` berücksichtigt.

Sie können die Maske durch `setfacl -m m:rwx datei` explizit einstellen und so die ACL-Rechte limitieren. Beachten Sie aber, dass Ihre eigene Maske nur so lange gilt, bis Sie eine neue ACL-Regel definieren. Dadurch wird die ACL-Maske automatisch neu berechnet (es sei denn, Sie verhindern das durch die Option `-n`).

Standard-ACL

Für Verzeichnisse können Sie einen zweiten Satz Regeln für die Standard-ACL festlegen. Die Standard-ACL steuert nicht den Zugriff auf das Verzeichnis, sondern gilt als Muster für neue Dateien. Jede Datei, die innerhalb des Verzeichnisses neu erzeugt wird, erbt gewissermaßen die Standard-ACL des Verzeichnisses. Bei vielen ACL-Anwendungen dient ein neues Verzeichnis mit einer geschickt gewählten Standard-ACL als Ausgangspunkt.

ACL-Kompatibilität

Das größte Hindernis für die weitere Verbreitung von ACLs besteht darin, dass viele Standardkommandos und nahezu alle Anwendungsprogramme ACLs einfach ignorieren. Wenn Sie eine Datei mit ACL-Regeln mit `cp` einfach kopieren, hat die Kopie alle ACL-Regeln verloren. Dasselbe gilt, wenn Sie die Datei mit einem Editor, mit OpenOffice oder mit Gimp öffnen und unter einem anderen Namen speichern. Bei `cp` schafft die Option `-p` Abhilfe, aber bei den meisten anderen Kommandos und Programmen fehlen vergleichbare Optionen bzw. ein ACL-konformes Verhalten.

Problematisch sind auch Backups. `tar` und `rsync` eliminieren ACL-Regeln. Das Dateisystem von CDs und DVDs sieht keine ACLs vor, sodass diese Informationen auch dort verloren gehen. Es bestehen zwei Auswege: Entweder setzen Sie statt `tar` die ACL-kompatible Variante `star` ein, oder Sie erzeugen vor dem Backup eine zusätzliche Textdatei, die die ACL-Regeln aller Dateien enthält. Nach dem Backup stellen Sie die ACL-Regeln anhand dieser Datei wieder her.

```
user$  getfacl -R --skip-base . > acl-backup     (ACL-Regeln speichern)
user$  setfacl --restore=acl-backup              (ACL-Regeln wiederherstellen)
```

Extended Attributes

setfattr und getfattr

Die folgenden Beispiele zeigen, wie Sie mit `setfattr` Attribute speichern und diese mit `getfattr` auslesen.

```
user$  touch datei2
user$  setfattr -n user.language -v de datei2
user$  setfattr --name=user.charset --value=utf8 datei2
user$  getfattr -d datei2
# file: datei2
user.charset="utf8"
user.language="de"
```

`getfattr` liefert normalerweise nur Attribute, deren Name mit »user.« beginnt. Wenn Sie andere Attribute sehen möchten, müssen Sie deren Namen durch `-n` oder deren Muster durch `-m` angeben.

```
user$  getfattr -n security.selinux -d tst
# file: tst
security.selinux="user_u:object_r:user_home_t:s0^000"
```

EA-Kompatibilität

Es gibt momentan leider kaum Programme, die Extended Attributes beim Kopieren, Archivieren etc. erhalten. Selbst `cp -p` ignoriert die Attribute. Bei Backups gehen Sie am besten ähnlich wie bei ACLs so vor, dass Sie vor dem Backup eine Datei mit allen EAs erstellen. Anhand dieser Datei können Sie die EAs später wiederherstellen.

```
user$  getfattr -R . > ea-backup          (Attribute speichern)
user$  setfattr --restore=ea-backup       (Attribute wiederherstellen)
```

Capabilities

Zu den interessantesten Anwendungen von Extended Attributes gehört die Möglichkeit, bei ausführbaren Dateien anzugeben, welche Operationen für das Programm zulässig sind, also welche »Capabilities« das Programm hat. Das würde es erlauben, weniger Programme mit dem Setuid-Bit zu kennzeichnen und auf diese Weise die Sicherheit von Linux-Distributionen zu erhöhen. Leider gibt es zurzeit keine gängige Distribution, die von diesen Möglichkeiten auch Gebrauch macht.

Voraussetzungen

Damit Capabilities funktionieren, müssen drei Voraussetzugen erfüllt sein:

- Es muss ein ausreichend aktueller Kernel vorliegen (zumindest Version 2.6.24), wobei beim Kompilieren die Capabilities-Optionen aktiviert wurden (`CONFIG_SECURITY_CAPABILITIES` und `CONFIG_SECURITY_FILE_CAPABILITIES`).
- Die Bibliothek `libcap` muss installiert sein (`/lib/libcap*` oder `/lib64/libcap*`).
- Das Dateisystem muss EAs unterstützen, weil die Capability-Daten in Form von EAs gespeichert werden. Bei `ext`-Dateisystemen muss daher die `mount`-Option `user_xattr` verwendet werden.

Bei den meisten Distributionen sind die ersten zwei Voraussetzungen standardmäßig erfüllt. Der dritte Punkt erfordert in der Regel eine Änderung von `/etc/fstab`. Weitere Grundlagen zu Capabilities können Sie hier nachlesen:

http://lwn.net/Articles/313047
http://www.friedhoff.org/posixfilecaps.html

getcap und setcap

Um Capabilities zu administrieren, benötigen Sie die Kommandos `getcap` und `setcap`. Sie müssen bei vielen Distributionen extra installiert werden (Paket `libcap-ng-utils`). Das folgende Beispiel demonstriert die Anwendung von Capabilities: Das Netzwerkkommando `ping` ist bei den meisten Distributionen mit dem `setuid`-Bit ausgestattet, sodass es von gewöhnlichen Benutzern verwendet werden kann. Sobald Sie dieses Bit löschen, kann nur noch `root` mit `ping` arbeiten:

```
root#  chmod u-s /bin/ping
user$  ping yahoo.de
ping: icmp open socket: Die Operation ist nicht erlaubt
```

Anstatt nun das unsichere `setuid`-Bit wieder zu setzen, reicht es auch, dem Kommando `ping` mit `setcap` den Zugriff auf Netzwerkfunktionen des Kernels zu geben. Mit `getcap` können Sie nachsehen, welche Capabilities ein Kommando hat.

```
root#  setcap cap_net_raw=ep /bin/ping
root#  getcap /bin/ping
/bin/ping = cap_net_raw+ep
```

15.8 Linux-Verzeichnisstruktur

Filesystem Hierarchy Standard

Ein typisches Unix-System besteht aus Tausenden von Dateien. Während der Entwicklung von Unix haben sich bestimmte Regeln herauskristallisiert, in welchen Verzeichnissen welche Dateien normalerweise gespeichert werden. Diese Regeln wurden an die Besonderheiten von Linux angepasst und in einem eigenen Dokument zusammengefasst: dem Filesystem Hierarchy Standard (FHS). Die meisten Linux-Distributionen halten sich bis auf wenige Ausnahmen an diesen Standard.

http://www.pathname.com/fhs

Die in diesem Abschnitt zusammengefassten Informationen geben eine erste Orientierungshilfe. Dabei wurde nicht nur der FHS berücksichtigt, sondern auch die Gepflogenheiten populärer Linux-Distributionen.

Das Dateisystem beginnt mit dem Wurzelverzeichnis. Dort befinden sich normalerweise keine Dateien, sondern nur Verzeichnisse:

`/bin` enthält elementare Linux-Kommandos zur Systemverwaltung, die von allen Benutzern ausgeführt werden können. Weitere Programme befinden sich in `/usr/bin`. Bei modernen Distributionen ist `/bin` einfach ein Link auf `/usr/bin`; die Trennung zwischen `/bin` und `/usr/bin` wurde damit aufgehoben.

`/boot` enthält Dateien, die zum Booten des Systems (im Regelfall durch GRUB) verwendet werden. Bei den meisten Distributionen befindet sich hier auch der Kernel.

`/dev` enthält alle Device-Dateien. Auf fast alle Hardware-Komponenten – etwa die serielle Schnittstelle oder eine Festplattenpartition – wird über sogenannte Device-Dateien zugegriffen. Diese werden dynamisch

durch das udev-System eingerichtet (siehe Abschnitt 15.9). Bei den meisten Distributionen befindet sich das /dev-Verzeichnis in einer RAM-Disk, d. h., der Inhalt des Verzeichnisses bleibt bei einem Neustart des Rechners nicht erhalten.

/etc enthält Konfigurationsdateien für das ganze System. Innerhalb von /etc gibt es eine Menge Unterverzeichnisse, die die Konfigurationsdateien in Gruppen ordnen – z. B. /etc/X11 für alle X-spezifischen Dateien. Viele Dateien aus /etc sind in den Konfigurationskapiteln dieses Buchs beschrieben. Werfen Sie auch einen Blick in das Stichwortverzeichnis (Buchstabe E)!

/home enthält die Heimatverzeichnisse aller regulären Linux-Anwender. Das Heimatverzeichnis ist jenes Verzeichnis, in dem sich der Anwender nach dem Einloggen automatisch befindet und auf dessen Dateien er uneingeschränkte Zugriffsrechte hat. Ein Sonderfall ist wie so oft root: Dessen Heimatverzeichnis lautet /root.

/lib[64] enthält einige gemeinsame Bibliotheken (Shared Libraries) oder symbolische Links darauf. Die Dateien werden zur Ausführung von Programmen benötigt. /lib/modules enthält Kernelmodule, die im laufenden Betrieb dynamisch aktiviert bzw. deaktiviert werden. Weitere Bibliotheken befinden sich in /usr/lib[64]. Das Verzeichnis /lib/firmware enthält die Firmware diverser Hardware-Komponenten (z. B. WLAN-Controller).

Bei aktuellen Distributionen ist /lib ein Link auf /usr/lib. Damit werden alle Bibliotheken zentral im /usr-Verzeichnis abgelegt.

/lost+found ist normalerweise leer. Enthält es doch Dateien, dann handelt es sich um Dateifragmente, die beim Versuch, das Dateisystem durch fsck zu reparieren, nicht mehr zugeordnet werden konnten. Mit anderen Worten: Es wurden Sektoren gefunden, aber es ist unklar, zu welcher Datei der Sektor einmal gehört hat. Anstatt derartige Dateifragmente einfach zu löschen, kopiert fsck diese in das lost+found-Verzeichnis.

fsck wird automatisch während des Systemstarts ausgeführt, wenn Linux nicht ordnungsgemäß beendet wurde (Stromausfall, Absturz etc.) oder wenn das Dateisystem längere Zeit nicht mehr überprüft wurde. Das Ziel von fsck ist es, das Dateisystem wieder in einen klar definierten Zustand zu bringen.

/media enthält Unterverzeichnisse wie cdrom oder usb-stick-name, an deren Stelle externe Dateisysteme eingebunden werden. Traditionell war

hierfür /mnt üblich, in den vergangenen Jahren hat sich stattdessen aber /media durchgesetzt. Bei neuen Distributionen gibt es mittlerweile wieder einen anderen Ort: externe Datenträger werden im Verzeichnis /run/media/benutzername/datenträgername in das Dateisystem integriert.

/opt ist für Zusatzpakete vorgesehen, wird von den gängigen Distributionen aber nur selten genutzt – vermutlich deswegen, weil unklar ist, wie sich Zusatzpakete von normalen Paketen unterscheiden.

/proc enthält Unterverzeichnisse für alle laufenden Prozesse. Es handelt sich hierbei nicht um echte Dateien! Das /proc-Verzeichnis spiegelt lediglich die Linux-interne Verwaltung der Prozesse wider.

/root enthält die Dateien des Benutzers root, also des Systemadministrators.

/run enthält bei vielen aktuellen Distributionen Dateien mit den Prozess-IDs sowie weiteren Informationen von manchen Systemdiensten. In der Vergangenheit wurden diese Dateien im Verzeichnis /var/run gespeichert.

Das Unterverzeichnis /run/lock/ enthält Locking-Dateien. Bei älteren Distributionen finden Sie die Locking-Dateien stattdessen in /var/lock.

Bei vielen Distributionen werden entweder das gesamte /run-Verzeichnis oder zumindest einzelne /run-Unterverzeichnisse in einer RAM-Disk abgelegt. Die überwiegend sehr kleinen Dateien in /run werden somit nie physikalisch auf einer Festplatte oder SSD gespeichert und gehen beim Neustart des Rechners verloren.

/sbin enthält Kommandos zur Systemverwaltung. Ein gemeinsames Merkmal aller darin gespeicherten Programme ist, dass sie nur von root ausgeführt werden dürfen. Bei modernen Distributionen ist /sbin ein Link auf /usr/sbin; alle Kommandos zur Systemverwaltung befinden sich nun in /usr/sbin.

/share enthält manchmal architekturunabhängige Dateien, also Dateien, die unabhängig vom Prozessor sind. Der korrekte Ort ist eigentlich /usr/share.

/srv enthält bei einigen Distributionen (Fedora, RHEL) Daten für Server-Prozesse, z. B. /srv/www für alle Apache-Dokumente oder /srv/ftp für FTP-Dateien.

/sys enthält ab Kernel 2.6 das sysfs-Dateisystem. Es liefert wie das proc-Dateisystem Informationen über den Zustand des Rechners.

/tmp enthält temporäre Dateien. Oft werden temporäre Dateien aber auch in /var/tmp gespeichert.

/usr enthält alle Anwendungsprogramme, das komplette X-System, die Quellcodes zu Linux etc. Der Inhalt dieses Verzeichnisses ändert sich normalerweise nur bei Paketinstallationen und Updates. Für veränderliche Dateien ist das Verzeichnis /var vorgesehen. Tabelle 15.9 gibt aber eine kurze Beschreibung der wichtigsten Unterverzeichnisse von /usr.

/var enthält veränderliche Dateien. Wichtige Unterverzeichnisse sind adm (distributionsabhängige Administrationsdateien), lock (Locking-Dateien zum Zugriffsschutz auf Devices), log (Logging-Dateien), mail (E-Mail-Dateien, oft auch in /var/spool/mail), run (Dateien mit Prozess-IDs von manchen Systemdiensten) und spool (zwischengespeicherte Druckdateien, News-Dateien etc.).

Verzeichnis	Inhalt
/usr/bin	ausführbare Programme
/usr/games	Spiele; evtl. Link auf /usr/share/games
/usr/include	C-Include-Dateien
/usr/lib[64]	diverse Libraries, außerdem zahllose Unterverzeichnisse für C-Compiler, diverse andere Programmiersprachen, große Programmpakete wie emacs oder LaTeX etc.
/usr/local	Anwendungen und Dateien, die nicht unmittelbar zur Linux-Distribution gehören oder später installiert wurden
/usr/sbin	nur von root ausführbare Programme
/usr/share	architekturunabhängige Daten (z. B. Emacs-Lisp-Dateien, Ghostscript-Zeichensätze etc.), Dokumentation (/usr/share/doc)
/usr/src	Quellcode zu Linux und eventuell zu anderen Programmen)

Tabelle 15.9 /usr-Verzeichnisse

Die grundsätzliche Struktur der Verzeichnisse auf Wurzelebene ist also recht gut zu verstehen. Die Probleme beginnen erst mit der Unterteilung von /usr und /var in zahllose Unterverzeichnisse. Prinzipiell werden dabei viele Verzeichnisse gleich benannt wie in der Wurzel-Ebene – etwa bin für ausführbare Programme.

Dabei tritt das Problem auf, dass es mehrere Gruppen ausführbarer Programme gibt: textorientierte Kommandos, X-Programme etc. In der Vergangenheit gab es für diese Programmgruppen einzelne Verzeichnisse, z. B. /usr/bin/X11 für Programme mit

grafischer Benutzeroberfläche. Mittlerweile bemühen sich die meisten Distributionen, möglichst alle Programme in *ein* Verzeichnis zu installieren, also nach `/usr/bin`. Symbolische Links stellen die Kompatibilität zu vergangenen Standards her.

15.9 Device-Dateien

Im Linux-Dateisystem werden nicht nur Dateien und Verzeichnisse verwaltet, sondern auch sogenannte Devices. Dabei handelt es sich um speziell gekennzeichnete Dateien, in denen keine Daten gespeichert werden, sondern die vielmehr eine Verbindung zum Linux-Kernel herstellen.

Major und Minor Device Number

Devices ermöglichen den Zugriff auf viele Hardware-Komponenten des Rechners, also etwa auf Festplatten, Diskettenlaufwerke, serielle und parallele Schnittstellen, den Arbeitsspeicher (RAM) etc. Devices sind durch drei Informationen charakterisiert: die Major Device Number, die Minor Device Number und den Typ des Zugriffs (block- oder zeichenorientiert).

Die Major Device Number gibt an, welcher Treiber des Linux-Kernels für die Verwaltung zuständig ist. Die meisten Treiber sind mit ihrer Major Device Number auf der folgenden Seite aufgelistet:

http://www.kernel.org/doc/Documentation/devices.txt

Bei vielen Treibern dient die Minor Device Number zur Differenzierung zwischen verschiedenen (verwandten) Einzelgeräten – etwa beim Treiber für Festplatten zwischen unterschiedlichen Partitionen.

Der Zugriffstyp gibt an, ob die Geräte gepuffert sind (das ist bei allen blockorientierten Geräten wie Festplatten etc. der Fall) oder nicht (zeichenorientierte Geräte wie serielle oder parallele Schnittstellen).

Wenn Sie mit `ls -l` das Inhaltsverzeichnis von `/dev` betrachten, werden statt der Dateigröße die Device-Nummern (Major und Minor) ausgegeben. Das erste Zeichen der Zugriffsbits lautet `b` oder `c` (block- oder zeichenorientiert).

```
user$  ls -l /dev/sda?
brw-rw---- 1 root root 8, 1 2010-02-02 10:39 /dev/sda1
brw-rw---- 1 root root 8, 2 2010-02-02 10:39 /dev/sda2
...
```

Interna

Linux-intern befinden sich im `/dev`-Verzeichnis nur sogenannte Inodes; das sind die kleinsten Verwaltungseinheiten eines Dateisystems, aber keine richtigen Dateien mit Inhalt. Neue Device-Dateien können mit dem Kommando `mknod` eingerichtet werden. In der Praxis ist das aber selten notwendig, weil sich das `udev`-System automatisch darum kümmert.

Die Major und Minor Device Number werden seit Kernel 2.6 zu einer 64-Bit-Zahl zusammengesetzt. Bis Kernel 2.4 waren dafür nur 32 Bit vorgesehen.

Auf viele Devices dürfen aus Sicherheitsgründen nur `root` bzw. die Mitglieder einer bestimmten Gruppe zugreifen. Um auch anderen Benutzern Zugriff auf diese Devices zu ermöglichen, fügen Sie den Benutzer dieser Gruppe hinzu.

Einige Device-Dateien haben eine besondere Funktion: So dient `/dev/null` als »schwarzes Loch«, an das Daten gesendet werden können, die dort für immer verschwinden – etwa zur Umleitung von Kommandoausgaben, die nicht angezeigt werden sollen. `/dev/zero` ist eine unerschöpfliche Quelle von 0-Bytes, die manchmal dazu verwendet wird, Dateien bis zu einer vorgegebenen Größe mit Nullen zu füllen. `/dev/random` und `/dev/urandom` liefern zufällige Zahlen.

udev-System

In der Vergangenheit erzeugten Distributionen während der Installation eine riesige Anzahl von Device-Dateien. Bei Red Hat 9 gab es beispielsweise beinahe 8000 derartige Dateien! Tatsächlich genutzt werden höchstens ein paar Hundert Dateien – aber es sind eben auf jedem Rechner, je nach Hardware-Ausstattung, andere Device-Dateien.

Abhilfe schafft seit Kernel 2.6 das `udev`-System. Das Hintergrundprogramm `udevd` erkennt alle mit dem Rechner verbundenen Hardware-Komponenten und erzeugt die erforderlichen Device-Dateien nach Bedarf. `udevd` wird am Beginn des Init-V-Prozesses gestartet. Die Konfiguration erfolgt durch die Dateien des Verzeichnisses `/etc/udev`.

Das `udev`-System funktioniert an sich ausgezeichnet und kommt auch mit externen Festplatten, Memory-Sticks und diversen anderen Hardware-Komponenten zurecht, die im laufenden Betrieb angeschlossen und wieder gelöst werden. Das größte Problem des `udev`-Systems besteht darin, dass das Einrichten der Device-Dateien während des Rechnerstarts relativ lange dauert, unter Umständen mehrere Sekunden. Da ein Teil der Device-Dateien für den weiteren Verlauf des Starts erforderlich sind, insbesondere zum Zugriff auf Festplatten und Netzwerkschnittstellen, lässt sich `udev` nur schwer auf später verschieben bzw. im Hintergrund ausführen.

Im Zuge der Bemühungen, Linux schneller zu starten, gibt es deswegen Überlegungen, `udev` durch ein effizienteres System zu ersetzen oder zumindest teilweise zu einer statischen Konfiguration zurückzukehren. Das im folgenden Artikel beschriebene `devtmpfs`-System steht ab Kernel 2.6.32 zur Verfügung. Es bleibt abzuwarten, wie weit die Distributionen es nutzen werden.

http://lwn.net/Articles/331818

Device	Bedeutung
/dev/cdrom	Link auf das CD-ROM-Device
/dev/console	das gerade aktive virtuelle Terminal
/dev/disk/*	zusätzliche Links auf Festplatten- und Partitions-Devices
/dev/dri/*	Direct Rendering Infrastructure (3D-Grafik mit X)
/dev/dsp*	Zugang zur Soundkarte (Digital Sampling Device)
/dev/fb*	Frame Buffer (Grafikkarte)
/dev/input/*	Maus
/dev/kbd	Tastatur (PS/2)
/dev/kmem	Speicher (RAM) im Core-Format (für Debugger)
/dev/lp*	parallele Schnittstellen für Drucker etc.
/dev/mapper	Mapping-Dateien für LVM, Krypto-Container etc.
/dev/md*	Meta-Devices (RAID etc.)
/dev/mem	Speicher (RAM)
/dev/mixer*	Zugang zur Soundkarte
/dev/psaux	PS/2-Maus
/dev/port	IO-Ports
/dev/pts/*	virtuelle Terminals gemäß Unix 98
/dev/ptyp*	virtuelle Terminals unter X (Master)
/dev/ram	RAM-Disk
/dev/raw1394	direkter Zugriff auf Firewire-Geräte
/dev/sd*	SCSI/SATA/USB/Firewire-Festplatten
/dev/scd*	SCSI/SATA/USB/Firewire-CD/DVD-Laufwerke
/dev/shm	POSIX Shared Memory
/dev/snd	ALSA-Sound (Link auf /proc/asound/dev)
/dev/scd*	SCSI/SATA/USB/Firewire-CD/DVD-Laufwerke
/dev/tty*	virtuelle Terminals im Textmodus
/dev/ttyp*	virtuelle Terminals unter X (Slave)
/dev/ttyS*	serielle Schnittstellen (Modem, Maus etc.)
/dev/usb/*	USB-Geräte (siehe auch /proc/bus/usb)

Tabelle 15.10 Wichtige Device-Dateien

Kapitel 16
Prozessverwaltung

Dieses Kapitel beschreibt, wie Linux mit Prozessen umgeht. Im Verlauf dieses Kapitels lernen Sie,

- welche Möglichkeiten es gibt, Programme zu starten und (zur Not auch gewaltsam) wieder zu beenden,
- wie Sie ein Programm als gewöhnlicher Benutzer ausführen, als wären Sie `root`,
- was Dämonen sind und
- wie Sie Programme zu bestimmten Zeiten automatisch starten können.

16.1 Prozesse starten, verwalten und stoppen

Programme, Kommandos, Prozesse, Tasks

In diesem Kapitel ist überwiegend von Prozessen die Rede. Ein Prozess ist auf Betriebssystemebene für die Ausführung eines Programms oder Kommandos verantwortlich. Das klingt nach einer eher trivialen Aufgabe; da aber in der Regel eine Menge Programme und Hintergrunddienste parallel laufen, ist es gar nicht so einfach, die Rechenzeit zwischen allen Programmen sinnvoll zu verteilen.

Programme und Kommandos

Ein Programm bzw. ein Kommando ist eigentlich nur eine ausführbare Datei. Eine Programmdatei unterscheidet sich von anderen Dateien also dadurch, dass das Zugriffsbit `x` gesetzt ist.

Linux-intern gibt es keine Unterscheidung zwischen einem Programm wie Firefox oder einem Kommando wie `ls`. Umgangssprachlich werden textorientierte Programme wie `ls` aber oft als Kommandos bezeichnet.

Erst durch den Start einer gleichsam leblosen Programmdatei wird diese zu einem lebendigen Prozess, der vom Linux-Kernel verwaltet wird. So gesehen müsste die Überschrift dieses Abschnitts eigentlich lauten: *Programme und Kommandos starten, Prozesse verwalten und stoppen*.

*.exe-Dateien

Hin und wieder taucht die Frage auf, wo denn unter Linux die *.exe-Dateien sind. Bis vor einigen Jahren hieß die richtige Antwort: Es gibt keine *.exe-Dateien. Ausführbare Programme sind durch das Zugriffsbit x gekennzeichnet; die von Windows bekannte Dateikennung *.exe ist somit überflüssig.

Mittlerweile ist diese Antwort insofern nicht mehr ganz richtig, als es auf vielen Linux-Systemen tatsächlich vereinzelte *.exe-Dateien gibt. Dabei handelt es sich um Programme, die in der Programmiersprache C# entwickelt wurden und die zur Ausführung auf die Mono-Bibliothek zurückgreifen. Die Mono-Bibliothek ist wiederum eine Open-Source-Implementierung des .NET Frameworks von Microsoft.

Programme starten

Programmstart unter X

Unter X starten Sie Programme im Regelfall über ein Menü oder durch das Anklicken eines Icons. Desktop-Systeme wie KDE, Gnome oder Unity bieten mit den Tastenkürzeln Alt+F2 oder ⊞ eine weitere Möglichkeit, Programme rasch zu starten.

Textkonsole, Terminalfenster

Alternativ können Sie Programme auch in einem Terminalfenster oder in einer Textkonsole starten. Dazu geben Sie einfach den Namen des Programms ein und drücken ↵. Gerade Linux-Profis wählen oft diesen Weg, weil es schneller geht, ein paar Buchstaben einzutippen als das Programm in verzweigten Menüs zu suchen.

Normalerweise reicht es aus, wenn Sie einfach den Namen des Programms angeben. Der Shell-Interpreter sucht das Programm dann in allen Verzeichnissen, die in der Umgebungsvariable PATH angegeben sind. Die folgenden Zeilen zeigen eine typische Einstellung dieser Variable:

```
user$  echo $PATH
  /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

Wenn Sie ein Programm starten möchten, das sich in keinem dieser Verzeichnisse befindet, müssen Sie den vollständigen Pfad angeben. Das gilt auch für Programme im gerade aktuellen Verzeichnis! Hier wird der Pfad einfach durch einen Punkt angegeben, also beispielsweise ./meinprogramm.

Vordergrund- und Hintergrundprozesse

Wenn Sie Programme unter X per Menü starten, laufen diese selbstverständlich als sogenannte Hintergrundprozesse, ohne sich gegenseitig zu behindern. Sie können also weitere Programme starten, ohne auf das Ende der bisher gestarteten Programme warten zu müssen.

Ganz anders ist das Verhalten, wenn Sie ein Programm in einer Textkonsole bzw. einem Terminal ausführen. Das Programm wird als Vordergrundprozess gestartet.

Bevor Sie im Terminal das nächste Kommando eingeben können, müssen Sie auf das Ende des zuletzt gestarteten Programms warten.

Aber auch in Textkonsolen oder Shell-Fenstern können Sie Programme im Hintergrund starten. Dazu geben Sie einfach am Ende des Kommandos das Zeichen & an:

```
user$  emacs &
```

Vom Vordergrund in den Hintergrund

Wenn Sie & vergessen haben, können Sie das Programm auch nachträglich in einen Hintergrundprozess umwandeln. Unterbrechen Sie die Programmausführung mit Strg+Z, und setzen Sie das Programm mit bg fort:

```
user$  emacs
<Strg>+<Z>
+  Stopped  emacs
user$  bg
+ emacs &
```

Wenn Sie statt bg das Kommando fg verwenden, wird das Programm als Vordergrundprozess fortgesetzt.

Bei manchen Kommandos stören diverse Textausgaben bei der Hintergrundausführung. Diese können Sie aber leicht unterdrücken, indem Sie sie nach /dev/null umleiten. Beispielsweise wird durch das folgende Kommando ein USB-Stick im Hintergrund formatiert:

```
root#  mkfs.ext4 /dev/sdc > /dev/null &
```

Liste aller laufenden Prozesse (ps, top)

ps

Eine Liste der zurzeit laufenden Prozesse können Sie sehr einfach mit ps erzeugen. Ohne Optionen zeigt ps nur Ihre eigenen Prozesse an – und nur solche, die aus Textkonsolen bzw. Shell-Fenstern gestartet wurden. ps kann durch zahllose Optionen gesteuert werden, wobei viele Optionen ohne das sonst übliche vorangestellte Minuszeichen angegeben werden. Wenn der Prozessname in eckigen Klammern steht, handelt es sich um einen Prozess des Kernels. Im folgenden Beispiel wurde die Liste der Prozesse aus Platzgründen stark gekürzt. Auf einem typischen Linux-System mit grafischer Benutzeroberfläche laufen normalerweise deutlich mehr als 100 Prozesse zugleich.

```
user$  ps ax
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss     0:00 init [2]
    2 ?        S      0:00 [kthreadd]
    3 ?        S      0:00 [ksoftirqd/0]
 ...
```

```
 3064 pts/2    S      0:39 emacs command.tex
 3151 pts/2    S+     1:23 /bin/sh ./lvauto
 3735 pts/4    S      0:00 su -l
 3740 pts/4    S+     0:00 -bash
```

top Praktischer als `ps` ist meist `top`: Dieses Kommando ordnet die Prozesse danach, wie sehr sie die CPU belasten, und zeigt die gerade aktiven Prozesse zuerst an. Das Programm gibt auch einen Überblick über den aktuellen Speicherbedarf etc. Die Prozessliste wird alle paar Sekunden aktualisiert, bis das Programm mit Q beendet wird. Die folgenden Zeilen zeigen einen Webserver nahezu im Leerlauf:

```
top - 20:50:38 up 11 days, 12:18,  1 user,  load average: 0.10, 0.09, 0.08
Tasks: 114 total,   1 running, 113 sleeping,   0 stopped,   0 zombie
Cpu(s):  2.6%us,  0.2%sy,  0.0%ni, 96.8%id,  0.4%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:   4049808k total,  1580060k used,  2469748k free,   203396k buffers
Swap:   521212k total,        0k used,   521212k free,   804400k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
32601 www-data  20   0  346m  32m 4296 S    5  0.8   0:00.15 apache2
32592 www-data  20   0  344m  31m 4324 S    3  0.8   0:00.47 apache2
  851 mysql     20   0 1403m  53m 7948 S    0  1.4   6:40.10 mysqld
    1 root      20   0 24336 2184 1272 S    0  0.1   0:01.07 init
  ...
```

Der Wert in der PID-Spalte gibt die Prozessnummer an. Wenn Sie diese Nummer kennen, können Sie außer Kontrolle geratene Programme oder Hintergrundprozesse mit dem Kommando `kill` gewaltsam stoppen.

Prozesse können verschiedene Zustände annehmen. Die zwei häufigsten Zustände sind R (*running*) und S (*sleeping*, das Programm hat also gerade nichts zu tun und wartet auf Eingaben). Programme können auch vorübergehend unterbrochen werden und weisen dann den Zustand T (*stopped*) auf.

`top` nimmt auch interaktiv Kommandos entgegen. Damit können Sie Prozesse stoppen (K, `kill`) oder ihre Priorität verändern (R, `renice`).

htop Eine wesentlich komfortablere Alternative zu `top` ist das Kommando `htop`, das bei den meisten Distributionen separat installiert werden muss. Es erlaubt unter anderem ein horizontales und vertikales Scrollen in der Prozessliste.

iotop Wenn Sie nicht die CPU- und Speicherauslastung, sondern die Zugriffe auf Festplatten und andere Datenträger verfolgen möchten, starten Sie statt `top` das Kommando `iotop`. Mit der Option `-o` schränken Sie die Ausgabe auf Prozesse ein, die tatsächlich IO-Aktivität verursachen. `-u` beschränkt die Ausgabe auf eigene Prozesse. `iotop` ist Bestandteil des gleichnamigen Pakets, das in der Regel extra installiert werden muss.

Grafische Varianten zu top

Zu den textbasierten Kommandos `top` und `htop` gibt es natürlich auch grafische Alternativen, z. B. `ksysguard` (KDE) oder `gnome-system-monitor` (Gnome, siehe Abbildung 16.1).

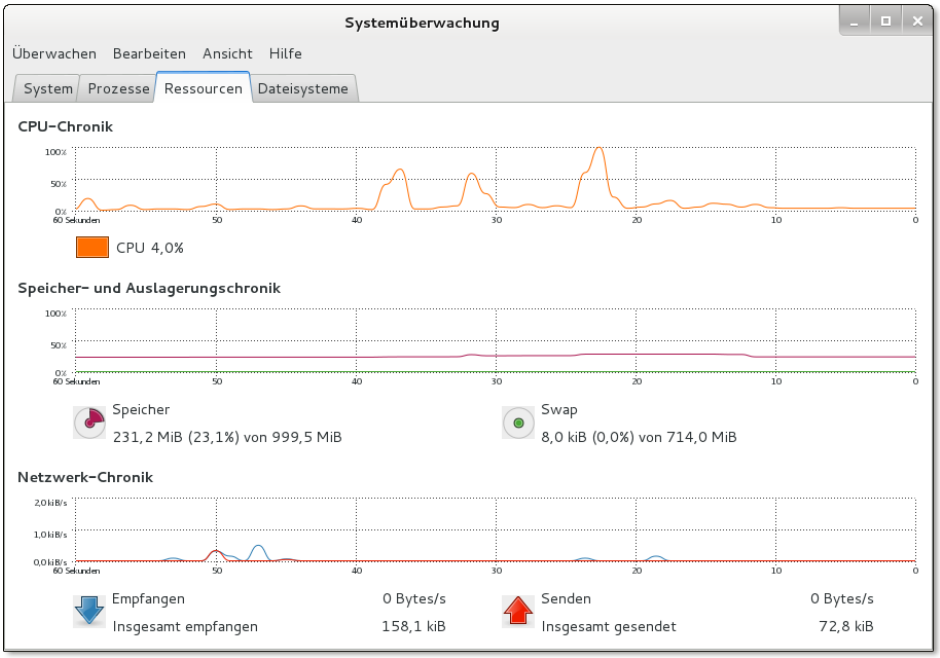


Abbildung 16.1 Prozessübersicht mit gnome-system-monitor

Ungleich mehr Darstellungs- und Konfigurationsmöglichkeiten bietet Conky. Dieses Programm zeigt Daten über die laufenden Prozesse an, aber auch alle erdenklichen anderen Statusinformationen, vom Datum bis hin zu den neuesten RSS-Feed-Eingängen. Wenn die Pakete `lm-sensors` und `hddtemp` installiert sind, kann Conky auch die CPU- und Festplattentemperatur anzeigen. Die Darstellung erfolgt direkt auf dem Desktop-Hintergrund, also nicht in einem eigenen Fenster. Die Konfiguration erfolgt durch die Textdatei `.conkyrc`.

In der Standardkonfiguration zeigt Conky relativ spärliche Informationen in einem schwarzen Rechteck links oben im Bildschirm an. In dieser Form bietet Conky wenig Vorteile im Vergleich zu einem Terminal mit `top`. Im Internet finden Sie aber Conky-Konfigurationen, die wahre Kunstwerke sind und aus einem faden Desktop-Hintergrund eine originelle und nützliche Informationszentrale machen. Werfen Sie einen Blick auf die folgende Webseite mit 16 Beispielkonfigurationen:

http://applyinglife.blogspot.co.at/2013/03/16-awesome-conky-configurations.html

Das manuelle Einrichten einer Conky-Konfiguration ist leider mit viel Arbeit verbunden. Viele der im Internet angebotenen Konfigurationsdateien sind veraltet oder passen nur zu einer speziellen Distribution. Auf Debian- und Ubuntu-Systemen hilft der Conky Manager bei der Installation fertiger Conky-Konfiguration:

http://teejeetech.blogspot.co.at/p/conky-manager.html

Prozessnummer ermitteln

Wenn Sie den Programmnamen wissen und die dazugehörende Prozessnummer (PID) ermitteln möchten, hilft `pidof`. Wenn es mehrere Prozesse mit dem gleichen Namen gibt, liefert `pidof` eine ganze Liste von Nummern:

```
root#  pidof nscd
1777 1776 1775 1774 1765 1763 1753
```

Manchmal ist es auch nützlich, festzustellen, welche Programme auf eine bestimmte Datei oder ein Verzeichnis zugreifen. Die entsprechenden Prozessnummern können Sie mit `fuser` feststellen. Ein Verzeichnis gilt auch dann als benutzt, wenn darin ein Programm gestartet wurde. Das folgende Kommando zeigt, dass die Shell `bash` das Verzeichnis `/media/dvd` nutzt:

```
root#  fuser -v /media/dvd
                     USER        PID ACCESS COMMAND
/media/dvd           kofler     2183 ..c..  bash
                     root     Kernel mount  /media/dvd
```

Beachten Sie, dass ein Dateizugriff nur festgestellt werden kann, wenn das Programm die Datei wirklich geöffnet hat. Das ist bei einem Texteditor beispielsweise nicht der Fall: Der Editor hat die Datei zum Laden geöffnet, dann aber wieder geschlossen. Zum Speichern öffnet er die Datei wiederum nur für kurze Zeit.

PID-Dateien

Manche Hintergrundprozesse speichern im Verzeichnis `/var/run` eine PID-Datei, z. B. `/var/run/httpd.pid`. Diese Datei enthält in der ersten Zeile die Prozessnummer; weitere Zeilen können Zusatzinformationen enthalten, z. B. die Netzwerkschnittstelle. PID-Dateien ermöglichen das gezielte Beenden eines bestimmten Prozesses durch das Init-System, und zwar auch dann, wenn es mehrere gleichnamige Prozesse gibt.

Prozesshierarchie

Intern wird mit jedem Prozess auch die PID-Nummer des Elternprozesses gespeichert. Diese Information ermöglicht die Darstellung eines Prozessbaums, an dessen Spitze immer der Prozess `init` steht. `init` ist das erste Programm, das unmittelbar nach dem Laden des Kernels gestartet wird (siehe Kapitel 27, »Das Init-System«). Die Darstellung der Prozesshierarchie gelingt am einfachsten mit dem Kommando `pstree`. Mit der Option `-h` werden die Elternprozesse zum gerade laufenden Prozess fett hervorgehoben. In Abbildung 16.2 wurde `pstree` von einer `bash`-Shell in einem `gnome-terminal`-Fenster ausgeführt.

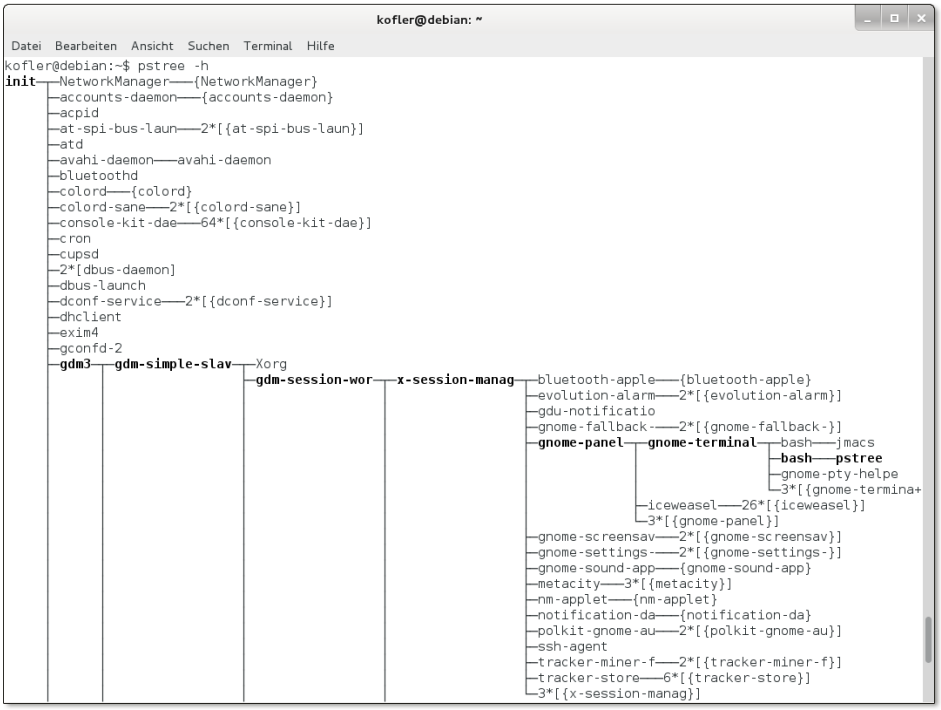


Abbildung 16.2 Prozessübersicht mit pstree

Prozesse gewaltsam beenden (kill, xkill)

Normalerweise endet ein Prozess mit dem Programmende. Aber leider kommt es auch unter Linux vor, dass Programme Fehler enthalten, sich nicht mehr stoppen lassen und womöglich immer mehr Speicher und CPU-Kapazität beanspruchen. In solchen Fällen muss der Prozess gewaltsam beendet werden. Bei textorientierten Kommandos hilft in den meisten Fällen einfach Strg+C. Damit wird das Programm sofort beendet.

kill

Das Kommando `kill` versendet Signale an einen laufenden Prozess, der durch die PID-Nummer spezifiziert wird. (Diese Nummer können Sie mit `top` oder `ps` ermitteln.) Um ein Programm »höflich« zu beenden, wird das Signal 15 verwendet. (`kill` verwendet dieses Signal per Default.) Hilft das nicht, muss das Signal 9 eingesetzt werden (hier für den Prozess 2725):

```
user$  kill -9 2725
```

`kill` kann nur für eigene Prozesse verwendet werden. Nur `root` darf auch fremde Prozesse beenden.

top Auch mit `top` können Sie Prozesse beenden: Geben Sie einfach K und anschließend die Prozessnummer und das gewünschte Signal ein!

killall `killall` ist insofern bequemer, als keine Prozessnummer, sondern der Programmname angegeben werden kann. Allerdings werden nun *alle* Prozesse dieses Namens beendet.

```
root# killall -9 firefox
```

xkill Unter X geht es noch bequemer. Starten Sie in einem Shell-Fenster `xkill`, und klicken Sie einfach das Fenster des Programms an, das Sie beenden wollen. An den Prozess wird wiederum das Signal 9 gesandt.

Unter KDE können Sie `xkill` auch mit Strg+Alt+Esc starten. Wenn das irrtümlich passiert, können Sie `xkill` mit Esc abbrechen.

Hartnäckige Fälle Manchmal wird durch `xkill` zwar das Fenster geschlossen, der Prozess oder Teile davon laufen aber weiter. Vergewissern Sie sich mit `top` bzw. mit `ps`, dass das Programm wirklich beendet ist. Zur Not müssen Sie mit `kill -9 n` nachhelfen.

Blockierte Tastatur oder Maus Wirklich unangenehm wird es, wenn ein X-Programm nicht nur hängen bleibt, sondern dabei auch den Tastatur- und Maus-Fokus an sich reißt oder X sonstwie blockiert. Der Rechner reagiert dann auf keine Eingaben mehr. In solchen Fällen hilft manchmal die magische Tastenkombination Strg+Alt+F1 weiter, mit der der Wechsel in die erste Textkonsole erfolgt. Dort können Sie sich einloggen und das betreffende Programm mit `top` suchen und beenden.

Wenn die Tastatur vollständig blockiert ist, besteht immer noch die Möglichkeit, sich über ein Netzwerk via `ssh` einzuloggen und `kill` auf diese Weise auszuführen. Diese Variante ist natürlich nur möglich, wenn Sie in einem lokalen Netz arbeiten und auf dem lokalen Rechner `sshd` läuft.

Sollte X selbst nach dem Ende des Programms blockiert bleiben, können Sie versuchen, auch X gewaltsam zu beenden bzw. schließlich `shutdown` auszuführen. All diese Varianten sind besser als das Drücken der Reset-Taste, was zu Datenverlusten führen kann!

Prozessgröße beschränken Bei Programmen, die über eine Shell gestartet werden (etwa bei allen Kommandos, die in einem Shell-Fenster ausgeführt werden), können Sie mit dem Shell-Kommando `ulimit` den maximalen Speicherverbrauch, die maximale Größe erzeugter Dateien etc. begrenzen. `ulimit` wird üblicherweise in `/etc/profile` eingestellt.

Verteilung der Rechenzeit (nice, renice, ionice)

Im alltäglichen Betrieb von Linux ist die Rechenkapazität meist mehr als ausreichend, um alle laufenden Prozesse ohne Verzögerungen auszuführen. Wenn Linux gerade mit rechenaufwendigen Prozessen beschäftigt ist – z. B. während des Kompilierens eines umfangreichen Programms –, versucht es, die zur Verfügung stehende Rechenzeit gerecht an alle Prozesse zu verteilen.

In manchen Fällen ist es sinnvoll, einem Prozess bewusst mehr oder weniger Rechenzeit zuzuteilen. Dazu dient das Kommando `nice`, mit dem Programme mit reduzierter oder erhöhter Priorität gestartet werden können. Dazu wird an `nice` die gewünschte Priorität übergeben, die von 19 (ganz niedrig) bis -20 (ganz hoch) reicht. Per Default werden Prozesse mit der Priorität 0 gestartet. Im folgenden Beispiel wird ein Backup-Programm mit niedrigerer Priorität gestartet, damit es keine anderen Prozesse beeinträchtigt. (Es ist ja egal, ob das Backup ein paar Sekunden länger dauert.)

```
user$  nice -n 10 sichere
```

renice

Mit `renice` kann auch die Priorität von bereits laufenden Prozessen geändert werden. Als Parameter muss die Prozess-ID angegeben werden, die vorher mit `top` oder `ps` ermittelt wurde. Details zu `renice` finden Sie auf der `man`-Seite. Auch `top` (Kommando R) ist in der Lage, interaktiv die Priorität eines Prozesses zu verändern. Allerdings kann nur `root` Programme mit einer höheren Priorität als 0 starten bzw. die Priorität eines bereits laufenden Prozesses erhöhen.

ionice

Bei Rechnern mit Multi-Core-CPUs ist oft die Festplatte der limitierende Faktor bei der Ausführung von Programmen. Wenn Sie vermeiden möchten, dass beispielsweise ein Backup-Script die gesamte I/O-Kapazität des Rechners für sich beansprucht und damit andere, vielleicht zeitkritischere Prozesse bremst, können Sie es mit `ionice` mit reduzierter I/O-Priorität ausführen. Das folgende Kommando liest ein Logical Volume aus, komprimiert seinen Inhalt und speichert ihn in einer Image-Datei:

```
root#  ionice -c 3 cat /dev/vg1/snap | lzop -c > /backup/image.lzo
```

Threading (NPTL)

Linux kann nicht nur mehrere Prozesse parallel ausführen, sondern unterscheidet auch innerhalb eines Prozesses zwischen Teilprozessen (Threads). Vor allem Server-Anwendungen verteilen ihre Funktionen oft auf mehrere Threads. Das steigert die Performance insbesondere dann, wenn mehrere CPUs oder mehrere CPU-Cores zur Verfügung stehen. Bei der Verwaltung und Kommunikation der Threads helfen Kernelfunktionen. Seit Kernel 2.6 unterstützt die *Native POSIX Thread Library* Threads gemäß dem POSIX-Standard.

Ein- und Ausgabeumleitung, Pipe

Fast alle textorientierten Kommandos erwarten Eingaben über den sogenannten Standardeingabekanal (per Default die Tastatur) und senden Ausgaben an den Standardausgabekanal; in einem Terminal wird der resultierende Text einfach angezeigt. Sowohl die Ein- als auch die Ausgabe lassen sich umleiten, wodurch sich viele Möglichkeiten ergeben. Beispielsweise speichert das folgende Kommando die Liste aller Dateien des Verzeichnisses `xy` in der Datei `z`:

```
user$  ls xy > z
```

Durch sogenannte Pipes kann die Ausgabe eines Kommandos als Eingabe für das nächste Kommando verwendet werden. Beim folgenden Beispiel filtert `grep` aus der Liste aller installierten Pakete diejenigen heraus, die die Zeichenkette »mysql« in beliebiger Groß- und Kleinschreibung enthalten. `sort` sortiert diese Liste schließlich.

Mit anderen Worten: Die Ausgaben des Kommandos `rpm` werden dank des Zeichens `|` an das zweite Kommando `grep` weitergeleitet und dessen Ausgaben mit dem zweiten Zeichen `|` an `sort`. Mehr Details und Beispiele zur Ein- und Ausgabeumleitung sowie zur Verwendung von Pipes finden Sie in Abschnitt 14.4.

```
user$  rpm -qa | grep -i mysql | sort
mysql-5.1.32-1.fc11.i586
mysql-connector-java-3.1.12-7.fc11.i586
...
```

16.2 Prozesse unter einer anderen Identität ausführen (su)

Bei der Programmausführung durch gewöhnliche Benutzer gibt es zwei Einschränkungen:

- Gewöhnliche Benutzer dürfen nur die Prozesse ausführen, bei denen die Zugriffsrechte (Besitzer, Gruppe, r- und x-Zugriffsbits) dies zulassen. Bei gewöhnlichen Programmen ist das keine Einschränkung. Es gibt aber beispielsweise im Verzeichnis `/usr/sbin` einige Kommandos zur Systemadministration, die nur von `root` gestartet werden können.
- Prozesse gehören gleichsam dem Benutzer, der sie gestartet hat. Das bedeutet, dass der Prozess auf die gleichen Dateien zugreifen darf wie der Benutzer. Umgekehrt formuliert: Dateien, die Sie als Benutzer nicht verändern dürfen, dürfen auch nicht von Programmen verändert werden, die Sie starten. Vom Prozess neu erzeugte Dateien gehören ebenfalls dem Benutzer, der das Programm gestartet hat (siehe auch Abschnitt 15.6).

Als gewöhnlicher Benutzer können Sie aus diesen Gründen viele administrative Arbeiten nicht durchführen. Die offensichtlich einfachste Lösung besteht darin, sich als `root` einzuloggen. Ich habe in diesem Buch aber schon mehrfach darauf hingewiesen, dass es keine gute Idee ist, ständig als `root` zu arbeiten: Die Gefahr ist einfach zu groß, dass Sie irrtümlich Schaden anrichten. Aus diesem Grund sperren manche Distributionen den `root`-Login vollständig. So ist unter Ubuntu ein direkter `root`-Login unmöglich.

Dieser Abschnitt beschreibt, wie Sie mit `su` bzw. `ssh` dennoch administrative Tätigkeiten durchführen können, ohne sich als gewöhnlicher Benutzer auszuloggen. Der nächste Abschnitt zeigt eine alternative Vorgehensweise mit `sudo`, die sich vor allem unter Ubuntu bewährt hat. Abschnitt 16.4 präsentiert das Programm PolicyKit, das ganz neue Wege bei der Ausführung von `root`-Aufgaben geht.

Wie so oft gäbe es mehr zu schreiben, als hier Platz hat. Weitere Informationsquellen sind das Security-HOWTO und das Remote-X-Mini-HOWTO. Beide Dokumente sind zwar schon ziemlich alt, die darin enthaltenen Tipps sind aber noch immer gültig:

http://www.tldp.org/HOWTO/Security-HOWTO/index.html
http://www.tldp.org/HOWTO/Remote-X-Apps.html

su

In vielen Fällen geht es nur darum, rasch ein Kommando als `root` auszuführen – da wäre ein Verlassen von X sehr unkomfortabel. Die einfachste Möglichkeit, innerhalb eines X-Shell-Fensters den Benutzer zu ändern, bietet das Kommando `su` *name*. Wenn Sie das Kommando nicht als `root` ausführen, werden Sie nach dem Passwort des jeweiligen Anwenders gefragt. Innerhalb des Terminals können Sie jetzt Kommandos unter dem geänderten Namen ausführen, bis Sie durch `exit` oder Strg+D zurück in den Normalmodus wechseln.

Die folgenden Zeilen zeigen, wie ein gewöhnlicher Benutzer sich kurz als `root` anmeldet, als `root` eine Festplattenpartition in den Verzeichnisbaum einbindet und sich dann als `root` wieder ausloggt und normal weiterarbeitet:

```
user$  su -l root
Password:  xxx
root#  mount -t ext2 /test /dev/sda7
root#  <Strg>+<D>
logout
user$  ls /test
```

Damit `su` ein vollwertiger Ersatz für einen `root`-Login ist, müssen Sie die Option `-l` verwenden! Damit erreichen Sie, dass alle Login-Startdateien eingelesen werden, was unter anderem zur korrekten Definition von `PATH` notwendig ist.

kdesu Unter KDE verwenden Sie am besten `kdesu` zum Start von X-Programmen mit Administratorrechten. Das Programm zeigt einen ansprechenden Dialog zur Eingabe des `root`-Passworts an.

```
user$  kdesu kate /etc/fstab
```

`kdesu` funktioniert nur, wenn der Dämon `kdesud` läuft. Dieser wird üblicherweise beim KDE-Start gestartet. Eine Zusammenfassung der zahlreichen `kdesu`-Optionen erhalten Sie mit `kdesu -help-all`. Bei einigen Distributionen ist `kdesu` direkt in das KDE-Menü integriert. Wenn Sie also ein Programm starten, das Administratorrechte beansprucht, erscheint automatisch die `kdesu`-Login-Box.

gksu Das Gnome-Gegenstück zu `kdesu` heißt `gksu`. Es funktioniert ohne einen zusätzlichen Hintergrundprozess. Eine Zusammenfassung der Optionen gibt `man gksu`.

su-to-root Debian (aber nicht Ubuntu!) verwendet zum Start von Administratorwerkzeugen aus dem Gnome- oder KDE-Menü vereinzelt das desktop-unabhängige Script `su-to-root`. Das Script ist Teil des `menu`-Pakets. `man su-to-root` fasst die wenigen Optionen zusammen.

consolehelper Als Variante zu `gksu` kommt vor bei älteren Versionen von Fedora und Red Hat `consolehelper` zum Einsatz. Dieses Programm bietet ebenfalls einen ansprechenden Passwortdialog, ist aber ganz anders implementiert. Die Grundidee besteht darin, dass die betreffenden Administratorwerkzeuge in das `/usr/sbin`-Verzeichnis installiert werden, in dem sie nur für `root` zugänglich sind. Für gewöhnliche Benutzer befindet sich in `/usr/bin` ein symbolischer Link auf `consolehelper`. Das folgende Kommando zeigt eine derartige Konfiguration für `system-config-network` (Netzwerkkonfiguration für RHEL 6):

```
user$  ls -l /usr/bin/system-config-network /usr/bin/system-config-network
-rwxr-xr-x ...  root root   /usr/sbin/system-config-network
lrwxrwxrwx ...  root root   /usr/bin/system-config-network -> consolehelper
```

Führt nun `root` das Kommando `system-config-network` aus, wird direkt `/usr/bin/system-config-network` gestartet. Führt dagegen ein gewöhnlicher Benutzer `system-config-network` aus, wird `consolehelper` gestartet. Wenn der Benutzer das korrekte `root`-Passwort angibt, startet `consolehelper` das gewünschte Programm `system-config-network`.

ssh Bei den meisten Distributionen funktioniert `su` nur für Textkommandos. Das kann mehrere Gründe haben: Erstens ist zum Start eines X-Programms die Umgebungsvariable `DISPLAY` erforderlich. Diese Variable muss den Namen des Rechners enthalten, auf dem das Programm angezeigt werden soll (`export DISPLAY=localhost:0`). Zweitens kann X aus Sicherheitsgründen verbieten, dass fremde Benutzer Programme starten können; Abhilfe schafft das Kommando `xhost`. Drittens kann der Netzwerk-Port für die Kommunikation zum X-Server gesperrt sein.

Wenn kdesu, gksu oder consolehelper nicht zur Verfügung stehen, bietet ssh die einfachste Lösung all dieser Probleme: Führen Sie das gewünschte Kommando einfach in der folgenden Form aus:

```
user$  ssh -X -l benutzer localhost
```

Setuid- und Setgid-Zugriffsbits

Die Setuid- und Setgid-Zugriffsbits stellen eine weitere Möglichkeit dar, bestimmte Programme so zu kennzeichnen, dass jeder sie ausführen kann, als wäre er bzw. sie root oder ein anderer Benutzer oder Mitglied einer anderen Gruppe. Der wesentliche Unterschied zu sudo besteht darin, dass die Setuid- und Setgid-Zugriffsbits für *alle* Benutzer gelten (während die Benutzer bei sudo in /etc/sudoers explizit aufgezählt werden müssen). Weitere Informationen zu den Setuid- und Setgid-Zugriffsbits finden Sie in Abschnitt 15.6.

16.3 Prozesse unter einer anderen Identität ausführen (sudo)

sudo verfolgt einen ganz anderen Ansatz als die oben beschriebenen su-Varianten. Das Programm ermöglicht nach entsprechender Konfiguration bestimmten Benutzern die Ausführung bestimmter Programme mit root-Rechten. Zur Sicherheit muss nochmals das *eigene* Passwort angegeben werden, also eben *nicht* das root-Passwort.

sudo führt diese Programme dann so aus, als wären sie von einem anderen Benutzer gestartet worden (Default: root). Damit können einzelne Benutzer administrative Aufgaben übernehmen bzw. systemkritische Kommandos ausführen, ohne dazu das root-Passwort kennen zu müssen. sudo protokolliert alle ausgeführten Kommandos sowie gescheiterte Versuche üblicherweise in /var/log/messages.

sudo merkt sich das Passwort für 15 Minuten. Wenn Sie innerhalb dieser Zeit ein weiteres Kommando mit sudo ausführen, werden Sie nicht neuerlich nach dem Passwort gefragt. Die Merkzeit kann in /etc/sudoers mit dem Schlüsselwort timestamp_timeout verändert werden.

Konfiguration

Die Konfiguration von sudo erfolgt durch die Datei /etc/sudoers. Vereinfacht ausgedrückt, beschreibt die Datei in drei Spalten, welche Benutzer von welchem Rechner aus welche Programme ausführen dürfen. Die folgende Zeile bedeutet, dass die Benutzerin kathrin am Rechner uranus das Kommando /sbin/fdisk ausführen darf. Das Schlüsselwort ALL bedeutet, dass kathrin das Kommando unter jedem beliebigen Account ausführen darf, also als root, als news, als lp etc.

```
# in /etc/sudoers
kathrin uranus=(ALL) /sbin/fdisk
```

Wenn der ersten Spalte von sudoers das Zeichen % vorangestellt wird, gilt der Eintrag für alle Mitglieder der angegebenen Gruppe. Diverse weitere Syntaxvarianten beschreibt man sudoers.

Ändern Sie /etc/sudoers mit visudo!

Aus Sicherheitsgründen sollte /etc/sudoers ausschließlich mit den Kommando visudo editiert werden (siehe auch dessen man-Seite)! visudo führt vor dem Speichern einen Syntaxtest durch und stellt so sicher, dass Sie sich nicht durch eine fehlerhafte sudoers-Datei selbst von weiteren Administrationsarbeiten ausschließen. Besonders wichtig ist das bei Distributionen wie Ubuntu, die keinen root-Login vorsehen.

visudo verwendet, wie der Name vermuten lässt, normalerweise den Editor vi; wenn Sie einen anderen Editor vorziehen, müssen Sie dessen exakten Pfad in der Umgebungsvariablen VISUAL oder EDITOR angeben.

Anwendung

Kathrin kann nun fdisk folgendermaßen ausführen:

```
kathrin$  sudo /sbin/fdisk /dev/sda
Password: xxxxxx
```

Als Passwort muss das Passwort der Benutzerin kathrin angegeben werden. Bei fdisk muss der vollständige Pfad angegeben werden, falls sich fdisk nicht in einem der PATH-Verzeichnisse von kathrin befindet. fdisk wird automatisch im Account root ausgeführt. Ein anderer Account kann mit sudo -u *account* gewählt werden.

sudo ohne Passwort

Es besteht die Möglichkeit, einem bestimmten Benutzer das Ausführen von sudo ohne Passwortangabe zu erlauben. Dazu fügen Sie in sudoers eine Zeile nach dem folgenden Muster ein:

```
kofler ALL=(ALL) NOPASSWD: ALL
```

Das ist natürlich ein Sicherheitsrisiko, aber wer oft Administratoraufgaben ausführen muss, wird die so gewonnene Bequemlichkeit schätzen. Beachten Sie, dass das NOPASSWD-Tag nur gültig ist, wenn es keine anderen sudoers-Zeilen gibt, die vom selben Benutzer ein Passwort verlangen. Das gilt auch für Gruppeneinträge, also z. B. %admin.

Mehrere Kommandos mit sudo ausführen

Bei umfangreicheren Administrationsaufgaben wird es zunehmend lästig, jedem Kommando sudo voranzustellen. Eleganter ist es, mit sudo -s in den root-Modus zu wechseln. Alle weiteren Kommandos werden wie von root ausgeführt. Sie beenden diesen Modus mit Strg+D.

gksudo

Beim Start von Administrationsprogrammen unter X kommt bei vielen Distributionen gksudo zum Einsatz. Dieses Programm ermöglicht die Passwort-Eingabe in einem Dialog und startet dann das gewünschte Programm.

Die Konfiguration von /etc/sudoers bietet viel mehr syntaktische Möglichkeiten, als hier angedeutet wurde. Lesen Sie die man-Seiten zu sudo und zu sudoers! Noch mehr Details sind auf der sudo-Homepage nachzulesen: Link

http://www.courtesan.com/sudo

sudo bei Ubuntu

Bei Ubuntu und einigen anderen Distributionen ist root ohne gültiges Passwort eingerichtet. Ein root-Login ist damit unmöglich. Auch su oder ssh -l root funktionieren nicht, wohl aber sudo su -l. Die einzige Möglichkeit zur Ausführung administrativer Kommandos bietet somit sudo. Die Datei /etc/sudoers enthält nur wenige Zeilen:

```
# Defaultkonfiguration in /etc/sudoers bei Ubuntu
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path=\
  "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
root        ALL=(ALL) ALL
%admin      ALL=(ALL) ALL
%sudo       ALL=(ALL:ALL) ALL
```

Defaults env_reset bewirkt, dass beim Benutzerwechsel alle Umgebungsvariablen zurückgesetzt werden. Defaults mail_badpass führt dazu, dass nach einem fehlerhaften Login-Versuch eine Warn-E-Mail an den Administrator versandt wird. Defaults secure_path legt den Inhalt der PATH-Umgebungsvariable für sudo-Kommandos fest.

Die vierte Zeile gibt root uneingeschränkten Zugriff auf alle Programme. Die Zeile ist unter Ubuntu eigentlich zwecklos, weil der root-Login gesperrt ist. Am wichtigsten sind die letzten zwei Zeilen: Sie erlauben allen Mitgliedern der Gruppen sudo und admin den Aufruf sämtlicher Programme.

Normalerweise ist unter Ubuntu nur der erste Benutzer, also der, der während der Installation eingerichtet wurde, Mitglied der sudo-Gruppe. Weitere Benutzer können ebenfalls dieser Administratoren-Gruppe zugeordnet werden. Bei älteren Ubuntu-Versionen wurde anstelle der sudo-Gruppe die admin-Gruppe verwendet.

Die folgende zusätzliche Zeile in /etc/sudoers erlaubt es dem Benutzer kofler, das Kommando apt-get und das Programm Synaptic ohne Passwort auszuführen. Damit können auch Updates ohne Passworteingabe durchgeführt werden.

```
# Ergänzung in /etc/sudoers bei Ubuntu
kofler ALL=NOPASSWD: /usr/sbin/synaptic, /usr/bin/apt-get
```

sudo bei Fedora

Bei aktuellen Fedora-Distributionen können Sie während der Installation einen neuen Benutzer einrichten und diesen zum Administrator machen. Das bedeutet, dass er der Gruppe `wheel` zugeordnet wird. `/etc/sudoers` enthält für diese Gruppe die folgende Zeile:

```
# in /etc/sudoers bei Fedora
...
%admin     ALL=(ALL) ALL
```

Ansonsten verhält sich `sudo` weitgehend wie bei Ubuntu, d. h., `wheel`-Gruppenmitglieder müssen ihr eigenes Passwort angeben, um `sudo`-Kommandos ausführen zu dürfen. Losgelöst von `sudo` gibt es weiterhin den Benutzer `root` mit einem eigenen Passwort.

sudo bei SUSE

Bei SUSE spielt `sudo` eine viel kleinere Rolle als unter Ubuntu. Wenn Sie dennoch `sudo` einsetzen möchten, müssen Sie auf einige Besonderheiten in der Defaultkonfiguration achten bzw. diese gegebenenfalls ändern.

```
# Defaultkonfiguration in /etc/sudoers bei openSUSE
Defaults always_set_home  # verhindert die Ausführung von X-Programmen
Defaults env_reset        # verhindert die Ausführung von X-Programmen
Defaults env_keep = "LANG LC_ADDRESS LC_CTYPE ..."
Defaults targetpw         # sudo fragt nach dem Passwort des Zielbenutzers
ALL ALL=(ALL) ALL         # mit dem richtigen Passwort darf jeder alles
root    ALL=(ALL) ALL
```

Die ersten drei Zeilen verhindern aus Sicherheitsgründen die Ausführung von X-Programmen mit `sudo`. Wenn `sudo` den direkten Start solcher Programme unterstützen soll, müssen Sie diese Zeile löschen bzw. ein #-Zeichen voranstellen.

`Defaults targetpw` bedeutet, dass grundsätzlich das Passwort für den Account angegeben werden muss, in dem das Kommando ausgeführt werden soll, in der Regel also das `root`-Passwort. Die Zeile `ALL ALL=(ALL) ALL` erlaubt schließlich allen Benutzern, jedes Kommando auszuführen, sofern das richtige Passwort für den Ziel-Account bekannt ist.

16.4 Prozesse unter einer anderen Identität ausführen (PolicyKit)

Konzept

Die Grundidee des PolicyKits besteht darin, Programme in zwei Komponenten zu zerlegen: Der eine Teil enthält die Benutzeroberfläche und läuft mit gewöhnlichen Benutzerrechten. Der zweite Teil des Programms, der in der Nomenklatur des PolicyKits als *mechanism* bezeichnet wird, ist für Systemeingriffe zuständig und läuft mit `root`-Rechten. Diese Trennung hat den fundamentalen Vorteil, dass nicht mehr ein riesiges Programm mit `root`-Rechten laufen muss, sondern nur noch kleine Teile. Das reduziert mögliche Sicherheitsrisiken. Außerdem besteht theoretisch die Möglichkeit, dass verschiedene Benutzeroberflächen (z. B. ein Gnome- und ein KDE-Programm) auf ein einheitliches Set von Mechanismen zurückgreifen.

Die Kommunikation zwischen den beiden Komponenten erfolgt durch ein Bussystem (in der Regel über den D-Bus). Ob ein bestimmter Mechanismus ausgeführt werden darf oder nicht, entscheiden Funktionen der PolicyKit-Bibliothek, die auf eine zentrale Rechtedatenbank zurückgreifen. Für die Entscheidung werden drei Kriterien berücksichtigt:

- **Subjekt:** Wer bzw. welcher Benutzer will Systemänderungen durchführen?
- **Objekt:** Welches Objekt soll verändert werden (z. B. eine Datei, eine Partition oder eine Netzwerkverbindung)?
- **Aktion:** Was soll gemacht werden (z. B. eine Partition in das Dateisystem einbinden)?

Benutzersicht

In vielen Fällen bemerkt der Benutzer gar nichts vom PolicyKit. Beispielsweise erlaubt die Standardkonfiguration bei den meisten aktuellen Distributionen dem Dateimanager, externe Datenträger in das Dateisystem einzubinden. Dazu ist keine weitere Authentifizierung erforderlich, der Vorgang erfolgt automatisch, sobald der Datenträger angeschlossen wird.

Eine zweite Variante besteht darin, dass die PolicyKit-Regeln eine Autorisierung verlangen – beispielsweise zur Durchführung eines Updates mit dem PackageKit. In diesem Fall erscheint ein Authentifizierungsdialog. Bemerkenswert ist, dass sich das PolicyKit bei entsprechender Konfiguration die Authentifizierung merkt und in `*.auths`-Dateien in `/var/lib/PolicyKit/` speichert. Wenn ein Benutzer sich also ein einziges Mal für einen bestimmten Vorgang authentifiziert hat, fragt PolicyKit in Zukunft nicht mehr nach.

Auf eine dritte Variante stoßen Sie bei diversen Gnome-Administrationswerkzeugen: Hier führt ein mit einem Vorhängeschloss gekennzeichneter Button zum Authentifizierungsdialog. Erst nach der Angabe des `root`- oder Benutzerpassworts können Systemveränderungen durchgeführt werden.

Konfiguration

Die Konfiguration des PolicyKits erfolgt an folgenden drei Orten:

`/etc/polkit-1/*`	(globale Konfiguration, Voreinstellungen)
`/usr/share/polkit-1/action/*.policy`	(Aktionen)
`/var/lib/polkit-1/*`	(Rechte)

Bei der Grundkonfiguration gibt es distributionsspezifische Besonderheiten. Beispielsweise gibt `/etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf` bei Ubuntu-Systemen allen Benutzern der `admin`- und `sudo`-Gruppen Administratorrechte. Unter Fedora gilt eine analoge Regel für `wheel`-Gruppenmitglieder.

16.5 Systemprozesse (Dämonen)

Als Dämonen (englisch *daemons*) werden Hintergrundprozesse zur Systemverwaltung bezeichnet. Diese Prozesse werden normalerweise während des Hochfahrens des Rechners im Rahmen des Init-V-Prozesses gestartet. Wenn Sie mit der Windows-Diktion vertraut sind, entsprechen Linux-Dämonen den Windows-Services. Tabelle 16.1 beschreibt ganz kurz die Aufgaben der wichtigsten Dämonen. Soweit die Programme in diesem Buch beschrieben werden, werden die betreffenden Abschnitte angegeben.

Kernel-Threads

Neben gewöhnlichen Server-Diensten wie `httpd` (Apache) gibt es Hintergrundprozesse, bei denen es sich aber nicht um richtige Programme handelt, sondern um Teilprozesse (Threads) des Kernels. Sie erkennen diese Prozesse daran, dass `ps axu` ihre Namen in eckige Klammern stellt. Manchen dieser Teilprozesse ist eine Nummer hintangestellt, die auf die CPU hinweist. `kblockd/0` verwaltet somit den Block-Device-Buffer für die erste CPU, `kblockd/1` den Buffer für die zweite CPU etc.

Die meisten Kernel-Threads betreffen Low-Level-Aufgaben des Betriebssystems (Speicherverwaltung, Prozessverwaltung, CPU-Steuerung etc.). Sie werden überwiegend bereits während der Systeminitialisierung zu Beginn des Systemstarts gestartet. Für normale Anforderungen ist keine spezielle Konfiguration erforderlich. Die Funktion der wichtigsten Kernel-Threads ist in Tabelle 16.2 zusammengefasst.

Prozess	Bedeutung
afpd	Server für das Apple Filing Protocol (Abschnitt 32.3)
apache2	Webserver (Abschnitt 35.1)
atd	startet andere Programme zu vorgegebenen Zeiten (ähnlich wie cron).
avahi-daemon	automatische Netzwerkkonfiguration (ZeroConf, Rendezvous, Bonjour)
bluetoothd	Bluetooth-Verwaltung
cron	startet andere Programme zu vorgegebenen Zeiten (Abschnitt 16.6).
cupsd	Drucker-Spooler (Abschnitt 33.2)
dbus-daemon	D-BUS-Kommunikation (Abschnitt 21.6)
dhclient	DHCP-Client (Abschnitt 29.3)
dhcpd	weist anderen Rechnern die IP-Netzwerkadresse zu (Abschnitt 30.5).
dhcpcd	liest die IP-Netzwerkadresse (Abschnitt 29.3).
gdm	Gnome-Login-Manager (Abschnitt 24.2)
hpiod	HP-Druck- und -Scan-Funktionen (Abschnitt 33.2)
httpd	Webserver (z. B. Apache)
kdm	KDE-Login-Manager (Abschnitt 24.2)
lockd	NFS-3-Locking
lpd	herkömmlicher Drucker-Spooler auf der Basis von BSD-LPD
mdnsd	automatische Netzwerkkonfiguration (ZeroConf, Rendezvous, Bonjour)
mysqld	MySQL-Datenbank-Server (Abschnitt 36)
named	Domain-Nameserver
NetworkManager	Network Manager (Abschnitt 29.1)
nmbd	Nameserver für Windows/Samba (Abschnitt 31.1)
nscd	Cache für Benutzer-, Gruppen- und Rechnernamen (Abschnitt 21.4)
ntpd	Zeiteinstellung mit dem Network Time Protocol (Abschnitt 21.3)
portmap	Port-Mapper für den NFS-3-Server (Abschnitt 32.2)
postfix	Mail-Server zum Versenden von E-Mails (Abschnitt 37.2)
rpc.*	RPC-Netzwerkdienste (Remote Procedure Call), zumeist für NFS 3
sdpd	Bluetooth-Verwaltung
sendmail	Mail-Server zum Versenden von E-Mails
smartd	SMART-Festplattenüberwachung (Abschnitt 25.16)

Tabelle 16.1 Wichtige Systemprozesse

Prozess	Bedeutung
smbd	Datei-Server für Windows/Samba (Abschnitt 31.1)
squid	Web-Proxy und -Cache (Abschnitt 41.1)
sshd	Secure-Shell-Server (Abschnitt 34)
rsyslogd	protokolliert Systemmeldungen (Abschnitt 21.7).
udevd	Device-Verwaltung (Abschnitt 15.9)
vsftpd	FTP-Server (Abschnitt 35.7)
xdm	X-Display Manager (Abschnitt 24.2)
xinetd	startet andere Netzwerkdämonen (Abschnitt 27.9).

Tabelle 16.1 Wichtige Systemprozesse (Forts.)

Kernel-Thread	Bedeutung
aio	asynchrone IO-Verwaltung (z. B. für Netzwerkprozesse)
events	Ereignis- und Software-Interrupt-Verwaltung
kacpid	ACPI-Funktionen
kblockd	verwaltet den Block-Device-Buffer.
khelperd	lädt bzw. entfernt Kernelmodule für Benutzerprogramme.
khubd	verwaltet das Ein- und Ausstecken von USB-Geräten.
kjournald	führt das Journaling für ext3/4-Dateisysteme durch.
knfsd	NFS-Server
kthread	verwaltet Threads.
nfsd	NFS-Server
kscand	Speicherverwaltung
kseriod	kommuniziert mit seriellen Geräten.
ksoftirqd	Hardware-Interrupt-Verwaltung
kswapd	Swapping
lockd	NFS-Locking
migration	bestimmt, welche Prozesse auf welcher CPU laufen.
pdflush	speichert Dateiänderungen physikalisch.
rpciod	NFS
scsi_eh	verwaltet SCSI-Fehler und -Timeouts.
watchdog	überwacht, ob das System noch reagiert.

Tabelle 16.2 Wichtige Kernel-Threads

Systemdienste starten und beenden

Die in Tabelle 16.1 aufgezählten Dämonen werden über ein Init-System gestartet. Grundlagen und Details verschiedener Init-Systeme werden ausführlich in Kapitel 27 beschrieben. Dort erfahren Sie auch, wie Sie selbst neue Scripts in das System integrieren.

An dieser Stelle finden Sie lediglich eine kurze Zusammenfassung, wie Sie einen Systemdienst manuell starten bzw. stoppen, was Sie tun müssen, damit der Dämon beim Systemstart automatisch gestartet wird, bzw. wie Sie den automatischen Start vermeiden. Diese Informationen werden Sie insbesondere beim Einrichten und Konfigurieren von Netzwerkdiensten häufig benötigen. Beachten Sie, dass nicht nur das Kommando, sondern auch der Dienstname je nach Distribution variieren kann. Beispielsweise heißt das Script zum Starten des Webservers Apache bei Debian, Ubuntu und SUSE `apache2`, bei Fedora und Red Hat dagegen `httpd`.

Manuell starten

Um einen Dämon bzw. Netzwerkdienst oder -Server zu starten, führen Sie eines der folgenden Kommandos aus. `service` funktioniert auf den meisten gängigen Distributionen. Die Verfügbarkeit der restlichen Kommandos hängt von der Distribution bzw. vom Init-System ab.

```
root#  service name start              (funktioniert bei fast allen Distributionen)
root#  /etc/init.d/name start          (Init-V-Prozesse)
root#  invoke-rc.d name start          (Debian-spezifisch für Init-V)
root#  rcname start                    (SUSE-spezifisch für Init-V)
root#  start name                      (Upstart, z.B. unter Ubuntu)
root#  systemctl start name.service    (Systemd, z.B. Fedora und openSUSE)
```

Manuell stoppen

So sieht das Kommando aus, um einen Dienst wieder zu stoppen:

```
root#  service name stop               (fast alle aktuellen Distributionen)
root#  /etc/init.d/name stop           (Init-V-Prozesse)
root#  invoke-rc.d name stop           (Debian-spezifisch für Init-V)
root#  rcname stop                     (SUSE-spezifisch für Init-V)
root#  stop name                       (Upstart)
root#  systemctl stop name.service     (Systemd)
```

Reload/Restart

Viele Netzwerkdienste sind in der Lage, im laufenden Betrieb die Konfigurationsdateien neu einzulesen. Die `reload`-Anweisung ist notwendig, damit der Dienst Änderungen an der Konfigurationsdatei berücksichtigt. Dienste, die `reload` nicht unterstützen, müssen Sie durch `restart` vollständig neu starten.

```
root#  service name reload/restart          (fast alle aktuellen Distributionen)
root#  /etc/init.d/name reload/restart      (Init-V-Prozesse)
root#  invoke-rc.d name reload/restart      (Debian-spezifisch für Init-V)
root#  rcname reload/restart                (SUSE-spezifisch für Init-V)
root#  reload/restart name                  (Upstart)
root#  systemctl reload name.service        (Systemd)
```

Automatischer Start beim Hochfahren

Sobald ein Netzwerkdienst einmal korrekt eingerichtet ist, soll er in der Regel beim Hochfahren des Rechners automatisch gestartet, beim Herunterfahren automatisch gestoppt werden. Bei manchen Distributionen (z. B. Debian, Ubuntu) werden die Dienste bereits bei der Paketinstallation entsprechend konfiguriert. Bei anderen Distributionen ist das aus Sicherheitsgründen nicht der Fall, und der automatische Start muss explizit aktiviert werden!

Unter Debian ab Version 6 sowie unter SUSE kümmert sich das Kommando `insserv` um das Einrichten der Init-V-Start-Links und -Stopp-Links.

Bei Red Hat und Fedora reicht in vielen Fällen das erste `chkconfig`-Kommando. Das zweite Kommando ist nur erforderlich, wenn das Init-V-Script keine Angaben enthält, in welchem Runlevel der Dienst normalerweise gestartet werden soll – fast immer 3 und 5.

```
root#  insserv name                      (Debian- und SUSE-spezifisch für Init-V)
root#  chkconfig --add name              (Red-Hat-spezifisch für Init-V)
root#  chkconfig --level 35 name on      (Red-Hat-spezifisch für Init-V)
root#  systemctl enable name.service     (Systemd)
```

Automatischen Start verhindern

Die folgenden Kommandos verhindern in Zukunft den automatischen Start beim Hochfahren. Wenn der Dienst bereits läuft, wird er durch das folgende Kommando allerdings nicht gestoppt; dazu ist ein eigenes `stop`-Kommando erforderlich.

```
root#  insserv -r name                   (Debian- und SUSE-spezifisch für Init-V)
root#  chkconfig --del name               (Red-Hat-spezifisch für Init-V)
root#  systemctl disable name.service     (Systemd)
```

Bei Systemdiensten, die von Upstart gestartet werden (Ubuntu, Fedora 9 bis 14, RHEL 6) gibt es kein einfaches Kommando, um den automatischen Start zu verhindern. Sie müssen die betreffende Upstart-Konfigurationsdatei im Verzeichnis `/etc/init` mit einem Editor ändern oder das Paket deinstallieren.

16.6 Prozesse automatisch starten (Cron)

Wenn Ihr Rechner plötzlich – scheinbar unvermittelt – damit beginnt, die Festplatte zu durchsuchen, Ihnen E-Mails zusendet etc., dann ist die Ursache fast immer der automatische Start von Prozessen durch den Dämon Cron. Dieses Programm wird beim Rechnerstart durch den Init-Prozess automatisch gestartet. Es wird einmal pro Minute aktiv, analysiert alle `crontab`-Dateien und startet die dort angegebenen Programme. Cron wird in erster Linie für Wartungsarbeiten verwendet – um Logging-Dateien zu komprimieren und zu archivieren, um temporäre Dateien zu löschen, um Verzeichnisse zu aktualisieren, Backups durchzuführen etc.

Die globale Konfiguration von Cron erfolgt durch die Datei `/etc/crontab`. Darüber hinaus dürfen Benutzer Ihre eigenen Cron-Jobs in den benutzerspezifischen Dateien `/var/spool/cron/[tabs/]username` definieren.

Das Recht der benutzerspezifischen Cron-Steuerung kann mit den beiden Dateien `/var/spool/cron/allow` und `/deny` eingestellt werden. Wenn `allow` existiert, dürfen nur die hier eingetragenen Benutzer Cron-Kommandos ausführen. Wenn `deny` existiert, sind die hier eingetragenen Benutzer ausgeschlossen. Existiert keine dieser Dateien, hängt es von der Kompilation von Cron ab, ob irgendwelche Benutzer außer `root` Cron verwenden dürfen.

Minimalinstallationen ohne Cron

Bei gewöhnlichen Linux-Installationen wird Cron automatisch installiert. Beachten Sie aber, dass Cron bei Minimalinstallationen, wie sie im Server- und Virtualisierungsbereich üblich sind, mitunter fehlt! Abhilfe: Führen Sie `yum install cronie` (RHEL) bzw. `apt-get install cron` (Debian/Ubuntu) aus!

/etc/crontab

Die Datei `/etc/crontab` bzw. die Dateien in `/etc/cron.d` enthalten zeilenweise Einträge für die auszuführenden Programme. Die Syntax sieht so aus:

```
# in /etc/crontab
min hour day month weekday user command
```

Spalte	Bedeutung
`min`	gibt an, in welcher Minute (0–59) das Programm ausgeführt werden soll.
`hour`	gibt die Stunde an (0–23).
`day`	gibt den Tag im Monat an (1–31).
`month`	gibt den Monat an (1–12).
`weekday`	gibt den Tag der Woche an (0–7, 0 und 7 bedeuten jeweils Sonntag).
`user`	gibt an, für welchen Benutzer das Kommando ausgeführt wird (meist `root`).
`command`	enthält schließlich das auszuführende Kommando.

Tabelle 16.3 crontab-Spalten

Wenn in den ersten fünf Feldern statt einer Zahl ein * angegeben wird, wird dieses Feld ignoriert. `15 * * * *` bedeutet beispielsweise, dass das Kommando immer 15 Minuten nach der ganzen Stunde ausgeführt werden soll, in jeder Stunde, an jedem Tag, in jedem Monat, unabhängig vom Wochentag. `29 0 * * 6` bedeutet, dass das Kommando an jedem Samstag um 0:29 Uhr ausgeführt wird.

Für die Zeitfelder ist auch die Schreibweise `*/`*n* erlaubt. Das bedeutet, dass das Kommando jede *n*-te Minute/Stunde etc. ausgeführt wird. `*/15 * * * *` würde also bedeu-

ten, dass das Kommando viertelstündlich (*n*:00, *n*:15, *n*:30 und *n*:45) ausgeführt wird. Um die globale Cron-Konfiguration zu verändern, können Sie `/etc/crontab` bzw. die Dateien in `/etc/cron.d/*` direkt mit einem Editor bearbeiten.

Die Cron-Syntax erfordert einen Zeilenumbruch nach der letzten Zeile

Achten Sie darauf, dass alle Cron-Konfigurationsdateien mit einem Zeilenumbruch enden müssen – andernfalls wird die letzte Zeile ignoriert!

Benutzerspezifische crontab-Dateien

Die Dateien `/var/spool/cron/[tabs/]`*user* haben dasselbe Format wie `crontab`. Der einzige Unterschied besteht darin, dass die `user`-Spalte fehlt. Um benutzerspezifische Cron-Einträge zu verändern, sollten Sie dazu das Kommando `crontab -e` einsetzen. Führen Sie vorher `export EDITOR=emacs` aus, wenn Sie nicht mit dem `vi` arbeiten möchten. `man cron` und `man crontab` geben weitere Informationen.

cron.hourly, .daily, .weekly, .monthly

Bei den meisten Distributionen sieht die Defaultkonfiguration so aus, dass `/etc/crontab` einige Einträge enthält, die bewirken, dass einmal pro Stunde alle Script-Dateien in `/etc/cron.hourly/*` ausgeführt werden und einmal pro Tag die Script-Dateien in `/etc/cron.daily/*` etc. Bei Ubuntu sieht `/etc/crontab` so aus:

```
# /etc/crontab
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || \
                      ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || \
                      ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || \
                      ( cd / && run-parts --report /etc/cron.monthly )
```

Im Klartext bedeutet das, dass Cron

- 17 Minuten nach jeder vollen Stunde alle Script-Dateien des Verzeichnisses `/etc/cron.hourly` ausführt,
- täglich um 6:25 alle Script-Dateien des Verzeichnisses `/etc/cron.daily` ausführt,
- wöchentlich am Sonntag um 6:47 alle Script-Dateien des Verzeichnisses `/etc/cron.weekly` ausführt und
- an jedem Ersten des Monats um 6:52 alle Script-Dateien des Verzeichnises `/etc/cron.monthly` ausführt.

Die Scripts aus `/etc/cron.daily`, `-.weekly` und `-.monthly` werden nicht ausgeführt, wenn Anacron installiert ist (siehe unten).

Um selbst regelmäßig ein Backup-, Update- oder sonstiges Script auszuführen, fügen Sie die entsprechende Script-Datei einfach in eines der Verzeichnisse `/etc/cron.hourly`, `-.daily`, `-.weekly` oder `-.monthly` ein. Vergessen Sie nicht, das *execute*-Bit zu setzen (`chmod a+x datei`)!

Regeln für Dateinamen in /etc/cron.daily, -.weekly, -.monthly

Die Dateinamen eigener Scripts in `cron.daily`, `cron.weeky` und `cron.monthly` dürfen ausschließlich aus Zahlen, Buchstaben und Binde- und Unterstrichen bestehen! Sobald der Dateiname auch nur einen Punkt enthält, wird das Script von `run-parts` ignoriert! Diese Regeln sollen vermeiden, dass bei der Veränderung einer Script-Datei entstehende Backup-Dateien ebenfalls ausgeführt werden.

Wenn Sie sich vergewissern möchten, welche Scripts aus `run.daily` täglich ausgeführt werden, führen Sie `run-parts --test /etc/cron.daily` aus.

Wenn Sie mit der durch `crontab` vorgesehenen Zeit für die `/etc/cron.xxx`-Verzeichnisse nicht einverstanden sind, können Sie natürlich auch `/etc/crontab` um eine Zeile erweitern und den gewünschten Ausführungszeitpunkt und Ihr Script dort eintragen. Noch übersichtlicher ist es, in `/etc/cron.d` eine entsprechende neue Datei anzulegen.

Anacron

Neben Cron ist bei den meisten Distributionen auch Anacron installiert. Anacron kümmert sich darum, dass täglich, wöchentlich oder monatlich auszuführende Aufgaben auch dann erledigt werden, wenn ein Rechner nur unregelmäßig in Betrieb ist und beispielsweise über Nacht oder am Wochenende ausgeschaltet wird.

Anacron führt einmalig (soweit erforderlich) die Scripts der Verzeichnisse `/etc/cron.daily`, `-.weekly` und `-.monthly` aus. Anders als Cron endet Anacron nach der Ausführung aller Scripts und läuft nicht im Hintergrund weiter. Anacron kümmert sich nicht um die `hourly`-Jobs – für die ist in jedem Fall ausschließlich Cron verantwortlich.

Anacron speichert den Ausführungszeitpunkt in Dateien des Verzeichnisses `/var/spool/anacron`. Damit wird ausgeschlossen, dass ein für die tägliche Ausführung bestimmtes Script am selben Tag zweimal ausgeführt wird. Anacron wird durch `/etc/anacrontab` gesteuert, wobei die Standardkonfiguration in der Regel ausreichend ist.

Anacron ist nicht für den Server-Betrieb gedacht!

Auf einem Server, der ja zumeist wochenlang ohne Unterbrechung läuft, ist die Verwendung von Anacron nicht zweckmäßig! Anacron führt die Cron-Jobs der Verzeichnisse `/etc/cron.daily`, `-.weekly` und `-.monthly` nur einmalig aus. Cron wiederum ignoriert diese Jobs, wenn Anacron installiert ist. Das führt dazu, dass sämtliche `daily`-, `weekly`- und `monthly`-Jobs maximal ein einziges Mal ausgeführt werden, ganz egal, wie lange der Server läuft! Stellen Sie also sicher, dass Anacron auf Ihrem Server nicht installiert ist!

Kapitel 17
Konverter für Grafik, Text und Multimedia

Linux stellt zahllose Kommandos zur Verfügung, mit denen Sie Bilder, Texte und andere Dateien von einem Format in das andere konvertieren können: von GIF zu JPEG, von Latin1- zu Unicode-Text, von PostScript zu PDF, von HTML zu einfachem Text, von MP3 zu WAV etc.

Dieses Kapitel gibt einen ersten Überblick über derartige Kommandos und zeigt einige Anwendungsbeispiele. Wenn das eine oder andere Kommando aus diesem Kapitel bei Ihnen nicht zur Verfügung steht, müssen Sie das entsprechende Paket suchen und installieren – denn nur selten sind alle Pakete, die Sie brauchen, schon installiert.

17.1 Grafik-Konverter

Unter den vielen Grafik-Konvertern für Linux stechen zwei Pakete heraus: Image Magick und Netpbm. Beide Pakete kommen jeweils mit unzähligen Grafikformaten zurecht und bieten auch Kommandos bzw. Optionen zur einfachen Bildverarbeitung an (Bildgröße ändern, Bildausschnitt ändern, Kontrast verbessern, Farbanzahl reduzieren etc.). Im Folgenden finden Sie eine kurze Vorstellung dieser beiden Pakete sowie einiger anderer Kommandos bzw. Bibliotheken zur Konvertierung von Bilddateien.

Image Magick

Das Programmpaket Image Magick besteht aus mehreren Einzelkommandos, deren wichtigstes `convert` ist. Es erzeugt aus einer vorhandenen Bilddatei eine neue und ändert dabei das Format. Quell- und Zielformat gehen dabei einfach aus den Dateinamen hervor. Das folgende Kommando erzeugt also die Datei `bild.png` im PNG-Format:

```
user$  convert bild.jpg bild.png
```

Durch über 100 Optionen können gleichzeitig diverse Bildparameter verändert werden (Größe, Farbanzahl, Kompressionsgrad etc.):

```
user$  convert -resize 100x100 bild.jpg bild.png
user$  convert -type Grayscale bild.jpg bild.eps
user$  convert -quality 80 bild.bmp bild.jpg
```

`mogrify` funktioniert so ähnlich wie `convert`, verändert aber die vorhandene Datei (anstatt eine neue zu erzeugen):

```
user$  mogrify -resize 50% test.jpg
```

Abschließend noch kurz ein Überblick über weitere Kommandos: `compare` vergleicht zwei Bilder. `conjure` führt Bildverarbeitungskommandos der Magick Scripting Language (MSL) aus. `identify` liefert eine Beschreibung der Bilddatei, also Format, Größe etc. `import` erstellt einen Screenshot und speichert das Bild in einer Datei. `montage` setzt mehrere Bilder zu einem neuen zusammen.

```
user$  identify -verbose bild.png
Image: bild.png
  Format: PNG (Portable Network Graphics)
  Geometry: 85x100
  Type: TrueColor
  ...
```

Ein Beispiel für ein kleines Shell-Script, das von allen als Parameter übergebenen Dateien Thumbnails (verkleinerte Bilder) erzeugt, finden Sie in Abschnitt 14.8. Eine umfassende Dokumentation zu allen Kommandos finden Sie auf der folgenden Website:

http://www.imagemagick.org

Wenn Sie die Funktionen von Image Magick mit einer grafischen Benutzeroberfläche nutzen möchten, bietet sich hierfür das Programm Converseen an:

http://converseen.sourceforge.net

Netpbm

Einen ähnlichen Ansatz wie Image Magick verfolgt auch das Netpbm-Paket, ehemals *Portable Bitmap Utilities*. Allerdings muss hier jede Datei zur Bearbeitung in das interne Pnm- oder Pbm-Format umgewandelt werden. Das folgende Beispiel zeigt die Konvertierung einer TIF-Datei in eine EPS-Datei, wobei der Farbraum des Bilds gleichzeitig normalisiert wird (`pnmnorm`):

```
user$  tifftopnm bild.tif | pnmnorm | pnmtops -noturn -rle -scale 0.5 > bild.eps
```

Eine Beschreibung der ca. 200 Netpbm-Kommandos finden Sie hier:

http://netpbm.sourceforge.net/doc

libtiff-Bibliothek

Das `libtiff`-Paket enthält die gleichnamige Bibliothek sowie diverse Kommandos zur Bearbeitung und Konvertierung von TIFF-Dateien. Zu den wichtigsten Konvertierungskommandos zählen `bmp2tiff`, `gif2tiff`, `tiff2pdf` und `tiff2ps`. Bei der Manipulation von TIFF-Dateien helfen unter anderem `tiffcp`, `tiffinfo` und `tiffsplit`.

libwmf-Bibliothek

Das `libwmf`-Paket enthält die gleichnamige Bibliothek sowie einige Kommandos zur Verarbeitung von WMF- und EMF-Dateien (Windows Metafile bzw. Enhanced Metafile). Wichtige Konvertierkommandos sind `wmf2eps`, `wmf2svg` sowie `wmf2gd` (Konvertierung in die Formate JPEG und PNG).

SVG-Konverter

Je nach Distribution enthält das Paket `librsvg2` oder `librsvg2-bin` die Kommandos `rsvg` und `rsvg-convert`, um SVG-Dateien (Scalable Vector Graphics) in Bitmap-Dateien umzuwandeln.

EXIF

Je nach Distribution stehen verschiedene Bibliotheken und Kommandos zur Verarbeitung der EXIF-Daten in JPEG-Dateien zur Auswahl, beispielsweise `exif`, `exiftran` oder `exiv2`.

RAW-Dateien

Manche Digitalkameras bieten die Möglichkeit, Fotos ohne Qualitätsverlust in herstellerspezifischen RAW-Dateien zu speichern. Bei der Umwandlung derartiger Dateien in gewöhnliche Bilddateien hilft das Kommando `dcraw` aus dem gleichnamigen Paket.

17.2 Audio- und Video-Konverter

Tabelle 17.1 gibt einen Überblick über die wichtigsten Kommandos, um Audio-Dateien von der CD zu lesen bzw. um Audio- und Video-Dateien von einem Format in ein anderes umzuwandeln. Soweit der Paketname nicht ohnedies aus dem Kommando hervorgeht, ist er in Klammern angegeben. Der Paketname kann allerdings von Distribution zu Distribution variieren.

Im Folgenden finden Sie einige Zusatzinformationen und Beispiele zu ausgewählten Kommandos. Auf eine Referenz der Optionen dieser Kommandos verzichte ich aus Platzgründen. (Bei Bedarf hilft `man` *`kommandoname`* weiter.)

CD-Ripper

Beim CD-Ripper geht es nicht um *Jack the Ripper*, sondern um die Kunst, Audio-Tracks möglichst effizient und ohne Qualitätsverlust von einer CD auf die Festplatte zu übertragen. Zu den populärsten derartigen Kommandos zählen `cdparanoia` und `icedax` (ehemals `cdda2wav`). `cdparanoia` hat den Ruf, auch bei Problemfällen wie zerkratzten CDs besonders gute Ergebnisse zu liefern. Beide Kommandos werden mit einer Unzahl von Parametern gesteuert.

Format	Kommando (Paket)
CD → WAV	icedax, cdparanoia
MP3 → WAV	mpg123, mpg321, madplay
WAV → MP3	lame
OGG → WAV	oggdec (vorbis-tools)
WAV → OGG	oggenc (vorbis-tools)
MP3 → OGG	mp32ogg
AAC → WAV	faad
WAV → AAC	faac
WAV ↔ FLAC	flac
Audio ↔ Audio	sox
Audio ↔ Audio	sfconvert (audiofile)
Audio/Video ↔ Audio/Video	avconv (Audio/Video-Konverter, ehemals ffmpeg)
Audio/Video ↔ Audio/Video	mencoder (allgemeiner Audio/Video-Konverter)

Tabelle 17.1 Audio- und Video-Konverter

Hier zwei Beispiele: Das erste Kommando liest Track 3 einer CD im ersten SCSI-CD-Laufwerk. Die resultierende Datei bekommt den Namen audio.wav:

```
root#  icedax -D /dev/scd0 -t 3
```

Das folgende Kommando liest Track 4 von einer CD im selben Laufwerk. Das Ergebnis ist die Datei cdda.wav im lokalen Verzeichnis:

```
root#  cdparanoia -d  /dev/scd0 "4"
```

MP3-Encoder

Wegen der in Kapitel 10 erwähnten Patentprobleme gibt es kaum noch Linux-Distributionen, die einen MP3-Encoder in offiziellen Paketen mitliefern. Diverse Encoder sind aber im Internet als Zusatzpakete verfügbar. Das bekannteste Programm ist lame:

http://lame.sourceforge.net

Die Anwendung ist denkbar einfach: lame *input.wav output.mp3* erzeugt aus der Ausgangsdatei im WAV-Format eine entsprechende MP3-Datei. Der Vorgang und insbesondere die gewünschte Qualität der MP3-Datei wird durch zahlreiche Optionen gesteuert.

MP3 → OGG

Die in Tabelle 17.1 aufgezählten Kommandos können kombiniert werden, um beispielsweise eine MP3-Datei in das Ogg-Vorbis-Format umzuwandeln. Beachten Sie aber, dass derartige Umwandlungen immer mit Qualitätsverlusten behaftet sind und möglichst vermieden werden sollten!

```
user$ mpg321 -s in.mp3 -w - | oggenc - -o out.ogg
```

Leider gehen bei der Umwandlung die Info-Tags (ID3) verloren. Dieser Nachteil kann durch den Einsatz des MP3-Ogg-Konverter-Scripts vermieden werden (`mp32ogg` von *http://faceprint.com/code*).

FLAC

FLAC steht für *Free Lossless Audio Codec*. FLAC-Dateien sind zwar größer als MP3- oder Ogg-Dateien, aber wesentlich kleiner als WAV-Dateien. Der wesentliche Vorteil im Vergleich zu MP3 oder Ogg besteht darin, dass die Audio-Daten verlustfrei codiert werden. Zum Codieren und Decodieren verwenden Sie das Kommando `flac`.

SoX

SoX steht für *Sound Exchange* und bietet mit dem Kommando `sox` eine weitere Möglichkeit, Audio-Dateien von einem Format in ein anderes umzuwandeln. `sox` kennt mehr Formate als `sfconvert` (siehe unten). Zu `sox` gibt es die X-Oberfläche `xsox` sowie die Gnome-Oberfläche `gsox`.

Audio File Bibliothek

Das Paket `audiofile` implementiert die wichtigsten Funktionen der gleichnamigen Audio-File-Bibliothek des Computerherstellers SGI. Das interessanteste Kommando ist `sfconvert`: Es konvertiert Audio-Dateien zwischen den Formaten `aiff`, `aifc`, `next` und `wave`. `sfinfo` versucht zu ermitteln, welches Format eine Audio-Datei nutzt.

SoundConverter

Wenn Sie bei der Konvertierung von Audio-Dateien mehr Komfort wünschen, werden Sie vielleicht am Gnome-Programm SoundConverter Gefallen finden. Es konvertiert alle zuvor ausgewählten Audio-Dateien in das mit mit BEARBEITEN • EINSTELLUNGEN gewählte Format, standardmäßig OGG-VORBIS. Die neuen Dateien werden im selben Verzeichnis wie die Ursprungsdateien gespeichert, erhalten aber natürlich eine neue Endung, also beispielsweise `*.ogg`.

Video-Konverter (avconv und mencoder)

Das Kommando `avconv` (ehemals `ffmpeg`) aus dem gleichnamigen Paket konvertiert Audio- und Video-Dateien von einem Format in ein anderes. Die Liste der unterstützten Formate ist lang und kann mit `avconv -formats` ermittelt werden.

Bei der Angabe von Optionen müssen Sie beachten, dass diese für die als Nächstes angegebene Datei gelten. Die Reihenfolge der Optionen ist daher entscheidend für die korrekte Funktion des Kommandos. Soweit Sie keine abweichenden Einstellungen vornehmen, verwendet `avconv` für die Ergebnisdatei dieselben Codecs und Einstellungen wie in der Quelldatei und vermeidet so nach Möglichkeit Qualitätsverluste. Im folgenden Beispiel erstellt `avconv` eine Filmdatei in DVD-Auflösung:

```
user$  avconv -i in.avi out.mpg
user$  avconv -i in.avi -y -target pal-dvd out.avi
```

avconv eignet sich auch dazu, Audio- und Video-Daten zum Brennen einer eigenen DVD aufzubereiten. Ein entsprechendes Beispiel gibt man avconv. Wenn Sie sich die vielen avconv-Optionen nicht merken wollen, können Sie zur Umwandlung von Video-Dateien auch eine grafische Benutzeroberfläche verwenden, z. B. winff.

Eine Alternative zu avconv ist das Kommando mencoder. Es verwendet dieselbe Code-Basis wie der Video-Player MPlayer und wird zusammen mit diesem installiert. mencoder kommt mit allen Audio- und Video-Formaten zurecht, die auch von MPlayer unterstützt werden.

17.3 Text-Konverter (Zeichensatz und Zeilentrennung)

Dieser Abschnitt stellt die Kommandos recode, iconv, unix2dos und dos2unix vor. Sie dienen dazu, den Zeichensatz bzw. die Zeilentrennzeichen von reinen Textdateien zu ändern. Das ist dann erforderlich, wenn Sie Textdateien zwischen Systemen mit unterschiedlichen Zeichensätzen bzw. Textformatkonventionen austauschen.

recode

recode führt eine Zeichensatzkonvertierung von Zeichensatz 1 nach Zeichensatz 2 durch. Das folgende Kommando konvertiert die DOS-Datei dosdat in eine Linux-Datei mit dem Latin-1-Zeichensatz:

```
user$  recode ibmpc..latin1 < dosdat > linuxdat
```

Wie das folgende Beispiel beweist, kann recode auch das Zeilentrennzeichen verändern. Das Kommando ersetzt in der Datei windowsdat alle Zeilenenden (CR plus LF, also *Carriage Return* und *Line Feed*) durch das unter Linux übliche Zeilenende (nur LF). Der eigentliche Zeichensatz wird nicht geändert. Die resultierende Datei wird in linuxdat gespeichert.

```
user$  recode latin1/cr-lf..latin1 < windowsdat > linuxdat
```

recode liest die im Zeichensatz Latin-1 codierte Textdatei latin1dat und speichert sie als UTF-8-Datei (Unicode):

```
user$  recode latin1..u8 < latin1dat > utf8dat
```

iconv

Eine populäre Alternative zu recode ist das Kommando iconv. Dieses Kommando ist allerdings nicht in der Lage, die Zeilentrennungszeichen zu verändern. Das folgende Beispiel erzeugt abermals aus einer Latin-1-codierten Textdatei eine entsprechende UTF-8-Datei:

```
user$  iconv -f latin1 -t utf-8 latin1dat > utf8dat
```

dos2unix, unix2dos

Die Kommandos `dos2unix` und `unix2dos` ändern die Zeilentrennungszeichen zwischen dem DOS/Windows-typischen Format (CR plus LF) und dem Unix/Linux-typischen Format (nur LF). Die Kommandos eignen sich nur für Textdateien mit Ein-Byte-Zeichensätzen (z. B. ASCII, Latin-1), nicht für Unicode-Dateien!

```
user$  dos2unix datei.txt
```

17.4 Dateinamen-Konverter (Zeichensatz)

convmv

Bis vor ca. einem Jahrzehnt war es unter Linux üblich, Dateinamen im Zeichensatz Latin-1 darzustellen. Mittlerweile gilt hingegen Unicode (UTF-8) als Standard. Bei der Umstellung der Dateinamen von einem Zeichensatz auf einen anderen hilft das Kommando `convmv`. Dieses Kommando steht allerdings selten standardmäßig zur Verfügung. Bei einigen Distributionen kann es mühelos in Form eines gleichnamigen Pakets installiert werden. Sollte für Ihre Distribution kein entsprechendes Paket existieren, müssen Sie das Perl-Script von der folgenden Seite herunterladen:

http://j3e.de/linux/convmv

Um rekursiv alle Dateien eines Verzeichnisses vom Zeichensatz Latin-1 auf UTF-8 umzustellen (mit Rückfrage für jede einzelne Änderung), rufen Sie `convmv` so auf:

```
user$  convmv -r -i --notest -f iso-8859-1 -t utf8 verzeichnisname
```

`convmv` verändert nur den Namen, nicht den Inhalt der Dateien! Bei ersten Tests ist es empfehlenswert, auf die Option `--notest` zu verzichten: `convmv` zeigt dann nur die geplanten Änderungen an, ohne diese tatsächlich auszuführen.

`convmv` versucht selbstständig Dateinamen zu erkennen, die bereits den UTF-8-Zeichensatz nutzen, und verzichtet in diesem Fall auf eine neuerliche Namensänderung. Diesen Schutz können Sie durch die Option `--nosmart` deaktivieren.

17.5 Dokument-Konverter (PostScript, PDF, HTML, LaTeX)

Dieser Abschnitt stellt Kommandos vor, die bei der Bearbeitung und Konvertierung von Dokumenten in den Formaten PostScript, PDF, HTML etc. helfen. Tabelle 17.2 gibt einen ersten Überblick.

Text → PostScript

Wenn Sie Textdateien mit `lpr datei` direkt ausdrucken, kümmert sich das Drucksystem normalerweise automatisch um die Formatierung des Texts. Wenn Sie allerdings besondere Wünsche haben, wie der resultierende Ausdruck formatiert werden

Format	Kommando
Text → PostScript	a2ps, enscript, mpage
HTML → Text, PostScript	html2text, html2ps
PostScript ↔ PDF	ps2pdf, epstopdf, pdf2ps, pdftops
PostScript, PDF → Bitmap, Druckerformat	gs
PostScript → PostScript (Seiten extrahieren etc.)	psutils
PDF → PDF (Bilder/Seiten extrahieren etc.)	pdftk, pdfnup, pdfjoin, pdfedit
PDF → Text	pdftotext
LaTeX → DVI, PostScript, PDF	latex, pdflatex, dvips, dvipdf

Tabelle 17.2 Dokument-Konverter

soll, empfiehlt sich eine manuelle Konvertierung und ein anschließender Ausdruck der PostScript-Datei. Dazu eignen sich unter anderem die Kommandos `a2ps`, `enscript` und `mpage`. Die drei Kommandos bieten dieselben Grundfunktionen, unterscheiden sich aber durch diverse Formatierungsoptionen.

a2ps

`a2ps` steht für *Any to PostScript* und kann beispielsweise auch Texinfo-Dateien in das PostScript-Format umwandeln. Die folgenden Beispiele beschränken sich aber auf reine Textdateien. Beachten Sie, dass die Textdateien einen Latin-Zeichensatz nutzen müssen (nicht Unicode!). Standardmäßig formatiert das Kommando den Text in einer zweispaltigen Seite im Querformat.

```
user$ a2ps text.txt -o postscript.ps
```

Das folgende Kommando verarbeitet mehrere Textdateien und formatiert die Ausgabe mit vier kleinen Seiten pro Blatt. Wenn `a2ps` den Text als Programmcode erkennt, führt es automatisch eine Syntaxhervorhebung durch (Schlüsselwörter fett, Kommentare kursiv etc.).

```
user$ a2ps datei1.c datei2.c datei3.h -4 -o postscript.ps
```

enscript

`enscript` konvertiert Textdateien in die Formate PostScript, HTML und RTF. Das Kommando erwartet die Textdatei im Zeichensatz Latin-1. Das folgende Kommando erzeugt DIN-A4-Seiten im Querformat mit drei Spalten pro Seite:

```
user$ enscript -M A4 --landscape -3 text.txt -p postscript.ps
```

mpage

Auch `mpage` konvertiert Textdateien in das PostScript-Format, per Default mit vier Seiten pro Blatt und im Letter-Format. Das folgende Kommando erzeugt DIN-A4-Seiten im Querformat mit zwei Seiten pro Blatt:

```
user$ mpage -2 -bA4  text.txt > postscript.ps
```

Unicode

Leider kommt keines der oben vorgestellten Kommandos dieser Programme mit Unicode-Text (UTF-8) zurecht. Wenn Sie Unicode-Dokumente ausdrucken möchten, nehmen Sie am besten einen Unicode-Editor zu Hilfe. Eine einfache Konvertierung in das PostScript-Format können Sie auch mit `cnprint` vornehmen:

http://www.neurophys.wisc.edu/~cai/software

HTML → Text, PostScript

html2text

`html2text` konvertiert HTML-Dokumente in reine Textdateien. Das ist dann praktisch, wenn HTML-Dateien in einer Form weitergegeben werden sollen, die ein bequemes Lesen ohne Webbrowser möglich macht.

```
user$ html2text datei.html > text.txt
```

`html2text` liefert Latin-1-Text (nicht Unicode!). Die Formatierung des Texts wird durch einige Optionen sowie durch `/etc/html2textrc` bzw. durch `.html2textrc` gesteuert (siehe `man html2textrc`). Zur Konvertierung von HTML in Text können Sie auch textbasierte Webbrowser wie Lynx, ELinks oder `w3m` einsetzen.

html2ps

Für die automatische Konvertierung vom HTML- in das PostScript-Format eignet sich das Perl-Script `html2ps`. Die Verwendung ist denkbar einfach: `html2ps -D name.html > name.ps`. Die Option `-D` bewirkt, dass `html2ps` DSC-konforme Kommentare in die PostScript-Datei einbaut, was deren Weiterverarbeitung sehr erleichtert.

Sie sollten sich freilich keine Hoffnungen machen, dass `html2ps` mit modernen HTML-Seiten mit Javascript-Code, CSS-Formatierung etc. zurechtkommt. Zufriedenstellende Ergebnisse liefert `html2ps` nur bei sehr simplen HTML-Dokumenten. Für die manuelle Umwandlung von HTML zu PostScript oder PDF können Sie die Druckfunktionen Ihres Webbrowsers einsetzen. Sie werden aber feststellen, dass selbst das nur bescheidene Ergebnisse liefert, insbesondere was den Seitenumbruch betrifft.

PostScript ↔ PDF

ps2pdf

`ps2pdf quelle.ps ziel.pdf` erzeugt aus einer beliebigen PostScript-Datei eine PDF-Datei. Das Kommando erfüllt damit im Prinzip dieselbe Funktion wie das kommerzielle Programm Adobe Distiller. Es basiert auf Ghostscript (`gs`).

`ps2pdf` erzeugt momentan Dateien, die zum PDF-Format 1.2 für den Acrobat Reader 3.*n* kompatibel sind. Die Dokumentation weist aber darauf hin, dass sich das Defaultverhalten in Zukunft ändern kann. Wenn Sie die Kompatibilität zu einer bestimmten PDF-Version sicherstellen möchten, sollten Sie die Kommandos `ps2pdf12`, `ps2pdf13` und `ps2pdf14` einsetzen.

Die Qualität der PDF-Dateien hängt stark davon ab, welche Schriftarten im PostScript-Dokument verwendet werden. Bei nicht unterstützten Schriften müssen die Zeichen durch Bitmaps ersetzt werden, was die Darstellungsqualität stark mindert. Das Verhalten von `ps2pdf` wird durch unzählige Optionen gesteuert. Eine vollständige Dokumentation war zuletzt hier zu finden:

http://ghostscript.com/doc/current/Ps2pdf.htm

epstopdf Wenn Sie aus einer EPS-Abbildung eine PDF-Datei erstellen möchten, bietet sich `epstopdf` an. EPS steht für *Encapsulated PostScript* und bezeichnet PostScript-Dateien, bei denen durch eine sogenannte Bounding Box die exakte Bildgröße angegeben ist. EPS-Dateien eignen sich gut zum Einbetten in andere Dokumente (z. B. mit LaTeX oder OpenOffice).

`epstopdf` befindet sich üblicherweise im `tetex`-Paket, das TeX, LaTeX und andere TeX-spezifische Programme enthält. Im Unterschied zu `ps2pdf` berücksichtigt `epstopdf` die Größe des Bildes. Leider ist `epstopdf` nicht in der Lage, in der EPS-Datei enthaltene Bitmaps unverändert in die PDF-Datei zu übertragen, auch nicht mit der Option `--nocompress`.

pdf2ps Die Umkehrung zu `ps2pdf` ist `pdf2ps quelle.pdf ziel.ps`. Auch `pdf2ps` greift auf `gs` zurück.

pdftops `pdftops` erfüllt zwar prinzipiell dieselbe Aufgabe wie `pdf2ps`, ist intern aber anders implementiert und bietet wesentlich mehr Optionen zur Beeinflussung der resultierenden PostScript-Dateien. Beispielsweise können Sie den gewünschten PostScript-Level, die Papiergröße etc. angeben.

PostScript/PDF → Druckerformat/Bitmap

gs Das Kommando `gs`, bekannter unter dem Namen Ghostscript, konvertiert PostScript- und PDF-Dokumente in diverse Bitmap- und Druckerformate. Ghostscript ist ein wichtiger Baustein des Linux-Drucksystems (z. B. von CUPS, siehe Kapitel 33), weil es den Ausdruck von PostScript-Dokumenten auf Druckern ohne PostScript-Funktionen ermöglicht. Das Programm wird aber auch von diversen PostScript-Viewern und -Konvertern eingesetzt.

`gs` greift auf die auf dem Rechner installierten Schriftarten sowie auf eine Sammlung eigener Fonts zurück, die sich üblicherweise im Paket `ghostscript-fonts` befinden. Diese Fonts sind erforderlich, um PostScript-Schriften in eine Bitmap-Darstellung umzuwandeln.

Ghostscript ist in verschiedenen Versionen erhältlich. Auf den meisten Linux-Distributionen kommt GNU Ghostscript oder dessen Variante ESP Ghostscript zum

Einsatz. Diese beiden Versionen unterstehen der GPL. ESP Ghostscript ist speziell für die Zusammenarbeit mit CUPS optimiert. ESP steht dabei für den Firmennamen *Easy Software Products*.

Daneben gibt es kommerzielle Ghostscript-Versionen, wie Artifex Ghostscript, die beispielsweise an Druckerhersteller verkauft werden. Weitere Informationen zu den verschiedenen Ghostscript-Versionen finden Sie hier:

http://www.ghostscript.com
http://www.artifex.com

Externe Druckertreiber (Gutenprint)

Eine Menge Druckertreiber sind direkt in Ghostscript integriert. Daneben wurden aber diverse Treiber außerhalb des Ghostscript-Projekts entwickelt. Das wichtigste derartige Treiberprojekt ist Gutenprint (ehemals Gimp-Print). Weitere Informationen finden Sie hier:

http://gimp-print.sourceforge.net

An dieser Stelle ebenfalls erwähnenswert ist HPLIP (HP Linux Imaging and Printing). In diesem Projekt stellt die Firma HP Open-Source-Treiber für viele ihrer Drucker und Scanner zur Verfügung. Das HPLIB-Projekt hat allerdings nichts mit Ghostscript zu tun und wird in Kombination mit dem Drucksystem CUPS genutzt.

Manueller Aufruf

Wegen der guten Integration von Ghostscript in das Drucksystem und in diverse andere Programme wird `gs` nur selten manuell eingesetzt. Damit `gs` korrekt funktioniert, müssen mindestens zwei Optionen angegeben werden: `-sOutputFile=` zur Angabe der Datei, in die das Ergebnis geschrieben werden soll, sowie `-sDEVICE=`*name* oder `@`*name*`.upp` zur Einstellung des Ausgabeformats. In der Regel ist es sinnvoll, auch die Option `-dNOPAUSE` zu verwenden. Falls Sie auf DIN-A4-Papier drucken möchten, sollten Sie schließlich noch `-sPAPERSIZE=a4` angeben. Die folgende Anweisung übersetzt `test.ps` in das Format des HP-Laserjet 3. Das Ergebnis wird in die Datei `out.hp` geschrieben:

```
user$  gs -sDEVICE=ljet3 -sOutputFile=out.hp -sPAPERSIZE=a4 \
          -dNOPAUSE -dBATCH test.ps
```

Das zweite Beispiel wandelt eine PostScript- in eine PDF-Datei um. Auch `ps2pdf` ist in Wirklichkeit nichts anderes als ein Script, das `gs` aufruft.

```
user$  gs -dNOPAUSE -dBATCH -sDEVICE=pdfwrite -sOutputFile=out.pdf test.ps
```

Zu guter Letzt sehen Sie hier ein Kommando, das eine EPS-Datei in eine PNG-Datei umwandelt:

```
user$  gs -dNOPAUSE -dBATCH -sDEVICE=png16m -sOutputFile=out.png \
          -dEPSCrop -r100 bild.eps
```

PostScript-Utilities

psutils-Paket

Bei der Bearbeitung von PostScript-Dateien helfen die Kommandos des `psutils`-Pakets. Dabei handelt es sich teils um eigenständige Programme, teils um `bash`- oder Perl-Script-Dateien.

Kommando	Funktion
`epsffit`	passt die Größe einer EPS-Datei an.
`extractres`	analysiert die Datei und liefert `%%IncludeResource`-Kommentare für alle benötigten Fonts, Dateien etc.
`fixfmps`	passt FrameMaker-Dateien an die `psutils`-Konventionen an.
`fixmacps`	passt Macintosh-Dateien an die `psutils`-Konventionen an.
`fixscribeps`	passt Scribe-Dateien an die `psutils`-Konventionen an.
`fixtpps`	passt Troff/Tpscript-Dateien an die `psutils`-Konventionen an.
`fixwfwps`	passt MS Word-Dateien an die `psutils`-Konventionen an.
`fixwpps`	passt WordPerfect-Dateien an die `psutils`-Konventionen an.
`fixwwps`	passt MS Write-Dateien an die `psutils`-Konventionen an.
`getafm`	erzeugt AFM-Dateien zur Beschreibung von Fonts.
`includeres`	fügt die mit `extractres` erzeugten Kommentare in eine PostScript-Datei ein.
`psbook`	ordnet die Seiten eines Textes so an, dass ganze Bögen (etwa mit je 16 Seiten) gedruckt werden können.
`psnup`	ordnet mehrere verkleinerte Seiten auf einem Blatt an.
`psresize`	verändert die erforderliche Papiergröße eines Dokuments; das Kommando löst das regelmäßig auftretende Problem des Ausdrucks von PostScript-Dokumenten, die für das US-Letter-Format erzeugt wurden.
`psselect`	extrahiert einzelne Seiten aus einer PostScript-Datei.
`pstops`	ordnet die Seiten eines Dokuments in einer neuen Reihenfolge.

Tabelle 17.3 psutils-Kommandos

Das folgende Beispiel zeigt, wie eine mit LaTeX und DVIPS erzeugte PostScript-Datei mit dem Manuskript dieses Buches in eine Darstellung mit 64 Seiten pro Blatt umgewandelt wird. Damit erscheint jede Seite nur noch briefmarkengroß. Das ermöglicht anschließend in einem PostScript-Viewer eine rasche, übersichtsartige Kontrolle des Seitenlayouts (ähnlich wie die Druckvorschau bei Microsoft Word mit dem kleinstmöglichen Zoomfaktor):

```
user$ psnup -b-0.4cm -64 -q < linux.ps > vorschau.ps
```

Die obigen Kommandos funktionieren nur dann, wenn die PostScript-Dateien DSC-konforme Kommentare enthalten. (DSC steht für *Document Structuring Conventions*.) Die Kommentare werden nicht ausgedruckt, enthalten aber wichtige Informationen über die Größe einer Seite, über den Beginn und das Ende von Seiten etc.) EPS-Dateien sind einseitige PostScript-Dateien, die spezielle Kommentare zur Einbettung in andere Dokumente enthalten (insbesondere Bounding-Box-Angaben über die Größe des Ausdrucks).

PS-Dateien zusammenfügen

Um zwei oder mehrere PostScript-Dateien aneinanderzufügen, setzen Sie am einfachsten das Ghostscript-Kommando `gs` ein. Zufriedenstellende Ergebnisse erzielen Sie allerdings nur dann, wenn `gs` alle Font-Dateien findet.

```
user$ gs -sDEVICE=pswrite -sOutputFile=out.ps -dNOPAUSE -dBATCH in1.ps in2.ps ...
```

PDF-Utilities

pdftk

Das Kommando `pdftk` (PDF-Toolkit) bietet für PDF-Dokumente ähnliche Funktionen wie `psutils` für PostScript-Dateien. Sie können damit Seiten extrahieren, mehrere PDF-Dokumente zusammenführen, eine unverschlüsselte Version eines verschlüsselten PDF-Dokuments erstellen (vorausgesetzt, Sie kennen das Passwort), PDF-Formulare ausfüllen etc. Ausführliche Informationen finden Sie auf der folgenden Website:

http://www.accesspdf.com/pdftk

Das folgende Kommando liest die Seiten 10 bis 20 sowie 30 bis 40 aus `in.pdf` und schreibt sie in die neue Datei `out.pdf`:

```
user$  pdftk in.pdf cat 10-20 30-40 output out.pdf
```

Auch um mehrere PDF-Dateien aneinanderzufügen, verwenden Sie das Kommando `cat`:

```
user$  pdftk in1.pdf in2.pdf in3.pdf cat output out.pdf
```

Das folgende Beispiel erzeugt für jede einzelne Seite in `in.pdf` eine eigene PDF-Datei mit dem Namen `pg_`*n*, wobei *n* die Seitennummer ist. Wenn Sie andere Dateinamen wünschen, müssen Sie eine Zeichenkette in `printf`-Syntax an `output` übergeben, z. B. `output seite-%02d.pdf`.

```
user$  pdftk in.pdf burst
```

Das nächste Beispiel erzeugt eine verschlüsselte PDF-Datei. Die Datei kann zwar ohne das Passwort `xxx` gelesen, nicht aber ausgedruckt oder sonstwie bearbeitet werden. Wenn Sie selbst das Lesen der Datei schützen möchten, verwenden Sie statt `owner_pw` das Kommando `user_pw`.

```
user$  pdftk in.pdf output encrpyted.pdf owner_pw xxx
```

Poppler Poppler ist eine Sammlung von Kommandos zur Umwandlung von PDF-Dokumenten in andere Formate (Text, Bitmap, PostScript etc.). Poppler wird unter Linux von vielen PDF-Viewern eingesetzt. Das Programm befindet sich üblicherweise im Paket `poppler-utils`.

xpdf-utils Das Paket `xpdf-utils` enthält unter anderem die Kommandos `pdftops` (erzeugt PostScript-Dateien aus PDF-Dokumenten), `pdfinfo` (extrahiert die PDF-Dokument-Eigenschaften), `pdfimages` (extrahiert Bilder aus PDF-Dateien) und `pdftotext` (extrahiert den Text aus einer PDF-Datei).

pdfedit Das Paket `pdfedit` enthält diverse Werkzeuge und eine Benutzeroberfläche, um PDF-Dateien zu verändern.

pdfjam Das Paket `pdfjam` enthält die Kommandos `pdfnup`, `pdfjoin` und `pdf90`. Damit können Sie PDF-Dateien aneinanderfügen und rotieren.

GUIs Auch wer Kommandos und ihre Optionen verabscheut und sich stattdessen nach einer grafischen Benutzeroberfläche sehnt, findet eine reiche Auswahl von häufig Java-basierten Open-Source-Programmen. Neben dem schon erwähnten Programm PDFedit sind vor allem PDF-Shuffler, Bookbinder, JPDF Tweak sowie PDF Split and Merge (PDF Sam) interessant.

LaTeX & Co.

LaTeX ist ein System zum Setzen (Layouten) wissenschaftlicher Texte. Dieser Abschnitt beschreibt ganz kurz die wichtigsten Kommandos, um LaTeX-Dateien (`*.tex`) in andere Formate umzuwandeln, ohne aber auf die LaTeX-Syntax einzugehen.

latex Das Kommando `latex name.tex` erzeugt aus der LaTeX-Datei eine DVI-Datei. Diese Datei enthält alle Anweisungen für das Seitenlayout in einer drucker- bzw. device-unabhängigen Sprache.

dvips Sobald die DVI-Datei vorliegt, kann sie mit den Programmen `xdvi` oder `kdvi` betrachtet werden. `dvips` wandelt die DVI-Datei in das PostScript-Format um. Das folgende Kommando zeigt die prinzipielle Syntax des Kommandos:

```
user$  dvips [optionen] -o name.ps name.dvi
```

dvipdf Oft möchte man LaTeX-Dokumente als PDF-Datei weitergeben. Dazu gibt es viele Möglichkeiten:

- Sie wandeln die LaTeX-Datei mit `pdflatex` direkt in eine PDF-Datei um.
- Sie erzeugen zuerst mit `dvips` eine PostScript-Datei und wandeln diese dann mit `ps2pdf` oder mit dem Adobe Distiller in eine PDF-Datei um. Adobe Distiller ist Teil

des kommerziellen Programmpakets Adobe Acrobat, von dem es zurzeit leider keine Linux-Version gibt.

- Sie wandeln die DVI-Datei mit `dvipdf` oder `dvipdfm` in eine PDF-Datei um. `dvipdf` entspricht dabei dem obigen Punkt, weil als Zwischenschritt ebenfalls eine PostScript-Datei erzeugt wird.

Als Ergebnis erhalten Sie eine PDF-Datei, die wie die äquivalente PostScript-Datei aussieht. Ob auch PDF-Zusatzfunktionen (Inhaltsverzeichnis, anklickbare Links etc.) genutzt werden können, hängt vom Umwandlungsweg und von den im LaTeX-Dokument eingesetzten Zusatzpaketen ab:

- `pdflatex`: Dieses Programm sieht eine Reihe zusätzlicher LaTeX-Kommandos vor, um die PDF-Funktionen zu steuern. Sofern Sie nicht `pdflatex`-inkomptabile Pakete einsetzen, ist diese Lösung vorzuziehen.
- `dvips`/`ps2pdf` bzw. `dvipdf`: PDF-Funktionen können durch das LaTeX-Paket `hyperref` genutzt werden.
- `dvipdfm`: Hier müssen Sie zusätzliche `\special`-Kommandos in das LaTeX-Dokument einfügen.

Kapitel 18
Netzwerk-Tools

Dieses Kapitel stellt Kommandos zur Benutzung und Steuerung elementarer Netzwerkdienste vor. Sie lernen hier, wie Sie sich mit `ssh` auf einem anderen Rechner im Netzwerk einloggen, mit `wget` Dateien übertragen etc.

18.1 Netzwerkstatus ermitteln

Dieser Abschnitt gibt einen Überblick über Kommandos zum Test der Grundfunktionen des Netzwerks. Weitere Informationen zu den hier vorgestellten Kommandos finden Sie in Abschnitt 29.3, wo es um die manuelle Konfiguration des Netzwerkzugangs geht, sowie in der Syntaxreferenz am Ende des Buchs.

Netzwerkschnittstellen ermitteln

Das Kommando `ip addr` liefert eine Liste aller bekannten Netzwerkschnittstellen.

```
root#  ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc ...
    link/ether 00:1c:42:55:4f:0e brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.42/24 brd 10.0.0.255 scope global eth0
    inet6 fe80::21c:42ff:fe55:4f0e/64 scope link
       valid_lft forever preferred_lft forever
```

Typische Schnittstellen sind `eth`*n* (Ethernet), `wlan0` (WLAN) und `ppp`*n* (Internetzugang via UMTS-Modem, ADSL oder VPN). Fedora sowie Ubuntu Server verwenden mitunter andere Bezeichnungen für die Ethernet-Schnittstellen.

Eine Sonderrolle nimmt die Schnittstelle `lo` ein: Sie ermöglicht es lokalen Programmen, über das Netzwerkprotokoll zu kommunizieren. Das funktioniert selbst dann, wenn ein Rechner nicht nach außen hin mit einem Netzwerk verbunden ist.

Wenn `ip addr` nur bei der Schnittstelle `lo` eine IP-Adresse angibt, wurde noch keine Netzwerkschnittstelle aktiviert. Abhilfe schafft das von Ihrer Distribution vorgesehene Werkzeug zur Netzwerkkonfiguration. Sie können die Netzwerkschnittstelle mit dem `ip`-Kommando auch manuell aktivieren. Details dazu sowie zur IPv6-Konfiguration finden Sie in Kapitel 29, »Netzwerkkonfiguration«.

Erreichbarkeit von localhost testen

`ping` sendet einmal pro Sekunde ein kleines Netzwerkpaket an die angegebene Adresse. Wenn sich dort ein Rechner befindet, sendet dieser eine Antwort, es sei denn, eine Firewall verhindert das. `ping` läuft so lange, bis es mit Strg+C beendet wird. `ping localhost` überprüft, ob das Loopback-Interface und damit die elementaren Netzwerkfunktionen des eigenen Rechners funktionieren.

```
user$  ping localhost
PING localhost (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=0.152 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=0.114 ms
...
```

Erreichbarkeit des lokalen Netzes testen

Indem Sie an `ping` statt `localhost` die IP-Nummer eines anderen Rechners im lokalen Netz übergeben, testen Sie, ob das lokale Netz funktioniert. `-c 2` bewirkt, dass `ping` nicht endlos läuft, sondern nach zwei Paketen endet.

```
user$  ping -c 2 192.168.0.99
PING 192.168.0.99 (192.168.0.99): 56 data bytes
64 bytes from 192.168.0.99: icmp_seq=0 ttl=255 time=0.274 ms
64 bytes from 192.168.0.99: icmp_seq=1 ttl=255 time=0.150 ms
...
```

Wenn es im lokalen Netz einen Nameserver gibt, der der IP-Nummer 192.168.0.99 einen Namen zuordnet, oder wenn die Datei `/etc/hosts` diese Aufgabe übernimmt, können Sie bei `ping` statt der IP-Nummer den Rechnernamen angeben.

```
user$  ping -c 2 mars
PING mars.sol (192.168.0.99) 56(84) bytes of data.
64 bytes from mars.sol (192.168.0.99): icmp_seq=1 ttl=64 time=0.281 ms
64 bytes from mars.sol (192.168.0.99): icmp_seq=2 ttl=64 time=0.287 ms

--- mars.sol ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.281/0.284/0.287/0.003 ms
```

Internetzugang testen

Als Nächstes können Sie testen, ob die Verbindung zum Internet gelingt. Das folgende Kommando testet gleichzeitig zwei Aspekte der Netzwerkkonfiguration: die Erreichbarkeit des Nameservers und die Funktion des Gateways.

```
user$  ping -c 2 www.yahoo.com
PING www.yahoo-ht2.akadns.net (209.73.186.238) 56(84) bytes of data.
64 bytes from f1.www.vip.re3.yahoo.com (209.73.186.238): icmp_seq=1 time=122 ms
64 bytes from f1.www.vip.re3.yahoo.com (209.73.186.238): icmp_seq=2 time=123 ms

--- www.yahoo-ht2.akadns.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 122.731/123.256/123.782/0.631 ms
```

Wenn das nicht funktioniert, sind mehrere Ursachen denkbar:

- Vielleicht ist der Server von Yahoo gerade unerreichbar, oder der Server hat aus Sicherheitsgründen die Antwort auf `ping` deaktiviert. Probieren Sie eine andere bekannte Internetadresse aus.
- Für die Ermittlung der IP-Adresse zu `yahoo.com` ist der Nameserver verantwortlich. Wenn Sie die Fehlermeldung *unknown host yahoo.com* erhalten, gibt es Probleme mit dem Nameserver. Überprüfen Sie, ob `/etc/resolv.conf` dessen Adresse enthält.
- Das Gateway ist dafür zuständig, IP-Pakete aus dem lokalen Netzwerk an das Internet weiterzuleiten. Wenn das nicht funktioniert, erhalten Sie die Fehlermeldung *connect: Network is unreachable*. Die Gateway-Konfiguration können Sie mit `ip route` überprüfen. Das Kommando liefert normalerweise mehrere Zeilen. Die Gateway-Adresse befindet sich in der dritten Spalte der Zeile, die mit `default` beginnt:

  ```
  user$  ip route
  default via 10.0.0.138 dev eth0
  10.0.0.0/24 dev eth0  proto kernel  scope link  src 10.0.0.42
  ```

- Falls Sie in einem lokalen Netz einen eigenen Rechner als Gateway eingerichtet haben, besteht die Möglichkeit, dass Sie die Masquerading-Funktion vergessen haben. In diesem Fall würde der Internetzugang für das gesamte lokale Netzwerk nicht funktionieren. Eine detaillierte Anleitung zur Konfiguration eines Internet-Gateways finden Sie in Kapitel 30.

Den Weg von IP-Paketen verfolgen

Mit `traceroute` finden Sie heraus, welchen Weg ein Netzwerkpaket von Ihrem Rechner zu einem anderen Rechner nimmt und wie viele Millisekunden die Laufzeit bis zur jeweiligen Zwischenstation beträgt. Standardmäßig unternimmt das Kommando drei Versuche und liefert daher entsprechend drei Zeiten. Das Kommando funktioniert nicht, wenn sich auf einer der Zwischenstationen eine Firewall befindet, die den von `traceroute` genutzten UDP-Port 33434 blockiert. In diesem Fall liefert `traceroute` für diese und alle weiteren Stationen nur noch drei Sterne.

Die folgenden Zeilen zeigen den Weg von meinem Arbeitsrechner zu `google.at`. Zeile 1 beschreibt mein Internet-Gateway (den Rechner `mars.sol`), Zeile 2 den ADSL-Router und Zeile 3 das Gateway meines Internet-Providers. Ab Zeile 9 splittern sich die Ergebnisse zwischen verschiedenen redundanten Google-Rechnern auf.

```
user$  traceroute google.at
traceroute to google.at (66.102.9.104), 30 hops max, 40 byte packets
 1  mars.sol.0.168.192.in-addr.arpa (192.168.0.1)    0.277 ms ...
 2  192.168.1.1 (192.168.1.1)                        0.373 ms ...
 3  N704P030.adsl.highway.telekom.at (62.47.31.254)  8.598 ms ...
 4  172.19.90.193 (172.19.90.193)                   11.864 ms ...
...
14  66.102.9.104 (66.102.9.104)                     52.741 ms ...
```

mtr Das Kommando `mtr` sendet regelmäßig Netzwerkpakete zum angegebenen Host und analysiert die Antworten. Die Ergebnisliste kombiniert Daten von `ping` und `traceroute`. Beachten Sie, dass es zwei Versionen dieses Programms gibt: das hier beschriebene Textkommando sowie eine Variante mit grafischer Benutzeroberfläche. Bei Desktop-Installationen von Debian und Ubuntu ist standardmäßig die GTK-Variante installiert. Um stattdessen die Textversion zu installieren, führen Sie `apt-get install mtr-tiny` aus.

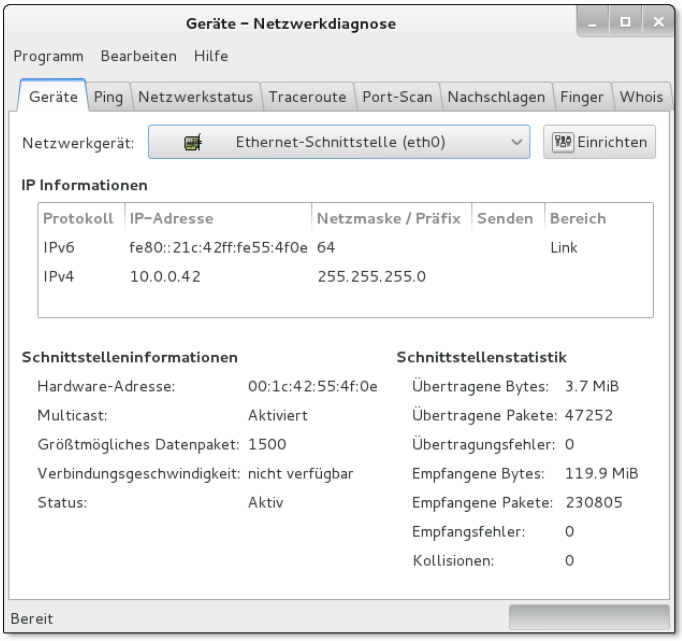


Abbildung 18.1 Netzwerkdiagnose unter Gnome

```
user$  mtr -c 10 -r google.de
HOST: michaels-computer           Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- speedtouch.lan             0.0%    10   42.6  48.5   6.0  95.9  28.9
  2.|-- 178-191-207-254.adsl.high  0.0%    10   18.9  20.4  18.6  23.2   1.9
  3.|-- 195.3.74.129               0.0%    10   19.4  18.8  17.9  19.4   0.5
  4.|-- AUX10-GRAZBC10.highway.te  0.0%    10   21.2  21.3  20.7  22.0   0.3
  5.|-- 195.3.70.154               0.0%    10   21.2  27.3  20.9  81.2  18.9
  6.|-- 62.47.120.150              0.0%    10   25.3  25.5  24.9  26.0   0.4
  7.|-- 209.85.243.119             0.0%    10   25.6  25.9  25.2  28.2   0.8
  8.|-- 216.239.46.88              0.0%    10   25.8  26.3  25.8  27.7   0.6
  9.|-- bud01s08-in-f23.1e100.net  0.0%    10   25.7  25.8  25.0  26.8   0.5
```

gnome-nettool

Wer unter Gnome arbeitet, kann einen Großteil der oben aufgezählten Informationen ganz komfortabel mit dem Programm `gnome-nettool` ermitteln (siehe Abbildung 18.1).

18.2 Auf anderen Rechnern arbeiten (SSH)

Die Programme `telnet`, `rlogin` und `ssh` ermöglichen es, so auf einem anderen Rechner zu arbeiten, als stünde er vor Ihnen. Das funktioniert sowohl für kommandoorientierte Programme als auch für X-Programme. Dieser Abschnitt beschränkt sich auf die Beschreibung von `ssh` (Secure Shell). Die älteren Programme `telnet` und `rlogin` sollten aus Sicherheitsgründen nicht mehr eingesetzt werden. Sie übertragen die Login-Informationen inklusive des Passworts unverschlüsselt.

Die Grundvoraussetzung für die Anwendung von `ssh` besteht darin, dass auf dem zweiten Rechner ein SSH-Server läuft, also das Programm `sshd`. Bei manchen Linux-Distributionen ist dies standardmäßig der Fall, bei anderen muss das Programm (zumeist als Paket `openssh-server`) zuerst installiert werden. Wenn auf den Rechnern Firewalls laufen, dürfen diese den Port 22 nicht blockieren.

Einen eigenen SSH-Server einrichten

Informationen zur Installation, Konfiguration und Absicherung eines SSH-Servers folgen in Kapitel 34. Dort erfahren Sie auch, wie Sie den SSH-Server absichern.

Gewöhnliche Shell-Session

Wenn Sie auf dem Rechner `uranus` arbeiten und nun eine Shell-Session auf dem Rechner `mars` starten möchten, führen Sie zum Verbindungsaufbau das folgende Kommando aus:

```
user@uranus$  ssh mars
user@mars's password:  ********
```

Beim ersten Verbindungsaufbau zu einem neuen Rechner erscheint eine Warnung nach dem folgenden Muster:

```
The authenticity of host 'mars (192.168.0.10)' can't be established.
RSA1 key fingerprint is 1e:0e:15:ad:6f:64:88:60:ec:21:f1:4b:b7:68:f4:32.
Are you sure you want to continue connecting (yes/no)?  yes
Warning: Permanently added 'mars,192.168.0.10' (RSA1) to the list
  of known hosts.
```

Das bedeutet, dass `ssh` sich nicht sicher ist, ob es dem Rechner `mars` mit der IP-Adresse 192.168.0.10 vertrauen darf. Es könnte sein, dass ein fremder Rechner vortäuscht, `mars` zu sein. Wenn Sie die Rückfrage mit YES beantworten, speichert `ssh` den Namen, die Adresse und den RSA-Fingerprint (einen Code zur eindeutigen Identifizierung des Partnerrechners) in `~/.ssh/known_hosts`.

Falls Sie auf `mars` unter einem anderen Login-Namen als auf `uranus` arbeiten möchten (z. B. als `root`), geben Sie den Namen mit der Option `-l` an:

```
user@uranus$  ssh -l root mars
root@mars's password:  xxx
```

SSH-Authentifizierung mit Schlüsseln

Wesentlich sicherer als ein Login mit Passwort ist die Authentifizierung durch einen Schlüssel. Die Vorgehensweise wird im Detail in Abschnitt 34.3 beschrieben. Die Verwendung von Schlüsseln ermöglicht es auch, auf SSH basierende Kommandos und Scripts automatisch per Script auszuführen.

Kommandos ausführen

Statt `ssh` interaktiv zu nutzen, können Sie auf dem entfernten Rechner auch einfach nur ein Kommando ausführen. Das Kommando und seine Parameter werden einfach als weitere Parameter an `ssh` übergeben. `ssh` endet nach diesem Kommando.

```
user@uranus$  ssh mars kommando optionen
user@mars's password:  xxx
```

Aus dieser scheinbar trivialen Funktion ergeben sich weitreichende Möglichkeiten: Sie können nun beispielsweise auf dem entfernten Rechner `tar` starten, das damit erstellte Archiv an die Standardausgabe weiterleiten (Bindestrich - nach der Option `-f`) und die Standardausgabe mit `|` als Eingabe für ein zweites `tar`-Kommando verwenden, das lokal läuft. Damit können Sie einen ganzen Verzeichnisbaum sicher via SSH kopieren.

Das folgende Kommando zeigt, wie ich den gesamten `htdocs`-Verzeichnisbaum meines Webservers `kofler.info` in das lokale Verzeichnis `~/bak` kopiere:

```
user$  ssh -l username kofler.info tar -cf - htdocs | tar -xC ~/bak/ -f -
username@kofler.info's password:  ******
```

SSH und X

Grundsätzlich kann in einer SSH-Session auch ein Programm mit grafischer Benutzeroberfläche ausgeführt werden. Das Programm läuft dann auf dem entfernten Rechner, wird aber auf dem lokalen Rechner angezeigt und empfängt dort auch alle Tastatur- und Mauseingaben. Da das gesamte Protokoll des X-Window-Grafiksystems nun über das Netzwerk läuft, ist eine gute Netzwerkverbindung erforderlich, damit komfortabel gearbeitet werden kann.

Damit `ssh` X-Programme ausführen kann, muss es mit der Option `-X` gestartet werden. (Wenn `/etc/ssh_config` die Zeile `ForwardX11 yes` enthält, kann auf die Option `-X` verzichtet werden.) `ssh` kümmert sich selbstständig um die korrekte Einstellung der `DISPLAY`-Variablen.

Die folgenden Kommandos bewirken, dass auf dem Rechner `mars` der Editor XEmacs gestartet wird. Das Editorfenster wird aber auf dem Desktop des Rechners `uranus` sichtbar und kann dort bedient werden! Das funktioniert selbst dann, wenn auf dem Rechner `mars` gar kein X-Server läuft. Alle X-Bibliotheken müssen aber installiert sein!

```
user@uranus$  ssh -X mars
user@mars's password:  xxx
user@mars$  xemacs &
```

Dateien sicher kopieren mit scp

Um eine Datei via SSH über das Netzwerk zu kopieren, gibt es das Kommando `scp`. Die Syntax sieht so aus:

```
user$  scp [[user1@]host1:]filename1 [[user2@]host2:][filename2]
user2@host2's password:  ******
```

Damit wird die Datei `filename1` vom Rechner `host1` zum Rechner `host2` übertragen und dort in der Datei `filename2` gespeichert. Einige Anmerkungen zu den vielen optionalen Bestandteilen der Kopieranweisung:

- `host1` und `host2` müssen nicht angegeben werden, wenn der lokale Rechner (also `localhost`) gemeint ist.
- `user1` muss nicht angegeben werden, wenn der aktive Benutzer gemeint ist.
- `user2` muss nicht angegeben werden, wenn auf dem Rechner `host2` der aktuelle Benutzername von `host1` bzw. `user1` verwendet werden soll.
- `filename1` darf auch ein Verzeichnis sein. Sie müssen dann die Option `-r` angeben, damit das gesamte Verzeichnis mit allen Unterverzeichnissen übertragen wird.
- `filename2` muss nicht angegeben werden, wenn der Dateiname unverändert bleiben soll. Die Datei wird dann in das Home-Verzeichnis von `user2` kopiert.

  Statt `filename2` kann auch das Zielverzeichnis angegeben werden, wobei wie üblich `~` für das Home-Verzeichnis von `user2` verwendet wird.

Zum Abschluss noch ein Beispiel: Nehmen Sie an, die Benutzerin `gabi` arbeitet auf dem Rechner `uranus`. Sie will die Datei `abc.txt` in das Verzeichnis `~/efg` auf dem Rechner `mars` übertragen. Das `scp`-Kommando sieht so aus:

```
gabi@uranus$  scp abc.txt mars:~/efg/
gabi@mars's password:  ******
```

Falls Sie beim `scp`-Kommando eine IPv6-Adresse angeben wollen, müssen Sie diese in eckige Klammern stellen. Andernfalls kommt `scp` mit den vielen Doppelpunkten durcheinander.

```
user$  scp kofler@[2001:1234:5678::1]:datei.txt .
```

SFTP

SFTP (*Secure FTP*) ist eine auf SSH basierende sichere Variante zum Protokoll FTP. Details zu SFTP folgen im nächsten Abschnitt, der die Übertragung von Dateien via FTP und HTTP zum Thema hat.

SSH-Tunnel

Eine SSH-Anwendungsmöglichkeit für fortgeschrittene Linux-Anwender ist der Tunnelbau. Derartige Tunnel eignen sich zwar nicht als Transportmöglichkeit für Autos oder Züge, sie ermöglichen aber die Übertragung aller IP-Pakete, die an einen bestimmten Port gerichtet sind. SSH-Tunnel bieten damit einen sicheren Weg, um IP-Pakete zwischen zwei Rechnern zu übertragen – und das selbst dann, wenn sich zwischen den beiden Rechnern eine Firewall befindet, die den Port eigentlich blockiert. Eine Einführung in die Welt der IP-Pakete und eine Erklärung des Begriffs *Port* finden Sie übrigens im Firewall-Abschnitt 40.1.

Wenn der Tunnelbau vom Client-Rechner aus erfolgt, kommt die Option `-L localport:localhost:remoteport` zum Einsatz. Beispielsweise bewirkt das folgende Kommando, dass der Port 3306 des Rechners `mars` über den Port 3307 des lokalen Rechners zugänglich ist. Durch das Kommando wird gleichzeitig eine SSH-Session gestartet, was Sie durch `-N` aber verhindern können (wenn Sie nur den Tunnel, aber keine Shell benötigen). Falls der Login bei `mars` unter einem anderen Namen erfolgen soll, müssen Sie den Login-Namen wie üblich durch `-l name` oder durch `name@remotehost` angeben.

```
user@uranus$  ssh -L 3307:localhost:3306 username@mars
user@mars's password:  ******
```

Der Tunnel bleibt so lange offen, bis die SSH-Session mit Strg+D beendet wird. Falls Sie `ssh` mit der Option `-N` gestartet haben, muss das Programm mit Strg+C gestoppt werden.

3306 ist der übliche Port von MySQL. Sie können nun auf dem Rechner `uranus` über dessen Port 3307 auf den MySQL-Server zugreifen, der auf `mars` läuft. Beim `mysql`-Kommando müssen der Port 3307 und der Hostname 127.0.0.1 angegeben werden,

damit der SSH-Tunnel tatsächlich benutzt wird. Standardmäßig stellt `mysql` lokale Verbindungen über eine Socket-Datei her.

```
user@uranus$  mysql -u mysqllogin -P 3307 -h 127.0.0.1 -p
Enter password:  *******
```

Damit der MySQL-Login funktioniert, müssen zwei Voraussetzungen erfüllt sein:

- Erstens muss der MySQL-Server auf dem Rechner `mars` grundsätzlich IP-Verbindungen akzeptieren. Der MySQL-Server kann aus Sicherheitsgründen auch so konfiguriert sein, dass Verbindungen nur über eine Socket-Datei möglich sind. Dann hilft ein Tunnel nicht weiter, weil ein Tunnel nur Ports verbinden kann.
- Zweitens muss der MySQL-Server die Kombination aus Login-Name und Hostname akzeptieren. Als Hostname wird der Name des Rechners verwendet, zu dem `ssh` den Tunnel errichtet hat – hier also `mars` bzw. `mars.sol`, wenn die Domain `sol` lautet.

VPN

Es gibt noch weit mehr und oft viel komplexere Anwendungsmöglichkeiten für SSH-Tunnel. Beispielsweise können Sie die Tunnel dazu verwenden, um ein Virtual Private Network zu bilden. Weiterführende Dokumentation finden Sie z. B. hier:

http://www.tldp.org/HOWTO/VPN-HOWTO

SSH-Dateisystem

Mit dem Kommando `sshfs`, das sich bei vielen Distributionen im gleichnamigen Paket befindet, können Sie das Dateisystem eines externen Rechners in den lokalen Verzeichnisbaum integrieren. Das kann beispielsweise die Durchführung von Backups vereinfachen. Beachten Sie aber, dass Sie im SSH-Dateisystem wegen der Verschlüsselung aller Daten zumeist einen geringeren Durchsatz als mit Samba oder NFS erzielen werden. Das SSH-Dateisystem ist deswegen für den Einsatz in lokalen Netzwerken nur bedingt geeignet.

```
root#  mkdir /media/ext-host
root#  sshfs user@hostname /media/ext-host
root#  ...
root#  umount /media/ext-host
```

18.3 Dateien übertragen (FTP)

FTP

Grundlagen

FTP steht für *File Transfer Protocol* und bezeichnet ein recht altes Verfahren zur Übertragung von Dateien über ein Netzwerk. Seine große Popularität verdankt FTP der Spielart Anonymous FTP: Viele große Internet-Server bieten allen Anwendern Zugang zu sogenannten FTP-Archiven. Dieser Zugang ist (im Gegensatz zum sonstigen FTP) nicht durch ein Passwort versperrt.

Ein großer Nachteil von FTP besteht darin, dass beim Login-Prozess der Benutzername und das Passwort unverschlüsselt übertragen werden. Eine sichere Alternative ist SFTP (Secure FTP) auf der Basis von SSH (siehe Abschnitt 18.3). Auch HTTP, also das Protokoll zur Übertragung von Webseiten, wird oft als Alternative zu FTP eingesetzt.

In diesem Kapitel geht es nur um die Nutzung von FTP, also um die Client-Sichtweise. Damit FTP funktioniert, muss auf der Gegenstelle ein FTP-Server laufen. Dessen Konfiguration ist in Abschnitt 35.7 beschrieben.

Kommando	Funktion
`?`	zeigt eine Liste aller FTP-Kommandos an.
`!`	ermöglicht die Ausführung von Shell-Kommandos.
`ascii`	wechselt in den Textmodus.
`binary`	wechselt in den Binärmodus.
`bye`	beendet FTP.
`cd verz`	wechselt in das angegebene FTP-Verzeichnis.
`close`	beendet die Verbindung zum FTP-Server.
`get datei`	überträgt die Datei vom FTP-Archiv in das aktuelle Verzeichnis.
`help kommando`	zeigt eine kurze Info zum angegebenen Kommando an.
`lcd verz`	wechselt das aktuelle Verzeichnis auf dem lokalen Rechner.
`ls`	zeigt die Liste der Dateien auf dem FTP-Server an.
`lls`	zeigt die Liste der Dateien auf dem lokalen Rechner an.
`mget *.muster`	überträgt alle passenden Dateien vom FTP-Archiv in das aktuelle Verzeichnis (siehe auch `prompt`).
`open`	stellt die Verbindung zum fremden Rechner her (wenn es beim ersten Versuch nicht geklappt hat).
`prompt`	aktiviert/deaktiviert die automatische Rückfrage vor der Übertragung jeder Datei durch `mget`.
`put datei`	überträgt die Datei vom aktuellen Verzeichnis in das FTP-Archiv (*upload*)
`quit`	beendet FTP.
`reget datei`	setzt die Übertragung einer bereits teilweise übertragenen Datei fort.
`user`	ermöglicht einen neuen Login.

Tabelle 18.1 ftp-Kommandos

FTP-Kommando

Der Urahn aller FTP-Clients ist das interaktive Textkommando `ftp`. Da es Dateien normalerweise aus dem aktuellen Verzeichnis bzw. in das aktuelle Verzeichnis überträgt, sollten Sie vor dem Start von `ftp` mit `cd` in das gewünschte Arbeitsverzeichnis wech-

seln. Die FTP-Sitzung wird dann mit dem Kommando `ftp user@ftpservername` oder einfach `ftp ftpservername` eingeleitet. Falls Sie Anonymous FTP nutzen möchten, geben Sie als Benutzernamen `anonymous` ein.

Nach dem Verbindungsaufbau und der Eingabe des Passworts kann es losgehen: Mit den Kommandos `cd`, `pwd` und `ls`, die dieselbe Bedeutung wie unter Linux haben, können Sie sich durch die Verzeichnisse des FTP-Archivs bewegen. Um eine Datei vom FTP-Archiv in das aktuelle Verzeichnis Ihres Rechners zu übertragen, führen Sie `get datei` aus. Der Dateiname bleibt dabei unverändert.

Umgekehrt können Sie mit `put` eine Datei aus Ihrem aktuellen Verzeichnis in ein Verzeichnis des FTP-Archivs übertragen. Das geht freilich nur dann, wenn Sie eine Schreiberlaubnis für das Verzeichnis haben. Bei Anonymous FTP ist das zumeist nur für ein Verzeichnis mit einem Namen wie `/pub/incoming` der Fall. Die FTP-Sitzung wird mit dem Kommando `quit` oder `bye` beendet. Eine Referenz der wichtigsten FTP-Kommandos gibt Tabelle 18.1.

Text- versus Binärmodus

Bevor Sie eine Datei übertragen, müssen Sie mit `binary` in den Binärmodus umschalten. Im Textmodus interpretiert FTP die Dateien als Texte und versucht, diese in das Format des jeweiligen Rechners zu konvertieren. Binärdateien werden durch so eine Konvertierung unbrauchbar. Die meisten FTP-Server sind glücklicherweise so konfiguriert, dass `binary` als Grundeinstellung gilt.

Die folgenden Zeilen zeigen den Download des Linux-Kernelcodes von einem FTP-Server:

```
user$  cd ~/src
user$  ftp ftp.kernel.org
Connected to zeus-pub.kernel.org.
220 Welcome to ftp.kernel.org.
Name (ftp.kernel.org:kofler):  anonymous
331 Please specify the password.
Password:  name@mysite.de
Using binary mode to transfer files.
ftp>  cd pub/linux/kernel/v3.0
250 Directory successfully changed.
ftp>  ls
...
ftp>  get linux-3.10.tar.bz2
local: linux-3.10.tar.bz2 remote: linux-3.10.tar.bz2
227 Entering Passive Mode (204,152,191,5,20,69)
150 Opening BINARY mode data connection for linux-3.10.tar.bz2 (69305709 bytes).
...
ftp>  quit
```

Andere FTP-Programme

Das Kommando `ftp` ist nicht komfortabel zu bedienen. Zum Glück gibt es unzählige Alternativen:

- Webbrowser, Dateimanager: Alle unter Linux verfügbaren Webbrowser und Dateimanager können auch zum FTP-Download verwendet werden. Manche Programme ermöglichen sogar einen komfortablen Upload.
- Grafische FTP-Clients: Programme wie `gftp` (Gnome) sind speziell für tpyische FTP-Aufgaben optimiert. Sie bieten Spezialfunktionen wie Bookmark- und Passwortverwaltung, die parallele Übertragung mehrerer Dateien, die Synchronisation von Verzeichnissen etc.
- `ncftp`: Diese Alternative zu `ftp` hat zwar eine textbasierte Benutzeroberfläche, ist aber komfortabler als das Original zu bedienen.
- `sftp`: Dieses Programm ist ähnlich minimalistisch wie `ftp`, aber dafür deutlich sicherer. Allerdings muss an der Gegenstelle ein SSH-Server laufen (kein FTP-Server). `sftp` wird im folgenden Abschnitt beschrieben.
- `wget`, `curl`, `lftp`: Diese Kommandos helfen bei der automatisierten Übertragung von Dateien bzw. ganzer Verzeichnisbäume via FTP (siehe Abschnitt 18.3).

FTP-Adresse mit Passwort

Wenn Sie das Protokoll FTP nicht als Benutzer `anonymous` nutzen möchten, sondern sich mit Name und Passwort anmelden können, gilt bei den meisten FTP-Clients die folgende Syntax:

```
ftp://benutzername:password@servername
```

Passiver Modus

Manche FTP-Clients funktionieren nicht richtig, wenn sich zwischen Ihrem Rechner und dem FTP-Server eine Firewall befindet oder wenn Sie in einem lokalen Netzwerk arbeiten, das mittels Masquerading mit dem Internet verbunden ist. In solchen Fällen hilft es fast immer, den Client in einen sogenannten passiven Modus zu versetzen. Leider gibt es dafür kein einheitliches Kommando – werfen Sie also einen Blick in die Dokumentation! Die meisten Clients erkennen derartige Situationen selbstständig und aktivieren den passiven Modus automatisch.

SFTP (Secure FTP)

Das Kommando `sftp` ist Teil des `openssh`-Pakets. `sftp` verwendet intern ein ganz anderes Protokoll als `ftp` und kann wie `ssh` nur eingesetzt werden, wenn auf der Gegenstelle ein SSH-Server läuft. Anonymous FTP ist mit `sftp` nicht möglich. Davon abgesehen, erfolgt die Bedienung des Programms wie die von `ftp`. Mit `sftp -b batchdatei` können Sie SFTP-Downloads automatisieren.

SFTP-Alternative

Vielen ist `sftp` zu spartanisch. Die Auswahl komfortablerer SFTP-Clients ist allerdings kleiner als bei FTP. Außerdem ist manchmal etwas Überredungskunst erforderlich, bis der Verbindungsaufbau klappt:

- `gftp`: `gftp` bietet vielseitige SFTP-Konfigurationsmöglichkeiten (FTP • OPTIONEN • SSH). Wenn es Probleme gibt, achten Sie darauf, dass Sie den richtigen Port verwenden (22 für SSH, nicht 21 wie bei FTP). Häufig müssen Sie außerdem VERWENDE SSH2 SFTP FUNKTIONEN im Optionsdialog aktivieren.
- KDE, Gnome: Mit Dolphin oder Nautilus initiieren Sie eine SFTP-Verbindung, indem Sie die Adresse `sftp://user@servername` eingeben. Nach der Passwortabfrage verhält sich Konqueror wie bei einem lokalen Verzeichnis. Beide Dateimanager unterstützen auch direkt das SSH-Protokoll, das selbst dann funktioniert, wenn `sftp` nicht zur Verfügung steht. Dazu geben Sie die Adresse in der Form `fish://user@servername` an.

wget

Der interaktive Ansatz des Kommandos `ftp` ist zur Automatisierung von Downloads – beispielsweise in einem Script – ungeeignet. Auch sonst ist `ftp` reichlich inflexibel. Beispielsweise ist es unmöglich, einen unterbrochenen Download selbstständig wieder aufzunehmen. Abhilfe schafft das Kommando `wget`, das speziell zur Durchführung großer Downloads bzw. zur Übertragung ganzer Verzeichnisse konzipiert ist. `wget` unterstützt gleichermaßen die Protokolle FTP, HTTP und HTTPS.

Beispiele

In der Grundform lädt `wget` die angegebene Datei einfach herunter:

```
user$  wget ftp://myftpserver.de/name.abc
```

Wenn der Download aus irgendeinem Grund unterbrochen wird, kann er mit `-c` ohne Umstände wieder aufgenommen werden:

```
user$  wget -c ftp://myftpserver.de/name.abc
```

Downloads von großen Dateien, beispielsweise von ISO-Images von Linux-Distributionen, dauern selbst mit einem guten Internetzugang oft Stunden. Es bietet sich daher an, den Download über Nacht durchzuführen. Das folgende Kommando stellt nahezu sicher, dass sich die Datei am nächsten Morgen tatsächlich auf dem Rechner befindet. Wegen `-t 20` wird der Download nach einem Verbindungsabbruch bis zu 20-mal neu aufgenommen. `--retry-connrefused` bewirkt, dass selbst nach dem Fehler *connection refused* ein neuer Versuch gestartet wird. Das ist dann zweckmäßig, wenn der Download-Server bekanntermaßen unzuverlässig ist und immer wieder für kurze Zeit unerreichbar ist.

```
user$  wget -t 20 --retry-connrefused http://mydownloadserver.de/name.iso
```

Das folgende Kommando lädt sämtliche Dateien herunter, die notwendig sind, um die angegebene Webseite später in unverändertem Zustand offline zu lesen. Kurz zur Bedeutung der Optionen: `-p` lädt auch CSS-Dateien und Bilder herunter. `-k` verändert in den heruntergeladenen Dateien die Links, sodass diese auf lokale Dateien verweisen. `-E` fügt heruntergeladenen Script-Dateien (ASP, PHP etc.) die Kennung `.html` hinzu. `-H` verfolgt auch Links auf externe Websites.

```
user$  wget -p -k -E -H http://mywebsite.de/seite.html
```

Wenn Sie eine ganze Website offline lesen möchten, hilft das folgende rekursive Download-Kommando (Option `-r`). Die Rekursionstiefe wird durch `-l 4` auf vier Ebenen limitiert.

```
user$  wget -r -l 4 -p -E -k http://mywebsite.de
```

curl

Das Kommando `curl` hilft dabei, Dateien von oder zu FTP-, HTTP- oder sonstigen Servern zu übertragen. Die `man`-Seite listet eine beeindruckende Palette von Protokollen auf, die `curl` beherrscht. In diesem Abschnitt beschränke ich mich allerdings auf FTP-Uploads. Für die Script-Programmierung besonders praktisch ist, dass `curl` auch Daten aus der Standardeingabe verarbeiten bzw. zur Standardausgabe schreiben kann. Sie müssen also nicht zuerst eine `*.tar.gz`-Datei erstellen und diese dann zum FTP-Server übertragen, sondern können beide Operationen mittels einer Pipe gleichzeitig ausführen.

Das folgende Kommando überträgt die angegebene Datei zum FTP-Server `backupserver` und speichert sie im Verzeichnis `verz`:

```
user$  curl -T datei -u username:password ftp://backupserver/verz
```

Um Daten aus dem Standardeingabekanal zu verarbeiten, geben Sie mit `-T` als Dateinamen einen Bindestrich an. Das folgende Kommando speichert das aus dem `tar`-Kommando resultierende Ergebnis direkt in der Datei `name.tgz` auf dem FTP-Server:

```
user$  tar czf - verz/ | curl -T - -u usern:pw ftp://bserver/name.tgz
```

lftp

`lftp` ist eigentlich ein komfortabler interaktiver FTP-Client. Das Kommando eignet sich aber auch gut, um FTP-Uploads oder andere Kommandos in einem Script auszuführen. Dazu können Sie an `lftp` entweder mit `-c` mehrere durch Strichpunkte getrennte FTP-Kommandos übergeben oder mit `-f` eine Datei angeben, die diese Kommandos zeilenweise enthält. Das erste Kommando wird dabei immer

`user` *benutzername*`,`*passwort servername* lauten, um die Verbindung zum FTP-Server herzustellen. Das folgende Kommando demonstriert einen Datei-Upload:

```
root#  lftp -c "open -u username,password backupserver; put www.tgz"
```

Wenn Sie der Datei auf dem FTP-Server einen anderen Namen geben möchten, geben Sie zusätzlich die Option `-o` *neuerName* an. `lftp` zeigt während des Uploads den aktuellen Fortschritt an.

Um statt einer Datei ein ganzes Verzeichnis zum Backup-Server zu übertragen, verwenden Sie das Kommando `mirror -R`. (`mirror` kopiert normalerweise Verzeichnisse vom FTP-Server auf den lokalen Rechner. `-R` dreht die Übertragungsrichtung um.) Auch hierzu ein Beispiel:

```
root#  lftp -c "open -u usern,passw bserver; mirror -R verzeichnis"
```

Im Unterschied zu anderen FTP-Clients unterstützt `lftp` das Kommando `du`, mit dem Sie feststellen können, wie viel Speicherplatz Ihre Backup-Dateien bereits belegen. Das ist dann wichtig, wenn Ihr Speicherplatz auf dem Backup-Server streng limitiert ist. Das folgende Kommando zeigt, wie Sie ohne interaktiven Eingriff den bereits belegten Speicherplatz ermitteln. Option `-s` gibt an, dass Sie nur an der Endsumme interessiert sind. `-m` bewirkt, dass als Maßeinheit MByte verwendet wird.

```
user$  lftp -c "open -u username,password bserver; du -s -m"
2378   .
```

Wenn Sie das Ergebnis für eine Berechnung verwenden möchten, stört die zweite Spalte (also der Punkt, der angibt, dass sich der Zahlenwert auf das aktuelle Verzeichnis bezieht). Stellen Sie dem Kommando einfach `cut -f 1` hintan, um die erste Spalte zu extrahieren:

```
user$  lftp -c "open -u usern,passw bserver; du -s -m" | cut -f 1
2378
```

rsync, mirror, sitecopy

`rsync` hilft dabei, ganze Verzeichnisbäume zu kopieren bzw. zu synchronisieren. Eine ausführliche Beschreibung dieses Kommandos finden Sie in Abschnitt 39.4. Sofern auf dem Partnerrechner weder ein SSH- noch ein `rsync`-Server läuft, können Sie anstelle von `rsync` auf die Kommandos `mirror` oder `sitecopy` zurückgreifen. Das Perl-Script `mirror` aus dem gleichnamigen Paket kopiert ganze Verzeichnisbäume von einem FTP-Server auf den lokalen Rechner. Das Kommando `sitecopy` ist hingegen dahingehend optimiert, einen Verzeichnisbaum auf einen Webserver hochzuladen, wobei der Datentransfer wahlweise via FTP oder WebDAV erfolgt.

Kapitel 19
Vim

Im Mittelpunkt dieses Kapitels stehen der Editor Vi und dessen Open-Source-Implementierung Vim (*Vi Improved*). Diese Editoren sind – ebenso wie der im nächsten Kapitel vorgestellte Editor Emacs – relativ schwer zu erlernen. Dieser Aufwand lohnt sich nur, wenn Sie ständig Text, Programmcode, HTML-Dokumente etc. bearbeiten, wenn ein Texteditor also ein ständiges und unverzichtbares Werkzeug für Sie ist. Wenn Sie zu dieser Zielgruppe gehören, bieten Vi und Emacs Ihnen schier unendlich viele Spezialfunktionen.

Bleibt noch die Königsfrage: Vi oder Emacs? Beide Programme sind Urgesteine der Unix/Linux-Geschichte. Beide bieten unzählige Spezialfunktionen, z. B. die automatische Syntaxhervorhebung für zahllose Programmiersprachen und Dokumenttypen oder das Suchen und Ersetzen mit regulären Ausdrücken. Über die Frage, welches Programm nun besser ist, wurden im Internet schon endlose Diskussionen geführt. Wirklich objektiv kann auch ich die Frage nicht beantworten: Da ich sämtliche Auflagen dieses Buchs mit Emacs-Varianten verfasst habe (dieses Kapitel natürlich ausgenommen, so viel Vi muss sein!), ist mir der Emacs viel vertrauter als irgendwelche Vi-Varianten.

Persönlich erscheint mir der Editor Emacs intuitiver zu bedienen und einfacher zu erlernen. Beim Vi treibt einen die Unterscheidung zwischen dem Standard- und dem Einfügemodus anfänglich leicht zum Wahnsinn. Für Vi & Co. spricht andererseits, dass das Programm ein De-facto-Standard unter Unix/Linux ist. Es beansprucht wesentlich weniger Ressourcen und steht selbst auf minimalen Rescue-Systemen zur Verfügung, wo für den Emacs kein Platz mehr ist. Echte Unix/Linux-Freaks sollten ohnedies beide Editoren in ihren Grundfunktionen beherrschen – und viel mehr vermittle ich in diesem Buch nicht.

Der ursprüngliche Editor Vi ist ein kommerzielles Programm und steht daher unter Linux nicht zur Verfügung. Vim ist dagegen ein Open-Source-Programm, das zu Vi kompatibel ist und darüber hinaus zahllose Verbesserungen und Erweiterungen bietet. Das Programm kann wahlweise mit den Kommandos `vi` oder `vim` gestartet werden.

Vim im Grafikmodus

Grundsätzlich wird Vim in einer Textkonsole bzw. in einem Konsolenfenster ausgeführt. Wenn Sie ein richtiges Menü und ordentliche Bildlaufleisten bevorzugen, sollten Sie einen Blick auf `gvim` werfen (siehe Abbildung 19.1). Diese grafische Variante zu Vim muss eventuell extra installiert werden, wobei der Paketname meist `vim-X11` oder `vim-gnome` lautet.

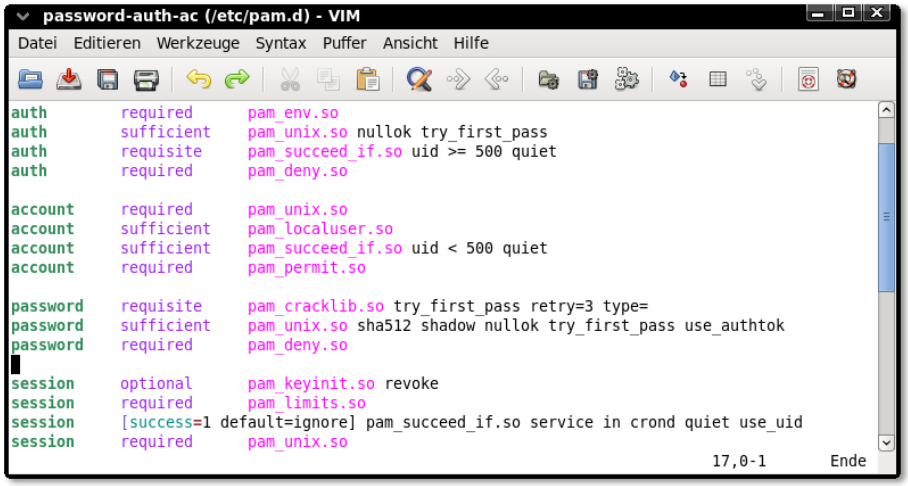


Abbildung 19.1 Die grafische Variante des Editors vim

Links

Aus Platzgründen kann dieses Kapitel nur eine Einführung zu Vim geben. Für Einsteiger sehr hilfreich ist das Tutorial, das Sie durch das Kommando `vimtutor` starten. (Dadurch wird `vim` gestartet und ein deutschsprachiger Hilfetext geladen, der eine Einführung sowie Beispiele zum Ausprobieren enthält.) Die folgenden Links verweisen auf Seiten mit weiterführenden Informationen:

http://www.vim.org	(Homepage)
http://vimdoc.sourceforge.net/vimfaq.html	(FAQ)
http://www.tuxfiles.org/linuxhelp/vimcheat.html	(Tastenkürzel)
http://www.truth.sk/vim/vimbook-OPL.pdf	(500-seitiges Vim-Buch)

Vim ist Charityware

Der Hauptentwickler Bram Moolenaar bezeichnet Vim als »Charityware«: Vim ist kostenlos unter einer GPL-kompatiblen Lizenz verfügbar. Wer Vim regelmäßig nutzt, wird aber gebeten, sich in Form einer Spende zu bedanken, die einer Kinderhilfsorganisation in Uganda zugutekommt. Weitere Informationen liefert das Vim-Kommando Esc : `help uganda` ↵.

19.1 Schnelleinstieg

Sie starten Vim üblicherweise in der Form `vim dateiname` innerhalb einer Textkonsole oder in einem Konsolenfenster. Die zu ändernde Datei wird direkt in der Konsole angezeigt.

Standardmodus

Bevor Sie darauflosschreiben können, müssen Sie sich allerdings mit einer Eigenheit auseinandersetzen: Das Programm unterscheidet zwischen unterschiedlichen Bearbeitungsmodi. Der Standardmodus dient nicht zur Eingabe von Text, sondern zur Ausführung von Kommandos. Wenn Sie im Standardmodus beispielsweise [L] eingeben, bewegen Sie damit den Cursor um ein Zeichen nach links. [D] [W] löscht ein Wort, [P] fügt es an der aktuellen Cursorposition wieder ein etc.

Einfügemodus

Um Text einzugeben, müssen Sie mit [I] (*insert*) oder [A] (*append*) in den Einfügemodus wechseln. `vim` zeigt nun in der untersten Zeile ganz links den Text `-- EINFÜGEN --` an. Im Einfügemodus können Sie Text eingeben, den Cursor bewegen und einzelne Zeichen löschen ([Entf] und [←]). Der Unterschied zwischen [I] und [A] besteht darin, dass die Eingabe bei [I] an der aktuellen Cursorposition beginnt, bei [A] beim Zeichen dahinter.

Bevor Sie wieder ein Kommando eingeben können, müssen Sie mit [Esc] zurück in den Standardmodus wechseln. Dieser Modus wird nicht extra gekennzeichnet. Der linke Teil der letzten Zeile ist jetzt also leer.)

Moduswechsel ohne Änderung der Cursorposition

Beim Wechsel vom Einfüge- in den Standardmodus bewegt sich der Cursor um ein Zeichen nach links – es sei denn, er steht bereits am Beginn einer Zeile. Dieses merkwürdige Verhalten ist laut Vim-FAQ beabsichtigt und kann nicht verhindert werden. Um ein einzelnes Kommando auszuführen, ohne den Einfügemodus zu verlassen – und damit auch ohne die aktuelle Cursorposition zu verändern –, leiten Sie die Kommandoeingabe mit [Strg]+[O] ein.

Text löschen

Im Einfügemodus können Sie mit [Entf] und [←] wie üblich einzelne Zeichen löschen. Wenn Sie Wörter, Zeilen oder ganze Bereiche löschen möchten, wechseln Sie zuerst mit [Esc] in den Standardmodus. Anschließend löscht [D], [W] ein Wort und [D], [D] eine ganze Zeile. Wenn Sie eine Zahl voranstellen, wird das Löschkommando entsprechend oft wiederholt. [5], [D], [D] löscht also fünf Zeilen. [.] wiederholt das zuletzt ausgeführte Kommando.

Tastenkürzel	Funktion
I	aktiviert den Einfügemodus.
A	aktiviert den Einfügemodus. Die Texteingabe beginnt beim nächsten Zeichen.
Esc	aktiviert den Standardmodus bzw. bricht die Kommandoeingabe ab.
Kommandos im Standardmodus	
D, W	löscht ein Wort.
D, D	löscht die aktuelle Zeile.
n D, D	löscht *n* Zeilen.
P	fügt den zuletzt gelöschten Text hinter der Cursorposition ein.
⇧+P	fügt den zuletzt gelöschten Text vor der Cursorposition ein.
.	wiederholt das letzte Kommando.
U	macht die letzte Änderung rückgängig (Undo).
⇧+U	widerruft alle Änderungen in der aktuellen Zeile.
Strg+R	macht Undo rückgängig (Redo, ab Vim 7).
: w	speichert die Datei.
: q	beendet `vim`.
: q!	beendet `vim` auch dann, wenn es nicht gespeicherte Dateien gibt.
Kommandos im Einfügemodus	
Strg+O *kommando*	führt das Kommando aus, ohne den Einfügemodus zu verlassen.

Tabelle 19.1 Elementare Kommandos

P (*put*) fügt den zuletzt gelöschten Text hinter der aktuellen Cursorposition ein, ⇧+P davor. U (*undo*) widerruft die letzten Änderungen, Strg+R (*redo*) stellt die Änderungen wieder her. (Vim 6 kann nur die letzte Änderung widerrufen, ein nochmaliges U stellt die Änderung wieder her.)

Speichern und beenden

Um die geänderte Datei zu speichern, wechseln Sie mit Esc in den Standardmodus und geben dann das Kommando : w ↵ (*write*) ein. : q ↵ (*quit*) beendet den Editor, sofern alle offenen Dateien gespeichert sind. Mit : q! ↵ erzwingen Sie ein Ende selbst dann, wenn es nicht gespeicherte Änderungen gibt. : wq ↵ kombiniert das Speichern und das Programmende.

Hilfe

Vim stellt eine umfassende Online-Hilfe in englischer Sprache zur Verfügung. Zur Startseite des Hilfesystems gelangen Sie von jedem Modus aus mit F1. Alternativ führen im Standardmodus : help bzw. : help *thema* zur Hilfe. Wenn Sie wissen möchten, welche Hilfethemen es gibt, die das Schlüsselwort *abc* enthalten, geben Sie : help *abc* Strg+D ein.

Das Hilfefenster

Der Hilfetext wird in einem eigenen Teilbereich von vim angezeigt (einem sogenannten Fenster, auch wenn es sich dabei nicht um ein eigenständiges Fenster im Sinne des Linux-Grafiksystems handelt). Dieses Fenster schließen Sie mit : q wieder. Sie können das Hilfefenster aber auch geöffnet lassen und im ursprünglichen Text weiterarbeiten. Dazu wechseln Sie mit Strg+W, W das gerade aktive Fenster. Mehr Informationen zum Umgang mit vim-Fenstern, -Puffern und zur Bearbeitung mehrerer Dateien folgen in Abschnitt 19.5.

Navigation in der Hilfe

Im Hilfetext sind Verweise auf andere Hilfethemen hervorgehoben (in der von mir getesteten Version hellblau). Um zu diesem Thema zu springen, bewegen Sie den Cursor auf das Schlüsselwort und führen Strg+] aus. Noch einfacher geht es, wenn die Maus aktiviert ist (siehe Abschnitt 19.7): Dann reicht ein Doppelklick auf das Hilfethema, um dorthin zu springen. Strg+T führt zur ursprünglichen Seite zurück.

19.2 Cursorbewegung

Die Cursortasten funktionieren sowohl im Standardmodus als auch im Einfügemodus. Außerdem können Sie die Cursorposition durch diverse Tastenkombinationen im Standardmodus ändern (siehe Tabelle 19.2). Vi-Freaks bewegen sich damit effizienter durch den Text als mit den Cursortasten.

Eine Eigenheit von vim besteht darin, dass ← am Beginn einer Zeile den Cursor nicht an das Ende der vorherigen Zeile stellt. Analog funktioniert auch → am Ende einer Zeile nicht wie gewohnt. Um das übliche Verhalten anderer Editoren zu erzielen, führen Sie im Standardmodus : set whichwrap=b,s,<,>,[,] aus bzw. fügen dieses set-Kommando in .vimrc ein.

Cursorpositionen speichern

M *buchstabe* speichert die aktuelle Cursorposition in einem Positionsmarker. Mit ' *buchstabe* bewegen Sie den Cursor zurück an die so gespeicherte Position.

Vim merkt sich die Cursorposition, an der eine neue Cursorbewegung beginnt. ' ' führt zurück zu dieser Position. Nochmals ' ' bewegt den Cursor wieder an die letzte Position. ' [bzw. '] bewegen den Cursor an den Beginn bzw. das Ende des zuletzt veränderten Textabschnitts.

Tastenkürzel	Funktion
Cursortasten	Die Cursortasten haben die übliche Bedeutung.
H / L	bewegt den Cursor nach links/rechts.
J / K	bewegt den Cursor nach unten/oben.
⇧+H / ⇧+L	bewegt den Cursor an den Beginn bzw. das Ende der aktuellen Seite.
⇧+M	bewegt den Cursor in die Mitte der aktuellen Seite.
B / W	bewegt den Cursor um ein Wort nach links/rechts.
E	bewegt den Cursor an das Ende des Worts.
G, E	bewegt den Cursor an den Anfang des Worts.
(,)	bewegt den Cursor an den Beginn des aktuellen/nächsten Satzes.
{, }	bewegt den Cursor an den Beginn des aktuellen/nächsten Absatzes.
^, $	bewegt den Cursor an den Beginn bzw. das Ende der Zeile.
⇧+G	bewegt den Cursor an das Ende der Datei.
G, G	bewegt den Cursor an den Beginn der Datei.
n ⇧+G	bewegt den Cursor in die Zeile *n*.
n |	bewegt den Cursor in die Spalte *n*.
%	bewegt den Cursor zum korrespondierenden Klammerzeichen ()[]{}.

Tabelle 19.2 Tastenkürzel zur Cursorbewegung im Standardmodus

Wo bin ich?

Im Einfügemodus zeigt Vim rechts in der Statuszeile die aktuelle Zeilen- und Spaltennummer sowie eine Prozentzahl an, die angibt, in welchem Abschnitt des Texts Sie sich befinden (z. B. 92 % – also in den letzten 10 Prozent). Mit Strg+G. zeigt Vim in der Statuszeile auch den Namen der Datei, ihren Zustand (z. B. *Verändert*), die gesamte Länge in Zeilen und die relative Position im Text in Prozent an.

19.3 Text bearbeiten

Textzeichen mehrfach einfügen

Um ein Textzeichen mehrfach einzufügen, geben Sie im Standardmodus die Anzahl, das Kommando A (*append*), das gewünschte Zeichen und schließlich Esc ein. Um also 50-mal das Zeichen = einzugeben, geben Sie 5, 0, A, =, Esc ein. Nach dem Kommando befinden Sie sich wieder im Standardmodus.

Tippfehler

Vim hilft auch bei der Korrektur typischer Tippfehler: ~ ändert die Groß- und Kleinschreibung des aktuellen Buchstabens. X, P vertauscht die folgenden zwei Buchstaben.

Text löschen

Tabelle 19.3 gibt einen Überblick über die wichtigsten Kommandos zum Löschen von Text. Wenn Sie vor dem Löschkommando eine Zahl eingeben, wird das Löschkommando entsprechend oft wiederholt. Wie für alle anderen Vim-Kommandos gilt: . wiederholt das letzte Kommando, *n* . wiederholt es *n*-mal.

Tastenkürzel	Funktion im Einfügemodus
Entf, ←	Diese Tasten haben die übliche Bedeutung.
	Funktion im Standardmodus
X	löscht das Zeichen an der Cursorposition bzw. den markierten Text.
⇧+X	löscht das Zeichen vor dem Cursor.
D, D	löscht die aktuelle Zeile.
D *cursorkommando*	löscht den Text entsprechend dem Kommando zur Cursorbewegung (siehe Tabelle 19.2). Beispiele: D, $ löscht bis zum Ende der Zeile. D, B löscht das vorige Wort. D, W löscht das nächste Wort.

Tabelle 19.3 Text löschen

Text wird grundsätzlich in ein Kopierregister gelöscht. Der zuletzt gelöschte Text kann von dort mit ⇧+P an der aktuellen Cursorposition bzw. mit P hinter der Cursorposition wieder in den Text eingefügt werden.

Eine eigentümliche Art, Text zu löschen und dann durch neuen Text zu ersetzen, bieten die C-Kommandos (*change*): Beispielsweise löscht C, W das aktuelle Wort und aktiviert den Einfügemodus. Sie geben nun das neue Wort ein und schließen die Eingabe mit Esc ab. Analog funktioniert C auch für andere Cursorkommandos.

Text kopieren

Sie können Text auch in das Kopierregister einfügen, ohne ihn zu löschen. Tabelle 19.4 fasst die entsprechenden Kommandos zusammen. Alle gelten für den Standardmodus.

Tastenkürzel	Funktion
Y	kopiert den markierten Text in das Kopierregister.
Y, Y	kopiert die aktuelle Zeile in das Kopierregister.
Y *cursorkommando*	kopiert den durch die Cursorbewegung erfassten Text; Beispiel: Y, } kopiert den Text bis zum Ende des Absatzes.

Tabelle 19.4 Text in das Kopierregister kopieren

Text markieren

Einige (Lösch-)Kommandos setzen voraus, dass Sie zuerst einen Textausschnitt markieren. Vim sieht dazu drei verschiedene Markierungsmodi vor, die Sie mit V, ⇧+V bzw. Strg+V am Startpunkt der Markierung aktivieren bzw. ebenso wieder deaktivieren. Während einer dieser Modi aktiv ist, enthält die unterste Vim-Zeile den Text `-- VISUELL --`. Sie bewegen den Cursor nun zum Endpunkt der Markierung oder erweitern die Markierung durch einige spezielle Markierungskommandos (siehe Tabelle 19.5). Solange der Markierungsmodus aktiv ist, stehen Ihnen diverse Kommandos zur Bearbeitung des markierten Texts zur Auswahl (siehe Tabelle 19.6).

Tastenkürzel	Funktion
V	(de)aktiviert den Zeichenmarkierungsmodus.
⇧+V	(de)aktiviert den Zeilenmarkierungsmodus.
Strg+V	(de)aktiviert den Blockmarkierungsmodus.
A, W	vergrößert die Markierung um ein Wort.
A, S	vergrößert die Markierung um einen Satz.
A, P	vergrößert die Markierung um einen Absatz.
A, B	vergrößert die Markierung um eine ()-Ebene.
A, ⇧+B	vergrößert die Markierung um eine {}-Ebene.
G, V	markiert den zuletzt markierten Text nochmals.
O	wechselt die Cursorposition zwischen Markierungsanfang und -ende.

Tabelle 19.5 Text markieren

Tastenkürzel	Funktion
X	löscht den markierten Text.
Y	kopiert den markierten Text in das Kopierregister.
~	ändert die Groß-/Kleinschreibung.
J	fügt die markierten Zeilen zu einer langen Zeile zusammen.
G, Q	führt einen Zeilenumbruch durch (für Fließtext).
>, <	rückt den Text um eine Tabulatorposition ein oder aus.
=	rückt den Text dem aktuellen `indent`-Modus entsprechend neu ein.
!sort	sortiert die Zeilen mit dem externen Kommando `sort`.

Tabelle 19.6 Markierten Text bearbeiten

Zeilen einrücken

Gerade beim Editieren von Code ist das richtige Einrücken von Zeilen wichtig. Vim hilft dabei auf vielfältige Weise. Die elementarsten Kommandos sind [>], [>] bzw. [<], [<]. Sie rücken die aktuelle Zeile um eine Tabulatorposition ein oder aus. Wenn Sie vorher mehrere Zeilen Text markieren, können Sie die Kommandos auf einen ganzen Block anwenden. Dabei reicht die einfache Eingabe von [>] bzw. [<]. [:] `set shiftwidth=`*n* verändert die Einrücktiefe (normalerweise 8 Zeichen).

Vim kann auch versuchen, neue Zeilen schon während der Eingabe automatisch einzurücken. Dazu aktivieren Sie einen Einrückmodus, beispielsweise durch [:] `set cindent`. Im Folgenden sind die Grundfunktionen der wichtigsten Vim-Einrückmodi kurz zusammengefasst:

- **autoindent:** Rückt die folgende Zeile genauso weit ein wie die vorherige.
- **smartindent:** Funktioniert wie `autoindent`, berücksichtigt aber zusätzlich {}-Klammerebenen. Damit Vim die schließenden Klammern richtig erkennt, sollten diese am Beginn einer neuen Zeile angegeben werden. Das Ausmaß der Einrückung je nach Klammernebene steuern Sie durch die Option `shiftwidth`. Zuvor markierter Text kann durch [=] neu eingerückt werden.
- **cindent:** Funktioniert wie `smartindent`, berücksichtigt aber auch diverse Codestrukturen von C bzw. C++. Der Einrückmechanismus kann durch verschiedene Optionen den persönlichen Vorlieben angepasst werden (siehe [:] `help C-indenting`).

Fließtext

Vim ist so vorkonfiguriert, dass das Verfassen von Code bzw. das Ändern von Konfigurationsdateien möglichst gut funktioniert. Aus diesem Grund führt Vim keinen automatischen Zeilenumbruch durch (d. h., Sie müssen neue Zeilen selbst mit [↵] beginnen). Sie können Vim aber selbstverständlich auch zum Verfassen gewöhnlichen Texts einsetzen (etwa für E-Mails). Tabelle 19.7 fasst einige spezielle Kommandos und Optionen zusammen, die dabei helfen:

Tastenkürzel	Funktion
[⇧]+[J]	verbindet die aktuelle Zeile mit der folgenden.
n [⇧]+[J]	verbindet *n* Zeilen zu einer langen Zeile.
[G], [Q], [A], [P]	umbricht den aktuellen Absatz neu und stellt den Cursor an den Beginn des nächsten Absatzes.
[G], [W], [A], [P]	wie oben, aber belässt den Cursor am aktuellen Ort.
[:] `set textwidth=`*n*	automatischer Zeilenumbruch nach maximal *n* Zeichen (normalerweise: 0 = deaktiviert)

Tabelle 19.7 Fließtext bearbeiten

Die G-Kommandos berücksichtigen automatisch den `autoindent`-Modus sowie die Einstellung von `textwidth`. Wenn `textwidth` 0 enthält, beträgt die maximale Zeilenlänge 79 Zeichen. Eine Menge Konfigurationsmöglichkeiten für eine besonders komfortable Fließtexteingabe bietet die Option `formatoptions` (siehe den dazugehörigen Hilfetext).

Wortergänzungen

Das Eintippen langer Wörter und von Funktions- und Variablennamen ist mühsam und fehleranfällig. Vim hilft Ihnen dabei auf geniale Weise: Sie geben lediglich die ersten Buchstaben ein und drücken dann Strg+P. Wenn das Wort bereits eindeutig bestimmt ist, wird es sofort vervollständigt. Andernfalls können Sie mit Strg+P bzw. den Cursortasten das gewünschte Wort auswählen. Vim berücksichtigt bei der Wortergänzung alle Wörter aller geladenen Dateien, wobei Wörter aus der aktuellen Datei und dabei wiederum Wörter in der Nähe der Cursorposition bevorzugt werden.

19.4 Suchen und Ersetzen

Text suchen

Im Standardmodus bewegt / *suchtext* ↵ den Cursor zum gesuchten Text. N wiederholt die Suche, ⇧+N wiederholt die Suche rückwärts. Um von vornherein rückwärts zu suchen, beginnen Sie die Suche mit ? *suchausdruck*. Tabelle 19.8 fasst die wichtigsten Sonderzeichen zusammen, mit denen Sie im Suchausdruck nach Mustern suchen.

Zeichen	Bedeutung
.	ein beliebiges Zeichen
^ $	Zeilenanfang/Zeilenende
\> \>	Wortanfang/Wortende
[a-e]	ein Zeichen zwischen *a* und *e*
\s, \t	ein Leerzeichen bzw. ein Tabulatorzeichen
\(\)	fasst ein Suchmuster als Gruppe zusammen.
\=	Der Suchausdruck muss 0- oder einmal auftreten.
*	Der Suchausdruck darf beliebig oft (auch 0-mal) auftreten.
\+	Der Suchausdruck muss mindestens einmal auftreten.

Tabelle 19.8 Sonderzeichen im Suchausdruck

Groß- und Kleinschreibung

Vim unterscheidet bei der Suche standardmäßig zwischen Groß- und Kleinschreibung. Wenn Sie das nicht möchten, leiten Sie das Suchmuster mit `/c` ein (gilt nur für diese Suche) oder führen : `set ignorecase` aus (gilt für alle weiteren Suchen).

Inkrementelle Suche

Mit : set incsearch aktivieren Sie die sogenannte inkrementelle Suche: Bereits während der Eingabe des Suchtexts durch / *suchausdruck* bewegt Vim den Cursor zum ersten passenden Ort. ↵ beendet die Suche, Esc bricht sie ab. Nach der Suche bleiben alle Übereinstimmungen im Text markiert, bis Sie eine neue Suche durchführen oder : nohlsearch ausführen.

Suchen und Ersetzen

Um alle Vorkommen des Texts *abc* ohne Rückfrage durch *efg* zu ersetzen, führen Sie im Standardmodus : %s/*abc*/*efg*/g aus. ' ' führt anschließend zurück an den Beginn der Suche. Tabelle 19.9 fasst einige Varianten des Suchen-und-Ersetzen-Kommandos zusammen. Beim Suchen und Ersetzen mit Rückfrage können Sie mit Y oder N für jeden gefundenen Suchausdruck angeben, ob dieser durch den neuen Text ersetzt werden soll oder nicht. Q bricht den Vorgang ab, A ersetzt alle weiteren Vorkommen. Im Ersetzen-Ausdruck können Sie sich mit *n* auf die *n*-te Gruppe im Suchmuster beziehen. Eine Menge weiterer Tipps zum Suchen und Ersetzen sowie zahlreiche Beispiele finden Sie in der Online-Hilfe (: help substitute).

Tastenkürzel	Funktion
: %s/*abc*/*efg*/g	ersetzt ohne Rückfrage alle Vorkommen von *abc* durch *efg*.
: %s/*abc*/*efg*/gc	ersetzt mit Rückfrage alle Vorkommen von *abc* durch *efg*.
: %s/*abc*/*efg*/gci	ersetzt ohne Berücksichtigung der Groß- und Kleinschreibung.

Tabelle 19.9 Suchen und Ersetzen

19.5 Mehrere Dateien gleichzeitig bearbeiten

Im Standardmodus lädt : e *dateiname* eine neue Datei. Die neue Datei ersetzt die momentan bearbeitete Datei, die Sie vorher speichern müssen – andernfalls bricht Vim den Vorgang ab. Sie können das Laden der Datei mit : e! *dateiname* zwar erzwingen, verlieren dann aber alle durchgeführten Änderungen an der zuletzt aktuellen Datei.

Puffer und Fenster

Selbstverständlich können Sie in Vim auch mehrere Dateien gleichzeitig bearbeiten. Vorher sollten Sie allerdings das nicht besonders intuitive Konzept verstehen, wie Vim intern Texte verwaltet und anzeigt. Jeder im Editor dargestellte Text befindet sich intern in einem sogenannten Puffer. Das gilt sowohl für Dateien als auch für Hilfetexte. Solange es nur einen Puffer gibt, wird dieser auf der gesamten Vim-Arbeitsfläche angezeigt. Um mehrere Puffer gleichzeitig anzuzeigen, wird die Arbeitsfläche in mehrere sogenannte Fenster aufgeteilt, wie dies auch bei der Anzeige von Hilfetexten der Fall ist. Ein derartiges Fenster ist kein eigenständiges Fenster im Sinne des Linux-Grafiksystems, sondern nur ein Teilbereich der Arbeitsfläche.

Die Puffer veränderter Dateien sind immer in einem Fenster sichtbar. Puffer von Dateien, die seit dem letzten Speichern nicht mehr geändert wurden, können dagegen ausgeblendet werden. Die Puffer bleiben dabei im Speicher, gelten nun aber als nicht mehr aktiv. (Vorsicht: Wenn Sie ein Fenster mit einer noch nicht gespeicherten Datei schließen, gehen alle Änderungen verloren! Der inaktive Puffer der Datei bleibt zwar verfügbar, enthält aber die Datei zum Zeitpunkt der letzten Speicherung.)

Vim ist auch in der Lage, eine Datei gleichzeitig in mehreren Fenstern darzustellen, z. B. um unterschiedliche Teile eines sehr langen Texts zu bearbeiten.

Tabbed-Fenster

Seit Version 7 erleichtert Vim die Bearbeitung mehrerer Dateien mit sogenannten Tabbed-Fenstern (siehe Abbildung 19.2). Das sind übereinanderliegende Fenster, die in der obersten Zeile wie in Firefox oder anderen Webbrowsern beschriftet sind. Wirklich komfortabel funktionieren Tabbed-Fenster, wenn Sie die Maus aktiviert haben (siehe Abschnitt 19.7): Dann können Sie bequem mit der Maus das gerade aktive Tabbed-Fenster auswählen bzw. schließen (mit dem X-Button rechts oben). Weitere Informationen zu Tabbed-Fenstern erhalten Sie mit `:help tabpage`.

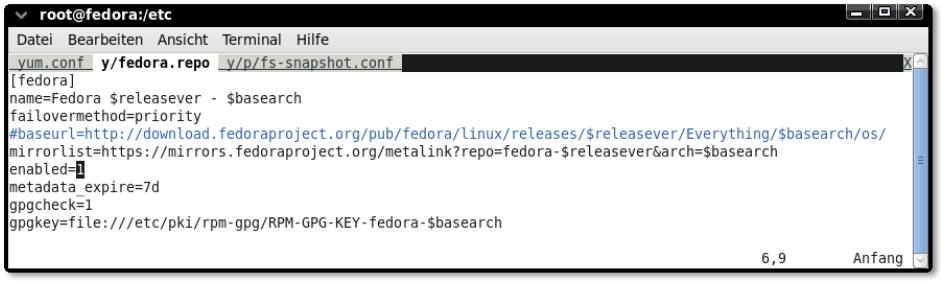


Abbildung 19.2 Drei Dateien in drei Tabbed-Fenstern

Eine neue Datei laden

Je nachdem, ob Sie mit Fenstern oder Tabbed-Fenstern arbeiten möchten, laden Sie neue Dateien mit `:new` *dateiname* oder `:tabnew` *dateiname*. Wenn Sie beim Programmstart mehrere Dateien übergeben, also beispielsweise `vim datei1 datei2 datei3`, wird lediglich die erste Datei angezeigt; die anderen werden in unsichtbare Puffer geladen. Um jede Datei in einem Fenster bzw. in einem Tabbed-Fenster zu öffnen, müssen Sie zusätzlich die Option `-o` bzw. `-p` übergeben.

Tabelle 19.10 fasst die wichtigsten Kommandos zusammen, um Dateien zu laden und zu speichern, zwischen (Tabbed-)Fenstern zu wechseln etc.

Tastenkürzel	Funktion
`:e` *dateiname*	lädt eine Datei in den aktuellen Puffer.
`:w`	speichert die aktuelle Datei.

Tabelle 19.10 Dateien, Puffer und Fenster

Tastenkürzel	Funktion
: wall	speichert alle offenen Dateien.
: wq	speichert und schließt den Puffer.
: e *dateiname*	lädt eine Datei in den aktuellen Puffer.
: w	speichert die aktuelle Datei.
: wall	speichert alle offenen Dateien.
: wq	speichert und schließt den Puffer.
: q	schließt den aktuellen Puffer und beendet Vim, wenn keine weiteren Puffer mehr offen sind.
: q!	schließt den Puffer auch mit ungesicherten Änderungen.
: qall	schließt alle Puffer und beendet Vim.
: split	teilt das Fenster und zeigt in beiden Fenstern denselben Text an.
: new	erzeugt einen leeren Puffer und zeigt ihn in einem Fenster an.
: new *dateiname*	lädt eine Datei in einen neuen Puffer.
: only	maximiert das aktuelle Fenster und schließt die anderen Puffer.
: all	zeigt alle Puffer in entsprechend verkleinerten Fenstern an.
: buffers	liefert die Liste aller Puffer.
: buffer *n*	zeigt den Puffer *n* an und löscht den aktuellen Puffer.
: buffer *dateiname*	zeigt den Puffer mit der Datei im aktuellen Fenster an.
: tabnew	erzeugt einen Puffer und zeigt ihn in einem Tabbed-Fenster an.
: tabnew *dateiname*	lädt eine Datei und zeigt sie in einem Tabbed-Fenster an.
: tabnext	wechselt in das nächste Tabbed-Fenster.
: tabprevious	wechselt in das vorige Tabbed-Fenster.
Strg + Bild↑ / Bild↓	wechselt in das nächste/vorige Tabbed-Fenster.
: tabclose	schließt das aktuelle Tabbed-Fenster.
: tabonly	schließt alle anderen Tabbed-Fenster.

Tabelle 19.10 Dateien, Puffer und Fenster (Forts.)

19.6 Interna

Optionen

Auf den vorigen Seiten wurden immer wieder besondere Funktionen von Vim durch Optionen aktiviert oder verändert, und dieser Abschnitt stellt eine Menge weiterer Optionen vor. Beachten Sie, dass manche Optionen nur lokal für die aktuelle Datei bzw. den aktuellen Puffer gelten. : set verändert in diesem Fall nur die lokale Ein-

stellung. Um die Option global zu verändern, verwenden Sie : setglobal. Tabelle 19.11 fasst die wichtigsten Kommandos zur Bearbeitung von Optionen zusammen.

Tastenkürzel	Funktion
: help options	liefert allgemeine Informationen sowie eine Optionsreferenz.
: help '*option*'	liefert Informationen zur angegebenen Option.
: set	liefert alle Optionen, die nicht im Grundzustand sind.
: set *booleoption*	aktiviert die boolesche Option.
: set no*booleoption*	deaktiviert die boolesche Option.
: set inv*booleoption*	invertiert den aktuellen Zustand der Option.
: set *option*?	zeigt die Einstellung der Option an.
: set *option=wert*	stellt die Option neu ein.
: set *option+=wert*	verändert die Option.
: set *option-=wert*	verändert die Option.
: set *option*&	setzt die Option auf den Grundzustand zurück.

Tabelle 19.11 Umgang mit Optionen

Konfiguration (vimrc)

Sämtliche Optionseinstellungen gehen beim Beenden von Vim verloren. Um Optionen bleibend einzustellen, verändern Sie die Vim-Konfigurationsdatei .vimrc. Beachten Sie, dass Kommentare durch das Zeichen " eingeleitet werden!

Die folgenden Zeilen geben ein einfaches Beispiel, wie .vimrc aussehen kann. Alle dort verwendeten Optionen wurden bzw. werden in diesem Kapitel vorgestellt. Wenn Sie im Internet nach vimrc suchen, finden Sie zahllose weitere Beispiele.

```
" Beispiel für ~/.vimrc
" Cursorposition mit der Maus festlegen
set mouse=a
" <Cursor links> am Zeilenanfang bewegt den Cursor an das Ende der vorigen Zeile,
" <Cursor rechts> am Zeilenende bewegt den Cursor an den Beginn der nächsten
" Zeile
set whichwrap=b,s,<,>,[,]
" Backups (name~) beim Speichern erzeugen
set backup
" inkrementelle Suche aktivieren
set incsearch
" generell Leerzeichen statt Tabs einfügen
set expandtab
```

Die Konfigurierbarkeit von Vim geht aber noch viel weiter: Sie können Vim-Optionen für unterschiedliche Dateitypen unterschiedlich einstellen, neue Funk-

tionen selbst programmieren etc. Erfinden Sie aber nicht das Rad neu! Unter der folgenden Adresse finden Sie zahllose fertige Lösungen, die Sie mit wenig Aufwand nutzen können. In der Regel reicht es aus, die betreffende Datei in `.vimrc` durch `source dateiname` einzubinden.

http://www.vim.org/scripts

Unabhängig von der Backup-Einstellung aktualisiert Vim während des Schreibens regelmäßig eine sogenannte Swap-Datei. Der Name dieser Datei ergibt sich aus einem vorangestellten Punkt, dem aktuellen Dateinamen sowie der Endung `.swp` (also beispielsweise `.mycode.c.swp`, wenn Sie gerade `mycode.c` bearbeiten). Diese Datei enthält in einem Binärformat alle Änderungen, die Sie seit dem letzten Speichern durchgeführt haben. Sie wird automatisch aktualisiert, wenn Sie mehr als 200 Zeichen neuen Text eingegeben haben oder vier Sekunden lang keine Eingaben durchgeführt haben. Die Swap-Datei wird beim regulären Beenden von Vim gelöscht.

Sollte der Strom ausfallen, Linux oder Vim abstürzen etc., können Sie Ihre ungesicherte Arbeit beim nächsten Vim-Start wiederherstellen. Vim bemerkt beim Öffnen der Datei, dass eine Swap-Datei existiert, und stellt verschiedene Optionen zur Auswahl. Im Regelfall werden Sie sich für [W] (Wiederherstellen) entscheiden und die so gerettete Datei anschließend speichern. Anschließend sollten Sie Vim verlassen und die Swap-Datei explizit löschen (das erfolgt nicht automatisch!).

Zeichensatz

Vim kommt standardmäßig mit den meisten wichtigen Zeichensätzen zurecht, unter anderem mit diversen Latin-Varianten, Unicode (utf-8, utf-16, ucs-2, ucs-2l, ucs-4 etc.) sowie einigen asiatischen 2-Byte-Zeichensätzen (z. B. `euc-kr`, also Koreanisch).

Vim ermittelt beim Start den Standardzeichensatz des Betriebssystems (Option `encoding`). Beim Lesen einer neuen Datei versucht Vim, auch deren Zeichensatz zu erkennen (Option `fileencoding`). Dabei werden der Reihe nach alle in der Option `fileencodings` aufgezählten Zeichensätze ausprobiert, bis ein Zeichensatz zur fehlerfreien Darstellung des gesamten Texts gefunden wird. (Die Grundeinstellung für `fileencodings` lautet oft `utf-8,latin1`.)

Setzen Sie Vim möglichst in einer UTF8-Umgebung ein!

Wenn `encoding` und `fileencoding` nicht übereinstimmen, führt Vim beim Laden und Speichern automatisch eine Konvertierung durch. Falls der `encoding`-Zeichensatz weniger Zeichen darstellen kann als `fileencoding`, kann es dabei zu Verlusten kommen. Um das zu vermeiden, sollte Vim nach Möglichkeit in einer UTF-8-Umgebung eingesetzt werden. Unter Linux ist das standardmäßig der Fall.

Um herauszufinden, welchen Zeichensatz die gerade bearbeitete Datei nutzt, führen Sie : `set fileencoding?` aus. Mit : `set fileencoding=`*`neuerZeichensatz`* verändern Sie den Zeichensatz. Wenn Sie die Datei nun speichern, wird sie im neuen Zeichensatz gespeichert!

19.7 Tipps und Tricks

:-Kommandos effizient eingeben

Bei der Eingabe von Kommandos, die mit : beginnen, gibt es einige Eingabehilfen: Mit den Cursortasten können Sie durch die zuletzt benutzten Kommandos blättern. (Vim speichert die Kommandos in `.viminfo` und merkt sich die Kommandos somit auch nach dem Programmende.) Weiters können Sie mit ⇆ Schlüsselwörter vervollständigen (z. B. bei der Eingabe von Optionen). Und zu guter Letzt können Sie viele :-Kommandos abkürzen (z. B. : `tabn` statt : `tabnext`).

Zeilennummern anzeigen

: `set number` zeigt neben jeder Zeile die Zeilennummer an. : `set nonumber` deaktiviert diesen Modus wieder.

Backups

Standardmäßig erstellt Vim beim Speichern kein Backup (also keine Kopie der ursprünglichen Datei). Wenn Sie das wünschen, führen Sie im Standardmodus : `set backup` aus. Die Backup-Datei erhält den Namen `alternname~`. Um Backups generell zu aktivieren, fügen Sie `set backup` in `.vimrc` ein.

Maus aktivieren

Wenn Sie Vim in einer Textkonsole oder in einem Konsolenfenster verwenden, dann ist die Funktion der Maus auf ihre Grundfunktionen unter X beschränkt: Sie können damit zwar Text kopieren und an der aktuellen Cursorposition einfügen, Sie können aber nicht die aktuelle Cursorposition verändern etc.

Um der Maus in Vim mehr Funktionen zu geben, verwenden Sie entweder die grafische Variante `gvim`, oder Sie führen im Standardmodus : `set mouse=a` aus. Sie können nun den Cursor durch einen Mausklick neu positionieren, das aktive Vim-Fenster auswählen, mit dem Mausrad durch den Text scrollen etc.

Dieser Mausmodus hat allerdings einen Nachteil: Die mittlere Maustaste fügt nun den zuletzt in Vim gelöschten Text ein. Die Maus kann nicht mehr zum Kopieren von Text zwischen Vim und anderen Programmen genutzt werden. Abhilfe ist aber einfach: Die herkömmlichen Mausfunktionen sind weiterhin verfügbar, wenn Sie zusätzlich die ⇧-Taste drücken. Achten Sie aber darauf, dass sich Vim beim Einfügen von Text tatsächlich im Einfügemodus befindet! Andernfalls wird der per Maus eingefügte Text als Kommando interpretiert, und das kann schiefgehen.

Leerzeichen statt Tabulatoren

Damit Vim in Ihren Text grundsätzlich Leerzeichen statt Tabulatorzeichen einfügt, führen Sie : `set expandtab` aus bzw. fügen die Anweisung in `.vimrc` ein. Um in der vorhandenen Datei alle Tabulatorzeichen durch die entsprechende Anzahl von

Leerzeichen zu ersetzen, führen Sie anschließend : retab aus. Um umgekehrt Leerzeichen durch Tabulatoren zu ersetzen, führen Sie : set unexpandtab und dann : retab! aus.

Makros

. wiederholt das letzte Kommando – so viel wissen Sie schon. Wenn Sie aber eine ganze Abfolge von Kommandos mehrfach ausführen möchten, definieren Sie ein Makro. Dazu starten Sie im Standardmodus mit Q den Makromodus. Das nächste Zeichen gibt den Namen des Makros an (genau genommen den Namen des Registers, in dem das Makro gespeichert wird). Alle weiteren Kommandos werden im Makro gespeichert, bis Sie die Eingabe abermals durch Q beenden. Das so aufgezeichnete Makro können Sie nun mit @ *makroname* ausführen. (Wenn Sie Vim verlassen, gehen alle gespeicherten Makros verloren.)

Ein Beispiel: Die folgende Tastensequenz zeichnet das Makro *a* auf, das am Beginn und am Ende eines Worts das Anführungszeichen " einfügt:

Q A I " Esc E A " Esc Q

Wenn der Cursor nun innerhalb eines Worts steht und Sie @, A ausführen, wird dieses Wort in Anführungszeichen gestellt. @, @ wiederholt das letzte Registerkommando, ohne dass Sie sich an den Makro- bzw. Registernamen erinnern müssen.

Linux-Kommandos ausführen

Wenn Sie in Vim ein Linux-Kommando ausführen möchten, ohne Vim zu verlassen, führen Sie im Standardmodus : !*kommandoname* aus (also beispielsweise !ls, um die Liste der Dateien im aktuellen Verzeichnis zu ermitteln). Vim zeigt das Ergebnis des Kommandos an. Mit ↵ gelangen Sie zurück in den Editor. Zur Ausführung mehrerer Kommandos öffnen Sie mit : sh eine neue Shell. Von dort gelangen Sie mit Strg+D zurück in den Editor.

Vim im Easy-Modus verwenden

Wenn Sie sich nicht an die verschiedenen Vim-Modi gewöhnen können, auf Vim aber nicht mehr verzichten möchten, starten Sie das Programm am besten mit vim -y bzw. führen : set insertmode aus. Damit verbleibt der Editor immer im Einfügemodus. Sie müssen nun jedes Kommando mit Strg+O einleiten. Um mehrere Kommandos auf einmal auszuführen, ist es auch möglich, mit Strg+L für längere Zeit in den Standardmodus zu wechseln und diesen mit Esc zu verlassen.

Noch ähnlicher zu anderen Editoren verhält sich Vim, wenn Sie evim starten: Damit wird der Editor in der grafischen Benutzeroberfläche gvim gestartet. Textmarkierungen können mit ⇧ und den Cursortasten durchgeführt werden. Texte werden mit Strg+C kopiert, mit Strg+X gelöscht und mit Strg+V wieder eingefügt. man evim bezeichnet den Easy-Modus als »Vim for gumbies« (was auch immer ein *gumby* ist ...): Sie verlieren damit so viel von den Grundeigenschaften von Vim, dass es besser ist, gleich einen anderen Editor einzusetzen.

Kapitel 20
Emacs

Emacs einfach nur als Editor zu bezeichnen, greift zu kurz: Das Programm eignet sich nicht nur zur Bearbeitung von Texten, sondern auch als komplette Entwicklungsumgebung, als E-Mail-Programm etc. Für manche Anwender ist der Emacs gleichsam ein Ersatzbetriebssystem für alle Funktionen der alltäglichen Arbeit. Wenn Sie mit dem Emacs erst einmal umgehen können, werden Sie nie wieder einen anderen Editor benötigen. Es versteht sich eigentlich von selbst, dass ich fast das gesamte Buch seit der ersten Auflage mit dem Emacs geschrieben habe ...

Wo viel Licht ist, da gibt es bekanntlich auch Schatten: Die Bedienung des Emacs sieht auf den ersten Blick ein wenig abschreckend aus. Es wimmelt nur so von Strg- und Alt-Sequenzen, mit denen die zahllosen Kommandos aufgerufen werden. Nicht umsonst behaupten Spötter, der Name Emacs stünde für *Escape Meta Alt Control Shift*. Auch die Benutzeroberfläche (Menü, Symbolleiste) wirkt antiquiert, deutschsprachige Menüs fehlen überhaupt, die Konfiguration ist umständlich etc. Kurz und gut: Der Emacs ist ein Editor für Profis, die bereit sind, Zeit für die Einarbeitung zu investieren, und die sich nicht an Äußerlichkeiten stören.

20.1 Schnelleinstieg

GNU Emacs versus XEmacs

Unter Linux gibt es *zwei* Emacs-Versionen: den GNU Emacs und den XEmacs (ehemals Lucid Emacs). Beide Versionen können sowohl in einer Textkonsole als auch unter X verwendet werden, und beide unterstehen der GPL. Auch sonst gibt es viele Ähnlichkeiten, aber auch viele kleine Unterschiede. Dieses Kapitel bezieht sich explizit auf den GNU Emacs in der Version 24.*n*.

Neben den beiden großen Emacs-Versionen existieren einige kleinere Varianten: `jed`, `jmacs` (aus dem Paket `joe`), `jove` und `zile` sind durchweg brauchbare Miniversionen. Ihr Hauptvorteil besteht darin, dass ihr Ressourcenbedarf viel geringer ist. Damit eignen sich diese Programme ideal für Notfallsysteme oder für ältere Rechner mit langsamen CPUs und wenig Speicher etc.

Abbildung 20.1 Der GNU Emacs

Links Weitere Informationen zum Emacs finden Sie hier:

http://www.gnu.org/software/emacs/emacs.html
http://www.emacswiki.org

Texte laden und speichern, Programm beenden

Der Emacs wird durch die Eingabe von `emacs` gestartet. Wenn Sie beim Start des Programms einen oder mehrere Dateinamen angeben, werden diese Dateien automatisch geladen. Dabei sind auch Suchmuster erlaubt: `emacs Makefile *.[ch]` lädt die Datei `Makefile` sowie alle `*.c`- und `*.h`-Dateien des aktuellen Verzeichnisses. Sobald das Programm einmal läuft, laden Sie weitere Dateien mit Strg+X, Strg+F *Dateiname* ↵.

Mit Strg+X, Strg+S speichern Sie die geänderte Datei. Strg+X, Strg+C beendet das Programm. Wenn der Emacs dabei irgendwelche noch nicht gespeicherten Dateien entdeckt, erscheint eine Sicherheitsabfrage, ob Sie den Emacs tatsächlich ohne zu speichern verlassen möchten. Antworten Sie auf diese Abfrage durch die Eingabe von *yes* ↵, falls Sie die Änderungen tatsächlich verwerfen möchten. Um eine Datei unter einem anderen Namen zu speichern, geben Sie Strg+X, Strg+W *Dateiname* ↵ ein.

Wenn Sie den Emacs in einer Textkonsole verwenden, können Sie das Programm mit Strg+Z vorübergehend verlassen. Mit `fg` nehmen Sie die Arbeit wieder auf. Unter X bewirkt Strg+Z lediglich die Verkleinerung in ein Icon.

Tastenkürzel	Funktion
Strg+X, Strg+F *datei* ↵	lädt eine Datei (Find).
Strg+X, I	fügt eine Datei in den vorhandenen Text ein (Insert).
Strg+X, Strg+S	speichert eine Datei (Save).
Strg+X, S	speichert alle Dateien (mit Rückfrage).
Strg+X, S, !	speichert alle offenen Dateien (ohne Rückfrage).
Strg+X, Strg+W *datei* ↵	speichert unter einem neuen Namen (Write).
Strg+X, Strg+C	beendet den Editor.

Tabelle 20.1 Dateien laden und speichern, Emacs beenden

Sicherheitskopien

Der Emacs erstellt beim Speichern automatisch eine Sicherheitskopie `name~`, in der der ursprüngliche Text enthalten ist. Außerdem speichert der Emacs in regelmäßigen Abständen den aktuellen Zustand des Textes in der Datei `#name#`. Auf diese Datei können Sie zurückgreifen, wenn während des Arbeitens der Strom ausgefallen ist oder wenn Sie aus einem anderen Grund den Emacs nicht ordnungsgemäß verlassen konnten.

Beachten Sie, dass die #-Dateien im Emacs-internen Zeichensatz gespeichert werden und nicht in dem Zeichensatz, in dem Sie Ihre Datei bearbeitet haben. Aus diesem Grund sollten Sie zur Wiederherstellung der Dateien Alt+X `recover-session` einsetzen. Alternativ können Sie auch direkt die #-Dateien laden und mit Strg+X, ↵, F *zeichensatz* deren Zeichensatz verändern.

Elementare Kommandos

Üblicherweise bewegen Sie den Cursor mit den Cursortasten sowie mit Bild↑ bzw. Bild↓. Sollte das nicht funktionieren (z. B. wenn Sie den Emacs über ein schlecht funktionierendes Terminalprogramm gestartet haben), klappt es auf jeden Fall mit den in Tabelle 20.2 zusammengefassten Kommandos.

Sie können an jeder beliebigen Stelle neuen Text eingeben. Mit Entf und ← löschen Sie einzelne Zeichen. Alternativ existiert das Tastaturkommando Strg+D zum Löschen des Zeichens an der Cursorposition (Delete).

Undo

Mit Strg+X, U (Undo) oder mit Strg+_, im deutschen Tastaturlayout also Strg+⇧+-, widerrufen Sie die letzten Änderungen. Diese Undo-Funktion funktioniert für beliebig komplexe Kommandos und praktisch unbegrenzt!

Tastenkürzel	Funktion
Strg+F	bewegt den Cursor ein Zeichen nach links (Forwards).
Strg+B	bewegt den Cursor ein Zeichen nach rechts (Backwards).
Strg+P	bewegt den Cursor eine Zeile nach oben (Previous).
Strg+N	bewegt den Cursor eine Zeile nach unten (Next).
Strg+V	bewegt den Text eine Seite nach oben.
Alt+V	bewegt den Text eine Seite nach unten.

Tabelle 20.2 Tastenkürzel, falls die Cursortasten versagen

Wenn Ihnen während der Eingabe eines Kommandos ein Fehler unterläuft, können Sie die Kommandoeingabe mit Strg+G abbrechen. Das ist besonders dann praktisch, wenn Sie irrtümlich Esc drücken.

Online-Hilfe

Der Emacs stellt zahlreiche Kommandos zum Aufruf der englischsprachigen Online-Hilfe zur Verfügung. Das für den Einstieg wichtigste Kommando lautet F1, T (Tutorial). Mit Strg+X, B, ↵ gelangen Sie in den ursprünglichen Text zurück.

Wenn nach der Ausführung eines Hilfe-Kommandos mehrere Textabschnitte (Fenster) übrig bleiben, können Sie mit Strg+X, O (»Oh«) den Textcursor in das jeweils nächste Fenster stellen. Strg+X, 0 (»Null«) entfernt das aktuelle Fenster; Strg+X, 1 löscht alle Fenster außer dem aktuellen Fenster. Mit den drei Kommandos können Sie also zwischen dem Hilfe- und dem Textfenster hin- und herspringen und schließlich das Hilfefenster wieder entfernen.

Wird der Hilfetext dagegen Seiten füllend angezeigt, können Sie mit Strg+X, B, ↵ zurück in Ihren eigentlichen Text springen. Intern wird die Verwaltung mehrerer Texte – also beispielsweise Ihres Textes und des Hilfetextes – durch sogenannte Puffer realisiert. Mehr zum Umgang mit Puffern und Fenstern erfahren Sie in Abschnitt 20.8.

Die wichtigste Informationsquelle zum Emacs ist das interne `info`-System, das offiziell als Emacs-Handbuch gilt. Bei manchen Distributionen wird dieses Handbuch auch im HTML-Format mitgeliefert, sodass es noch komfortabler gelesen werden kann.

Tastenkürzel	Funktion
F1, F1	Übersicht über vorhandene Hilfekommandos
F1, A *text* ↵	Übersicht über alle Kommandos, die *text* enthalten (Apropos)
F1, B	Übersicht über alle Tastenkürzel (Bindings)
F1, C *tastenkürzel*	Kurzbeschreibung des zugeordneten Kommandos (Command)
F1, F *kommando* ↵	Kurzbeschreibung des Kommandos (Function)
F1, ⇧+F	Emacs-FAQ (Frequently Asked Questions)
F1, I	startet das `info`-System zur Anzeige hierarchischer Hilfetexte (zur Bedienung siehe Abschnitt 13.3).
F1, N	Zusammenfassung der Neuerungen in der aktuellen Version im Vergleich zu den früheren Versionen
F1, T	Einführung in die Bedienung von Emacs (Tutorial)
F1, Strg+F *name*	startet das `info`-System und zeigt Informationen zum angegebenen Kommando an.
F1, Strg+P	Informationen über die Idee freier Software

Tabelle 20.3 Online-Dokumentation nutzen

Info-Modus

Die eingebaute Online-Hilfe des Emacs liegt im Info-Format vor (siehe auch Abschnitt 13.3). Beim Lesen von `info`-Texten wird im Emacs ein eigener `info`-Modus aktiviert. Querverweise bzw. Menüeinträge können Sie einfach durch Klicken mit der mittleren Maustaste verfolgen. Mit L gelangen Sie zur zuletzt sichtbaren Seite zurück.

20.2 Grundlagen

Bearbeitungsmodi

Der Emacs kennt verschiedene Bearbeitungsmodi, in denen zusätzliche Kommandos zur Bearbeitung spezieller Dateien zur Verfügung stehen. Dabei wird zwischen Haupt- und Nebenmodi unterschieden: Es kann immer nur ein Hauptmodus aktiv sein. Dieser kann aber durch mehrere Nebenmodi ergänzt werden.

Zu den wichtigsten Hauptmodi zählen solche für fast alle gängigen Programmiersprachen (C, C++, Java etc.) sowie der LaTeX-Modus zur Bearbeitung von LaTeX-Dateien. Der Emacs aktiviert beim Laden einer Datei automatisch den Modus, der ihm passend erscheint (z. B. den C-Modus, wenn der Dateiname mit `.c` endet). Wenn der Emacs keinen passenden Modus erkennen kann, wählt er den Fundamental-Modus als Grundeinstellung.

Zu den wichtigsten Nebenmodi gehören der Fill-Modus zur Bearbeitung von Fließtext mit Absätzen über mehrere Zeilen und der Abbrev-Modus zur automatischen Auflösung von Abkürzungen.

Die elementaren Emacs-Kommandos funktionieren in allen Modi gleich, weswegen Sie sich mit den Bearbeitungsmodi vorläufig noch nicht beschäftigen müssen. Wenn Sie Eigenmächtigkeiten des Emacs aufgrund eines bestimmten Modus deaktivieren möchten (z. B. das automatische Einrücken von Programmzeilen im C-Modus), schalten Sie einfach mit Alt+X `fundamental-mode` ↵ in den Grundmodus um. Genauere Informationen zu den Bearbeitungsmodi finden Sie in Abschnitt 20.9.

Tastaturkonventionen

Generell gibt es drei Möglichkeiten zur Eingabe von Emacs-Kommandos: das Menü, die Verwendung von Tastenkürzeln (zumeist eine Kombination mit Strg oder Alt) oder die Eingabe des gesamten Kommandonamens. Die dritte Variante wird mit Alt+X eingeleitet, also etwa Alt+X `delete-char` ↵.

Die Eingabe von Kommandos und anderen Parametern wird durch zwei Mechanismen erleichtert:

- Während der Eingabe können Sie den Kommandonamen wie bei der Kommandoeingabe im Shell-Terminal mit ⇆ ergänzen. Der Emacs unterscheidet dabei zwischen Groß- und Kleinschreibung. In gleicher Weise können auch Dateinamen ergänzt werden. Wenn mehrere Möglichkeiten bestehen, zeigt der Emacs diese auf dem Bildschirm an.
- Auf früher bei Alt+X angegebene Kommandos können Sie (nach der Einleitung des neuen Kommandos durch Alt+X) mit Alt+P (Previous) und Alt+N (Next) zurückgreifen.

In diesem Buch werden die Tastenfolgen so angegeben, wie sie auf einer deutschen Tastatur bei korrekter Installation eingegeben werden können. Dabei bedeutet ein Plus-Zeichen, dass mehrere Tasten gleichzeitig gedrückt werden müssen, während ein Komma darauf hinweist, dass die Tasten nacheinander gedrückt werden. Buchstaben werden immer als Großbuchstaben angegeben, obwohl die ⇧-Taste dabei nicht gedrückt werden muss! Alt+X bedeutet also, dass Sie die Tasten Alt und X gleichzeitig drücken sollen, nicht aber ⇧!

In der Dokumentation zum Emacs werden Tastenkürzel etwas abweichend dargestellt: `DEL` bedeutet nicht Entf, sondern ←! `C` steht für Control (gemeint ist Strg) und `M` für Meta.

Eine direkte Entsprechung der Meta-Taste existiert auf einer Standard-PC-Tastatur nicht. `M-x` kann auf einer PC-Tastatur auf zwei Weisen nachgebildet werden: durch Esc und X (nacheinander) oder durch Alt+X. In diesem Buch wird generell die bequemere Alt-Tastenkombination angegeben.

Feinheiten

Bei manchen Emacs-kompatiblen Programmen bzw. bei der Verwendung des Emacs in einer Textkonsole gibt es allerdings Probleme mit der Taste Alt. Statt Alt+X müssen Sie dort Esc, X benutzen. Beachten Sie, dass der Emacs zwischen Strg+X, Strg+B und der ähnlich aussehenden Kombination Strg+X, B unterscheidet! Es ist also nicht egal, wie lange Sie die Strg-Taste gedrückt halten.

Maus-unterstützung

In Emacs gelten die unter X üblichen Konventionen, d. h., Sie markieren Text mit der Maus und fügen ihn dann mit der mittleren Maustaste wieder ein. Wenn Sie im Emacs mehrere Texte gleichzeitig anzeigen, können Sie auch die Trennleiste zwischen den Textbereichen mit der linken Maustaste verschieben. Mit der rechten Maustaste stellen Sie den Endpunkt des gerade markierten Textbereichs ein, der danach bearbeitet werden kann. Die Maustasten in Kombination mit ⇧ bzw. Strg dienen zur Ausführung diverser Kommandos (z. B. zur Auswahl des Fonts, der zur Darstellung des Texts verwendet wird).

Startoptionen

Beim Start des Emacs unter X können Sie durch Kommandozeilenoptionen zahlreiche Einstellungen für Farben, Zeichensätze etc. vornehmen. Tabelle 20.4 zählt die wichtigsten Optionen auf. Eine vollständige Beschreibung finden Sie in der Manual-Seite zum Emacs.

Option	Bedeutung
`-nw`	Textversion des Emacs im Shell-Fenster starten (No Window)
`-fg farbe`	Vordergrundfarbe (Textfarbe; normalerweise Schwarz)
`-bg farbe`	Hintergrundfarbe (normalerweise Weiß)
`-cr farbe`	Farbe des Textcursors (normalerweise Schwarz)
`-geometry bxh+x+y`	Größe (Breite mal Höhe) und Position des Emacs-Fensters voreinstellen; alle Angaben in Textzeichen
`-fn zeichensatz`	startet Emacs mit dem angegebenen Zeichensatz.

Tabelle 20.4 Kommandozeilenoptionen

20.3 Cursorbewegung

Neben den Cursortasten kennt Emacs eine Menge Tastenkürzel zur Cursorbewegung. Die wichtigsten Kürzel sind in Tabelle 20.5 zusammengefasst.

Cursor-kommandos mehrfach ausführen

Der Emacs ist in der Lage, ein beliebiges Kommando mehrfach hintereinander auszuführen. Dazu müssen Sie zuerst Alt+*n* eingeben, wobei *n* eine beliebige Zahl ist. Die Ziffern müssen vom alphanumerischen Tastaturteil stammen (nicht vom Zehnerblock im rechten Teil der Tastatur). Während der gesamten Zahleneingabe

müssen Sie Alt gedrückt halten. Anschließend geben Sie das gewünschte Kommando an. Beispielsweise wird der Text durch Alt+*n*, Bild↓ um *n* Seiten nach unten gescrollt. Dieses Verfahren kann auch zur Eingabe von Textzeichen verwendet werden. Beispielsweise zeichnet Alt+60, - eine Linie.

Tastenkürzel	Funktion
Alt+F / Alt+B	bewegt den Cursor ein Wort vor bzw. zurück (For-/Backwards).
Strg+A / Strg+E	stellt den Cursor an den Beginn bzw. das Ende der Zeile.
Alt+A / Alt+E	stellt den Cursor an den Beginn bzw. das Ende des Absatzes.
Strg+V / Alt+V	bewegt den Text eine Seite nach unten bzw. oben.
Alt+< / Alt+⇧+>	bewegt den Cursor an den Beginn bzw. das Ende des Textes.
Strg+L	scrollt den Text so, dass der Cursor in der Bildmitte steht.
Alt+G *n* ↵	stellt den Cursor in Zeile *n*.
Strg+X, R, ␣ z ↵	speichert die aktuelle Cursorposition im Register z.
Strg+X, R, J z ↵	springt zu der im Register z gespeicherten Position.

Tabelle 20.5 Cursorbewegung

Wo bin ich?

Wenn Sie wissen möchten, in welcher Zeile Sie sich gerade befinden, geben Sie Alt+X `what-line` ↵ ein; der Emacs zeigt jetzt die aktuelle Zeilennummer in der untersten Bildschirmzeile an. Noch praktischer ist es, mit Alt+X `line-number-mode` ↵ eine ständige Anzeige der Zeilennummer zu aktivieren. Leider funktioniert diese Anzeige bei sehr langen Texten (im MByte-Bereich) nicht mehr. Natürlich kann auch die Spaltennummer angezeigt werden – aktivieren Sie den `column-number-mode`!

Cursorpositionen in Registern speichern

In einem längeren Text ist es oft wünschenswert, wenn rasch zwischen verschiedenen Stellen im Text hin- und hergesprungen werden kann. Zu diesem Zweck kann die aktuelle Cursorposition mit einem Kommando in einem sogenannten Register gespeichert werden (siehe die vorletzte Zeile in Tabelle 20.5). Ein Register ist ein Speicherplatz, der durch ein Textzeichen (Buchstabe oder Ziffer) gekennzeichnet wird. Zu einem späteren Zeitpunkt können Sie durch die Angabe dieses Registers wieder an den ursprünglich gespeicherten Ort springen. Beachten Sie bitte, dass Register beim Verlassen des Emacs nicht gespeichert werden.

20.4 Text markieren, löschen und einfügen

Die Tasten Entf oder Strg+D sowie ← zum Löschen einzelner Zeilen haben Sie schon kennengelernt. Um größere Textmengen zu löschen, setzen Sie die in Tabelle 20.6 zusammengefassten Kommandos ein. Wenn Sie die dort aufgezählten Löschkommandos mehrmals unmittelbar hintereinander ausführen, fügt Strg+Y den gesamten gelöschten Text wieder ein. Strg+Y kann mehrfach und an beliebigen Stellen im Text ausgeführt werden. Das Kommando ermöglicht es daher, den gelöschten Text an eine andere Stelle zu verschieben bzw. zu kopieren.

Tastenkürzel	Funktion
Alt+D	löscht das nächste Wort bzw. das Ende des Wortes ab dem Cursor.
Alt+←	löscht das vorige Wort bzw. den Beginn des Wortes bis zum Cursor.
Strg+K	löscht das Zeilenende ab der Cursorposition.
Alt+0, Strg+K	löscht den Zeilenanfang vor der Cursorposition.
Alt+M	löscht den nächsten Absatz.
Alt+Z, *x*	löscht alle Zeichen bis zum nächsten Auftreten von x (das Zeichen x wird mit gelöscht).
Strg+Y	fügt den zuletzt gelöschten Text an der Cursorposition wieder ein.

Tabelle 20.6 Text löschen und wieder einfügen

Die obigen Kommandos sind relativ unflexibel, weil die zu löschende Textmenge starr vorgegeben ist. Wenn Sie einen beliebigen Textausschnitt löschen möchten, markieren Sie diesen zuvor. Dazu führen Sie zuerst am Anfang oder am Ende des Bereichs Strg+␣ aus. Diese Markierung bleibt unsichtbar, der Emacs zeigt aber die Meldung »Mark set« an. Als markierter Bereich gilt von nun an der Text zwischen dem markierten Punkt und der aktuellen Position des Textcursors.

Tastenkürzel	Funktion
Strg+␣	setzt einen (unsichtbaren) Markierungspunkt.
Strg+W	löscht den Text zwischen dem Markierungspunkt und der aktuellen Cursorposition.
Strg+Y	fügt den gelöschten Text wieder ein.
Strg+X, Strg+X	vertauscht Cursorposition und Markierungspunkt.

Tabelle 20.7 Text markieren

Wenn Sie sich nicht an die Bereichsmarkierung mit Strg+X gewöhnen möchten, können Sie im Emacs auch die unter Windows übliche Form der Markierung mit ⇧ aktivieren. Ab Emacs 23.1 steht diese Markiermethode standardmäßig zur Verfügung; bei älteren Emacs-Versionen müssen Sie vorher Alt+X `pc-selection-mode` ausführen bzw. die Emacs-Konfiguration entsprechend verändern.

CUA-Modus

Mit Alt+X `cua-mode` können Sie den Common-User-Access-Modus aktivieren. Sofern Sie mit ⇧ Text markiert haben, können Sie diesen wie in nahezu jedem anderen Programm mit Strg+C in die Zwischenablage kopieren bzw. mit Strg+X ausschneiden. Strg+V fügt den Inhalt der Zwischenablage an der aktuellen Cursorposition wieder ein. Wenn kein Text markiert ist, leitet Strg+X wie bisher diverse Emacs-Kommandos ein.

20.5 Text bearbeiten

Text einfügen bzw. überschreiben

Der Emacs befindet sich normalerweise im Einfügemodus. Das heißt, neu eingegebener Text wird an der aktuellen Cursorposition in den vorhandenen Text eingefügt. Wenn Sie stattdessen den vorhandenen Text überschreiben möchten, wechseln Sie mit Alt+X `overwrite-mode` ↵ in den Überschreibmodus. Die nochmalige Ausführung des Kommandos schaltet den Modus wieder aus. Bei einer korrekten Konfiguration der Tastatur können Sie den Modus auch mit Einfg umschalten.

Zur Veränderung der Groß- und Kleinschreibung bereits geschriebener Wörter bietet der Emacs die in Tabelle 20.8 zusammengefassten Kommandos an.

Tippfehler

Ein häufiger Tippfehler ist das Vertauschen zweier Buchstaben. Mit Strg+T können Sie solche Vertauschungen bequem korrigieren. Der Cursor muss dabei auf dem zweiten der beiden betroffenen Buchstaben stehen, im Wort »vertaushcen« also auf »c«.

Analog können mit Alt+T zwei Wörter vertauscht werden. Wenn der Cursor dabei am Beginn eines Wortes steht, wird dieses Wort mit dem vorangegangenen vertauscht. Steht der Cursor dagegen irgendwo im Wort, dann wird das Wort mit dem folgenden Wort vertauscht. Das mehrfache Ausführen von Alt+T führt dazu, dass das erste der beiden Wörter immer weiter nach vorn bewegt wird.

Mit Strg+X, Strg+T vertauschen Sie schließlich die aktuelle Zeile mit der vorherigen Zeile. Die mehrfache Ausführung des Kommandos führt dazu, dass die Zeile oberhalb des Curors immer weiter nach unten rutscht.

Tastenkürzel	Funktion
Alt+C	Buchstabe an der Cursorposition groß, alle weiteren Buchstaben des aktuellen Wortes klein (Capitalize)
Alt+L	alle Buchstaben des Wortes ab Cursorposition klein (Lower)
Alt+U	alle Buchstaben des Wortes ab Cursorposition groß (Upper)
Esc, -, Alt+C	erster Buchstabe groß, Rest klein; wenn der Cursor am Beginn eines Wortes steht, wird das vorige Wort verändert.
Esc, -, Alt+L	alle Buchstaben des Wortes bis zur Cursorposition klein; wenn der Cursor am Beginn eines Wortes steht, dann das vorige Wort klein.
Esc, -, Alt+U	alle Buchstaben des Wortes bis zur Cursorposition groß; wenn der Cursor am Beginn eines Wortes steht, dann das vorige Wort groß.
Strg+␣	Markierungspunkt setzen
Strg+X, Strg+L	Bereich zwischen Markierungspunkt und Cursor klein
Strg+X, Strg+U	Bereich zwischen Markierungspunkt und Cursor groß

Tabelle 20.8 Groß- und Kleinschreibung ändern

Tabulatoren

In der Grundeinstellung und bei der Bearbeitung eines normalen ASCII-Texts wird durch ↹ ein Tabulatorzeichen eingefügt. Tabulatoren sind nicht sichtbar. Ob an einer Stelle ein Tabulatorzeichen oder mehrere Leerzeichen stehen, merken Sie erst, wenn Sie den Cursor darüber bewegen. Bei Tabulatoren bewegt sich der Cursor in Sprüngen.

Je nachdem, welchen Text (z. B. eine `*.tex`-Datei) Sie mit dem Emacs bearbeiten, wird automatisch ein dazu passender Bearbeitungsmodus aktiviert (siehe Abschnitt 20.9). Bei manchen dieser Modi werden einzelne Tasten umdefiniert. Dies betrifft insbesondere auch die Taste ↹. Im C-Modus bewirkt die Taste beispielsweise, dass der Zeilenanfang entsprechend der Programmstruktur eingerückt wird. Im LaTeX-Modus hat die ↹-Taste gar keine Wirkung. Wenn ↹ also nicht so funktioniert, wie Sie erwarten, ist zumeist der Bearbeitungsmodus schuld. Es bestehen mehrere Möglichkeiten, dennoch Tabulatoren einzugeben:

- Mit Strg+Q, ↹ können Sie unabhängig von allen Modi ein Tabulator-Zeichen in den Text einfügen.
- Mit Alt+I können Sie unabhängig vom Bearbeitungsmodus ein Tabulator-Zeichen oder entsprechend viele Leerzeichen einfügen (je nach Einstellung von `indent-tabs-mode`, siehe unten).

- Mit Alt+X fundamental-mode können Sie den gerade aktuellen Bearbeitungsmodus deaktivieren. Dann funktioniert ↹ wie in anderen Programmen gewohnt, allerdings verlieren Sie gleichzeitig auch alle Spezialfunktionen des bisher gültigen Bearbeitungsmodus.

Tabulatorweite

Als Tabulatorweite gelten normalerweise acht Zeichen. Mit Alt+X set-variable tab-width können Sie aber auch eine andere Tabulatorweite einstellen. Wenn Sie generell mit vier statt mit acht Zeichen pro Tabulator arbeiten möchten, können Sie diese Einstellung auch in der Konfigurationsdatei ~/.emacs vornehmen.

Wechsel zwischen Leerzeichen und Tabulatoren

In einigen Bearbeitungsmodi ersetzt der Emacs automatisch lange Folgen von Leerzeichen durch Tabulatoren. Mit den beiden Kommandos Alt+X tabify können Sie im vorher markierten Bereich alle Leerzeichenserien durch Tabulator-Zeichen ersetzen. Alt+X untabify funktioniert genau umgekehrt und ersetzt Tabulatoren durch eine ausreichende Anzahl von Leerzeichen.

indent-tabs-mode

Wenn Sie in die Konfigurationsdatei .emacs die folgenden Zeile einbauen, dann fügt der Emacs generell statt Tabulaturzeichen Leerzeichen ein:

```
(setq-default indent-tabs-mode nil)
```

Text manuell ein- und ausrücken

Das Ein- und Ausrücken von Text ist insbesondere in Programmlistings zur Strukturierung des Codes erforderlich. Das wichtigste Kommando wird mit Strg+X, ↹ aufgerufen. Es rückt den Text zwischen dem Markierungspunkt (Strg+␣) und der aktuellen Cursorposition um ein Leerzeichen ein. Wenn Sie vor diesem Kommando Alt+*n* ausführen, wird der markierte Textbereich um *n* Zeichen eingerückt. Durch ein vorangestelltes Esc, - wird der Text aus- statt eingerückt.

Tastenkürzel	Funktion
Strg+␣	Markierungspunkt setzen
Strg+X, ↹	Text zwischen Markierungspunkt und Cursorposition um ein Zeichen einrücken
Esc, -, Strg+X, ↹	Text um ein Zeichen ausrücken
Alt+*n*, Strg+X, ↹	Text um *n* Zeichen einrücken
Esc, -, Alt+*n*, Strg+X, ↹	Text um *n* Zeichen ausrücken

Tabelle 20.9 Text ein- und ausrücken

Rechteck-Kommandos

Wenn Sie rechteckige Textblöcke innerhalb von Zeilen einfügen oder löschen möchten (etwa bei der Bearbeitung von Tabellen oder zum Ein- oder Ausrücken von Kommentaren am Ende von Programmzeilen), müssen Sie mit den sogenannten Rechteck-Kommandos arbeiten (siehe Tabelle 20.10). Als Rechteck gelten dabei alle Zeichen im Bereich zwischen dem Markierungspunkt und der Cursorposition.

Noch komfortabler lassen sich rechteckige Textblöcke im CUA-Modus bearbeiten: Wenn dieser Modus aktiv ist, beginnen Sie die Rechteckmarkierung mit Strg+↵. Anschließend können Sie mit Entf Zeichen in allen Zeilen löschen bzw. mit allen anderen Tasten neuen Text einfügen.

Tastenkürzel	Funktion
Strg+␣	Markierungspunkt setzen
Strg+X, R, O	rechteckigen Bereich öffnen (Rectangle Open), d. h., in den rechteckigen Bereich Leerzeichen einfügen
Strg+X, R, K	rechteckigen Bereich löschen (Rectangle Kill)
Strg+X, R, Y	gelöschten rechteckigen Bereich an der Cursorposition einfügen (Rectangle Yank)
Alt+X string-rectangle	einen Text vor jede Zeile des markierten Bereichs einfügen
Strg+↵	Rechteck-Markierung im CUA-Modus

Tabelle 20.10 Rechteck-Kommandos

Der Emacs kennt darüber hinaus einige Bearbeitungsmodi, in denen Einrückungen automatisch durchgeführt werden. So werden im C-Modus Programmzeilen bei jeder geschweiften Klammer { oder } um einige Leerzeichen ein- oder ausgerückt (siehe Abschnitt 20.9).

20.6 Fließtext

Bisher habe ich angenommen, dass Sie mit dem Emacs Programmcode, Konfigurationsdateien etc. bearbeiten. Ein wenig anders sieht der Umgang mit dem Emacs aus, wenn Sie Fließtext bearbeiten möchten. Der Emacs führt normalerweise keinen automatischen Umbruch durch. Wenn Zeilen länger sind als die Bildschirm- oder Fensterbreite, dann wird am linken Ende ein \-Zeichen dargestellt und der Text in der nächsten Zeile fortgesetzt.

Wenn Sie eine einzelne längere Zeile umbrechen möchten, führen Sie das Kommando Alt+Q aus: Damit werden an geeigneten Stellen Leerzeichen durch Zeilenumbrüche ersetzt. Aus einer langen Zeile werden so mehrere kurze Zeilen. Dabei

betrachtet der Emacs alle Zeilen, die nicht explizit durch eine vollkommen leere Zeile von anderen Zeilen getrennt sind, als einen Absatz. Bei einem Programmlisting sind die Folgen dieses Kommandos natürlich fatal! Führen Sie mit Strg+X, U ein Undo durch.

Zeilenumbruch in LaTeX-Dokumenten

Wenn Sie TeX- oder LaTeX-Dateien bearbeiten, gilt für Alt+Q eine Besonderheit: Zeilen, die mit einem \-Zeichen beginnen, gelten als Absatzgrenze und werden nicht umbrochen. Um einen Umbruch dennoch durchzuführen, müssen Sie diese Zeile manuell mit der vorhergehenden Zeile verbinden und nochmals Alt+Q ausführen. Noch bequemer ist es, das AUC-TEX-Paket zu installieren und zu aktivieren: Dann versteht der Emacs LaTeX besser und führt den Zeilenumbruch intelligenter durch.

Bei der Eingabe eines neuen Textes ist es natürlich lästig, ständig Alt+Q zu drücken. Daher existiert ein eigener Fließtextmodus, der mit Alt+X `auto-fill-mode` ↵ aktiviert wird. Wenn sich der Emacs in diesem Modus befindet, werden alle Neueingaben automatisch umbrochen. Bereits vorhandener Text wird durch diesen Modus nicht verändert. Auch das Löschen von Text führt nicht zu einem automatischen Umbruch, weswegen nach Änderungen in einem bereits vorhandenen Fließtext häufig ein manueller Umbruch mit Alt+Q erzwungen werden muss. Der Umbruch erfolgt normalerweise spätestens nach 70 Zeichen. Sie können die Umbruchspalte mit dem folgenden Kommando verändern: Alt+X `set-variable` ↵ `fill-column` ↵ *n* ↵.

Tastenkürzel	Funktion
Alt+Q	führt einen manuellen Zeilenumbruch durch.
Alt+X `auto-fill-mode` ↵	aktiviert den Fließtextmodus (automatischer Zeilenumbruch).

Tabelle 20.11 Fließtext umbrechen

Wenn Sie mehrere Absätze eingerückten Textes eingeben möchten, können Sie die erste gültige Spalte voreinstellen. Dazu müssen Sie so viele Leer- oder Tabulatorzeichen in einer sonst leeren Zeile eingeben, wie Ihr Text eingerückt werden soll. Anschließend führen Sie Strg+X, . aus, also Strg+X, Punkt. Das Programm rückt jetzt ab der zweiten Zeile eines Absatzes alle Zeilen bis zur Einrückspalte ein.

Zum Neuformatieren größerer Textmengen, die unterschiedlich stark eingerückt sind, eignet sich das Kommando Alt+x `fill-individual-paragraphs` ↵. Dieses Kommando formatiert den gesamten Bereich zwischen dem Markierungspunkt (Strg+ ␣) und der aktuellen Cursorposition. Dabei werden die aktuellen Einrückungen beibehalten.

Tastenkürzel	Funktion
Strg+X, .	definiert die Einrückspalte durch die aktuelle Cursorposition. Der Cursor muss dazu in einer leeren (!) Zeile stehen.
Alt+M	bewegt den Cursor an den Beginn einer eingerückten Zeile (ähnlich wie Strg+A).
Strg+Leer	setzt den Markierungspunkt.
Alt+x fill-individ ↵	formatiert den Bereich zwischen Markierungspunkt und Cursorposition neu und behält die aktuellen Einrückungen bei.

Tabelle 20.12 Fließtext einrücken

Wenn Sie sehr viel mit Einrückungen arbeiten, ist der Textmodus bequemer als die oben beschriebene Vorgehensweise. Diesen Modus aktivieren Sie mit Alt+X `text-mode` ↵. Um in diesem Modus Fließtext zu bearbeiten, aktivieren Sie außerdem den dafür vorgesehenen Nebenmodus mit Alt+X `auto-fill-mode` ↵. Nebenmodi definieren einige zusätzliche Kommandos, die parallel zu einem beliebigen Hauptmodus verwendet werden können – siehe auch Abschnitt 20.9.

Die einzige wesentliche Neuerung des Textmodus besteht darin, dass der Emacs beim Zeilenumbruch jede neue Zeile automatisch so weit einrückt wie die vorhergehende Zeile. Auch Alt+Q für den manuellen Umbruch orientiert sich jetzt automatisch an der Einrückung der ersten Zeile.

Tastenkürzel	Funktion
Alt+X `text-mode`	aktiviert den Textmodus.
Alt+X `auto-fill-mode`	aktiviert den Nebenmodus für Fließtext.
Alt+Q	führt einen manuellen Umbruch durch und orientiert sich dabei an der Einrückung der aktuellen Zeile.
Alt+S	zentriert die aktuelle Zeile.
Alt+⇧+S	zentriert den aktuellen Absatz.

Tabelle 20.13 Textmodus

Wenn Sie Zeilen oder Absätze zentrieren möchten, ohne deswegen in den Textmodus zu wechseln, können Sie die entsprechenden Kommandos in den anderen Modi mit Alt+X `center-line` ↵ bzw. mit Alt+X `center-paragraph` ↵ aufrufen.

Abkürzungen

Eine Besonderheit des Emacs besteht darin, dass Sie ohne Vorarbeit Abkürzungen verwenden können. Dazu geben Sie die ersten Buchstaben eines Wortes ein und drücken Alt+/. Der Emacs sucht daraufhin zuerst im vorangehenden, dann im nachfolgenden Text und schließlich in allen geöffneten Dateien nach Wörtern, die mit diesen Zeichen beginnen. Wenn Sie an dieser Stelle im Text Um Alt+/ eingeben, ersetzt der Emacs »Um« durch »Umgebung«. Wenn Sie Alt+/ öfter drücken, bietet der Emacs weitere mögliche Ergänzungen an, etwa »Umgang« und »Umgehen«.

Dynamische Erweiterungen funktionieren nur, wenn sich ein Wort bereits im Text einer geladenen Datei befindet (es muss nicht die aktuelle Datei sein) und wenn die Anfangsbuchstaben übereinstimmen.

20.7 Suchen und Ersetzen

Am schnellsten finden Sie Text mit Strg+S *suchtext*. Das Kommando weist gegenüber den Suchkommandos anderer Programme eine Besonderheit auf: Es beginnt die Suche sofort nach der Eingabe des ersten Zeichens. Wenn Sie also »Nebenmodus« suchen und Strg+S Neb eingeben, dann springt der Cursor bereits zum ersten Wort, das mit »Neb« beginnt. Anstatt die weiteren Buchstaben einzugeben, können Sie jetzt durch das abermalige Drücken von Strg+S zum nächsten Wort springen, das auch mit »Neb« beginnt. (Wenn Sie nur Kleinbuchstaben eingeben, wird nicht zwischen Groß- und Kleinschreibung unterschieden.)

Wenn Sie jetzt auf die Idee kommen, dass Sie eigentlich nach »Neuigkeit« suchen, löschen Sie das »b« mit ←. Der Emacs springt zum ersten Wort zurück (ausgehend von der Position beim Beginn der Suche), das mit »Ne« beginnt. Mit der Eingabe von U springt Emacs weiter zum ersten Wort, das mit »Neu« beginnt. Probieren Sie es einfach einmal aus – Sie werden von diesem Konzept sofort begeistert sein!

Sobald Sie ↵ oder eine Cursortaste drücken, nimmt das Programm an, dass die Suche beendet ist, und setzt den Cursor an die gefundene Stelle. Der Beginn der Suche wird dabei durch einen Markierungspunkt gespeichert. Daher können Sie mit Strg+X, Strg+X den Cursor mühelos wieder dorthin zurückstellen, wo er zu Beginn der Suche stand. Ein abermaliges Strg+X, Strg+X führt Sie wieder an die Stelle des Suchtextes.

Durch zweimaliges Drücken von Strg+S können Sie die Suche wieder aufnehmen und zum nächsten Auftreten des Suchtextes springen. Wenn Sie rückwärts suchen möchten, drücken Sie einfach Strg+R statt Strg+S.

Tastenkürzel	Funktion
Strg+S	inkrementelle Suche vorwärts
Strg+R	inkrementelle Suche rückwärts
Alt+P	wählt einen früher verwendeten Suchtext aus (Previous).
Alt+N	wählt einen später verwendeten Suchtext aus (Next).
Strg+G	Abbruch der Suche
Strg+X, Strg+X	vertauscht den Markierungspunkt (Beginn der Suche) und die aktuelle Cursorposition.
Strg+Alt+S	inkrementelle Mustersuche vorwärts
Strg+Alt+R	inkrementelle Mustersuche rückwärts
Alt+%	Suchen und Ersetzen ohne Muster
Alt+X query-replace-r ↵	Suchen und Ersetzen mit Muster

Tabelle 20.14 Kommandos zum Suchen und Ersetzen

Wenn Sie zu einem späteren Zeitpunkt nach einem Text suchen möchten, den Sie früher schon einmal gesucht haben, können Sie nach Strg+S mit Alt+P (Previous) und Alt+N (Next) einen Text aus der gespeicherten Liste der Suchtexte auswählen.

Suche nach Mustern (mit regulären Ausdrücken)

Die inkrementelle Suche findet Texte, die exakt dem Suchtext entsprechen. Häufig ist es aber wünschenswert, nach Texten zu suchen, die einem bestimmten Muster entsprechen. Eine derartige Suche starten Sie mit Strg+Alt+S bzw. +R.

Im Suchtext wird zwischen Groß- und Kleinschreibung unterschieden. Zur Syntax der Musterzeichenkette folgen jetzt noch einige erklärende Beispiele:

- `\<[Dd]ie\>` sucht nach dem Artikel »die«, egal ob er klein- oder großgeschrieben ist. Wortzusammensetzungen mit »die« (also etwa »dieser«) werden ignoriert.
- `[Dd]ie[a-z]+` sucht nach Wortzusammensetzungen, die mit »Die« oder »die« beginnen und denen mindestens ein weiterer Buchstabe folgt. Der Cursor bleibt jeweils am Ende des Wortes stehen (beim ersten Zeichen, das kein Buchstabe zwischen a und z ist).
- `[Dd]ie[a-zäöüß]+` funktioniert wie oben beschrieben, findet aber auch Wortzusammensetzungen, die deutsche Sonderzeichen enthalten.

Die Zeichenpaare \(und \) haben keinen Einfluss auf die eigentliche Suche. Die Zeichen im gesuchten Text, die den in der Gruppe enthaltenen Zeichen entsprechen, können dann aber zum Bilden des Ersetzen-Textes wiederverwendet werden (siehe unten).

Suchmuster	Funktion
\<	Anfang eines Wortes
&	Ende eines Wortes
^	Anfang der Zeile
$	Ende der Zeile
.	ein beliebiges Zeichen mit Ausnahme eines Zeilenumbruchs
.*	beliebig viele (auch 0) beliebige Zeichen (wie * in Dateinamen)
.+	beliebig viele (aber mindestens ein) beliebige(s) Zeichen
.?	kein oder ein beliebiges Zeichen
[abc..]	eines der aufgezählten Zeichen
[^abc..]	keines der aufgezählten Zeichen
\(	Beginn einer Gruppe (siehe unten »Suchen und Ersetzen«)
\)	Ende einer Gruppe
\x	Sonderzeichen *x* (z. B. \\ zur Suche nach einem \-Zeichen oder \. zur Suche nach einem Punkt)
\&	Platzhalter im Ersetzen-Muster für den gesamten gefundenen Text
\1	Platzhalter im Ersetzen-Muster für die erste \(...\)-Gruppe im Suchtext ()

Tabelle 20.15 Aufbau eines regulären Suchmusters

Suchen und Ersetzen

Auch beim Suchen und Ersetzen unterscheidet der Emacs zwischen dem normalen Kommando und der erweiterten Version mit Mustersuche. Bei der normalen Variante mit Alt+% wird die Groß- und Kleinschreibung bei der Suche ignoriert. Beim Ersetzen (siehe Tabelle 20.16) bleiben die Anfangsbuchstaben von Wörtern so erhalten, wie sie bisher waren, wenn der Ersetzen-Text vollständig kleingeschrieben ist. Das Suchen- und Ersetzen-Kommando kann nicht für mehrzeilige Texte verwendet werden, weil die Joker-Zeichen * und + nicht über eine Zeile hinaus wirksam sind.

Das Suchen und Ersetzen mit Mustern starten Sie mit Alt+X query-replace-r ↵. In der Ersetzen-Zeichenkette können Sie mit \& und *n* Platzhalter angeben, die dem ganzen Suchmuster bzw. einem Teil davon entsprechen (siehe Tabelle

20.15). Damit lassen sich sehr komplexe Operationen effizient durchführen. Zur Veranschaulichung ein Beispiel:

Sie ersetzen `funktion(\([^,]*\),\([^,]*\))` durch `funktion(\2,\1)`: Bei jedem Aufruf von `funktion` werden die beiden Parameter vertauscht. Aus `funktion(a+b,2*e)` wird daher `funktion(2*e,a+b)`. Einzige Bedingung: In den Parametern der Funktion dürfen keine Kommata auftreten. Beim Vertauschen der Parameter in `funktion(f(a,b), g(x,y))` versagt das Kommando.

Verwenden Sie das Kommando zum Suchen und Ersetzen mit Mustern zunächst mit Vorsicht, und speichern Sie zuvor Ihren Text. Gerade bei den ersten Versuchen kommt es häufig vor, dass mit dem Suchmuster ganz andere (oft viel größere) Texte erfasst werden, als Sie geplant haben. Strg+X, Strg+U macht fehlerhafte Ersetzen-Kommandos bei Bedarf wieder rückgängig.

Tastenkürzel	Funktion
␣ oder Y	ersetzen, Suche fortsetzen
,	ersetzen, aber Cursor stehen lassen, damit das Ergebnis kontrolliert werden kann; wenn alles in Ordnung ist, kann das Kommando mit ␣ fortgesetzt werden.
← oder N	nicht ersetzen, Suche fortsetzen
Esc	nicht ersetzen, Kommando abbrechen
!	alle weiteren Ersetzungen ohne Rückfrage durchführen
Strg+R	Kommando vorläufig unterbrechen, um an der aktuellen Cursorposition eine manuelle Korrektur vorzunehmen (Recursive Edit)
Strg+Alt+R	Ersetzen-Kommando wieder aufnehmen

Tabelle 20.16 Tastenkürzel zur Bearbeitung des gefundenen Texts

20.8 Puffer und Fenster

Bei der Bearbeitung mehrerer Texte verwaltet Emacs jeden Text in einem sogenannten Puffer. Selbst wenn Sie mit nur einem Text arbeiten, existieren mehrere Puffer: einer für den Text (der Name des Puffers stimmt mit dessen Dateinamen überein), einer für ein irgendwann geöffnetes Info- oder Hilfefenster (Puffername `*info*` oder `*help*`), einer für die zuletzt angezeigte Liste mit möglichen Kommandos, die durch ↹ ergänzt wurden (`*completions*`) etc.

Neben dem Begriff des Puffers kennt der Emacs auch Fenster: Ein Fenster ist ein Bereich innerhalb des Emacs, in dem ein Puffer angezeigt wird. Normalerweise

wird nur ein einziges Fenster verwendet, das den gesamten zur Verfügung stehenden Raum nutzt. Bei der Ausführung mancher Kommandos (z. B. zur Anzeige von Hilfe- oder anderen Emacs-internen Informationen) wird der Bildschirm horizontal in zwei Fenster geteilt. Auch eine Unterteilung in mehrere horizontale oder vertikale Streifen ist möglich. Dabei kann in jedem Bereich (Fenster) ein anderer Puffer angezeigt werden.

Es besteht auch die Möglichkeit, in zwei Fenstern denselben Puffer darzustellen. Das ist vor allem bei sehr langen Texten praktisch: Sie können so zwei unterschiedliche Abschnitte des Textes bearbeiten, ohne ständig umständliche Cursorbewegungen durchführen zu müssen.

Verschiedene »Fenster«-Arten

Der Fensterbegriff in Emacs hat nichts mit einem herkömmlichen Fenster unter Gnome oder KDE zu tun, sondern meint nur einen Teilbereich innerhalb des Emacs-Fensters. Wenn Sie tatsächlich ein zweites Emacs-Fenster benötigen, etwa um zwei Programmlistings bequem nebeneinander zu bearbeiten, führen Sie File • New Frame aus.

Die Kommandos in Tabelle 20.17 beziehen sich auf das gerade aktuelle Fenster (also auf das Fenster, in dem der Cursor steht). Die Kommandos wechseln den Puffer, der in diesem Fenster angezeigt wird.

Tastenkürzel	Funktion
Strg+X, B, ↵	aktiviert den zuvor verwendeten Puffer.
Strg+X, B, *name* ↵	aktiviert den angegebenen Puffer.
Strg+X, Strg+B	zeigt in einem Fenster die Liste aller möglichen Puffer an. Dieses Fenster kann mit Strg+X, 1 wieder gelöscht werden.
Strg+X, K *name* ↵	löscht den angegebenen Puffer. Wenn der Puffer eine noch nicht gespeicherte Datei enthält, erscheint eine Sicherheitsabfrage.

Tabelle 20.17 Pufferkommandos

Die Kommandos in Tabelle 20.18 wirken sich nur auf die Anzeige der Puffer in verschiedenen Bildschirmbereichen (Fenstern) aus. Die Trennlinie zwischen den Fenstern kann mit der Maus bewegt werden. Die Puffer werden durch das Löschen eines Fensters nicht berührt; sie werden zwar unsichtbar, bleiben aber weiterhin im Speicher und können jederzeit wieder angezeigt werden.

Tastenkürzel	Funktion
Strg+X, O	springt zum nächsten Fenster (»Oh«).
Strg+X, 0	löscht das aktuelle Fenster (»Null«).
Strg+X, 1	löscht alle Fenster außer dem, in dem der Cursor steht.
Strg+X, 2	teilt das aktuelle Fenster in zwei horizontale Bereiche.
Strg+X, 3	teilt das aktuelle Fenster in zwei vertikale Bereiche.
Strg+X, <	verschiebt den Fensterinhalt nach links.
Strg+X, >	verschiebt den Fensterinhalt nach rechts.

Tabelle 20.18 Fensterkommandos

20.9 Besondere Bearbeitungsmodi

Zahlreiche Bearbeitungsmodi verändern die Funktionalität des Editors und stellen zusätzliche Spezialkommandos zur Verfügung. Damit wird der Emacs optimal an einen Texttyp angepasst. Je nach Modus werden außerdem Schlüsselwörtern und Kommentare farblich hervorgehoben.

Der Emacs unterscheidet zwischen Haupt- und Nebenmodi (siehe Tabellen 20.19 und 20.20). Es kann immer nur ein Hauptmodus aktiv sein. Dieser Modus wird automatisch entsprechend der Kennung des Dateinamens und nach Schlüsselwörtern im Text gewählt. Der Hauptmodus kann durch Nebenmodi ergänzt werden. Für jede im Emacs bearbeitete Datei (für jeden Puffer) gilt eine eigene Moduseinstellung. Die manuelle Veränderung des Modus wirkt sich immer nur auf den gerade aktuellen Puffer aus. Durch den Wechsel in einen anderen Hauptmodus wird der bisherige Modus deaktiviert. Das Ein- oder Ausschalten eines Nebenmodus verändert den Hauptmodus nicht.

Eine Übersicht über alle verfügbaren Modi gibt F1, A mode ↵. Informationen zum gerade aktiven Hauptmodus erhalten Sie mit F1, M.

Syntaxhervorhebung

Das vielleicht attraktivste Merkmal der Bearbeitungsmodi ist das sogenannte Syntax-Highlighting. Dabei werden Kommandos, Kommentare etc. durch Farben oder Schriftattribute gekennzeichnet. Programmcode, LaTeX-Dokumente etc. gewinnen dadurch erheblich an Übersichtlichkeit.

PHP-Modus

Unbegreiflicherweise enthält der Emacs standardmäßig keinen PHP-Modus. Einzig Fedora liefert entsprechende Erweiterungsdateien gleich mit. Bei den anderen Distributionen ist ein wenig Handarbeit erforderlich:

http://php-mode.sourceforge.net
http://kofler.info/blog/157/126/PHP-Mode-fuer-Emacs

Tastenkürzel	Funktion
Alt+X fundamental-mode ↵	Standardmodus (Grundeinstellung)
Alt+X text-mode ↵	Modus zur bequemen Einrückung von Text
Alt+X c-mode ↵	C-Modus
Alt+X c++-mode ↵	C++-Modus
Alt+X emacs-lisp-mode ↵	Emacs-Lisp-Dateien bearbeiten (z. B. `~/.emacs`)
Alt+X html-mode ↵	HTML-Modus
Alt+X java-mode ↵	Java-Modus
Alt+X latex-mode ↵	LaTeX-Modus
Alt+X sh-mode ↵	Modus zur Bearbeitung von Shell-Scripts

Tabelle 20.19 Wichtige Emacs-Hauptmodi

Tastenkürzel	Funktion
Alt+X auto-fill-mode ↵	Fließtextmodus (automatischer Wortumbruch)
Alt+X cua-mode ↵	CUA-Modus (Strg+C, Strg+X und Strg+V)
Alt+X font-lock-mode ↵	farbige Syntaxmarkierung
Alt+X iso-accents-mode ↵	Eingabe fremdsprachiger Sonderzeichen
Alt+X abbrev-mode ↵	Abkürzungsmodus (automatische Auflösung von Abkürzungen)

Tabelle 20.20 Wichtige Emacs-Nebenmodi

Automatische und explizite Moduseinstellung

Der Emacs versucht beim Laden einer Datei aus der Dateikennung und dem Inhalt der ersten Zeilen automatisch zu erkennen, um welchen Dateityp es sich handelt, und aktiviert dann den entsprechenden Modus. Nur wenn das nicht klappt, müssen Sie den Modus wie oben beschrieben manuell aktivieren. Wenn die automatische Aktivierung nicht funktioniert, können Sie auch in der ersten Zeile der Datei einen Kommentar einfügen, der die Zeichen `*-*` *name* `*-*` enthält. Statt *name* müssen Sie den Namen des gewünschten Modus angeben (also etwa `*-* html *-*`).

20.10 Konfiguration

Wohl kein anderer Editor bietet mehr Konfigurationsmöglichkeiten als der Emacs. Dieser Abschnitt gibt zuerst einen Überblick über die Konfigurationsdateien und beschreibt dann einige elementare Konfigurationsschritte.

Wenn sich Ihre Emacs-Version anders verhält, als in diesem Buch beschrieben wird, dann ist oft die Konfiguration Ihrer Linux-Distribution verantwortlich. Die Einstellungen können sich sowohl in den persönlichen als auch in den globalen Konfigurationsdateien (`site-start.el`) befinden. Beachten Sie insbesondere, dass bei vielen Distributionen beim Anlegen neuer Linux-Benutzer automatisch Konfigurationsdateien aus `/etc/skel` in das Benutzerverzeichnis kopiert werden!

Persönliche Konfiguration

Die benutzerspezifische Konfiguration kann wahlweise durch Menükommandos (Options-Menü) oder durch eine direkte Veränderung der Konfigurationsdateien `.emacs` durchgeführt werden.

Globale Konfiguration

Neben den persönlichen Konfigurationsdateien gibt es auch globale Konfigurationsdateien, deren Einstellungen für alle Benutzer gelten. Diese Dateien enthalten je nach Distribution diverse Voreinstellungen.

`/usr/share/emacs/site-lisp/site-start.el`	
`/usr/share/emacs/site-lisp/debian-startup.el`	(Debian, Ubuntu)
`/usr/share/emacs/site-lisp/site-start.d/*`	(Red Hat, Fedora)
`/usr/share/emacs/site-lisp/site-start.el`	(SUSE)

Konfiguration per Mausklick

Beim Emacs können Sie einige elementare Einstellungen direkt über Einträge des Options-Menüs vornehmen. Damit beispielsweise der Schiebebalken wie in allen anderen Programmen auf der rechten Seite angezeigt wird, führen Sie Options • Show/Hide • Scrollbar • On the Right aus. Die Einstellungen werden sofort wirksam, gehen aber verloren, wenn Sie den Emacs verlassen. Um geänderte Einstellungen bleibend in `.emacs` zu speichern, müssen Sie Options • Save Options ausführen!

Alle weitergehenden Einstellmöglichkeiten, von denen es Tausende gibt, sind über Options • Customize Emacs • Top-level Customization Group erreichbar (siehe Abbildung 20.2). Dieses Kommando öffnet einen neuen Emacs-Puffer, der wie ein Dialog aussieht. Die Buttons dieser Seite führen zu weiteren Dialogen für verschiedene Gruppen von Optionen. Auf jeder Seite können Sie durch Buttons alle durchgeführten Änderungen nur bis zum Programmende oder bleibend in `.emacs` speichern (Set for Current Session bzw. Save for Future Sessions).

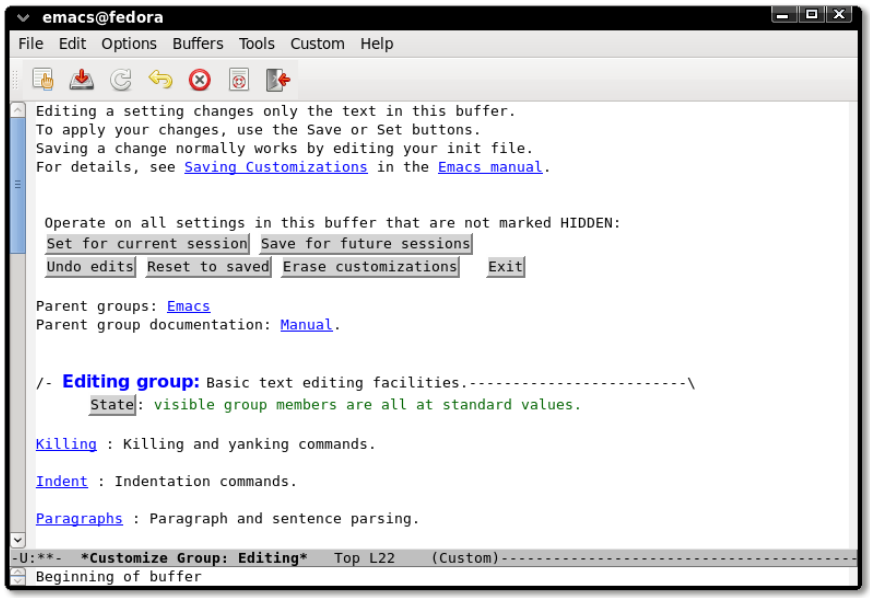


Abbildung 20.2 Emacs-Konfiguration

Die Bedienung der Dialogoptionen ist nicht schwierig; das Problem besteht aber darin, dass die Dialoge tief verschachtelt sind und es nicht immer ganz einfach ist, den richtigen Dialog für eine bestimmte Option zu finden.

Schriftart und -größe einstellen

Am schnellsten kann die Schriftart hier mit ⇧ und der linken Maustaste eingestellt werden. Allerdings besteht keine Möglichkeit, diese Einstellung auch zu speichern. Alternativ können Sie die Standardschrift auch mit OPTIONS • CUSTOMIZE • SPECIFIC FACE einstellen, wobei Sie die Schrift `default` auswählen. Im nun erscheinenden Dialog können Sie sowohl die Schriftfamilie als auch die Schriftgröße (Height) einstellen. Falls dem Namen der Schrift deren Hersteller vorangestellt wird, muss dies mit einem Bindestrich erfolgen (z. B. Adobe-Courier). An dieser Stelle können Sie auch die Hintergrundfarbe des Emacs einstellen: Geben Sie einfach im BACKGROUND-Feld der Schriftart `default` den Namen der gewünschten Farbe an (z. B. Lightgrey).

Mit SET FOR CURRENT SESSION können Sie Ihre Einstellungen ausprobieren. Der Schriftwechsel dauert einige Sekunden und führt dazu, dass auch die Fenstergröße von Emacs verändert wird. Mit SAVE FOR FUTURE SESSIONS wird die Einstellung in `.emacs` gespeichert.

Beispiel für .emacs

Anstatt sich durch verschachtelte Dialoge zu klicken, können Sie die Konfiguration auch direkt in `.emacs` durchführen. Der Platz reicht hier nicht für eine ausführliche Beschreibung aus. Stattdessen gibt das folgende kommentierte Listing einige Bei-

spiele für beliebte Optionen und Einstellungen. Bei manchen Linux-Distributionen gelten einige dieser Einstellungen standardmäßig.

```
;Beispiel für .emacs

;kein Begrüßungsbildschirm
(setq inhibit-startup-message t)

;Zeilen- und Spaltennummer in der Statuszeile anzeigen
(line-number-mode 1)
(column-number-mode 1)

;markierten Textbereich sichtbar machen
(setq-default transient-mark-mode t)

;mit <Tab> Leerzeichen statt Tabulatoren einfügen
(setq-default indent-tabs-mode nil)

;letzte Zeile automatisch mit Newline-Code abschließen
(setq require-final-newline t)

;Syntaxhervorhebung automatisch aktivieren
(global-font-lock-mode t)

;Cursorposition speichern
(require 'saveplace)
(setq-default save-place t)

;Scrollbar auf der rechten statt auf der linken Seite
(set-scroll-bar-mode 'right)

;AUC TEX aktivieren (das ist ein erweiterter LaTeX-Modus;
;das auctex-Paket muss separat installiert werden!)
(require 'tex-site)

; ein paar Tastaturkürzel:
(global-set-key [f2]  'switch-to-buffer)         ;Buffer wechseln
(global-set-key [f3]  'font-lock-fontify-buffer) ;Syntaxhervorhebung
(global-set-key [f4]  'goto-line)                ;zur Zeile n springen
(global-set-key [f5]  'advertised-undo)          ;Undo-Funktion
```

Emacs-Lisp-Programmierung

Noch viel mehr Konfigurationsmöglichkeiten haben Sie, wenn Sie sich auf die Emacs-Lisp-Programmierung einlassen. Damit können Sie in der Konfigurationsdatei `.emacs` eigene Kommandos, Tastenkürzel etc. definieren. Schauen Sie sich dazu *http://www.dotemacs.de* an.

20.11 Unicode

Emacs kommt dank der Mule-Erweiterung (Multilingual Enhancement) mit den meisten gängigen Zeichensätzen zurecht. Mule-Kommandos können über das Menü OPTIONS • MULE ausgeführt werden. Mit Version 23 wurde die interne Textverwaltung vollständig auf Unicode umgestellt (Native Unicode Support); ältere Emacs-Versionen verwenden ein eigenes Textformat. Für den Anwender ergeben sich durch diese Umstellung aber keine Änderungen.

Zeichensatz explizit angeben

Der Emacs erkennt den Zeichensatz von Dateien in vielen Fällen selbstständig bzw. verwendet einfach den Standardzeichensatz Ihrer Distribution. In manchen Fällen ist es aber notwendig, den Zeichensatz explizit zu bestimmen. Dazu geben Sie mit dem Kommando Strg+X, ↵, C *codierung* an, welcher Zeichensatz bei der Ausführung des nächsten Kommandos gelten soll. Die zur Auswahl stehenden Codierungen ermitteln Sie dabei bequem mit ↹.

Kurzbezeichnung	Bedeutung
iso-8859-n	ISO-8859-*n*-Dateien
iso-latin-n	ISO-Latin-*n*-Dateien
utf-8	UTF-8-Dateien
utf-8-dos	UTF-8-Dateien mit DOS/Windows-Zeilenkennung
utf-8-unix	UTF-8-Dateien mit Unix/Linux-Zeilenkennung
binary	Binärdatei

Tabelle 20.21 Häufig eingesetzte Codierungen

Um die Codierung eines bereits geladenen Buffers zu verändern, führen Sie Strg+X, ↵, F *codierung* aus. Welcher Zeichensatz gerade benutzt wird, geht aus den ersten Zeichen der Statuszeile hervor. `-U` bedeutet beispielsweise, dass ein Unicode-Text vorliegt.

Hilfsfunktionen

Strg+H, ⇧+C, ↵ beschreibt die Codierung des aktuellen Buffers. Strg+U, Strg+X, = beschreibt den Code des Zeichens unter dem Cursor.

Eingabe fremdsprachiger Sonderzeichen

Mit den oben beschriebenen Kommandos bzw. Funktionen sollte es Ihnen gelingen, Unicode-Dateien korrekt zu laden, darzustellen und wieder zu speichern. Meist wollen Sie derartige Texte aber auch selbst ändern. Aber was tun Sie, wenn das gewünschte Zeichen nicht auf der Tastatur zu finden ist?

Unicode-Zeichen

Jedes Unicode-Zeichen kann durch seinen hexadezimalen Code eingegeben werden. Dazu führen Sie Alt+X ucs-insert *n* oder kürzer Alt+X 8 ↵ *n* aus. Das Euro-Zeichen geben Sie beispielsweise mit Alt+X 8 ↵ 20ac ein. Das Kommando ucs-insert akzeptiert auch die Namen von Unicode-Zeichen. Daher fügt auch Alt+X 8 ↵ euro sign das Euro-Zeichen ein. Weitere Tipps zur Eingabe von Unicode-Zeichen finden Sie hier:

http://ergoemacs.org/emacs/emacs_n_unicode.html

Latin-9-Prefix-Modus

Mit Alt+X set-input-method ↵ latin-9-prefix aktivieren Sie einen speziellen Modus. Er hilft bei der Eingabe von Zeichen aus dem Latin-Zeichensatz, die durch Akzente, Striche, Kreise oder anders modifiziert sind. Beispiele sind etwa à, á, â, ã, å, ä, ø oder ç. Der Modus ist auch dann praktisch, wenn Sie die Zeichen äöüß auf einer Tastatur mit US-Layout eingeben möchten.

Die Tasten ", ~, ^, /, ' und ` haben jetzt eine neue Bedeutung: Wird direkt anschließend ein passender Buchstabe eingegeben, verbindet der Emacs die beiden Zeichen zu einem neuen Buchstaben. Die Eingabe " O liefert also den Buchstaben Ö, " s ein ß, ~, c ein ç, /, a ein å, /, e ein æ, /, o ein ø. Um ein " einzugeben, müssen Sie nun allerdings " ␣ oder Strg+Q, " tippen.

Andere Eingabemodi

Mit Alt+X set-input-method ↵ ⇆ können Sie zwischen rund 50 weiteren Modi auswählen. Diese Modi helfen z. B. bei der Eingabe chinesischer, japanischer und koreanischer Zeichen. Der gewählte Eingabemodus kann durch die Tastenkombination Strg+\ jederzeit deaktiviert bzw. anschließend wieder aktiviert werden.

TEIL IV

Systemkonfiguration und Administration

Kapitel 21
Basiskonfiguration

Dieses Kapitel ist das erste einer ganzen Reihe von Kapiteln zur Linux-Systemkonfiguration. Nach einigen einleitenden Informationen geht es in diesem Kapitel um elementare Funktionen:

- Konfiguration von Textkonsolen
- Einstellung von Datum und Uhrzeit
- Benutzerverwaltung
- Internationalisierung, Zeichensatz, Unicode
- Überblick über die Hardware-Konfiguration
- Logging-Dateien

Die weiteren Kapitel behandeln dann die Paketverwaltung, die Verwaltung der Systembibliotheken, die Konfiguration des Grafiksystems (X), die Administration des Dateisystems, den Systemstart (GRUB, Init-System) und den Umgang mit dem Kernel und seinen Modulen.

21.1 Einführung

Dieses und die folgenden Kapitel geben Ihnen einen Blick hinter die Kulissen der Linux-Konfigurationsprogramme. Sie sollen verstehen, was wie wo gesteuert und voreingestellt wird. Daher werden Sie hier eine Menge Hintergrundinformationen darüber finden, wie das Gesamtsystem funktioniert.

Leider unterscheiden sich unterschiedliche Distributionen bei der Konfiguration in vielen kleinen Details. In diesem Buch versuche ich, den gemeinsamen Nenner möglichst vieler Linux-Systeme zu beschreiben. Dennoch kann es vorkommen, dass gerade bei Ihrer Distribution einzelne Details ein wenig anders gelöst sind. In solchen Fällen bleibt Ihnen ein Blick in die Dokumentation bzw. eine Internet-Suche nicht erspart.

Auch wenn das für Sie vielleicht hin und wieder unangenehm ist, bin ich dennoch überzeugt, dass der allgemeingültige Ansatz der bessere ist als ein Buch zur

Red-Hat-Administration, ein weiteres zur SUSE-Administration etc. – nicht zuletzt deswegen, weil sich ja auch die einzelnen Distributionen von Version zu Version ändern. Über kurz oder lang müssen Sie also in jedem Fall lernen, selbst die oft englischsprachigen Manuals, Hilfeseiten etc. zu lesen und zu verstehen. Dieses Buch will keine Originalhandbücher oder Schritt-für-Schritt-Anleitungen ersetzen, sondern Grundlagenwissen vermitteln!

Wer ist hier der Systemadministrator?

Bisher war der sogenannte Systemadministrator vielleicht irgendeine fremde Person, die Ihnen – oft unwillig und überarbeitet – zu Hilfe kam. Wenn Sie nicht in einem großen Betrieb arbeiten, dann ist der Administrator wohl überhaupt nur ein abstrakter Begriff aus vielen Büchern, so etwa nach dem Motto: »Wenn's nicht mehr weitergeht, fragen Sie den Systemadministrator ...«

Indem Sie Linux selbst auf Ihren Rechner installiert haben, ändert sich dieses Bild: Nun sind *Sie* der Systemadministrator! Erschrecken Sie nicht vor diesem Begriff – der Systemadministrator ist einfach die Person, die sich um die Konfiguration des Rechners kümmert. Solange es um die Linux-Grundfunktionen geht, kann das jeder!

Konfigurations- und Administrationswerkzeuge

Viele Distributionen bieten komfortable Konfigurationsprogramme an, die sowohl während als auch nach der Installation verwendet werden können, z. B. diverse `system-xxx`-Programme bei Red Hat und Fedora bzw. YaST bei SUSE. Diese Werkzeuge sollten bei grundlegenden Konfigurationsproblemen immer die erste Wahl sein! Sie sind speziell für die jeweilige Distribution optimiert und können Ihnen viel Arbeit und Mühe abnehmen.

Neben den mitgelieferten Konfigurationsprogrammen gibt es auch externe Werkzeuge bzw. eigene Linux-Distributionen mit zusätzlichen Administrationswerkzeugen. Viele davon lassen sich über eine Webschnittstelle bedienen. Tabelle 21.1 gibt einen Überblick über einige populäre Werkzeuge. Beachten Sie bitte, dass der Einsatzzweck und der Funktionsumfang dieser Werkzeuge sehr weit variiert. Ein Teil der aufgezählten Werkzeuge ist speziell zur Wartung vieler gleichartiger Linux-Installationen gedacht. Ein Bullet in der Spalte FREI bedeutet, dass es sich um Open-Source-Software handelt, die auch in Unternehmen kostenlos genutzt werden kann. Auch bei den meisten kommerziellen Produkten gibt es freie Varianten mit reduziertem Funktionsumfang.

Vermeiden Sie Abhängigkeiten!

Mit kommerziellen Administrationswerkzeugen rutschen Sie leicht in neue Abhängigkeiten. Zudem habe ich in der Vergangenheit schon eine Menge Administrationswerkzeuge kommen und wieder gehen gesehen. Entscheiden Sie sich nicht leichtfertig für externe Administrationswerkzeuge!

Link	Funktion	frei
http://webmin.com	System- und Netzwerkadministration	•
http://fai-project.org	Software-Verteilung und -Installation	•
http://m23.sourceforge.net	Software-Verteilung und -Administration	•
http://directory.fedoraproject.org	LDAP-Benutzeroberfläche für RHEL/Fedora	•
https://oss.gonicus.de/labs/gosa	LDAP-Account-Verwaltung für Debian	•
http://redhat.com/rhn	Red Hat-Administration	
http://novell.com/zenworks	Novell/SUSE-Administration	
http://canonical.com/landscape	Ubuntu-Administration	
http://univention.de/produkte/ucs	LAN- und Mail-Server-Konfiguration	
http://zentyal.org	LAN-Server-Konfiguration (ehemals eBox)	
http://cpanel.net	Root- und Webserver-Administration	
http://parallels.com/plesk	Root- und Webserver-Administration	

Tabelle 21.1 Ausgewählte Administrationswerkzeuge

Konfigurationsdateien

Ausgefeilte Konfigurationswerkzeuge mit schönen Benutzeroberflächen nehmen Ihnen die Mühe ab, Linux-Konfigurationsdateien direkt zu verändern. Gerade für Linux-Einsteiger ist dies zweifelslos praktisch. Es gibt aber eine ganze Reihe von Gründen, sich dennoch mit den Konfigurationsdateien und damit mit den Interna von Linux auseinanderzusetzen:

- Die Konfigurationsdateien lassen sich mit jedem beliebigen Texteditor verändern, auch in einer Textkonsole oder über eine SSH-Verbindung.
- Sobald Sie einmal verstanden haben, wie die Konfiguration einer bestimmten Linux-Funktion erfolgt, können Sie dieses Wissen bei beinahe jeder anderen Linux-Distribution anwenden.
- Nur durch die direkte Veränderung der Konfigurationsdateien können Sie alle Aspekte einer Systemfunktion steuern. Konfigurationswerkzeuge beschränken sich dagegen oft auf einige besonders wichtige Details.
- Konfigurationsdateien lassen sich leicht von einem Rechner zum anderen kopieren. Das kann eine Menge Zeit sparen, wenn Sie einen Distributionswechsel durchführen, Linux auf einem anderen Rechner neu installieren etc.
- Je besser Sie verstehen, wie die Konfigurationsdateien aufgebaut sind und welche Steuerungsmöglichkeiten sie bieten, desto besser verstehen Sie Linux und desto weniger ist Ihr Rechner die sprichwörtliche »Black Box«, in die keiner hineinblicken kann.

Das Zeilenende kann entscheidend sein!

Achten Sie beim Editieren von Konfigurationsdateien darauf, dass auch die letzte Zeile mit ↵ abgeschlossen wird. Manche Linux-Programme bearbeiten Dateien nicht korrekt, wenn in der letzten Zeile das Zeilenende fehlt.

/etc-Verzeichnis

Fast alle Linux-Konfigurationsdateien befinden sich im `/etc`-Verzeichnis. Eine Referenz aller im Buch behandelten Konfigurationsdateien finden Sie daher im Stichwortverzeichnis unter dem Buchstaben E. Zusammengehörende Konfigurationsdateien größerer Programme sind oft in eigenen Unterverzeichnissen organisiert (siehe Tabelle 21.2).

Verzeichnis	Inhalt
`/etc/default`	distributionsspezifische Dateien (Debian, Ubuntu)
`/etc/init.d`, `/etc/rc*.d`	Init-V-System (siehe Kapitel 27)
`/etc/init`	Upstart (siehe Kapitel 27)
`/etc/systemd`	Systemd (siehe Kapitel 27)
`/etc/sysconfig`	distributionsspezifische Dateien (Fedora, Red Hat, SUSE)
`/etc/X11`	Grafiksystem

Tabelle 21.2 Wichtige /etc-Verzeichnisse

/etc-Backup

Es ist eine gute Idee, eine Sicherheitskopie des gesamten `/etc`-Verzeichnisses anzulegen. Damit können Sie nach Änderungen jederzeit rasch feststellen, wie der ursprüngliche Zustand einer bestimmten Konfigurationsdatei war.

```
root#  mkdir /etc-backup
root#  cp -a /etc/* /etc-backup
```

Konfigurationsdateien suchen

Wenn Sie eine Konfigurationsdatei in Ihrer Distribution nicht finden, kann das mehrere Ursachen haben: Möglicherweise sind die zugrunde liegenden Programmpakete gar nicht installiert, oder die Konfigurationsdateien befinden sich bei Ihrer Distribution an einem anderen Ort. Verwenden Sie zur Suche die Kommandos `locate`, `find` und `grep`. Das folgende Kommando zeigt, wie Sie in `/etc` und allen Unterverzeichnissen nach Dateien suchen können, deren Inhalt (nicht der Dateiname) das Wort `abcde` enthält:

```
root#  cd /etc
root#  find -type f -exec grep -q abcde {} \; -print
```

Während der Arbeit an diesem Buch habe ich oft danach gesucht, wo bei der Distribution *x* die Funktion *y* gesteuert oder das Programm *z* aufgerufen wird. Dazu hätte

ich das obige Kommando wohl einige Hunderte Male eintippen müssen. Um Zeit und Mühe zu sparen, habe ich als Alternative das Mini-Script `grepall` geschrieben, das diese Aufgabe übernimmt (siehe Abschnitt 14.8).

Neue Konfiguration aktivieren

Bei manchen Programmen werden Änderungen an den Konfigurationsdateien erst wirksam, wenn Sie das Programm neu starten bzw. es explizit dazu auffordern, die Konfigurationsdateien neu einzulesen. Hierfür müssen Sie je nachdem, welches Init-System in Ihrer Distribution zum Einsatz kommt, eines der folgenden Kommandos ausführen (siehe auch Abschnitt 16.5):

```
root#  /etc/init.d/funktionsname reload     (Debian 6, alte Distributionen)
root#  /etc/init.d/funktionsname restart
root#  service funktionsname reload         (die meisten gängigen Distributionen)
root#  service funktionsname restart
```

Im Gegensatz zu Windows ist es fast nie erforderlich, den Rechner neu zu starten. Ausnahmen sind nur Veränderungen am Kernel sowie einige hardware-spezifische Einstellungen, die nur unmittelbar beim Systemstart durchgeführt werden können.

21.2 Konfiguration der Textkonsolen

Bei modernen Distributionen startet Linux direkt das Grafiksystem, und Linux-Einsteiger wissen oft gar nicht, dass es auch Textkonsolen gibt. Hin und wieder kommt es freilich vor, dass die X-Konfiguration fehlerhaft ist oder aus anderen Gründen kein grafisches System zur Verfügung steht. Bei Server-Installationen wird oft bewusst auf das Grafiksystem verzichtet. In solchen Fällen müssen Sie sich mit den Textkonsolen anfreunden. Für elementare Einstellungen wie das Tastaturlayout und die Schriftart ist je nach Distribution entweder das `kbd`-System oder das neuere `console`-System verantwortlich. Im Detail sieht die Konfiguration bei jeder Distribution ein wenig anders aus.

Tastaturlayout

Debian, Ubuntu

Unter Debian und Ubuntu kümmern sich die Programme des Pakets `console-setup` um das Tastaturlayout. Die Konfigurationsdatei `/etc/default/console-setup` steuert die Schriftart, die Datei `/etc/default/keyboard` das Tastaturlayout. Hierfür kommen dieselben Parameter wie bei der X-Konfiguration zur Anwendung (siehe auch Abschnitt 24.5):

```
# /etc/default/console-setup
...
# Schriftart
CHARMAP="UTF-8"
```

```
CODESET="Lat15"
FONTFACE="VGA"
FONTSIZE="16"

# /etc/default/keyboard
# Tastatur
XKBMODEL="pc105"
XKBLAYOUT="de"
XKBVARIANT=""
XKBOPTIONS="lv3:ralt_switch"
```

Unter Debian werden beide Dateien vom Script `/bin/setupcon` ausgewertet, das wiederum vom Init-V-Script `/etc/init.d/keyboard-setup` ausgeführt wird.

Unter Ubuntu erfolgt die Auswertung der `console-setup`-Konfigurationsdatei durch das `udev`-System, genau genommen durch das Script `/lib/udev/console-setup-tty`. Die Konfiguration der Tastatur erfolgt durch Upstart (`/etc/init/console-setup.conf`). Dabei wird aber nicht `/etc/default/keyboard` gelesen, sondern die Datei `/etc/console-setup/cached.kmap.gz`. Diese Datei wird bei der Erzeugung der Initrd-Datei durch das Script `/usr/bin/ckbcomp` aktualisiert.

Egal, ob Debian oder Ubuntu: Veränderungen am Tastaturlayout sollten Sie nach Möglichkeit nicht durch eine direkte Veränderung der Konfigurationsdateien vornehmen, sondern mit dem folgenden Kommando:

```
root#  dpkg-reconfigure keyboard-configuration
```

Das stellt sicher, dass alle Dateien aktualisiert werden und die Einstellungen sofort wirksam werden.

Fedora

Fedora verwendet das `kbd`-Paket zur Einstellung des Tastaturlayouts. Bei aktuellen Fedora-Versionen ist Systemd für das Tastaturlayout verantwortlich. Die Einstellungen werden in zwei Dateien gespeichert: in `/etc/vconsole.conf` für den Textmodus und in `/etc/X11/xorg.conf.d/00-keyboard.conf` für den Grafikmodus.

```
# Datei /etc/vconsole.conf
KEYMAP="de"
FONT="latarcyrheb-sun16"
```

Das Kommando `localectl list-keymaps` liefert eine Liste aller möglichen Tastaturlayouts. Zur Konfiguration können Sie `localectl set-keymap` verwenden. `localectl` versucht die Einstellung auch für den Grafikmodus zu übernehmen, was aber nicht immer gelingt. Im folgenden Beispiel werden zuerst alle deutschen Tastaturlayouts ermittelt und dann die Variante für Apples Mac-Tastatur eingestellt:

```
root#  localectl list-keymaps | egrep '^de.*|de-'
de
de-deadacute
de-mac
...
root#  localectl set-keymap de-mac
```

Bei RHEL sowie bei älteren Fedora-Versionen bestimmt hingegen die Datei `/etc/sysconfig/keyboard` das Tastaturlayout: RHEL

```
# Datei /etc/sysconfig/keyboard
KEYTABLE="de-latin1-nodeadkeys"
MODEL="pc105"
LAYOUT="de"
VARIANT="nodeadkeys"
```

Die Tastaturtabelle wird während des Systemstarts von einem Initrd-Script eingestellt. Damit Änderungen an dieser Datei wirksam werden, müssen Sie mit dem Kommando `dracut` die Initrd-Dateien neu erzeugen:

```
root#  dracut -f
```

Auch SUSE verwendet das `kbd`-Paket. Die Konfiguration befindet sich in `/etc/sysconfig/keyboard`. Sie wird durch das Init-V-Script `/etc/init.d/kbd` ausgewertet. Die Einstellungen gelten nur für die Konsole, nicht für X. SUSE

Schriftart

Konsolen sind grundsätzlich Unicode-kompatibel. Allerdings ist die Maximalanzahl der möglichen Zeichen in Konsolenschriften sehr klein (256 bzw. 512). Daher können Konsolenschriften immer nur einen winzigen Bruchteil aller Unicode-Zeichen abbilden.

Die Konfigurationseinstellungen befinden sich in `/etc/default/console-setup` und werden während des Systemstarts durch das Script `setupcon` ausgewertet. Unter Debian ist dafür das Init-V-Script `/etc/init.d/console-setup` verantwortlich, unter Ubuntu die Upstart-Konfigurationsdatei `/etc/init/console-setup.conf`. Debian, Ubuntu

Aktuelle Fedora-Versionen speichern die Konsolenschrift in der Datei `/etc/vconsole.conf`. Diese Datei wird durch Systemd ausgewertet. Fedora

Bei RHEL und älteren Fedora-Versionen wird die Schriftart mit `setfont` durch ein Script der Initrd-Datei eingestellt, wobei die Konfigurationsdatei `/etc/sysconfig/i18n` ausgewertet wird. Änderungen an dieser Datei werden nur wirksam, wenn Sie die Initrd-Dateien mit `dracut -f` neu erzeugen. RHEL

SUSE

Bei SUSE wird die Konsolenschrift durch `/etc/init.d/kbd` eingestellt. Dieses Script wertet `/etc/sysconfig/console` aus und stellt die Schrift mit `setfont` ein. Standardmäßig kommt die Schrift `lat9w-16.psfu` zum Einsatz, die neben den Latin-1-Zeichen auch das Euro-Symbol enthält.

gpm-Konfiguration (Maus)

Die Verwendung der Maus ist eigentlich nur im X Window System vorgesehen. Das Programm `gpm` erlaubt eine eingeschränkte Benutzung der Maus aber auch in Textkonsolen: Insbesondere können Sie nun mit der linken Maustaste Text markieren und ihn mit der mittleren oder rechten Maustaste an der aktuellen Cursorposition einfügen. Beachten Sie aber, dass Sie bei den meisten Konsolenprogrammen die Cursorposition nicht mit der Maus verändern können.

Sofern `gpm` installiert ist, wird es durch das Init-System gestartet. Die Konfiguration erfolgt je nach Distribution durch `/etc/gpm.conf` oder `/etc/sysconfig/mouse`, wobei es selten erforderlich ist, die Standardeinstellungen zu verändern.

21.3 Datum und Uhrzeit

Wegen der internationalen Vernetzung von Rechnern ist die Verwendung einer weltweit einheitlichen Uhrzeit erforderlich, nämlich der Greenwich Mean Time. Auf Unix-Rechnern ist die GMT das Maß aller Dinge bzw. der Zeit. Anstelle von GMT ist als zweite Abkürzung auch UTC üblich (Universal Time, Coordinated).

Wenn Sie eine Datei speichern, dann wird nicht die aktuelle Ortszeit gespeichert, sondern eine auf diesen internationalen Standard umgerechnete Zeit. Wenn Sie die Datei anschließend mit `ls -l` ansehen, wird die Uhrzeit wieder auf die Ortszeit am Standort des Rechners zurückgerechnet. Dieses Verfahren ermöglicht es festzustellen, welche Datei aktueller ist: eine um 18:00 Ortszeit in München gespeicherte Datei oder eine um 12:30 Ortszeit in New York gespeicherte Datei.

Zeiteinstellung während des Rechnerstarts

Während der Rechner hochfährt, wird mit dem Kommando `hwclock` die Uhrzeit aus der CMOS-Uhr Ihres Rechners gelesen. Die CMOS-Uhr Ihres Rechners kann die lokale Zeit oder GMT enthalten. Auf reinen Linux-Rechnern ist es zweckmäßig, die CMOS-Uhr mit der GMT zu stellen. Windows erwartet hingegen die lokale Zeit, es sei denn Sie verändern einen Eintrag in der Registry:

```
> reg.exe add HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation
             /v RealTimeIsUniversal /t REG_DWORD /d 1 /f
```

Bei RHEL und SUSE enthält die Konfigurationsdatei `/etc/sysconfig/clock` Informationen darüber, ob die CMOS-Uhr die lokale Zeit oder die GMT-Zeit enthält und in

welcher Zeitzone sich Ihr Rechner befindet. Aktuelle Debian- und Fedora-Versionen entnehmen diese Information der Datei `/etc/adjtime`, Ubuntu wertet `/etc/default/rcS` aus.

Einstellung der Zeitzone

Damit Kommandos wie `ls` oder die Datei-Manager von KDE und Gnome die GMT-Zeit in die lokale Zeit umrechnen und entsprechend anzeigen können, muss jedes Programm wissen, in welcher Zeitzone es läuft. Fast alle Linux-Programme greifen dazu auf Funktionen der glibc-Bibliothek zurück. Diese Bibliothek wertet die Datei `/etc/localtime` aus. Bei dieser Datei handelt es sich um den Link oder eine Kopie einer Zeitzonendatei aus dem Verzeichnis `/usr/share/zoneinfo`. `localtime` kann auch ein symbolischer Link auf eine Zeitzonendatei sein. Zur Neueinstellung der Zeitzone richten Sie den Link auf die gewünschte Zeitzonendatei neu ein. Um das möglichst komfortabel zu machen, gibt es für die meisten größeren Städte eigene Zeitzonendateien. Jene von Berlin enthält die Information, dass für Berlin die mitteleuropäische Sommerzeit gilt (Zeitzone MESZ).

```
root#  ln -s -f /usr/share/zoneinfo/Europe/Berlin /etc/localtime
```

Bei Debian und Ubuntu gibt auch die Textdatei `/etc/timezone` die Zeitzone an. Diese Datei wird aber nicht unmittelbar von der glibc-Bibliothek ausgewertet, sondern nur von den Werkzeugen zur Neueinstellung der `localtime`-Datei.

Konfigurationswerkzeuge

Je nach Distribution können Sie ein Konfigurationsprogramm verwenden, um die Zeitzone sowie Datum und Uhrzeit der Rechner-Uhr zu verändern:

Gnome 2.*n*:	`time-admin`
Gnome 3.*n*:	Systemeinstellungensmodul DATUM UND ZEIT
KDE:	Kontrollzentrum-Modul SYSTEMVERWALTUNG • DATUM/ZEIT
Debian, Ubuntu:	`dpkg-reconfigure tzdata`
Fedora/Systemd:	`timedatectl`
Red Hat:	`system-config-date`
SUSE:	YaST-Modul SYSTEM • ZEITZONE

NTP

Statt die notorisch ungenaue CMOS-Uhr des Rechners auszuwerten, können Sie die Uhrzeit über das *Network Time Protocol* (NTP) mit einem Zeit-Server im Internet abgleichen. Zur Nutzung von NTP bestehen zwei Möglichkeiten:

- Das Kommando `ntpdate` bezieht *einmal* die exakte Zeit und stellt die Uhr des Rechners. Bei Rechnern, die häufig ein- und ausgeschaltet werden, ist das ausreichend genau.

- Bei einem Server, der oft wochen- oder monatelang läuft, reicht die einmalige korrekte Einstellung der Uhrzeit nicht aus. Die Uhrzeit des Rechners wird im Laufe der Zeit immer stärker von der exakten Zeit abweichen. Abhilfe schafft der Dämon `ntpd`, der regelmäßig Kontakt zu anderen Zeit-Servern herstellt und die lokale Uhrzeit in kleinen Schritten korrigiert. `ntpd` kann gleichzeitig selbst als Zeit-Server für andere Rechner fungieren (beispielsweise für alle Clients im lokalen Netzwerk).

  Auch wenn Sie auf einem Rechner `ntpd` einsetzen, ist `ntpdate` praktisch, um die Uhrzeit erstmalig exakt einzustellen. `ntpd` funktioniert nämlich nur dann, wenn die anfängliche Abweichung zwischen der exakten und der lokalen Uhrzeit kleiner als eine Minute ist.

Anstelle der klassischen NTP-Werkzeuge (`ntpdate`, `ntpd`) kann zur Zeiteinstellung auch das modernere Programm Chrony verwendet werden (siehe den folgenden Abschnitt). Chrony basiert ebenfalls auf NTP und kommt unter Fedora seit Version 16 standardmäßig zum Einsatz.

Abrupte Zeitänderungen sind gefährlich

Es gibt eine ganze Menge Programme, die plötzliche Zeitänderungen schlecht vertragen. Dazu zählen beispielsweise das Authentifizierungssystem Kerberos, der POP3- und IMAP-Server Dovecot sowie Datenbank-Server. Es ist empfehlenswert, solche Programme vor der Ausführung von `ntpdate` bzw. vor der manuellen Veränderung der Uhrzeit herunterzufahren und anschließend neu zu starten. Dovecot endet automatisch, wenn es entdeckt, dass die Uhrzeit zurückgestellt wurde.

Links

Weitere Informationen zur Verwaltung von Datum und Uhrzeit finden Sie auf den folgenden Seiten:

http://www.ntp.org
http://tldp.org/HOWTO/TimePrecision-HOWTO
http://wwp.greenwichmeantime.com

Debian, Ubuntu

Ob und wie die Programme `ntpdate` und `ntpd` gestartet werden, hängt von der gewählten Distribution ab. Bei Ubuntu ist `ntpdate` standardmäßig installiert und wird immer dann ausgeführt, wenn eine Verbindung zu einem Netzwerk hergestellt wird (Script `/etc/network/if-up.d/ntpdate`). Debian verhält sich ebenso, allerdings wird `ntpdate` nicht per Default installiert.

Wenn Sie auf dem Rechner auch `ntpd` ausführen möchten, müssen Sie das Paket `ntp` installieren. Außerdem sollten Sie der Datei `/etc/ntp.conf` die Adresse eines nahegelegenen, gut erreichbaren NTP-Servers hinzufügen.

Mit `ntpq -p` überzeugen Sie sich davon, dass `ntpd` funktioniert. Entscheidend ist die `offset`-Spalte der Ausgabe dieses Kommandos: Sie gibt die Differenz zwischen der lokalen Uhr und der Uhr verschiedener Referenz-Server in Millisekunden an. Die Differenz sollte möglichst klein sein. Damit `ntpq -p` brauchbare Ergebnisse liefert, muss `ntpd` einige Zeit laufen (zumindest mehrere Minuten lang). Beachten Sie, dass `ntpd` die Zeit bei kleinen Abweichungen nicht einfach korrigiert, sondern die Uhr eine Weile etwas schneller oder etwas langsamer laufen lässt, bis die korrekte Zeit erreicht wird. Dadurch werden abrupte Zeitänderungen vermieden.

```
root#  ntpq -p
     remote       refid  st t when poll reach   delay   offset  jitter
==============================================================================
 europium.canoni  ...     2 u    2   64    1   21.565  -117.64   0.002
 www.alter-provi  ...     2 u    1   64    1   20.436  -118.56   0.002
```

Sollte die Zeitabweichung größer als eine Sekunde sein (das entspricht einem Wert größer 1000 in der Offset-Spalte), muss die Uhrzeit manuell mit `ntpdate` eingestellt werden:

```
root#  service ntp stop
root#  ntpdate de.pool.ntp.org
root#  service ntp start
```

Red Hat

Bei RHEL 6 hilft `system-config-date` bei der NTP-Konfiguration. Wenn Sie in diesem Programm NTP aktivieren, wird beim Rechnerstart `ntpd` gestartet. Mit `ntpq -p` überzeugen Sie sich davon, dass alles funktioniert. Sollte die anfängliche Zeitabweichung zu groß sein, müssen Sie `ntpd` vorübergehend stoppen und mit `ntpdate` die lokale Uhrzeit synchronisieren:

```
root#  service ntpd stop
root#  ntpdate de.pool.ntp.org
root#  service ntpd start
```

SUSE

openSUSE verwendet standardmäßig NTP. Die Konfiguration erfolgt im YaST-Modul System • Datum und Zeit; bei einer Konfigurationsänderung wird einmalig `ntpdate` ausgeführt. Um selbst einen NTP-Server einzurichten, starten Sie das YaST-Modul Netzwerkdienste • NTP-Einrichtung und aktivieren die Option Starte NTP-Dienst jetzt und beim Booten. Entscheidend ist, dass Sie der Konfiguration einen oder mehrere NTP-Server hinzufügen. Standardmäßig wird nur die lokale Uhr verwendet, was unzureichend ist. `ntpd` wird nun durch das Init-V-Script `ntp` gestartet.

Chrony

Beginnend mit Version 16 haben die Fedora-Entwickler den klassischen NTP-Dämon durch das neue Programm Chrony ersetzt. Es eignet sich besonders gut für Notebooks und virtuelle Maschinen, die nicht ständig mit dem Internet verbunden

sind und deren Zeit nach längeren Offline-Perioden oft deutlich korrigiert werden muss. Die Konfiguration erfolgt durch `/etc/chrony.conf`. Sollte die automatische Neueinstellung der Uhrzeit nach einer längeren Offline-Periode nicht korrekt funktionieren, führen Sie das folgende Kommando aus:

```
root# service chronyd restart
```

Weitere Informationen zu diesem Programm können Sie hier nachlesen:

http://chrony.tuxfamily.org

21.4 Benutzer und Gruppen, Passwörter

Bei der Benutzerverwaltung geht es in erster Linie darum, wer auf welche Dateien zugreifen darf, wer welche Programme ausführen darf, wer auf welche Hardware-Komponenten (Device-Dateien) zugreifen darf etc. Eine Benutzer- und Zugriffsverwaltung ist immer dann erforderlich, wenn auf einem Rechner mehrere Personen arbeiten dürfen. Es muss Regeln geben, unter welchen Umständen ein Benutzer Daten eines anderen Benutzers lesen oder verändern darf.

Unter Linux wird dazu eine Liste von Benutzern verwaltet. Außerdem ist jeder Benutzer zumindest einer, möglicherweise aber auch mehreren Gruppen zugeordnet. Gruppen dienen dazu, mehreren Benutzern den Zugriff auf gemeinsame Dateien bzw. Programme zu ermöglichen.

Damit die Verwaltung der Zugriffsrechte funktioniert, werden zusammen mit jeder Datei auch ein Besitzer, die Gruppenzugehörigkeit und sogenannte Zugriffsbits gespeichert. Da auch Programme Dateien sind und der Zugriff auf Hardware-Komponenten oft über sogenannte Device-Dateien erfolgt, ist dieser Mechanismus sehr allgemeingültig.

Konfigurationsprogramme

Prinzipiell können Sie als `root` die Benutzerverwaltung weitgehend manuell durchführen, indem Sie die in diesem Abschnitt beschriebenen Dateien direkt ändern. Komfortabler und sicherer ist es, die mit den meisten Distributionen mitgelieferten Werkzeuge zur Benutzer- und Gruppenverwaltung einzusetzen:

Gnome 2.*n*:	`users-admin` (Teil der `gnome-system-tools`)
Gnome 3.*n*:	Systemeinstellungsmodul BENUTZER
KDE:	Systemeinstellungsmodul BENUTZERVERWALTUNG
Debian, Ubuntu:	Gnome- oder KDE-Werkzeuge
Red Hat, Fedora:	`system-config-users` (siehe Abbildung 21.1)
SUSE:	YaST-Modul SICHERHEIT • BENUTZER UND GRUPPEN

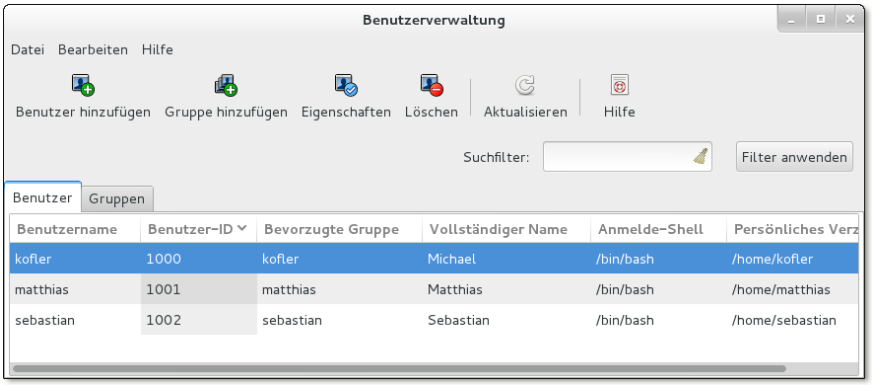


Abbildung 21.1 Benutzerverwaltung unter Fedora

Kommandos

Wenn Sie auf komfortable Benutzeroberflächen verzichten können oder die Benutzerverwaltung in Scripts automatisieren möchten, können Sie auf die in Tabelle 21.3 zusammengefassten Kommandos zurückgreifen. Das folgende Beispiel zeigt, wie Sie den neuen Benutzer `testuser` anlegen und ihm ein Passwort zuweisen:

```
root#  useradd -m testuser
root#  passwd testuser
New passwd: xxx
Re-enter new passwd: xxx
```

Es wird Ihnen sicherlich auffallen, dass es für manche Aufgaben gleich zwei Kommandos gibt, z. B. `adduser` und `useradd`. Bei `adduser`, `addgroup`, `deluser` und `delgroup` handelt es sich um Debian-spezifische Erweiterungen zu den herkömmlichen Kommandos `useradd`, `groupadd` etc. Unter Debian und Ubuntu berücksichtigen diese Kommandos die in `/etc/adduser.conf` und `/etc/deluser.conf` definierten Regeln.

Für Konfusion sorgen Red Hat und Fedora: Dort stehen die Kommandos `adduser`, `addgroup`, `deluser` und `delgroup` ebenfalls zur Verfügung. Allerdings handelt es sich dabei nicht um die von Debian vertrauten Kommandos, sondern um Links auf `useradd`, `groupadd`, `userdel` und `groupdel`. Aus diesem Grund hat `adduser` unter Fedora dieselbe Syntax wie `useradd`, aber eine andere Syntax als `adduser` unter Debian!

Auch SUSE geht eigene Wege: Die Kommandos `adduser/-group` und `deluser/-group` stehen dort nicht zur Verfügung. Für `groupadd/-del/-mod` und `useradd/-del/-mod` verwendet man eine eigene Implementierung, die zwar in den wichtigsten, aber nicht in allen Optionen kompatibel zu den Kommandos der anderen Distributionen ist.

Kommando	Funktion
adduser	richtet einen neuen Benutzer ein (Debian).
addgroup	richtet eine neue Gruppe ein (Debian).
chage	steuert, wie lange ein Passwort gültig bleibt.
chgrp	ändert die Gruppenzugehörigkeit einer Datei.
chmod	ändert die Zugriffsbits einer Datei.
chown	ändert den Besitzer einer Datei.
chsh	verändert die Standard-Shell eines Benutzers.
delgroup	löscht eine Gruppe (Debian).
deluser	löscht einen Benutzer (Debian).
groupadd	richtet eine neue Gruppe ein.
groupdel	löscht eine Gruppe.
groupmod	verändert Gruppeneigenschaften.
groups	zeigt die Gruppen des aktuellen Benutzers an.
id	zeigt die aktuelle Benutzer- und Gruppen-ID-Nummer an.
newgrp	ändert die aktive Gruppe eines Benutzers.
newusers	richtet mehrere neue Benutzer ein.
passwd	verändert das Passwort eines Benutzers.
useradd	richtet einen neuen Benutzer ein.
userdel	löscht einen Benutzer.
usermod	verändert Benutzereigenschaften.

Tabelle 21.3 Kommandos zur Benutzer- und Gruppenverwaltung

Benutzerverwaltung

Unter Linux bzw. generell bei Unix-ähnlichen Systemen gibt es drei Typen von Benutzern:

- **Super-User alias Systemadministrator alias root:** Dieser Benutzer hat üblicherweise den Namen `root`. Wer das `root`-Passwort kennt und sich als `root` anmeldet, hat uneingeschränkte Rechte: Er oder sie darf alle Dateien ansehen, verändern, löschen, alle Programme ausführen etc. Derart viele Rechte sind nur zur Systemadministration erforderlich. Alle anderen Aufgaben sollten aus Sicherheitsgründen nicht als `root` ausgeführt werden!

- **Gewöhnliche Benutzer:** Diese Benutzer verwenden Linux, um damit zu arbeiten. Sie haben uneingeschränkten Zugriff auf ihre eigenen Dateien, aber nur eingeschränkten Zugriff auf den Rest des Systems. Als Login-Name wird zumeist der Vor- oder Nachname des Anwenders verwendet z. B. `kathrin` oder `hofer`.
- **Systembenutzer für Dämonen und Server-Dienste:** Schließlich gibt es eine Reihe von Benutzern, die nicht für die interaktive Arbeit am Computer vorgesehen sind, sondern zur Ausführung bestimmter Programme dienen. Beispielsweise wird der Webserver Apache nicht vom Benutzer `root` ausgeführt, sondern von einem eigenen Benutzer, der je nach Distribution `apache` oder `wwwrun` oder `httpd` oder so ähnlich heißt. Diese Vorgehensweise wird gewählt, um eine möglichst hohe Systemsicherheit zu erzielen.

/etc/passwd

Die Liste aller Benutzer wird in der Datei `/etc/passwd` gespeichert. Dort werden für jeden Benutzer der Login-Name, der vollständige Name, die UID- und GID-Nummer, das Heimatverzeichnis und die Shell gespeichert. Dabei gilt folgendes Format:

Login:Passwort:UID:GID:Name:Heimatverzeichnis:Shell

Die folgenden Zeilen zeigen einige Benutzerdefinitionen in `/etc/passwd` unter Ubuntu Linux:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
...
kofler:x:1000:1000:Michael Kofler,,,:/home/kofler:/bin/bash
huber:x:1001:1001:Herbert Huber,,,:/home/huber:/bin/bash
```

Der Name `passwd` lässt vermuten, dass in der Datei auch die Passwörter gespeichert werden. Das war früher tatsächlich der Fall. Heute enthält `/etc/passwd` anstelle der Passwortinformationen nur das Zeichen x. Der verschlüsselte Passwort-Hash wird in der separaten Datei `/etc/shadow` gespeichert (siehe Abschnitt 21.4).

Login-Name

Der Login-Name sollte nur aus Kleinbuchstaben (US-ASCII-Buchstaben und Zahlen) bestehen und nicht länger als acht Zeichen sein. Zwar sind sowohl Nicht-ASCII-Zeichen als auch mehr als acht Zeichen prinzipiell zulässig, es kann aber passieren, dass Probleme in der Kombination mit manchen Programmen auftreten. Für den getrennt gespeicherten vollständigen Namen gelten diese Einschränkungen nicht.

UID und GID

Die UID-Nummer (User Identification) dient zur internen Identifizierung des Benutzers. Die Nummer wird insbesondere als Zusatzinformation zu jeder Datei gespeichert, sodass klar ist, wem die Datei gehört.

Für die Vergabe von UID-Nummern gibt es Regeln: `root` hat immer UID=0. Für Server-Dienste und Dämonen sind bei den meisten Distributionen UID-Nummern

zwischen 1 und 999 vorgesehen. Für gewöhnliche Benutzer sind dementsprechend Nummern ab 1000 vorgesehen. RHEL 6 sowie einige andere Distributionen verwenden noch ältere Regeln: Für Server-Dienste ist der Wertebereich zwischen 1 und 499 vorgesehen, für Benutzer alle IDs ab 500.

Die GID-Nummer (Group Identification) gibt an, zu welcher Gruppe der Anwender gehört. Mehr Details zu Gruppen folgen im nächsten Abschnitt.

Heimatverzeichnis

Das Heimatverzeichnis ist der Ort, an dem der Benutzer seine privaten Daten speichern kann. Bei gewöhnlichen Benutzern wird dazu üblicherweise der Pfad `/home/`*`login-name`* verwendet. Im Heimatverzeichnis werden auch die persönlichen Konfigurationseinstellungen des Benutzers für diverse Programme gespeichert. Beispielsweise enthält die Datei `.emacs` die Konfigurationseinstellungen für den Editor Emacs. Da die Namen derartiger Konfigurationsdateien meistens mit einem Punkt beginnen, sind sie unsichtbar. Sie können mit dem Kommando `ls -la` angezeigt werden.

Damit bei neuen Benutzern sofort sinnvolle Standardeinstellungen für die wichtigsten Programme vorliegen, sollten beim Anlegen eines neuen Benutzers alle Dateien aus `/etc/skel` in das neu erzeugte Heimatverzeichnis kopiert werden. Viele Programme zum Anlegen neuer Benutzer erledigen diesen Schritt automatisch. Der Inhalt von `/etc/skel` stellt damit die Ausgangseinstellung für jeden neuen Benutzer dar.

Shell

Die Shell ist ein Interpreter, mit dem der Benutzer nach dem Login Kommandos ausführen kann. Da unter Linux mehrere Shells zur Auswahl stehen, muss in der `passwd`-Datei angegeben werden, welche Shell zum Einsatz kommen soll. Unter Linux ist dies meistens die Shell `bash`, die in Kapitel 14 ausführlich beschrieben wird. In der `passwd`-Datei muss der vollständige Dateiname der Shell gespeichert werden, also beispielsweise `/bin/bash`.

Gruppenverwaltung

Der Sinn von Gruppen besteht darin, mehreren Benutzern den gemeinsamen Zugriff auf Dateien zu ermöglichen. Dazu wird jeder Benutzer einer primären Gruppe (Initial Group) zugeordnet. Außerdem kann ein Benutzer beliebig vielen weiteren Gruppen (Supplementary Groups) zugeordnet werden, also Mitglied mehrerer Gruppen sein.

Die Datei `/etc/group` enthält die Liste aller Gruppen. Die folgenden Zeilen zeigen einige Gruppendefinitionen in `/etc/group`. Es gilt folgendes Format:

Gruppenname:Passwort:GID:Benutzerliste

Die folgenden Zeilen stammen aus der `group`-Datei eines Ubuntu-Systems:

```
root:x:0:
daemon:x:1:
bin:x:2:
...
dialout:x:20:cupsys,kofler,huber
...
users:x:100:
admin:x:114:kofler
...
kofler:x:1000:
huber:x:1001:
...
```

Die Zuordnung zwischen Benutzer und Gruppe erfolgt auf zwei Weisen:

- Die primäre Gruppe eines Benutzers wird in `/etc/passwd` gespeichert. Beim Benutzer `kofler` lautet die primäre Gruppe ebenfalls `kofler`; das geht aus dem Wert 1000 in der GID-Spalte in der `/etc/passwd`-Datei hervor.
- Die Zugehörigkeit zu weiteren Gruppen wird gespeichert, indem der Name des Benutzers in der letzten Spalte der Datei `/etc/group` angegeben wird. So gehört `kofler` auch zu den Gruppen `adm`, `admin` und `dialout`. Das erlaubt dem Benutzer `kofler`, auf Ubuntu-Systemen Administrationsarbeiten durchzuführen und eine Internet-Verbindung herzustellen.

Bei den GID-Nummern ist 0 für `root` vorgesehen, 1 bis 99 für Systemdienste. GID=100 ist normalerweise für die Gruppe `users` reserviert. GIDs größer 100 dürfen für eigene Zwecke definiert werden.

Primäre Gruppe

Für die Zuordnung zwischen Benutzern und ihren primären Gruppen gibt es zwei gängige Strategien:

- Beim herkömmlichen Verfahren, das seit vielen Jahren unter Unix/Linux zum Einsatz kommt, sind alle gewöhnlichen Benutzer der primären Gruppe `users` zugeordnet. SUSE ist bis heute ein Anhänger dieser sehr einfachen Strategie.
- Debian-basierte Distributionen sowie Red Hat und Fedora setzen auf ein anderes Verfahren: Jeder Benutzer bekommt seine eigene primäre Gruppe. In diesem Fall gibt es für die Benutzer `kofler` und `huber` jeweils eine gleichnamige Gruppe. Die Gruppe `users` spielt keine Rolle mehr.

  Das Verfahren hat unter bestimmten Umständen Vorteile – etwa dann, wenn mehrere Mitglieder einer sekundären Gruppe gemeinsame Dateien erzeugen. Diese Vorteile kommen aber nur bei einer entsprechenden Systemadministration zum Tragen.

Passwörter

Linux-Passwörter bestehen üblicherweise nur aus ASCII-Zeichen. Internationale Sonderzeichen sind zwar grundsätzlich erlaubt, können aber leicht zu Problemen führen. Aus Sicherheitsgründen sollten Passwörter sowohl Groß- als auch Kleinbuchstaben sowie mindestens eine Ziffer enthalten.

Passwörter werden unter Linux in Form sogenannter Hash-Codes gespeichert, die eine Kontrolle, aber keine Rekonstruktion von Passwörtern ermöglichen. Die Passwörter dürfen beliebig lang sein. Aktuelle Distributionen verwenden den als sicher geltenden Hash-Algorithmus SHA512 in Kombination mit einem zufälligen Initialisierungscode für das Passwort, dem sogenannten Salz. Das »Salz« bewirkt, dass für ein- und dasselbe Passwort jedes Mal ein anderer Hash-Code gespeichert wird. Damit ist in `/etc/shadow` nicht erkennbar, ob mehrere Benutzer dasselbe Passwort haben. Der Hash-Algorithmus wird durch die Variable `ENCRYPT_METHOD` in `/etc/login.defs` festgelegt.

Um potenziellen Angreifern das Leben zu erschweren, werden die verschlüsselten Passwort-Codes nicht direkt in `/etc/passwd` gespeichert, sondern in der getrennten Datei `/etc/shadow`. Der Vorteil besteht darin, dass diese Datei nur von `root` gelesen werden kann. `/etc/passwd` und `/etc/group` sind hingegen für alle Benutzer des Systems lesbar, weil sie elementare Verwaltungsinformationen enthalten. Bei `/etc/shadow` reicht es dagegen aus, wenn nur die Programme zur Passwort-Verifizierung und -Änderung darauf zugreifen dürfen. Ein potenzieller Angreifer muss daher zuerst `root`-Zugang erhalten, bevor er nur die verschlüsselten Passwort-Codes lesen kann.

Für die `shadow`-Datei gilt das folgende Format:

Login:Passwort-Code:d1:d2:d3:d4:d5:d6:reserved

Die folgenden Zeilen zeigen einen Ausschnitt aus einer `shadow`-Datei:

```
root:$6$Ecrkix...:14391:0:99999:7:::
daemon:*:14391:0:99999:7:::
bin:*:14391:0:99999:7:::
...
kofler:$6$TZR7...:14391:0:99999:7:::
```

Bei den meisten Systembenutzern wird statt eines Passworts nur ein Stern oder ein Ausrufezeichen gespeichert. Das bedeutet, dass es kein gültiges Passwort gibt, ein Login also unmöglich ist. Die System-Accounts können dennoch verwendet werden: Programme, die zuerst mit `root`-Rechten gestartet werden, können später gleichsam ihren Besitzer wechseln und dann als `bin`, `daemon`, `lp` etc. fortgesetzt werden. Genau das ist bei den meisten Systemprozessen der Fall: Sie werden während des System-

starts von `root` automatisch gestartet und wechseln dann aus Sicherheitsgründen sofort den Besitzer.

Die Felder `d1` bis `d6` können optionale Zeitangaben enthalten: **d1 bis d6**

- `d1` gibt an, wann das Passwort zum letzten Mal geändert wurde. (Die Angabe erfolgt in Tagen, die seit dem 1.1.1970 vergangen sind.)
- `d2` gibt an, in wie vielen Tagen das Passwort geändert werden darf.
- `d3` gibt an, in wie vielen Tagen das Passwort spätestens geändert werden muss, bevor es ungültig wird. (Details zu den Feldern erhalten Sie mit `man 5 shadow`.)
- `d4` gibt an, wie viele Tage vor dem Ablaufen des Passworts der Benutzer gewarnt wird.
- `d5` gibt an, nach wie vielen Tagen ein abgelaufener Account ohne gültiges Passwort vollständig deaktiviert wird.
- `d6` gibt an, seit wann ein Account deaktiviert ist.

Normalerweise werden für *d1* bis *d3* Standardwerte verwendet, sodass das Passwort jederzeit geändert werden kann und unbeschränkt gültig bleibt. *d1* bis *d6* können aber auch dazu verwendet werden, die Gültigkeit von Passwörtern zu beschränken, Login-Accounts zeitlich automatisch zu deaktivieren etc., etwa zur Verwaltung von Studenten-Accounts an einer Universität oder Schule.

Die Einstellung der Daten `d1` bis `d6` erfolgt durch das Kommando `chage`. Im folgenden Beispiel wird der Benutzer gezwungen, sein Passwort sofort nach dem ersten Login zu ändern. Außerdem muss er in Zukunft sein Passwort alle 100 Tage ändern. Schließlich steht das Konto nur bis zum 31.12.2015 zur Verfügung. Danach wird jeder Login blockiert: **chage**

```
root#  chage -d 0 -M 100 -E 2015-12-31 loginname
```

Eine Menge Parameter zur internen Administration von Passwörtern und Logins befinden sich in der Datei `/etc/login.defs`. Die Einstellungen gelten für `useradd`, `groupmod` etc. In `logins.def` ist beispielsweise festgeschrieben, wie viele Tage Passwörter standardmäßig gelten, welcher Wertebereich für neue UIDs und GIDs verwendet wird etc. **/etc/login.defs**

Die PAM-Konfiguration (siehe Abschnitt 21.4) definiert darüber hinaus Regeln für die Passwortüberprüfung. Die PAM-Regeln werden unter anderem vom Kommando `passwd` sowie bei jedem Login berücksichtigt.

Um Ihr eigenes Passwort zu verändern, führen Sie das Kommando `passwd` aus. Sie werden jetzt zuerst nach Ihrem alten Passwort gefragt und dann zweimal hintereinander aufgefordert, ein neues Passwort einzutippen. Nur wenn beide Eingaben **Passwörter ändern**

übereinstimmen, wird das neue Passwort akzeptiert. Ab jetzt müssen Sie bei jedem Einloggen das neue Passwort verwenden.

Während normale Benutzer nur ihr eigenes Passwort ändern können, darf `root` auch die Passwörter fremder Anwender verändern:

```
root#  passwd hofer
New password:  ******
Re-enter new password:  ******
Password changed.
```

Passwortqualität

Welche Passwortregeln zulässig sind, entscheidet bei den meisten Linux-Distributionen die Bibliothek `pam_cracklib`. Normalerweise muss das Passwort zumindest acht oder neun Zeichen lang sein, muss sich von Wörtern unterscheiden, die in einem Wörterbuch vorkommen, und darf keine zu großen Ähnlichkeiten mit dem bisherigen Passwort haben. Je nach Distribution können auch andere Regeln gelten. Wie diese eingestellt werden, ist hier ausführlich dokumentiert:

http://www.deer-run.com/~hal/sysadmin/pam_cracklib.html

Bei aktuellen Fedora-Versionen stellt `pam_pwquality` die Passwortqualität sicher. Die Konfiguration erfolgt durch `/etc/security/pwquality.conf`.

Die Passwortregeln gelten nur für gewöhnliche Benutzer. `root` darf beliebig schlechte Passwörter einstellen, obwohl dies natürlich nicht empfehlenswert ist.

Sichere Passwörter generieren

Wenn Sie häufig Benutzerkonten einrichten, ist es oft am einfachsten, automatisch generierte Passwörter zu verwenden. Dabei helfen die Programme `mkpasswd` aus dem Fedora- bzw. RHEL-Paket `expect` bzw. `makepasswd` aus dem gleichnamigen Debian- bzw. Ubuntu-Paket.

```
root# makepasswd
aGjoQK1Ezo
```

root-Passwort vergessen

Was tun Sie, wenn Sie Ihr `root`-Passwort vergessen haben? Am einfachsten macht es Ihnen RHEL 6: Sie müssen das System lediglich durch die Angabe des zusätzlichen GRUB-Parameters `single` im Single-User-Modus booten. Damit gelangen Sie in eine `root`-Shell, in der Sie ohne Weiteres ein neues Passwort einstellen können.

Bei den meisten anderen Distributionen benötigen Sie hingegen eine Live- oder Rescue-CD bzw. einen entsprechenden USB-Stick. Damit starten Sie den Rechner und binden dann die Systempartition Ihres Linux-Systems in ein beliebiges Verzeichnis ein. Mit `chroot` machen Sie das Verzeichnis zum neuen Root-Verzeichnis. Nun können Sie mit `passwd` das `root`-Passwort neu einstellen:

```
root#  mkdir /rescue
root#  mount -t ext4 /dev/xxx /rescue
root#  chroot /rescue
root#  passwd
root#  <Strg>+<D>
root#  reboot
```

Wenn Sie andere Benutzer daran hindern möchten, auf die gerade beschriebene Weise das `root`-Passwort zu verändern, müssen Sie im BIOS/EFI Ihres Rechners alle Bootmedien außer der ersten Festplatte deaktivieren und das BIOS/EFI selbst durch ein Passwort absichern. Dieses Passwort sollten Sie dann aber wirklich nicht vergessen! Eine andere Möglichkeit besteht darin, die ganze Systempartition zu verschlüsseln.

faillog

Je nach der Einstellung von `/etc/login.defs` werden alle fehlerhaften Login-Versuche in `/var/log/faillog` protokolliert. Im Gegensatz zu vielen anderen Logging-Dateien kommt dabei ein binäres Format zum Einsatz.

Mit `faillog -u name` stellen Sie fest, wie viele fehlerhafte Login-Versuche bei einem bestimmten Benutzer seit der letzten gültigen Anmeldung aufgetreten sind.

Mit `faillog -u name -m max` kann eine Maximalanzahl fehlerhafter Login-Versuche für einen bestimmten Benutzer fixiert werden. Wird diese Zahl überschritten, wird der Login blockiert, bis `root` den Login durch das Kommando `faillog -u name -r` wieder erlaubt. (Damit wird der Login-Zähler zurückgesetzt.)

Sie können die maximale Login-Anzahl durch `faillog -m max` auch generell festlegen. Allerdings sollten Sie dann immer auch `faillog -u root -m 0` ausführen, damit `root` von dieser Schutzmaßnahme ausgeschlossen ist. Andernfalls könnte es passieren, dass Sie sich selbst als `root` nicht mehr einloggen können, nachdem ein anderer Benutzer mehrere vergebliche `root`-Login-Versuche durchgeführt hat.

Gruppenpasswörter

Wie bei Benutzern können auch bei Gruppen Passwörter definiert werden (Kommando `gpasswd`). Aber während bei Benutzern Passwörter unbedingt zu empfehlen sind, sind Gruppenpasswörter unüblich. Ihr Hauptnachteil besteht darin, dass alle Gruppenmitglieder das Passwort kennen müssen, was die Administration erschwert.

Falls tatsächlich Gruppenpasswörter zum Einsatz kommen sollen, werden diese in der Datei `/etc/gshadow` gespeichert. Ein Gruppenpasswort muss dann eingegeben werden, wenn ein Benutzer mit dem Kommando `newgrp` seine gerade aktive Gruppe wechselt.

Zusammenspiel der Konfigurationsdateien

Die folgenden Zeilen fassen nochmals zusammen, wie die drei Dateien `passwd`, `group` und `shadow` zusammenspielen. Für jeden Anwender enthält `passwd` eine Zeile nach folgendem Muster:

```
# eine Zeile in /etc/passwd
kofler:x:1000:1000:Michael Kofler:/home/kofler:/bin/bash
```

Dabei ist `kofler` der Login-Name. 1000 ist gleichermaßen UID und GID, `Michael Kofler` der vollständige Name, `/home/kofler` sein Benutzerverzeichnis und `/bin/bash` seine Shell. Die UID muss eine eindeutige Nummer sein, die für die Verwaltung der Zugriffsrechte von Dateien wichtig ist.

Die dazugehörende Zeile in `/etc/shadow` mit den Passwortinformationen sieht so aus:

```
# eine Zeile in /etc/shadow
kofler:$6$9dkO$...:13479:0:99999:7:::
```

Die Zeichenkette nach `kofler:` ist das verschlüsselte Passwort. Wenn auf die Zeichenkette verzichtet wird, kann der Login ohne Passwort verwendet werden. Wenn statt der Zeichenkette ein `*` oder `!` eingetragen ist, ist der Login gesperrt.

Die GID-Nummer in `/etc/passwd` muss mit einer Gruppe aus `/etc/group` übereinstimmen. Bei vielen Distributionen ist jedem gewöhnlichen Benutzer eine gleichnamige Gruppe zugeordnet:

```
# eine Zeile aus /etc/group
kofler:x:1000:
```

Benutzerverwaltung im Netzwerk

Wenn Sie mehrere Linux-Rechner miteinander vernetzen und mit NFS einen gegenseitigen Zugriff auf Dateien ermöglichen möchten, dann müssen Sie darauf achten, dass die UID- und GID-Nummern auf allen Rechnern einheitlich sind. Das allein wird bei mehreren Rechnern schon recht aufwendig. Wenn Sie nun auch noch möchten, dass sich jeder Benutzer auf jedem Rechner einloggen kann, und zwar natürlich immer unter dem gleichen Login-Namen und mit dem gleichen Passwort, dann müssen Sie alle `/etc/passwd`-Dateien ständig synchronisieren. Der Administrationsaufwand ist dann riesig.

Um diesen Aufwand zu vermeiden, wird in solchen Fällen meist ein zentraler Server zur Benutzerverwaltung eingesetzt. Zur Authentifizierung der Clients stehen eine ganze Menge alternativer Verfahren bzw. Protokolle zur Auswahl, deren Beschreibung in diesem Buch aber aus Platzgründen leider nicht möglich ist:

- LDAP (Lightweight Directory Access Protocol)
- NIS (Network Information Service, gilt als veraltet)
- Kerberos
- Samba bzw. die Windows-Benutzerverwaltung

PAM

Die Pluggable Authentication Modules (PAM) sind eine Bibliothek, deren Funktionen bei Authentifizierungsaufgaben helfen. Wenn Sie auf einem Linux-Rechner einen Login durchführen oder sich auf andere Weise authentifizieren bzw. Ihr Passwort verändern, greifen die jeweiligen Programme auf die PAM-Bibliothek zurück. Auch Cron und PolicyKit nutzen PAM. Mit `ldd` können Sie feststellen, ob ein bestimmtes Kommando auf PAM-Bibliotheken zurückgreift:

```
root#  ldd /usr/bin/passwd | grep libpam
  libpam.so.0 => /lib/x86_64-linux-gnu/libpam.so.0
  libpam_misc.so.0 => /lib/x86_64-linux-gnu/libpam_misc.so.0
```

Eine umfassende Dokumentation zu PAM finden Sie hier:

http://www.kernel.org/pub/linux/libs/pam

PAM ist standardmäßig so konfiguriert, dass es die lokalen Passwortdateien auswertet, also z. B. `/etc/shadow`. Wenn ergänzend auch ein anderes Authentifizierungsverfahren genutzt werden soll (z. B. LDAP), muss die PAM-Konfiguration entsprechend verändert werden. Dabei helfen je nach Distribution unterschiedliche Werkzeuge:

Fedora, Red Hat:	`system-config-authentication`, `authconfig`
SUSE:	YaST-Modul Sicherheit • Benutzer- und Gruppenverwaltung
Ubuntu:	`pam-auth-update`

pam.conf

Die Konfigurationsdateien befinden sich im Verzeichnis `/etc/pam.d/`. Darüber hinaus wird auch die Datei `/etc/pam.conf` ausgewertet. Die Konfigurationsdateien enthalten zeilenweise Regeln. Jede Regel besteht aus mindestens drei Teilen bzw. Spalten:

```
Typ Reaktion PAM-Modul [Modulargumente]
```

Einträgen in `pam.conf` muss zudem der Name des Service vorangestellt werden, z. B. `login` bzw. `other` für Standardeinträge. Bei den Dateien in `/etc/pam.d` ergibt sich der Service-Name aus dem Dateinamen.

Regeltyp (erste Spalte)

PAM unterscheidet zwischen vier Regeltypen. Bei Debian, SUSE und Ubuntu enthalten die Dateien `common-account`, `common-auth`, `common-password` und `common-session` Standardregeln für diese vier Typen:

- `account`: ermöglicht die Limitierung von Diensten je nach Tageszeit, Auslastung, Login-Ort (z. B. Konsole) etc.
- `auth`: betrifft die Autorisierung, also die Passwortabfrage und -überprüfung, sowie die anschließende Zuweisung von Privilegien, z. B. Gruppenzugehörigkeiten.
- `password`: betrifft den Mechanismus zur Änderung des Passworts.
- `session`: ermöglicht es, Aktionen vor oder nach dem eigentlichen Dienst auszuführen: Logging, Dateisysteme einbinden/lösen, Status der Mailbox anzeigen etc.

Reaktion (zweite Spalte)

Die zweite Spalte in den Konfigurationsdateien gibt an, wie PAM reagieren soll, wenn eine Regel erfüllt bzw. nicht erfüllt ist. Es gibt zwei Möglichkeiten, die Reaktion zu beschreiben: entweder durch ein einfaches Schlüsselwort (z. B. `required`, `requisite`) oder durch ein in eckige Klammern gesetztes Wert/Ergebnis-Paar (z. B. `[success=1 new_authtok_reqd=done default=ignore]`). Die Bedeutung der vier wichtigsten Schlüsselwörter der einfachen Syntaxvariante ist in Tabelle 21.4 erklärt.

Schlüsselwort	Reaktion
`requisite`	Bei einem Regelverstoß liefert die PAM-Funktion sofort ein negatives Ergebnis, und die weiteren Regeln werden nicht mehr abgearbeitet.
`required`	Bei einem Regelverstoß liefert die PAM-Funktion ein negatives Ergebnis; weitere Regeln werden abgearbeitet, ihr Ergebnis wird aber nicht berücksichtigt.
`sufficient`	Bei Einhaltung der Regel liefert PAM sofort ein positives Ergebnis (es sei denn, es liegt bereits ein Verstoß gegen eine vorangegangene `requisite`-Regel vor); weitere Regeln werden nicht mehr berücksichtigt. Bei einem Regelverstoß setzt PAM mit der nächsten Regel fort.
`optional`	Das Ergebnis der Regel ist nur dann relevant, wenn es sich um die einzige Regel für einen bestimmten Regeltyp und einen bestimmten Service (z. B. `su`) handelt.

Tabelle 21.4 Reaktion auf PAM-Regelverstöße

Bei der zweiten Syntaxvariante geben Sie mehrere Wert/Ergebnis-Paare in der Form `[value1=result1 value2=result2 ...]` an. Für `value` gibt es eine ganze Reihe vordefinierter Schlüsselwörter, die das Ergebnis einer Regel ausdrücken. `result` kann entweder eine Zahl sein, die angibt, wie viele weitere Regeln nun übersprungen werden sollen, oder ein Schlüsselwort, das das gewünschte PAM-Ergebnis angibt (`ignore`, `bad`, `die`, `ok`, `done` oder `reset`). Das folgende Listing gibt an, wie die Schlüsselwörter der ersten Syntaxvariante in der zweiten Schreibweise ausgedrückt werden:

```
requisite  = [success=ok new_authtok_reqd=ok ignore=ignore default=die]
required   = [success=ok new_authtok_reqd=ok ignore=ignore default=bad]
sufficient = [success=done new_authtok_reqd=done default=ignore]
optional   = [success=ok new_authtok_reqd=ok default=ignore]
```

Modul und Optionen (dritte Spalte)

Die dritte Spalte gibt den Namen des PAM-Moduls an, das die Regel auswertet. Das Verhalten des Moduls kann durch Optionen beeinflusst werden. Leider gibt es keine zentrale Dokumentation der zulässigen Optionen und ihrer Bedeutung.

Standardkonfiguration

Das folgende Listing fasst die Einstellungen von Fedora zusammen. Beachten Sie, dass die Standardeinstellungen je nach Distribution stark variieren und oft über mehrere Dateien verteilt sind, z. B. auf `common-xxx` bei Debian, SUSE und Ubuntu.

```
# Datei /etc/pam.d/password-auth (Fedora)
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass \
                          use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond \
                          quiet use_uid
session     required      pam_unix.so
```

PAM-Konfiguration bei Fedora und RHEL

Unter Fedora und RHEL sollten Sie es möglichst vermeiden, Dateien in `/etc/pam.d` direkt zu verändern. Besser ist es, die Konfiguration in `/etc/sysconfig/authconfig` durchzuführen. Das Kommando `authconfig` wertet diese Datei aus und überschreibt dann die betreffenden Dateien in `/etc/pam.d`. Leider bietet `authconfig` nur wenige Einstellmöglichkeiten und ist nicht besonders gut dokumentiert.

Name Service Switch (NSS)

Bei einem Login, bei der Verwaltung der Zugriffsrechte auf Dateien, bei Netzwerkzugriffen etc. sind alle möglichen Informationen über Benutzer- und Gruppennamen, UIDs und GIDs, Hostnamen, Ports von Netzwerkdiensten etc. erforderlich. Diese Daten befinden sich standardmäßig in den Dateien `/etc/passwd`, `/etc/group`, `/etc/hosts`, `/etc/services` etc.

In der Unix- bzw. Linux-Nomenklatur wird der Zugriff auf diese Daten unter dem Begriff *Name Services* zusammengefasst. Zuständig für diese Aufgabe ist der Name Service Switch (NSS), eine Sammlung von Funktionen der `libc`-Bibliothek. Ähnlich wie bei der Authentifizierung lässt sich die Datenquelle für NSS einstellen, beispielsweise wenn ein LDAP-Server die Daten zur Verfügung stellt. Die entscheidende Konfigurationsdatei ist `/etc/nsswitch.conf`. Die folgenden Zeilen zeigen die Standardkonfiguration unter Ubuntu:

```
# Datei /etc/nsswitch.conf (Ubuntu)
passwd:         compat
group:          compat
shadow:         compat
hosts:          files mdns4_minimal [NOTFOUND=return] dns mdns4
networks:       files
protocols:      db files
...
```

Die erste Spalte in `nsswitch.conf` bezeichnet die Datenbank bzw. Datei. Nach dem Doppelpunkt beschreiben Schlüsselwörter die Zugriffsmethode auf die Daten sowie optional in eckigen Klammern die Reaktion auf Nachschlageergebnisse. Die folgende Liste erklärt die wichtigsten Schlüsselwörter für die Zugriffsmethoden. Wenn eine Zeile mehrere Zugriffsmethoden nennt, werden diese der Reihe nach angewendet, bis eine Methode erfolgreich ist. Weitere Syntaxdetails verrät `man nsswitch.conf`.

- `files`: greift auf die traditionellen Konfigurationsdateien zurück (`/etc/passwd` und `/etc/group`).
- `compat`: wie `files`, wobei den Benutzer- und Gruppenangaben die Zeichen `+` und `-` vorangestellt werden können. Das erhöht die Kompatibilität zu NIS. `compat` kann nicht mit anderen Schlüsselwörtern kombiniert werden.
- `db`: liest die Daten aus einer BDB-Datenbankdatei (BDB = *Berkeley Database*).
- `dns`: kontaktiert einen Name-Server.
- `mdns`: verwendet Multicast DNS (alias Zeroconf bzw. Apple Bonjour/Rendezvous).

Die Zugriffsmethoden setzen voraus, dass die entsprechende Bibliothek installiert ist, beispielsweise `libnss_db` für `db`. Fehlt die Bibliothek, wird das entsprechende Schlüsselwort einfach ignoriert, ohne dass ein Fehler gemeldet wird.

nscd (Name Service Caching Daemon)

Bei einigen Distributionen (z. B. Fedora, Red Hat und SUSE) wird standardmäßig das Programm `nscd` installiert und während des Hochfahrens des Rechners aktiviert. Bei Debian und Ubuntu ist eine optionale Installation möglich.

`nscd` steht für *Name Service Caching Daemon*. Das Programm merkt sich bei entsprechender Konfiguration Login-, Gruppen- und Hostnamen sowie deren IP-Nummern. Im Unterschied zu einem Nameserver stellt `nscd` diese Informationen aber nur dem lokalen Rechner zur Verfügung, nicht anderen Rechnern im Netzwerk. Sinnvoll ist der Einsatz von `nscd` vor allem dann, wenn die Benutzerverwaltung durch einen Netzwerkdienst erfolgt (z. B. LDAP). `nscd` dient dann als Cache für Informationen und vermeidet unnötige LDAP-Anfragen, die oft nur vergleichsweise langsam beantwortet werden.

/etc/nscd.conf

Die Konfiguration von `nscd` erfolgt durch `/etc/nscd.conf`. Üblicherweise enthält die Datei Einträge in drei Gruppen: `passwd` für Login-Namen, `group` für Gruppen und `host` für Hostnamen. Die Einstellungen jeder Gruppe legen fest, wie lange die Daten gespeichert werden, wie viele Einträge maximal verwaltet werden sollen etc.

21.5 Spracheinstellung, Internationalisierung, Unicode

In diesem Abschnitt geht es um zwei Dinge:

- **Lokalisierung bzw. Spracheinstellung:** Diese Einstellung bestimmt, in welcher Sprache Fehlermeldungen, Menüs, Dialoge, Hilfetexte etc. angezeigt werden. Auch die Formatierung von Datum, Uhrzeit, Währungsbeträgen etc. ändert sich dadurch entsprechend.
- **Zeichensatz:** Der Zeichensatz bestimmt, welche Codes zur Speicherung von Buchstaben verwendet werden. Hier herrscht generelle Einigkeit nur für 7-Bit-ASCII. Beinahe jeder Zeichensatz verwendet den Code 65 für den Buchstaben A. Abweichungen gibt es hingegen bei internationalen Zeichen: Daher gelten für den Buchstaben Ä je nach Zeichensatz unterschiedliche Codes. Es gibt sogar Zeichensätze, in denen Ä überhaupt nicht vorkommt, um so Platz für andere Zeichen, z. B. kyrillische oder hebräische Buchstaben, zu schaffen.

Was bedeutet i10n und i18n?

Im Zusammenhang mit der Lokalisierung von Programmen werden Sie immer wieder auf die merkwürdigen Kürzel `i18n` und `l10n` stoßen: Dabei handelt es sich um die Kurzschreibweise für »Internationalization« (*i* plus 18 Buchstaben plus *n*) bzw. »Localization«. Diese Kürzel eignen sich auch gut als Suchbegriff, falls Sie im Internet nach weiteren Informationen suchen möchten.

Zeichensatz-Grundlagen

Ein Zeichensatz (*character set*) beschreibt die Zuordnung zwischen Zahlencodes und Buchstaben. Bekannte Zeichensätze sind ASCII (7 Bit), ISO-Latin-*n* (8 Bit) und Unicode (16 Bit).

- **ASCII:** Der ASCII-Zeichensatz beschreibt lediglich 127 Zeichen, darunter die Buchstaben a–z bzw. A–Z, die Ziffern 0–9 sowie diverse Interpunktionszeichen.
- **ISO-8859, Latin-Zeichensätze:** Die ISO-Zeichensätze enthalten neben den 127 ASCII-Zeichen bis zu 128 zusätzliche Sonderzeichen für verschiedene Sprachregionen. Beispielsweise enthält ISO-8859-1 = Latin-1 alle in Westeuropa üblichen Zeichen, ISO-8859-2 = Latin-2 die in Zentral- und Osteuropa wichtigsten Zeichen etc. Der Zeichensatz ISO-8859-15 = Latin-9 entspricht Latin-1, enthält aber zusätzlich das Euro-Zeichen. Unter Windows werden Zeichensätze *Code Pages* genannt. Code Page 1252 stimmt weitgehend mit Latin-1 überein.
- **Unicode:** Um das Durcheinander verschiedenster 8-Bit-Zeichensätze zu lösen, wurde der 16-Bit-Zeichensatz Unicode (ISO-10646) entworfen. Damit können nicht nur alle europäischen Sonderzeichen codiert werden, sondern auch die meisten asiatischen Zeichen. Da für jedes Zeichen 16 Bit vorgesehen sind, bietet dieser Zeichensatz Platz für über 65.000 Zeichen.

  Unicode regelt nur, welcher Code welchem Zeichen zugeordnet ist, nicht aber, wie die Codes gespeichert werden. Die einfachste Lösung ist es, jedes Zeichen einfach durch 2 Byte, also 16 Bit, darzustellen. Diese Formatierung wird UTF-16 genannt (Unicode Transfer Format). Sie hat allerdings zwei Nachteile: Erstens verdoppelt sich der Speicherbedarf, und zwar auch in solchen Fällen, in denen überwiegend europäische Zeichen oder sogar nur US-ASCII-Zeichen gespeichert werden sollen. Zweitens tritt der Bytecode 0 an beliebigen Stellen in Unicode-Zeichenketten auf. Viele C-Programme, E-Mail-Server etc. setzen aber voraus, dass das Byte 0 das Ende einer Zeichenkette markiert.

  Deswegen gibt es auch andere Möglichkeiten, Unicode-Texte zu repräsentieren. Die bei Weitem populärste Alternative zu UTF-16 ist UTF-8. Dabei werden die US-ASCII-Zeichen (7 Bit) wie bisher durch ein Byte dargestellt, deren oberstes Bit 0 ist. Alle anderen Unicode-Zeichen werden durch zwei bis vier Byte lange Byte-Ketten dargestellt. Der offensichtliche Nachteil dieses Formats besteht darin, dass es keinen unmittelbaren Zusammenhang zwischen der Byteanzahl und der Anzahl der Zeichen eines Dokuments gibt. Wegen der größeren Kompatibilität zu existierenden Programmen und einer Reihe anderer Vorteile hat sich UTF-8 unter Unix/Linux dennoch als Standard etabliert, während unter Microsoft-Windows häufig UTF-16 verwendet wird. Wenn im Zusammenhang mit Linux also von Unicode die Rede ist, ist in den meisten Fällen Unicode im UTF-8-Format gemeint. Fast alle Distributionen verwenden standardmäßig UTF-8.

Auswirkungen des Zeichensatzes

Der aktive Zeichensatz entscheidet darüber, wie Zeichen in Textdateien bzw. in Dateinamen codiert werden. Die Dateisysteme von Linux kommen mit jedem Zeichensatz zurecht. Als Dateiname gilt jede Zeichenkette, die mit dem Bytecode 0 endet. Je nachdem, welcher Zeichensatz gerade gültig ist, kann die Bytefolge und -anzahl für einen Dateinamen wie `äöü.txt` aber ganz unterschiedlich sein! Wenn der aktuelle Zeichensatz Latin-1 lautet, kann dieser Name durch 7 Byte (plus ein 0-Byte) ausgedrückt werden. Wenn als Zeichensatz dagegen Unicode/UTF-8 verwendet wird, ist der Dateiname 10 Byte lang, weil zur Darstellung von ä, ö und ü jeweils zwei Byte benötigt werden.

Es gibt eine Reihe von Programmen, die unabhängig vom Zeichensatz funktionieren bzw. mit mehreren Zeichensätzen gleichzeitig zurechtkommen: Beispielsweise können E-Mail-Programme und Webbrowser auch E-Mails bzw. Webseiten darstellen, die nicht den gerade aktiven Zeichensatz verwenden. Damit das funktioniert, enthält jede E-Mail bzw. jede Webseite Informationen über den eingesetzten Zeichensatz. Moderne Textverarbeitungsprogramme speichern den Text zumeist in einem Unicode-Zeichensatz oder unter Verwendung eines eigenen Codes. Auch Editoren wie Emacs oder XEmacs sind grundsätzlich in der Lage, Textdateien in verschiedenen Codierungen zu verarbeiten bzw. zu speichern.

Zeichensatzprobleme

Probleme treten am häufigsten auf, wenn Sender und Empfänger beim Austausch von (Text-)Dateien einen unterschiedlichen Zeichensatz verwenden. Beispielsweise verfasst ein Benutzer einer Linux-Distribution mit Unicode-Zeichensatz mit einem Editor eine Textdatei mit internationalen Sonderzeichen. Nun soll ein Benutzer eines anderen Betriebssystems mit Latin-Zeichensatz die Datei weiterbearbeiten. Dieser Benutzer stellt zu seiner Verwunderung fest, dass alle Nicht-ASCII-Zeichen falsch dargestellt werden. Derartige Probleme lassen sich mit den Kommandos `recode` bzw. `iconv` zumeist leicht lösen (siehe Abschnitt 17.3).

Dieselben Probleme betreffen auch Dateinamen, insbesondere im Zusammenspiel mit NFS3: Wenn Sie auf einem Rechner mit UTF8-Zeichensatz die Datei `äöü.txt` erzeugen und ein anderer Rechner mit Latin-Zeichensatz via NFS auf diese Datei zugreift, sieht der Dateiname so ähnlich wie `Ã¤Ã¶Ã¼.txt` aus. Abhilfe schaffen die Verwendung eines einheitlichen Zeichensatzes auf allen Rechnern des Netzwerks oder der Einsatz von NFS4. Wenn Sie den Zeichensatz für die Namen zahlreicher schon vorhandener Dateien ändern möchten, hilft das in Abschnitt 17.4 beschriebene Kommando `convmv` weiter.

Schriftart (Font)

Die Schriftart darf nicht mit einem Zeichensatz verwechselt werden. Sie ist dafür zuständig, wie ein bestimmtes Zeichen auf dem Bildschirm angezeigt wird. Dazu gibt es verschiedene Schriftarten (z. B. Arial, Courier, Helvetica, Palatino, um einige bekannte zu nennen).

Natürlich haben Schriftarten und Zeichensätze miteinander zu tun: Bevor ein Zeichen mit dem Code 234 korrekt auf dem Bildschirm dargestellt werden kann, muss klar sein, welcher Zeichensatz für die Codierung verwendet wurde. Manche alten Schriftarten waren auf 256 Zeichen beschränkt und standen daher in getrennten Versionen für verschiedene Zeichensätze zur Verfügung. Neuere Schriften enthalten hingegen mehr Zeichen und sind zu mehreren Zeichensätzen kompatibel.

Lokalisation und Zeichensatz einstellen

Konfigurationswerkzeuge

Je nach Distribution bzw. Desktop-System können Sie verschiedene Werkzeuge zur Konfiguration der Sprache einsetzen. Als Zeichensatz kommt fast immer UTF-8 zum Einsatz. Nur wenige Distributionen bieten noch die Möglichkeit, einen 8-Bit-Zeichensatz einzustellen. Bei allen Distributionen müssen Sie sich neu einloggen, damit veränderte Spracheinstellungen wirksam werden. Gnome berücksichtigt die Spracheinstellung des Systems und bietet hierfür selbst keine Konfigurationswerkzeuge an.

Debian:	`dpkg-reconfigure locales`
Fedora:	`localectl`
Gnome 3.*n*:	Systemeinstellungsmodul Region und Sprache
KDE:	Systemeinstellungsmodul Persönliches • Land/Region
RHEL 6:	`system-config-language`
SUSE:	YaST-Modul System • Sprache
Systemd:	`localectl`
Ubuntu:	`gnome-language-selector`

Außerdem bieten viele Display Manager mit dem Login-Dialog zu KDE, Gnome, Unity etc. die Möglichkeit, für die nächste Sitzung die gewünschte Sprache auszuwählen.

Konfigurationsdateien

Natürlich variiert der Ort, an dem die Konfigurationseinstellungen gespeichert werden:

Debian, Ubuntu:	`/etc/default/locale`
Fedora/Systemd:	`/etc/locale.conf`
RHEL 6:	`/etc/sysconfig/i18n`
SUSE:	`/etc/sysconfig/language`

`/etc/locale.conf` ist der vom Systemd-Entwickler vorgeschlagene neue Ort, vermutlich werden nach und nach auch andere Distributionen diese Datei verwenden. Um eine neue Standardsprache einzustellen, können Sie bei Distributionen mit einer aktuellen Systemd-Version das Kommando `localectl set-locale` verwenden. Eine Liste aller möglichen Einstellungen liefert `localectl list-locales`. Viele Distributionen berücksichtigen darüber hinaus benutzerspezifische Einstellungen in `.i18n`.

LC- und LANG-Variablen

Intern wird sowohl die Lokalisation als auch der Zeichensatz durch Umgebungsvariablen wie LC_CTYPE und LANG gesteuert. Für die Auswertung dieser Variablen ist die glibc-Bibliothek verantwortlich, die in fast allen Linux-Programmen zum Einsatz kommt. Die Lokalisation kann kategorieweise durchgeführt werden. Damit ist es möglich, beispielsweise für Datums- und Zeitangaben das in Deutschland übliche Format zu verwenden, Fehlermeldungen aber dennoch in Englisch anzuzeigen. Tabelle 21.5 zählt die wichtigsten Variablen auf.

Variable	Bedeutung
LANG	bestimmt den Standardwert für alle nicht eingestellten LC-Variablen.
LC_CTYPE	bestimmt den Zeichensatz.
LC_COLLATE	bestimmt die Sortierordnung.
LC_MESSAGES	bestimmt die Darstellung von Nachrichten, Fehlermeldungen etc.
LC_NUMERIC	bestimmt die Darstellung von Zahlen.
LC_TIME	bestimmt die Darstellung von Datum und Uhrzeit.
LC_MONETARY	bestimmt die Darstellung von Geldbeträgen.
LC_PAPER	bestimmt die Papiergröße.
LC_ALL	überschreibt alle individuellen LC-Einstellungen.

Tabelle 21.5 Wichtige Lokalisationsvariablen

Natürlich berücksichtigt nicht jedes Programm alle Kategorien; manche Programme ignorieren die LC_-Variablen sogar vollständig. Wenn einzelne Kategorien nicht eingestellt sind, verwenden Programme als Standardwert C bzw. POSIX. Das bedeutet, dass Fehlermeldungen auf Englisch erscheinen, Daten und Zeiten im amerikanischen Format dargestellt werden etc.

Anstatt alle Variablen einzeln einzustellen, können Sie einfach die Variable LANG einstellen. Damit wird für alle undefinierten Variablen der LANG-Standardwert verwendet. Einzig bei LC_COLLATE bleibt die Grundeinstellung POSIX. Bei den meisten Distributionen erfolgt die gesamte Spracheinstellung über die LANG-Variable.

Noch stärker als LANG wirkt LC_ALL. Wenn diese Variable gesetzt wird, gilt für alle Kategorien diese Einstellung, egal, wie LANG oder andere LC_-Variablen eingestellt sind.

Bei den meisten Programmen befinden sich Fehlermeldungen und andere Texte für jede Sprache separat in eigenen Verzeichnissen, z. B. in /usr/share/locale*/*sprache*/LC_MESSAGES. Weitere Hintergrundinformationen zum Thema *Locales and Internationalization* geben das Kommando man locale sowie die folgende Website:

http://www.gnu.org/software/libc/manual

Lokalisation testen

Den aktuellen Zustand der Lokalisationseinstellung können Sie am einfachsten mit dem Kommando `locale` ermitteln. Dieses Kommando wertet auch `LANG` und `LC_ALL` aus und ermittelt daraus die resultierenden Einstellungen. Das folgende Beispiel zeigt die Einstellung auf meinem Rechner:

```
user$  locale
LANG=de_DE.UTF-8
LC_CTYPE="de_AT.UTF-8"
LC_NUMERIC="de_AT.UTF-8"
LC_TIME="de_AT.UTF-8"
...
LC_ALL=
```

Zum Testen der Lokalisation können Sie auch ein beliebiges Kommando fehlerhaft ausführen. Die Fehlermeldung sollte in der eingestellten Sprache erscheinen. Wenn `LANG` auf `de_DE` eingestellt ist, sollte die Fehlermeldung des `mount`-Kommandos wie folgt aussehen:

```
user$  mount /xy
mount: Konnte /xy nicht in /etc/fstab oder /etc/mtab finden
```

env

Wenn Sie ein einzelnes Kommando mit einer anderen Spracheinstellung ausführen möchten, ohne gleich die gesamte Konfiguration zu ändern, verwenden Sie am besten das Kommando `env`. Dieses Kommando erwartet eine Reihe von Variablenzuweisungen und schließlich das eigentliche Kommando, das unter Berücksichtigung der eingestellten Variablen ausgeführt wird:

```
user$  env LANG=C mount /xy
mount: can't find /xy in /etc/fstab or /etc/mtab
```

Falls die Fehlermeldung trotz geänderter `LANG`-Einstellung noch immer in der jeweiligen Landessprache (statt in Englisch) erscheint, versuchen Sie, auch `LANGUAGE` zurückzusetzen:

```
user$  env LANG=C LANGUAGE=C mount /xy
mount: can't find /xy in /etc/fstab or /etc/mtab
```

Um `LANG` für den gesamten Verlauf einer Sitzung einzustellen, führen Sie `export LANG=C` aus.

Zulässige LC/LANG-Einstellungen

Eine Liste aller möglichen Einstellungen ermitteln Sie mit `locale -a`. Üblicherweise wird die Schreibweise *x_y* verwendet, wobei *x* durch zwei Buchstaben die Sprache und *y* durch zwei Buchstaben das Land bezeichnet. Im deutschen Sprachraum sollten Sie `de_DE` verwenden. Für die englische Standardeinstellung ist die Kurzschreibweise `C` erlaubt. Neuere glibc-Versionen verstehen auch Einstellungen wie `deutsch` oder `german`. Die Datei `/usr/share/locale/locale.alias` enthält eine Tabelle, die die zulässigen Kurzschreibweisen dem vollständigen Lokalisationsnamen zuordnet.

Lokalisierungspakete

Ob Menüs, Dialoge, Fehlermeldungen, Hilfetexte etc. tatsächlich in der richtigen Sprache angezeigt werden, hängt davon ab, ob die dazu erforderlichen Lokalisierungsdateien installiert sind. Aus Platzgründen ist dies oft nur für eine oder zwei Sprachen, z. B. Englisch und Deutsch, der Fall. Wenn Sie Ihre Distribution auch in französischer Sprache nutzen möchten, müssen Sie für Gnome, KDE, OpenOffice, Firefox etc. entsprechende Zusatzpakete installieren. Bei SUSE und Ubuntu helfen Ihnen dabei die in der Einleitung dieses Kapitels aufgezählten Konfigurationswerkzeuge, bei anderen Distributionen ist hier aber Handarbeit erforderlich.

Nicht jedes Linux-Programm ist für jede Sprache lokalisiert. Besonders große Lücken gibt es bei der Online-Dokumentation, also bei `man`-Seiten, Handbüchern und Hilfetexten. Wenn geeignete Lokalisierungsdateien fehlen, zeigt Linux englische Texte an.

Einstellung des Zeichensatzes

Zusammen mit der Lokalisation wird auch der Zeichensatz eingestellt. Der Zeichensatz folgt dem Ländercode nach einem Punkt, z. B. `de_DE.ISO-8859-1` oder `de_DE.utf8`.

21.6 Hardware-Referenz

In diesem Buch gibt es kein eigenes Hardware-Kapitel. Die richtige Konfiguration von Hardware-Komponenten wird stattdessen in den dazu passenden Kapiteln behandelt: Wenn Sie also beispielsweise Probleme mit einer Netzwerkkarte haben, ist Kapitel 29 zur Netzwerkkonfiguration der richtige Startpunkt.

Dieser Abschnitt hat somit zwei Aufgaben: Zum einen soll er die Suche nach weiteren Informationen zu bestimmten Hardware-Komponenten erleichtern. Zum anderen finden Sie hier kurze Informationen zu Hardware-Themen, die im Rest des Buchs zu kurz kommen. Natürlich gibt es eine Menge Hardware-Komponenten, die in diesem Buch aus den verschiedensten Gründen *nicht* beschrieben sind. Das liegt primär daran, dass ich nicht die Testmöglichkeiten habe, über die beispielsweise eine Computerzeitschrift verfügt.

Zuerst recherchieren, dann kaufen!

Erkundigen Sie sich *vor dem Kauf*, ob Ihre neue Hardware Linux-kompatibel ist! Werfen Sie einen Blick auf die üblichen Linux-Hardware-Seiten (siehe Abschnitt 1.1). Führen Sie im Internet eine Suche mit den Begriffen *linux modellname* durch. Auch Linux-orientierte Zeitschriften sind für diesen Zweck naturgemäß eine aktuellere Informationsquelle als Bücher.

Device-Dateien

Die meisten Hardware-Komponenten werden über sogenannte Devices angesprochen – z. B. `/dev/sda` für eine SATA-Festplatte. Die Device-Dateien werden dynamisch bei Bedarf durch das `udev`-System erzeugt. Eine Liste mit den wichtigsten Linux-Device-Dateien finden Sie in Abschnitt 15.10.

/proc- und /sys-Dateien

Bei vielen Komponenten geben virtuelle Dateisysteme in den Verzeichnissen `/proc` und `/sys` detaillierte Informationen. Einen Überblick über solche Hardware-Dateien finden Sie in Abschnitt 28.3.

Kernelmodule

Die Treiber zu zahllosen Hardware-Komponenten befinden sich in Kernelmodulen. Ein Teil dieser Module wird während des Systemstarts geladen, die restlichen Module erst bei Bedarf. Wenn das automatische Laden von Modulen nicht funktioniert, sollten Sie einen Blick in die Dateien `/etc/mmodprobe.conf` bzw. `/etc/modprobe.conf.d/*` werfen. Der Umgang mit Modulen und die Funktion dieser Dateien werden in Abschnitt 28.1 beschrieben.

Was beim Laden von Modulen geschieht und ob die Hardware erfolgreich initialisiert werden kann, geht aus den Kernelmeldungen hervor. Diese lesen Sie mit dem Kommando `dmesg`.

Hardware-Überblick

Um einen Überblick über die laufende Hardware zu erlangen, führen Sie die Kommandos `lsblk`, `lspci` und `lsusb` aus. Auch ein Blick in die Kernelmeldungen mit `dmesg` ist oft aufschlussreich.

CPU und Speicher

CPU

Welche CPUs in Ihrem Rechner laufen, geht aus der Datei `/proc/cpuinfo` hervor. Die folgende, stark gekürzte Ausgabe entstand auf einem Rechner mit einem Intel-i7-Prozessor. Linux betrachtet die Cores wie eigenständige Prozessoren. Dabei enthält die Zeile `model name` die maximale Taktfrequenz.

```
user$  cat /proc/cpuinfo
cat /proc/cpuinfo
processor       : 0
model name      : Intel(R) Core(TM) i7 CPU         860  @ 2.80GHz
...
processor       : 1
model name      : Intel(R) Core(TM) i7 CPU         860  @ 2.80GHz
...
```

Bei Prozessoren mit variabler Taktfrequenz sind `cpufreq`-Module für die energiesparende Reduzierung der Frequenz zuständig. Gute Hintergrundinformationen zu diesem System geben die folgenden zwei Seiten:

http://www.kernel.org/doc/Documentation/cpu-freq
https://wiki.archlinux.org/index.php/CPU_Frequency_Scaling

Daten zum aktuellen Zustand des Systems sowie Steuerungsmöglichkeiten bieten die Dateien des folgenden Verzeichnisses:

```
/sys/devices/system/cpu/cpun/cpufreq/
```

CPU-Frequenz limitieren

Um zu vermeiden, dass die CPU schnell heiß läuft, kann man die maximale CPU-Frequenz limitieren. Dazu verwenden Sie das Kommando `cpufreq-set` aus dem Paket `cpufrequtils`. Das folgende Kommando limitiert die Frequenz auf 800 MHz:

```
root#  cpufreq-set -r -max 0.8GHz
```

Über den Nutzen dieser Anweisung kann man allerdings geteilter Meinung sein: Rechenintensive Aufgaben dauern nun einfach länger, und dabei wird in der Regel noch mehr Wärme freigesetzt.

CPU-Temperatur überwachen

Wenn Sie wissen möchten, welche Temperatur Ihre CPU gegenwärtig aufweist, installieren Sie das Paket `lm-sensors`. Nach der Installation führen Sie als `root` das Kommando `sensors-detect` aus. Es stellt fest, welche Hardware-Komponenten Informationen über ihren Zustand liefern. Neben der CPU können das auch die Festplatte, die Grafikkarte oder diverse Lüfter sein, die ihre Drehzahl melden. Die zur Auswertung erforderlichen Kernelmodule fügt `sensors-detect` auf Wunsch gleich in `/etc/modules` ein. Diese Einstellungen gelten allerdings erst ab dem nächsten Rechnerstart. Den ersparen Sie sich durch ein manuelles Laden der betreffenden Module mit `modprobe`.

Nach diesen Vorbereitungsarbeiten liefert das Kommando `sensors` eine aktuelle Temperaturliste:

```
root#  sensors
coretemp-isa-0000
Adapter: ISA adapter
Physical id 0:  +31.0°C  (high = +80.0°C, crit = +98.0°C)
Core 0:         +26.0°C  (high = +80.0°C, crit = +98.0°C)
Core 1:         +29.0°C  (high = +80.0°C, crit = +98.0°C)
```

Es gibt diverse Programme, die diese Daten eleganter darstellen. Für erste Experimente bietet sich `xsensors` an, das die Daten aller Sensoren in einem Fenster anzeigt (siehe Abbildung 21.2). Unter Ubuntu installieren Sie das Paket `indicator-sensors` oder `psensor`.

Speicher (RAM)

Informationen über den verfügbaren Speicher erhalten Sie mit dem Kommando `free`. Wenn Sie vermuten, dass Ihr Rechner defekte Speicherbausteine hat, bietet das Programm Memtest86 eine gute Möglichkeit, das RAM zu testen. Bei fast allen Distributionen kann das Programm komfortabel während des Systemstarts gestartet werden. Sollte das bei Ihnen nicht funktionieren, finden Sie auf der folgenden Website ein ISO-Image, um eine bootfähige CD zu brennen:

http://www.memtest86.com

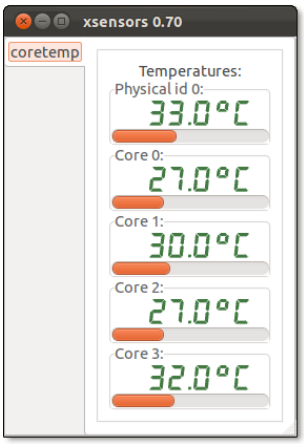


Abbildung 21.2 Temperaturanzeige mit xsensors

Energieverwaltung

ACPI

ACPI steht für *Advanced Configuration and Power Interface* und steuert die Energieverwaltungsfunktionen marktüblicher PCs und Notebooks seit ca. 1999. ACPI wird seit Kernel 2.6 von Linux unterstützt. Die erforderlichen Kernelmodule werden automatisch geladen, wovon Sie sich mit `dmesg | grep ACPI` überzeugen können. Gleichzeitig werden der Kernelprozess `kacpid` und der ACPI-Dämon `acpid` gestartet. Diese beiden Programme verarbeiten ACPI-Ereignisse. `acpid` wird durch die Dateien in `/etc/acpi` gesteuert.

Das Kommando `acpi -V` und die Dateien des Verzeichnisses `/proc/acpi` geben Informationen über den aktuellen Zustand des ACPI-Systems (Ladezustand der Akkus, deren Temperatur etc.).

Falls ACPI beim Start Probleme verursacht, finden Sie in Abschnitt 28.4 einige Kernelparameter, um ACPI ganz oder teilweise zu deaktivieren. Weitere Informationen zu ACPI und Linux finden Sie hier:

http://www.lesswatts.org/projects/acpi

Suspend

ACPI unterstützt verschiedene Schlafmodi, in denen der Rechner wenig (Bereitschaft, Stand-by-Modus) bzw. gar keinen Strom verbraucht (Suspend-Modus, Hibernate-Modus, Ruhezustand). Bei den meisten Distributionen bzw. Desktop-Systemen versetzen Sie den Rechner über das Systemmenü in den gewünschten Schlafmodus.

Im sogenannten Ruhezustand wird der aktuelle Speicherinhalt in der Swap-Partition der Festplatte gespeichert und der Rechner vollständig ausgeschaltet. Das setzt voraus, dass die Swap-Partition ausreichend groß ist! Beim Aufwachen wird der Speicher wieder von der Festplatte gelesen. Außerdem müssen sämtliche Hardware-

Komponenten neu initialisiert werden. Dieser Prozess ist sehr komplex und erfordert ein optimales Zusammenspiel des Linux-Kernels, seiner Module und des ACPI-Systems.

Aus der Ruhe erwachen ...

Meine persönlichen Erfahrungen mit dem Ruhezustand sind leider überwiegend negativ. Soweit nicht schon beim Versuch der Aktivierung ein Fehler auftrat, gelang es oft nicht mehr, den Rechner aus dem Schlafmodus wieder aufzuwecken. Mehr Glück hatte ich auf meinen Testrechnern mit dem Bereitschaftsmodus, der auf fast allen Geräten zuverlässig funktionierte.

Auf jeden Fall sollten Sie die Suspend-Funktionen anfangs mit Vorsicht testen: Sichern Sie vorher alle Daten, führen Sie `sync` aus, und lösen Sie alle nicht benötigten Dateisysteme aus dem Verzeichnisbaum!

powertop

Das Kommando `powertop` hilft bei der Suche nach Programmen, die die CPU aus dem Ruhezustand holen. Gleichzeitig gibt das Programm Tipps, wie der Energieverbrauch minimiert werden kann.

```
root#  powertop
Cn                Verweildauer       P-States (Frequenzen)
C0 (Prozessor läuft)    ( 1,8%)         1,80 GHz     0,0%
zyklisches AbfraC1 halt           0,0m  1,60 GHz     0,0%
C1 halt           0,0ms ( 0,0%)         1400 MHz     0,0%
C2               17,7ms (98,2%)         1200 MHz     0,0%
C3                0,0ms ( 0,0%)          600 MHz   100,0%
C4                0,0ms ( 0,0%)
Aufwachen pro Sekunde : 55,3    Intervall: 3,0s
Stromverbrauch (ACPI-Schätzung): 20,1W (1,2 Std.)
Häufigste Ursachen für das Aufwachen:
  23,0% ( 15,7)       <interrupt> : ehci_hcd:usb1, uhci_hcd:usb2, ...
  21,6% ( 14,7)    USB Gerät  3-2 : Optical USB Mouse (Logitech)
  13,7% (  9,3)       <interrupt> : extra timer interrupt
  12,7% (  8,7)     <Kernel Kern> : usb_hcd_poll_rh_status (rh_timer_func)
   9,8% (  6,7)     <Kernel Kern> : hrtimer_start (tick_sched_timer)
Vorschlag: Aktivieren Sie "USB autosuspend" durch Drücken der U-Taste
oder durch Anhängen der Bootoption "usbcore.autosuspend=1" an die Kernel-
kommandozeile oder in der GRUB-Konfiguration.
```

Lüftersteuerung

Nichts nervt mehr, wenn bei einem an sich leisen Notebook ständig der Lüfter heult. Lässt sich dagegen etwas machen? Nach meinen Erfahrungen eher nicht – achten Sie schon beim Kauf darauf, ein Modell auszuwählen, das leise ist. Für alle, die den Krach doch per Software mindern möchten, folgen hier einige Empfehlungen.

Fan Control

Für manche Notebooks gibt es spezielle Programme zur Steuerung des Lüfters. Diese Programme setzen voraus, dass zuvor das Paket `lm-sensors` installiert und konfiguriert wurde. Es ist notwendig, damit die CPU-Temperatur überwacht werden kann. Sofern diese Voraussetzung erfüllt ist, können Sie einstellen, ab welcher Temperatur welcher Lüfter in welcher Drehzahl laufen soll.

Eines der populärsten Programme zur Lüftersteuerung hat den Namen `tpfanco`. Es ist zu fast allen Notebooks von IBM und Lenovo kompatibel. Aktuelle Debian-Pakete gibt es hier zum Download:

http://code.google.com/p/tpfanco/downloads/list

Nach der Installation und dem manuellen Start des tpfan-Dämons (`service tpfand start`) kann die Lüftersteuerung mit `tpfan-admin` kontrolliert werden (erfordert `root`-Rechte). In dieser grafischen Benutzeroberfläche kann die Einschaltschwelle für jeden der im System erkannten Temperatursensoren individuell eingestellt werden. Ich habe das Programm auf dem Lenovo-Notebook E320 einige Tage lang ausprobiert. Ich habe zwar erreicht, dass der Lüfter weniger häufig als zuvor lief, ganz verhindern konnte ich dessen Betrieb aber nicht.

Vorsicht

Naturgemäß erfolgt die manuelle Lüftersteuerung auf eigene Gefahr. Wenn die CPU oder andere Komponenten des Rechners regelmäßig zu heiß sind, verringert sich deren Lebensdauer! Setzen Sie Programme zur Lüftersteuerung daher mit Vorsicht ein, und recherchieren Sie vorher im Internet, welche Erfahrungen andere Benutzer gemacht haben.

Schnittstellen und Bussysteme

Serielle und parallele Schnittstelle

Unter Linux sind serielle bzw. parallele Schnittstellen über die Device-Dateien `/dev/ttyS`*n* bzw. `/dev/lp`*n* zugänglich. Am ehesten treffen Sie auf diese veralteten Schnittstellen bei der Konfiguration eines Analogmodems bzw. eines alten Druckers.

IDE, SATA, SCSI

Interne Festplatten, CD- und DVD-Laufwerke sowie diverse andere Datenträger sind in der Regel über die Bussysteme IDE, SATA oder SCSI mit dem Rechner verbunden (siehe auch Abschnitt 25.2). Aktuelle Linux-Versionen kommunizieren mit IDE-, SATA- und SCSI-Geräten über das SCSI-System des Kernels. Nur bei wenigen IDE-Controllern, die inkompatibel zur der `libata`-Erweiterung des SCSI-Systems sind, kommen noch die alten IDE-Treiber zum Einsatz.

Informationen über den Zustand der IDE- und SCSI-Systeme und aller damit verwalteten Geräte geben das Kommando `lsscsi` sowie die folgenden Dateien:

```
/sys/bus/ide/*
/sys/bus/scsi/*
/proc/scsi/*
```

USB

Der *Universal Serial Bus* (USB) wird zur Verbindung zwischen dem Computer und diversen externen Geräten eingesetzt – von der Maus bis zum Scanner. Die erforderlichen USB-Kernelmodule werden automatisch geladen. USB-Datenträger (also USB-Festplatten, Memorysticks, externe CD- und DVD-Laufwerke) etc. werden wie SCSI-Geräte behandelt.

Das virtuelle Dateisystem `usbfs` gibt im Verzeichnis `/proc/usb` Informationen über alle angeschlossenen USB-Geräte. Weitere Daten können Sie dem Verzeichnis `/sys/bus/usb` entnehmen. Eine ausführliche Liste aller USB-Schnittstellen und -Geräte liefert `lsusb -v` (Paket `usbutils`).

Firewire

Das Bussystem Firewire ist eine Alternative zu USB. Firewire ist durch den Standard IEEE 1394 definiert und auch unter dem von Sony bevorzugten Namen *i.Link* bekannt. Firewire ist etwas schneller als USB und ist vor allem zur Datenübertragung von Videokameras beliebt. Umfassende Informationen zum Thema Linux und IEEE 1394 finden Sie auf der folgenden Website:

http://www.linux1394.org

Beim Anschluss von Firewire-Geräten werden die erforderlichen Module (insbesondere `ieee1394`) automatisch geladen. Informationen über die angeschlossenen Geräte und den Status des Firewire-Systems geben die Dateien in `/sys/bus/ieee1394`.

PCI

Informationen über PCI-Komponenten in Ihrem Rechner ermitteln Sie am besten mit dem Kommando `lspci`. Die Dateien in `/proc/bus/pci/` und `/sys/bus/pci/` enthalten dieselben Informationen, sind aber wesentlich schwieriger zu interpretieren. Die folgende Ausgabe ist aus Platzgründen stark gekürzt:

```
root#  lspci
00:00.0 Host bridge: Intel Corporation 82P965/G965 Memory Controller Hub
00:01.0 PCI bridge: Intel Corporation 82P965/G965 PCI Express Root Port
00:1a.0 USB Controller: Intel Corporation 82801H (ICH8 Family) USB UHCI #4
00:1b.0 Audio device: Intel Corporation 82801H (ICH8 Family) HD Audio Controller
01:00.0 VGA compatible controller: nVidia Corporation G70 [GeForce 7600 GS]
02:00.0 Ethernet controller: Marvell Technology Group Ltd. 88E8056 PCI-E Gigabit
        Ethernet Controller (rev 12)
```

Grafik (X) Grafikkarten werden unter Linux durch das X Window System genutzt. Dessen Konfiguration ist Thema von Kapitel 24.

Netzwerk-Schnittstellen Detaillierte Informationen zur Konfiguration von LAN- und WLAN-Schnittstellen sowie zum Umgang mit ADSL- und UMTS-Modems finden Sie in Kapitel 29.

Bluetooth Bluetooth ist ein Verfahren zur Kommunikation von Hardware-Geräten per Funk. Bluetooth hat eine geringere Reichweite als WLAN und wird überwiegend in elektronischen Kleingeräten eingesetzt (Tastaturen, Mäuse, Handys etc.). Linux kommt mit den meisten Bluetooth-Geräten auf Anhieb und ohne besondere Konfigurationsarbeiten zurecht.

Unter Gnome helfen das im Panel angezeigte `bluetooth-applet` sowie der `bluetooth-wizard` beim Einrichten neuer Bluetooth-Geräte. Unter KDE übernehmen `kbluetooth` und der `kbluetooth-devicemanager` diese Aufgaben. Hinter den Kulissen ist der Dämon `bluetoothd` im Zusammenspiel mit `udev` für die Verwaltung der Bluetooth-Geräte verantwortlich. Die entsprechenden Konfigurationsdateien befinden sich im Verzeichnis `/etc/bluetooth`. Weitere Informationen zu Bluetooth unter Linux finden Sie hier:

http://www.bluez.org

Sollte es erforderlich sein, Bluetooth auf Kommandozeilenebene zu konfigurieren, helfen dabei die Kommandos `hcitool scan` und `bluez-xxx`, die üblicherweise vom Paket `bluez` bereitgestellt werden.

Mit `hcitool dev` finden Sie den Device-Namen Ihres Bluetooth-Steckers heraus (in aller Regel `hci0`), mit `hcitool scan` die ID des Bluetooth-Geräts, mit dem Sie die Verbindung herstellen möchten. Achten Sie darauf, dass das Gerät eingeschaltet ist!

`bluez-simple-agent` macht den Bluetooth-Empfänger und das Bluetooth-Gerät miteinander bekannt (in der Bluetooth-Nomenklatur *pairing* genannt). Dabei müssen Sie einen PIN-Code eingeben, bei Eingabegeräten (Tastatur, Maus) üblicherweise einfach 0000 oder 1234.

`bluez-test-input connect` stellt die Verbindung zum angegebenen Eingabegerät her. Falls die Eingaben nicht berücksichtigt werden, muss unter Umständen das Kernelmodul `uinput` geladen werden.

Das Kommando `bluez-test-device trusted` bewirkt, dass sich das Bluetooth-System merkt, dass das angegebene Gerät vertrauenswürdig ist. Damit gelingt später ein automatischer Verbindungsaufbau. Intern wird diese Information in der Datei `/var/lib/bluetooth/<hci-id>/trusts` gespeichert.

```
root#  update-rc.d dbus defaults
root#  apt-get install bluez python-gobject
```

```
root#  hcitool dev
Devices: hci0    00:1F:CF:41:00:A2
root#  hcitool scan
Scanning ...
        00:25:BC:FB:C1:E5       Michael Koflers Tastatur
root#  bluez-simple-agent hci0 00:25:BC:FB:C1:E5
RequestPinCode (/org/bluez/1878/hci0/dev_00_25_BC_FB_C1_E5)
Enter PIN Code:  0000
Release
New device (/org/bluez/1878/hci0/dev_00_25_BC_FB_C1_E5)
root#  bluez-test-input connect 00:25:BC:FB:C1:E5
root#  bluez-test-device trusted 00:25:BC:FB:C1:E5 yes
root#  modprobe -i uinput
root#  echo uinput >> /etc/modules
```

Hotplug-System

Bei modernen Rechnern können im laufenden Betrieb Festplatten, USB-Sticks und andere Geräte angeschlossen bzw. wieder entfernt werden. Linux muss auf die geänderte Hardware-Situation rasch und möglichst automatisch reagieren. Diese Aufgabe übernimmt das Hotplug-System, dessen Komponenten im Verlauf der letzten Jahre immer wieder verändert wurden. Zuletzt wurde der als ineffizient bekannte *Hardware Abstraction Layer* (HAL) aus den meisten Distributionen entfernt bzw. nur noch in Sonderfällen aktiviert. Die aktuelle Vorgehensweise sieht so aus:

- **Kernel:** Der Kernel stellt Veränderungen an der Hardware fest, z. B. dass der Benutzer einen USB-Stick angesteckt hat.
- **udev:** Der Kernel erzeugt via `udev` neue Device-Dateien (siehe Abschnitt 15.9) und startet geeignete Programme, um die neuen Geräte zu verwalten bzw. um Benachrichtigungen an das Desktop-System zu versenden. Dabei werden Regeldateien aus den Verzeichnissen `/lib/udev/rules.d` sowie `/etc/udev/rules.d` ausgewertet. Tipps zum Verfassen bzw. Verändern dieser Regeln finden Sie hier:

  http://www.reactivated.net/writing_udev_rules.html
- **DeviceKit:** Für manche Geräte bzw. Komponenten hilft das sogenannte DeviceKit bei der Verwaltung. Es besteht aus den Bibliotheken `libudev` und `libgudev`, die üblicherweise in gleichnamige Pakete verpackt sind. Für Festplatten(partitionen) und externe Datenträger sind die Programme und Scripts des Pakets `udisks` verantwortlich (ehemals `DeviceKit-disks`). Um die Energieverwaltung kümmern sich die Regeln und Programme des Pakets `upower` (ehemals `DeviceKit-power`). Weitere Informationen finden Sie hier:

  http://freedesktop.org/wiki/Software/DeviceKit
  http://www.freedesktop.org/wiki/Software/udisks
  http://upower.freedesktop.org

- **Desktop:** In KDE 4 ist das Framework Solid für die Verarbeitung von D-Bus-Nachrichten zuständig. Unter Gnome kümmert sich Nautilus im Zusammenspiel mit PolicyKit (siehe Abschnitt 16.4) um die externen Datenträger. Die Konfiguration erfolgt in den Systemeinstellungen im Modul Details • Wechselmedien.
- **D-Bus:** Zur Kommunikation zwischen den verschiedenen Ebenen des Hotplug-Systems wird das D-Bus-Kommunikationssystem (kurz D-Bus) verwendet. Auf der Basis der Bibliothek `libdbus` kann die Kommunikation direkt zwischen zwei Programmen erfolgen. Wenn Nachrichten zwischen mehreren Programmen ausgetauscht werden sollen, kommt als zentrale Vermittlungsstelle das Hintergrundprogramm `dbus-daemon` zum Einsatz.

Audio-System (ALSA)

ALSA

ALSA steht für *Advanced Linux Sound Architecture* und ist seit Kernel 2.6 für die Ansteuerung von Sound-Karten auf unterster Ebene verantwortlich. In früheren Kernelversionen kam stattdessen OSS (Open Sound System) zum Einsatz. ALSA bietet bei Bedarf durch die Module `snd-pcm-oss`, `snd-seq-oss` und `snd-mixer-oss` eine Kompatibilitätsschicht zu OSS.

Bei vom Kernel unterstützten Audio-Controllern wird das erforderliche ALSA-Modul automatisch geladen. Die Namen aller ALSA-Module beginnen mit `snd`. Der Befehl `lsmod | grep snd` liefert daher einen raschen Überblick über alle aktiven ALSA-Module. Der Zugriff auf diverse Soundfunktionen erfolgt über Dateien im Verzeichnis `/proc/asound`.

Sie konfigurieren das ALSA-System durch die Dateien `/etc/alsa/*`, `/etc/asound.conf` sowie `.asoundrc`. Bei einer gewöhnlichen Nutzung des Audio-Systems besteht keine Notwendigkeit, diese Dateien zu verändern. Die Hardware-Erkennung sollte automatisch gelingen. Wer besondere Audio-Anforderungen hat (Musiker), zwischen mehreren Audio-Karten differenzieren will oder andere Sonderwünsche hat, der findet auf der folgenden Website und dem dazugehörenden Wiki umfassende Hintergrundinformationen zu ALSA und zu seiner Konfiguration:

http://www.alsa-project.org

Beim Herunterfahren des Rechners bzw. beim nächsten Neustart werden durch das Init-System die Lautstärkeeinstellungen gespeichert bzw. wiederhergestellt.

ALSA-Tools

Zur direkten Nutzung von ALSA stehen diverse Kommandos zur Auswahl (Paket `alsa-utils`), von denen hier die wichtigsten kurz vergestellt werden: `alsactl` speichert bzw. lädt alle ALSA-Einstellungen, also z. B. die zuletzt eingestellte Lautstärke. `alsamixer` verändert die Lautstärke bzw. den Eingangspegel diverser ALSA-Audio-Kanäle. `aplay` spielt eine Audio-Datei ab. `arecord` nimmt eine Audio-Datei auf.

Fehlersuche im Audio-System

Wenn die Lautsprecher still bleiben, ist die Ursache oft nur ein auf 0 gestellter Lautstärkeregler. Für gewöhnliche Anwendungen sind drei Kanäle wichtig: Die Master-Lautstärke steuert die Lautstärke des Gesamtsignals. Die PCM-Lautstärke gibt an, wie laut von Audio- und Video-Playern erzeugte Audio-Daten in das Gesamtsignal eingespeist werden. (PCM steht für *Pulse Code Modulation*.) Die CD-Lautstärke gibt schließlich an, wie laut die direkt vom CD-Laufwerk kommenden Daten in das Gesamtsignal einfließen, wenn das CD-Laufwerk und die Audio-Karte mit einem Kabel verbunden sind.

Bei modernen Distributionen fehlen bisweilen grafische Benutzeroberflächen, um die Audio-Eingänge und -Ausgänge einzeln einzustellen. Abhilfe: Starten Sie `alsamixer` in einer Textkonsole. Nun können Sie mit den Cursortasten die Kanäle auswählen und deren Pegel justieren. `M` schaltet einen Kanal ganz ein bzw. wieder aus (*mute*).

Audio-Bibliotheken

Viele Audio-Programme verwenden ALSA nicht direkt, sondern greifen auf Sound-Bibliotheken, Sound-Server etc. zurück. Diese Zwischenschicht zwischen dem Low-Level-System ALSA und den eigentlichen Audio-Anwendungen soll die Programmierung vereinfachen, Audio-Anwendungen netzwerktauglich machen und die konfliktfreie Kooperation gleichzeitig laufender Audio-Programme sicherstellen.

Das Problem besteht nun darin, dass es momentan keine einheitliche Audio-Architektur oberhalb von ALSA gibt: KDE und Gnome gehen jeweils eigene Wege. Anspruchsvolle Audio-Anwendungen, für die die vorhandenen Audio-Bibliotheken unzureichend sind, implementieren elementare Audio-Funktionen selbst neu. Es ist extrem schwierig, Audio-Programme zu entwickeln, die unabhängig vom Desktop-System einfach funktionieren. Programmierer der Firma Adobe gaben Audio-Probleme als einen wesentlichen Grund dafür an, weswegen die Entwicklung des Flash-Plugins für Linux so lange dauerte.

Die folgenden Punkte stellen einige gängige Audio-Systeme kurz vor:

- **GStreamer:** Die GStreamer-Bibliothek ist ein umfassendes Multimedia-Framework, das von vielen Gnome-Programmen eingesetzt wird. Dank einer Plugin-Architektur ist es sehr modular und kann gut erweitert werden. Auch Codecs zur Verarbeitung verschiedener Audio- und Video-Formate sind als Plugins verfügbar. Die GStreamer-Bibliothek enthält keinen eigenen Sound-Dämon; das Zusammenführen mehrerer Audio-Signale übernimmt direkt ALSA. Weitere Informationen finden Sie hier:

  http://www.gstreamer.net

- **Phonon:** Das Multimedia-Fundament von KDE 4 heißt Phonon. Die Bibliothek bietet eine einheitliche Programmierschnittstelle zur Nutzung von Audio- und Video-Funktionen, die auf vorhandene Multimedia-Bibliotheken zurückgreift

(oft Xine, aber je nach installiertem Backend kommen auch GStreamer oder VLC infrage). Phonon wird auch von der Qt-Bibliothek als Multimedia-Schnittstelle verwendet. Weitere Details verrät die Phonon-Website:

http://phonon.kde.org

- **PulseAudio:** PulseAudio ist ein netzwerkfähiger Sound-Server, der von den meisten Distributionen verwendet wird. Alle Audio-Streams können mit dem Programm `pavucontrol` getrennt gesteuert und unterschiedlichen Audio-Karten bzw. -Ausgabegeräten zugewiesen werden. PulseAudio sollte auch zusätzliche Audio-Hardware – z. B. USB-Boxen – automatisch erkennen und aktivieren. Weitere Details verrät die folgende Seite:

  http://www.freedesktop.org/wiki/Software/PulseAudio

Zu diesen Audio-Systemen gesellen sich diverse Programme, die selbst umfassende Audio- bzw. Multimedia-Bibliotheken enthalten und diese auch anderen Programmen zur Verfügung stellen. Ein prominentes Beispiel ist der Video-Player Xine auf Basis der `xinelib`. Man kann sich leicht ausrechnen, dass Inkompatibilitäten zwischen verschiedenen Audio-Programmen und -Bibliotheken wortwörtlich vorprogrammiert sind.

Für Musiker bzw. professionelle Audio-Anwender gibt es eigene Distributionen, die speziell in Hinblick auf die optimale und störungsfreie Nutzung der Audio-Programme zusammengestellt sind. Am populärsten ist zurzeit Ubuntu Studio (*http://ubuntustudio.org*).

21.7 Logging

Der Kernel, diverse administrative Werkzeuge (PAM, APT, dpkg) und die meisten Netzwerkdienste protokollieren alle erdenklichen Ereignisse in zahllose Dateien in `/var/log`. Diese Logging-Dateien sind während der Inbetriebnahme eines neuen Dienstes ausgesprochen praktisch, um Konfigurationsfehler zu finden. Im laufenden Betrieb eines Servers können die Logging-Dateien Hinweise auf Sicherheitsprobleme geben.

Syslog

Damit nicht jedes Programm das Rad neu erfinden muss, greifen der Kernel sowie eine Menge administrativer Werkzeuge und Server-Dienste auf zentrale Logging-Funktionen zurück, die üblicherweise als Syslog bezeichnet werden. Es gibt verschiedene Implementierungen von Syslog; die populärste ist momentan `rsyslogd`. Wenn Sie sich einen Überblick über die von Syslog verwalteten Logging-Dateien verschaffen möchten, führen Sie die folgenden Kommandos aus:

```
root#  cd /var/log
root#  ls $(find -user syslog)
```

Allerdings nutzen nicht alle Netzwerkdienste Syslog! Insbesondere die »großen« Server-Dienste, beispielsweise Apache, CUPS, MySQL und Samba, verwenden jeweils ihre eigenen, in das Programm integrierten Logging-Funktionen. Sie entziehen sich damit der globalen Syslog-Konfiguration. Die Logging-Parameter werden vielmehr in den jeweiligen Konfigurationsdateien des Programms eingestellt.

Journal

Fedora verwendet zusätzlich zur Protokollierung mancher Ereignisse die Journal-Funktion von Systemd. Im Unterschied zu Syslog gilt für Journal ein binäres Dateiformat, das gegen nachträgliche Veränderungen geschützt ist. Mehr Details zu Journal folgen am Ende dieses Abschnitts.

rsyslogd

Konfiguration

Bei den meisten aktuellen Distributionen (Debian, Fedora, openSUSE, Ubuntu) werden die Syslog-Dienste durch das Programm `rsyslogd` realisiert. Dessen Konfiguration erfolgt durch die Dateien `/etc/rsyslogd.conf` und `/etc/rsyslog.d/*.conf`. Im Folgenden beschreibe ich exemplarisch die Konfiguration unter Ubuntu. Dort befinden sich die meisten Einstellungen in `/etc/rsyslog.d/50-default.conf`.

Die Syslog-Konfigurationsdateien enthalten Regeln, die aus zwei Teilen bestehen:

- **Selektor:** Der erste Teil jeder Regel gibt an, was protokolliert werden soll.
- **Aktion:** Der zweite Teil steuert, was mit der Meldung geschehen soll.

Regeln können mit dem Zeichen \ über mehrere Zeilen verteilt werden. Es ist möglich, dass auf eine Meldung mehrere Regeln zutreffen. In diesem Fall wird die Meldung mehrfach protokolliert bzw. weitergegeben.

Selektor

Jeder Selektor besteht aus zwei durch einen Punkt getrennten Teilen: *dienst.prioritätsstufe*. Es ist erlaubt, mehrere durch einen Strichpunkt separierte Selektoren anzugeben. Des Weiteren können in *einem* Selektor mehrere Dienste durch Kommas getrennt werden. Alle Linux-Programme, die Syslog verwenden, müssen ihren Meldungen einen Dienst und eine Priorität zuordnen.

Syslog kennt die folgenden Dienste (Facilities): `auth`, `authpriv`, `cron`, `daemon`, `ftp`, `kern`, `lpr`, `mail`, `news`, `syslog`, `user`, `uucp` sowie `local0` bis `local7`. Das Zeichen * umfasst alle Dienste.

Syslog kennt außerdem diese Prioritätsstufen (in steigender Wichtigkeit): `debug`, `info`, `notice`, `warning` = `warn`, `err` = `error`, `crit`, `alert` und `emerg` = `panic`. Die Schlüsselwörter `warn`, `error` und `panic` gelten als veraltet – verwenden Sie stattdessen `warning`, `err`

und emerg. Das Zeichen * umfasst alle Prioritätsstufen. Das Schlüsselwort none gilt für Nachrichten, denen keine Priorität zugeordnet ist.

Die Angabe einer Prioritätsstufe schließt alle höheren (wichtigeren) Prioritätsstufen mit ein. Der Selektor mail.err umfasst also auch crit-, alert- und emerg-Meldungen des Mail-Systems. Wenn Sie explizit nur Nachrichten einer bestimmten Priorität wünschen, stellen Sie das Zeichen = voran (also etwa mail.=err).

Aktion Als Aktion wird normalerweise der Name einer Logging-Datei angegeben. Normalerweise werden Logging-Dateien nach jeder Ausgabe synchronisiert. Wenn dem Dateinamen ein Minuszeichen vorangestellt ist, verzichtet Syslog auf die Synchronisierung. Das ist wesentlich effizienter, allerdings gehen dann bei einem Absturz noch nicht physikalisch gespeicherte Meldungen verloren.

Syslog kann Nachrichten auch an FIFO-Dateien (First In First Out) oder Pipes weiterleiten. In diesem Fall stellen Sie dem Dateinamen das Zeichen | voran. Die Datei /dev/xconsole, die im folgenden Listing vorkommt, ist eine besondere FIFO-Datei zur Weitergabe von Meldungen an das Grafiksystem X.

Das Zeichen * bedeutet, dass die Nachricht an alle in Konsolen bzw. via SSH eingeloggten Benutzer gesendet wird. Da das sehr störend ist, wird es standardmäßig nur für kritische Meldungen verwendet. Weitere Details zur Syntax von rsyslog.conf gibt die gleichnamige man-Seite.

Beispiel Die folgenden Zeilen geben die Syslog-Standardkonfiguration von Ubuntu leicht gekürzt und etwas übersichtlicher formatiert wieder:

```
# Datei /etc/rsyslog.d/50-default.conf bei Ubuntu
# Selektor                      Aktion
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
kern.*                          -/var/log/kern.log
mail.*                          -/var/log/mail.log
mail.err                        /var/log/mail.err
*.emerg                         :omusrmsg:*
daemon.*;mail.*;\
        news.err;\
        *.=debug;*.=info;\
        *.=notice;*.=warn       |/dev/xconsole
```

Im Klartext bedeutet die obige Konfiguration:

- /var/log/auth enthält Authentifizierungsmeldungen aller Prioritätsstufen. Dazu zählen gescheiterte und erfolgreiche Login-Versuche (auch via SSH), PAM-Meldungen, sudo-Kommandos etc. Als einzige Logging-Datei wird auth bei jeder Meldung sofort synchronisiert.

- `/var/log/syslog` enthält *alle* via Syslog protokollierten Meldungen (inklusive Authentifizierungsmeldungen, denen keine Priorität zugewiesen ist). Der allumfassende Ansatz ist zugleich ein Vor- und ein Nachteil. Einerseits können Sie so aus einer einzigen Datei alle erdenklichen Informationen extrahieren. Andererseits ist es in diesem Sammelsurium natürlich besonders schwierig, relevante Einträge zu finden.
- `/var/log/kern.log` enthält alle Kernelmeldungen.
- Die Nachrichten des Mail-Systems (z. B. Postfix) werden über mehrere Dateien verteilt. In `mail.log` werden *alle* Nachrichten gespeichert, in `mail.err` nur Fehlermeldungen.
- Kritische Systemmeldungen, z. B. über einen bevorstehenden Shutdown oder über Kernelfehler, werden durch `:omusrmsg:*` an alle Benutzer weitergeleitet, genau genommen an alle Terminalfenster und Konsolen. `omusrmsg` ist ein rsyslog-Modul, um Nachrichten an Benutzer zu senden.
- Außerdem werden diverse Warnungen und Fehlermeldungen an das X-System weitergeleitet. Um diese Meldungen unter X zu verfolgen, starten Sie das Programm `xconsole`. Es sieht wie ein kleines Terminalfenster aus, erlaubt aber keine Eingaben.

Damit Änderungen an der Syslog-Konfiguration wirksam werden, muss der Syslog-Dienst neu gestartet werden!

```
root#  service rsyslog restart
```

logger

Mit dem Kommando `logger` können Sie selbst in einem Script Syslog-Nachrichten aufzeichnen oder neue Syslog-Regeln testen. Normalerweise verwenden Sie das Kommando wie folgt:

```
user$  logger -t tag -p authpriv.info "xxx has a new password"
```

Anstelle von `tag` können Sie ein beliebiges Schlüsselwort angeben, das Ihnen später bei der Suche in den Logging-Dateien hilft. Mit `-p` geben Sie den Selektor an. Syslog fügt Ihrer Nachricht automatisch Zeitinformationen hinzu. In der betreffenden Logging-Datei sieht der vorhin erzeugte Eintrag dann so aus:

```
Jun 16 07:55:03 localhost tag: xxx has a new password
```

Kernel-Logging

Meldungen des Kernels werden in einen 16 kByte großen Ringpuffer im RAM geschrieben. Wenn dieser Puffer voll ist, werden alte Nachrichten gelöscht, um Platz für neue Nachrichten zu schaffen. Den Inhalt dieses Ringpuffers können Sie mit `dmesg` ansehen. Wenn Sie dabei die Option `-c` angeben, wird der Ringpuffer gleichzeitig geleert.

Alle Kernelnachrichten werden außerdem in die virtuelle Datei `/proc/kmsg` geschrieben. Diese Datei dient zur Weitergabe der Kernelnachrichten an Syslog.

Den `dmesg`-Kernelmeldungen ist oft eine Zeitangabe in der Form `[nnn.nnnnnn]` vorangestellt. Die Zahl vor dem Komma gibt die Anzahl der Sekunden seit dem Systemstart an, die weiteren sechs Stellen präzisieren die Zeitangabe auf millionstel Sekunden. Bei der Speicherung der Kernelmeldungen in einer Logging-Datei wird diese Zeitangabe in der Regel durch die absolute Zeit ergänzt.

Init-Meldungen

Meldungen des Init-Systems (siehe Kapitel 27) werden leider nur bei wenigen Distributionen aufgezeichnet. Zu den positiven Ausnahmen zählen Fedora und RHEL (Datei `/var/log/boot.log`).

logrotate

Logging-Dateien werden nach und nach immer größer. Um den Speicherbedarf der Logging-Dateien unter Kontrolle zu behalten, bietet sich `logrotate` an. Dieses Programm wird bei vielen Distributionen einmal täglich durch das Cron-Script `/etc/cron.daily/logrotate` aufgerufen. Es verarbeitet dann alle Logging-Dateien, die in den Konfigurationsdateien in `/etc/logrotate.d` beschrieben sind. Wie `logrotate` mit den Logging-Dateien umgeht, hängt im Detail von der jeweiligen Programmkonfiguration ab. Die prinzipielle Vorgehensweise ist aber immer dieselbe und sieht so aus:

- Logrotate benennt die aktuelle Logging-Datei um. Aus `name` wird `name.0`.
- Logrotate erzeugt eine neue, leere Logging-Datei `name`.
- Bei vielen Server-Diensten fordert Logrotate den Dämon durch `service name reload` dazu auf, die Konfiguration neu einzulesen. Bei dieser Gelegenheit erkennt der Dämon, dass es eine neue, leere Logging-Datei gibt, und verwendet nun diese.
- Logrotate komprimiert `name.0` oder `name.1` (Option `delaycompress`). `delaycompress` vermeidet Konflikte zwischen dem Dämon, der vielleicht noch in `name.0` schreibt, und dem Komprimierkommando.
- Logrotate benennt bereits vorhandene Logging-Archive um. Aus `name.4.gz` wird `name.5.gz`, aus `name.3.gz` wird `name.4.gz` etc. Dieser Vorgang wird »rotieren« genannt und gibt dem Paket seinen Namen.
- Wenn es mehr als eine vorgegebene Maximalanzahl von Logging-Archiven gibt, werden die ältesten Archivdateien gelöscht.

Konfiguration

`/etc/logrotate.conf` enthält einige Defaulteinstellungen für Logrotate. Diese Einstellungen gelten nur, soweit die programmspezifischen Konfigurationsdateien keine abweichenden Daten enthalten.

/etc/logrotate.d enthält Detaileinstellungen zu diversen Programmen, die Logging-Dateien produzieren. Diese Dateien stammen nicht aus dem Logrotate-Paket, sondern aus den Paketen des jeweiligen Programms. Das samba-Paket stellt also beispielsweise /etc/logrotate.d/samba zur Verfügung. Das stellt sicher, dass die Dateien zur jeweils installierten Programmversion passen und dass Logrotate den jeweiligen Server-Dienst über das Umbenennen der Logging-Dateien informiert bzw. neu startet.

Die folgenden Zeilen zeigen als Beispiel die logrotate-Konfiguration für Apache unter Ubuntu: Logrotate bearbeitet die Logging-Dateien einmal pro Woche. Die Logging-Dateien werden umbenannt und komprimiert. Dabei werden auch die Zugriffsrechte neu eingestellt, sodass die Logging-Dateien nur noch von root sowie Mitgliedern der adm-Gruppe gelesen werden können. Das Archiv ist auf 52 Dateien limitiert, d. h., Sie können bei Bedarf auf alle Logging-Daten eines ganzen Jahres zurückgreifen. Sofern Apache läuft, wird es durch reload davon informiert, dass es neue Logging-Dateien gibt.

```
# Datei /etc/logrotate.d/apache
/var/log/apache2/*.log {
   weekly
   missingok
   rotate 52
   compress
   delaycompress
   notifempty
   create 640 root adm
   sharedscripts
   postrotate
      if [ -f "`. /etc/apache2/envvars ; \
               echo ${APACHE_PID_FILE:-/var/run/apache2.pid}`" ]; then
         /etc/init.d/apache2 reload > /dev/null
      fi
   endscript
}
```

logwatch

Das manuelle Lesen der Logging-Dateien mag die ersten Tage oder während der Suche nach einem Fehler ganz interessant sein; nach kurzer Zeit werden Sie aber wie jeder andere Server-Administrator die Lust am Logging-Studium verlieren und Ihre Logging-Dateien mehr und mehr vernachlässigen! Automatisierte Tools zur Logging-Auswertung sollen hier Abhilfe schaffen. Exemplarisch stelle ich hier das Programm logwatch vor, das bei den meisten Distributionen als Paket mitgeliefert wird.

Nach der Installation wird Logwatch einmal täglich durch `/etc/cron.daily/*logwatch` ausgeführt. Es wertet die Einträge der Logging-Dateien für die letzten 24 Stunden aus, fasst die relevanten Informationen in einer E-Mail zusammen und versendet diese an `root`.

Logging-Updates per E-Mail

Logwatch setzt voraus, dass auf Ihrem Rechner ein E-Mail-Server läuft, um die Logging-Zusammenfassung zu versenden! Wenn während der Logwatch-Installation Postfix installiert wird und Sie nur lokale E-Mails verarbeiten möchten, also keinen richtigen E-Mail-Server einrichten möchten, wählen Sie die Konfigurationsoption NUR LOKAL (siehe auch Abschnitt 37.2). Standardmäßig werden `root`-E-Mails an den Standardbenutzer laut `/etc/aliases` weitergeleitet. Lokale E-Mails lesen Sie am einfachsten mit Mutt (siehe Abschnitt 8.8).

Die Logging-Zusammenfassung ist üblicherweise etliche Seiten lang – eigentlich zu lang, um sie täglich vollständig zu lesen. Der Textumfang hängt davon ab, wie viele Server-Dienste installiert sind und wie viele Ereignisse während des letzten Tages protokolliert worden sind. Die folgenden Zeilen zeigen eine aus Platzgründen stark gekürzte Logwatch-E-Mail:

```
Logwatch 7.4.0 (03/01/11)
Processing Initiated: Tue Jul 10 06:25:02 2012
Date Range Processed: yesterday

---------- Denyhosts Begin ------------------------

new denied hosts:
    60.12.251.5
    222.45.235.70

---------- pam_unix Begin ------------------------

sshd:
   Authentication Failures:
      root (222.45.235.70): 7 Time(s)
      root (60.12.251.5): 3 Time(s)
      unknown (60.12.251.5): 1 Time(s)
   Invalid Users:
      Unknown Account: 1 Time(s)

---------- Postfix Begin ------------------------

   3.347K  Bytes accepted                              3,427
   2.343K  Bytes sent via SMTP                         2,399
   4.910K  Bytes delivered                             5,028
```

```
--------------------- SSHD Begin ------------------------

Failed logins from:
   60.12.251.5: 3 times
   222.45.235.70: 7 times
Illegal users from:
   undef: 1 time
   60.12.251.5: 1 time
...

--------------------- Disk Space Begin ------------------------

Filesystem              Size  Used Avail Use% Mounted on
/dev/mapper/vg0-root     20G  1.2G   18G   6% /
/dev/mapper/vg0-var      20G  723M   19G   4% /var
/dev/mapper/vg0-backup  100G   12G   84G  13% /backup
/dev/md0               1016M   75M  890M   8% /boot
```

Konfiguration

Vielleicht wundern Sie sich, warum Logwatch wie von Zauberhand ohne jede Konfiguration funktioniert. Der Grund ist einfach: Zusammen mit Logwatch wird eine Standardkonfiguration in das Verzeichnis `/usr/share/logwatch/default.conf` installiert. Die dort befindliche Datei `logwatch.conf` enthält einige globale Grundeinstellungen. Dort ist beispielsweise eingestellt, an wen die Zusammenfassung gesendet wird (`MailTo = root`), für welchen Zeitraum die Logging-Dateien ausgewertet werden sollen (`Range = yesterday`), wie detailliert die Zusammenfassung sein soll (`Detail = Low`) etc.

Außerdem enthalten die Dateien `default.conf/services/*.conf` Konfigurationseinstellungen für zahlreiche Server-Dienste, z. B. für Apache, Postfix, ClamAV, Dovecot, Sendmail, SSH etc. Diese Konfigurationsdateien werden natürlich nur wirksam, sofern die betreffenden Dienste tatsächlich laufen. Relevante Ergebnisse erhalten Sie zudem nur, wenn Sie die Orte der Standard-Logging-Dateien nicht verändert haben.

Das Verzeichnis `/usr/share/logwatch/dist.conf` ist für distributionsspezifische Änderungen gegenüber der Standardkonfiguration vorgesehen. Hier durchgeführte Einstellungen haben Vorrang gegenüber der Standardkonfiguration.

Um die Konfiguration selbst zu ändern, kopieren Sie die betreffende Datei in das entsprechende Verzeichnis in `/etc/watchlog` und modifizieren sie dort. Es reicht aus, wenn diese Datei nur die Änderungen gegenüber dem Original enthält. Zum Ausprobieren führen Sie anschließend Logwatch manuell aus:

```
root#  logwatch --mailto name@host
```

Journal (Systemd)

Das in Kapitel 27 beschriebene Init-System Systemd enthält eigene Logging-Funktionen, das sogenannte »Journal«. Für die Protokollierung ist der Hintergrundprozess `systemd-journald` verantwortlich. Im Vergleich zu Syslog gibt es zwei große Unterschiede:

- Das Journal wird in einem binären Format gespeichert. Das spart Platz und somit Zeit.
- Das Journal ist gegen nachträgliche Änderungen geschützt. Damit ist es für einen Einbrecher unmöglich, seine Spuren zu beseitigen:

  https://plus.google.com/115547683951727699051/posts/g1E6AxVKtyc

Trotz dieser offensichtlichen Vorteile wird es wohl einige Zeit dauern, bis sich das Journal in allen Distributionen durchsetzen kann. Der Hauptgrund besteht darin, dass unzählige Tools voraussetzen, dass die Logging-Dateien im Textformat vorliegen und unkompliziert mit `grep` ausgewertet werden können.

Fedora Zu den ersten Distributionen, die Gebrauch vom Journal machen, gehört natürlich Fedora. Kernelmeldungen sowie Systemd-Nachrichten werden dort in der binären Protokolldatei `/run/log/journal/`*`uuid`*`/system.journal` gespeichert. Das Protokoll kann mit dem Kommando `journalctl` ausgelesen werden. Beachten Sie, dass sich das Verzeichnis `/run` in einem temporären Dateisystem befindet; die Logging-Dateien gehen daher mit jedem Neustart verloren.

Das Journal läuft momentan parallel zu Syslog. `/var/log/messages`, `/var/log/secure` etc. liegen also weiterhin im Textformat vor und werden bleibend gespeichert.

Kapitel 22
Software- und Paketverwaltung

Unter Windows ist es üblich, neue Programme durch das Ausführen von `setup.exe` zu installieren. Linux verfolgt einen ganz anderen Ansatz: Mit einem Paketverwaltungssystem wird eine Datenbank verwaltet, die Informationen über alle bereits installierten Software-Pakete enthält. Neue Programme werden durch die Kommandos des Paketverwaltungssystems installiert.

Dieses Konzept hat eine Menge Vorteile: So können Abhängigkeiten und Konflikte zwischen Software-Paketen berücksichtigt werden. Wenn beispielsweise ein Programm A die Bibliothek B voraussetzt, lässt das Paketverwaltungssystem die Installation von A erst zu, nachdem B installiert worden ist. Es lässt sich jederzeit nachvollziehen, zu welchem Paket eine bestimmte Datei gehört, ob sich diese Datei noch im ursprünglichen Zustand befindet etc.

Paketformate

Der Linux-Markt wird von zwei verschiedenen Paketverwaltungssystemen dominiert:

- **RPM:** Red Hat, Fedora, Mandriva, SUSE sowie zahllose weitere Distributionen verwenden das von Red Hat entwickelte Paketformat RPM.
- **DEB:** Debian und alle davon abgeleiteten Distributionen nutzen dagegen das Paketformat DEB.

Die Kommandos zur Installation, Deinstallation und zum Update dieser Pakete (`rpm`, `dpkg` etc.) sind allerdings relativ primitiv. Sie können weder Pakete aus Paketquellen herunterladen noch Paketabhängigkeiten auflösen.

Paketverwaltungssysteme

Deswegen entstanden aufbauend auf `rpm` bzw. `dpkg` neue Paketverwaltungssysteme mit einer Menge Zusatzfunktionen. Dazu zählen die automatische Installation abhängiger Pakete, die Durchführung von Updates für das gesamte System und die Berücksichtigung von Paketquellen aus dem Internet. Beispiele für derartige Paketverwaltungssysteme sind Yum und ZYpp für RPM-Pakete sowie APT und Aptitude für DEB-Pakete.

Distributionsspezifische Werkzeuge

Ergänzend zu diesen Standardprogrammen gibt es bei manchen Distributionen eigene Programme zur Paketverwaltung und zur Durchführung von Updates:

Debian, Ubuntu:	`update-manager`
Fedora, RHEL 6:	`packagekit`
SUSE:	YaST-Module der Gruppe SOFTWARE
Ubuntu:	Ubuntu Software Center, `gnome-language-selector`

Nicht nur die Paketverwaltungswerkzeuge unterscheiden sich von Distribution zu Distribution, auch sonst gibt es trotz gemeinsamer Standards viele distributionsspezifische Eigenheiten. Diese sind in Abschnitt 22.10 zusammengefasst.

Vermeiden Sie es, Pakete unterschiedlicher Distributionen zu mischen

Die Pakete einer Linux-Distribution sind aufeinander abgestimmt. Das bedeutet, dass sie einheitliche Bibliotheken nutzen, mit demselben Compiler kompiliert wurden etc. Als Linux-Einsteiger sind Sie deshalb gut beraten, nur Pakete zu installieren, die für Ihre Distribution gedacht sind. Nicht zu empfehlen ist die Installation eines Red-Hat-Pakets unter SUSE (oder umgekehrt). Die dabei auftretenden Probleme, wie fehlende Bibliotheken oder nicht erfüllte Paketabhängigkeiten, lassen sich – wenn überhaupt – nur von Linux-Profis beheben.

Nachteile der Paketverwaltung

Die Paketverwaltung gängiger Distributionen funktioniert gut, ist aber auch mit Nachteilen verbunden:

- Die bei vielen Distributionen beinahe täglichen Updates verunsichern Anwender, die von Windows oder Mac OS X größere Update-Zeitspannen gewohnt sind.
- Der Download-Bedarf für die Updates ist groß. Mehrere Hundert MByte pro Monat sind nicht unüblich.
- Viele Linux-Anwender würden eine Distribution gerne länger verwenden, dabei aber einige wenige Programme aktualisieren – oft Desktop-Anwendungen wie LibreOffice oder Gimp. Genau das machen gängige Distributionen so gut wie unmöglich. Es werden zwar Sicherheits-Updates angeboten, nicht aber grundlegend neue Versionen.

  Wenn Sie in einer älteren Distribution die neueste Version von LibreOffice nutzen möchten, müssen Sie eine manuelle Installation durchführen oder auf nicht offizielle Paketquellen zurückgreifen. Beides ist nur fortgeschrittenen Benutzern zu empfehlen. Unter Windows oder Mac OS X ist es ungleich einfacher, die gerade aktuelle LibreOffice-Version zu installieren.

  Es gibt technische Gründe, warum das so ist: Die meisten Linux-Programme verwenden unzählige Bibliotheken. Ein Versions-Update von LibreOffice setzt voraus, dass auch einige Bibliotheken aktualisiert werden müssen. Das kann

Inkompatibilitäten mit anderen Programmen auslösen, die ebenfalls auf diese Bibliothek zurückgreifen.

Ein möglicher Ausweg besteht darin, bei wichtigen Programmen die dazugehörigen Bibliotheken zu integrieren. Google Chrome hat diesen Weg von Anfang an beschritten, und auch die Firefox- und Thunderbird-Pakete aktueller Distributionen werden mittlerweile so gewartet. Aber auch diese Vorgehensweise ist mit Nachteilen verbunden: Aufgrund der nun unvermeidlichen Redundanzen steigen der Platzbedarf auf der Festplatte, das Download-Volumen bei jedem Update und der RAM-Bedarf bei der gleichzeitigen Ausführung mehrerer Programme. Tritt in einer Bibliothek ein Sicherheitsproblem auf, kann es nicht mehr zentral behoben werden. Vielmehr müssen alle Programme, die diese Bibliothek verwenden, aktualisiert werden.

Zentrale Administration

Wenn Sie für 50, 100 oder 1000 Linux-Rechner verantwortlich sind, wird die Administration und Paketverwaltung trotz der in diesem Kapitel vorgestellten Werkzeuge zur Qual. Sie benötigen ein Werkzeug, um zentral auf allen oder auf zuvor ausgewählten Rechnern ein Update durchzuführen, ein neues Programm zu installieren oder die Konfiguration zu verändern. Je nach Distribution bieten sich hierfür Red Hat Network, ZENworks (Novell/SUSE), m23 (Debian) oder Landscape (beide Ubuntu) an.

http://www.redhat.com/rhn
http://www.novell.com/de-de/products/zenworks/configurationmanagement
http://m23.sourceforge.net
http://www.canonical.com/enterprise-services/ubuntu-advantage/landscape

tar-Pakete

Das Kommando `tar` hilft dabei, eine Menge Dateien zu einem Archiv zusammenzufassen bzw. ein derartiges Archiv wieder auszupacken. In den Anfangszeiten von Linux, noch bevor es die Paketformate RPM und DEB gab, verwendeten die meisten Distributionen `tar`-Archive wie Pakete. Selbst heute gibt es noch Distributionen, die `tar`-Archive als Paketersatz verwenden, z. B. Slackware.

Aber auch für alle anderen Distributionen spielen `tar`-Archive eine gewisse Rolle im Alltag fortgeschrittener Linux-Anwender: Viele Software-Entwickler, die keine Lust dazu haben, RPM- oder DEB-Pakete zu erzeugen, stellen stattdessen einfache `tar`-Archive mit allen erforderlichen Dateien zur Verfügung. Das Archiv muss lediglich am richtigen Ort mit `tar czf name.tgz` ausgepackt werden – schon ist das Programm installiert. Allerdings führt `tar` an der Paketverwaltung Ihrer Distribution vorbei! Ein so installiertes Programm lässt sich schwer aktualisieren, nicht deinstallieren und kann Konflikte verursachen. Die Installation von `tar`-Paketen ist daher nur zu empfehlen, wenn Sie wissen, was Sie tun, und wenn das gewünschte Programm in keiner anderen Form verfügbar ist.

Sonstige Paketformate

Neben den in diesem Buch behandelten RPM- und DEB-Paketformaten gibt es einige weitere, die bis jetzt aber keine große Bedeutung erlangt haben. Zu den wichtigsten Zielen neuer Paketformate zählt eine höhere Distributionsunabhängigkeit sowie die Möglichkeit, Pakete bzw. Software ohne `root`-Rechte in lokale Benutzerverzeichnisse zu installieren. Weitere Informationen finden Sie unter:

http://0install.net

22.1 RPM-Paketverwaltung

Das Kommando `rpm` installiert und verwaltet RPM-Pakete. Es hilft dabei,

- im Rahmen einer Installation automatisch Änderungen in schon vorhandenen Dateien durchzuführen (etwa in Script-Dateien).
- ein Programm durch eine aktuellere Version zu ersetzen, wobei von geänderten Dateien automatisch Updates erstellt werden.
- alle Dateien eines Programms wieder zu entfernen.
- sicherzustellen, dass vor der Installation eines Programms alle Voraussetzungen erfüllt sind, dass also alle erforderlichen Bibliotheken in der richtigen Version zur Verfügung stehen.
- zu überprüfen, ob eine Datei seit der Installation des Pakets verändert wurde.
- festzustellen, zu welchem Paket eine bestimmte Datei gehört.

Die erforderlichen Verwaltungsinformationen befinden sich in jedem RPM-Paket. Bei der Installation werden diese Informationen in eine Datenbank eingetragen, deren Dateien sich im Verzeichnis `/var/lib/rpm` befinden.

Grundlagen

Die meisten RPM-Pakete werden in zwei Varianten zur Verfügung gestellt: als Binärpaket und als Quellcodepaket. Das Binärpaket enthält die zur Ausführung des Programms notwendigen Dateien. Das Quellcodepaket ist nur für Entwickler interessant. Es enthält den Quellcode, der erforderlich war, um das Binärpaket zusammenzustellen.

Der Paketname enthält ziemlich viele Informationen: `abc-2.0.7-1.i686.rpm` bezeichnet beispielsweise das Paket `abc` mit der Versionsnummer 2.0.7, Release-Nummer 1. Falls bei der Zusammenstellung eines Pakets ein Fehler aufgetreten ist, zusätzliche Online-Dokumentation beigefügt wurde oder andere Änderungen durchgeführt

wurden, entstehen Release-Ziffern größer als 1 für eine bestimmte Versionsnummer. Die Versionsnummer bezieht sich also auf das eigentliche Programm, die Release-Nummer auf die `rpm`-Zusammenstellung.

Die Kennung `i686` weist darauf hin, dass das Paket Binärdateien für Pentium-II-kompatible Prozessoren enthält. Wenn das Paket `abc` Script- oder Textdateien enthält, die von der CPU-Architektur unabhängig sind, wird statt der CPU-Kennung das Kürzel `noarch` verwendet. Wenn das Paket den Quellcode enthält, ist stattdessen das Kürzel `src` üblich.

Metadaten

Die Paketdatei enthält neben den zu installierenden Dateien zahlreiche Verwaltungsinformationen: eine kurze Paketbeschreibung, abermals Informationen über Versionsnummern, die Einordnung in die Gruppenhierarchie, Abhängigkeiten von anderen Paketen etc. Abhängigkeiten bestehen dann, wenn ein Paket eine bestimmte Programmiersprache, wie Perl, oder eine bestimmte Library voraussetzt. In diesem Fall müssen zuerst diese Pakete installiert werden.

`rpm` verwaltet eine Datenbank mit Informationen über alle installierten Binärpakete. Diese Datenbank wird in diversen Dateien im Verzeichnis `/var/lib/rpm` gespeichert. Die Datenbank enthält nur Informationen zu Binärpaketen; eventuell auch installierte Pakete mit Quellcode werden nicht in die Datenbank aufgenommen.

Damit die RPM-Datenbank mit der tatsächlichen Installation übereinstimmt, dürfen Pakete nicht einfach durch Löschen der Dateien, sondern müssen durch ein Deinstallieren (`rpm -e`) entfernt werden!

Delta-RPM-Pakete

Um ein RPM-Paket zu aktualisieren, wird oft das gesamte neue Paket heruntergeladen. Gerade bei Sicherheits-Updates, bei denen oft nur winzige Änderungen an wenigen Dateien erforderlich sind, ist das ineffizient. Aus diesem Grund gibt es Delta-RPM-Pakete, die nur die Änderungen gegenüber einer bestimmten Version des Pakets enthalten.

Die Anwendung von Delta-RPMs ist grundsätzlich einfach: Zuerst erzeugt das Kommando `applydeltarpm` aus dem Delta-RPM und dem Original-Paket bzw. dessen installierten Dateien das neue, aktualisierte RPM-Paket. Dieses wird dann ganz normal installiert (`rpm -U`). `applydeltarpm` ist Teil des Pakets `deltarpm`.

`applydeltarpm` setzt voraus, dass momentan eine ganz bestimmte Version des Pakets installiert ist. Ist das nicht der Fall bzw. wurden deren Dateien nach der Installation verändert, ist zur Durchführung des Updates die Original-RPM-Datei erforderlich.

32/64-Bit-Probleme

Bei 64-Bit-Distributionen kann es vorkommen, dass `rpm -qi name` trotz eines eindeutigen Paketnamens Informationen zu *zwei* Paketen auflistet. Das ist kein Fehler;

vielmehr handelt es sich um zwei gleichnamige Pakete mit den Dateien der 32- und der 64-Bit-Variante eines Programms bzw. einer Bibliothek.

SUSE vermeidet gleichnamige Pakete mit unterschiedlichem Inhalt, indem es die 32-Bit-Varianten im Paketnamen mit dem Anhang `32bit` kennzeichnet. `rpm -qa | grep 32bit` liefert dort eine Liste aller 32-Bit-Pakete, die aus Kompatibilitätsgründen erforderlich sind.

RPM-Datenbank reparieren

In seltenen Fällen passiert es, dass die RPM-Datenbank inkonsistente Daten enthält. Das äußert sich darin, dass das `rpm`-Kommando nicht mehr verwendet werden kann bzw. Fehlermeldungen wie *cannot open packages database* liefert. Abhilfe schaffen meistens die Kommandos `rm -f /var/lib/rpm/__db*` und dann `rpm --rebuilddb`. Damit wird die RPM-Datenbank neu erzeugt. Das dauert allerdings eine Weile.

Das rpm-Kommando

Es mag auf den ersten Blick überraschend wirken, aber Sie werden mit dem `rpm`-Kommando selten ein Paket installieren oder wieder entfernen. Dazu setzen Sie in aller Regel `yum`, `zypper` oder eine grafische Benutzeroberfläche ein, und `rpm` kommt nur hinter den Kulissen zum Einsatz.

Der praktische Nutzen des `rpm`-Kommandos liegt heute primär darin, die Paketdatenbank auszulesen und daraus Informationen zu extrahieren, die Ihnen `yum` oder `zypper` gar nicht oder nur viel umständlicher geben. Tabelle 22.1 fasst die wichtigsten `rpm`-Kommandos zusammen. Die folgenden Beispiele zeigen die praktische Anwendung.

Beispiele

Nehmen Sie an, Sie entdecken im `/etc`-Verzeichnis eine Datei, die Ihnen bisher noch nie aufgefallen ist und von der Sie wissen möchten, welchen Zweck sie hat. `rpm -qf` verrät, zu welchem Paket sie gehört. `rpm -qi` liefert eine kurze Beschreibung des Pakets, und `rpm -ql` zeigt alle anderen Dateien, die ebenfalls von diesem Paket stammen:

```
user$  rpm -qf /etc/login.defs
shadow-utils-4.1.5.1-5.fc19.x86_64
user$  rpm -qi shadow-utils
Name        : shadow-utils
Summary     : Utilities for managing accounts and shadow password files
...
```

```
user$  rpm -ql shadow-utils
/etc/default/useradd
/etc/login.defs
/usr/bin/chage
...
```

Vielleicht möchten Sie wissen, welche `perl`-Pakete installiert sind. `rpm -qa` liefert eine Liste aller installierten Pakete. Mit `grep` filtern Sie daraus die interessanten Pakete heraus; `sort` sortiert die Liste:

```
user$  rpm -qa | grep perl
perl-5.16.3-265.fc19.x86_64
perl-Carp-1.26-243.fc19.noarch
perl-Data-Dumper-2.145-1.fc19.x86_64
...
```

Perl macht Schwierigkeiten, und Sie sind sich nicht sicher, ob das Perl-Paket korrekt installiert ist. Sind noch alle installierten Dateien dieses Pakets im Originalzustand? Die Antwort gibt `rpm -V`. Es listet alle Dateien auf, die sich geändert haben:

```
user$  rpm -V perl
S.5....T.    /usr/share/perl5/utf8.pm
```

Unter Fedora oder RHEL können Sie das Paket nun mit `yum reinstall` reparieren:

```
root#  yum reinstall perl
```

Aufgabe	Kommando
Paket installieren	`rpm -i datei.rpm`
Paket aktualisieren	`rpm -U datei.rpm`
Paketinstallation überprüfen (verify)	`rpm -V datei.rpm`
Paket entfernen	`rpm -e paketname`
Alle installierten Pakete ermitteln	`rpm -qa`
Paket ermitteln, das diese Datei zur Verfügung stellt	`rpm -qf datei`
Paketbeschreibung anzeigen	`rpm -qi paketname`
Liste aller Dateien des Pakets ermitteln	`rpm -ql paketname`
Liste aller Konfigurationsdateien des Pakets ermitteln	`rpm -qc paketname`
Informationen zu einem noch nicht installierten Paket ermitteln	`rpm -qpli datei.rpm`

Tabelle 22.1 Wichtige rpm-Kommandos

22.2 Yum

Yum ist ein Programm, das die Verwaltung von RPM-Paketen vereinfacht. Es wird von vielen RPM-basierten Kommandos zur Paketverwaltung verwendet, z. B. von Fedora und RHEL. Yum bietet eine Menge Zusatzfunktionen:

- Als Datenquelle (*repository*) dienen Yum-Archive im Internet. Das ist eine Sammlung von RPM-Paketen, zu denen im Verzeichnis `repodata` zusätzliche Metadaten gespeichert sind. Sie geben Informationen über den Inhalt und die Abhängigkeiten aller Pakete.
- Yum kann mehrere Mirrors für eine Paketquelle verwalten und versucht, den gerade schnellsten Mirror zu verwenden.
- Yum löst Paketabhängigkeiten auf, lädt alle erforderlichen Pakete und installiert sie. Wenn Sie beispielsweise ein Paket aus der Paketquelle A installieren, kann es sein, dass Yum nach einer Rückfrage abhängige Pakete aus den Quellen B und C herunterlädt und ebenfalls installiert.
- Yum kann alle bereits installierten Pakete mit einem einzigen Kommando aktualisieren. Dazu wird für jedes Paket getestet, ob es in einer der registrierten Paketquellen eine neuere Version des Pakets gibt. Wenn das der Fall ist, werden die entsprechenden Pakete heruntergeladen und installiert. Natürlich werden auch dabei alle Paketabhängigkeiten aufgelöst.

Locking-Konflikte

Es ist nicht zulässig, mehrere Yum-Instanzen parallel auszuführen. Wenn bereits ein Yum-Kommando oder -Programm läuft, führt ein neuerlicher Start zur Fehlermeldung *another copy is running*.

Konfiguration

Die Grundkonfiguration von Yum erfolgt durch die Datei `/etc/yum.conf`. Die folgenden Zeilen zeigen auszugsweise die Konfiguration von Fedora:

```
# Datei /etc/yum.conf
[main]
cachedir=/var/cache/yum/$basearch/$releasever
keepcache=0
debuglevel=2
logfile=/var/log/yum.log
exactarch=1
obsoletes=1
gpgcheck=1
plugins=1
installonly_limit=3
color=never
```

Kurz eine Erläuterung zu den wichtigsten Einstellungen: `keepcache=0` bewirkt, dass heruntergeladene Pakete nach der Installation nicht archiviert werden. In der Regel ist das eine zweckmäßige Einstellung, weil der Platzbedarf für die Pakete im Laufe der Zeit recht groß wird und normalerweise kein Grund dazu besteht, die Pakete ein zweites Mal zu installieren. Es kann allerdings passieren, dass `yum` während der Installation ein Problem feststellt und die Installation abbricht. Auch in diesem Fall werden die heruntergeladenen Pakete gelöscht. Wenn Sie das Problem beheben können und anschließend das Update wiederholen, müssen alle Pakete neuerlich heruntergeladen werden. Diese Situation vermeiden Sie mit `keepcache=1`. Um die heruntergeladenen Pakete in `/var/cache/yum` explizit zu löschen, führen Sie `yum clean packages` aus.

`exactarch=1` bewirkt, dass Yum nur Updates berücksichtigt, bei denen die Architektur mit dem bereits installierten Paket übereinstimmt. i386-Pakete können also nicht durch neuere x86_64-Pakete ersetzt werden.

`gpgcheck=1` bewirkt, dass Yum mit einem Schlüssel die Authentizität der Pakete sicherstellt. `gpgcheck` kann abweichend von der Einstellung in `yum.conf` auch individuell für jede Paketquelle eingestellt werden. `plugins` entscheidet, ob Yum Plugins berücksichtigt.

Es gibt Pakete, die Yum installieren, aber nicht aktualisieren soll. Dazu zählen insbesondere Kernelpakete: Bei einem Kernel-Update wird das neue Kernelpaket zusätzlich installiert, ohne das alte Kernelpaket anzurühren. Mit der Variable `installonlypkgs` werden die Namen derartiger Pakete eingestellt. Standardmäßig hat diese Variable die Einstellung `kernel`, `kernel-smp`, `kernel-bigmem`, `kernel-enterprise`, `kernel-debug`, `kernel-unsupported`. Die in `yum.conf` enthaltene Variable `installonly_limit` steuert schließlich, wie viele Versionen derartiger Pakete parallel installiert werden. Die Standardeinstellung `3` bewirkt, dass immer nur die aktuellsten drei Kernelversionen installiert bleiben. Ältere Kernelpakete werden entfernt.

`color=never` bewirkt, dass das Kommando `yum` im Terminal keine Farben nutzt. Wenn Sie das möchten, verwenden Sie `color=always`.

Paketquellen einrichten

Jede Paketquelle wird in einer eigenen `*.repo`-Datei im Verzeichnis `/etc/yum.repos.d` definiert. Die folgenden Zeilen zeigen die Paketquelle für die Basispakete von Fedora:

```
# Datei /etc/yum.repos.d/fedora.repo
[fedora]
name=Fedora $releasever - $basearch
failovermethod=priority
mirrorlist=https://mirrors.fedoraproject.org/\
  metalink?repo=fedora-$releasever&arch=$basearch
enabled=1
metadata_expire=7d
```

```
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch
```

Die Adresse der Paketquelle kann wahlweise absolut mit `baseurl=...` oder mit `mirrorlist=...` in Form einer Mirror-Datei angegeben werden. Diese Datei enthält eine Liste von Mirror-Servern. Yum entscheidet sich selbstständig für einen der Mirrors. Yum ersetzt in der Konfigurationsdatei die Variablen `$releasever`, `$arch` und `$basearch` durch die Versionsnummer der Linux-Distribution und deren Architektur. Kurz zur Herkunft dieser drei Variablen:

- `$arch` wird mit dem Kommando `uname` ermittelt (genau genommen mit der gleichnamigen, auf `uname` basierenden Python-Funktion) und liefert beispielsweise auf einem 64-Bit-Intel/AMD-Rechner `x86_64`.
- `$basearch` ist die `$arch` zugrunde liegende Basisarchitektur (beispielsweise `i386`).
- `$releasever` ergibt sich aus der Versionsnummer des Pakets `redhat-release` bzw. `fedora-release`. Es besteht die Möglichkeit, in `yum.conf` mit dem Schlüsselwort `distroverpkg` den Namen eines anderen Pakets anzugeben. Die Versionsnummer dieses Pakets gilt dann als Versionsnummer der Distribution.

`metadata_expires` gibt an, wie lange die von einer Paketquelle heruntergeladenen Metadaten gültig sind. Yum speichert die Metadaten in einem Cache und verzichtet auf ein neuerliches Herunterladen, wenn die Metadaten noch nicht veraltet sind. Das spart Zeit und Download-Volumen, kann aber dazu führen, dass Yum kürzlich durchgeführte Änderungen in der Paketquelle ignoriert. Gegebenenfalls erzwingen Sie durch `yum clean metadata` das Löschen der lokalen Metadaten. Damit ist Yum beim nächsten Mal gezwungen, die Metadaten aller Paketquellen neu einzulesen.

Die optimale Einstellung für `metadata_expires` variiert je nach Paketquelle: Bei Paketquellen, die sich selten oder nie ändern, ist ein langer Zeitraum zweckmäßig. Bei Update-Paketquellen ist es dagegen besser, einen kurzen Zeitraum anzugeben oder ganz auf eine Einstellung zu verzichten.

Pakete sperren

Wenn Sie möchten, dass bestimmte Pakete von Yum nicht angetastet und beim Vorliegen einer neuen Version auch nicht aktualisiert werden, fügen Sie in `yum.conf` oder in die `*.repo`-Datei der Paketquelle eine Zeile mit `exclude name1 name2 name3` ein. In den Paketnamen können Sie Jokerzeichen verwenden, d. h., auch `exclude xemacs*` ist erlaubt.

Plugins

Yum lässt sich durch Plugins erweitern und bietet dann noch mehr Funktionen. Die Konfiguration der Plugins erfolgt durch Dateien im Verzeichnis `/etc/yum/pluginconf.d`.

Presto

Presto ermöglicht die Verwendung von Delta-RPMs für Updates. Der Download-Umfang von Updates sinkt um 60 bis 80 Prozent, allerdings ist die CPU-Belastung während der Anwendung der Updates höher. Bis Fedora 18 war Presto ein Yum-Plugin, mit Fedora 19 wurde es direkt in Yum integriert.

Fastest Mirror

Yum versucht, immer den »besten« Mirror zum Download von Paketen zu verwenden. Das gelingt allerdings nicht immer. Gegebenenfalls können Sie die Fastest-Mirror-Logik manuell optimieren. Dazu erzeugen Sie die Datei `/etc/yum/pluginconf.d/fastestmirror.conf` und schließen darin einzelne besonders lahme Server mit `exclude` aus:

```
# in /etc/yum/pluginconf.d/fastestmirror.conf
...
exclude=gd.tuwien.ac.at
```

Das Yum-Kommando

Tabelle 22.2 fasst die wichtigsten Yum-Kommandos zusammen. Wenn Sie `yum` zum ersten Mal ausführen, werden Metainformationen zu allen eingerichteten Paketquellen heruntergeladen, was eine Weile dauern kann. Alle weiteren Kommandos werden dann sofort ausgeführt, bis das nächste Update der Metainformationen ansteht.

Aufgabe	Kommando
Paket installieren	`yum install name`
Lokale Paketdatei installieren	`yum localinstall datei.rpm`
Liste der verfügbaren Updates ermitteln	`yum check-update`
Ein Paket aktualisieren	`yum update name`
Alle Pakete aktualisieren	`yum update`
Paket entfernen	`yum remove name`
Liste aller installierten Pakete ermitteln	`yum list installed`
Liste aller verfügbaren Pakete ermitteln, deren Name mit `abc` beginnt	`yum list available 'abc*'`
Pakete suchen, die den Begriff `abc` in der Paketbeschreibung enthalten	`yum search 'abc'`
Paketgruppen bearbeiten	`yum grouplist/groupinstall/...`
Liste der letzten Yum-Aktionen anzeigen	`yum history`
Details zur Aktion *n* ermitteln	`yum history info n`

Tabelle 22.2 Wichtige yum-Kommandos

Beispiele

Die folgenden Kommandos demonstrieren die Anwendung von Yum, wobei die Ausgaben aus Platzgründen gekürzt sind.

```
root#  yum check-update
acl.x86_64                2.2.49-6.fc19          updates
cifs-utils.x86_64         4.6-1.fc19             updates
...
root#  yum install mariadb-server
...
Installieren:
 mariadb-server     x86_64   1:5.5.31-4.fc19  updates   9.9 M
Als Abhängigkeiten installiert:
 mariadb            x86_64   1:5.5.31-4.fc19  updates   8.8 M
 mariadb-libs       x86_64   1:5.5.31-4.fc19  updates   743 k
 ...
Installieren  1 Paket (+25 Abhängige Pakete)
Gesamte Downloadgröße: 23 M, Installationsgröße: 113 M
Is this ok [y/d/N]:  y
```

Paketgruppen

`yum` kennt Paketgruppen, um mit wenig Aufwand alle erforderlichen Pakete für eine bestimmte Aufgabe zu installieren. Eine Liste der verfügbaren Paketgruppen samt der englischsprachigen Gruppen-IDs liefert `yum grouplist -v`. Der Befehl `yum groupinfo` *name* verrät, welche Pakete zu einer Gruppe gehören. `yum groupinfo` unterteilt die Pakete in drei Kategorien: *mandatory*, *default* und *optional*. `yum groupinstall` *name* installiert alle *mandatory*- und *default*-Pakete. `yum` kennt keine Option, um auch die optionalen Pakete zu installieren. Wenn Sie das möchten, müssen Sie die folgende Änderung in `yum.conf` durchführen:

```
# Ergänzung in /etc/yum.conf
group_package_types = mandatory default optional
```

Um eine Paketgruppe zu aktualisieren bzw. zu entfernen, verwenden Sie `yum groupupdate` bzw. `yum groupremove`.

Quellcodepakete

`yum` ist von sich aus nicht in der Lage, Quellcodepakete zu installieren. Diese Aufgabe übernimmt stattdessen das Kommando `yumdownloader`, das sich im Paket `yum-utils` befindet. Das folgende Kommando lädt das Quellcodepaket des Editors `gedit` in das lokale Verzeichnis. Dabei werden die normalerweise nicht aktiven `source`-Quellen in den `*.repo`-Dateien automatisch aktiviert.

```
user$  yumdownloader --source gedit
```

Yum Extender (Yumex)

Yumex ist eine einfache und funktionelle grafische Benutzeroberfläche zu Yum. Beim Start aktualisiert Yumex die lokalen Metadaten zu allen Paketquellen. Anschließend können Sie nach Paketen suchen, diese zur Installation markieren und die Installation schließlich durchführen.

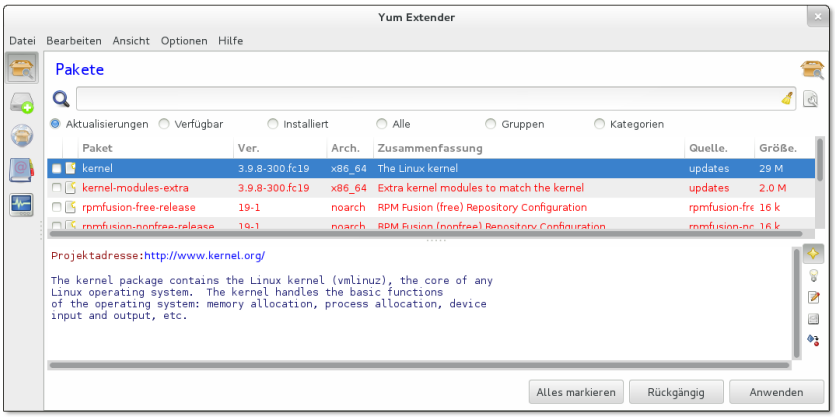


Abbildung 22.1 Paketverwaltung mit dem Yum Extender

Automatische Downloads und Updates

Wenn das Paket `yum-updatesd` installiert ist, wird beim Rechnerstart das gleichnamige Programm gestartet. Es überprüft regelmäßig, ob Updates zur Verfügung stehen. Je nachdem, wie die Einstellungen in `/etc/yum/yum-updatesd.conf` aussehen, werden die Update-Pakete gleich heruntergeladen und installiert. Das folgende Listing zeigt die Standardkonfiguration unter Fedora, bei der *keine* automatischen Updates durchgeführt werden. Wenn Sie das möchten, müssen Sie dreimal `no` durch `yes` ersetzen.

```
# /etc/yum/yum-updatesd.conf
[main]
# einmal pro Stunde testen, ob neue Updates zur Verfügung stehen
run_interval = 3600
# höchstens alle 10 Minuten den Update-Server kontaktieren
updaterefresh = 600
# lokale Update-Benachrichtigung via dbus durchführen
emit_via = dbus
dbus_listener = yes
# Updates automatisch herunterladen
do_download = no
# auch abhängige Pakete für Updates herunterladen
do_download_deps = no
# Updates automatisch installieren
do_update = no
```

Leider führt das nun ständig laufende Yum-Update-Programm gelegentlich zu Locking-Problemen. Abhilfe: Stoppen Sie `yum-updatesd`, bevor Sie die Paketverwaltung nutzen. Vergessen Sie aber nicht, `yum-updatesd` wieder zu starten!

```
root# service yum-updatesd stop
root# ... manuelle Pakete installieren oder entfernen ...
root# service yum-updatesd start
```

22.3 ZYpp

SUSE verwendet wie Fedora und Red Hat RPM-Pakete. Die auf RPM aufbauende Paketverwaltung ZYpp ist allerdings eine Novell/SUSE-Eigenentwicklung. ZYpp steht für *ZENworks, YaST, Packages and Patches*, wobei die Verwendung von ZENworks optional und nur in SUSE-Enterprise-Distributionen vorgesehen ist. Umfassende Informationen zu ZYpp finden Sie unter:

http://en.opensuse.org/Zypp

libzypp

Hinter den Kulissen stellt die Bibliothek `libzypp` die ZYpp-Grundfunktionen zur Verfügung. `libzypp` kommt sowohl mit YaST- als auch mit YUM-Paketquellen zurecht. Sämtliche Konfigurations-, Datenbank- und Cache-Dateien befinden sich im Verzeichnis `/var/lib/zypp`. Sowohl YaST als auch PackageKit greifen unter openSUSE auf `libzypp` zurück.

Updates versus Patches

`zypper` unterscheidet zwischen Updates und Patches! Updates sind gewöhnliche RPM-Pakete, die in einer neueren Version als der installierten zur Verfügung stehen. Patches sind dagegen Ergänzungs- bzw. Aktualisierungspakete (Delta-RPMs).

SUSE verwendet zur Aktualisierung seiner eigenen Pakete Patches in Form von Delta-RPMs. Externe Paketquellen, wie Packman, stellen neue Paketversionen dagegen in Form von Updates zur Verfügung.

Paketquellen

Paketquellen werden in Textdateien im Verzeichnis `/etc/zypp/repos.d` gespeichert. Wenn Sie diese Dateien mit einem Editor verändern, achten Sie darauf, anschließend alle Sicherheitskopien zu löschen! Andernfalls bekommen Sie Doppelgänger in der Liste der Paketquellen. Die folgenden Zeilen zeigen die Definition der Open-Source-Paketquelle für openSUSE:

```
# Datei /etc/zypp/repos.d/repo-oss.repo
[repo-oss]
name=openSUSE-12.3-Oss
enabled=1
autorefresh=1
baseurl=http://download.opensuse.org/distribution/12.3/repo/oss/
type=yast2
keeppackages=0
```

Das zypper-Kommando

`zypper` ist eine Kommandoschnittstelle zu `libzypp`. `zypper` ist damit das SUSE-Gegenstück zu `yum` bzw. `apt-get`. Sie können damit Pakete suchen, installieren, aktualisieren und entfernen sowie Paketquellen verwalten. `zypper` muss von `root` ausgeführt werden.

Aufgabe	Kommando
Metadaten der Paketquellen neu einlesen	`zypper refresh`
Paket installieren	`zypper install name`
Paket entfernen	`yum remove name`
Liste aller Updates ermitteln	`yum -t package list-updates`
Alle Pakete aktualisieren	`yum -t package update`
Distributions-Update durchführen	`yum dup`
Informationen zu einem Paket ermitteln	`yum info name`
Pakete suchen, deren Paketname `abc` enthält	`yum search abc`
Pakete suchen, deren Paketbeschreibung `abc` enthält	`yum search -d abc`
Liste aller Paketquellen ermitteln	`yum repos`
Neue Paketquelle einrichten	`yum addrepo uri name`

Tabelle 22.3 Wichtige zypper-Kommandos

Die folgenden Beispiele zeigen die Anwendung von `zypper`. Das erste Kommando listet die Paketquellen auf, das zweite aktualisiert die Quellen, das dritte installiert den Editor `emacs`, und das vierte stellt fest, welche Updates zur Verfügung stehen. **Beispiele**

```
root#  zypper repos
#  Alias               Name                    Aktiviert Aktualisieren
1  ftp.gwdg.de-suse    Packman Repository      Ja        Ja
2  repo-non-oss        openSUSE-12.3-Non-Oss   Ja        Ja
3  repo-oss            openSUSE-12.3-Oss       Ja        Ja
...
root#  zypper refresh
All repositories have been refreshed.
root#  zypper install emacs
The following NEW packages are going to be installed:
  ctags emacs emacs-info emacs-x11 fribidi libotf0 m17n-db m17n-lib xaw3d
9 new packages to install.
Overall download size: 21.0 MiB.
After the operation, additional 85.5 MiB will be used.
Continue? [y/n/?] (y):  y
```

Paketgruppen

Um alle erforderlichen Pakete für eine bestimmte Aufgabe zu installieren, etwa zur Verwendung des Rechners als Datei-Server, kennt ZYpp sogenannte *pattern*. `zypper search -t pattern` ermittelt eine Liste aller derartigen Paketgruppen. `zypper info -t pattern` *name* verrät, welche Pakete zu einer Paketgruppe gehören. Mit `zypper install -t pattern` *name* installieren Sie alle Pakete einer Paketgruppe.

history

Die Datei `/var/log/zypp/history` enthält eine ausgesprochen praktische Referenz darüber, wann welches Paket aus welcher Paketquelle installiert oder entfernt wurde und welche Konfigurationsarbeiten dabei durchgeführt wurden.

Distributions-Updates

Mit `zypper dup` führen Sie ein Distributions-Update im laufenden Betrieb durch:

```
root# zypper updates    (Update für die bisherige Version)
root# ...               (Paketquellen auf die neue Version umstellen)
root# zypper dup        (alte Pakete durch neue ersetzen)
root# reboot            (Neustart)
```

22.4 Debian-Paketverwaltung (dpkg)

Die Verwaltung von Debian-Paketen erfolgt auf zwei Ebenen: Dieser Abschnitt beschreibt das Kommando `dpkg`, das auf der unteren Ebene für die Installation und Verwaltung von Paketen verantwortlich ist. `dpkg` ist mit `rpm` vergleichbar. Das Kommando kann einzelne Pakete installieren, aktualisieren, entfernen und dabei testen, ob alle Paketabhängigkeiten erfüllt sind.

Ähnlich wie `rpm` scheitert auch `dpkg` daran, nicht erfüllte Paketabhängigkeiten selbst aufzulösen oder Pakete selbstständig von Paketquellen zu laden. Genau diese Aufgaben erfüllt APT (*Advanced Package Tool*, siehe Abschnitt 22.5). Es baut auf `dpkg` auf und bietet ähnliche Funktionen wie die gerade vorgestellten Systeme Yum und ZYpp. Zur eigentlichen Paketverwaltung stehen zwei Kommandos zur Wahl: `apt-get` wird standardmäßig unter Ubuntu eingesetzt, während `aptitude` in Debian als das bevorzugte Werkzeug zur Paketinstallation gilt. Die Unterschiede zwischen diesen beiden Kommandos sind aber gering.

Auch wenn in diesem und dem folgenden Abschnitt von Debian-Paketen die Rede ist, gelten die Informationen für alle Linux-Distributionen, die dieses Paketformat nutzen. Neben Debian sind das beispielsweise die Ubuntu-Familie und Linux Mint. Wenn Sie von einer RPM-basierten Distribution auf eine Distribution mit Debian-Paketen umsteigen, finden Sie auf dieser Seite eine gute Übersicht über `rpm`-Kommandos sowie dazu äquivalente `dpkg`- und `apt`-Kommandos:

https://help.ubuntu.com/community/SwitchingToUbuntu/FromLinux/RedHatEnterpriseLinuxAndFedora

Metadaten

`dpkg` verwaltet zu allen Paketen umfassende Metainformationen (eine Paketbeschreibung, eine Liste aller Dateien des Pakets, Abhängigkeitsdaten etc.). Diese Daten liegen im dctrl-Format (*Debian control*) vor. Das Paket `dctrl-tools` enthält diverse Kommandos, um Abfragen in den dctrl-Daten durchzuführen. `man grep-dctrl` gibt eine ausführliche Beschreibung dieser Kommandos und eine Menge konkreter Anwendungsbeispiele.

Das dpkg-Kommando

Tabelle 22.4 gibt einen Überblick über die wichtigsten `dpkg`-Optionen. In der Praxis werden Sie `dpkg` zumeist einsetzen, um Informationen über installierte oder verfügbare Pakete zu ermitteln.

Aufgabe	Kommando
Paket installieren bzw. aktualisieren	`dpgk --install datei.deb`
Paket konfigurieren	`dpgk --configure datei.deb`
Paket entfernen	`dpkg --remove paketname`
Paket vollständig entfernen (auch geänderte Dateien)	`dpkg --purge paketname`
Alle installierten Pakete ermitteln	`dpkg --list`
Pakete suchen, deren Paketbeschreibung `abc` enthält	`dpkg --list abc`
Liste aller Dateien des Pakets ermitteln	`dpkg --listfiles paketname`
Liste aller Konfigurationsdateien des Pakets ermitteln	`rpm -qc paketname`

Tabelle 22.4 Wichtige dpkg-Kommandos

Beispiele

Die folgenden Beispiele verdeutlichen die Anwendung von `dpkg` in Standardsituationen:

```
root#  dpkg --install test.deb
root#  dpkg --search /etc/sensors3.conf
libsensors4:adm64 /etc/sensors3.conf
root#  dpkg --listfiles libsensors4
/usr/lib
/usr/lib/libsensors.so.4.3.2
/etc
/etc/sensors3.conf
/etc/sensors.d
...
```

`dpkg --list` liefert eine Liste aller installierten Pakete. Dabei wird ein Statuscode angezeigt, der aus bis zu drei Buchstaben besteht. Der erste Buchstabe gibt den gewünschten Zustand an (`u` = *unknown*, `i` = *install*, `r` = *remove*, `p` = *purge*, `h` = *hold*),

der zweite Buchstabe gibt den tatsächlichen Zustand an (`n` = *not*, `i` = *installed*, `c` = *config files*, `u` = *unpacked*, `f` = *failed config*, `h` = *half installed*), der optionale dritte den Fehlercode (`h` = *hold*, `r` = *reinstall required*, `x` = *hold + reinstall required*).

```
root#  dpkg --list | grep cups
ii  cups         1.5.3-5  amd64  Common UNIX Printing System - server
ii  cups-bsd     1.5.3-5  amd64  Common UNIX Printing System - BSD commands
ii  cups-client  1.5.3-5  amd64  Common UNIX Printing System - client programs
ii  cups-common  1.5.3-5  all    Common UNIX Printing System - common files
```

Die beiden häufigsten Statuscodes sind `ii` (installiertes Paket) und `rc` (entferntes Paket, die Konfigurationsdateien sind aber noch verfügbar). Um `rc`-Pakete vollständig zu entfernen, führen Sie `dpkg --purge` *name* aus.

Der Status *hold* bedeutet, dass ein Paket bei einem Update nicht aktualisiert werden soll. Die beiden folgenden Kommandos zeigen, wie Sie ein Paket in den *hold*-Status bringen bzw. diesen Status wieder aufheben:

```
root#  echo "paketname hold"    | dpkg --set-selections
root#  echo "paketname install" | dpkg --set-selections
```

Weitere Details zum Paketstatus und zur Behebung von Problemen finden Sie mit `man dpkg`.

get-selections und set-selections

Um rasch eine sortierte Liste aller installierten Pakete zu ermitteln, führen Sie `dpkg --get-selections` aus. Die Paketliste enthält weniger Detailinformationen als jene von `dpkg --list` und ist viel übersichtlicher. Wenn Sie die Liste in eine Textdatei umleiten und speichern, können Sie alle Pakete später auf einem anderen Rechner mit `dpkg --set-selections` installieren.

```
root#  dpkg --get-selections
accountsservice                                 install
acl                                             install
acpi-support                                    install
acpid                                           install
...
```

Paket neu konfigurieren

Bei der Installation von Debian-Paketen werden automatisch Installations- und Konfigurations-Scripts ausgeführt. Bei einigen wenigen Programmen gibt es darüber hinaus interaktive Setup-Programme, die bei der individuellen Konfiguration des Pakets helfen, z. B. bei der Grundkonfiguration des E-Mail-Servers Postfix. Wenn Sie die Konfiguration später wiederholen möchten, führen Sie `dpkg-reconfigure paketname` aus.

22.5 APT

APT (*Advanced Packaging Tool*) ist für Debian-Pakete das, was Yum für RPM-Pakete ist: ein High-Level-Paketverwaltungssystem, das Pakete selbstständig von Paketquellen herunterlädt und Paketabhängigkeiten automatisch auflöst. Die Kombination aus Debian-Paketen und APT ergibt momentan das wohl ausgereifteste Paketverwaltungssystem für Linux. Es wird unter anderem von Ubuntu und Debian als Standardsystem zur Paketverwaltung eingesetzt.

Zur eigentlichen Paketverwaltung stehen zwei alternative Kommandos zur Auswahl: `apt-get` und `aptitude`. Beide Kommandos sind einander sehr ähnlich und weisen bei einfachen Operationen sogar dieselbe Syntax auf. Sowohl `apt-get install paketname` als auch `aptitude install paketname` laden das angegebene Paket und alle davon abhängigen Pakete herunter und installieren sie.

Momentan kommt `apt-get` standardmäßig unter Ubuntu zum Einsatz, während Debian den Einsatz von `aptitude` empfiehlt. Unter Debian sind standardmäßig *beide* Kommandos installiert.

Wie Yum erfordert auch APT spezielle Paketquellen, die neben den DEB-Paketen auch Metainformationen über den Inhalt der Pakete und deren Abhängigkeiten zur Verfügung stellen.

Konfiguration

Die Konfiguration von APT erfolgt durch die beiden Dateien `apt.conf.d/*` und `sources.list` im Verzeichnis `/etc/apt`. Weitere Definitionen von Paketquellen können sich im Verzeichnis `sources.list.d` befinden.

`apt.conf.d/*` enthält in der Regel nur wenige Basiseinstellungen, die Sie zumeist so belassen, wie sie von Ihrer Distribution vorgegeben sind. Schon interessanter ist `sources.list`. Diese Datei enthält zeilenweise die APT-Paketquellen. Die Syntax jeder Zeile sieht so aus:

```
pakettyp uri distribution [komponente1] [komponente2] [komponente3] ...
```

Der Pakettyp lautet `deb` für gewöhnliche Debian-Pakete bzw. `deb-src` für Quellcodepakete. Die zweite Spalte gibt das Basisverzeichnis der Paketquelle an. Neben HTTP- und FTP-Verzeichnissen unterstützt APT auch gewöhnliche Verzeichnisse, RSH- oder SSH-Server sowie CDs bzw. DVDs.

Die dritte Spalte bezeichnet die Distribution. Alle weiteren Spalten geben die Komponenten der Distribution an, die berücksichtigt werden können. Die Komponentennamen sind von der Distribution und von der Paketquelle abhängig! Beispiels-

weise unterscheidet Ubuntu zwischen *main*-, *restricted*-, *universe*- und *multiverse*-Paketen, während Debian zwischen den Komponenten *main*, *contrib*, *non-free* etc. differenziert.

Die zuerst genannten Paketquellen werden bevorzugt: Wenn ein bestimmtes Paket also in mehreren Quellen zum Download zur Verfügung steht, lädt APT es von der ersten Quelle herunter. Das folgende Listing verdeutlicht die Syntax. Aus Platzgründen wurde dabei jeder Eintrag über zwei Zeilen verteilt.

```
# Datei /etc/apt/sources.list
deb http://de.archive.ubuntu.com/ubuntu/ saucy          \
                                main restricted universe multiverse
deb http://de.archive.ubuntu.com/ubuntu/ saucy-updates  \
                                main restricted universe multiverse
deb http://security.ubuntu.com/ubuntu    saucy-security \
                                main restricted universe multiverse
```

Veränderungen an `sources.list` führen Sie am einfachsten mit einem Texteditor durch. Alternativ können Sie auch das Programm `apt-setup` oder eine grafische Benutzeroberfläche wie Synaptic zu Hilfe nehmen.

APT-Schlüssel installieren

Bei den meisten APT-Quellen im Internet sind die Metadateien zur Beschreibung der Paketquellen durch einen Schlüssel signiert. Weiters enthalten die APT-Inhaltsverzeichnisse Prüfsummen für alle Pakete. Mit diesem Kontrollmechanismus kann sichergestellt werden, dass kein Paket nachträglich verändert wurde. Diese Kontrolle funktioniert aber nur, wenn APT den öffentlichen Teil des Schlüssels kennt und somit die Authentizität des Paketarchivs feststellen kann. Um einen Schlüssel für APT einzurichten, verwenden Sie das Kommando `apt-key`:

```
root#  apt-key add schlüsseldatei.gpg
```

Das apt-get-Kommando

Die eigentliche Paketverwaltung führen Sie wahlweise mit den Kommandos `apt-get` oder mit dem im nächsten Abschnitt beschriebenen Kommando `aptitude` durch. Die wichtigsten `apt-get`-Kommandos sind in Tabelle 22.5 zusammengefasst.

Beispiele

Bevor Sie Pakete installieren, sollten Sie `apt-get update` ausführen und damit die neuesten Informationen aus den Paketquellen herunterladen. Dadurch werden weder Pakete installiert noch aktualisiert; es geht hier nur um die Paketbeschreibungen, also um die Metadaten! Die meisten anderen Paketverwaltungssysteme (Yum, ZYpp) aktualisieren diese Metadaten bei Bedarf selbstständig – aber eben nicht bei `apt-get` und `aptitude`. Anschließend können Sie ein neues Paket mit `apt-get install` herunterladen und installieren:

Aufgabe	Kommando
Metadaten aus den Paketquellen aktualisieren	`apt-get update`
Paket installieren	`apt-get install name`
Alle Pakete aktualisieren	`apt-get upgrade`
Wie oben, aber bei Bedarf auch neue, abhängige Pakete installieren	`apt-get dist-upgrade`
Paket entfernen	`apt-get remove name`
Nicht mehr benötigte Pakete entfernen	`apt-get autoremove`

Tabelle 22.5 Wichtige apt-get-Kommandos

```
root#  apt-get update
root#  apt-get install apache2
...
Die folgenden zusätzlichen Pakete werden installiert:
  apache2-mpm-worker apache2-utils apache2.2-common libapr1 libaprutil1
Vorgeschlagene Pakete:
  apache2-doc apache2-suexec apache2-suexec-custom
Die folgenden NEUEN Pakete werden installiert:
  apache2 apache2-mpm-worker apache2-utils apache2.2-common libapr1 libaprutil1
0 aktualisiert, 6 neu installiert, 0 zu entfernen und 11 nicht aktualisiert.
Es müssen 1472kB an Archiven heruntergeladen werden.
Nach dieser Operation werden 5452kB Plattenplatz zusätzlich benutzt.
Möchten Sie fortfahren [J/n]?
...
```

`apt-get remove paketname` entfernt das angegebene Paket. Ursprünglich zusammen mit dem Paket installierte abhängige Pakete bleiben davon aber unberührt. Abhilfe schafft `apt-get autoremove`. Dieses Kommando entfernt alle nicht mehr benötigten Pakete.

Das richtige Kommando zur Durchführung von Updates ist in aller Regel `apt-get dist-upgrade`. Wenn es aufgrund geänderter Paketabhängigkeiten erforderlich ist, werden dadurch auch zusätzliche Pakete installiert bzw. vorhandene Pakete entfernt. `apt-get upgrade` führt zwar auch ein Update durch, rührt aber Pakete nicht an, wo aufgrund von geänderten Abhängigkeiten zusätzliche Pakete erforderlich sind.

```
qqroot#  apt-get dist-upgrade
```

Quellcode installieren

`apt-get source paketname` installiert den Quellcode des gewünschten Pakets in das aktuelle Verzeichnis. Weitere Details finden Sie in Abschnitt 23.2.

Distributions-Updates

Um ein Update auf die nächste Version von Debian oder Ubuntu durchzuführen, passen Sie zuerst die Paketquellen in `/etc/apt/sources.list` entsprechend an. Anschließend führen Sie `apt-get dist-upgrade` aus. Der Download und die Installation der Pakete wird je nach Installationsumfang ca. eine halbe Stunde dauern. Danach starten Sie Ihren Rechner neu – fertig!

Leider sind Release-Updates trotz des ausgezeichneten Debian-Paketverwaltungssystems eine heikle Angelegenheit. Dass nach dem Update wirklich alle Programme und Server-Dienste wie bisher funktionieren, ist eher ein Glücks- als der Regelfall.

Das aptitude-Kommando

Das Kommando `aptitude` baut ebenfalls auf APT auf. Wenn Sie das Programm kommandoorientiert einsetzen (`aptitude install paketname`), ist es weitgehend syntaxkompatibel zu `apt-get`. Alle in Tabelle 22.5 aufgezählten Kommandos mit der Ausnahme von `autoremove` stehen in gleicher Form für `aptitude` zur Verfügung.

Alternativ können Sie das Programm auch mit einer Text-Benutzeroberfläche in einer Konsole nutzen (siehe Abbildung 22.2), indem Sie das Programm einfach ohne weitere Parameter starten. Zur Menüauswahl verwenden Sie die Tastenkombination Strg+T. Wirklich intuitiv ist `aptitude` trotz Menü nicht zu bedienen; die meisten Anwender verwenden `aptitude` daher wie `apt-get` einfach zum Ausführen einzelner Kommandos.

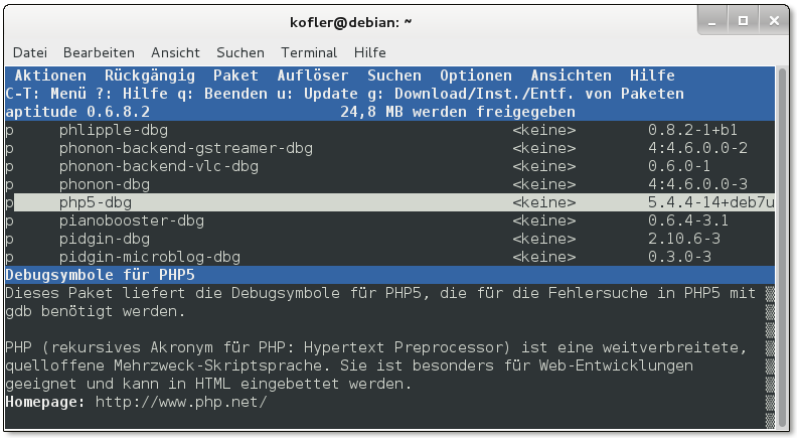


Abbildung 22.2 Paketverwaltung mit aptitude

`aptitude` bietet im Vergleich zu `apt-get` einen entscheidenden Vorteil: Das Programm merkt sich, welche abhängigen Pakete installiert wurden, und entfernt diese bei einer Deinstallation automatisch wieder. Wenn Sie beispielsweise das Programm `xyz` installieren und dieses fünf weitere Pakete (`lib-abc`, `lib-efg` etc.) voraussetzt, dann

werden diese Pakete bei der Deinstallation von `xyz` wieder entfernt, sofern mittlerweile kein anderes Paket davon abhängig ist. Wenn Sie `xyz` dagegen mit `apt-get` oder Synaptic entfernen, bleiben die abhängigen Pakete `lib-abc`, `lib-efg` etc. erhalten. Nach einer Weile weiß niemand mehr, warum die Pakete installiert sind. Debian empfiehlt deswegen explizit die Verwendung von `aptitude` anstelle von `apt-get` zur Paketverwaltung.

Beispiel

Die beiden folgenden Kommandos installieren zuerst das Paket `mysql-server` und entfernen es dann wieder. Bemerkenswert ist, dass beim zweiten Kommando die zahlreichen zusammen mit `mysql-server` installierten abhängigen Pakete ebenfalls wieder entfernt werden.

```
root#  aptitude install mysql-server
Die folgenden NEUEN Pakete werden zusätzlich installiert:
  libaio1a libdbd-mysql-perla libdbi-perla libhtml-template-perla
  libmysqlclient18a libnet-daemon-perla libplrpc-perla
  mysql-client-5.5a mysql-commona mysql-server mysql-server-5.5a
  mysql-server-core-5.5a
0 Pakete aktualisiert, 12 zusätzlich installiert, 0 werden entfernt
root#  aptitude remove mysql-server
Die folgenden Pakete werden ENTFERNT:
  libaio1u ... mysql-server-core-5.5u
0 Pakete aktualisiert, 0 zusätzlich installiert, 12 werden entfernt
```

APT-Zusatzkommandos

tasksel

Zur Installation von Paketgruppen greifen Debian und Ubuntu in der Regel auf Metapakete zurück: Das sind leere Pakete, die lediglich eine Menge Paketabhängigkeiten definieren. Beispielsweise wird zusammen mit dem Metapaket `build-essential` eine ganze Sammlung von Paketen mit grundlegenden Entwicklungswerkzeugen installiert (Compiler, `make` etc.).

Daneben gibt es noch einen zweiten Mechanismus zur Definition von Paketgruppen, der auf dem Kommando `tasksel` basiert. Dieser Mechanismus ist vor allem dazu gedacht, während der Installation der Distribution auf einfache Weise Paketgruppen auszuwählen. `tasksel` kann aber natürlich auch später im laufenden Betrieb verwendet werden: Eine Liste aller verfügbaren Paketgruppen liefert `tasksel --list-task`. Zur Installation von Paketgruppen verwenden Sie `tasksel install` *gruppenname*. Wenn `tasksel` ohne Optionen ausgeführt wird, erscheint ein Dialog zur Auswahl der gewünschten Paketgruppen.

apt-cache

`apt-cache` ermittelt diverse Daten zu den verfügbaren bzw. zu bereits installierten Paketen:

```
root#  apt-cache show apache2
Package: apache2
```

```
Description: next generation, scalable, extendable web server
...
root#  apt-cache  search scribus | sort
lprof - Hardware Color Profiler
scribus - Open Source Desktop Publishing
scribus-template - additional scribus templates
```

apturl Unter Ubuntu ist standardmäßig das Paket `apturl` mit dem Programm `apturl-gtk` installiert. Es ermöglicht nach einer Rückfrage die Installation von Paketen einfach durch das Anklicken spezieller `atp:`-Links im Webbrowser. Auf derartige Links stoßen Sie vor allem auf Ubuntu-Wikis und -Foren.

Updates automatisieren

APT wird normalerweise so installiert, dass Sie lediglich einige Konfigurationsdateien anpassen müssen, um Updates automatisch herunterzuladen und eventuell auch gleich zu installieren. Die erforderlichen Konfigurationsdateien sind Teil des Pakets `unattended-upgrades`, das unter Debian und Ubuntu standardmäßig installiert ist.

Ausgangspunkt für die Download- und Update-Automatik ist das Programm Cron, das einmal täglich das Script `/etc/cron.daily/apt` ausführt. Es wertet die Konfigurationsdatei `/etc/apt/apt.conf.d/*` aus und führt bei Bedarf das Upgrade-Kommando `unattended-upgrade` aus.

Automatische Updates aktivieren Sie, indem Sie den Parameter `Unattended-Upgrade` auf 1 stellen. Dieser Wert gibt an, nach wie vielen Tagen ein Update versucht werden soll. 0 bedeutet: kein automatisches Update durchführen.

```
// Datei /etc/apt/apt.conf.d/10periodic
// tägliche Updates aktivieren
APT::Periodic::Unattended-Upgrade "1";
```

Die Datei `50unattended-upgrades` enthält einige weitere Optionen: Mit `Allowed-Origins` steuern Sie, welche Paketquellen für das automatische Update berücksichtigt werden sollen. Mit `Package-Blacklist` können Sie einzelne Pakte vom automatischen Update ausschließen. Zu guter Letzt können Sie mit `Mail` eine Adresse angeben, an die das Kommando `unattended-upgrade` nach erfolgten Updates einen kurzen Statusbericht sendet. Der E-Mail-Versand setzt voraus, dass auf dem Rechner ein E-Mail-Server eingerichtet und das Paket `mailx` installiert ist.

```
// Datei /etc/apt/apt.conf.d/50unattended-upgrades
Unattended-Upgrade::Allowed-Origins {
  "origin=Debian,archive=stable,label=Debian-Security";
};
```

```
// folgende Pakete nicht aktualisieren
Unattended-Upgrade::Package-Blacklist {
  "vim";
  ...
};
// E-Mail über Update-Status senden
Unattended-Upgrade::Mail "root@localhost";
```

Abschließend noch einige Interna zum Upgrade-Prozess: `/etc/cron.daily/apt` enthält ein `sleep`-Kommando, das das Script für eine zufällige Anzahl von bis zu 1800 Sekunden anhält, also für bis zu einer halben Stunde. Diese Zwangspause vermeidet, dass Tausende Rechner aufgrund des Cron-Jobs gleichzeitig auf die Paketquellen zugreifen.

Das Script `/usr/bin/unattended-upgrade` protokolliert alle Updates bzw. Update-Versuche in Logging-Dateien im Verzeichnis `/var/log/unattended-upgrade`. Außerdem legt `/etc/cron.daily/apt` im Verzeichnis `/var/lib/apt/periodic/` Timestamp-Dateien an, aus denen hervorgeht, wann bestimmte Operationen zum letzten Mal durchgeführt wurden.

`unattended-upgrade` aktualisiert keine Pakete, für die ein sogenannter `conffile prompt` besteht, d. h., deren Konfigurationsdatei manuell verändert wurde. Leider geht das nur aus den Logging-Dateien hervor, nicht aus der Status-E-Mail. Da dieser Fall in der Praxis immer wieder vorkommt, müssen Sie trotz der automatisierten Updates regelmäßig kontrollieren, ob es nicht doch Updates gibt, die manuell durchzuführen sind.

Kernel-Updates werden erst wirksam, wenn der Rechner neu gestartet wird. `unattended-upgrade` kümmert sich darum nicht – Sie müssen den Rechner also durch ein `reboot`-Kommando selbst neu starten.

Für und wider automatische Updates

Automatische Updates mindern das Risiko, dass ein Angreifer eine bereits behobene Sicherheitslücke ausnutzt; aber sie können auch fatale Folgen haben, wenn einzelne Server-Funktionen aufgrund eines defekten Updates plötzlich nicht mehr richtig laufen. Eine Alternative zu automatischen Updates ist ein Cron-Script, das einmal täglich die Verfügbarkeit neuer Updates überprüft (z. B. durch `apt-get dist-upgrade --simulate`) und das Ergebnis als E-Mail an den Administrator sendet.

Paket-Proxy

Wenn in Ihrem Netzwerk Dutzende Debian- oder Ubuntu-Rechner laufen und jeder für sich seine Updates von einer externen Paketquelle bezieht, ergibt das ein Datenvolumen von einigen GByte pro Monat. Auch wenn die meisten Internetzugänge momentan ohne Download-Limit angeboten werden, verstopfen die Updates das Netz und machen den Internetzugang für das LAN langsamer als notwendig.

Es liegt auf der Hand, im LAN einen zentralen Zwischenspeicher (Proxy) einzurichten, über den alle anderen Rechner Paket-Updates beziehen. Hierfür gibt es eine ganze Palette von Programmen, z. B. `apt-cacher`, `apt-cacher-ng`, `squid-deb-proxy`, `apt-proxy` (wird nicht mehr gewartet) sowie `approx`. Ich stelle Ihnen an dieser Stelle exemplarisch `apt-cacher` vor.

Server-Konfiguration

Auf dem Cache-Server, also auf dem Rechner, der den Zwischenspeicher verwaltet, muss das Paket `apt-cacher` installiert werden. Viele `apt-cacher`-Anleitungen im Internet behaupten, dass Sie auch Apache installieren müssen. Das ist nicht richtig! `apt-cacher` arbeitet selbstständig. Ein Zusammenspiel mit Apache ist nur dann zweckmäßig, wenn die Kommunikation zu `apt-cacher` über den HTTP-Port 80 erfolgen soll.

```
root#  apt-get install apt-cacher
```

Damit `apt-cacher` in Zukunft automatisch als Dämon gestartet wird, müssen Sie eine kleine Änderung an `/etc/default/apt-cacher` durchführen:

```
# Datei /etc/default/apt-cacher
AUTOSTART=1
...
```

`/etc/apt-cacher/apt-cacher.conf` enthält die restliche Konfiguration. Die meisten Einstellungen können Sie so lassen, wie sie sind: Der APT-Proxy ist dann über den Port 3142 für alle Rechner zugänglich. Die Paketdateien werden im Verzeichnis `/var/cache/apt-cacher` gespeichert. Aus Sicherheitsgründen empfiehlt es sich, die folgenden Änderungen an der Konfiguration durchzuführen:

```
# Datei /etc/apt-cacher/apt-cacher.conf
...
daemon_addr=192.168.0.1
allowed_hosts=192.168.0.0/24
...
```

Damit binden Sie den Dämon an eine bestimmte Adresse (hier 192.168.0.1, wichtig bei Rechnern mit mehreren Netzwerkschnittstellen) und erlauben nur Clients aus dem Adressbereich 192.168.0.*, den Proxy zu nutzen. Diese Adressen müssen Sie natürlich an die Gegebenheiten Ihres lokalen Netzwerks anpassen! Außerdem ist es

zweckmäßig, den Port 3142 internet-seitig durch eine Firewall zu blockieren. Nach diesen Konfigurationsarbeiten starten Sie `apt-cacher` erstmalig:

```
root#  service apt-cacher start
```

`apt-cacher` protokolliert alle Zugriffe sowie eventuelle Fehler in Logging-Dateien im Verzeichnis `/var/log/apt-cacher`.

Vorhandene Pakete importieren

Das Verzeichnis `/var/cache/apt/archive` auf dem Server enthält normalerweise bereits eine Menge Pakete, die von der lokalen Paketverwaltung für Installationen bzw. Updates heruntergeladen wurden. Sie können diese Pakete in den Cache von `apt-cacher` importieren. Das ist zweckmäßig, wenn zu erwarten ist, dass diese Pakete von anderen Rechnern im LAN benötigt werden:

```
root#  cd /usr/share/apt-cacher
root#  ./apt-cacher-import.pl /var/cache/apt/archives
```

Client-Konfiguration

Am Client vergewissern Sie sich mit einem Webbrowser, dass `apt-cacher` via HTTP erreichbar ist. Dazu geben Sie die folgenden Adressen ein, wobei Sie natürlich `mein-apt-cacher` durch den Hostnamen oder die IP-Adresse des Proxy-Servers ersetzen:

```
http://mein-apt-cacher:3142
http://mein-apt-cacher:3142/report
```

Die erste Seite fasst die Konfiguration zusammen, die zweite Seite gibt Informationen über die Effizienz des Proxys, die umso besser ist, je länger der Proxy läuft und je mehr Clients ihn benutzen.

Wenn `apt-cacher` prinzipiell funktioniert, müssen Sie nur noch eine kleine Änderung an der APT-Konfiguration durchführen, damit auch `apt-get` den Proxy verwendet. Dazu erstellen Sie die folgende neue Datei, wobei Sie wieder `mein-apt-cacher` durch den Hostnamen oder die IP-Adresse des Proxy-Servers ersetzen:

```
// Datei /etc/apt/apt.conf.d/01proxy
Acquire::http::Proxy "http://mein-apt-cacher:3142/";
```

Von nun an verwenden alle APT-Kommandos den neuen Proxy. Dateien, die dort noch nicht verfügbar sind, müssen natürlich wie bisher aus dem Internet heruntergeladen werden. Aber wenn der zweite Rechner im LAN ebenfalls ein Update durchführt oder ein Paket installiert, das vor Kurzem auch auf einen anderen Rechner installiert wurde, stehen die erforderlichen Pakete sofort zur Verfügung. Beachten Sie aber, dass Sie die `Aquire`-Zeile mit `//` auskommentieren müssen, wenn Sie mit Ihrem Notebook unterwegs sind und Updates oder Pakete installieren möchten, obwohl Sie gerade keinen Zugang zum Proxy-Server haben!

Synaptic

Die populärste grafische Benutzeroberfläche zur Administration von Debian-Paketen auf der Basis der APT-Kommandos heißt Synaptic. Aktuelle Versionen von Debian und Ubuntu installieren zwar standardmäßig die PackageKit-Benutzeroberfläche `gpk-application` bzw. das Ubuntu Software-Center, persönlich ziehe ich aber weiterhin das optionale Programm Synaptic vor, um gezielt nach Paketen zu suchen und diese zu installieren (siehe Abbildung 22.3).

Paketsuche

Synaptic besitzt gleich zwei Suchfunktionen: eine Schnellsuche für Paketnamen und -beschreibungen und eine herkömmliche Suchfunktion, in der Sie auch nach anderen Kriterien suchen können. Beide Suchfunktionen können miteinander kombiniert werden: Die Schnellsuche bezieht sich dann auf die Suchergebnisse der herkömmlichen Suche.

Installation

Um ein bestimmtes Paket zu installieren, wählen Sie es per Doppelklick zur Installation aus. Wenn das Paket von anderen Paketen abhängig ist, erscheint ein Dialog mit allen weiteren Paketen, die ebenfalls installiert werden müssen. Die eigentliche Installation beginnt mit dem Button ANWENDEN, wobei Sie noch eine Zusammenfassung aller geplanten Aktionen bestätigen müssen.

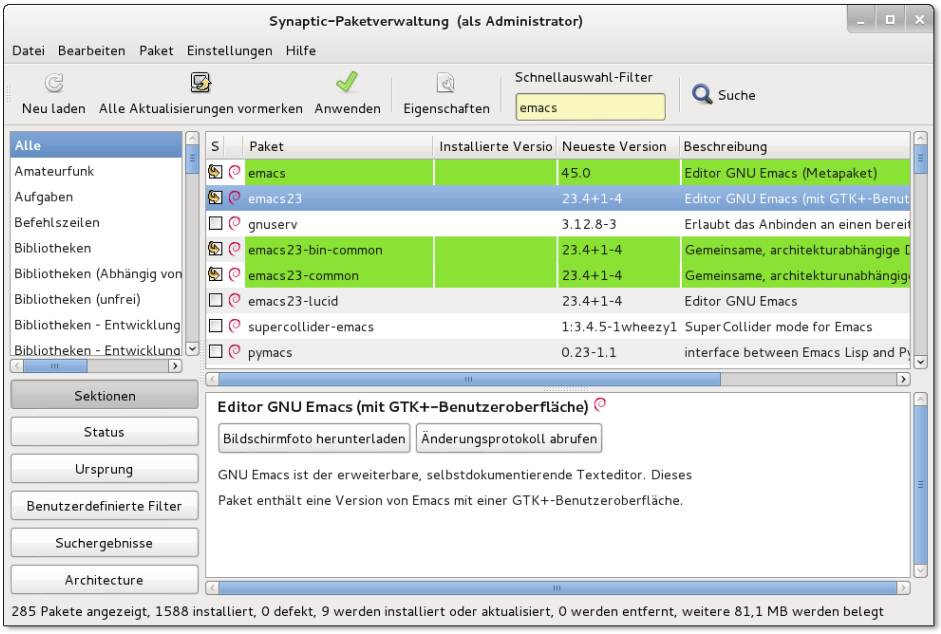


Abbildung 22.3 Paketverwaltung mit Synaptic

Die Liste aller zur Installation vorgemerkten Pakete sehen Sie, wenn Sie zuerst den Button Benutzerdefinierte Filter und dann den Listeneintrag Vorgemerkte Änderungen anklicken. Synaptic merkt sich alle Installationsvorgänge. Sie können diese jederzeit mit Datei • Chronik nachvollziehen.

Paketquellen verwalten

Die Verwaltung der Paketquellen erfolgt im Dialog Einstellungen • Paketquellen. Dort werden alle bekannten Paketquellen angezeigt. Durch einen Klick auf das Auswahlhäkchen können Sie einzelne Paketquellen rasch aktivieren bzw. deaktivieren. Mit Bearbeiten verändern Sie die Eigenschaften vorhandener Paketquellen, mit Hinzufügen richten Sie eine neue Paketquelle ein.

Defekte Pakete

Ein Paket gilt als »defekt«, wenn während der Installation oder Deinstallation ein Problem auftritt und der Vorgang nicht korrekt abgeschlossen werden kann. Synaptic und andere Paketverwaltungswerkzeuge verweigern ihren Dienst, bis dieses Problem gelöst ist.

Zur Abhilfe klicken Sie in Synaptic in der Seitenliste auf den Button Benutzerdefinierte Filter und dann auf den Eintrag Defekt. Synaptic zeigt nun eine Liste aller defekten Pakete an. Markieren Sie alle Pakete durch Strg+A, klicken Sie die Liste mit der rechten Maustaste an, und wählen Sie den Eintrag Zum erneuten Installieren vormerken. Anschließend führen Sie die Neuinstallation durch Anwenden aus. Sollten dabei abermals Probleme auftreten, markieren Sie die betreffenden Pakete zum Entfernen.

Locking-Probleme

Es kann immer nur ein Paketverwaltungsprogramm laufen. Beim Versuch, zwei Paketverwaltungsprogramme gleichzeitig auszuführen, erscheint die Warnung *unable to get exclusive lock*. Das bedeutet, dass das Programm nicht allein auf die internen Paketverwaltungsdateien zugreifen kann. Abhilfe: Beenden Sie eines der beiden Programme.

In seltenen Fällen tritt die *lock*-Warnung auch dann auf, wenn augenscheinlich kein anderes Paketverwaltungsprogramm mehr läuft. Die Ursache ist zumeist, dass ein Programm die `lock`-Datei beim Programmende nicht ordnungsgemäß entfernt hat. Gegebenenfalls löschen Sie die `lock`-Datei ganz einfach: `rm /var/lib/dpkg/lock`.

22.6 PackageKit

PackageKit ist eine Benutzeroberfläche zur Paketinstallation und -verwaltung. Die größte Besonderheit des Programms besteht darin, dass es zu mehreren Paketverwaltungssystemen kompatibel ist, unter anderem zu APT, Yum und Zypper. PackageKit bzw. dessen KDE-Variante KPackageKit wird unter anderem von Debian, Fedora, Kubuntu und openSUSE eingesetzt, in openSUSE allerdings nur zur Durchführung von Updates. PackageKit greift zur Erlangung von `root`-Rechten auf PolicyKit zurück (siehe Abschnitt 16.4).

Interna und Konfiguration

PackageKit ist aus mehreren Teilen zusammengesetzt, die üblicherweise in eigenen Paketen verpackt sind: Zu den wichtigsten Komponenten zählen die Grundfunktionen bzw. -kommandos (Paket `packagekit`), die Schnittstelle zum zugrunde liegenden Paketverwaltungssystem (z. B. `packagekit-backend-apt`) und die grafische Benutzeroberfläche (Paket `gnome-packagekit` bzw. `apper`). Die Paketnamen können je nach Distribution variieren.

PackageKit wird durch die Dateien `/etc/PackageKit/*` konfiguriert. Die wichtigste Einstellung ist `DefaultBackend` in `PackageKit.conf`: Diese Variable gibt an, auf welches *backend*, also auf welches Paketverwaltungssystem PackageKit zurückgreifen soll.

Der Dämon `packagekitd` ist für die Koordination der PackageKit-Operationen erforderlich. Das Programm wird bei Bedarf automatisch von den PackageKit-Kommandos bzw. -Benutzeroberflächen gestartet.

Mit dem Kommando `pkcon` können Sie sämtliche Paketoperationen auch in einer Konsole ausführen oder durch ein Script automatisieren. Beachten Sie, dass das Kommando nicht von `root` ausgeführt werden darf! Sie müssen das Kommando als gewöhnlicher Benutzer starten. Soweit erforderlich, verwendet das Kommando PolicyKit, um `root`-Rechte zu erlangen. Falls Sie in einer Konsole verfolgen möchten, was PackageKit gerade macht, führen Sie `pkmon` aus.

Installation von Paketen

Die weitere Beschreibung von PackageKit bezieht sich auf dessen grafische Benutzeroberfläche für Gnome. Zur Installation zusätzlicher Pakete bzw. zum Entfernen vorhandener Pakete starten Sie das Programm `gpk-application`. Sie können nun nach dem Paketnamen suchen (siehe Abbildung 22.4) oder durch diverse Gruppen zusammengehöriger Pakete blättern (Paket-Zusammenstellungen).

Über das Filter-Menü können Sie die bisweilen riesigen Ergebnislisten einschränken – z. B. auf bereits installierte Pakete, auf Entwicklerpakete oder auf Pakete mit grafischer Benutzeroberfläche. Mit Anwenden starten Sie die Installation bzw. Deinstallation des ausgewählten Pakets.

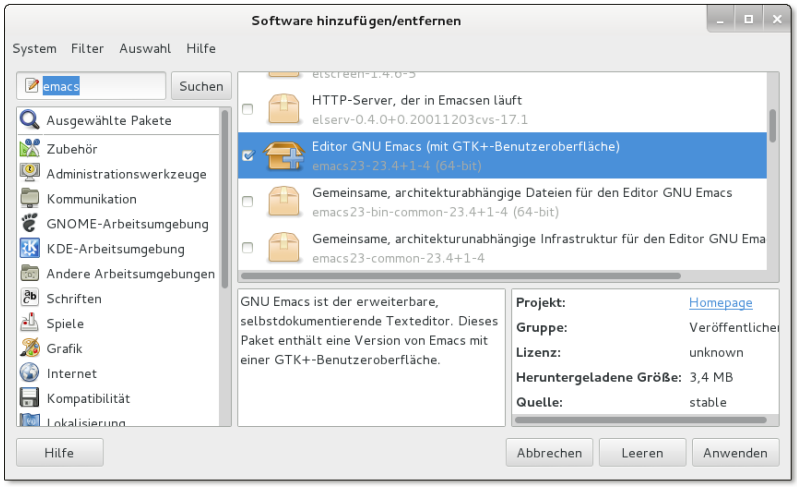


Abbildung 22.4 Paketinstallation mit dem PackageKit

22.7 tar

Mit dem Kommando `tar` können Sie ähnlich wie unter Windows mit WinZIP komprimierte Dateiarchive erstellen und auspacken. Eine genauere Beschreibung des Kommandos und speziell seiner Anwendung für Backup-Aufgaben finden Sie in Kapitel 39.

Vor allem bei erfahrenen Linux-Anwendern kommt es häufig vor, dass Linux-Software installiert werden soll, die nicht in Form eines Pakets einer bestimmten Distribution organisiert ist. Auch dabei kommt zumeist das `tar`-Format zur Anwendung.

Mit `gzip` komprimierte Archive weisen üblicherweise die Dateikennungen `*.tgz` oder `*.tar.gz` auf. Die Archive müssen mit dem Programm `tar` auf Ihrem Rechner installiert werden. Beachten Sie beim Auspacken, dass `tar` relativ zum gerade aktuellen Verzeichnis arbeitet. Stellen Sie sicher, dass Sie sich im richtigen Verzeichnis befinden!

```
root#  tar -tzf archiv.tar.gz           (Inhalt des Archivs anzeigen)
root#  tar -xzf archiv.tar.gz           (Dateien auspacken)
root#  tar -xzf archiv.tar.gz  "*.tex"  (nur *.tex-Dateien auspacken)
root#  tar -xzf archiv.tar.gz -C verz   (in ein Verzeichnis auspacken)
```

Immer häufiger wird zur Komprimierung der Archive das leistungsstärkere Programm `bzip2` verwendet. Sie erkennen derartige Archive an der Kennung `*.tar.bz2`. Zum Anzeigen bzw. Dekomprimieren müssen Sie nun statt `-z` die `tar`-Option `-j` verwenden, also beispielsweise `tar -tjf archiv.tar.bz2`.

In vielen Fällen liegt die Software nur im Quellcode vor und muss vor ihrer Verwendung noch kompiliert werden. Das setzt voraus, dass Sie die wichtigsten Entwicklungswerkzeuge sowie alle erforderlichen Bibliotheken installiert haben (`gcc`, `make`, `devel`-Pakete etc., siehe Abschnitt 23.2).

Achtung

Die Installation von Software-Paketen durch `tar` umgeht die Paketverwaltung des jeweiligen Systems. Die RPM-Datenbanken wissen daher nichts von den Programmen, die Sie installiert haben. Aus diesem und anderen Gründen ist es immer vorzuziehen, Pakete zu installieren, die speziell für die jeweilige Distribution vorbereitet wurden.

22.8 Umwandlung zwischen Paketformaten (alien)

Was können Sie tun, wenn ein Paket nur im RPM-Format zu finden ist, Sie aber unter Debian oder Ubuntu arbeiten? Was tun Sie, wenn Sie aus einem RPM-Paket nur eine einzige Datei ansehen möchten? Die Antwort lautet: Verwenden Sie `alien`. Dieses Kommando wandelt Pakete zwischen verschiedenen Formaten um (RPM, DEB, `tar`-Archiv und Stampede SLP).

`alien` funktioniert leider nur bei einfachen Paketen problemlos. Wenn ein Paket dagegen Installations-Scripts oder andere spezifische Eigenheiten des jeweiligen Paketformats nutzt, wird die Installation des zuvor umgewandelten Pakets meist scheitern. Generell ist `alien` eher ein Werkzeug für Linux-Profis.

Das gewünschte Paketformat wird durch die Optionen `--to-deb` (Debian), `--to-rpm` (RPM) oder `--to-tgz` (`tar`-Archiv) angegeben. `alien` muss von `root` ausgeführt werden, damit die Besitzer und Zugriffsrechte der neuen Pakete richtig eingestellt werden. Das folgende Kommando wandelt ein Debian-Paket in ein RPM-Paket um:

```
root#  alien --to-rpm paket.deb
```

Die folgenden Kommandos zeigen, wie Sie eine einzelne Datei aus einem RPM-Paket extrahieren. Dazu wandeln Sie das Paket zuerst in ein `tar`-Archiv um und verwenden dann `tar`, um die Datei daraus zu extrahieren und dann mit `less` anzuzeigen. (Statt `tar` können Sie natürlich auch den Dateimanager Konqueror oder Archivprogramme wie `ark` oder `file-roller` einsetzen. Diese Programme zeigen den Inhalt des Archivs in einer ansprechenden Benutzeroberfläche an.)

```
root#  alien --to-tgz paket.rpm
root#  tar -xzf paket.tgz ./usr/share/doc/packages/paket/TODO
root#  less ./usr/share/doc/packages/paket/TODO
```

22.9 Verwaltung von Parallelinstallationen (alternatives)

Unter Linux stehen oft mehrere alternative Programme zur Auswahl, die denselben Zweck erfüllen und manchmal sogar denselben Kommandonamen nutzen: Drucksysteme, Editoren, Java-Umgebungen etc. In manchen Situationen ist es zweckmäßig, mehrere Varianten bzw. sogar mehrere Versionen ein- und desselben Programms parallel zu installieren. Sofern dabei jede Programmversion in einem eigenen Verzeichnisbaum landet, ist die Installation an sich ohne Konflikte möglich. Welche Programmversion kommt aber zum Einsatz, wenn der Anwender ein bestimmtes Kommando ausführt?

Zur Beantwortung dieser Frage verwenden viele gängige Distributionen ein zuerst von Debian eingesetztes Konzept, das auf symbolischen Links im Verzeichnis `/etc/alternatives` basiert. Die folgende Liste gibt an, in welchem Paket das `alternatives`-Verzeichnis und das dazugehörende Verwaltungskommando `update-alternatives` enthalten ist:

Debian, Ubuntu:	Paket `dpkg`
Red Hat, Fedora:	Paket `chkconfig`
SUSE:	Paket `update-alternatives`

Am einfachsten ist das Konzept anhand eines Beispiels zu verstehen. Nehmen wir an, auf einem Rechner sind zwei Java-Versionen installiert. Java-Programme werden mit `java klasse` ausgeführt. Nun ist `/usr/bin/java` als Link auf `/etc/alternatives/java` realisiert. `/etc/alternatives/java` ist ein weiterer Link, der auf die gewünschte Java-Version verweist.

```
user$  ls -l /usr/bin/java
...   /usr/bin/java -> /etc/alternatives/java
user$  ls -l /etc/alternatives/java
...   /etc/alternatives/java -> /usr/lib/jvm/java-6-openjdk/jre/bin/java
```

Die Verwaltung der Links erfolgt in der Regel automatisch durch Scripts bei der Paketinstallation. Dabei kommt das Kommando `update-alternatives` zur Anwendung. Unter Red Hat/Fedora ist das Kommando auch unter dem Namen `alternatives` verfügbar.

Alternativen auflisten

Mit `update-alternatives --display` stellen Sie fest, welche Versionen eines bestimmten Programms verfügbar sind und welche Version standardmäßig gilt. Die folgenden Zeilen zeigen das Ergebnis für `editor` auf einem Debian-System mit mehreren installierten Texteditoren. Die `slave`-Zeilen betreffen Kommandos, die dem eigentlichen Programm untergeordnet sind, und `man`-Seiten. `update-alternatives` aktualisiert bei einer Veränderung des Kommando-Links automatisch auch alle `slave`-Links.

```
root#  update-alternatives --display editor
editor - Auto-Modus
  Link verweist zur Zeit auf /usr/bin/joe
/bin/nano - Priorität 40
  Slave editor.1.gz: /usr/share/man/man1/nano.1.gz
/usr/bin/jmacs - Priorität 50
  Slave editor.1.gz: /usr/share/man/man1/jmacs.1.gz
  Slave editorrc: /etc/joe/jmacsrc
/usr/bin/joe - Priorität 70
  Slave editor.1.gz: /usr/share/man/man1/joe.1.gz
  Slave editorrc: /etc/joe/joerc
...
Gegenwärtig »beste« Version ist »/usr/bin/joe«.
```

Normalerweise erfolgt die Link-Verwaltung im Automatikmodus: Jedes installierte Paket enthält eine Prioritätsnummer. `update-alternative` aktiviert bei jeder (De-)Installation die Alternative mit der höchsten Priorität.

Andere Alternative auswählen

`update-alternatives -config` bestimmt die in Zukunft aktive Variante. Das Kommando liefert die Liste der zur Auswahl stehenden Alternativen, von denen Sie dann eine aktivieren. `update-alternatives` aktualisiert nun die Links. `update-alternatives -auto` führt bei Bedarf zurück in den Automatikmodus. Im folgenden Beispiel wird `jmacs` als Default-Editor eingestellt:

```
root#  update-alternatives --config editor
Es gibt 7 Auswahlmöglichkeiten für die Alternative editor,
welche /usr/bin/editor bereitstellen.

  Auswahl  Pfad            Priorität Status
* 0        /usr/bin/joe     70        Auto-Modus
  1        /bin/nano        40        manueller Modus
  2        /usr/bin/jmacs   50        manueller Modus
...
Drücken Sie die Eingabetaste, um die aktuelle Wahl[*] beizubehalten,
oder geben Sie die Auswahlnummer ein:  2
update-alternatives: /usr/bin/jmacs wird verwendet, um
/usr/bin/editor (editor) im manueller Modus bereitzustellen
```

Interne Verwaltungsinformationen zu den Links werden je nach Distribution im Verzeichnis `/var/lib/alternatives` oder `/var/lib/rpm/alternatives` gespeichert.

22.10 Distributionsspezifische Eigenheiten

Bei diesem Kapitel ist es schwierig, die allgemeine Beschreibung von Paketverwaltungswerkzeugen von den spezifischen Besonderheiten einzelner Distributionen zu trennen. In den bisherigen Abschnitten habe ich mich bemüht, Ihnen die Grundlagen und Kommandos zu beschreiben, die für mehrere Distributionen gemeinsam gelten. In diesem Abschnitt folgen nun einige Besonderheiten, die nur für eine bestimmte Distribution gelten. Das betrifft insbesondere die Konfiguration der Paketquellen sowie distributionsspezifische Programme wie das Ubuntu Software-Center.

Debian

Debian-Pakete sind in drei Gruppen eingeteilt: Paketgruppen

- *Main:* Das sind die Basispakete von Debian. Der Quellcode dieser Pakete ist unter einer Lizenz verfügbar, die den strengen Regeln des Debian-Projekts entspricht. Das garantiert, dass die Nutzung und Weitergabe wirklich frei im Sinne der Open-Source-Idee ist.
- *Contrib:* Pakete dieser Gruppe sind ebenfalls samt Quellcode frei verfügbar. Die Pakete können allerdings nur in Kombination mit *Non-Free*-Paketen verwendet werden. Das betrifft z. B. alle Programme, die auf Bibliotheken aufbauen, deren Lizenz in irgendeiner Weise Einschränkungen unterliegt.
- *Non-Free:* Pakete dieser Gruppe sind zwar kostenlos, ihre Lizenz entspricht aber nicht dem Open-Source-Ideal des Debian-Projekts. Zu vielen *Non-Free*-Paketen steht überhaupt kein öffentlicher Quellcode zur Verfügung.

Zudem unterscheidet Debian zwischen *Stable*-, *Testing*- und *Unstable*-Paketen:

- Als *Stable* gelten nur die Pakete, die Bestandteil der aktuellen, offiziellen Debian-Distribution sind. Diese Pakete sind in der Regel stabil und sicher, aber nicht besonders aktuell.
- Aktuellere Versionen können Sie installieren, wenn Sie die *Unstable*-Paketquellen einrichten. Wie der Name bereits ausdrückt, setzen Sie damit zu einem gewissen Grad die Stabilität Ihres Systems aufs Spiel. (Aber auch Ubuntu greift überwiegend auf *Unstable*-Pakete zurück – zu viel Angst ist also nicht angebracht.) Die Summe der *Unstable*-Pakete stellt den aktuellen Debian-Entwicklungsstand dar. Für den *Unstable*-Zweig sind keine offiziellen Updates vorgesehen. Bekannte Fehler werden einfach durch die Veröffentlichung einer neuen Version behoben.

- Sozusagen als Übergangsstadium zwischen *Stable* und *Unstable* sind die *Testing*-Pakete gedacht. *Unstable*-Pakete, bei denen zehn Tage lang keine kritischen Fehler entdeckt werden, landen automatisch in *Testing* (allerdings nur, wenn auch alle abhängigen Pakete frei von kritischen Fehlern sind!).

Die drei Zweige haben jeweils Debian-interne Codenamen: Momentan steht »Wheezy« für *Stable*, »Jessie« für *Testing* und »Sid« für *Unstable*. Der Codename für *Unstable* bleibt immer gleich. Wenn Debian 8 fertig wird, bekommt es den Namen »Jessie«, und der *Testing*-Zweig erhält einen neuen Namen.

Je nach Entwicklungsstand kann es vorübergehend auch *Experimental*-Pakete geben, um fundamental neue Konzepte auszuprobieren.

sources.list

Damit das APT-System Zugriff auf alle Pakete samt Updates hat, sollte `sources.list` wie im folgenden Beispiel aussehen:

```
deb http://debian.inode.at/debian/ wheezy         main contrib non-free
deb http://debian.inode.at/debian/ wheezy-updates main contrib non-free
deb http://security.debian.org/    wheezy/updates main contrib non-free
```

Dabei ersetzen Sie `debian.inode.at` durch einen geografisch nahe liegenden Mirror-Server. Beachten Sie, dass nach einer Debian-Neuinstallation `non-free` nicht enthalten ist. Wenn Sie also Zugang zu *Non-Free*-Paketen wünschen, müssen Sie `non-free` selbst hinzufügen! Falls Sie auch Quellcodepakete installieren möchten, kopieren Sie die obigen drei Zeilen und ersetzen jeweils `deb` durch `deb-src`.

Backports

Eine mögliche Alternative zur *testing*-Paketquelle ist die *backports*-Paketquelle. Die dort enthaltenen Pakete gelten als etwas stabiler, dafür ist die Auswahl deutlich geringer. Um die Backports-Paketquelle zu nutzen, fügen Sie die folgende Zeile zu `/etc/apt/sources.lst` hinzu; dabei ersetzen Sie wieder `debian.inode.at` durch einen nahegelegenen Mirror-Server.

```
# in /etc/apt/sources.lst
deb http://debian.inode.at/debian/ wheezy-backports main contrib non-free
```

Um zu vermeiden, dass beim nächsten Update alle installierten Pakete durch neuere Backport-Versionen ersetzt werden, sind die Backports-Pakete durch die Einstellung `NotAutomatic: yes` in der Release-Datei der Paketquelle so gekennzeichnet, dass sie eine geringere Priorität als normale Pakete haben. Deswegen müssen Sie bei der Installation von Backports-Paketen mit `aptitude` explizit die Option `-t wheezy-backports` angeben.

```
root#  aptitude -t wheezy-backports install paketname
```

Fedora

Zusätzliche Paketquellen

Zur Installation von proprietären Treibern, Multimedia-Codecs etc. müssen Sie die Paketquelle RPM Fusion einrichten (siehe Abschnitt 3.3).

FedUp

Der Fedora Upgrader, kurz FedUp, ermöglicht es, ein Fedora-System im laufenden Betrieb zu aktualisieren. Um ein Update von Fedora 18 auf Version 19 durchzuführen und die erforderlichen Pakete aus dem Netzwerk herunterzuladen, gehen Sie so vor:

```
root#  yum install fedup
root#  fedup-cli --network 19
root#  reboot
```

Beim Neustart enthält der Bootloader einen neuen FedUp-Eintrag zur Durchführung des Updates. Das eigentliche Update wird erst jetzt automatisch durchgeführt. Der Vorgang dauert ca. eine viertel Stunde. Danach wird der Rechner automatisch neu gestartet. Bei meinen Tests hat das Update gut funktioniert. Hintergrundinformationen und Tipps zum Umgang mit FedUp finden Sie hier:

https://fedoraproject.org/wiki/FedUp

DNF

Man würde meinen, es gäbe mit Yum, APT und ZYpp bereits genug Paketmanager. Die Fedora-Entwickler sehen das offensichtlich anders: Parallel zu Yum, das weiterhin standardmäßig zum Einsatz kommt, gibt es seit Version 18 den neuen, noch experimentellen Paketmanager mit dem Namen DNF (Paketname `dnf`). DNF ist in der Bedienung kompatibel zu YUM, basiert aber auf anderen Bibliotheken:

- Die ursprünglich von openSUSE entwickelte Bibliothek `libsolv` ist für die korrekte Auflösung der Paketabhängigkeiten verantwortlich.
- `hawkey` kümmert sich um die Kommunikation mit RPM und `libsolv`. RPM bleibt also auch für DNF das Fundament.

Im Vergleich zu Yum soll DNF einen besser strukturierten Code aufweisen, weniger Speicher beanspruchen und schneller sein. Davon abgesehen ändert sich wenig. Zur Installation eines Pakets führen Sie nun `dnf install name` aus, ein Update führen Sie mit `dnf update` durch etc. Bei meinen wenigen Tests hat sich DNF wie YUM verhalten, d. h., ich konnte weder Vor- noch Nachteile feststellen. Beachten Sie aber, dass es für etliche Yum-Plugins noch keine DNF-Alternativen gibt. Insbesondere müssen Sie bei Updates auf Delta-RPMS verzichten. Weitere Informationen zu DNF können Sie hier nachlesen:

http://fedoraproject.org/wiki/Features/DNF

openSUSE

Paketverwaltung mit YaST

Unter openSUSE können Sie zur Paketverwaltung YaST verwenden. Dieses Konfigurationsprogramm stellt in der Gruppe Software gleich fünf Module zur Auswahl. Gerade SUSE-Einsteigern fällt es manchmal schwer, unter den ähnlich lautenden Einträgen den richtigen zu finden. Der folgende Überblick gibt eine erste Orientierungshilfe. Die wichtigsten Module werden im Anschluss genauer vorgestellt.

- Medien-Überprüfung testet, ob eine Installations-CD oder -DVD frei von Fehlern ist.
- Online-Aktualisierung startet YOU (YaST Online Update), um aktualisierte Pakete oder Sicherheits-Updates herunterzuladen. Neben YOU gibt es noch zwei weitere Update-Programme, die beide auf PackageKit basieren: `apper` (KDE) und `gpk-update-viewer` (Gnome).
- Software installieren und löschen führt zum zentralen Paketverwaltungsmodul, mit dem Sie neue SUSE-Pakete installieren, vorhandene entfernen oder aktualisieren können etc. Dieses Modul werden Sie vermutlich am häufigsten einsetzen.
- Software Repositories hilft bei der Verwaltung der Paketquellen. Mit Hinzufügen • Community/Gemeinschafts-Repositories können Sie populäre Paketquellen mit wenigen Mausklicks einrichten.
- Zusatz-Produkte ermöglicht die Installation zumeist kommerzieller Programme, die auf einer SUSE-kompatiblen CD oder in SUSE-Paketquellen im Internet angeboten werden. Dieses Modul ist *nicht* dazu gedacht, um gewöhnliche, zu SUSE gehörende Pakete zu installieren – dazu verwenden Sie Software installieren!

Software installieren

Für das YaST-Modul Software • Software installieren und löschen gibt es zwei grundverschiedene Implementierungen: Die KDE-Variante entspricht dem, was SUSE-Anwender seit vielen Jahren gewöhnt sind. Die neuere Gnome-Variante bietet dieselben Funktionen, ist aber etwas einfacher zu bedienen. Im Folgenden beziehe ich mich auf die KDE-Version.

Im Hauptfenster können Sie mit dem Button Anzeigen verschiedene Ansichten (Dialogblätter) öffnen und im weiteren Verlauf zwischen ihnen wechseln. In Abbildung 22.5 sind nur zwei dieser Dialogblätter offen.

- Suchen: In dieser Ansicht können Sie nach Paketen suchen, deren Namen oder deren Funktion Sie kennen.
- RPM-Gruppen: Hier werden die Pakete in einer baumartigen Gruppenstruktur dargestellt (z. B. alle Pakete der Gruppe Entwicklung • Werkzeuge • Building). Die Orientierung in dem verzweigten Baum ist allerdings schwierig.

- INSTALLATIONSÜBERBLICK: In dieser Ansicht sehen Sie, welche Pakete momentan zur Installation, zum Update oder zum Entfernen markiert sind.
- PAKETGRUPPEN: In dieser Ansicht werden Pakete angezeigt, die inhaltlich zusammenpassen, z. B. alle Spiele.
- SCHEMATA: In dieser Ansicht werden Pakete angezeigt, die funktionell zusammengehören, z. B. alle Pakete zum Einrichten eines Webservers (siehe Abbildung 22.5). Damit können Sie rasch und bequem alle Pakete zur Erfüllung einer bestimmten Aufgabe zur Installation auswählen. Im Prinzip verfolgen SCHEMATA und PAKETGRUPPEN dieselbe Idee, einzig die Gruppierungslogik ist anders.
- SPRACHEN: Diese Ansicht zeigt alle Lokalisierungspakete für eine bestimmte Sprache.
- INSTALLATIONSQUELLEN: Diese Ansicht zeigt alle Pakete einer ausgewählten Paketquelle. Optional kann die oft sehr lange Paketliste mit einem zweiten Filter reduziert werden.

Der Paketmanager überprüft bei jeder Installation die Paketabhängigkeiten und aktiviert gegebenenfalls weitere Pakete zur automatischen Installation bzw. zum Update. Falls Abhängigkeitskonflikte auftreten, zeigt YaST verschiedene Vorschläge an, wie das Problem zu beheben ist.

Der Status von Paketen wird durch Symbole ausgedrückt. Der Zustand kann per Maus (verwenden Sie gegebenenfalls das Kontextmenü mit der rechten Maustaste!) oder per Tastatur verändert werden. Eine vollständige Beschreibung aller Symbole erhalten Sie mit HILFE • SYMBOLE.

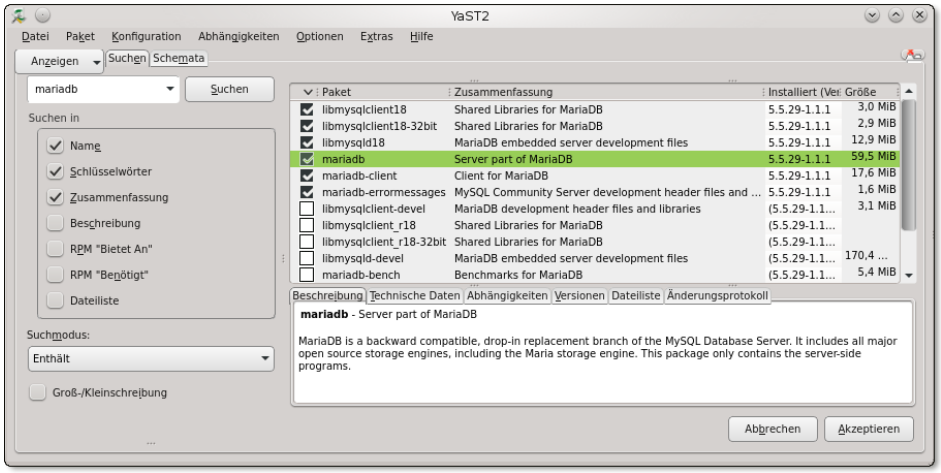


Abbildung 22.5 Installation von Software-Paketen mit YaST unter KDE

One-Click-Install (*.ymp-Dateien)

Das Verfahren *One-Click-Install* ermöglicht es, dass ein Klick im Webbrowser auf eine YMP-Datei die angeführten Paketquellen bleibend einrichtet und alle angegebenen Pakete installiert. Hinter den Kulissen kümmert sich ein YaST-Modul um diese Arbeiten. Vor dem Beginn der Installation müssen Sie natürlich das `root`-Passwort angeben. Bei den YMP-Dateien handelt es sich um einfache XML-Dateien, die alle erforderlichen Informationen (Paketquellen, Paketnamen etc.) enthalten. YMP steht dabei für *Yast Meta Package*. One-Click-Links lassen sich von `root` auch durch das Kommando `OCICLI` installieren:

```
root# OCICLI "http://eine-website.de/ein-tooles-programm.ymp"
```

Zusätzliche Paketquellen

Die ZYpp-Paketverwaltung greift auf die Installations-DVD sowie Paketquellen aus dem Internet zurück. Beim Einrichten weiterer Paketquellen hilft das YaST-Modul Software Repositories. Falls Sie die Installations-DVD nach der Installation *nicht* weiter als Paketquelle verwenden möchten, können Sie die DVD-Paketquelle in diesem Modul explizit deaktivieren. Damit verschwinden die lästigen Fragen nach dem Einlegen der DVD bei jeder Paketinstallation.

Hinzufügen • Community/Gemeinschaft-Repositories hilft beim Einrichten populärer Paketquellen. Tabelle 22.6 zählt die wichtigsten Kandidaten auf. Der openSUSE BuildService ist mit Ubuntus PPAs zu vergleichen. Wenn Sie eine dieser Paketquellen aktivieren, können Sie unkompliziert aktuelle Versionen von KDE, Gnome, LibreOffice, VirtualBox etc. installieren. Die Paketquellen werden von der openSUSE-Community zur Verfügung gestellt.

http://de.opensuse.org/Build_Service

Paketquelle	Inhalt
Packman	Multimedia-Pakete
nVidia Graphics Drivers	proprietäre NVIDIA-Grafiktreiber
openSUSE BuildService	aktuelle Versionen von KDE, Gnome, LXDE, PHP, Python, Perl etc.

Tabelle 22.6 Wichtige openSUSE-Paketquellen

Updates

openSUSE leistet sich den Luxus, *zwei* Update-Manager mitzuliefern: PackageKit und das YaST-Modul Online-Aktualisierung. PackageKit ist dafür zuständig, aus dem jeweiligen Desktop-System heraus Updates durchzuführen, wobei es für Gnome und KDE jeweils eigene Oberflächen gibt. YOU (*Yast Online Update*) ist hingegen ein Relikt aus früheren SUSE-Zeiten. Sein Einsatz empfiehlt sich nur, wenn die KDE- oder Gnome-Update-Werkzeuge Probleme bereiten oder Sie einen KDE- und Gnome-freien Desktop nutzen. Alternativ können Sie Updates auch in einem Terminalfenster durchführen:

```
root# zypper update
```

Automatische Installation des Flash-Plugins

Im Rahmen des ersten Updates wird automatisch das Flash-Plugin von Adobe installiert. Für den Automatismus ist ein winziges, vorinstalliertes Trigger-Paket verantwortlich, dessen Namen mit `pullin` beginnt (z. B. `pullin-flash-player`). Eine Liste dieser Pakete erstellt `rpm -qa | grep pullin`. Erst das Update der `pullin`-Pakete initiiert die Installation der eigentlichen Pakete.

Distributions-Updates

SUSE bietet zwei Möglichkeiten, ein Distributions-Update durchzuführen:

- **Mit einer Installations-DVD:** Diese Update-Variante verläuft ähnlich wie eine Neuinstallation. Sie starten den Rechner mit der Installations-DVD neu. Das Installationsprogramm erkennt die vorhandene openSUSE-Version und bietet deren Aktualisierung als Option an. Diese Vorgehensweise ist gut ausgereift und wird weiterhin unterstützt, sie hat aber einen großen Nachteil: Das System ist während des Updates, das circa eine halbe Stunde dauert, *offline*.
- **Im laufenden Betrieb:** Um ein Update im laufenden Betrieb durchführen, müssen Sie zuerst die vorhandenen Repositories löschen und durch neue Repositories für die gerade aktuelle openSUSE-Version ersetzen. Anschließend führen Sie in einer Konsole `zypper dup` aus. Anschließend ist ein Neustart erforderlich.

Rolling Release mit Tumbleweed

Linux-Experten und -Entwickler, die nach Möglichkeit immer die neuesten Software-Versionen einsetzen möchten, können mit dem Projekt Tumbleweed openSUSE zu einer Rolling-Release-Distribution machen. Das bedeutet, dass neue Programmversionen im Rahmen von täglichen Updates installiert werden und keine Notwendigkeit besteht, immer wieder eine neue openSUSE-Version zu installieren bzw. ein entsprechendes Distributions-Update durchzuführen.

```
root#  zypper ar --refresh \
    http://download.opensuse.org/repositories/openSUSE:/Tumbleweed/standard/ \
     Tumbleweed
root#  zypper dup
```

Tumbleweed versucht, neue Software-Versionen zu aktivieren, sobald diese einigermaßen stabil sind. Dennoch sind beim Einsatz von Tumbleweed natürlich gelegentlich Probleme zu erwarten, wenn eine neue Software-Version doch noch Fehler enthält oder Inkompatibilitäten mit anderen Komponenten verursacht. Die Tumbleweed-Projektseite warnt vor dem Einsatz von Tumbleweed, wenn Sie proprietäre Treiber benötigen (NVIDIA, ATI), zusätzliche Paketquellen außer *Oss*, *Non-Oss* und *Update* aktiviert haben oder openSUSE in einer virtuellen Maschine ausführen:

http://en.opensuse.org/Portal:Tumbleweed

Sprachpakete

Um die Lokalisierungspakete für eine bestimmte Sprache zu installieren, starten Sie das YaST-Modul System • Sprache und wählen dort die gewünschten Sprachen aus.

Ubuntu

Software-Center

Ubuntu versucht Linux-Einsteigern die Paketinstallation mit dem Software-Center besonders einfach zu machen (siehe Abbildung 22.6). Das Programm hat gewisse Ähnlichkeiten mit Apples App Store und bietet ein paar Spiele zum Kauf an. Lassen Sie sich davon nicht irritieren – nahezu alle Programme, die das Ubuntu Software-Center feilbietet, sind natürlich kostenlose Open-Source-Pakete!

Abbildung 22.6 Das Ubuntu Software-Center

Das Software-Center hilft auch bei der Installation von proprietären Treibern. Dazu führen Sie BEARBEITEN • PAKETQUELLEN aus und wechseln in das Dialogblatt ZUSÄTZLICHE TREIBER. Das Programm analysiert nun Ihre Hardware und bietet gegebenenfalls passende Treiber zur Installation an.

Paketquellen

Es gibt vier Ubuntu-Paketgruppen, die alle standardmäßig in `/etc/apt/sources.list` aktiviert sind:

- **Uneingeschränkt unterstützt (main):** Diese Pakete sind Bestandteil von Ubuntu, sind frei verfügbar und können ohne Lizenzprobleme frei weitergegeben werden. `main`-Pakete werden vom Ubuntu-Team gewartet und mit Updates versorgt.
- **Eingeschränktes Copyright (restricted):** `restricted`-Pakete enthalten Programme, die für die Funktion von Ubuntu Linux wichtig sind, die aber nicht als Open-Source-Software vorliegen. Dabei handelt es sich insbesondere um Hardware-Treiber für Grafik- und WLAN-Karten. Auch die `restricted`-Pakete werden offiziell von Ubuntu unterstützt und gewartet. Bei Sicherheits-Updates ist das Ubuntu-

Team allerdings auf die Unterstützung der Firmen angewiesen, die die jeweiligen Programme zur Verfügung stellen.

- **Von der Gemeinschaft verwaltet (universe):** `universe`-Pakete enthalten Open-Source-Programme, die nicht vom Ubuntu-Team gewartet werden. Stattdessen kümmern sich Mitglieder der Ubuntu-Community um diese Pakete.
- **Unfrei (multiverse):** `multiverse`-Pakete enthalten Programme oder Daten, die nicht unter einer Open-Source-Lizenz stehen bzw. die nicht den Debian-Regeln für eine freie Verbreitung entsprechen. Die Pakete werden wie `universe`-Pakete nicht von Ubuntu gewartet.

Partner-Pakete

Die `partner`-Paketquelle wird von der Firma Canonical gewartet. Sie enthält kommerzielle Programme, die kostenlos weitergegeben werden dürfen – zuletzt z. B. den Adobe Reader und Skype. In der Vergangenheit wurden die Pakete der `partner`-Paketquelle leider nur sehr schlecht gewartet; im Laufe der Zeit waren die wenigen verfügbaren Pakete auch noch veraltet. Am einfachsten aktivieren Sie die `partner`-Paketquelle im Software-Center mit BEARBEITEN • PAKETQUELLEN im Dialogblatt ANDERE SOFTWARE.

Personal Package Archives

PPA steht für *Personal Package Archive* und ist eine Möglichkeit für Ubuntu-Entwickler, aktuelle Versionen von diversen Programmen zur Verfügung zu stellen, ohne diese offiziell in die Ubuntu-Paketquellen zu integrieren. PPAs bieten oft die schnellste Möglichkeit, um neue (Test-)Versionen von X-Treibern, LibreOffice, Gimp etc. relativ gefahrlos in Ubuntu zu integrieren. Weitere Informationen über PPAs finden Sie hier:

https://launchpad.net/ubuntu/+ppas

Um eine PPA-Paketquelle einzurichten, führen Sie einfach das folgende Kommando aus:

```
user$ sudo add-apt-repository ppa:name
```

Sprachpakete

Im Systemeinstellungsmodul SPRACHEN können Sie Sprachpakete für die aktuelle oder für eine weitere Sprache installieren bzw. vervollständigen und die Standardsprache einstellen. Die Änderung der Standardsprache wird beim nächsten Login wirksam. Das Modul SPRACHEN kümmert sich allerdings nur um direkt zu Ubuntu gehörige Programme. Wenn Sie außerdem auch KDE-Programme installiert haben (z. B. Amarok), müssen Sie für deren Lokalisierung das Paket `kde-l10n-de` installieren.

Updates

Wenn Ubuntu Software-Updates feststellt, startet es automatisch das Programm SOFTWARE-AKTUALISIERUNG (`update-manager`), wobei das Fenster aber minimiert bleibt. Es taucht also plötzlich das Icon des Update-Managers im Dock auf. Weil viele Anwender dieses Icon ganz einfach übersehen, weist Ubuntu auch im Systemmenü auf mögliche Updates hin.

Distributions-Updates

Durch das Update-System werden normalerweise nur einzelne Programme aktualisiert, nicht aber die ganze Distribution. Sobald das Update-System eine neue Ubuntu-Version erkennt, fragt es, ob es ein vollständiges Distributions-Update durchführen soll. Antworten Sie nicht leichtfertig mit JA! Distributions-Updates dauern relativ lange und sind häufig mit Problemen verbunden.

Bei Bedarf können Sie das Distributions-Update auch manuell mit `do-release-update -m desktop` (für Desktop-Systeme) bzw. `-m server` (für Server) starten. Bei Ubuntu LTS-Versionen sind Release-Updates nur für die nächste LTS-Version vorgesehen, also z. B. von 12.04 auf 14.04. Wenn Sie ein Update auf eine Nicht-LTS-Version durchführen möchten, müssen Sie vorher in `/etc/update-manager/release-upgrades` die Variable `Prompt` von `lts` auf `normal` stellen.

Kapitel 23
Bibliotheken, Java und Mono

Im Mittelpunkt dieses Kapitels stehen Bibliotheken, die zur Ausführung von Programmen erforderlich sind. Die meisten Linux-Programme stehen in kompilierter Form zur Verfügung und greifen auf diverse Bibliotheken zurück, die dynamisch bei Bedarf geladen werden. Der erste Abschnitt dieses Kapitels führt in die unter Linux übliche Bibliotheksverwaltung ein.

Wenn Sie mit gängigen Distributionen arbeiten, installieren Sie zumeist nur fertig kompilierte Programme in Form von sogenannten Binärpaketen. Wenn Sie allerdings ganz neue Programmversionen oder selten benutzte Programme einsetzen möchten, kann es sein, dass Sie keine vorkompilierte Version des Programms zum Download finden. In solchen Fällen müssen Sie den Quellcode (meist in den Sprachen C oder C++) herunterladen und das Programm selbst kompilieren. Abschnitt 23.2 gibt dazu einige einführende Tipps, ohne aber im Detail auf das unerschöpfliche Thema *Programmentwicklung unter Linux* einzugehen.

Das Kapitel beschreibt auch, wie unter Linux Java- bzw. .NET-Programme ausgeführt werden. Dazu muss eine Java-Laufzeitumgebung bzw. Mono installiert werden. Bei vielen Distributionen ist das standardmäßig der Fall.

Scripts, die von einem Interpreter ausgeführt werden, sind nicht Thema dieses Kapitels. Unter Linux sind diverse Script-Sprachen üblich, unter anderem Perl, Python, PHP sowie die Shell `bash`. Dieses Buch geht allerdings nur auf die `bash` ausführlich ein (siehe Kapitel 14).

23.1 Bibliotheken

Praktisch alle Linux-Programme verwenden dieselben Standardfunktionen, beispielsweise zum Zugriff auf Dateien, zur Ausgabe am Bildschirm, zur Unterstützung von X etc. Es wäre sinnlos, wenn jedes noch so kleine Programm all diese Funktionen unmittelbar im Code enthalten würde – riesige Programmdateien wären die Folge. Stattdessen bauen die meisten Linux-Programme auf sogenannten *Shared Libraries* auf: Bei der Ausführung eines Programms werden automatisch die erforderlichen

Bibliotheken geladen. Der Vorteil: Wenn mehrere Programme Funktionen derselben Bibliothek nutzen, muss die Bibliothek nur einmal geladen werden.

Bibliotheken spielen eine zentrale Rolle dabei, ob und welche Programme auf Ihrem Rechner ausgeführt werden können. Fehlt auch nur eine einzige Bibliothek bzw. steht sie in einer zu alten Version zur Verfügung, kommt es beim Programmstart zu einer Fehlermeldung. Damit Sie in solchen Fällen nicht ganz hilflos den Tiefen der Linux-Interna ausgeliefert sind, vermittelt dieser Abschnitt einige Grundlageninformationen zu Bibliotheken.

glibc

Zu den wichtigsten und grundlegendsten Linux-Bibliotheken zählt die GNU C Library (glibc), die mitunter auch als libc 6 bezeichnet wird. Im Sommer 2013 lag die glibc in der Versionsnummer in der Version 2.17 vor. Normalerweise gibt es pro Jahr zwei bis drei Versions-Updates.

Aufgrund von Schwierigkeiten mit dem Verwalter der glibc-Bibliothek verwenden Debian und Ubuntu nicht die originale glibc-Bibliothek, sondern die dazu vollkommen kompatible Bibliothek eglibc.

Dynamisch und statisch gelinkte Programme

Gewöhnliche Programme greifen wie oben beschrieben auf Bibliotheken zurück. Diese Bibliotheken werden erst zur Laufzeit dynamisch geladen und sind vom Konzept her mit Windows-DLLs (Dynamic Link Libraries) zu vergleichen.

Beim Kompilieren eines Programms besteht auch die Möglichkeit, Libraries statisch zu linken. Das bedeutet, dass die Library-Funktionen direkt in den Programmcode integriert werden. Die Programmdatei wird dadurch größer, ist aber nicht mehr von irgendwelchen Libraries abhängig. Das ist praktisch, um Programme unkompliziert weiterzugeben.

Bibliotheken automatisch laden

Sofern Sie Linux als Anwender und nicht als Programmierer nutzen, werden Sie mit Bibliotheken nur dann konfrontiert, wenn diese fehlen. Meistens treten solche Probleme auf, wenn Sie manuell, also ohne Paketverwaltungswerkzeuge, ein neues Programm installieren. Beim Versuch, das Programm zu starten, erscheint eine Fehlermeldung, in der das Fehlen einer bestimmten Library angezeigt wird.

Bibliotheksliste feststellen

Dem Kommando `ldd` wird als Parameter der vollständige Dateiname des Programms übergeben. Als Reaktion listet `ldd` alle Libraries auf, die das Programm benötigt. Außerdem wird angegeben, wo sich eine passende Library befindet und welche Libraries fehlen bzw. nur in einer veralteten Version zur Verfügung stehen.

```
user$  ldd /bin/cp
  linux-vdso.so.1 =>  (0x00007fff021fe000)
  libselinux.so.1 => /lib64/libselinux.so.1 (0x00000030a8e00000)
  libacl.so.1 => /lib64/libacl.so.1 (0x00000030c2e00000)
  libattr.so.1 => /lib64/libattr.so.1 (0x00000030bca00000)
  libc.so.6 => /lib64/libc.so.6 (0x00000030a7200000)
  libdl.so.2 => /lib64/libdl.so.2 (0x00000030a7600000)
  libpcre.so.1 => /lib64/libpcre.so.1 (0x00000030a8a00000)
  libpthread.so.0 => /lib64/libpthread.so.0 (0x00000030a7a00000)
  /lib64/ld-linux-x86-64.so.2 (0x00000030a6e00000)
```

Bei X-, KDE- und Gnome-Programmen ist die Bibliotheksliste wesentlich länger. Das ist auch der Grund, warum der Start dieser Programme relativ lange dauert. Wenn `ldd` hingegen das Ergebnis *not a dynamic executable* liefert, handelt es sich um ein Programm, das alle erforderlichen Bibliotheken bereits enthält, also um ein statisch gelinktes Programm.

Bibliotheksnamen

Kurz einige Informationen zur Nomenklatur der Libraries: Das Kürzel `.so` weist darauf hin, dass es sich um eine Shared Library handelt (im Gegensatz zu `.a` für statische Libraries). Die folgende Ziffer gibt die Hauptversionsnummer an. `cp` benötigt also Version 6 der `libc`-Bibliothek.

In den Verzeichnissen `/lib`, `/lib64`, `/usr/lib` etc. befinden sich oft Links von der Hauptversion auf die tatsächlich installierte Version. So benötigt `cp` die Bibliothek `ld-linux-x86-64` in der Version 2. Tatsächlich ist aber die dazu kompatible Version 2.17 installiert:

```
user$  ls -l /lib64/ld-*
... /lib64/ld-2.17.so
... /lib64/ld-linux-x86-64.so.2 -> ld-2.17.so
```

Programmstart

Beim Start eines Programms ist der sogenannte *Runtime Linker* `ld.so` dafür zuständig, alle Bibliotheken zu finden und zu laden. Dazu wertet der Linker die Datei`/etc/ld.so.cache` aus. Diese Binärdatei enthält alle relevanten Bibliotheksdaten, also Versionsnummern, Zugriffspfade etc. Der Zweck dieser Datei besteht darin, dem Linker eine langwierige Suche nach den Bibliotheken zu ersparen.

`/etc/ld.so.cache` wird vom Programm `ldconfig` erzeugt. `ldconfig` wertet seinerseits `/etc/ld.so.conf` aus. Diese Datei enthält eine Liste mit Pfadangaben bzw. Querverweise auf andere Konfigurationsdateien.

Die Verzeichnisse `/lib` und `/usr/lib` werden auf jeden Fall berücksichtigt und fehlen daher zumeist in `ld.so.conf` bzw. in den weiteren Konfigurationsdateien. Wenn außer `/lib` und `/usr/lib` keine weiteren Verzeichnisse zu berücksichtigen sind, kann `ld.so.conf` auch ganz fehlen.

Bei manchen Distributionen wird `ldconfig` bei jedem Rechnerneustart ausgeführt, um so sicherzustellen, dass die Cache-Datei auf dem aktuellsten Stand ist. `ldconfig` muss unbedingt ausgeführt werden, wenn neue Bibliotheken manuell installiert werden! Andernfalls sind die Bibliotheken für das System nicht sichtbar. Falls sich die Bibliotheken in einem neuen Verzeichnis befinden, muss außerdem die Datei `/etc/ld.so.conf` entsprechend ergänzt werden. Bei der Installation von Bibliothekspaketen kümmert sich in der Regel der Paketmanager um diese Aufgaben.

`ld.so` berücksichtigt zusätzlich alle in der Umgebungsvariable `LD_LIBRARY_PATH` enthaltenen Verzeichnisse. Die Verzeichnisse müssen durch Doppelpunkte getrennt sein. Bei vielen Distributionen ist diese Umgebungsvariable leer.

32- und 64-Bit-Bibliotheken

Die meisten gängigen Distributionen gibt es momentan in zumindest zwei Ausführungen: für Intel/AMD-kompatible 32-Bit-Prozessoren und für Intel/AMD-kompatible 64-Bit-Prozessoren. Bei 32-Bit-Distributionen gibt es naturgemäß nur 32-Bit-Bibliotheken. Dies gilt aber leider nicht analog für 64-Bit-Distributionen: Nach wie vor gibt es Programme, die sich nicht für 64-Bit-Systeme kompilieren lassen.

/lib und /lib64

Zur Ausführung von 32-Bit-Programmen auf 64-Bit-Distributionen sind 32-Bit-Bibliotheken erforderlich. Um Konflikte zu vermeiden, werden die Bibliotheken in unterschiedliche Verzeichnisse installiert. Im Linux-Jargon heißt diese Vorgehensweise *Multi Architecture* (*Multiarch*) bzw. exakter *Bi-architecture*, weil mehrere bzw. zwei Prozessorarchitekturen parallel unterstützt werden. Bei den meisten Distributionen sind die Verzeichnisse `/lib` und `/lib64` üblich, um zwischen 32- und 64-Bit-Bibliotheken zu differenzieren. Diese Doppelgleisigkeit ist natürlich mit Nachteilen verbunden: Die doppelte Installation von Bibliotheken erfordert zusätzlichen Platz auf der Festplatte und macht die Wartung komplizierter.

Bei älteren Debian- und Ubuntu-Versionen wurde in der Regel das Metapaket `ia32-libs` benutzt, um auf 64-Bit-Systemen einen Grundstock von 32-Bit-Bibliotheken zu installieren.

Multiarch

Ein neuer Ansatz besteht darin, innerhalb von `/usr/lib` Unterverzeichnisse für die jeweilige CPU-Architektur zu schaffen, z. B. `/usr/lib/x86_64-linux-gnu` (Debian ab Version 7, Ubuntu ab Version 12.04). Der Vorteil dieses Ansatzes besteht darin, dass er über die Intel/AMD-Welt hinaus auch auf ganz andere CPU-Architekturen übertragbar ist.

Die Multiarch-Idee erstreckt sich über Verzeichnispfade hinweg auch auf die Paketverwaltung: Es muss zum Beispiel möglich sein, ein und dasselbe Paket bei Bedarf

mehrfach zu installieren, einmal in der 32-Bit- und einmal in der 64-Bit-Version. Zur klareren Unterscheidung kann dem Paketnamen die Architektur mit einem Doppelpunkt angehängt werden, z. B. `gvfs:i386` (bezeichnet die 32-Bit-Version des `gvfs`-Pakets). Auch die Abhängigkeitsüberprüfung muss nun doppelläufig arbeiten (also für 32- und 64-Bit-Abhängigkeiten). Das `dpkg`-Kommando unterstützt den Multiarch-Ansatz bereits gut.

Das Multiarch-Konzept macht das `ia32-libs`-Paket obsolet. Aus Kompatibilitätsgründen existiert dieses Paket aber weiterhin. Es definiert nun nur noch die Abhängigkeit zu `ia32-libs-multiarch`. Dabei handelt es sich um ein reines 32-Bit-Metapaket. Eine ausführliche Beschreibung der Multiarch-Implementierung unter Debian und Ubuntu finden Sie hier:

http://lwn.net/Articles/482952
https://lists.ubuntu.com/archives/ubuntu-devel/2011-October/034279.html

Prelinking

Beim Start eines Programms, das auf dynamische Bibliotheken zurückgreift, muss eine Verbindung zwischen dem Programm und den Bibliotheken hergestellt werden. Dieser Vorgang wird als *Linking* bezeichnet. Er beansprucht bei komplexen Programmen geraume Zeit.

Das Programm `prelink` kann die erforderlichen Link-Informationen im Voraus ermitteln, was beim ersten Mal ebenfalls lange dauert. Bei diesem Vorgang müssen alle ausführbaren Programme durchsucht werden. Welche Verzeichnisse für Programme und Bibliotheken `prelink` berücksichtigt, wird durch die Datei `/etc/prelink.conf` konfiguriert. Weitere Optionen können Sie in `/etc/sysconfig/prelink` bzw. `/etc/default/prelink` (Debian, Ubuntu) einstellen.

In der Folge kann jedes so präparierte Programm viel schneller auf seine Bibliotheken zugreifen und daher schneller starten. Besonders stark merkt man die Beschleunigung beispielsweise bei LibreOffice oder bei KDE-Programmen, deren Startzeit sich in etwa halbiert. Die Prelinking-Informationen müssen allerdings jedes Mal aktualisiert werden, wenn eine Bibliothek aktualisiert wird.

Prelinking hat den Nachteil, dass dadurch die ausführbaren Dateien aller Programme und Bibliotheken verändert werden. Es ist anschließend nicht mehr möglich, die Integrität dieser Dateien zu kontrollieren. Immerhin können Sie mit `prelink -ua` alle Prelinking-Veränderungen rückgängig machen. Hintergrundinformationen zum Prelinking finden Sie auf der `man`-Seite zu `prelink` sowie unter:

http://www.gentoo.org/doc/en/prelink-howto.xml

Debian, Ubuntu Um Prelinking unter Debian und Ubuntu zu nutzen, müssen Sie das Paket `prelink` installieren und in `/etc/default/prelink` die Einstellung `PRELINKING=yes` vornehmen. `prelink` wird täglich durch einen Cron-Job ausgeführt.

Red Hat, Fedora Bei Fedora und Red Hat ist Prelinking standardmäßig eingerichtet. Die Prelinking-Informationen werden regelmäßig aktualisiert (Cron-Job `/etc/cron.daily/prelink`, Konfigurationsdatei `/etc/sysconfig/prelink`).

SUSE Um Prelinking in SUSE-Distributionen zu nutzen, müssen Sie das Paket `prelink` installieren und dann in `/etc/sysconfig/prelink` die Einstellung `PRELINKING=yes` vornehmen. `prelink` wird in Zukunft nach jeder Installation von Programmen oder Bibliotheken durch das YaST-Script `/sbin/conf.d/SuSEconfig.prelink` ausgeführt.

23.2 Programme selbst kompilieren

Es gibt zumeist nur zwei Gründe dafür, Linux-Programme selbst zu kompilieren: Entweder finden Sie für das gewünschte Programm und Ihre Distribution kein Binärpaket mit dem fertig kompilierten Programm, oder Sie möchten das Programm mit einer vom Standard abweichenden Konfiguration kompilieren.

Voraussetzungen Bevor Sie zur Tat schreiten, müssen einige Voraussetzungen erfüllt sein:

- Die *GNU Compiler Collection* (Pakete `gcc` und `gcc-c++`) muss installiert sein. Diese Pakete enthalten Compiler für C und C++.
- Hilfswerkzeuge wie `make`, `automake`, `autoconf` etc. müssen installiert sein. Diese Programme sind für die Konfiguration und Durchführung des Kompilationsprozesses erforderlich.
- Die Entwicklerversionen diverser Bibliotheken müssen installiert sein. Die Namen der entsprechenden Pakete enden bei Red Hat, Fedora und SUSE üblicherweise auf `-devel`, bei Debian und Ubuntu auf `-dev`. Beispielsweise enthält `glibc-devel` bzw. `libc6-dev` die Entwicklungsdateien für die glibc-Basisbibliothek. Welche Entwicklerpakete Sie sonst noch brauchen, hängt von der Natur des Programms ab, das Sie kompilieren möchten. Fehlermeldungen, in denen sich der Compiler oder Linker über fehlende Bibliotheken beklagt, sind ein eindeutiges Indiz dafür, dass Sie ein wichtiges Entwicklerpaket übersehen haben.

Debian, Ubuntu Bei Debian und Ubuntu definiert das Metapaket `build-essential` Abhängigkeiten für die wichtigsten Entwicklerpakete. Deswegen führt die Installation von `build-essential` automatisch zur Installation diverser weiterer Pakete, die zusammen die Grundausstattung für die Programmentwicklung in C/C++ bilden.

Fedora

Um die Grundvoraussetzungen für die Programmentwicklung in Fedora zu erfüllen, führen Sie am einfachsten `yum groupinstall development-tools` aus. Auch für die KDE- und Gnome-Programmentwicklung gibt es eigene Paketgruppen: `kde-software-development` und `gnome-software-development`.

SUSE

Angehende SUSE-Entwickler installieren in YaST alle Pakete des Paketschemas Grundlegende Entwicklungsumgebung. Falls Sie vorhaben, KDE- oder Gnome-Programme zu entwickeln, installieren Sie auch die Selektionen KDE- bzw. Gnome-Entwicklung. Wenn Sie `zypper` vorziehen, führen Sie `zypper install -t pattern devel_basis` bzw. `devel_kde` bzw. `devel_gnome` aus.

Code auspacken

tar

Im Internet finden Sie den Quellcode zumeist in komprimierten TAR-Archiven. Nach dem Download entpacken Sie den Code in ein lokales Verzeichnis:

```
user$  tar xzf name.tar.gz      (für .gz oder .tgz)
user$  tar xjf name.tar.bz2     (für .bz2)
user$  tar xJf name.tar.xz      (für .xz)
user$  cd name
```

SRPM-Pakete

Eine Alternative zu den TAR-Archiven sind Quellcodepakete, die exakt den Code enthalten, aus dem ein bestimmtes Programm Ihrer Distribution kompiliert wurde. Die Quellcodepakete finden Sie in der Regel auf dem (FTP-)Server Ihrer Distribution. Bei Distributionen auf Basis von RPM-Paketen befinden sich die Quellcodedateien in SRPM-Paketen mit der Dateikennung `*.src.rpm`. Zur Installation führen Sie wie üblich `rpm -i` aus:

```
root#  rpm -i name.src.rpm
```

Es hängt von der Distribution ab, wo der Quellcode nun tatsächlich landet:

Fedora, Red Hat:	`/usr/src/redhat/`
SUSE:	`/usr/src/packages/`

- `SOURCES/name.tar.xxx` enthält den eigentlichen Code. Das TAR-Archiv muss wie oben beschrieben entpackt werden.
- `SOURCES/name-xxx.patch` (Red Hat) oder `SOURCES/name.dif` (SUSE) enthält distributionsspezifische Veränderungen am ursprünglichen Code. Wenn Sie die Codedateien entsprechend ändern (patchen) möchten, führen Sie das folgende Kommando aus:

  ```
  user$  cd name-quellcodeverzeichnis
  user$  patch < name.dif/patch
  ```

Je nachdem, welches Verzeichnis gerade aktuell ist und wie die Verzeichnisangaben innerhalb der Patch-Datei sind, müssen Sie zusätzlich die Option `-p1` angeben (siehe `man patch`).

- `SPECS/name.spec` enthält eine Paketbeschreibung, die auch zur Erstellung von RPM-Paketen dient. Wenn Sie aus selbst kompilierten Programmen wieder ein RPM-Paket erstellen möchten, müssen Sie dazu das Kommando `rpmbuild` einsetzen, auf das ich hier aber nicht eingehe. Lesen Sie `man rpmbuild`!

Debian-Quellcodepakete

Bei Debian-basierten Distributionen befindet sich der Quellcode in mehreren Dateien, die Sie am besten mit `apt-get source` in das aktuelle Verzeichnis installieren:

```
user$ apg-get source paketname
```

Im aktuellen Verzeichnis finden Sie nun drei neue Dateien und ein Verzeichnis:

- `paketname.dsc` enthält eine Kurzbeschreibung des Pakets.
- `paketname.orig.tar.gz` enthält ein TAR-Archiv mit dem ursprünglichen Quellcode des Programmentwicklers.
- `paketname.diff.gz` enthält alle Debian- bzw. Ubuntu-spezifischen Änderungen am Originalquellcode.
- Das neue Verzeichnis `paketname/` enthält schließlich den bereits extrahierten Inhalt von `paketname.diff.gz`, wobei alle Änderungen aus der `diff`-Datei bereits ausgeführt wurden.

Programm kompilieren

Zum Kompilieren und Installieren von Programmen sind drei Kommandos erforderlich, die manchmal auch als »Dreischritt« bezeichnet werden: `./configure`, `make` und `make install`. Die drei Kommandos werden im Folgenden näher beschrieben. Dabei setze ich voraus, dass Sie sich im Quellcodeverzeichnis befinden.

configure

`configure` ist ein Script, das testet, ob alle erforderlichen Programme und Bibliotheken verfügbar sind. Da sich das Script im lokalen Verzeichnis befindet, muss es in der Form `./configure` ausgeführt werden. Das Script adaptiert die Datei `Makefile`, die alle Kommandos enthält, um die diversen Codedateien zu kompilieren und zu linken. Bei manchen (zumeist eher kleineren Programmen) kann es sein, dass es das Script `configure` nicht gibt. In diesem Fall führen Sie sofort `make` aus.

```
user$ ./configure
```

make

`make` löst die Verarbeitung der Compile- und Link-Kommandos aus. Sie sehen nun (manchmal schier endlose) Nachrichten und Warnungen der verschiedenen Compiler-Läufe über das Konsolenfenster huschen. Solange kein Fehler auf-

tritt, können Sie diese Meldungen getrost ignorieren. Als Ergebnis sollte sich im Quellcodeverzeichnis nun die ausführbare Datei `name` befinden.

```
user$ make
```

In vielen Fällen können Sie das Programm nun sofort starten (Kommando `./name`) und testen. Beachten Sie aber, dass insbesondere Netzwerk-Dienste eine spezielle Konfiguration erfordern und zumeist nur durch Init-V-Scripts korrekt gestartet werden!

make install

Der letzte Schritt besteht darin, das Programm allen Benutzern zugänglich zu machen. Dazu müssen die Programm- und eventuell auch Bibliotheksdateien in öffentlich zugängliche Verzeichnisse kopiert werden. Das erfordert `root`-Rechte. Vor der Ausführung von `make install` sollten Sie sicherstellen, dass das betreffende Programm nicht schon installiert ist! Wenn das der Fall ist, sollte es vorher deinstalliert werden.

```
root# make install
```

Mögliche Probleme

Während des Kompilierens können vielfältige Probleme auftreten. Am wahrscheinlichsten ist, dass irgendwelche Compiler-Hilfswerkzeuge oder zum Kompilieren notwendige Entwicklerversionen von Bibliotheken fehlen. Diese Probleme werden in der Regel bereits durch `configure` festgestellt und lassen sich meist relativ leicht beheben, indem das fehlende Paket einfach installiert wird.

Schon schwieriger wird es, wenn `configure` nach Bibliotheken verlangt, die in Ihrer Distribution nicht oder nicht in der erforderlichen Version verfügbar sind: Dann müssen Sie sich im Internet auf die Suche nach der betreffenden Bibliothek machen und eventuell zuerst die Bibliothek kompilieren. Zu komplexen Programmen, wie Apache oder `mplayer`, finden Sie im Internet richtiggehende Kompilieranleitungen, in denen Schritt für Schritt beschrieben wird, was in welcher Reihenfolge installiert und kompiliert werden muss.

Noch problematischer ist es, wenn während der Kompilierung ein Syntaxfehler auftritt, die Kompilation also mit einer Fehlermeldung abbricht. Schuld daran ist oft nicht ein Programmfehler, sondern eine Inkompatibilität zwischen Ihrem Compiler und dem Code. Manche Programme können nur mit einer bestimmten Version von `gcc` kompiliert werden, wobei es oft *gerade nicht* die neueste Version sein muss. Die Lösung besteht hier darin, die gewünschte Compiler-Version zu installieren. Auch hierzu finden Sie im Internet oder in den `README`-Dateien zum Quellcode oft genaue Anweisungen.

Paketverwaltung

Selbst kompilierte Programme oder Bibliotheken können die Paketverwaltung durcheinanderbringen. Das Problem besteht darin, dass das selbst kompilierte Programm `abc` zwar nun auf Ihrem System installiert ist, die RPM- oder DEB-Datenbank aber nichts davon weiß. Wenn Sie nun versuchen, das Paket `xyz` zu installieren, das von `abc` abhängt, kommt es zu einer Fehlermeldung wegen scheinbar nicht erfüllter Paketabhängigkeiten. Mit `rpm` können Sie das Paket dank der Optionen `-nodeps` und `-force` dennoch installieren.

Die eleganteste Lösung besteht darin, das Programm nicht mit `make install` zu installieren, sondern zuerst in ein Paket zu verpacken und dieses dann zu installieren. Das setzt voraus, dass Sie sich zuerst mit den Kommandos zum Erstellen von Paketen vertraut machen. Außerdem ist diese Vorgehensweise ziemlich umständlich, insbesondere wenn ein Programm mehrfach getestet und neu kompiliert werden muss.

Beispiele

Hello World in C

Der Platz in diesem Buch reicht nicht aus, um auch eine Einführung in die Programmierung in C und C++ zu geben. Da ich aber in der Vergangenheit immer wieder diesbezügliche Fragen erhalten habe, finden Sie hier eine kurze Anleitung, wie Sie das klassische »Hello World«-Programm in C und C++ programmieren und kompilieren. Für die C-Version schreiben Sie mit einem Editor die folgenden Zeilen in die Datei `hello.c`:

```
// hello.c
#include <stdio.h>
int main(void)
{
  printf("Hello World!\n");
}
```

Mit den folgenden Kommandos kompilieren Sie das Programm und führen es aus:

```
user$  gcc -o hello hello.c
user$  ./hello
Hello World!
```

Hello World in C++

Der vergleichbare Code in C++ sieht so aus:

```
// hello.cpp
#include <iostream>
int main()
{
  std::cout << "Hello World!\n";
  return 0;
}
```

Zum Kompilieren verwenden Sie nun `g++` statt `gcc`:

```
user$  g++ -o hello hello.cpp
user$  ./hello
Hello World!
```

Anjuta, KDevelop, Eclipse, Emacs oder Vi?

Wenn Sie unter Linux eine komfortable Entwicklungsumgebung zur Programmierung in C oder C++ suchen, sollten Sie KDevelop (KDE) oder Anjuta (Gnome) ausprobieren. Eine mögliche Alternative ist die Entwicklungsumgebung Eclipse, die zwar speziell für Java optimiert ist, aber auch für andere Programmiersprachen verwendet werden kann. Echte Unix/Linux-Freaks betrachten auch die Editoren Vi und Emacs als Entwicklungsumgebung.

23.3 Java

Auf Desktop-Rechnern ist Java primär als Webbrowser-Plugin sowie für diverse LibreOffice-Zusatzfunktionen von Bedeutung. Außerdem setzt eine stetig wachsende Zahl von plattformunabhängigen Programmen Java voraus. Von deutlich größerer Bedeutung für Linux ist Java auf Servern, die in Java programmierte Websites oder Webservices anbieten (Tomcat, Jakarta etc.). Interessant ist Java aber natürlich auch für viele Schüler und Studenten, die mit dieser Sprache und oft mit Eclipse als Entwicklungsumgebung programmieren lernen, Projektarbeiten durchführen etc.

Die *Java Standard Edition*, der Java-Compiler `javac`, das *Java Development Kit*, die *Java Virtual Machine* und die Java-Klassenbibliothek stehen seit 2006 als Open-Source-Code gemäß der GPL zur Verfügung. Tabelle 23.1 fasst die wichtigsten Java-Abkürzungen zusammen.

OpenJDK/IcedTea

Neben den offiziellen Java-Paketen von Oracle, die zwar kostenlos zur Verfügung stehen, aber nicht mit Linux-Distributionen ausgeliefert werden können, gibt es reine Open-Source-Implementierungen von Java: Sie basieren auf dem GPL-Code von Sun, setzen daneben aber auch Komponenten aus anderen Open-Source-Projekten ein, insbesondere IcedTea und OpenJDK.

Die meisten aktuellen Linux-Distributionen liefern zur Zeit Java 7 auf Basis des OpenJDK-Projekts aus. Diese Java-Version ist zu mehr als 99 Prozent kompatibel zum Original von Oracle. Das verbleibende Prozent ist auf Java-Komponenten zurückzuführen, die aufgrund von Lizenzproblemen nicht als Open-Source-Code veröffentlicht werden können und zu denen noch keine Open-Source-Ersatzlösungen verfügbar sind.

Abkürzung	Bedeutung
JVM	Java Virtual Machine (führt Java-Programme aus)
JRE	Java Runtime Environment zur Ausführung von Java-Programmen; enthält die JVM sowie eine Menge Java-Bibliotheken
JDK	Java Software Development Kit zur Java-Programmentwicklung
Java SE = JSE	Java Standard Edition für Desktop-Anwendungen
Java EE = JEE	Java Enterprise Edition für Server-Anwendungen
JavaFX	Java-Framework für Webapplikationen, vergleichbar mit Adobe Flash und Microsoft Silverlight

Tabelle 23.1 Java-Abkürzungen

Installierte Java-Version feststellen

Um die auf Ihrem Rechner installierte Java-Version herauszufinden, führen Sie `java -version` aus. Wenn das Kommando `java` nicht zur Verfügung steht, ist Java gar nicht installiert. Abhilfe schafft bei den meisten Distributionen die Installation des Pakets `java-n.n-openjdk` oder `openjdk-n-jdk`. Die folgenden Zeilen zeigen, dass Java 7 installiert ist. Das heißt, die Java-interne Versionsnummer 1.7 bezeichnet das, was umgangssprachlich Java 7 genannt wird.

```
user$  java -version
java version "1.7.0_25"
OpenJDK Runtime Environment (fedora-2.3.10.3.fc19-x86_64)
OpenJDK 64-Bit Server VM (build 23.7-b01, mixed mode)
```

23.4 Mono

Das .NET Framework ist eine riesige Klassenbibliothek, die viele Ähnlichkeiten mit den für Java verfügbaren Bibliotheken aufweist. Auch die speziell für die .NET-Programmierung entwickelte Sprache C# wirkt Java-Programmierern auf Anhieb vertraut. Das .NET Framework und C# ergeben zusammen ein objektorientiertes Fundament für die Windows- und Webprogrammierung, an der – zumindest innerhalb der Microsoft-Welt – kein Weg mehr vorbei führt.

Was hat dies alles nun mit Linux zu tun? Obwohl die Linux-Gemeinde im Allgemeinen nicht besonders Microsoft-verliebt ist, gefiel einigen Open-Source-Entwicklern das Konzept gut. Sie begannen daher unter dem Namen *Mono* mit einer Open-Source-Implementierung von C# und wesentlichen Teilen des .NET Frameworks. Hinter dem Mono-Projekt stand ursprünglich Ximian, später Novell. Mittlerweile ist die Firma Xamarin der kommerzielle Partner des Mono-Projekts.

Mono ist mittlerweile praxistauglich und wird von einigen Distributionen standardmäßig installiert. Einige Programme aus dem Gnome-Umfeld basieren auf Mono, darunter der Audio-Player Banshee und das Notizzettelprogramm Tomboy. Ausführliche Informationen über das Mono-Projekt und über das Ausmaß der Kompatibilität zu C# bzw. zum .NET Framework gibt die folgende Website:

http://www.mono-project.com

Patentsorgen und ihre Lösung

Das Mono-Projekt ist naturgemäß nicht unumstritten. Gegner von Mono befürchten eine zu starke Abhängigkeit von Microsoft, das versuchen könnte, das Projekt auf der Basis von Software-Patenten zu bekämpfen. Zuletzt konnte man aber den Eindruck gewinnen, dass Microsoft gar nicht so unglücklich über das Mono-Projekt ist: Es gibt dem .NET Framework eine gewisse Plattformunabhängigkeit und stärkt so die Position gegenüber Java. Zudem sind die Sprache C# sowie Teile des .NET Frameworks in ECMA-Standards festgeschrieben; zumindest diese Teile sollten rechtlich auf sicherem Boden stehen.

Mono-Interna

Mono wird üblicherweise in Form einiger `mono-xxx`- und `libmono-xxx`-Pakete installiert, deren wichtigstes `mono-runtime` ist. Es enthält unter anderem den C#-Compiler `mcs`, die *Mono Virtual Machine*, eine Sammlung von .NET-kompatiblen Bibliotheken (`*.dll`-Dateien im Verzeichnis `/usr/lib/mono/gac`) sowie einige Mono-Konfigurationsdateien (Verzeichnis `/etc/mono`).

Mono-Programme haben die Endung `*.exe` und liegen ähnlich wie Java-Programme in einem Byte-Code vor. Um ein Mono-Programm auszuführen, übergeben Sie den Dateinamen der `*.exe`-Datei an das Kommando `mono`. Da dies in der Praxis zu umständlich ist, existieren zum Start von Mono-Anwendungsprogrammen kleine Scripts.

Für Mono-Entwickler gibt es die grafische Benutzeroberfläche MonoDevelop, die ursprünglich aus dem Windows-Programm SharpDevelop entstanden, mittlerweile aber davon unabhängig ist.

Kapitel 24
Grafiksystem

Seit mehreren Jahrzehnten ist das *X Window System* (nicht *Windows*!) die Basis für alle Grafiksysteme unter Unix und Linux. X ist eine Sammlung von Bibliotheken und Treibern, mit deren Hilfe grafische Informationen auf dem Bildschirm ausgegeben und Maus und Tastatur verwaltet werden. Diese Funktionen stehen auch für den Netzbetrieb zur Verfügung.

Unter Linux kommt bei praktisch allen Distributionen die X-Implementierung des X.org-Projekts zum Einsatz. Dieses Kapitel beschreibt verschiedene Aspekte der Konfiguration des X-Servers inklusive der Integration der Binärtreiber von NVIDIA.

Gegenwärtig sieht es so aus, als wären die Tage des X Window Systems gezählt. Als mögliche Nachfolger stehen das von Canonical/Ubuntu favorisierte System Mir sowie das von der Open-Source-Community bevorzugte System Wayland in den Startlöchern. Voraussichtlich wird Ubuntu 13.10 die erste große Distribution sein, die den ersten Schritt weg von X wagt und standardmäßig Mir ausliefert, wenn auch mit der Kompatibilitätsschicht XMir und dem herkömmlichen X-Server als Fallback. Dieses Kapitel enthält mangels gesicherter Fakten nur einen kurzen Abschnitt zu Mir, XMir und Wayland.

24.1 Grundlagen

X Window System

Das X Window System (kurz X) wurde ursprünglich vom Massachusetts Institute of Technology entwickelt. X bezeichnet Basisfunktionen zum Zeichnen von Punkten, Rechtecken etc., aber auch ein Netzwerkprotokoll, das es ermöglicht, ein X-Programm auf Rechner A auszuführen und die Ergebnisse auf Rechner B darzustellen.

X ist die Basis für eine grafische Benutzeroberfläche unter Linux. X stellt aber selbst keine Benutzeroberfläche zur Verfügung! Das Aussehen von X-Programmen und die Bedienung von X-Programmen hängt davon ab, welcher Window Manager läuft und welche Bibliotheken bei der Programmierung eingesetzt wurden – z. B. GTK bei Gnome-Programmen, QT bei KDE-Programmen.

X-Server

Der X-Server stellt die Schnittstelle zwischen dem X Window System und der Hardware her. Der Server ist modularisiert: Das bedeutet, dass der eigentliche Server durch ein Modul mit den spezifischen Funktionen für die jeweilige Grafikkarte ergänzt wird.

X-Erweiterungsmodule

Die Standardfunktionen des X-Servers können durch diverse Zusatzmodule (Extensions) erweitert werden, die beispielsweise für 3D-Grafik, für die Video-Ausgabe etc. verantwortlich sind.

Window Manager

Der Window Manager ist ein X-Programm, das für die Verwaltung der Fenster zuständig ist. Sie können mit dem Window Manager andere Programme starten, zwischen Fenstern wechseln, Fenster verschieben und schließen etc. – also eigentlich recht triviale Aufgaben ausführen. Dennoch ist es wichtig, sich vor Augen zu halten, dass diese Aufgaben vom Window Manager und nicht von X selbst erledigt werden. KDE und Gnome haben jeweils ihren eigenen Window Manager.

Das Treiberdilemma

Bevor die folgenden Abschnitte ausführlich die Konfiguration und den Betrieb von X beschreiben, möchte ich an dieser Stelle auf das größte Problem von X eingehen: die mangelnde Unterstützung moderner Grafikkarten durch Open-Source-Treiber.

Die überwiegende Mehrheit aller aktuellen PCs und Notebooks enthält Grafik-Chips der folgenden drei Firmen: ATI/AMD, Intel und NVIDIA, wobei es die Intel-Grafikchips nur in Form von kompletten Chipsätzen gibt, also nicht als eigenständige Grafikkarten.

Zuerst die gute Nachricht: Die in X enthaltenen Open-Source-Grafiktreiber funktionieren grundsätzlich in Kombination mit den meisten gängigen Grafikkarten. Und nun die schlechte: Die damit erzielte Geschwindigkeit ist nicht immer optimal, teilweise bleiben 3D-, Zusatz- oder Energiesparfunktionen ungenutzt.

Bei einigen Grafikkarten können die von den Herstellern kostenlos zur Verfügung gestellten Binärtreiber Abhilfe schaffen. Diese Treiber basieren allerdings nicht auf Open-Source-Code und sind deswegen mit diversen Nachteilen verbunden. Die folgenden Absätze fassen die aktuelle Treiber-Situation zusammen, alphabetisch geordnet nach Grafikkartenhersteller.

ATI/AMD

Für die Grafikkarten von ATI/AMD gibt es sowohl den Open-Source-Treiber `radeon` als auch den Binärtreiber von ATI/AMD `fglrx`. Da ATI/ADM gut mit den Open-Source-Entwicklern kooperiert, funktioniert der freie `radeon`-Treiber auf nahezu allen Grafikkarten anstandslos. Eine Matrix, die zeigt, welche Funktionen auf welchen Grafikkarten unterstützt werden, finden Sie hier:

http://www.x.org/wiki/RadeonFeature

Der `fglrx`-Treiber von ATI/AMD hat gleichzeitig an Bedeutung verloren. Er unterstützt nur aktuelle Grafikkarten. Dennoch gibt es natürlich Fälle, in denen der `fglrx`-Treiber wesentlich bessere Ergebnisse als der `radeon`-Treiber liefert – vor allem bei ganz neuen Grafikkarten.

Intel

Die bei Weitem beste Open-Source-Unterstützung gibt es momentan für Intel-Grafikchips. Das liegt daran, dass Intel ausgezeichnet mit der Open-Source-Gemeinde zusammenarbeitet und den selbst entwickelten Treiber `intel` als Open-Source-Code weitergibt.

NVIDIA

NVIDIA verharrt bis heute auf seinem Standpunkt, dass Lizenzvereinbarungen mit anderen Unternehmen und Patente die Entwicklung eines Open-Source-Treibers unmöglich machen und eine öffentliche Dokumentation der internen Schnittstellen verhindern würden. Stattdessen stellt NVIDIA den kostenlosen Binärtreiber `nvidia` zur Verfügung. Dessen Qualität war in der Vergangenheit zwar wesentlich besser als bei ATI/AMD, das ändert aber nichts an den prinzipiellen Nachteilen eines Nicht-Open-Source-Treibers (siehe unten).

Trotz des Widerstands von NVIDIA hat die Open-Source-Gemeinde mit `nouveau` einen eigenen Treiber entwickelt, der mittlerweile bei fast allen Distributionen standardmäßig zum Einsatz kommt und gut funktioniert. Probleme machen aber nach wie vor neue Grafikkarten sowie die Nutzung der Energiesparfunktionen.

VIA

Eher trist ist das Bild bei VIA: Der in X integrierte Open-Source-Treiber kommt leider nur mit alten VIA-Modellen zurecht. Für neuere VIA-Modelle haben Sie die Wahl zwischen drei schlechten Alternativen: dem langsamen VESA-Treiber, dem relativ alten und nicht mehr gewarteten Open-Source-Treiber der Firma VIA, der aufgrund seiner Mängel nicht in X enthalten ist, und einem weiteren Open-Source-Treiber des openChrome-Projekts, der aber noch nicht fertig ist. Ich gehe auf den VIA-Chipsatz in diesem Kapitel nicht weiter ein. Den aktuellen Status der VIA-Treiber fasst die folgende Seite zusammen:

http://www.phoronix.com/scan.php?page=news_item&px=MTM3OTE

Hybrid-Lösungen

Auf immer mehr Notebooks und vereinzelt auch auf Desktop-Rechnern befinden sich mittlerweile gleich *zwei* Grafiksysteme: ein energiesparendes System, das in der Regel direkt in die CPU integriert ist, und ein zweites System für hohe 3D-Leistung. Dieser hybride Ansatz versucht, eine hohe Laufzeit mit hoher Grafikleistung zu vereinen – je nachdem, was der Benutzer gerade braucht. Mit den geeigneten Treibern unter Windows oder OS X kann das aktive Grafiksystem im laufenden Betrieb gewechselt werden, ohne dass der Benutzer dies bemerkt.

Unter Linux funktioniert dies leider nicht oder nur mit Einschränkungen! Ohne aufwendige Konfiguration spricht Linux nur die langsame Chipsatz-Grafik an, ist aber nicht in der Lage, das zweite Grafiksystem in einen Energiesparmodus zu versetzen. Mit anderen Worten: Das Grafiksystem ist langsam *und* verbraucht unnötig viel Strom.

Immerhin lassen sich viele Hybrid-Grafiksysteme mittlerweile mit etwas Mühe so konfigurieren, dass sie unter Linux zufriedenstellend laufen. Einen guten Überblick über verschiedene Hybridgrafiksysteme sowie eine Sammlung von Tipps und Links zu deren Nutzung unter Linux finden Sie auf den folgenden Webseiten bzw. in leider kostenpflichtigen, dafür aber ausgezeichnet recherchierten c't-Artikeln:

http://hybrid-graphics-linux.tuxfamily.org
https://wiki.ubuntu.com/Bumblebee
http://www.heise.de/artikel-archiv/ct/2012/8/184
http://shop.heise.de/katalog/ct-linux-2013

Selbst habe ich ein Hybrid-Grafiksystem nie ausprobiert, weil ich mich beim Kauf von Rechnern selbst an die folgenden Empfehlungen halte.

Kaufempfehlung

Seit Intel die Grafikfunktionen in die CPU integriert hat, ist eine Empfehlung recht einfach: Egal ob Notebook oder Desktop-PC, entscheiden Sie sich für einen Rechner mit integrierter Intel-Grafik und ohne zusätzliche Grafikkarte! Die Grafikleistung ist für typische Linux-Anwendungen mehr als ausreichend, der Stromverbrauch ist minimal, und Sie gehen allen Treiberproblemen aus dem Weg. Egal, welche Linux-Distribution Sie installieren – das Grafiksystem läuft ohne umständliche Treiberinstallationen auf Anhieb problemlos!

Wenn Sie wirklich eine dezidierte Grafikkarte brauchen, ist ein nicht ganz neues Modell mit einem AMD-Grafikchip die zweitbeste Wahl. Um NVIDIA-Grafikkarten sowie um Rechner mit Hybridgrafik sollten Sie einen weiten Bogen machen. Computer mit Hybridgrafik erkennen Sie oft an Marketingbezeichnungen wie *NVIDIA Optimus*, *ATI Hybrid Graphics* oder *Virtu GPU Virtualization*.

Probleme nichtfreier Treiber

Vielleicht stehen Sie auf dem Standpunkt, die Unterscheidung zwischen »echten« Open-Source-Treibern und kostenlosen Herstellertreibern (auch proprietäre Treiber, Binärtreiber oder im Englischen *Restricted Driver* genannt) sei Haarspalterei – Hauptsache, es funktioniert. Es gibt aber gute Gründe, die für Open-Source-Treiber und gegen Binärtreiber sprechen:

- Die Stabilität der Herstellertreiber war in der Vergangenheit nicht immer besonders hoch.
- Die Grafiktreiber müssen zur X-Version passen. Gerade Fedora-Anwender, deren Distribution oft die allerneuste, erst halb fertige X-Version enthält, wissen davon

ein Lied zu singen: In der Vergangenheit dauerte es oft monatelang, bis es kompatible Herstellertreiber gab.

- Grafiktreiber erfordern eine enge Verzahnung mit dem Linux-Kernel. Dazu befindet sich zwischen dem eigentlichen Treiber (Closed-Source) und dem Kernel (GPL) ein kleines Kernelmodul, das nur als Schnittstelle dient. Viele Linux-Entwickler haben Zweifel daran, dass diese Vorgehensweise GPL-konform ist, und dulden sie nur widerwillig. Die Kernelentwickler bezeichnen den Kernel als *tainted* (makelhaft), sobald ein Nicht-GPL-Treiber geladen wird, und verweigern in diesem Fall jegliche Unterstützung bei Problemen.

  Die Verzahnung mit dem Kernel hat einen weiteren Nachteil: Nach jedem Kernel-Update muss auch das Kernelmodul des Grafiktreibers aktualisiert werden. Wie kompliziert dieser Vorgang ist, hängt von der Distribution ab. Im Idealfall wird der neue Grafiktreiber vom Paketverwaltungssystem automatisch heruntergeladen und installiert; im ungünstigsten Fall funktioniert nach dem Kernel-Update das Grafiksystem nicht mehr und Sie müssen in einer Textkonsole ein neues Kernelmodul für den Treiber kompilieren.
- Wegen der oben erwähnten GPL-Konflikte ist die Weitergabe der Binärtreiber schwierig. Bei vielen Distributionen müssen Sie die Treiber daher nach der Installation der Distribution extra herunterladen und installieren.
- Wenn im Treiber ein Sicherheitsproblem auftritt – was zuletzt im Juli 2012 beim NVIDIA-Treiber der Fall war –, können Linux-Distributoren nur darauf hoffen, dass die Grafikfirmen möglichst rasch ein Update zustande bringen. Bei Open-Source-Code kann die Entwicklergemeinde den Fehler dagegen selbst beheben, was in der Regel schneller geht.
- Mangels Code ist es unmöglich, die Treiber für andere Betriebssysteme, CPU-Architekturen etc. zu portieren. Die Grafikfirmen entscheiden, welche Systeme unterstützt werden. Beispielsweise gab es lange Zeit keine Treiber für 64-Bit- oder BSD-Systeme.
- Die Grafikunterstützung unter Linux ist von der Gunst des Herstellers abhängig. Ältere Grafikkarten werden zumeist nicht unterstützt, was zur Verwendung alter X-Versionen oder zum Kauf neuer Hardware zwingt.
- Wenn Sie UEFI Secure Boot nutzen und Ihre Distribution nur signierte Kernelmodule zulässt, wie dies beispielsweise unter Fedora der Fall ist, können Sie keine proprietären Grafiktreiber verwenden.

Auf Dauer kann Linux nur dann ein Open-Source-System bleiben, wenn auch die wichtigsten Komponenten frei verfügbar sind. Und dazu zählen zweifelsohne die Grafiktreiber. Suchen Sie Ihren nächsten Rechner bzw. Ihre nächste Grafikkarte auch unter dem Gesichtspunkt aus, ob es dafür freie Treiber gibt!

Glossar

In der X-Welt wimmelt es nur so von Abkürzungen und obskuren Begriffen. Dieser Abschnitt gibt in alphabetischer Reihenfolge eine erste Orientierungshilfe. Leider ist X eine große Baustelle, in der mit jeder Version neue Komponenten eingeführt und alte Komponenten schrittweise entfernt werden. Selbst Linux-Profis fällt es hier oft schwer, den Überblick zu behalten.

AIGLX *Accelerated Indirect GL X*, kurz AIGLX, erlaubt die Verwendung von GLX-Funktionen auf der Ebene des X-Servers. AIGLX ist die Voraussetzung für die 3D-Desktop-Effekte von Compiz bzw. modernen Window Managern.

DRI und DRM Das *Direct Rendering Interface* (DRI) ermöglicht die Nutzung der 3D-Funktionen der Grafikkarte – sofern es einen passenden DRI-Treiber für die Karte gibt. Momentan ist DRI2 aktuell, eine verbesserte Version der ursprünglichen DRI-Funktionen. Der Binärtreiber von ATI/AMD kooperiert dazu mit dem DRI-Modul von X. Der NVIDIA-Treiber enthält dagegen eine eigene Implementierung der DRI-Funktionen.

Ein Teil des DRI muss im Kernel (und nicht in den Grafikkartenteilen) implementiert werden. Dieser Teil wird *Direct Rendering Manager* (DRM) genannt.

EXA EXA ist eine Bibliothek, um 2D-Operationen wie das Verschieben von Bildschirminhalten durch die Grafik-Hardware zu beschleunigen. EXA und seine Variante UXA lösen XAA ab, sind aber voraussichtlich nur Übergangslösungen: Längerfristig soll die gesamte Grafikbeschleunigung auf Open GL aufbauen und über diesen Weg die 3D-Funktionen der Grafikkarte nutzen. Die Bezeichnung EXA hat keine klare Definition; das Xorg-Glossar bezeichnet EXA als eine *acceleration architecture with no well-defined acronym*.

GEM Der *Graphics Execution Manager* (GEM) ist eine Bibliothek zur Speicherverwaltung für Grafiktreiber. GEM wird von den Intel-Grafiktreibern genutzt.

GLX und libGL Unter X werden die Open-GL-Funktionen über die GLX-Bibliothek genutzt. Diese Bibliothek stellt die Verbindung zwischen dem X Window System und Open GL her. GLX stellt beispielsweise sicher, dass Open-GL-Ausgaben nur im gerade sichtbaren Teil eines Fensters erfolgen und nicht mit anderen Fenstern kollidieren. GLX ist durch ein Modul in X integriert.

KMS *Kernel Mode Setting* (KMS) bedeutet, dass der Linux-Kernel und nicht X den Grafikmodus einstellt. KMS wird von allen wichtigen Open-Source-Treibern unterstützt. KMS ermöglicht es, die gewünschte Grafikauflösung bereits unmittelbar nach dem Rechnerstart einzustellen. Im Idealfall entfällt dann das früher übliche Flackern beim Start von X. Falls der Kernel beim Booten nicht die richtige Auflösung wählt, kann diese mit der Kerneloption `video` eingestellt werden (siehe Abschnitt 28.4).

Mir

Mir ist ein neuer, von Canonical entwickelter Display Server. Er soll in zukünftigen Ubuntu-Versionen X ablösen, und zwar sowohl auf herkömmlichen Computern als auch auf Smartphones und Tablets. Die Kompatibilität zu herkömmlichen X-Programmen stellt XMir her.

Open GL

Open GL (oft auch kurz GL genannt) ist eine von SGI entwickelte Bibliothek zur Darstellung von 3D-Grafiken, die auf fast allen Unix/Linux-Rechnern zur Verfügung steht. Daher bauen nahezu alle unter Linux verfügbaren 3D-Programme und -Spiele auf Open GL auf. Open GL ist also gewissermaßen das Unix/Linux-Gegenstück zu Microsofts DirectX-Bibliothek.

Da der Code von Open GL ursprünglich nicht frei verfügbar war, ist die dazu kompatible Open-Source-Bibliothek Mesa entstanden. Mesa war anfänglich eine reine Software-Lösung, nutzt aber mittlerweile 3D-Funktionen der Grafikkarte.

RandR

Die *Resize and Rotate Extension* (RandR) erlaubt es, einige Einstellungen von X im laufenden Betrieb zu ändern. Dazu zählen die Auflösung, die Bildfrequenz und die Bilddrehung. Via RandR kann auch ein zweiter Bildschirm aktiviert werden.

TTM

Die *Translation Table Maps* (TTM) ist ähnlich wie GEM eine Bibliothek zur Speicherverwaltung für Grafiktreiber. TTM ist weniger Intel-spezifisch implementiert als GEM und macht das Zusammenspiel mit anderen Treibern einfacher.

UXA

Die *UMA Acceleration Architecture* (UXA) ist eine Intel-spezifische Variante zu EXA, kümmert sich also um die schnelle Verarbeitung von 2D-Operationen. Der wesentliche Unterschied zu EXA besteht darin, dass UXA die Speicherverwaltungsfunktionen von GEM nutzt.

Wayland

Das auf X basierende Grafiksystem ist in seinen Grundzügen mehrere Jahrzehnte alt. Deswegen ist es immer schwieriger, zeitgemäße Grafikanwendungen auf Basis von X effizient zu implementieren. Abhilfe soll in einigen Jahren das neue Grafiksystem *Wayland* schaffen (die Entwickler sprechen genau genommen von einem *Display Server Protocol*), das seit 2008 in Entwicklung ist.

XAA

Die *X Acceleration Architecture* (XAA) beschleunigt 2D-Grafikoperationen. Diese Art der Hardware-Beschleunigung ist historisch gesehen älter als die 3D-Funktionen und wird von X schon lange standardmäßig unterstützt. Leider ist das Zusammenspiel zwischen XAA und Open GL bzw. mit den 3D-Funktionen generell problematisch. Aus diesem Grund haben EXA und UXA bei vielen Grafiktreibern XAA abgelöst.

Xgl

Xgl ist eine obsolete Variante zu AIGLX, die Mitte 2008 aus X entfernt wurde. Xgl wurde von Novell entwickelt und war einige Jahre in SUSE-Distributionen enthalten, um 3D-Desktop-Effekte zu realisieren. Dabei wird zuerst ein gewöhnlicher X-Server gestartet, der nur zur Darstellung eines einzigen Fensters ohne Rahmen

verwendet wird. Dieses Fenster ist zur Nutzung der Open-GL-3D-Funktionen erforderlich. Für den Inhalt dieses Fensters ist der Xgl-Server verantwortlich, der darin den eigentlichen Desktop dargestellt.

XRender

Die *X Rendering Extension* (kurz XRender) ist eine Bibliothek zur Erzielung von Transparenz- und Überlagerungseffekten (Alpha Blending). Die Bibliothek wird auch zur Textausgabe verwendet. XRender greift aus Geschwindigkeitsgründen auf 3D-Hardware-Funktionen zurück.

Links

Weiterführende Informationen sowie Berichte über aktuelle X-Entwicklungstendenzen finden Sie hier:

http://www.x.org/wiki
http://blog.mecheye.net/2012/06/the-linux-graphics-stack
http://www.phoronix.com

24.2 X starten und beenden

Dieser Abschnitt fasst einige Informationen zum Starten und Stoppen von X zusammen. In der Regel müssen Sie sich darum nur kümmern, wenn der automatische Start von X beim Hochfahren des Rechners bzw. das Beenden von X beim Herunterfahren nicht funktioniert bzw. wenn Sie in den Prozess manuell eingreifen möchten.

X manuell starten und beenden

Display Manager

Üblicherweise wird nicht X an sich gestartet, sondern ein sogenannter Display Manager. Dieses Programm kümmert sich um den Start von X, zeigt einen Login-Bildschirm an und startet nach dem Login das Desktop-System (z. B. Gnome oder KDE) bzw. einen Window Manager. Bei manchen Display Managern kann beim Login die gewünschte Sprache und das Desktop-System ausgewählt werden.

Je nach Distribution kommt als Display Manager die KDE-Variante `kdm` oder die Gnome-Variante `gdm` zum Einsatz, unter Ubuntu `lightdm`. Nur wenige Distributionen greifen auf das minimalistische Programm `xdm` zurück. Die Entwicklung verschiedener Display Manager hat primär optische Gründe und erlaubt es, das Aussehen des Display Managers an den Desktop anzupassen. Grundsätzlich ist aber jeder Display Manager in der Lage, jedes Desktop-System zu starten. Sie können also auch mit `kdm` Gnome starten oder mit `gdm` KDE!

Init-System

Das Grafiksystem wird, während der Rechner hochfährt, durch das Init-System initialisiert (siehe Kapitel 27). Je nach Distribution kommen unterschiedliche Init-Systeme zum Einsatz:

- **Init-V (Debian, openSUSE):** Bei Debian führt der Init-V-Prozess in den Runleveln 2 bis 5 das Script `/etc/init.d/gdm3` oder `kdm` aus. Bei SUSE führt der Init-V-Prozess im Runlevel 5 das Script `/etc/init.d/xdm` aus. Das gilt auch für openSUSE mit Systemd als Init-System. Für den Start des Display Managers ist dennoch zumindest bis openSUSE 12.3 ein Init-V-Script zuständig.
- **Upstart (Ubuntu, RHEL 6):** Ubuntu und RHEL 6 verwenden Upstart zum Start von X. Die Startregeln sind in der Konfigurationsdatei `/etc/init/lightdm.conf` (Ubuntu) bzw. in `/etc/init/prefdm.conf` (RHEL) formuliert.
- **Systemd (Fedora):** Für den Start des Display Managers ist unter Fedora die Konfigurationsdatei `/lib/systemd/system/gdm.service` verantwortlich.

X neu starten

Änderungen an der X-Konfiguration werden erst nach einem Neustart von X wirksam. Wie Sie X neu starten, ist aber stark distributionsabhängig.

```
root#  service gdm3 restart              (Debian)
root#  restart prefdm                    (RHEL 6)
root#  systemctl restart gdm             (Fedora)
root#  service xdm restart               (SUSE)
root#  service lightdm restart           (Ubuntu)
```

Die obigen Kommandos sollten Sie in einer Textkonsole ausführen, nachdem Sie sich aus X ausgeloggt haben. Je nachdem, welchen Display Manager Sie einsetzen, müssen Sie in den obigen Kommandos `gdm` durch `kdm` oder `xdm` ersetzen. Wenn Sie X nicht neu starten, sondern beenden möchten, ersetzen Sie `restart` durch `stop`.

Automatischen Start deaktivieren

Manchmal ist es zweckmäßig, den automatischen X-Start zu deaktivieren – beispielsweise bei der Verwendung des Rechners als Server. Bei vielen Distributionen ändern Sie dazu einfach den Standard-Runlevel, der in der Datei `/etc/inittab` eingestellt ist und vom Init-V-System und von der Upstart-Variante von RHEL ausgewertet wird. Für Multiuser-Systeme ohne X ist unter RHEL 6 der Runlevel 3 vorgesehen. Die Änderung ist ab dem nächsten Rechnerstart wirksam.

```
# in /etc/inittab (RHEL 6)
...
# Standard-Runlevel 3 (Multiuser-System ohne X)
id:3:initdefault:
```

Um den automatischen X-Start erneut zu aktivieren, stellen Sie den Standard-Runlevel zurück auf 5.

Bei Distributionen mit Systemd müssen Sie den `default.target`-Link neu einrichten:

```
root# cd /etc/systemd/system/
root# ln -sf /lib/systemd/system/multi-user.target default.target      (Fedora)
root# ln -sf /usr/lib/systemd/system/multi-user.target default.target  (openSUSE)
```

Bei Debian lassen Sie den Runlevel unverändert, verhindern aber mit dem folgenden Kommando den automatischen Start des Display Managers. Um X in Zukunft wieder automatisch zu starten, führen Sie `insserv gdm3` aus. Anstelle von `gdm3` müssen Sie je nach Desktop-System `kdm` oder `xdm` angeben.

```
root#  insserv -r gdm3                (Debian)
```

Ubuntu verwendet Upstart zum Start von X. Um den Start zu vermeiden, setzen Sie der mehrzeiligen Anweisung `start on (...)` in der Datei `/etc/init/lightdm.conf` Kommentarzeichen voran (in allen betroffenen Zeilen!).

X manuell starten (startx)

Wenn X momentan nicht läuft und Sie rasch einige Arbeiten im Grafikmodus erledigen möchten, loggen Sie sich im Textmodus ein und führen dann das Kommando `startx` aus. Es erscheint keine Login-Box. Derjenige Benutzer, der `startx` ausführt, ist auch der Benutzer unter X. `startx` ist auch das ideale Kommando, um eine geänderte X-Konfiguration unkompliziert auszuprobieren.

Xsession

Während des Starts von X werden die Script-Datei `/etc/X11/Xsession` sowie alle Scripts im Verzeichnis `/etc/X11/Xsession.d` ausgeführt. Dieses Verzeichnis ist der geeignete Ort, wenn Sie während des X-Starts irgendwelche Einstellungen verändern oder sonstige Konfigurationsarbeiten durchführen möchten.

DontZap-Option

In der Vergangenheit was es möglich, mit Strg+Alt+← X zu beenden (»abzuschießen«). Dabei wurden alle unter X laufenden Programme sofort beendet. Um ein unbeabsichtigtes Ende von X samt einhergehender Datenverluste zu vermeiden, ist diese Tastenkombination heute bei vielen Distributionen deaktiviert.

Bei SUSE funktioniert die Tastenkombination weiterhin, wenn sie innerhalb von zwei Sekunden *zweimal* hintereinander gedrückt wird. Damit Sie die Tastenkombination unter Ubuntu verwenden können, suchen Sie im Modul Region und Sprache der Systemeinstellungen nach der Option Tastenkombination zum erzwungenen Beenden des X-Servers und aktivieren diese.

Bei anderen Distributionen müssen Sie in die Konfigurationsdatei `/etc/X11/xorg.conf` die folgenden Zeilen einbauen, um Strg+Alt+← zu aktivieren. (Es gibt nichts Schöneres als eine doppelte Verneinung.)

```
Section "ServerFlags"
        Option  "DontZap"  "false"
EndSection
```

Konfiguration des Display Managers

gdm

gdm ist der Display Manager des Gnome-Desktops. Die Konfigurationsdateien befinden sich in /etc/gdm oder /etc/gdm3. Sie steuern unter anderem, welche Programme, Kommandos und Scripts für verschiedene Funktionen des Display Managers genutzt werden sollen.

kdm

kdm ist das KDE-Gegenstück zu gdm. Die Konfiguration von kdm erfolgt je nach Distribution durch /etc/kde4/kdm/kdmrc oder durch /usr/share/kde4/config/kdm/kdmrc. Die meisten Einstellungen von kdmrc können Sie komfortabler im Systemeinstellungsmodul Anmeldebildschirm vornehmen.

lightdm

Unter Ubuntu kommt als Display Manager lightdm zum Einsatz. Die Konfiguration erfolgt durch zwei minimalistische Dateien in /etc/lightdm. Änderungen an diesen Dateien sind nur selten erforderlich. Mit der Anweisung allow-guest=false in lightdm.conf können Sie unter Ubuntu Gast-Sitzungen deaktivieren.

.desktop-Dateien

Wenn Sie mehrere Desktop-Systeme installiert haben, können Sie beim Login im Display Manager in einem Menü auswählen, welcher Desktop bzw. Window Manager gestartet werden soll. Die Daten für dieses Menü befinden sich bei den meisten Distributionen in *.desktop-Dateien im Verzeichnis /usr/share/xsession (Schlüsselwort SessionDesktopDir in der gdm-Konfiguration). Beispielsweise enthält die Desktop-Datei zum Start von Gnome die folgenden Zeilen:

```
[Desktop Entry]
Name=GNOME
Comment=This session logs you into GNOME
Exec=gnome-session
...
```

Auto-Login

Auf Desktop-Systemen ist es oft erwünscht, dass der Standardbenutzer beim Start des Rechners automatisch eingeloggt wird. Das ist zwar ein Sicherheitsrisiko, dafür aber bequem. Bei vielen Distributionen können Sie den Auto-Login in den Systemeinstellungen konfigurieren, bei Gnome-Systemen und unter Ubuntu in der Benutzerverwaltung. Die folgenden Absätze erklären die manuelle Konfiguration.

gdm

Wenn Ihre Distribution gmd als Display Manager verwendet, fügen Sie die folgenden Zeilen in den [daemon]-Abschnitt von custom.conf ein:

```
# Datei /etc/gdm[3]/custom.conf
...
[daemon]
  AutomaticLoginEnable=true
  AutomaticLogin=loginname
```

kdm Bei `kdm` fügen Sie die folgende Zeile in `kdmrc` ein:

```
# Datei /etc/kde4/kdm/kdmrc
...
AutoLoginUser=loginname
```

lightdm Bei `lightdm` steuert die Variable `autologin-user` in `lightdm.conf` den Auto-Login:

```
# Datei /etc/lightm/lightdm.conf
[SeatDefaults]
autologin-user=loginname
...
```

SUSE SUSE sieht eigene Konfigurationsdateien für den Auto-Login von KDE und Gnome vor. Direkte Veränderungen in KDE oder Gnome sind nicht zu empfehlen, weil `SuSEconfig` die Einstellungen bei der nächsten Gelegenheit überschreibt. Stattdessen verändern Sie die Datei `/etc/sysconfig/displaymanager`. Um den Auto-Login zu deaktivieren, weisen Sie der `AUTOLOGIN`-Variablen eine leere Zeichenkette zu. Die Änderungen werden erst gültig, wenn Sie das Kommando `SuSEconfig` ausführen.

```
# /etc/sysconfig/displaymanager
...
DISPLAYMANAGER_AUTOLOGIN="benutzername"
```

X-Protokolldatei

Beim Start von X werden zahlreiche Meldungen, Warnungen und eventuell auch Fehlermeldungen in der Datei `/var/log/Xorg.0.log` gespeichert. Dieses Startprotokoll enthält ausführliche Informationen darüber, welche Konfigurationsdatei verwendet wurde, welche Module geladen wurden, welche Probleme dabei aufgetreten sind, welche Grafikmodi aus welchen Gründen verworfen wurden etc. Einträge innerhalb der Logging-Datei sind durch folgende Codes gekennzeichnet:

- `(**)` Einstellung aus der Konfigurationsdatei
- `(++)` Einstellung aus der Kommandozeile
- `(==)` X-Standardeinstellung
- `(--)` Einstellung, die sich aus erkannter Hardware ergibt
- `(!!)` Hinweis
- `(II)` Hinweis
- `(WW)` Warnung
- `(EE)` Fehler

Falls es in `/var/log/` mehrere X-Logging-Dateien gibt, halten Sie Ausschau nach der aktuellsten Datei. Aufgrund der Fülle der Informationen in `Xorg.0.log` gleicht die Suche nach wirklich relevanten Daten leider der sprichwörtlichen Suche nach der Nadel im Heuhaufen. Gegebenenfalls senden Sie einfach die gesamte Logging-Datei jemandem, der sich besser damit auskennt, bzw. posten sie in ein Support-Forum.

X-Version feststellen

Wenn Sie wissen möchten, welche Version des X-Servers auf Ihrem Rechner verwendet wird, führen Sie das folgende Kommando aus. Auf dem Beispielrechner läuft der X.org-Server in Version 1.14.

```
user$  X -showconfig
X.Org X Server 1.14.1.902
Release Date: 2013-04-17
X Protocol Version 11, Revision 0
```

Eine alternative Vorgehensweise bietet das Kommando `xdpyinfo`:

```
user$  xdpyinfo | grep release
vendor release number:    11401000
```

24.3 Basiskonfiguration

xorg.conf

Zur Konfiguration von X dienen die Dateien `/etc/X11/xorg.conf` und `/etc/X11/xorg.conf.d/*.conf`. In der Vergangenheit spielte die dort gespeicherte Konfiguration eine große Rolle: Ein Start von X war unmöglich, wenn diese Datei fehlte. Mittlerweile hat sich das aber radikal geändert – aktuelle X-Versionen kommen vollkommen ohne `xorg.conf` aus: X ermittelt beim Start die aktuelle Hardware (Grafikkarte, Monitor, Maus, Tastatur) und lädt automatisch geeignete Treiber und Module. Solange keine besonderen Konfigurationswünsche erfüllt werden sollen, funktioniert X also ganz ohne `xorg.conf`!

Eine manuelle Konfiguration ist nur erforderlich, wenn die automatische Konfiguration versagt. Dieser Abschnitt führt in die Syntax von `xorg.conf` ein und gibt diverse Konfigurationstipps. Beachten Sie, dass Änderungen an `xorg.conf` erst mit einem Neustart von X wirksam werden (siehe Abschnitt 24.2). Fehler in `xorg.conf` können dazu führen, dass X gar nicht mehr gestartet werden kann. In diesem Fall müssen Sie die Korrekturarbeiten in einer Textkonsole durchführen. Machen Sie sich damit vertraut, bevor Sie an `xorg.conf` herumspielen (siehe Kapitel 13, »Terminalfenster und Konsolen«)!

Konfigurationswerkzeuge

Die Konfiguration des X-Servers erfolgt normalerweise bereits während der Installation. Je nachdem, mit welcher Distribution Sie arbeiten und ob Sie binäre Treiber von ATI/AMD oder NVIDIA installiert haben, stehen zudem die folgenden Konfigurationswerkzeuge zur Auswahl:

ATI/AMD:	`amdcccle` (Catalyst Control Center)
Debian, Ubuntu:	`dpkg-reconfigure xserver-xorg`
NVIDIA:	`nvidia-settings`

Daneben enthalten auch KDE und Gnome Konfigurationswerkzeuge, mit denen Sie die Auflösung und die Bildfrequenz ändern und eine Konfiguration für mehrere Bildschirme einrichten können. Diese Programme verändern allerdings nicht `xorg.conf`, sondern ändern über den RandR-Mechanismus dynamisch die X-Konfiguration. Die geänderte Konfiguration wird in einer Konfigurationsdatei des Benutzers gespeichert und gilt nur für den aktiven Nutzer und nur für das laufende Desktop-System. Weitere Informationen zu RandR folgen in Abschnitt 24.6.

Aufbau der Konfigurationsdatei xorg.conf

Die Datei `/etc/X11/xorg.conf` ist in mehrere Abschnitte gegliedert, die mit `Section "name"` eingeleitet und mit `EndSection` abgeschlossen werden (siehe Tabelle 24.1). Bei aktuellen Distributionen gibt es oft gar keine `xorg.conf`-Datei, oder die Datei enthält nur wenige Abschnitte.

Abschnitt	Bedeutung	Details
`Monitor`	Monitordaten	Abschnitt 24.3
`Device`	Konfiguration der Grafikkarte	Abschnitt 24.3 und 24.4
`Screen`	Bildschirmauflösung	Abschnitt 24.3
`Files`	Dateinamen (z. B. Font-Verzeichnisse)	Abschnitt 24.3
`Module`	Zusatzmodule (z. B. freetype, dri)	Abschnitt 24.3
`ServerFlags`	verschiedene Server-Optionen	Abschnitt 24.3
`InputClass`	Device-Gruppe (z. B. alle Tastaturen)	Abschnitt 24.5
`InputDevice`	Tastatur, Maus, Touchpad	Abschnitt 24.5

Tabelle 24.1 xorg.conf-Abschnitte

Minimalkonfiguration

Das folgende Listing zeigt eine Minimalkonfiguration für Notfälle, wenn das Grafiksystem gar nicht funktionieren will. Die hier vorgeschlagene Konfiguration verwendet den VESA-Treiber und bietet damit keine 3D-Unterstützung.

```
Section "Monitor"
  Identifier "mon0"
  HorizSync 31 - 94
  VertRefresh 60
EndSection
Section "Device"
  Identifier "dev0"
  Driver "vesa"
EndSection
Section "Screen"
  Identifier "screen0"
```

```
  Monitor "mon0"
  Device  "dev0"
  DefaultDepth 24
  SubSection "Display"
    Depth 24
    Modes "1024x768"
  EndSubSection
EndSection
```

Identifier

Die `Identifier`-Zeile gibt dem Abschnitt einen Namen und ermöglicht Querverweise zwischen den Abschnitten. Beispielsweise verweist der Abschnitt `Screen` auf das Device `dev0` und den Monitor `mon0`.

In manchen `xorg.conf`-Dateien werden Sie in vielen Abschnitten auch `Board-`, `Vendor-` und `ModelName`-Zeichenketten vorfinden. Diese Zusatzinformationen dienen nur zur besseren Orientierung in der Konfigurationsdatei. Sie werden von X nicht ausgewertet und haben keinerlei Relevanz für die Funktion von X.

Von den weiteren Schlüsselwörtern werden die wichtigsten im Verlauf der folgenden Abschnitte beschrieben. Eine vollständige Referenz gibt `man xorg.conf`.

Monitor-Abschnitt

Der `Monitor`-Abschnitt ist im Regelfall überflüssig, weil moderne Monitore ihre Eckdaten an die Grafikkarte übermitteln. Sollte das bei uralten Monitoren oder in einer virtuellen Maschine nicht funktionieren, können Sie den zulässigen Bereich für die horizontale Zeilenfrequenz (in kHz) und für die Bildfrequenz (in Hz) angeben. Die folgenden Angaben gelten für einen Monitor mit einer Auflösung von 1600×1200 Pixeln und einer maximalen Bildfrequenz von 75 Hz:

```
Section "Monitor"
  ...
  HorizSync    30-95     # Zeilenfrequenz 30 bis 95 kHz (Zeilen/sec)
  VertRefresh  58-78     # Bildfrequenz 58 bis 78 Hz  (Bilder/sec)
EndSection
```

ModeLine

Optional können Sie mit `ModeLine` exakt angeben, in welchem Grafikmodus der Monitor betrieben werden soll. Ein Grafikmodus wird durch seinen Namen und neun Zahlenwerte bestimmt. Die folgende Zeile zeigt ein Beispiel:

```
ModeLine "640x480"  25.175   640 664 760 800   480 491 493 525
```

Damit wird ein Grafikmodus mit 640×480 Pixeln beschrieben. Die Zeichenkette `"640x480"` ist gleichzeitig auch der Name dieses Modus. Der Zahlenwert 25.175 gibt die Pixelfrequenz (Videobandbreite) in MHz an.

Die nächsten vier Werte betreffen das horizontale Timing: Eine einzelne Bildschirmzeile mit 640 *sichtbaren* Pixeln wird in Wirklichkeit aus 800 *virtuellen* Pixeln zusammengesetzt. Die ersten 640 Pixel werden tatsächlich angezeigt. Während der verbleibenden 160 Pixel wird der Elektronenstrahl durch den HSync-Impuls zurück an den Beginn der nächsten Zeile bewegt. Während dieser Zeit hat der Elektronenstrahl die Intensität 0. Die vier Werte kommen also wie folgt zustande:

640 640 Bildschirmpixel anzeigen
664 24 weitere Pixel dunkel tasten
760 96 Pixel lang einen HSync-Impuls erzeugen
800 nochmals 40 Pixel dunkel tasten, d. h. insgesamt 800 virtuelle Punkte

Ganz analog wie beim horizontalen Timing sind auch die Angaben für das vertikale Timing in Bildschirmzeilen zu interpretieren:

480 480 Zeilen anzeigen
491 11 Zeilen dunkel tasten
493 2 Zeilen lang einen VSync-Impuls erzeugen
525 nochmals 32 Zeilen dunkel tasten, d. h. insgesamt 525 virtuelle Zeilen

Aus den jeweils letzten Werten der Vierergruppen und der Pixelfrequenz ergeben sich übrigens die horizontale Zeilenfrequenz und die vertikale Bildfrequenz: 25,175 MHz dividiert durch 800 Pixel pro Zeile ergibt eine Zeilenfrequenz von 31,469 kHz. Die Zeilenfrequenz dividiert durch 525 Zeilen pro Bild liefert die vertikale Bildfrequenz von 60 Hz.

gtf

Die Parameter für eine `ModeLine`-Zeile können Sie ganz komfortabel mit dem Kommando `gtf` ermitteln. Dazu übergeben Sie an das Kommando die gewünschte Auflösung und Bildfrequenz:

```
user$  gtf 1600 1200 60
# 1600x1200 @ 60.00 Hz (GTF) hsync: 74.52 kHz; pclk: 160.96 MHz
Modeline "1600x1200_60.00" 160.96 1600 1704 1880 2160 \
  1200 1201 1204 1242 -HSync +Vsync
```

ModeLine-Beispiel

Nicht immer sind die so generierten `ModeLine`-Parameter perfekt. In der Vergangenheit hatte ich bisweilen Probleme mit einem alten LCD-Monitor mit einer Auflösung von 1600×1200 Punkten, dessen maximale Signalfrequenz 160 MHz beträgt. Aktuelle Modelle in dieser Auflösung verkraften eine wesentlich höhere Signalfrequenz. Beim Anschluss des Monitors mit einem DVI-Kabel kam kein Bild zustande. Beim Studium von `/var/log/Xorg.0.log` stellte ich fest, dass X die maximale Signalfrequenz des Monitors überschritt. Abhilfe schuf der folgende Modus mit einer Signalfreqenz von nur noch ca. 130 MHz (1728 × 1250 × 60):

```
ModeLine "1600x1200"  129.60  1600 1664 1696 1728  1200 1201 1204 1250
```

DisplaySize

Schließlich können Sie mit `DisplaySize` die Breite und Höhe des Monitors in Millimetern angeben. X wertet diese Informationen aus, um den DPI-Wert zu bestimmen (siehe Abschnitt 24.10).

```
DisplaySize 336 252
```

Device-Abschnitt (Grafikkarte)

Das wichtigste Schlüsselwort im Device-Abschnitt ist `Driver`. Es bestimmt, welcher Treiber geladen werden soll. Die zur Auswahl stehenden Grafiktreiber befinden sich im Verzeichnis `/usr/lib[64]/xorg/modules/drivers`. Im Regelfall erkennt X selbst den geeigneten Treiber. Eine explizite Treibereinstellung ist nur bei ganz neuen Grafikkarten erforderlich oder wenn Sie einen binären Herstellertreiber verwenden.

Falls mehrere PCI-Grafikkarten in den Rechner eingebaut sind, können Sie mit `BusID` genau angeben, welche Sie meinen. Die drei Ziffern geben den PCI-Bus, die Device-Nummer und die Funktion an. Die korrekten Werte können Sie herausfinden, indem Sie in einer Textkonsole `X -scanpci` ausführen. X darf zu diesem Zeitpunkt nicht laufen.

```
Section "Device"
  Driver        "radeon"
  BusID         "1:0:0"
EndSection
```

Welcher Treiber für welche Grafikkarte?

Wenn Sie nicht wissen, welche Grafikkarte Sie haben, können Sie als `root` das Kommando `lspci` ausführen:

```
root#  lspci
...
01:00.0 VGA compatible controller: ATI Technologies Inc M10 NT
                                   [FireGL Mobility T2] (rev 80)
```

Leider geht aus dem Ergebnis nicht immer auch der erforderliche Grafiktreiber hervor. Hilfreich bei der Treiberauswahl sind die `man`-Seiten. Beispielsweise gibt `man radeon` Details zum X.org-Radeon-Treiber, `man nv` Details zum X.org-NVIDIA-Treiber etc.

Wenn Sie Pech haben, wird Ihre neue Grafikkarte von X.org noch gar nicht oder nur teilweise unterstützt. Manchmal scheitert es nur an der richtigen Erkennung der Grafikkarte: Sie haben also im `Device`-Abschnitt das richtige Modul angegeben, aber X erkennt die Grafikkarte nicht. In diesem Fall können Sie versuchen, im `Device`-Abschnitt mit `ChipId` die ID-Nummer einer kompatiblen Karte einzusetzen (z. B. `ChipId "0x1234"`). Eine Liste gültiger ID-Nummern finden Sie in der Datei `pci.ids`. Der Ort dieser Datei kann je nach Distribution variieren; werfen Sie zuerst einen Blick in das Verzeichnis `/usr/share/misc`.

Sollten Sie Ihre Karte nicht zum Laufen bringen, finden Sie in Abschnitt 24.4 Tipps zu den Treibern `vga`, `vesa` oder `fbdev`. Damit funktioniert nahezu jede Grafikkarte, allerdings nur in bescheidener Geschwindigkeit und ohne 3D-Funktionen.

Treiberspezifische Optionen

Nahezu jeder Treiber kennt Optionen zur Steuerung von Spezialeinstellungen, zur Umgehung von Problemen bzw. zur Aktivierung besonderer Funktionen. Detaillierte Informationen gibt die jeweilige `man`-Seite (also beispielsweise `man radeon`). Die folgenden Zeilen zeigen die Anwendung der Option `DisplayPriority`. Sie war auf einem älteren Notebook erforderlich, um in Kombination mit einer Docking-Station ein stabiles Bild auf dem externen TFT-Monitor (via DVI) zu erreichen.

```
Driver      "radeon"
Option      "DisplayPriority" "HIGH"
```

Screen-Abschnitt (Auflösung, Farbanzahl)

Der `Screen`-Abschnitt verbindet den Monitor und die Grafikkarte und gibt an, in welcher Auflösung und mit wie vielen Farben die Grafikkarte verwendet werden soll. Die Schlüsselwörter `Device` und `Monitor` verweisen auf die bereits definierte Grafikkarte und den Monitor. `DefaultDepth` gibt an, wie viele Farben zur Verfügung stehen. Die Angabe erfolgt in Bit pro Pixel. Bei 24 Bit stehen je Grundfarbe 8 Bit – also je 256 Rot-, Grün- und Blautöne – zur Verfügung, insgesamt 2^{24} Farben. Bei 16 Bit stehen je Farbton nur 5 Bit zur Verfügung, ein Bit bleibt üblicherweise ungenutzt.

Innerhalb des `Screen`-Abschnitts können mehrere `Display`-Unterabschnitte angegeben werden, je einer für jede Farbkonfiguration (Schlüsselwort `Depth`). Im Beispiel unten ist nur ein Modus mit 24 Bit pro Pixel definiert:

```
Section "Screen"
  Identifier     "Screen0"
  Device         "Videocard0"
  DefaultDepth   24
  SubSection "Display"
    Depth        24
    Modes        "1280x1024"
  EndSubSection
EndSection
```

In der optionalen `Modes`-Zeile kann die gewünschte Auflösung angegeben werden. Wenn die Zeile weggelassen wird, entscheidet sich X automatisch für die bestmögliche Auflösung, die für den Monitor und die Grafikkarte geeignet ist.

Außerdem kann in jedem `Display`-Abschnitt die Größe des virtuellen Bildschirms eingestellt werden. `Virtual 2540 1440` bewirkt beispielsweise, dass ein virtueller Bildschirm von 2540×1440 Punkten verwaltet wird, unabhängig davon, mit welcher Auflösung der Monitor tatsächlich verwendet wird.

Files-Abschnitt

Im `Files`-Abschnitt werden die Orte diverser Verzeichnisse angegeben, aus denen der X-Server Dateien lädt. Angaben sind nur erforderlich, soweit die Verzeichnisse von den Standardverzeichnissen abweichen.

```
Section "Files"
  FontPath        "/etc/X11/fonts/Type1"
  ...
EndSection
```

Module-Abschnitt

Im `Module`-Abschnitt geben Sie mit dem Schlüsselwort `Load` an, welche Erweiterungsmodule (Extensions) der X-Server verwenden soll:

```
Section "Module"
  Load        "modulname"
  ...
EndSection
```

Der `Module`-Abschnitt ist optional, alle erforderlichen Module werden in der Regel automatisch geladen. Die Moduldateien befinden sich in den Unterverzeichnissen von `/usr/lib/xorg/modules/`. Welche Module geladen sind, stellen Sie so fest:

```
root#  grep LoadModule /var/log/Xorg.0.log
(II) LoadModule: "extmod"
(II) LoadModule: "dbe"
(II) LoadModule: "glx"
...
```

ServerFlags-Abschnitt

Im `ServerFlags`-Abschnitt können Sie Optionen angeben, die das Verhalten des X-Servers beeinflussen:

```
Section "ServerFlags"
  Option      "DontZap"               "false"
EndSection
```

Im Folgenden werden nur drei oft eingesetzte Optionen beschrieben. Eine vollständige Referenz aller Optionen erhalten Sie mit `man xorg.conf`.

- `AllowMouseOpenFail` (Default `off`): Die Einstellung `on` bewirkt, dass X selbst dann gestartet wird, wenn die Initialisierung oder Erkennung der Maus scheitert.
- `DefaultServerLayout`: Die Option gibt an, welches `ServerLayout` verwendet werden soll. Die Option ist erforderlich, wenn `xorg.conf` mehrere `ServerLayout`-Abschnitte enthält.

- DontZap (Grundeinstellung true): Die Einstellung false aktiviert die Tastenkombination Strg+Alt+← zum sofortigen Beenden des X-Servers. Bei manchen Distributionen muss die Tastenkombination außerdem in den Tastatureinstellungen aktiviert werden.

24.4 Grafiktreiber (ATI/AMD, NVIDIA & Co.)

Dieser Abschnitt gibt Tipps zur Installation und Konfiguration der Grafiktreiber für ATI/ADM-, Intel- und NVIDIA-Grafikkarten bzw. Grafikchips. Er endet mit einer kurzen Beschreibung der VESA-, Framebuffer- und VGA-Treiber, die als Notlösung verwendet werden können, wenn es keinen besser geeigneten Treiber gibt (z. B. für manche VIA-Grafikchips).

ATI/AMD-Treiber

Für aktuelle ATI/AMD-Grafikkarten stehen zwei Treiber zur Wahl:

- radeon ist der in X.org integrierte Open-Source-Treiber für aktuelle ATI/AMD-Grafikkarten mit einem Radeon-Grafikchip. Der Treiber ist grundsätzlich zu fast allen momentan verfügbaren Radeon-Chips kompatibel. Der Treiber bietet eine gute 3D-Unterstützung.
- fglrx ist der Binärtreiber der Firma ATI/AMD für Radeon-Modelle ab R600. Der Treiber unterstützt bei neuen Grafikkarten mehr Funktionen als radeon, ist allerdings inkompatibel zu älteren Modellen.

radeon-Treiber

Der radeon-Treiber ist Teil des X.org-Systems, eine separate Installation ist daher nicht notwendig. Die folgenden Zeilen zeigen eine minimale Konfiguration in xorg.conf:

```
Section "Device"
    Identifier   "Device0"
    Driver       "radeon"
EndSection
```

Diverse Spezialfunktionen der Grafikkarte werden durch unzählige Optionen gesteuert (siehe man radeon). Die folgenden Zeilen geben ein gutes Beispiel für die vielen Möglichkeiten und die damit verbundene Komplexität. Diese Konfiguration war erforderlich, um ein älteres IBM-Notebook und einen besonders hartnäckigen Beamer zur Kooperation zu bewegen.

Kurz eine Erklärung zu den eingesetzten Optionen: `MonitorLayout` gibt an, dass sowohl der interne Notebook-Bildschirm als auch der externe Analog-Ausgang (CRT) genutzt werden soll. `MergedFB` bedeutet, dass beide Signalausgänge auf einen gemeinsamen Grafikspeicherbereich zugreifen. Die beiden `CRT2`-Optionen geben die zulässigen Signalfrequenzen am Analog-Ausgang an (also für den Beamer). `IgnoreEDID` bewirkt, dass die vom Beamer zur Verfügung gestellten EDID-Daten ignoriert werden sollen. EDID steht für *Extended Display Identification Data* und ist ein Teil der via DDC (Display Data Channel) vom Monitor an die Grafikkarte übermittelten Daten. Beim vorliegenden Beamer waren diese Daten offensichtlich falsch. `MetaModes` gibt an, welche Auflösungen auf den beiden Signalausgängen genutzt werden sollen – hier also jeweils 1024×768 Pixel:

```
Section "Device"
    Identifier    "device0"
    Driver        "radeon"
    Option        "MonitorLayout" "LVDS,CRT"
    Option        "MergedFB"      "yes"
    Option        "CRT2HSync"     "30-120"
    Option        "CRT2VRefresh"  "58-65"
    Option        "IgnoreEDID"    "yes"
    Option        "MetaModes"     "1024x768-1024x768"
EndSection
```

fglrx-Treiber

Paketinstallation

`fglrx` ist der Binärtreiber der Firma AMD für ATI-Grafikkarten (der Einfachheit halber spreche ich hier auch kurz vom ATI/AMD-Grafiktreiber). Da der Treiber nicht auf Open-Source-Code basiert, ist er in vielen Distributionen nicht enthalten und muss extra installiert werden. Zu den wenigen Ausnahmen zählt Ubuntu.

Für die meisten anderen Distributionen gibt es nichtoffizielle, aber gut gewartete Paketquellen, die die Installation des Treibers sehr einfach machen. Details zu diesem Prozess sind für einige Distributionen in Kapitel 3 zusammengefasst.

aticonfig

Je nach Distribution müssen Sie zur Aktivierung des Treibers anschließend als `root` das Kommando `aticonfig --initial` ausführen. Es verändert `xorg.conf` so, dass statt des bisher eingestellten Treibers der `fglrx`-Treiber zum Einsatz kommt. Im einfachsten Fall enthält der `Device`-Abschnitt nur zwei Zeilen:

```
Section "Device"
    Identifier  "Device0"
    Driver      "fglrx"
EndSection
```

`aticonfig` hilft auch beim Einrichten komplexerer Konfigurationen, beispielsweise für die gleichzeitige Nutzung mehrerer Monitore (`aticonfig --initial=dual`). Einen

Syntaxüberblick sowie mehrere Beispiele liefert `aticonfig`, wenn Sie das Kommando ohne weitere Parameter aufrufen. Eine systematische Dokumentation der zahlreichen Optionen scheint es aber nicht zu geben. Die neue `xorg.conf`-Datei wird wie üblich erst nach einem X-Neustart wirksam.

Die 3D-Funktionen der Grafikkarte lassen sich nur nutzen, wenn das Kernelmodul `fglrx` geladen ist. Normalerweise kümmert sich der ATI-Treiber darum selbst. Ob das Kernelmodul tatsächlich aktiv ist, stellen Sie am einfachsten mit `lsmod | grep fglrx` fest. Wurde das Modul nicht geladen, ist es wahrscheinlich nicht installiert bzw. nicht kompatibel zur aktuellen Kernelversion. Abhilfe schafft ein Update des betreffenden Pakets bzw. das Neukompilieren des Moduls. Das Kernelmodul ist nur für die 3D-Funktionen erforderlich. Der `fglrx`-Treiber funktioniert auch ohne das Kernelmodul, allerdings müssen dann die 3D-Funktionen per Software emuliert werden, was sehr langsam ist.

Nachträgliche Änderungen an der Konfiguration nehmen Sie entweder mit `aticonfig` oder mit der grafischen Oberfläche `amdcccle` vor (siehe unten).

Manuelle Treiberinstallation

Wenn es für Ihre Distribution keine fertigen Treiberpakete gibt oder wenn diese nicht ausreichend aktuell sind, müssen Sie selbst Hand anlegen. Dazu installieren Sie zuerst alle Entwicklungswerkzeuge, die zum Kompilieren von Kernelmodulen erforderlich sind (siehe Abschnitt 28.1). Anschließend laden Sie von der folgenden Webseite das für Ihre Grafikkarte und die Architektur Ihrer Distribution (32 oder 64 Bit) passende Installationsprogramm herunter (ca. 120 MByte):

http://support.amd.com/us/gpudownload/Pages/index.aspx

Dann packen Sie die ZIP-Datei aus und führen mit `sh` das Installationsprogramm aus:

```
root#  unzip amd-driver-installer-<n-n>-x86.x86_64.zip
root#  sh amd-driver-installer-<n-n>-x86.x86_64.run
```

Nun klicken Sie sich durch die Dialoge des grafischen Installationsprogramms. Details über den Installationsprozess verät die Protokolldatei `/usr/share/ati/fglrx-install.log`. Sofern keine Probleme auftreten, lädt das Installationsprogramm zuletzt das Kernelmodul `fglrx`, wovon Sie sich mit `lsmod | grep fglrx` überzeugen können.

Alternativ besteht die Möglichkeit, zuerst ein Treiberpaket für Ihre Distribution zu erzeugen und dieses dann zu installieren. Das ist etwas umständlicher, erleichtert aber die Wartung und ermöglicht eine spätere Deinstallation mit jedem beliebigen Paketverwaltungswerkzeug. `ati-driver-installer --listpkg` liefert eine Liste der unterstützten Paketformate und Distributionen. `ati-driver-installer --buildpkg` *`distribution/version`* erzeugt dann das entsprechende Paket.

Wenn das Kernelmodul `flgrx` geladen werden kann, müssen Sie noch `aticonfig` ausführen, um `xorg.conf` dahingehend zu ändern, dass der `fglrx`-Treiber verwendet wird:

```
root#  aticonfig --initial
```

Beachten Sie, dass Sie das Installationsprogramm nach jedem Kernel-Update neuerlich ausführen müssen. Dabei wird das Kernelmodul `fglrx` neu kompiliert, damit es zu Ihrer jetzigen Kernelversion kompatibel ist!

Um den Treiber zu deinstallieren, führen Sie das folgende Kommando aus:

```
root#  /usr/share/ati/fglrx-uninstall.sh
```

Sebastian Siebert hat für openSUSE das Script `makerpm-ati` entwickelt, das den Treiber automatisch herunterlädt und in ein openSUSE-kompatibles Paket verpackt, das Sie anschließend nur noch installieren müssen. Sie finden dieses Script hier:

http://de.opensuse.org/SDB:AMD/ATI-Grafiktreiber

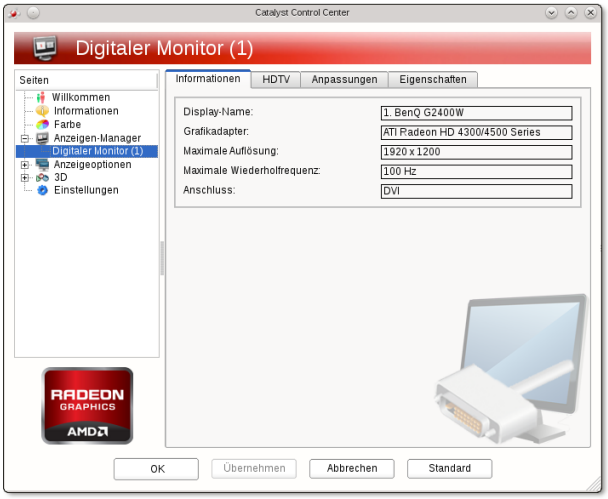


Abbildung 24.1 ATI/AMD-Treiberkonfiguration

Catalyst Control Center

Zur weiteren Konfiguration des `fglrx`-Treibers verwenden Sie am besten das *Catalyst Control Center* (Kommando `amdcccle`, siehe Abbildung 24.1). Auch wenn die Benutzeroberfläche den Charme des vorigen Jahrtausends versprüht, ist das Programm doch komfortabler zu nutzen als `aticonfig`. Die meisten Einstellungen können mit gewöhnlichen Benutzerrechten vorgenommen werden. Die Einstellungen werden in Dateien des Verzeichnisses `/etc/ati` gespeichert. Lediglich die Konfiguration des ANZEIGEN-MANAGERS, der unter anderem für Dual-Screen-Setups verantwortlich ist, erfordert den Start des Programms mit `root`-Rechten.

Intel-Treiber

Der Open-Source-Treiber `intel` ist kompatibel zu allen gängigen Intel-Chipsätzen inklusive Ivy Bridge, Sandy Bridge und Haswell. Die einzige Ausnahme sind die Grafikkerne GMA 500, 600, 3600 und 3650 (»Poulsbo«), und die in manchen Netbooks zum Einsatz kamen und nach wie vor in einigen Atom-CPUs integriert sind. Allgemeine Informationen zum Intel-Treiber geben `man intel` sowie die folgende Website:

https://01.org/linuxgraphics

Da der Treiber offizieller Bestandteil von X ist, entfällt die mühsame Installation von Zusatzpaketen. Der Treiber erkennt die Hardware selbstständig, die explizite Einstellung von Optionen ist im Regelfall nicht notwendig.

Den neuesten Intel-Treiber installieren

Nicht immer ist der von Ihrer Distribution mitgelieferte Intel-Treiber auf dem aktuellsten Stand. Solange das Grafiksystem problemlos funktioniert, spielt das keine Rolle. Sollten Sie aber aus irgendeinem Grund den allerneuesten Intel-Grafiktreiber ausprobieren wollen, finden Sie unter *https://01.org/linuxgraphics/downloads* ein spezielles Setup-Programm für aktuelle Fedora- und Ubuntu-Versionen.

NVIDIA-Treiber

Wenn Sie eine NVIDIA-Grafikkarte nutzen, haben Sie die Wahl zwischen zwei Treibern:

- `nouveau` ist ein Open-Source-Treiber, der auf fast allen gängigen Distributionen standardmäßig zum Einsatz kommt. `nouveau` unterstützt zwar 3D-Funktionen, allerdings noch nicht für alle NVIDIA-Chip-Modelle. Auch die korrekte Steuerung der Energiesparfunktionen bereitet bei manchen Modellen Probleme.
- `nvidia` ist der Binärtreiber der Firma NVIDIA. Er unterstützt nahezu alle Funktionen aller aktuellen Grafikkarten. Den Binärtreiber gibt es in zwei Varianten: Die offizielle Version unterstützt nur aktuelle Modelle, die Legacy-Version ältere Modelle.

Der nouveau-Treiber

Normalerweise erkennt der X.org-Server Intel-Grafikchips und aktiviert den `nouveau`-Treiber selbstständig. Sollte das nicht klappen, helfen die folgenden Zeilen in `xorg.conf`:

```
Section "Device"
    Identifier    "Device0"
    Driver        "nouveau"
EndSection
```

Es gibt nur relativ wenige Optionen, die in `man nouveau` beschrieben sind. Weitere Informationen finden Sie hier:

http://nouveau.freedesktop.org/wiki

Der nvidia-Treiber

Nur bei wenigen Distributionen werden der `nvidia`-Treiber und das gleichnamige Kernelmodul mitgeliefert bzw. sofort installiert. Häufig existieren aber Paketquellen, die zum gerade aktuellen Kernel passende Treiberpakete enthalten. Damit ist die Installation ein Kinderspiel: Nach dem Einrichten der Paketquelle wird der Treiber mit den üblichen Paketverwaltungskommandos installiert. Details zu diesem Prozess sind für einige Distributionen in Kapitel 3 zusammengefasst (siehe auch den Eintrag »`nvidia`-Treiber« im Stichwortverzeichnis). Besonders komfortabel gelingt die Treiberinstallation unter Ubuntu: Dort führen Sie im Startmenü das Programm SOFTWARE & AKTUALISIERUNG aus. Die für Ihr System passenden Treiber werden im Dialogblatt ZUSÄTZLICHE TREIBER aufgelistet (siehe Abbildung 24.2). Zur Aktivierung müssen Sie den Rechner neu starten.

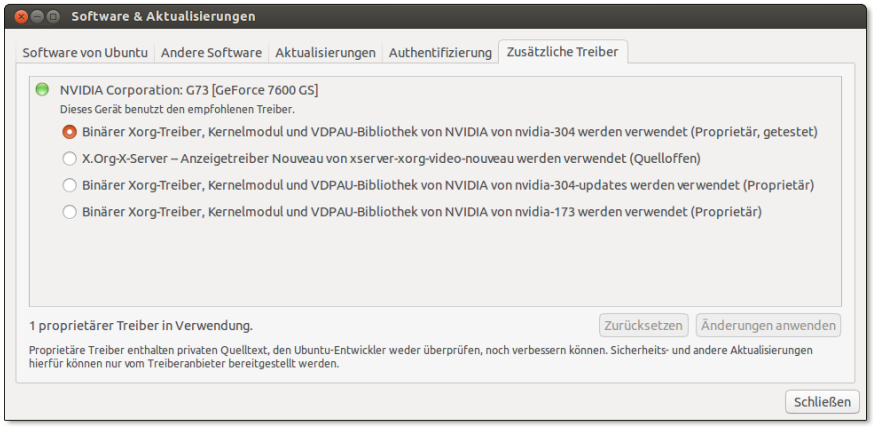


Abbildung 24.2 Installation des NVIDIA-Treibers unter Ubuntu

xorg.conf

Zur Aktivierung des Treibers führen Sie als `root` das Kommando `nvidia-xconfig` aus. Es verändert `xorg.conf` so, dass statt des bisher eingestellten Treibers der `nvidia`-Treiber zum Einsatz kommt. Wenn Sie spezielle Konfigurationswünsche haben, übergeben Sie an `nvidia-xconfig` weitere Parameter, die in der `man`-Seite beschrieben sind. Im einfachsten Fall enthält der `Device`-Abschnitt nur zwei Zeilen:

```
Section "Device"
    Identifier  "Device0"
    Driver      "nvidia"
EndSection
```

Der NVIDIA-Treiber ist inkompatibel mit der DRI-Erweiterung von X.org und realisiert diese Funktionen stattdessen selbst. Aus diesem Grund darf `xorg.conf` die Zeile `Load "dri"` nicht enthalten.

nvidia-settings

Sobald der NVIDIA-Treiber grundsätzlich läuft, setzen Sie zur weiteren Konfiguration das Programm `nvidia-settings` ein (siehe Abbildung 24.3). Es ermöglicht die unmittelbare Veränderung zahlreicher Optionen, also ohne X-Neustart. Wenn das Ergebnis zufriedenstellend ist, können Sie die Änderungen in `xorg.conf` speichern. Dabei müssen Sie dann das `root`- oder Ihr eigenes Passwort für `sudo` angeben.

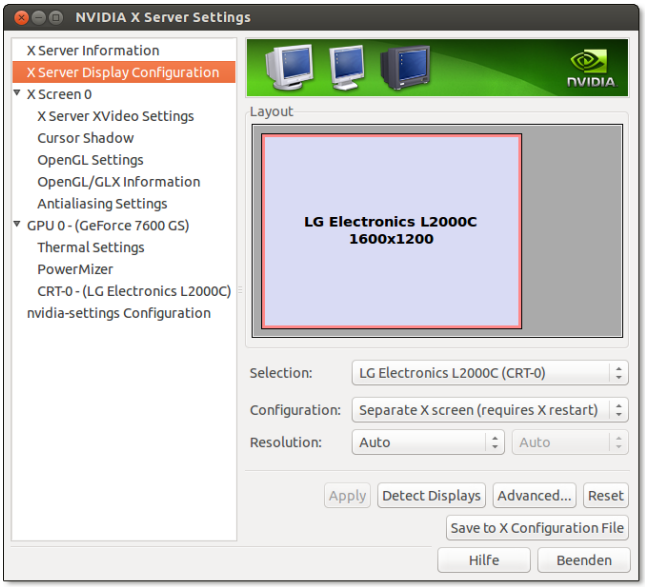


Abbildung 24.3 NVIDIA-Treiberkonfiguration

NVIDIA-Kernelmodul

Anders als bei ATI/AMD setzt der NVIDIA-Treiber das `nvidia`-Kernelmodul unbedingt voraus. Wenn das Kernelmodul fehlt bzw. wenn es für die falsche Kernelversion kompiliert wurde, funktioniert der Treiber überhaupt nicht und X kann nicht gestartet werden!

TwinView

Für den Betrieb mit zwei Monitoren bietet der NVIDIA-Treiber mit dem `TwinView`-Modus eine interessante Alternative zu Xinerama (das ebenfalls unterstützt wird). Im `TwinView`-Modus verwaltet der NVIDIA-Treiber einen durchgängigen Bildschirmbereich (`Screen`), der über beide Monitore verteilt dargestellt wird. Die Vorteile

gegenüber Xinerama bestehen darin, dass alle 3D-Funktionen monitorübergreifend genutzt werden können und dass die Konfiguration sehr einfach ist.

Die folgenden Zeilen zeigen die wichtigsten Abschnitte einer einfachen TwinView-Konfiguration. Dabei war ein TFT-Monitor mit 1920×1200 Pixel am DVI-Ausgang der Grafikkarte angeschlossen, ein zweiter TFT-Monitor mit 1600×1200 Pixel am CRT-Ausgang. TwinView macht daraus eine virtuelle Auflösung von 3520×1200 Pixel.

Obwohl das System zwei Monitore umfasst, gibt es nur einen Screen-Abschnitt. Die Eckdaten der Monitore werden automatisch ermittelt. TwinViewXineramaInfoOrder DFP bewirkt, dass der DVI-Ausgang der Grafikkarte als Primärausgang gilt. Dank dieser Option erscheinen beispielsweise der X-Login sowie die KDE- und Gnome-Panels auf dem hier angeschlossenen Monitor.

```
Section "Device"
    Identifier     "Device0"
    Driver         "nvidia"
    VendorName     "NVIDIA Corporation"
    BoardName      "GeForce 7600 GS"
EndSection
Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    DefaultDepth    24
    Option         "TwinView" "1"
    Option         "TwinViewXineramaInfoOrder" "DFP"
    Option         "metamodes" "DFP: nvidia-auto-select +0+0, \
                                CRT: nvidia-auto-select +1920+0"
    SubSection     "Display"
        Depth       24
    EndSubSection
EndSection
```

Manuelle Installation

Wenn es für Ihre Distribution keine fertigen Treiberpakete gibt oder wenn diese Pakete nicht aktuell sind, müssen Sie den Treiber selbst installieren und insbesondere das Kernelmodul nvidia selbst kompilieren. Dazu installieren Sie zuerst alles, was notwendig ist, um Kernelmodule zu kompilieren (C-Compiler, make, Kernel-Header-Dateien etc. – siehe auch Abschnitt 28.1). Darüber hinaus benötigen Sie die Pakete xorg-x11-server-sdk bzw. xserver-xorg-dev sowie pkgconfig bzw. pgk-config.

Von der folgenden Webseite laden Sie das für Ihre Grafikkarte und die Architektur Ihrer Distribution (32 oder 64 Bit) passende Installationsprogramm herunter:

http://www.nvidia.com/Download/index.aspx

Anschließend beenden Sie X und starten dann als root das Installationsprogramm:

```
root#  sh NVIDIA-Linux-version.run
```

Das Installationsprogramm läuft im Textmodus, ist aber dialoggesteuert und komfortabel zu bedienen. Es testet zuerst, ob es für Ihre Kernelversion bereits ein vorkompiliertes `nvidia`-Kernelmodul auf der Website von NVIDIA gibt. Ist das nicht der Fall, wird ein passendes Kernelmodul kompiliert. Sofern alle Voraussetzungen erfüllt sind, dauert das nur wenige Sekunden. Das Installationsprogramm installiert anschließend die NVIDIA-spezifischen `libGL`-Bibliotheken und führt nach einer Rückfrage das oben schon erwähnte Kommando `nvidia-xconfig` aus.

Ein ausführliches Protokoll aller durchgeführten Aktionen finden Sie in `/var/log/nvidia-installer.log`. Sofern keine Fehler aufgetreten sind, steht einem X-Neustart mit dem NVIDIA-Treiber nichts mehr im Wege.

Beachten Sie, dass Sie das Installationsprogramm nach jedem Kernel-Update neuerlich ausführen müssen. Dabei wird das Kernelmodul `nvidia` neu kompiliert, damit es zu Ihrer jetzigen Kernelversion kompatibel ist.

Um den Treiber zu deinstallieren, führen Sie das folgende Kommando aus. Dadurch wird die bisherige `xorg.conf`-Datei wiederhergestellt und das `nvidia`-Kernelmodul gelöscht, und es werden Links auf die originalen `libGL`-Bibliotheken eingerichtet.

```
root#  nvidia-installer --uninstall
```

VESA-, Framebuffer- und VGA-Treiber

Wenn Sie eine Grafikkarte nutzen, zu der es keine Treiber gibt, stellen die drei in diesem Abschnitt vorgestellten Treiber eine Notlösung dar. Auch wenn der Bildaufbau vergleichsweise langsam ist und natürlich keinerlei 3D-Funktionen zur Verfügung stehen, ermöglichen die Treiber zumindest überhaupt eine Nutzung des Grafiksystems.

VESA-Treiber

Mit dem VESA-Treiber können Sie alle VESA-Modi Ihrer Grafikkarte nutzen. Kurz einige Hintergrundinformationen: Die *Video Electronics Standard Association* (VESA) hat eine Reihe von Grafikmodi für Standardauflösungen normiert. Jeder Modus ist durch die folgenden Eckdaten bestimmt: Auflösung (z. B. 1280×1024 Pixel), Farbtiefe und Bildfrequenz. Fast alle Grafikkarten unterstützen neben eigenen Grafikmodi auch eine Menge VESA-Modi.

Wie die nächsten Zeilen zeigen, ist die Verwendung des VESA-Treibers denkbar einfach. Sofern die restliche Konfigurationsdatei korrekt ist, werden alle VESA-Modi berücksichtigt, die die Grafikkarte unterstützt und die der Monitor darstellen kann.

```
# in /etc/X11/xorg.conf
...
Section "Device"
  Identifier    "myDevice"
  Driver        "vesa"
EndSection
```

Framebuffer-Treiber

Der `fbdev`-Treiber greift direkt auf den Speicher (Framebuffer) der Grafikkarte zu. Der Treiber setzt damit noch eine Ebene tiefer an als der VESA-Treiber. Er sollte mit fast allen Grafikkarten funktionieren, sofern der Linux-Kernel mit Framebuffer-Unterstützung kompiliert wurde. Dass diese Unterstützung vorhanden ist, erkennen Sie daran, dass die Datei `/proc/fb` existiert.

Eine grundlegende Voraussetzung für die Nutzung des Treibers besteht allerdings darin, dass bereits beim Booten des Rechners der richtige VGA-Modus ausgewählt wird. Bis zum Neustart des Rechners kann X nur in dem so festgelegten Grafikmodus betrieben werden. Zur Auswahl des Modus fügen Sie in die GRUB-Konfigurationsdatei die Kerneloption `vga=`*n* ein. Die richtigen Werte (dezimal) für *n* finden Sie in der folgenden Tabelle. Unter SUSE können Sie außerdem mit `hwinfo -framebuffer` eine Liste der Framebuffer-Modi ermitteln, die Ihre Grafikkarte unterstützt.

	640x480	800x600	1024x640	1024x768	1280x1024	1440x900	1600x1200
8 bpp	769	771	874	773	775	864	796
16 bpp (5:5:5)	784	787	875	790	793	865	797
16 bpp (5:6:5)	785	788	876	791	794	866	798
24 bpp	786	789	877	792	795	867	799
32 bpp	809	814	878	824	829	868	834

In `xorg.conf` müssen Sie lediglich die richtige `Driver`-Zeichenkette angeben:

```
# in /etc/X11/xorg.conf
...
Section "Device"
  Identifier    "myDevice"
  Driver        "fbdev"
EndSection
```

vga-Treiber

Der `vga`-Treiber unterstützt nur 640×480 oder 800×600 Pixel bei einer Farbtiefe von 4 Bit (also 16 Farben) und ist somit nur die letzte Notlösung. Weitere Details finden Sie mit `man vga`.

24.5 Tastatur und Maus

Es gibt verschiedene Treiber, über die X mit der Tastatur, der Maus oder einem Touchpad kommuniziert: Die meisten aktuellen Distributionen verwenden den `evdev`-Treiber für Maus und Tastatur. Auf Notebooks mit einem Touchpad kommt außerdem der `synaptics`-Treiber zum Einsatz. Welche Treiber X auf Ihrem Rechner verwendet, stellen Sie am schnellsten mit einem Blick in die X-Logging-Datei fest:

```
root#  grep LoadModule /var/log/Xorg.0.log
...
(II) LoadModule: "evdev"
(II) LoadModule: "synaptics"
```

evdev-Treiber (Tastatur und Maus)

Der größte Vorteil des `evdev`-Treibers im Vergleich zu den älteren `xkbd`- und `mouse`-Treibern besteht darin, dass er problemlos mit Tastaturen und Mäusen zurechtkommt, die im laufenden Betrieb angeschlossen bzw. entfernt werden.

Der Sektionsname `InputClass` in `xorg.conf` und das Schlüsselwort `MatchIsKeyboard` ermöglichen es, Einstellungen für eine ganze Gruppe von Geräten derselben Klasse durchzuführen, hier also für alle Tastaturen, die an den Rechner angeschlossen sind. Mit `MatchVendor` ist es möglich, die Konfiguration auf einen bestimmten Hersteller einzuschränken, mit `MatchDevicePath` auf einen bestimmten Device-Namen.

```
Section "InputClass"
  Identifier      "mykeyboard"
  MatchIsKeyboard "on"
  Option          "XkbModel"      "pc105"
  Option          "XkbLayout"     "de"
  Option          "XkbVariant"    "nodeadkeys"
  Option          "XkbOptions"    "terminate:ctrl_alt_bksp,"
EndSection
```

Die einzelnen Optionen stimmen mit denen des `xkbd`-Treibers überein und sind etwas weiter unten beschrieben. Wie die Konfiguration durchgeführt wird, ist distributionsabhängig:

- Bei Debian und Ubuntu liest das `udev`-Script `/lib/udev/rules.d/64-xorg-xkb.rules` die Variablen `XKBxxx` aus der Datei `/etc/default/keyboard`.
- Bei Fedora und anderen Distributionen mit einer aktuellen Systemd-Version werden die Tastatureinstellungen für die Konsole in `/etc/locale.conf` gespeichert, für X in der Datei `/etc/X11/xorg.conf.d/00-keyboard.conf`. Direkte Änderungen dieser Dateien sollten vermieden werden; stattdessen ist das Kommando `localectl` zur Einstellung der Tastaturoptionen vorgesehen.
- Bei openSUSE erfolgt die Konfiguration statisch durch die Datei `/etc/X11/xorg.conf.d/90-keytable.conf`.

Einstellungen für die Mausfunktionen des `evdev`-Treibers sind in der Regel nicht erforderlich. Sollte das doch einmal der Fall sein, erfolgen die Mauseinstellungen wie die Tastatureinstellungen in einem `InputClass`-Abschnitt, der diesmal aber durch das Schlüsselwort `MatchIsPointer` markiert wird. Die einzelnen Optionen entsprechen denen des weiter unten beschriebenen `mouse`-Treibers.

```
Section "InputClass"
  Identifier      "mymouse"
  MatchIsPointer  "on"
  Option          "Emulate3Buttons" "on"
  Option          ...
EndSection
```

xkbd-Treiber (Tastatur)

Der `xkbd`-Treiber wird durch einen `InputDevice`-Abschnitt in `xorg.conf` statisch konfiguriert. Fehlt dieser Abschnitt, funktioniert die Tastatur zumeist dennoch, allerdings mit dem US-Tastaturlayout. Die folgenden Zeilen zeigen die erforderlichen Einstellungen für ein deutsches Tastaturlayout:

```
Section "InputDevice"
  Identifier  "myKeyboard"
  Driver      "Keyboard"
  Option      "XkbModel"    "pc105"
  Option      "XkbLayout"   "de"
  Option      "XkbVariant"  "nodeadkeys"
EndSection
```

Die folgenden Punkte fassen die wichtigsten Einstellungen für die Schlüsselwörter `XkbXxx` zusammen:

- **`XkbRules`** bestimmt, wie die Einstellungen für die weiteren Optionen ausgewertet werden sollen. Im Regelfall lautet hier die richtige Einstellung `xorg`.
- **`XkbModel`** beschreibt die Tastatur. Zulässige Einstellungen sind unter anderem:

`pc101`	US-Tastatur ohne Windows-Tasten (Standardeinstellung)
`pc102`	internationale Tastatur ohne Windows-Tasten
`pc104`	US-Tastatur mit Windows-Tasten
`pc105`	internationale Tastatur mit Windows-Tasten

- **`XkbLayout`** beschreibt die Anordnung der Tasten auf der Tastatur. Diese ist länderabhängig. Als Einstellungen sind die üblichen Ländercodes zulässig, beispielsweise `us` (Englisch), `de` (Deutsch) oder `fr` (Französisch).
- **`XkbVariant`** ermöglicht Zusatzeinstellungen zum Tastaturlayout. Die gebräuchlichste Einstellung lautet `nodeadkeys`. Sie bewirkt, dass die Zeichen `~ ^ ' ` unmittelbar eingegeben werden können und nicht zur Komposition von Zeichen aus Fremdsprachen dienen. Bei Apple-Tastaturen geben Sie die Einstellung `mac` an.
- **`XkbOptions`** enthält Zusatzoptionen zur Weiterleitung an `setxkbmap -option`.

Um eine Tastatur mit vielen Sondertasten unter Linux optimal zu nutzen, können Sie das Programm LinEAK installieren (*Linux support for Easy Access and Internet Keyboards*, Paketname `lineak*`). Detaillierte Informationen zur Konfiguration geben `man lineakd` sowie die folgende Website:

http://lineak.sourceforge.net

mouse-Treiber (Maus)

Auch der `mouse`-Treiber wird durch einen `InputDevice`-Abschnitt konfiguriert. Wenn der Abschnitt fehlt, versucht X eine passende Konfiguration selbst zu erraten, was zumeist gelingt. Die folgenden Zeilen zeigen eine Minimalkonfiguration für eine Maus mit Mausrad:

```
Section "InputDevice"
  Identifier   "myMouse"
  Driver       "mouse"
  Option       "Protocol"    "Auto"
  Option       "Device"      "/dev/input/mice"
  Option       Buttons 5
  Option       "ZAxisMapping" "4 5"
EndSection
```

Zur Konfiguration der Maus sind folgende Schlüsselwörter vorgesehen:

- `Protocol` gibt an, wie die Kommunikation zwischen Maus und Computer erfolgt. Übliche Einstellungen sind `auto` oder `usb`.
- `Device` gibt an, wie die Maus mit dem Computer verbunden ist. Übliche Einstellungen sind `/dev/input/mouse`*n* bzw. `/dev/input/mice`, wobei im zweiten Fall alle angeschlossenen Mäuse und Touchpads parallel ausgewertet werden.
- `Buttons` gibt an, wie viele Tasten die Maus hat. Standardmäßig nimmt X an, dass es drei Tasten gibt. Beachten Sie, dass jedes Rad wie zwei Tasten gerechnet wird. Bei einer Maus mit drei Tasten und einem Rad lautet die richtige Einstellung also 5.
- `ZAxisMapping` gibt an, welchen virtuellen Buttons eventuell vorhandene Räder zugeordnet werden. Wenn Sie das Mausrad in die eine Richtung drehen, wertet X das wie das Drücken eines Buttons aus. Wenn Sie das Rad in die andere Richtung drehen, entspricht dies einem zweiten Button.
- `Emulate3Buttons` ermöglicht es, durch das gleichzeitige Drücken der rechten und linken Maustaste eine fehlende mittlere Maustaste zu simulieren. Das ist eine Notlösung für Mäuse ohne Mausrad. Beachten Sie, dass diese Option bei aktuellen Xorg-Versionen standardmäßig deaktiviert ist!

  Mit `Emulate3Timeout` kann die Zeit in Millisekunden angegeben werden, innerhalb der beide Tasten gedrückt werden müssen. Wählen Sie diese Zeit zu klein, wird das nicht ganz gleichzeitige Drücken beider Tasten separat gewertet. Zu große Werte sind aber auch unpraktisch, weil die Reaktion auf jeden Mausklick um die-

se Zeit verzögert wird (weil X noch nicht weiß, wie es den Mausklick werten soll). Brauchbare Einstellungen sind:

```
Option "Emulate3Buttons" "on"
Option "Emulate3Timeout" "50"
```

synaptics-Treiber (Touchpad)

Auf den meisten Notebooks befinden sich Touchpads der Firma Synaptics oder dazu kompatible Komponenten. Grundsätzlich emuliert das Protokoll dieser Geräte eine Standardmaus, sodass zur Verwendung unter X keine speziellen Treiber erforderlich sind. Um aber auch diverse Zusatzfunktionen des Touchpads zu nutzen, wird statt des `mouse`-Treibers in der Regel der `synaptics`-Treiber verwendet.

X lädt den Treiber beim Start automatisch – und das auch bei Distributionen, die für die Tastatur und herkömmliche Mäuse den `evdev`-Treiber nutzen. Wie bei `xkbd` und `mouse` ist eine manuelle Konfiguration in `xorg.conf` nur erforderlich, wenn die von X gewählten Standardeinstellungen nicht zufriedenstellend funktionieren. Die unzähligen Optionen dieses Treibers dokumentiert `man synaptics`. In der Regel können Sie sich die Lektüre aber sparen und Ihr Touchpad komfortabler in den KDE- oder Gnome-Systemeinstellungen konfigurieren.

Xmodmap

Obwohl das Verfahren schon seit vielen Jahren als veraltet gilt, ist es nach wie vor möglich, die Tastatur- und Mauskonfiguration durch das Kommando `xmodmap` bzw. durch `Xmodmap`-Dateien zu verändern. Ein Anwendungsbeispiel ist das Vertauschen von Tasten. Wenn Sie eine deutsche Apple-Tastatur unter Linux verwenden, sind mitunter die Tasten [<] und [^] vertauscht. Abhilfe schafft die folgende Datei `.Xmodmap`, die beim Einloggen automatisch berücksichtigt wird. Außerdem müssen Sie natürlich noch das Apple-spezifische Tastaturlayout einstellen, z. B. mit den Tastaturkonfigurationsprogrammen von Gnome oder KDE.

```
keycode  94 = asciicircum degree asciicircum degree notsign notsign notsign
keycode  49 = less greater less greater bar brokenbar bar
```

Und gleich noch ein Tipp für Mac-Liebhaber: Wenn Sie sich unter OS X an das verkehrte Scroll-Verhalten von Mausrad und Touchpad gewöhnt haben, können Sie auch X so konfigurieren. Eine einzige Zeile in `.Xmodmap` reicht dazu aus:

```
pointer = 1 2 3 5 4 7 6
```

Beachten Sie die abweichende Reihenfolge der Zahlen 4 und 5 sowie 6 und 7! Damit wird die Funktion der Maustasten 4 und 5 sowie 6 und 7 umgedreht. Diese vier virtuellen Maustasten repräsentieren Linux-intern die Drehung des Mausrads bzw. das Drücken des Mausrads nach rechts oder links. Eine Sammlung weiterer `Xmodmap`-Beispiele finden Sie hier:

http://www.pro-linux.de/artikel/2/1198/zauberspiele-mit-xmodmap.html

Gnome und KDE

Unabhängig von der X-Konfiguration geben auch die Systemeinstellungen von Gnome und KDE die Möglichkeit, die Tastatur, die Maus und das Touchpad individuell einzurichten. Zur Konfiguration der Tastatur öffnen Sie unter Gnome 3 das Modul REGION UND SPRACHE, unter KDE verwenden Sie das Modul EINGABEGERÄTE. Mit diesen Programmen können Sie auch einstellen, wie sich die CapsLock-Taste verhalten soll und ob eine Taste (z. B. die Windows-Taste) als Compose-Taste dienen soll. Damit können Sie die zwei Zeichen gleichsam vereinen. Beispielsweise liefert Compose, A, E das Zeichen Æ.

24.6 Dynamische Konfigurationsänderungen mit RandR

Die *Resize and Rotate Extension* (RandR) erlaubt es, Teile der Konfiguration von X im laufenden Betrieb zu verändern, soweit der Grafiktreiber dies unterstützt. Aktuelle Desktop-Systeme passen sich automatisch an die neuen Rahmenbedingungen – beispielsweise an die geänderte Bildschirmauflösung – an und müssen nicht neu gestartet werden.

Manuelle Änderungen können Sie mit dem Kommando `xrandr` ausführen. Mehr Komfort bieten die entsprechenden Module der Gnome- bzw. KDE-Systemeinstellungen.

xrandr

Wenn Sie `xrandr` ohne Parameter bzw. mit der Option `-q` ausführen, zeigt es den aktuellen Status von X an. Die folgende Ausgabe bedeutet, dass der Monitor den DVI-Signalausgang nutzt und mit einer Auflösung von 1680×1050 Pixeln betrieben wird. Die Angaben in Klammern bedeuten, dass das Bild gedreht, gespiegelt oder invertiert werden kann. Die nachfolgende Liste zeigt an, welche anderen Auflösungen eingestellt werden können. Wichtig sind auch die Namen der Signalausgänge (hier VGA-0 und DVI-I-0), weil diese Zeichenketten je nach Grafiktreiber variieren.

```
user$  xrandr
Screen 0: minimum 320 x 200, current 1680 x 1050, maximum 4080 x 4096
VGA-0 disconnected
DVI-I-0 connected 1680x1050+0+0 (normal left inverted right x axis y axis)
 434mm x 270mm
   1680x1050      60.0*+
   1400x1050      60.0
   1280x1024      75.0     60.0
   1280x960       60.0
   1152x864       75.0
   1024x768       75.0     70.1     60.0
   ...
   640x480        75.0     72.8     75.0     59.9
```

`xrandr` kann mit gewöhnlichen Benutzerrechten ausgeführt werden. Alle durchgeführten Änderungen gelten aber nur bis zum nächsten Logout. Das folgende Kommando reduziert die Auflösung auf 1280×1024 Punkte:

```
user$  xrandr --size 1280x1024
```

Das nächste Kommando aktiviert beide Ausgänge. Auf beiden Monitoren wird dasselbe Bild angezeigt. Die Option `--auto` bewirkt, dass jeder Monitor in der für ihn optimalen Auflösung und Bildfrequenz betrieben wird.

```
user$  xrandr --output DVI-I-0 --auto --output VGA-0 --auto
user$  xrandr --output VGA-0 --off   (schaltet den VGA-Ausgang wieder ab)
```

Weitere `xrandr`-Beispiele folgen im nächsten Abschnitt zur Dual-Head-Konfiguration.

Neue Auflösungen definieren

Mit `xrandr` können Sie nur solche Auflösungen aktivieren, die der Treiber der Grafikkarte für den angeschlossenen Monitor vorsieht (siehe das Ergebnis von `xrandr`). Wenn Sie eine andere Auflösung wünschen, z. B. zur Aufnahme eines Screencasts, müssen Sie diese zuerst mit `xrandr --newmode` definieren, beispielsweise so:

```
user$  xrandr --newmode 1280x720 74.18 1280 1390 1430 1650 720 725 730 750
user$  xrandr --addmode HDMI1 1280x720
user$  xrandr --size 1280x720
```

Beim zweiten `xrandr`-Kommando ist es entscheidend, dass Sie an die Option `--addmode` den Namen des aktiven Grafikausgangs übergeben. Falls Sie die Parameter für den gewünschten Modus nicht kennen (die Syntax ist dieselbe wie bei den `XMode`-Zeilen in `xorg.conf`), finden Sie im Internet in der Regel ein entsprechendes Beispiel. Suchen Sie z. B. nach *modeline 1280x720*. Alternativ können Sie die Parameter auch mit dem Kommando `gtf` errechnen:

```
root#  gtf 1280 720 60
# 1280x720 @ 60.00 Hz (GTF) hsync: 44.76 kHz; pclk: 74.48 MHz
Modeline "1280x720_60.00"  74.48  1280 1336 1472 1664 \
   720 721 724 746 -HSync +Vsync
```

RandR-Einstellungen in Gnome und KDE

Unter Gnome 3.*n* verändern Sie die RandR-Konfiguration mit dem Modul Monitore der Systemeinstellungen (siehe Abbildung 24.4). Unter Gnome 2.*n* starten Sie stattdessen `gnome-display-properties`.

Wenn es mehr als einen Monitor gibt, wird standardmäßig auf beiden dasselbe Bild angezeigt (Bildschirme spiegeln), wobei sich die Bildgröße aus dem jeweils kleineren Wert der horizontalen und vertikalen Auflösung ergibt. Erst wenn Sie die Option Bildschirme spiegeln deaktivieren, können Sie die beiden Monitore getrennt konfigurieren und ihre Position relativ zueinander verändern. Die Einstellungen werden in `.config/monitors.xml` gespeichert. Sie gelten nur für den aktuellen Benutzer.

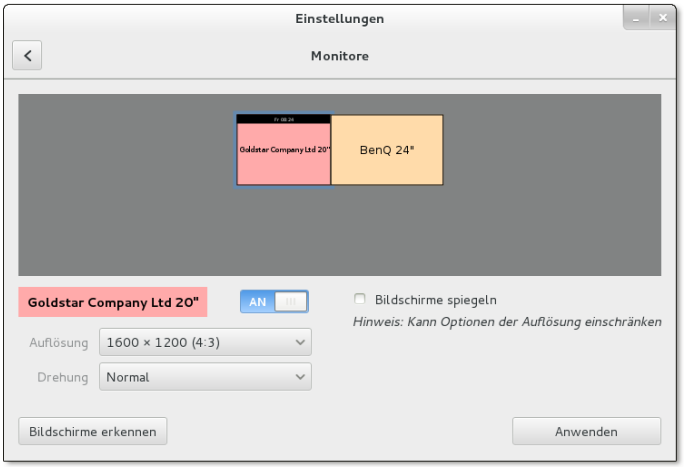


Abbildung 24.4 RandR-Einstellungen unter Gnome verändern

Um die Bildschirmeinstellungen auch für den von `gdm` angezeigten Login-Bildschirm zu verändern, kopieren Sie `monitors.xml` in das `gdm`-Verzeichnis:

```
user$  sudo cp ~/.config/monitors.xml /var/lib/gdm/.config
```

Das KDE-Gegenstück zu `gnome-display-properties` ist das Modul ANZEIGE UND MONITOR der Systemeinstellungen. Es bietet im Wesentlichen dieselben Funktionen, speichert seine Einstellungen aber in der Datei `.kde4/share/config/krandrrc`. Wenn Ihre Einstellungen beim nächsten Login nicht berücksichtigt werden, haben Sie vergessen, nach Abschluss der Konfiguration den Button ALS STANDARD SPEICHERN anzuklicken.

Ubuntu verwendet eine modifizierte Variante des Gnome-Einstellungsmoduls. Die Syntax und der Speicherort der Konfigurationsdatei sind wie unter Gnome.

24.7 Dual-Head-Konfiguration und Beamer

Von einer »Dual-Head-Konfiguration« spricht man, wenn an eine Grafikkarte zwei Monitore angeschlossen sind. Es gibt auch Grafikkarten, die mehr Monitore ansteuern können, aber auf diesen Fall gehe ich hier nicht ein. Eine Variante der Dual-Head-Konfiguration ist der Anschluss eines Notebooks an einen Beamer oder an einen externen Monitor.

Im Regelfall verwenden Sie zur Konfiguration des Dual-Head-Betriebs die vorhin beschriebenen Module der Gnome- oder KDE-Systemeinstellungen. In den meisten Fällen gelingt die Konfiguration damit rasch und problemlos. Die weitere Lektüre

dieses Abschnitts lohnt sich nur, wenn dieser Normalweg versagt und Sie manuell in die Konfiguration eingreifen müssen.

Primären Bildschirm konfigurieren

Auf welchem Monitor soll das Systemmenü, das Panel oder das Dock erscheinen? Die Gnome-Systemeinstellungen bieten hierfür keine Option. Ad hoc schafft `xrandr` Abhilfe. Zuerst ermitteln Sie mit dem Kommando die Namen aller angeschlossenen Bildschirme, dann stellen Sie einen von ihnen als primären Bildschirm ein:

```
user$  xrandr --output HDMI1 --primary
```

Die Einstellung wird sofort wirksam, gilt aber nur bis zum nächsten Logout. Eine dauerhafte Konfiguration können Sie unter Gnome 3 in der Datei `.config/monitors.xml` vornehmen. Dort suchen Sie für jeden Monitor die Zeile `<primary>` und stellen die Option auf `yes` oder `no`. Die Einstellung wird mit dem nächsten Login wirksam.

Wesentlich unkomplizierter ist die Sache unter KDE sowie unter Ubuntu/Unity. Im KDE-Einstellungsmodul wählen Sie den Bildschirm für das Panel mit der Option HAUPTBILDSCHIRM. Unter Ubuntu werden das Panel und das Dock standardmäßig auf allen Monitoren angezeigt. Sie können aber im Systemeinstellungsmodul ANZEIGEGERÄTE im Listenfeld STARTERPOSITION einen primären Monitor auswählen.

Konfigurationsvarianten

X sieht grundsätzlich zwei verschiedene Konfigurationsvarianten für den Betrieb mit mehreren Bildschirmen vor:

- Die einfachste Variante besteht darin, die Konfiguration mit RandR durchzuführen. Dazu ist ein virtueller Bildschirm (`Screen`) erforderlich, der mindestens so groß ist, dass er beide Monitore abdeckt. Wenn Sie beispielsweise zwei Bildschirme mit 1280×1024 Pixel bzw. 1600×1200 Pixel besitzen und diese nebeneinander nutzen möchten, muss die virtuelle Auflösung 2880×1200 Pixel betragen. Sind diese Voraussetzungen erfüllt, können Sie mit `xrandr` oder anderen RandR-Konfigurationswerkzeugen den zweiten Bildschirm aktivieren. Das funktioniert mit den meisten gängigen Grafiktreibern.
- Die NVIDIA-spezifische Variante dieser Konfiguration heißt TwinView. Die Konfiguration erfolgt in `xorg.conf`, nicht durch RandR.

Dual-Head-Konfiguration mit RandR

Die Dual-Head-Konfiguration mit RandR setzt voraus, dass die virtuelle Auflösung groß genug ist, um beide Monitore abzudecken. Bei vielen Grafiktreibern ist das standardmäßig der Fall. Der Intel-Treiber sieht sogar eine maximale Größe von mehr als 32.000 * 32.000 Pixel vor!

```
user$  xrandr | grep Screen
Screen 0: minimum 320 x 320, current 3250 x 1200, maximum 32767 x 32767
```

Bei manchen Grafiktreibern ist die virtuelle Auflösung allerdings nur so groß wie die Auflösung des primären Monitors; bei Notebooks entspricht sie der Auflösung des eingebauten Bildschirms. In solchen Fällen ist es erforderlich, eine höhere virtuelle Auflösung fix einzustellen. Dazu bauen Sie die folgenden Einstellungen in `xorg.conf` ein. Soweit vorhanden, belassen Sie die `Identifier`-Angaben für `Screen` und `Device`. Achten Sie aber darauf, dass im `Screen`-Abschnitt auf das richtige `Device` verwiesen wird.

```
Section "Screen"
    Identifier  "Screen0"
    Device      "Device0"
    SubSection "Display"
        Virtual 2880 1200
    EndSubSection
EndSection
Section "Device"
    Identifier  "Device0"
EndSection
```

Nach einem Neustart von X können Sie die beiden Monitore mit `xrandr` einrichten:

```
user$  xrandr
Screen 0: minimum 320 x 200, current 1280 x 800, maximum 2880 x 1200
VGA disconnected (normal left inverted right x axis y axis)
LVDS connected 1280x800+0+0 (normal left inverted right x axis y axis)
   331mm x 207mm
   1280x800       59.9*+
HDMI-1 connected 1280x800+0+0 (normal left inverted right x axis y axis)
   519mm x 324mm
   1280x800       59.9*+
user$  xrandr --output HDMI-1 --mode 1600x1200 --right-of LVDS
```

Welche Möglichkeiten RandR bietet, geht aus dem folgenden Kommando hervor, das ich mit dem `nouveau`-Treiber und zwei Monitoren mit 1680×1050 (DVI) und 1600×1200 Pixel (VGA) getestet habe. Es definiert einen virtuellen Arbeitsbereich von 3864×2415 Pixel. Im kleineren Monitor wird der gesamte Arbeitsbereich verkleinert um den Faktor 2,3 angezeigt (3864 / 2,3 = 1680). Der größere Bildschirm zeigt einen Ausschnitt von 1600×1200 Pixel rund um die aktuelle Position des Mauszeigers im Maßstab 1:1. Neben der Maus sind zumindest 256 weitere Pixel zu sehen (es sei denn, die Maus ist am Rand des virtuellen Bildschirms). Wenn Sie schon immer wissen wollten, wie es wäre, mit einem Bildschirm von 3864×2415 Pixel zu arbeiten – jetzt können Sie es kostengünstig ausprobieren!

```
root#  xrandr -fb 3864x2415 --output DVI-I-0 --scale 2.3x2.3 \
              --output VGA-0 --pos 0x0 \
              --panning 3864x2415+0+0/3864x2415+0+0/256/256/256/256
```

xorg.conf

Natürlich können Sie die Multi-Head-Konfiguration auch fix in `xorg.conf` einrichten. Das Konfigurationsprinzip besteht darin, dass Sie die eingesetzten Monitore in `Monitor`-Abschnitten aufzählen. Beim zweiten Monitor geben Sie an, wie er relativ zum ersten positioniert ist. Die zulässigen Schlüsselwörter `RightOf`, `LeftOf`, `Below` etc. entsprechen den `xrandr`-Optionen. Bei Bedarf können Sie mit `Option "Position" "x y"` auch eine exakte Positionierung innerhalb des virtuellen `Screen` vornehmen. Im `Device`-Abschnitt geben Sie an, welche Signalausgänge `monitor-xxx` mit welchem Monitor verbunden sind.

Die folgende Konfiguration gilt für den `nouveau`-Treiber. Bei anderen Treibern müssen Sie die Zeichenketten `monitor-xxx` ändern, weil jeder Treiber eine andere Nomenklatur zur Bezeichnung der Signalausgänge verwendet. Führen Sie einfach `xrandr` aus, um herauszufinden, wie die Signalausgänge bei Ihrem System heißen! Auf eine explizite Einstellung der virtuellen Screen-Größe können Sie beim `nouveau`-Treiber verzichten, weil standardmäßig bis zu 4080×4096 Pixel zulässig sind.

```
# /etc/X11/xorg.conf
Section "Monitor"
        Identifier      "dvi0"
EndSection
Section "Monitor"
        Identifier      "vga0"
        Option          "RightOf" "dvi0"
EndSection
Section "Device"
        Identifier      "device0"
        Driver          "nouveau"
        Option          "monitor-VGA-0"    "vga0"
        Option          "monitor-DVI-I-0" "dvi0"
EndSection
```

Die Einstellungen in `xorg.conf` werden erst nach einem Neustart von X wirksam. Die Einstellungen werden aber ignoriert, wenn Sie mit Gnome- oder KDE-Werkzeugen die RandR-Konfiguration verändert haben. Löschen Sie gegebenenfalls `.config/monitors.xml` (Gnome) bzw. `.kde/share/config/krandrrc` (KDE)!

TwinView-Konfiguration mit einem Screen (NVIDIA)

Wenn Sie den `nvidia`-Grafiktreiber nutzen, ist die obige Vorgehensweise nicht möglich. Stattdessen müssen Sie den NVIDIA-spezifischen `TwinView`-Modus nutzen. Zur Konfiguration verwenden Sie am besten das Programm `nvidia-settings` (siehe Abbildung 24.3).

Die folgenden Zeilen zeigen die wichtigsten Abschnitte einer einfachen `TwinView`-Konfiguration. Dabei war ein TFT-Monitor mit 1920×1200 Pixel am DVI-Ausgang

der Grafikkarte angeschlossen, ein zweiter TFT-Monitor mit 1600×1200 Pixel am CRT-Ausgang. `TwinView` macht daraus eine virtuelle Auflösung von 3520×1200 Pixel.

Die Eckdaten der Monitore werden automatisch ermittelt. `TwinViewXineramaInfoOrder DFP` bewirkt, dass der DVI-Ausgang der Grafikkarte als Primärausgang gilt. Dank dieser Option erscheinen beispielsweise der X-Login sowie die KDE- und Gnome-Panels auf dem hier angeschlossenen Monitor. Bei Grafikkarten mit einem CRT-Ausgang betrachtet der NVIDIA-Treiber standardmäßig diesen Ausgang als Primärausgang, was nicht mehr zeitgemäß ist.

```
# /etc/X11/xorg.conf
Section "Device"
    Identifier     "Device0"
    Driver         "nvidia"
    VendorName     "NVIDIA Corporation"
    BoardName      "GeForce 7600 GS"
EndSection
Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    DefaultDepth    24
    Option         "TwinView" "1"
    Option         "TwinViewXineramaInfoOrder" "DFP"
    Option         "metamodes" "DFP: nvidia-auto-select +0+0, \
                                CRT: nvidia-auto-select +1920+0"
    SubSection     "Display"
        Depth       24
    EndSubSection
EndSection
```

Tipps zum Beamer-Anschluss

Jeder, der schon einmal mit seinem Notebook eine Präsentation halten musste, kennt den Nervenkitzel: Gelingt die Bildsynchronisation am Beamer? In den letzten Jahren hatte ich damit nie Probleme – die RandR-Konfiguration unter Gnome gelang jedes Mal auf Anhieb. In der ferneren Vergangenheit war es aber oft erforderlich, noch rasch ein paar Änderungen in `xorg.conf` einzubauen. Wenn es Probleme gibt, sollten Sie die folgenden Regeln beherzigen:

- Schließen Sie Ihr Notebook zuerst an den Beamer an, und schalten Sie es erst dann ein! In der Regel wird dadurch der interne Bildschirm des Notebooks deaktiviert und der externe Signalausgang aktiviert. Mit etwas Glück erscheinen bereits die Startmeldungen direkt auf dem Beamer. Gegebenenfalls stellen Sie dann unter KDE oder Gnome die für den Beamer optimale Auflösung ein.
- Bei manchen Notebooks können Sie den externen Signalausgang im BIOS oder EFI explizit aktivieren.

- Testen Sie den externen Ausgang Ihres Notebooks zu Hause an einem beliebigen Monitor. Zwar haben Sie keine Garantie dafür, dass sich der Beamer genauso wie Ihr Monitor verhalten wird, dennoch ist dieser Test ein erster Indikator für mögliche Probleme.
- Um das Beamer-Problem zu umgehen, können Sie in `xorg.conf` die Auflösung fix auf 1024×768 Punkte einstellen, die Zeilenfrequenz auf ca. 53 kHz und die Bildfrequenz auf ca. 60 Hz reduzieren. Das sind Daten, mit denen die meisten Beamer (auch ältere Modelle) zurechtkommen:

```
Section "Monitor"
    ...
    HorizSync    31.5 - 53
    VertRefresh  57-63
EndSection
Section "Screen"
    ...
    DefaultDepth     24
    SubSection "Display"
        Modes     "1024x768"
    EndSubSection
EndSection
```

24.8 3D-Grafik

Als typischer Linux-Anwender werden Sie sich vielleicht fragen: »Wozu brauche ich 3D-Grafik? Ich spiele keine Spiele und verwende keine 3D-Grafikprogramme.« Ganz so einfach ist es aber leider nicht: Alle modernen Desktop-Systeme, also Gnome, KDE und Unity, verwenden die 3D-Funktionen der Grafikkarte zum Verschieben von Fenstern sowie für alle möglichen visuellen Effekte. Ohne 3D-Grafikfunktionen können viele aktuelle Distributionen nicht mehr vernünftig genutzt werden.

Wenn Sie auf realer Hardware arbeiten und keine ganz neue Grafikkarte verwenden, gibt es zum Glück nur selten 3D-Treiberprobleme. Die Open-Source-Treiber `intel`, `nouveau` und `radeon` bieten mittlerweile gute 3D-Unterstützung. Anders sieht es leider oft in virtuellen Maschinen aus: Viele Virtualisierungssysteme können 3D-Funktionen gar nicht weitergeben, und selbst wenn dies vorgesehen ist, treten dabei in der Praxis oft Probleme auf.

Dieser Abschnitt gibt einen Überblick über die in Linux eingesetzten 3D-Technologien. Weitere Hintergrundinformationen zum Thema 3D-Grafik und Linux finden Sie auf der folgenden Seite:

http://www.mesa3d.org
http://dri.freedesktop.org/wiki

3D-Test

Mit dem Programm `glxinfo`, das sich je nach Distribution im Paket `mesa-utils`, `glx-utils` oder `Mesa-demo-x` versteckt, können Sie die 3D-Funktionen Ihres Systems überprüfen. Das Programm liefert eine Menge Detailinformationen über das laufende GLX-System, also über die OpenGL-3D-Erweiterungen des X Window Systems. Mit `grep` filtern Sie die entscheidenden Zeilen heraus. Das folgende Ergebnis bedeutet, dass der Intel-Grafiktreiber aktiv ist.

```
root#  glxinfo | grep render
direct rendering: Yes
OpenGL renderer string: Mesa DRI Intel(R) Sandybridge Desktop
```

Wenn dagegen kein 3D-beschleunigter Treiber läuft, sieht die Ausgabe wie in einem der drei folgenden Beispiele aus. Im ersten Beispiel stehen gar keine 3D-Funktionen zur Verfügung, im zweiten Fall werden sie per Software durch die Mesa-Bibliothek nachgebildet und im dritten Fall durch die `llvmpipe`-Bibliothek. Die seit 2012 gebräuchliche `llvmpipe`-Bibliothek erhöht zwar den Rechenaufwand der CPU beträchtlich, ermöglicht aber bei vielen Distributionen die Nutzung von 3D-Funktionen auch ohne einen richtigen 3D-Grafiktreiber.

```
root#  glxinfo | grep render
Xlib: extension "GLX" missing on display ":0.0"
root#  glxinfo | grep render
direct rendering: No
OpenGL renderer string: Mesa GLX Indirect
root#  glxinfo | grep render
direct rendering: Yes
OpenGL renderer string: Gallium 0.4 on llvmpipe (LLVM 3.3, 128 bits)
```

3D-Desktop-Funktionen

Mit »3D-Desktop-Funktionen« sind grafische Effekte gemeint, die das Öffnen, Schließen und Verschieben von Menüs und anderen Desktop-Elementen begleiten. Dreidimensional sehen diese Effekte heute zwar nur noch selten aus, das ändert aber nichts daran, dass zu ihrer Realisierung 3D-Funktionen der Grafikkarte verwendet werden.

Als 3D-Desktop-Funktionen 2006 erstmals verwendet wurden, sah das noch anders aus: Im Überschwang der technischen Möglichkeiten wurden Fenster beim Verschieben verzerrt, der Desktop beim Wechsel der Arbeitsfläche auf einen 3D-Würfel projiziert etc. Das sah lustig aus, lenkte aber ab und machte die Arbeit nicht produktiver. Deswegen sind in der Defaultkonfiguration heute dezentere Effekte üblich.

Compiz

Für die Realisierung der 3D-Effekte ist der Window Manager verantwortlich. In Gnome 2 und KDE 3 kam dazu das Programm Compiz zum Einsatz. Gnome 3 verwendet den 3D-fähigen Window Manager *Mutter* und ist nicht mehr auf Compiz angewiesen. Auch KDE 4 kommt ohne Compiz aus und realisiert die 3D-Effekte selbst. Ein Sonderfall ist aber Ubuntu, das zur Fensterverwaltung die Compiz-Erweiterung

Unity verwendet. Compiz ist somit nur noch für ältere Distributionen sowie unter Ubuntu von Bedeutung.

Compiz besteht im Wesentlichen aus zwei Programmen:

- `compiz` ist der eigentliche Window Manager. Er ist dafür verantwortlich, welches Fenster gerade sichtbar ist, welches Fenster den Eingabefokus hat, welche Effekte beim Erscheinen, Verschieben und Schließen der Fenster zum Einsatz kommen und welche Tastenkombinationen dabei gelten. Für die eigentlichen 3D-Effekte sind Plugins zuständig.
- `compiz-decorator` zeichnet rund um den eigentlichen Fensterinhalt die sogenannte Dekoration, zu der unter anderem die Titelleiste mit einigen Buttons zählt.

Compiz-Anwender können nahezu jeden einzelnen Effekt und die dazugehörenden Tastenkürzel mit dem Compiz Config Settings Manager (CCSM) einrichten (Paket `compizconfig-settings-manager`, siehe Abbildung 24.5). Die Bedienung dieses Programms ist allerdings wenig intuitiv.

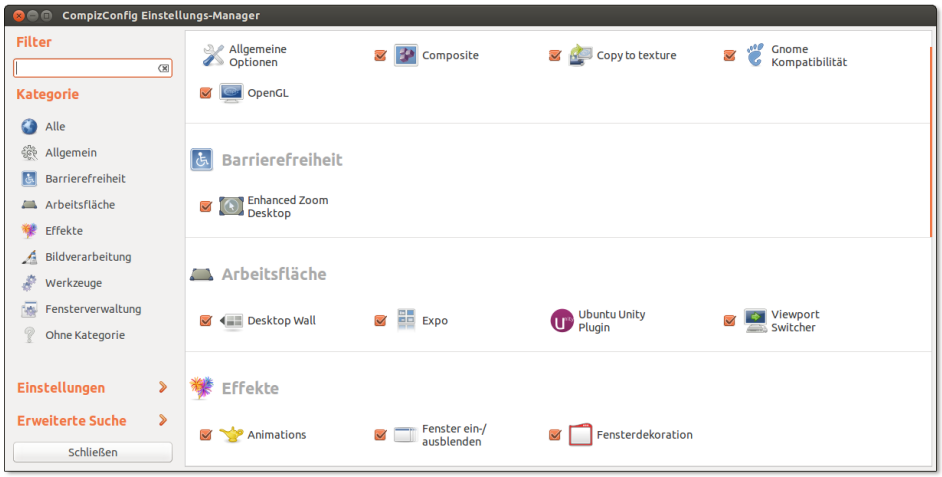


Abbildung 24.5 Compiz-Konfiguration für Fortgeschrittene

24.9 X im Netzwerk

Eine Besonderheit von X besteht darin, dass das gesamte Protokoll netzwerkfähig ist. Sie können sich also über eine Netzwerkverbindung auf einem beliebigen Rechner anmelden und ein grafisches Programm starten. Dieses Programm wird auf dem lokalen Rechner angezeigt und kann dort bedient werden, es läuft aber tatsächlich auf dem entfernten Rechner. Dieser Abschnitt stellt verschiedene Verfahren vor, diesen Mechanismus zu nutzen.

ssh Den einfachsten und sichersten Weg, auf einem entfernten Rechner zu arbeiten, bietet das in Abschnitt 18.2 vorgestellte Kommando `ssh`. Drei Voraussetzungen müssen erfüllt sein: Auf dem entfernten Rechner muss ein SSH-Server laufen, der SSH-Port 22 darf nicht durch eine Firewall blockiert sein, und Sie müssen beim Aufruf von `ssh` die Option `-X` verwenden, damit sich `ssh` um die korrekte Einstellung der `DISPLAY`-Variablen kümmert. Mit `ssh -X root@localhost` können Sie auch auf dem lokalen Rechner als `root` ein X-Programm ausführen.

VNC VNC steht für *Virtual Network Computing* und erlaubt einem anderen Benutzer, Ihren Desktop auf seinem Rechner darzustellen und zu steuern. Damit kann eine andere Person im Netzwerk die Kontrolle über die Benutzeroberfläche Ihres Rechners übernehmen. Die Funktion ist vor allem dann ausgesprochen praktisch, wenn ein Anwender ein Problem mit seinem Rechner hat und ein zweiter Anwender helfen möchte. VNC steht nicht nur unter X bzw. Linux, sondern auch für die meisten anderen Betriebssysteme zur Verfügung, inklusive Microsoft Windows.

Es gibt zahlreiche VNC-Implementierungen. Unter Linux am gebräuchlichsten sind Vinagre (Gnome) und TightVNC. Der gemeinsame Nenner vieler VNC-Programme ist das Protokoll RFB (Remote Frame Buffer). Damit sind die meisten VNC-Programme zumindest in den Grundfunktionen kompatibel zueinander. Über das RFB-Protokoll werden Tastatur- und Mauseingaben sowie Veränderungen am Bildschirminhalt übertragen.

VNC ist ein Client/Server-Protokoll. Damit VNC funktioniert, muss auf einem Rechner ein VNC-Server laufen. Der zweite Rechner startet einen VNC-Client (beispielsweise `vncviewer`, `vinagre` oder `krdc`) und stellt damit die Verbindung zum Server her. Im Fenster des VNC-Clients wird dann der Desktop des Servers dargestellt.

Standardmäßig erfolgt die Datenübertragung zwischen Client und Server über die TCP/IP-Ports 5900 bis 5906. VNC-Clients auf Java-Basis, die in einem Webbrowser ausgeführt werden, nutzen in der Regel die Ports 5800 bis 5806. Diese Ports dürfen nicht durch eine Firewall blockiert werden! Beachten Sie auch, dass Fernwartung nur gelingen kann, wenn sich beide Rechner im selben lokalen Netzwerk befinden oder öffentliche IP-Adressen haben. Pech haben Sie, wenn sich einer oder beide Rechner in unterschiedlichen privaten Netzwerken befinden, wie sie beispielsweise von jedem ADSL-Router und vielen WLAN-Routern gebildet werden.

Beim Start des VNC-Clients übergeben Sie den Netzwerknamen bzw. die Netzwerkadresse des Rechners, auf dem der VNC-Server läuft. Außerdem müssen Sie entweder die Display-Nummer (:*n*) oder die Port-Nummer (::*nnnn*) angeben.

```
user$  vncviewer 192.168.0.17:0        (X-Screen 0 anzeigen)
user$  vncviewer 192.168.0.17::5901    (Port 5901 verwenden)
```

VNC mit SSH-Verschlüsselung

VNC an sich ist nicht sicher, die Übertragung der Daten erfolgt unverschlüsselt. Wenn Sie Wert auf mehr Sicherheit legen, müssen Sie den VNC-Datenstrom über einen verschlüsselten Tunnel leiten oder VNC-Implementierungen mit integrierter Verschlüsselung nutzen. Wie Sie VNC über einen SSH-Tunnel leiten, ist hier beschrieben:

http://linuxwiki.de/VNC

VNC in Gnome und KDE

Gnome und KDE bieten jeweils komfortable Benutzerschnittstellen zu VNC, die allerdings bei manchen Distributionen extra installiert werden müssen. Unter Gnome 3.*n* starten Sie die Fernwartung als Hilfesuchender mit dem Programm *Freigabe der Arbeitsfläche* (Programmname `vino-preferences`, Paket `vino`, siehe Abbildung 24.6). Der VNC-Server wird durch die Bibliothek `vino-server` realisiert und nutzt standardmäßig Port 5900. Der Helfer kann einen beliebigen VNC-Client einsetzen, beispielsweise `vinagre`.

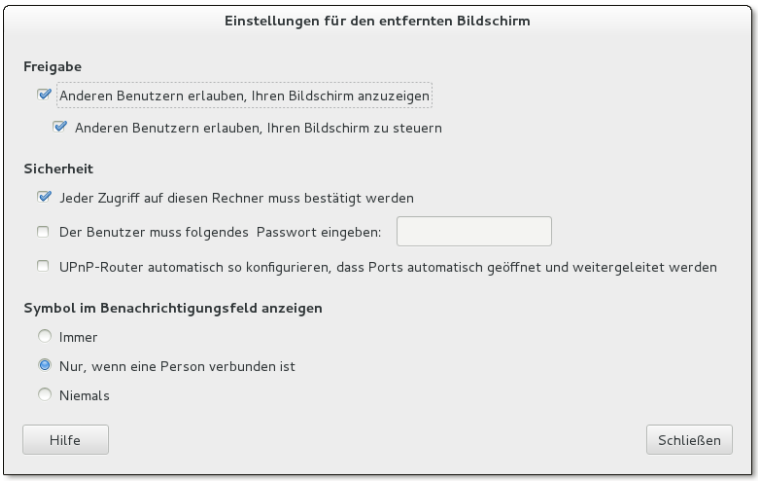


Abbildung 24.6 VNC-Freigabe unter Gnome einrichten

Unter KDE starten Sie eine VNC-Verbindung mit ANWENDUNGEN • SYSTEM • VERBINDUNG ZU FREMDRECHNER • ARBEITSFLÄCHE FREIGEBEN bzw. dem Programm `krfb`. Der Helfer kann einen beliebigen VNC-Client oder das KDE-Programm `krdc` einsetzen.

TeamViewer

VNC und alle darauf basierenden Programme leiden unter einer wesentlichen Einschränkung: Die Fernwartung funktioniert nur in lokalen Netzwerken gut. Via Internet gibt es aber oft Probleme: Bei Privatanwendern erfolgt die Internetverbindung über einen Router bzw. mittels NAT (Network Address Translation). Das führt dazu, dass der Rechner keine öffentliche IP-Adresse hat, sondern eine IP-Adresse in einem privaten IP-Adressraum. Eine Fernwartung via VNC ist dann leider unmöglich.

Abhilfe schaffen in solchen Fällen kommerzielle Werkzeuge, die andere Kommunikationsmechanismen verwenden. Das populärste derartige Programm ist TeamViewer, das auch für Linux zur Verfügung steht. Die private Nutzung ist kostenlos.

http://teamviewer.com

24.10 Schriftarten (Fonts)

X unterscheidet zwischen skalierbaren und nichtskalierbaren Schriften. Seit X moderne, skalierbare Fonts nutzen kann, also TrueType, Type-1 und OpenType, spielen nicht skalierbare Schriften im X-Alltag keine Rolle mehr.

fc-list und xlsfonts

Die historische Differenzierung zwischen skalierbaren und nichtskalierbaren Fonts spiegelt sich aber noch immer in der Doppelgleisigkeit vieler Verwaltungskommandos wider. Beispielsweise liefert das Kommando `fc-list | sort` eine Liste aller skalierbaren Fonts. Dieselbe Funktion erfüllt `xlsfonts` für nichtskalierbare Fonts. Mit dem Programm `xfontsel` können Sie gezielt nach nichtskalierbaren Fonts suchen.

Font-Verzeichnisse

Allgemein verfügbare Font-Dateien befinden sich üblicherweise in den Verzeichnissen `/etc/X11/fonts` oder `/usr/share/fonts`. Bei nichtskalierbaren Fonts gibt es für jede Größe eine eigene Datei. Bei skalierbaren Fonts reicht eine Datei für alle Größen aus.

Darüber hinaus ist es möglich, im Verzeichnis `.fonts` persönliche Schriften zu installieren. Dazu ist es ausreichend, die Font-Dateien dorthin zu kopieren.

fontconfig-Bibliothek

Um die Verwaltung der skalierbaren Fonts kümmert sich das `fontconfig`-System. Für die Integration von X und `fontconfig` ist die `Xft`-Bibliothek zuständig. Für die Konfiguration des `fontconfig`-Systems ist die Datei `/etc/fonts/fonts.conf` verantwortlich.

xorg.conf

Falls Sie Fonts außerhalb der dem X-Server bekannten Verzeichnisse installieren möchten, müssen Sie diese Verzeichnisse im `Files`-Abschnitt in `xorg.conf` angeben:

```
# in /etc/X11/xorg.conf
Section "Files"
  FontPath     "/usr/share/fonts/myown"
  ...
EndSection
```

Damit Änderungen an der Font-Konfiguration wirksam werden, reicht zumeist das folgende Kommando aus. Wenn das nichts hilft, müssen Sie sich neu einloggen oder X neu starten.

```
root#  xset fp rehash
```

gucharmap

Das Gnome-Programm `gucharmap` zeigt alle Zeichen eines skalierbaren Fonts an und ermöglicht es, einzelne Sonderzeichen in die Zwischenablage zu kopieren.

Installation zusätzlicher Schriften

Bei Linux-Distributionen können nur »freie« Schriften mitgeliefert werden. Dieser Abschnitt gibt einige Tipps zur Installation eigener Fonts. Grundsätzlich sind hierfür zwei Schritte erforderlich:

- Die Font-Dateien müssen in ein dafür vorgesehenes Verzeichnis kopiert werden. Die infrage kommenden Verzeichnisse sind in `xorg.conf` aufgezählt bzw. werden in `/var/log/Xorg.0.log` angegeben. Außerdem ist `.fonts` ein geeigneter Installationsort.
- Die interne Fonts-Verwaltung muss aktualisiert werden. Dazu führen Sie im Font-Verzeichnis das Kommando `fc-cache` aus. Es erzeugt die `fonts.cache`-Dateien, die für das `fontconfig`-System und die Xft-Bibliothek erforderlich sind.

KDE

KDE zeigt im Systemeinstellungsmodul SCHRIFTARTEN-VERWALTUNG alle verfügbaren Fonts an. Mit diesem Modul können Sie auch eigene Schriften in das Verzeichnis `.fonts` installieren.

Microsoft-Internet-Fonts

Microsoft bot einige Zeit lang TrueType-Fonts zum Download an (Andale Mono, Arial, Comic Sans etc.). Die Fonts sollten es allen Anwendern ermöglichen, Webseiten, in denen Microsoft-Fonts eingesetzt werden, in optimaler Qualität zu betrachten. Die ursprüngliche Download-Website gibt es zwar nicht mehr, die Fonts können nun aber von der unten angegebenen `corefonts`-Website heruntergeladen werden. Die Fonts dürfen kostenlos genutzt werden, die kommerzielle Weitergabe ist aber untersagt! Daher werden die Fonts bei kommerziellen Distributionen nicht mitgeliefert.

Leider ist die Installation der Fonts unter Linux umständlich, weil die Fonts in `*.exe`-Dateien verpackt sind und nicht in einer anderen Form weitergegeben werden dürfen. Eine ausführliche Installationsanleitung für Distributionen mit RPM-Paketen finden Sie hier:

http://corefonts.sourceforge.net

Je nach Distribution gibt es Scripts, die beim Download und der Installation der Schriften helfen:

- Debian, Ubuntu: Das Paket `msttcorefonts` enthält das Script `update-ms-fonts`. Es installiert die Fonts in das Verzeichnis `/usr/share/fonts/truetype/msttcorefonts`.
- SUSE: Das Paket `fetchmsttfonts` enthält ein Script zum Download der Schriften. Sie finden die Font-Dateien anschließend im Verzeichnis `/usr/share/fonts/truetype`.

Anti-Aliasing

X verwendet standardmäßig Anti-Aliasing (kurz AA) bzw. Hinting, um TrueType- und Type-1-Fonts möglichst glatt anzuzeigen. Die Anti-Aliasing- und Sub-Pixel-Rendering-Funktionen werden durch die XML-Dateien `/etc/fonts/fonts.conf` und `/etc/fonts/conf.d/*.conf` gesteuert.

Unter KDE können Sie die Schriftdarstellung im Systemeinstellungsmodul Erscheinungsbild von Anwendungen konfigurieren. Gnome 3 enthält leider keine vergleichbare Konfigurationsmöglichkeit mehr; mit dem inoffiziellen Gnome Tweak Tool können Sie aber grundlegende Schrifteinstellungen verändern (siehe Abbildung 24.7).

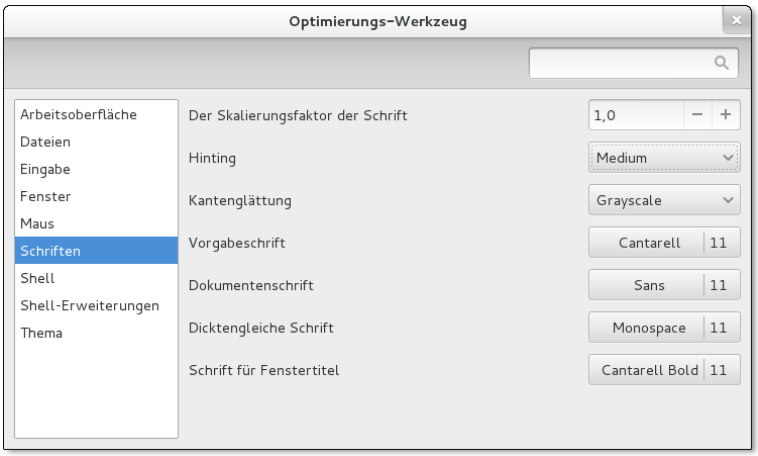


Abbildung 24.7 Font-Einstellungen mit dem Gnome Tweak Tool

DPI-Einstellung

DPI steht für *Dots per Inch* und gibt die Bildschirmauflösung an. Dazu gleich ein Beispiel: Wenn Ihre genutzte Bildschirmbreite 29 cm und die horizontale Auflösung 1280 Pixel beträgt, dann werden pro Zoll ca. 112 Pixel dargestellt (1280 / 36 × 2,54).

Welche Rolle spielt nun der DPI-Wert? Damit Text am Bildschirm unabhängig von der Bildschirmgröße und der Grafikauflösung gut gelesen werden kann, sollten je nach DPI-Wert unterschiedlich große Schriftarten verwendet werden. Dazu muss X wissen, wie groß der Monitor ist. Moderne Monitore übermitteln diese Information via DDC (Display Data Channel) an X. Sollte das nicht funktionieren, geben Sie diese Information (in mm) mit dem Schlüsselwort `DisplaySize` im `Monitor`-Abschnitt an:

```
Section "Monitor"
  ...
  DisplaySize 400 300
EndSection
```

Alternativ können Sie in den Dialogen zur Schriftkonfiguration von KDE oder Gnome einen beliebigen DPI-Wert explizit einstellen oder `xrandr --dpi n` ausführen. Sollte das nicht möglich sein, hilft auch die folgende Zeile in der Datei `.Xresources`:

```
Xft.dpi: 96
```

Den aktuellen DPI-Wert stellen Sie mit `xdpyinfo` fest. Das folgende Ergebnis gilt für einen 20-Zoll-Monitor:

```
root#  xdpyinfo | grep -C 1 dimensions
screen #0:
  dimensions:    1600x1200 pixels (411x311 millimeters)
  resolution:    99x98 dots per inch
```

24.11 Mir und Wayland

Die meisten Linux-Grafikexperten sind sich einig: Das X Window System ist keine zeitgemäße Basis mehr für ein modernes Betriebssytem. Deswegen hat schon vor Jahren die Entwicklung von Wayland begonnen, einem neuen Display Server für Linux. Im März 2013 verkündete dann Canonical, dass man mit Mir an einem alternativen Projekt arbeite, das im Wesentlichen dieselben Vorzüge wie Wayland bieten würde, darüber hinaus aber auch geeignet für Smartphones und Tablets sei. Canonical ist es damit einmal mehr gelungen, große Teile der Open-Source-Community zu verprellen. Viele KDE- und Gnome-Entwickler stellten sich nach der Mir-Ankündigung demonstrativ hinter das Wayland-Projekt.

Der Erfolg eines neuen Grafiksystems für Linux wird stark davon abhängen, ob es geeignete Treiber gibt. Während die Open-Source-Treiber relativ leicht angepasst werden können, ist die Linux-Gemeinschaft bei den proprietären Treibern auf das Wohlwollen von NVIDIA bzw. AMD angewiesen. Im Sommer 2013 war unklar, ob diese Firmen überhaupt willens sind, neue Treiber zu entwickeln, und wenn ja, für welches der beiden konkurrierenden Systeme. Es ist nicht auszuschließen, dass Canonical hier die besseren Karten hat.

Dieser kurze Abschnitt fasst einige Impressionen zu Mir und Wayland zusammen. Beachten Sie aber, dass ich die Arbeiten an diesem Buch im Sommer 2013 abgeschlossen habe. Zu diesem Zeitpunkt waren weder Mir noch Wayland praxistauglich. Bis dieses Buch erschienen sein wird, gibt es im Internet und in Zeitschriften sicher schon mehr Informationen und technische Details, wann und wie einzelne Distributionen den Umstieg auf Mir oder Wayland angehen werden.

Mir und XMir

Zeitplan

Canonical plante, Ubuntu 13.10 standardmäßig mit Mir auszuliefern. Auf Mir aufbauend sollte XMir die herkömmlichen Funktionen des X Window System zur Verfügung stellen. Allerdings stellte sich Anfang Oktober heraus, dass XMir nicht ausreichend stabil war. Mir und XMir stehen deswegen in Ubuntu 13.10 als optionale Pakete zur Verfügung, werden aber nicht automatisch installiert.

Mir funktioniert momentan nur mit den Open-Source-Treibern `intel`, `nouveau` und `radeon`. Für Systeme, auf denen keiner dieser drei Treiber läuft, gibt es einen Fallback-Modus mit dem traditionellen X Window System.

Unity und alle anderen Komponenten der Ubuntu-Benutzeroberfläche bleiben ganz gewöhnliche X-Programme. Aus Anwendersicht ändert der Umstieg auf Mir/XMir vorerst nichts – es sei denn, es treten Kompatibilitätsprobleme auf. Aufgrund der XMir-Zwischenschicht sind keinerlei Geschwindigkeitsverbesserungen zu erwarten.

Canonical hofft, dass NVIDIA und AMD bis zur Fertigstellung von Ubuntu 14.04 eigene Treiber für Mir zur Verfügung stellen können. In Ubuntu 14.04 sollen dann immer Mir zum Einsatz kommen. Einen Fallback-Modus soll es dann nicht mehr geben. Aber auch in Ubuntu 14.04 ist zusätzlich XMir erforderlich: Unity und alle anderen Programme sind weiterhin reine X-Programme.

Die Vorzüge von Mir werden voraussichtlich erst Ubuntu 14.10 spürbar: Dann soll das direkt auf Mir basierende Unity 8 fertig sein. Außerdem soll es dann Mir-kompatible Versionen der GTK- und QT-Bibliotheken geben, sodass aus vielen X-Programmen echte Mir-Programme werden.

Testbetrieb

Mir und XMir ließen sich bereits im Sommer 2013 ausprobieren. Auf meinem Rechner mit Intel-Grafiksystem funktionierte das einigermaßen gut und ohne Abstürze. Aufgrund der XMir-Zwischenschicht bot Mir zu diesem Zeitpunkt allerdings keinerlei Vorteile im Vergleich zu einem gewöhnlichen X-System, besaß dafür jedoch dafür etliche Einschränkungen bzw. Probleme:

- Der Mauszeiger erschien doppelt und an unterschiedlichen Positionen. Der »richtige« Mauszeiger ist weiß, der falsche schwarz.
- Der Wechsel in Textkonsolen mit Strg+Alt+Fn funktionierte nicht mehr.
- Die Konfiguration mehrerer Monitore war unmöglich.

Dass Mir und XMir tatsächlich laufen, sehen Sie nicht nur am fehlerhaften Mauszeiger; es geht auch aus der Prozessliste und den Logging-Dateien hervor:

```
user$  ps ax | grep compositor
... /usr/sbin/unity-system-compositor --from-dm-fd 9 --to-dm-fd 13 --vt 7
user$  grep -i mir /var/log/Xorg.0.log
```

```
xorg-server 2:1.13.3+xmir1-0
(II) LoadModule: "xmir"
(II) Loading /usr/lib/xorg/modules/extensions/libxmir.so
(II) Module xmir: vendor="X.Org Foundation"
...
```

Der Display Manager `lightdm` ist dafür verantwortlich, dass Mir und nicht das herkömmliche X Window System startet. Seine Konfigurationsdateien müssen im Abschnitt `[SeatDefault]` die Einstellung `type=unity` enthalten. Wenn Sie diese Einstellung auskommentieren, startet `lightdm` das herkömmliche X Window System.

```
user$  cat /etc/lightdm/lightdm.conf.d/10-unity-system-compositor.conf
[SeatDefaults]
type=unity
```

Links

Viele Details zu Mir und XMir können Sie auf der Mir-Website und in der *ubuntu-devel*-Liste nachlesen:

https://wiki.ubuntu.com/Mir
https://lists.ubuntu.com/archives/ubuntu-devel/2013-June/037401.html

Wayland

Wayland soll wie Mir ein neues Grafikfundament für Linux werden. Damit Anwendungsprogramme von Wayland profitieren können, müssen Sie Wayland-kompatible Bibliotheken einsetzen. Bei der vom Gnome-Projekt verwendeten GTK-Bibliothek sind die Portierungsarbeiten schon relativ weit fortgeschritten. Es ist zu erwarten, dass es spätestens 2014 möglich sein wird, Gnome-Programme nativ in Wayland auszuführen. Bis dahin ist die Zwischenschicht XWayland erforderlich, die die Kompatibilität zum alten X Window System herstellt.

Weston Compositor

Wayland war im Sommer 2013 ebenso wenig praxistauglich wie Mir, in Fedora 19 waren aber erste Tests schon möglich. Das Programm `weston` führt innerhalb eines ganz gewöhnlichen Fensters den Weston Compositor aus, eine Wayland-Referenzimplementierung (siehe Abbildung 24.8). In der Testumgebung können dann mehrere Terminalfenster geöffnet werden. Dabei handelt es sich um das speziell für Wayland kompilierte Programm `weston-terminal`.

```
root#  yum install weston
user$  weston
```

Innerhalb des Weston-Terminals können Sie die Wayland-kompatible GTK-Bibliothek aktivieren und dann ausgewählte Gnome-Programme als Wayland-Programme starten, z. B. GEdit. Hier zeigt sich dann aber, wie unfertig die Wayland-Implementierung der GTK-Bibliothek gegenwärtig ist: Der Texteditor reagiert weder auf

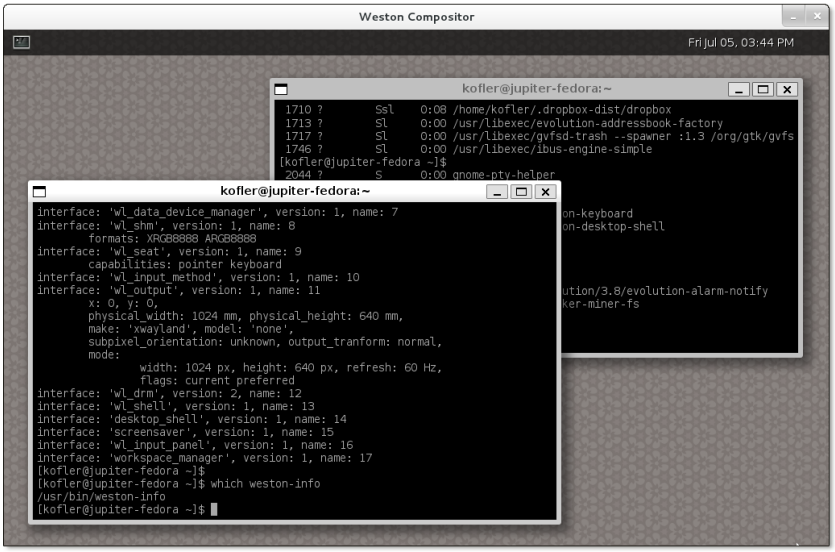


Abbildung 24.8 Wayland-Test in einem Fenster mit dem Weston Compositor

Mausklicks noch auf Tastatureingaben. Außerdem fehlt dem Programm eine Fensterleiste, mit der es verschoben oder minimiert werden könnte.

```
user$  export GDK_BACKEND=wayland
user$  gedit
```

Sofern Sie X vorher beenden, können Sie `weston` als `root` auch aus einer Textkonsole heraus starten. Weston läuft dann im Vollbildmodus. Aber was nützt das, wenn es außer `weston-terminal` kein weiteres Programm gibt, das vernünftig läuft?

Links Ausführliche Informationen über die Hintergründe des Wayland-Projekts können Sie auf der Projektseite nachlesen:

http://wayland.freedesktop.org

Kapitel 25
Administration des Dateisystems

Dieses Kapitel beschreibt verschiedene Facetten der Administration des Dateisystems. Das Kapitel richtet sich an fortgeschrittene Linux-Anwender und geht auf die folgenden Themen ein:

- **Wie alles zusammenhängt:** Dieser Abschnitt gibt einen ersten Überblick darüber, wie verschiedene Aspekte des Linux-Dateisystems zusammenhängen.
- **Device-Namen:** Linux-intern werden Festplatten und andere Datenträger sowie deren Partitionen über Device-Dateien wie `/dev/sdc3` angesprochen. Dieser Abschnitt fasst das Schema für die Nomenklatur und Nummerierung zusammen.
- **Partitionierung der Festplatte:** Die Partitionierung der Festplatte ist ein zentraler Bestandteil der Installation von Linux. Manchmal ist es aber auch im Betrieb von Linux erforderlich, eine neue Partition hinzuzufügen. Je nachdem, welche Partitionierungsart für die Festplatte gilt (MBR oder GPT) müssen unterschiedliche Werkzeuge zur Veränderung der Partitionierung verwendet werden.
- **Dateisystemtypen:** Wenige Betriebssysteme unterstützen so viele Dateisystemtypen wie Linux. Dieser Abschnitt fasst die wichtigsten Varianten zusammen.
- **Verwaltung des Dateisystems:** Hier erfahren Sie, wie einzelne Datenpartitionen manuell in das Dateisystem eingefügt werden (`mount`) und wie dieser Vorgang automatisiert wird (`/etc/fstab`).
- **Linux- und Windows-Dateisysteme:** Mehrere Abschnitte geben Tipps und Hinweise zur Nutzung der Dateisysteme `ext3`, `ext4`, `btrfs`, `xfs`, `vfat` und `ntfs`.
- **CDs/DVDs:** Für Daten-CDs und Daten-DVDs gibt es ebenfalls eigene Dateisystemtypen, die in diesem Abschnitt kurz vorgestellt werden.
- **Externe Datenträger (USB, Firewire):** Wenn Sie eine Firewire-Festplatte oder einen USB-Memorystick anschließen, erscheint zumeist automatisch ein Fenster des Dateimanagers und gibt Ihnen Zugriff auf die Daten. Dieser Abschnitt erklärt, was hinter den Kulissen passiert und wie Sie externe Datenträger bei Bedarf auch manuell nutzen.

- **Swap-Partitionen:** Wenn Linux zur Ausführung der Programme zu wenig Arbeitsspeicher hat, lagert es Teile des Speichers in sogenannte Swap-Partitionen aus.
- **RAID:** Mit RAID (*Redundant Array of Inexpensive/Independent Disks*) verknüpfen Sie die Partitionen mehrerer Festplatten miteinander, um auf diese Weise ein zuverlässigeres und/oder schnelleres Gesamtsystem zu erreichen. Dieser Abschnitt geht kurz auf die Grundlagen von RAID ein und beschreibt dann die Einrichtung eines RAID-0-Systems (Striping).
- **LVM:** Der *Logical Volume Manager* (kurz LVM) ermöglicht eine flexiblere Verwaltung von Partitionen. Mit LVM können Sie beispielsweise Partitionen mehrerer Festplatten zu einer virtuellen Partition vereinen, die Größe von Partitionen im laufenden Betrieb ändern etc.
- **SMART:** Die *Self-Monitoring Analysis and Reporting Technology* (SMART) ermöglicht es, während des Betriebs von Festplatten statistische Daten zu erfassen und auf diese Weise drohende Zuverlässigkeitsprobleme schon zu erkennen, bevor es zu Datenverlusten kommt.
- **SSD-TRIM:** Mit dem TRIM-Befehl, den alle aktuellen Solid State Disks unterstützen, kann das Betriebssystem der SSD mitteilen, welche Speicherblöcke des Dateisystems nach dem Löschen einer Datei ungenutzt sind. Die SSD kann dann die interne Nutzung der Speicherzellen optimieren.
- **Verschlüsselte Dateisysteme:** Wenn Sie vermeiden möchten, dass unbefugte Personen – etwa nach einem Rechnerdiebstahl – Ihre Daten lesen können, müssen Sie Ihre Dateien bzw. Dateisysteme verschlüsseln. Linux stellt hierfür unterschiedliche Verfahren zur Auswahl, wobei das populärste Verfahren momentan auf dem `dm_crypt`-Kernelmodul basiert.

Auch über die Administration von Dateisystemen ließe sich natürlich noch mehr sagen bzw. schreiben. So viel Platz ist hier aber nicht. Stattdessen müssen hier einige Querverweise genügen:

- **Nutzung des Dateisystems:** Kommandos zum Kopieren von Dateien oder zum Erstellen von Backups, Hintergründe zu den Zugriffsrechten von Dateien etc. wurden in diesem Buch bereits in Kapitel 15 vorgestellt.
- **Netzwerk-Dateisysteme:** Linux gibt Ihnen die Möglichkeit, Verzeichnisse anderer Rechner in Ihren Verzeichnisbaum zu integrieren. Ich gehe in diesem Buch auf die Dateisysteme SSHFS (siehe Abschnitt 18.2), CIFS (Windows/Samba, siehe Abschnitt 31.7) und NFS (siehe Abschnitt 32.1) ein.

- **Disk-Quotas:** Dabei handelt es sich um ein System, das steuert, wie viel Platz einzelne Benutzer auf der Festplatte beanspruchen dürfen. Wird die Grenze überschritten, können keine neuen Dateien mehr angelegt werden. Eine gute Einführung finden Sie unter:

  http://www.tldp.org/HOWTO/Quota.html

- **Cluster-Dateisysteme:** Cluster-Dateisysteme bzw. globale Dateisysteme verbinden Daten mehrerer Rechner zu einem virtuellen Dateisystem. Damit lassen sich riesige Datenspeicher bilden und von mehreren Rechnern parallel nutzen.

  Abermals bietet Linux gleich mehrere Verfahren, um derartige Dateisysteme zusammenzustellen, z. B. mit dem OCFS (*Oracle Cluster Filesystem*), mit GFS (*Global Filesystem*) oder mit Ceph:

  http://oss.oracle.com/projects/ocfs2
  http://sourceware.org/cluster/gfs
  http://ceph.com

25.1 Wie alles zusammenhängt

Die Zusammenhänge bei der Verwaltung des Dateisystems sind bisweilen verwirrend. Dieser Abschnitt versucht, die wichtigsten Zusammenhänge kurz und übersichtlich darzustellen. Um den Text möglichst übersichtlich zu halten, beschränke ich mich hier auf eingebaute Festplatten und gewöhnliche Linux-Dateisysteme. CD- und DVD-Laufwerke, externe Datenträger, LVM- und RAID-Systeme etc. bleiben außen vor.

Festplatten und SSDs

Den eingebauten Festplatten und SSDs sind unter Linux Device-Dateien zugeordnet. Neuere Distributionen verwenden `/dev/sda`, `/dev/sdb` etc. für sämtliche Festplatten. Ganz alte Distributionen verwenden `/dev/hda`, `/deb/hdb` etc. für IDE-Festplatten und `/dev/sda`, `/dev/sdb` etc. nur für SATA- und SCSI-Festplatten. Generell schreibe ich in diesem Buch zumeist einfach von »Festplatten«; damit meine ich gleichermaßen herkömmliche Festplatten und moderne Solid State Disks.

Partitionen

Um auf einer Festplatte mehrere, voneinander unabhängige Dateisysteme unterzubringen, muss diese in Abschnitte (Partitionen) unterteilt werden. Auch den Partitionen sind Device-Dateien zugeordnet, beispielsweise `/dev/sda1` für die erste Partition der ersten Festplatte. Im Detail ist die Device-Nomenklatur für Partitionen im nächsten Abschnitt zusammengefasst.

Systempartition

Beim Start von Linux greift der Kernel als Erstes auf die Systempartition (root-Partition) zu. Deren Device-Name oder die UUID (Universal Unique Identifier) des darauf enthaltenen Dateisystems wird in einem Kernelparameter in der GRUB-Konfigurationsdatei angegeben.

Weitere Partitionen

Neben der Systempartition, die unbedingt erforderlich ist, kann es weitere Partitionen geben, die bereits beim Start von Linux berücksichtigt werden sollen. Diese Dateien sind in der Datei `/etc/fstab` verzeichnet. Diese Datei muss sich wiederum in der Systempartition befinden. Sie wird im Rahmen des Init-Prozesses ausgewertet.

Konsistenztest

Beim Einbinden von Partitionen in den Verzeichnisbaum wird automatisch die Konsistenz der Dateisysteme überprüft. Ist der Rechner zuletzt abgestürzt bzw. wurde er wegen eines Stromausfalls nicht ordnungsgemäß heruntergefahren, kommt es zu einer automatischen Reparatur des Dateisystems oder anderen Sicherheitsmaßnahmen, die weitere Konsistenzfehler oder -schäden verhindern sollen. Ein entsprechender Konsistenztest wird aber auch automatisch nach einer bestimmten Nutzungsdauer durchgeführt. Im Detail ist dieser Vorgang wiederum von der Distribution und der individuellen Konfiguration abhängig.

Verzeichnisbaum statt Laufwerksbuchstaben

Während es unter Windows üblich ist, getrennte Dateisysteme über Laufwerksbuchstaben anzusprechen (A:, C:, D: etc.), werden in Linux sämtliche Dateisysteme in einem Verzeichnisbaum zusammengefasst. Der Zugriff auf die Systempartition erfolgt über das Wurzelverzeichnis `/`. Der Startpunkt aller anderen Dateisysteme kann je nach Distribution und Konfiguration variieren. Üblich sind aber `/mnt`- oder `/media`-Unterverzeichnisse, beispielsweise `/media/dvd` für eine Daten-DVD. Neue Distributionen verwenden das Verzeichnis `/run/media/`*`benutzername/dvdname`*.

Dateisysteme hinzufügen

Es ist möglich, im laufenden Betrieb weitere Dateisysteme in den Verzeichnisbaum einzubinden bzw. wieder aus im zu lösen. Beim Anstecken eines externen Datenträgers (z. B. eines USB-Sticks) erfolgt das zumeist automatisch. Wenn dieser Automatismus nicht funktioniert bzw. wenn er bewusst deaktiviert wurde, kann `root` mit den Kommandos `mount` und `umount` Dateisysteme auch manuell einbinden bzw. lösen. Die einzige Konstante ist die Systempartition: Sie kann während des Betriebs nicht aus dem Dateisystem gelöst werden. Das ist erst beim Herunterfahren des Rechners möglich.

Dateisystemtypen

Linux unterstützt sehr viele Dateisystemtypen. Die Systempartition muss in einem Linux-Dateisystem vorliegen (z. B. `ext3`, `ext4`, `btrfs` oder `xfs`). Bei den restlichen Partitionen ist die Auswahl noch größer. Infrage kommen beispielsweise auch Windows-, Unix- oder Apple-Dateisysteme.

25.2 Device-Namen für Festplatten und andere Datenträger

IDE, SATA und SCSI sind die zurzeit üblichen Standards, um einen Computer mit seinen Laufwerken zu verbinden. Tabelle 25.1 fasst die Bedeutung dieser und einiger weiterer Abkürzungen zusammen.

Abkürzung	Bedeutung
ATA	Advanced Technology Attachment (Schnittstelle zum Anschluss von Festplatten)
ATAPI	ATA Packet Interface (ATA-Erweiterung für CD- und DVD-Laufwerke)
IDE	Integrated Device Electronics (alternative Bezeichnung für PATA)
PATA	Parallel ATA (alte ATA-Schnittstelle mit paralleler Datenübertragung)
SATA	Serial ATA (neue ATA-Schnittstelle mit serieller Datenübertragung)
SCSI	Small Computer System Interface (Alternative zu IDE/SATA)

Tabelle 25.1 Glossar

Kernelinterna

Linux-intern erfolgt der Zugriff auf interne und externe Festplatten und deren Partitionen, auf CD- und DVD-Laufwerke sowie auf andere Datenträger über Device-Dateien. Das sind besondere Dateien, die als Schnittstelle zwischen Linux und der Hardware dienen.

Diese Device-Dateien benötigen Sie nur zu Verwaltungszwecken, d. h., wenn Sie die Partitionierung einer Festplatte ändern oder eine bestimmte Partition in das Dateisystem einbinden möchten. Im normalen Betrieb greifen Sie auf das gesamte Dateisystem über Verzeichnisse zu. Dabei bezeichnet `/` den Start des Dateisystems. Einzelne Partitionen können darin an beliebigen Orten eingebunden werden – eine zusätzliche Linux-Partition etwa unter dem Namen `/data`, eine Windows-Partition beispielsweise unter dem Namen `/media/win`.

Im Kernel gibt es zwei grundlegende Treiberfamilien für Festplatten und andere Datenträger:

- **IDE:** Der IDE-Treiber ist heute nur noch für ganz alte IDE-Festplatten und IDE-DVD/CD-Laufwerke zuständig. Der IDE-Code im Kernel wird nicht mehr gewartet.
- **SCSI:** Über das SCSI-System werden nicht nur alle SCSI-Geräte verwaltet, sondern auch alle Laufwerke, die an die Bussysteme SATA, USB oder Firewire angeschlossen sind. Seit 2007 werden auch IDE-Festplatten über den SCSI-Treiber angesprochen, der dazu um das `libata`-Modul erweitert wurde. Somit werden nahezu alle Datenträger einheitlich behandelt. Lediglich einige ganz alte Mainboards bzw. Chipsätze sind nicht `libata`-kompatibel und erfordern weiterhin den IDE-Treiber.

Device-Namen

Alle Festplatten und Flash-Datenträger werden mit `/dev/sdxy` benannt. Die Speichermedien heißen also der Reihe nach `/dev/sda`, `/dev/sdb` etc. Bei SATA-Geräten werden der Reihe nach alle genutzten Kanäle mit einem Buchstaben verbunden. Moderne Mainboards sehen zumeist mindestens sechs oder acht Kanäle vor. Wenn beispielsweise zwei Festplatten an die SATA-Kanäle 1 und 3 angeschlossen sind, erhalten diese die Device-Namen `/dev/sda` und `/dev/sdb`. Wenn später eine dritte Festplatte an den Kanal 2 angeschlossen wird, ändert sich der Device-Name der zweiten Festplatte von `/dev/sdb` in `/dev/sdc`.

Bei SCSI-Geräten hängt die Reihenfolge von den ID-Nummern der Geräte ab. Löcher in der ID-Reihenfolge werden nicht berücksichtigt. Drei SCSI-Geräte mit den ID-Nummern 0, 2 und 5 bekommen also die Device-Namen `/dev/sda` bis `/dev/sdc`. Ähnlich wie bei SATA-Geräten können sich durch eine spätere Konfigurationsänderung die Device-Namen ändern: Wenn ein viertes Gerät mit der ID-Nummer 3 hinzugefügt wird, bekommt dieses den Namen `/dev/sdc`; das Gerät mit der ID-Nummer 5 wird jetzt als `/dev/sdd` angesprochen. Wenn gleichzeitig Geräte verschiedener Bussysteme angeschlossen sind, hängt es vom BIOS und von den genutzten PCI-Steckplätzen ab, welches Bussystem zuerst berücksichtigt wird.

Externe USB- und Firewire-Geräte werden wie SCSI-Geräte behandelt, wobei für *x* der erste freie Buchstabe verwendet wird. Für die Zuweisung der Buchstaben ist die Reihenfolge entscheidend, in der die Geräte angeschlossen werden. CD- und DVD-Laufwerke bekommen eigene Device-Namen, die je nach Distribution `/dev/scdn` oder `/dev/srn` lauten.

Device	Bedeutung
`/dev/sda`	erste Festplatte
`/dev/sdb`	zweite Festplatte
...	
`/dev/scd0` oder `/dev/sr0`	erstes CD/DVD-Laufwerk
`/dev/scd1` oder `/dev/sr1`	zweites CD/DVD-Laufwerk
...	

Tabelle 25.2 Device-Namen

Virtuelle Datenträger (virtio)

Wenn Linux in einer virtuellen Maschine ausgeführt wird und dabei der virtio-Treiber zum Einsatz kommt, spricht der Kernel die virtuellen Festplatten über die Device-Namen `/dev/vda`, `/dev/vdb` etc. an. Der virtio-Treiber ermöglicht eine besonders effiziente Kommunikation zwischen dem Virtualisierungssystem und dem Kernel in der virtuellen Maschine. Die Virtualisierungssysteme KVM und Xen unterstützen virtio standardmäßig.

Partitionsnummern (MBR)

Das Nummerierungsschema für Partitionen hängt davon ab, wie die Festplatte partitioniert ist. Zurzeit sind zwei Partitionierungsvarianten möglich: die klassische MBR-Methode, bei der sich die Partitionierungstabelle im Master Boot Record (MBR) befindet, und die neuen GUID Partition Tables (GPTs), die vor allem bei sehr großen Festplatten sowie auf EFI-Systemen zum Einsatz kommen.

Bei der MBR-Partitionierung sind die Ziffern 1 bis 4 für primäre oder erweiterte Partitionen reserviert und die Ziffern ab 5 für logische Partitionen innerhalb der erweiterten Partitionen. Aus diesem Grund kommt es recht häufig vor, dass es in der Nummerierung Löcher gibt. Wenn die Festplatte beispielsweise eine primäre, eine erweiterte und drei logische Partitionen aufweist, haben diese die Nummern 1, 2, 5, 6 und 7. Tabelle 25.3 gibt einige Beispiele.

Die Anzahl der Partitionen pro Festplatte ist limitiert: Einerseits sind aus historischen Gründen maximal vier primäre bzw. drei primäre und eine erweiterte Partition zulässig. Andererseits limitiert Linux die Anzahl der verwendbaren logischen Partitionen auf 11. Daraus ergibt sich eine Gesamtanzahl von 15 Partitionen.

Device	Bedeutung
`/dev/sda`	die erste SCSI/SATA-Platte (bzw. die erste IDE-Festplatte bei libata-Kernel)
`/dev/sda1`	die erste primäre Partition dieser Festplatte
`/dev/sdd3`	die dritte primäre Partition der vierten SCSI/SATA-Platte
`/dev/sdd5`	die erste logische Partition der vierten SCSI/SATA-Platte
`/dev/sdd15`	die elfte logische Partition der vierten SCSI/SATA-Platte

Tabelle 25.3 Beispiele für die Partitionsnummerierung (MBR)

Partitionsnummern (GPT)

Wesentlich einfacher ist die Nummerierung bei Festplatten mit einer GPT: Die Unterscheidung zwischen primären, erweiterten und logischen Partitionen entfällt. Die Partitionen werden einfach der Reihe nach durchnummeriert. Das Kernel-Limit von 15 Partitionen bleibt aber bestehen, obwohl eine GPT bis zu 128 Partitionen erlaubt.

Unkonventionelle Nummerierung

Es ist möglich, dass die physikalische Reihenfolge der Partitionen von der Nummerierung abweicht! Nehmen Sie an, auf einer Festplatte mit 3 TByte wurden drei Partitionen mit je 1 TByte angelegt (`/dev/sda1` bis `/dev/sda3`). Anschließend wird die mittlere Partition gelöscht. Im freien Bereich werden nun zwei neue Partitionen mit je 500 GByte erzeugt. Diese beiden Partitionen erhalten die Device-Namen `/dev/sda2` und `/dev/sda4`! Bei einer MBR-Partitionierung ist dieser Sonderfall nicht möglich, weil zwischen `/dev/sda1` und `/dev/sda3` nur *eine* Partition eingefügt werden kann.

lsblk

Ein ungemein praktisches und wertvolles Werkzeug auf Rechnern mit mehreren Datenträgern ist `lsblk`. Es liefert eine baumartige Liste mit den Device-Namen aller Datenträger und Partitionen inklusive deren Verwendung bzw. `mount`-Punkt. Beim folgenden Beispiel enthält das erste Laufwerk die System- und die Swap-Partition. Auf dem zweiten Laufwerk ist die erste Partition (`sdb1`) ungenutzt. In der zweiten Partition befindet sich ein LVM-System, das wiederum zwei aktive Logical Volumes enthält.

```
root#  lsblk
NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda                   8:0    0    16G  0 disk
  sda1                8:1    0    15G  0 part /
  sda2                8:2    0     1K  0 part
  sda5                8:5    0  1022M  0 part [SWAP]
sdb                   8:16   0    64G  0 disk
  sdb1                8:17   0     2G  0 part
  sdb2                8:18   0    62G  0 part
    vg1-lv1 (dm-0) 252:0    0    10G  0 lvm  /backup
    vg1-lv2 (dm-1) 252:1    0    15G  0 lvm  /data
sr0                  11:0    1  1024M  0 rom
```

Alternative Device-Namen

Wie ich oben erklärt habe, kann sich durch den nachträglichen Einbau weiterer SCSI- oder SATA-Festplatten der Device-Name der bisherigen Geräte ändern. Unvorhersehbar sind die Device-Namen bei externen Geräten: Sie ergeben sich aus der Reihenfolge, in der die Geräte angeschlossen werden.

Um trotz variierender Device-Namen einheitlich auf einzelne Geräte bzw. Partitionen zuzugreifen (z. B. in einem Backup-Script), enthält das Verzeichnis `/dev/disk` zusätzliche Links auf alle Datenträger, die nach verschiedenen Kriterien geordnet sind:

- `/dev/disk/by-id/`*`id`* verwendet IDs, die sich aus dem Bussystem, dem Gerätenamen und einer Modell- oder Seriennummer zusammensetzen.
- `/dev/disk/by-label/`*`label`* verwendet den Namen, der dem Dateisystem gegeben wurde.
- `/dev/disk/by-path/`*`path`* verwendet einen Pfadnamen, der sich aus der PCI-Schnittstelle, dem Bussystem und der Partitionsnummer ergibt. Vorsicht: Wenn ein USB- oder Firewire-Gerät beim nächsten Mal an einen anderen USB-Stecker angeschlossen wird, ändert sich sein Pfadname!
- `/dev/disk/by-uuid/`*`uuid`* verwendet die UUIDs der Dateisysteme. Universal Unique Identifiers sind eindeutige ID-Nummern, die einem Dateisystem beim Formatieren zugeordnet werden. UUIDs ermöglichen eine Identifizierung von Dateisystemen auch nach einer Änderung an der Hardware-Konfiguration.

Die Anzahl der Links in den /dev/disk-Verzeichnissen variiert. /dev/disk/by-label und by-uuid enthalten beispielsweise nur Links auf Partitionen, die benannt sind bzw. eine UUID haben. Für die automatische Erzeugung der Links ist das udev-System verantwortlich (siehe Abschnitt 15.9). Das folgende ls-Kommando zeigt ein Beispiel für die Links eines Testsystems mit einer SATA-Festplatte, einem USB-Stick und einer SD-Karte. Um die Lesbarkeit zu erhöhen, habe ich die Zeilen ein wenig eingerückt und die Informationen zu den Zugriffsrechten entfernt.

```
user$  cd /dev/
user$  ls -lR disk/
disk/by-id:
   scsi-SATA_ST3320620AS_5QF194H9                -> ../../sda
   scsi-SATA_ST3320620AS_5QF194H9-part1          -> ../../sda1
   scsi-SATA_ST3320620AS_5QF194H9-part2          -> ../../sda2
   usb-Generic_USB_CF_Reader_058F312D81B         -> ../../sdc
   ...

disk/by-path:
   pci-0000:00:1d.7-usb-0:5:1.0-scsi-0:0:0:1     -> ../../sdc
   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-part2           -> ../../sda2

disk/by-uuid:
   008f06ef-28be-45c9-acbc-20cda51f712b          -> ../../sda2
   366CA8D16CA88D65                              -> ../../sda1
```

25.3 Partitionierung der Festplatte oder SSD

An sich ist die Partitionierung einer Festplatte oder SSD nichts Geheimnisvolles. Das Problem besteht aber darin, dass die Grundlagen der Partitionierung zurück in die 80er-Jahre reichen, als eine Festplatte mit 50 MByte *riesig* war und sich noch niemand eine Solid State Disk vorstellen konnte. In den vergangenen drei Jahrzehnten hat die Datenträgertechnologie fast unvorstellbare Fortschritte gemacht, während sich an den Partitionierungsgrundlagen nur ganz zaghaft etwas geändert hat. Einen wirklich modernen Standard zur Speicherung der Partitionierungsdaten stellen erst GUID Partition Tables (GPTs) dar, die aber noch immer nicht sehr weit verbreitet sind. Das ändert sich zum Glück momentan rasant.

Kurzum: Damit Sie bei der Partitionierung Ihrer Festplatte oder SSD keine Fehler machen, müssen Sie Grundlagen und Prinzipien verstehen, die weit in die Vergangenheit zurückreichen. Aus diesem Grund fällt dieser Abschnitt recht umfangreich aus. Einleitende Informationen zu Partitionen und Partitionstypen finden Sie in

Abschnitt 2.6. Wie Partitionen unter Linux benannt und nummeriert sind, habe ich im vorigen Abschnitt beschrieben.

Achtung

Partitionierungsprogramme können den Inhalt Ihrer gesamten Festplatte bzw. SSD zerstören! Lesen Sie diesen Abschnitt vollständig, bevor Sie Partitionierungswerkzeuge einsetzen! Sie dürfen nie eine Partition verändern, die momentan verwendet wird, d. h., deren Dateisystem in den Verzeichnisbaum eingebunden bzw. »gemountet« ist!

Partitionierungswerkzeuge

Während der Installation bietet beinahe jede Linux-Distribution einfach zu bedienende Werkzeuge zur Partitionierung der Festplatte an. Aber nur bei wenigen Distributionen stehen diese Werkzeuge auch im laufenden Betrieb zur Verfügung – z. B. bei SUSE das YAST-Modul System • Partitionieren. Ansonsten haben Sie, wenn Sie nach der Installation Änderungen an der Partitionierung durchführen möchten, die Wahl zwischen einer ganzen Palette von Partitionierwerkzeugen: Zu den wichtigsten Vertretern zählen die textorientierten Kommandos `fdisk` und `parted` sowie das grafische Programm `gparted`.

LVM

Wenn Sie häufig Änderungen an der Partitionierung durchführen müssen, sollten Sie sich unbedingt mit LVM anfreunden (siehe Abschnitt 25.15): LVM fügt eine virtuelle Ebene zwischen den physikalischen Partitionen der Festplatte und den für Dateisysteme genutzten Partitionen ein und vereinfacht nachträgliche Änderungen ungemein.

MBR oder GPT?

Es gibt zwei Verfahren, wie die Partitionierungsdaten gespeichert werden können: im Master Boot Record (MBR) oder als GUID Partition Table (GPT). Das MBR-Verfahren ist seit Jahrzehnten gebräuchlich, aber nur für Festplatten bis zu 2 TByte geeignet. Zwingend ist der Einsatz einer GPT nur in drei Fällen erforderlich:

- bei Festplatten, die größer als 2 TByte sind
- bei Festplatten, die parallel auch zum Start von OS X verwendet werden (also üblicherweise in einem Mac)
- wenn Windows 7 oder eine neuere Windows-Version im EFI-Modus gestartet werden soll

In allen anderen Fällen ist der Einsatz der GPT optional! Das GPT-Format ist zwar Teil der EFI-Spezifikation, EFI kommt aber selbstverständlich auch mit mit MBR-Festplatten zurecht. Umgekehrt können auch nahezu alle Rechner mit herkömmlichem BIOS Linux starten, wenn die Festplatte eine GPT enthält. Zur GRUB-2-Installation

sollten Sie in diesem Fall aber eine eigene BIOS-GRUB-Partition vorsehen, wie dies in Kapitel 26 beschrieben ist.

Die Entscheidung für ein Partitionierungssystem ist endgültig. Ein späterer Wechsel ist zwar jederzeit möglich, geht aber mit dem Verlust aller Daten einher! Persönlich richte ich auf neuen Festplatten generell eine GPT ein, weil ich das Gewurstel mit primären, erweiterten und logischen Partitionen leid bin.

Festplatte/SSD initialisieren

Aktuelle Linux-Distributionen kommen sowohl mit MBR- als auch mit GPT-Datenträgern zurecht. Wenn es aber darum geht, die Partitionierung neu einzurichten (egal, ob es sich um noch ganz leere oder um vorformatierte Datenträger handelt), bieten die meisten Installationsprogramme wenig Optionen: Auf leeren Festplatten wird die Partitionierungstabelle zumeist ungefragt in den MBR geschrieben, bereits formatierte Festplatten werden nicht angerührt.

Wenn Sie den Partitionierungstyp also selbst bestimmen möchten, ist Handarbeit erforderlich, die Sie am besten in einem Live-System durchführen. Dort starten Sie in einem Terminal-Fenster mit root-Rechten das Programm `parted` und führen das entsprechende `mklabel`-Kommando aus. (Um es ein letztes Mal zu betonen: Mit `mklabel xxx` verlieren Sie alle Daten auf Ihrer Festplatte!)

```
root#  parted /dev/sda
(parted)  mklabel gpt        (für GPT)
(parted)  mklabel msdos      (für MBR)
(parted)  quit
```

Grundregeln

Unabhängig vom eingesetzten Werkzeug müssen Sie einige Grundregeln beachten:

- Es ist unmöglich, im laufenden Betrieb Änderungen an der Systempartition durchzuführen. Wenn Sie beispielsweise die Systempartition vergrößern möchten, starten Sie den Rechner am besten mit einer Live-CD. Besonders gut geeignet sind die für die Festplattenpartitionierung optimierten Minidistributionen GParted-Live-CD, Parted Magic und SystemRescueCd:

  http://gparted.sourceforge.net/livecd.php
  http://partedmagic.com
  http://www.sysresccd.org

- Eine Vergrößerung einer Partition ist grundsätzlich nur möglich, wenn hinter der Partition freier Platz ist. Sie können Partitionen nicht auf der Festplatte »verschieben«.
- Wenn Sie die Größe einer Partition ändern, verändert sich damit *nicht* automatisch auch die Größe des darauf enthaltenen Dateisystems! Dazu sind weitere Kommandos erforderlich, die je nach Dateisystemtyp variieren.

- Linux kann grundsätzlich nur 15 Partitionen pro Festplatte ansprechen. Wenn Ihnen das zu wenig ist, müssen Sie LVM einsetzen.

  Bei der MBR-Partitionierung ist eine dieser 15 Partitionen die erweiterte Partition, die zwar andere Partitionen, aber nicht direkt Daten bzw. ein Dateisystem aufnehmen kann. Damit reduziert sich die Maximalanzahl der für Dateisysteme geeigneten Partitionen auf 3 primäre und 11 logische Partitionen.

- Wenn Sie die Partitionierung einer Festplatte ändern, die momentan genutzt wird (z. B. weil eine Partition die Systempartition Ihrer Linux-Distribution ist), fordert das Partitionierungsprogramm Sie unter Umständen dazu auf, den Rechner neu zu starten. Bei `fdisk` lautet die Warnung so: *Re-read table failed with error 16: Device or resource busy. Reboot your system to ensure the partition table is updated*.

  Der Grund besteht darin, dass ältere Linux-Kernel nicht in der Lage sind, im laufenden Betrieb die Partitionierungstabelle neu einzulesen. Die Änderungen wurden also gespeichert, werden aber für den Kernel erst nach einem Neustart aktiv. Sie *müssen* Linux neu starten, bevor Sie die geänderte Partitionierung nutzen können.

- Der Start von Windows Vista bzw. von allen neueren Windows-Versionen auf Datenträgern mit MBR-Partitionierung setzt voraus, dass die Windows-Partition mit Sektor 2048 beginnt, sodass das erste MByte der Festplatte für den MBR und den Bootloader frei bleibt. Die Installationswerkzeuge aller gängigen Distributionen kümmern sich darum automatisch.

Festplatten und SSDs mit 4-kByte-Sektoren

Neue Festplatten sowie SSDs verwenden statt der jahrzehntelang üblichen 512-Byte-Sektoren längere Sektoren von 4096 Byte (4 kByte). Das hat viele Vorteile, unter anderem eine höhere Geschwindigkeit und eine höhere Festplattenkapazität. Aus Kompatibilitätsgründen melden aber solche Festplatten eine 512-Byte-Sektorgröße an das Betriebssystem.

Um Festplatten mit 4-kByte-Sektoren effizient zu nutzen, müssen Partitionen so eingerichtet werden, dass die Startposition jeder Partition ein Vielfaches von 4 kByte beträgt. Ist das nicht der Fall und will das Dateisystem einen 4-kByte-Bereich verändern, muss die Festplatte zwei 4-kByte-Sektoren lesen, modifizieren und schreiben. Das würde Schreibvorgänge massiv bremsen.

Aktuelle Windows- und Linux-Versionen nehmen bei der Installation Rücksicht auf die 4-kByte-Sektorgröße und richten die Partitionsgrenzen bei der Installation an Vielfachen von 1 MByte aus.

Wenn Sie selbst Partitionen einrichten und Programme verwenden, die mit 512-Byte-Sektoren rechnen (z. B. alte `fdisk`-Versionen), müssen Sie darauf achten, dass die Partitionsgrenzen ein Vielfaches von 8 Sektoren betragen! Technische Hintergründe zur optimalen Nutzung von Festplatten mit 4-kByte-Sektoren können Sie hier nachlesen:

http://lwn.net/Articles/377895
http://heise.de/-938237

Größenanpassung der erweiterten Partition (nur bei der MBR-Partitionierung)

Die in diesem Kapitel vorgestellten Partitionierungswerkzeuge, aber auch die während einer Linux-Installation eingesetzten Partitionierungshilfen unterscheiden sich in einem entscheidenden Punkt: Manche Werkzeuge belassen die erweiterte Partition so, wie Sie sie ursprünglich eingerichtet haben. Ich bezeichne diese Programme hier als Typ 1. Dazu zählen `fdisk`, `parted`, die Installationsprogramme von Fedora, Red Hat und SUSE sowie die Partitionierwerkzeuge von Windows.

Andere Programme passen die Größe der erweiterten Partition dagegen automatisch so an, dass alle logischen Partitionen exakt darin Platz haben (Typ 2). Dazu zählen die Installationsprogramme von Debian und Ubuntu.

Beide Vorgehensweisen sind an sich in Ordnung, problematisch ist nur der Mischbetrieb: Beispielsweise erzeugen Sie mit einem Werkzeug des Typs 2 eine neue, logische Partition. Bei dieser Gelegenheit verkleinert das Programm die erweiterte Partition. Wenn Sie anschließend mit einem Werkzeug des Typs 1 versuchen, eine weitere logische Partition anzulegen, meldet dieses, dass die erweiterte Partition schon voll ist. Programme des Typs 1 sind mit der Ausnahme von `parted` nicht in der Lage, die Größe erweiterter Partitionen zu ändern, wenn sich darin bereits logische Partitionen befinden.

Abhilfe: Starten Sie nochmals ein Programm des Typs 2, und ändern Sie die Partitionierung. Sie können auch mit einem Typ-2-Partitionierwerkzeug eine ausreichend große logische Platzhalterpartition erzeugen. Damit vergrößert sich automatisch die erweiterte Partition. Anschließend löschen Sie die Platzhalterpartition mit einem Partitionierungsprogramm des Typs 1 und können nun den freien Platz in der erweiterten Partition nutzen.

Naturgemäß gehen Sie dem Ärger mit erweiterten Partitionen ganz aus dem Weg, wenn Sie sich von vornherein für die GPT-Partitionierung entscheiden.

fdisk (MBR)

`fdisk` zählt zu den ältesten Linux-Partitionierprogrammen. Die Benutzeroberfläche ist altmodisch, dafür ist das Programm ausgereift und vor allem bei langjährigen Linux-Anwendern beliebt.

fdisk ist nicht GPT-kompatibel!

`fdisk` ist nur für Festplatten/SSDs mit MBR-Partitionierung geeignet! Wenn `fdisk` beim Start erkennt, dass sich auf dem Datenträger eine GPT befindet, empfiehlt es den Einsatz von `parted`. Wenn Sie nicht den ganzen Inhalt Ihrer Festplatte oder SSD verlieren möchten, sollten Sie diesen Rat beherzigen! Anstelle von `parted` können Sie auch `gdisk` einsetzen. Das Programm ist vor allem dann interessant, wenn Sie mit der `fdisk`-Logik vertraut sind.

Start

`fdisk` kann immer nur eine Festplatte bzw. SSD bearbeiten, deren Device-Name beim Start angegeben werden muss, z. B. `/dev/sdc` für den dritten SATA/SCSI-Datenträger. Wenn Sie stattdessen die Option `-l` übergeben, zeigt `fdisk` eine Liste aller Partitionen auf allen Festplatten an. Nach dem Start liefert M (*menu*) eine kurze Übersicht der zur Verfügung stehenden Kommandos. P (*print*) zeigt eine Liste der Partitionen an, die zurzeit auf der ausgewählten Festplatte vorhanden sind.

Aktuelle `fdisk`-Versionen sind kompatibel zu modernen Festplatten und SSDs mit 4-kByte-Sektoren. `fdisk` rechnet automatisch in Sektoren und nimmt keine Rücksicht auf DOS und Windows XP. Wenn Sie das zur Wartung von Uralt-Installationen wünschen, müssen Sie `fdisk` mit den Optionen `-c=dos -u=cylinders` starten. Das dürfen Sie aber keinesfalls bei einer Festplatte oder SSD mit 4-kByte-Sektoren machen! Wenn Sie umgekehrt eine aktuelle Festplatte oder SSD mit einer alten `fdisk`-Version bearbeiten, wie sie z. B. unter RHEL 6 noch immer zum Einsatz kommen, müssen Sie beim Start die Optionen `-c -u` angeben, um zu vermeiden, dass `fdisk` die Partitionen ungünstig ausrichtet.

Neue Partition erstellen

Mit N (*new*) richten Sie neue Partitionen ein. Dabei können maximal vier primäre Partitionen eingerichtet werden. Wenn mehr als vier Partitionen verwaltet werden sollen, muss eine der vier primären Partitionen als erweitert (*extended*) deklariert werden. Im Bereich der erweiterten Partition dürfen dann bis zu elf logische Partitionen eingerichtet werden. Falls beim Einrichten einer neuen Festplattenpartition unterschiedliche Typen infrage kommen (primär, erweitert oder logisch), antwortet `fdisk` mit einer zusätzlichen Rückfrage bezüglich des Partitionstyps.

Nachdem geklärt ist, welchen Typ die neue Partition haben soll, fragt das Programm, an welcher Stelle die Partition beginnen soll (normalerweise beim ersten freien Zylinder) und wo sie enden soll (Endzylinder). Die Größenangabe kann auch

bequemer in der Form `+nM` oder `+nG` erfolgen, also `+50G` für eine 50 GByte große Partition.

Nach der Definition einer neuen Partition kann die gesamte Partitionstabelle mit P (*print*) angezeigt werden. Anschließend können weitere Partitionen definiert und bereits definierte Partitionen wieder gelöscht werden etc.

Partitions-ID

`fdisk` erzeugt neue Partitionen immer vom Typ *Linux native* (ID-Nummer 83). Wenn Sie einen anderen Typ benötigen, müssen Sie die ID-Nummer der neu eingerichteten Partition mit T (*type*) ändern. Übliche ID-Nummern in hexadezimaler Schreibweise sind:

82: Linux-Swap-Partition
83: Linux-Dateisystem (für alle Linux-Dateisysteme: `ext`, `reiser`, `xfs` etc.)
8e: Linux-LVM-Partition
fd: Linux-RAID-Partition

Eine Liste aller verfügbaren ID-Nummern erhalten Sie mit L. Die Liste enthält auch die Codes für zahllose andere Betriebssysteme wie DOS, Windows, UNIX etc.

Änderungen speichern

`fdisk` führt sämtliche Änderungen erst dann aus, wenn Sie das Kommando W (*write*) ausführen. Vorher können Sie mit V (*verify*) überprüfen, ob alle internen Informationen mit der Platte übereinstimmen. Das ist eine zusätzliche Sicherheitskontrolle. Normalerweise besteht die Reaktion auf V nur darin, dass die Anzahl der 512-Byte-Sektoren, die von keiner primären oder logischen Partition erfasst und somit noch ungenutzt sind, angezeigt wird.

Wenn Sie sich unsicher sind, können Sie `fdisk` jederzeit mit Q (*quit*) oder auch mit Strg+C verlassen – Ihre Festplatte bleibt dann so, wie sie ist.

Partitionieren und formatieren ...

Die mit `fdisk` eingerichteten Partitionen sind noch leer, d. h., `fdisk` installiert kein Dateisystem! Die Kommandos zur Einrichtung eines Dateisystems hängen vom gewünschten Dateisystem ab – etwa `mkfs.ext4` für ein `ext4`-Dateisystem. Die Kommandos werden in den folgenden Abschnitten vorgestellt. Falls Sie eine Swap-Partition manuell einrichten möchten, finden Sie diesbezügliche Informationen in Abschnitt 25.13. An dieser Stelle geht es ausschließlich um die Partitionierung!

Partition vergrößern

`fdisk` kann grundsätzlich die Größe einer existierenden Partition nicht verändern. Die einzige Ausnahme liegt dann vor, wenn die zu ändernde Partition die letzte Partition auf der Festplatte bzw. die letzte logische Partition innerhalb einer erweiterten Partition ist, und dahinter noch Platz frei ist. In diesem Fall können Sie diese Partition löschen und anschließend vergrößert neu anlegen.

`fdisk` verändert nur die Partitionstabelle, lässt die eigentlichen Daten auf der Festplatte aber unberührt. Das bedeutet, dass das Dateisystem in der vergrößerten Partition nicht mitwächst. Damit ist nun ein Teil der Partition ungenutzt. Eine Vergrößerung des Dateisystems ist nur bei manchen Dateisystemen möglich (siehe Abschnitt 25.7).

Generell ist die Veränderung einer Partition bzw. eines Dateisystems eine sehr gefährliche Operation, die nur Linux-Profis zu empfehlen ist! Führen Sie nach Möglichkeit vorher ein Backup durch!

Tastenkürzel	Bedeutung
D	Partition löschen (*delete*)
L	Partitions-ID-Nummer anzeigen (*list*)
M	Online-Hilfe (*menu*)
N	neue Partition anlegen (*new*)
P	Partitionsliste anzeigen (*print*)
Q	Programm beenden (ohne die Partitionstabelle zu verändern; *quit*)
T	Partitionstyp verändern
U	Maßeinheit zwischen Zylindern und Sektoren umschalten (*unit*)
V	Partitionstabelle überprüfen (*verify*)
W	Partitionstabelle ändern (*write*)

Tabelle 25.4 fdisk-Tastenkürzel

Beispiel

Das folgende Beispiel zeigt die Erstellung einer neuen Partition auf einer Festplatte mit 4-kByte-Sektoren. Das Kommando P gibt Auskunft über den aktuellen Zustand der Festplatte. Die Festplatte ist 255 × 63 × 182401 × 512 Byte = ca. 1,36 TByte groß. Wenn man wie die Festplattenhersteller rechnet, also mit 1 TByte = 10^{12} Byte, dann ergeben sich 1,5 TByte. Ich rechne hier aber wie `fdisk` mit 2er-Potenzen, also mit 1 kByte = 2^{10} Byte, 1 TByte = 2^{40} Byte.

Anfänglich sind zwei primäre Partitionen vorhanden. Die erste Partition beginnt bei Sektor 2048 bzw. an der Byte-Position 2048 × 512 Byte = 1 MByte. Diese Partition ist 48.827.392 Blöcke groß (ein »Block« ist 1024 Byte), also 48.827.392 × 1024 Byte = ca. 46,6 GByte. Die zweite Partition beginnt bei Sektor 97.656.832, exakt 47.684 MByte nach dem Beginn der Festplatte. Die Partitionen sind also an 1-MByte-Grenzen ausgerichtet. Diese Partition ist 1.952.768 × 1024 Byte = ca. 1,9 GByte groß.

```
root#  fdisk -c -u /dev/sda
Befehl (m für Hilfe):  p
Platte /dev/sda: 1500.3 GByte, 1500301910016 Byte
255 Köpfe, 63 Sektoren/Spur, 182401 Zylinder, zusammen 2930277168 Sektoren
Einheiten = Sektoren von 1 × 512 = 512 Bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x0004b057

   Gerät  boot.     Anfang        Ende     Blöcke   Id  System
/dev/sda1   *        2048    97656831    48827392   83  Linux
/dev/sda2        97656832   101562367     1952768   82  Linux Swap / Solaris
```

N erzeugt nun eine neue, primäre Partition. Als Startzylinder wird der erste freie Zylinder gewählt. Anstatt den Endzylinder anzugeben, bewirkt +30G, dass die Partition 30 GByte groß wird.

```
Befehl (m für Hilfe):  n
Befehl  Aktion
   e      Erweiterte
   p      Primäre Partition (1-4)
p
Partitionsnummer (1-4):  3
Erster Sektor (101562368-2930277167, Vorgabe: 101562368):  <return>
Benutze den Standardwert 101562368
Last Sektor, +Sektoren or +sizeK,M,G (101562368-2930277167,
  Vorgabe: 2930277167):  +30G

Befehl (m für Hilfe):  p
   Gerät  boot.     Anfang        Ende     Blöcke   Id  System
/dev/sda1   *        2048    97656831    48827392   83  Linux
/dev/sda2        97656832   101562367     1952768   82  Linux Swap / Solaris
/dev/sda3       101562368   164476927    31457280   83  Linux
```

Mit W wird die geänderte Partitionstabelle gespeichert. Da einige andere Partitionen der Festplatte zurzeit genutzt werden, gelingt es nicht, die neue Tabelle korrekt einzulesen. Der Rechner muss also neu gestartet werden, bevor die neue Partition genutzt werden kann.

```
Befehl (m für Hilfe):  w
Die Partitionstabelle wurde verändert!
Rufe ioctl() um Partitionstabelle neu einzulesen.
WARNING: Re-reading the partition table failed with error 16: Device or
resource busy. The kernel still uses the old table. The new table will be
used at the next reboot or after you run partprobe(8) or kpartx(8)
Synchronisiere Platten.
```

parted (MBR und GPT)

Die Bedienung von `parted` ist mindestens ebenso umständlich wie die von `fdisk`. Zudem ist im Umgang mit `parted` noch mehr Vorsicht angesagt als bei `fdisk`: Jede Änderung wird sofort ausgeführt! Der größte Vorteil von `parted` besteht darin, dass das Programm im Gegensatz zu `fdisk` auch mit GUID Partition Tables (GPTs) zurechtkommt. Details zu den vielen Funktionen von `parted` finden Sie unter:

http://www.gnu.org/software/parted

Start

Beim Start von `parted` geben Sie das Festplatten-Device an. H führt zur Anzeige der zur Auswahl stehenden Kommandos. `H` *kommando* liefert einen knappen Hilfetext zu den einzelnen Kommandos. P zeigt die Partitionstabelle an – hier für eine 1,5-TByte-Festplatte, die bereits drei Partitionen enthält:

```
root#  parted /dev/sda
(parted)  print
Modell: ATA WDC WD15EARS-00Z (scsi)
Festplatte  /dev/sda:  1500GB

Sektorgröße (logisch/physisch): 512B/512B
Partitionstabelle: msdos

Anzahl  Beginn  Ende    Größe   Typ      Dateisystem     Flags
 1      1049kB  50,0GB  50,0GB  primary  ext4            boot
 2      50,0GB  52,0GB  2000MB  primary  linux-swap(v1)
 3      52,0GB  84,2GB  32,2GB  primary
```

MB versus MiB, GB versus GiB

Standardmäßig zeigt `parted` Partitionsgrenzen und -größen in dezimalen Maßeinheiten an, also in `MB` = 10^6 Byte oder `GB` = 10^9 Byte. Eingaben ohne Maßeinheit werden als dezimale MByte interpretiert. Sie können auch explizit die gewünschte Einheit angeben – beispielsweise `100MiB` oder `15GB`.

Mit `unit` können Sie die gewünschte Maßeinheit für alle Ein- und Ausgaben festlegen. Mögliche Einstellungen sind `MB` und `GB`, `MiB` und `GiB` (binäre Zählweise, also `GiB` = 2^{30} Byte) sowie `%` für Prozentangaben relativ zur Größe der Festplatte.

```
(parted)  unit MiB
(parted)  print
...
Festplatte  /dev/sda:  1397GiB
...
Anzahl  Beginn    Ende      Größe     Typ      Dateisystem     Flags
 1      1,00MiB   47684MiB  47683MiB  primary  ext4            boot
 2      47684MiB  49591MiB  1907MiB   primary  linux-swap(v1)
 3      49591MiB  80311MiB  30720MiB  primary
```

mklabel

Wenn die Festplatte noch vollkommen ungenutzt ist und keine Partitionstabelle enthält, müssen Sie diese einrichten. Dazu führen Sie `mklabel msdos` für MBR-Partitionen oder `mklabel gpt` für GPT-Partitionen aus. Beachten Sie, dass Sie mit `mklabel` alle bisher vielleicht gespeicherten Daten der Festplatte verlieren!

mkpart und rm

Mit den Kommandos `mkpart` bzw. `rm` erzeugen bzw. löschen Sie Partitionen. Bei `mkpart` müssen Sie bei MBR-Partitionen den Typ (`primary`, `extended` oder `logical`) sowie die gewünschte Start- und Endposition angeben. Bei GPT-Partitionen wird der erste Parameter als frei wählbarer Partitionsname interpretiert.

```
(parted)  mkpart primary 1MiB 10GiB     (MBR)
(parted)  mkpart part1   1MiB 10GiB     (GPT)
```

Normalerweise erzeugt `mkpart` Partitionen, die später ein Linux-Dateisystem aufnehmen (entspricht Partitions-ID `82` bei `fdisk`). Dieser Partitionstyp ist auch für Software-RAID und LVM geeignet. Wenn Sie hingegen eine Swap- oder eine Windows-Partition erzeugen möchten, müssen Sie in einem zusätzlichen Parameter vor der Startposition den Dateisystemtyp angeben, z. B. `linux-swap`, `fat32` oder `ntfs`:

```
(parted)  mkpart primary linux-swap 1MiB 10GiB     (MBR)
(parted)  mkpart part1   linux-swap 1MiB 10GiB     (GPT)
```

Um eine Partition zu löschen, ermitteln Sie zuerst mit `print` die Partitionsliste. Anschließend löschen Sie mit `rm` *n* die gewünschte Partition, wobei *n* eine Partitionsnummer laut `print` ist.

Um eine neue logische Partition zu erzeugen, müssen Sie vorher eine erweiterte Partition anlegen oder mit `resize` vergrößern.

set

Wenn Sie die neue Partition als Teil eines LVM- oder RAID-Systems nutzen möchten, müssen Sie den Partitionstyp entsprechend einstellen. Das erforderliche Kommando lautet `set` *partitionsnummer attributname* `on`. Mögliche Attribute sind `boot`, `lvm` und `raid`.

Beispiel 1 (MBR)

Die folgenden Kommandos richten zuerst eine primäre Partition (500 MiB), dann eine erweiterte Partition (19,5 GiB) und darin eine logische Partition in derselben Größe ein. Beachten Sie, dass der Startpunkt für die logische Partition um 1 MiB größer ist als der Startpunkt der erweiterten Partition. Dadurch entsteht zwar eine kleine, ungenutzte Lücke, dafür sind die Partitionen aber optimal ausgerichtet.

```
root#  parted /dev/sdb
(parted)  mklabel msdos
(parted)  mkpart primary 1mib 500mib
(parted)  mkpart extended 500mib 20gib
(parted)  mkpart logical 501mib 20gib
(parted)  unit GiB
```

```
(parted)  print
Nummer  Anfang   Ende     Größe    Typ       Dateisystem  Flags
 1      0,00GiB  0,49GiB  0,49GiB  primary
 2      0,49GiB  20,0GiB  19,5GiB  extended               LBA
 5      0,49GiB  20,0GiB  19,5GiB  logical
```

Nun soll auf der Festplatte eine weitere logische Swap-Partition eingerichtet werden. Dazu muss zuerst die erweiterte Partition vergrößert werden. `resize` zeigt dabei eine vollkommen irreführende Warnung an – eine erweiterte Partition enthält ja ohnedies nie ein Dateisystem.

```
(parted)  resize 2 0,49GiB 21GiB
WARNUNG: Sie versuchen parted auf einem Dateisystem (resize) zu verwenden ...
(parted)  mkpart logical linux-swap 20GiB 21GiB
(parted)  unit GiB
(parted)  print
Nummer  Anfang   Ende     Größe    Typ       Dateisystem  Flags
 1      0,00GiB  0,49GiB  0,49GiB  primary
 2      0,49GiB  21,0GiB  20,5GiB  extended               LBA
 5      0,49GiB  20,0GiB  19,5GiB  logical
 6      20,0GiB  21,0GiB  1,00GiB  logical
```

Beispiel 2 (GPT)

In einem zweiten Beispiel sollen auf einer Festplatte mit GPT zwei Partitionen eingerichtet werden, von denen eine später als Physical Volume für ein LVM-System dienen wird:

```
root#
(parted)  mklabel gpt
(parted)  mkpart part1 1mib 2gib
(parted)  mkpart part2 2gib 64gib
(parted)  set 2 lvm on
(parted)  print
Nummer  Anfang   Ende     Größe    Dateisystem  Name   Flags
 1      0,00GiB  2,00GiB  2,00GiB              part1
 2      2,00GiB  64,0GiB  62,0GiB              part2  LVM
```

Bearbeiten Sie mit parted nur die Partitionen, nicht deren Inhalt!

`parted` kennt diverse Kommandos, die nicht nur die Partitionen bearbeiten, sondern auch das darauf enthaltene Dateisystem. Das Handbuch rät von der Benutzung dieser Kommandos ab; in zukünftigen `parted`-Versionen sollen diese Kommandos ganz eliminiert werden. Verwenden Sie `parted` ***nur*** zur Partitionierung! Um Dateisysteme einzurichten oder zu verändern, verwenden Sie besser die dafür vorgesehenen Kommandos außerhalb von `parted`, z. B. `mkfs.ext4` oder `resize2fs`.

sfdisk (MBR)

`sfdisk` ist im Vergleich zu `fdisk` und `parted` ein relativ simples Kommando: Sie können damit die Partitionen einer Festplatte oder SSD auflisten bzw. einen Datenträger, basierend auf einer in Textform vorliegenden Partitionierungstabelle, neu partitionieren. Eine interaktive Bedienung ist nicht vorgesehen. Attraktiv ist der Einsatz von `sfdisk` vor allem dann, wenn Sie – z. B. für eine RAID-Konfiguration – die Partitionierung einer Festplatte exakt auf eine zweite Festplatte übertragen möchten. `sfdisk` eignet sich nur für Datenträger mit MBR-Partitionierung!

Beispiel

Im folgenden Beispiel ermittelt `sfdisk -d /dev/sda` eine für `sfdisk` lesbare Partitionsliste der ersten Festplatte. `|` gibt diese Liste an ein zweites `sfdisk`-Kommando weiter, das die zweite Festplatte entsprechend formatiert:

```
root#  sfdisk -d /dev/sda | sfdisk /dev/sdb
```

Bei meinen Tests beschwerte sich `sfdisk` bisweilen, dass die zweite Festplatte in Verwendung sei. Nachdem ich mich vergewissert hatte, dass das nicht der Fall war (unter anderem durch `dmesg | grep sdb`), habe ich beim zweiten `sfdisk`-Kommando die Option `--force` verwendet. Anschließend war ein Neustart des Rechners erforderlich, damit der Kernel die neue Partitionierung der zweiten Festplatte akzeptierte:

```
root#  sfdisk -d /dev/sda | sfdisk --force /dev/sdb
root#  reboot
```

Die Option `--force` müssen Sie auch einsetzen, wenn sich `sfdisk` darüber beklagt, dass eine Partition nicht exakt auf einer Zylindergrenze endet. Für Linux und die meisten anderen Betriebssysteme bilden die Zylindergrenzen eine willkürliche Unterteilung der Festplatte, die für den Betrieb nicht relevant ist.

sgdisk

Wie schon erwähnt ist `sfdisk` nur für Datenträger mit MBR-Partitionstabelle geeignet. Für Festplatten mit GPT können Sie anstelle von `sfdisk` das Kommando `sgdisk` einsetzen. Der Paketname lautet üblicherweise `gdisk`. Beachten Sie aber, dass `sgdisk` trotz des ähnlich klingenden Namens ganz andere Optionen erwartet als `sfdisk`!

gparted (MBR, GPT)

Zu `parted` gibt es die grafische Benutzeroberfläche `gparted`. Das Programm kann nur Partitionen verändern, die momentan unbenutzt sind, die also nicht in den Verzeichnisbaum eingebunden sind. Alle benutzten Partitionen werden im Programm mit einem Vorhängeschloss gekennzeichnet, und die Bearbeitungsbuttons sind gesperrt. Abhilfe: Starten Sie `gparted` von einer Linux-Live-CD.

Anders als `parted` merkt sich `gparted` alle Aktionen, führt diese aber vorerst nicht aus. BEARBEITEN • RÜCKGÄNGIG widerruft die Aktionen, BEARBEITEN • AUSFÜHREN führt sie endgültig aus.

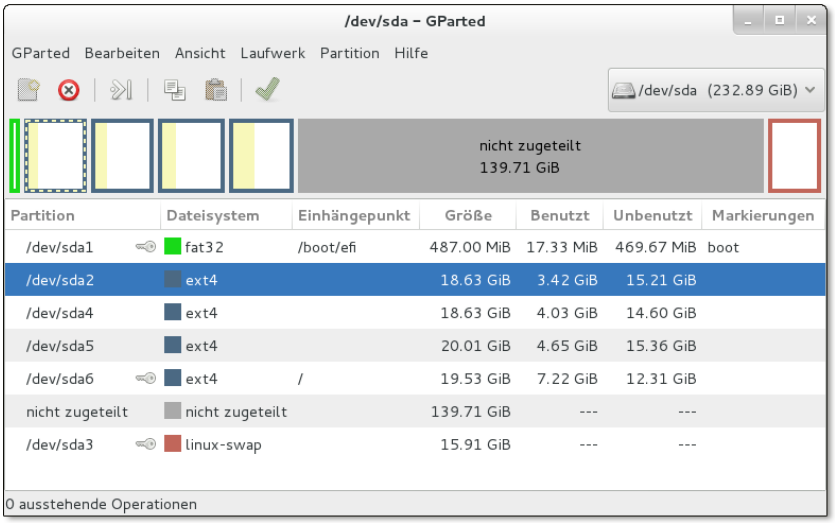


Abbildung 25.1 gparted

Um eine Partition zur Verwendung für RAID oder LVM zu kennzeichnen, klicken Sie die Partition mit der rechten Maustaste an und führen MARKIERUNGEN BEARBEITEN aus. Anschließend können Sie diverse Flags setzen, die die Funktion der Partition bezeichnen.

Unter SUSE können Sie als Alternative zu `gparted` auch das YaST-Modul SYSTEM • PARTITIONIEREN einsetzen. Bei den meisten anderen Distributionen fehlt ein vergleichbares Werkzeug.

gnome-disks (MBR und GPT)

Das relativ neue Programm *Laufwerke* (Programmname `gnome-disks`) hilft bei der Partitionierung von Festplatten und SSDs, beim Einrichten von Dateisystemen und beim Einbinden von Dateisystemen in den Verzeichnisbaum (inklusive der Veränderung von `/etc/fstab`). `gnome-disks` löst beginnend mit Gnome 3.6 das Programm Palimpsest ab, das in älteren Gnome-Versionen ähnliche Aufgaben erledigt. Bei vielen Distributionen befindet sich das Programm im Paket `gnome-disk-utils` und muss unter Umständen extra installiert werden.

Ärgerlich beim Umgang mit dem Programm ist der Umstand, dass `gnome-disks` darauf besteht, auf jeder neuen Partition sofort ein Dateisystem einzurichten. Wenn Sie das nicht möchten, wählen Sie TYP = BENUTZERDEFINIERT und geben im Textfeld DATEISYSTEM eine ungültige Bezeichnung an (z. B. `none`). Das führt zwar zu einer Fehlermeldung, die Partition wird aber ohne Dateisystem erzeugt. Anschließend öffnen Sie mit dem Zahnrad-Button ein Kontextmenü und wählen PARTITION BEARBEITEN.

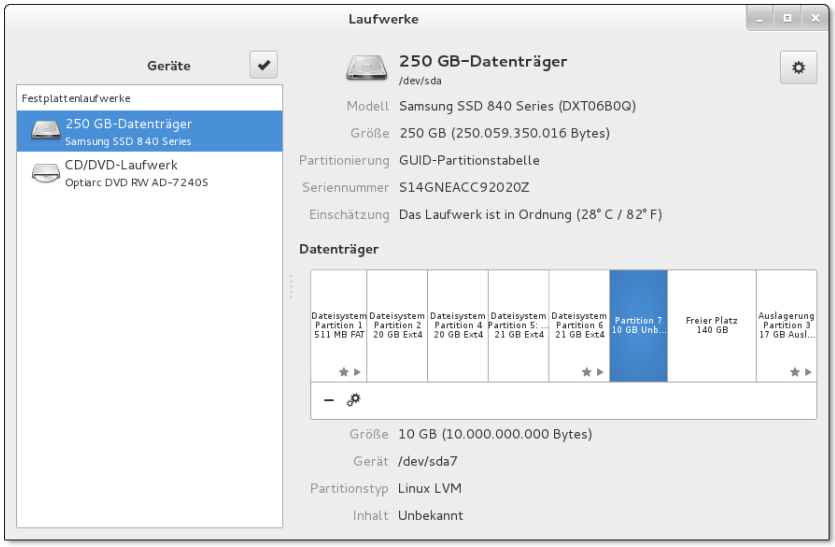


Abbildung 25.2 Gnome Disks

An dieser Stelle haben Sie nun die Möglichkeit, die Partition zur Nutzung für RAID, LVM etc. zu markieren.

25.4 Dateisystemtypen

Dieser Abschnitt gibt einen Überblick über die Dateisystemtypen, die unter Linux genutzt werden können. Auf einige besonders wichtige Dateisystemtypen gehe ich im weiteren Verlauf dieses Kapitels dann detaillierter ein: `ext2` bis `ext4`, `btrfs`, `xfs`, `vfat`, `ntfs` und `iso9660`. Welchen bzw. welche Dateisystemtypen Sie zurzeit verwenden, können Sie übrigens ganz leicht mit dem Kommando `df -T` feststellen.

Linux

»Linux-Dateisysteme« sind zur Installation und zum Betrieb von Linux geeignet. Im Alltagsbetrieb werden Sie gar nicht bemerken, mit welchem der im Folgenden aufgezählten Dateisystemtypen Sie arbeiten. Elementare Kommandos wie `ls` oder `cp`, die Verwaltung der Zugriffsrechte etc. – all das funktioniert unabhängig vom Dateisystem.

Die Dateisysteme unterscheiden sich durch Merkmale, die überwiegend für fortgeschrittene Anwender bzw. für den Server-Einsatz interessant sind: Geschwindigkeit beim Umgang mit sehr großen oder mit sehr vielen eher kleinen Dateien, Effizienz bei Schreib- und Lese-Operationen, CPU-Belastung, Journaling-Funktion (Verhalten nach einem Absturz), Quota-Funktion (die Möglichkeit, den maximalen Speicherver-

brauch pro Benutzer einzuschränken), NFS-Kompatibilität, Verwaltungs-Overhead, Unterstützung zusätzlicher Zugriffsrechte (ACL), Kompatibilität mit SELinux etc.

- **ext:** `ext2` (Extended Filesystem, Version 2) war in den Anfangszeiten von Linux das dominierende Linux-Dateisystem. Ab 2002 hat `ext3` seine Nachfolge angetreten. `ext3` ist zu `ext2` weitgehend kompatibel, unterstützt aber Journaling-Funktionen und ab Kernel 2.6 auch ACLs. Die maximale Dateigröße beträgt 2 TByte, die maximale Dateisystemgröße 8 TByte.

  Ende 2008 wurde `ext4` offiziell fertiggestellt. `ext4` ist aufwärtskompatibel zu `ext3`, viele Funktionen sind aber effizienter implementiert. Außerdem steigt die maximale Dateisystemgröße auf ein Exabyte (1.048.576 TByte), was für eine Weile reichen sollte ...
- **btrfs:** Wenn es nach dem Willen namhafter Kernelentwickler geht, ist `btrfs` das Linux-Dateisystem der Zukunft. Das mit der Unterstützung von Oracle von Grund auf neu entwickelte Dateisystem beinhaltet Device-Mapper-, Snapshot- und RAID-Funktionen und ist am ehesten mit Suns ZFS zu vergleichen. Leider ist `btrfs` noch nicht ausgereift.
- **xfs:** `xfs` kam ursprünglich als Dateisystem auf den Workstations der Firma SGI unter dem Betriebssystem IRIX zum Einsatz. Es eignet sich insbesondere für die Verwaltung sehr großer Dateien und ist beispielsweise ideal für Video-Streaming geeignet. Es unterstützt Quotas und erweiterte Attribute (ACLs). Das Dateisystem kann im laufenden Betrieb vergrößert werden. `xfs` wird voraussichtlich in RHEL 7 standardmäßig zum Einsatz kommen.
- **reiser:** `reiserfs`, dessen Name sich von seinem Initiator Hans Reiser ableitet, war das erste Dateisystem mit Journaling-Funktionen, das den Einzug in den Linux-Kernel schaffte. Das Dateisystem wird allerdings nicht mehr weiterentwickelt und kaum noch eingesetzt.
- **jfs:** `jfs` steht für Journaled File System. Es wurde ursprünglich von IBM entwickelt und später auf Linux portiert. `jfs` erreichte unter Linux nie große Popularität und fristet momentan ein Schattendasein unter den Linux-Dateisystemen:

  http://jfs.sourceforge.net

Das »beste« oder »schnellste« Dateisystem gibt es nicht – jede Wertung hängt vom Verwendungszweck ab. Meine Empfehlung geht in Richtung `ext4` sowohl für Desktop- als auch für Server-Installationen. Auch `ext3` ist nach wie vor eine gute Wahl, vor allem dann, wenn Ihnen ein unkomplizierter Datenaustausch mit Windows wichtig ist.

Unix

Falls Sie auf Ihrem Rechner ein zweites Unix-ähnliches Betriebssystem installiert haben, helfen die folgenden Dateisysteme beim Datenaustausch:

- **sysv:** Dieses Dateisystem wird von SCO-, Xenix- und Coherent-Systemen eingesetzt.
- **ufs:** Dieses Dateisystem wird von FreeBSD, NetBSD, NextStep und SunOS verwendet. Linux kann derartige Dateisysteme nur lesen, aber nicht verändern. Zum Zugriff auf BSD-Partitionen ist zusätzlich die BSD-disklabel-Erweiterung erforderlich. Eine analoge Erweiterung existiert auch für Sun-OS-Partitionstabellen.
- **ZFS:** ZFS ist ein Dateisystem, das Sun für Solaris entwickelt hat und nun Oracle gehört. Da der ZFS-Code nicht GPL-kompatibel ist, kann er nicht in den Linux-Kernel integriert werden. Es ist aber nicht schwierig, den Treiber als binäres Modul oder als Quellcode zu installieren. Weitere Informationen finden Sie hier:

  http://zfsonlinux.org

Windows, Mac OS X

Die folgenden Dateisysteme helfen beim Datenaustausch mit DOS-, Windows- und Macintosh-Systemen:

- **vfat:** Dieses Dateisystem wird von Windows 9x/ME sowie auf den meisten SD-Karten verwendet. Linux kann derartige Dateisysteme lesen und schreiben.
- **ntfs:** Dieses Dateisystem kommt unter allen aktuellen Windows-Versionen ab Windows NT zum Einsatz. Linux kann Dateien lesen und schreiben.
- **hfs und hfsplus:** Diese Dateisysteme werden auf Apple-Rechnern eingesetzt. Linux kann derartige Dateisysteme lesen und schreiben. Das Schreiben funktioniert allerdings nur, wenn die Dateisysteme unter OS X *ohne* Journaling-Funktionen eingerichtet wurden. Das ist in der Praxis freilich die Ausnahme und nur für den Datenaustausch zwischen OS X und Linux zweckmäßig.

CD-ROM/DVD

Auf Daten-CD-ROMs und DVDs werden üblicherweise eigene Dateisysteme verwendet:

- **iso9660:** Das Dateisystem für CD-ROMs wird durch die ISO-9660-Norm definiert. Diese Norm sieht allerdings nur kurze Dateinamen vor. Lange Dateinamen werden je nach Betriebssystem durch unterschiedliche Erweiterungen unterstützt (Rockridge, Joliet).
- **udf:** Als Nachfolger zu ISO 9660 hat sich das *Universal Disk Format* etabliert. Es kommt häufig bei DVDs zum Einsatz.

Netzwerkdateisysteme

Dateisysteme müssen sich nicht auf der lokalen Festplatte befinden – sie können auch über ein Netzwerk eingebunden werden. Der Linux-Kernel unterstützt diverse Netzwerkdateisysteme, von denen die folgenden vier am häufigsten zum Einsatz kommen:

- **nfs:** Das *Network File System* (NFS) ist das unter Unix wichtigste Netzwerkdateisystem.
- **smbfs/cifs:** Diese Dateisysteme ermöglichen das Einbinden von Windows- oder Samba-Netzwerkverzeichnissen in den Verzeichnisbaum.
- **sshfs:** Das eher selten eingesetzte Dateisystem `sshfs` ermöglicht es, über SSH erreichbare Verzeichnisse in den lokalen Verzeichnisbaum einzubinden.
- **coda:** Dieses Dateisystem ist am ehesten mit NFS vergleichbar. Es bietet eine Menge Zusatzfunktionen, ist aber nicht sehr verbreitet.
- **ncpfs:** Dieses Dateisystem basiert auf dem *Netware Core Protocol*. Es wird von Novell Netware eingesetzt.

Virtuelle Dateisysteme

Unter Linux gibt es eine Reihe von Dateisystemen, die nicht zum Speichern von Daten auf einer Festplatte oder einem anderen Datenträger gedacht sind, sondern lediglich zum Informationsaustausch zwischen dem Kernel und Anwendungsprogrammen. In `/proc/filesystems` sind diese Dateisysteme mit dem Begriff `nodev` gekennzeichnet. Im Folgenden werden nur die wichtigsten derartigen Dateisysteme kurz vorgestellt.

- **devpts:** Dieses Dateisystem ermöglicht via `/dev/pts/*` den Zugriff auf Pseudo-Terminals (kurz PTYs) gemäß der Unix-98-Spezifikation. Pseudo-Terminals emulieren eine serielle Schnittstelle und werden z. B. in Terminal-Fenstern eingesetzt.
- **proc und sysfs:** Das `proc`-Dateisystem dient zur Abbildung von Verwaltungsinformationen des Kernels bzw. der Prozessverwaltung. Ergänzend dazu bildet das `sysfs`-Dateisystem die Zusammenhänge zwischen dem Kernel und der Hardware ab. Die beiden Dateisysteme sind an den Positionen `/proc` und `/sys` eingebunden.
- **tmpfs:** Dieses Dateisystem ist die Basis für Shared Memory gemäß System V. Es wird zumeist an der Position `/dev/shm` eingebunden und ermöglicht einen effizienten Datenaustausch zwischen zwei Programmen. Bei vielen Distributionen werden die Verzeichnisse `/var/run` und `/var/lock` mit dem `tmpfs`-Dateisystem realisiert. Das ist schnell und stellt sicher, dass beim Ausschalten keine Dateien in `/var/run` oder `/var/lock` zurückbleiben können.
- **usbfs:** `usbfs` gibt ab Kernel 2.6 Informationen über die angeschlossenen USB-Geräte. Es ist üblicherweise in das `proc`-Dateisystem integriert (`/proc/bus/usb`).

Sonstige Dateisysteme

Abschließend folgen hier noch einige Dateisysteme bzw. Schlüsselwörter, die sich in die obigen Gruppen nicht einordnen lassen:

- **auto:** Ein `auto`-Dateisystem gibt es in Wirklichkeit gar nicht. `auto` darf aber in `/etc/fstab` bzw. bei `mount` zur Angabe des Dateisystems verwendet werden. Linux versucht dann, das Dateisystem selbst zu erkennen. Das funktioniert für die meisten wichtigen Dateisysteme.
- **autofs, autofs4:** Auch `autofs` und die neuere Variante `autofs4` sind keine eigenen Dateisysteme, sondern Kernelerweiterungen, die für die gerade benötigten Dateisysteme automatisch `mount` ausführen. Wird das Dateisystem eine Weile nicht mehr verwendet, wird ebenfalls automatisch `umount` ausgeführt. Dieses Verfahren bietet sich vor allem dann an, wenn von zahlreichen NFS-Verzeichnissen immer nur einige wenige aktiv genutzt werden.

  Intern wird dazu beim Systemstart das Programm `automount` gestartet. Das Programm ist beispielsweise bei Red Hat und Fedora standardmäßig installiert. `autofs` wird allerdings erst nach einer Konfiguration von `/etc/auto.master` bzw. `/etc/auto.misc` aktiv. Weitere Details finden Sie hier:

  http://tldp.org/HOWTO/Automount.html
- **cgroup:** Die sogenannten Control Groups ermöglichen es, die Nutzung von Ressourcen durch einzelne Prozesse zu steuern bzw. zu limitieren. Das virtuelle *Cgroup Filesystem* hilft dabei, die aktuellen Cgroup-Einstellungen auszulesen oder zu verändern. Die Grundlagen der Control Groups sind hier dokumentiert:

  http://www.kernel.org/doc/Documentation/cgroups/cgroups.txt
- **cramfs und squashfs:** Das *Cram Filesystem* und das *Squash Filesystem* sind Read-Only-Dateisysteme. Sie dienen dazu, möglichst viele Daten in komprimierter Form in ein Flash Memory bzw. in ein ROM (Read Only Memory) zu packen.
- **fuse:** Das *Filesystem in Userspace* (FUSE) ermöglicht es, Dateisystemtreiber außerhalb des Kernels zu entwickeln und zu nutzen. FUSE wird also immer zusammen mit einem externen Dateisystemtreiber eingesetzt. FUSE wird beispielsweise vom NTFS-Treiber `ntfs-3g` verwendet.
- **gfs und ocfs:** Das *Global File System* (GFS) und das *Oracle Cluster File System* (OCFS) ermöglichen den Aufbau riesiger, vernetzter Dateisysteme, auf die mehrere Rechner parallel zugreifen.
- **loop:** Das *Loopback-Device* ist ein Adapter, der eine gewöhnliche Datei wie ein Block-Device ansprechen kann. Damit können Sie in einer normalen Datei ein beliebiges Dateisystem unterbringen und mit `mount` in den Verzeichnisbaum einbinden. Die dazugehörige Kernelfunktion *Loopback Device Support* ist im Modul `loop` realisiert. Das Loopback-Devices wird z. B. für die Erstellung einer Initial-

RAM-Disk für GRUB, für die Realisierung von verschlüsselten Dateisystemen oder zum Testen von ISO-Images verwendet.

- **none:** Naturgemäß ist auch `none` kein Dateisystem. Es besteht aber die selten genutzte Möglichkeit, ein lokales Verzeichnis an einem anderen Ort in den Verzeichnisbaum einzubinden. Dabei geben Sie bei `mount` bzw. in `/etc/fstab` als Dateisystemtyp `none` und als zusätzliche Option `bind` an. Die Wirkung ist ähnlich wie bei einem symbolischen Link, die interne Realisierung aber vollkommen anders. Diese Vorgehensweise ist z. B. bei der Konfiguration eines NFS4-Servers zweckmäßig.
- **unionfs/aufs:** Das Konzept von `unionfs` bzw. dessen Variante `aufs` ermöglicht es, mehrere Dateisysteme quasi übereinanderzulegen, wobei das oberste Dateisystem Vorrang hat. `unionfs` und `aufs` kommen bei manchen Live-Systemen zur Anwendung: Linux startet direkt von der CD oder DVD. Dem Read-Only-Dateisystem der CD/DVD wird ein RAM-Disk-Dateisystem übergestülpt, in dem Änderungen durchgeführt werden können. Nach außen hin ist nur ein Dateisystem sichtbar, das sich aus der Grundstruktur der CD/DVD und den in der RAM-Disk durchgeführten Änderungen ergibt.
- **Verschlüsselte Dateisysteme:** Linux kennt verschiedene Verfahren, um den Inhalt von Dateisystemen zu verschlüsseln. Einige dieser Verfahren basieren direkt auf eigenen Dateisystemen (z. B. CryptoFS oder eCryptfs). Verbreiteter ist allerdings die Kombination von LVM und Verschlüsselung.

Welche Dateisysteme direkt in den laufenden Kernel integriert bzw. zurzeit als Modul geladen sind, können Sie der Datei `/proc/filesystems` entnehmen. Welche Kernelmodule für weitere Dateisysteme darüber hinaus noch zur Verfügung stehen, sehen Sie im Verzeichnis `/lib/modules/`*n*`/kernel/fs/`.

25.5 Verwaltung des Dateisystems (mount und /etc/fstab)

Nach der Installation von Linux müssen Sie sich normalerweise nicht um die Verwaltung des Dateisystems kümmern: Über diverse Verzeichnisse können Sie auf alle oder zumindest die meisten Datenpartitionen der Festplatte zugreifen. Beim Einlegen von CDs oder DVDs bzw. beim Anschließen externer Datenträger werden deren Dateisysteme automatisch in den Verzeichnisbaum integriert. Alles funktioniert gleichsam wie von Zauberhand.

Dieser Abschnitt wirft einen Blick hinter die Kulissen und beschreibt die Kommandos `mount` und `umount` sowie die Datei `/etc/fstab`:

- `mount` bzw. `umount` werden immer dann ausgeführt, wenn eine Partition oder ein Datenträger in den Verzeichnisbaum integriert bzw. wieder daraus gelöst wird. Selbstverständlich können Sie diese Kommandos als `root` auch selbst ausführen, wenn die Automatismen versagen bzw. wenn Sie ohne ein grafisches Desktop-System arbeiten.
- Die Konfigurationsdatei `/etc/fstab` steuert, welche Dateisysteme beim Rechnerstart automatisch in den Verzeichnisbaum integriert werden und welche Optionen dabei gelten. `/etc/fstab` wird während der Linux-Installation vorkonfiguriert. Wenn Sie mit dieser Konfiguration nicht zufrieden sind bzw. wenn sich später Ihre Anforderungen ändern, müssen Sie die Datei mit einem Editor verändern. Dieser Abschnitt beschreibt die Syntax dieser Datei.

Überraschenderweise gibt es nur wenige grafische Konfigurationswerkzeuge, die anstelle von `mount` bzw. statt einer manuellen Änderung von `/etc/fstab` eingesetzt werden können. Zu den wenigen Ausnahmen zählen das im vorigen Abschnitt kurz vorgestellte Programm *Gnome Disks* sowie das YaST-Modul System • Partitionieren (SUSE).

Einen Sonderfall stellen externe Datenträger wie USB-Memorysticks oder Firewire-Festplatten dar: Die meisten Distributionen binden solche Datenträger automatisch in das Dateisystem ein, sobald sie mit dem Rechner verbunden werden. Details zum Umgang mit externen Datenträgern folgen in Abschnitt 25.12.

Aktuellen Zustand des Dateisystems ermitteln

df

Wenn Sie wissen möchten, wie Ihr Linux-System zurzeit organisiert ist, führen Sie am einfachsten das Kommando `df -h` aus. Dieses Kommando zeigt an, an welcher Stelle im Dateisystem Festplatten, Datenträger etc. eingebunden sind und wie viel Platz auf den einzelnen Festplatten noch frei ist.

mount

Das Kommando `mount` ohne weitere Optionen liefert noch detailliertere Informationen über die eingebundenen Dateisysteme. Außerdem zeigt das Kommando alle aktiven `mount`-Optionen. Leider gehen die wirklich interessanten Einträge im Ergebnis oft zwischen unzähligen virtuellen Dateisystemen unter. Im folgenden Beispiel wurde die Ausgabe spaltenweise eingerückt, um die Lesbarkeit zu verbessern.

```
user$  mount
/dev/mapper/vg-ubuntu on /              type ext4     (rw,errors=remount-ro)
/dev/mapper/vg-myhome on /myhome        type ext4     (rw)
/dev/mapper/vg-virt   on /virt          type ext4     (rw)
/dev/sda3             on /boot          type ext3     (rw)
cgroup                on /sys/fs/cgroup type tmpfs    (rw,relatime,mode=755)
proc                  on /proc          type proc     (rw)
udev                  on /dev           type devtmpfs (rw,mode=0755)
```

```
tmpfs                   on /run           type tmpfs    (rw,noexec,nosuid,...)
none                    on /run/lock      type tmpfs    (rw,noexec,nosuid,...)
none                    on /run/shm       type tmpfs    (rw,nosuid,nodev)
...
```

Ähnliche Informationen wie `mount` liefern auch die Dateien `/etc/mtab` und `/proc/mounts`. Sie enthalten jeweils eine Liste aller Datenträger, die momentan eingebunden sind, zusammen mit dem Dateisystemtyp und den verwendeten `mount`-Optionen. `/etc/mtab` ändert sich jedes Mal, wenn ein Dateisystem in den Verzeichnisbaum eingebunden oder aus ihm gelöst wird. Die Syntax in `mtab` ist dieselbe wie in `/etc/fstab` (siehe unten). `/proc/mounts` enthält darüber hinaus auch Optionen, die in `/etc/fstab` bzw. beim `mount`-Kommando nicht explizit angegeben wurden.

Dateisysteme manuell einbinden und lösen (mount und umount)

Nach der Installation einer aktuellen Linux-Distribution ist das System so konfiguriert, dass Sie `mount` nur sehr selten benötigen: Alle Linux-Dateisysteme sind in den Verzeichnisbaum eingebunden. Beim Einlegen von CDs/DVDs oder beim Anschließen externer Datenträger erscheint automatisch ein neues Fenster des KDE- oder Gnome-Datei-Managers. Auch wenn es vielleicht so aussieht, als würde das Ganze wie von Zauberhand funktionieren, wird hinter den Kulissen immer wieder das Kommando `mount` ausgeführt, um Dateisysteme in den Verzeichnisbaum einzubinden bzw. wieder daraus zu lösen.

Die Syntax von `mount` sieht folgendermaßen aus:

```
mount [optionen] device verzeichnis
```

In den Optionen wird unter anderem der Dateisystemtyp angegeben (`-t xxx`). Der Device-Name bezeichnet die Partition bzw. das Laufwerk (siehe Abschnitt 25.2). Als Verzeichnis kann ein beliebiges Verzeichnis des aktuellen Dateisystems angegeben werden. Dieses Verzeichnis muss bereits existieren. Erzeugen Sie es gegebenenfalls mit `mkdir`!

`mount` kann im Regelfall nur von `root` ausgeführt werden. Es besteht aber die Möglichkeit, dass `/etc/fstab` für einzelne Partitionen allen Benutzern erlaubt, `mount` auszuführen (Option `user` bzw. `users`).

Beispiele

Am einfachsten ist `mount` anhand einiger Beispiele zu verstehen: Das erste Beispiel ermöglicht den Zugriff auf die Daten einer Windows-Partition über das Verzeichnis `/windows`:

```
root#  mkdir /windows
root#  mount -t ntfs /dev/sda2 /windows
```

Das folgende Kommando bindet das CD-ROM-Laufwerk mit einer Daten-CD (ISO-9660-Dateisystem) im Verzeichnis `/media/cdrom` in das Dateisystem ein. Das Device `/dev/scd0` bedeutet, dass das Beispiellaufwerk über das SCSI-System des Kernels angesprochen wird. Je nach Distribution müssen Sie stattdessen das Device `/dev/sr0` angeben.

```
root#  mount -t iso9660 /dev/scd0 /media/cdrom
```

Wenn die Parameter für das CD-ROM-Laufwerk (Dateisystemtyp, Device-Name, Verzeichnis) in `/etc/fstab` eingetragen sind, reicht auch das folgende Kommando zum Einbinden des Laufwerks in den Verzeichnisbaum:

```
root#  mount /media/cdrom
```

remount

Mit `mount -o remount` können Sie Optionen eines bereits eingebundenen Dateisystems verändern. Das folgende Kommando aktiviert beispielsweise die `exec`-Option für eine DVD, sodass darauf enthaltene Programme ausgeführt werden können:

```
root#  mount /media/dvd -o remount,exec
```

Falls beim Einbinden der Systempartition während des Rechnerstarts Probleme auftreten, wird die Partition nur read-only eingebunden. Um die Fehlerursache – etwa einen falschen Eintrag in `/etc/fstab` – zu beheben, ist es aber oft erforderlich, Änderungen im Dateisystem durchzuführen. Dazu führen Sie das folgende Kommando aus. Mit ihm wird die Systempartition neu eingebunden, wobei jetzt auch Schreibzugriffe möglich sind.

```
root#  mount -o remount,rw /
```

umount

Um ein Dateisystem aus dem Verzeichnisbaum zu lösen, führen Sie `umount` aus:

```
root#  umount /media/dvd
```

Dateisysteme automatisch einbinden (/etc/fstab)

Es wäre sehr mühsam, wenn Sie nach jedem Systemstart diverse Partitionen neu einbinden müssten, bei jedem CD-Wechsel `mount` mit allen Optionen angeben müssten etc. Der Schlüssel zur Arbeitserleichterung heißt `/etc/fstab`: Diese Datei gibt an, welche Datenträger beim Systemstart in das Dateisystem aufgenommen werden. Auf jeden Fall muss `fstab` die Systempartition sowie alle zur internen Verwaltung notwendigen Dateisysteme enthalten.

Beispiel

Je nach Distribution kann eine minimale `fstab`-Datei wie folgt aussehen:

```
# zwei Beispielzeilen in /etc/fstab
/dev/sda2   /       ext4    defaults    1 1
none        /proc   proc    defaults    0 0
...
```

Durch die erste Zeile wird die zweite Partition der ersten Festplatte als Systemverzeichnis genutzt. Je nachdem, auf welcher Festplattenpartition Sie Linux installiert haben, müssen Sie statt `sda2` natürlich den Device-Namen Ihrer Linux-Partition angeben!

Mit der zweiten Zeile wird das System zur Prozessverwaltung in das Dateisystem eingebunden. Die Dateien und Verzeichnisse des `/proc`-Verzeichnisses existieren nicht tatsächlich auf der Festplatte; es handelt sich nur um ein Abbild von Daten, die kernelintern verwaltet werden.

Die Syntax in /etc/fstab

Aus den obigen Beispielen geht bereits das prinzipielle Format von `fstab` hervor: Jede Zeile beschreibt in sechs Spalten einen Datenträger (eine Partition, ein Dateisystem).

Erste Spalte

Die erste Spalte enthält den Device-Namen des Datenträgers. Informationen zur Nomenklatur für Festplattenpartitionen finden Sie in Abschnitt 25.2. Weitere Beispiele für Linux- und Windows-Partitionen, CD-ROM-Laufwerke etc. folgen im weiteren Verlauf dieses Kapitels.

Statt des Device-Namens können Sie auch den *Volume Name* (so üblich bei Red Hat und Fedora) oder die ID-Nummer des Dateisystems angeben (z. B. bei Ubuntu). Die korrekte Syntax lautet in diesem Fall `LABEL=zeichenkette` oder `UUID=nnn-nnn`. Mit `blkid` ermitteln Sie den Partitionsnamen und die UUID einer Partition. Um diese Daten zu ändern, setzen Sie je nach Dateisystem unterschiedliche Werkzeuge ein, beispielsweise `tune2fs`.

```
root#  blkid /dev/sda9
/dev/sda9: UUID="5a954fc1-00c6-4c25-a943-d4220eff350d" TYPE="ext4"
```

Der Vorteil von Labels oder UUIDs im Vergleich zu Device-Namen besteht darin, dass die Angabe selbst dann noch korrekt ist, wenn sich der Device-Name geändert hat. Das kann insbesondere bei USB-Datenträgern leicht passieren: Je nachdem, welche Datenträger vorher verwendet wurden, kann es durchaus sein, dass die externe Festplatte einmal unter `/dev/sdc` und das nächste Mal unter `/dev/sde` angesprochen wird.

Leider wird `fstab` insbesondere bei der Verwendung von UUIDs sehr unübersichtlich. Probleme kann es auch geben, wenn mehrere Linux-Distributionen parallel installiert werden. In der Regel werden bei jeder Installation einzelne Partitionen neu formatiert. Sie erhalten bei dieser Gelegenheit neue UUIDs. Die bisher installierten Distributionen kennen diese Partitionen nun nicht mehr, und `fstab` muss mühsam an die neuen UUIDs angepasst werden.

Zweite Spalte

Die zweite Spalte gibt an, bei welchem Verzeichnis der Datenträger in den Dateibaum eingebunden wird. Die in der zweiten Spalte angegebenen Verzeichnisse müssen bereits existieren. Die Verzeichnisse müssen nicht leer sein, allerdings können Sie nach dem Einbinden des Dateisystems auf die darin enthaltenen Dateien nicht mehr zugreifen, sondern nur auf die Dateien des eingebundenen Datenträgers.

Dritte Spalte

Die dritte Spalte gibt das Dateisystem an. Tabelle 25.5 listet in alphabetischer Reihenfolge die wichtigsten Dateisysteme auf.

Dateisystem	Verwendung
`auto`	Dateisystem automatisch erkennen (CD-ROMs, Disketten)
`btrfs`	`btrfs`-Dateisystem
`cifs`	Windows-Netzwerkverzeichnis (Samba)
`devpts`	Pseudo-Terminals gemäß Unix-98-Spezifikation
`ext2, -3, -4`	`ext`-Dateisystem Version 2, 3 und 4
`iso9660`	CD-ROMs, DVDs
`nfs`	Unix-Netzwerkverzeichnis (NFS)
`ntfs`	Windows-Dateisystem
`proc`	Prozessverwaltung (`/proc`)
`reiserfs`, `reiser4`	`reiser`-Dateisystem Version 3.*n* bzw. 4
`smbfs`	Windows-Netzwerkverzeichnis (Samba)
`swap`	Swap-Partitionen oder -Dateien
`sysfs`	Systemverwaltung (`/sys`)
`tmpfs`	Datenaustausch zwischen Programmen (System V Shared Memory)
`udf`	Universal Disk Format (DVDs, CD-RWs)
`usbfs`	Verwaltung von USB-Geräten
`vfat`	Windows-9x/ME-Dateisystem

Tabelle 25.5 Dateisysteme

Es ist auch zulässig, mehrere Dateisysteme durch Kommas getrennt anzugeben. Beispielsweise bietet sich `iso9660,udf` für CD- und DVD-Laufwerke an, weil für CDs und DVDs in der Regel nur diese beiden Dateisysteme infrage kommen. `mount` entscheidet sich zwischen den zur Auswahl stehenden Systemen automatisch für das richtige. Achten Sie darauf, dass die Dateisystemnamen nicht durch Leerzeichen getrennt werden dürfen!

Vierte Spalte

Die vierte Spalte bestimmt Optionen für den Zugriff auf den Datenträger. Mehrere Optionen werden durch Kommata getrennt. Abermals dürfen keine Leerzeichen eingefügt werden! Tabelle 25.6 zählt die wichtigsten universellen `mount`-Optionen auf. Wenn Sie gar keine Option nutzen möchten, geben Sie `defaults` an.

Option	Bedeutung
`defaults`	Standardoptionen verwenden
`dev`	Kennzeichnung von Character- oder Block-Devices auswerten
`discard`	SSD-Trim aktivieren (`ext4`, `btrfs`, `xfs` und `swap`)
`exec`	Programmausführung zulassen (z. B. für CD/DVD-Laufwerke)
`noauto`	Datenträger nicht beim Systemstart einbinden
`nodev`	Kennzeichnung von Character- oder Block-Devices ignorieren
`noexec`	keine Programmausführung erlaubt
`nosuid`	Suid- und Guid-Zugriffsbits nicht auswerten
`ro`	Read Only (Schreibschutz)
`sw`	Swap (Swap-Datei oder -Partition)
`suid`	Suid- und Guid-Zugriffsbits auswerten
`sync`	Schreibzugriffe nicht puffern (sicherer, aber langsamer)
`owner`	Der Besitzer darf `(u)mount` ausführen.
`user`	Jeder darf `mount` ausführen, aber nur der Benutzer des letzten `mount`-Aufrufs darf `umount` ausführen.
`users`	Jeder darf `mount` und `umount` ausführen.

Tabelle 25.6 mount-Optionen

Fünfte Spalte

Die fünfte Spalte enthält Informationen für das Programm `dump` und wird zurzeit ignoriert. Es ist üblich, für die Systempartition 1 und für alle anderen Partitionen oder Datenträger 0 einzutragen.

Sechste Spalte

Die sechste Spalte gibt an, ob und in welcher Reihenfolge die Dateisysteme beim Systemstart überprüft werden sollen. Oft wird 1 für die Systempartition und 0 für alle anderen Partitionen eingetragen. Das bedeutet, dass beim Rechnerstart nur die Systempartition auf Fehler überprüft und gegebenenfalls repariert wird.

Falls Sie möchten, dass weitere Partitionen automatisch überprüft werden, geben Sie bei diesen Partitionen die Ziffer 2 an, d. h., die Überprüfung soll nach der Kontrolle der Systempartition erfolgen. Wenn Einträge in der fünften und sechsten Spalte in `/etc/fstab` fehlen, wird 0 angenommen.

25.6 Dateisystemgrundlagen

Im Mittelpunkt der folgenden Seiten stehen die Linux-Dateisysteme `ext2`, `ext3`, `ext4`, `btrfs` und `xfs`. Bevor ich deren Einrichtung und Administration beschreibe, gibt dieser Abschnitt einige Grundlageninformationen, die unabhängig vom Dateisystemtyp sind.

Journaling

Alle gängigen Linux-Dateisysteme unterstützen Journaling-Funktionen. In seiner einfachsten Form bedeutet Journaling, dass der Beginn und das Ende jeder Dateioperation in einer speziellen Datei mitprotokolliert werden. Dank des Protokolls kann später geprüft werden, ob eine bestimmte Dateioperation vollständig ausgeführt wurde. Wenn das nicht der Fall ist, kann die Operation widerrufen werden. In der Datenbankwelt spricht man hier von Transaktionen.

Bei fortgeschrittenen Journaling-Systemen besteht die Möglichkeit, die eigentlichen Änderungen an den Dateien im Journal zu protokollieren. Das verlangsamt den gewöhnlichen Betrieb, gibt aber mehr Möglichkeiten zur späteren Rekonstruktion.

Wenn nun eine Dateioperation nicht vollständig abgeschlossen werden kann, geht dies aus dem Protokoll hervor. Bei einfachem Journaling sind die Änderungen zwar verloren, der bisherige Zustand der Datei steht aber zumeist noch zur Verfügung. Versprechen Sie sich also keine Wunder von der Journaling-Funktion!

Der große Vorteil der Journaling-Funktionen besteht darin, dass das Dateisystem beim nächsten Rechnerstart sehr rasch wieder in einen konsistenten Zustand gebracht und beinahe sofort wieder genutzt werden kann. Das ist ein großer Unterschied im Vergleich zu früher, wo nach einem Absturz oder Stromausfall das gesamte Dateisystem systematisch nach eventuellen Fehlern durchsucht werden musste. Das dauerte mehrere Minuten, bei sehr großen Festplatten eventuell sogar Stunden!

Datenverluste trotz Journaling

Bei einem Stromausfall gibt auch Journaling keine Garantie für ein konsistentes Dateisystem! Das Problem liegt bei den Festplatten bzw. SSDs: Diese verwenden aus Effizienzgründen beim Schreiben einen internen Zwischenspeicher. Daher kann es passieren, dass das Dateisystem vom Datenträger die Bestätigung erhält, dass er die Daten empfangen und gesichert hat. Tatsächlich kann es danach aber noch Sekunden dauern, bis die Daten vom Zwischenspeicher physikalisch auf die Festplatte geschrieben werden. Bei SSDs ist diese Zeitspanne viel kürzer, aber das ändert nichts am prinzipiellen Problem.

Tritt in dieser Zeitspanne ein Stromausfall auf, gehen die Daten im Zwischenspeicher verloren. Bei manchen Festplatten lässt sich dieser Cache deaktivieren. Dadurch verringert sich die Geschwindigkeit von Schreiboperationen aber derart, dass in der Praxis zumeist darauf verzichtet wird.

Unabhängig vom Schreib-Cache ist das Verhalten einer Festplatte während eines plötzlichen Stromausfalls undefiniert. Es kann also auch passieren, dass die Festplatte statt Ihrer Daten Zufallsbits schreibt, bevor der Schreibkopf in Sicherheit gebracht wird. Eine Diskussion zu diesem Thema finden Sie hier:

http://lwn.net/Articles/191352

Anders formuliert: Journaling-Dateisysteme sind eine feine Sache, schließen einen Datenverlust bei einem Stromausfall aber nicht aus. Wenn Ihnen Ihre Daten etwas wert sind, investieren Sie 100 EUR für eine kleine UPS-Anlage (*Uninterruptable Power Supply*), die sicherstellt, dass Sie Ihre Rechner auch bei einem Stromausfall geordnet herunterfahren können.

Automatische Überprüfung des Dateisystems

Wenn Linux beim Starten erkennt, dass der Rechner zuletzt nicht ordnungsgemäß heruntergefahren wurde, führt es für die Systempartition und je nach Konfiguration auch für andere in `/etc/fstab` genannte Partitionen eine Überprüfung des Dateisystems durch. Ob eine Überprüfung stattfindet oder nicht, entscheidet die sechste Spalte in `/etc/fstab` – siehe auch Abschnitt 25.5. Dank der Journaling-Funktionen ist diese Überprüfung normalerweise blitzschnell erledigt.

Davon losgelöst sehen einige Dateisysteme (unter anderem `ext` in allen Versionen) eine regelmäßige Überprüfung des Dateisystems auf Konsistenzfehler vor. Diese relativ zeitaufwendigen Tests erfolgen beim Start des Rechners, wenn seit dem letzten Test eine bestimmte Zeitspanne oder Anzahl von `mount`-Vorgängen überschritten wurde.

Nach der Einführung der Journaling-Funktionen wurde vielfach argumentiert, der regelmäßige Konsistenztest sei jetzt überflüssig. Das stimmt aber leider nicht ganz: Ein Dateisystem kann auch durch Hardware-Fehler der Festplatte inkonsistent werden – und die Wahrscheinlichkeit solcher Fehler steigt mit der zunehmenden Festplattengröße!

Beispielsweise habe ich im Datenblatt meiner 1-TByte-Festplatte die Angabe gefunden, dass die Wahrscheinlichkeit für Bitfehler (*Nonrecoverable Read Errors per Bits Read*) kleiner als 1 zu 10^{15} ist. Das klingt wirklich vernachlässigbar. Wenn Sie allerdings in Rechnung stellen, dass auf dieser Festplatte 8×10^{12} Bits Platz finden, wird klar, dass Datenfehler im regulären Betrieb – also ohne irgendwelche Beschädigungen – sehr wohl zu erwarten sind. Ein regelmäßiger Konsistenztest des Dateisystems kann diese Fehler zwar nicht verhindern, bietet aber eine gewisse Chance, ein Fehlverhalten festzustellen und zu korrigieren, zumindest dann, wenn für die interne Verwaltung des Dateisystems kritische Bereiche betroffen sind.

Wirklich fehlertolerant sind die in diesem Buch vorgestellten Dateisysteme leider alle nicht. Dateisysteme, die durch Prüfsummen Hardware-Fehler erkennen bzw.

durch redundante Speicherung derartige Fehler sogar korrigieren können, sind momentan aber ein heißes Forschungsgebiet. Eine ausgezeichnete Einführung in die Welt der Dateisysteme geben die beiden folgenden Artikel:

http://lwn.net/Articles/190222
http://lwn.net/Articles/196292

Zurück zur Dateisystemüberprüfung während des Rechnerstarts: Details der Steuerung dieses Prozesses sind wie so oft distributionsabhängig. Im Regelfall erfolgt die Überprüfung ohne Benutzerinteraktion und verlangsamt lediglich den Boot-Prozess. Wirklich unangenehm wird es erst, wenn bei der Überprüfung nicht korrigierbare Fehler festgestellt werden. In diesem Fall wird die Partition im Read-Only-Modus geladen. Nach einem `root`-Login können Sie nun manuell die Dateisystemüberprüfung wiederholen und interaktiv angeben, wie das Überprüfungsprogramm mit defekten Daten umgehen soll. Im Regelfall sollte es so gelingen, das Dateisystem zumindest wieder in einen konsistenten Zustand zu bringen, auch wenn möglicherweise einzelne Dateien nicht zu retten sind. Anschließend müssen Sie den Rechner neu starten.

Manuelle Überprüfung des Dateisystems

Eine manuelle Überprüfung können Sie einfach mit dem Kommando `fsck` durchführen. Die betreffende Partition darf während der Kontrolle allerdings nicht verwendet werden, d. h., Sie müssen vorher `umount` ausführen.

Die Systempartition können Sie im laufenden Betrieb allerdings nicht überprüfen, weil Sie das Dateisystem nicht mit `umount` abmelden können. Stattdessen führen Sie als `root` das Kommando `touch /forcefsck` aus und starten den Rechner neu. Die Datei `forcefsck` wird auch erzeugt, wenn Sie `shutdown` mit der zusätzlichen Option `-F` ausführen.

Wenn die Datei `/forcefsck` existiert, wird bei fast allen Distributionen beim nächsten Start automatisch eine Überprüfung des Dateisystems durchgeführt. Sollte das nicht funktionieren, fahren Sie den Rechner mit einem Rescue-System oder mit einer Live-CD (Knoppix) hoch und führen `fsck` von dort aus.

Größenlimits

In der Vergangenheit tauchte immer wieder die Frage auf, wie groß Dateien maximal sein dürfen. Die Antwort hängt davon ab, welchen Kernel, welche CPU-Architektur, welche glibc-Bibliothek und welches Dateisystem Sie verwenden. Aktuelle Distributionen unterstützen durchweg die LFS-Erweiterungen in der glibc-Bibliothek. LFS steht dabei für *Large Filesystem Support*. Die Dateigröße ist dank LFS mit 2^{63} Byte nahezu unbegrenzt. Zum anderen geben aber auch die verschiedenen Dateisystemtypen Limits für die maximale Datei(system)größe vor. Tabelle 25.7 fasst die Daten zusammen. Dabei gilt: 1 TByte (Terabyte) = 1024 GByte.

Dateisystem	Maximale Dateigröße	Maximale Dateisystemgröße
btrfs	16.777.216 TByte	16.777.216 TByte
ext3	2 TByte	32 TByte (bei 8 kByte Blockgröße)
ext4	16 TByte	1.048.576 TByte = 1 Exabyte
xfs	9.437.184 TByte	9.437.184 TByte
ZFS	16.777.216 TByte	16.777.216 TByte

Tabelle 25.7 Maximale Dateisystemgröße

Beachten Sie, dass Sie zum Anlegen von ext4-Dateisystemen mit mehr als 16 TByte zumindest die seit November 2011 verfügbare Version 1.42 der e2fsprogs benötigen.

Änderung des Dateisystemtyps

Für die meisten Fälle gibt es keine Werkzeuge zur Umwandlung eines Dateisystemtyps, z. B. von ext4 nach xfs. Zu den wenigen Ausnahmen zählt btrfs-convert zur Konvertierung von ext3/-4 nach btrfs. Wenn es kein derartiges Kommando gibt, müssen Sie das gewünschte Dateisystem in einer neuen Partition anlegen und dann alle Dateien dorthin kopieren.

25.7 Das ext-Dateisystem (ext2, ext3, ext4)

Versionen

Die verschiedenen ext-Versionen dominieren die Welt der Linux-Dateisysteme. Kurz ein historischer Rückblick:

- ext, also die erste Version des ext-Dateisystems, wurde nur kurz in der Anfangsphase von Linux eingesetzt (1992). Die maximale Dateisystemgröße betrug 2 GByte.
- ext2 war von 1993 bis ca. 2001 das dominierende Linux-Dateisystem. Die maximale Dateisystemgröße wuchs in dieser Version auf 8 TByte.
- Die wichtigsten Neuerungen in ext3 waren die Journaling-Funktionen und die ACL-Unterstützung (ab Kernel 2.6). Der Siegeszug von ext3 ab 2002 war nicht zuletzt durch die vollständige Kompatibilität bedingt: Vorhandene ext2-Dateisysteme mussten nicht neu formatiert werden, sondern konnten mit minimalem Aufwand auf ext3 umgestellt werden. Sofern das Dateisystem ordnungsgemäß mit umount gelöst wird, kann es anschließend sogar wieder als ext2-Dateisystem genutzt werden.
- Ende 2008 wurde das Dateisystem ext4 offiziell fertiggestellt. Fast alle aktuellen Distributionen verwenden ext4 jetzt als Standarddateisystem.

Die maximale Dateisystemgröße steigt in ext4 auf ein Exabyte (1.048.576 Terabyte), und der Zeitpunkt von Dateiänderungen wird genauer als bisher protokolliert. Extents ermöglichen es, aneinanderliegende Blöcke des Dateisystems als Gruppen anzusprechen, was den Aufwand zur Verwaltung großer Dateien deutlich senkt. Außerdem wurden eine Menge Geschwindigkeitsoptimierungen durchgeführt: Sowohl das Löschen großer Dateien als auch die Dateisystemüberprüfung wird nun um ein Vielfaches schneller als bei ext3 durchgeführt.

Abermals wurde auf Kompatibilität geachtet: Eine Migration von ext3 zu ext4 ist problemlos möglich. Beachten Sie aber, dass es diesmal nach einer Umstellung von ext3 auf ext4 kein Zurück mehr gibt!

Die Kompatibilität der verschiedenen ext-Dateisystemversionen drückt sich auch dadurch aus, dass diverse Administrationswerkzeuge weiterhin die Versionsnummer 2 im Kommandonamen haben, obwohl sie auch für neuere Versionen eingesetzt werden können, z. B. tune2fs oder resize2fs.

Die ext-Entwicklung steht seit der Veröffentlichung von ext4 keineswegs still. Es gibt zwar momentan keine Pläne für ext5, es werden aber laufend neue Funktionen in ext4 eingebaut, zuletzt z. B. Prüfsummen für Metadaten. Über den aktuellen Stand der Entwicklung berichtet regelmäßig *lwn.net*, z. B. mit diesem Artikel:

http://lwn.net/Articles/469805

Einträge für ext3/ext4-Dateisysteme in /etc/fstab sehen üblicherweise so wie im folgenden Beispiel aus: /etc/fstab

```
# /etc/fstab: Linux-Dateisysteme
/dev/sdb8   /          ext4   defaults        1 1
/dev/sdb9   /boot      ext3   defaults        0 0
/dev/sdb9   /data      ext4   acl,user_xattr  0 0
```

Journaling

Das ext-Dateisystem unterstützt seit Version 3 Journaling-Funktionen. Die Journaling-Datei verwendet normalerweise spezielle Inodes und ist daher im Dateisystem nicht sichtbar. Sie enthält nur Informationen über Dateien, die noch nicht vollständig auf der Festplatte gespeichert wurden. Sobald die Änderungen ausgeführt sind, gilt der Eintrag als *committed* und kann durch neue Journaleinträge überschrieben werden. Es ist möglich (aber unüblich), die Journaling-Datei in einem eigenen Device anzulegen.

Das ext-Dateisystem kennt drei verschiedene Verfahren, wie das Journaling durchgeführt wird:

- data=ordered: Bei diesem Modus werden im Journal nur Metadaten gespeichert, also Informationen *über* Dateien, aber keine Inhalte. Im Journal werden Dateien erst dann als korrekt (*committed*) gekennzeichnet, wenn sie vollständig auf der Festplatte gespeichert worden sind. Nach einem Crash kann das Dateisystem sehr rasch wieder in einen konsistenten Zustand gebracht werden, weil alle unvollständig gespeicherten Dateien anhand des Journals sofort erkannt werden. Es ist aber nicht möglich, unvollständig gespeicherte Dateien wiederherzustellen.

  Im Modus data=ordered wird das Journal alle fünf Sekunden mit der Festplatte synchronisiert. Bei ext3 hat das zur Folge, dass sämtliche Änderungen an irgendwelchen Dateien innerhalb von fünf Sekunden physikalisch auf der Festplatte gespeichert werden. Dieses Standardverhalten ist zwar nicht besonders effizient, dafür aber sehr sicher: Selbst bei Totalabstürzen und Stromausfällen sind massive Datenverluste äußerst selten. data=ordered hat bei ext3 eine unerfreuliche Nebenwirkung: Bei jedem Aufruf der fsync-Funktion wird nicht nur eine bestimmte Datei, sondern das gesamte Dateisystem synchronisiert. Das kann zu spürbaren Verzögerungen führen.

  Bei ext4 wird das Journal zwar ebenfalls alle fünf Sekunden synchronisiert, die Datenänderungen werden aber aufgrund der *Delayed Allocation* (siehe unten) oft erst viel später gespeichert. Nur ein expliziter Aufruf der fsync-Funktion stellt die sofortige physikalische Speicherung einer Datei sicher! Glücklicherweise erfordert fsync bei ext4 nicht, dass das gesamte Dateisystem synchronisiert werden muss. Die Funktion wird daher wesentlich schneller ausgeführt.

- data=writeback: Dieser Modus ähnelt dem ordered-Modus. Der einzige Unterschied besteht darin, dass das Journal und die Dateioperationen nicht immer vollständig synchron sind. Das Dateisystem wartet mit den *committed*-Einträgen im Journal nicht auf den Abschluss der Speicheroperation auf der Festplatte. Damit ist das Dateisystem etwas schneller als im ordered-Modus. Nach einem Crash ist die Integrität des Dateisystems weiterhin sichergestellt. Allerdings kann es vorkommen, dass veränderte Dateien alte Daten enthalten. Dieses Problem tritt nicht auf, wenn Anwendungsprogramme – wie im POSIX-Standard vorgesehen – den Speichervorgang mit fsync abschließen (siehe oben).

- data=journal: Im Gegensatz zu den beiden anderen Modi werden jetzt im Journal auch die tatsächlichen Daten gespeichert. Dadurch müssen alle Änderungen *zweimal* gespeichert werden (zuerst in das Journal und dann in die betroffene Datei). Deswegen ist ext3 in diesem Modus deutlich langsamer. Dafür können nach einem Crash Dateien wiederhergestellt werden, deren Änderungen bereits vollständig in das Journal (aber noch nicht in die Datei) eingetragen worden sind.

Grundsätzlich wird das Journal alle fünf Sekunden physikalisch auf der Festplatte gespeichert. Diese Zeitspanne kann durch die `mount`-Option `commit` verändert werden. Wenn das Paket `laptop-mode` installiert und konfiguriert ist und ein Notebook im Batteriebetrieb läuft, ist die `commit`-Zeitspanne wesentlich höher.

Intern kümmert sich der in den Kernel integrierte Journaling-Dämon `kjournald` um die regelmäßige Aktualisierung der Journaling-Datei. Dieser Prozess wird automatisch gestartet, sobald ein `ext3`- oder `ext4`-Dateisystem mit `mount` in den Verzeichnisbaum eingebunden wird.

Delayed Allocation

Die aus Performance-Sicht wichtigste Neuerung in `ext4` ist die sogenannte Delayed Allocation – eine Funktion, die es auch in vielen anderen modernen Dateisystemen gibt, z. B. `btrfs`, HFS+, `reiser4`, `xfs` und ZFS. Delayed Allocation (auch *Allocation on Flush* genannt) bedeutet, dass bei Änderungen die Datenblöcke zur Speicherung von Dateiänderungen nicht sofort reserviert werden, sondern erst zu dem Zeitpunkt, zu dem die Daten physikalisch gespeichert werden – und das kann durchaus eine halbe Minute dauern. Das bringt zwei wesentliche Vorteile mit sich: Zum einen können nun Speicheroperationen gebündelt werden, was die Geschwindigkeit erhöht und die Fragmentierung des Dateisystems mindert. Zum anderen kommt es bei temporären Dateien, die nur wenige Sekunden existieren, oft zu gar keiner physikalischen Speicherung.

Leider hat die Delayed Allocation auch Nachteile: Das Hauptproblem besteht darin, dass Metadaten (also Informationen über den Zustand einer Datei) oft schon vor den eigentlichen Änderungen gespeichert werden. In der ursprünglichen Implementierung des `ext4`-Treibers führte das dazu, dass eine geänderte, aber noch nicht synchronisierte Datei nach einem Absturz plötzlich leer war. Dieses Problem tritt besonders oft bei Konfigurationsdateien auf. Viele Anwender würden es akzeptieren, wenn eine Datei nach einem Absturz einfach den alten Zustand enthält. Aber dass der Inhalt der Datei und somit die Konfiguration eines Programms komplett verloren geht, das ist inakzeptabel.

Laut Theodore Ts'o, dem Hauptentwickler aller `ext`-Versionen, treten die Datenverluste nur deswegen auf, weil viele Programme `fsync` vergessen. Laut POSIX-Standard garantiert aber erst diese Funktion, dass Änderungen tatsächlich gespeichert werden. Dennoch wurde der `ext4`-Treiber verbessert, um das Problem zu minimieren: Wenn zur Änderung vorhandener Dateien die Funktionen `rename` oder `ftruncate` eingesetzt werden (das sind die üblichen Vorgehensweisen), verzichtet `ext4` auf die Delayed Allocation. Es ist möglich, die Delayed Allocation durch die `mount`-Option `nodelalloc` komplett zu deaktivieren. Das ist aber mit erheblichen Effizienzeinbußen verbunden und macht einen Teil der Performance-Fortschritte in `ext4` zunichte.

Standardverhalten und Optionen

Sofern der Journaling-Modus und die Allozierung im `mount`-Kommando bzw. in `/etc/fstab` nicht explizit eingestellt werden, gilt das folgende Standardverhalten:

`ext3` bis Kernel 2.6.29:	`data=ordered`
`ext3` ab Kernel 2.6.30:	`data=writeback`
`ext3` ab Kernel 2.6.36:	`data=ordered`
`ext4`:	`data=ordered` mit Delayed Allocation

Um herauszufinden, welcher Journaling-Modus aktiv ist, müssen Sie die Kernelmeldungen lesen. Im folgenden Beispiel gibt es je eine `ext3`- und eine `ext4`-Partition.

```
root#  dmesg | grep EXT
EXT3 FS on sda3, internal journal
EXT3-fs: mounted filesystem with ordered data mode.
...
EXT4-fs (sda4): mounted filesystem with ordered data mode
```

Um einen bestimmten Journaling-Modus explizit auszuwählen, geben Sie bei `mount` oder in `/etc/fstab` die Option `data=xxx` an. Bei `ext4` können Sie zudem die Delayed Allocation durch die Option `nodelalloc` deaktivieren.

Administration

Dateisystem einrichten

`ext2`-, `ext3`- und `ext4`-Dateisysteme werden mit `mkfs.ext2`, `mkfs.ext3` oder `mkfs.ext4` formatiert. Im folgenden Beispiel wird auf einem 20 GByte großen Logical Volume (also einer durch LVM verwalteten Partition) ein `ext4`-Dateisystem eingerichtet. `mke2fs` entscheidet sich selbstständig für eine Blockgröße von 4 kByte und für 1.310.720 Inodes.

Das bedeutet, dass Sie im Dateisystem maximal 1,3 Millionen Dateien anlegen können. Die durchschnittliche Dateigröße würde dann 16 kByte betragen. Wenn Sie mehr kleinere oder weniger größere Dateien speichern möchten, können Sie mit `-i` *n* angeben, nach wie vielen Bytes jeweils ein Inode vorgesehen werden soll. Wenn die durchschnittliche Dateigröße kleiner ist als *n*, limitiert nicht die Größe der Partition, sondern die Inode-Anzahl das Dateisystem.

Beachten Sie, dass die absolute Anzahl der Inodes nicht mehr verändert werden kann, auch nicht bei einer späteren Vergrößerung des Dateisystems! In den meisten Fällen ist der Vorgabewert von `mkfs.ext4` zweckmäßig.

```
root#  mkfs.ext4 /dev/mapper/vg1-test
mke2fs 1.42.4 (12-Jun-2012)
Blöcke des Gerätes werden verworfen: erledigt
Dateisystem-Label=
OS-Typ: Linux
```

```
Blockgröße=4096 (log=2)
Fragmentgröße=4096 (log=2)
1310720 Inodes, 5242880 Blöcke
262144 Blöcke (5.00%) reserviert für den Superuser
Erster Datenblock=0
Maximale Dateisystem-Blöcke=4294967296
160 Blockgruppen
32768 Blöcke pro Gruppe, 32768 Fragmente pro Gruppe
8192 Inodes pro Gruppe
Superblock-Sicherungskopien gespeichert in den Blöcken:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
        4096000
Schreibe Inode-Tabellen: erledigt
Erstelle Journal (32768 Blöcke): erledigt
Schreibe Superblöcke und Dateisystem-Accountinginformationen: erledigt
```

Konvertierung von ext3 in ext4

Um ein vorhandenes `ext3`-Dateisystem in ein `ext4`-Dateisystem umzuwandeln, führen Sie einfach das unten angegebene Kommando aus. `tune2fs` kann im laufenden Betrieb ausgeführt werden; um die neuen `ext4`-Funktionen zu nutzen, muss das Dateisystem aber neu in den Verzeichnisbaum eingebunden werden. `mount -o remount` ist nicht möglich.

```
root#  tune2fs -O extents /dev/sda5
root#  umount /dev/sda5
root#  mount /dev/sda5 /home
```

Die nachträgliche Umwandlung eines `ext3`-Dateisystems hat den Nachteil, dass vorhandene Dateien keine Extents nutzen (nur neue Dateien). Abhilfe würde das Defragmentierprogramm `e4defrag` schaffen, das aber noch nicht zur Verfügung steht.

Dateisystemüberprüfung

`ext`-Dateisysteme werden beim Rechnerstart regelmäßig auf Fehler überprüft, und zwar nach einer bestimmten Anzahl von `mount`-Vorgängen (standardmäßig 36) bzw. nach einer gewissen Zeit (6 Monate), je nachdem, welches Kriterium vorher erfüllt war. Einige Distributionen stellen die maximale `mount`-Anzahl bzw. das Zeitintervall großzügiger ein oder ganz auf 0 (keine Überprüfung). Zudem konfigurieren die meisten Distributionen `fstab` so, dass – wenn überhaupt – nur die Systempartition überprüft wird. Das betrifft die sechste Spalte in `fstab` (siehe Abschnitt 25.5).

Trotz der Journaling-Funktionen ist eine Überprüfung des Dateisystems hin und wieder sehr zu empfehlen, zumindest ein- bis zweimal pro Jahr! Zum einen werden so eventuelle Hardware-Fehler der Festplatte erkannt. Zum anderen kann es sein, dass die Dateisystemtreiber noch unbekannte Fehler enthalten. Je früher daraus resultierende Fehler korrigiert werden, desto kleiner ist der potenzielle Schaden.

Eine manuelle Überprüfung können Sie jederzeit mit dem Kommando `fsck.ext2/ext3/ext4` durchführen. Die betreffende Partition darf während der Kontrolle aller-

dings nicht gerade verwendet werden, d. h., Sie müssen gegebenenfalls vorher `umount` ausführen.

```
root#  fsck.ext4 -f /dev/mapper/vg1-test
...
/dev/mapper/vg1-test: 21357/1310720 Dateien (1.3% nicht zusammenhängend),
  2062135/5242880 Blöcke
```

Meist stellt sich bei der Überprüfung heraus, dass alles in Ordnung ist. Andernfalls werden die Reste nicht mehr rekonstruierbarer Dateien im `/lost+found`-Verzeichnis der jeweiligen Partition gespeichert. Falls es sich um Textdateien gehandelt hat, können Sie vielleicht aus den Überresten noch brauchbare Informationen entnehmen.

Überprüfungs-Intervall

Die aktuellen Intervalle für die automatische Überprüfung des Dateisystems können Sie mit `tune2fs` feststellen und verändern. Dabei geben Sie mit `-c` die maximale `mount`-Anzahl und mit `-i` das Zeitintervall in Tagen an:

```
root#  tune2fs -l /dev/mapper/vg1-test
...
Mount count:              1
Maximum mount count:      35
Last checked:             Wed Jul 15 11:45:54 2009
Check interval:           15552000 (6 months)
...
root#  tune2fs -c 100 -i 90  /dev/mapper/vg1-test
Setting maximal mount count to 100
Setting interval between check 7776000 seconds
```

Mit `tune2fs -c 0 -i 0` deaktivieren Sie die automatische Dateisystemüberprüfung vollständig.

Partitionsnamen einstellen

Mit `e2label` können Sie den internen Namen eines `ext`-Dateisystems (*Filesystem Volume Name*) ermitteln bzw. einstellen:

```
root#  e2label /dev/sda1 mylabel
```

Diesen Namen können Sie in der ersten Spalte von `/etc/fstab` statt des Device-Namens angeben.

UUID einstellen

Beim Einrichten erhält das Dateisystem automatisch eine UUID, die Sie mit `blkid` ermitteln. Bei Bedarf verändern Sie diese Nummer mit `tune2fs -U`. Die Veränderung kann im laufenden Betrieb erfolgen, `umount` ist nicht erforderlich.

```
root#  tune2fs -U random /dev/sda1                                (zufällige UUID)
root#  tune2fs -U f7c49568-8955-4ffa-9f52-9b2ba9877021 /dev/sda1  (eigene UUID)
```

Größe des Dateisystems ändern

Mit `resize2fs` können Sie ein `ext`-Dateisystem vergrößern oder verkleinern. Beachten Sie, dass Sie bei einer Vergrößerung *vorher* die zugrunde liegende Partition oder das LV vergrößern müssen, bei einer Verkleinerung die Partition oder das LV aber erst *nachher* verkleinern dürfen! Im folgenden Beispiel wird das LV mit `lvextend` vergrößert. Weitere Details zur LVM-Administration folgen in Abschnitt 25.15.

```
root#  lvextend -L 40G /dev/mapper/vg1-test
  Extending logical volume test to 40,00 GB
  Logical volume test successfully resized
root#  resize2fs /dev/mapper/vg1-test
resize2fs 1.42.4 (12-Jun-2012)
Das Dateisystem auf /dev/mapper/vg1-test ist auf /test eingehängt;
  Online-Größenveränderung nötig
old desc_blocks = 2, new_desc_blocks = 3
Führe eine Online-Größenänderung von /dev/mapper/vg1-test
  auf 10485760 (4k) Blöcke durch.
Das Dateisystem auf /dev/mapper/vg1-test ist nun 10485760 Blöcke groß.
```

Eine Vergrößerung des Dateisystems ist im laufenden Betrieb möglich. Allerdings ist eine Vergrößerung über 16 TByte laut verschiedenen Internet-Berichten problematisch bzw. überhaupt unmöglich. Ich habe das mangels eines ausreichend großen RAID-Verbunds nicht selbst testen können. Für eine Verkleinerung muss das Dateisystem vorher aus dem Verzeichnisbaum gelöst werden (`umount`).

Fragmentierung des Dateisystems

Unter »Fragmentierung« versteht man den Zustand, dass einzelne Dateien nicht in aneinanderliegenden Blöcken, sondern über die ganze Partition verteilt gespeichert werden. Dazu kann es kommen, wenn abwechselnd Dateien gelöscht, neu angelegt, verlängert oder verkürzt werden. Die Fragmentierung kann den Dateizugriff erheblich verlangsamen.

Die `ext2/3/4`-Treiber versuchen eine Fragmentierung so gut wie möglich zu vermeiden. Das gelingt allerdings nur, wenn das Dateisystem nie zu mehr als ca. 90 Prozent mit Daten gefüllt ist.

Es gibt momentan keine Defragmentierungswerkzeuge für die `ext`-Dateisysteme. Für `ext4` ist ein derartiges Programm unter dem Namen `e4defrag` aber immerhin in der Entwicklung. Es wird – wenn es einmal fertiggestellt ist – eine Defragmentierung im laufenden Betrieb ermöglichen.

Windows-Zugriff auf ext4-Dateisysteme

Sie können auch unter Windows auf Linux-Partitionen zugreifen. Eine Zusammenstellung der kostenlosen Programme bzw. Treiber finden Sie hier:

http://wiki.ubuntuusers.de/Linux-Partitionen_unter_Windows

Die Firma Paragon arbeitet an einem kommerziellen `ext`-Treiber für Windows:

http://www.paragon-software.com/home/extfs-windows-beta/index.html

25.8 Das btrfs-Dateisystem

Aller Voraussicht nach wird `btrfs` das Linux-Dateisystem der Zukunft. `btrfs` ist definitiv schon jetzt das modernste Dateisystem für Linux. Die Entwicklung von `btrfs` wurde ursprünglich von Oracle initiiert, erfolgt mittlerweile aber in Kooperation mit zahlreichen anderen Firmen und Kernelentwicklern. Der `btrfs`-Treiber ist in den Kernel integriert und untersteht wie der gesamte Kernelcode der Lizenz GPL.

Funktionen

Die folgende Liste fasst die wichtigsten Eigenschaften von `btrfs` zusammen:

- Copy on Write: Geänderte Dateiblöcke werden nicht überschrieben, sondern an einer anderen Stelle gespeichert. Das ermöglicht im Zusammenspiel mit Journaling besonders sichere Dateiänderungen.
- automatische Berechnung von Prüfsummen, um Bitfehler zu entdecken
- direkte Unterstützung von RAID-0, -1, -5, -6 und -10
- Snapshots und Subvolumes
- Komprimierung der Dateien (`mount`-Option `compress`)
- SSD-Optimierung (`mount`-Option `ssd`)
- Defragmentierung im laufenden Betrieb

Geplant, aber im Sommer 2013 noch nicht implementiert sind eine Dateisystemüberprüfung im laufenden Betrieb sowie eine Deduplizierungsfunktion, um redundante Daten, also z. B. zwei inhaltlich identische Dateien, nur einmal zu speichern.

Mit Subvolumes, Snapshots und RAID bietet `btrfs` ähnliche Funktionen wie die im Kernel schon enthaltenen *Multi Device* und *Logical Volume Manager* (siehe die Abschnitte 25.14 und 25.15). An sich sind solche Doppelgleisigkeiten im Kernel unerwünscht, im Falle von `btrfs` wurden sie aber akzeptiert. Der Grund: Einerseits ermöglicht die direkte Integration von RAID-Funktionen in den Dateisystemtreiber aufgrund der Prüfsummen eine noch höhere Datensicherheit, andererseits haben die `btrfs`-Entwickler glaubhaft nachweisen können, dass die `btrfs`-Snapshots wesentlich effizienter sind als die von LVM.

In diesem Abschnitt setze ich bei der Beschreibung der fortgeschrittenen `btrfs`-Funktionen voraus, dass Sie die in Abschnitt 2.7 zusammengefassten RAID- und LVM-Grundbegriffe kennen.

Status

`btrfs` ist nach wie vor unausgereift, auch wenn Oracle und SUSE das Gegenteil behaupten und den `btrfs`-Einsatz bereits empfehlen! In der `btrfs`-Mailingliste ist regelmäßig von Datenverlusten zu lesen. Es kann Ihnen durchaus passieren, dass `mount` bei einem bisher funktionierenden Dateisystem plötzlich eine Fehlermeldung liefert und sich das Dateisystem nicht mehr verwenden lässt!

Bevor Sie btrfs auf einem Rechner oder Server einrichten, lesen Sie unbedingt das Archiv der btrfs-Mailingliste der vergangenen zwei, drei Monate!

http://dir.gmane.org/gmane.comp.file-systems.btrfs

Immerhin gibt es seit Frühjahr 2012 das Kommando btrfsck zur Reparatur defekter Dateisysteme. Aber auch dieses Werkzeug ist noch unausgereift und zu wenig getestet. Eine Zusammenstellung weiterer bekannter Probleme können Sie hier nachlesen:

https://btrfs.wiki.kernel.org/index.php/FAQ
https://btrfs.wiki.kernel.org/index.php/Gotchas
https://btrfs.wiki.kernel.org/index.php/Problem_FAQ

Trotz dieser Mängel unterstützen mittlerweile die meisten Distributionen btrfs während der Installation. Es gibt aber noch keine Distribution, die auch grafische Werkzeuge für die weitere Administration anbieten kann.

Benchmarks

btrfs bietet im Vergleich zu ext4 eine Menge Zusatzfunktionen, ist aber nur in wenigen Fällen schneller. Generell sind Benchmark-Tests zur Beurteilung der Geschwindigkeit eines Dateisystems eine diffizile Angelegenheit. In der Vergangenheit ist btrfs aber selten als Sieger hervorgegangen. Wenn es Ihnen in erster Linie um maximale Geschwindigkeit geht, ist btrfs also nicht unbedingt die erste Wahl. Querverweise auf zuletzt durchgeführte Benchmark-Tests finden Sie hier:

https://btrfs.wiki.kernel.org/index.php/Main_Page

GRUB

GRUB 0.97 ist nicht btrfs-kompatibel. GRUB 2 unterstützt btrfs grundsätzlich, kommt aber nicht mit allen btrfs-Sonderfällen und -Varianten zurecht. Insofern sollten Sie selbst beim Einsatz von GRUB 2 eine eigene ext*n*-Bootpartition verwenden.

Administration

Die btrfs-Administration erfolgt überwiegend durch das Kommando btrfs. Dieses Kommando befindet sich zusammen mit mkfs.brtfs und brtfsck je nach Distribution im Paket btrfs-tools, btrfs-progrs oder btrfsprogs. Wenn Sie nicht schon während der Installation ein btrfs-Dateisystem eingerichtet haben, müssen Sie dieses Paket in der Regel extra installieren.

btrfs-Dateisystem einrichten

Um ein neues btrfs-Dateisystem in einer leeren Partition bzw. einem leeren Logical Volume einzurichten, führen Sie das folgende Kommando aus (wobei Sie natürlich /dev/sdb1 durch Ihren eigenen Device-Namen ersetzen müssen):

```
root#  mkfs.btrfs /dev/sdb1
fs created label (null) on /dev/sdb1
        nodesize 4096 leafsize 4096 sectorsize 4096 size 20.00GB
Btrfs Btrfs v0.19
```

Anschließend binden Sie das Dateisystem in den Verzeichnisbaum ein:

```
root#  mkdir /media/btrfs
root#  mount /dev/sdb1 /media/btrfs
```

Dateisystem vergrößern/ verkleinern

Wenn sich ein `btrfs`-Dateisystem als zu klein herausstellt, ist es am einfachsten, ein weiteres Device (also eine Festplattenpartition oder ein Logical Device) hinzuzufügen (siehe Abschnitt 25.8). Es ist aber auch möglich, die Größe eines vorhandenen `btrfs`-Dateisystems im laufenden Betrieb zu erhöhen und sogar zu verringern! In der Praxis funktioniert das am besten, wenn sich das Dateisystem in einem Logical Volume befindet.

Um ein `btrfs`-Dateisystem so zu vergrößern, dass es ein zuvor mit `lvextend` vergrößertes Logical Volume komplett nutzt, führen Sie das folgende Kommando aus:

```
root#  btrfs filesystem resize max /media/btrfs
```

Statt `max` können Sie auch die neue absolute Größe des Dateisystems angeben oder mit `+` oder `-` die relative Änderung. Dabei sind die Kürzel `k`, `m` und `g` für kByte, MByte und GByte erlaubt. Das folgende Kommando verkleinert das Dateisystem um 2 GByte:

```
root#  btrfs filesystem resize -2g /media/btrfs
```

Dateisystem überprüfen

Zur Überprüfung der Konsistenz des Dateisystems sieht `btrfs` das Kommando `btrfsck` vor. Das Kommando kann nur für nicht eingebundene Dateisysteme ausgeführt werden. Als einzigen Parameter übergeben Sie den Device-Namen der Partition mit dem `btrfs`-Dateisystem:

```
root#  btrfsck /dev/sdb1
```

Konvertierung von ext3/ext4 zu btrfs

Es ist möglich, ein vorhandenes `ext3`- oder `ext4`-Dateisystem mit `btrfs-convert` in ein `btrfs`-Dateisystem umzuwandeln. Die Konvertierung erfolgt überraschend schnell, weil dabei nur die `btrfs`-Metadaten neu angelegt werden, die eigentlichen Datenblöcke aber unverändert bleiben. Das folgende Beispiel geht davon aus, dass sich das ursprüngliche `ext4`-Dateisystem in `/dev/sdb1` befindet.

```
root#  fsck.ext4 -f /dev/sdb1
root#  btrfs-convert /dev/sdb1
creating btrfs metadata.
creating ext2fs image file.
cleaning up system chunk.
conversion complete.
root#  mount /dev/sdb1 /media/btrfs
```

`btrfs-convert` legt bei der Konvertierung den Snapshot `ext2_saved` an, der den Zustand des bisherigen `ext`-Dateisystems archiviert. Solange es diesen Snapshot gibt, können Sie das `btrfs`-System sogar zurück in ein `ext`-Dateisystem verwandeln! Veränderungen, die Sie in der Zwischenzeit im `btrfs`-Dateisystem durchgeführt haben, gehen dabei aber verloren.

```
root#  umount /dev/sdb1
root#  btrfs-convert -r /dev/sdb1
```

Wenn Sie nach der Konvertierung bei `btrfs` bleiben möchten, sollten Sie den Snapshot `ext2_saved` löschen. Je mehr Änderungen Sie im `btrfs`-Dateisystem durchführen, desto mehr Platz erfordert der Snapshot.

```
root#  btrfs subvolume delete /media/btrfs/ext2_saved
```

Technische Hintergründe zur Konvertierung können Sie hier nachlesen:

https://btrfs.wiki.kernel.org/index.php/Conversion_from_Ext3

Dateien komprimieren

`btrfs` unterstützt die automatische und transparente Komprimierung von Dateien. Dazu muss das Dateisystem mit der `mount`-Option `compress=zlib` oder `compress=lzo` in den Verzeichnisbaum eingebunden werden. Die Option `compress` gilt nur für neue bzw. geänderte Dateien. Vorhandene Dateien bleiben unverändert, solange sie nur gelesen werden. Die Option gilt für das gesamte Dateisystem, kann also nicht nur für einzelne Verzeichnisse aktiviert werden. Die Komprimierung erfolgt wahlweise durch den besser komprimierenden `zlib`-Algorithmus oder den schnelleren, aber weniger platzsparenden `lzo`-Algorithmus (siehe *http://lwn.net/Articles/411577*). Es gibt sogar Überlegungen, die `lzo`-Komprimierung in Zukunft standardmäßig zu aktivieren.

`compress` beschleunigt in vielen Fällen Dateioperationen. Das mag auf den ersten Blick verwundern, weil die Kompression bzw. Dekompression beim Lesen ja zusätzlichen Aufwand verursacht. Bei einer schnellen CPU ist dieser Aufwand aber gering im Vergleich zu der Ersparnis, die sich dadurch ergibt, dass weniger Datenblöcke der Festplatte oder der SSD gelesen bzw. verändert werden müssen. Als Zusatznutzen kommt natürlich die Platzersparnis hinzu.

Sie können das komprimierte Dateisystem später selbstverständlich auch ohne die Option `compress` nutzen. Neue bzw. veränderte Dateien sind dann nicht mehr komprimiert, bereits vorhandene Dateien bleiben aber komprimiert, solange die Dateien nur gelesen werden.

Die `compress`-Option eignet sich besonders gut für Verzeichnisse, die viele Textdateien enthalten (z. B. `/usr/`, die Platzersparnis beträgt hier fast 50 Prozent!). Nicht

empfehlenswert ist die Option hingegen für Ihr Benutzerverzeichnis, wenn sich dort überwiegend bereits komprimierte Dateien befinden, also z. B. Audio-, Video-, PDF- und LibreOffice-Dateien. Eine weitere Komprimierung gelingt dann nicht. Das erkennt auch der `btrfs`-Treiber und verzichtet bei der betreffenden Datei auf die Komprimierung. Dennoch kostet dieser Test etwas Zeit.

In der Praxis ist es bei Desktop-Systemen zweckmäßig, für die Systempartition `compress` zu verwenden, für die Home-Partition aber häufig nicht. Leider können Sie nicht bei jeder Distribution die `mount`-Optionen bereits bei der Installation einstellen. Bei openSUSE ist das möglich, und eine Testinstallation mit `compress=zlib` ergab, dass der Platzbedarf für die Systempartition bei einer Standardinstallation von 3,5 auf 1,8 GByte sank!

Natürlich gibt es Sonderfälle: Wenn Sie z. B. einen MySQL-Datenbank-Server betreiben und dabei den InnoDB-Tabellentreiber einsetzen, der die Tabellen automatisch komprimiert, sollte das MySQL-Datenbankverzeichnis `/var/lib/mysql` nicht in einem `btrfs`-Dateisystem mit `compress`-Option liegen.

Subvolumes

Von herkömmlichen Dateisystemen kennen Sie die Regel »Eine Partition bzw. ein Logical Volume – ein Dateisystem«. Bei `btrfs` ist das anders: *Subvolumes* ermöglichen es, innerhalb eines `btrfs`-Dateisystems gewissermaßen mehrere virtuelle Dateisysteme einzurichten und in einem eigenen `mount`-Verzeichnis zu nutzen.

Subvolumes erzeugen

Am einfachsten ist das anhand eines Beispiels zu verstehen. Dabei gehe ich davon aus, dass sich das `btrfs`-Dateisystem in der Partition `/dev/sdb1` befindet und im Verzeichnis `/media/btrfs` eingebunden ist.

`btrfs subvolume create` erzeugt nun zwei neue Subvolumes: `sub1` und `data/sub2`. Der Befehl `mount` mit der Option `subvol=name` bindet die Subvolumes in den Verzeichnisbaum ein.

```
root#  btrfs subvolume create /media/btrfs/sub1
root#  btrfs subvolume create /media/btrfs/data/sub2
root#  mkdir /media/sub{1,2}
root#  mount -o subvol=sub1 /dev/sdb1 /media/sub1
```

`mount -o subvol=name` funktioniert allerdings nur für Subvolumes, die sich direkt im Wurzelverzeichnis des `btrfs`-Dateisystems befinden. Ist das nicht der Fall, müssen Sie mit `btrfs subvolume list` die Volume-ID-Nummer des Subvolumes ermitteln und diese Nummer mit der `mount`-Option `subvolid` angeben:

```
root#  btrfs subvolume list /media/btrfs
ID 257 top level 5 path sub1
```

```
ID 258 top level 5 path data/sub2
root#  mount -o subvolid=258 /dev/sdb1 /media/sub2
```

Nun können Sie `/media/sub1` und `/media/sub2` wie zwei eigene Dateisysteme verwenden. Alle dort gespeicherten Dateien finden Sie aber auch direkt im `btrfs`-Dateisystem in den Verzeichnissen `sub1` und `data/sub2`, die bei der Ausführung von `btrfs subvolume create` automatisch erstellt wurden.

```
root#  touch /media/sub1/tst1
root#  ls /media/btrfs/sub1
tst1
root#  touch /media/sub2/tst2
root#  ls /media/btrfs/data/sub2
tst2
```

Mit anderen Worten: Die Subvolumes sind zwar als eigenständige Dateisysteme verwendbar, sie sind aber auch über Verzeichnisse des `btrfs`-Dateisystems les- und veränderbar.

Default-Subvolume

Mit `btrfs subvolume set-default` können Sie das Subvolume festlegen, das beim nächsten `mount`-Kommando standardmäßig verwendet wird, wenn nicht mit den `mount`-Optionen `subvol` oder `subvolid` explizit ein anderes Subvolume ausgewählt wird. An `set-default` müssen Sie die Volume-ID übergeben, die Sie vorher mit `btrfs subvolume list` ermitteln. Wenn Sie die folgenden Kommandos ausführen, enthält `/media/btrfs` die Dateien des Subvolumes `sub1`:

```
root#  btrfs subvolume set-default 257 /media/btrfs/
root#  umount /media/btrfs
root#  mount /dev/sdb1 /media/btrfs    (Subvolume sub1)
```

Wie können Sie nun bei Bedarf wieder das `btrfs`-Wurzelverzeichnis aktivieren? Dieses wird intern wie ein Subvolume behandelt, das die ID-Nummer 5 hat. Wenn Sie das Ergebnis von `btrfs subvolume list` genau studieren, sehen Sie, dass 5 als ID-Nummer des Top Levels angegeben wird:

```
root#  btrfs subvolume set-default 5 /media/btrfs/
root#  umount /media/btrfs
root#  mount /dev/sdb1 /media/btrfs    (Top Level)
```

Subvolumes löschen

Mit `btrfs subvolume delete name` löschen Sie ein Subvolume inklusive aller darin enthaltenen Dateien. Das Subvolume muss vorher natürlich aus dem Verzeichnisbaum gelöst werden.

```
root#  umount /media/sub2
root#  btrfs subvolume delete /media/btrfs/data/sub2
```

Beachten Sie, dass der von Subvolumes beanspruchte Speicher mit der Ausführung von `btrfs subvolume delete` nicht sofort freigegeben wird, sondern erst nach und nach. Ein Kernelprozess kümmert sich im Hintergrund um die erforderlichen Aufräumarbeiten.

Snapshots

Snapshots ermöglichen es, das `btrfs`-Dateisystem bzw. ein Subvolume des Dateisystems auf zwei Zweige aufzuteilen. Neue Snapshots können vom Dateisystem selbst, von einem Subvolume oder von einem anderen Snapshot erstellt werden.

Anfänglich enthalten das Ausgangs-Volume und der Snapshot dieselben Daten. Anschließend können beide Dateisysteme losgelöst voneinander geändert werden, wobei `btrfs` nur die Änderungen speichert. Beim Erstellen des Snapshots wird also nicht der gesamte Datenbestand kopiert.

Snapshots können z. B. für Backups verwendet werden. Sie erstellen zuerst den Snapshot und führen dann ein Backup des Snapshots aus. Das stellt sicher, dass sich während des Backups keine Dateien ändern. Gleichzeitig können Sie während des Backups ganz normal weiterarbeiten. Sobald das Backup abgeschlossen ist, löschen Sie den Snapshot.

Eine andere Anwendung besteht darin, vor kritischen Operationen, z. B. vor einem Kernel-Update, einen Sicherungspunkt zu erstellen. Sollte das Update scheitern, können Sie auf den Snapshot zurückgreifen.

`btrfs`-intern werden Snapshots wie Subvolumes behandelt. Deswegen gelten die meisten `subvolume`-Befehle von `btrfs` gleichermaßen für Subvolumes und Snapshots. Der wesentliche Unterschied zwischen Subvolumes und Snapshots besteht darin, dass Subvolumes anfänglich leer sind, Snapshots dagegen eine virtuelle Kopie des Ausgangsverzeichnisses enthalten. Wie gesagt: Vorerst werden keine Daten kopiert. Vielmehr werden nur die Veränderungen gegenüber dem ursprünglichen Zustand gespeichert.

btrfs versus LVM

Der Begriff »Snapshot« wird in `btrfs` und LVM vollkommen unterschiedlich verwendet. In LVM ist ein Snapshot ein unveränderliches Abbild eines Logical Volumes (LV). Sie müssen beim Erzeugen des Snapshots angeben, wie viel Speicherplatz der Snapshot maximal beanspruchen darf. Dieser Speicherplatz dient dazu, bei Bedarf Datenblöcke des ursprünglichen LVs zu archivieren, bevor diese geändert werden. Wenn der Snapshot-Speicherplatz aufgebraucht ist, wird der Snapshot ungültig und kann nicht mehr verwendet werden.

Bei `btrfs` ist der Inhalt des Snapshots dagegen veränderlich! Ein Snapshot ist also ein neuer Zweig eines Verzeichnisbaums, der zum Zeitpunkt der Erstellung des Snapshots eins zu eins mit diesem identisch ist. Ab diesem Zeitpunkt können sich beide Zweige unabhängig voneinander weiterentwickeln. Die beiden Zweige beanspruchen umso mehr Speicherplatz, je mehr Dateien geändert werden. `btrfs` verwendet zur Speicherung der Änderungen einfach den `btrfs`-Speicherpool. Das funktioniert

so lange, bis die Kapazität des gesamten Dateisystems erschöpft ist. btrfs-Snapshots bieten somit wesentlich mehr Funktionen und Flexibilität als LVM-Snapshots!

Grenzen und Design-Limits

Auf den ersten Blick scheinen Snapshots unbegrenzte Möglichkeiten zur Administration des Dateisystems zu bieten. Tatsächlich weist die Implementierung momentan aber noch Schwächen auf:

- Es kann nicht festgestellt werden, wie viel Speicherplatz ein Snapshot beansprucht.
- Es ist zwar möglich, einen Snapshot als neues Default-Volume zu definieren (`btrfs subvolume set-default`), es ist aber unmöglich, das ursprüngliche Basissystem zu löschen. Diese Einschränkung können Sie umgehen, indem Sie sofort nach dem Anlegen eines btrfs-Dateisystems einen Snapshot oder ein Subvolume einrichten und das Startsystem darin speichern. Das ermöglicht es, dieses Startsystem später zugunsten eines Snapshots zu löschen. Die bisweilen verwirrenden Details und Implikationen wurden in der btrfs-Mailingliste schon mehrfach diskutiert, z. B. hier:

  http://www.mail-archive.com/linux-btrfs@vger.kernel.org/msg03484.html
  http://www.mail-archive.com/linux-btrfs@vger.kernel.org/msg05334.html
  http://www.mail-archive.com/linux-btrfs@vger.kernel.org/msg04968.html

Beispiel

Als Ausgangspunkt für das folgende Beispiel dient ein btrfs-Dateisystem in der Partition `/dev/sdb1`. Das Dateisystem ist an der Stelle `/media/btrfs` in den Verzeichnisbaum integriert. `btrfs subvolume snap` erzeugt nun einen Snapshot vom gesamten Dateisystem. Dabei wird zugleich das Verzeichnis `/media/btrfs/snap1` erzeugt. Der Snapshot kann über dieses Verzeichnis verwendet werden oder mit `mount` wie ein eigenes Dateisystem in den Verzeichnisbaum eingebunden werden. Dabei muss die vom vorigen Abschnitt schon bekannte `mount`-Option `subvol=name` verwendet werden:

```
root#  btrfs subvolume snapshot /media/btrfs/ /media/btrfs/snap1
root#  mkdir /media/snap1
root#  mount -o subvol=snap1 /dev/sdb1 /media/snap1/
```

Sie können nun sowohl im ursprünglichen Dateisystem als auch im Snapshot unabhängig voneinander (also ohne gegenseitige Beeinflussung) Dateien anlegen, verändern und löschen.

btrfs-Snapshots sind normalerweise veränderlich. Wenn Sie für Backups einen Read-only-Snapshot wünschen, führen Sie `btrfs subvolume snapshot` mit der Option `-r` aus.

btrfs-Snapshots in Fedora und SUSE

Wenn Sie Fedora in ein btrfs-Dateisystem installieren, können Sie das YUM-Zusatzpaket `yum-plugin-fs-snapshot` installieren. Damit erstellt YUM bei jeder Paketinstallation bzw. bei jedem Update Snapshots aller btrfs-Dateisysteme. Die Snap-

shots bekommen den Namen `yum_datum_uhrzeit`. Prinzipiell bieten diese Snapshots die Möglichkeit, nach einem missglückten Update das ursprüngliche System wiederherzustellen. Die zunehmende Anzahl von Snapshots kostet allerdings im Laufe der Zeit immer mehr Platz auf der Festplatte; um die Administration der Snapshots müssen Sie sich selbst kümmern.

Die SUSE-Entwickler haben sich Gedanken darüber gemacht, wie man `btrfs`-Snapshots bequemer administrieren könnte; daraus resultierten das Kommando `snapper` und ein neues YaST-Modul. Ähnlich wie bei Fedora erzeugt auch Snapper bei entsprechender Konfiguration automatische Snapshots, und das nicht nur bei Paketinstallationen, sondern auch bei anderen grundlegenden Änderungen an der Konfiguration. Wie bei Fedora lässt sich diese Funktion nur dann zweckmäßig einsetzen, wenn sich private Daten und Datenbanken in einem getrennten Dateisystem befinden; andernfalls würden bei einem Zurücksetzen des Dateisystems auf einen früheren Zeitpunkt auch alle privaten Änderungen verloren gehen, die seither erfolgt sind.

btrfs-Dateisysteme über mehrere Devices verteilen, RAID

Der `btrfs`-Treiber kann Dateisysteme über mehrere Festplatten bzw. Devices verteilen und unterstützt dabei die RAID-Level 0, 1, 5, 6 und 10, ohne auf den sonst üblichen Linux-RAID-Treiber `mdadm` zurückzugreifen.

Device hinzufügen

Der einfachste Fall von Multi-Device-Dateisystemen entsteht zumeist dann, wenn ein `btrfs`-Dateisystem zu klein wird: Sie können nun ganz einfach ein weiteres Device hinzufügen (also eine leere Festplattenpartition oder ein ungenutztes Logical Volume). Damit wird das Dateisystem entsprechend vergrößert. Sie müssen weder eine Partition neu formatieren noch die Größe des Dateisystems explizit ändern – `btrfs` erledigt all diese Aufgaben selbstständig.

```
root#  btrfs device add /dev/sdb2 /media/btrfs
```

Anfänglich befinden sich nun alle Daten auf dem ersten Device, während das zweite Device erst nach und nach genutzt wird. Falls sich die Devices auf unterschiedlichen physikalischen Festplatten befinden (und nur dann!), erzielen Sie einen Geschwindigkeitsgewinn, wenn Sie die vorhandenen Dateien mit `btrfs filesystem balance` über alle Devices verteilen. Beachten Sie aber, dass `btrfs filesystem balance` sehr lange dauert und nur selten der Mühe wert ist.

```
root#  btrfs filesystem balance /media/btrfs
```

Es ist auch möglich, ein Device wieder zu entfernen. Die auf dem Device enthaltenen Daten werden dann zuerst auf die anderen Devices übertragen, weswegen die Ausführung des folgenden Kommando sehr lange dauern kann:

```
root#  btrfs device delete /dev/sdb1 /media/btrfs/
```

mkfs.btrfs mit mehreren Devices

Sie können ein `btrfs`-Dateisystem auch von vornherein mit mehreren Devices einrichten, indem Sie an `mkfs.btrfs` mehrere Devices übergeben:

```
root#  mkfs.btrfs /dev/sdb1 /dev/sdc1
```

Standardmäßig werden dann die Metadaten des Dateisystems dupliziert (entspricht RAID-1), die eigentlichen Daten aber über alle Devices verteilt. Die Metadaten enthalten die Verwaltungsinformationen des Dateisystems, also z. B. Inode-Listen sowie Bäume zum Suchen nach Dateien. Leider ist beim resultierenden Dateisystem nun weder die Geschwindigkeit optimal (es ist langsamer als ein RAID-0-System wegen der Duplizierung der Metadaten) noch kann es sicherheitstechnisch mit RAID-1 mithalten, weil die eigentlichen Daten nicht redundant gespeichert werden.

Bei der Ausführung von `mount` geben Sie ein beliebiges Device des Dateisystems an. (Nach einem Rechnerneustart muss das Kommando `btrfs device scan` ausgeführt werden, damit `btrfs` weiß, welche Devices mit `btrfs`-Dateisystemen es gibt und wie sie zusammengehören.)

```
root#  mount -t /dev/sdb1 /media/btrfs
```

Welche RAID-Variante für welche Art von Daten verwendet wird, finden Sie mit `btrfs filesystem df` heraus:

```
root#  btrfs filesystem df /media/btrfs
Data, RAID0: total=1.56GB, used=128.00KB
System, RAID1: total=8.00MB, used=4.00KB
Metadata, RAID1: total=1.00GB, used=24.00KB
...
```

RAID-0

Wenn Sie ein »richtiges« RAID-System anlegen möchten, bei dem Daten und Metadaten einheitlich behandelt werden, übergeben Sie an `mkfs.btrfs` mit `-d` (für die Daten) und `-m` (für die Metadaten) den gewünschten RAID-Level. Außerdem übergeben Sie an `mkfs.btrfs` die gewünschte Anzahl von Devices. Das folgende Kommando erstellt ein RAID-0-System (Striping):

```
root#  mkfs.btrfs -d raid0 -m raid0 /dev/sdb1 /dev/sdc1
```

RAID-1

Ein RAID-1-Dateisystem wird analog mit diesem Kommando eingerichtet:

```
root#  mkfs.btrfs -d raid1 -m raid1 /dev/sdb1 /dev/sdc1
```

Interessant wird es, wenn ein Device ausfällt. Um diesen Fall zu testen, habe ich die Festplatte `/dev/sdc` entfernt. Damit das Dateisystem verwendet werden kann, muss nun die zusätzliche `mount`-Option `degraded` verwendet werden:

```
root#  mount -o degraded /dev/sdb1 /media/btrfs
```

Um den RAID-Verbund wiederherzustellen, fügen Sie dem Dateisystem ein neues, möglichst gleich großes Device wieder hinzu. Im folgenden Beispiel ist das wieder `/dev/sdc1`, wobei diese Partition nun aber von einer neuen Festplatte stammt. Um das Dateisystem wieder über beide Devices zu verteilen und somit die RAID-1-Redundanz wiederherzustellen, müssen Sie außerdem `btrfs filesystem balance` ausführen. Bei großen Dateisystemen dauert die Ausführung dieses Kommandos naturgemäß sehr lange. Immerhin kann das Dateisystem in dieser Zeit genutzt werden, wenn auch mit stark verminderter Geschwindigkeit.

```
root#  btrfs device add /dev/sdc1 /media/btrfs
root#  btrfs filesystem balance /media/btrfs
```

Erst jetzt kann das defekte Device aus dem Dateisystem entfernt werden. Dabei verwenden Sie zur Device-Angabe das Schlüsselwort `missing`:

```
root#  btrfs device delete missing /media/btrfs
```

Beim nächsten `mount`-Kommando können Sie nun auf die Option `degraded` verzichten.

Die Nutzung eines btrfs-Dateisystems ermitteln (df)

Bei anderen Dateisystemen können Sie ganz einfach mit `df -h` feststellen, wie viel Speicherplatz vorhanden ist, wie viel davon belegt ist und wie viel noch frei ist. Bei `btrfs`-Dateisystemen liefert `df` aber oft vollkommen falsche Ergebnisse, insbesondere im Zusammenhang mit RAID. Dafür gibt es drei Gründe:

- `btrfs` liefert momentan an `df` keine Informationen darüber wie die Devices genutzt werden, also z. B. den RAID-Level. Das ist nicht zuletzt deswegen unmöglich, weil `btrfs` für Daten und Metadaten unterschiedliche RAID-Level erlaubt.
- `btrfs` gliedert die Speichernutzung in drei verschiedene Bereiche: Systemdaten (hierbei handelt es sich um ganz kleine Datenmengen), Metadaten (Prüfsummen und Verwaltungsinformationen, um die Suche nach Dateien zu beschleunigen) und Nutzdaten (Platz für den eigentlichen Inhalt der Dateien).
- `btrfs` beansprucht nicht einfach den gesamten Speicherplatz sofort für sich, sondern nutzt den Speicher als Pool, aus dem es sich bei Bedarf Datenblöcke für die System-, Metadaten oder die eigentlichen Daten reserviert. Dabei fällt auf, dass `btrfs` relativ viel Metadaten konsumiert, die vor allem zur Speicherung von Dateiprüfsummen verwendet werden.

Leider sind auch die `btrfs`-Kommandos `filesystem show` und `filesystem df` nicht in der Lage, wirklich konkrete Zahlen dazu zu ermitteln, wie viel Speicherplatz noch frei ist. Das folgende Beispiel soll Ihnen dabei helfen, zumindest die Daten korrekt

zu interpretieren, die `btrfs` liefert. Als Ausgangspunkt dient ein kleines `btrfs`-RAID-1-System aus zwei je 8 GByte großen Partitionen. In dieses Dateisystem wurde das gesamte `/usr`-Verzeichnis des Testsystems kopiert (Platzbedarf laut `du` ca. 2,1 GByte).

```
root#  mkfs.btrfs -d raid1 -m raid1 /dev/sdb1 /dev/sdc1
root#  mount /dev/sdb1 /media/btrfs
root#  cp -r /usr /media/btrfs
```

df

Das Ergebnis von `df` ist vollständig falsch. Das liegt daran, dass `df` nicht erkennen kann, dass `btrfs` im RAID-1-Level arbeitet. Die Gesamtgröße ergibt sich aus der Summe der Partitionsgrößen. Der benutzte Speicher laut `df` ist in Wirklichkeit der für `btrfs` reservierte Speicher.

```
root#  df -h /media/btrfs/
Dateisystem    Größe Benutzt Verf. Verw% Eingehängt auf
/dev/sdb1        16G    3,7G   12G   25% /media/btrfs
```

filesystem show

`btrfs filesystem show` verrät, dass das Dateisystem aus zwei jeweils 8 GByte großen Devices zusammengesetzt ist. Insgesamt enthält das Dateisystem 1,9 GByte System-, Meta- und Nutzdaten. Außerdem wissen wir jetzt, dass auf jedem Device jeweils ca. 3,5 GByte Daten reserviert wurden. `filesystem show` liefert allerdings keine Informationen, wie die Devices miteinander verbunden sind (also welcher RAID-Level aktiv ist). Daher ist es auch unmöglich zu sagen, wie groß die gesamte Kapazität des Dateisystems ist. (Bei RAID-0 würde sie 16 GByte betragen, bei RAID-1 aber nur 8.)

```
root#  btrfs filesystem show  /dev/sdb1
Label: none  uuid: dc691a5d-187e-4cb4-a94a-d12dabdffde4
        Total devices 2 FS bytes used 1,89GB
        devid    1 size 7.81GB used 3,53GB path /dev/sdb1
        devid    2 size 7.81GB used 3,54GB path /dev/sdc1
```

filesystem df

`btrfs filesystem df` gibt Auskunft darüber, wie die reservierten Daten verwendet werden. `btrfs` hat bisher 3 GByte für die eigentlichen Daten reserviert und davon ca. 1,6 GByte tatsächlich genutzt. Weiters hat `btrfs` 512 MByte für Metadaten reserviert und davon rund 190 MByte genutzt. Schließlich hat `btrfs` 32 MByte für Systemdaten reserviert und gerade einmal 4 KByte davon tatsächlich genutzt. 3,00 + 0,5 + 0,03 ergibt die 3,53 GByte, die `filesystem show` angezeigt hat.

```
root#  btrfs filesystem df /media/btrfs/
Data, RAID1:     total=3.00GB, used=1.62GB
System, RAID1:   total=32.00MB, used=4.00KB
System:          total=4.00MB, used=0.00
Metadata, RAID1: total=512.00MB, used=191.02MB

Data:     total=2.61GB, used=1.70GB
Metadata: total=1.01GB, used=198.82MB
System:   total=12.00MB, used=4.00KB
```

Wie viel Speicherplatz ist nun wirklich frei? Wir wissen, dass insgesamt 16 GByte Speicherplatz zur Verfügung stehen. Wegen der mit RAID-1 verbundenen Redundanz sinkt der nutzbare Speicherplatz auf die Hälfte, also auf 8 GByte. Davon sind bereits 3,53 GByte reserviert. Der für die eigentlichen Daten reservierte Bereich kann somit noch maximal um 4,3 GByte vergrößert werden und würde dann knapp 7 GByte groß sein. Davon sind 1,6 GByte bereits genutzt. Das ergibt einen freien Speicherplatz für Dateien von ca. 5,4 GByte. Allerdings geht diese Rechnung nur auf, wenn `btrfs` nicht zwischenzeitlich nochmals Platz für Metadaten reservieren muss.

Sie sehen schon, es ist nicht ganz trivial, den freien Speicherplatz zu ermitteln. Bei den RAID-Leveln 5 und 6 ist die Sache noch wesentlich komplizierter. In der `btrfs`-Mailingliste gibt es zudem immer wieder Berichte darüber, dass `btrfs` keinen freien Speicherplatz mehr meldet, obwohl eigentlich noch eine Menge Platz frei sein müsste. Kurzum: Es empfiehlt sich, auf `btrfs`-Dateisystemen generell eine großzügige Platzreserve freizuhalten.

25.9 Das xfs-Dateisystem

Das `xfs`-Dateisystem wurde von der Firma SGI für deren Workstations mit dem Unix-ähnlichen Betriebssystem IRIX entwickelt. Später wurde das Dateisystem für Linux portiert. Das Dateisystem gilt als ausgereift, stabil und vor allem im Umgang mit sehr großen (Multimedia-)Dateien als effizient. Weitere Informationen zum `xfs`-Dateisystem finden Sie hier:

http://en.wikipedia.org/wiki/XFS
http://xfs.org/index.php/XFS_FAQ

XFS-Eigenheiten

Bei der Nutzung von `xfs` müssen Sie zwei Besonderheiten beachten: Zum einen können `xfs`-Dateisysteme mit `xfs_growfs` nur vergrößert, aber nicht verkleinert werden.

Zum anderen nutzt das Dateisystem die Partition vom ersten Byte an und lässt im Gegensatz zu den anderen Linux-Dateisystemen keinen Platz für einen Bootsektor. Deshalb zerstört die Installation von GRUB in den Bootsektor einer `xfs`-Partition Teile des Dateisystems! Bei BIOS-Rechnern sollten Sie GRUB daher ausschließlich in den Master-Bootsektor der Festplatte installieren, wie dies das GRUB-Handbuch ohnedies empfiehlt. Vorsicht ist in diesem Zusammenhang vor allem bei openSUSE angebracht, das GRUB bei BIOS-Rechnern zumindest bis Version 12.3 standardmäßig in den Bootsektor einer Partition installiert. Bei EFI-Rechnern können diese Probleme nicht auftreten, denn dort wird GRUB in jedem Fall in die EFI-Partition installiert.

/etc/fstab

Einträge für ein `xfs`-Dateisystem in `/etc/fstab` sehen üblicherweise wie im folgenden Beispiel aus. Zusätzliche `mount`-Optionen werden nur ganz selten benötigt. Sie sind in `man mount` verzeichnet.

```
# /etc/fstab
/dev/sdb13      /data          xfs  defaults 0 0
```

xfs-Dateisystem einrichten

Um in einer Partition ein `xfs`-Dateisystem einzurichten, führen Sie einfach `mkfs.xfs` aus:

```
root#  mkfs.xfs /dev/sdc1
meta-data=/dev/sdc1     isize=256    agcount=16, agsize=152742 blks
         =              sectsz=512   attr=0
data     =              bsize=4096   blocks=2443872, imaxpct=25
         =              sunit=0      swidth=0 blks, unwritten=1
naming   =version 2     bsize=4096
log      =internal log  bsize=4096   blocks=2560, version=1
         =              sectsz=512   sunit=0 blks
realtime =none          extsz=65536  blocks=0, rtextents=0
```

Jetzt fehlt nur noch ein `mount`-Kommando, und schon können Sie das Dateisystem nutzen:

```
root#  mount -t xfs /dev/sdc1 /test
```

Dateisystem überprüfen

Die Integrität von `xfs`-Dateisystemen wird bei jedem `mount`-Vorgang automatisch überprüft. Dabei wird aber nur das Journaling-Protokoll ausgewertet. Zur manuellen Überprüfung führen Sie `xfs_check` aus. Das ist nur möglich, wenn das Dateisystem nicht eingebunden ist. Falls das Kommando Fehler entdeckt, können Sie versuchen, diese mit `xfs_repair` zu beheben.

Um für Kompatibilität zu den anderen Dateisystemen zu sorgen, existiert auch das Kommando `fsck.xfs`. Dieses Kommando erfüllt aber keine Aufgabe und liefert als Ergebnis immer OK.

Parameter des Dateisystems ändern

`xfs_growfs` vergrößert ein `xfs`-Dateisystem im laufenden Betrieb. Das Dateisystem muss dazu eingebunden sein! Das Kommando setzt voraus, dass die zugrunde liegende Datenpartition vorher bereits vergrößert wurde. `xfs_admin` verändert diverse Parameter des Dateisystems, beispielsweise den Namen (Label) und die UUID-Nummer. Das Dateisystem muss vorher aus dem Verzeichnisbaum gelöst werden (`umount`).

25.10 Windows-Dateisysteme (vfat, ntfs)

Viele Linux-Anwender haben auf ihrem Rechner parallel eine Windows-Version installiert. Aber auch externe Datenträger nutzen häufig Windows-Dateisysteme (USB-Sticks, Speicherkarten von Digitalkameras etc.). Im Folgenden lernen Sie, wie Sie unter Linux auf Windows-Dateisysteme zugreifen – ganz egal, ob sich diese in einer Partition der internen Festplatte oder auf einem externen Datenträger befinden.

Varianten

Es gibt zwei fundamental unterschiedliche Windows-Dateisysteme, FAT und NTFS:

- **FAT, VFAT, exFAT:** Vom FAT-Dateisystem gibt es unzählige Varianten. Die historisch ältesten Versionen sind FAT12 für Disketten, FAT16 für Dateisysteme bis 2 GByte sowie FAT32 für Dateisysteme bis 8 TByte und Dateien bis 4 GByte. Mit Windows 95 wurde außerdem VFAT eingeführt, das endlich Dateinamen mit mehr als 8+3 Zeichen erlaubte. Die Kombination aus FAT32 und VFAT ist heute am häufigsten im Einsatz, z. B. auf fast allen SD-Karten.

  Eine relativ neue FAT-Variante ist exFAT: Dieses Dateisystem wurde speziell für große Flash-Karten entwickelt (z. B. für Digitalkameras). Es erlaubt Dateien bis zu 16.777.216 TByte Größe und unterstützt ACLs und Transaktionen.

- **NTFS:** Das *New Technology File System* wurde mit Windows NT eingeführt und wird von allen aktuellen Windows-Versionen genutzt. Im Vergleich zu FAT bietet NTFS eine höhere Sicherheit (Zugriffsrechte, Journaling etc.) sowie diverse Zusatzfunktionen. Die Dateisystemgröße ist mit 16.777.216 TByte nahezu unbegrenzt.

Linux-Unterstützung

Linux kann (V)FAT- und NTFS-Dateisysteme lesen und schreiben. Problematischer ist die exFAT-Unterstützung: Es gibt momentan eine Beta-Version eines Open-Source-Treibers (*http://code.google.com/p/exfat*) sowie einen kommerziellen Treiber der Firma Tuxera (*http://tuxera.com*). Eine Integration des exFAT-Treibers in den Kernel ist aufgrund von Patenten leider unmöglich.

Es ist unter Linux nur selten notwendig, Windows-Dateisysteme einzurichten – aber es ist möglich: Mit `mkfs.vfat` formatieren Sie eine Partition im VFAT32-Format und mit `mkfs.ntfs` im NTFS-Format. `mkfs.ntfs` befindet sich üblicherweise im Paket `ntfsprogs`, das oft erst installiert werden muss.

Konvertierung von Textdateien

Unabhängig vom Dateisystem bereitet der Textaustausch zwischen Linux und Windows oft Probleme, weil je nach Betriebssystem unterschiedliche Zeichensätze und Kennzeichnungen für das Zeilenende zur Anwendung kommen. Diese Probleme lassen sich mit diversen Konvertierungswerkzeugen lösen (siehe Kapitel 17, »Konverter für Grafik, Text und Multimedia«).

Zugriffsrechte

VFAT kennt das Konzept von Zugriffsrechten überhaupt nicht. NTFS unterstützt zwar Zugriffsrechte, aber nicht in der Unix/Linux-typischen Art und Weise. Daraus ergibt sich ein Problem: Welcher Linux-Benutzer verfügt über welche Zugriffsrechte auf Windows-Dateien? Die Antwort geben die `mount`-Optionen `uid`, `gid` und `umask`/`fmask`/`dmask`. Diese Optionen stellen den Besitzer, die Gruppenzugehörigkeit und die Zugriffsbits für das Windows-Dateisystem ein, und zwar einheitlich für alle Dateien dieses Dateisystems und unabhängig von eventuellen NTFS-Zugriffsrechten.

Vermeiden Sie Datenverluste beim Zugriff auf Windows-Dateisysteme!

Auf einem Dual-Boot-Rechner, der wahlweise unter Linux oder unter Windows läuft, können unter Linux durchgeführte Schreibzugriffe gleich aus zwei Gründen zu einem inkonsistenten Windows-Dateisystem und zu Datenverlusten führen:

- Wenn Windows nicht vollständig heruntergefahren ist, sondern sich in einem Ruhe- oder Schnellstart-Modus befindet, sind zuletzt durchgeführte Änderungen in einer speziellen Datei außerhalb des eigentlichen Dateisystems gesichert. Linux sieht diese Datei nicht. Achten Sie deshalb darauf, dass Sie Windows vor einem Wechsel zu Linux vollkommen herunterfahren. Das gilt insbesondere für Windows 8! Dessen Schnellstartfunktion basiert darauf, dass Windows eben *nicht* richtig beendet wird, sondern in einen speziellen Ruhezustand versetzt wird.
- Wenn eine herkömmliche Festplatte mit einem SSD-Cache verbunden ist, sieht Linux normalerweise nur den Inhalt der Festplatte. Auch in diesem Fall kann es sein, dass zuletzt durchgeführte Änderungen am Dateisystem nur im SSD-Cache gespeichert und somit für Linux unsichtbar sind.

Am einfachsten gehen Sie derartigen Problemen aus dem Weg, indem Sie gemeinsame Windows/Linux-Daten extern synchronisieren, z. B. mit einem Dropbox-Verzeichnis.

Das VFAT-Dateisystem

Standardeinstellungen

Vorweg eine kurze Zusammenfassung der Standardeinstellungen des `vfat`-Dateisystemtreibers: Der Treiber erkennt den FAT-Typ (FAT12/-16/-32) selbstständig. Die Windows-Dateinamen werden unter Linux im Zeichensatz Latin-1 (ISO8859-1) dargestellt. Der Benutzer, der `mount` ausführt, darf alle Dateien und Verzeichnisse lesen und schreiben; alle anderen Benutzer dürfen alles lesen, aber nichts verändern. Selbstverständlich können Sie alle Einstellungen durch Optionen verändern.

VFAT in /etc/fstab

Ein typischer Eintrag in `/etc/fstab` für eine lokale VFAT-Partition auf der Festplatte sieht wie folgt aus:

```
# /etc/fstab
/dev/sda1      /media/win1  vfat    utf8,uid=1000  0 0
```

Sie erreichen damit, dass der Benutzer mit der Benutzernummer 1000 alle Dateien verändern darf und dass Sonderzeichen in Windows-Dateinamen unter Linux als UTF8-Zeichen dargestellt werden.

Die folgende `fstab`-Zeile bindet die Windows-Partition nicht automatisch in den Verzeichnisbaum ein (`noauto`). Dank `users` darf aber jeder Benutzer `mount` ausführen. `gid=users` bewirkt, dass die Gruppenzugehörigkeit der Windows-Dateien durch die Standardgruppe (und nicht die gerade aktuelle Gruppe) des Benutzers bestimmt wird.

```
# /etc/fstab
/dev/sda1      /media/win1  vfat    noauto,users,gid=users,utf8  0 0
```

Das NTFS-Dateisystem (ntfs-3g)

In der Vergangenheit gab es diverse `ntfs`-Treiber für Linux. Zuletzt hat sich der `ntfs-3g`-Treiber durchgesetzt. Er unterstützt Lese- und Schreibzugriffe und kann mit Streams umgehen. Der Treiber kann allerdings keine verschlüsselten Dateien lesen/schreiben und keine komprimierten Dateien erzeugen (wohl aber lesen). Nahezu alle großen Distributionen installieren den `ntfs-3g`-Treiber standardmäßig.

Im Gegensatz zu den meisten anderen Dateisystemtreibern ist `ntfs-3g` nicht als Kernelmodul implementiert, sondern als sogenannter FUSE-Treiber. FUSE steht für *Filesystem in Userspace*. Dabei handelt es sich um ein Kernelmodul, das mit externen Programmen kommuniziert. FUSE ermöglicht es also, den eigentlichen Dateisystemtreiber außerhalb des Kernels zu implementieren.

NTFS in /etc/fstab

Eine typische `fstab`-Zeile zur automatischen Integration einer NTFS-Partition in den Verzeichnisbaum sieht folgendermaßen aus:

```
# /etc/fstab
/dev/sda1     /media/win    ntfs-3g    uid=1000,gid=1000  0 0
```

Bei den meisten Distributionen können Sie das Dateisystem statt mit `ntfs-3g` auch einfach mit `ntfs` bezeichnen.

Streams

Streams sind eine Besonderheit des NTFS-Dateisystems: Eine NTFS-Datei kann aus mehreren Streams bestehen. Dabei hat jeder Stream dieselbe Funktion wie eine herkömmliche Datei. Beim gewöhnlichen Dateizugriff wird automatisch der Standardstream gelesen bzw. verändert.

Beim `ntfs-3g`-Treiber steuert die Option `streams_interface` den Zugriff auf Streams. In der Standardeinstellung `xattr` werden Streams wie Dateiattribute betrachtet. Der Zugriff auf Streams erfolgt durch die Kommandos `get-` bzw. `setfattr` aus dem Paket `attr` (siehe Abschnitt 15.7). `getfattr -d -e text` liefert eine Liste aller Attribute, wobei deren Inhalt in Textform angezeigt wird.

```
root#  mount /dev/sda1 /media/win
root#  cd /media/win
root#  cat > streamtest
 abc (Strg)+(D)
root#  setfattr -n user.stream1 -v "efg" streamtest
root#  setfattr -n user.stream2 -v "xyz" streamtest
root#  cat streamtest
abc
root#  getfattr -d -e text streamtest
# file: streamtest
user.stream1="efg"
user.stream2="xyz"
root#  cd
root#  umount /media/win
```

Alternativ können Sie auch mit `streams_interface=windows` arbeiten. Diese Einstellung aktiviert die Windows-typische Schreibweise in der Form `dateiname:streamname`.

```
root#  mount -o streams_interface=windows /dev/sda1 /media/win
root#  cd /media/win
root#  cat streamtest
abc
root#  cat streamtest:stream1
efg
```

Administration

Das Paket `ntfsprogs` enthält diverse Kommandos, die bei der Administration von NTFS-Dateisystemen helfen. Tabelle 25.8 gibt einen Überblick.

Kommando	Bedeutung
`mkntfs`	richtet ein NTFS-Dateisystem ein.
`ntfsclone`	kopiert ein NTFS-Dateisystem.
`ntfsinfo`	liefert Informationen über ein NTFS-Dateisystem.
`ntfslabel`	benennt eine NTFS-Partition.
`ntfsresize`	ändert die Größe des NTFS-Dateisystems.
`ntfsundelete`	versucht, gelöschte Dateien wiederherzustellen.

Tabelle 25.8 Kommandos des ntfsprogs-Pakets

25.11 CDs und DVDs

Daten-CDs und -DVDs

CD- und DVD-Laufwerke werden im Prinzip wie Festplatten verwaltet. Es gibt aber zwei wesentliche Unterschiede: Erstens ist bei einem CD/DVD-Laufwerk ein Wechsel der CD/DVD möglich, während Sie eine herkömmliche Festplatte im laufenden Betrieb nicht wechseln können. Zweitens verwenden Daten-CDs und -DVDs ein anderes Dateisystem: ISO 9660 oder UDF.

ISO 9660 und UDF

ISO 9660 ist ein allgemein akzeptierter Standard für Daten-CDs. Aufgrund einiger grundlegender Einschränkungen haben sich aber einige Erweiterungen etabliert: Die Unix-typische Rockridge-Extension erlaubt es, lange Dateinamen und Zugriffsrechte zu speichern. Die Windows-typische Joliet-Erweiterung sieht die Verwendung von Unicode-Zeichen in Dateinamen vor. Die El-Torito-Erweiterung ermöglicht es, einen Rechner direkt von der CD zu starten.

Das *Universal Disk Format* (UDF) ist der Nachfolger zu ISO 9660. Es wird auf vielen DVDs verwendet. DVDs können alternativ aber auch das ISO-9660-Format nutzen. Anders als unter ISO 9660 dürfen unter UDF Dateien größer als 2 GByte werden, Dateinamen können ohne irgendwelche Erweiterungen aus bis zu 255 Unicode-Zeichen bestehen, Read-Write-Medien werden besser unterstützt (Packet Writing) etc.

CD/DVD-Device-Namen

Tabelle 25.9 gibt an, welche Device-Namen beim Zugriff auf das CD/DVD-Laufwerk verwendet werden. Der Device-Name hängt davon ab, wie das Laufwerk angeschlossen ist (SCSI, SATA, USB oder Firewire). Die größte Trefferwahrscheinlichkeit gibt `/dev/scd0`. Auf die Device-Namen `/dev/hda`, `/dev/hdb` etc. werden Sie nur bei alten Rechnern stoßen. Mitunter gibt es auch Device-Dateien wie `/dev/cdrom`, `/dev/dvd` oder `/dev/dvd-recorder`. Dabei handelt es sich um Links auf die tatsächliche Device-Datei.

Device-Name	Bedeutung
`/dev/scd0` **oder** `/dev/sr0`	erstes CD/DVD-Laufwerk
`/dev/scd1` **oder** `/dev/sr1`	zweites CD/DVD-Laufwerk

Tabelle 25.9 CD/DVD-Device-Namen

Automatischer Betrieb

Bei den meisten Distributionen ist das Desktop-System so vorkonfiguriert, dass beim Einlegen einer Daten-CD oder -DVD automatisch ein Dateimanager-Fenster erscheint und den Inhalt des Datenträgers anzeigt. Sie können die CD/DVD jederzeit auswerfen, wahlweise durch den Knopf am Laufwerk oder über das Kontextmenü eines Laufwerk-Icons auf dem Desktop. Für diesen Komfort sind hinter den Kulissen die Linux-Hardware-Verwaltung und ein KDE-Dienst oder Gnome-Dämon zuständig.

Manueller Betrieb

Wenn Sie in einer Konsole oder mit einem Desktop ohne CD/DVD-Automatismen arbeiten, müssen Sie Ihre CDs/DVDs nach dem Einlegen manuell in den Verzeichnisbaum einbinden. Wie üblich variieren dabei die Device- und Verzeichnisnamen je nach Hardware und Distribution.

```
root#  mount -t iso9660 -o ro /dev/scd0 /media/dvd  (ISO-9660-CDs/DVDs)
root#  mount -t udf -o ro /dev/scd0 /media/dvd      (UDF-DVDs)
```

Standardmäßig sind alle Verzeichnisse und Dateien für alle Benutzer lesbar. Falls Sie Programme, die sich auf der CD bzw. DVD befinden, unmittelbar starten möchten, müssen Sie zusätzlich die Option `exec` angeben. Um internationale Dateinamen korrekt zu verarbeiten, sollten Sie die Option `iocharset=utf8` bzw. einfach `utf8` verwenden.

Bevor Sie die CD/DVD auswerfen können, müssen Sie explizit `umount` ausführen:

```
root#  umount /media/dvd
```

umount oder eject

Statt `umount` können Sie auch `eject` ausführen. Durch dieses Kommando wird die CD nicht nur aus dem Dateisystem gelöst, sondern auch gleich ausgeworfen. Falls es im Rechner mehrere Datenträger gibt, die ausgeworfen werden können, werden diese Möglichkeiten der Reihe nach getestet; der erste gefundene Datenträger wird ausgeworfen. Optional können Sie den gewünschten Datenträger durch den Device-Namen oder Mount-Punkt angeben.

Device is busy

Wenn `umount` den Fehler *device is busy* liefert, bedeutet das, dass ein anderes Programm noch Daten der CD-ROM nutzt. Das ist unter anderem auch dann der Fall, wenn in irgendeiner Shell ein Verzeichnis der CD-ROM geöffnet ist. Führen Sie dort `cd` aus, um in das Heimatverzeichnis zu wechseln. Bei der Suche nach dem Prozess, der die `umount`-Probleme verursacht, kann `fuser` helfen. Führen Sie `fuser -m /cdrom` aus!

/etc/fstab

Bei den meisten Distributionen fehlt aufgrund der oben beschriebenen Automatismen ein Eintrag für das CD/DVD-Laufwerk in `/etc/fstab` (es ist keiner notwendig). Wenn Sie CDs/DVDs häufig manuell in den Verzeichnisbaum einbinden, ist ein derartiger Eintrag aber zweckmäßig. Er sieht dann ähnlich wie das folgende Muster aus:

```
# /etc/fstab
/dev/scd0  /media/dvd udf,iso9660  users,noauto,ro  0 0
```

Jetzt reichen die Kommandos `mount /media/dvd` bzw. `umount /media/dvd` aus, um eine CD/DVD in den Verzeichnisbaum zu integrieren bzw. aus ihm zu lösen. Jeder Benutzer darf diese Kommandos ausführen.

Audio-CDs, Video-DVDs etc.

Audio-CDs

Audio-CDs werden anders als Daten-CDs behandelt. Sie werden nicht mit `mount` in das Dateisystem eingebunden, sondern mit speziellen Programmen direkt ausgelesen, unter KDE bzw. Gnome beispielsweise mit Amarok bzw. Rhythmbox. Auch das digitale Auslesen von Audio-Tracks ist möglich. Einen Überblick über Audio-Tools finden Sie in Kapitel 10, »Audio und Video«.

Video-DVDs

Video-DVDs verwenden in der Regel UDF. Zum Abspielen solcher DVDs benötigen Sie einen Video- oder Multimedia-Player.

CDs/DVDs brennen

Um CDs und DVDs zu brennen, verwenden Sie unter KDE das Programm K3B, unter Gnome Brasero bzw. in der Konsole `wodim` (siehe Abschnitt 15.5).

25.12 Externe Datenträger (USB, Firewire & Co.)

USB-Sticks, Speicherkarten von Digitalkameras und externe Festplatten haben ein gemeinsames Merkmal: Sie werden im laufenden Betrieb mit dem Computer verbunden und auch wieder gelöst. Intern werden nahezu alle derartigen Laufwerke wie SCSI-Laufwerke behandelt.

Automatischer Betrieb

Die Desktop-Systeme (KDE, Gnome) nahezu aller Distributionen reagieren beim Einstecken von Datenträgern damit, dass ein neues Fenster des Dateimanagers erscheint, das komfortabel Zugriff auf den Datenträger gibt. Eventuell erscheint auf dem Desktop auch ein Icon, das den Datenträger symbolisiert und Ihnen per Kontextmenü die Möglichkeit gibt, das Dateisystem explizit aus dem Verzeichnisbaum zu lösen.

Zuerst »umount«, dann Stecker/Kabel lösen!

Achten Sie darauf, sämtliche Partitionen eines Datenträgers explizit aus dem Verzeichnisbaum zu lösen, bevor Sie das Kabel zum Datenträger abziehen! Normalerweise stellt der Dateimanager dazu ein Kommando wie Auswerfen oder Sicher entfernen zur Verfügung. Hinter den Kulissen wird dann `umount` ausgeführt. Das stellt sicher, dass alle offenen Schreiboperationen ausgeführt werden, bevor die Verbindung zum Laufwerk tatsächlich gekappt wird. Wenn Sie auf diesen Schritt verzichten, riskieren Sie ein beschädigtes Dateisystem und fehlerhafte Dateien!

Unter KDE und Gnome ist es möglich, dass mehrere Benutzer parallel eingeloggt sind. In diesem Fall bekommt in der Regel der zuerst eingeloggte Benutzer Zugriffsrechte auf neu eingesteckte Datenträger. Dieser Sonderfall ist allerdings je nach Distribution unterschiedlich (oder gar nicht) gelöst und kann Probleme verursachen. Vermeiden Sie also Benutzerwechsel, wenn Sie mit externen Datenträgern arbeiten!

Hotplug-Interna

Die Hotplug-Verwaltung basiert bei aktuellen Distributionen auf einem Zusammenspiel des Kernels, des `udev`-Systems, des Kommunikationssystems D-Bus und des Programms PolicyKit. Bei älteren Installationen werden Sie vereinzelt auf die Programme `supermount`, `magicdev` oder `subfs/submount` stoßen, die aber allesamt nicht besonders gut funktionieren.

Manueller Betrieb

Beim Arbeiten im Textmodus bzw. mit einem Desktop-System ohne automatische Datenträgerverwaltung müssen Sie das entsprechende `mount`-Kommando selbst ausführen. Zuerst stellen Sie fest, welchen Device-Namen Ihr Gerät hat – in der Regel `/dev/sd`*x*, wobei *x* der alphabetisch erste momentan nicht genutzte Buchstabe ist. Einen Überblick über alle Datenträger und Partitionen gibt das Kommando `lsblk`. Beim folgenden Beispiel ist `/dev/sdc1` die erste und einzige Partition auf einem ca. 250 MByte großen USB-Memorystick:

```
root#  lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sda      8:0    0 232,9G  0 disk
  sda1   8:1    0   487M  0 part /boot/efi
  sda2   8:2    0  18,6G  0 part /
  sda3   8:3    0  15,9G  0 part [SWAP]
sdb      8:16   1   7,4G  0 disk
  ...
sdc      8:32   1   245M  0 disk
  sdc1   8:33   1   245M  0 part
sr0     11:0    1  1024M  0 rom
```

`parted` liefert nun Informationen darüber, welches Dateisystem sich auf den Partitionen befindet:

```
root#  parted /dev/sdc print
Modell: Hama FlashPen (scsi)
Festplatte  /dev/sdc:  245MiB
Partitionstabelle: msdos
Nummer  Anfang   Ende    Größe   Typ      Dateisystem  Flags
 1      0,02MiB  245MiB  245MiB  primary  fat16        boot, lba
```

USB-Memorysticks und Flash-Karten können auch wie eine sogenannte Superfloppy formatiert sein. Das bedeutet, dass es keine Partitionierungstabelle gibt. In diesem Fall wird das gesamte Laufwerk über den Device-Namen `/dev/sdc` angesprochen, anstatt wie im obigen Beispiel mit `/dev/sdc1`.

Wenn Sie die Device-Nummer wissen, ist alles Weitere einfach: Sie erstellen ein neues Verzeichnis und führen das folgende `mount`-Kommando aus:

```
root#  mkdir /media/memorystick
root#  mount /dev/sdc1 /media/memorystick
```

Externe Datenträger können die unterschiedlichsten Dateisystemtypen nutzen. In der Praxis kommt am häufigsten VFAT zum Einsatz. Das gilt auch für Speicherkarten für diverse elektronische Geräte.

Nachdem Sie alle Daten gelesen oder geschrieben haben, führen Sie wie üblich `umount` aus. Entfernen Sie auf keinen Fall die USB- oder Firewire-Verkabelung, bevor das `umount`-Kommando beendet ist – Sie riskieren Datenverluste!

```
root#  umount /media/memorystick
```

/etc/fstab

Nur `root` darf das Kommando `mount` ausführen. Wenn gewöhnliche Benutzer externe Datenträger selbst in den Verzeichnisbaum einbinden bzw. daraus wieder lösen sollen, fügen Sie in `fstab` eine entsprechende Zeile mit der Option `users` ein. Für einen USB-Memorystick mit VFAT-Dateisystem könnte diese Zeile so aussehen:

```
# /etc/fstab: USB-Stick
/dev/sdc1  /media/memorystick  vfat  users,gid=users,utf8,noatime,noauto  0 0
```

Damit kann jeder Benutzer den USB-Stick mit `mount /media/memorystick` in den Verzeichnisbaum einbinden und die enthaltenen Daten lesen und verändern. Die Vorgehensweise hat allerdings zwei gravierende Nachteile:

- Je nachdem, in welcher Reihenfolge die Geräte eingesteckt werden, ändert sich deren Device-Name. Wenn der USB-Stick als zweites oder drittes Gerät eingesteckt wird, lautet der Device-Name vielleicht `/dev/sdg`, und der Zugriff über das Verzeichnis `/media/memorystick` scheitert.
- Umgekehrt kann der obige `fstab`-Eintrag zum Zugriff auf einen anderen externen Datenträger genutzt werden, was ebenfalls nicht beabsichtigt ist.

Die beste Lösung für dieses Problem besteht darin, in `/etc/fstab` den Device-Namen des Datenträgers nicht direkt, sondern über einen `by-uuid`-Link anzugeben. Die UUID ermitteln Sie mit dem Kommando `blkid`:

```
root#  blkid /dev/sdc1
/dev/sdc1: UUID="4550-9BD2" TYPE="vfat"
```

Der dazu passende `fstab`-Eintrag wurde hier nur aus Platzgründen auf zwei Zeilen verteilt:

```
# /etc/fstab: USB-Stick
/dev/disk/by-uuid/4550-9BD2 /media/memorystick  vfat  \
                      users,gid=users,utf8,noatime,noauto 0 0
```

Prinzipiell wäre es auch möglich, die `fstab`-Zeile mit `UUID=4550-9BD2` einzuleiten. Das `mount`-Kommando funktioniert dann wie bei der obigen Variante, bei `umount` gibt es aber Probleme: Trotz des `UUID`-Eintrags trägt `mount` den Datenträger in `/etc/mtab` mit den gerade aktuellen Device-Namen ein. Daher stimmen bei `umount` die `/etc/fstab`-Zeile und die `/etc/mtab`-Zeile nicht überein, was zu einem Fehler führt.

25.13 Swap-Partitionen und -Dateien

Wenn der Arbeitsspeicher zur Ausführung aller Programme nicht ausreicht und Swap-Partitionen oder -Dateien zur Verfügung stehen, lagert Linux Teile des Speichers dorthin aus (Paging). Linux kann auf diese Weise mehr Speicher nutzen, als RAM verfügbar ist.

Das Einrichten einer Swap-Partition erfolgt normalerweise im Rahmen der Installation. Ob und wie viel Swap-Speicher zur Verfügung steht bzw. tatsächlich verwendet wird, überprüfen Sie mit dem Kommando `free`. Im Beispiel unten stehen 1519 MByte RAM und 2000 MByte Swap-Speicher zur Verfügung. Vom RAM werden zurzeit 401 MByte für Programme und Daten verwendet, der Rest wird als Puffer bzw. Cache für Dateien genutzt. Der Swap-Speicher ist momentan ungenutzt.

```
root#  free -m
             total       used       free     shared    buffers     cached
Mem:          1519       1479         39          0         67       1010
-/+ buffers/cache:        401       1117
Swap:         2000          0       2000
```

Wenn ein Rechner länger läuft, wird er zumeist irgendwann den Swap-Speicher nutzen, selbst wenn sehr viel RAM zur Verfügung steht. Der Grund: Der Kernel verwaltet einen Cache für Lesezugriffe auf Dateien. Wird eine Datei später wieder benötigt, kann sie aus dem Cache gelesen werden. Sobald der Cache größer ist als das ansonsten freie RAM, lagert Linux seit langer Zeit nicht mehr genutzte Speicherblöcke in die Swap-Partition aus. Das ist durchaus kein Zeichen dafür, dass zu wenig RAM zur Verfügung steht. Linux versucht lediglich, den verfügbaren Speicher möglichst effizient zu nutzen.

/etc/fstab

Die folgenden Zeilen zeigen zwei Einträge für Swap-Partitionen in `/etc/fstab`. Die Option `pri` bewirkt, dass die beiden Partitionen von Linux gleichwertig behandelt werden. Das sorgt für eine Geschwindigkeitssteigerung wie beim Striping oder bei RAID-0 (siehe Abschnitt 25.14), sofern sich die Partitionen auf zwei voneinander unabhängigen Festplatten befinden. Wenn es nur eine Swap-Partition gibt, geben Sie statt `pri=0` einfach `defaults` an.

```
# /etc/fstab: Swap-Partitionen
/dev/sda9    swap    swap    pri=1    0 0
/dev/sdb7    swap    swap    pri=1    0 0
```

Swap-Verhalten steuern

Wenn der Speicher im RAM knapp wird, entscheidet der Linux-Kernel nach einem relativ komplexen Algorithmus, ob Cache-Speicher zugunsten anderer Speicheranforderungen freigegeben wird oder ob zuletzt ungenutzte Speicherbereiche in die Swap-Partition ausgelagert werden sollen. Mit dem Kernelparameter `/proc/sys/vm/swappiness` können Sie selbst einstellen, ob der Kernel nach Möglichkeit eher den

Cache verkleinert oder Daten auslagert. Was Kernelparameter sind und wie Sie sie einstellen, erfahren Sie in Abschnitt 28.5.

Die Standardeinstellung für `swappiness` lautet 60, der mögliche Wertebereich reicht von 0 bis 100. 0 bedeutet, dass der Kernel Paging nach Möglichkeit vermeidet. 100 bedeutet, dass längere Zeit ungenutzter Speicher möglichst bald in einer Swap-Partition landet. Weitere Details zum `swappiness`-Parameter finden Sie auf folgenden Seiten:

http://lwn.net/Articles/83588
http://kerneltrap.org/node/3000

In der Praxis werden Sie das Swap-Verhalten am ehesten bemerken, wenn Sie Ihren Rechner über Nacht laufen lassen und in Ihrer Abwesenheit ein Programm auf viele Dateien der Festplatte zugreift, etwa ein Backup-Script oder ein Programm zur Erstellung eines Suchindex. Wegen der vielen Dateizugriffe wächst der Cache stark an. Mit `swappiness=60` oder einem noch höheren Wert wird der Kernel nun seit Stunden nicht genutzten Speicher auslagern. Das könnte beispielsweise die Speicherseiten von Firefox oder Gimp betreffen. Wenn Sie am nächsten Tag in Gimp weiterarbeiten möchten, wird es ein paar Sekunden dauern, um diese Seiten aus der Swap-Partition wieder in den Arbeitsspeicher zu übertragen. Mit `swappiness=0` vermeiden Sie diese Wartezeit.

Wie viel Swap-Speicher?

In der Vergangenheit lautete die Empfehlung, etwa das Zweifache des RAMs als Swap-Speicher vorzusehen. Mit zunehmender RAM-Größe ist diese Faustregel aber nur noch selten zielführend. Wenn Sie Linux vor allem als Desktop-System verwenden, reicht eine wesentlich kleinere Swap-Partition vollkommen aus (z. B. 512 MByte Swap-Speicher bei 2 GByte RAM).

Wenn Sie bei Notebooks den Ruhezustand (*Suspend to Disk*) nutzen möchten, was nach meinen Erfahrungen aber selten funktioniert, wird der gesamte Arbeitsspeicher in der Swap-Partition gespeichert. Das setzt voraus, dass die Swap-Partition größer ist als der Arbeitsspeicher, z. B. um den Faktor 1,5.

Wiederum andere Anforderungen werden an große Server-Systeme gestellt. Beispielsweise empfiehlt Oracle für seinen Datenbankserver je nach verfügbarem RAM unterschiedliche Faktoren zur Berechnung der Swap-Größe:

Bis 2 GByte:	Faktor 1,5
2 bis 8 GByte:	Faktor 1
Mehr als 8 GByte:	Faktor 0,75

Auf 32-Bit-Systemen beträgt die maximale Größe einer Swap-Partition 2 GByte. Sollten Sie mehr Swap-Speicher benötigen, können Sie einfach mehrere Swap-Partitionen verwenden. Noch sinnvoller ist dann aber ein Wechsel auf eine 64-Bit-Distribution.

Linux ohne Swap-Partition

Immer wieder taucht die Frage auf, ob man ganz auf eine Swap-Partition verzichten kann bzw. sollte, wenn man eine Menge RAM hat. Grundsätzlich funktioniert Linux auch ohne Swap-Speicher; ein Argument spricht aber für eine Swap-Partition: Sollte eines Ihrer Programme außer Kontrolle geraten oder aus anderen Gründen mehr Speicher brauchen als erwartet, ist der verfügbare Speicher irgendwann erschöpft. Das kann zum Absturz des nächsten Prozesses führen, der weiteren Speicher anfordert. Das kann irgendein Prozess sein, nicht unbedingt Ihr außer Kontrolle geratenes Programm.

Grundsätzlich ändert eine Swap-Partition nichts an diesem Problem – auch der Swap-Speicher ist ja begrenzt. Durch die immer intensivere Nutzung des Swap-Speichers laufen alle Programme aber immer langsamer, sodass Sie rechtzeitig bemerken, dass auf Ihrem Rechner etwas nicht stimmt. Bevor es zu einem Absturz kommt, können Sie das fehlerhafte Programm beenden, zur Not durch `kill`. Wenn Sie sich intensiver mit dem Thema befassen möchten, hier zwei Leseempfehlungen:

http://www.thomashertweck.de/linuxram.html
http://kerneltrap.org/node/3202

Neue Swap-Partition einrichten

Falls sich die Swap-Partition als zu klein herausstellt oder Sie aus anderen Gründen eine weitere Swap-Partition benötigen, richten Sie eine neue Partition ein. Als Partitionstyp geben Sie *Linux swap* an (Code 82 in `fdisk`). Nachdem die Partition mit `mkswap` formatiert worden ist, kann sie mit `swapon` aktiviert werden. Wenn das klappt, ergänzen Sie `/etc/fstab`.

Aus Geschwindigkeitsgründen sollten Sie möglichst nur eine Swap-Partition pro Festplatte einrichten. Idealerweise sollte sich die Swap-Partition auf einer sonst nicht oder wenig genutzten Festplatte befinden.

Swap-Dateien

Statt einer Swap-Partition kann Speicher auch in eine Swap-Datei ausgelagert werden. Diese Notlösung verlangsamt aber den Zugriff auf das Dateisystem. Der Vorteil einer Swap-Datei besteht darin, dass keine eigene Partition erforderlich ist.

Um eine neue Swap-Datei anzulegen, erzeugen Sie mit dem Kommando `dd` eine leere Datei mit einer vorgegebenen Größe. Dabei wird als Datenquelle `/dev/zero` verwendet. Die Größenangabe ergibt sich aus dem Produkt der Parameter `bs` und `count`, hier also 1 GByte. Anschließend wird die Swap-Datei wie eine Swap-Partition mit `mkswap` formatiert und mit `swapon` aktiviert:

```
root#  dd bs=1M if=/dev/zero of=/swapfile count=1024
root#  mkswap /swapfile 1000
root#  sync
root#  swapon -v /swapfile
swapon on device /swapfile
```

Swap-Dateien können wie Swap-Partitionen in `fstab` aufgenommen werden:

```
# Erweiterung zu /etc/fstab
/swapfile  none      swap          sw       0  0
```

Beachten Sie, dass das `btrfs`-Dateisystem Swap-Dateien nicht unterstützt!

25.14 RAID

Was RAID ist, welche RAID-Level es gibt und wodurch sich Hardware-RAID, BIOS-Software-RAID und Linux-Software-RAID voneinander unterscheiden, habe ich bereits in Abschnitt 2.7 erklärt. Dieser Abschnitt hier behandelt ausschließlich die Administration von Linux-Software-RAID auf der Basis von `mdadm`. Aus Platzgründen gehe ich zudem nur auf die RAID-Level 0 und 1 ein.

Bitte beachten Sie, dass es im Internet diverse veraltete RAID-HOWTOs gibt. Sie beschreiben die Konfiguration auf der Basis der `raidtools`, die bei modernen Linux-Distributionen nicht mehr gebräuchlich sind.

Falls Sie das neue Dateisystem `btrfs` nutzen und die RAID-Level 0, 1, 5, 6 oder 10 verwenden möchten, können Sie auf die hier beschriebenen RAID-Funktionen des *Multi Device Drivers* verzichten. `btrfs` enthält selbst RAID-Funktionen.

Grundlagen

mdadm

Sofern Sie nicht schon während der Installation einen RAID-Verbund eingerichtet haben, müssen Sie das Paket `mdadm` installieren. Es enthält das gleichnamige Kommando zur RAID-Administration.

`mdadm` empfiehlt auch die Installation eines Mail-Servers (Mail Transfer Agents), damit bei RAID-Problemen eine E-Mail an den Administrator versandt werden kann. Wenn Sie sich noch nicht mit dem Thema E-Mail-Server beschäftigt haben, sollten Sie darauf aber verzichten. Unter Debian und Ubuntu verwenden Sie deswegen bei der Installation mit `apt-get` die Option `--no-install-recommends`.

md_mod

Linux-intern ist für Software-RAID der sogenannte *Multi Devices Driver* zuständig. Bei einigen Distributionen ist dieser Treiber direkt in den Kernel integriert, andernfalls wird das Kernelmodul `md_mod` (ehemals einfach `md`) während des Systemstarts

automatisch geladen. `dmesg` sollte auf jeden Fall entsprechende Meldungen enthalten. Vergewissern Sie sich auch, dass die Pseudodatei `/proc/mdstat` existiert. Sie gibt Auskunft über den aktuellen Zustand des RAID-Systems.

`md_mod` setzt eine logische Schicht zwischen den Treiber zum Festplattenzugriff (SATA/IDE/SCSI) und den Dateisystemtreiber (z. B. `ext4`). `md_mod` bildet aus mehreren Festplatten-Partitionen ein neues, logisches Device, auf das der Dateisystemtreiber zugreifen kann (`/dev/md`*n*). Nach der RAID-Konfiguration verwenden Sie nicht mehr direkt eine Festplattenpartition, sondern eine RAID-Partition `/dev/md`*n*, um darauf Ihr Dateisystem einzurichten.

mdadm.conf

Die zentrale RAID-Konfigurationsdatei ist `/etc/mdadm/mdadm.conf`. Diese Datei sollte neben einigen globalen RAID-Einstellungen Daten über alle aktiven RAID-Verbunde enthalten. Eine vollständig neue Konfigurationsdatei können Sie mit `/usr/share/mdadm/mkconf` erstellen. Das ist dann praktisch, wenn die Konfigurationsdatei verloren gegangen ist oder wenn Sie auf einem Live- oder Rescue-System arbeiten.

Die übliche Vorgehensweise bei der Konfiguration ist ungewöhnlich: Zuerst richten Sie durch die Ausführung von `mdadm`-Kommandos die gewünschten RAID-Verbunde ein oder modifizieren sie. Anschließend erweitern Sie die zumeist schon vorhandene Datei `mdadm.conf` auf der Grundlage der nun vorliegenden Konfiguration. Die Eckdaten der aktiven RAID-Verbunde ermitteln Sie mit `mdadm --examine --scan`, und Sie fügen sie mit `>>` zur existierenden Konfigurationsdatei hinzu.

```
root#  mdadm --examine --scan >> /etc/mdadm/mdadm.conf
```

Falls `mdadm.conf` schon vorher RAID-Definitionen enthielt, müssen Sie diese mit einem Editor entfernen, damit kein Verbund doppelt definiert ist. Die folgenden Zeilen zeigen ein Beispiel für den Aufbau von `mdadm.conf`:

```
# Datei /etc/mdadm/mdadm.conf
DEVICE partitions
CREATE owner=root group=disk mode=0660 auto=yes
HOMEHOST <system>
MAILADDR root
ARRAY /dev/md0 level=raid1 num-devices=2 UUID=36c426b0:...
ARRAY /dev/md1 level=raid1 num-devices=2 UUID=71dfc474:...
ARRAY /dev/md2 level=raid1 num-devices=2 UUID=e0f65ea0:...
```

Status

Aktuelle Informationen über den RAID-Status gibt die schon erwähnte Datei `/proc/mdstat`. Im folgenden Beispiel gibt es drei RAID-1-Verbunde, die aus jeweils zwei Partitionen bestehen. Alle drei Verbunde sind aktiv und laufen fehlerfrei: `[UU]` bedeutet, dass die erste und die zweite Partition des Verbunds *up* ist (also problemlos funktioniert).

```
root#  cat /proc/mdstat
Personalities : [raid0] [raid1] [linear] [multipath]
                [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sda1[0] sdb1
      979840 blocks [2/2] [UU]
md1 : active raid1 sda2[0] sdb2
      1951808 blocks [2/2] [UU]
md2 : active raid1 sda3[0] sdb3
      387730624 blocks [2/2] [UU]
unused devices: <none>
```

Nun ist es natürlich nicht praktikabel, ständig in dieser Datei nachzusehen, ob alles in Ordnung ist. Wesentlich zweckmäßiger ist es, dass `mdadm --monitor` diese Aufgabe übernimmt. Zumeist wird dieses Kommando durch das Init-System beim Hochfahren des Rechners gestartet. Je nach Distribution kann es aber sein, dass Sie `mdadm` vorher entsprechend konfigurieren müssen. Dazu führen Sie beispielsweise unter Ubuntu das folgende Kommando aus:

```
root#  dpkg-reconfigure mdadm
```

Vier Dialoge führen nun durch die `mdadm`-Konfiguration: Im ersten Schritt können Sie eine automatische Redundanzüberprüfung aktivieren, die einmal pro Monat (am ersten Sonntag um 1:06 Uhr) die Daten auf den RAID-Partitionen miteinander vergleicht. Diese Kontrolle hilft dabei, Festplattendefekte auch in Bereichen bzw. Dateien festzustellen, die schon länger nicht mehr gelesen oder verändert wurden. Intern erfolgt die Redundanzüberprüfung durch das Kommando `checkarray`, das durch das Cron-Script `/etc/cron.d/mdadm` gestartet wird.

Im zweiten und dritten Schritt aktivieren Sie die Überwachung des RAID-Status und geben an, an welche E-Mail-Adresse eventuell auftretende Warnungen bzw. Fehlerberichte versandt werden sollen. Intern erfolgt die Überwachung durch `mdadm --monitor`. Unter Debian und Ubuntu wird das Kommando vom Init-System gestartet, sofern `/etc/default/mdadm` die Einstellung `START_DAEMON=true` enthält. Die E-Mail-Adresse wird in `/etc/mdadm/mdadm.conf` gespeichert. Sollte ein Problem auftreten, sendet `mdadm` eine Benachrichtigungs-E-Mail an `root`. Damit das funktioniert, muss auf dem Rechner ein Mail-Server installiert sein (siehe Kapitel 37, »Postfix und Dovecot«)! Die E-Mail-Adresse können Sie in `/etc/mdadm/mdadm.conf` mit der Variablen `MAILADDR` einstellen.

Im vierten Schritt geben Sie schließlich an, ob Ihr Server beim Neustart auch dann starten soll, wenn er einen Defekt in einer RAID-Partition feststellt. Bei Root-Servern ist das empfehlenswert.

GRUB und RAID

GRUB 0.97 ist nur zu RAID-1 kompatibel. Wenn Sie für die Systempartition einen anderen RAID-Level wählen und mit GRUB 0.97 arbeiten, brauchen Sie daher eine zusätzliche Bootpartition. GRUB 2 ist dagegen zu allen RAID-Leveln kompatibel und kann den Kernel und die Initrd-Datei direkt aus dem RAID-Verbund lesen. Es ist keine separate Bootpartition erforderlich.

Administration

RAID-0-Verbund einrichten

Für RAID-0 benötigen Sie zumindest zwei noch ungenutzte Partitionen. Die Partitionen sollten gleich groß sein, das ist aber nicht unbedingt erforderlich. Je nach RAID-Level führt eine unterschiedliche Größe aber dazu, dass die Geschwindigkeit nicht optimal ist bzw. dass Teile der größeren Partition nicht genutzt werden.

Die Partitionen müssen als RAID-Partitionen gekennzeichnet sein. Wenn Sie zum Partitionieren `fdisk` verwenden, stellen Sie die Partitions-ID-Nummer mit dem Kommando T auf den hexadezimalen Wert `fd`. Bei `parted` führen Sie `set` *`partitionsnummer`* `raid on` aus.

Im Folgenden werden die Partitionen mit den Device-Namen `/dev/sda3` und `/dev/sdc1` zu einem RAID-0-System verbunden. Die Partitionen müssen für sich nicht formatiert werden. `fdisk -l` zeigt die Beispielkonfiguration:

```
root#  fdisk -l /dev/sda /dev/sdc
Disk /dev/sda: 320.0 GB, 320072933376 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sda1               1         973     7815591   83  Linux
/dev/sda2             974        1034      489982+  82  Linux swap / Solaris
/dev/sda3            1035        2251     9775552+  fd  Linux raid autodetect
Disk /dev/sdc: 320.0 GB, 320072933376 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1               1        1217     9775521   fd  Linux raid autodetect
```

Ein einziges `mdadm`-Kommando reicht aus, um aus den beiden Partitionen `/dev/sda3` und `/dev/sdc1` einen RAID-0-Verbund zu bilden:

```
root#  mdadm --create /dev/md0 --level=0 --raid-devices=2 /dev/sda3 /dev/sdc1
mdadm: array /dev/md0 started.
```

Als Nächstes müssen Sie auf der neuen virtuellen Partition `/dev/md0` ein Dateisystem anlegen. Diese Partition kann mit `mount` in das Linux-Dateisystem eingebunden werden. Die Partition wird hier über das Verzeichnis `/striped` angesprochen – selbstverständlich können Sie stattdessen auch einen anderen Namen verwenden.

```
root#  mkfs.ext4 /dev/md0
root#  mkdir /striped
root#  mount /dev/md0 /striped/
```

Wenn alles klappt, sollten Sie die neue Partition in `/etc/fstab` aufnehmen. Bei allen aktuellen Linux-Distributionen wird das RAID-System beim nächsten Systemstart durch das Init-System automatisch initialisiert.

```
# in /etc/fstab
/dev/md0    /striped   ext4    defaults    0 0
```

Außerdem müssen Sie die Konfigurationsdatei `mdadm.conf` um eine Zeile erweitern, die den neuen RAID-0-Verbund beschreibt. `mdadm --examine --scan` liefert die Zeile in der vorgeschriebenen Syntax.

RAID-1-Verbund einrichten

Die Vorgehensweise beim Einrichten eines RAID-1-Verbunds ist exakt dieselbe wie bei RAID-0. Einzig das Kommando zum Einrichten des RAID-Systems sieht ein wenig anders aus und enthält nun `--level=1` statt `--level=0`:

```
root#  mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sda3 /dev/sdc1
mdadm: array /dev/md0 started.
root#  mkfs.ext4 /dev/md0
```

Falls Sie – wie oben beschrieben – `/dev/md0` vorher probeweise als RAID-0-Partition eingerichtet haben, müssen Sie die Partition mit `mount` aus dem Verzeichnisbaum lösen und mit `mdadm --stop` deaktivieren, bevor Sie `mdadm --create` ausführen können! `mdadm` erkennt dennoch, dass die Partitionen `/dev/sda3` und `/dev/sdc1` bisher anders genutzt wurden, und verlangt eine Bestätigung, dass Sie `/dev/md0` wirklich neu einrichten möchten.

RAID-1-Verbund testen

Um die Funktionsweise eines RAID-1-Verbunds zu testen – möglichst noch bevor Sie kritische Daten dort gespeichert haben –, markieren Sie eine Partition als defekt:

```
root#  mdadm /dev/md0 --fail /dev/sdc1
```

Sofern im Rahmen des Systemstarts `mdadm --monitor` gestartet wurde, sollte `root` auf dem lokalen Rechner nun sofort eine Verständigungs-E-Mail erhalten. Ansonsten können Sie den Verbund weiter nutzen; alle Änderungen werden nun aber nur noch auf der verbleibenden Festplattenpartition gespeichert. `/proc/mdstat` zeigt nun den Status `U_`. Das bedeutet, dass eine Partition läuft (`U` für *up*) und eine fehlt (`_`).

```
root#  cat /proc/mdstat
md0 : active raid1 sda3
      979840 blocks [2/1] [_U]
```

Um `/dev/sdc1` wieder zu `/dev/md0` hinzuzufügen, müssen Sie die als defekt gekennzeichnete Partition zuerst explizit entfernen:

```
root#  mdadm --remove /dev/md0 /dev/sdc1
root#  mdadm --add    /dev/md0 /dev/sdc1
```

Es beginnt nun die automatische Resynchronisation der beiden Partitionen, die je nach der Größe des Verbunds geraume Zeit dauert (Richtwert: ca. 20 Minuten pro 100 GByte). Immerhin können Sie in dieser Zeit weiterarbeiten. Das Dateisystem wird allerdings langsamer als sonst reagieren.

```
root#  cat /proc/mdstat
md0 : active raid1 sda3 sdc1[2]
      485454656 blocks [2/1] [U_]
      [>.....................]  recovery =  3.0% (14577856/485454656)
                               finish=72.8min speed=107724K/sec
root#  mdadm --detail /dev/md0   (während die Synchronisation läuft)
...
          State : clean, degraded, recovering
 Active Devices : 1
Working Devices : 2
 Failed Devices : 0
  Spare Devices : 1
 Rebuild Status : 75% complete
...
    Number   Major   Minor   RaidDevice State
       0       3        3        0      active sync   /dev/sda3
       1       0        0        -      removed
       2      22        2        1      spare rebuilding   /dev/sdc1
root#  mdadm --detail /dev/md0   (nach Abschluss der Synchronisation)
...
          State : clean
 Active Devices : 2
Working Devices : 2
 Failed Devices : 0
  Spare Devices : 0
...
    Number   Major   Minor   RaidDevice State
       0       3        3        0      active sync   /dev/sda3
       1      22        2        1      active sync   /dev/sdc1
```

Defekte RAID-1-Festplatte austauschen

Allzu oft kommt es ja zum Glück nicht vor – aber wenn tatsächlich eine Festplatte Defekte zeigt und `mdadm` einzelne Partitionen dieser Festplatte als defekt kennzeichnet, sollten Sie alle Partitionen dieser Festplatte explizit aus den jeweiligen RAID-Verbunden entfernen:

```
root#  mdadm --remove   /dev/md0 /dev/sdc1
...
```

Anschließend müssen Sie schleunigst eine Ersatzfestplatte besorgen. Die neue Festplatte muss genug Platz bieten, um auf ihr genauso große Partitionen zu erzeugen wie auf den existierenden Festplatten.

Passen Sie auf, dass Sie wirklich die defekte Festplatte ausbauen und nicht irrtümlich die noch funktionierende! Diese Empfehlung klingt trivial, aber wenn ein Rechner zwei oder mehrere baugleiche Festplatten enthält, ist es gar nicht so einfach, die richtige Festplatte zu finden. Eindeutig ist nur die Seriennummer! Welche Seriennummer mit welchem Device-Namen verbunden ist, verraten `hdparm` oder `smartctl`. Beide Kommandos können nur ausgeführt werden, wenn vorher das gleichnamige Paket installiert wird.

```
root#  smartctl -i /dev/sdc
...
Device Model:     SAMSUNG HD403LJ
Serial Number:    S0NFJ1MPA07356

root#  hdparm -i /dev/sdc
/dev/sdb:
...
Model=SAMSUNG HD403LJ, FwRev=CT100-12,
SerialNo=S0NFJ1MPA07356
```

Nach dem Austausch der Festplatte müssen Sie auf der neuen Festplatte neue Partitionen einrichten, die mindestens so groß sind wie die bereits vorhandenen RAID-Partitionen. Eine große Hilfe kann dabei das Kommando `sfdisk` sein (siehe Abschnitt 25.3). Die Partitionen müssen als RAID-Partitionen gekennzeichnet werden (hexadezimaler ID-Code `fd`). Nach diesen Vorbereitungsarbeiten ist der Rest ein Kinderspiel: Sie fügen die Partitionen der neuen Festplatte den RAID-Verbunden hinzu:

```
root#  mdadm --add /dev/md0 /dev/sdc1
...
```

Der Kernel beginnt nun, die Partitionen der neuen Festplatte mit den vorhandenen RAID-Daten zu synchronisieren. Den Status der Synchronisation verfolgen Sie mit `cat /proc/mdstat`.

Üben für den Notfall

Ich empfehle Ihnen nachdrücklich, eine RAID-Reparatur auf einem Testsystem in Ruhe auszuprobieren. Einen Festplattendefekt können Sie simulieren, indem Sie eine Partition mit `mdadm --fail` als defekt kennzeichnen oder das Kabel zu einer Festplatte vorübergehend lösen (aber natürlich nicht im laufenden Betrieb!).

RAID-Verbund deaktivieren

`mdadm --stop` deaktiviert einen RAID-Verbund. Das darauf enthaltene Dateisystem muss vorher mit `umount` aus dem Verzeichnisbaum gelöst werden!

```
root#  umount /mount-verzeichnis/
root#  mdadm --stop /dev/md0
```

RAID-Verbund wieder aktivieren

Nur wenn Sie nach `mdadm --stop` keine Veränderungen an den zugrunde liegenden Partitionen durchgeführt haben, können Sie den RAID-Verbund mit `mdadm --assemble` ohne Datenverluste wieder zusammensetzen und aktivieren:

```
root#  mdadm --assemble /dev/md0 /dev/sda3 /dev/sdc1
mdadm: /dev/md0 has been started with 2 drives.
```

Partitionen analysieren

In allen Festplattenpartitionen, die Sie mit `mdadm` zu RAID-Partitionen zusammengefügt haben, wurden in einem speziellen Block Kontextinformationen (Metadaten) gespeichert. Diese Informationen können Sie mit `mdadm --query` auslesen, beispielsweise um den Status eines unbekannten Systems zu ermitteln.

```
root#  mdadm --query /dev/sda3
/dev/sda3: is not an md array
/dev/sda3: device 0 in 2 device active raid1 md0.  Use mdadm --examine
  for more detail.
root#  mdadm --query /dev/md0
/dev/md0: 9.32GiB raid1 2 devices, 0 spares. Use mdadm --detail for more detail.
/dev/md0: No md super block found, not an md component.
```

`mdadm --examine` liefert Detailinformationen zu einer Partition, die Teil eines RAID-Verbunds ist:

```
root#  mdadm --examine /dev/sda3
/dev/sda3:
     Raid Level : raid1
   Raid Devices : 2
  Total Devices : 2
            ...
 Active Devices : 2
Working Devices : 2
      Number   Major   Minor   RaidDevice State
   0     0       3        3        0      active sync   /dev/sda3
   1     1      22        1        1      active sync   /dev/sdc1
```

Analog dazu liefert `mdadm --detail` Detailinformationen zu einem RAID-Verbund:

```
root#  mdadm --detail /dev/md0
/dev/md0:
        Version : 00.90.03
  Creation Time : Thu Nov  9 16:55:35 2006
     Raid Level : raid1
     Array Size : 9775424 (9.32 GiB 10.01 GB)
    Device Size : 9775424 (9.32 GiB 10.01 GB)
   Raid Devices : 2
  Total Devices : 2
...
```

Kontrolle der Dateiintegrität

Woher wissen Sie, dass wirklich alle redundant gespeicherten Daten korrekt sind? Normalerweise führt das RAID-System Integritätstests nur durch, wenn es Dateien liest oder schreibt. Viele Dateien werden aber oft monatelang nicht angerührt. Um also mit Sicherheit festzustellen, dass die Festplatten in Ordnung sind, muss das RAID-System sämtliche Datenblöcke lesen und die redundanten Daten vergleichen. Dieser Vorgang wird auch *Scrubbing* genannt.

```
root#  echo check > /sys/block/mdn/md<n>/sync_action
```

Wenn dabei Fehler auftreten, können diese repariert werden:

```
root#  echo check > /sys/block/mdn/md<n>/sync_action
```

Unter Debian und Ubuntu kümmert sich darum das Script `/usr/share/mdadm/checkarray`, das monatlich via `cron` gestartet wird. Dieselbe Funktion erfüllt unter Fedora das `cron`-Script `/etc/cron.weekly/99-raid-check`.

RAID-Metadaten löschen

Die Speicherung der RAID-Metadaten in ansonsten ungenutzten Sektoren der RAID-Partition ist normalerweise eine nützliche Sache. Wenn Sie die Festplatte zu einem späteren Zeitpunkt aber anders einsetzen möchten, können die RAID-Metadaten zum Problem werden: Linux-Installationsprogramme und `mdadm` erkennen die Überreste der RAID-Konfiguration und wollen partout nicht einsehen, dass diese Partitionen jetzt anders genutzt werden sollen. Abhilfe schafft das folgende Kommando, das auf alle RAID-Partitionen angewendet werden muss:

```
root#  mdadm --zero-superblock /dev/sda3
```

Falls Sie auch mit BIOS-RAID experimentiert haben, können Sie dessen Metadaten auf allen Festplatten mit `dmraid -r -E` löschen.

25.15 Logical Volume Manager (LVM)

Der Logical Volume Manager setzt eine logische Schicht zwischen das Dateisystem und die Partitionen der Festplatte. Das Prinzip, die Vorzüge und die Nomenklatur von LVM wurden bereits in Abschnitt 2.7 erläutert. Dieser Abschnitt konzentriert sich auf die LVM-Administration.

Konfigurationshilfen

Manche Distributionen stellen grafische Werkzeuge zur Administration von LVM im laufenden Betrieb zur Verfügung. Bei Fedora und Red Hat hilft Ihnen `system-config-lvm` bei der Konfiguration, bei SUSE das YaST-Modul System • LVM.

Auch wenn die Programme die LVM-Konfiguration erleichtern, setzen sie doch ein gutes Verständis der LVM-Konzepte voraus. Beachten Sie, dass bei Größenänderungen in der Regel nur die *Logical Volumes* (LVs) geändert werden, nicht aber die darauf

enthaltenen Dateisysteme. Deren Größe müssen Sie bei Verkleinerungen vorher, bei Vergrößerungen nachher selbst verändern.

dm_mod

Linux-intern ist für LVM das Kernelmodul `dm_mod` zuständig. Bei manchen Distributionen sind die LVM-Funktionen direkt in den Kernel kompiliert und erscheinen daher nicht im `lsmod`-Ergebnis.

GRUB

Sofern LVM bereits während der Installation eingerichtet wird, kann sich auch die Systempartition in einem LV befinden. Allerdings ist nur GRUB 2 LVM-kompatibel. Wenn Sie mit GRUB 0.97 arbeiten, brauchen Sie eine eigene, LVM-freie Bootpartition.

RAID

Sie können LVM und RAID kombinieren. Üblicherweise richten Sie dazu zuerst einen RAID-Verbund ein und nutzen dann das resultierende Device `/dev/mdn` als *Physical Volume* (PV).

Ein Sonderfall ist RAID-0. Diese RAID-Variante wird von LVM direkt unterstützt. Um diese Funktion nutzen zu können, müssen Sie auf zwei oder mehr Festplatten jeweils ein PV einrichten. Diese PVs werden zu einer *Volume Group* (VG) vereint. Nun können Sie mit `lvcreate -i n` ein LV einrichten, das die Daten auf mehrere PVs und damit auf *n* PVs verteilt.

LVM-Kommandos

Die LVM-Administration erfolgt durch eine ganze Palette von Kommandos. Die Namen der Kommandos beginnen mit `pv`, `vg` oder `lv`, je nachdem, ob sie zur Bearbeitung von Physical Volumes, Volume Groups oder Logical Volumes gedacht sind. Die wichtigsten Vertreter sind in Tabelle 25.10 aufgezählt. Die Kommandos sind Teil des Pakets `lvm2`, das möglicherweise erst installiert werden muss.

Anstelle der Einzelkommandos können Sie die gesamte LVM-Administration auch mit dem Kommando `lvm` ausführen, wobei Sie als ersten Parameter den gewünschten Befehl übergeben. Die Kommandos `lvcreate` und `lvm lvcreate` sind also gleichwertig.

Beispiele

Die folgenden Beispiele zeigen die Anwendung einiger LVM-Kommandos. Dabei gehe ich davon aus, dass während der Installation kein LVM eingerichtet wurde. Nun soll die zusätzliche Festplatte `/dev/sdc` via LVM genutzt werden. Die Partitionierung der Festplatte sieht so aus:

```
root#  fdisk -l /dev/sdc
Disk /dev/sdc: 320.0 GB, 320072933376 bytes
   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1               1        1217     9775521   8e  Linux LVM
/dev/sdc2            1218        2434     9775552+  8e  Linux LVM
```

Um LVM zu initialisieren, führen Sie `modprobe` und `vgscan` aus. Sobald ein LVM-System eingerichtet ist, wird das LVM-Kernelmodul automatisch während des Rechnerstarts ausgeführt. Die manuelle Initialisierung ist also nur beim ersten Mal erforderlich:

```
root#  modprobe dm_mod
root#  vgscan
  Reading all physical volumes (this may take a while...)
  No volume groups found
```

Kommando	Funktion
lvcreate	richtet ein neues LV in einer VG ein.
lvdisplay	liefert Detailinformationen zu einem LV.
lvextend	vergrößert ein LV.
lvreduce	verkleinert ein LV.
lvremove	löscht ein LV.
lvrename	gibt dem LV einen neuen Namen.
lvscan	listet alle LVs auf.
pvcreate	kennzeichnet eine Partition oder ein Device als PV.
pvdisplay	liefert Detailinformationen zu einem PV.
pvremove	entfernt die PV-Kennzeichnung eines ungenutzten PVs.
pvscan	listet alle PVs auf.
vgchange	ändert die Attribte einer VG.
vgcreate	erzeugt eine neue VG aus einem oder mehreren PVs.
vgdisplay	liefert Detailinformationen zu einer VG.
vgextend	vergrößert eine VG um ein PV.
vgmerge	vereint zwei VGs.
vgreduce	verkleinert eine VG um ein ungenutztes PV.
vgrename	gibt einer VG einen neuen Namen.
vgscan	listet alle VGs auf.

Tabelle 25.10 LVM-Kommandoübersicht

Aus didaktischen Gründen richte ich LVM zuerst auf der Partition `/dev/sdc1` ein und erweitere das LVM-System später um `/dev/sdc2`. Wenn ohnedies klar ist, dass Sie die gesamte Festplatte für LVM nutzen möchten, ist es natürlich einfacher, gleich eine Partition in Maximalgröße mit `pvcreate` für die LVM-Nutzung zu kennzeichnen.

```
root#  pvcreate /dev/sdc1
  Physical volume "/dev/sdc1" successfully created
```

Nun müssen alle PVs zu einer VG zusammengefasst werden. In diesem Beispiel gibt es zwar vorerst nur ein einziges PV, der Schritt ist aber dennoch erforderlich. An das

Kommando `vgcreate` muss auch der gewünschte Name der VG übergeben werden. In diesem Beispiel bekommt die VG den Namen `myvg1`:

```
root#  vgcreate myvg1 /dev/sdc1
  Volume group "myvg1" successfully created
```

`myvg1` stellt jetzt eine Art Datenpool dar, der aber noch ungenutzt ist. Zur Nutzung müssen Sie innerhalb von `myvg1` ein LV einrichten, also eine Art virtueller Partition. Dazu müssen Sie an das Kommando `lvcreate` drei Informationen übergeben: die gewünschte Größe des LVs, den Namen des neuen LVs und den Namen der existierenden VG:

```
root#  lvcreate -L 2G -n myvol1 myvg1
  Logical volume "myvol1" created
```

Durch das Kommando wird gleichzeitig auch die Datei `/dev/myvg1/myvol1` erzeugt. Dabei handelt es sich um einen Link auf die Datei `/dev/mapper/myvg1-myvol1`. Das LV kann jetzt unter einem dieser beiden Device-Namen wie eine gewöhnliche Festplattenpartition verwendet werden.

Um in einem Logical Volume ein Dateisystem einzurichten, verwenden Sie beispielsweise `mkfs.ext4` oder `mkfs.xfs`:

```
root#  mkfs.ext4 /dev/myvg1/myvol1
```

Mit `mount` können Sie sich davon überzeugen, dass alles geklappt hat:

```
root#  mkdir /test
root#  mount /dev/myvg1/myvol1 /test
```

Dateisystem vergrößern

Ein Grund dafür, LVM überhaupt zu verwenden, besteht darin, ein Dateisystem nachträglich vergrößern zu können, ohne die Festplatte neu partitionieren zu müssen. Im folgenden Beispiel wird das vorhin eingerichtete Dateisystem (`/dev/myvg1/myvol1` via `/test`) von ursprünglich 2 GByte auf 3 GByte vergrößert. `df` zeigt die Kapazität von `/test` vor der Änderung:

```
root#  df -h -T /test
Dateisystem   Typ    Größe Benut  Verf Ben% Eingehängt auf
/dev/mapper/myvg1-myvol1
              ext4     2,0G  760M  1,2G  40% /test
```

Dazu muss zuerst das Logical Volume vergrößert werden. Zu diesem Zweck müssen Sie den Device-Namen und die neue Größe an `lvextend` übergeben. Anschließend wird auch das `ext4`-Dateisystem entsprechend vergrößert.

```
root#  lvextend -L 3G /dev/myvg1/myvol1
  Extending logical volume myvol1 to 3,00 GB
  Logical volume myvol1 successfully resized
root#  resize2fs /dev/myvg1/myvol1
```

`df` beweist, dass alles funktioniert hat:

```
root#  df -h -T /test
Dateisystem   Typ    Größe Benut  Verf Ben% Eingehängt auf
/dev/mapper/myvg1-myvol1
              ext4    3,0G  76OM  2,1G  27% /test
```

Grundsätzlich ist auch eine Verkleinerung möglich. Allerdings müssen Sie dazu das betroffene Dateisystem zuerst aus dem Verzeichnisbaum lösen, mit `fsck.ext4` überprüfen und schließlich mit `resize2fs` verkleinern. Erst jetzt dürfen Sie mit `lvreduce` das zugrunde liegende LV verkleinern.

Solange im Speicherpool (in der Volume Group) noch Platz ist, können Logical Volumes leicht vergrößert werden. Aber was tun Sie, wenn auch die VG voll ist? In diesem Fall legen Sie auf einer beliebigen Festplatte Ihres Rechners eine neue Partition an, richten diese Partition als Physical Volume ein und fügen sie mit `vgextend` zur Volume Group hinzu.

Die beiden folgenden Kommandos demonstrieren dies für die Partition `/dev/sdc2`. `myvg1` bekommt damit eine Gesamtkapazität von rund 19 GByte, wovon 16 GByte frei sind:

```
root#  pvcreate /dev/sdc2
  Physical volume "/dev/sdc2" successfully created
root#  vgextend  myvg1 /dev/sdc2
  Volume group "myvg1" successfully extended
root#  vgdisplay myvg1
...
  VG Size               18,64 GB
  Alloc PE / Size       640 / 2,50 GB
  Free  PE / Size       4132 / 16,14 GB
...
```

Snapshots

Mit LVM können Sie Snapshots anlegen. Ein Snapshot ist ein unveränderliches Abbild des Dateisystems zu einem bestimmten Zeitpunkt. Der Snapshot kann wie ein eigenes Dateisystem in den Verzeichnisbaum integriert werden. Wenn sich das zugrunde liegende Dateisystem ändert, werden die originalen Daten für den Snapshot archiviert. Sie müssen bereits beim Anlegen des Snapshots angeben, wie viel Speicherplatz LVM für diesen Zweck reservieren soll. Ist dieser Speicherplatz erschöpft, wird der Snapshot ungültig und kann nicht mehr verwendet werden.

LVM-Snaphots bieten wesentlich weniger Funktionen als `btrfs`-Snapshots. LVM-Snapshots werden in der Regel für Backups verwendet. Sie stellen sicher, dass sich die Dateien während des Backups nicht ändern, das Backup also konsistent ist.

Die folgenden Kommandos zeigen, wie Sie zuerst einen Snapshot des LV `myvol1` erstellen, diesen im Verzeichnis `/media/backup` in den Verzeichnisbaum einbinden,

ein Backup davon erstellen, den Snapshot wieder aus dem Verzeichnisbaum lösen und schließlich löschen. Während das Backup läuft, kann das LV `myvol1` uneingeschränkt weiterbenutzt werden (z. B. als Speicherplatz für einen Datenbank-Server). Die während des Backups durchgeführten Änderungen dürfen allerdings 100 MByte nicht überschreiten. Während des Backups können Sie mit `lvdisplay /dev/vg1/snap` ermitteln, wie viel Prozent dieses Speicherplatzes bereits in Verwendung sind.

Beachten Sie, dass Sie den Device-Namen des zugrunde liegenden Logical Volumes in der Form `/dev/vgname/lvname` angeben müssen, nicht in der Form `/dev/mapper/vgname-lvname`!

```
root#  lvcreate -s -L 100M snap /dev/myvg1/myvol1
 Logical volume snap created
root#  mkdir /media/backup
root#  mount /dev/vg1/snap /media/backup
root#  backup-script /media/backup     (Backup erstellen)
root#  umount /media/backup
root#  lvremove /dev/vg1/snap
```

25.16 SMART

SMART steht für *Self-Monitoring, Analysis and Reporting Technology* und ist ein Merkmal nahezu aller marktüblichen IDE-, SATA- und SCSI-Festplatten. Dank SMART werden verschiedene Parameter der Festplatte regelmäßig gespeichert. Diese Parameter erlauben einen Rückschluss auf eventuelle Defekte der Festplatte und auf ihre voraussichtliche Lebensdauer. Über eine spezielle Schnittstelle können die SMART-Parameter ausgelesen werden. Die regelmäßige Überwachung der Parameter durch das Betriebssystem ist eine Art Frühwarnsystem. Damit lassen sich Festplattenprobleme erkennen, bevor Datenverluste eintreten. Dieser Abschnitt gibt einen Überblick über die unter Linux verfügbaren Werkzeuge zum Auslesen der SMART-Parameter.

Voraussetzungen

Damit SMART genutzt werden kann, müssen einige Voraussetzungen erfüllt sein:

- Die Festplatte muss SMART unterstützen. Das können Sie beispielsweise mit `hdparm -I /dev/sdx` feststellen.
- Es muss sich um eine interne Festplatte oder um eine eSata-Festplatte handeln. Bei externen USB- und Firewire-Festplatten können die SMART-Funktionen leider nicht genutzt werden.
- Bei Festplatten, die über einen Hardware-RAID-Controller gesteuert werden, können die SMART-Funktionen nur in Einzelfällen genutzt werden. Details gibt `man smartctl` bei der Option `-d`.

smartctl

Sie können den SMART-Status aber auch über die Kommandozeile ermitteln, was vor allem bei Server-Installationen wichtig ist. Das dazu erforderliche Kommando `smartctl` ist bei den meisten Distributionen Teil des Pakets `smartmontools`, das vielfach extra installiert werden muss. Je nach Distribution wird dabei automatisch auch ein E-Mail-Server (MTA) installiert, um SMART-Benachrichtigungen per E-Mail zu versenden. Auf einem Server ist das zweckmäßig, auf einem Desktop-Rechner hingegen zumeist nicht. Bei Debian und Ubuntu vermeiden Sie die Installation des E-Mail-Servers, wenn Sie an `apt-get` die Option `--no-install-recommends` übergeben.

In der einfachsten Form liefert `smartctl` diverse Statusinformationen. Wenn `smartctl -i` in der letzten Zeile *SMART support is Disabled* meldet, aktivieren Sie SMART mit `smartctl -s on`.

```
root#  smartctl -i /dev/sdb
smartctl 5.41 ..., Copyright (C) 2002-11 by Bruce Allen
Device Model:     SAMSUNG SSD 830 Series
Serial Number:    S0Z3NYAC210778
LU WWN Device Id: 5 002538 043584d30
Firmware Version: CXM03B1Q
User Capacity:    128.035.676.160 bytes [128 GB]
Sector Size:      512 bytes logical/physical
Device is:        Not in smartctl database [for details use: -P showall]
ATA Version is:   8
ATA Standard is:  ACS-2 revision 2
Local Time is:    Wed Jul  4 09:45:45 2012 CEST
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

`smartctl -H` bzw. `smartctl --health` gibt an, ob die Festplatte momentan in Ordnung ist und voraussichtlich die nächsten 24 Stunden noch funktionieren wird. Sollte `smartctl` hier nicht *PASSED* als Ergebnis liefern, sollten Sie *sofort* damit beginnen, ein komplettes Backup durchzuführen!

```
root#  smartctl -H /dev/sda
...
SMART overall-health self-assessment test result: PASSED
```

`smartctl -A` bzw. `smartctl --attributes` liefert eine Liste von herstellerspezifischen Festplattenattributen. Für diese Attribute existiert kein festgeschriebener Standard, die wichtigsten Attribute werden aber von vielen Festplattenherstellern unterstützt. Bei der Interpretation der Werte sind zwei Spalten entscheidend: `VALUE` gibt den aktuellen Wert an, `THRESH` den Grenzwert. Wenn der aktuelle Wert den Grenzwert unterschreitet, sind Probleme zu erwarten bzw. hat die Festplatte ihre vorgesehene Lebensdauer erreicht.

Die Werte sind auf einen Basiswert von 100 normalisiert. Beispielsweise beginnt `Power_On_Hour` bei einer neuen Festplatte mit dem Wert 100. Nach einer bestimm-

ten Anzahl von Betriebsstunden sinkt der Wert auf 99 etc. Die bisher absolvierten Betriebsstunden gehen aus der `RAW_VALUE`-Spalte hervor. Bei der Testfestplatte lautet der Wert 451, das sind ca. 56 Arbeitstage zu je 8 Stunden. Manche Festplatten messen die Betriebsdauer in Minuten oder Sekunden. In diesem Fall erreichen Sie durch `-v 9,minutes` oder `-v 9,seconds` eine korrekte Anzeige.

Die folgenden, etwas gekürzten Ergebnisse stammen von einer circa ein dreiviertel Jahre alten SATA-Festplatte. Es gibt keinerlei Anzeichen für Probleme.

```
root#  smartctl -A /dev/sda
...
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          VALUE WORST THRESH TYPE      UPDATED  RAW_VALUE
  1 Raw_Read_Error_Rate     109   099   006    Pre-fail  Always   24386832
  3 Spin_Up_Time            096   095   000    Pre-fail  Always   0
  4 Start_Stop_Count        100   100   020    Old_age   Always   167
  5 Reallocated_Sector_Ct   100   100   036    Pre-fail  Always   0
  7 Seek_Error_Rate         065   060   030    Pre-fail  Always   3391200
  9 Power_On_Hours          100   100   000    Old_age   Always   451
...
198 Offline_Uncorrectable   100   100   000    Old_age   Offline  0
199 UDMA_CRC_Error_Count    200   200   000    Old_age   Always   0
```

`smartctl -l error` liefert Informationen über die fünf zuletzt aufgetretenen Fehler. Oft ist das Ergebnis einfach leer (*no errors logged*). Vereinzelte Fehler, die sich nicht wiederholen, sind im Regelfall kein Anlass zur Beunruhigung.

```
root#  smartctl -l error /dev/sda
SMART Error Log Version: 1
No Errors Logged
```

Selbsttest durchführen

SMART sieht verschiedene Varianten von Selbsttests vor, um den aktuellen Zustand der Festplatte noch genauer zu ermitteln. Derartige Tests starten Sie mit `smartctl -t short/long`. Ein kurzer Test dauert wenige Minuten, ein ausführlicher Test (`long`) unter Umständen mehrere Stunden. Der Test wird im Hintergrund durchgeführt; Sie können ganz normal weiterarbeiten. Nachdem das Testende erreicht ist, sehen Sie sich mit `smartctl -l selftest` das Ergebnis an. Die Spalte *remaining* besagt dabei, wie weit der Selbsttest bereits ausgeführt ist. Wenn der Wert größer als 0 Prozent ist, läuft der Test noch! *LifeTime* gibt an, wie viele Stunden die Festplatte bereits im Betrieb war. *LBA* gibt den Ort (Sektor) des ersten Fehlers an. Im folgenden Ergebnis wurden drei Selbsttests ausgeführt: einer unmittelbar nach dem Einbau der Platte nach 40 Betriebsstunden, die anderen beiden nach ca. 2600 Stunden.

```
root#  smartctl -t short /dev/sda
Num  Test_Description  Status                  Remaining  LifeTime  LBA
# 1  Extended offline  Completed without error   00%      2592     -
# 2  Short offline     Completed without error   00%      2591     -
# 3  Short offline     Completed without error   00%        40     -
```

Automatische Überwachung (smartd)

`smartctl` ist sicherlich ein interessantes Werkzeug, um Informationen über die Festplatte zu sammeln. Für eine regelmäßige Überwachung aller Festplatten ist das Kommando aber zu unhandlich. Diese Aufgabe übernimmt das Programm `smartd`. Dabei handelt es sich um einen Dämon (Systemdienst). Die Kommandos für den automatischen Start variieren je nach Distribution und sind in Abschnitt 16.5 zusammengefasst.

`smartd` wird durch `/etc/smartd.conf` gesteuert. Bei einigen Distributionen wertet das Init-Script auch die Dateien `/etc/sysconfig/smartmontools` oder `/etc/default/smartmontools` aus. Diese Dateien enthalten zusätzliche Kommandooptionen für `smartd`. Bei Debian und Ubuntu müssen Sie in `smartmontools` die Einstellung `start_smartd=yes` vornehmen!

Eine einfache Konfiguration für einen Rechner mit zwei SATA-Festplatten (`/dev/sda` und `/dev/sdb`) sieht folgendermaßen aus:

```
# Datei /etc/smartd.conf
/dev/sda -d sat -H -m root -M test
/dev/sdb -d sat -H -m root -M test
```

Das bedeutet, dass die »Gesundheit« der angegebenen Festplatten alle halbe Stunde überwacht wird (wie durch `smartctl -H`). Wird dabei ein Fehler festgestellt, sendet `smartd` eine E-Mail an den lokalen Benutzer `root`. (Das setzt allerdings einen lokalen E-Mail-Server voraus.) `-d sat` kennzeichnet die Festplatten als SATA-Geräte. `-M test` dient zum Testen, ob der E-Mail-Versand prinzipiell funktioniert. Starten Sie `smartd`:

```
root#  service smartd start
```

Wenn Sie die Test-E-Mail erhalten haben, entfernen Sie `-M test` aus der Konfiguration. Eine Menge weiterer Konfigurationsbeispiele finden Sie in der mit `smartmontools` mitgelieferten Datei `smartd.conf`.

25.17 SSD-TRIM

Linux läuft auf SSDs (Solid State Disks) vollkommen problemlos – und natürlich viel schneller als auf herkömmlichen Festplatten. Allerdings unterscheidet sich die Nutzung von SSDs in einem Punkt von herkömmlichen Festplatten: Für die interne Optimierung der Speicherzellen ist es erforderlich, dass das Betriebssystem die SSD darüber informiert, welche Speicherblöcke des Dateisystems momentan ungenutzt sind (etwa, weil eine Datei gelöscht wurde). Dieser Vorgang wird SSD-TRIM genannt. Die technischen Hintergründe können Sie in der Wikipedia nachlesen:

http://de.wikipedia.org/wiki/Solid-State-Drive

Keine mir bekannte Linux-Distribution führt standardmäßig die TRIM-Funktion aus. Diese Standardeinstellung lässt sich damit begründen, dass der daraus resultierende Performance-Verlust bei modernen SSDs und normaler Nutzung relativ klein ist. Zudem gibt es unterschiedliche Verfahren, das SSD-TRIM durchzuführen – und jede ist mit Vor- und Nachteilen verbunden.

TRIM-Varianten

Linux-Profis, denen die optimale Geschwindigkeit ihrer SSD ein Anliegen ist, müssen sich selbst um das SSD-TRIM kümmern. Sie haben die Wahl zwischen zwei Varianten: dem Online-TRIM, bei dem Linux die SSD bei jeder gelöschten Datei sofort benachrichtigt, oder dem Batch-TRIM, das in regelmäßigen Abständen (z. B. einmal pro Woche) durchgeführt wird.

Online-Trim oder Batch-Trim?

Online-Trim hat den Nachteil, dass die SSD-internen Aufräumarbeiten gerade dann ausgeführt werden, wenn die SSD ohnedies beschäftigt ist – nämlich während intensiver Schreibvorgänge. Das Online-TRIM verlangsamt *jeden* Schreibvorgang.

Gegen das Batch-TRIM spricht der Umstand, dass dabei alle ausstehenden TRIM-Operationen eines ganzen Tages oder einer ganzen Woche ausgeführt werden. Während dieser Prozess läuft, ist jeder SSD-Zugriff deutlich langsamer.

Persönlich ist mir das Batch-TRIM lieber. Zum einen ist die Konfiguration einfacher, zum anderen kann ich bei Servern den Batch-Trim in der Nacht ausführen, womit der laufende Betrieb kaum beeinträchtigt wird.

Online-TRIM

Um das Online-TRIM-Verfahren zu aktivieren, müssen Sie in die Datei `/etc/fstab` für die betroffenen Dateisysteme die Option `discard` einfügen. Diese Option steht für die Dateisysteme `ext4`, `btrfs` und `xfs` zur Verfügung. Achten Sie darauf, dass Sie in `/etc/fstab` keine Syntaxfehler einbauen! Die Liste der `mount`-Optionen darf kein Leerzeichen enthalten.

```
# Datei /etc/fstab
UUID=018e... / ext4 errors=remount-ro,user_xattr,discard 0 1
```

Batch-TRIM

Ein manuelles Batch-TRIM stoßen Sie im Terminal-Fenster mit dem Kommando `fstrim` an:

```
root#  fstrim -v /
/: 6493835264 bytes were trimmed
```

Sie können das TRIM-Kommando auch auf größere Datenblöcke einschränken. Damit werden nur freie Datenblöcke ab der angegebenen Mindestgröße an die SSD gemeldet. `fstrim` kann dann wesentlich schneller ausgeführt werden und erzielt dennoch eine sehr gute Wirkung.

```
root#  fstrim -m 64K -v /
```

Um den Prozess zu automatisieren, richten Sie eine neue Cron-Systemdatei ein (optional mit der Option `-m`). Falls Sie Ihr Dateisystem über mehrere Partitionen verteilt haben, müssen Sie `fstrim` für jeden `mount`-Punkt ausführen.

```
# Datei /etc/cron.weekly/fstrim
/sbin/fstrim /
```

Einschränkungen und Sonderfälle

TRIM funktioniert problemlos im Zusammenspiel mit LVM. Software-RAID unterstützt TRIM erst ab der Kernelversion 3.7. Wenn Sie Ihr Dateisystem verschlüsseln, ist die Freigabe ungenutzter Datenblöcke durch TRIM zwar grundsätzlich möglich; die Sicherheit der verschlüsselten Daten wird dadurch aber vermindert.

Grundsätzlich kann die `mount`-Option `discard` auch für die Swap-Partition verwendet werden. Bei Desktop-Systemen ist das nicht erforderlich, weil Linux bei jedem Rechnerstart die gesamte Swap-Partition per TRIM freigibt. Bei einem Server, der über Monate läuft, kann die Option aber unter Umständen zweckmäßig sein.

25.18 Verschlüsselung

Notebooks und USB-Sticks können verloren gehen bzw. werden gestohlen. Schlimmer als der eigentliche Verlust des Geräts ist oft der Umstand, dass damit wichtige Daten in fremde Hände geraten: der Zugang zum Online-Banking, Versicherungsnummern, Krankenakten, Firmengeheimnisse, militärisch relevante Informationen etc. Das ist unnötig. Eine relativ simple Verschlüsselung des Dateisystems reicht aus, um die Daten wirksam zu schützen. Dieser Abschnitt gibt einige Hintergrundinformationen zum Umgang mit verschlüsselten Dateien und Dateisystemen.

Einzelne Dateien verschlüsseln

gpg

Eine einzelne Datei verschlüsseln Sie am einfachsten mit dem Kommando `gpg`. `gpg -c` fordert Sie zweimal zur Angabe eines Passworts auf, verschlüsselt dann die angegebene Datei und speichert das Ergebnis unter dem Namen `datei.gpg`. Dabei kommt standardmäßig der Verschlüsselungsalgorithmus CAST5 zur Anwendung. Die ursprüngliche Datei können Sie nun löschen. `gpg -d` stellt die Datei wieder her.

```
user$  gpg -c datei
Geben Sie die Passphrase ein:  **********
Geben Sie die Passphrase nochmals ein:  **********
user$  gpg -d datei.gpg > datei
Geben Sie die Passphrase ein:  **********
```

gpg kann zur Codierung bzw. Decodierung auch einen öffentlichen bzw. privaten Schlüssel verwenden, kann Dateien signieren, Schlüssel verwalten etc. Die Beschreibung der unzähligen Optionen in der man-Seite ist dementsprechend rund 50 Seiten lang! Die manuelle Verwendung von gpg ist aber eher unüblich. Häufiger wird gpg von E-Mail-Clients eingesetzt, um (mehr oder weniger automatisch) E-Mails zu signieren oder zu verschlüsseln.

Ein Dateisystem verschlüsseln (USB-Stick, externe Festplatte)

dm_crypt und LUKS

In der Vergangenheit wurden unzählige Verfahren zur Verschlüsselung von Dateisystemen entwickelt: CryptoFS, eCryptfs, Enc-FS, Loop-AES und LUKS. Ein Teil dieser Verfahren ist noch immer im Einsatz, andere wurden – oft aus Sicherheitsgründen – wieder verworfen. Momentan ist das *Linux Unified Key Setup* (kurz LUKS) die populärste Spielart.

LUKS basiert auf dem Kernelmodul dm_crypt, das den auch für LVM eingesetzten Linux-Device-Mapper um Kryptografiefunktionen erweitert. Das Modul ist eine logische Schicht zwischen den verschlüsselten Rohdaten auf der Festplatte und dem Dateisystem, so wie es der Linux-Anwender sieht. dm_crypt unterstützt diverse Verschlüsselungsalgorithmen. dm_crypt wird oft mit LVM kombiniert, das ist aber keineswegs notwendig; Sie können dm_crypt auch auf einem LVM-freien System einsetzen!

LUKS fügt den verschlüsselten Daten einen Header mit Metainformationen hinzu. Der Header gibt unter anderem an, mit welchem Verfahren die Daten verschlüsselt sind. LUKS vereinfacht die Integration von verschlüsselten Datenträgern in Linux ganz erheblich.

cryptsetup

Um verschlüsselte Dateisysteme einzurichten, nehmen Sie das Kommando cryptsetup aus dem gleichnamigen Paket zu Hilfe. Die folgenden Zeilen zeigen, wie Sie einen USB-Stick (/dev/sdh1) zuerst als Crypto-Device formatieren (luksFormat) und das Device dann unter dem willkürlich gewählten Namen mycontainer aktivieren (luksOpen). Naturgemäß sind Ihre Daten nur so sicher wie Ihr Passwort bzw. die aus mehreren Wörtern bestehende Passphrase. Empfohlen wird eine Passwortlänge von zumindest 20 Zeichen.

Anschließend können Sie /dev/mapper/mycontainer wie eine Festplattenpartition oder ein LV nutzen – also ein Dateisystem einrichten, dieses in den Verzeichnisbaum einbinden etc. Nach umount müssen Sie daran denken, das Crypto-Device wieder zu deaktivieren (luksClose), um /dev/sdh1 freizugeben. Erst jetzt dürfen Sie den USB-Stick ausstecken.

```
root#  cryptsetup luksFormat /dev/sdh1
Daten auf /dev/sdh1 werden unwiderruflich überschrieben.
Are you sure? (Type uppercase yes):  YES
Enter LUKS passphrase:  **********
Verify passphrase:  **********
Command successful.
root#  cryptsetup luksOpen /dev/sdh1 mycontainer
Enter LUKS passphrase:  **********
root#  mkfs.ext4 /dev/mapper/mycontainer
root#  mount /dev/mapper/mycontainer /test
root#  touch /test/xy
root#  umount /test/
root#  cryptsetup luksClose mycontainer
```

Selbstverständlich können Sie statt eines USB-Sticks auch eine Partition einer internen oder externen Festplatte, ein RAID-Device oder ein Logical Volume Ihres LVM-Systems verwenden. Dazu ersetzen Sie einfach `/dev/sdh1` durch den Device-Namen der Partition bzw. des LVs.

Standardmäßig verwendet `cryptsetup` den Verschlüsselungsalgorithmus AES mit einer Schlüssellänge von 128 Bit. Sie können sich davon mit `cryptsetup luksDump` überzeugen: Dieses Kommando liefert die Crypto-Metainformationen, die LUKS in einem speziellen Sektor des Datenträgers speichert.

```
root#  cryptsetup luksDump /dev/sdh1
LUKS header information for /dev/sdh1
Version:        1
Cipher name:    aes
Cipher mode:    cbc-essiv:sha256
Hash spec:      sha1
Payload offset: 1032
MK bits:        128
...
```

Wenn Sie einen anderen Verschlüsselungsalgorithmus oder einen längeren Schlüssel einsetzen möchten, übergeben Sie die gewünschten Daten mit den Optionen `-c` und `-s` an `cryptsetup luksFormat`. Welche Algorithmen zur Auswahl stehen, verrät `cat /proc/crypto`. Als sicher gelten zurzeit die Algorithmen AES und TwoFish. Beachten Sie, dass Verschlüsselungsalgorithmen ein Forschungsgebiet sind, in dem sich vieles schnell ändert: Immer wieder stellen sich Algorithmen als weniger sicher als gedacht heraus. Eine kurze Beschreibung der Algorithmen können Sie im Gentoo-Wiki nachlesen:

http://de.gentoo-wiki.com/wiki/DM-Crypt

Mit `cryptsetup luksAddKey` können Sie den Zugriff auf ein LUKS-Device durch insgesamt acht verschiedene Passwörter absichern. Das erlaubt die gemeinsame Nutzung eines Datenträgers, bei der jeder Benutzer sein eigenes Passwort verwendet.

luksFormat

`luksFormat` erleichtert das Einrichten einer verschlüsselten Partition oder eines verschlüsselten Datenträgers ein wenig. Das Kommando führt zuerst `cryptsetup luksFormat` und dann `mkfs.vfat` auf. Wenn Sie einen anderen Dateisystemtyp wünschen, müssen Sie ihn mit `-t` angeben.

Tipp

Nach der Ausführung des Kommandos (oft aber auch dann, wenn Fehler aufgetreten sind), bleibt ein aktives Crypto-Device `/dev/mapper/luksformat`*n* zurück. Bevor Sie den Datenträger entfernen oder nochmals als Crypto-Device einrichten können, müssen Sie `cryptsetup luksClose luksFormat`*n* ausführen!

Desktop-Nutzung

Wenn Sie LUKS-formatierte externe Datenträger mit Ihrem Rechner verbinden und unter Gnome oder KDE arbeiten, wird der Datenträger automatisch als Crypto-Device erkannt. Es erscheint ein Dialog, in dem Sie das Verschlüsselungspasswort angeben müssen. Anschließend wird der Datenträger in das Dateisystem eingebunden. Der Container-Name für `/dev/mapper` lautet `luks_crypto_`*uuid*. Beim Aushängen wird auch `luksClose` ausgeführt – die Nutzung des verschlüsselten Datenträgers könnte nicht einfacher sein!

crypttab

Wenn Sie ein verschlüsseltes Dateisystem in einer Partition einer lokalen Festplatte eingerichtet haben, wollen Sie vermutlich, dass dieses Dateisystem beim Hochfahren des Rechners in den Verzeichnisbaum eingebunden wird. Zur Automatisierung dieses Vorgangs enthält das Paket `cryptsetup` bereits die erforderlichen Initrd- und Init-V-Scripts. Diese setzen allerdings voraus, dass das Crypto-Device in die Datei `/etc/crypttab` eingetragen wird.

Der Aufbau dieser Datei ist einfach: Die erste Spalte gibt den gewünschten Namen für `/dev/mapper` an, die zweite Spalte den Device-Namen, die dritte Spalte die Datei, aus der der Schlüssel gelesen werden soll (z. B. von einem USB-Stick), oder `none`, wenn das Verschlüsselungspasswort interaktiv eingegeben wird, und die vierte Spalte enthält Optionen.

Im folgenden Beispiel soll das Device `/dev/sda7` unter dem Namen `/dev/mapper/cdisk1` eingerichtet werden. Das Passwort soll während des Rechnerstarts angegeben werden, und das Crypto-Device wurde mit LUKS eingerichtet. Eine Menge weiterer Optionen sind in `man crypttab` beschrieben.

```
# Datei /etc/crypttab
# Mapper-Name   Device          Schlüsseldatei   Optionen
cdisk1          /dev/sda7       none             luks
```

Damit das Crypto-Device nicht nur aktiviert, sondern sein Dateisystem auch in den Verzeichnisbaum eingebunden wird, muss auch `/etc/fstab` ergänzt werden. Die folgende Zeile bewirkt, dass das Dateisystem über das Verzeichnis `/media/private-data` genutzt werden kann:

```
# Datei /etc/fstab
...
/dev/mapper/cdisk1    /media/private-data    ext4    defaults    0 0
```

Anschließend starten Sie den Rechner neu und testen, ob alles funktioniert.

Nachteile

Die Verschlüsselung einer Partition ist mit Nachteilen verbunden. Zum einen erfolgen sämtliche Dateioperationen spürbar langsamer als im Normalbetrieb – und umso langsamer, je aufwendiger (und sicherer) das Verschlüsselungsverfahren ist. Verwenden Sie nach Möglichkeit eine schnelle CPU mit mehreren Cores! Zum anderen müssen Sie bei jedem Bootvorgang das Passwort eingeben. Das ist nicht nur lästig, sondern macht auch einen Neustart in Abwesenheit unmöglich. Grundsätzlich werden Sie mit verschlüsselten Partitionen zumeist nur auf lokalen PCs arbeiten, nicht oder nur in Ausnahmefällen auf Servern.

TrueCrypt

Eine interessante Alternative zur hier präsentierten Vorgehensweise auf der Basis von `dm_crypt` und LUKS ist TrueCrypt. Diese Verschlüsselungssoftware ist auch für Windows und Mac OS X verfügbar und erlaubt daher einen leichten Datenaustausch über die Grenzen von Linux hinaus. Der Quellcode ist zwar Open Source, einige Teile sind aber nicht GPL-kompatibel. Deswegen ist TrueCrypt in den gängigen Distributionen nicht enthalten.

http://www.truecrypt.org

ecryptfs (Ubuntu)

Ubuntu bietet die Möglichkeit, das ganze Heimatverzeichnis zu verschlüsseln. Das verschlüsselte Verzeichnis wird beim Login automatisch in das Dateisystem eingebunden und beim Logout wieder entfernt. Intern kommen dabei nicht `dm_crypt` und LUKS zum Einsatz, sondern das Dateisystem `ecryptfs`. Persönlich bin ich kein Fan von diesem Verschlüsselungsverfahren, weil es bei Hardware- oder Boot-Problemen sehr schwierig ist, die verschlüsselten Daten zu retten (auch wenn Sie Ihren Schlüssel kennen).

Gesamtes System verschlüsseln

Mit der im vorigen Abschnitt vorgestellten Datei `/etc/crypttab` ist es nur noch ein kleiner Schritt von der Verschlüsselung einer lokalen Partition (z. B. `/home`) zur Verschlüsselung des gesamten Systems inklusive der Systempartition. Zwei Details sind wichtig: Zum einen kann GRUB auf die verschlüsselten Daten nicht zugreifen – deswegen ist unbedingt eine eigene, nichtverschlüsselte Bootpartition erforderlich. Zum anderen ist zum Zugriff auf die Systempartition die Eingabe des Verschlüsselungspassworts erforderlich; die dafür notwendigen Funktionen müssen als Scripts in die Initrd-Datei integriert werden. (Das `cryptsetup`-Paket enthält alle erforderlichen Dateien.)

Vorweg ist aber zu klären, wer die Verschlüsselung des gesamten Systems überhaupt braucht: Eigentlich sollte es ja reichen, nur die privaten Dateien in `/home` zu verschlüsseln. Allerdings kann auch die Systempartition für den Notebook-Dieb, so er denn tatsächlich an den Daten interessiert ist, aufschlussreich sein: `/var/cache` oder `/var/tmp` können Überreste von versandten E-Mails, ausgedruckten Dokumenten, gelesenen PDFs etc. enthalten; `/var/log` dokumentiert, wer wann auf dem Computer gearbeitet hat; die Swap-Partition enthält womöglich ausgelagerte Datenblöcke mit sicherheitskritischen Informationen etc. Kurzum: Wenn Sie Ihre Daten bzw. Ihre Privatsphäre am Rechner wirklich vollständig schützen wollen, müssen Sie wohl oder übel das gesamte System verschlüsseln.

Installation

Die meisten großen Distributionen bieten im Installationsprogramm eine Option, um das gesamte System zu verschlüsseln. Allerdings müssen Sie bei Distributionen, die mehrere Installationsverfahren oder -medien zur Wahl stellen, in der Regel die traditionelle Variante verwenden; Installationsprogramme, die von einer Live-CD oder -DVD starten, sind prinzipbedingt ungeeignet! Die folgende Liste zählt geeignete Installationsmedien für die wichtigsten Distributionen auf:

Debian:	alle Standard-CDs/DVDs (inklusive NetInstall, aber keine Live-CDs)
Fedora:	Installation von einer DVD (keine Live-CDs)
openSUSE:	Installation von einer DVD (keine Live-CDs)
Ubuntu:	Standardinstallation ab Version 12.10

Bei Debian und Ubuntu wählen Sie die Partitionierungsvariante VERSCHLÜSSELTES LVM-SYSTEM, bei Fedora aktivieren Sie im Partitionierungsdialog die Option VERSCHLÜSSELTES SYSTEM. Bei openSUSE wählen Sie bei der Partitionierung die Optionen LVM-BASIERT und VERSCHLÜSSELT.

Systemaufbau

Der Aufbau des verschlüsselten Systems sieht bei den meisten Distributionen einheitlich aus: Es wird eine unverschlüsselte Bootpartition für GRUB eingerichtet sowie eine zweite Partition, die verschlüsselt ist und als Physical Volume für LVM dient. Auf diese Weise sind alle via LVM eingerichteten Partitionen (Swap-Partition, Systempartition, Datenpartitionen) automatisch verschlüsselt. Außerdem muss nicht für jede Partition ein eigenes Passwort definiert werden; vielmehr reicht ein zentrales Passwort für das gesamte LVM-System. Abbildung 25.3 zeigt den schematischen Aufbau eines derartigen Systems, wobei ich die Bezeichnung der Devices bzw. LVs von Fedora übernommen habe.

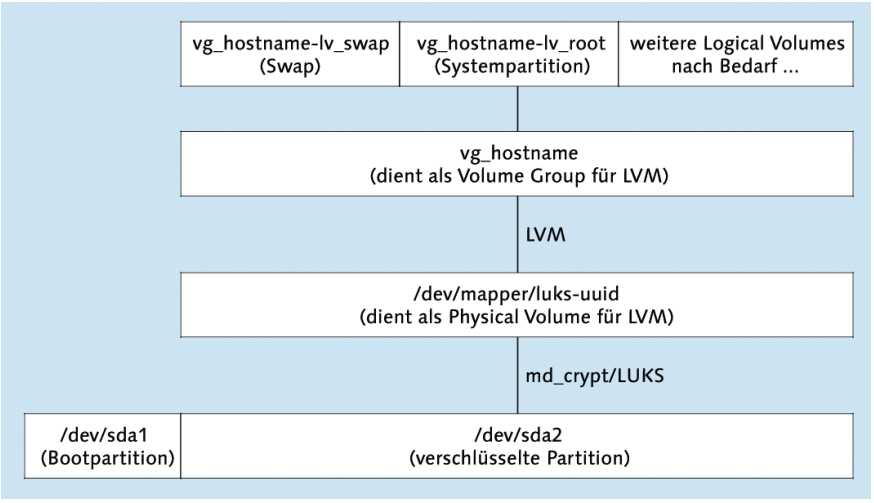


Abbildung 25.3 Vollständig verschlüsseltes Linux-System

Natürlich gibt es zu dem in Abbildung 25.3 präsentierten Aufbau viele Alternativen. Eine mögliche Variante besteht darin, auf LVM zu verzichten und jede Partition für sich zu verschlüsseln. Für die Swap-Partition kann dabei ein Zufallsschlüssel verwendet werden, der bei jedem Systemstart neu aus `/dev/urandom` erzeugt wird.

Denkbar ist auch eine andere Form der Schlüsselangabe: Statt interaktiv ein Passwort einzugeben, kann der Schlüssel während des Bootprozesses aus einer Datei eines USB-Sticks gelesen werden. Der USB-Stick dient dann gewissermaßen als Hardware-Schlüssel, der zum Booten des Rechners erforderlich ist. Auch manche Kartenlesegeräte lassen sich unter Linux nutzen; die Integration in die Verschlüsselungs-Software erfordert aber Handarbeit.

SSDs verschlüsseln

Grundsätzlich können Sie die hier beschriebenen Verschlüsselungsmethoden gleichermaßen für herkömmliche Festplatten und für SSDs verwenden. Prinzipbedingt ist die Verschlüsselung eines Dateisystems auf einer SSD aber mit zwei großen Nachteilen verbunden:

- Aus Sicherheitsgründen sollte immer der gesamte Inhalt des Dateisystems verschlüsselt werden, also auch die Datenblöcke, die momentan gar nicht genutzt werden. Sicherheitstechnisch ist es deswegen nicht zweckmäßig, der SSD per TRIM freie Datenblöcke zu melden. Langfristig wird die Performance der SSD darunter aber leiden.
- Viele SSDs versuchen, die zu speichernden Daten vorher zu komprimieren. Das gilt insbesondere für alle SSDs mit dem weit verbreiteten Sandforce-Controller. Bei verschlüsselten Daten ist eine Komprimierung aber unmöglich, was bei derartigen SSDs zu deutlichen Geschwindkeitseinbußen führt.

Den besten Ausweg aus diesem Dilemma bieten SSDs, bei denen eine Verschlüsselung auf Hardware-Ebene durchgeführt werden kann. Die Kontrolle über die Verschlüsselung erfolgt dann nicht durch Linux, sondern durch das EFI bzw. BIOS des Mainboards. Es lässt sich allerdings nur sehr schwer beurteilen, wie sicher die in die SSD eingebauten Verschlüsselungsalgorithmen sind.

Kapitel 26
GRUB

Das Programm GRUB ist ein sogenannter Bootloader. Es wird als erstes Programm nach dem Einschalten des Rechners gestartet und zeigt normalerweise ein Menü an, in dem Sie Windows oder eine Linux-Distribution auswählen können. Bei den meisten aktuellen Distributionen kommt die GRUB-Version 2 zum Einsatz. Diese Version steht im Mittelpunkt dieses Kapitels. Auf die ältere und schon seit Jahren nicht mehr gewartete GRUB-Version 0.97 *legacy* werden Sie weiterhin in älteren Linux-(Enterprise-)Installationen stoßen, weswegen ich auch auf diese Version kurz eingehe.

26.1 Grundlagen

GRUB steht für *Grand Unified Bootloader*. Das Programm startet Linux und hilft bei Parallelinstallationen von Linux und Windows, das gewünschte Betriebssystem beim Rechnerstart auszuwählen.

GRUB-Versionen

Seit Juni 2012 ist GRUB in der Version 2.0 verfügbar. Sie kommt bei fast allen gängigen Distributionen zum Einsatz. Die Vorgängerversion von GRUB 2 hat die merkwürdige Bezeichnung GRUB 0.97 *legacy*. Der Zusatz *legacy* weist darauf hin, dass diese Version schon seit Jahren nicht mehr weiterentwickelt wird. Und die Versionsnummer 0.97 macht klar, dass diese GRUB-Variante nie die Version 1.0 erreicht hat. Stattdessen haben verschiedene Distributoren GRUB 0.97 mehrfach in Eigenregie erweitert, was dazu geführt hat, dass einzelne GRUB-Funktionen je nach Distribution unterschiedlich realisiert sind!

Auch wenn aktuelle Distributionen nun überwiegend GRUB 2 einsetzen, ist GRUB 0.97 nach wie vor weit verbreitet: Zum einen werden Sie auf vielen älteren Linux-Installationen auf GRUB 0.97 stoßen, zum anderen wird GRUB 0.97 von diversen Enterprise-Distributionen nach wie vor als primärer Bootloader eingerichtet, z. B. von RHEL 6.

Neu in GRUB 2

Die folgende Aufzählung fasst die wichtigsten Neuerungen in GRUB 2 gegenüber der offiziellen GRUB-0.97-Version zusammen:

- GRUB 2 ist kompatibel zu LVM und Software-RAID. LVM- und RAID-Installationen erfordern somit keine eigene `/boot`-Partition mehr.
- GRUB 2 ist `ext4`- und `btrfs`-kompatibel.
- GRUB 2 erlaubt es, Partitionen über die UUID des Dateisystems anzusprechen.
- GRUB 2 ist kompatibel zu den BIOS-Alternativen EFI und coreboot (ehemals LinuxBIOS).
- GRUB 2 kann beliebige Unicode-Zeichen in den Menüeinträgen darstellen.
- GRUB-Zusatzfunktionen sind als Module realisiert, die zur Laufzeit geladen werden. Das soll eine relativ einfache Erweiterung und Wartung ermöglichen.
- Die GRUB-Konfiguration ist wesentlich komplexer geworden. Die Konfigurationsdatei `grub.cfg` entsteht als Ergebnis diverser Konfigurations-Scripts. `grub.cfg` kann selbst Script-Code in einer shell-ähnlichen Script-Sprache oder in der Programmiersprache LUA enthalten.

Komponenten und Pakete

Die für GRUB 2 notwendigen Dateien sind oft über mehrere Pakete verteilt: Bei Debian und Ubuntu enthält `grub-common` plattformunabhängige Konfigurationsdateien und Kommandos, und `grub-pc` enthält die BIOS-spezifischen Dateien. Für Rechner, die statt des BIOS auf EFI, coreboot etc. setzen, ist statt `grub-pc` eines der Pakete `grub-efi-amd64` oder `grub-efi-ia32` bzw. `grub-coreboot` erforderlich. Zu guter Letzt enthält `grub-rescue-pc` eine IMG- und eine ISO-Datei, um ein GRUB-Rescue-System auf einem USB-Stick oder einer CD zu speichern. Das ermöglicht es im Notfall, GRUB vom USB-Stick oder von der CD zu starten und dann durch die manuelle Eingabe von GRUB-Kommandos bzw. durch die Veränderung der vorgesehenen Menüeinträge das System zu starten.

Fedora hat die Filetierung in unzählige Pakete vermieden: `grub2` enthält GRUB für BIOS-Rechner, und `grub2-efi` enthält die EFI-kompatible Version. Für die Aktualisierung der GRUB-Konfiguration nach Kernel-Updates sorgen die Fedora-spezifischen Scripts des Pakets `grubby`.

GRUB 2 setzt unabhängig von der Distribution die Installation des Pakets `os-prober` voraus. Das gleichnamige Kommando sucht auf allen erreichbaren Partitionen nach Betriebssystemen. Das Ergebnis von `os-prober` fließt in das automatisch erzeugte GRUB-Menü ein.

Dokumentation

Die offizielle GRUB-Dokumentation finden Sie auf der GRUB-Homepage:

http://www.gnu.org/software/grub

BIOS-Systemstart

Bevor die Einzelheiten der GRUB-Installation und -Konfiguration behandelt werden, ist es sinnvoll, sich ein Bild davon zu machen, was während des Bootvorgangs passiert. Der Startprozess unterscheidet sich stark, je nachdem, ob auf Ihrem Rechner ein traditionelles BIOS oder das modernere EFI läuft (siehe Abschnitt 26.1).

Nach dem Einschalten eines BIOS-Rechners wird das *Basic Input Output System* initialisiert. Während dieses Vorgangs erscheinen meist ein paar Systemmeldungen auf dem Bildschirm, z. B. sehen Sie, wie viel Speicher Ihr Computer hat. Anschließend lädt das BIOS den Inhalt des ersten Sektors der ersten Festplatte in den Speicher und führt diesen Code aus. Dieser spezielle Sektor der Festplatte heißt *Master Boot Record* (MBR).

Der Kampf um den Master Boot Record

Es gibt nur einen MBR, aber möglicherweise mehrere Betriebssysteme auf Ihrer Festplatte. Das birgt natürlich Konfliktpotenzial! Sowohl bei Linux- als auch bei Windows-Installationen wird der MBR überschrieben. Während GRUB auch Windows starten kann, nimmt Windows leider keine Rücksicht auf Linux. Deswegen müssen Sie nach einer Windows-Installation GRUB reparieren, wofür Sie am besten ein Live- oder Notfallsystem verwenden. Besser ist es, zuerst Windows und dann Linux zu installieren! Sollte bei einer späteren Windows-Installation der MBR mit GRUB überschrieben werden, finden Sie Notfalltipps für GRUB 2 in Abschnitt 26.3, für GRUB 0.97 in Abschnitt 26.4.

Windows-Bootloader

Wenn auf einem Rechner Windows installiert ist, befindet sich im MBR ein winziges Programm. Es sucht die als »aktiv« gekennzeichnete Partition und führt dann den Windows-Bootloader aus, der sich im Bootsektor dieser Partition befindet. Falls auf dem Rechner mehrere Windows-Versionen installiert sind, können Sie im Windows-Bootloader zwischen diesen Versionen wählen.

Linux-Bootloader

Wenn auf dem Rechner auch Linux installiert ist, wird der MBR üblicherweise durch den Code des Linux-Bootloaders GRUB ersetzt. GRUB kann dann wahlweise Linux starten oder in den Windows-Bootloader verzweigen (siehe Abbildung 26.1).

Eine alternative Vorgehensweise besteht darin, den MBR nicht anzurühren, GRUB in den Bootsektor der Linux-Systempartition zu installieren und diese Partition als »aktiv« zu markieren. Diese Vorgehensweise würde zwar den MBR-Konventionen entsprechen, ist aber weniger robust und deswegen kaum gebräuchlich.

Der MBR ist nur 512 Byte groß – zu klein, um das gesamte Bootloader-Programm zu speichern. Deswegen enthält der MBR gerade so viel Code, um den Rest des Bootloaders von der Festplatte zu laden. Dementsprechend ist der GRUB-Code in zwei

oder drei Teile zerlegt: `stage1` befindet sich im MBR und hat die Aufgabe, die ersten Sektoren von `stage1_5` oder `stage2` zu laden. `stage1_5` enthält Zusatzcode für den Zugriff auf Dateien in verschiedenen Dateisystemen. `stage2` enthält schließlich den eigentlichen Bootloader.

Sobald der Bootloader läuft, erscheint ein Menü mit einer Auswahl aller Betriebssysteme, die bei der GRUB-Konfiguration definiert wurden. Mit den Cursortasten können Sie nun das gewünschte Betriebssystem auswählen und dann mit ↵ starten. Oft ist GRUB so eingestellt, dass nach einer gewissen Zeit ein Betriebssystem automatisch gestartet wird.

Linux-Start

Wenn Sie sich im Bootloader dafür entscheiden, Linux zu starten, muss der Bootloader die Linux-Kerneldatei in den Speicher laden und ausführen. Die Kerneldatei hat normalerweise den Dateinamen `/boot/vmlinuz`. Der letzte Buchstabe `z` weist darauf hin, dass der Kernel komprimiert ist. Der Bootloader muss also in der Lage sein, eine vollständige Datei aus einem Linux-Dateisystem zu laden.

Kernelparameter

An den Kernel werden meist einige Parameter übergeben, mindestens aber einer: der Device-Name der Systempartition (z. B. `root=/dev/sdb13`). Damit weiß der Kernel, welches die Systempartition ist. Sobald der Kernel läuft, gibt er die Kontrolle an das Linux-Programm `/sbin/init` weiter. Dieses Programm ist für die Initialisierung des Linux-Systems zuständig und wird in Kapitel 27 ausführlich beschrieben. Es kümmert sich beispielsweise darum, alle Netzwerkdienste zu starten.

Zugriff auf Kernelmodule

Der Linux-Kernel ist modularisiert. Das bedeutet, dass der Kernel an sich nur relativ elementare Funktionen enthält. Zusatzfunktionen zum Zugriff auf bestimmte Hardware-Komponenten, zum Lesen und Schreiben verschiedener Dateisysteme etc. befinden sich dagegen in Modulen, die bei Bedarf aus dem Dateisystem geladen werden und den Kernel so erweitern.

Damit der Startprozess gelingt, muss der Kernel auf die Systempartition zugreifen können. Falls diese Partition in einem Dateisystem vorliegt, das der Kernel nicht direkt unterstützt, oder wenn sich die Partition auf einer SCSI-Festplatte befindet, für die der Kernel keinen Hardware-Treiber enthält, so tritt ein Henne-Ei-Problem auf: Der Kernel kann nicht auf das Dateisystem zugreifen und daher die Module nicht laden, die er benötigen würde, um Dateien des Dateisystems zu lesen ...

Initrd-Datei

Die Lösung des Problems besteht darin, dass der Bootloader nicht nur den Kernel lädt, sondern auch eine sogenannte Initrd-Datei. Dabei handelt es sich um eine spezielle Datei, die alle für den Startprozess erforderlichen Kernelmodule enthält. Die Datei steht dem Kernel vorübergehend als RAM-Disk zur Verfügung, d. h., der Kernel kann die erforderlichen Module unmittelbar nach dem Start von der RAM-Disk laden. (Initrd ist die Abkürzung für *Initial RAM Disk*.) Die Initrd-Datei hat üblicherwei-

se den Dateinamen `/boot/initrd` oder `/boot/initrd.gz`. Die meisten Distributionen stellen Werkzeuge zur Verfügung, um eine zum Kernel passende `initrd`-Datei zu erzeugen.

GRUB-Installation und -Konfiguration

Wenn in diesem Buch von »Software-Installation« die Rede ist, dann ist damit üblicherweise die Installation eines Programmpakets auf der Festplatte gemeint. In diesem Kapitel gelten allerdings andere Regeln: Mit der »Installation von GRUB« wird der Prozess bezeichnet, den GRUB-Startcode in den Bootsektor einer Festplatte zu schreiben.

Die GRUB-Konfiguration erfolgt je nach GRUB-Version unterschiedlich: Bei GRUB 0.97 ist die zentrale Konfigurationsdatei `/boot/grub/menu.lst`. Bei GRUB 2 gibt es eine ganze Sammlung von Konfigurations-Scripts im Verzeichnis `/etc/grub.d/`. Durch die Ausführung dieser Scripts wird die eigentliche GRUB-2-Konfigurationsdatei `grub.cfg` erstellt.

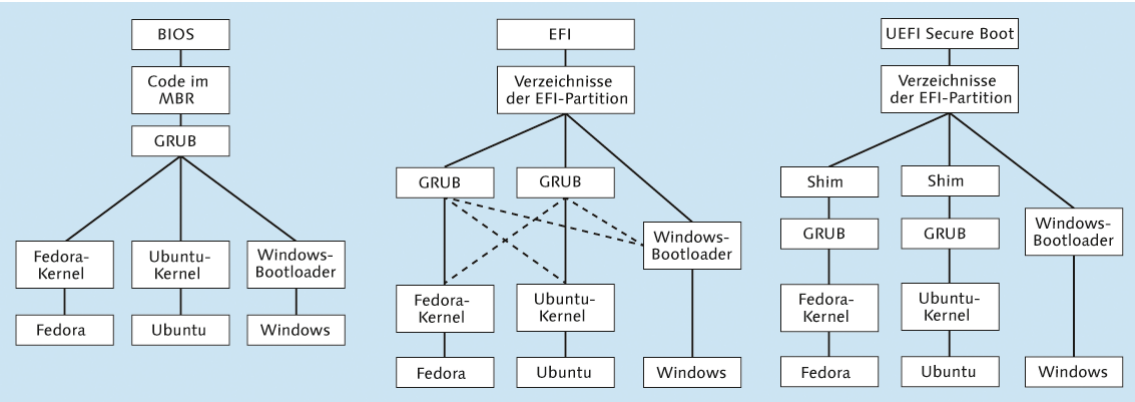


Abbildung 26.1 Bootvorgang für drei Betriebssysteme mit BIOS, EFI und UEFI Secure Boot

EFI-Systemstart

Parallelinstallationen

Das *Extensible Firmware Interface* (EFI) vereinfacht die Parallelinstallation mehrerer Betriebssysteme. Während das BIOS grundsätzlich nur die Installation *eines* Betriebssystems vorsah und jede Parallelinstallation einen Bootmanager voraussetzte, unterstützt EFI von sich aus die Installation mehrerer Betriebssysteme: Jedes Betriebssystem kann seinen eigenen Bootloader in ein eigenes Verzeichnis innerhalb der EFI-Partition speichern. Beim Start des Rechners wird nach der EFI-Initialisierung automatisch der Bootloader des Default-Betriebssystems gestartet. In der Regel handelt es sich dabei um das zuletzt installierte Betriebssystem. Wird während des Rechnerstarts eine spezielle Tastenkombination gedrückt, zeigt das EFI ein Menü aller Bootloader an.

In Kombination mit EFI muss GRUB also nur noch Linux starten. Die zweite Funktion von GRUB, nämlich die Auswahl zwischen verschiedenen Betriebssystemen, ist im Zusammenspiel mit EFI eigentlich entbehrlich; weil sich das GRUB-Menü aber als praktisch erwiesen hat, wird es weiterhin oft angezeigt. Daraus ergeben sich die in Abbildung 26.1 durch dünne graue Linien angedeuteten Startwege.

EFI und GRUB

Damit EFI und GRUB korrekt zusammenspielen, muss eine spezielle EFI-Version von GRUB eingerichtet werden. Die Installationsprogramme gängiger Distributionen kümmern sich darum automatisch. Das setzt allerdings voraus, dass das Installationsprogramm im EFI-Modus und nicht im BIOS-Modus ausgeführt wird!

EFI-Partition

Der GRUB-Code wird bei EFI-Rechnern nicht in den MBR installiert, sondern in ein Verzeichnis der EFI-Partition. Dabei handelt es sich um eine spezielle Partition mit einem VFAT-Dateisystem. Die Partition muss durch eine spezielle UID markiert sein: 0xEF (MBR) bzw. C12A7328-F81F-11D2-BA4B-00A0C93EC93B (GPT).

Microsoft empfiehlt, die EFI-Partition als erste Partition auf der Festplatte einzurichten, obwohl der EFI-Standard dies nicht verlangt. Die Partition muss nicht besonders groß sein, ca. 100 bis 200 MByte reichen.

Die EFI-Partition muss im Verzeichnis `/boot/efi` in das Linux-Dateisystem eingebunden werden! Bei einer manuellen Partitionierung während einer Linux-Installation müssen Sie sich selbst darum kümmern.

Kernel, Initrd-Datei

Sobald GRUB einmal läuft, verläuft der eigentliche Linux-Start exakt genauso wie auf einem BIOS-Rechner: GRUB lädt den Kernel und startet diesen, wobei es die Initrd-Datei und Kernelparameter übergibt.

UEFI Secure Boot

Die seit Herbst 2012 verfügbare EFI-Erweiterung *Secure Boot* hat den Boot-Prozess nochmals komplizierter gemacht. Wenn diese EFI-Erweiterung aktiv ist, startet das EFI nur solche Programme, die mit einem dem EFI bekannten Schlüssel signiert sind. Die meisten Mainboards kennen nur einen einzigen Schlüssel – den von Microsoft! Glücklicherweise bietet Microsoft für Linux-Distributoren und andere Unternehmen einen Signierdienst an. Damit ist es prinzipiell möglich, einen Bootloader so signieren zu lassen, dass EFI bereit ist, diesen zu starten.

Allerdings sind mit dem Signierdienst Auflagen verbunden: Die Teilnehmer müssen sich dazu verpflichten, das zu startende System gegen Manipulationen abzusichern, sodass Secure Boot seinem Namen gerecht wird und keine Schad-Software lädt, sondern nur den originalen Linux-Kernel der jeweiligen Distribution.

Secure Boot bei Fedora und Ubuntu

Für die Linux-Distributoren ist die Realisierung eines sicheren Bootprozesses schwierig. Im Sommer 2013 gab es nur wenige Distributionen, bei denen Secure Boot problemlos funktionierte – Fedora, Ubuntu sowie SUSE Enterprise ab Version 11 SP3. Auch openSUSE kommt ab Version 12.3 mit Secure Boot zurecht, sofern die entsprechende Option während der Installation gesetzt wird. RHEL wird Secure Boot vermutlich erst ab Version 7 unterstützen.

Um den mit dem Microsoft-Schlüssel signierten Code möglichst klein zu halten, haben sich die Distributoren dazu entschlossen, einen Zwischenschritt einzulegen: Bei Fedora und Ubuntu startet EFI das signierte Programm Shim. Die einzige Aufgabe dieses winzigen Programms ist es, die Signaturkette sicherzustellen und GRUB zu starten. GRUB setzt dann wie bisher den Bootprozesses fort (siehe Abbildung 26.1 rechts).

Wie Tabelle 26.1 zeigt, haben Fedora, SUSE und Ubuntu die Secure-Boot-Anforderungen unterschiedlich genau interpretiert. Bei Fedora ist Shim durch einen Microsoft-Schlüssel signiert. In Shim ist außerdem ein Fedora-eigener Schlüssel eingebaut; damit kann überprüft werden, dass der zu startende GRUB-Bootloader nicht modifiziert wurde. Anschließend überprüft auch GRUB die Signatur des Kernels und der Kernel die Signatur jedes zu ladenden Moduls.

Bei SUSE bzw. openSUSE verläuft der Bootprozess ebenso, allerdings enthält SUSEs Shim einen SUSE-eigenen Schlüssel; GRUB und der Kernel sind entsprechend mit diesem SUSE-Schlüssel signiert. Ubuntu geht analog vor, allerdings ist dort die Signatur des Kernels optional; Module werden gar nicht überprüft.

Komponente	Fedora	SUSE	Ubuntu
Shim	Microsoft-Signatur	Microsoft-Signatur	Microsoft-Signatur
GRUB	Fedora-Signatur	SUSE-Signatur	Ubuntu-Signatur
Kernel	Fedora-Signatur	SUSE-Signatur	Ubuntu-Signatur (optional)
Kernelmodule	Fedora-Signatur	SUSE-Signatur	–

Tabelle 26.1 Signaturkette des Secure-Boot-Verfahrens von Fedora, SUSE und Ubuntu

Der Preis der Sicherheit

Die Fedora- und SUSE-Entwickler argumentieren damit, dass nur ihre sehr exakte Befolgung der Secure-Boot-Vorgaben sicherstellt, dass die Vertrauenskette zu keinem Zeitpunkt durchbrochen werden kann. Andernfalls ist nicht auszuschließen, dass Microsoft den Schlüssel für Shim aus Sicherheitsbedenken zurückziehen könnte.

Aus den strengen Secure-Boot-Implementierungen von Fedora und openSUSE ergeben sich aus Linux-Sicht leider dramatische Einschränkungen:

- Die Kernelmodule der NVIDIA- und ATI/AMD-Grafiktreiber können nicht geladen werden. Da diese Module direkt von NVIDIA bzw. AMD kompiliert sind, ist es unmöglich, sie mit dem Schlüssel zu signieren, der nur den Fedora-Entwicklern vorliegt. Dieselbe Einschränkung gilt natürlich auch für alle anderen Kernelmodule von proprietären Hardware-Treibern.
- Es ist nicht ohne Weiteres möglich, einen eigenen Kernel zu kompilieren und einzurichten. Auch dieser Kernel muss ja signiert werden, den dazu erforderlichen Schlüssel hat aber nur der Distributor. Ein Ausweg aus diesem Dilemma ist das von SUSE entwickelte Verfahren *Machine Owner Keys* (MOK). Damit wird in Shim zusätzlich zum SUSE-Schlüssel ein weiterer, von Ihnen selbst zur Verfügung gestellter Schlüssel hinterlegt. Ein selbst kompilierter Kernel und dessen Module können dann ebenfalls mit diesem Schlüssel signiert werden.
- GRUB kann nur dann eine andere Linux-Distribution starten, wenn diese mit demselben Schlüssel signiert ist.
- Der Ruhemodus (*suspend to disk*) funktioniert nicht.
- Die Kernel-Funktionen `kexec` und `kdump` können nicht genutzt werden.

Am einfachsten umgehen Sie diese Einschränkungen, indem Sie Secure Boot deaktivieren. Ubuntus etwas laxerer Umgang mit Secure Boot ist aus Anwendersicht deutlich bequemer, es bleibt aber abzuwarten, ob Microsoft die Implementierung ausreichend sicher findet.

Wogegen schützt Secure Boot?

Secure Boot soll verhindern, dass bereits beim Bootprozess Schad-Software geladen wird, die sich in der Folge allen weiteren Sicherheitsmaßnahmen, wie z. B. Viren-Scannern, entzieht. Derartige Angriffe hat es in den letzten Jahrzehnten so gut wie nie gegeben, nicht unter Windows, und schon gar nicht bei Linux. Salopp formuliert: Secure Boot schützt Sie vor einer Gefahr, die es gar nicht gibt.

Die Sicherheitsprobleme, die Windows und vereinzelt auch Linux in den vergangenen Jahren plagten, waren durchwegs Fehler in einzelnen Anwendungsprogrammen – sei es nun der Internet Explorer oder der Apache Webserver. Diese Probleme wird es wohl weiter geben. Secure Boot ändert daran überhaupt nichts.

Links

Wenn Sie sich für die technischen Details der Implementierung von Secure Boot unter Linux interessieren, können Sie hier weiterlesen:

http://mjg59.dreamwidth.org/12368.html
http://lwn.net/Articles/523367

http://fedoraproject.org/wiki/Features/SecureBoot
http://en.opensuse.org/openSUSE:UEFI#Secure_Boot
https://www.suse.com/releasenotes/x86_64/SUSE-SLES/11-SP3
https://www.suse.com/communities/conversations/uefi-secure-boot-details
https://lists.ubuntu.com/archives/ubuntu-devel/2012-June/035445.html

Initrd-Dateien

Henne oder Ei? Kernelmodule beim Bootprozess

Linux verwendet einen modularisierten Kernel. Viele Zusatzfunktionen – z. B. für die Ansteuerung einer SCSI-Karte, für den Zugriff auf bestimmte Dateisysteme, RAID-Verbunde oder LVM-Partitionen – befinden sich nicht im Kernel, sondern in Modulen. Beim Systemstart ist das aber problematisch – wie soll der Kernel ein Modul laden, wenn er noch gar nicht in der Lage ist, auf das Dateisystem zuzugreifen? Deswegen werden die für den unmittelbaren Start erforderlichen Module in eine Initial RAM Disk verpackt. Die entsprechende Initrd-Datei übergibt GRUB an den Kernel (Schlüsselwort `initrd` in der GRUB-Konfigurationsdatei).

Initrd-Interna

Der Kernel und die Initrd-Datei befinden sich üblicherweise im Verzeichnis `/boot`, ihr Name variiert aber je nach Distribution. Die Initrd-Datei muss Kernelmodule enthalten, deren Version exakt mit der Version des Kernels übereinstimmt. Aus diesem Grund muss jedes Mal, wenn ein neuer Kernel installiert oder selbst kompiliert wird, auch eine dazu passende Initrd-Datei erstellt werden. Bei einem Kernel-Update kümmert sich normalerweise das Update-Programm um diesen Prozess. Wenn Sie den neuen Kernel dagegen selbst installieren, müssen Sie sich auch um die Initrd-Datei selbst kümmern.

Die Bezeichnung »Initrd-Datei« ist genau genommen bei den meisten aktuellen Distributionen falsch: Es handelt sich in Wirklichkeit um `initramfs`-Dateien, deren Aufbau etwas weiter unten beschrieben wird. Weil aber sowohl die GRUB-Optionen als auch die Kommandos zum Erzeugen der Dateien den Begriff `initrd` nutzen und der Kernel die Datei trotz der falschen Bezeichnung korrekt interpretiert, bleibe ich in diesem Buch ebenfalls bei dieser Bezeichnung – gewissermaßen wider besseres Wissen.

Die Initrd-Datei ist nicht immer zwingend erforderlich: Wenn Ihr Kernel alle Komponenten enthält, die während des Bootprozesses erforderlich sind, gelingt der Start auch ohne Initrd-Datei. Dazu muss der Kernel aber entsprechend kompiliert sein – und genau das ist bei den meisten Distributionen nicht der Fall.

Bedauerlicherweise ist die Erzeugung von Initrd-Dateien nicht standardisiert. Jede Distribution verwendet ihre eigenen Werkzeuge. Die Initrd-Dateien enthalten nicht nur Kernelmodule, sondern auch Scripts zur Hardware-Initialisierung und unter

Umständen ein minimales Rescue-System, sodass Rettungsarbeiten selbst dann durchgeführt werden können, wenn das Einbinden der Systempartition nicht gelingt.

update-initramfs (Debian, Ubuntu)

Unter Debian und Ubuntu ist zur Erzeugung und Administration der Initrd-Dateien das Script `update-initramfs` vorgesehen. Im einfachsten Fall geben Sie einfach nur die Option `-u` an, um die Initrd-Datei der aktuellsten installierten Kernelversion zu aktualisieren. Wenn Sie die Initrd-Datei für eine andere Kernelversion aktualisieren möchten, geben Sie die Versionsnummer mit `-k` an. `-k all` aktualisiert die Initrd-Dateien für alle installierten Kernelversionen.

Mit den Optionen `-c` bzw. `-d` erzeugt `update-initramfs` eine neue Initrd-Datei bzw. löscht eine vorhandene Initrd-Datei. In diesem Fall ist die Angabe der Kernelversion durch `-k` zwingend erforderlich.

```
root#  update-initramfs -c -k 3.9-13-generic
update-initramfs: Generating /boot/initrd.img-3.9-13-generic
```

Hinter den Kulissen greift `update-initramfs` auf das Script `mkinitramfs` zurück, um Initrd-Dateien zu erzeugen. Die Basiskonfiguration erfolgt in `/etc/initramfs-tools/initramfs.conf` sowie durch die Dateien in `/etc/initramfs-tools/conf.d`. Darüber hinaus werden der Initrd-Datei alle in `/etc/initramfs-tools/modules` aufgezählten Module hinzugefügt (ein Modul pro Zeile).

`mkinitramfs` erzeugt in der Standardkonfiguration mit `MODULES=most` in `initramfs.conf` ziemlich große Initrd-Dateien mit unzähligen Kernelmodulen. Sollten Sie `mkinitramfs` direkt aufrufen, müssen Sie zumindest den Namen der neuen Initrd-Datei übergeben (Option `-o`). Wenn die Initrd-Datei nicht für die aktuelle Kernelversion erzeugt werden soll, geben Sie zusätzlich die gewünschte Version an:

```
root#  mkinitramfs -o myinitrd 3.9-13-generic
```

dracut (Fedora, Red Hat)

Fedora ab Version 12 sowie Red Hat Enterprise Linux ab Version 6 verwenden `dracut` zur Erzeugung der Initrd-Datei. `dracut` wird bei jedem Kernel-Update automatisch ausgeführt. Das Kommando `dracut` berücksichtigt die Einstellungen aus `/etc/dracut.conf`. Um für einen selbst kompilierten Kernel 3.9.3 in der Datei `/boot/vmlinuz-3.9.3` manuell eine Initrd-Datei zu erzeugen, führen Sie das folgende Kommando aus:

```
root#  dracut /boot/initrd-3.9.3  3.9.3
```

Beginnend mit Fedora 19 erzeugt Dracut kompaktere Initrd-Dateien, die nur solche Kernelmodule enthalten, die im laufenden Betrieb aktiv sind. Das spart Platz und beschleunigt den Bootprozess, kann aber nach Hardware-Erweiterungen zu Bootproblemen führen. Aus diesem Grund gibt es nun für das Rescue-System eine

spezielle Initrd-Datei mit allen Modulen. Falls der gewöhnliche Bootprozess nach einem Hardware-Umbau scheitern sollte, booten Sie das Rettungssystem und führen dann das folgende Kommando aus:

```
root#  dracut --regenerate-all --force
```

mkinitrd (SUSE)

SUSE-Distributionen erzeugen ihre Initrd-Dateien mit dem Kommando `mkinitrd`. Normalerweise müssen an das Kommando keinerlei Parameter oder Optionen übergeben werden. `mkinitrd` erzeugt automatisch Initrd-Dateien zu allen Kerneldateien, die es im Verzeichnis `/boot` findet. Die neuen Initrd-Dateien bekommen den Namen `/boot/initrd-nnn`, wobei `nnn` die Kernelversion ist. Außerdem richtet `mkinitrd` einen Link ein, der von `/boot/initrd` auf die zu `vmlinuz` passende Initrd-Datei verweist.

Wenn Sie nur eine bestimmte Initrd-Datei erzeugen möchten, können Sie mit den Optionen `-k` und `-i` die Kernel- bzw. Initrd-Dateien angeben (standardmäßig im `/boot`-Verzeichnis). `mkinitrd` wertet die Variable `INITRD_MODULES` aus der Datei `/etc/sysconfig/kernel` aus. Diese Variable enthält alle zum Booten erforderlichen Module und kann beispielsweise so aussehen:

```
# in /etc/sysconfig/kernel
INITRD_MODULES="thermal ahci ata_piix ata_generic processor fan"
```

Zusätzliche Module geben Sie mit `-m` an. Weitere Informationen zu `mkinitrd` bekommen Sie mit der Option `-h`, mit `man mkinitrd` oder im Quelltext des Scripts (Datei `/sbin/mkinitrd`).

Kernel-Updates

Wenn eine Distribution ein Kernel-Update durchführt und sich dadurch der Name der Kerneldatei ändert, muss auch die GRUB-Menüdatei entsprechend geändert und eine zum neuen Kernel passende Initrd-Datei erzeugt werden. Alle gängigen Distributionen erledigen diese Aufgaben im Rahmen der Update-Verwaltung automatisch, sodass beim nächsten Neustart des Rechners automatisch der neue Kernel verwendet wird. Bei vielen Distributionen gibt es für den alten Kernel weiterhin einen GRUB-Menüeintrag, damit bei Update-Problemen eine Möglichkeit besteht, das System mit dem alten Kernel weiterzunutzen.

Initrd-Datei ansehen

Initrd-Dateien werden seit der Kernelversion 2.6 intern als `initramfs`-Dateien dargestellt. Die Initrd-Datei ist eine komprimierte Archivdatei (`cpio`-Datei), die aus diversen Verzeichnissen und Dateien zusammengesetzt ist. Wenn Sie sich den Inhalt des Archivs ansehen möchten, gehen Sie so vor:

```
root#  cd /boot
root#  cp initrd-n.n initrd-test.gz
root#  gunzip initrd-test
root#  mkdir test
root#  cd test
root#  cpio -i < ../initrd-test
root#  ls -lR
```

26.2 GRUB-Bedienung (Anwendersicht)

Nach einer Linux-Installation erscheint beim Neustarten des Rechners ein Menü zur Auswahl des gewünschten Betriebssystems (siehe Abbildung 26.2). Das Aussehen von GRUB kann je nach Konfiguration stark variieren. Manche Distributionen starten GRUB im Grafikmodus und nehmen dem Programm damit seinen spartanischen Anstrich. Um diverse Zusatzfunktionen von GRUB nutzen zu können, müssen Sie den Grafikmodus mit Esc verlassen. Andere Distributionen vermeiden die Anzeige des GRUB-Menüs nach Möglichkeit überhaupt. Wenn beispielsweise Ubuntu als einziges Betriebssystem auf einem Rechner installiert ist, bekommen Sie das GRUB-Menü nur zu sehen, wenn Sie während des Rechnerstarts eine Taste drücken.

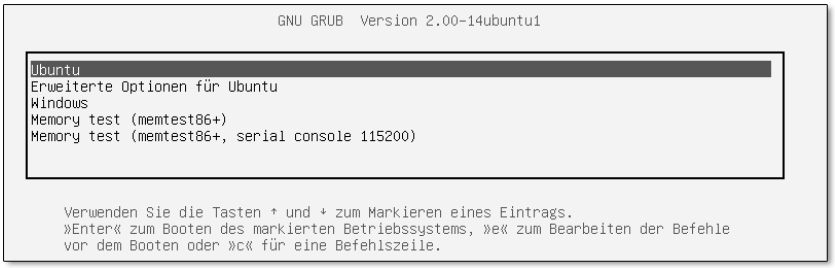


Abbildung 26.2 Ein minimalistisches GRUB-Menü

Passwort

GRUB kann durch ein Passwort abgesichert sein. In diesem Fall können Sie die interaktiven Funktionen von GRUB erst verwenden, nachdem Sie P gedrückt und dann das Passwort angegeben haben.

Tastatur

Unter GRUB gilt normalerweise das US-Tastaturlayout. Falls Sie mit einer deutschen Tastatur arbeiten, finden Sie in Abschnitt 2.12 eine Tabelle zur Eingabe wichtiger Sonderzeichen. Beachten Sie, dass auch Y und Z vertauscht sind.

Linux-Kernel-Bootoptionen übergeben

Sofern das GRUB-Menü nicht durch ein Passwort abgesichert ist, können Sie den gerade mit den Cursortasten ausgewählten Eintrag des GRUB-Menüs mit E (*edit*) verändern. Es werden nun einige Zeilen angezeigt, die in einer recht eigenwilligen Syntax beschreiben, wie das Betriebssystem gestartet werden soll.

Die Editierfunktionen von GRUB werden vor allem dazu verwendet, vor dem Start von Linux zusätzliche Kerneloptionen anzugeben, z. B. zur Umgehung von Hardware-Problemen. Dazu suchen Sie nach einer Zeile, die so ähnlich wie das folgende Muster aussieht:

```
linux /boot/vmlinuz-n.n.n root=/dev/sdb13
```

Am Ende dieser Zeile können Sie Parameter hinzufügen bzw. verändern. Strg+X oder F10 startet dann Linux mit den veränderten Parametern. Die Änderungen werden aber nicht gespeichert!

Interaktiv Kommandos ausführen

Vom GRUB-Menü gelangen Sie mit C in einen interaktiven Kommandomodus. Dort können Sie diverse GRUB-Kommandos manuell ausführen. Das bietet die Möglichkeit, ein Linux-Betriebssystem auch dann zu starten, wenn der dazugehörende GRUB-Menüeintrag fehlt oder fehlerhaft ist. Sie müssen dazu nur wissen, auf welcher Partition sich Ihr Linux befindet und wie die entsprechenden GRUB-Kommandos lauten. Details dazu folgen im weiteren Verlauf des Kapitels. Beachten Sie, dass sich die Syntax von GRUB 0.97 und GRUB 2 deutlich unterscheidet.

Mit den folgenden Kommandos für GRUB 2 wird beispielsweise eine Linux-Distribution gestartet, die sich in der Partition `/dev/sdb13` mit einem `ext4`-Dateisystem befindet. (`insmod ext2` lädt einen Treiber, der gleichermaßen `ext2`, `ext3` und `ext4` unterstützt.)

```
grub>  insmod ext2
grub>  set root='(hd1,13)'
grub>  linux  /boot/vmlinuz-n.n.n root=/dev/sdb13 ro
grub>  initrd /boot/initrd-n.n.n
grub>  boot
```

Bei der Eingabe der Dateinamen vervollständigt GRUB mit ↹ die Dateinamen für das durch `root` bzw. durch eine Laufwerksangabe ausgewählte Dateisystem. Mit `cat` können Sie einzelne Textdateien sogar anzeigen. Daneben bietet der GRUB-Kommandomodus noch viele andere Möglichkeiten, auf die hier aber aus Platzgründen nicht eingegangen wird. `help` liefert die Liste aller Kommandos, `help kommandoname` gibt genauere Informationen zu diesem Kommando.

Menü bleibend verändern

GRUB 0.97 liest das Bootmenü aus der Datei `/boot/grub/menu.lst`, GRUB 2 verwendet stattdessen `grub.cfg`, die je nach Distribution in `/boot/grub`, `/boot/grub2` oder `/boot/efi/EFI/distribname` gespeichert wird.

`menu.lst` bzw. `grub.cfg` enthalten Kommandos, die die Einträge des GRUB-Menüs beschreiben. Wenn Sie also das GRUB-Menü bleibend verändern möchten, müssen Sie Linux starten und die GRUB-Menüdatei verändern. Bei GRUB 0.97 werden Sie `menu.lst` direkt mit einem Editor bearbeiten, bei GRUB 2 verändern Sie stattdessen andere Konfigurationsdateien und generieren daraus eine neue Fassung von `grub.cfg`. GRUB berücksichtigt Ihre Änderungen automatisch ab dem nächsten Start. Detaillierte Informationen zum Aufbau der GRUB-Konfigurationsdateien folgen in den weiteren Abschnitten dieses Kapitels.

26.3 GRUB 2

Basiskonfiguration

grub.cfg

Das GRUB-Menü wird durch die Datei `grub.cfg` definiert, die sich je nach Distribution an unterschiedlichen Orten befindet:

`/boot/grub/grub.cfg`	(Debian und Ubuntu)
`/boot/grub2/grub.cfg`	(Fedora und openSUSE auf BIOS-Rechnern)
`/boot/efi/EFI/fedora/grub.cfg`	(Fedora auf EFI-Rechner)
`/boot/grub2-efi/grub.cfg`	(openSUSE auf EFI-Rechner)
`/etc/grub2.cfg`	(Link auf `grub.cfg` in Fedora)
`/etc/grub2-efi.cfg`	(Link auf `grub.cfg` in Fedora mit EFI)

/etc/grub.d/

Manuelle Veränderungen an `grub.cfg` sind *nicht* vorgesehen! Die Zugriffsrechte dieser Datei sind deswegen auf *read-only* gestellt. Wenn Sie das GRUB-Menü modifizieren möchten, verändern Sie die zugrunde liegenden Konfigurationsdateien. Die Orte dieser Dateien sind erfreulicherweise bei Debian, Fedora, openSUSE und Ubuntu identisch:

`/etc/grub.d/*`	(allgemeine GRUB-Konfigurationsdateien)
`/etc/default/grub`	(distributionsspezifische Ergänzungen)

update-grub

Um nach Änderungen an diesen Dateien oder nach einem Kernel-Update die GRUB-Menüdatei `grub.cfg` neu zu generieren, müssen Sie eines der folgenden Kommandos ausführen:

```
root#  update-grub                                  (Debian und Ubuntu)
root#  grub2-mkconfig -o /etc/grub2.cfg             (Fedora mit BIOS)
root#  grub2-mkconfig -o /etc/grub2-efi.cfg         (Fedora mit EFI)
root#  grub2-mkconfig -o /boot/grub2/grub.cfg       (openSUSE mit BIOS)
root#  grub2-mkconfig -o /boot/grub2-efi/grub.cfg   (openSUSE mit EFI)
```

Beispiel für grub.cfg

Die resultierende Datei `grub.cfg` sieht so ähnlich wie das folgende Beispiel aus. Das folgende Listing einer automatisch erzeugten Fassung von `grub.cfg` unter Ubuntu ist aus Platzgründen stark gekürzt. Lassen Sie sich übrigens von der Zeile `insmod ext2` nicht irritieren: Dieses GRUB-Modul ist für alle `ext`-Dateisysteme zuständig, also auch für `ext3` und `ext4`. Weitere Erläuterungen zur Syntax in `grub.cfg` folgen im weiteren Verlauf dieses Abschnitts.

```
# Beispiel für /boot/grub/grub.cfg

# aus /etc/grub.d/00_header
# Code zur Variablenverwaltung ...
# Definition diverser Funktionen: savedefault, recordfail, load_video
# Font-Dateien suchen ...
```

```
# aus /etc/grub.d/05_debian_theme
# Farben für den Textmodus einstellen ...

# aus /etc/grub.d/10_linux
# Definition der Funktion gfxmode ...

# Ubuntu starten
menuentry 'Ubuntu' ... {
  recordfail
  load_video
  gfxmode $linux_gfx_mode
  insmod gzio
  insmod part_msdos
  insmod ext2
  set root='hd0,msdos1'
  search --no-floppy --fs-uuid --set=root 0f65...
  linux   /boot/vmlinuz-3.10.0-2-generic root=UUID=0f65... ro quiet \
    splash $vt_handoff
  initrd  /boot/initrd.img-3.10.0-2-generic
}

# Menü mit alten Ubuntu-Versionen und dem Rettungssystem
submenu 'Erweiterte Optionen für Ubuntu' ... {
  menuentry 'Ubuntu, mit Linux 3.10.0-2-generic' ... { ... }
  menuentry 'Ubuntu (Wiederherstellungsmodus)' ... {
    ...
    linux   /boot/vmlinuz-3.10.0-2-generic root=UUID=0f65... ro \
      recovery nomodeset
  }
}

# aus /etc/grub.d/20_memtest86+: Speichertest durchführen
menuentry 'Memory test (memtest86+)' {
  insmod part_msdos
  insmod ext2
  set root='hd0,msdos1'
  search --no-floppy --fs-uuid --set=root 0f65...
  linux16 /boot/memtest86+.bin
}

# aus /etc/grub.d/30_os-prober: Windows starten
menuentry "Windows (loader) (on /dev/sda1)" {
  insmod ntfs
  set root='(hd0,1)'
  search --no-floppy --fs-uuid --set 2ca80f2ba80ef35e
  chainloader +1
}
```

grub.cfg neu erzeugen

Unter Debian und Ubuntu erzeugt das Kommando `update-grub` eine neue Version von `grub.cfg`. Unter Fedora und openSUSE führen Sie stattdessen `grub2-mkconfig -o /boot/grub2/grub.cfg` aus. Das Debian/Ubuntu-spezifische Script `update-grub` enthält ebenfalls nur dieses Kommando.

`grub2-mkconfig` wertet die im Folgenden beschriebenen Konfigurationsdateien bzw. -Scripts aus. Dabei werden unter anderem GRUB-Menüeinträge für sämtliche Kerneldateien in `/boot` erzeugt. Außerdem werden alle erreichbaren Partitionen untersucht. Wenn sie andere Betriebssysteme enthalten, werden auch hierfür GRUB-Menüeinträge erzeugt. Aus diesem Grund dauert die Ausführung von `update-grub` auf Rechnern mit vielen Partitionen eine Weile.

`grub2-mkconfig` wird automatisch bei jedem Kernel-Update ausgeführt und stellt sicher, dass der neueste Linux-Kernel im Grub-Menü enthalten ist.

/etc/default/grub

Die Datei `/etc/default/grub` enthält einige globale GRUB-Einstellungen. Vergessen Sie nicht, dass hier durchgeführte Änderungen erst wirksam werden, wenn Sie `grub.cfg` neu generieren! In Ubuntu enthält die Konfigurationsdatei die folgenden Einstellungen:

```
# Datei /etc/default/grub
GRUB_DEFAULT=0
GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
GRUB_TIMEOUT=10
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash"
GRUB_CMDLINE_LINUX=""
```

Die Standardkonfiguration von Fedora sieht so aus:

```
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="rd.md=0 rd.lvm=0 rd.dm=0 \
  $([ -x /usr/sbin/rhcrashkernel-param ] && \
    /usr/sbin/rhcrashkernel-param || :) rd.luks=0 \
  vconsole.font=latarcyrheb-sun16 vconsole.keymap=de rhgb quiet"
GRUB_DISABLE_RECOVERY="true"
GRUB_THEME="/boot/grub2/themes/system/theme.txt"
```

Im Folgenden erkläre ich Ihnen die Bedeutung der vielen Parameter:

- `GRUB_DEFAULT` gibt an, welcher GRUB-Menüeintrag standardmäßig ausgewählt werden soll. Die Einstellung `"saved"` bedeutet, dass der zuletzt ausgewählte Menüeintrag aktiviert wird. Das funktioniert allerdings nur, wenn sich die GRUB-Dateien in einer gewöhnlichen Partition befinden! Ist dagegen LVM oder RAID im Spiel, kann GRUB nach der Menüauswahl keine Umgebungsvariablen speichern.

  Eine weitere Möglichkeit besteht darin, `GRUB_DEFAULT` die `menuentry`-Zeichenkette des gewünschten Menüeintrags zuzuweisen. Dabei müssen Sie aber darauf achten, die Schreibweise exakt einzuhalten.

- Die Variable `GRUB_HIDDEN_TIMEOUT` ist dann von Bedeutung, wenn GRUB während der Installation nur eine einzige Linux-Distribution auf Ihrem Rechner erkennt. In diesem Fall gibt `GRUB_HIDDEN_TIMEOUT` an, wie lange der Benutzer Zeit hat, um mit ⇧ das GRUB-Menü anzuzeigen. Während dieser Wartezeit bleibt der Bildschirm schwarz.

  Unter Ubuntu bewirkt `GRUB_HIDDEN_TIMEOUT=0`, dass GRUB das Betriebssystem sofort startet. Um in den Bootvorgang einzugreifen, müssen Sie unmittelbar nach dem Rechnerstart ⇧ drücken. Wenn mehrere Betriebssysteme installiert sind, ignoriert GRUB die `GRUB_HIDDEN_TIMEOUT`-Einstellung und zeigt das Menü an.

- `GRUB_HIDDEN_TIMEOUT_QUIET=true` verhindert, dass während der `GRUB_HIDDEN_TIMEOUT`-Wartezeit ein Countdown-Zähler angezeigt wird. Wenn Sie möchten, dass das GRUB-Menü immer angezeigt wird (auch dann, wenn nur Ubuntu auf dem Rechner installiert ist), stellen Sie den Zeilen `GRUB_HIDDEN_TIMEOUT=...` und `GRUB_HIDDEN_TIMEOUT_QUIET=...` jeweils das Kommentarzeichen `#` voran.

- `GRUB_TIMEOUT=n` gibt an, wie viele Sekunden GRUB auf die Auswahl eines Menüeintrags wartet. Wenn diese Zeit ohne Benutzereingaben verstreicht, startet GRUB das ausgewählte Betriebssystem. Die hier eingestellte Zeit kommt nur zur Geltung, wenn das GRUB-Menü überhaupt erscheint.

- Die Variable `GRUB_DISTRIBUTOR` wird vom weiter unten beschriebenen Script `10_linux` ausgewertet und gibt den Namen der aktuellen Distribution an, also z. B. `Ubuntu` oder `Fedora`.

- Auch `GRUB_CMDLINE_LINUX` und `GRUB_CMDLINE_LINUX_DEFAULT` werden von `10_linux` berücksichtigt und geben an, welche Optionen an den Kernel übergeben werden sollen. Die `GRUB_CMDLINE_LINUX`-Optionen gelten für jeden Start; die `GRUB_CMDLINE_LINUX_DEFAULT`-Optionen werden zusätzlich für den Standardstart hinzugefügt, aber nicht für den Recovery Mode.

- Standardmäßig wird das GRUB-Menü im Grafikmodus in einer Auflösung von 640 * 480 Pixel angezeigt. Wenn Sie eine höhere Auflösung wünschen, können Sie diese mit `GRUB_GFXMODE` einstellen. Wenn Sie auf den Grafikmodus ganz verzichten möchten, aktivieren Sie die dafür vorgesehene Einstellung `GRUB_TERMINAL=console`. Beide Variablen werden vom Script `00_header` ausgewertet. In der Standardeinstellung gibt es keinen optisch sichtbaren Unterschied zwischen dem Text- und dem Grafikmodus, allerdings können nur im Grafikmodus Unicode-Zeichen angezeigt werden.
- GRUB übergibt normalerweise das Root-Verzeichnis als UUID-Nummer an den zu startenden Linux-Kernel. Wenn Sie stattdessen die Angabe des Device-Namens (z. B. `/dev/sda1`) vorziehen, aktivieren Sie die Zeile `GRUB_DISABLE_LINUX_UUID=true`. Diese Einstellung gilt nur für den Start der aktiven Distribution (Script `10_linux`), nicht für andere Distributionen.
- `update-grub` bzw. `grub2-mkconfig` erzeugt normalerweise auch Menüeinträge zum Start von Linux im Recovery Mode. Dabei wird Linux im Single-User-Modus und ohne Anzeige eines Splash-Bildschirms gestartet. Mit `GRUB_DISABLE_RECOVERY="true"` werden keine Recovery-Einträge erzeugt.
- Mit `GRUB_INIT_TUNE=...` können Sie beim Start von GRUB einen Ton ausgeben lassen.

Automatische Erzeugung von grub.cfg

Die Grundidee der GRUB-Konfiguration besteht darin, dass Sie selbst nur die Eckdaten der GRUB-Konfiguration vorgeben. Die finale Konfigurationsdatei `grub.cfg` wird unter Berücksichtigung dieser Vorgaben durch ein Script automatisch erzeugt. Der springende Punkt dabei ist, dass die GRUB-Scripts versuchen, *alle* auf dem Rechner installierten Betriebssysteme zu erkennen und entsprechende Menüeinträge in die `grub.cfg` einzubauen. Das gilt auch für alle Betriebssysteme, die zu einem späteren Zeitpunkt hinzugekommen sind.

Das Verzeichnis `/etc/grub.d` enthält dazu mehrere ausführbare Script-Dateien (siehe Tabelle 26.2). Wenn eine neue Version von `grub.cfg` erzeugt werden soll, führt `update-grub` alle in `grub.d` enthaltenen Scripts der Reihe nach aus. Das Ergebnis, also die Standardausgabe der Scripts, landet in `grub.cfg`. Die Script-basierte Vorgehensweise macht die Konfigurationsdateien leider recht unübersichtlich: In den eigentlichen Code sind immer wieder Anweisungen der Form `cat << EOF` eingebettet, die alle folgenden Zeilen bis zum Kürzel EOF an die Standardausgabe leiten. Diese Zeilen enthalten selbst oft Script-Code, der erst von GRUB beim Systemstart ausgewertet wird.

Die beiden interessantesten Scripts sind `10_linux` und `30_os-prober`. `10_linux` liefert für jede Kernelversion im `/boot/`-Verzeichnis zwei GRUB-Menüeinträge: einen zum gewöhnlichen Start und einen zweiten für einen Recovery-Start im

Single-User-Modus und ohne Splash-Bildschirm. Die Menüeinträge sind nach Versionsnummern sortiert, die aktuellste Version steht am Anfang der Liste.

Datei	Funktion
00_header	GRUB-Grundeinstellungen
05_debian_theme	farbliche Gestaltung des Menüs (nur unter Debian und Ubuntu)
10_linux	Menüeinträge zum Start der aktuellen Distribution
20_linux_xen	Menüeinträge zum Start virtueller Maschinen
20_memtest86+	Menüeintrag zum Start von Memtest86 (nur unter Debian/Ubuntu)
30_os-prober	Menüeinträge zum Start aller anderen Betriebssysteme
40_custom	Muster für eigene Konfigurationsdateien
41_custom	baut in grub.cfg den Text aus custom.cfg ein

Tabelle 26.2 Dateien im Verzeichnis /etc/grub.d/

30_os-prober ruft das Script os-prober auf. Es liefert eine Liste aller Betriebssysteme auf allen zugänglichen Festplattenpartitionen. Für jedes dieser Betriebssysteme werden nun Menüeinträge erzeugt, wobei bei Linux-Distributionen auf die eventuell vorhandene GRUB-Konfiguration zurückgegriffen wird. Dabei kommt es zum Aufruf unzähliger Scripts, die alle Teil des Pakets os-prober sind.

grub.cfg individuell erweitern

Wenn Sie grub.cfg um eigene Einträge erweitern möchten, fügen Sie dem Verzeichnis grub.d eigene Scripts hinzu. Die Scripts werden in der durch die Startnummer vorgegebenen Reihenfolge ausgeführt; bei gleichlautender Startnummer in alphabetischer Abfolge. Denken Sie daran, das Execute-Bit zu setzen. Beachten Sie auch, dass die Datei nicht einfach unverändert in grub.cfg eingebaut wird, sondern dass nur das Ergebnis (die Standardausgabe) in grub.cfg einfließt!

Die Musterdatei 40_custom zeigt eine mögliche Vorgehensweise: Dabei wird das tail-Kommando auf die Datei angewandt (Parameter $0). Die Option -n +3 bewirkt, dass tail die Datei ab der dritten Zeile ausgibt, die ersten zwei Zeilen also überspringt.

```
#!/bin/sh
exec tail -n +3 $0
# This file is an example on how to add custom entries
...
```

Eine andere Variante zeigt 41_custom auf. Der dort enthaltene Code wird unverändert in grub.cfg übertragen und erst zur Laufzeit (also bei der Anzeige des GRUB-Menüs) ausgewertet. Zu diesem Zeitpunkt wird getestet, ob die Datei /boot/grub/custom.cfg (Ubuntu) bzw. /boot/grub2/custom.cfg (Fedora, openSUSE) existiert. Ist das der Fall, wird sie der GRUB-Konfiguration hinzugefügt. Da source zur

GRUB-Laufzeit ausgeführt wird, werden Änderungen in `custom.cfg` wirksam, ohne dass die GRUB-Konfigurationsdatei `grub.cfg` neu erzeugt werden muss.

```
#!/bin/sh
cat <<EOF
if [ -f  \$prefix/custom.cfg ]; then
  source \$prefix/custom.cfg;
fi
EOF
```

Syntax und Interna

Eine vollständige Syntaxbeschreibung aller in `grub.cfg` erlaubten Schlüsselwörter ist hier aus Platzgründen unmöglich. Ich beschränke mich daher im Folgenden auf die wichtigsten Schlüsselwörter, die in den Beispielen dieses Abschnitts vorkommen. Das offizielle GRUB-Handbuch (die PDF-Fassung umfasst mehr als 100 Seiten!) finden Sie hier:

http://www.gnu.org/software/grub/manual

Variablen

Mit `set varname=wert` führen Sie Variablenzuweisungen durch. Zum Auslesen von Variablen verwenden Sie die Schreibweise `$varname`. Wenn Sie interaktiv GRUB-Kommandos ausführen, zeigt `echo $varname` den Inhalt einer Variablen an, und `set` gibt alle definierten Variablen zurück.

Einige Variablen haben außerdem eine besondere Bedeutung. Dazu zählen z. B. `default`, `timeout`, `color_xxx`, `menu_color_xxx` und insbesondere `root`: Bei sämtlichen Zugriffen auf Dateien wird automatisch die durch `root` definierte Partition gelesen.

GRUB kann Variablen zur Laufzeit bleibend speichern. Dazu muss zuerst im Linux-Dateisystem die Datei `/boot/grub[2]/grub-editenv` eingerichtet werden, was bei den meisten Distributionen standardmäßig der Fall ist:

```
root#  grub-editenv /boot/grub[2]/grubenv create
```

GRUB kann nun zur Laufzeit mit `save_env` *varname* eine Variable in dieser Datei speichern bzw. mit `load_env` alle Variablen aus dieser Datei lesen. Vorher muss die GRUB-Variable `root` so eingestellt werden, dass sie auf die Partition mit der Environment-Datei verweist.

Partitionen

GRUB kennt eine eigene Nomenklatur zur Bezeichnung von Festplatten und den darauf enthaltenen Partitionen (siehe Tabelle 26.3). Inkonsequent ist dabei die Numerierung: Die erste Festplatte hat die Nummer 0, die erste Partition hingegen die Nummer 1!

GRUB-2-Device-Name	Bedeutung
(hd0)	die erste Festplatte/SSD (entspricht /dev/sda)
(hd1)	die zweite Festplatte/SSD (entspricht /dev/sdb)
(hd0,1)	die erste Partition der ersten Festplatte/SSD (/dev/sda1)
(hd2,8)	die achte Partition der dritten Festplatte/SSD (/dev/sdc8)

Tabelle 26.3 GRUB-2-Partitionsnamen

Es ist zulässig, der Partitionsnummer ein Kürzel voranzustellen, das das Partitionierungsverfahren angibt: `msdos` für Datenträger mit der Partitionstabelle im MBR, `gpt` für Datenträger mit einer GUID Partition Table. Daraus ergeben sich dann Partitionsnamen wie `(hd0,msdos3)` oder `(hd0,gpt2)`.

Umgang mit UUIDs (search)

In `grub.cfg` kommt mehrfach die folgende Kommandosequenz vor:

```
set root=(hd1,1)
search --no-floppy --fs-uuid --set 724f...
```

Das erste Kommando initialisiert die Variable `root`. Die zweite Anweisung sucht nach einem Dateisystem mit der angegebenen UUID, also z. B. `724f`. Falls die Suche erfolgreich ist, speichert GRUB aufgrund der Option `--set` den entsprechenden Partitionsnamen in der Variablen `root`. Diese Doppelgleisigkeit ist eine Vorsichtsmaßnahme. Sie stellt sicher, dass GRUB die Partition auch dann findet, wenn das Dateisystem inzwischen neu formatiert wurde (andere UUID) oder der Datenträger aufgrund einer anderen Verkabelung eine andere Device-Nummer hat.

Module

Mit `insmod name` lädt GRUB zur Laufzeit Erweiterungsmodule mit Zusatzfunktionen. GRUB sucht nach den Moduldateien `name.mod` im Verzeichnis `/boot/grub[2]` in der durch die Variable `root` eingestellten Partition. Wichtige Module sind unter anderem `part_msdos` und `part_gpt` (Partitionstabellen lesen), `ext2` (Dateisysteme `ext2` bis `ext4`), `raid`, `raid5rec`, `raid6rec` und `mdraid` (Software-RAID), `lvm`, `gfxterm` (grafische Konsole), `vbe` (Grafiksystem) sowie `jpeg`, `tga` und `png` zum Lesen von Grafikdateien.

GRUB-Menüeinträge

menuentry und submenu

GRUB-Menüeinträge werden mit dem Schlüsselwort `menuentry` eingeleitet. Der nachfolgende Text steht in Anführungszeichen und darf internationale Zeichen enthalten. Beginnend mit GRUB-Version 2.00 unterstützt GRUB auch Untermenüs. Bei der Bedienung von GRUB gelangen Sie gegebenenfalls mit Esc aus einem Untermenü zurück in das Hauptmenü.

```
menuentry "Linux" {
  startkommandos ...
}
submenu 'Untermenü' {
  menuentry 'Eintrag 1' { ... }
  menuentry 'Eintrag 2' { ... }
}
```

Linux starten

Ein GRUB-2-Menüeintrag zum Start von Linux sieht in der Minimalvariante wie das folgende Beispiel aus:

```
menuentry "Linux" {
  set root=(hd0,3)
  linux   /boot/vmlinuz-n.n.n    root=... ro quiet splash
  initrd  /boot/initrd.img-n.n.n
}
```

`set root` gibt die Partition an, in der sich der Kernel- und die Initrd-Datei befinden. Die Schlüsselwörter `linux` und `initrd` geben relativ zur Partition die Dateinamen an. Die angegebenen Parameter werden an den Kernel übergeben. Unbedingt erforderlich sind `root` zur Angabe der Systempartition und `ro`, damit der Zugriff auf die Systempartition anfänglich nur lesend erfolgt. Alle weiteren Parameter sind distributionsabhängig. Einige Beispiele:

Debian: `root=UUID=xxx ro quiet`
Fedora: `root=/dev/xxx ro rhgb quiet vconsole.font=... LANG=...`
openSUSE: `root=UUID=xxx resume=/dev/xxx splash=silent showopts video=nxn quiet`
Ubuntu: `root=UUID=xxx ro quiet splash`

Wenn es eine eigene Bootpartition gibt, geben Sie mit `set root` diese Partition an. Bei `linux` und `initrd` entfällt dann die Angabe des Bootverzeichnisses:

```
menuentry "Linux - Mit eigener Bootpartition" {
  set root=(hd0,2)
  linux   /vmlinuz-n.n.n     root=... ro quiet splash
  initrd  /initrd.img-n.n.n
}
```

Wenn die Partition mit den Kernel- und Initrd-Dateien Teil eines LVM-Systems und/oder eines Software-RAIDs ist, müssen Sie die entsprechenden GRUB-Module laden. Bei RAID-5 bzw. RAID-6 kommt noch das Modul `raid5rec` bzw. `raid6rec` hinzu. In `set root` können Sie nun die Systempartition in der Schreibweise (*lvname*) bzw. (md*n*) angeben:

```
menuentry "Linux - Mit Software-RAID" {
  insmod raid mdraid
  set root=(md0)
  linux   /boot/vmlinuz-n.n.n    root=... ro quiet splash
  initrd  /boot/initrd.img-n.n.n
}
menuentry "Linux - Mit LVM" {
  insmod lvm
  set root=(vg1-root)
  linux   /boot/vmlinuz-n.n.n    root=... ro quiet splash
  initrd  /boot/initrd.img-n.n.n
}
menuentry "Linux - LVM auf RAID-5" {
  insmod raid raid5rec mdraid lvm
  set root=(vg1-root)
  linux   /boot/vmlinuz-n.n.n    root=/dev/mapper/... ro quiet splash
  initrd  /boot/initrd.img-n.n.n
}
```

Wenn Sie sich nicht auf Device-Nummern verlassen möchten, können Sie die Systempartition auch durch `search` anhand der UUID suchen. Ist das `search`-Kommando erfolgreich, wird die GRUB-Variable `root` entsprechend geändert. Das funktioniert auch für LVM- und RAID-Partitionen, sofern vorher die richtigen GRUB-Module geladen wurden.

```
menuentry "Linux - root-Variable anhand UUID einstellen" {
  set root=(hd0,3)
  search --no-floppy --fs-uuid --set 12af...
  linux   /boot/vmlinuz-n.n.n    root=... ro quiet splash
  initrd  /boot/initrd.img-n.n.n
}
```

Linux auf EFI-Rechner starten

In GRUB-Dateien auf EFI-Rechnern ersetzen Sie `linux` durch `linuxefi` und `initrd` durch `initrd`. Außerdem müssen Sie sicherstellen, dass das `part_gpt`-Modul geladen ist.

```
menuentry 'linux/efi' {
  insmod part_gpt
  set root=(hd0,gpt6)
  linuxefi /boot/vmlinuz-n.n.n root=UUID=a57a... ro quiet
  initrdefi /boot/initramfs-n.n.n
}
```

Windows auf einem BIOS-Rechner starten

Um Windows auf einem BIOS-Rechner zu starten, wählen Sie mit `set root` die Windows-Systempartition aus und starten dann mit `chainloader +1` dessen Bootloader. Beachten Sie, dass Windows ab Version 7 standardmäßig zwei Partitionen einrichtet: eine rund 100 MByte große Bootpartition mit den Dateien `bootmgr` und `bootsect.bak` sowie eine wesentlich größere Systempartition. In GRUB müssen Sie die Bootpartition angeben. Das `search`-Kommando ist wie immer optional. Auch auf `drivemap` können Sie in der Regel verzichten. Das Kommando versucht Windows vorzumachen, dass sich Windows auf der ersten Festplatte befindet, selbst wenn das tatsächlich gar nicht der Fall ist. In seltenen Fällen ist das erforderlich, damit Windows startet.

```
menuentry "Windows 7" {
  set root=(hd0,1)
  search --no-floppy --fs-uuid --set 12345678...
  drivemap -s (hd0) $root
  chainloader +1
}
```

Wie Sie Windows auf einem EFI-Rechner per GRUB starten, verrät der nächste Abschnitt.

In einen anderen Bootloader verzweigen

GRUB gibt Ihnen mit dem bereits erwähnten `chainloader`-Kommando die Möglichkeit, in einen anderen Bootloader zu verzweigen. Die entsprechenden Anweisungen betten Sie am besten in eine Konfigurationsdatei ein, die Sie entsprechend dem Muster `/etc/grub.d/40_custom` gestalten.

In einen BIOS-Bootloader verzweigen

Wenn Sie auf Ihrem Rechner einen weiteren Bootloader in den Startsektor einer Partition installiert haben, können Sie aus dem GRUB-2-Menü in diesen Bootloader verzweigen. Dazu geben Sie dessen Partition mit `set root` an (optional auch mit `search`) und führen `chainloader +1` aus:

```
menuentry "GRUB in /dev/sdb7" {
  set root=(hd1,7)
  search --no-floppy --fs-uuid --set 12345678...
  chainloader +1
}
```

Sollten die obigen Zeilen nicht zum gewünschten Ergebnis führen, können Sie versuchen, auf `set root` zu verzichten und die gewünschte Partition direkt mit `chainloader` anzugeben, also:

```
menuentry "GRUB 0.97 in /dev/sdb7" {
  chainloader (hd1,7)+1 --force
}
```

GRUB-Installationen in eine Partition

Unter GRUB 0.97 war es nichts Ungewöhnliches, GRUB in den Beginn einer gewöhnlichen Datenpartition zu installieren. Die obigen Beispiele setzen derartige GRUB-Installationen voraus.

Bei GRUB 2 sind solche Installationen aber nicht mehr empfehlenswert, und das Handbuch rät davon ausdrücklich ab! Auf BIOS-Rechnern soll GRUB 2 ausschließlich in den MBR der Festplatte oder SSD installiert werden.

In einen EFI-Bootloader verzweigen

Auf EFI-Rechnern können Sie aus GRUB heraus direkt einen anderen EFI-Bootloader starten. Die folgenden Beispiele gehen davon aus, dass die EFI-Partition die erste Partition der ersten Festplatte ist; andernfalls müssen Sie `set root` entsprechend anpassen.

```
menuentry "Windows-Bootloader starten (EFI)" {
  insmod part_gpt
  set root='(hd0,1)'
  chainloader  /EFI/Microsoft/Boot/bootmgfw.efi
}

menuentry "Ubuntu-Bootloader starten (EFI)" {
  insmod part_gpt
  set root='(hd0,1)'
  chainloader  /EFI/ubuntu/grubx64.efi
}
```

Geeignete EFI-Bootloader können Sie rasch mit diesem Kommando ermitteln:

```
root#  find /boot/efi -name '*.efi' | sort
/boot/efi/EFI/Microsoft/Boot/bootmgfw.efi
/boot/efi/EFI/Microsoft/Boot/bootmgr.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/efi/EFI/fedora/grubx64.efi
/boot/efi/EFI/fedora/shim.efi
...
```

Bei Windows-Installationen enthält `bootmgfw.efi` den Bootloader. `bootmgr.efi` lässt sich nicht starten.

Individuelle Konfiguration

GRUB 2 ist so vorkonfiguriert, dass damit alle Betriebssysteme auf einem BIOS-Rechner gestartet werden können. Die Standardkonfiguration funktioniert gut und ist sicherlich in den meisten Fällen ausreichend. Dieser Abschnitt richtet sich nur

an Linux-Anwender, die GRUB 2 individuell adaptieren möchten. Unter SUSE können Sie zum Einrichten bzw. Konfigurieren von GRUB auch das YAST-Modul System • Konfiguration des Bootloaders verwenden.

os-probe deaktivieren

Die Verarbeitung des Scripts `30_os-probe` dauert auf Rechnern mit vielen Partitionen recht lange. Wenn Sie dieses Script nicht benötigen – z. B. weil Sie zum Start anderer Linux-Distributionen lieber selbst definierte GRUB-Menüeinträge verwenden –, tragen Sie die Zeile `GRUB_DISABLE_OS_PROBER=true` in `/etc/default/grub` ein.

Grafische Gestaltung

Sie können das GRUB-Menü mit einem Bild hinterlegen. GRUB versteht die Formate JPG, PNG und TGA. Der erforderliche Code zur Integration einer Hintergrundgrafik ist bei Debian und Ubuntu im Script `05_debian_theme` bereits enthalten. Sie müssen lediglich drei Variablen ändern und dort den Dateinamen Ihres Bilds sowie die gewünschten Farben für den Text angeben.

```
# in /etc/grub.d/05_debian_theme
...
WALLPAPER="/boot/grub/myown.png"
COLOR_NORMAL="white/black"
COLOR_HIGHLIGHT="yellow/black"
```

GRUB 2 enthält auch eine experimentelle Unterstützung von Themen, die neben dem Hintergrund auch verschiedene Schriften und eine vom klassischen GRUB-Menü abweichende Bedienung ermöglichen. Zu den wenigen Distributionen, die davon Gebrauch machen, zählt openSUSE. Das Thema wird durch die Textdatei `/boot/grub2/themes/openSUSE/theme.txt` bestimmt. Für die Integration dieser Datei in die GRUB-Konfiguration ist `/etc/grub.d/00_header` verantwortlich. Tipps zur Realisierung eines vergleichbaren Themas für Ubuntu finden Sie hier:

http://ubuntuforums.org/showthread.php?t=2081013

Default-Betriebssystem festlegen

In `/etc/default/grub` können Sie die Nummer des GRUB-Menüeintrags festlegen, der automatisch gestartet wird. In der Praxis bringt das wenig: Wenn Sie beispielsweise möchten, dass standardmäßig Windows gestartet wird und dass dessen Menüeintrag an der zehnten Stelle steht, dann stellen Sie `GRUB_DEFAULT=9` ein, weil die Zählung mit 0 beginnt.

Es kann aber sein, dass das GRUB-Menü beim nächsten Kernel-Update zwei zusätzliche Einträge erhält – und dann ist Ihre Einstellung falsch. Besser ist es, `GRUB_DEFAULT=0` zu belassen und stattdessen den gewünschten GRUB-Menüeintrag vor allen anderen Einträgen einzufügen. Das gelingt am einfachsten durch ein zusätzliches Script in `/etc/grub.d`, wobei der Dateiname mit einer Nummer kleiner 10 beginnt. Die folgenden Zeilen können als Muster dienen:

```
#!/bin/sh
exec tail -n +3 $0
# Datei /etc/grub.d/09_boot-windows-by-default
menuentry "Windows 7" {
  set root=(hd0,1)
  chainloader +1
}
```

Eine andere Möglichkeit besteht darin, den Menüeintrag in `GRUB_DEFAULT` exakt anzugeben, z. B. so:

```
GRUB_DEFAULT='Windows 7 (loader) (on /dev/sda1)'
```

Diese Vorgehensweise ist aber nur dann zweckmäßig, wenn sich der Menüeintrag bei GRUB-Updates nicht ändert. Für Windows funktioniert das gut. Bei Linux enthalten die automatisch generierten Menüeinträge aber oft die Kernelversion – und die ändert sich bei jedem Kernel-Update.

Manuelle Installation und Erste Hilfe für BIOS-PCs

Normalerweise wird GRUB 2 während der Installation Ihrer Linux-Distribution korrekt eingerichtet. In der Folge werden Sie zwar vielleicht Änderungen an der GRUB-Konfiguration bzw. `grub.cfg` durchführen, die GRUB-Installation als solche müssen Sie aber nicht mehr anrühren.

Dieser Abschnitt für BIOS-PCs und der folgende Abschnitt für EFI-PCs sind nur dann relevant, wenn Sie aus irgendeinem Grund eine manuelle Installation von GRUB durchführen möchten oder wenn Sie eine defekte GRUB-Installation reparieren müssen – z. B. weil ein anderes Betriebssystem den Inhalt des MBR überschrieben hat.

Manuelle Installation mit grub-install

Das Script `grub-install`, das unter Fedora sowie openSUSE `grub2-install` heißt, installiert den Bootloader in die ersten Sektoren der angegebenen Festplatte bzw. SSD, also in den MBR sowie in weitere Sektoren, die sich vor dem Beginn der ersten Partition befinden. Als einzigen Parameter übergeben Sie in der Regel den Device-Namen des Datenträgers. Dabei ist sowohl die Linux- als auch die GRUB-Schreibweise zulässig, also `/dev/sda` oder `(hd0)`.

```
root#  grub-install /dev/sda
```

Eine Installation in den Startsektor einer Partition ist theoretisch möglich (also z. B. `grub-install /dev/sda3` bzw. `(hd0,3)`), wird aber anders als in GRUB 0.97 nicht mehr empfohlen: Der Platz zum Einbetten des GRUB-Codes ist zu klein, und die deswegen erforderliche Verwendung von Link-Listen mit Querverweisen auf woanders befindliche Datenblöcke gilt als instabil. Wenn diese Argumente Sie nicht überzeugen, können Sie die Installation mit der Option `--force` erzwingen.

Sonderfall BIOS-PC und GPT (bios_grub-Partition)

Grundsätzlich unterstützt Linux auch auf BIOS-Rechnern die Installation auf eine Festplatte oder SSD mit einer GUID Partition Table. Allerdings empfiehlt das GRUB-Handbuch in diesem Sonderfall, für die GRUB-Installation eine eigene Partition in der Größe von 1 MByte mit dem Flag `bios_grub` vorzusehen. Diese Partition ist nur für die Installation eines BIOS-kompatiblen Bootloaders gedacht. Diese `bios_grub`-Partition braucht nicht formatiert zu werden. Wenn Sie die Partition manuell einrichten, setzen Sie mit `parted` das Flag `bios_grub`, wobei Sie *n* durch die gewünschte Partitionsnummer ersetzen:

```
root#  parted /dev/sda set n bios_grub on
```

Achtung

Markieren Sie mit dem `bios_grub`-Flag keine Partition, die Daten enthält. Bei der GRUB-Installation wird der Beginn der Partition überschrieben; ein eventuell auf der Partition befindliches Dateisystem wird dadurch vollständig zerstört!

Wenn GRUB bei der Installation die Existenz einer `bios_grub`-Partition feststellt, installiert es den Beginn der GRUB-Codes wie üblich in den MBR der Festplatte, den restlichen GRUB-Code aber in die gekennzeichnete `bios_grub`-Partition. Diese Vorgehensweise ist bei GRUB-Installationen auf Festplatten mit GPT zwar nicht zwingend erforderlich, gilt aber als wesentlich robuster, vor allem, wenn auch andere Betriebssysteme (Windows) auf dem Rechner installiert werden.

Beachten Sie aber, dass es auch einen Nachteil gibt: Wenn eine derartige Partition existiert, ist es unmöglich, mehrere GRUB-2-Installationen parallel durchzuführen, weil bei jeder neuerlichen GRUB-Installation der Inhalt der `bios_grub`-Partition überschrieben wird. Weitere Informationen zum Thema GRUB 2 und GTP können Sie hier nachlesen:

http://www.gnu.org/software/grub/manual/html_node/BIOS-installation.html
http://www.wensley.org.uk/gpt

GRUB in einem Live-System reparieren (BIOS)

Wenn die GRUB-Installation fehlgeschlagen ist oder durch ein anderes Betriebssystem überschrieben wurde, müssen Sie GRUB von einer Live-CD mit aktuellen GRUB-2-Tools neu installieren. Nach dem Systemstart wechseln Sie in den `root`-Modus (`sudo -s` bei Ubuntu), binden die Systempartition und die aktiven `/dev`-, `/proc`- und `/sys`-Verzeichnisse in das Dateisystem ein und führen dann `chroot` aus. Gegebenenfalls binden Sie nun auch die Bootpartition in das neue `root`-Dateisystem ein.

Nun aktualisieren Sie die GRUB-Konfiguration und schreiben mit `grub[2]-install` GRUB an den gewünschten Ort, zumeist in den MBR der ersten Festplatte. Wie

üblich müssen Sie in den folgenden Kommandos `/dev/sdan` durch Ihre eigenen Device-Namen ersetzen!

```
root#  mkdir /syspart
root#  mount /dev/sda2 /syspart                  (Systempartition)
root#  mount -o bind /dev  /syspart/dev
root#  mount -o bind /proc /syspart/proc
root#  mount -o bind /sys  /syspart/sys
root#  chroot /syspart
root#  mount /dev/sda1 /boot                     (Bootpartition, falls vorhanden)
root#  update-grub                               (Debian/Ubuntu)
root#  grub-install /dev/sda                     (Debian/Ubuntu, Forts.)
root#  grub2-mkconfig -o /pfad/zu/grub.cfg       (Fedora/openSUSE)
root#  grub2-install /dev/sda                     (Fedora/openSUSE, Forts.)
root#  exit
```

Manuelle Installation und Erste Hilfe für EFI-PCs

Manuelle Installation mit grub-install

Eine manuelle Installation von GRUB 2 auf einem EFI-Rechner ist denkbar einfach. Sie müssen an `grub-install` keinerlei Parameter übergeben:

```
root#  grub-install
```

Durch dieses Kommando wird das Verzeichnis `/boot/efi/EFI/`*`distributionsname`* erzeugt. In dieses Verzeichnis wird eine neue Bootdatei mit der Endung `.efi` geschrieben, die den GRUB-Code enthält. Außerdem wird die `.efi`-Datei in die Liste der EFI-Booteinträge aufgenommen und dort an den ersten Platz gestellt. `grub-install` greift dazu auf das Kommando `efibootmgr` zurück, das ich Ihnen im übernächsten Abschnitt näher vorstelle.

Damit `grub-install` erfolgreich ausgeführt werden kann, müssen einige Voraussetzungen erfüllt sein:

- Die GRUB-Konfiguration in der Datei `/boot/grub[2]/grub.cfg` muss vorbereitet sein.
- Die EFI-Partition muss unter dem Pfad `/boot/efi` in den Verzeichnisbaum eingebunden sein.
- Das Kommando `efibootmgr` aus dem gleichnamigen Paket muss installiert sein.
- Das Kernelmodul `efivars` muss geladen sein. `modprobe efivars` gelingt allerdings nur, wenn die Distribution im EFI-Modus gestartet wurde, nicht im BIOS-Modus. Deswegen ist es ohne ein EFI-bootfähiges Live-System schwierig, eine zuerst im BIOS-Modus installierte Linux-Distribution auf EFI umzustellen.

GRUB in einem Live-System reparieren (EFI)

Im Prinzip erfolgt die GRUB-Reparatur für ein EFI-System ganz ähnlich wie bei einem BIOS-System. Entscheidend ist aber, dass Sie das Live-System im EFI-Modus starten, nicht im BIOS-Modus.

Anschließend wechseln Sie in den `root`-Modus, binden die Systempartition und die aktiven `/dev`-, `/proc`- und `/sys`-Verzeichnisse in das Dateisystem ein und führen dann `chroot` aus. Gegebenenfalls binden Sie nun auch die Bootpartition in das neue `root`-Dateisystem ein. Nun aktualisieren Sie die GRUB-Konfiguration und schreiben sie mit `grub-install` in die EFI-Partition. Vergessen Sie nicht, in den folgenden Kommandos `/dev/sda`*n* durch Ihre eigenen Device-Namen zu ersetzen!

```
root#  mkdir /syspart
root#  mount /dev/sda2 /syspart                    (Systempartition)
root#  mount -o bind /dev  /syspart/dev
root#  mount -o bind /proc /syspart/proc
root#  mount -o bind /sys  /syspart/sys
root#  chroot /syspart
root#  mount /dev/sda1 /boot/efi                   (EFI-Partition)
root#  update-grub
root#  grub-install
root#  exit
```

GRUB-Kommandos zum Linux-Start manuell eingeben

Wenn Sie zwar GRUB starten können, aber nach der Auswahl des Linux-Menüeintrags der Linux-Start scheitert, können Sie innerhalb des GRUB-Menüs mit C in den interaktiven Modus wechseln und dann die folgenden Kommandos ausführen:

```
grub>  set root=(hd0,1)
grub>  linux  /vmlinuz root=/dev/sda1
grub>  initrd /initrd.img
grub>  boot
```

Statt `(hd0,1)` und `/dev/sda1` geben Sie den Namen Ihrer Linux-Systempartition an. Die Dateien `/vmlinuz` und `/initrd.img` verweisen bei den meisten Distributionen auf die aktuellste Kernel- und Initrd-Datei im Verzeichnis `/boot`. Sollte das bei Ihnen nicht der Fall sein, müssen Sie den Ort der Kernel- und der Initrd-Datei exakt angeben. GRUB unterstützt Sie bei der Eingabe mit der Eingabevervollständigung durch ⇆.

EFI-Booteinträge und -Einstellungen ändern (efibootmgr)

Woher weiß EFI eigentlich, welche Betriebssysteme installiert sind bzw. welche Booteinträge es anzeigen soll? Bei EFI-Mainboards werden diese Informationen in einem nicht-flüchtigen Speicher (NVRAM) festgehalten. Jedes Mal, wenn ein neues Betriebssystem installiert wird, wird nach dem Einrichten der `*.efi`-Datei in der EFI-Partition ein entsprechender Eintrag im NVRAM gespeichert.

efibootmgr

Unter Linux können Sie die so gespeicherten EFI-Daten mit dem Kommando `efibootmgr` auslesen oder verändern. Das Kommando setzt voraus, dass das Kernelmodul `efivars` geladen ist. Sollte das nicht der Fall sein, führen Sie `modprobe efivars` aus. Das gelingt nur, wenn Linux im EFI-Modus gebootet wurde. Verwenden Sie für Reparaturarbeiten gegebenenfalls ein Linux-Live-System, das sich im EFI-Modus starten lässt!

Wenn `efibootmgr` ohne weitere Optionen ausgeführt wird, listet es die EFI-Booteinträge sowie einige weitere Parameter des EFI-Bootloaders auf. Das folgende Ergebnis bedeutet, dass auf dem Rechner Ubuntu, Fedora und Windows im EFI-Modus installiert sind. Bei nächsten Neustart wird nach einer Wartezeit von einer Sekunde automatisch Ubuntu gestartet (`BootCurrent`). Während dieser Wartezeit kann mit einer mainboard-spezifischen Tastenkombination (bei meinem Testrechner: F8) das EFI-Menü angezeigt werden.

```
root#  efibootmgr
BootCurrent: 0000
Timeout: 1 seconds
BootOrder: 0000,0005,0003,0001,0002
Boot0000* ubuntu
Boot0001* Hard Drive
Boot0002* CD/DVD-Laufwerk
Boot0003* Windows Boot Manager
Boot0005* Fedora
```

Wenn Sie möchten, dass beim nächsten Neustart einmalig Fedora gestartet werden soll, legen Sie dessen Booteintrag mit `-n` fest:

```
root#  efibootmgr -n 5
```

Soll die Bootreihenfolge hingegen bleibend geändert werden, geben Sie den gewünschten Eintrag mit der Option `-o` an:

```
root#  efibootmgr -o 5
```

Das folgende Kommando erzeugt einen neuen EFI-Booteintrag. Die Pfadangabe ist relativ zur EFI-Partition (also `/boot/efi`), und als Verzeichnistrenner muss `\` verwendet werden. Die Verdoppelung der `\`-Zeichen ist erforderlich, weil die Shell ein einfaches `\`-Zeichen als Kennzeichnung von Sonderzeichen interpretiert. Mit der Option `-L` geben Sie den Namen an, der im EFI-Menü angezeigt werden soll.

```
root#  efibootmgr -c -l \\EFI\\test\\abc.efi -L abc
```

Natürlich können Sie Booteinträge auch wieder entfernen. Dazu geben Sie mit `-b` die Nummer des Eintrags an:

```
root#  efibootmgr -b 6 -B
```

Weitere Optionen des Kommandos `efibootmgr` sind in dessen `man`-Seite dokumentiert.

Fehler in der EFI-Speicherverwaltung

Anfang 2013 wurde bekannt, dass einige PC-Hersteller ihr EFI fehlerhaft implementiert hatten. Das konnte nach einer GRUB-Installation die fatale Folge haben, dass der Rechner sich nicht mehr starten ließ. Schuld an dem Problem ist also nicht Linux, sondern der jeweilige Mainboard-Hersteller.

Um unnötige Schäden zu vermeiden, wurde daraufhin im Kernel ein Schutzmechanismus eingebaut, der fehlerhafte EFI-Versionen zu erkennen versucht und in diesem Fall eine Veränderung von EFI-Variablen blockiert. Das hat aber zur Folge, dass dann die GRUB-Installation scheitert – unter Umständen selbst dann, wenn das EFI eigentlich in Ordnung ist, aber die Erkennung nicht richtig gelang. Abhilfe schafft dann ein EFI-Update oder die manuelle Einrichtung von GRUB mit einem älteren Live-System, dessen Kernel diesen Schutzmechanismus noch nicht enthält. Weitere Hintergründe zu diesem Problem habe ich in meinem Blog beschrieben:

http://kofler.info/blog/208/15

26.4 GRUB 0.97

Auf vielen älteren und je nach Distribution auch bei manchen neueren Installationen werden Sie auf den Bootloader GRUB 0.97 stoßen. Aus diesem Grund fasst dieser Abschnitt die wichtigsten Grundlagen dieser an sich schon seit Jahren veralteten und nicht mehr offiziell gewarteten GRUB-Version zusammen.

Beachten Sie, dass GRUB 0.97 den Linux-Kernel weder aus Software-RAID- noch aus LVM-Volumes lesen kann. GRUB 0.97 ist auch zu vielen Dateisystemen inkompatibel (z. B. `btrfs`). Aus diesen Gründen ist es bei vielen Installationen erforderlich, eine eigene Bootpartition einzurichten, die sich außerhalb des RAID- oder LVM-Bereichs befindet und die ein von GRUB unterstütztes Dateisystem verwendet, z. B. `ext2` oder `ext3`. Viele Distributionen liefern eine gepatchte Version von GRUB 0.97 aus, die zumindest zu `ext4` kompatibel ist.

Konfiguration (Menüdatei)

menu.lst

Der Aufbau des GRUB-Menüs wird durch die GRUB-Menüdatei gesteuert, die üblicherweise den Namen `/boot/grub/menu.lst` hat. Im Vergleich zur Konfigurationsdatei von GRUB 2 ist die Syntax dieser Datei relativ einfach. Anders als bei GRUB 2 gibt es keine Scripts, um `menu.lst` automatisch zu erzeugen bzw. zu aktualisieren.

Distributionsspezifische Eigenheiten

Bei jedem Kernel-Update muss die GRUB-Konfigurationsdatei aktualisiert werden. Das stellt sicher, dass beim nächsten Neustart der neue Kernel genutzt wird. Allerdings kann es passieren, dass bei der automatischen GRUB-Neukonfiguration Ihre eigenen Änderungen überschrieben werden.

Bei alten Debian-Systemen ist für die GRUB-Neukonfiguration das Script `update-grub` zuständig. Das Script berücksichtigt speziell gekennzeichnete Kommentare beim Erstellen einer neuen Version der Konfigurationsdatei.

Unter RHEL 6 übernimmt das Kommando `grubby` ähnliche Aufgaben wie `update-grub`. Als »offizielle« GRUB-Konfigurationsdatei gilt bei RHEL 6 `/etc/grub.conf`. Dabei handelt es sich um einen Link auf die tatsächlich aktive GRUB-Konfigurationsdatei.

Partitionen

Die Bezeichnung von Partitionen in GRUB 0.97 erfolgt ganz ähnlich wie in GRUB 2. Es gibt aber zwei wesentliche Unterschiede:

- Die Nummerierung von Partitionen beginnt mit 0, nicht mit 1.
- Der Partitionsnummer darf kein Kürzel vorangestellt werden, das auf das Partitionierungsformat hinweist.

Wenn also in GRUB 2 von `(hd0,gpt3)` die Rede ist, müssen Sie dieselbe Partition in GRUB 0.97 mit `(hd0,2)` bezeichnen. Tabelle 26.4 gibt weitere Beispiele.

GRUB-0.97-Device-Name	Bedeutung
`(hd0)`	die erste Festplatte/SSD (entspricht `/dev/sda`)
`(hd1)`	die zweite Festplatte/SSD (entspricht `/dev/sdb`)
`(hd0,0)`	die erste Partition der ersten Festplatte/SSD (`/dev/sda1`)
`(hd2,7)`	die achte Partition der dritten Festplatte/SSD (`/dev/sdc8`)

Tabelle 26.4 Partitionsnamen in GRUB 0.97

devices.map

Intern verwendet GRUB die Datei `/boot/grub/devices.map` zur Zuordnung zwischen den Laufwerken und den GRUB-Device-Namen. Die Datei wird erstellt, wenn GRUB zum ersten Mal ausgeführt wird. Die Datei wird allerdings nach dem Hinzufügen neuer Laufwerke nicht automatisch aktualisiert. Gegebenenfalls können Sie die Datei einfach löschen und danach `grub` ausführen. Die Datei wird dann automatisch neu erstellt. Das kann bis zu eine Minute lang dauern.

In hartnäckigen Fällen können Sie auch versuchen, die Datei selbst zu verändern. Beachten Sie aber, dass Ihre Veränderungen mit den Informationen übereinstimmen müssen, die GRUB beim Rechnerstart vom BIOS erhält. Das Format der Datei sieht so aus:

```
# Beispiel für /boot/grub/devices.map
(hd0)   /dev/sda
(hd1)   /dev/sdb
```

Globaler Bereich in menu.lst

Grundsätzlich besteht die GRUB-Menüdatei aus einem globalen Bereich, der diverse Grundeinstellungen enthält, sowie aus mehreren Menüeinträgen, die jeweils mit der Zeile `title` beginnen. Die folgenden Zeilen zeigen ein Beispiel für den globalen Bereich von `menu.lst`:

```
# Globaler Bereich von /boot/grub/menu.lst
default 2                    # der dritte Menüeintrag gilt als Standardeintrag
timeout 30                   # 30 Sekunden warten, bevor das
                             # Standardsystem gestartet wird
color yellow/blue red/white  # Menüeinträge farbig darstellen
```

Die folgenden Absätze beschreiben die GRUB-Schlüsselwörter für den globalen Bereich von `menu.lst`:

- `default` gibt die Nummer des Menüeintrags an, der als Standardeinstellung gilt. Die Zählung beginnt mit 0! Statt einer Nummer ist auch `default saved` zulässig. In diesem Fall gilt der Menüeintrag als Standardeinstellung, der beim letzten Start verwendet wurde. Damit das funktioniert, muss allerdings jeder Menüeintrag das Schlüsselwort `savedefault` enthalten (mehr dazu folgt im nächsten Abschnitt). Wenn `menu.lst` keinen `default`-Eintrag enthält, bezeichnet der erste Menüeintrag das Standardsystem.
- `fallback` gibt die Nummer des Menüeintrags an, der genutzt wird, wenn der Standardeintrag fehlerhaft ist. Ohne `fallback`-Eintrag wechselt GRUB bei derartigen Fehlern in den interaktiven Modus.
- `timeout` gibt an, wie viele Sekunden GRUB auf eine Menüauswahl wartet. Nach dieser Zeit wird automatisch das Standardbetriebssystem gestartet. Wenn Sie möchten, dass GRUB endlos wartet, ohne ein Betriebssystem automatisch zu starten, stellen Sie der `timeout`-Zeile das Kommentarzeichen # voran.
- `hiddenmenu` bewirkt, dass GRUB kein Menü anzeigt. Nach der durch `timeout` angegebenen Zeit wird das Standardsystem gestartet. Bis zu diesem Zeitpunkt kann der Benutzer das Menü durch Esc anzeigen und dann wie üblich eine Menüauswahl treffen.
- `password -- md5 code` schützt GRUB durch ein Passwort. Die Menükommandos können ohne Passwort genutzt werden, die interaktiven Funktionen von GRUB stehen aber nur nach der Eingabe eines Passworts zur Verfügung.
- `color fg/bg menufg/menubg`steuert die Farben des GRUB-Menüs an. Dabei gibt `fg` die Vordergrundfarbe (Textfarbe) und `bg` die Hintergrundfarbe des gesamten

Bildschirms an. `menufg` und `menubg` geben entsprechend die Farben des gerade ausgewählten Menüeintrags an. Wenn Sie auf die `color`-Anweisung verzichten, erscheint das GRUB-Menü in Schwarz-Weiß.

- `splashimage` und `glxmenu`stehen nur in GRUB-Versionen mit inoffiziellen Erweiterungen zur Verfügung. Damit können Sie eine Hintergrundgrafik bzw. grafisch aufgepeppte Menüs darstellen.

Menüeinträge in menu.lst

Nach dem globalen Bereich folgen in `menu.lst` die Menüeinträge für verschiedene Betriebssysteme. Jeder Menüeintrag wird durch `title` eingeleitet. Der durch `title` angegebene Text ist der Inhalt der Menüzeile. Dabei sind nur ASCII-Zeichen erlaubt, keine internationalen Sonderzeichen.

Die weiteren Zeilen bis zur nächsten `title`-Anweisung bzw. bis zum Ende der Datei sind GRUB-Kommandos, die in dieser Reihenfolge ausgeführt werden. Wenn Sie die Kommandos interaktiv testen, müssen Sie zusätzlich noch `boot` ausführen. Dieses Kommando muss in der Menüdatei nicht angegeben werden.

Linux starten

Um Linux zu starten, müssen Sie mit `root` die Partition angeben, auf der sich der Kernel und die Initial-RAM-Disk-Datei befinden. Diese Partition wird für GRUB zur aktiven Partition. Die `kernel`- und `initrd`-Kommandos geben den genauen Ort der Dateien sowie eventuelle Kerneloptionen an.

Beachten Sie, dass für die Kerneloptionen die Linux-Nomenklatur zur Anwendung kommt. Deswegen heißt es hier `root=/dev/sdb13`. Alternative Schreibweisen sind `root=LABEL=`*`label`* sowie `root=UUID=`*`n`*, wobei Sie in diesen Fällen das Label bzw. die Identifikationsnummer der Partition angeben müssen. Beachten Sie weiters, dass die Dateinamen von `vmlinuz` und `initrd` auf Ihrem System abweichen können.

```
# Menüeintrag in /boot/grub/menu.lst
# Linux in /dev/sdb13 starten
title Linux
  root (hd1,12)
  kernel /boot/vmlinuz root=/dev/sdb13
  initrd /boot/initrd
```

Sie können auf das Kommando `root` auch verzichten. Dann müssen Sie aber bei jeder Datei die gewünschte Partition angeben:

```
# Linux in /dev/sdb13 starten
title Linux
  kernel (hd1,12)/boot/vmlinuz root=/dev/sdb13
  initrd (hd1,12)/boot/initrd
```

Wenn sich /boot nicht auf der Systempartition befindet, sondern in einer eigenen Bootpartition, müssen Sie das root-Kommando in grub entsprechend ändern. Da nun die Bootpartition als Ausgangspunkt für alle Dateien gilt, müssen die Pfadangaben ohne /boot geschrieben werden. Die folgenden Zeilen gehen davon aus, dass /dev/sda2 die /boot-Partition ist. (Entscheidend ist die Zeile root (hd0,1)!)

```
# Linux in /dev/sdb13 starten, wenn es eine eigene Bootpartition /dev/sda2 gibt
title Linux
  root (hd0,1)
  kernel /vmlinuz root=/dev/sdb13
  initrd /initrd
```

Linux-Kerneloptionen ändern

Beim Start des Kernels werden diverse Bootoptionen übergeben. Diese Optionen geben z. B. den Ort der Systempartition an oder steuern, wie die Meldungen des Init-Systems dargestellt werden. In menu.lst werden diese Optionen einfach am Ende der kernel-Zeile angegeben:

```
# Linux in /dev/sdb13 starten (mit zusätzlichen Kerneloptionen)
title Linux
  root (hd1,12)
  kernel /boot/vmlinuz root=/dev/sdb13 vga=normal
  initrd /boot/initrd
```

Windows starten

Wenn Sie Windows starten möchten, müssen Sie die aktive Partition mit rootnoverify statt mit root angeben. Das Kommando chainloader +1 bewirkt, dass der erste Sektor dieser Partition gelesen und ausgeführt wird. Damit wird der Windows-Bootloader gestartet, der sich um den eigentlichen Start von Windows kümmert.

```
# Windows in /dev/sda1 starten
title Windows
  rootnoverify (hd0,0)
  chainloader +1
```

Der Windows-Start gelingt nur, wenn sich Windows auf der ersten Festplatte befindet. Wenn das nicht der Fall ist, können Sie die Festplatten durch die folgenden Zeilen virtuell vertauschen:

```
# Windows in /dev/sdb1 starten
title Windows
  rootnoverify (hd1,0)
  map (hd0) (hd1)
  map (hd1) (hd0)
  chainloader +1
```

Einen anderen Bootloader starten

Bootloader wie GRUB werden üblicherweise in den MBR der ersten Festplatte installiert. Es besteht aber auch die Möglichkeit, sie in den Bootsektor einer beliebigen Partition zu installieren. Mit dem zentralen GRUB, der sich im MBR befindet, starten Sie indirekt den in eine Partition installierten GRUB. Diese Vorgehensweise kann sinnvoll sein, um mehrere Linux-Distributionen parallel auf einer Festplatte zu installieren.

```
# Bootloader im Bootsektor von /dev/sda7 starten
title Bootloader in /dev/sda7
  rootnoverify (hd0,6)
  chainloader +1
```

Letztes Betriebssystem merken

Wenn `menu.lst` viele Menüeinträge enthält, ist es oft praktisch, wenn sich GRUB den zuletzt ausgewählten Eintrag merkt. Dazu geben Sie im globalen Bereich von `menu.lst` die Option `default saved` an und ergänzen alle Menüeinträge um das Schlüsselwort `savedefault`:

```
# Linux in /dev/sdb13 starten, diese Auswahl merken
title Linux
  root (hd1,12)
  kernel /boot/vmlinuz root=/dev/sdb13
  initrd /boot/initrd
  savedefault
```

Achtung

Verwenden Sie `savedefault` auf keinen Fall bei Rechnern, auf denen das BIOS zwei oder mehr Festplatten zu einem RAID-Verbund zusammenschließt (BIOS-Software-RAID)! Sie riskieren Datenverluste bzw. gefährden die Synchronität!

GRUB-Konfiguration testen

Wenn Sie rasch und ohne Neustart testen möchten, ob eine geänderte GRUB-Menüdatei frei von syntaktischen Fehlern ist, starten Sie zuerst `grub` und führen dort das folgende Kommando aus:

```
root#  grub
grub>  configfile (hd1,12)/boot/grub/menu.lst
```

Statt `(hd1,12)` müssen Sie den GRUB-Namen für die Festplattenpartition angeben, in der sich die GRUB-Menüdatei befindet. Wenn alles klappt, zeigt GRUB das Menü an. Sie können allerdings kein Betriebssystem tatsächlich starten, weil Linux ja schon läuft.

GRUB-Aktualisierung

update-grub (Debian 5)

Debian 5 sieht zur Aktualisierung der GRUB-Konfiguration das Shell-Script `update-grub` vor. Es durchsucht `/boot` nach `vmlinuz-*`-Dateien und fügt für jede derartige Kerneldatei einen entsprechenden GRUB-Menüeintrag ein. Dabei werden auch zur jeweiligen Kernelversion passende `initrd-*`-Dateien berücksichtigt. `update-grub` wird automatisch nach jedem Kernel-Update ausgeführt.

`update-grub` berücksichtigt einige Einstellungen, die in `menu.lst` in der folgenden Form als Kommentare angegeben sind. Die einzelnen Variablen sind in `man update-grub` ausführlich beschrieben. Am wichtigsten ist die Variable `kopt`, die angibt, welche Optionen an den Kernel übergeben werden. Wenn Sie diesbezüglich Änderungen in `menu.lst` durchführen möchten, verändern Sie nicht direkt die Menüeinträge in `menu.lst`, sondern die `kopt`-Variable. Anschließend führen Sie `update-grub` aus.

```
# /etc/boot/menu.lst
...
# Einstellungen für update-grub
#
# kopt=root=/dev/sda13 ro          (Kerneloptionen)
# groot=(hd0,12)                   (Ort, an dem GRUB installiert ist)
# defoptions=                      (Kerneloptionen nur für den Default-Kernel)
# xenhopt=                         (Xen-Optionen)
# xenkopt=console=tty0             (Kerneloptionen für Xen-Kernel)
# altoptions=single                (Kerneloptionen für den alternativen Kernel)
# howmany=all                      (Maximalanzahl der Kerneleinträge)
# memtest86=true                   (Memtest-Eintrag hinzufügen)
# updatedefaultentry=false         (Default-Schlüsselwort in  menu.lst verändern)
...
```

grubby (RHEL 6)

Unter RHEL 6 hilft das Script `grubby` bei der Aktualisierung der GRUB-Konfiguration nach einem Kernel-Update. Das Script ist in einer `man`-Seite gut dokumentiert. Dort befinden sich allerdings auch der Hinweis, dass `grubby` ausschließlich für den internen Aufruf durch Red-Hat-spezifische Update-Scripts gedacht ist, nicht aber für den manuellen Einsatz.

GRUB 0.97 und EFI

RHEL 6 setzt auch bei EFI-Installationen auf GRUB 0.97. Offiziell unterstützt GRUB 0.97 EFI eigentlich gar nicht, Red Hat liefert in RHEL 6 aber eine gepatchte Version aus. Im Vergleich zum unmäßig komplexen GRUB 2 liegt der Charme der EFI-Version von GRUB 0.97 gerade in ihrer Einfachheit.

Der Bootloader befindet sich in der unveränderlichen Datei `grub.efi`, die auch bei BIOS-Rechnern in das Verzeichnis `/boot/efi/EFI/redhat` installiert wird. Die Datei ist

einfach Bestandteil des `grub`-Pakets. Ob `/boot/efi` eine eigene Partition ist oder nicht, wird nicht überprüft. Wenn Sie eine vorhandene BIOS-Installation später in eine EFI-Installation umbauen möchten, müssen Sie aber unbedingt sicherstellen, dass `/boot/efi` der `mount`-Punkt für die EFI-Partition ist.

`grub.efi` erwartet die Konfigurationsdatei im selben Verzeichnis. Bei EFI-Installationen ist `/etc/grub.conf` daher ein Link auf `/boot/efi/EFI/redhat/grub.conf`. Die Syntax von `grub.conf` ist dieselbe wie bei der BIOS-Version von GRUB 0.97. Bei EFI-Installationen wird auch `devices.map` in diesem Verzeichnis gespeichert.

GRUB-Installation in einem Live-System reparieren

Nach dem Start des Live-Systems starten Sie eine Konsole und führen darin `su -l` oder `sudo -s` aus, um `root`-Rechte zu erlangen. Als Nächstes müssen Sie die Partition suchen, in der sich Ihre Linux-Distribution und insbesondere das Verzeichnis `/boot` befinden.

```
root#  mkdir /test
root#  mount /dev/sda3 /test
```

Die gesuchte Partition erkennen Sie daran, dass es ein `/boot`-Verzeichnis mit Linux-Kerneldateien (`vmlinuzxxx`), dem Unterverzeichnis `/boot/grub` und der GRUB-Menüdatei `/boot/grub/menu.lst` gibt. Falls Sie eine eigene Bootpartition besitzen, enthält diese Partition kein `boot`-Verzeichnis. `vmlinuzxxx` und das Unterverzeichnis `grub` befindet sich in diesem Fall direkt im Wurzelverzeichnis der Partition.

Nach diesen Vorbereitungsarbeiten geht es nun darum, GRUB so in den Bootsektor der Festplatte zu installieren, dass beim Rechnerstart davon ausgehend alle weiteren GRUB-Dateien in `/dev/sda3` gelesen werden. Dabei ist `(hd0,2)` die für GRUB übliche Bezeichnung der Partition `/dev/sda3` und `(hd0)` die Bezeichnung für die gesamte erste Festplatte, in deren Bootsektor GRUB geschrieben werden soll.

```
root#  grub
grub>  root (hd0,2)     (Ort der System- bzw. Bootpartition)
grub>  setup (hd0)      (Ziel der GRUB-Installation: der MBR der ersten Festplatte)
grub>  quit
```

Kapitel 27
Das Init-System

Dieses Kapitel beschreibt die Vorgänge, die vom Kernelstart bis hin zum Login stattfinden. Der Kernel startet als ersten Prozess das Programm `/sbin/init`. Es kümmert sich um die Basiskonfiguration des Systems, um das Einbinden von Dateisystemen und um den Start zahlloser Netzwerkdienste und -dämonen.

Wie so oft in der Linux-Welt gibt es nicht *ein* Init-System, sondern mehrere. Dieses Kapitel stellt die drei wichtigsten vor:

- **Beim traditionellen Init-V-System** kümmern sich eine Menge durch Links verbundener Scripts um die Initialisierung des Rechners. Das Konzept und sein Name stammen vom Unix-Betriebssystem System V. Das Init-V-System kommt in immer weniger Distributionen standardmäßig zum Einsatz; bei den in diesem Buch beschriebenen Distributionen ist das nur noch in Debian der Fall. Bei älteren Distributionen werden Sie aber häufiger auf das Init-V-System stoßen. Außerdem sind alle modernen Init-Systeme weiterhin Init-V-kompatibel. Grundkenntnisse des Init-V-Systems sind daher auf jeden Fall zweckmäßig.
- **Upstart** ist ein ereignisorientiertes Init-System. Es kommt in Ubuntu seit Version 6.10 zum Einsatz, außerdem in Fedora 9 bis 13 sowie in RHEL 6.
- **Systemd** ist das zurzeit modernste Init-System, das erstmalig in Fedora 15 zum Einsatz kam. openSUSE ist mit Version 12.1 ebenfalls auf Systemd umgestiegen.

Tabelle 27.1 fasst zusammen, welches Init-System in welcher Distribution zum Einsatz kommt. Die Spalte RHEL gilt für Red Hat Enterprise Linux sowie für alle dazu kompatiblen Distributionen, also z. B. CentOS und Scientific Linux.

Init-System	Debian	Fedora	openSUSE	RHEL	Ubuntu
Init-V	bis 7	bis 8	bis 11.4	bis 5	bis 6.04
Upstart		9 bis 13		6	ab 6.10
Systemd		ab 14	ab 12.1	ab 7	

Tabelle 27.1 Init-Systeme je nach Distribution

Das Kapitel endet mit einer Vorstellung des *Internet Service Daemons*. Dieses Programm überwacht Netzwerkports. Wenn dort Anfragen eintreffen, startet es ein Programm, das geeignet ist, um darauf zu reagieren.

27.1 Das Init-V-System

Das traditionelle Init-V-System wird bei manchen aktuellen und vielen älteren Distributionen dazu verwendet, die Systeminitialisierung durchzuführen und Netzwerkdienste zu starten. Wie das Programm `/sbin/init` im Einzelnen ausgeführt wird, hängt von der jeweiligen Distribution ab: In welchen Verzeichnissen befinden sich welche Init-Dateien, mit welchen Nummern oder Buchstaben sind die sogenannten Runlevel bezeichnet, welche Konfigurationsdateien werden berücksichtigt etc.?

Obwohl aktuelle Fedora-, openSUSE- und Ubuntu-Versionen Upstart oder Systemd verwenden, ist in diesem Abschnitt mehrfach auch von diesen Distributionen die Rede. Das liegt daran, dass Upstart und Systemd Init-V-kompatibel ist und daher manche Init-V-Prinzipien weiterhin gültig bleiben. Auch wenn Sie ein Script für einen eigenen Systemdienst entwickeln möchten, bietet sich das Init-V-System als kleinster gemeinsamer Nenner an. Ein Beispiel für ein derartiges Script folgt in Abschnitt 27.4.

Ablauf

Die folgenden Punkte geben einen kurzen Überblick über einen normalen Linux-Systemstart durch das Init-V-System:

- GRUB lädt und startet den Kernel.
- Der Kernel startet das Programm `/sbin/init`.
- `init` wertet die Konfigurationsdatei `/etc/inittab` aus.
- `init` führt ein Script zur Systeminitialisierung aus.
- `init` führt das Script `/etc/rc.d/rc` oder `/etc/init.d/rc` aus. Das Script `rc` variiert von Distribution zu Distribution erheblich. Es ist für den Start der Script-Dateien verantwortlich, die sich im Verzeichnis `/etc/rc`*n*`.d` oder `/etc/init.d/rc`*n*`.d` befinden. (*n* ist der Runlevel – siehe unten.)
- Die Script-Dateien aus `/etc/rc`*n*`.d` bzw. `/etc/init.d/rc`*n*`.d` starten verschiedene Systemdienste, insbesondere für die Netzwerkfunktionen.

Runlevel

Der Kernel startet `/sbin/init` als erstes Programm. Dabei werden alle Bootoptionen, die der Kernel nicht kennt und daher nicht selbst verarbeiten kann, an das Init-System übergeben. Auf diese Weise kann beispielsweise erreicht werden, dass Linux im Single-User-Modus gestartet wird.

`init` ist also der erste laufende Prozess. Alle weiteren Prozesse werden entweder direkt von `init` oder indirekt durch Subprozesse von `init` gestartet. Führen Sie in einem Terminal `pstree` aus, dann erkennen Sie sofort die dominierende Rolle von `init`! Beim Herunterfahren des Rechners ist `init` der letzte noch laufende Prozess, der sich um das korrekte Beenden aller anderen Prozesse kümmert.

Runlevel für Fedora, Red Hat, SUSE

Für das Verständnis der System-V-Mechanismen ist der Begriff des Runlevels von zentraler Bedeutung. Der Runlevel beschreibt verschiedene Zustände, die das Betriebssystem einnehmen kann. Leider ist die Runlevel-Nummerierung je nach Distribution uneinheitlich. Die jeweilige Bedeutung der Runlevel ist in der Regel in `/etc/inittab` dokumentiert. Für die meisten Distributionen (aber nicht für Debian und Ubuntu!) gelten die folgenden Runlevel-Beschreibungen:

- Runlevel 0: Shutdown mit Halt
- Runlevel 1 und S: Single-User
- Runlevel 2: Multi-User ohne Netzwerk bzw. ohne NFS
- Runlevel 3: Multi-User mit Netzwerk, aber ohne automatischen X-Start
- Runlevel 4: üblicherweise unbenutzt
- Runlevel 5: Multi-User mit Netzwerk und X-Start. Das ist zumeist der Standard-Runlevel.
- Runlevel 6: Shutdown mit Reboot

Auf Systemen, die zwischen den Runleveln 1 und S differenzieren, werden die Runlevel-1-Scripts ausgeführt, um von einem gewöhnlichen Runlevel (2, 3 oder 5) in den Single-User-Runlevel zu wechseln. Die Runlevel-S-Scripts kommen dagegen nur zur Anwendung, wenn der Single-User-Runlevel direkt nach dem Booten aktiviert werden soll.

Runlevel für Debian und Ubuntu

Bei von Debian abgeleiteten Distributionen sind die Runlevel 2 bis 5 gleichwertig und starten jeweils ein Multiuser-System mit Netzwerk und X. Als Standard-Runlevel gilt 2. Der Runlevel S ist eigentlich kein eigener Level, sondern dient zur Initialisierung des Rechners unmittelbar nach dem Start, also noch bevor einer der anderen Level aktiviert wird. Die Netzwerkfunktionen werden bei Debian bzw. Ubuntu bereits während der Systeminitialisierung aktiviert und stehen daher in allen Runleveln zur Verfügung.

- Runlevel S: Initialisierung des Rechners unmittelbar nach dem Start
- Runlevel 0: Shutdown mit Halt
- Runlevel 1: Single-User mit Netzwerk
- Runlevel 2–5: Multi-User mit Netzwerk und automatischem X-Start
- Runlevel 6: Shutdown mit Reboot

Runlevel wechseln

`root` kann den Runlevel im laufenden Betrieb durch das Kommando `init x` verändern. `x` ist dabei eine Runlevel-Ziffer oder ein Runlevel-Buchstabe. Beispielsweise ist es für manche Wartungsarbeiten sinnvoll, in den Single-User-Modus zu wechseln. Auch `shutdown`, `halt`, `reboot` bzw. Strg+Alt+Entf in einer Textkonsole ändern den Runlevel und führen auf diese Weise zu einem Rechnerneustart.

Standard-Runlevel

Beim klassischen Init-V-System wird der Standard-Runlevel durch die `initdefault`-Zeile in `/etc/inittab` bestimmt. Bei den meisten aktuellen Distributionen gilt 5 als Standard-Runlevel, bei Debian ist es 2.

Bei Ubuntu wird der Standard-Runlevel in `/etc/init/rc-sysinit.conf` festgelegt. Diese Datei ist Teil des Upstart-Systems.

Bei Distributionen, die Systemd verwenden, wird der Standard-Runlevel durch `/etc/systemd/default.target` festgelegt. Dieser Link zeigt auf eine der vordefinierten Target-Dateien im Verzeichnis `/lib/systemd/system/`.

Inittab

Beim Systemstart wird `init` durch die Datei `/etc/inittab` gesteuert. Für die Syntax der `inittab`-Einträge gilt folgendes Schema:

```
id-code:runlevel:action:command
```

`id-code` besteht aus zwei Zeichen, die die Zeile eindeutig identifizieren. Der `runlevel` gibt an, für welchen Runlevel der Eintrag gilt. `action` enthält eine Anweisung für `init`. `command` gibt an, welches Linux-Kommando oder Programm gestartet werden soll. Tabelle 27.2 zählt die wichtigsten `action`-Schlüsselwörter auf. Eine vollständige Beschreibung erhalten Sie mit `man inittab`.

Das folgende Listing gibt die leicht gekürzte `inittab`-Datei von Debian wieder. Als Standard-Runlevel gilt 2. Bei einem normalen Systemstart führt `init` die Script-Dateien `rcS` und das Kommando `rc 2` aus. Schließlich wird für die Textkonsolen 1 bis 6 das Programm `mingetty` gestartet, das einen Login ermöglicht. (Wenn Sie mehr Textkonsolen haben möchten, ist hier der richtige Ort für Veränderungen. Beachten Sie aber, dass die Konsole 7 bei den meisten Distributionen für X reserviert ist.)

Schlüsselwort	Bedeutung
ctrlaltdel	gibt an, wie init auf Strg+Alt+Entf reagieren soll.
initdefault	definiert den Standard-Runlevel für init (siehe oben).
once	init startet das angegebene Kommando beim Runlevel-Wechsel.
respawn	init startet das Kommando nach seinem Ende wieder neu.
sysinit	init startet das Kommando einmal während des Bootprozesses.
wait	init wartet auf das Ende des nachfolgenden Kommandos.
bootwait	init startet den Prozess während des Bootprozesses und wartet auf das Ende des nachfolgenden Kommandos.

Tabelle 27.2 inittab-Schlüsselwörter (id-codes)

```
# Datei /etc/inittab bei Debian 6
# Standard-Runlevel
id:2:initdefault:

# Systemkonfiguration und -initialisierung unmittelbar nach dem Rechnerstart
si::sysinit:/etc/init.d/rcS

# Verhalten im Single-User-Modus (Kernelparameter su)
~~:S:wait:/sbin/sulogin

# Start der jeweiligen Runlevel
l0:0:wait:/etc/init.d/rc 0
l1:1:wait:/etc/init.d/rc 1
l2:2:wait:/etc/init.d/rc 2
l3:3:wait:/etc/init.d/rc 3
l4:4:wait:/etc/init.d/rc 4
l5:5:wait:/etc/init.d/rc 5
l6:6:wait:/etc/init.d/rc 6
# Die folgende Zeile sollte nie erreicht werden, sie ist nur für Notfälle da.
z6:6:respawn:/sbin/sulogin

# Reaktion auf Strg+Alt+Entf in einer Textkonsole
ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now

# Reaktion auf einen Stromausfall, der von einer unterbrechungsfreien
# Stromversorgung gemeldet wird
pf::powerwait:/etc/init.d/powerfail start
pn::powerfailnow:/etc/init.d/powerfail now
po::powerokwait:/etc/init.d/powerfail stop

# gettys (Terminalemulatoren) für die Textkonsolen starten
1:2345:respawn:/sbin/getty 38400 tty1
```

```
2:23:respawn:/sbin/getty 38400 tty2
3:23:respawn:/sbin/getty 38400 tty3
4:23:respawn:/sbin/getty 38400 tty4
5:23:respawn:/sbin/getty 38400 tty5
6:23:respawn:/sbin/getty 38400 tty6
```

Verhalten bei Strg-Alt-Entf ändern

Die meisten Distributionen sind so vorkonfiguriert, dass die Tastenkombination Strg+Alt+Entf in Textkonsolen zu einem Neustart des Rechners führt. Wenn Sie möchten, dass der Rechner stattdessen ausgeschaltet wird, geben Sie beim `shutdown`-Kommando in der `ca:`-Zeile die Option `-h` statt `-r` an. Wenn Sie diese Tastenkombination ganz deaktivieren möchten, setzen Sie vor die `ca:`-Zeile das Kommentarzeichen #. Beachten Sie aber, dass Änderungen in `inittab` nur bei solchen Distributionen zweckmäßig sind, die das Init-V-System verwenden!

Systeminitialisierung

Noch bevor die im Weiteren beschriebenen rc-Dateien die runlevel-spezifischen Dienste starten oder stoppen, wird unmittelbar nach dem Rechnerstart eine Systeminitialisierung durchgeführt (`si:`-Zeile in `inittab`). Der Name des Scripts hängt von der Distribution ab: Bei Debian ist es `/etc/init.d/rcS`, bei RHEL 5 `/etc/rc.d/rc.sysinit`, bei alten SUSE-Versionen `/etc/init.d/boot`. Bei Debian 6 ist `rcS` ein winziges Script, das seinerseits alle Script-Dateien `/etc/rcS.d/S*` ausführt.

Während der Systeminitialisierung werden die Dinge erledigt, die während des Rechnerstarts nur einmal getan werden müssen:

- diverse Systemvariablen initialisieren (inklusive Host- und Domainname)
- `/proc`-Dateisystem aktivieren
- Datum und Uhrzeit einstellen
- Tastaturlayout für die Textkonsole einstellen
- `udev`-System starten
- eventuell RAID und LVM aktivieren
- Dateisysteme überprüfen
- Root-Partition im Read-Write-Modus neu einbinden
- Dateisystem der weiteren Partition überprüfen, Partitionen einbinden
- Netzwerkgrundfunktionen teilweise oder ganz initialisieren

Init-V-Scripts für die Aktivierung der Runlevel

Nach der Systeminitialisierung wird der Standard-Runlevel laut `/etc/inittab` aktiviert. Für alle Details der Runlevel gibt es eigene Script-Dateien. Diese befinden sich je nach Distribution im Verzeichnis `/etc/init.d` oder in `/etc/rc.d/init.d`. Um eine höhere Kompatibilität zwischen den Distributionen zu erreichen, stellen meist Links sicher, dass beide Pfade gültig sind.

Zum Start der Init-V-Scripts führt `init` das Script `/etc/rc.d/rc` bzw. `/etc/init.d/rc` aus. An `rc` wird der gewünschte Runlevel *n* übergeben. `rc` führt zuerst einige Initialisierungsarbeiten durch. Dann werden alle `rcn.d/K*`-Script-Dateien zum Beenden laufender Prozesse ausgeführt. Schließlich werden alle `rcn.d/S*`-Script-Dateien zum Starten der neuen Prozesse für den jeweiligen Runlevel ausgeführt.

Der Vorteil dieses Systems besteht darin, dass es sehr einfach ist, neue Systemprozesse in den Init-V-Prozess einzubauen: Es müssen lediglich Links für die rc-Start- und -Stopp-Scripts in die richtigen Verzeichnisse eingerichtet werden – und genau das geschieht bei der Installation eines Pakets mit einem zusätzlichen Dämon. Die folgende Aufstellung für Debian zeigt, welche Script-Dateien für einige ausgewählte Runlevel ausgeführt werden:

```
user$  cd /etc/
user$  ls rcS.d/ rc2.d/ rc6.d/
rcS.d/:      (Systeminitialisierung)
S01hostname.sh              S07mtab.sh                 S14nfs-common
S01mountkernfs.sh           S08checkfs.sh              S15mountnfs.sh
S02udev                     S09mountall.sh             S16mountnfs-bootclean.sh
S03keyboard-setup           S10mountall-bootclean.sh   S17kbd
S04mountdevsubfs.sh         S11pppd-dns                S18console-setup
S05hdparm                   S11procps                  S19alsa-utils
S05hwclock.sh               S11udev-mtab               S19bootmisc.sh
S06checkroot.sh             S11urandom                 S19x11-common
S07checkroot-bootclean.sh   S12networking
S07kmod                     S13rpcbind

rc2.d/:      (Standard-Runlevel)
S01motd                     S17atd                     S18network-manager
S01nvidia-kernel            S17cron                    S19cups
S13rpcbind                  S17dbus                    S19gdm3
S14nfs-common               S17mysql                   S19pulseaudio
S16binfmt-support           S17speech-dispatcher       S19saned
S16rsyslog                  S17ssh                     S20bootlogs
S16sudo                     S18avahi-daemon            S21minissdpd
S17acpid                    S18bluetooth               S21rc.local
S17anacron                  S18exim4                   S21rmnologin
```

```
rc6.d/:      (Shutdown)
K01alsa-utils              K01speech-dispatcher       K05umountnfs.sh
K01atd                     K01unattended-upgrades     K06nfs-common
K01bluetooth               K01urandom                 K06rpcbind
K01exim4                   K02avahi-daemon            K07hwclock.sh
K01gdm3                    K02mysql                   K07networking
K01minissdpd               K02network-manager         K08umountfs
K01pulseaudio              K03sendsigs                K09umountroot
K01saned                   K04rsyslog                 K10reboot
```

In den `rcn.d`-Verzeichnissen befinden sich nicht unmittelbar die Script-Dateien, sondern lediglich Links darauf. Die eigentlichen Script-Dateien sind im Verzeichnis `/etc/rc.d/init.d` oder `/etc/init.d` gespeichert:

```
root#  cd /etc
root#  ls -l rc2.d/S19cups
...   rc2.d/S19cups -> ../init.d/cups
```

Nomenklatur

Die Namen der Links sind keineswegs so willkürlich, wie sie aussehen: Der Anfangsbuchstabe gibt an, ob es sich um ein Start- oder ein Kill-Script handelt. Die S- und K-Links verweisen auf dieselbe Datei; allerdings wird das Script je nach Anfangsbuchstabe von `rc` mit dem Parameter `start` oder `stop` ausgeführt.

Die nachfolgende Nummer bestimmt die Reihenfolge, in der die Script-Dateien ausgeführt werden. Beispielsweise setzen die meisten Netzwerkdämonen voraus, dass schon eine Netzwerkverbindung besteht, und müssen daher nach dem Script `network` gestartet werden. Eine Kurzbeschreibung vieler Dämonen, die durch `rc`-Script-Dateien gestartet werden, finden Sie in Abschnitt 16.5.

Dämonen manuell starten/stoppen

Die Runlevel-Script-Dateien können auch manuell ausgeführt werden. Beispielsweise stoppt das folgende Kommando den Windows-kompatiblen Datei-Server Samba:

```
root#  /etc/init.d/samba stop
```

Bei vielen Distributionen sind zum Starten/Stoppen von Dämonen eigene Kommandos vorgesehen, die weniger Tippaufwand bereiten. Am weitesten verbreitet ist das Kommando `service`. Es steht in allen in diesem Buch behandelten Distributionen unabhängig vom eingesetzten Init-System zur Verfügung, unter Debian allerdings erst ab Version 7.

```
root#  service samba start
```

Init-V-Script-Parameter

An die meisten Scripts kann einer der folgenden Parameter übergeben werden:

- `start` startet die betreffende Funktion.
- `stop` beendet die Funktion.

- `status` zeigt eine kurze Information an, ob die Funktion aktiv ist oder nicht.
- `reload` bietet sich dann an, wenn geänderte Konfigurationsdateien neu eingelesen werden sollen, ohne den Dämon dabei ganz zu stoppen. Allerdings sehen nicht alle Dienste diese Möglichkeit vor; sie müssen gegebenenfalls neu gestartet werden.
- `restart` bewirkt, dass der Dämon vollkommen gestoppt und anschließend neu gestartet wird. Eventuell vorhandene Verbindungen zu Clients gehen dabei verloren, bei Datenbank-Servern auch der Cache-Inhalt.

Verwaltung der Runlevel-Links

Dämonen automatisch starten/stoppen

Viele Runlevel-Script-Dateien werden automatisch beim Rechnerstart bzw. bei einem Runlevel-Wechsel durch das `rc`-Script gestartet bzw. gestoppt – je nachdem, ob es im `rc`*n*`.d`-Verzeichnis einen S- oder K-Link auf das Init-V-Script gibt. Wenn Sie also möchten, dass eine bestimmte Funktion in Zukunft automatisch aktiviert werden soll, müssen Sie derartige Links einrichten. Entsprechend müssen Sie die Links wieder entfernen, wenn Sie in Zukunft einen automatischen Start verhindern möchten.

Die folgenden Kommandos zeigen, welche Links Sie unter Debian einrichten müssen, um das Programm `samba` in Zukunft bei den Runleveln 2 bis 5 automatisch zu starten:

```
root#  cd /etc/
root#  ln init.d/samba rc0.d/K01samba
root#  ln init.d/samba rc1.d/K01samba
root#  ln init.d/samba rc2.d/S20samba
root#  ln init.d/samba rc3.d/S20samba
root#  ln init.d/samba rc4.d/S20samba
root#  ln init.d/samba rc5.d/S20samba
root#  ln init.d/samba rc6.d/K01samba
```

Das Entfernen der Links verursacht weniger Tippaufwand:

```
root#  rm rc?.d/*samba
```

insserv (Debian 7, SUSE)

In der Praxis werden Sie die obigen `ln`- bzw. `rm`-Kommandos selten manuell eintippen: Die meisten Distributionen stellen nämlich Kommandos zur Verfügung, die Ihnen diese Arbeit abnehmen, z. B. `insserv` ab Debian 6 sowie bei SUSE, `chkconfig` bei RHEL 6 und `update-rc.d` bei älteren Debian-Versionen sowie bei Ubuntu.

```
root#  insserv samba      (Start- und Stopp-Links einrichten)
root#  insserv -r samba   (Start- und Stopp-Links entfernen)
```

update-rc.d (Debian, Ubuntu)

Das Kommando `update-rc.d` ist eigentlich für die Installations-Scripts von Paketen gedacht. Es hilft bei der Installation bzw. Deinstallation von Paketen, die Runlevel-Links für das Init-V-Script des Pakets einzurichten bzw. wieder zu entfernen.

In älteren Debian-Versionen sowie unter Ubuntu können Sie das Kommando auch direkt nutzen. Beachten Sie aber, dass `update-rc.d` keine Änderungen an bereits vorhandenen Links durchführt! Sie müssen vorhandene Links zuerst löschen.

`update-rc.d` *`name`* `remove` entfernt alle Start- und Stopp-Links für den angegebenen Dienst. Das Kommando funktioniert allerdings nur, wenn `/etc/init.d/`*`name`* vorher deinstalliert wurde. Ist diese Voraussetzung nicht erfüllt, müssen Sie die Option `-f` (*force*) angeben.

`update-rc.d` *`name`* `defaults` richtet in allen Runleveln Links zum Starten (Runlevel 2–5) und Stoppen des Diensts (Runlevel 0, 1 und 6) ein. Die Link-Namen beginnen mit der durchlaufenden Zahl 30. Wenn das Script früher oder später im Start- bzw. Stopp-Prozess ausgeführt werden soll, müssen Sie die gewünschten Start- und Stopp-Werte selbst angeben – im folgenden Beispiel 30 für den Start und 1 für Stopp:

```
root#  update-rc.d gdm defaults 30 1
   /etc/rc0.d/K01gdm -> ../init.d/gdm
   /etc/rc1.d/K01gdm -> ../init.d/gdm
   /etc/rc6.d/K01gdm -> ../init.d/gdm
   /etc/rc2.d/S30gdm -> ../init.d/gdm
   /etc/rc3.d/S30gdm -> ../init.d/gdm
   /etc/rc4.d/S30gdm -> ../init.d/gdm
   /etc/rc5.d/S30gdm -> ../init.d/gdm
```

Um die Links wirklich für jeden Runlevel individuell einzurichten, übergeben Sie an `update-rc.d` Argumente in der Form *`name`* `start|stop` *`nn runlevel`*. Dabei ist *`nn`* die Zahl am Beginn des Runlevel-Links. Sie dürfen mehrere Runlevel und mehrere Argumentgruppen angeben. Allerdings muss jede Argumentgruppe mit einem Punkt abgeschlossen werden. Das folgende Kommando hat dieselbe Wirkung wie `gdm defaults 30 1`:

```
root#  update-rc.d gdm start 30 2 3 4 5 . stop 1 0 1 6 .
```

chkconfig (RHEL)

Unter RHEL hilft das Kommando `chkconfig` bei der Verwaltung der Links auf Init-V-Scripts. Mit der Option `--list` gibt das Kommando eine Übersicht über alle Scripts und zeigt an, in welchem Runlevel sie gestartet werden. Sofern `xinetd` installiert ist, werden auch dessen Dienste aufgelistet.

```
root#  chkconfig --list
NetworkManager  0:Aus   1:Aus   2:Ein   3:Ein   4:Ein   5:Ein   6:Aus
NetworkManagerD 0:Aus   1:Aus   2:Aus   3:Aus   4:Aus   5:Aus   6:Aus
acpid           0:Aus   1:Aus   2:Aus   3:Ein   4:Ein   5:Ein   6:Aus
...
```

Mit `--del` kann der Start eines Runlevel-Scripts generell verhindert werden:

```
root#  chkconfig --del samba
```

`chkconfig --add` fügt in allen vorgesehenen Runleveln Start- und Stopp-Links für einen neuen Service ein. Die Option `--add` funktioniert allerdings nur, wenn die Init-V-Script-Datei Informationen darüber enthält, in welchem Runlevel das Script standardmäßig gestartet werden soll.

Bei vielen Scripts fehlen diese Informationen. Damit ein derartiges Script in Zukunft automatisch gestartet wird, müssen Sie `chkconfig --level n name on/off` verwenden. Im folgenden Beispiel soll der Webserver in den Runlevel 3 und 5 gestartet werden. `chkconfig --list` zeigt das Ergebnis an:

```
root#  chkconfig --level 35 httpd on
root#  chkconfig --list httpd
httpd    0:Aus   1:Aus   2:Aus   3:Ein   4:Aus   5:Ein   6:Aus
```

Statusmeldungen während des Bootprozesses

Plymouth

Die meisten Distributionen sind so konfiguriert, dass während des Bootprozesses ein Hintergrundbild und eventuell ein Fortschrittsbalken oder eine andere grafische Fortschrittsanzeige zu sehen ist. Unabhängig vom Init-System ist dafür oft das Programm Plymouth verantwortlich.

Bootmeldungen lesen

Wenn es beim Bootprozess Probleme gibt, ist es oft hilfreich, die Bootmeldungen mitzuverfolgen. In der Regel müssen Sie dazu nur Esc drücken. Alternativ erreichen Sie die Darstellung der Bootmeldungen auch, wenn Sie in der GRUB-Konfiguration die Bootoption `quiet` entfernen.

Optimierung des Init-V-Prozesses

Der Init-V-Prozess ist sehr aufwendig: Unzählige Scripts und Programme müssen gestartet werden; für jedes einzelne Script muss ein Script-Interpreter ausgeführt werden. All dies waren Gründe für die Entwicklung von Upstart und Systemd. Aber selbst bei Distributionen mit Init-V-System ist es gelungen, diese Bootzeit stark zu reduzieren. Dieser Abschnitt fasst gängige Methoden zur Geschwindigkeitsoptimierung zusammen.

- **Dateien im Voraus laden:** Bei jedem Startprozess werden dieselben Dateien in derselben Reihenfolge von der Festplatte gelesen. Um diesen Prozess zu beschleunigen, starten einige Distributionen am Beginn des Init-Prozesses ein

Hintergrundprogramm, das alle Dateien liest, die in einer vorgegebenen Liste angegeben sind. Wenn eine Datei dann wenig später tatsächlich benötigt wird, befindet sie sich schon im Cache.

Diese Idee kommt losgelöst vom Init-V-System auch bei Upstart und Systemd zum Einsatz. Unter RHEL ist dafür das Programm `readahead` zuständig, unter Ubuntu `ureadahead`. Bei Fedora und openSUSE enthält die Systemd-Konfiguration `readahead`-Dienste. Nur Debian verzichtet auf diese Art der Optimierung, was angesichts der zunehmenden Verbreitung von SSDs ein pragmatischer Ansatz ist.

- **Parallelisierung:** Der Init-V-Prozess erfolgt üblicherweise sequenziell, d. h., es wird ein Init-V-Script nach dem anderen abgearbeitet. Das hat gute Gründe: Es ist z. B. unmöglich, ein NFS-Verzeichnis in das Dateisystem einzubinden, bevor die Netzwerkfunktionen initialisiert wurden. Allerdings sind nicht alle Init-V-Scripts voneinander abhängig. Aus diesen Gründen versuchen manche Distributionen, Init-V-Scripts möglichst parallel auszuführen.
- **Grafiksystem X früher starten:** In der Vergangenheit war es üblich, X erst zum Ende des Init-V-Prozesses zu starten. Mittlerweile wird X schon gestartet, sobald die Grundinitialisierung der Hardware abgeschlossen ist. Der frühe X-Start ist gewissermaßen ein weiterer Aspekt der Parallelisierung des Init-V-Prozesses.

27.2 Upstart

Als erste große Distribution hat Ubuntu den Schritt weg vom Init-V-System gewagt und ist mit Version 6.10 auf Upstart umgestiegen. Fedora ist mit Version 9 gefolgt, hat aber mit Version 15 einen weiteren Wechsel zu Systemd durchgeführt. Auch RHEL 6 verwendet Upstart. Mit RHEL 7 wird aber auch RHEL in das Systemd-Lager wechseln. Längerfristig wird also Ubuntu die einzige Distribution sein, die auf Upstart setzt.

Im Folgenden sind die wichtigsten Konzepte und Konfigurationsdateien von Upstart auf der Basis von Ubuntu zusammengefasst. Eine umfassende Dokumentation zu Upstart finden Sie auf der Projekt-Website:

http://upstart.ubuntu.com

Konzept

Upstart ist ereignisgesteuert. Ereignisse werden beim Starten und Stoppen von Programmen bzw. Diensten ausgelöst. Upstart verarbeitet die Ereignisse und reagiert darauf, indem es (weitere) Dienste startet/stoppt oder andere Ereignisse auslöst. Ereignisse bieten auch eine einfache Möglichkeit zur Kommunikation zwischen zwei Prozessen. Bei aktuellen Ubuntu-Versionen stellt das Programm `upstart-`

`monitor` aus dem gleichnamigen Paket eine simple grafische Benutzeroberfläche zur Überwachung von Upstart-Events zur Verfügung (siehe Abbildung 27.1).

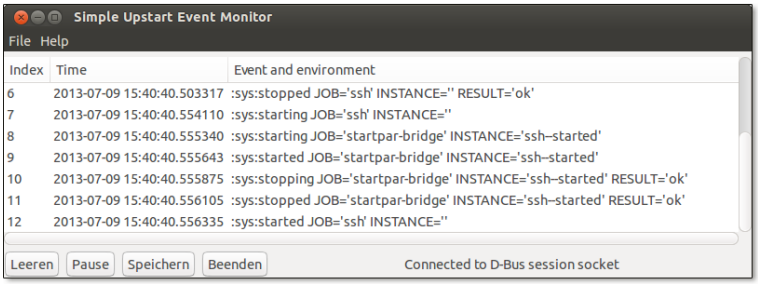


Abbildung 27.1 Upstart-Ereignisse mit dem Upstart-Event-Monitor verfolgen

Wie bei Init-V wird das Programm `/sbin/init` als erster Prozess vom Kernel gestartet. Das Programm `init` ist nun aber Teil des `upstart`-Pakets und hat nichts mit dem `init`-Programm des Init-V-Systems zu tun! Vielmehr kümmert sich `init` um die Auswertung der Konfigurationsdateien und um die Reaktion auf Ereignisse.

Der Ereignisfluss kommt durch `startup` in Gang. Dieses Ereignis wird nach dem Start von `/sbin/init` automatisch ausgelöst. Aus Kompatibilitätsgründen zum Init-V-System kennt Upstart auch Runlevel. Sie sind als Ereignisse mit dem Namen `runlevel n` implementiert.

Konfiguration

Die Datei `/etc/inittab` gibt es nicht mehr. Stattdessen befinden sich alle Konfigurationsdateien im Verzeichnis `/etc/init`. Das Programm `/sbin/init` liest alle `*.conf`-Dateien dieses Verzeichnisses. Eine typische Konfigurationsdatei sieht so aus:

```
# /etc/init/tty1.conf
start on stopped rc RUNLEVEL=[2345] and (
            not-container or
            container CONTAINER=lxc or
            container CONTAINER=lxc-libvirt)
stop on runlevel [!2345]
respawn
exec /sbin/getty -8 38400 tty1
```

Die Datei ist für den Start des Terminalemulators (Programm `getty`) auf der Textkonsole 1 verantwortlich. Die `exec`-Anweisung wird nicht sofort ausgeführt, sondern nur, wenn eines der mit `start on` definierten Ereignisse auftritt – also nach Abschluss der Scripts `rc2` bis `rc5` sowie unter bestimmten Umständen in virtuellen Maschinen. Analog wird `getty` wieder beendet, wenn eines der durch `stop on` definierten Ereignisse auftritt. `respawn` bewirkt, dass `getty` automatisch neu gestartet wird, sollte das Programm ungeplant enden.

Zusätzlich zu den oben enthaltenen Schlüsselwörtern existieren noch einige weitere Schlüsselwörter: Statt durch `exec` können die Startanweisungen für ein Programm auch durch `script` / `end script` formuliert werden. Alle dazwischen enthaltenen Zeilen werden durch die Shell `/bin/sh` ausgeführt. Falls beim Start bzw. Stopp zusätzliche Initialisierungs- oder Aufräumarbeiten erforderlich sind, werden die entsprechenden Kommandos mit `per-start script` / `end script` bzw. `post-stop script` / `end script` formuliert.

`console output` bewirkt, dass Ausgaben in der Konsole angezeigt werden, anstatt sie standardmäßig zu `/dev/null` zu leiten und somit zu ignorieren. Für die Reaktion auf die Tastenkombination Strg+Alt+Entf ist die Datei `control-alt-delete.conf` verantwortlich.

Wenn eine Upstart-Konfigurationsdatei selbst ein Ereignis auslösen möchte, kommt dazu das Kommando `emits eventname` zum Einsatz. Zu manchen Ereignissen gibt es sogar eigene `man`-Seiten (siehe z. B. `man local-filesystems`). Beachten Sie, dass manche Upstart-Ereignisse durch Scripts erzeugt werden, die sich außerhalb von `/etc/init` befinden! Beispielsweise wird das Ereignis `ifup` vom Script `/etc/network/if-up.d/upstart` mit dem Kommando `initctl` ausgelöst. Runlevel-Ereignisse werden vom Kommando `telinit` ausgelöst.

Init-V-Kompatibilität

In der gegenwärtigen Implementierung startet Upstart zwar viele, aber noch immer nicht alle Systemdienste. Für den Start der restlichen Dienste ist das Kompatibilitäts-Script `/etc/init.d/rc` bzw. `/etc/rc.d/rc` verantwortlich, das durch die Upstart-Konfigurationsdateien `rc.conf` und `rcS.conf` gestartet wird. `/etc/init.d/rc` funktioniert exakt so, wie es das Init-V-System vorsieht, d. h., es führt alle Start- bzw. Stopp-Scripts in `/etc/rc`*n*`.d` aus.

Es gibt aber auch eine umgekehrte Kompatibilität: Damit von Upstart verwaltete Dienste weiterhin durch Init-V-Kommandos gestartet bzw. gestoppt werden können, enthält `/etc/init.d/` bei Upstart-Diensten einen Link auf `/lib/init/upstart-job`. Dieses Script kümmert sich darum, passende Upstart-Kommandos auszuführen. Wenn Sie also unter Ubuntu `/etc/init.d/smbd stop` ausführen, führt das Script `upstart-job` das Kommando `stop smbd` aus. Die Links in `/etc/init.d` verraten auch auf einen Blick, wie viele Dienste bereits auf Upstart umgestellt wurden (`ls -l /etc/init.d`).

Steuerungskommandos

Upstart sieht eigene Kommandos vor, um Prozesse zu starten und zu stoppen, um einen Überblick über laufende Prozesse und anstehende Ereignisse anzuzeigen etc. Beachten Sie, dass diese Kommandos ausschließlich für Prozesse gelten, die direkt durch Upstart verwaltet werden. Dienste, die über die Init-V-Kompatibilitätsschicht gestartet wurden, werden weiterhin über die von Debian gebräuchlichen Kommandos administriert, also `invoke.rc`, `update-rc.d` etc.

`start` bzw. `stop` startet bzw. beendet einen Prozess, zu dem es eine entsprechende Konfigurationsdatei in `/etc/event.d` gibt. `status` gibt an, in welchem Zustand sich der Prozess gerade befindet.

```
root#  status tty2
tty2 start/running, process 4116
root#  stop tty2
tty2 stop/waiting
```

Statt `start` und `stop` können Sie auch das universellere Kommando `service` einsetzen, das mit vielen anderen Distributionen kompatibel ist:

```
root#  service tty1 stop
root#  service tty1 start
root#  service tty1 restart
```

`initctl` erledigt je nach dem als Parameter angegebenen Kommando diverse administrative Aufgaben (siehe `man initctl`). Beispielsweise erzeugt `initctl emit` *eventname* ein Ereignis mit dem angegebenen Namen. Das ist vor allem zum Test eigener Scripts praktisch. `initclt list` gibt einen Überblick über den Status aller laufenden Prozesse:

```
root#  initctl list | sort
acpid start/running, process 751
alsa-restore stop/waiting
alsa-store stop/waiting
anacron stop/waiting
apport stop/waiting
atd start/running, process 753
...
```

Dienst aktivieren/deaktivieren

Upstart sieht erstaunlicherweise keinen einfachen Weg vor, um einen Systemdienst zu deaktivieren bzw. wieder zu aktivieren. Wenn Sie einen Dienst vorübergehend nicht benötigen, ist es am einfachsten, das betreffende Paket ganz einfach zu deinstallieren. Alternativ können Sie auch die Upstart-Konfigurationsdatei mit einem Editor verändern – das setzt aber grundlegende Upstart-Kenntnisse voraus.

Runlevel

Wie bereits erwähnt wurde, benötigt Upstart eigentlich keine Runlevel. Aus Kompatibilitätsgründen zum Init-V-Prozess bildet Upstart aber auch das Runlevel-Konzept nach. Das Kommando `runlevel` gibt Auskunft über den aktuellen Runlevel. `telinit` *n* oder `init` *n* aktiviert den neuen Runlevel *n*.

Fedora- und RHEL-spezifische Besonderheiten

Obwohl Fedora 9 bis 13 und RHEL 6 zum Systemstart Upstart verwenden, wird der Standard-Runlevel bei diesen Distributionen weiterhin in `/etc/inittab` eingestellt. Alle anderen Einstellungen in dieser Datei werden aber ignoriert! Das Grafiksystem verwendet die Konsole 1 und nicht, wie bei vielen anderen Distributionen, die

Konsole 7. In der Konsole 1 wird deswegen beim Runlevel 5 *kein* Terminalemulator gestartet.

Falls während der Systeminitialisierung die Taste I gedrückt wurde, wird mit `touch` die Datei `/var/run/confirm` erzeugt; die Existenz dieser Datei wird von `/etc/rc.d/rc` überprüft. Falls sie existiert, erscheint in der Folge bei der Ausführung aller `rcn.d`-Script-Dateien eine Rückfrage (YES/NO/CONTINUE, wobei CONTINUE bedeutet, dass die weiteren Script-Dateien ohne Rückfrage ausgeführt werden sollen). Der interaktive Modus ist praktisch, wenn während der Ausführung der Init-V-Scripts zur Aktivierung eines Runlevels Probleme auftreten. Beachten Sie aber, dass der interaktive Modus erst nach dem Ende der Systeminitialisierung wirksam wird.

Die Datei `/etc/rc.d/rc.local` bietet eine einfache Möglichkeit, den Init-V-Prozess individuell anzupassen. Das Script wird nach allen anderen Init-V-Scripts ausgeführt, wenn der Runlevel 2, 3, 4 oder 5 aktiviert wird. Bei einem weiteren Runlevel-Wechsel oder beim Herunterfahren des Rechners wird das Script *nicht* mehr ausgeführt! Die Datei wird selbst bei aktuellen Fedora-Versionen berücksichtigt, die Systemd verwenden.

27.3 Systemd

Systemd ist ein neues Init-System, das vom Red-Hat-Mitarbeiter Lennart Poettering entwickelt wurde und erstmalig in Fedora 15 zum Einsatz kam. Auch openSUSE ist mit Version 12.1 auf Systemd umgestiegen. Dieser Abschnitt bezieht sich primär auf Fedora; openSUSE-spezifische Besonderheiten sind in Abschnitt 27.6 zusammengefasst. Beachten Sie insbesondere, dass in openSUSE die meisten Systemd-Dateien in `/usr/lib/systemd` gespeichert werden, während Fedora `/lib/systemd` als Speicherort verwendet!

Der vielleicht wichtigste Unterschied zwischen dem herkömmlichen Init-System und Systemd besteht darin, dass die Konfiguration nicht durch Shell-Scripts erfolgt, sondern durch einfache Textdateien. Systemd selbst ist ein kompiliertes Programm, wodurch sich ein spürbarer Geschwindigkeitsvorteil ergibt. Des Weiteren startet Systemd die Dienste parallel, was vor allem bei Multi-Core-Systemen von Vorteil ist.

Systemd verwendet Cgroups zur Ausführung und Überwachung von Prozessen. Die Abkürzung Cgroups steht für *Control Groups*. Dabei handelt es sich um eine Kernelfunktion, um die Ressourcen eines Prozesses zu limitieren (CPU, Speicher, I/O). Systemd startet jeden Prozess in einer eigenen Cgroup. Wenn die Anzahl der Prozesse in dieser Gruppe auf 0 sinkt, weiß Systemd, dass der Prozess beendet wurde oder abgestürzt ist, und kann ihn gegebenenfalls neu starten.

Administration

Das zentrale Kommando zur Administration von `systemd` lautet `systemctl`. Damit können Sie durch eine `*.service`-Datei beschriebene Dienste manuell starten, stoppen etc. Bei aktuellen Systemd-Versionen reicht es, einfach den Namen des Service anzugeben, also `ntpd` statt `ntpd.service`.

```
root#  systemctl start   ntpd.service   (NTP-Dämon starten)
root#  systemctl stop    ntpd.service   (NTP-Dämon stoppen)
root#  systemctl restart ntpd.service   (NTP-Dämon neu starten)
root#  systemctl reload  ntpd.service   (Konfiguration des NTP-Dämons neu einlesen)
root#  systemctl status  ntpd.service   (Status des NTP-Dämons ermitteln)
```

`systemctl` kann auch dazu verwendet werden, um einen Dienst dauerhaft zu aktivieren bzw. zu deaktivieren (so wie `chkconfig xxx on/off`):

```
root#  systemctl enable  ntpd.service
  ln -s '/lib/systemd/system/ntpd.service' \
        '/etc/systemd/system/multi-user.target.wants/ntpd.service'
root#  systemctl disable ntpd.service
  rm '/etc/systemd/system/multi-user.target.wants/ntpd.service'
```

Bei der Aktivierung von Diensten wird also ein neuer Link eingerichtet, und bei der Deaktivierung wird dieser Link wieder entfernt. Zumindest in diesem Punkt sind die Ähnlichkeiten mit dem Init-V-System unübersehbar.

Wenn `systemctl` ohne weitere Parameter aufgerufen wird, liefert es eine Liste aller Prozesse, die durch Systemd verwaltet werden:

```
user$  systemctl
UNIT                    LOAD   ACTIVE SUB       JOB DESCRIPTION
abrt-ccpp.service       loaded active exited    Install ABRT coredump hook
abrtd.service           loaded active running   ABRT Automated Bug Report...
abrt-oops.service       loaded active running   ABRT kernel log watcher
abrt-vmcore.service     loaded active exited    Harvest vmcores for ABRT
...
121 units listed. Pass --all to see inactive units, too.
```

Runlevel

In Systemd übernehmen »Targets« die Rolle von Runleveln. Aus Kompatibilitätsgründen gibt es aber spezielle Targets, die den herkömmlichen Runleveln entsprechen. Beispielsweise entspricht der Runlevel 0 dem `poweroff.target`, der Runlevel 5 dem `graphical.target`.

Anders als im Init-V-System können aber mehrere Targets zugleich aktiv sein. Eine Liste aller Targets ermitteln Sie mit dem folgenden Kommando. Aus dem Ergebnis geht hervor, dass sich das System in einem Zustand befindet, der dem Runlevel 5 entspricht. Genaugenommen ist das Target `graphical.target` aktiv.

```
user$  systemctl list-units --type=target
UNIT                LOAD   ACTIVE SUB      JOB DESCRIPTION
basic.target        loaded active active   Basic System
cryptsetup.target   loaded active active   Encrypted Volumes
getty.target        loaded active active   Login Prompts
graphical.target    loaded active active   Graphical Interface
local-fs-pre.target loaded active active   Local File Systems (Pre)
local-fs.target     loaded active active   Local File Systems
multi-user.target   loaded active active   Multi-User
network.target      loaded active active   Network
remote-fs.target    loaded active active   Remote File Systems
sockets.target      loaded active active   Sockets
sound.target        loaded active active   Sound Card
swap.target         loaded active active   Swap
sysinit.target      loaded active active   System Initialization
syslog.target       loaded active active   Syslog

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.
JOB    = Pending job for the unit.

14 units listed. Pass --all to see inactive units, too.
```

Um den aktuellen Runlevel zu ändern, führen Sie das folgende Kommando aus:

```
root#  systemctl isolate reboot.target    (Neustart des Rechners)
```

Default-Target einstellen

Das Default-Target, also gewissermaßen der Standard-Runlevel, wird durch den Link `/etc/systemd/system/default.target` definiert. Das folgende Kommando bewirkt, dass in Zukunft keine grafische Oberfläche mehr startet, sondern nur der Multi-User-Modus im Textmodus aktiviert wird:

```
root#  ln -sf /lib/systemd/system/multi-user.target \
         /etc/systemd/system/default.target
```

Konfiguration

Die Konfigurationsdateien für `systemd` befinden sich in den Verzeichnissen `/etc/systemd/` sowie `/lib/systemd/` (Fedora) bzw. `/usr/lib/systemd` (openSUSE). Insgesamt handelt es sich dabei um rund 300 Dateien – die Konfiguration ist also ziemlich komplex und zumindest ebenso unübersichtlich wie beim Init-V-System.

Eine zentrale Rolle im Systemd-Konzept spielen Units: Sie beschreiben Objekte, die durch das Init-System gesteuert werden sollen. Dazu zählen nicht nur Dienste, die gestartet oder gestoppt werden müssen, sondern auch Netzwerkschnittstellen, `mount`-Verzeichnisse, Swap-Partitionen etc.

Mit *.target-Dateien können mehrere Units zu einer Gruppe verbunden werden. Targets sind mit der Runlevel-Idee vergleichbar, es gibt aber in der Regel wesentlich mehr Targets, die sich aufeinander beziehen können. Jedes Target kann mit einem zusätzlichen *name*.target.wants-Verzeichnis verknüpft werden, in dem durch Dateien bzw. durch Links auf Dateien weitere Units aufgezählt werden, die ebenfalls aktiviert werden sollen. Beispielsweise enthält das Verzeichnis /lib/systemd/system/sysinit.target.wants diverse Links auf *.service-Dateien zur Systeminitialisierung.

*.service-Dateien beschreiben, welche Voraussetzungen für den Start eines Dienstes erfüllt sein müssen und welches Kommando gestartet werden soll. Diese Dateien befinden sich in den Verzeichnissen /etc/systemd/system und /lib/systemd/system. Als Beispiel zeigt das folgende Listing die Datei httpd.service, die unter Fedora für den Start des Webservers Apache verantwortlich ist:

```
# Datei /lib/systemd/system/httpds.service

[Unit]
Description=The Apache HTTP Server
After = network.target remote-fs.target nss-lookup.target

[Service]
Type=notify
EnvironmentFile = /etc/sysconfig/httpd
ExecStart       = /usr/sbin/httpd $OPTIONS -DFOREGROUND
ExecReload      = /usr/sbin/httpd $OPTIONS -k graceful
ExecStop        = /usr/sbin/httpd $OPTIONS -k graceful-stop
KillSignal      = SIGCONT
PrivateTmp      = true

[Install]
WantedBy = multi-user.target
```

Zur Konfiguration und vor allem zur Analyse von Systemd können Sie die Benutzeroberfläche systemadm starten (siehe Abbildung 27.2). Unter Fedora befindet sich dieses Programm im Paket systemd-ui.

Verhalten bei Strg-Alt-Entf

Wenn Sie in einer Textkonsole Strg+Alt+Entf drücken, wird der Rechner neu gestartet. Verantwortlich dafür ist die spezielle Target-Datei /lib/systemd/system/ctrl-alt-del.target.

Vereinheitlichung von Konfigurationsdateien

Im Zuge der Umstellung auf Systemd hat dessen Entwickler Lennart Poettering vorgeschlagen, auch diverse Konfigurationsdateien zu vereinheitlichen, die von (nahezu) jeder Distribution an einem anderen Ort gespeichert werden und die zum Teil auch unterschiedliche Syntaxregeln verwenden. Als erste Distribution hat Fedora 18 diese Ideen umgesetzt. Die in Tabelle 27.3 aufgezählten Konfigurationsdateien und -werkzeuge werden in Kapitel 21 näher beschrieben.

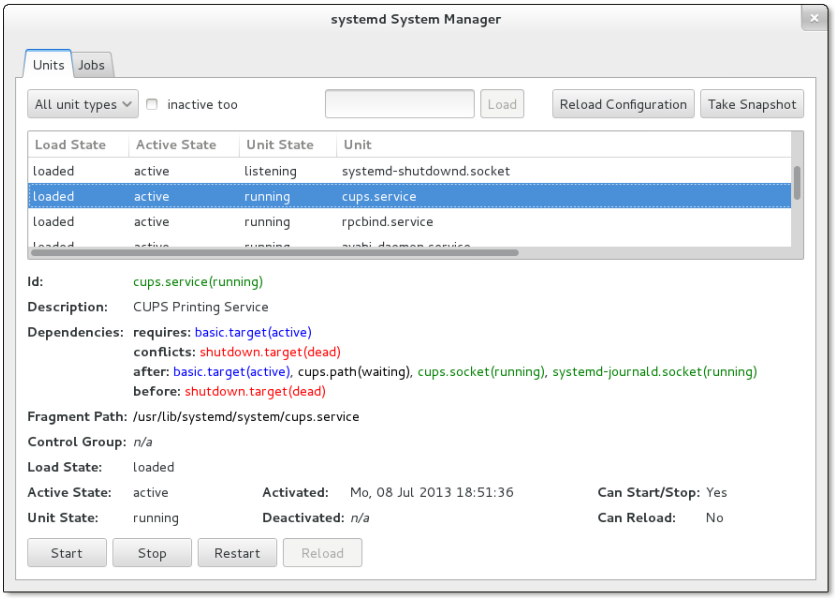


Abbildung 27.2 Systemd-Administration mit systemadm

Funktion	bisheriger Ort	neuer Ort	Konfigurationshilfe
Hostname	`/etc/sysconfig/network`	`/etc/hostname`	`hostnamectl`
Sprache	`/etc/sysconfig/i18n`	`/etc/locale.conf`	`localectl`
Tastatur	`/etc/sysconfig/keyboard`	`/etc/vconsole.conf`	`localectl`
Zeitzone	`/etc/sysconfig/clock`	`/etc/localtime`	`timedatectl`

Tabelle 27.3 Geänderte Konfigurationsdateien

Journal

Aktuelle Systemd-Versionen beinhalten auch ein neues Logging-System mit dem Namen »Journal«. Die Logging-Dateien werden in einem binären Format gespeichert und sind gegen nachträgliche Veränderungen abgesichert (siehe auch Abschnitt 21.7). Bis zum Sommer 2013 gab es allerdings noch keine Distribution, bei der der klassische Syslog-Dienst durch das neue Journal ersetzt wurde.

Kompatibilität

Systemd ist zum herkömmlichen Init-V-System kompatibel. Init-Scripts, die sich im Verzeichnis `/etc/init.d/` befinden, werden also wie bisher gestartet bzw. beendet. Während Fedora nahezu komplett auf Systemd umgestellt wurde, enthält das Verzeichnis `/etc/init.d/` bei openSUSE noch eine Menge Scripts, die auf eine Portierung nach Systemd warten.

Das mittlerweile von beinahe allen Distributionen unterstützte Kommando `service` funktioniert auch unter Systemd. Wenn Sie beispielsweise `service httpd stop` aus-

führen, erkennt `service`, dass der Webserver durch Systemd gesteuert wird, und führt `systemctl stop httpd.service` aus.

Dokumentation

Systemd ist ausgezeichnet dokumentiert: Alle Funktionen, Strategien und Vorzüge von Systemd sind beinahe schon überkomplett in diversen Manual-Seiten (insbesondere `man systemd`) sowie auf der Webseite des Systemd-Entwicklers Lennart Poettering beschrieben:

http://0pointer.de/blog/projects/systemd-docs.html

Auch die Website *heise open* hat sich ausführlich mit Systemd befasst:

http://heise.de/-1563259 und *http://heise.de/-1563461*

Wenn Sie kurze und prägnante Texte bevorzugen, sind die beiden folgenden Seiten hilfreich. Sie fassen die wichtigsten Änderungen im Vergleich zu Init-V zusammen und beantworten einige FAQs:

http://fedoraproject.org/wiki/SysVinit_to_Systemd_Cheatsheet
http://www.freedesktop.org/wiki/Software/systemd/FrequentlyAskedQuestions

27.4 Debian-Systemstart

Abbildung 27.3 gibt einen Überblick über den auf Init-V basierenden Sytemstart unter Debian. Beim Start führt das Init-System zuerst die Scripts aus dem Verzeichnis `/etc/rcS.d` aus, dann jene aus dem Verzeichnis `/etc/rc2.d` für den Runlevel 2. Für das Herunterfahren des Systems sind die Scripts in `/etc/rc0.d` verantwortlich. Tabelle 27.4 fasst den Ort der Konfigurationsdateien zusammen.

Funktion	Konfigurationsdateien
Systeminitialisierung	`/etc/init.d/rcS`, `/etc/rcS.d/*`
Init-Scripts	`/etc/init.d/*`
Runlevel-Links	`/etc/rc`*n*`.d/rc`*n*`.d/*`
Konfigurationsdateien	`/etc/default/*`

Tabelle 27.4 Konfiguration des Debian-Systemstarts

Interna beim Runlevel-Wechsel

Bei einem Runlevel-Wechsel werden nur solche Funktionen gestoppt, die im vorigen Runlevel gestartet wurden, im neuen Runlevel aber nicht mehr benötigt werden. Ebenso werden nur solche Funktionen neu gestartet, die bisher noch nicht aktiv waren. Um das festzustellen, überprüft das Script `rc`, ob es für die Funktion im vorherigen Level einen Start- oder Stopp-Link gibt.

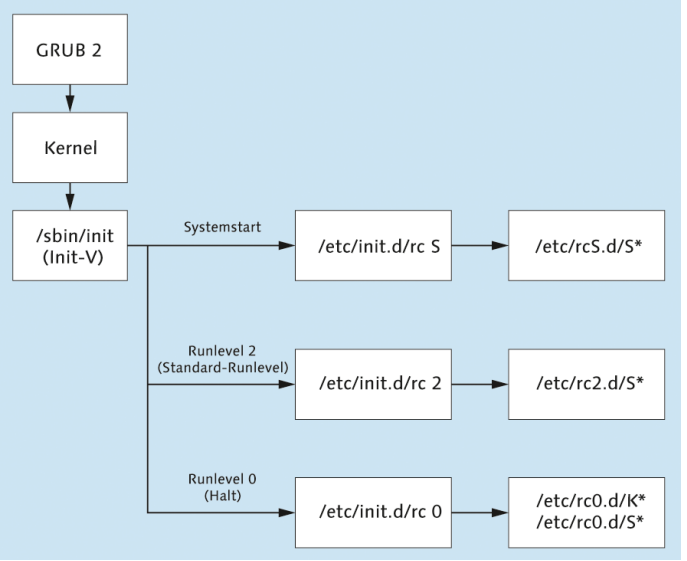


Abbildung 27.3 Debian starten und beenden

Init-V-Scripts starten

Das Kommando `invoke.rc` verringert den Tippaufwand für den manuellen Start eines Init-V-Scripts:

```
root#  invoke.rc samba restart
```

Grafiksystem

Das Grafiksystem X wird durch das Init-V-Script `gdm3` gestartet.

Individuelle Anpassung des Init-V-Prozesses

Die Datei `/etc/init.d/rc.local` bietet eine einfache Möglichkeit, den Init-V-Prozess individuell anzupassen. Das Script wird nach allen anderen Init-V-Scripts ausgeführt, wenn der Runlevel 2, 3, 4 oder 5 zum ersten Mal aktiviert wird. Bei einem weiteren Runlevel-Wechsel oder beim Herunterfahren des Rechners wird das Script *nicht* mehr ausgeführt, auch nicht zum Stoppen irgendwelcher dort gestarteten Programme!

Aufbau von Init-V-Script-Dateien

Die folgenden Zeilen zeigen den Aufbau des eigenen Init-V-Scripts `/etc/init.d/masquerading`, um den Rechner als Internet-Gateway einzurichten (Masquerading und eine minimale Firewall, siehe Abschnitt 30.3). Der `INIT-INFO`-Block gibt an, in welchen Runleveln das Script üblicherweise ausgeführt werden soll und welche anderen Dienste vorher gestartet werden müssen.

```
#!/bin/sh

### BEGIN INIT INFO
# Provides:          masquerading
# Required-Start:    $network $local_fs $remote_fs
# Required-Stop:     $network $local_fs $remote_fs
# Default-Start:     2 3 4 5
```

```
# Default-Stop:      0 1 6
# Short-Description: start masquerading
### END INIT INFO

DESC="masquerading"        # Bezeichnung des Scripts
ADSL=eth1                  # Schnittstelle, über die der Internetzugang erfolgt
. /lib/lsb/init-functions  # Grundfunktionen lesen
IPT=$(which iptables)      # iptables-Kommando suchen
if [ -z $IPT ]; then
  [ -x /sbin/iptables ]      && IPT=/sbin/iptables
  [ -x /usr/sbin/iptables ]  && IPT=/usr/sbin/iptables
fi
[ -z $IPT ] && (echo "iptables cannot be found!"; exit 0)

# Funktionen für start, stop und restart
case "$1" in
  start)
        log_begin_msg "Starting masquerading ..."
        ERROR=0
        $IPT -t nat -A POSTROUTING -o $ADSL -j MASQUERADE
        echo 1 > /proc/sys/net/ipv4/ip_forward
        log_end_msg $ERROR
        ;;

  stop)
        log_begin_msg "Stopping masquerading ..."
        ERROR=0
        echo 0 > /proc/sys/net/ipv4/ip_forward
        $IPT -t nat -D POSTROUTING -o $ADSL -j MASQUERADE
        log_end_msg $ERROR
        ;;

  restart)
        $0 stop
        $0 start
        ;;

  *)
        log_success_msg "Usage: masquerading {start|stop|restart}"
        exit 1
        ;;
esac
exit 0
```

Damit das Script in Zukunft automatisch beim Rechnerstart ausgeführt wird, führen Sie die folgenden Kommandos aus:

```
root#  insserv masquerading
```

27.5 Fedora-Systemstart

Abbildung 27.4 fasst zusammen, wie Fedora in das Standard-Target `graphical` (entspricht Runlevel 5) startet bzw. wie es wieder heruntergefahren wird. Die Abbildung gilt auch für openSUSE, allerdings befinden sich dort die Systemd-Dateien im Verzeichnis `/usr/lib/systemd`. Tabelle 27.5 gibt einen Überblick über die Fedora-Konfigurationsdateien.

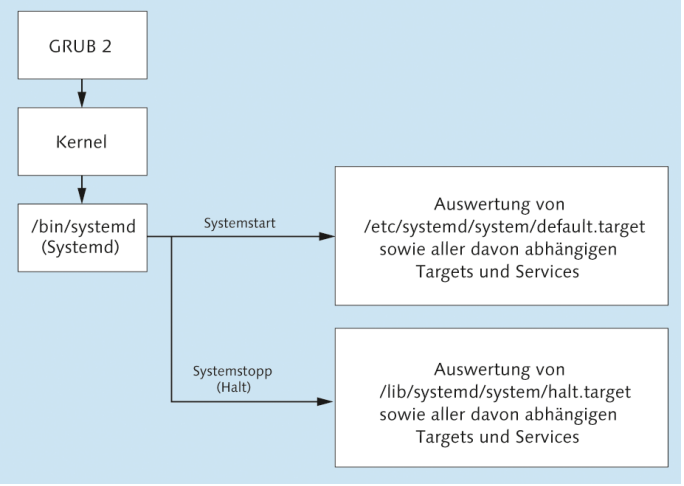


Abbildung 27.4 Fedora und openSUSE starten und beenden

Funktion	Konfigurationsdateien
Systemd	`/etc/systemd/*`, `/lib/systemd/*`
Systemd-Default-Target (Link)	`/etc/systemd/system/default.target`
Systeminitialisierung	`/lib/systemd/system/sysinit.target*`
Herkömmliche Init-V-Scripts	`/etc/rc.d/init.d/*`
Init-V-Runlevel-Links	`/etc/rc.d/rcn.d/*`
Konfigurationsdateien	`/etc/sysconfig/*`

Tabelle 27.5 Konfiguration des Fedora-Systemstarts

Fedora hat den Umstieg auf Systemd sehr konsequent vollzogen: Das Verzeichnis `/etc/init.d/` ist fast leer, und das ehemals für die System- und Hardware-Initialisierung verantwortliche Script `/etc/rc.d/rcsysconfig` gibt es gar nicht mehr.

Start des Grafiksystems

Für den Start des Grafiksystems ist die Konfigurationsdatei `/lib/systemd/system/gdm.service` verantwortlich.

Logging

Ein Protokoll aller von `systemd` gestarteten Dienste finden Sie in der Logging-Datei `/var/log/boot.log`. Systemd-Nachrichten werden parallel auch mit dem neuen Logging-Dienst *Journal* aufgezeichnet und können mit dem Kommando `journalctl` gelesen werden.

Konfiguration

Neben `systemctl` können Sie Systemd-Dienste auch mit der grafischen Benutzeroberfläche `system-config-services` aus dem gleichnamigen Paket starten, stoppen oder neu starten. In der Vergangenheit bot das Programm weitere Funktionen, etwa die Aktivierung oder Deaktivierung von Diensten. Diese Funktionen sind aber dem Systemd-Umstieg zum Opfer gefallen.

Init-V-Kompatibilität

Systemd ist Init-V-kompatibel und kümmert sich daher um die Ausführung von Scripts in `/etc/rcn.d`. Das Fedora- bzw. Red-Hat-spezifische Kommando `chkconfig` hilft weiterhin bei der Zuordnung der Links zu den Init-V-Scripts (siehe Abschnitt 27.1).

Die zur individuellen Anpassung des Systemstarts ehemals vorgesehene Datei `/etc/rc.d/rc.local` existiert standardmäßig nicht mehr. Wenn Sie am Ende des Systemstarts eigene Scripts ausführen möchten, können Sie dazu aber weiterhin `/etc/rc.d/rc.local` verwenden: Dazu erzeugen Sie diese Datei und stellen mit `chmod ug+x` sicher, dass die Datei auch ausführbar ist.

27.6 openSUSE-Systemstart

Da openSUSE mit Version 12.1 ebenfalls auf Systemd umgestiegen ist, gilt Abbildung 27.4 grundsätzlich auch für aktuelle openSUSE-Distributionen. Beachten Sie aber, dass sich die Systemd-Dateien bei openSUSE im Verzeichnis `/usr/lib/systemd` befinden und dass es auch sonst diverse Unterschiede in der Systemd-Konfiguration im Vergleich zu Fedora gibt. Tabelle 27.6 zählt die für den Systemstart relevanten Konfigurationsdateien auf.

Funktion	Konfigurationsdateien
Systemd	`/etc/systemd/*`, `/usr/lib/systemd/*`
Systemd-Default-Target (Link)	`/etc/systemd/system/default.target`
Systeminitialisierung	`/usr/lib/systemd/system/sysinit.target*`
Herkömmliche Init-V-Scripts	`/etc/init.d/*`
Runlevel-Links	`/etc/init.d/rcn.d/*`
Konfigurationsdateien	`/etc/sysconfig/*`

Tabelle 27.6 Konfiguration des SUSE-Systemstarts

Start des Grafiksystems

Das Grafiksystem X wird durch das Init-V-Script `xdm` gestartet. Welcher Display Manager tatsächlich gestartet wird (z. B. `kdm4`), bestimmt die Variable `DISPLAYMANAGER`, die in `/etc/sysconfig/displaymanager` eingestellt wird.

Init-V-Kompatibilität

Bei der Portierung des Systemstarts auf Systemd ist openSUSE nicht so weit wie Fedora: Unzählige Dienste werden weiterhin durch Init-V-Scripts gesteuert.

Herkömmliche Init-V-Scripts können Sie unter openSUSE auch in der Form `rcname` aufrufen, also z. B. `rcsmb`, um den Samba-Server zu starten oder zu stoppen. Dazu befinden sich in `/usr/sbin` entsprechende Links.

Konfigurationswerkzeuge

Zur Steuerung von Init-V- und Systemd-Diensten kann auch das Kommando `service` verwendet werden. Init-V-Links können mit `insserv` eingerichtet werden. `insserv` kümmert sich auch um die richtige Nummerierung der Links. Für die Entscheidung, welche Nummer der Link bekommt, werden die `Provides`- und `Requires`-Kommentare innerhalb der Init-V-Scripts ausgewertet. Gegebenenfalls werden durch `insserv` auch bereits vorhandene Links neu nummeriert.

Wohl aus Kompatibilitätsüberlegungen gibt es auch unter SUSE das Kommando `chkconfig`. Die Optionen `-add`, `-del` und `-list` funktionieren wie bei Red Hat, bei anderen Optionen gibt es aber Abweichungen. Intern greift `chkconfig` auf `insserv` zurück.

Parallelisierung

Init-V-Scripts, die nicht voneinander abhängig sind, werden standardmäßig parallel statt hintereinander ausgeführt. Die Details des Bootprozesses werden durch `/etc/sysconfig/boot` gesteuert. Damit die Parallelisierung funktioniert, müssen Init-V-Links mit `insserv` verändert werden, nicht durch die direkte Veränderung der Links! `insserv` erzeugt die Dateien `.depend.*`, die Informationen über die Abhängigkeiten der Init-V-Scripts enthalten. Weitere Informationen zum SUSE-Systemstart finden Sie in der Manual-Seite zu `init.d`.

boot.local

In der Datei `/etc/rc.d/boot.local` können Sie lokale Anpassungen durchführen. Das Script sollte ausschließlich Kommandos enthalten, die nur ein einziges Mal beim Systemstart ausgeführt werden sollen. Ein typisches Beispiel sind `modprobe`-Anweisungen, um ein ganz bestimmtes Kernelmodul zu laden. `boot.local` wird vor den `rc`-Scripts ausgeführt.

27.7 RHEL-6-Systemstart

Unter RHEL 6 bzw. CentOS läuft zwar Upstart als Init-System, tatsächlich werden aber fast alle System- und Netzwerkdienste durch Init-V-Scripts gestartet. RHEL 6 verlässt sich also weitestgehend auf die Init-V-Kompatibilität von Upstart. Abbildung 27.5 zeigt die wichtigsten Stationen beim Starten bzw. Beenden von RHEL. Der

Default-Runlevel ist 3 für den Server-Betrieb im Textmodus oder 5, falls auch ein grafisches Desktop-System installiert wurde. Tabelle 27.7 gibt einen Überblick über die wichtigsten Konfigurationsdateien.

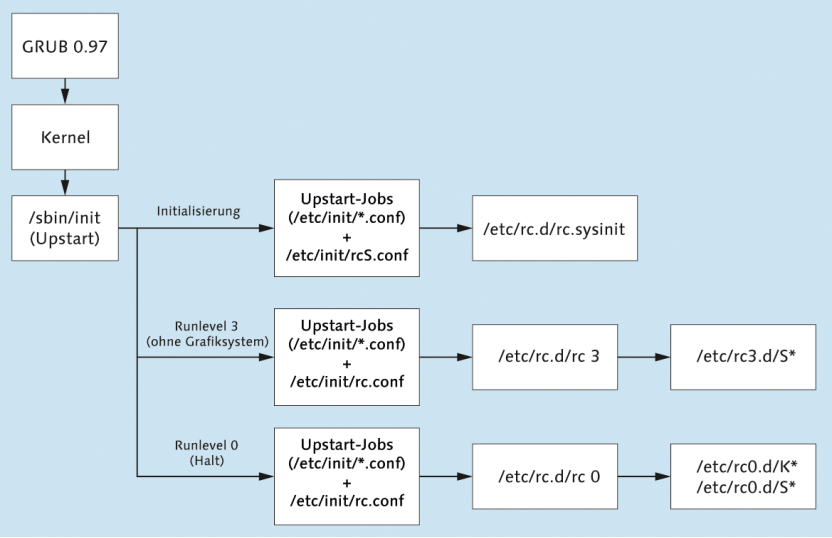


Abbildung 27.5 RHEL 6 starten und beenden

Funktion	Konfigurationsdateien
Upstart	`/etc/init/*.conf`
Default-Runlevel	`/etc/inittab`
Systeminitialisierung	`/etc/init/rcS.conf`, `/etc/rc.d/rc.sysinit`
Init-Scripts	`/etc/init.d/*`
Runlevel-Links	`/etc/rc.d/rc`*n*`.d/*`
Konfigurationsdateien	`/etc/sysconfg/*`

Tabelle 27.7 Konfiguration des Systemstarts von RHEL 6

Konfigurationswerkzeuge

Zum Starten von Init-V-Scripts können Sie das Kommando `service` verwenden, zum Einrichten von Init-V-Links das Kommando `chkconfig`.

Start des Grafiksystems

Für den Start von X ist die Upstart-Datei `prefdm.conf` verantwortlich. Für die Auswahl des Display Managers ist das Script `/etc/X11/prefdm` verantwortlich. In der Datei `/etc/sysconfig/desktop` kann der gewünschte Display Manager in der Variablen `DISPLAYMANAGER` eingestellt werden. Wenn diese Datei nicht existiert bzw. `DISPLAYMANAGER` nicht definiert ist, wird per Default `gdm` gestartet.

Single-User-Modus absichern

Eine Eigenheit von RHEL 6 besteht darin, dass Sie im Single-User-Modus ohne Passwort arbeiten können. Sofern Sie also Zugang zu einem RHEL-Server haben, müssen Sie lediglich in GRUB den zusätzlichen Kernelparameter `single` angeben und können dann ohne `root`-Passwort Konfigurations- oder Reparaturarbeiten durchführen. Falls Sie auch den Single-User-Modus durch ein Passwort absichern möchten, verändern Sie eine Zeile in `/etc/sysconfig/init`:

```
# Datei /etc/sysconfig/init
...
SINGLE=/sbin/sulogin
```

27.8 Ubuntu-Systemstart

Abbildung 27.6 zeigt, welche Dateien und Scripts für den Start bzw. das Herunterfahren von Ubuntu verantwortlich sind. Der Standard-Runlevel lautet 2. Tabelle 27.8 fasst den Ort der wichtigsten Konfigurationsdateien zusammen.

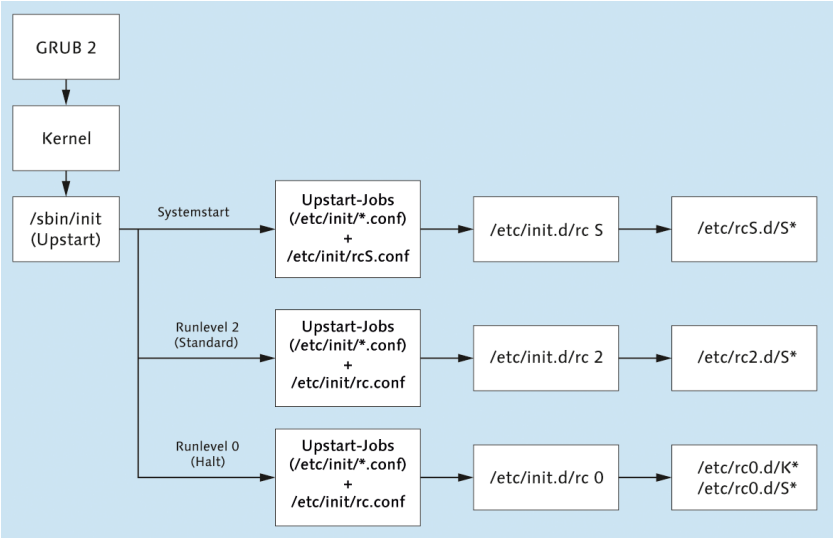


Abbildung 27.6 Ubuntu starten und beenden

Upstart ist bei Ubuntu für den Start der meisten System- und Netzwerkdienste verantwortlich. Die restlichen Initialisierungsaufgaben werden von den Init-V-Kompatibilitäts-Scripts erledigt. Der Init-V-Teil des Systemstarts verläuft dabei wie bei Debian (siehe Abschnitt 27.4). Auch die Administrationswerkzeuge sind dieselben. Der Standard-Runlevel wird durch die Datei `/etc/init/rc-sysinit.conf` eingestellt.

Funktion	Konfigurationsdateien
Upstart	/etc/init/*.conf
Default-Runlevel	/etc/init/rc-sysinit.conf
Systeminitialisierung	/etc/init.d/rcS, /etc/rcS.d/*
Init-Scripts	/etc/init.d/*
Runlevel-Links	/etc/rc*n*.d/rc*n*.d/*
Konfigurationsdateien	/etc/default/*

Tabelle 27.8 Konfiguration des Ubuntu-Systemstarts

Start von X

Das Grafiksystem X wird durch Upstart gestartet (Konfigurationsdatei `lightdm.conf`). Als Voraussetzungen für den Start von X gelten lediglich die Initialisierung des Dateisystems und der Start des DBUS-Systems. Der Display Manager wird also bereits wenige Sekunden nach Beginn des Boot-Prozesses gestartet.

Eigene Upstart-Konfigurationsdateien

Um selbst ein Programm im Rahmen des Systemstarts auszuführen, müssen Sie eine eigene Konfigurationsdatei in `/etc/init` erstellen. Das folgende Beispiel aktiviert bzw. deaktiviert Masquerading (siehe Abschnitt 30.3), startet aber keinen Hintergrundprozess. Daher gibt es weder eine `exec`-Zeile noch einen allgemeinen `script`-Block, sondern stattdessen die beiden Blöcke `pre-start script` und `post-stop script`. Die Masquerading-Funktion wird vor den Netzwerkschnittstellen eingeschaltet und beim Herunterfahren des Rechners wieder ausgeschaltet.

```
# Datei /etc/init/masquerading.conf
description     "masquerading"
start on (starting network-interface
          or starting network-manager
          or starting networking)
stop on runlevel [!023456]

pre-start script
  sysctl -q -w net.ipv4.ip_forward=1
  iptables -A POSTROUTING -t nat -o eth0 -j MASQUERADE
end script

post-stop script
  iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
  sysctl -q -w net.ipv4.ip_forward=0
end script
```

Sie können die Konfigurationsdatei mit den Kommandos `start masquerading` bzw. `stop masquerading` ausprobieren. Achten Sie darauf, dass Sie an `start` oder `stop` exakt den Dateinamen der Konfigurationsdatei übergeben (aber ohne `.conf`). Wenn Sie die Fehlermeldung *unknown job* erhalten, liegt in der Regel ein Syntaxfehler in der Konfigurationsdatei vor. Um die Syntax einer Konfigurationsdatei zu testen, führen Sie `init-checkconf` aus:

```
user$  init-checkconf /etc/init/masquerading.conf
File masquerading.conf: syntax ok
```

27.9 Internet Service Daemon

Programme, die Netzwerk- oder Internetdienste zur Verfügung stellen, können in zwei Gruppen eingeteilt werden:

- Die eine Gruppe besteht aus Programmen, die als sogenannte Dämonen ständig laufen. Nahezu alle in diesem Buch vorgestellten Netzwerkdienste – der Webserver Apache, der Datei-Server Samba, der SSH-Server etc. – zählen zu dieser Gruppe. Diese Programme werden durch das Init-System gestartet und überwachen dann einen IP-Port. Sobald ein IP-Paket eintrifft, das an diesen IP-Port adressiert ist, wird es ausgewertet und beantwortet.
- Die zweite Gruppe besteht aus selten benötigten Programmen, die erst bei Bedarf gestartet werden. Anstatt auch diese Programme alle zu starten, wird ein sogenannter *Internet Service Daemon* ausgeführt. Dieses Programm überwacht mehrere IP-Ports gleichzeitig und aktiviert erst bei Bedarf den entsprechenden Server-Dienst. Der Internet Service Daemon selbst wird übrigens ganz normal durch das Init-System gestartet.

Als *Internet Service Daemon* war früher `inted` weit verbreitet. Mittlerweile gilt dieses Programm aber als veraltet. Deswegen kommt je nach Distribution `openbsd-inetd` oder `xinetd` zum Einsatz. Standardmäßig ist zumeist keines dieser Pakete installiert: Eine Installation ist nur erforderlich, wenn ein anderes Programm die `inetd`-Funktionalität verlangt und im Paket eine entsprechende Abhängigkeit formuliert ist.

/etc/services

Unabhängig davon, welcher Internet Service Daemon bei Ihrer Distribution zum Einsatz kommt, stellt die Datei `/etc/services` die Zuordnung zwischen den Namen verschiedener Internetdienste (z. B. `ftp`, `telnet` etc.) und deren Protokolltypen und Port-Nummern her. Beispielsweise verwenden E-Mail-Server (MTAs) den Port 25 und die Protokolle `tcp` und `udp`. Die folgenden Zeilen zeigen einen Ausschnitt aus dieser Datei:

```
# /etc/services (auszugsweise)
# name      port/proto   alias   comment
ftp-data    20/tcp               # File Transfer [Default Data]
ftp-data    20/udp               # File Transfer [Default Data]
ftp         21/tcp               # File Transfer [Control]
ssh         22/tcp               # SSH Remote Login Protocol
ssh         22/udp               # SSH Remote Login Protocol
smtp        25/tcp       mail    # Simple Mail Transfer
...
```

/etc/hosts.allow und hosts.deny

Die Dateien `/etc/hosts.allow` und `/etc/hosts.deny` steuern, von welchem Rechner aus welche Dienste verwendet werden dürfen. Die Einstellungen gelten für alle Programme, die auf die TCP-Wrapper-Bibliothek zurückgreifen. Dazu zählen neben `xinetd` auch der SSH-Server, NFS und bei SUSE auch CUPS. Details zum Aufbau der Konfigurationsdateien `hosts.allow` und `hosts.deny` finden Sie in Abschnitt 40.2.

Ein Sonderfall ist `openbsd-inetd`: Dieses Programm ist zwar mit der TCP-Wrapper-Bibliothek verlinkt, standardmäßig sind seine Funktionen aber deaktiviert! Um TCP-Wrapper-Funktionen zu aktivieren, müssen Sie das Programm mit der Option `-l` starten. Bei Debian und Ubuntu erzeugen Sie dazu die Datei `/etc/default/openbsd-inetd` und fügen die folgende Zeile ein:

```
# Datei /etc/default/openbsd-inetd (Debian, Ubuntu)
# TCP-Wrapper-Funktionen aktivieren
OPTIONS="-l"
```

Mit dieser Option unterbleibt der in `inetd.conf` vorgesehene Aufruf von `tcpd`, um zu vermeiden, dass die TCP-Wrapper-Regeln zweimal überprüft werden.

openbsd-inetd

/etc/inetd.conf

Wenn auf Ihrer Distribution `openbsd-inetd` läuft, erfolgt dessen Konfiguration durch die Datei `/etc/inetd.conf`. Das Programm wird nur dann gestartet, wenn die Konfigurationsdatei `inetd.conf` zumindest einen aktiven Eintrag enthält. Jeder Eintrag in dieser Datei besteht aus einer Zeile mit sechs Spalten:

- Die erste Spalte gibt den Namen des Diensts an, der in `/etc/services` definiert sein muss.
- Die zweite und dritte Spalte beschreiben, wie der Dienst kommuniziert (Socket-Typ und Protokoll).
- Die vierte Spalte beschreibt, ob der gleiche Dienst bei mehreren Anfragen mehrfach gestartet werden soll (`nowait`) oder ob weitere Anfragen erst verarbeitet werden sollen, nachdem der bereits gestartete Dienst fertig ist (`wait`). Optional kann eine Timeout-Zeit in Sekunden angegeben werden.

- Die fünfte Spalte gibt an, mit welchen Rechten der Prozess gestartet werden soll.
- Der Rest der Zeile gibt das Kommando an, das ausgeführt werden soll. Dabei führt `tcpd` zuerst einen Test durch, ob eine Ausführung gemäß den TCP-Wrapper-Regeln erlaubt ist (siehe Abschnitt 27.9).

```
# Datei /etc/inetd.conf
swat  stream  tcp nowait.400  root  /usr/sbin/tcpd /usr/sbin/swat
...
```

Normalerweise müssen Sie sich nicht selbst um die Konfiguration von `inetd.conf` kümmern. Bei der Installation eines Pakets, das auf `inted` angewiesen ist, wird `inetd.conf` automatisch entsprechend erweitert. Beachten Sie, dass mit # eingeleitete Zeilen wie üblich als Kommentare gelten! Änderungen an `inetd.conf` werden erst wirksam, wenn Sie `/etc/init.d/openbsd-inetd reload` ausführen.

xinetd

/etc/xinetd.conf

Die Datei `/etc/xinetd.conf` enthält einige Grundeinstellungen für `xinetd`, die beispielsweise das Logging oder die Standard-IP-Adresse betreffen. Im Regelfall können die Einstellungen unverändert bleiben. Entscheidend ist die Anweisung `includedir`, die das Verzeichnis mit den weiteren Konfigurationsdateien angibt, üblicherweise `/etc/xinetd.d`.

xinetd.d/*

Das Verzeichnis `/etc/xinetd.d` enthält für jeden von `xinetd` gesteuerten Dienst eine eigene Konfigurationsdatei. Die Namen dieser Dateien in `/etc/xinetd.d` spielen keine Rolle: `xinetd` liest einfach alle Dateien aus diesem Verzeichnis und wertet sie aus. (Nicht berücksichtigt werden Dateien, deren Name mit ~ endet oder einen Punkt enthält.)

Der Aufbau der einzelnen Konfigurationsdateien ist einheitlich. Das folgende Beispiel zeigt die Datei für einen RSYNC-Server:

```
# /etc/xinetd.d/rsync
service rsync
{
        disable = yes
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/bin/rsync
        server_args     = --daemon
        log_on_failure  += USERID
}
```

Die folgende Liste ist eine kurze Erläuterung der wichtigsten Schlüsselwörter, die in `xinetd`-Konfigurationsdateien auftreten können. Eine ausführlichere Beschreibung gibt `man xinetd.conf`.

- `service` bezeichnet den Dienst (entsprechend `/etc/services`).
- `socket_type` und `protocol` geben an, wie die Daten zwischen Client und Server übertragen werden.
- `type = INTERNAL` gibt an, dass es sich um einen Dienst handelt, der direkt von `xinetd` zur Verfügung gestellt wird.
- `server` gibt den Programmnamen an (sofern es sich nicht um einen internen `xinetd`-Dienst handelt).
- `server_args` gibt optionale Parameter an, die beim Start an den Dienst übergeben werden sollen.
- `user` gibt an, unter welchem Account das Programm ausgeführt wird (oft `root`, es ist aber auch `news`, `mail` etc. möglich).
- `disable = Yes / No` gibt an, ob der Dienst aktiv oder blockiert ist. Bei blockierten Diensten enthält die Konfigurationsdatei `disable=Yes`. Bei Fedora und Red Hat können Sie `xinetd`-Dienste auch durch `chkconfig --del name` deaktivieren bzw. durch `chkconfig --add name` wieder aktivieren. Diese Kommandos verändern nur die `disable`-Zeile und rühren die restliche Konfiguration nicht an.
- `log_*` gibt an, ob die Nutzung des Dienstes protokolliert werden soll.

Kapitel 28
Kernel und Module

Dieses Kapitel beschäftigt sich mit dem Linux-Kernel und seinen Modulen. Module sind Teile des Kernels, die bei Bedarf geladen werden – etwa wenn eine bestimmte Hardware-Komponente zum ersten Mal angesprochen wird. Abschnitt 28.1 erklärt, warum das meistens automatisch funktioniert und was Sie tun müssen, wenn der Automatismus versagt.

Es besteht eher selten die Notwendigkeit, den Kernel neu zu kompilieren. Viel wahrscheinlicher ist es, dass Sie nur ein Modul kompilieren möchten, damit dieses zum aktuellen Kernel passt, etwa für den Treiber einer Grafikkarte oder für VirtualBox. Abschnitt 28.2 beweist, dass das Kompilieren von Modulen oder auch des gesamten Kernels keine Hexerei ist. Abschnitt 28.3 zeigt, wie Sie aus dem `/proc`- bzw. `/sys`-Dateisystem aktuelle Informationen über den Kernel ermitteln. Abschnitt 28.4 erklärt, wie Sie während des Rechnerstarts Optionen an den Kernel übergeben können. Und Abschnitt 28.5 beschreibt schließlich, wie Sie Kernelparameter im laufenden Betrieb verändern.

Es sollte klar sein, dass sich dieses Kapitel explizit an fortgeschrittene Linux-Anwender richtet. Linux-Einsteiger sind gut beraten, den für ihre Distribution vorgesehenen Kernel zu verwenden und nur zur Distribution passende Pakete zu installieren! Alle Informationen in diesem Kapitel gelten gleichermaßen für die Kernelversionen 2.6.*n* und 3.*n*.

28.1 Kernelmodule

Der Kernel ist jener Teil von Linux, der für elementare Funktionen wie Speicherverwaltung, Prozessverwaltung, Zugriff auf Festplatten und Netzwerkkarten etc. zuständig ist. Der Kernel verfolgt dabei ein modularisiertes Konzept: Anfänglich – also beim Hochfahren des Rechners – wird ein Basiskernel geladen, der nur jene Funktionen enthält, die zum Rechnerstart erforderlich sind.

Wenn im laufenden Betrieb Zusatzfunktionen benötigt werden, z. B. für spezielle Hardware, wird der erforderliche Code als Modul mit dem Kernel verbunden. Wer-

den diese Zusatzfunktionen eine Weile nicht mehr benötigt, kann das Modul wieder aus dem Kernel entfernt werden. Dieses modularisierte Konzept hat viele Vorteile:

- Kernelmodule können nach Bedarf eingebunden werden. Wenn ein bestimmtes Modul nur selten benötigt wird, kann so Speicher gespart werden, d. h., der Kernel ist nicht größer als unbedingt notwendig und optimal an die Hardware des Nutzers angepasst.
- Bei einer Änderung der Hardware (z. B. einer neuen Netzwerkkarte) muss kein neuer Kernel kompiliert, sondern nur das entsprechende Modul eingebunden werden. Alle gängigen Distributionen basieren auf diesem Konzept.
- Bei der Entwicklung eines Kernelmoduls muss nicht ständig der Rechner neu gestartet werden. Es reicht, ein Modul neu zu kompilieren. Anschließend kann es bei laufendem Betrieb getestet werden.

Eine Menge Hintergrundinformationen zum Umgang mit Kernelmodulen finden Sie auf der folgenden Seite:

http://www.tldp.org/HOWTO/Module-HOWTO

Module automatisch laden

Dafür, dass Kernelmodule tatsächlich automatisch geladen werden, sobald sie benötigt werden, ist die in den Kernel integrierte Komponente `kmod` verantwortlich. `kmod` wird durch die Datei `/etc/modprobe.conf` gesteuert. Diese Konfigurationsdatei wird etwas weiter unten genauer beschrieben.

Kernel und Module müssen zusammenpassen

Bis zur Kernelversion 2.6.15 mussten der Kernel und seine Module exakt zusammenpassen: Es war nicht möglich, ein Modul zu laden, das für eine andere, vielleicht nur geringfügig veränderte Kernelversion kompiliert wurde. Aus diesem Grund gibt es für jede Kernelversion ein eigenes Modulverzeichnis `/lib/modules/`*`kernelversion`*. Gerade bei Modulen, die nicht unmittelbar mit der Distribution mitgeliefert werden, stellt die strikte Versionsabhängigkeit oft ein Problem dar. Das betrifft z. B. die Kernelmodule für die Grafiktreiber von ATI/AMD und NVIDIA.

Module Versioning

Seit der Kernelversion 2.6.16 bringt der Mechanismus des *Module Versioning* eine gewisse Besserung: Zusammen mit dem Modul werden Zusatzinformationen gespeichert, die Aufschluss darüber geben, ob eine Zusammenarbeit zwischen dem Modul und dem Kernel auch bei unterschiedlicher Versionsnummer möglich ist. Damit können oft auch nicht zur Kernelversion passende Module genutzt werden. Dieser Mechanismus funktioniert allerdings nur, wenn das Module Versioning beim Kompilieren aktiviert wurde und wenn es zwischen der Kernel- und der Modulversion keine Änderungen an den Schnittstellen gegeben hat.

Wenn Sie unter SUSE eigene Kernelmodule kompilieren möchten, die Module Versioning unterstützen, müssen Sie vorher das Paket `kernel-syms` installieren. Module

Versioning ist auch unter dem Namen *Kernel Symbol Versions* oder *Modversions* bekannt. Im Detail ist der Mechanismus hier beschrieben:

http://www.oreilly.de/german/freebooks/linuxdrive2ger/kerver.html

Kommandos zur Modulverwaltung

Alle gängigen Distributionen sind so eingerichtet, dass Module bei Bedarf automatisch geladen werden. Ein Beispiel: Sie binden mit `mount` das Dateisystem eines USB-Sticks in den Verzeichnisbaum ein. Daraufhin wird automatisch das `vfat`-Modul aktiviert, das zum Lesen des Dateisystems erforderlich ist.

Im Regelfall erfolgt die Modulverwaltung also automatisch und transparent, ohne dass Sie mit den im Folgenden beschriebenen Kommandos zur manuellen Modulverwaltung eingreifen müssen. Dennoch sollten Sie die Modulkommandos kennen, um Module zur Not auch manuell laden zu können.

Alle Module befinden sich im Verzeichnis `/lib/modules/`*n*. Dabei ist *n* die Version des laufenden Kernels. Moduldateien haben die Dateiendung `*.ko`.

Kernelversion ermitteln

Das Kommando `uname -r` liefert die Versionsnummer des laufenden Kernels:

```
user$  uname -r
3.9.0-6-generic
```

Moduldatei laden

`insmod` integriert das angegebene Modul in den Kernel. Dabei muss der vollständige Dateiname übergeben werden. Zusätzlich können Parameter (Optionen) an das Modul übergeben werden. Falls Sie hexadezimale Werte angeben möchten, müssen Sie 0x voranstellen, also etwa `option=0xff`.

```
root#  insmod /lib/modules/3.9.0-6-generic/kernel/fs/fuse/fuse.ko
```

`insmod -f` versucht das Modul selbst dann zu laden, wenn es nicht zur laufenden Kernelversion passt. Ob das tatsächlich funktioniert, hängt davon ab, ob es zwischen der Kernel- und der Modulversion irgendwelche Inkompatibilitäten gibt.

Normalerweise werden Sie Kernelmodule nicht mit `insmod` laden, sondern mit `modprobe`. Dieses Kommando bietet im Vergleich zu `insmod` gleich mehrere Vorteile:

- `modprobe` sucht die Moduldatei selbst, d. h., Sie müssen nur den Modulnamen angeben. Bei Modulen, die schon beim Kompilieren in den Kernel integriert wurden, endet `modprobe` ohne Fehlermeldung.
- `modprobe` lädt gegebenenfalls auch alle Module, die als Voraussetzung für das gewünschte Modul benötigt werden.
- `modprobe` berücksichtigt alle in `/etc/modprobe.conf` angegebenen Moduloptionen.

`modprobe` setzt allerdings eine korrekte Modulkonfiguration durch die Dateien `modprobe.conf` und `modules.dep` voraus.

```
root#  modprobe fuse
```

Liste der geladenen Module

`lsmod` liefert eine normalerweise recht lange Liste aller momentan geladenen Kernelmodule. Beachten Sie, dass `lsmod` in den Kernel einkompilierte Module nicht anzeigt, sondern nur solche Module, die nachträglich geladen wurden!

```
root#  lsmod | sort
Module                  Size  Used by
ac                      4933  0
autofs4                19013  1
battery                 9285  0
bluetooth              44069  5 hidp,rfcomm,l2cap
button                  6609  0
...
fuse                   36313  0
...
```

Module entfernen

`rmmod` entfernt das angegebene Modul wieder aus dem Kernel und gibt den belegten Speicher frei. Das Kommando kann nur erfolgreich ausgeführt werden, wenn das Modul gerade nicht verwendet wird.

```
root#  rmmod fuse
```

Modulinformationen

`modinfo` liefert eine Menge Informationen über ein Modul. Das Modul muss sich nicht im Kernel befinden. Das folgende Beispiel zeigt die Daten für das Modul `e1000`. Dabei handelt es sich um den Treiber für Intel-Netzwerkadapter.

```
root#  modinfo e1000
filename:       /lib/modules/3.9.0-6-generic/kernel/drivers/net/ethernet
                /intel/e1000/e1000.ko
version:        7.3.21-k8-NAPI
license:        GPL
description:    Intel(R) PRO/1000 Network Driver
author:         Intel Corporation, <linux.nics@intel.com>
...
depends:
vermagic:       3.5.0-1.1-desktop SMP preempt mod_unload modversions
parm:           TxDescriptors:Number of transmit descriptors (array of int)
parm:           RxDescriptors:Number of receive descriptors (array of int)
...
```

Modulkonfiguration

Die Modulverwaltung funktioniert scheinbar wie von Zauberhand:

- Wenn Sie eine zusätzliche Partition in das Dateisystem einbinden und dabei ein bisher nicht genutztes Dateisystemformat zum Einsatz kommt, wird automatisch das Modul für dieses Dateisystem geladen.
- Wenn sich die Partition auf einer SATA-Festplatte befindet, werden auch die SATA-Module aktiviert, sofern diese nicht ohnedies schon geladen sind.
- Während der Initialisierung der Netzwerkfunktionen wird automatisch der erforderliche Treiber für Ihre Netzwerkkarte geladen etc.

Für das automatische Laden von Kernelmodulen ist die in den Kernel integrierte Komponente `kmod` verantwortlich. Dafür, dass all das funktioniert, sorgen unterschiedliche Konfigurationsmechanismen:

- **Für den Rechnerstart erforderliche Module:** Manche Kernelmodule werden sofort beim Start des Rechners benötigt – etwa Module zum Zugriff auf das Dateisystem. Soweit diese Module nicht integrale Bestandteile des Kernels sind, müssen sie in einer Initrd-Datei durch GRUB beim Rechnerstart an den Kernel übergeben werden (siehe Abschnitt 28.4).
- **Module für Grundfunktionen:** Die Module für die Basisverwaltung von Hardware-Komponenten (z. B. für das USB-System) werden von verschiedenen Scripts des Init-Prozesses direkt durch `modprobe`-Anweisungen geladen.
- **Module für Schnittstellen:** Eine Reihe weiterer Module wird dann geladen, wenn eine Schnittstelle zum ersten Mal benutzt wird. Hier tritt allerdings das Problem auf, dass es für manche Schnittstellen je nach der eingesetzten Hardware unterschiedliche Module gibt. Wenn Sie also die Schnittstelle `eth0` für die erste Netzwerkkarte im Rechner ansprechen, muss das zu dieser Karte passende Modul geladen werden.

  Da der Kernel nicht hellsehen kann, benötigt er eine Information darüber, welches Modul das richtige ist. Diese Information befindet sich in `/etc/modprobe.conf` sowie in den Dateien des Verzeichnisses `/etc/modprobe.d`. Dort befinden sich installations- oder distributionsspezifische Optionen sowie Anweisungen, welche Module *nicht* automatisch zu laden sind (`blacklist`-Datei).

  Auch die automatische Device-Verwaltung durch das `udev`-System lädt bei Bedarf die notwendigen Module. Die entsprechenden Regeln finden Sie in `/etc/udev/rules.d`.

- **Module für USB- und Firewire-Geräte etc.:** Derartige Hardware-Komponenten nehmen eine Sonderrolle ein. Mehrere `*.*map`-Dateien in `/lib/modules/`*`kernelversion`*`/` entscheiden anhand der Identifikationscodes der Komponenten darüber, welches Modul geladen wird.
- **Modulabhängigkeiten:** Eine Menge Module sind voneinander abhängig. Beispielsweise funktioniert das Modul `nfs` für das NFS-Dateisystem nur, wenn auch die Module `lockd`, `nfs_acl` und `sunrpc` geladen sind. Derartige Modulabhängigkeiten sind zentral in der Datei `/lib/modules/`*`n`*`/modules.dep` verzeichnet.

Module beim Rechnerstart laden

Manchmal wollen Sie unabhängig von den hier zusammengefassten Konfigurationswegen erreichen, dass beim Rechnerstart ein bestimmtes Kernelmodul geladen wird – und das, ohne sich auf irgendwelche Automatismen zu verlassen. Die optimale Vorgehensweise hängt von Ihrer Distribution ab.

Besonders einfach ist es bei Debian und Ubuntu: Dort kümmert sich das Init-V-Script `/etc/init.d/module-init-tools` darum, alle in `/etc/modules` zeilenweise aufgelisteten Module zu laden. Sie müssen also lediglich das gewünschte Modul in einer neuen Zeile in `/etc/modules` angeben.

Bei den meisten anderen Distributionen fügen Sie `modprobe modulname` in ein für lokale Anpassungen vorgesehenes Init-V-Script ein. Beachten Sie aber, dass die Module damit je nach Distribution erst zum Ende des Init-Prozesses geladen werden – also zu einem Zeitpunkt, zu dem es für manche System- und Netzwerkprozesse schon zu spät ist.

Red Hat, Fedora:	`/etc/rc.d/rc.local`
SUSE:	`/etc/init.d/boot.local`

modprobe-Syntax

Die folgenden Absätze beschreiben die wichtigsten Schlüsselwörter für `modprobe.conf` bzw. die Dateien in `modprobe.d/`. Weitere Details liefert `man modprobe.conf`.

alias

`alias`-Anweisungen geben an, welche Kernelmodule für welche Devices eingesetzt werden. Ein Beispiel: Für das Device `/dev/eth0` soll das Modul `8139too` verwendet werden.

```
alias eth0 8139too
```

Der Zugriff auf viele Hardware-Komponenten erfolgt durch block- und zeichenorientierte Device-Dateien im `/dev`-Verzeichnis. Aus der Sicht des Kernels werden diese Device-Dateien nicht durch ihren Namen, sondern durch die Major- und Minor-Device-Nummer charakterisiert (siehe auch Abschnitt 15.9). Zahlreiche `alias`-Anweisungen stellen den Zusammenhang zwischen Device-Nummern und Modulen

her. Analog sieht auch die Definition von Netzwerkprotokollen aus: Zur Nutzung eines bestimmten Protokolls sucht der Kernel nach einer Protokollfamilie mit dem Namen `net-pf-n`. Das folgende Beispiel bewirkt, dass für die Protokollfamilie 5 das AppleTalk-Modul geladen wird:

```
alias net-pf-5 appletalk
```

Wenn Sie dieses Protokoll nicht brauchen und womöglich das entsprechende Modul gar nicht installiert ist, erspart Ihnen die folgende Anweisung lästige Fehlermeldungen:

```
alias net-pf-5 off
```

options

`options`-Anweisungen geben an, mit welchen Optionen ein bestimmtes Modul geladen werden soll. Die folgende Anweisung bewirkt, dass das Modul `ne` (für NE-2000-kompatible Ethernet-Karten) mit der Option `io=0x300` geladen wird:

```
options ne io=0x300
```

include

`include`-Anweisungen laden weitere Konfigurationsdateien.

install

Mit `install`-Anweisungen geben Sie Kommandos an, die ausgeführt werden, anstatt das betreffende Modul einfach zu laden. Auch hierzu sehen Sie ein Beispiel, das aus Platzgründen auf zwei Zeilen verteilt wurde. Wenn das ALSA-Modul `snd` benötigt wird, sollen die folgenden Kommandos ausgeführt werden:

```
install snd modprobe --ignore-install snd $CMDLINE_OPTS && \
  { modprobe -Qb snd-ioctl32 ; : ; }
```

remove

Mit `remove` geben Sie Kommandos an, die beim Entfernen eines Moduls ausgeführt werden sollen.

blacklist

`blacklist` bewirkt, dass modulinterne Alias-Definitionen nicht berücksichtigt werden. `blacklist`-Anweisungen befinden sich üblicherweise in der Datei `/etc/modprobe.d/blacklist`. Sie enthält Module, die beispielsweise wegen Kompatibilitätsproblemen oder aufgrund von besseren Alternativen *nicht* geladen werden sollen. Beispielsweise verhindert die folgende Zeile, dass das Modul `usbmouse` geladen wird:

```
blacklist usbmouse
```

Ein zusätzliches Modul kompilieren

Wenn Sie Linux in Kombination mit VirtualBox einsetzen, die binären Grafiktreiber von ATI oder NVIDIA nutzen möchten oder ein anderes hardware-spezifisches Kernelmodul brauchen, das im Kernel Ihrer Distribution fehlt, müssen Sie das Modul passend zum laufenden Kernel kompilieren.

Entwicklungswerkzeuge

Zum Kompilieren eines Moduls sind neben dem C-Compiler `gcc` und `make` auch weitere grundlegende Entwicklungswerkzeuge erforderlich. Die meisten Distributionen erleichtern die Sache durch fertige Paketselektionen oder Meta-Pakete, die auf alle relevanten Pakete verweisen (siehe Tabelle 28.1).

Distribution	Kommando
Debian, Ubuntu	`apt-get install build-essential`
Fedora	`yum groupinstall development-tools`
SUSE	`zypper install -t pattern devel_basis`

Tabelle 28.1 Kommandos zur Installation grundlegender Entwicklungswerkzeuge

Kernel-Include-Dateien

Außerdem brauchen Sie zumindest die Include-Dateien (Header-Dateien) zum aktuellen Kernel. Diese Dateien sind Teil des Kernelcodes. Bei vielen Distributionen (aber nicht bei SUSE) befinden sich die Include-Dateien und der Rest des Codes in zwei getrennten Paketen. Das hat den Vorteil, dass Sie nicht gleich den riesigen Kernelcode installieren müssen, wenn Sie nur die vergleichsweise kleinen Include-Dateien brauchen.

Tabelle 28.2 gibt an, in welchen Paketen sich die Include-Dateien des Kernels bei den gängigen Distributionen befinden und wohin diese Dateien installiert werden. *n.n* ist dabei ein Platzhalter für die installierte Kernelversion. Diese Information ermitteln Sie mit dem Kommando `uname -a`.

Distribution	Paket	Pfad
Debian	`linux-headers-arch`	`/usr/include/linux`
Fedora, RHEL	`kernel-[PAE-]devel-n.n`	`/lib/modules/`*n.n*`/build/include`
SUSE	`kernel-devel`	`/usr/src/linux-`*n.n*`/include`
Ubuntu	`linux-headers-generic`	`/usr/include/linux`

Tabelle 28.2 Pakete mit den Kernel-Header-Dateien

Wenn Sie den Kernel selbst kompilieren (siehe den nächsten Abschnitt), landen die zum Kernel passenden Include-Dateien automatisch im Verzeichnis `/lib/modules/`*n.n*`/build/include`.

PAE

PAE steht für *Physical Address Extension* und ist ein Mechanismus, um mit 32-Bit-CPUs mehr als 4 GByte RAM zu nutzen. Die Aktivierung von PAE hat unabhängig von der Bit-Anzahl der CPU und dem verfügbaren RAM einen zweiten Vorteil: Nur mit PAE kann das Schutzsystem *No Execute* (NX) genutzt werden. NX verhindert, dass bei einem Pufferüberlauf Code aus dem Datenbereich eines Programms ausgeführt wer-

den kann. Aus diesem Grund läuft bei den meisten 32-Bit-Distributionen ein Kernel mit PAE-Unterstützung.

Modul kompilieren

Die meisten Programme, die eigene Kernelmodule benötigen, enthalten ein Installations-Script, das sich um das Kompilieren und Einrichten des Moduls kümmert. Das gilt beispielsweise für VMware, VirtualBox, die Grafiktreiber von ATI/AMD und NVIDIA etc. Bei manchen Distributionen ist der Prozess sogar dahingehend automatisiert, dass nach jedem Kernel-Update automatisch das Modul neu kompiliert wird (siehe *DKMS* etwas weiter unten).

Wenn Sie dagegen den Quellcode für eine noch nicht offiziell unterstützte Hardware-Komponente heruntergeladen haben, müssen Sie sich um den Kompilierprozess selbst kümmern. Dazu führen Sie in der Regel die folgenden Kommandos aus. Nur das letzte `make`-Kommando erfordert `root`-Rechte.

```
user$  cd quellcodeverzeichnis
user$  make clean
user$  make
root#  make install
```

DKMS

DKMS steht für *Dynamic Kernel Module Support* und hilft dabei, nach einem Kernel-Update selbst kompilierte Kernelmodule automatisch zu aktualisieren. DKMS besteht aus einigen Shell-Scripts und wurde von Dell entwickelt. Entsprechende `dkms`-Pakete stehen gegenwärtig für die Distributionen Debian, Fedora und Ubuntu zur Verfügung.

Um DKMS zu nutzen, muss der Quellcode des Moduls in einem Verzeichnis der Form `/usr/src/`*`name-version`* installiert werden. Das Verzeichnis muss die Datei `dkms.conf` enthalten, die DKMS erklärt, wie es mit dem Code umgehen soll. Die folgenden Zeilen stammen vom NVIDIA-Treiber für Ubuntu, wobei ich die Formatierung des Listings ein wenig geändert habe, um die Lesbarkeit zu verbessern.

```
# Datei /usr/src/nvidia-304-304.88/dkms.conf
PACKAGE_NAME            = "nvidia-304"
PACKAGE_VERSION         = "304.88"
CLEAN                   = "make clean"
BUILT_MODULE_NAME[0]    = "nvidia"
DEST_MODULE_NAME[0]     = "nvidia_304"
MAKE[0]                 = "make module KERNDIR = /lib/modules/$kernelver
                           IGNORE_XEN_PRESENCE=1 IGNORE_CC_MISMATCH=1
                           SYSSRC=$kernel_source_dir LD=/usr/bin/ld.bfd"
DEST_MODULE_LOCATION[0] = "/kernel/drivers/char/drm"
AUTOINSTALL             = "yes"
PATCH[0]                = "allow_sublevel_greater_than_5.patch"
PATCH[1]                = "buildfix_kernel_3.10.patch"
PATCH_MATCH[1]          = "^3.10"
```

Sind diese Voraussetzungen erfüllt, übergeben Sie das Kernelmodul mit `dkms add` der Kontrolle von DKMS, kompilieren es mit `dkms build` für den aktuellen Kernel und installieren es mit `dkms install`. In Zukunft geschieht dies bei Kernel-Updates automatisch. Die folgenden Beispiele beziehen sich wieder auf den NVIDIA-Kerneltreiber. Die Kommandos werden bei der Installation des Ubuntu-Pakets des Treibers automatisch ausgeführt. Nach meinen Erfahrungen funktioniert dieser Automatismus oft, aber leider nicht immer. Insbesondere die automatische Aktualisierung von Gast-Treibern in virtuellen Maschinen scheitert auf meinen Testsystemen häufig.

```
root#  dkms add     -m nvidia-current -v 304-304.88
root#  dkms build   -m nvidia-current -v 304-304.88
root#  dkms install -m nvidia-current -v 304-304.88
```

`dkms status` bzw. ein Blick in das Verzeichnis `/var/lib/dkms` verrät, welche Kernelmodule sich momentan unter der Kontrolle von DKMS befinden.

Weitere Informationen zu DKMS geben `man dkms` und die folgenden Webseiten:

http://www.linuxjournal.com/article/6896
http://wiki.centos.org/HowTos/BuildingKernelModules

DKMS unter Debian und Ubuntu

Bei Debian und Ubuntu gibt es eine ganze Reihe von `xxx-name-dkms`-Paketen, mit denen Kernelmodule für Hardware-Treiber kompiliert werden können:

```
root#  apt-cache --names-only search '.*-dkms' | sort
```

Bei Debian befinden sich die Pakete zum Teil in den Paketquellen *contrib* und *non-free*, die Sie vorher aktivieren müssen. Die Installation eines Kernelmoduls sieht dann wie folgt aus, wobei Sie einfach `nvidia` durch den Namen des gewünschten Treibers und `amd64` durch Ihre CPU-Architektur ersetzen:

```
root#  apt-get update
root#  apt-get install linux-headers-amd64 nvidia-kernel-dkms
```

Im Rahmen der Installation werden alle abhängigen Pakete installiert, das Kernelmodul kompiliert und als DKMS-Modul eingerichtet. Bei zukünftigen Kernel-Updates wird somit automatisch eine neue Version des Moduls erzeugt.

DKMS oder module-assistant?

Vor allem in Debian kamen zum Kompilieren von Kernelmodulen in der Vergangenheit häufig die Werkzeuge aus dem Paket `module-assistant` zum Einsatz. Das gleichnamige Kommando bzw. dessen Kurzform `m-a` existiert weiterhin; nach Möglichkeit sollten Sie aber DKMS-Pakete vorziehen!

28.2 Kernel selbst konfigurieren und kompilieren

Der durchschnittliche Linux-Anwender muss seinen Kernel nicht selbst kompilieren. Bei allen aktuellen Distributionen werden ein brauchbarer Standardkernel und eine umfangreiche Sammlung von Modulen mitgeliefert. Dennoch kann es Gründe geben, den Kernel neu zu kompilieren:

- Sie wollen Ihr System besser kennenlernen. Das Motto dieses Buchs ist es ja, Ihnen auch einen Blick hinter die Linux-Kulissen zu ermöglichen.
- Sie brauchen besondere Funktionen, die weder in den mitgelieferten Kernel integriert sind noch als Modul vorliegen.
- Sie möchten eine aktuellere Version des Kernels verwenden als die, die mit Ihrer Distribution mitgeliefert wurde.
- Sie möchten selbst an der Kernelentwicklung teilnehmen und daher mit dem neuesten Entwicklerkernel experimentieren.
- Sie wollen in Ihrem Bekanntenkreis mit Insider-Wissen auftrumpfen: »Ich habe den neuesten Linux-Kernel selbst kompiliert!«

Hürden

Es gibt allerdings gewichtige Gründe, die gegen das Kompilieren eines eigenen Kernels sprechen:

- Die meisten Distributionen verwenden nicht den Originalkernel, wie er von Linus Torvalds freigegeben wird, sondern eine gepatchte Version mit diversen Zusatzfunktionen, wobei natürlich jede Distribution andere Patches verwendet – siehe auch Abschnitt 28.2. An sich ist das eine feine Sache für den Anwender: Er bekommt auf diese Weise Zusatzfunktionen, von denen der Distributor glaubt, dass sie schon ausreichend stabil funktionieren. Wenn Sie sich nun aber selbst den Quellcode des Originalkernels herunterladen, fehlen diese Patches. Einzelne Funktionen Ihrer Distribution, die bisher einwandfrei gearbeitet haben, machen plötzlich Probleme oder funktionieren gar nicht mehr.
- Das Kompilieren eines eigenen Kernels ist nicht schwierig. Schwierig ist aber die vorherige Konfiguration des Kompilationsprozesses. Dabei stehen Tausende von Optionen zur Auswahl. Sie können mit diesen Optionen beeinflussen, welche Funktionen direkt in den Kernel integriert werden, welche als Module und welche gar nicht zur Verfügung stehen sollen. Wenn Sie sich – mangels Detailwissen – für die falschen Optionen entscheiden, ist das Ergebnis wie oben: Einzelne Funktionen verweigern den Dienst, und es ist relativ schwierig, die Ursache herauszufinden. Gerade für Linux-Einsteiger ist es praktisch unmöglich, die richtigen Einstellungen für alle Optionen richtig zu erraten.

Aus diesen Gründen verweigern die meisten Distributoren jeden Support, wenn Sie nicht den mit der Distribution mitgelieferten Kernel verwenden. Lassen Sie sich von diesen Warnungen aber nicht abschrecken, es einmal selbst zu versuchen. Wenn Sie nach der in Abschnitt 28.2 präsentierten Anleitung vorgehen, können Sie Ihren Rechner anschließend sowohl mit dem alten als auch mit dem neuen Kernel hochfahren – es kann also nichts passieren!

Entwicklungswerkzeuge

Zur Kompilierung des Kernels sind dieselben Entwicklungswerkzeuge wie zum Kompilieren eines einzelnen Moduls erforderlich (siehe Abschnitt 28.1).

Grundlagen

Kernelversionen

Bis zur Kernelversion 2.6.0 gab es »stabile« Kernelversionen (2.0.*n*, 2.2.*n*, 2.4.*n*) und sogenannte Entwickler- bzw. Hacker-Kernel (2.3.*n*, 2.5.*n* etc.). Die meisten Linux-Distributionen verwendeten stabile Kernelversionen, während die Entwicklerkernel für Programmierer gedacht waren, die sich an der Kernelentwicklung beteiligen. Neue Funktionen wurden zuerst im Hacker-Kernel getestet, bevor sie später in die nächste stabile Kernelgeneration Einzug hielten.

Mit Kernel 2.6 hat sich das Entwicklungsmodell geändert. Es gab keinen Hacker-Kernel 2.7.*n* mehr. Stattdessen erfolgt die Weiterentwicklung direkt in den 2.6.*n*-Versionen. Man könnte sagen, dass jede neue Kernelversion vorerst als Hacker-Kernel gilt; erst wenn Linus Torvalds entscheidet, dass die Version zuverlässig läuft, wird sie als stabile Version freigegeben. Der Hauptvorteil besteht darin, dass Neuerungen von wesentlich mehr Entwicklern getestet werden und viel schneller allgemein verfügbar werden.

Sollten in der jeweils letzten freigegebenen Kernelversion offensichtliche Fehler oder Sicherheitsmängel auftreten, werden diese in Zusatzversionen mit einer vierten Versionsnummer behoben. Daraus ergeben sich dann Kernelversionen wie 2.6.21.4.

Kernel 3.*n*

Im Frühjahr 2011 hat Linus Torvalds etwas überraschend festgestellt, dass es Zeit für eine neue Kernelnummerierung sei. Deswegen folgte auf Kernel 2.6.39 die Version 3.0. Die weiteren Versionen bekamen die Nummern 3.1, 3.2, 3.3 etc. Mit den weiterhin erforderlichen Updates ergeben sich dadurch Versionsnummern in der Art 3.5.4. Das ist ein gewisser Fortschritt, weil die Versionsnummer nun nur noch aus drei Teilen besteht und nicht mehr wie bisher aus vier. Ansonsten gingen mit dem neuen Nummerierungsschema keine grundlegenden Neuerungen einher – weder funktionell noch im Entwicklungsprozess.

Ksplice

Die meisten Updates eines Linux-Systems können im laufenden Betrieb erfolgen. Aktualisierte Netzwerkdienste müssen zwar anschließend neu gestartet werden, aber es besteht keine Notwendigkeit, den ganzen Rechner neu zu starten. Eine Ausnahme von dieser Regel ist der Kernel: Damit Sicherheits-Updates im Kernel wirksam werden, müssen Sie einen neuen Kernel und neue Module installieren und den Rechner anschließend neu starten. Auf Desktop-Rechnern, die üblicherweise jeden Tag ein- und ausgeschaltet werden, ist das egal. Aber bei Servern, die möglichst ohne Unterbrechung ständig verfügbar sein sollen, ist ein Neustart immer unerwünscht.

Abhilfe verspricht die Funktion Ksplice: Bei vielen Updates ist es möglich, die betreffende Kernelfunktion im laufenden Betrieb zu deaktivieren und durch neuen Code zu ersetzen. Die nicht eben trivialen technischen Hintergründe des Verfahrens sind auf den beiden folgenden Seiten beschrieben:

http://www.ksplice.com
http://lwn.net/Articles/340477

Mitte 2011 übernahm Oracle die Firma Ksplice. Kernel-Updates für Oracle Linux erfolgen zumindest teilweise mit Ksplice, was ein durchaus gewichtiges Unterscheidungsmerkmal zu Red Hat Enterprise Linux ist.

Statistik

Der Kernel besteht zurzeit (Version 3.11) aus mehr als 17 Millionen Zeilen Code, der Großteil davon ist in C geschrieben, ein kleiner Teil in Assembler. Wenn Sie wissen möchten, wer bzw. welche Firmen zur Kernelentwicklung beitragen, verfolgen Sie einfach die Linux-News-Site *lwn.net*. Dort finden Sie zu jedem Kernel-Release eine statistische Aufarbeitung, wer die meisten Änderungen durchgeführt hat.

http://lwn.net/Articles/563977 (für Version 3.11)

Links

Tipps zur Kompilierung des Kernels finden Sie auch auf den folgenden Seiten:

http://kernelnewbies.org/FAQ
http://www.tux.org/lkml

Wenn Sie sich für technische Interna interessieren, sind die Dokumentationsdateien des Kernelcodes sehr aufschlussreich. Gerade neue Funktionen des Kernels werden zuerst hier beschrieben, noch bevor die entsprechenden `man`-Seiten aktualisiert werden:

http://www.kernel.org/doc/Documentation

Kernelcode installieren

Der Quellcode für den Kernel befindet sich üblicherweise im Verzeichnis `/usr/src/linux`; nur bei Red Hat und Fedora gibt es abweichende Gepflogenheiten, die weiter unten behandelt werden. Falls dieses Verzeichnis leer ist, haben Sie den Kernelcode nicht installiert. Sie können nun wahlweise den Kernelquellcode Ihrer Distribution installieren oder den gerade aktuellen offiziellen Kernelcode herunterladen. Weniger Probleme bereitet zumeist die erste Variante, insbesondere für Einsteiger.

Beachten Sie, dass der Platzbedarf für den Kernelcode beachtlich ist: Die komprimierten Quellcodepakete sind mehr als 70 MByte groß. Nach dem Entpacken beträgt der Platzbedarf ca. weitere 500 MByte, und nach dem Kompilieren mit den dadurch resultierenden Binärdateien über vier GByte!

Kernelcode der Distribution installieren

Bei den meisten Distributionen gibt es ein eigenes Paket, das den Kernelquellcode enthält. Tabelle 28.3 gibt für einige gängige Distributionen an, in welchen Paketen sich der Kernelcode befindet. Dabei ist *n.n* ein Platzhalter für die installierte Kernelversion.

Distribution	Paket
Debian, Ubuntu	`linux-source-n.n`
Fedora, Red Hat	`kernel-n.n` (Quellcodepaket!)
SUSE	`kernel-source`

Tabelle 28.3 Pakete mit dem Kernelquellcode

Bei Debian und Ubuntu wird der Kernelcode als `tar`-Archiv in das Verzeichnis `/usr/src` installiert. Sie müssen das Archiv selbst mit `tar xJf linux-n.n.tar.xz` auspacken. Die Kennung `.xz` deutet darauf hin, dass der Quellcode mit dem besonders effizienten XZ-Verfahren komprimiert wurde.

Fedora

Für Fedora und Red Hat gelten einige Besonderheiten: Zum einen befindet sich der Kernelcode nicht in einem gewöhnlichen Paket, sondern in einem Quellcodepaket. Zum anderen empfehlen die Fedora-Richtlinien die Installation des Quellcodes nicht in `/usr/src`, sondern in das Unterverzeichnis `rpmbuild` des Heimatverzeichnisses. Das ermöglicht es, den Kernel ohne `root`-Rechte zu kompilieren.

Insgesamt ist die Vorgehensweise aber etwas umständlicher: Zuerst installieren Sie die Pakete `yumutils` und `rpmdevtools`; sie enthalten die Kommandos `yumdownloader` und `rpmdev-setuptree` sowie diverse Kommandos zur Erzeugung von RPM-Paketen. `rpmdev-setuptree` erzeugt das Verzeichnis `rpmbuild` und darin wiederum diverse Unterverzeichnisse. `yumdownloader` lädt das Quelltextpaket `kernel-n.n.src.rpm` herunter.

```
user$  su -c 'yum install yumutils rpmdevtools'
user$  rpmdev-setuptree
user$  yumdownloader --source kernel
```

`yum-builddep` installiert alle noch fehlenden Pakete, die zur Kompilierung des Kernels erforderlich sind. `rpm -i` packt das Kernelpaket aus. Das Archiv des Kernelquellcodes (Datei `linux-n.n.tar.xz`) sowie alle Fedora-spezifischen Patches landen damit im Verzeichnis `rpmbuild/SOURCES`. Fehlermeldungen der Art *Benutzer mockbuild existiert nicht - benutze Root* können Sie dabei ignorieren. `rpmbuild` extrahiert daraus den Quellcode und wendet alle Red-Hat- bzw. Fedora-spezifischen Patches an:

```
user$  su -c 'yum-builddep kernel-n.n.src.rpm'
user$  rpm -i kernel-n.n.src.rpm
user$  cd ~/rpmbuild/SPECS
user$  rpmbuild -bp --target=$(uname -m) kernel.spec
```

Anschließend finden Sie den Originalquellcode und den für Fedora gepatchten Quellcode in den folgenden Verzeichnissen:

`~/rpmbuild/BUILD/kernel-n.n/vanilla-n.n` (Orginalquellcode)
`~/rpmbuild/BUILD/kernel-n.n/linux-n.n` (Quellcode mit Fedora-Patches)

Um den Platzbedarf zu minimieren, sind identische Dateien durch Hardlinks verknüpft und somit nur einmal physikalisch gespeichert. Weitere Fedora-spezifische Tipps zum Kompilieren eines eigenen Kernels finden Sie auf der folgenden Webseite.

http://fedoraproject.org/wiki/Docs/CustomKernel

Dort ist insbesondere beschrieben, wie Sie vorgehen, damit der neue Kernel nach dem Kompilieren gleich in ein RPM-Paket verpackt wird.

Offiziellen Kernelcode installieren

Der mit der Distribution mitgelieferte Kernel ist oft schon veraltet. Den aktuellen Kernelcode in Form von komprimierten `tar`-Archiven finden Sie z. B. hier:

http://www.kernel.org
ftp://ftp.kernel.org/pub/linux/kernel

Ein typischer Dateiname für das Kernelarchiv ist etwa `linux-3.9.2.tar.xz` (Größe ca. 75 MByte). Zur Installation wechseln Sie in das Verzeichnis `/usr/src` und führen das folgende Kommando aus:

```
root#  cd /usr/src
root#  tar xJf linux-3.9.2.tar.xz
```

Die Installation erfolgt in das Verzeichnis `/usr/src/`. Um den Zugriff auf dieses Verzeichnis zu vereinfachen, zeigt normalerweise der Link `/usr/src/linux` auf das aktuelle Quellcodeverzeichnis:

```
root#  ln -s linux-3.9.2 linux
```

Kernelcode aktualisieren (patchen)

Mit sogenannten Patch-Dateien können Sie einen Versionswechsel von einer Version zu einer anderen durchführen. Patches sind komprimierte Textdateien, die angeben, in welchen Dateien welche Änderungen durchgeführt werden sollen. Patches sparen insbesondere bei kleinen Versionswechseln eine Menge Download-Volumen. Patches funktionieren allerdings nur dann, wenn sie auf die dafür gedachte (unveränderte!) Codebasis angewendet werden.

Die richtige Patch-Reihenfolge

Nehmen wir an, Sie wollen den Code von 3.9.5 auf 3.9.6 aktualisieren: Naheliegend wäre es, einfach den Patch 3.9.6 anzuwenden. Das funktioniert so aber nicht, weil der Patch 3.9.6 als Basis den unveränderten Code 3.9 erwartet (nicht 3.9.5!). Daher müssen Sie auch den Patch 3.9.5 herunterladen und diesen invers anwenden (Option `-R`), um von 3.9.5 zurück zur Codebasis 3.9 zu gelangen. Erst jetzt funktioniert der Patch 3.9.6!

Das `patch`-Kommando wird normalerweise in Kombination mit `bunzip2` eingesetzt. `bunzip2` dekomprimiert den Patch, `patch` führt die Änderungen aus. Falls die Patch-Datei unkomprimiert vorliegt, lautet das Patch-Kommando `patch -p1 < patchdatei`.

Generell sollten Sie vor der Anwendung jedes Patches mit der Option `--dry-run` sicherstellen, dass dabei keine Probleme auftreten. Nichts ist ärgerlicher als ein fehlerhaft oder nur teilweise angewendeter Patch!

Die Patches verändern nur den Code, nicht aber den Namen des Verzeichnisses, in dem sich der Code befindet. Um Verwirrung zu vermeiden, sollten Sie anschließend auch das Codeverzeichnis umbenennen. Die tatsächliche Versionsnummer können Sie der Datei `Makefile` direkt im Quellcodeverzeichnis entnehmen.

```
root#  cd /usr/src/linux-3.9.5
root#  bunzip2 -c patch-3.9.5.xz | patch -R -p1 --dry-run  (Invers-Patch testen)
... keine Fehlermeldungen
root#  bunzip2 -c patch-3.9.5.xz | patch -R -p1           (3.9.5 --> 3.9)
root#  bunzip2 -c patch-3.9.6.xz | patch -p1 --dry-run    (Patch testen)
... keine Fehlermeldungen
root#  bunzip2 -c patch-3.9.6.xz | patch -p1              (3.9 --> 3.9.6)
root#  cd /usr/src
root#  mv linux-3.9.5 linux-3.9.6
```

Funktions-Patches

Neben den gerade beschriebenen Update-Patches gibt es auch Patches mit inoffiziellen Zusatzfunktionen, die aus den verschiedensten Gründen noch nicht in den Standardkernel integriert sind (Funktions-Patches).

Grundsätzlich werden auch Funktions-Patches mit `patch` auf den Kernelcode angewendet. Allerdings müssen Sie darauf achten, dass Sie dieselbe Codebasis haben wie der Entwickler, der den Patch zur Verfügung gestellt hat. In der Regel ist als Codebasis nur der offizielle Kernelcode in der gerade aktuellen Version geeignet, nicht der oft schon gepatchte Kernelcode Ihrer Distribution.

Mitgelieferte Kernelkonfigurationsdateien verwenden

Der Kernel besteht aus Tausenden von Einzelfunktionen bzw. Komponenten. Bei nahezu allen Funktionen können Sie vor dem Kompilieren angeben, ob sie direkt in den Kernel integriert werden, als Modul kompiliert werden oder gar nicht verfügbar sein sollen. Dieser Vorgang heißt den »Kernel konfigurieren«.

.config-Datei

Die Kernelkonfiguration wird durch die Datei `.config` im Verzeichnis `/usr/src/linux-n.n` bestimmt. Dabei handelt es sich um eine rund 6000 Zeilen lange Textdatei, die angibt, ob eine Funktion direkt in den Kernel integriert (`name=y`) oder als Modul kompiliert werden soll (`name=m`). Nicht benötigte Funktionen erscheinen in der Konfigurationsdatei nicht bzw. nur in Kommentarzeilen. Die Datei kann auch zusätzliche Einstellungen enthalten (`name=wert`). Die folgenden Zeilen zeigen einen kleinen Ausschnitt aus einer `.config`-Datei:

```
CONFIG_X86=y
# CONFIG_X86_32 is not set
CONFIG_X86_64=y
CONFIG_X86_64_SMP=y
CONFIG_X86_ACPI_CPUFREQ=y
# CONFIG_X86_ACPI_CPUFREQ_PROC_INTF is not set
CONFIG_X86_BIOS_REBOOT=y
```

Wenn Sie bei der manuellen Kernelkonfiguration (siehe den folgenden Abschnitt) keinen Ausgangspunkt haben, müssen Sie sich wirklich um alle Kerneloptionen kümmern. Gerade beim ersten Mal ist es so gut wie sicher, dass Sie irgendetwas übersehen werden. Sie sparen eine Menge Zeit und Mühe, wenn Sie die mit Ihrer Distribution mitgelieferte Kernelkonfigurationsdatei als Ausgangspunkt verwenden:

```
root#  cp old-config /usr/src/linux-n.n/.config
```

Alternativ können Sie auch in das Quellcodeverzeichnis wechseln und dort das folgende Kommando ausführen:

```
root#  cd /usr/src/linux-n.n
root#  make oldconfig
```

Dieses Verfahren hat leider einen Nachteil: Wenn der ursprüngliche Kernelcode andere Patches enthält als der neu zu kompilierende Code, enthält auch die ursprüngliche Konfigurationsdatei Optionen, die im neuen Code nicht vorgesehen sind. Das kann zu Problemen führen. Wie ich schon erwähnt habe, bauen viele Distributoren diverse Patches in ihren Kernel ein, die im Standardkernel nicht enthalten sind.

Aktuelle Konfiguration feststellen

Bleibt noch die Frage offen, woher Sie die aktuelle Kernelkonfigurationsdatei nehmen. Bei nahezu allen Distributionen befindet sich im Verzeichnis `/boot` die zum laufenden Kernel passende Konfigurationsdatei, also z. B. `/boot/config-`*n*`.`*n*.

Bei Red Hat bzw. Fedora finden Sie weitere Konfigurationsmuster für SMP-, Xen- und andere Kernelvariationen nach der Installation des Kernelquellcodepakets im folgenden Verzeichnis:

```
rpmbuild/BUILD/kernel-n.n/linux-n.n/configs/
```

cloneconfig

Der mit SUSE mitgelieferte Kernel verwendet die `cloneconfig`-Option (Gruppe *General setup*). Das bedeutet, dass `/proc/config.gz` den komprimierten Inhalt der `.config`-Datei enthält, mit der der gerade laufende Kernel kompiliert wurde. Mit `make cloneconfig` kopieren Sie die zuletzt verwendete Konfiguration in die Datei `.config`.

Kernel manuell konfigurieren

Monolithischer oder modularisierter Kernel

Prinzipiell müssen Sie sich zwischen zwei Kerneltypen entscheiden: monolithischen Kerneln oder modularisierten Kerneln. Monolithische Kernel enthalten alle benötigten Treiber direkt im Kernel und unterstützen keine Module. Modularisierte Kernel sind über die integrierten Treiber hinaus in der Lage, im laufenden Betrieb zusätzliche Module aufzunehmen. Ein modularisierter Kernel ist in fast allen Fällen die bessere Entscheidung.

Komponentenauswahl

Bei den meisten Komponenten haben Sie die Wahl zwischen drei Optionen: YES, MODULE und NO. YES bedeutet, dass diese Komponente direkt in den Kernel integriert wird. MODULE bedeutet, dass diese Komponente als Modul kompiliert wird (nur sinnvoll bei einem modularisierten Kernel). NO bedeutet, dass die Komponente überhaupt nicht kompiliert wird. Es gibt auch eine Reihe von Funktionen, die nicht als Modul zur Verfügung gestellt werden können – dort reduziert sich die Auswahl auf YES oder NO.

Konfigurationsstrategien

Die übliche Vorgehensweise besteht darin, in den modularisierten Kernel nur relativ wenige elementare Funktionen zu integrieren und alle anderen Funktionen als Module verfügbar zu machen. Der Vorteil: Der Kernel an sich ist relativ klein, Module werden nur nach Bedarf nachgeladen.

Eine alternative Strategie besteht darin, einen monolithischen Kernel möglichst exakt für die eigenen Hard- und Software-Ansprüche zu optimieren. Alle Funktionen, die genutzt werden sollen, integrieren Sie direkt in den Kernel. Bei allen anderen Komponenten entscheiden Sie sich für NO.

Generell wird ein monolithischer Kernel immer etwas größer als ein modularisierter Kernel. Dafür funktioniert er ohne die dynamische Modulverwaltung, und der Rechnerstart gelingt ohne Initrd-Datei. Der Nachteil ist auch offensichtlich: Wenn Sie eine bestimmte Funktion später doch brauchen, müssen Sie den Kernel neu kompilieren. Und nur echte Linux-Profis können abschätzen, welche Funktionen sie nutzen werden.

Werkzeuge zur manuellen Kernelkonfiguration

Um abweichend von der aktuellen Konfiguration einzelne Einstellungen zu verändern, können Sie `.config` manuell editieren. Das ist aber fehleranfällig und erfordert eine gute Kenntnis der Namen der diversen Optionen. Besser ist es, mit `make xxx-config` ein spezielles Konfigurationsprogramm zu starten. Seit Kernelversion 2.6.35 stehen dazu fünf unterschiedliche Varianten zur Verfügung, die Sie mit einem der aufgelisteten `make`-Kommandos starten:

```
root#  cd /usr/src/linux-n.n
root#  make config              (Konfiguration in Textmodus)
root#  make menuconfig          (Dialoggeführte Konfiguration im Textmodus)
root#  make nconfig             (Dialoggeführte Konfiguration im Textmodus)
root#  make xconfig             (Konfiguration im Grafikmodus mit QT-Bibliothek)
root#  make gconfig             (Konfiguration im Grafikmodus mit GTK-Bibliothek)
root#  make localmodconfig      (automatische Konfiguration für die aktuelle Hardware)
```

make config

`make config` funktioniert immer, ist aber umständlich zu bedienen und nicht zu empfehlen. Sie müssen immer *alle* Optionen durchlaufen, auch wenn Sie nur eine einzige Option verändern möchten.

make menuconfig

`make menuconfig` setzt voraus, dass Sie vorher das Paket `ncurses-devel` bzw. `libncurses5-dev` installiert haben. Die Konfiguration erfolgt ebenfalls im Textmodus. Der große Vorteil im Vergleich zu `make config` besteht darin, dass die Einstellung der unzähligen Optionen durch verschachtelte Dialoge strukturiert ist.

make nconfig

Auch mit `make nconfig` erfolgt die Konfiguration im Textmodus, und wie bei bei `make menuconfig` müssen Sie vorher das `ncurses`-Entwicklerpaket installieren. Der wesentliche Unterschied besteht in der Navigation: Während `menuconfig` verschachtelte Dialoge verwendet, navigieren Sie bei `nconfig` durch einen Baum, dessen Äste Sie ein- und ausklappen.

make xconfig

Erheblich komfortabler ist `make xconfig`: Diese Variante setzt voraus, dass Sie unter X arbeiten und dass die Pakete `g++` (der C++-Compiler) und `qt3-devel` bzw. `libqt3-mt-dev` mit den Entwicklungsdateien der QT-Bibliothek installiert sind. `make` kompiliert zuerst die grafische Benutzeroberfläche `qconf` und startet diese dann (siehe Abbildung 28.1).

Die drei möglichen Zustände für Komponenten werden so ausgedrückt:

NO:	Das Optionskästchen ist nicht ausgewählt.
YES:	Das Optionskästchen ist mit einem Häkchen ausgewählt.
MODULE:	Das Optionskästchen ist mit einem Punkt ausgewählt.

Per Mausklick wechseln Sie zwischen den drei möglichen Zuständen. Sollten Sie eine bestimmte Option nicht finden, führen Sie OPTION • SHOW ALL OPTIONS aus. Damit zeigt das Programm auch normalerweise nicht benutzte Optionen an.

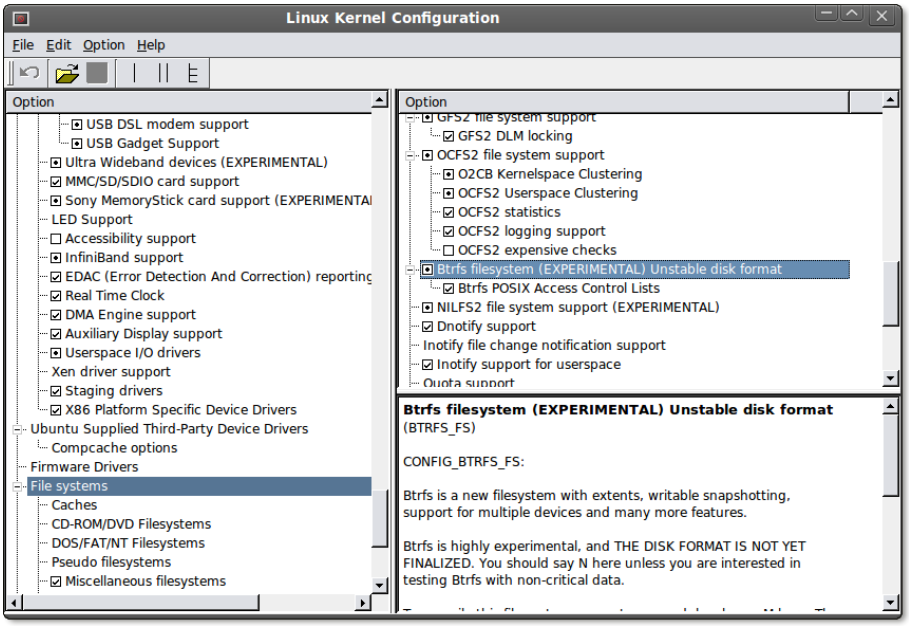


Abbildung 28.1 Kernelkonfiguration mit make xconfig

make gconfig

`make gconfig` kompiliert und startet `gconf`, das Gnome-Gegenstück zu `qconf`. Vorausgesetzt werden diesmal diverse Gnome-Entwicklerbibliotheken (unter anderem `[lib]gtk2-devel` und `libglade2-devel`). Aussehen und Bedienung von `gconf` sind nahezu identisch mit denen von `qconf`.

Zur Strukturierung der vielen Optionen stehen drei Darstellungsmodi zur Auswahl. Als ungeeignet hat sich dabei der (eigentlich übersichtlichste) Modus SPLIT herausgestellt: In diesem Modus sind manche verschachtelten Optionen nicht zugänglich.

make localmodconfig

`make localmodconfig` ist eine interessante Kompiliervariante für alle, die es eilig haben. Dabei werden nur die Module kompiliert, die im gerade laufenden Kernel tatsächlich genutzt werden. Das hat Vor- und Nachteile: Der offensichtliche Vorteil besteht darin, dass wirklich nur der Teil des Kernelcodes übersetzt wird, der tatsächlich benötigt wird. Das kann die Übersetzungszeit auf ein Drittel senken! Allerdings läuft der so kompilierte Kernel auf einem anderen Rechner unter Umständen nicht, wenn für dessen Hardware-Komponenten relevante Treiber fehlen. Auch das Nachladen eines Moduls, das zur Kompilierzeit nicht aktiv war, wird scheitern. Der Kernel ist also nur zu Testzwecken geeignet, nicht aber für eine längerfristige Nutzung. Detailinformationen zu dieser `make`-Variante können Sie hier nachlesen:

http://heise.de/-1402386

Kernel kompilieren und installieren

Nachdem Sie mit der Konfiguration des Kernels vermutlich einige Zeit verbracht haben, muss jetzt der Rechner arbeiten. Die folgenden Kommandos beschäftigen einen schnellen Rechner circa eine halbe Stunde. Wenn Ihr Rechner mehrere CPUs oder Cores enthält, können Sie den Kompilierprozess durch `make -j n all` beschleunigen. `make` startet dann *n* Prozesse parallel und lastet so alle CPUs/Cores aus.

```
root#  cd /usr/src/linux-n.n
root#  make all                  (alles kompilieren)
root#  make modules_install      (Module installieren)
```

Das Ergebnis am Ende dieses Prozesses ist die Datei `bzImage` im Verzeichnis `/usr/src/linux-n.n/arch/x86/boot`. Die Größe der Datei liegt meist in der Größenordnung zwischen 3 und 5 MByte und hängt davon ab, wie viele Funktionen direkt in den Kernel inkludiert sind und wie viele als Module bzw. überhaupt nicht kompiliert wurden.

Fehler beim Kompilieren

Wenn beim Kompilieren ein Fehler auftritt, sollten Sie naturgemäß versuchen, diesem auf den Grund zu gehen. Wenn das Problem bei einer für Sie nicht wichtigen Funktion auftritt, können Sie die Konfiguration so ändern, dass die betroffene Funktion eben nicht kompiliert wird.

Hartgesottene Linux-Freaks können `make` einfach mit der zusätzlichen Option `-k` aufrufen, also z. B. `make -k all`. Diese Option bewirkt, dass Fehler ignoriert werden. `make` fährt also einfach mit der Kompilation der nächsten Datei fort. Wenn Sie Glück haben, betrifft das Kompilationsproblem ein für Sie unwichtiges Modul, das dann eben nicht zur Verfügung steht.

`make modules_install` kopiert die Moduldateien dorthin, wo die Kommandos zur Modulverwaltung (etwa `insmod`) diese erwarten: in das Verzeichnis `/lib/modules/n`. Dabei ist *n* die genaue Versionsnummer des soeben kompilierten Kernels.

Kernel installieren

Der frisch erzeugte neue Kernel ist natürlich noch nicht aktiv! Bisher wurden nur ein paar neue Dateien erstellt, sonst nichts! Der neue Kernel kann erst beim nächsten Start von Linux aktiviert werden und auch dann nur, wenn Sie Ihren Boot-Loader GRUB so konfigurieren, dass der neue Kernel berücksichtigt wird.

Dazu kopieren Sie als Erstes die neue Kerneldatei in das Verzeichnis `/boot`. Es ist üblich, der Datei den Namen `vmlinuz-n.n` zu geben. Gleichzeitig sollten Sie auch eine Kopie der Konfigurationsdatei erstellen:

```
root#  cp /usr/src/linux-n.n/arch/x86/boot/bzImage /boot/vmlinuz-n.n
root#  cp /usr/src/linux-n.n/.config /boot/config-n.n
```

Systemstart vorbereiten

In der Regel müssen Sie nun eine neue, zum Kernel passende Initrd-Datei erzeugen. Dazu verwenden Sie je nach Distribution die Kommandos `mkinitrd`, `mkinitramfs` oder `update-initramfs` (siehe Abschnitt 26.1).

Wenn Sie mit GRUB 2 arbeiten, erfolgt die Aktualisierung der GRUB-Konfiguration fast automatisch:

```
root#  update-grub                                  (Debian, Ubuntu)
root#  grub2-mkconfig -o /boot/grub2/grub.cfg       (Fedora, openSUSE)
root#  grub2-mkconfig -o /boot/grub2-efi/grub.cfg   (openSUSE mit EFI)
```

Wenn Sie mit älteren Distributionen mit GRUB 0.97 arbeiten, müssen Sie `/boot/grub/menu.lst` selbst um einen Eintrag ergänzen. Bei der Angabe der Festplatte und der Optionen orientieren Sie sich an schon vorhandenen Einträgen in `menu.lst`. Beim anschließenden Neustart wählen Sie im GRUB-Menü den neuen Kernel aus:

```
# Ergänzung in /boot/grub/menu.lst
title kernel-n.n
    kernel (hd0,11)/boot/vmlinuz-n.n root=/dev/sda12 vga=normal
    initrd (hd0,11)/boot/initrd-n.n
```

Ob alles funktioniert hat, merken Sie beim Neustart. Sollte der neue Kernel aus irgendeinem Grund nicht funktionieren, starten Sie den Rechner einfach mit dem bisherigen Kernel und unternehmen einen weiteren Versuch, den Kernel richtig zu konfigurieren und neu zu kompilieren. Läuft der neue Kernel dagegen zufriedenstellend, sollten Sie die nun nicht mehr benötigten Objekt-Dateien des Compilers aufräumen. Sie gewinnen auf diese Weise rund 4 GByte Platz auf der Festplatte!

```
root#  cd /usr/src/linux-n.n
root#  make clean
```

28.3 Die Verzeichnisse /proc und /sys

Die Verzeichnisse `/proc` und `/sys` werden während des Systemstarts in das Dateisystem eingebunden. Sie dienen dazu, Informationen über den Kernel, laufende Prozesse, geladene Module und viele andere Parameter auf eine transparente Art und Weise sichtbar zu machen.

Intern sind die Verzeichnisse `/proc` und `/sys` als virtuelle Dateisysteme realisiert. Sie enthalten also keine echten Dateien und beanspruchen daher auch keinen Platz auf der Festplatte. Das gilt auch für die scheinbar sehr große Datei `/proc/kcore`, die den Arbeitsspeicher abbildet.

Die meisten der `/proc`- und `/sys`-Dateien liegen im Textformat vor. Um die Dateien zu lesen, müssen Sie unter Umständen `cat` statt `less` verwenden, weil manche `less`-Versionen mit virtuellen Dateien nicht zurechtkommen.

Das `/proc`-Verzeichnis liefert eine Menge interne Kernelinformationen sowie Daten zu allen gerade laufenden Prozessen (siehe Tabelle 28.4). Unter anderem ist dort jedem Prozess ein eigenes Unterverzeichnis zugeordnet. Innerhalb des Prozessverzeichnisses befinden sich dann einige Dateien mit diversen Verwaltungsdaten (z. B. die zum Start verwendete Kommandozeile). Diese Daten werden von diversen Kommandos zur Prozessverwaltung (z. B. `top`, `ps` etc.) ausgewertet.

Datei	Bedeutung
`/proc/`*n*`/*`	Informationen zum Prozess mit der PID=*n*
`/proc/asound`	ALSA (Advanced Linux Sound Architecture)
`/proc/bus/usb/*`	USB-Informationen
`/proc/bus/pccard/*`	PCMCIA-Informationen
`/proc/bus/pci/*`	PCI-Informationen
`/proc/cmdline`	GRUB-Boot-Parameter
`/proc/config.gz`	Kernelkonfigurationsdatei (SUSE)
`/proc/cpuinfo`	CPU-Informationen
`/proc/devices`	Nummern von aktiven Devices
`/proc/fb`	Informationen zum Frame-Buffer
`/proc/filesystems`	im Kernel enthaltene Dateisystemtreiber
`/proc/ide/*`	IDE-Laufwerke und -Controller

Tabelle 28.4 Wichtige /proc-Dateien

Datei	Bedeutung
/proc/interrupts	Nutzung der Interrupts
/proc/lvm/*	Nutzung des Logical Volume Managers
/proc/mdstat	RAID-Zustand
/proc/modules	aktive Module
/proc/mounts	aktive Dateisysteme
/proc/net/*	Netzwerkzustand und -nutzung
/proc/partitions	Partitionen der Festplatten
/proc/pci	PCI-Informationen (alt, siehe /proc/bus/pci)
/proc/scsi/*	SCSI-Laufwerke und -Controller
/proc/splash	steuert das VGA-Hintergrundbild für Textkonsole 1.
/proc/sys/*	System- und Kernelinformationen
/proc/uptime	Zeit in Sekunden seit dem Rechnerstart
/proc/version	Kernelversion

Tabelle 28.4 Wichtige /proc-Dateien (Forts.)

Das /sys-Verzeichnis ist seit Kernelversion 2.6 verfügbar. Es enthält teilweise dieselben Informationen wie /proc, allerdings sind die Daten systematischer organisiert (siehe Tabelle 28.5). Das Ziel des /sys-Verzeichnisses ist es, den Zusammenhang zwischen dem Kernel und der Hardware abzubilden.

Datei	Bedeutung
/sys/block/*	Informationen über alle Block-Devices (Festplatten etc.)
/sys/bus/*	Informationen über alle Bus-Systeme (IDE, USB etc.)
/sys/class/*	Informationen über Device-Klassen (Bluetooth, Grafik, Speicher etc.)
/sys/devices/*	Informationen über angeschlossene Hardware-Komponenten
/sys/firmware/*	Informationen über Hardware-Treiber und -Firmware (speziell ACPI)
/sys/kernel/*	Informationen über den Kernel
/sys/module/*	Informationen über geladene Module
/sys/power/*	Informationen über die Energieverwaltung

Tabelle 28.5 Wichtige /sys-Dateien

28.4 Kernel-Bootoptionen

Nicht immer, wenn ein Detail im Kernel geändert werden soll, muss der Kernel gleich neu kompiliert werden! Es gibt zwei Möglichkeiten, ohne ein Neukompilieren auf den Kernel Einfluss zu nehmen:

- Zum einen können Sie mit dem Boot-Loader während des Systemstarts Parameter an den Kernel übergeben. Dieser Mechanismus ist Thema dieses Abschnitts.
- Zum anderen können Sie eine Reihe von Kernelfunktionen dynamisch – also im laufenden Betrieb – verändern. Diese Art des Eingriffs ist insbesondere zur Steuerung von Netzwerkfunktionen gebräuchlich und wird im nächsten Abschnitt beschrieben.

Bei der Konfiguration von GRUB können Sie Kernel-Bootoptionen angeben (siehe Abschnitt 26.4). Derartige Optionen können Sie auch interaktiv beim Start eines Linux-Installationsprogramms oder beim Start des Boot-Loaders über die Tastatur eintippen. Die Syntax für die Angabe von Optionen sieht so aus: GRUB

```
optionA=parameter optionB=parameter1,parameter2
```

Die Parameter zu einer Option müssen ohne Leerzeichen angegeben werden. Mehrere Optionen müssen durch Leerzeichen voneinander getrennt werden, nicht durch Kommata. Hexadezimale Adressen werden in der Form 0x1234 angegeben. Ohne vorangestelltes 0x wird die Zahl dezimal interpretiert.

Kernel-Bootoptionen helfen oft dabei, Hardware-Probleme zu umgehen. Wenn der Linux-Kernel beispielsweise aufgrund eines fehlerhaften BIOS nicht erkennt, wie viel RAM Ihr Rechner hat, geben Sie den korrekten Wert mit dem Parameter `mem=` an.

Beachten Sie, dass die beim Linux-Start angegebenen Parameter nur Einfluss auf die in den Kernel integrierten Treiber haben! Parameter für Kernelmodule müssen dagegen in der Datei `/etc/modprobe.conf` angegeben werden.

Dieser Abschnitt beschreibt nur die wichtigsten Kernel-Bootoptionen. Weitere Informationen erhalten Sie mit `man bootparam` sowie auf den folgenden Seiten:

http://www.tldp.org/HOWTO/BootPrompt-HOWTO.html
http://www.kernel.org/doc/Documentation/kernel-parameters.txt

Wichtige Kernel-Bootoptionen

- `root=/dev/sdb3`: Die `root`-Option gibt an, dass nach dem Laden des Kernels die dritte primäre Partition des zweiten SCSI/SATA-Laufwerks als Systempartition für das Root-Dateisystem verwendet werden soll. Analog können natürlich auch andere Laufwerke und Partitionen angegeben werden.

  Wenn die Partition mit einem Label bezeichnet ist, kann die Systempartition auch in der Form `root=LABEL=xxx` angegeben werden. Insbesondere Fedora und Red Hat machen von dieser Möglichkeit Gebrauch. Als Name für die Systempartition wird üblicherweise das Zeichen / verwendet. Bei `ext3`-Partitionen ermitteln Sie den Partitionsnamen mit `e2label` bzw. verändern ihn mit `tune2fs`.

  Eine weitere Variante ist die Angabe der Systempartition durch `root=UUID=n`, wobei *n* die UUID der Festplattenpartition ist. Diese Identifikationsnummer ermitteln Sie mit `/lib/udev/vol_id` *partition*.

- `ro`: Die Option `ro` gibt an, dass das Dateisystem vorerst *read-only* gemountet werden soll. Das ist (in Kombination mit einer der beiden folgenden Optionen) praktisch, wenn ein defektes Dateisystem manuell repariert werden muss.

- `init`: Nach dem Kernelstart wird automatisch das Programm `/sbin/init` ausgeführt, das je nach Distribution den Init-V-Prozess, Upstart oder Systemd steuert (siehe Kapitel 27). Wenn Sie dies nicht wollen, können Sie mit der Option `init` ein anderes Programm angeben.

  Mit `init=/bin/sh` erreichen Sie beispielsweise, dass eine Shell gestartet wird. Die Option kann Linux-Profis helfen, ein Linux-System wieder zum Laufen zu bringen, wenn bei der Init-Konfiguration etwas schiefgegangen ist. Beachten Sie, dass das root-Dateisystem nur read-only zur Verfügung steht (das können Sie mit `mount -o remount` ändern, siehe Abschnitt 25.5), dass in der Konsole das US-Tastaturlayout gilt und dass die `PATH`-Variable noch leer ist.

- `single` oder `emergency`: Wenn Sie eine der zwei obigen Optionen verwenden, startet der Rechner im Single-User-Modus. Genau genommen werden diese Optionen nicht vom Kernel ausgewertet, sondern so wie alle unbekannten Optionen an das erste vom Kernel gestartete Programm weitergegeben. Dabei handelt es sich um `/sbin/init`, das für die Initialisierung des Systems zuständig ist (siehe Kapitel 27, »Das Init-System«).

- `initrd=name`: `initrd` gibt den Namen der zu ladenden Initial-RAM-Disk-Datei an. Wenn Sie *keine* Initrd-Datei verwenden möchten, geben Sie `initrd=` oder `noinitrd` an.

- `ipv6.disable=1`: Diese Option deaktiviert alle IPv6-Funktionen des Kernels.

- `reserve=0x300,0x20`: Diese Option gibt an, dass die 32 Bytes (hexadezimal 0x20) zwischen 0x300 und 0x31F von keinem Hardware-Treiber angesprochen wer-

den dürfen, um darin nach irgendwelchen Komponenten zu suchen. Die Option ist bei manchen Komponenten notwendig, die auf solche Tests allergisch reagieren. Sie tritt im Regelfall in Kombination mit einer zweiten Option auf, die die exakte Adresse der Komponente angibt, die diesen Speicherbereich für sich beansprucht.

- `pci=bios|nobios`: Diese Option steuert, ob das BIOS zur Hardware-Erkennung der PCI-Komponenten verwendet werden soll oder nicht. (PCI ist das Bussystem zur Erweiterung von PCs durch Steckkarten.) Wenn die automatische Hardware-Erkennung durch den Kernel nicht funktioniert, hilft manchmal `pci=bios`.
- `pci=nommconf`: Diese Option deaktiviert MMCONFIG für die PCI-Konfiguration. Das vermeidet Probleme bei manchen PCI-Express-Systemen.
- `quiet`: Diese Option bewirkt, dass während des Kernelstarts keine Meldungen auf dem Bildschirm dargestellt werden.
- `video=1024x768`: Mit dieser Option kann per *Kernel Mode Setting* (KMS) die gewünschte Grafikauflösung eingestellt werden, wenn der Kernel nicht selbst die optimale Auflösung wählt, z. B. wenn das Video-Signal über einen KVM-Switch geleitet wird. Wenn Sie auch die Farbtiefe (z. B. 24 Bit) und die Bildfrequenz angeben möchten, sieht die Syntax so aus: `video=1280x800-24@60`

  Die Einstellung der Grafikdaten funktioniert nur bei KMS-kompatiblen Treibern (zurzeit `intel`, `nouveau` und `radeon`). Die `video`-Einstellung gilt normalerweise für alle angeschlossenen Monitore. Wenn Sie die Auflösung nur für einen einzelnen Monitor ändern möchten, geben Sie den entsprechenden Signalausgang an, z. B. `video=VGA-1:1024x768`.
- `nomodeset`: Diese Option deaktiviert das Kernel Mode Setting (KMS).

SMP-Optionen

SMP steht für *Symmetric Multiprocessing* und bezeichnet die Fähigkeit des Kernels, mehrere CPUs bzw. CPU-Cores gleichzeitig zu nutzen. Sollten dabei Probleme auftreten, können die folgenden Optionen hilfreich sein:

- `maxcpus=1`: Wenn Sie bei einem Multiprozessorsystem Bootprobleme haben, können Sie mit dieser Option die Anzahl der genutzten Prozessoren auf 1 reduzieren. Der Wert 0 entspricht der Option `nosmp`.
- `nosmp`: Diese Option deaktiviert die SMP-Funktionen. Der Kernel nutzt nur eine CPU.
- `noht`: Diese Option deaktiviert die Hyper-Threading-Funktion. (Dank Hyper-Threading verhalten sich manche CPUs so, als stünden mehrere Cores zur Ver-

fügung. Daraus ergibt sich eine etwas höhere Rechenleistung, wenngleich die Steigerung nicht so hoch ist wie bei echtem SMP.)

- `nolapic`: APIC steht für *Advanced Programmable Interrupt Controller* und bezeichnet ein Schema, um Hardware-Interrupts an die CPUs weiterzuleiten. Bei aktuellen Kernelversionen wird APIC immer aktiviert. Wenn Sie Probleme mit APIC vermuten, verhindern Sie durch `nolapic`, dass der Kernel den lokalen APIC aktiviert bzw. nutzt.
- `noapic`: Diese Option reicht etwas weniger weit als `nolapic` und deaktiviert nur den IO-Teil von APIC.
- `lapic`: Diese Option aktiviert APIC explizit. Das ist dann notwendig, wenn APIC durch das BIOS deaktiviert ist, aber dennoch genutzt werden soll.

ACPI-Optionen

Das Energieverwaltungssystem APM (*Advanced Power Management*) und das neuere ACPI (*Advanced Configuration and Power Interface*) sind nicht nur für das Ein- und Ausschalten verantwortlich, sondern auch für den sparsamen Umgang mit Energie, für die Verwaltung verschiedener Hibernate-Modi etc. Im Folgenden sind die wichtigsten Optionen zur Steuerung der APM- und ACPI-Funktionen des Kernels zusammengefasst:

- `apm=on/off`: Diese Option (de)aktiviert die APM-Funktionen im Kernel.
- `acpi=on/off`: Diese Option (de)aktiviert die ACPI-Funktionen im Kernel.
- `acpi=oldboot`: Damit werden die ACPI-Funktionen nur während des Bootvorgangs genutzt. Sobald der Rechner läuft, werden die ACPI-Funktionen aber nicht mehr verwendet.
- `pci=noacpi`: Diese Option deaktiviert die Interrupt-Zuweisungen durch ACPI.
- `noresume`: Diese Option bewirkt, dass vorhandene Hibernate-Daten in der Swap-Partition ignoriert werden. Sie ist also dann sinnvoll, wenn der Rechner nicht mehr richtig aufwacht, z. B., weil die Hibernate-Daten defekt sind.

28.5 Kernelparameter verändern

Eine Menge Parameter des Kernels können im laufenden Betrieb über das `/proc`-Dateisystem verändert werden. Das folgende Beispiel zeigt, wie Sie die Masquerading-Funktion aktivieren, um den Rechner als Internet-Gateway für andere Rechner einzusetzen:

```
root#  echo 1 > /proc/sys/net/ipv4/ip_forward
```

sysctl

Einen eleganteren Weg bietet das Kommando `sysctl`, das mit den meisten aktuellen Distributionen mitgeliefert wird. Das analoge Kommando, um das Masquerading wieder abzuschalten, würde so aussehen:

```
root#  sysctl -w net.ipv4.ip_forward=1
```

`sysctl -a` liefert eine Liste aller Kernelparameter zusammen mit ihren aktuellen Einstellungen. Mit `sysctl -p` können die in einer Datei gespeicherten `sysctl`-Einstellungen aktiviert werden. Als Dateiname wird üblicherweise `/etc/sysctl.conf` verwendet. Die Syntax ist in der Manual-Seite zu `sysctl.conf` beschrieben. Viele Distributionen sehen vor, dass diese Datei während des Init-Prozesses automatisch ausgewertet und ausgeführt wird.

TEIL V

LAN-Server

Kapitel 29
Netzwerkkonfiguration

Dieses Kapitel beschreibt, wie Sie Ihren Linux-Rechner mit dem Internet bzw. mit einem lokalen Netzwerk verbinden. Das Kapitel stellt zuerst den Network Manager vor, der auf Notebooks und Desktop-Rechnern bei der Herstellung einer Internetverbindung hilft (LAN, WLAN, UMTS etc.). Die weiteren Abschnitte geben Grundlageninformationen zur Netzwerkkonfiguration und erklären, wie Sie eine statische Netzwerkkonfiguration auch ohne Konfigurationswerkzeuge durchführen. Das ist vor allem für den Server-Einsatz wichtig. Neu in dieser Auflage ist die umfassende Berücksichtigung von IPv6.

29.1 Der NetworkManager

Der NetworkManager ist das populärste Werkzeug zur LAN-, WLAN-, ADSL-, UMTS- und VPN-Konfiguration auf Desktop-Systemen. Für die Grundfunktionen ist ein Hintergrundprozess verantwortlich, der beim Hochfahren des Rechners gestartet wird. Die Benutzeroberfläche des NetworkManagers sieht je nach Desktop unterschiedlich aus. Ich konzentriere mich in diesem Abschnitt auf die Gnome-Variante. Unter KDE oder Ubuntu/Unity sehen die Dialoge ein wenig anders aus, die Bedienung erfolgt aber nach denselben Mustern wie unter Gnome.

Voraussetzungen

Der NetworkManager funktioniert nur, wenn das Programm die Kontrolle über die Schnittstellen hat. Alle gängigen Distributionen führen standardmäßig eine entsprechende Konfiguration durch, einzig unter openSUSE gab es in letzter Zeit immer wieder Probleme.

Bei Debian und Ubuntu stellen Sie sicher, dass `/etc/network/interfaces` nur Einstellungen für die Loopback-Schnittstelle enthält. Schnittstellen, die vom NetworkManager gesteuert werden sollen (typischerweise `eth0` und `wlan0`), dürfen nicht durch diese Datei konfiguriert werden!

```
# Datei /etc/network/interfaces (Debian, Ubuntu)
auto lo
iface lo inet loopback
```

Bei Fedora und Red Hat müssen die Dateien `/etc/sysconfig/network-scripts/ifcfg-`*name* den Eintrag `NM_CONTROLLED=yes` enthalten. Dabei gibt *name* den Device-Namen der Netzwerkschnittstelle an, z. B. `p`*n*`s`*n* oder `wlp`*n*`s`*n*. Bei einer Desktop- oder Notebook-Installation ist die Standardeinstellung korrekt.

```
# Datei /etc/sysconfig/network-scripts/ifcfg-xxx (Fedora, Red Hat)
...
NM_CONTROLLED="yes"
```

Bei SUSE kontrolliert das YaST-Modul NETZWERKGERÄTE • NETZWERKEINSTELLUNGEN, ob die Netzwerkkonfiguration durch den NetworkManager oder auf traditionelle Art und Weise durch YaST und `ifup` erfolgt. Standardmäßig verwendet openSUSE bei Desktop-PCs die traditionelle Konfiguration und nur bei Notebooks den Network Manager. Gegebenenfalls müssen Sie im Dialogblatt GLOBALE OPTIONEN die Option BENUTZERGESTEUERT MITHILFE VON NETWORKMANAGER aktivieren.

NetworkManager deaktivieren

Wenn Sie Ihren Rechner als Server oder Router konfigurieren, sollten Sie den NetworkManager deaktivieren und eine statische Netzwerkkonfiguration durchführen. Tipps dazu finden Sie in Abschnitt 29.5.

Konfiguration

Bei den meisten gängigen Distributionen zeigt ein Icon in der Menüleiste oder im Panel den aktuellen Netzwerkzustand an. Dieses Icon führt in ein Menü, das die aktive Verbindung und alle erreichbaren bzw. vorkonfigurierten Netzwerke auflistet (siehe Abbildung 29.1). Über dieses Menü oder im Modul NETZWERK der Systemeinstellungen können Sie bei Bedarf die Konfiguration verändern (siehe Abbildung 29.2).

Abbildung 29.1 Das Menü des NetworkManagers unter Gnome

Lokale Netzwerke mit DHCP

Der einfachste Anwendungsfall für den NetworkManager liegt dann vor, wenn Ihr Rechner über ein Netzwerkkabel mit einem lokalen Netzwerk oder einem ADSL-Router verbunden ist. Der NetworkManager überprüft standardmäßig für alle LAN-Schnittstellen, ob via DHCP Konfigurationsinformationen bezogen werden können. Gelingt dies, erfolgt die Netzwerkkonfiguration bereits während des Rechnerstarts vollautomatisch.

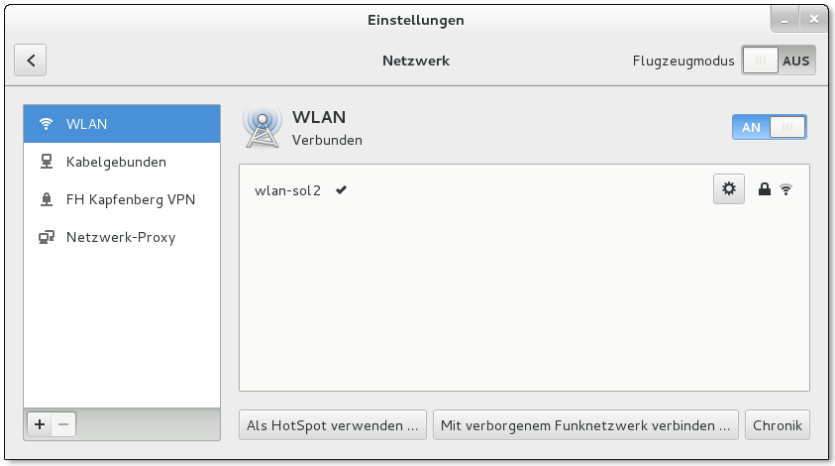


Abbildung 29.2 Einstellungsdialog des NetworkManagers

Netzwerkschnittstellen in RHEL aktivieren

Unter RHEL 6 scheitert der automatische Verbindungsaufbau mitunter. Abhilfe: Führen Sie im Menü des NetworkManagers VERBINDUNGEN BEARBEITEN aus, und suchen Sie im Konfigurationsdialog nach der Verbindung SYSTEM ETH0. Bei dieser Verbindung öffnen Sie mit BEARBEITEN den Detaildialog und aktivieren die Option AUTOMATISCH VERBINDEN. Warum diese Option nicht wie bei anderen Distributionen automatisch gesetzt ist, ist nur schwer verständlich.

Statische LAN-Konfiguration

Eine statische Konfiguration der LAN-Verbindung ist dann erforderlich, wenn Ihr Rechner nicht mit einem Router bzw. DHCP-Server verbunden ist und Sie die IP-Adresse, Netzmaske, Gateway-Adresse und die Nameserver-Adresse selbst angeben müssen. Alle hier aufgezählten Begriffe werden im Netzwerkglossar in Abschnitt 29.2 erläutert.

Zur Konfiguration führen Sie im Menü des NetworkManagers das Kommando NETZWERKEINSTELLUNGEN aus. Im Einstellungsdialog wählen Sie das Dialogblatt KABELGEBUNDEN, wählen dort die Schnittstelle aus und verändern über den Zahnrad-Button deren IPv4-Einstellungen. Für eine statische Konfiguration müssen Sie das Feld ADRESSEN auf MANUELL stellen.

WLAN-Zugang einrichten

Der NetworkManager erkennt selbstständig alle in Reichweite befindlichen Funknetze. Wenn Sie den Namen des WLANs zum ersten Mal im Menü des NetworkManagers auswählen, müssen Sie das WLAN-Passwort angeben.

Beim erstmaligen Verbindungsaufbau in Unternehmensnetzen mit dem Verschlüsselungssystem WPA & WPA2 ENTERPRISE müssen Sie im Einstellungsdialog des NetworkManager ein CA-Zertifikat auswählen. Geeignete Zertifikate befinden sich im Verzeichnis `/etc/ssl/certs`. Welches Zertifikat erforderlich ist, hängt von der Konfiguration des Unternehmensnetzwerks ab – fragen Sie gegebenenfalls den Administrator der Firma.

In Zukunft stellt der NetworkManager die Verbindung dann selbstständig her. Dazu werden alle WLAN-Passwörter zentral gespeichert, wobei der Speicherort je nach Distribution unterschiedlich ist. Unter Fedora richtet der NetworkManager für jede WLAN-Verbindung eine Textdatei in `/etc/sysconfig/network-scripts` ein; unter Ubuntu werden die WLAN-Passwörter hingegen im Verzeichnis `/etc/NetworkManager/system-connects/*` gespeichert.

Ein WLAN kann so konfiguriert sein, dass es seinen Namen nicht sendet. In diesem Fall wird es im Menü des NetworkManagers nicht angezeigt. Um dennoch eine Verbindung herzustellen, klicken Sie im Einstellungsdialog auf MIT EINEM VERBORGENEN FUNKNETZWERK VERBINDEN; anschließend können Sie den Netzwerknamen (ESSID = Extended Service Set Identification) und die Verschlüsselungstechnik selbst angeben.

Einen eigenen Hot-Spot einrichten

Wenn Ihr Rechner den Internetzugang über eine LAN-Schnittstelle bezieht und außerdem einen WLAN-Controller besitzt, können Sie diesen mit dem Network Manager so konfigurieren, dass Ihr Rechner jetzt als Hot-Spot fungiert und anderen WLAN-Geräten in Funkreichweite Internetzugang verschafft. Bei Smartphones wird dieses Verfahren oft als »Tethering« bezeichnet, in der Netzwerktechnik ist eher von einem WLAN-Access-Point die Rede.

Die Konfiguration ist einfach: Im WLAN-Dialogblatt der Netzwerkeinstellungen klicken Sie auf den Button • ALS HOTSPOT VERWENDEN. Nach einer Rückfrage zeigt der NetworkManager den Namen des Netzwerks und ein zufälliges Passwort an. Leider erfolgt die Verschlüsselung mit dem sicherheitstechnisch obsoleten WEP-Verfahren. Weitere Konfigurationsmöglichkeiten bestehen nicht.

Die Hotspot-Funktion kann allerdings nur mit ausgewählten WLAN-Controllern genutzt werden, deren Linux-Treiber den sogenannten Ad-hoc-Modus unterstützt. Auf meinen beiden Notebooks hatte ich kein Glück: Obwohl bei der Konfiguration keinerlei Fehlermeldungen auftraten, gelang es mir nicht, das WLAN-Netz des Rechners mit anderen Geräten zu nutzen.

ADSL-Modem

Wenn Ihr Internetzugang via ADSL erfolgt, führt der übliche Weg über einen ADSL-Router: Sie müssen Ihren Rechner über ein Netzwerkkabel oder via WLAN mit dem Router verbinden, also so, wie ich es auf den vorigen Seiten beschrieben habe.

Komplizierter wird es, wenn Sie keinen ADSL-Router, sondern ein zumeist älteres ADSL-Modem besitzen, das direkt mit dem Computer verbunden ist. Aktuelle Versionen des NetworkManagers bieten für diesen Fall keine Konfigurationsdialoge mehr an. Falls Ihr ADSL-Provider das in Deutschland eher unübliche Protokoll PPTP verwendet und das Modem mit einem Netzwerkkabel mit Ihrem Rechner verbunden ist (nicht mit einem USB-Kabel), können Sie zur Konfiguration die VPN-Dialoge des NetworkManagers verwenden. In allen anderen Fällen sind Sie auf eine manuelle Konfiguration angewiesen, z. B. mit dem Kommando `pppoeconfig` (siehe Abschnitt 29.1) oder unter openSUSE mit dem YaST-Modul NETZWERKGERÄTE • DSL.

Mobilfunk-Netzwerke

Wenn Sie einen USB-Modemstick einstecken, erscheint im Menü des NetworkManagers nach einigen Sekunden ein neuer Eintrag: MOBILES BREITBAND. Die weitere Konfiguration führen Sie im Einstellungsdialog durch. Sie müssen zuerst Ihr Land und dann Ihren Mobilfunkanbieter auswählen. Außerdem geben Sie den PIN-Code der SIM-Karte und bei manchen Providern außerdem ein Passwort für den Login an.

Interna

NetworkManager auf Kommandoebene

Ausführliche Statusinformationen über alle durch den NetworkManager verwalteten Verbindungen liefert das Kommando `nm-tool`. Außerdem können Sie die Verbindungen über das Kommando `nmcli` verwalten und steuern. Das ermöglicht die Steuerung des NetworkManagers durch Scripts oder bei Server-Installationen ohne grafische Benutzeroberfläche. Die folgenden Kommandos listen zuerst alle Verbindungen auf, die der NetworkManager kennt, und aktivieren dann die Verbindung mit dem Namen *System eth0*:

```
root#  nmcli con list
NAME          UUID                                  TYP              ...
System eth0   5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  802-3-ethernet   ...
root#  nmcli con up id 'System eth0'
```

Dispatcher

Es ist möglich, beim Herstellen bzw. Auflösen einer Verbindung automatisch Scripts auszuführen. Diese Scripts müssen im Verzeichnis `/etc/NetworkManager/dispatcher.d/` eingerichtet werden. Details und Beispiele zu diesem Mechanismus finden Sie auf der folgenden Seite:

http://wiki.ubuntuusers.de/NetworkManager/Dispatcher

Nameserver (Ubuntu)

Unter Ubuntu ist der NetworkManager so konfiguriert, dass automatisch das Programm Dnsmasq als Nameserver-Cache startet. Dnsmasq merkt sich die IP-Adressen von Hostnamen und ermöglicht so eine raschere Adressauflösung. Eine detaillierte Beschreibung von Dnsmasq folgt in Abschnitt 30.5.

Der NetworkManager erzeugt selbst eine Konfigurationsdatei für Dnsmasq und speichert diese unter dem Namen `/var/run/NetworkManager/dnsmasq.conf`. In vielen Fällen ist die Datei allerdings einfach leer – dann läuft `dnsmasq` mit den Defaulteinstellungen. Um herauszufinden, auf welche Nameserver `dnsmasq` seinerseits zurückgreift, führen Sie am besten das folgende Kommando aus:

```
user$ nm-tool | grep DNS
```

Falls Sie Sicherheitsbedenken wegen der Ausführung des lokalen Nameservers haben oder wenn es ohnedies einen Nameserver im lokalen Netzwerk gibt, können Sie den automatischen Start von Dnsmasq verhindern. Dazu entfernen Sie aus der Datei `/etc/NetworkManager/NetworkManager.conf` die Anweisung `dns=dnsmasq`. Hintergrundinformationen zur Ubuntu-spezifischen Konfiguration können Sie hier nachlesen:

http://www.stgraber.org/2012/02/24/dns-in-ubuntu-12-04

Alternativen zum NetworkManager

YaST (SUSE)

SUSE aktiviert bei Notebooks automatisch den NetworkManager, setzt bei Desktop-PCs aber weiterhin auf die traditionelle Steuerung der Netzwerkfunktionen durch YaST sowie `ifup`. Die Konfiguration erfolgt durch das YaST-Modul Netzwerkgeräte • Netzwerkeinstellungen. Im Dialogblatt Globale Optionen können Sie zwischen den Optionen Traditionelle Methode mit ifup oder Benutzergesteuert mithilfe von NetworkManager wählen.

Wenn Sie sich für die traditionelle Methode entscheiden, listet YaST im Dialogblatt Übersicht alle gefundenen Netzwerkschnittstellen auf. Sie können die einzelnen Schnittstellen nun Bearbeiten (siehe Abbildung 29.3). Standardmäßig konfiguriert YaST alle Ethernet-Schnittstellen so, dass diese ihre IP-Adresse und alle anderen Konfigurationseinstellungen per DHCP vom (ADSL-)Router des lokalen Netzwerks beziehen. Bei WLAN-Schnittstellen müssen Sie in einem zweiten Schritt den Netzwerknamen (ESSID), die Authentifizierungsmethode (WEP oder WPA) und das Passwort angeben.

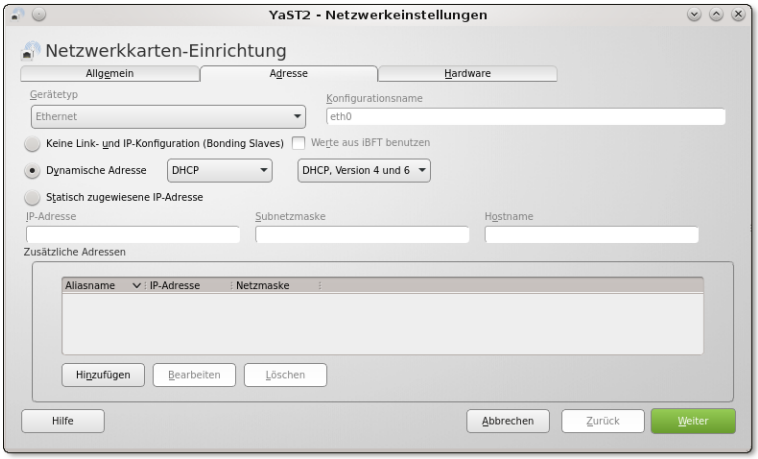


Abbildung 29.3 Netzwerkkonfiguration mit YaST

pppoeconfig (Debian/Ubuntu)

Debian und Ubuntu stellen für die ADSL-Modemkonfiguration das Textkommando `pppoeconf` zur Verfügung. Sie starten `pppoeconf` als `root` in einem Terminalfenster. Das Kommando sucht nun an allen Netzwerkschnittstellen nach einem ADSL-Modem. Eine vorherige Konfiguration der Netzwerkschnittstelle ist nicht erforderlich!

Nachdem das Modem gefunden worden ist, geben Sie den Benutzernamen und das Passwort ein. Die folgenden Rückfragen für die automatische DNS-Konfiguration sowie für die Konfiguration des MSS-Parameters können Sie einfach bestätigen.

Bei T-Online muss der Benutzername aus drei Informationen zusammengesetzt werden: aus der zwölfstelligen Anschlussnummer `A`, der T-Online-Nummer `T` und der Mitbenutzernummer (normalerweise `0001`). Die resultierende Zeichenkette sieht so aus:

```
AAAAAAAAAAAATTTTTTTTTT#0001@t-online.de
```

Wenn `T` aus 12 Zeichen oder mehr besteht, entfällt das Zeichen `#`.

Das Programm fragt schließlich, ob die ADSL-Verbindung automatisch beim Rechnerstart oder manuell hergestellt werden soll. Die erste Variante ist zweckmäßig, wenn Sie einen ADSL-Zugang ohne Zeitbeschränkung haben (Flatrate) und ständig online sein wollen. Bei der zweiten Variante müssen Sie den ADSL-Zugang manuell mit den folgenden Kommandos aktivieren bzw. wieder beenden:

```
root#  pon dsl-provider
...
root#  poff dsl-provider
```

29.2 Netzwerkgrundlagen und Glossar

Dieser Abschnitt fasst die Grundlagen der Netzwerkkonfiguration zusammen. Die Informationen gelten nicht nur für den Netzwerkanschluss an ein lokales Netz, sondern auch für die WLAN-, ADSL- und Modemkonfiguration.

Glossar

IP-Adressen und -Ports

Für den Großteil des Datenverkehrs in lokalen Netzen und im Internet ist das Protokoll TCP/IP verantwortlich (siehe auch Tabelle 29.1). Dabei werden Netzwerkdaten in Form von relativ kleinen Paketen transportiert. Zusammen mit jedem Paket werden mehrere Metadaten gespeichert, darunter die IP-Adresse und der IP-Port. Die IP-Adresse bestimmt den Empfänger des Pakets. Eine typische IP-Adresse für einen Rechner in einem lokalen Netz lautet 192.168.0.75. Die Port-Nummer gibt die Kategorie des Dienstes an. Vielen Internetdiensten (wie WWW oder E-Mail) sind jeweils eigene Port-Nummern zugeordnet.

Abkürzung	Funktion
IP = Internet Protocol	verbindungsloses Protokoll, Basis für TCP und UDP
TPC = Transmission Control Protocol	Ende-zu-Ende-Verbindung zwischen zwei Computern/Geräten
UDP = User Datagram Protocol	minimales, verbindungsloses Protokoll
ICMP = Internet Control Message Protocol	Austausch von IP-Status- und Fehlermeldungen
PPP = Point-to-Point Protocol	IP-Verbindungsaufbau über Wählleitungen, z. B. für ADSL und UMTS

Tabelle 29.1 Wichtige Netzwerkprotokolle

Host- und Domainname

IP-Adressen mögen für Computer praktisch sein, Menschen können sich IP-Adressen aber nur schwer merken. Aus diesem Grund werden Rechner im Netzwerk durch eine Kombination aus Host- und Domainnamen identifiziert. Beim Hostnamen handelt es sich um den eigentlichen Rechnernamen. Der Domainname bezeichnet das Teilnetz, innerhalb dessen der Rechner angesprochen werden kann. In lokalen Netzen können Sie den Domainnamen frei wählen; üblich ist z. B. `local`. Der Domainname kann auch mehrteilig sein.

Wenn Ihr Linux-Rechner als öffentlich im Internet sichtbarer Server agieren soll, müssen Sie den gewünschten Domainnamen bei einem Internet Service Provider bzw. einem Network Information Center (kurz NIC) registrieren – z. B. bei *http://www.*

denic.de für die .de-Domainnamen oder bei *http://www.corenic.org* für .com-, .net- und .org-Domainnamen.

Benennung von Rechnern in lokalen Netzen

Als Hostname sollte nicht der Name des Rechnerherstellers, des Besitzers oder des gerade anstehenden Projekts verwendet werden – all das kann Verwirrung stiften. Verwenden Sie kurze und einprägsame Namen von Tieren, Pflanzen, Planeten, Flüssen oder was immer Ihnen einfällt. Deutsche Sonderzeichen sind nicht erlaubt.

Meine Testrechner zu Hause sind beispielsweise nach den Planeten unseres Sonnensystems benannt, z. B. `jupiter`; als Domain dient `sol`. Daraus ergibt sich dann der vollständige Name `jupiter.sol`.

Verwenden Sie niemals `localhost` als Hostnamen! Dieser Name hat insofern eine Sonderstellung, als dass er als vollständiger Netzwerkname gilt (*fully qualified*). Dem Namen ist immer die Adresse 127.0.0.1 der Loopback-Schnittstelle zugeordnet, unabhängig von den restlichen Parametern der Netzwerkkonfiguration.

Schnittstelle (Interface)

Eine Schnittstelle kann wahlweise einen Hardware-Netzwerkadapter bezeichnen oder einen durch Software implementierten Verbindungspunkt zwischen verschiedenen Netzen.

Ein Rechner hat oft mehrere Schnittstellen mit unterschiedlichen IP-Adressen. Typische Schnittstellen sind die Loopback-Schnittstelle, Ethernet- und WLAN-Schnittstellen sowie eventuell eine PPP-Schnittstelle, falls Sie ein UMTS-Modem verwenden oder sich in einem *Virtual Private Network* befinden.

MAC-Adresse

Bei der MAC-Adresse (Media Access Control) handelt es sich um eine eindeutige ID-Nummer, mit der jeder Ethernet-Controller ausgestattet ist. Die MAC-Nummer ermöglicht eine Identifizierung des Netzwerk-Controllers, noch bevor ihm eine IP-Adresse zugewiesen wird. Die MAC-Adresse wird insbesondere vom Protokoll DHCP genutzt, das Sie im nächsten Kapitel kennenlernen.

Schnittstellennamen

Linux-intern bekommen alle Netzwerkschnittstellen einen Namen zugewiesen. Typische Namen sind `lo` für die Loopback-Schnittstelle, `eth0`, `eth1` etc. für die Ethernet-Schnittstelle, `wlan`*n* für WLAN-Schnittstellen und `ppp`*n* für die PPP-Schnittstellen. Fedora sowie manche Enterprise-Distributionen verwenden eine andere Nomenklatur, z. B. `p5p1` oder `wlp2s0`. Die zugrunde liegenden Namensregeln sollen sicherstellen, dass ein bestimmter Netzwerkadapter immer wieder denselben Device-Namen erhält, selbst dann, wenn ein Computer nachträglich mit weiteren Netzwerkschnittstellen ausgestattet wird.

Loopback-Interface

Die Loopback-Schnittstelle spielt eine besondere Rolle: Sie ermöglicht die Verwendung des Netzwerkprotokolls für lokale Dienste, also zur Kommunikation innerhalb des Rechners. Das klingt vielleicht widersinnig, ist aber für viele elementare Linux-Kommandos erforderlich. Der Grund: Manche Kommandos bauen ihre Kommunikation auf dem Netzwerkprotokoll auf, ganz egal, ob die Daten lokal auf dem Rechner bleiben oder über ein Netz auf einem fremden Rechner weiterverarbeitet werden. Ein Beispiel dafür ist das Druckersystem (CUPS), das Druckjobs sowohl lokal als auch von anderen Rechnern im Netzwerk entgegennimmt. Als IP-Adresse für das Loopback-Interface ist 127.0.0.1 vorgesehen.

Netzwerkmaske, Netzwerk- und Broadcast-Adresse

Die Ausdehnung eines lokalen Netzes wird durch eine sogenannte Maske ausgedrückt. Dabei handelt es sich um vierteilige Zifferngruppen, die intern als Bitmuster für IP-Adressen verwendet werden. Wenn das lokale Netz z. B. alle Nummern 192.168.0.*n* umfasst, lautet die dazugehörige Netzwerkmaske 255.255.255.0, die Netzwerkadresse 192.168.0.0 und die Broadcast-Adresse 192.168.0.255. Bei vielen Konfigurationsprogrammen brauchen Sie weder die Netzwerk- noch die Broadcast-Adresse anzugeben, da sich diese aus der IP-Adresse und der Maske ergeben.

Das resultierende Netzwerk wird jetzt mit 192.168.0.0/255.255.255.0 oder kurz mit 192.168.0.0/24 bezeichnet. Diese Kurzschreibweise heisst auch Präfix-Notation. Die Zahl hinter dem Schrägstrich gibt die Anzahl der binären Einser der Netzwerkmaske an. Zwei Rechner mit den IP-Adressen 192.168.0.71 und 192.168.0.72 können sich in diesem Netzwerk also direkt miteinander verständigen, weil die IP-Adressen im Bereich der Netzwerkmaske übereinstimmen. Die maximale Anzahl von Rechnern, die gleichzeitig in diesem Netz kommunizieren können, beträgt 254 (.1 bis .254) – die Nummern .0 und .255 sind reserviert.

Gateway

Ein Gateway ist ein Rechner, der an der Schnittstelle zwischen zwei Netzen steht, oft zwischen dem lokalen Netz und dem Internet. Damit Ihr Linux-Rechner in einem lokalen Netz auf das Internet zugreifen kann, müssen Sie bei der Konfiguration die Gateway-Adresse angeben.

Die Gateway-Adresse bezeichnet also einen besonderen Rechner im lokalen Netz. In Privathaushalten ist das Gateway oft ein ADSL-Modem oder ein damit verbundener WLAN-Router. Auch ein als HotSpot eingesetztes Smartphone (Tethering) kann als lokales Gateway dienen; in diesem Fall kommunizieren andere Rechner über das WLAN mit dem Smartphone, und dieses leitet die IP-Pakete dann über das Mobilfunknetz in das Internet weiter.

Nameserver

Ein Nameserver ist ein Programm, das Rechnernamen bzw. Internetadressen wie *www.yahoo.com*) in IP-Adressen übersetzt. Bei kleinen Netzen erfolgt die Zuordnung zwischen Namen und Nummern manchmal durch eine statische Tabelle in der Datei `/etc/hosts`. Im Internet übernehmen Rechner mit entsprechenden Datenbanken die-

se Aufgabe. Statt des Begriffs *Nameserver* ist auch die Abkürzung DNS für *Domain Name Server* oder *Services* üblich.

Wenn Sie in einem Webbrowser die Seite *www.yahoo.com* ansehen möchten, wird daher als Erstes der Nameserver kontaktiert, um die IP-Adresse des Webservers von *www.yahoo.com* herauszufinden. Erst nachdem das gelungen ist, wird eine Verbindung mit dieser IP-Adresse hergestellt.

DHCP

Das *Dynamic Host Configuration Protocol* (DHCP) wird oft in lokalen Netzwerken verwendet, um die Administration des Netzwerks zu zentralisieren. Anstatt bei jedem Rechner manuell die IP-Adresse, die Maske, das Gateway, den Nameserver etc. einzustellen, übernimmt ein zentraler DHCP-Server bzw. ein ADSL-Router diese Aufgabe. Alle Rechner im lokalen Netzwerk nehmen beim Hochfahren Kontakt mit dem DHCP-Server auf und fragen diesen, welche Einstellungen sie verwenden sollen. Das reduziert die Client-Konfiguration auf ein Minimum.

IP-Adressen

IP-Adressen werden zur Identifizierung von Rechnern innerhalb eines Netzwerks verwendet. Das gilt sowohl in lokalen Netzen als auch im Internet. Dieser Abschnitt vermittelt Hintergrundinformationen über die Verwendung von IP-Adressen, wobei ich mich vorerst auf das »alte« Protokoll IPv4 beziehe. Informationen zu IPv6 folgen dann im nächsten Abschnitt.

Theoretisch sieht das Protokoll IPv4 256^4, also rund 4 Milliarden IP-Adressen vor. Tatsächlich sind aber weit weniger IP-Adressen verfügbar: Zum einen ist ein Teil der Nummern für Spezialfunktionen reserviert, unter anderem alle IP-Adressen, die mit .0 bzw. .255 enden; zum anderen wurden IP-Adressen früher in recht großzügigen Paketen an Staaten bzw. Firmen vergeben. Mittlerweile ist der Vorrat an freien IPv4-Adressen erschöpft. Internet-Provider sowie Betreiber von Mobilfunknetzen sind deswegen als Erste auf IPv6 umgestiegen.

IP-Adressen im Internet

Wenn Sie einen eigenen Webserver mit dem Internet verbinden möchten, benötigen Sie nicht nur einen weltweit gültigen Domainnamen (z. B. »meinefirma.de«), sondern auch eine eigene IP-Adresse. Diese bekommen Sie von Ihrer Hosting-Firma zugewiesen.

IP-Adressen in lokalen Netzen

Firmen oder Organisationen verwenden in lokalen Netzwerken zumeist IP-Adressen des privaten Adressraums. Nur das Gateway der Firma bzw. bei Privathaushalten der ADSL-Router haben eine öffentliche IP-Adresse. Alle Rechner des lokalen Netzwerks nutzen diese IP-Adresse dann gemeinsam. Das zugrunde liegende Verfahren wird *Masquerading* genannt. Es ist Thema des nächsten Kapitels.

Adressbereich	Netzwerk/Teilnetze
10.0.0.0 – 10.255.255.255	ein Netzwerk für ca. 16 Millionen Adressen
172.16.0.0 – 172.31.255.255	16 Teilnetze (z. B. 172.23.*.*) für je ca. 65.000 Adressen
192.168.0.0 – 192.168.255.255	256 Teilnetze (z. B. 192.168.54.*) für je 254 Adressen

Tabelle 29.2 Reservierte IP-Bereiche für private Netzwerke

Im IPv4-Zahlenraum wurden drei Bereiche für lokale Netzwerke reserviert (siehe Tabelle 29.2): Ganz egal, in welchem Teilnetz Sie Ihr lokales Netz bilden – es ist sichergestellt, dass es zu keinen Adresskonflikten mit »richtigen« IP-Internetadressen kommt.

Ein Rechner, mehrere IP-Adressen

Eine IP-Adresse bezeichnet nicht einen Rechner, sondern eine IP-Schnittstelle. Da die meisten Rechner über mehrere Schnittstellen verfügen, z. B. für den Ethernet-Controller, für den WLAN-Controller und für die Localhost-Schnittstelle, sind einem Rechner oft mehrere IP-Adressen zugewiesen! Wenn von *der* IP-Adresse die Rede ist, als gäbe es nur eine einzige, dann ist zumeist diejenige Adresse gemeint, über die der Rechner im lokalen Netz oder im Internet angesprochen wird.

IPv6

Bis jetzt habe ich mich immer auf IP-Version 4 bezogen (IPv4). Das gesamte Internet in seiner jetzigen Form basiert auf dieser IP-Version. Allerdings gibt es bereits seit 2011 keine freien IPv4-Adressblöcke mehr. Außerdem weist das Protokoll einige funktionelle Mängel auf, weswegen IP für manche Anwendungen schlecht geeignet ist, z. B. für Audio- und Video-Streaming.

IPv6-Adressen

Die schon seit 1998 (!) standardisierte IP-Version 6 behebt diese Mängel. Die wohl markanteste und für Administratoren offensichtlichste Änderung besteht darin, dass für IP-Adressen nun statt 32 gleich 128 Bit vorgesehen sind. In der herkömmlichen Schreibweise würde eine IPv6-Adresse dann so aussehen:

```
121.57.242.17.122.58.243.18.19.123.59.20.244.124.60.245
```

Es ist offensichtlich, dass das nicht praktikabel ist. Um etwas Platz zu sparen, werden IPv6-Adressen in bis zu acht durch das Zeichen : getrennte Gruppen hexadezimaler Zahlen gegliedert, wobei in jeder Gruppe führende Nullen entfallen dürfen:

```
abcd:17:2ff:12aa:2222:783:dd:1234 = abcd:0017:02ff:12aa:2222:0783:00dd:1234
```

Um den Schreibaufwand zu minimieren, gilt :: als Kurzform für mehrere 0-Gruppen:

`abcd:17:0:0:0:0:dd:1234` → `abcd:17::dd:1234`
`0:0:0:0:0:783:dd:1234` → `::783:dd:1234`

Für `localhost` gibt es die noch kompaktere Kurzschreibweise `::1`.

Wenn IPv4-Adressen in IPv6 abgebildet werden, sind die ersten fünf Gruppen 0, die sechste `ffff`. Die abschließenden 32 Bit dürfen statt in hexadezimaler Schreibweise auch in der vertrauten dezimalen Schreibweise angegeben werden:

Abbildung einer IPv4-Adresse: `::ffff:110.111.112.113`

IPv6-Adresstypen

IPv6 unterscheidet zwischen verschiedenen Typen von Adressen, von denen ich hier nur die wichtigsten vorstelle. Beachten Sie, dass Netzwerkschnittstellen zugleich *mehrere* IPv6-Adressen besitzen dürfen, z. B. eine private lokale Adresse (Link-Local) und eine öffentliche Adresse (Global Unicast).

- **Global Unicast:** Das sind »gewöhnliche«, weltweit gültige IP-Adressen. Sie beginnen zumeist mit der Ziffer 2 und eignen sich für eine Punkt-zu-Punkt-Kommunikation.
- **Link-Local:** Das sind private Adressen innerhalb eines lokalen Netzes im Adressbereich fe80::/64. Die Adressen werden automatisch generiert und ermöglichen eine konfigurationslose Kommunikation innerhalb eines lokalen Netzwerks, vergleichbar mit dem Zeroconf-Verfahren für IPv4, das in Abschnitt 29.6 behandelt wird.
- **Site-Local:** Das sind private Adressen innerhalb der Adressbereiche fec0:: bis feff::. Sie können ähnlich wie der IPv4-Bereich 10.*.*.* zur Definition privater lokaler Netzwerke verwendet werden.
- **Multicast:** Adressen im Bereich ff00::/8 sind Multicast-Adressen. An solche Adressen gesendete Pakete werden an alle Geräte im betreffenden Netzwerk geleitet. Der Aufbau von Multicast-Adressen ist durch den Standard RFC 4291 definiert. Multicast-Adressen ersetzen die von IPv4 bekannten Broadcast-Adressen, bieten darüber hinaus aber zusätzliche Möglichkeiten.

Eine detailliertere Beschreibung der IPv6-Grundlagen sowie weiterer Sonderfälle von IPv6-Adressen finden Sie in der Wikipedia und auf der alten, aber weiterhin hilfreichen Linux-IPv6-HowTo-Seite:

http://de.wikipedia.org/wiki/IPv6
http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO

IPv6-Masken und -Subnetze

Auch in IPv6 gilt das Konzept, dass Teilnetze durch Adressmasken gebildet werden. Die Maske wird ausschließlich in der Kurzschreibweise `/n` formuliert; wie bei IPv4 gibt `n` die Anzahl der Bits am Beginn der Adresse an, die unveränderlich sind. Je kleiner `n` ist, desto größer ist die Anzahl der möglichen Adressen im Teilnetz.

Die Adresse 2001:78b:f2f:417::2/64 bedeutet, dass der Rechner ohne Router mit allen anderen Geräten kommunizieren kann, die eine Adresse der Form 2001:78b:f2f:417:* haben. /64 bedeutet, dass die ersten 64 Bit der IP-Adresse das Teilnetz bestimmen und somit vorgegeben sind. Die restlichen 64 Bit dienen zur Identifizierung der Teilnehmer innerhalb des Teilnetzes. Ein /64-Netz bietet Platz für $2^{64} = 18 * 10^{18}$ Adressen, also ca. 4 Milliarden mal mehr Adressen als im gesamten IPv4-Netz!

Da es an IPv6-Adressen keinen Mangel gibt, sehen die IPv6-Richtlinen einen *äußerst* großzügigen Umgang mit Teilnetzen vor: Kleinere Teilnetze als /64 sind gar nicht vorgesehen! Vielmehr ist geplant, dass Internet-Provider jedem Kunden grundsätzlich ein /64-Netz zur Verfügung stellen. Da es erst recht wenige IPv6-Provider gibt, bleibt abzuwarten, ob das auch in der Praxis der Fall sein wird. Sollte es dabei bleiben, wird es beim Aufbau lokaler Firmen- oder Heimnetze keine Limits geben: Wenn Sie nicht gerade jedem Atom Ihres Haushalts seine eigene IPv6-Adresse zuordnen möchten, besteht keine Gefahr, dass Sie den Vorrat Ihrer IPv6-Adressen erschöpfen.

IPv6 und Linux

Der Linux-Kernel kommt mit IPv6 prinzipiell schon seit Anfang 2000 gut zurecht. Auch die meisten Netzwerkanwendungen und Distributionen sind längst IPv6-kompatibel. Wenn Sie beispielsweise einen Blick in die Datei `/etc/hosts` auf Ihrem Rechner werfen, werden Sie feststellen, dass es dort Einträge für *zwei* Localhost-Adressen gibt, einmal für IPv4 und einmal für IPv6:

```
# Datei /etc/hosts
127.0.0.1 localhost
::1       ip6-localhost
```

Mit dem Testkommando `ping6` können Sie IPv6-Pakete an `ip6-localhost` oder an die Adresse `::1` senden:

```
root#  ping6 ip6-localhost
ping6 ip6-localhost
PING ip6-localhost(ip6-localhost) 56 data bytes
64 bytes from ip6-localhost: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from ip6-localhost: icmp_seq=2 ttl=64 time=0.023 ms
<Strg>+<C>
```

Kompatibilität und Tunnel

Grundsätzlich sind IPv4- und IPv6-Netze komplett voneinander getrennt! In einem IPv4-Netz können Sie keine IPv6-Rechner ansprechen und umgekehrt. Immerhin ist ein Parallelbetrieb möglich: Sie können also einen Rechner bzw. eine Netzwerkschnittstelle so einrichten, dass diese IPv4 *und* IPv6 spricht.

IPv4 und IPv6 werden noch über viele Jahre parallel existieren. Um den Mischbetrieb zu vereinfachen, existieren verschiedene Verfahren, um IPv6-Pakete auch über IPv4-Netze zu transportieren – und umgekehrt! Am populärsten sind hierfür sogenannte Tunnel, also spezielle Programme, die z. B. IPv6-Pakete nochmals verpacken und in einem IPv4-Netz zum nächsten IPv6-Router transportieren. Die erforderlichen Tunnelprotokolle sind aber nicht Teil des IPv6-Standards!

Mehrere Firmen bieten kostenlose Tunnel-Services an, z. B. *http://www.tunnelbroker.net*, *http://www.gogo6.com* oder *http://www.sixxs.net*. Nach einer Registrierung können Sie mit diesen Diensten IPv6 ausprobieren, auch wenn Sie selbst nur einen IPv4-Internetzugang haben. Entsprechende Konfigurationsbeispiele folgen in Abschnitt 29.3. Weitere Details können Sie auf der folgenden Website nachlesen, wobei die meisten Informationen über Ubuntu hinaus gültig sind:

https://wiki.ubuntu.com/IPv6

IPv6-Test

Wenn Sie unsicher sind, ob Ihr Rechner IPv6-Zugang hat, besuchen Sie am besten eine der vielen IPv6-Testseiten, z. B. *http://test-ipv6.com* oder *http://ipv6-test.com*. Alternativ können Sie mit `ping6 google.com` ausprobieren, ob Sie eine IPv6-Verbindung zu Google herstellen können. Zu guter Letzt können Sie die Kommandos `ip -6 addr` und `ip -6 route` ausführen. Die Interpretation der Ergebnisse ist aber nicht ganz einfach (siehe auch Abschnitt 29.3).

IPv6 in der Praxis

In der Praxis haben Sie als Desktop-Anwender in der Regel nichts mit IPv6 zu tun. Selbst wenn Ihr Mobilfunk- oder Internet-Provider intern IPv6 verwendet, erfolgt die Kommunikation zu Ihnen meist in einem Tunnel und es sieht so aus, als befänden Sie sich in einem IPv4-Netzwerk. Das ist auch gut so, denn wenn Sie einen echten IPv6-Zugang ohne IPv4-Kompatibilität hätten, gäbe es momentan (Sommer 2013) nur ganz wenige Websites, die Sie besuchen könnten. Ich habe versuchsweise nach *hotel berlin* gesucht und die ersten 20 Treffer in einem reinen IPv6-Netz angeklickt. Ergebnis: Im IPv6-Netz sieht die Berlin-Touristik mager aus, keine einzige Website funktioniert ...

Auch für die Administration lokaler Netzwerke ist IPv6 normalerweise nicht relevant: Es spricht nichts dagegen, ein LAN weiterhin als privates IPv4-Netzwerk einzurichten, z. B. im Adressbereich 192.168.0.*. Im nächsten Kapitel zeige ich Ihnen dennoch, wie Sie allen lokalen Rechnern *zusätzlich* auch eine weltweit eindeutige IPv6-Adresse zuweisen können. Echte Vorteile ergeben sich daraus nur wenige, dafür aber mögliche Sicherheits- und Privacy-Probleme.

Bleibt die Frage, wie wichtig IPv6 für Root-Server ist. Selbst hier können Sie IPv6 noch aus dem Weg gehen, wenn der Server überwiegend für europäische und amerikanische Benutzer gedacht ist. Anders sieht es in manchen afrikanischen oder

asiatischen Ländern aus; hier gibt es eine zunehmende Anzahl von Internetanwendern, die ausschließlich über eine IPv6-Verbindung ohne Tunnel oder andere Kompatibilitätsschichten verfügen. Langfristig geht deswegen für Root-Server kein Weg am Parallelbetrieb von IPv4 und IPv6 vorbei, also an einer sogenannten »Dual-Stack«-Konfiguration. Google, Facebook oder heise.de haben diesen Schritt bereits vor einigen Jahren vollzogen.

WLAN-Standards, Glossar

Zur Beschreibung drahtloser Netze haben sich mehrere Abkürzungen eingebürgert. Am gängigsten ist WLAN (*Wireless Local Area Network*) oder dessen deutsche Variante *Funk-LAN*. In englischen Texten ist sehr oft von WiFi (*Wireless Fidelity*) die Rede, wobei der Begriff oft synonym mit WLAN verwendet wird. Manchmal ist aber auch die *WiFi-Alliance* gemeint, ein Herstellerkonsortium, das sich um die Kompatibilität von WLAN-Produkten kümmert.

802.11x Dieser Abschnitt fasst kurz die WLAN-Terminologie zusammen. Die wichtigsten WLAN-Standards sind durch das IEEE (*Institute of Electrical and Electronics Engineers*) definiert und beginnen alle mit der Nummer 802.11. Die ergänzenden Buchstaben beziehen sich in chronologischer Reihenfolge auf Versionen bzw. Varianten des Standards.

Brutto/netto Die Bruttoübertragungsrate (z. B. 54 MBit/s für 802.11g) in den Prospekten sieht oft vielversprechend aus. Nach Abzug des großen Protokoll-Overheads bleibt davon netto deutlich weniger als die Hälfte übrig – und auch das nur, solange nicht mehr als zwei WLAN-Teilnehmer miteinander kommunizieren, die Funkverbindung gut ist und sich keine Teilnehmer im Netz befinden, deren Hardware noch einen alten WLAN-Standard verwendet.

WLAN-Hardware Es gibt verschiedene Arten von WLAN-Hardware:

- In alle modernen Notebooks ist ein **WLAN-Controller** eingebaut. Bei Desktop-Rechnern oder älteren Geräten kann ein WLAN-USB-Stick diese Funktion übernehmen.
- Eine **WLAN-Bridge** verbindet einen einzelnen Computer mit einem WLAN. Die Bridge erfüllt also dieselbe Funktion wie der eingebaute WLAN-Controller eines Notebooks, nur der Anschluss an den Rechner ist anders: Die Bridge wird durch ein Ethernet-Kabel mit dem Computer verbunden.
- Ein **Access-Point** stellt in einem lokalen Netzwerk einen Zugangspunkt für mehrere WLAN-Clients her. Der Access-Point wird mit einem Ethernet-Kabel an das lokale Netzwerk angeschlossen. Im Unterschied zur Bridge kann ein Access-Point mit mehreren Clients gleichzeitig kommunizieren.

- Ein **WLAN-Router** agiert ähnlich wie ein Access-Point, ist aber »intelligenter«: Das Gerät enthält unter anderem einen eigenen DHCP-Server, um den WLAN-Clients Ihre IP-Daten zuzuweisen. In viele moderne ADSL-Modems ist ein WLAN-Router integriert. Derartige Geräte bezeichnet man dann oft als *Gateways*.

Die Konfiguration von WLAN-Geräten erfolgt zumeist durch einen Webbrowser. Dazu stellen die Geräte unter einer bestimmten IP-Adresse (z. B. *http://192.168.0.1*) eigene Webseiten zur Konfiguration zur Verfügung. Beachten Sie aber, dass es vereinzelt auch WLAN-Geräte gibt, die nur durch ein unter Windows laufendes Setup-Programm konfiguriert werden können. Das betrifft insbesondere WLAN-Bridges. Solche Geräte sind für Linux nur eingeschränkt brauchbar.

WLAN-Verbindungsparameter

Wenn Sie eine Verbindung zwischen zwei WLAN-Geräten herstellen, müssen Sie diverse Parameter einstellen.

Network-Modus

WLAN-Komponenten können auf unterschiedliche Arten miteinander kommunizieren. Im Folgenden sind nur die drei wichtigsten Modi kurz beschrieben:

- Der *Infrastructure Mode* (manchmal auch *Managed Mode* genannt) erlaubt die Kommunikation mit einem zentralen Zugangspunkt. Die Netzwerkstruktur ist also sternförmig. Meist ist der Zugangspunkt ein Access-Point oder ein WLAN-Router, es kann aber auch ein entsprechend konfigurierter Rechner sein.
- Das WLAN-Gerät des Access Points läuft im *Master Mode*. Der Infrastucture Mode gilt also gewissermaßen für die Clients, während der Master Mode für den Server eines WLANs zur Anwendung kommt.
- Beim *Ad-hoc Mode* kommuniziert jedes WLAN-Gerät direkt mit jedem anderen WLAN-Gerät, das in Funkreichweite ist.

SSID bzw. ESSID

Die Abkürzungen SSID (*Service Set Identification*) bzw. ESSID (*Extended SSID*) bezeichnen eine Zeichenkette, die einem WLAN-Netz einen Namen gibt. WLAN-Geräte können nur dann miteinander kommunizieren, wenn ihre SSIDs übereinstimmen.

Als SSID ist oft der Herstellername voreingestellt. Deswegen können Geräte desselben Herstellers oft auf Anhieb miteinander kommunizieren, während bei Geräten unterschiedlicher Herkunft zuerst eine gemeinsame SSID-Zeichenkette eingestellt werden muss.

Manche WLAN-Karten sehen für die SSID eine Auto-Konfiguration vor (Einstellung ANY). Beachten Sie, dass bei der SSID-Zeichenkette zwischen Groß- und Kleinschreibung unterschieden wird!

NWID

Innerhalb eines WLAN-Netzes mit einheitlicher SSID kann es mehrere Teilnetze (Cells) geben, zwischen denen mit der NWID (*Network ID*) differenziert wird. In der Praxis kommt das aber nur selten vor, weswegen manche Konfigurationsprogramme auf die NWID gleich ganz verzichten.

Manchmal wird statt NWID der verwirrende Begriff *Domain* verwendet. Mit dem herkömmlichen Domainnamen von IP-Adressen hat die NWID aber nichts zu tun.

Channel

Innerhalb des durch den jeweiligen 802.11x-Standard vorgesehenen Frequenzbandes gibt es mehrere Teilbereiche (Kanäle, Channels), auf denen parallel gesendet werden kann. Im Infrastructure Mode erkennen WLAN-Adapter selbstständig den vom Access Point verwendeten Kanal. Eine explizite Einstellung des Kanals ist nur notwendig, wenn es zu Interferenzen mehrerer WLANs kommt.

WLAN-Sicherheit

Grundsätzlich ist es möglich, ein WLAN unverschlüsselt zu betreiben. Dann kann aber jeder, der sich in Reichweite des Funknetzes befindet, dieses nutzen und die gesamte Kommunikation abhören. Ein unverschlüsselter Betrieb ist daher grob fahrlässig!

WEP

Zur Verschlüsselung des Datenverkehrs kam bei den ersten WLAN-Generationen das Verfahren *Wired Equivalent Privacy* (WEP) zum Einsatz. Dabei werden die Daten wahlweise mit einem 40- oder 104-Bit-Schlüssel verschlüsselt. Oft ist auch von 64- bzw. 128-Bit-Verschlüsselung die Rede. Die restlichen 24 Bit dienen aber nicht zur eigentlichen Verschlüsselung.

Der WEP-Schlüssel wird in der Regel als hexadezimale Zahl angegeben (10 bzw. 26 Stellen, je nach der Bitanzahl des Schlüssels). Manche Konfigurationswerkzeuge bieten Ihnen auch die Möglichkeit, den Schlüssel aus einer »Passphrase« zu erzeugen, also aus einem Text, der auch aus mehreren Wörtern bestehen darf.

Bei der WEP-Konfiguration können bis zu vier Schlüssel eingegeben werden. Tatsächlich genutzt wird immer nur einer. Die Verwaltung von vier Schlüsseln hat aber den Vorteil, dass Sie bei einem Wechsel des WLAN-Netzes nicht den ganzen Schlüssel neu eingeben müssen, sondern einfach den aktiven Schlüssel wechseln.

Vermeiden Sie WEP!

WEP hat sich aufgrund von gravierenden Konzeptmängeln als unsicher herausgestellt! Selbst ein 104-Bit-Schlüssel kann durch simples Abhören des WLAN-Verkehrs innerhalb weniger Minuten ermittelt werden.

WPA, WPA2

Die Nachfolge von WEP haben die Verfahren *WiFi Protected Access* (kurz WPA) sowie dessen verbesserte Version WPA2 angetreten. Die genaue Spezifikation von WPA2 ist im Standard 802.11i niedergeschrieben. Der wichtigste Unterschied zwischen WPA und WPA2 ist der Verschlüsselungsalgorithmus: RC4 bei WPA, AES bei WPA2.

WPA war als Übergangslösung bis zur Fertigstellung des 802.11i-Standards gedacht. Da es aber WLAN-Hardware gibt, die nur WPA, aber noch nicht WPA2 unterstützt, werden auf absehbare Zeit beide Varianten im Einsatz bleiben.

Der wesentliche Vorteil von WPA besteht darin, dass der Schlüssel nur zur Initialisierung der Verbindung eingesetzt wird. Sobald die Verbindung steht, werden die Schlüssel nach einem ausgeklügelten Verfahren ständig gewechselt. WPA und WPA2 gelten nach aktuellem Stand der Technik als sicher, sofern eine ausreichend lange Passphrase eingesetzt wird, also ein aus mehreren Wörtern und Zeichen bestehender Schlüssel.

Dieses Buch behandelt nur die WPA/WPA2-Variante *Pre-Shared Key* (kurz PSK, oft auch *WPA-Personal* genannt): Hier melden sich alle WLAN-Nutzer mit demselben Schlüssel im Netz an. Bei der noch sichereren Variante *Managed Key* hat jeder Nutzer einen eigenen Schlüssel, allerdings müssen die Schlüssel nun auf einem zentralen Server verwaltet werden.

Sichern Sie auch das WLAN-Gerät an sich ab!

Die Einstellungen des WLAN-Routers oder Access Points werden normalerweise per Webbrowser verändert. Der Webzugang ist durch ein firmenspezifisches Passwort abgesichert, das Sie unbedingt ändern sollten! Generell sollten Sie die Fernwartung so weit wie möglich einschränken und nicht per WLAN, sondern nur über eine LAN-Verbindung durchführen.

Firewall und VPN

Durch eine Firewall können Sie den WLAN-Datenverkehr gezielt auf bestimmte Protokolle, Netzwerksegmente etc. beschränken. Ein anderer Ansatzpunkt besteht darin, das WLAN trotz aller anderen Schutzmaßnahmen als unsicher zu betrachten. Um dennoch sicher zu kommunizieren, verschlüsseln Sie Ihren Datenverkehr selbst. Am populärsten ist für diesen Zweck die Verwendung eines VPN (Virtual Private Network).

Linux-Unterstützung für WLANs

Wireless-Tools und iw

In der Vergangenheit spielten die Linux-Wireless-Tools einge große Rolle bei der Nutzung von WLAN-Komponenten. Die Wireless-Tools bestehen aus mehreren Kommandos (`iwconfig`, `iwlist` etc.) zur Konfiguration der WLAN-Adapter.

Die Wireless-Tools sind aus dem Linux-WLAN-Alltag zwar noch nicht ganz wegzudenken, sie gelten aber als konzeptionell veraltet. Mit der vor einigen Jahren begonnenen Generalüberholung der Linux-WLAN-Treiber wurde das neue Steuerungskommando `iw` entwickelt. `iw` kann allerdings nur für WLAN-Controller verwendet werden, deren Treiber die nl80211-Schnittstelle unterstützen.

Aus diesem Grund installieren viele Linux-Distributionen die Kommandos `iwconfig` und `iw` parallel. Hintergrundinformationen zu beiden Linux-Wireless-Systemen finden Sie hier:

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
http://wireless.kernel.org

Hardware-Treiber

Die eigentlichen WLAN-Hardware-Treiber befinden sich in Kernelmodulen. Aktuelle Treiber basieren auf dem mac80211-Framework und sind zur nl80211-Schnittstelle und damit zum Kommando `iw` kompatibel. Linux enthält Treiber zu nahezu allen marktüblichen WLAN-Adaptern – aber wie immer gibt es Ausnahmen. Besonders problematisch sind ganz neue WLAN-Adapter: Selbst bei einer guten Kooperation zwischen dem Hardware-Hersteller und der Linux-Entwicklergemeinde dauert es oft ein ganzes Jahr, bis neue Treiber den Weg in aktuelle Distributionen finden. Es lohnt sich also, vor dem Kauf eines Notebooks ein wenig im Internet zu recherchieren!

Firmware

Die meisten WLAN-Controller können Sie selbst programmieren. Damit sie funktionieren, muss während der Initialisierung die sogenannte Firmware, also controllerinterner Programmcode, in den Controller übertragen werden. Die Firmware stammt von den Controller-Herstellern und darf unter Einhaltung der jeweiligen Lizenzbedingungen frei weitergegeben werden. Um die Übertragung des Codes in den Controller kümmert sich in der Regel das Kernelmodul oder das `udev`-System. Der Controller-Code befindet sich in Binärdateien (Blobs), zumeist im Verzeichnis `/lib/firmware`.

Die Chip-Hersteller stellen die Firmware nur in binärer Form zur Verfügung, nicht als Quellcode. Das ist aus Open-Source-Sicht betrüblich und wird vor allem von der Debian-Entwicklergemeinde kritisiert. Bei der Installation von Debian müssen Sie Firmware-Dateien zuerst aus dem Internet herunterladen und dann auf einem eigenen Datenträger zur Verfügung stellen (siehe Abschnitt 3.2).

Persönlich sehe ich das Firmware-Problem entspannter als die Debian-Entwickler: Früher wäre dem WLAN-Controller ein EPROM hinzugefügt worden, und kein Hahn hätte danach gekräht, dass dieses keinen Open-Source-Code enthält. Die jetzige Lösung ist billiger und erlaubt Updates. Natürlich wäre es wünschenswert, wenn auch für die im Controller ausgeführten Programme der Quellcode verfügbar wäre, aber diese Hoffnung ist unrealistisch.

29.3 Manuelle LAN- und WLAN-Konfiguration

Normalerweise wird Ihr LAN- bzw. WLAN-Controller während des Rechnerstarts automatisch erkannt und initialisiert. Dieser Abschnitt zeigt, wie dieser Prozess hinter den Kulissen abläuft bzw. welche Schritte erforderlich sind, um die Initialisierung von Hand durchzuführen. Das hilft, die Netzwerkgrundlagen besser zu verstehen und die Benutzeroberflächen gängiger Konfigurationswerkzeuge sicherer zu verwenden.

LAN-Controller manuell aktivieren

Der Netzwerk- bzw. LAN-Controller ist in der Regel ein Chip auf dem Mainboard Ihres Rechners, der Ethernet-Netzwerkfunktionen zur Verfügung stellt. Der Controller kann aber auch in die CPU integriert sein oder extern in Form eines USB-Steckers realisiert sein. Unabhängig davon, wie die Netzwerkfunktionen physikalisch realisiert sind, spreche ich im Folgenden nur noch vom Netzwerk-Controller.

Hardware-Erkennung

Im ersten Schritt stellen Sie sicher, dass das richtige Kernelmodul für Ihren Netzwerk-Controller geladen wird. Oft gelingt dies dem Kernel automatisch. In diesem Fall wird das Kommando `ip link set eth0 up` ohne Fehlermeldung ausgeführt. Treten an dieser Stelle Probleme auf, müssen Sie herausfinden, welcher Netzwerk-Controller in Ihrem Rechner steckt und welches Kernelmodul dafür verantwortlich ist. Erste Informationen liefert in solchen Fällen `lspci`:

```
root#  lspci | grep -i net
02:01.0 Ethernet controller: Intel Corporation 82540EP Gigabit Ethernet
                             Controller (Mobile) (rev 03)
```

Das Notebook verwendet also den Gigabit-Ethernet-Controller 82540EP von Intel. Der zweite Schritt besteht nun darin, dem Controller einen passenden Treiber zuzuordnen (also ein Kernelmodul aus dem Verzeichnis `/lib/modules/n.n/net/*`). Eine Internetsuche nach *linux kernel module 82540EP* führt rasch zum richtigen Kernelmodul `e1000`:

```
root#  modinfo e1000
filename:       /lib/modules/3.2.0-26-generic/kernel/drivers/net/ethernet/intel/
                  e1000/e1000.ko
description:    Intel(R) PRO/1000 Network Driver
...
```

Mit `lsmod` können Sie nun überprüfen, ob das Modul bereits geladen ist. In der Regel wird das der Fall sein, d. h., Linux hat den Controller während des Systemstarts bereits richtig erkannt. Nur wenn das nicht der Fall ist, müssen Sie mit `modprobe` das passende Modul laden:

```
root#  modprobe e1000
```

`dmesg` zeigt, ob beim Laden des Moduls Fehler auftreten (was hier nicht der Fall ist). Die Warnung *link is not ready* besagt nur, dass die Schnittstelle momentan mangels Konfiguration noch nicht aktiv ist.

```
root#  dmesg -c
...
Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
e1000 0000:02:01.0: PCI INT A -> Link[LNKA] -> GSI 11 (level, low) -> IRQ 11
e1000: 0000:02:01.0: e1000_probe: (PCI:33MHz:32-bit) 00:11:25:32:4f:5d
e1000: eth0: e1000_probe: Intel(R) PRO/1000 Network Connection
ADDRCONF(NETDEV_UP): eth0: link is not ready
...
```

Im Regelfall wird das Modul automatisch während der Initialisierung des Rechners geladen. Sollte das nicht funktionieren, tragen Sie die Zuordnung zwischen der Schnittstelle `eth0` und dem Kernelmodul `e1000` in die Modulkonfigurationsdatei ein:

```
# Modulkonfigurationsdatei /etc/modprobe.d/config.conf
alias eth0 e1000
```

Liste der Netzwerkschnittstellen

Netzwerkschnittstellen haben je nach Distribution unterschiedliche Namen. Während die erste Ethernet-Schnittstelle unter Debian, openSUSE und Ubuntu `eth0` heißt, verwendet Fedora Device-Namen wie `enp0s5` oder `p5p1`. Eine Liste aller auf Ihrem Rechner verfügbaren Netzwerkschnittstellen liefert das Kommando `ip link show`:

```
root#  ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 ...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 ...
```

Aktivierung der Schnittstelle

Anschließend aktivieren Sie die gewünschte Netzwerkschnittstelle mit `ip link set xxx up`:

```
root#  ip link set eth0 up
```

Konfiguration der Schnittstelle

Um die Netzwerkschnittstelle zu konfigurieren, führen Sie das Kommando `ip addr add` aus. `ip addr show eth0` zeigt anschließend alle bekannten Informationen zur Netzwerkschnittstelle an:

```
root#  ip addr add 192.168.0.2/24 dev eth0
root#  ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
          pfifo_fast state UP qlen 1000
    link/ether 00:1c:42:85:09:a1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.2/24 scope global eth0
       valid_lft forever preferred_lft forever
```

Nun können Sie mit `ping` überprüfen, ob Sie Kontakt zu anderen Rechnern im lokalen Netzwerk aufnehmen können. Die Option `-c 2` bewirkt, dass genau zwei `ping`-Pakete versendet werden:

```
root#  ping -c 2 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=2.95 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.169 ms

--- 192.168.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.169/1.560/2.952/1.392 ms
```

»ip« versus »ifconfig« und »route«

In vielen Büchern zur Linux-Netzwerkkonfiguration sind die Kommandos `ifconfig` und `route` beschrieben. Das galt auch für die ersten 12 Auflagen dieses Buchs. `ifconfig` und `route` gelten aber schon seit einiger Zeit als veraltet.

`ip` bietet diverse Zusatzfunktionen, die in `ifconfig` und `route` fehlen, und ist speziell für die Netzwerkfunktionen des Linux-Kernels optimiert. Erfahrene Administratoren sollten sich jetzt von alten Gewohnheiten trennen und auf das neue Kommando `ip` umsteigen! Und Linux-Einsteiger machen um `ifconfig` und `route` am besten von Anfang an einen weiten Bogen.

Nameserver-Konfiguration

`ping` funktioniert momentan nur, wenn Sie die richtige IP-Adresse angeben. Damit Sie stattdessen auch einen Rechnernamen angeben können, muss `/etc/resolv.conf` die IP-Adresse eines Nameservers enthalten. Das folgende Beispiel geht davon aus, dass es im lokalen Netz einen eigenen Nameserver mit der IP-Adresse 192.168.0.1 gibt. Der Nameserver kann aber auch außerhalb sein und vom Internet-Provider zur Verfügung gestellt werden. (Details zu dieser Konfigurationsdatei folgen in Abschnitt 29.4.)

```
# /etc/resolv.conv
nameserver 192.168.0.1
```

Default-Gateway

Momentan können Pakete nur innerhalb des lokalen Netzwerks versandt werden. Damit auch ein Kontakt in das Internet möglich wird, muss der Rechner wissen, wohin er derartige Pakete leiten soll. Sie müssen dazu die Adresse des Internet-Gateways Ihres Netzwerks mit `ip route` angeben. Das folgende Beispiel geht davon aus, dass die IP-Adresse des Gateways 192.168.0.1 ist:

```
root#  ip route add default via 192.168.0.1
```

`ip route` ohne weitere Parameter liefert die Routing-Tabelle. Die Gateway-Adresse ist in der Zeile enthalten, die mit `default` beginnt.

```
root#  ip route
default via 10.211.55.1 dev eth0
192.168.0.0/24 dev eth0  proto kernel  scope link  src 192.168.0.2
```

Jetzt sollte es möglich sein, Pakete an beliebige Adressen im Internet zu senden:

```
root#  ping -c 2 yahoo.com
PING yahoo.com (216.109.112.135) 56(84) bytes of data.
64 bytes from w2.rc.vip.dcn.yahoo.com (216.109.112.135): icmp_seq=1
  ttl=52 time=116 ms
64 bytes from w2.rc.vip.dcn.yahoo.com (216.109.112.135): icmp_seq=2
  ttl=52 time=115 ms

--- yahoo.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 115.397/115.807/116.217/0.410 ms
```

Loopback-Schnittstelle aktivieren

Eine manuelle Konfiguration der Loopback-Schnittstelle ist selten erforderlich. Falls doch, führen Sie die beiden folgenden Kommandos aus:

```
root#  ip link set lo up
root#  ip addr add 127.0.0.1 dev lo
```

Deaktivierung der Schnittstelle

Grundsätzlich können Sie mit `ip addr del` bzw. `ip route del` zuvor durchgeführte Adresszuweisungen oder Routen-Definitionen wieder rückgängig machen. Dabei müssen Sie exakt dieselben Parameter angeben wie beim entsprechenden Kommando `ip xxx add`:

```
root#  ip addr add 192.168.0.2/24 dev eth0
root#  ip addr del 192.168.0.2/24 dev eth0
```

Um eine Netzwerkschnittstelle ganz zu deaktivieren, also alle Adress- und Routen-Daten zu löschen, führen Sie `ip addr flush` aus:

```
root#  ip addr flush dev eth0
```

DHCP-Informationen abrufen

DHCP-Informationen abrufen

Falls es im Netzwerk einen DHCP-Server gibt, können Sie diesen zur Konfiguration zu Hilfe nehmen. Nach der Aktivierung der Schnittstelle durch `if link set eth0 up` führen Sie bei den meisten Distributionen das Kommando `dhclient` aus:

```
root#  dhclient eth0
...
Listening on LPF/eth0/00:11:25:32:4f:5d
Sending on   LPF/eth0/00:11:25:32:4f:5d
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
```

```
DHCPOFFER from 192.168.0.1
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.0.1
bound to 192.168.0.15 -- renewal in 36624 seconds.
```

Bei SUSE kommen Sie mit `dhcpcd` zum Ziel:

```
root#  dhcpcd eth0
```

Ad-hoc-Netzwerkkonfiguration

Die Kommandos `dhclient` bzw. `dhcpcd` bieten oft den schnellsten Weg, um auf einem noch nicht konfigurierten Rechner ad hoc einen Netzwerkzugang herzustellen. Sie ersparen sich die `ip`-Kommandos und die manuelle Einstellung von `/etc/resolv.conf`. Die einzige Voraussetzung ist ein DHCP-Server im lokalen Netzwerk.

IPv6-Konfiguration

Alle bisherigen Beispiele haben sich auf IPv4 bezogen. Selbstverständlich können Sie mit dem `ip`-Kommando auch eine IPv6-Konfiguration durchführen. Die folgenden Kommandos setzen voraus, dass Sie über das IPv6-Subnetz 2a01:4f8:161:107::/64 verfügen und die Gateway-Adresse fe80::1 verwenden können. Der Schnittstelle `eth0` wird die Adresse 2a01:4f8:161:107::2 zugewiesen. Zum Ausprobieren senden Sie mit `ping6` Kommandos an einen Server, von dem Sie wissen, dass er IPv6-tauglich konfiguriert ist.

```
root#  ip -6 addr add 2a01:4f8:161:107::2/64 dev eth0
root#  ip -6 route add default via fe80::1 dev eth0
root#  ping6 -n google.com
PING google.com(2a00:1450:4009:805::1002) 56 data bytes
64 bytes from 2a00:1450:4009:805::1002: icmp_seq=1 ttl=54 time=19.7 ms
64 bytes from 2a00:1450:4009:805::1002: icmp_seq=2 ttl=54 time=19.1 ms
<Strg>+<C>
```

IPv6-Konfiguration testen

Das gerade erwähnte Kommando `ping6` eignet sich für erste IPv6-Tests am besten. Sollte `ping6` die Fehlermeldung *connect: Das Netzwerk ist nicht erreichbar* liefern, können Sie die IPv6-Konfiguration mit dem Kommando `ip` genauer ansehen.

`ip addr show xxx` liefert detaillierte Daten zur Netzwerkschnittstelle `xxx`. Die mit `link/ether` beginnende Zeile gibt die MAC-Adresse der Schnittstelle an. Die mit `inet` beginnende Zeile enthält die IPv4-Adresse samt Maske in der Kurzschreibweise `/n` sowie die Broadcast-Adresse. Die Zeilen, die mit `inet6` beginnen, geben die IPv6-Adressen an; das können mehrere sein. Eine »richtige« IPv6-Konfiguration setzt voraus, dass die Schnittstelle mit einer globalen Unicast-Adresse verbunden ist, die üblicherweise mit der Ziffer 2 beginnt.

Eine IPv6-Adresse alleine reicht nicht aus, Linux muss auch wissen, wohin es IPv6-Pakete leiten soll. Mit `ip -6 route | grep default` ermitteln Sie das Default-Gateway für IPv6.

Im ersten Beispiel besteht nur eine IPv4-Konfiguration. Die in der Zeile `inet6` angegebene Adresse ist nur eine sogenannte Link-Local-Adresse, die automatisch eingerichtet wird und eine Kommunikation innerhalb eines lokalen Netzwerks erlaubt (vergleichbar mit Zeroconf für IPv4, siehe auch Abschnitt 29.6). Es gibt kein IPv6-Gateway.

```
root#  ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 ...
  link/ether 00:1c:42:d0:29:34 brd ff:ff:ff:ff:ff:ff
  inet  10.0.0.13/24 brd 10.0.0.255 scope global eth0
  inet6 fe80::21c:42ff:fed0:2934/64 scope link
    valid_lft forever preferred_lft forever
root#  ip -6 route | grep default
-- kein Ergebnis --
```

Das zweite Beispiel zeigt die Ergebnisse auf einem Root-Server mit IPv4- *und* IPv6-Konfiguration. Der Schnittstelle `eth0` ist die Unicast-Adresse 2a01:xxx::2 zugewiesen (`scope global` im `ip`-Ergebnis), als IPv6-Gateway ist fe80::1 eingerichtet.

```
root#  ip  addr show eth0
3: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 54:04:a6:f1:74:1f brd ff:ff:ff:ff:ff:ff
    inet 5.9.22.18 peer 5.9.22.1/32 brd 5.9.22.31 scope global eth0
    inet6 2a01:4f8:161:107::2/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::5604:a6ff:fef1:741f/64 scope link
       valid_lft forever preferred_lft forever
root#  ip -6 route | grep default
default via fe80::1 dev eth0  metric 1024
```

IPv6-Tunnel einrichten (Gogo)

Damit Sie IPv6 auch dann ausprobieren können, wenn Sie nur eine IPv4-Anbindung haben, gibt es verschiedene, zum Teil sogar kostenlose Tunnel-Dienste. Ich stelle Ihnen hier exemplarisch die Verwendung des Dienstes Freenet6 von *gogo6.com* vor. Damit können Sie einzelne Rechner unkompliziert mit einer IPv6-Adresse ausstatten. Der Dienst funktioniert selbst dann problemlos, wenn sich Ihr Rechner in einem lokalen Netzwerk mit NAT befindet.

Der IPv6-Tunnel wird durch das Programm `gogoc` eingerichtet. Fedora und Ubuntu stellen dazu das gleichnamige Paket zur Verfügung, bei anderen Distributionen müssen Sie das Programm eventuell von *gogo6.com* herunterladen. `gogoc` funktioniert prinzipiell auf Anhieb und ohne Registrierung und Konfiguration. Allerdings erhalten Sie dann nur eine dynamische, anonyme IPv6-Adresse. Das reicht aus, um mit Ihrem Rechner externe IPv6-Dienste zu testen.

Wenn Sie möchten, dass Ihr Rechner selbst aus dem Internet mit einer immer gleich bleibenden IPv6-Adresse erreichbar ist, müssen Sie sich auf der folgenden Website kostenlos registrieren:

http://www.gogo6.com/freenet6/register-amsterdam

Sie erhalten dann eine E-Mail mit Ihrem Benutzernamen und Passwort. In der Konfigurationsdatei `/etc/gogoc/gogoc.conf` ändern Sie die folgenden vier Zeilen:

```
# Datei /etc/gogoc/gogoc.conf
userid=<login-name>
passwd=<passwort>
server=amsterdam.freenet6.net
auth_method=any
```

Unter Fedora starten Sie das Programm erstmalig durch das Kommando `gogoc`. Beim ersten Start müssen Sie bestätigen, dass Sie eine Verbindung zum Server *amsterdam.freenet6.net* herstellen möchten. Unter Ubuntu führen Sie vor dem ersten Start `gogoc -n` aus, um den erforderlichen Schlüssel herunterzuladen. Sobald das gelungen ist, beenden Sie das Programm mit Strg+C.

In der Folge starten Sie `gogoc` mit `service` als Hintergrunddienst. Dabei wird die Schnittstelle `tun` mit Ihrer IPv6-Adresse eingerichtet. Diese Schnittstelle dient auch als IPv6-Gateway:

```
root#  service gogoc start
root#  ip addr show tun
4: tun: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1280 qdisc ...
    link/none
    inet6 2001:5c0:4100:b::5256/128 scope global
       valid_lft forever preferred_lft forever
root#  ip -6 route
2001:5c0:4100:b::5256 dev tun  metric 0
    cache
2001:5c0:4100:b::5256 dev tun  proto kernel  metric 256  mtu 1280
2000::/3 dev tun  metric 1
fe80::/64 dev p5p1  proto kernel  metric 256
fe80::/64 dev wlp2s0  proto kernel  metric 256
default dev tun  metric 1
```

Nachdem Sie sich vergewissert haben, dass alles funktioniert, können Sie den `gogoc`-Dienst nun mit `service gogo start/stop` starten und beenden. Unter Ubuntu wird der Dienst in Zukunft automatisch gestartet. Unter Fedora müssen Sie hingegen einmal das folgende Kommando ausführen:

```
root#  systemctl enable gogoc
```

Vorsicht – der IPv6-Tunnel funktioniert in beide Richtungen!

Jetzt haben Sie Ihren Rechner also mit einer statischen IPv6-Adresse ausgestattet: »Sie sind drin!«, um den alten Werbeslogan nochmals aufzuwärmen. Das heißt aber auch: Ihr Rechner ist aus dem gesamten IPv6-Internet erreich- und angreifbar! Während Ihr Rechner bei einer IPv4-Konfiguration einen gewissen Schutz durch die vom ADSL-Router eingesetzten Masquerading-Technik und eventuell auch durch die Firewall des Routers genießt, gilt dies für IPv6 nicht mehr!

Sie sollten also sicherstellen, dass keine durch IPv6 erreichbaren Netzwerkdienste laufen, bzw. diese durch eine Firewall absichern! Dieser Rat ist freilich leichter ausgesprochen als befolgt, weil die meisten Firewall-Werkzeuge keine Trennung zwischen IPv4 und IPv6 vorsehen. Wenn Sie einen Rechner im lokalen Netzwerk per IPv4 nutzen und es gleichzeitig einen IPv6-Tunnel gibt, wäre es wünschenswert, den Zugriff auf Samba-Verzeichnisse per IPv4 zuzulassen, aber per IPv6 zu blockieren. Wenn Ihre Firewall hierfür keine Lösung bietet, müssen Sie die einzelnen Dienste – also den SSH-Dämon, den Samba-Server etc. – einzeln entsprechend konfigurieren.

IPv6-Tunnel einrichten (SixXs)

Die Organisation SixXs (*http://www.sixxs.net*) bietet ähnlich wie Gogo kostenlose IPv6-Tunnel an. Die technische Realisierung ist ein wenig anders. Den Tunnel stellt ein Client-Programm mit dem merkwürdigen Namen `aiccu` her. Das funktioniert auch aus einem privaten IPv4-Netz heraus (NAT). Im Unterschied zu Gogo6 ist die Registrierung bei SixXs unausweichlich. Ihre Angaben werden manuell verarbeitet, was ein wenig Geduld erfordert.

Dafür erhalten Sie aber nicht nur eine einzelne IPv6-Adresse, sondern können im nächsten Schritt ein ganzes /64-Adresspaket anfordern, später sogar ein /48-Netz. Im nächsten Kapitel zeige ich Ihnen, wie Sie einen Router konfigurieren, um Ihr ganzes lokales Netzwerk auf IPv6 umzustellen.

Die Kurzschreibweise /64 bedeutet, dass die ersten 64 Bit der Netzwerkmaske gesetzt sind. Das resultierende Netz enthält 4 Milliarden Mal mehr Adressen als das gesamte IPv4-Netz!

Nach der Installation des `aiccu`-Pakets müssen Sie Ihre per E-Mail zugesandten Daten in die Konfigurationsdatei `/etc/aiccu.conf` eintragen:

```
# Datei /etc/aiccu.conf
username xxxxx-SIXXS
password yyyyyy
server tic.sixxs.net
tunnel_id Tnnnnnn
automatic true
behindnat true
```

Anschließend können Sie den Dienst mit `service` starten:

```
root#  service aiccu start
root#  ip -6 addr sixxs
5: sixxs: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1280 qlen 500
    inet6 2001:78b:f2f:417::2/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::48b:f2f:741:2/64 scope link
       valid_lft forever preferred_lft forever
root#  ip -6 route | grep default
default via 2001:78b:f2f:417::1 dev sixxs  metric 1024
```

Wenn alles funktioniert, müssen Sie sich bei einigen Distributionen noch darum kümmern, dass `aiccu` in Zukunft automatisch ausgeführt wird, z. B. durch `systemctl enable aiccu` unter Fedora.

WLAN-Controller manuell steuern

Hardware-Erkennung

Das Kernelmodul für den WLAN-Controller wird im Regelfall automatisch geladen. Bei den meisten Distributionen hat die WLAN-Schnittstelle den Namen `wlan0`, aber auch die Schnittstellennamen `eth1` oder `wlpxxx` sind gebräuchlich. Wenn Sie unsicher sind, ermitteln Sie mit `ip link` eine Liste aller Schnittstellen. `dmesg | egrep -i 'wlan|wifi'` liefert alle relevanten Kernelmeldungen.

Aktuellen Status ermitteln

Mit `iw dev` *name* `info` und `iw dev` *name* `link` können Sie den Status der Schnittstelle herausfinden. Im folgenden Beispiel existiert eine aktive Verbindung.

```
root#  iw dev wlan0 info
Interface wlan0
        ifindex 3
        type managed
        wiphy 2
root#  iw dev wlan0 link
Connected to 00:16:b6:9d:ff:4b (on wlan0)
        SSID: wlan-sol2
        freq: 2462
        RX: 102262 bytes (1784 packets)
        TX: 12815 bytes (86 packets)
        signal: -59 dBm
        tx bitrate: 54.0 MBit/s
        bss flags:      short-preamble short-slot-time
        dtim period:    0
        beacon int:     100
```

Eine Zusammenfassung über die aktuelle Qualität der WLAN-Verbindung gibt auch die Pseudodatei `/proc/net/wireless`:

```
root#  cat /proc/net/wireless
Inter-| sta-|   Quality        |   Discarded packets               | Missed | WE
```

```
face | tus | link level noise |  nwid  crypt   frag  retry   misc | beacon | 22
 eth1: 0020   91.  189.    0.       0      0      0      0      4        0
```

WLAN-Schnittstelle einrichten und löschen

Wenn `iw` die Schnittstelle `wlan0` nicht kennt (Fehlermeldung *no such device*), müssen Sie die Schnittstelle zuerst einrichten. Dazu dient das `iw`-Kommando `interface add`:

```
root#  iw phy phy0 interface add wlan0 type managed
```

`phy0` adressiert den ersten (und bei den meisten Rechnern auch einzigen) WLAN-Controller. Anstelle von `managed` können Sie auch die Schnittstellentypen `monitor`, `wds`, `mesh` bzw. `mp` sowie `ibss` bzw. `adhoc` angeben. Die neue Schnittstelle muss anschließend aktiviert werden.

```
root#  ip link set wlan0 up
```

Sollten Sie die Schnittstelle nicht mehr benötigen, können Sie sie mit `iw del` wieder löschen:

```
root#  iw dev wlan0 del
```

WLAN-Verbindung herstellen

`iw scan` liefert detaillierte Informationen zu allen in Reichweite befindlichen Funknetzen. `grep` macht daraus eine simple Liste aller Netzwerknamen (SSIDs):

```
root#  iw dev wlan0 scan | grep SSID
    SSID: myhome
    SSID: wlan-sol2
    ...
```

Einen manuellen Verbindungsaufbau können Sie bei nicht abgesicherten WLAN-Netzen mit `iw ... connect` herstellen. Dabei müssen Sie den Namen des Netzwerks (also die SSID) angeben. `iw` kümmert sich nur um die WLAN-Verbindung. Die Ethernet-Konfiguration führen Sie anschließend mit `dhclient` durch (`dhcpcd` unter SUSE).

```
root#  iw dev wlan0 connect hotel-wlan-1
root#  dhclient wlan0
```

`iw disconnect` beendet die Verbindung wieder:

```
root#  iw dev wlan0 disconnect
```

WLAN-Verschlüsselung

WLAN-Verbindung mit WEP

Wenn das Funknetz durch WEP abgesichert ist, können Sie den Schlüssel mit einem zusätzlichen Parameter in der Form *n:xxx* übergeben. Dabei gibt `n` die Schlüsselnummer an (0 bis 3). Der eigentliche Schlüssel wird wahlweise in Form von 5 oder 13 ASCII-Zeichen bzw. durch 10 oder 26 hexadezimale Ziffern angegeben.

```
root#  iw dev wlan0 connect hotel-wlan-1 keys 0:1a790bcc31
root#  dhclient wlan0
```

WLAN-Verbindung mit WPA

Etwas komplizierter ist die Vorgehensweise, wenn WPA oder WPA2 im Spiel sind. In diesem Fall ist für die Initialisierung der Verbindung und für den weiteren Austausch von sich immer wieder ändernden Schlüsseln das Hintergrundprogramm `wpa_supplicant` aus dem gleichnamigen Paket zuständig. Nach dessen Installation richten Sie eine Konfigurationsdatei ein, wobei Sie als Dateiname z. B. `/etc/wpa_supplicant.conf` wählen.

Die Datei kann einige globale Einstellungen enthalten. Anschließend folgen spezifische Parameter für verschiedene WLAN-Netze. Das folgende Beispiel zeigt eine Minimumvariante, die für den Verbindungsaufbau zu einem WLAN-Router oder -Access-Point mit WPA- oder WPA2-Personal-Verschlüsselung ausreicht. Die beiden entscheidenden Parameter sind `ssid` zur Identifizierung des Netzwerks und `psk` mit dem aus Sicherheitsgründen nochmals verschlüsselten Schlüssel. (Es ist auch zulässig, den WPA-Schlüssel in Anführungszeichen als Klartext anzugeben.)

```
# /etc/wpa_supplicant.conf
network={
     ssid="sol"
     psk=00a38f42e6681596e1a5a4c5ede9a15250fb2a01c21028c6d490bb3458b8ea00
}
network={
     ssid="wlan-sol2"
     psk=053633deb59038da9e9168e015fef97d3d54ae3794d4a12d31ee75a830cccec2
}
```

Bei der Verschlüsselung Ihres WPA-Passworts hilft `wpa_passphrase`. Das Ergebnis dieses Kommandos können Sie direkt in `wpa_supplicant.conf` kopieren, wobei Sie die Zeile mit dem Passwort im Klartext tunlichst entfernen.

```
root#  wpa_passphrase sol 'Mein ganz geheimes Passwort!'
network={
        ssid="sol"
        #psk="Mein ganz geheimes Passwort!"
        psk=020d93e2ddb2cdee51e800b977ff7d58fde47d0913cd394f2133648a147f513f
}
```

Jetzt können Sie `wpa_supplicant` starten. Das Kommando läuft, bis Sie es mit Strg+C beenden. Es kümmert sich um die Initialisierung der WLAN-Verbindung und in der Folge um die regelmäßige Erneuerung der Schlüssel für die Verbindung. Mit anderen Worten: Das Programm muss laufen, solange Sie die WLAN-Verbindung nutzen. Arbeiten Sie also in einer anderen Konsole weiter.

Kurz noch einige Anmerkungen zu den Optionen des Kommandos: `-i` gibt die Netzwerkschnittstelle an, `-c` die Konfigurationsdatei, deren Namen Sie frei wählen dürfen. `-D` gibt den oder die von Ihnen eingesetzten WLAN-Treiber an. Versuchen Sie es mit `nl80211,wext`: Damit werden sowohl die alten Linux-WLAN-Treiber als auch

die neuen Implementierungen unterstützt. `man wpa_supplicant` liefert eine Liste aller unterstützten Treiber.

```
root#  wpa_supplicant -iwlan0 -Dnl80211,wext -c /etc/wpa_supplicant.conf
Trying to associate with 00:13:46:b5:25:6e (SSID='sol' freq=0 MHz)
Associated with 00:13:46:b5:25:6e
WPA: Key negotiation completed with 00:13:46:b5:25:6e [PTK=TKIP GTK=TKIP]
CTRL-EVENT-CONNECTED - Connection to 00:13:46:b5:25:6e completed (auth)
  [id=0 id_str=]
...
```

Links

Weitere Tipps zum Umgang mit `wpasupplicant` finden Sie auf den folgenden Seiten:

http://w1.fi/wpa_supplicant
http://wiki.ubuntuusers.de/WLAN/wpa_supplicant

29.4 LAN-Konfigurationsdateien

Dieser Abschnitt stellt die wichtigsten Konfigurationsdateien für die Anbindung des Rechners an ein lokales Netzwerk vor. Leider gibt es nur für einen Teil dieser Dateien Regeln, die für alle wichtigen Distributionen einheitlich sind. Bei den restlichen Dateien beziehen sich die in diesem Abschnitt zusammengestellten Informationen auf Debian, Fedora, openSUSE, RHEL und Ubuntu (Stand: Sommer 2013). In der Regel werden Sie eine direkte Veränderung der Konfigurationsdateien vermeiden und stattdessen die Konfigurationswerkzeuge Ihrer Distribution einsetzen. Die in diesem Abschnitt vorgestellten distributionsspezifischen Konfigurationsdateien sind nur relevant, wenn Sie *nicht* den NetworkManager verwenden!

Für die meisten Beispiele in diesem Abschnitt gilt: Der zu konfigurierende Rechner heißt `uranus`. Er befindet sich in einem lokalen Netzwerk mit der Domain `sol`. Andere Rechner im lokalen Netz heißen `jupiter`, `saturn` etc. Das lokale Netz verwendet 192.168.0.*-Adressen. Der lokale Rechner hat die IP-Adresse 192.168.0.2. Der Gateway-Rechner im lokalen Netz hat die IP-Adresse 192.168.0.1. Auf dem Gateway-Rechner läuft ein eigener Nameserver. Namen und Nummern haben natürlich nur Beispielcharakter.

Basiskonfiguration

/etc/hosts

`/etc/hosts` enthält eine Liste bekannter IP-Adressen und der ihnen zugeordneten Namen. Die Datei muss auf jeden Fall die Daten der Loopback-Schnittstelle enthalten. Die Minimalvariante sieht so aus:

```
# /etc/hosts (Minimalvariante)
127.0.0.1   localhost
```

Bei den meisten Linux-Distributionen ist `localhost` auch für IPv6 definiert. Die folgenden Zeilen zeigen die Defaulteinstellungen unter Fedora und RHEL:

```
# /etc/hosts (Defaultkonfiguration unter Red Hat und Fedora)
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
```

Bei einer statischen Netzwerkkonfiguration, z. B. auf einem Root-Server, kann `hosts` auch einen Eintrag mit der IP-Adresse und dem Hostnamen des Rechners enthalten.

```
# /etc/hosts (Fortsetzung, statische Konfiguration des lokalen Rechners)
...
192.168.0.2  uranus.sol uranus
```

Wenn Sie die anderen Rechner im lokalen Netz namentlich ansprechen möchten und es keinen lokalen Nameserver gibt (siehe das folgende Kapitel), müssen Sie auch deren Namen in `/etc/hosts` angeben. Statt `ping 192.168.0.13` können Sie dann also einfach `ping saturn` ausführen, um die Verbindung zum Rechner `saturn` zu testen.

```
# /etc/hosts (Fortsetzung, statische Konfiguration anderer Rechner)
...
192.168.0.1   mars.sol    mars
192.168.0.2   uranus.sol  uranus
192.168.0.3   saturn.sol  saturn
```

Analoge Einträge sind in den `/etc/hosts`-Dateien aller Rechner im lokalen Netz erforderlich. Je mehr Rechner es im lokalen Netzwerk gibt, desto mühsamer wird die Administration der `/etc/hosts`-Dateien. Aus diesem Grund empfiehlt es sich bei größeren Netzwerken, auf einem Rechner einen Nameserver einzurichten. Der Nameserver weiß, wie alle anderen Rechner im Netzwerk heißen. Die Rechner im lokalen Netz können den Nameserver kontaktieren, um diese Information zu ermitteln. `/etc/hosts` benötigt dann nur die `localhost`-Zeilen.

/etc/host.conf

`/etc/host.conf` gibt an, wie TCP/IP unbekannte IP-Adressen ermitteln soll. Die folgende Beispieldatei bestimmt, dass zuerst die Datei `/etc/hosts` ausgewertet (Schlüsselwort `hosts`) und danach der in `/etc/resolv.conf` angegebene Nameserver befragt werden soll (`bind`). Die zweite Zeile erlaubt, dass einem in `/etc/hosts` angegebenen Hostnamen mehrere IP-Adressen zugeordnet werden dürfen.

Diese Datei liegt bei fast allen Distributionen in der hier angegebenen Form vor und muss nicht verändert werden.

```
# /etc/host.conf
order hosts, bind
multi on
```

/etc/resolv.conf

`/etc/resolv.conf` steuert, wie die IP-Adressen für unbekannte Netzwerknamen (Hostnamen) ermittelt werden. »Unbekannt« bedeutet, dass die Namen nicht in `hosts.conf` definiert sind.

Mit den Schlüsselwörtern `domain` und `search` wird erreicht, dass unvollständige Namen mit dem Domainnamen erweitert werden, also beispielsweise `jupiter` zu `jupiter.sol`. Das erhöht in erster Linie die Bequemlichkeit, weil lokale Hostnamen in verkürzter Form angegeben werden können. Bei `search` dürfen mehrere Domainnamen angegeben werden, bei `domain` aber nur einer. Dafür hat der `domain`-Name Vorrang vor den `search`-Namen, wird also zuerst getestet. Wenn wie hier nur ein einziger Domainname angegeben wird, kann auf die `domain`-Zeile verzichtet werden.

Die wichtigsten Einträge in `/etc/resolv.conf` werden mit dem Schlüsselwort `nameserver` eingeleitet: Damit können bis zu drei IP-Adressen von Nameservern angegeben werden. Diese Server werden immer dann angesprochen, wenn die IP-Adresse eines unbekannten Rechnernamens ermittelt werden soll. Die Angabe eines Nameservers ist unbedingt erforderlich, damit Internetadressen in IP-Adressen aufgelöst werden können. Auf den meisten ADSL-Routern läuft ein lokaler DNS, der wiederum auf den DNS des Providers zurückgreift. In größeren lokalen Netzen gibt es zumeist eigene Nameserver.

```
# /etc/resolv.conf
domain sol               # Hostnamen gelten für .sol
search sol               # Hostnamen gelten für .sol
nameserver 192.92.138.35  # erster DNS
nameserver 195.3.96.67    # zweiter DNS (falls der erste ausfällt)
```

Wenn Sie IPv6 verwenden, müssen Sie auch die Adresse eines IPv6-Nameservers angeben. Falls Ihr Internet-Provider nur IPv4 unterstützt und Sie einen IPv6-Tunnel-Service verwenden, können Sie die Adresse eines öffentlichen IPv6-Nameservers angeben, z. B. den von Google:

```
# /etc/resolv.conf
...
nameserver 2001:4860:4860::8888
```

Bei vielen Distributionen wird `resolv.conf` dynamisch erzeugt:

- Wenn Ihre lokale Netzwerkverbindung (LAN, WLAN) mit DHCP konfiguriert ist, trägt das Script für den Verbindungsaufbau bzw. der NetworkManager die vom DHCP-Server übertragenen Nameserver-Adressen ein.
- Wenn eine Internetverbindung per PPP (ADSL, UMTS, VPN) hergestellt wird, trägt das Script für den Verbindungsaufbau automatisch die `nameserver`-Adressen Ihres Internet-Providers in `/etc/resolv.conv` ein.

- Ubuntu richtet ab Version 12.04 standardmäßig einen lokalen Nameserver ein. Dabei kommt das Programm Dnsmasq zum Einsatz, das Sie im nächsten Kapitel kennenlernen werden. Die Nameserver-Adresse lautet deswegen 127.0.0.1, verweist also auf localhost. Wenn Sie den Nameserver manuell einrichten möchten, müssen Sie dessen Adresse `/etc/network/interfaces` mit dem Schlüsselwort `dns-nameservers` angeben:

  ```
  # Datei /etc/network/interfaces (ab Ubuntu 12.04)
  ...
  auto eth0
    iface eth0 inet static
    ...
    dns-nameservers 10.0.17.1
  ```

  Für die Verwaltung von `/etc/resolv.conf` ist das Paket `resolvconf` zuständig. Eine direkte Veränderung von `/etc/resolv.conf` ist nicht vorgesehen!

resolv.conf vor Änderungen schützen

Die automatische Anpassung von `resolv.conf` ist in den meisten Fällen zweckmäßig. Wenn Sie dies aber nicht wünschen, können Sie die automatische Veränderung in den meisten Fällen verhindern.

Bei Debian und Ubuntu müssen Sie bei PPP-Verbindungen das Schlüsselwort `usepeerdns` aus `/etc/ppp/peers/`*name* entfernen. Bei Netzwerkschnittstellen mit DHCP hängt es davon ab, welcher DHCP-Client installiert ist. Wenn `dhcp3-client` installiert ist, müssen Sie dessen Konfigurationsdatei `dhclient.conf` verändern:

```
# /etc/dhcp/dhclient.conf
...
supersede domain-name "sol";
prepend domain-name-servers 192.168.0.1;
```

Ab Ubuntu 12.04 müssen Sie außerdem das Paket `resolvconf` deinstallieren.

Bei Red Hat bzw. Fedora müssen Sie dabei die `ifcfg-xxx`-Datei für die jeweilige Schnittstelle verändern:

```
# /etc/sysconfig/network-scripts/ifcfg-xxxx (Red Hat, Fedora)
PEERDNS=no
```

Bei SUSE ändern Sie die folgende Konfigurationsdatei:

```
# /etc/sysconfig/network/config (SUSE)
NETCONFIG_DNS_POLICY=""
```

Gateway

Es gibt keinen einheitlichen Standard, wie bzw. in welcher Datei die Gateway-Konfiguration erfolgt. In lokalen Netzen wird die Adresse des Gateways meist per DHCP übermittelt. Bei einer statischen Konfiguration sind je nach Distribution unterschiedliche Dateien verantwortlich.

Bei Debian und Ubuntu beschreibt `/etc/network/interfaces` alle Netzwerkschnittstellen. Bei statisch konfigurierten Schnittstellen wird das Gateway durch das Schlüsselwort `gateway` eingestellt:

```
# in /etc/network/interfaces (Debian, Ubuntu)
...
iface eth0 inet static
  address 192.168.0.2
  netmask 255.255.255.0
  gateway 192.168.0.1
```

Bei Red Hat bzw. Fedora enthält die Konfigurationsdatei für die Netzwerkschnittstelle die Variable `GATEWAY`:

```
# /etc/sysconfig/network-scripts/ifcfg-xxxx (Red Hat, Fedora)
GATEWAY=192.168.0.1
```

Bei SUSE erfolgt die Konfiguration zentral durch die folgende Datei:

```
# in /etc/sysconfig/network/routes (SUSE)
default 192.168.0.1 - -
```

Hostname

Der aktuelle Hostname kann mit dem Kommando `hostname` ermittelt werden. Soweit der Hostname nicht durch DHCP eingestellt wird, erfolgt die Konfiguration durch unterschiedliche Dateien, die in Tabelle 29.3 aufgeführt sind. Denken Sie daran, auch `/etc/hosts` anzupassen, falls diese Datei eine Zeile mit dem Hostnamen des Rechners enthält.

Distribution	Datei
Debian, Ubuntu	`/etc/hostname`
Fedora ab Version 19, Systemd	`/etc/hostname`
ältere Fedora-Versionen, RHEL 6	`/etc/sysconfig/network`
SUSE	`/etc/HOSTNAME`

Tabelle 29.3 Datei zur Einstellung des Hostnamens

Zuordnung zwischen Controllern und Netzwerkschnittstellen

Bei mehreren Netzwerkschnittstellen ist es oft schwierig, die Zuordnung zwischen den `eth`*n*-Devices und der physikalischen Hardware zu ermitteln. Je nach Hardware ist es möglich, die in die Buchse integrierte Leuchtdiode mit `ethtool -p eth0 10` für 10 Sekunden zum Blinken anzuregen. Wenn der Netzwerktreiber diese Operation nicht unterstützt, erhalten Sie die Fehlermeldung *operation not supported*.

Bei vielen Linux-Distributionen kümmert sich das udev-System um die Zuordnung zwischen Netzwerk-Controllern und Schnittstellennamen. Im Detail steuert die Datei net_persistent_names.rules die Benennung der Netzwerkschnittstellen. In diese Datei wird jeder neu entdeckte Netzwerk-Adapter mit seiner MAC-Adresse eingetragen. Diese Datei kann beispielsweise so aussehen:

```
# Datei /etc/udev/rules.d/70-persistent-net.rules
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}==
  "00:16:17:cd:c3:81", ATTR{type}=="1", KERNEL=="eth*", NAME="eth0"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}==
  "00:14:6c:8e:d9:71", ATTR{type}=="1", KERNEL=="eth*", NAME="eth1"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}==
  "00:4f:4e:0f:8e:a0", ATTR{type}=="1", KERNEL=="eth*", NAME="eth2"
```

Fedora hat schon in Version 15 einen neuen Weg gesucht, um Netzwerkschnittstellen so zu benennen, dass sich die Device-Namen vorhandener Schnittstellen auch beim Hinzufügen weiterer Netzwerk-Hardware nicht ändern. Aktuelle Ubuntu-Server-Versionen haben diese Idee ebenfalls aufgegriffen.

Mit Fedora 19 wurde das Verfahren nochmals adaptiert. Für die Benennung der Devices ist jetzt Systemd in Kombination mit neuen udev-Regeln verantwortlich. On-Board-Devices erhalten den Namen eno*n*, PCI-Express-Adapter den Namen ens*n*, externe Geräte den Namen enp*n*s*m* und WLAN-Adapter den Namen wlp*n*s*m*. Dabei beziehen sich *n* und *m* jeweils auf Hardware-Eigenschaften, z. B. auf den PCI-Slot. Weitere Hintergrundinformationen finden Sie hier:

http://www.freedesktop.org/wiki/Software/systemd/PredictableNetworkInterfaceNames

29.5 Distributionsspezifische Konfigurationsdateien

In diesem Abschnitt geht es darum, eine bleibende Netzwerkkonfiguration durchzuführen, ohne Konfigurationswerkzeuge zu Hilfe zu nehmen. Die hier beschriebenen Vorgehensweisen sind insbesondere dann zweckmäßig, wenn Sie einen Server einrichten oder eine virtuelle Maschine konfigurieren. In beiden Fällen stehen häufig weder eine grafische Benutzeroberfläche noch die dazugehörenden Administrationswerkzeuge zur Verfügung. Sie müssen deswegen die distributionsspezifischen Dateien zur Netzwerkkonfiguration selbst editieren.

NetworkManager deaktivieren

Die folgenden Anleitungen gelten natürlich auch für Desktop-Systeme. Dort müssen Sie aber unbedingt vorher den NetworkManager deinstallieren! Dazu führen Sie je nach Distribution eines der folgenden Kommandos aus:

```
root#  yum remove NetworkManager
root#  apt-get remove network-manager
```

Bei manchen Distributionen, z. B. Fedora, müssen Sie außerdem explizit das Init-Script für die traditionelle Netzwerkkonfiguration ausführen und aktivieren:

```
root#  systemctl start network.service
root#  systemctl enable network.service
```

Bei SUSE stellen Sie im YaST-Modul NETZWERKGERÄTE • NETZWERKEINSTELLUNGEN ein, ob die Netzwerkkonfiguration traditionell oder durch den NetworkManager erfolgen soll.

Fedora und Red Hat

Unter Fedora und Red Hat erfolgt die Konfiguration jeder Netzwerkschnittstelle durch die Datei `/etc/sysconfig/network-scripts/icfg-xxx`, wobei `xxx` der Name der Netzwerkschnittstelle ist. Ich verwende in den folgenden Beispielen `eth0`, aber Sie müssen den Schnittstellennamen natürlich an Ihre Gegebenheiten anpassen! Im Regelfall existiert die Konfigurationsdatei bereits, und Sie müssen lediglich einige Einstellungen verändern. Die MAC-Adresse des Netzwerkadapters ermitteln Sie bei Bedarf mit `ip addr`.

DHCP-Konfiguration

Wenn der Rechner die Netzwerkparameter via DHCP bezieht, richten Sie einfach die Datei `ifcfg-eth0` wie folgt ein:

```
# Datei /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=xx:xx:xx:xx:xx:xx
NM_CONTROLLED=no
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
```

Statische Konfiguration

Bei einer statischen Konfiguration muss die Datei dem folgenden Muster entsprechen, wobei Sie die IP-Adressen und -Masken durch eigene Werte ersetzen müssen:

```
# Datei /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=xx:xx:xx:xx:xx:xx
NM_CONTROLLED=no
ONBOOT=yes
BOOTPROTO=none
TYPE=Ethernet
IPADDR=10.0.17.33
NETMASK=255.255.255.0
```

```
NETWORK=10.0.17.0
BROADCAST=10.0.17.255
GATEWAY=10.0.17.1
```

Die Gateway-Adresse können Sie statt in `ifcfg-xxx` auch in `/etc/sysconfig/network` einstellen. Das ist dann zweckmäßig, wenn es ein zentrales Gateway für alle Netzwerkschnittstellen gibt.

IPv6-Konfiguration

Wenn Sie IPv6 nutzen möchten, muss die Datei `/etc/sysconfig/network` unter RHEL 6 die Zeile `NETWORKING_IPV6=yes` enthalten. Unter Fedora ist dieser Eintrag nicht mehr erforderlich.

Außerdem müssen Sie in `ifcfg-xxx` auch IPv6-Variablen initialisieren. Das folgende Listing zeigt die Einstellungen für eine automatische Konfiguration, bei der die Schnittstelle das *Router Advertisement* des IPv6-Routers auswertet:

```
# Datei /etc/sysconfig/network-scripts/ifcfg-eth0 (automatische Konfiguration)
...
IPV6INIT=yes
IPV6_AUTOCONF=yes
```

Wenn auf dem IPv6-Router ein DHCP-Server läuft, sieht die Konfiguration so aus:

```
# Datei /etc/sysconfig/network-scripts/ifcfg-eth0 (DHCPv6-Konfiguration)
...
IPV6INIT=yes
DHCPV6C=yes
```

Zu guter Letzt folgt hier noch die Variante für eine statische Konfiguration:

```
# Datei /etc/sysconfig/network-scripts/ifcfg-eth0
...
IPV6INIT=yes
IPV6ADDR=2a01:4f8:161:107::2/64
IPV6_DEFAULTGW=fe80::1
```

Firewall-Zonen

In aktuellen Fedora-Versionen können Sie in `ifcfg-xxx` auch die gewünschte Firewall-Zone für die Schnittstelle angeben:

```
# Datei /etc/sysconfig/network-scripts/ifcfg-eth0
...
ZONE="trusted"
```

Ohne diese Angabe verwendet das Firewall-System von Fedora automatisch die Defaultzone `public`. Hintergründe zur Firewall-Konfiguration von Fedora folgen in Kapitel 40.

Hostname

Falls Sie den Hostnamen verändern möchten, finden Sie den entsprechenden Parameter bei vielen Red-Hat- und Fedora-Versionen in der Datei `/etc/sysconfig/network`:

```
# Datei /etc/sysconfig/network (RHEL 6, Fedora bis Version 18)
HOSTNAME=uranus.sol
```

Ab Fedora 19 wird der Hostname hingegen durch die Datei `/etc/hostname` eingestellt!

```
# Datei /etc/hostname (Fedora ab Version 19)
uranus.sol
```

Im Regelfall ist es zweckmäßig, die Zuordnung der IP-Adresse des Rechners zu seinem Hostnamen darüber hinaus auch in `/etc/hosts` einzutragen.

Probleme bei der manuellen Netzwerkkonfiguration unter Fedora 19

In Fedora 19 wurde die Datei `/etc/sysconfig/network` entfernt, da der Hostname jetzt in `/etc/hostname` eingestellt wird und die anderen Einstellungen dieser Datei nicht mehr benötigt werden. Die Scripts für die manuelle Netzwerkkonfiguration führen aber zu Fehlermeldungen, wenn die Datei fehlt. Wenn Sie eine Netzwerkkonfiguration ohne NetworkManager durchführen wollen, müssen Sie die Datei unbedingt erzeugen!

```
root# touch /etc/sysconfig/network
```

Nameserver

Sofern nicht ein DHCP-Server die Adresse des IPv6-Nameservers übermittelt, müssen Sie diese selbst in `/etc/resolv.conf` eintragen.

```
# /etc/resolv.conf
nameserver 10.0.17.1              # erster DNS
nameserver 10.0.17.2              # zweiter DNS
nameserver 2001:4860:4860::8888   # öffentlicher IPv6-Nameserver von Google
```

Konfiguration aktivieren

Zuletzt starten Sie das Init-Script, das für die manuelle Netzwerkkonfiguration verantwortlich ist:

```
root#  service network start        (gilt sofort)
root#  chkconfig network on         (gilt ab dem nächsten Neustart)
```

Wenn Sie nur eine einzelne Schnittstelle aktivieren bzw. wieder deaktivieren möchten, verwenden Sie die `ifup`- und `ifdown`-Scripts:

```
root#  ifup eth0
root#  ifdown eth0
```

Debian und Ubuntu

/etc/network/interfaces

Für die Konfiguration aller Schnittstellen ist die Datei `/etc/network/interfaces` zuständig. Die Syntax ist ausgesprochen einfach: Jede Schnittstelle, die beim Rechnerstart aktiviert werden soll, muss durch `auto` *name* genannt werden. `iface` *name*

optionen beschreibt die Basiskonfiguration der Schnittstelle. Bei einer statischen Konfiguration folgen in den weiteren Zeilen die Parameter `address`, `netmask` und `gateway`.

DHCP-Konfiguration

Wenn der Rechner die Netzwerkparameter via DHCP beziehen soll, umfasst die gesamte Konfiguration nur vier Zeilen! Die ersten beiden Zeilen aktivieren die Loopback-Schnittstelle, die immer erforderlich ist. Sie dient zur rechnerinternen Netzwerkkommunikation. Die zwei weiteren Zeilen aktivieren die Schnittstelle `eth0`.

```
# /etc/network/interfaces
auto lo
iface lo inet loopback

# dynamische Verbindung zu einem DHCP-Server,
# der die Eckdaten des Internetzugangs vermittelt
auto eth0
iface eth0 inet dhcp
```

Statische Konfiguration

Wenn die Verbindung in das Internet statisch konfiguriert wird, enthält die `iface`-Zeile das Schlüsselwort `static`. Die Netzwerkparameter werden in der Folge durch mehrere Schlüsselwörter angegeben, deren Bedeutung selbsterklärend ist.

```
# /etc/network/interfaces
auto lo
iface lo inet loopback

# statische Netzwerkkonfiguration
auto eth0
iface eth0 inet static
  address         211.212.213.37
  netmask         255.255.255.224
  gateway         211.212.213.1
```

Nameserver

Bei aktuellen Ubuntu-Versionen (ab 12.04) können Sie in `interfaces` auch die Adressen von einem oder mehreren DNS-Servern angeben. Für die Auswertung des Schlüsselworts `dns-nameservers` ist das Paket `resolvconf` verantwortlich.

```
# /etc/network/interfaces (Ubuntu ab Version 12.04)
...
auto eth0
iface eth0 inet static
  ...
  dns-nameservers 211.222.233.244 212.223.234.245
```

Bei älteren Ubuntu-Versionen sowie unter Debian müssen Sie die Nameserver-Adressen hingegen direkt in `/etc/resolv.conf` angeben:

```
# /etc/resolv.conf (Debian, Ubuntu bis Version 11.10)
nameserver 211.222.233.244    # erster DNS
nameserver 212.223.234.245    # zweiter DNS
```

IPv6-Konfiguration

Wenn Sie auch IPv6 nutzen möchten, definieren Sie die betreffende Schnittstelle in `/etc/network/interfaces` einfach ein zweites Mal mit dem Schlüsselwort `inet6`. Das Schlüsselwort `auto` gibt an, dass die IPv6-Konfiguration das sogenannte *Router Advertisement* des Gateways bzw. IPv6-Routers berücksichtigt (siehe auch Abschnitt 30.6).

```
# /etc/network/interfaces (automatische IPv6-Konfiguration)
...
auto eth0
iface eth0 inet dhcp
iface eth0 inet6 auto
```

Wenn das IPv6-Gateway einen DHCPv6-Server verwendet, lautet die korrekte Methode `dhcp`. Wenn außerdem die Router-Adresse per *Router Advertisement* konfiguriert werden soll, ist die Zusatzoption `accept_ra 1` erforderlich. Das ist beispielsweise der Fall, wenn Sie als DHCP-Server `dnsmasq` mit der Option `enable-ra` einsetzen, wie dies im nächsten Kapitel beschrieben ist.

```
# /etc/network/interfaces (DHCPv6-Konfiguration)
...
auto eth0
iface eth0 inet dhcp
iface eth0 inet6 dhcp
  accept_ra 1
```

Bei einer statischen Konfiguration muss `interfaces` so aussehen:

```
# /etc/network/interfaces (statische IPv6-Konfiguration)
...
auto eth0
iface eth0 inet static
  ... (IPv4-Konfiguration wie bisher)
iface eth0 inet6 static
  address 2a01:4f8:161:107::2
  netmask 64
  gateway fe80::1
```

Hostname

Falls Sie den Hostnamen neu einstellen möchten, führen Sie die Änderungen in `/etc/hostname` und eventuell auch in `/etc/hosts` durch.

Änderungen aktivieren

Damit Änderungen an der Konfiguration wirksam werden, führen Sie das folgende Kommando aus:

```
root#  /etc/init.d/networking restart
```

Bei aktuellen Debian-Versionen liefert das obige Kommando die Warnung */etc/init.d/networking restart is deprecated*. Das Kommando funktioniert in der Regel dennoch, und es gibt keine vernünftige Alternative dazu. Wenn Sie nur eine einzelne

Schnittstelle neu starten möchten, können Sie auf die im Folgenden beschriebenen Kommandos `ifdown` und `ifup` ausweichen:

```
root#  ifdown eth0
root#  ifup eth0
```

ifup, ifdown

Die eigentlichen Konfigurationsarbeiten übernehmen die Debian/Ubuntu-spezifischen Kommandos `ifup` und `ifdown` aus dem Paket `ifupdown`. `ifup -a` wertet `/etc/network/interfaces` aus und aktiviert alle `auto`-Schnittstellen. Soweit Schnittstellen via DHCP konfiguriert werden, greift `ifup` auf das Kommando `dhclient` zur Übertragung und Auswertung der DHCP-Daten zurück. Für die Konfiguration ist `/etc/dhcp3/dhclient.conf` zuständig.

SUSE

Bei SUSE-Distributionen empfiehlt es sich, die Konfiguration mit YaST durchzuführen. YaST steht bei Minimalinstallationen auch im Textmodus zur Verfügung. Im Modul Netzwerkgeräte • Netzwerkeinstellungen aktivieren Sie die globale Option Traditionelle Methode mit ifup und deaktivieren so den NetworkManager. Anschließend wechseln Sie in das Dialogblatt Übersicht und bearbeiten dort die Einstellungen der Netzwerkadapter.

29.6 Zeroconf und Avahi

Ich gehe in diesem Buch in der Regel davon aus, dass Sie die Rechner in Ihrem Netzwerk entweder selbst konfigurieren oder die IP-Konfiguration von einem zentralen Router oder DHCP-Server beziehen. Daneben gibt es aber noch einen dritten Weg: die automatische Konfiguration durch Zeroconf.

Bei diesem Verfahren tauschen alle im Netzwerk verbundenen Rechner ihre Konfigurationsdaten aus. Neu an das Netzwerk angeschlossene Rechner bzw. Geräte konfigurieren sich anhand dieser Informationen selbst so, dass sie ohne Konflikte mit den anderen Geräten kommunizieren können. Die automatisch konfigurierten Rechner verwenden Adressen aus dem IP-Bereich 169.254.*.* sowie Hostnamen, die auf `.local` enden. Die Zeroconf-Kommunikation erfolgt über den UDP-Port 5454. Damit Zeroconf funktioniert, darf dieser Port innerhalb des LANs nicht durch eine Firewall blockiert werden!

Zeroconf wurde zuerst von Apple unter dem Namen *Rendezvous* implementiert. Dieses Projekt wurde später in *Bonjour* umgetauft und steht auch für Windows zur Verfügung. Diese Implementierung liegt zwar als Open-Source-Code vor, die Lizenz ist aber nicht GPL-kompatibel. Aus diesem Grund entstand für Linux ein

eigenes Zeroconf-Projekt unter dem Namen Avahi, dessen Code unabhängig von Bonjour ist. Als Lizenz kommt die LGPL zum Einsatz. (Die Entstehungsgeschichte des merkwürdigen Namens Avahi ist mir nicht bekannt.)

Zeroconf-kompatible Programme können nun alle anderen im Netzwerk sichtbaren Zeroconf-Rechner und deren Ressourcen anzeigen, z. B. Netzwerkverzeichnisse, SSH-, HTTP- und FTP-Server. Damit ist es ohne explizite Konfiguration möglich, zwei oder mehr Rechner in ein Netzwerk zu integrieren und Daten auszutauschen.

Die zunehmende Verbreitung von ADSL- und WLAN-Routern macht Zeroconf eigentlich überflüssig. Dass Avahi-Pakete dennoch standardmäßig von vielen Linux-Distributionen installiert werden, liegt eher an den Browsing-Funktionen: Dass sich die Rechner gegenseitig sehen und namentlich kennen, ist ganz losgelöst von der Art der Netzwerkkonfiguration ein großer Vorteil. Außerdem nutzt Apple in all seinen Geräten Bonjour. Wenn Sie möchten, dass Ihr Linux-Rechner für Apple-Geräte sichtbar ist (z. B. für die AirPrint-Funktion), muss auf dem Rechner der Avahi-Dämon laufen. Weitere Informationen und Tipps finden Sie auf den folgenden Websites:

http://avahi.org
http://wiki.ubuntuusers.de/Avahi

Zeroconf ist nur für IPv4 erforderlich

Zeroconf ist ein IPv4-spezifisches Verfahren. In IPv6 besteht keine Notwendigkeit für Zeroconf, weil jeder Netzwerkschnittstelle automatisch eine Link-Local-IPv6-Adresse zugewiesen wird. Diese Adresse wird für IPv6-interne Konfigurationsaufgaben benötigt, kann aber auch für Anwendungen in der Art von Zeroconf verwendet werden.

avahi-daemon

Für die Kommunikation zwischen den Avahi-Rechnern ist der Dienst `avahi-daemon` zuständig. Die Konfiguration erfolgt durch `/etc/avahi/avahi-daemon.conf`, wobei Sie die Grundeinstellungen zumeist beibehalten können. Die einzige Ausnahme ist oft die Variable `enable-dbus`: Sie steuert, ob Avahi den Kommunikationsmechanismus zulässt. Einige Avahi-kompatible Programme setzen DBUS voraus. Um DBUS zu aktivieren, ändern Sie `avahi-daemon.conf` wie folgt:

```
# /etc/avahi/avahi-daemon.conf
[server]
...
enable-dbus=yes
```

Anschließend starten Sie den Dienst neu:

```
root#  service avahi-daemon restart
```

Namens-auflösung

Wenn Sie externe Rechner mit gewöhnlichen, nicht Avahi-kompatiblen Netzwerkprogrammen über deren `.local`-Namen ansprechen möchten (z. B. mit `ping merkur.local`), müssen Sie mit `avahi-dnsconfd` einen weiteren Netzwerk-Dämon installieren und starten. Dabei handelt es sich um eine Art Nameserver für Avahi-Hostnamen. Sie brauchen diesen Dämon nicht, wenn in Ihrem Netzwerk ohnedies ein Nameserver läuft.

Damit alle Programme bei der Namensauflösung auf `avahi-dnsconfd` zurückgreifen, müssen Sie dafür sorgen, dass die Bibliothek `libnss-mdns` installiert ist und dass die `hosts:`-Zeile in `/etc/nsswitch.conf` das Schlüsselwort `mdns4` enthält. Bei einigen Distributionen ist dies standardmäßig der Fall.

```
# in /etc/nsswitch.conf
...
hosts: files dns  mdns4
...
```

Browsing

Nach diesen Vorbereitungsarbeiten können Sie ausprobieren, welche Rechner bzw. Dienste Avahi in Ihrem Netz kennt. Dabei helfen das Konsolenkommando `avahi-browse -a -t` bzw. dessen grafische Entsprechung `avahi-discovery` (siehe Abbildung 29.4). Die Kommandos müssen bei vielen Distributionen extra installiert werden und befinden sich unter Fedora beispielsweise in den Paketen `avahi-tools` und `avahi-ui-tools`.

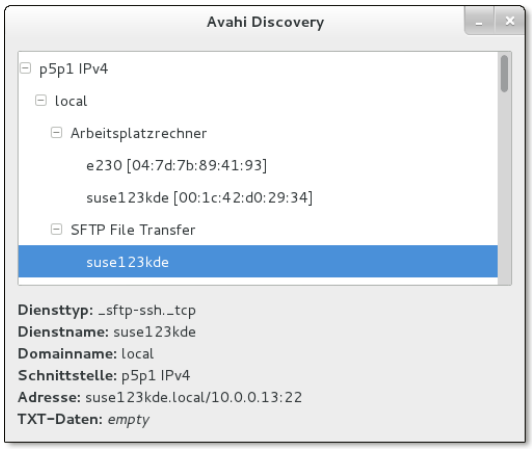


Abbildung 29.4 Avahi-Browser

Der Gnome-Dateimanager zeigt in der Netzwerkansicht standardmäßig alle Avahi-Rechner an. Der KDE-Dateimanager bietet unter der Adresse `zeroconf:/` eine ähnliche Funktion, sofern die entsprechende Erweiterung installiert ist (je nach Distribution z. B. aus dem Paket `kde-zeroconf`). Auch diverse Messaging- und Multimedia-Anwendungen unterstützen Zeroconf.

29.7 PPP-Grundlagen

Das *Point-to-Point Protocol* (PPP) ermöglicht eine TCP/IP-Verbindung zwischen zwei Rechnern über eine serielle Verbindung. PPP kam in der Vergangenheit bei der Verwendung von Analog- und ISDN-Modems zum Einsatz. Für ADSL- und UMTS-Modems sowie für VPNs mit PPTP spielt es bis heute eine wichtige Rolle. Unter Linux ist der PPP-Dämon `pppd` für die PPP-Verbindung verantwortlich. Dieses Programm kann grundsätzlich sowohl als Client als auch als Server eingesetzt werden – hier geht es aber ausschließlich um die Client-Variante.

PPP-Varianten

Bei ADSL-Verbindungen kommt zumeist eine der drei folgenden `pppd`-Erweiterungen zum Einsatz:

- **PPPoE:** *Point-to-Point Protocol over Ethernet* ist ein öffentlich dokumentiertes Protokoll, das im RFC 2516 beschrieben ist. Sein Hauptnachteil besteht darin, dass es die maximale Länge von IP-Paketen einschränkt (MTU-Problem, siehe Abschnitt 29.9).
- **PPPoA:** *Point-to-Point Protocol over ATM* ist eine Alternative zu PPPoE. ATM steht dabei für *Asynchronous Transfer Mode*.
- **PPTP:** Das *Point-to-Point Tunneling Protocol* ist ein von Microsoft definiertes bzw. aus anderen Standards weiterentwickeltes Protokoll, das ebenfalls öffentlich dokumentiert ist (RFC 2637). Seine ursprüngliche Aufgabe bestand darin, Virtual Private Networks zu ermöglichen. Aufgrund bekannter Sicherheitsprobleme sollte der Einsatz von PPTP aber vermieden werden.

Authentifizierung

Am Beginn des PPP-Verbindungsaufbaus steht immer die Authentifizierung: Ihr Rechner muss sich also beim Internet-Provider mit einem Login-Namen und einem dazugehörenden Passwort anmelden. Hierfür gibt es zwei Verfahren: PAP und CHAP. CHAP unterstützt wiederum zahllose Varianten (z. B. MS-CHAPv2), die das Verfahren sicherer machen.

- **PAP:** Beim *Password Authentication Protocol* überträgt der Client den Login-Namen und das Passwort zumeist unverschlüsselt.
- **CHAP:** Beim sichereren *Challenge Handshake Authentication Protocol* initiiert der Server die Authentifizierung und sendet ein sogenanntes *Challenge*-Paket an den Client. `pppd` verwendet diese Daten, um aus seinem Passwort einen Hash-Wert zu berechnen. `pppd` sendet dann den Login-Namen und den Hash-Wert zurück an den Provider. Auf diese Weise wird vermieden, dass das Passwort selbst übertragen wird!

pppd-Konfigurationsdateien und -Scripts

/etc/ppp/options

`/etc/ppp/options` enthält globale `pppd`-Optionen. Diese Optionen gelten als Defaulteinstellung für alle Verbindungen, die mit `pppd` hergestellt werden. Um Konflikte zwischen verschiedenen PPP-Einsatzformen zu vermeiden, sollte `options` möglichst wenig Einstellungen enthalten. Verwenden Sie zur Optionseinstellung stattdessen die verbindungsspezifischen Dateien in `/etc/ppp/peers/`! Sie vermeiden damit, dass eine Option, die für die Verbindungsvariante A zutrifft, eventuell einen Verbindungsaufbau bei Variante B blockiert.

/etc/ppp/peers/name

`/etc/ppp/peers/`*name* enthält verbindungsspezifische Optionen. Um `pppd` unter Anwendung dieser Optionen zu starten, führen Sie das folgende Kommando aus:

```
root#  pppd call  name
```

Einstellungen in `/etc/ppp/peers/`*name* haben Vorrang gegenüber `/etc/ppp/options`.

/etc/ppp/pap-secrets und chap-secrets

`/etc/ppp/pap-secrets` und `chap-secrets` enthalten eine Liste aller Login-Namen und Passwörter für die PAP- bzw. CHAP-Authentifizierung. Wenn Sie nicht sicher sind, ob die Authentifizierung per PAP oder CHAP erfolgt, fügen Sie denselben Eintrag einfach sowohl in `pap-secrets` als auch in `chap-secrets` ein. Sicherer und weiter verbreitet sind CHAP-Varianten (CHAP, MS-CHAP oder MS-CHAPv2). Die Einträge für Client-Verbindungen sehen so aus:

```
#/etc/ppp/pap-secrets und /etc/ppp/chap-secrets
#login name     server IP address   password        client IP adress
"hofer"         *                   "qwe44trE"      *
```

Statt des * zwischen dem Login-Namen und dem Passwort kann die IP-Adresse des PPP-Servers angegeben werden, zu dem die Verbindung hergestellt werden soll. In diesem Fall gilt die Passwortinformation nur für diese IP-Adresse. Das ist ein zusätzlicher Schutzmechanismus gegen missbräuchliche Verwendung, der aber nur möglich ist, wenn die IP-Adresse bekannt und unveränderlich ist.

Statt des zweiten Sterns können Sie angeben, für welche Client-IP-Adresse die Kombination aus Login-Name und Passwort gelten soll. Diese Adresse ist in der Regel unbekannt, weil der PPP-Server dem Client bei jedem Verbindungsaufbau eine andere, gerade freie Adresse zuweist. Der zweite Stern erlaubt daher beliebige Client-IP-Adressen.

/etc/ppp/ip-up und ip-down

Die beiden Script-Dateien `/etc/ppp/ip-up` und `/etc/ppp/ip-down` werden unmittelbar nach Herstellung der Verbindung bzw. nach deren Beendigung ausgeführt. Mögliche Anwendungen sind die Einstellung von `/etc/resolv.conf` sowie das Einrichten oder Verändern von Routing-, Masquerading- und Firewall-Funktionen.

An die beiden Scripts werden sechs Parameter übergeben. Der erste Parameter enthält den Schnittstellennamen (z. B. `ppp0`), der vierte die lokale IP-Adresse, der fünfte die IP-Adresse des PPP-Partners und der sechste die Identifikationszeichenkette der PPP-Verbindung (Option `ipparam`). Die Parameter zwei und drei sind ungenutzt. Wenn beim Verbindungsaufbau DNS-Adressen übertragen werden (Option `usepeerdns`), stehen außerdem in den Variablen `DNS1` und `DNS2` die beiden Adressen zur Verfügung.

29.8 UMTS-Interna

Die meisten aktuellen Modems sehen wie ein USB-Stick aus. Obwohl sich die Bezeichnung »UMTS-Modem« eingebürgert hat, sind die meisten Modems zu älteren Standards kompatibel (GSM, GPRS, EDGE etc.). Das Modem verwendet je nach Empfang automatisch das schnellste verfügbare Netz. Das gilt natürlich auch für LTE-Modems, die zum neuesten Mobilfunkstandard kompatibel sind und nach und nach UMTS-Modems ablösen.

Treiber

Die Unterstützung für UMTS-Modems unter Linux ist erfreulich gut. Sofern Sie eine aktuelle Distribution verwenden, werden die meisten UMTS-Modems sofort beim Anstecken als solche erkannt. Sie können sich davon mit `dmesg` überzeugen:

```
root#  dmesg
...
usb 1-4: new high speed USB device using ehci_hcd and address 3
...
USB Serial support registered for GSM modem (1-port)
option 1-4:1.0: GSM modem (1-port) converter detected
usb 1-4: GSM modem (1-port) converter now attached to ttyUSB0
option 1-4:1.1: GSM modem (1-port) converter detected
usb 1-4: GSM modem (1-port) converter now attached to ttyUSB1
usbcore: registered new interface driver option
option: v0.7.2:USB Driver for GSM modems
```

Hat die Hardware-Erkennung einmal funktioniert, ist es zumeist kein Problem, mit dem NetworkManager eine Internetverbindung herzustellen.

Linux-intern werden die meisten Modems als serielle Geräte behandelt. Bei einigen Geräten ist dazu der Nozomi-Treiber aus dem gleichnamigen Kernelmodul erforderlich; andere Geräte werden direkt als serielle USB-Geräte erkannt. Anschließend kann das Modem über eine Device-Datei gesteuert werden, beispielsweise `/dev/ttyUSB`*n*, `/dev/ttyACM`*n* oder `/dev/nozomi`*n*. Aus Sicht von Linux verhält sich ein modernes UMTS-Modem damit ganz ähnlich wie ein 20 Jahre altes Analogmodem! Selbst die AT-Kommandos sind weiterhin erforderlich. Zur Steuerung einiger mobil-

funkspezifischer Funktionen wurden einfach neue AT-Kommandos definiert, z. B. `AT+CPIN=nnnn` zur Übermittlung des PIN-Codes.

Aus diesem Grund ist es prinzipiell möglich, UMTS-Modems mit den eigentlich für Analogmodems konzipierten Programmen `gnome-ppp` oder KPPP zu steuern. Das funktioniert allerdings nur, wenn Sie vorher die PIN-Abfrage deaktivieren, und ist insofern nur eine Notlösung.

Doppelfunktion als Speichermedium

Die meisten gängigen UMTS-Modems haben eine Doppelfunktion: Sie erscheinen dem Computer anfänglich als USB-Datenträger und ermöglichen so die komfortable Installation der auf dem Modem gleich mitgelieferten Windows- bzw. OS-X-Treiber. Erst durch einen speziellen Code wird die eigentliche Modemfunktion aktiviert.

Unter Linux kann diese Doppelgleisigkeit zu Problemen führen. Bei bekannten Modellen sendet der Linux-Kernel derartigen Modems eine spezielle Bytesequenz, um die Modemfunktion zu aktivieren. Verantwortlich für diesen Automatismus ist das Kommando `usb_modeswitch` aus dem gleichnamigen Paket. Das Kommando wird mit der richtigen Bytesequenz ausgeführt, sobald das udev-System ein UMTS-Modem erkennt. Die entsprechende udev-Regel befindet sich unter Ubuntu in der Datei `/lib/udev/usb_modeswitch`. Eine komprimierte Datenbank aller bekannten Modems und der dazugehörigen Umschaltsequenzen enthält `/usr/share/usb_modeswitch/configPack.tar.gz`. Weitere Details zu diesem Mechanismus können Sie hier nachlesen:

http://wiki.ubuntuusers.de/USB_ModeSwitch

Sollte der Automatismus bei Ihrem ganz neuen Modem nicht funktionieren, führen Sie nach dem Anstecken manuell `eject /dev/xxx` aus, wobei Sie den Device-Namen des zuletzt eingebundenen USB-Datenträgers angeben. `df` ermittelt eine Liste aller Datenträger, aus der Sie den richtigen auswählen müssen.

Alternativ können Sie versuchen, eine eigene `usb_modeswitch`-Regel einzurichten. Im Regelfall ist die Umschaltsequenz von verschiedenen Modems eines Herstellers identisch. Deswegen reicht es zumeist aus, mit `lsusb` die USB-ID des Modems zu ermitteln und in eine einfache udev-Regeldatei einzutragen:

```
root#  lsusb
...
ID 1234:5678 <hersteller abc> HSDPA/HSUPA Modem
```

Nun erzeugen Sie die Datei `/lib/udev/rules.d/61-my-usb-modeswitch.conf` nach dem folgenden Muster. Die gesamte Anweisung muss in einer einzigen Zeile angegeben werden. Außerdem müssen Sie die Codes 1234 und 5678 durch die USB-ID Ihres Modems ersetzen.

```
ATTRS{idVendor}=="1234", ATTRS{idProduct}=="5678",
  RUN+="modem-modeswitch -v 0x%s{idVendor} -p 0x%s{idProduct} -t option-zerocd"
```

Verbindungsparameter

UMTS-Konfigurationsprogramme sehen üblicherweise Eingabefelder für die Telefonnummer, eine APN-Zeichenkette, den Login-Namen, das Passwort und den PIN-Code vor. Als Telefonnummer ist bei allen Providern die Zeichenkette *99# üblich. Die APN-Zeichenkette (*Access Point Name*) hängt vom Provider ab und bezeichnet den Namen des Anschlusspunkts im Mobilfunknetz. Der Login-Name und das Passwort können bei vielen Providern leer bleiben bzw. werden nicht ausgewertet.

PIN/PUK-Probleme

Wenn der NetworkManager oder andere Programme immer wieder zur Eingabe von PIN- und PUK-Codes auffordern, liegt ein Problem vor. Vermeiden Sie allzu viele Experimente! Es besteht die Gefahr, dass die SIM-Karte nach zu vielen vermeintlich falschen PIN-Eingaben gesperrt wird.

Sicherer ist es, den PIN-Code der SIM-Karte zu deaktivieren: Dazu entfernen Sie die SIM-Karte aus dem USB-Modemstecker, legen sie in ein entsperrtes Handy ein und deaktivieren dort den PIN. Anschließend bauen Sie die SIM-Karte wieder in den USB-Stecker ein. Die Internetverbindung kann jetzt ohne PIN-Code hergestellt werden. Verlieren Sie Ihren Modemstecker aber nicht! Jeder kann Ihr Modem nun ohne PIN-Code nutzen!

29.9 ADSL-Interna

Modem versus Router

Bei einem ADSL-Zugang gibt es zwei prinzipielle Varianten, wie Ihr Rechner mit dem Internet verbunden wird: Heute sind zum Glück ADSL-Router üblich; in der Vergangenheit mussten Sie sich hingegen oft mit der Konfiguration eines ADSL-Modems plagen.

- **ADSL-Router:** Ein ADSL-Router verbindet die Funktionen eines ADSL-Modems mit denen eines Routers bzw. Gateways. An den Router können Sie über Netzwerkkabel oder via WLAN mehrere Computer anschließen. Die Computer beziehen alle Konfigurationsdaten via DHCP vom ADSL-Router, sodass keine Client-Konfiguration erforderlich ist.
- **ADSL-Modem:** Bei einem ADSL-Modem handelt es sich genau genommen um ein *ADSL-Network-Termination*-Gerät, kurz ANT. An ein ADSL-Modem kann nur *ein* Rechner angeschlossen werden. Die Kommunikation zwischen Ihrem Computer und dem Modem erfolgt über ein Ethernet- oder USB-Kabel.

  Je nach Modem und Provider kommen die Protokolle PPPoE, PPPoA oder PPTP zum Einsatz. Die vielen Varianten können die Konfiguration schwierig machen. Mit etwas Glück gelingt die Konfiguration mit dem NetworkManager oder mit

distributionsspezifischen Werkzeugen, also mit `pppoeconfig` bei Debian und SUSE, mit `system-config-network` bei Fedora und Red Hat oder mit YaST bei SUSE. Sollte das nicht der Fall sein, finden Sie auf den folgenden Seiten eine Anleitung zur manuellen Konfiguration.

ADSL-Router-Konfiguration

Viele Provider liefern einen Router gleich mit. Wenn nicht, lege ich Ihnen den Kauf eines ADSL-Routers ans Herz. Dabei müssen Sie auf drei Dinge achten: Der Router muss das von Ihrem Provider eingesetzte Protokoll unterstützen (z. B. PPPoE), er muss mit der eingesetzten ADSL-Technologie kompatibel sein (z. B. ADSL2+), und er muss den richtigen Telefonanschluss haben (Annex A oder Annex B).

Bei Annex A bzw. B handelt es sich um Anhänge zur Richtlinie G.992.1, die die parallele Nutzung der Übertragungskanäle für herkömmliche Telefonie und ADSL beschreibt. In Deutschland werden alle ADSL-Anschlüsse gemäß Annex B ausgeführt. Damit kann die Telefonleitung parallel für ISDN und ADSL genutzt werden. In den meisten anderen Ländern werden ADSL-Anschlüsse dagegen in der Regel gemäß Annex A ausgeführt. Diese Spezifikation erlaubt die parallele Nutzung der Leitung für analoge Telefonanschlüsse und ADSL.

Vor der ersten Verwendung müssen Sie den ADSL-Router konfigurieren. Normalerweise verbinden Sie Ihren Rechner mit dem Router, starten einen Webbrowser und geben die IP-Adresse des Routers ein, also z. B. `http://192.168.0.101`. (Die richtige Adresse steht im Handbuch zum Router.) Damit gelangen Sie in ein komfortables Web-Interface zur ADSL-Konfiguration. Für eine PPPoE-Konfiguration müssen Sie dort nur den Benutzernamen und das Passwort Ihrer ADSL-Verbindung angeben.

Wenn Ihr Provider dagegen PPPoA einsetzt, müssen Sie auch die Parameter VPI (*Virtual Path Identifier*) und VCI (*Virtual Channel Identifier*) einstellen. Die richtigen Werte hängen von der ATM-Infrastruktur des Providers ab und sind provider- und landesspezifisch. Die folgende Tabelle fasst einige gängige Werte zusammen:

Belgien:	VPI=8 VCI=35
Dänemark:	VPI=0 VCI=35
Italien:	VPI=8 VCI=35
Frankreich:	VPI=8 VCI=35
Niederlande:	VPI=8 VCI=48
Österreich:	VPI=8 VCI=48
Spanien:	verschiedene Kombinationen, z. B. 1/32, 1/33, 8/32 und 8/35

Fragen Sie gegebenenfalls Ihren Provider, welche Werte Sie einsetzen müssen, oder suchen Sie im Internet nach *VPI VCI list*.

Manuelle ADSL-Modem-Konfiguration für PPPoE

Konfiguration der Netzwerkkarte

Die Verbindung zwischen dem ADSL-Modem und Ihrem Computer erfolgt über ein Ethernet-Kabel. Dabei wird allerdings nicht wie sonst üblich das Protokoll TCP/IP verwendet. Daher werden weder die IP-Adresse noch die Netzmaske der Netzwerkschnittstelle berücksichtigt. Eine Konfiguration ist daher nicht erforderlich. Insbesondere darf die Netzwerkschnittstelle nicht als Gateway konfiguriert werden!

pppd-Konfiguration

PPPoE wird unter Linux von einem Kernelmodul verarbeitet. Damit `pppd` die Netzwerkschnittstelle für PPPoE nutzen kann, setzen Sie das `pppd`-Plugin `rp-pppoe.so` ein. Diese Datei wird bei den meisten gängigen Linux-Distributionen zusammen mit `pppd` installiert.

Zur `pppd`-Konfiguration benötigen Sie eine Konfigurationsdatei in `/etc/ppp/peers/`. Die folgenden Zeilen setzen voraus, dass `/etc/options` leer ist. Das Passwort zur `name`-Einstellung muss sich in `chap-` oder `pap-secrets` befinden.

```
# /etc/ppp/peers/adsl
# PPPoE-spezifische Optionen
plugin rp-pppoe.so
mru 1492
mtu 1492

# an diese Schnittstelle ist das ADSL-Modem angeschlossen
eth0

# Standard-PPP-Optionen
lock
noauth
noipdefault
defaultroute
usepeerdns

# Login-Name für /etc/ppp/pap-secrets bzw. chap-secrets
name "hofer"

# bei Verbindungsabbruch nach 4 Sekunden Wartezeit
# eine neue Verbindung herstellen
persist
holdoff 4
maxfail 25

# für Red Hat/Fedora
ipparam "adsl"
```

Durch `persist` wird die Verbindung nach einem Abbruch automatisch wiederhergestellt. `holdoff` stellt die Wartezeit zwischen einem Verbindungsabbruch und dem

Neustart ein. `maxfail` gibt an, nach wie vielen erfolglosen Verbindungsversuchen `pppd` aufgibt.

Die `ipparam`-Option ist notwendig, damit die automatische DNS-Konfiguration bei Red Hat bzw. Fedora funktioniert. Dort ist zusätzlich die folgende Datei erforderlich:

```
# /etc/sysconfig/network-scripts/ifcfg-adsl
PEERDNS=yes
```

Automatischer Verbindungstest

`pppd` bemerkt unter Umständen nicht selbstständig, wenn bei Ihrem Internet-Provider Probleme auftreten und dieser nicht mehr reagiert. Die folgenden Erweiterungen in der Konfigurationsdatei bewirken, dass `pppd` alle 60 Sekunden eine Aufforderung an den Provider sendet, sich zu melden. Wenn zweimal hintereinander keine Antwort kommt, beendet `pppd` die Verbindung. Falls die Konfigurationsdatei `persist` enthält, wird anschließend die Verbindung sofort wieder neu aufgebaut, in der Hoffnung, dass es dann wieder funktioniert.

```
# Ergänzung in /etc/ppp/peers/adsl
lcp-echo-interval 60
lcp-echo-failure 2
```

MTU und MRU

Im Internet werden Daten nicht Byte für Byte, sondern in Paketen übertragen. Die Ethernet-Defaultgröße für solche Pakete beträgt 1500 Byte. Falls sich auf dem Weg zwischen zwei Internetpartnern Hard- oder Software befindet, für die die Datenpakete zu groß sind, werden sie automatisch in kleinere Pakete zerlegt und später wieder zusammengesetzt. Das ist allerdings nicht besonders effizient, weswegen manche Betriebssysteme (unter ihnen Linux) versuchen, die maximale Paketgröße durch das Versenden spezieller ICMP-Pakete herauszufinden. Diese Pakete werden allerdings von manchen Firewalls verschluckt, weswegen die Feststellung der richtigen Paketgröße versagt und mit etwas Pech die Datenübertragung ganz scheitert.

Dieses Problem tritt normalerweise nicht auf, weil der kleinste gemeinsame Nenner, nämlich eine Paketgröße von 1500 Byte, selten überschritten wird. Genau das passiert aber bei PPPoE-Verbindungen, weil ein paar der 1500 Byte für zusätzliche Protokollinformationen verloren gehen. Deswegen müssen MTU (Maximum Transmit Unit) und MRU (Maximum Receive Unit) auf 1492 reduziert werden.

pppd starten und stoppen

Der Start von `pppd` erfolgt durch das folgende Kommando:

```
root#  pppd call adsl
```

Wenn Sie die Verbindung wieder beenden möchten, stoppen Sie `pppd` durch `killall`:

```
root#  killall pppd
```

Bei Debian-basierten Distributionen verwenden Sie alternativ `pon adsl` bzw. `poff adsl`.

Automatischer ADSL-Start durch ein Init-Script

Da die Nutzung von ADSL normalerweise zeitlich unbeschränkt ist, liegt es nahe, sofort beim Hochfahren des Rechners eine Internetverbindung herzustellen und diese bis zum Ausschalten aufrechtzuerhalten. Am besten führen Sie das in einem Init-Script durch, das während des Rechnerstarts ausgeführt wird. Der distributionsunabhängige Teil eines derartigen Scripts könnte beispielsweise so aussehen:

```
# /etc/init.d/adsl

# ... distributionsspezifische Anweisungen ...

case "$1" in
    start)
        echo "Starting adsl"
        pppd call adsl
        ;;

    stop)
        echo "Shutting down adsl"
        [ -f /var/run/ppp-adsl.pid ] && \
           kill $(head -1 /var/run/ppp-adsl.pid)
    *)
        echo "Usage: $0 {start|stop}"
        exit 1
        ;;
esac
```

Das Script vermeidet das Kommando `killall pppd`, weil es möglich ist, dass auf einem Rechner mehrere `pppd`-Prozesse laufen. `killall` würde alle derartigen Prozesse stoppen. Dieses Script stoppt dagegen nur den `pppd`-Prozess, dessen Prozessnummer es aus der Datei `/var/run/ppp-adsl.pid` liest. Dabei wird zuerst getestet, ob diese Datei existiert. Wenn das der Fall ist, ermittelt `head -1` die erste Zeile, die die Prozessnummer enthält, und übergibt diese an `kill`.

Damit `pppd` seine Prozessnummer tatsächlich in `/var/run/ppp-adsl.pid` speichert, müssen Sie die folgende Zeile in die `pppd`-Konfigurationsdatei einfügen:

```
# Ergänzung in /etc/ppp/peers/adsl
linkname "adsl"
```

Nachdem Sie das Script mit `/etc/init.d/adsl start` bzw. `stop` getestet haben, müssen Sie es noch so einrichten, dass es automatisch gestartet wird (siehe Abschnitt 16.5).

MSS-Clamping

Leider gelten die MTU- und MRU-Optionen für `pppd` nur für den lokalen Rechner. Wenn dieser Rechner gleichzeitig ein Internet-Gateway für andere Rechner ist (siehe das folgende Kapitel), dann müsste auch auf jedem Client-Rechner die MTU-Einstellung verändert werden.

Um den dadurch verursachten Konfigurationsaufwand zu vermeiden, gibt es eine bessere Lösung, das sogenannte MSS-Clamping. Dabei wird am Gateway die MSS-Option von TCP-Datenpaketen an den lokalen MTU-Wert angepasst. (MSS steht für *Maximum Segment Size*. Um wirklich zu verstehen, was hier vor sich geht, müssen Sie TCP-Experte sein.)

Um das MSS-Clamping kümmert sich das `iptables`-System des Kernels, wenn Sie die folgende Paketfilterregel aktivieren. Dabei ersetzen Sie `eth0` durch die Schnittstelle, an der Ihr ADSL-Modem angeschlossen ist:

```
root#  iptables -o eth0 --insert FORWARD 1 -p tcp --tcp-flags SYN,RST SYN \
               -m tcpmss --mss 1400:1536 -j TCPMSS --clamp-mss-to-pmtu
```

Üblicherweise wird dieses Kommando Teil des Firewall-Scripts des Gateway-Rechners sein. Sie können die Regel aber auch in das oben beschriebene Init-Script einbauen. Allerdings müssen Sie dann sicherstellen, dass die Regel bei einem mehrfachen Start des ADSL-Systems nur einmal ausgeführt wird.

Kapitel 30
Internet-Gateway

An dieser Stelle beginnen mehrere Kapitel, die sich mit der Konfiguration eines Linux-Servers für das lokale Netzwerk (LAN) beschäftigen. Es wäre vermessen zu versuchen, die gesamte Bandbreite der Linux-Server-Konfiguration darin abzuhandeln. Beinahe jeder Abschnitt dieser Kapitel würde ein eigenes Buch rechtfertigen.

In den Kapiteln zur Server-Konfiguration versuche ich primär, Ihnen einen ersten Einstieg in dieses für fortgeschrittene Linux-Anwender so wichtige Thema zu geben. Ich richte mich dabei vor allem an Personen, die verhältnismäßig kleine, lokale Netze verwalten, wobei sich in diesen Netzen durchaus auch Windows-Clients befinden dürfen.

ADSL-Router ...

In diesem Kapitel geht es darum, ein Internet-Gateway für das lokale Netzwerk zusammenzustellen. Im Privatbereich erfüllt oft ein ADSL-Router diese Aufgabe. Das hat durchaus Vorteile: Die Konfiguration ist unkompliziert, das Gerät läuft lautlos und verbraucht wenig Strom. Kurz und gut: Wenn Sie mit Ihrem ADSL-Router zufrieden sind, behalten Sie ihn, und überspringen Sie dieses Kapitel! Sie ersparen sich damit eine Menge Zeit und Mühe.

... versus eigenes Gateway

Es gibt aber Fälle, in denen die Konfigurationsmöglichkeiten eines ADSL-Routers unzureichend sind. Das führt zum Inhalt dieses Kapitels, also der Konfiguration eines eigenen Rechners, der die folgenden drei Funktionen des ADSL-Routers übernimmt: Masquerading, DHCP-Server und Nameserver. Jedes Internet-Gateway sollte unbedingt durch eine Firewall abgesichert werden. Diesbezügliche Informationen folgen in Kapitel 40, »Firewalls«.

IPv6

Ich gehe in diesem Kapitel vorerst davon aus, dass Sie Ihr lokales Netzwerk für IPv4 konfigurieren. Wie Sie *zusätzlich* jedem Rechner im LAN eine IPv6-Adresse und Zugang zum IPv6-Netz geben, beschreibt ein eigener Abschnitt am Ende des Kapitels. Dort begründe ich auch, warum eine reine IPv6-Konfiguration momentan nicht zweckmäßig ist und warum selbst der Parallelbetrieb von IPv4 und IPv6 nicht unbedingt ein Vorteil sein muss.

30.1 Einführung

Dieses Kapitel beschreibt die Installation der folgenden Komponenten bzw. Dienste:

- **Masquerading/NAT:** Mit Masquerading können alle Clients im lokalen Netz mit dem Internet verbunden werden. Es gibt also einen Linux-Rechner, der via ISDN oder ADSL eine Internetverbindung herstellt. Alle anderen Rechner sind mit diesem Rechner verbunden und können so ebenfalls das Internet nutzen. Es ist nicht notwendig, jeden Rechner mit seinem eigenen Modem auszustatten!
- **DHCP und DNS:** DHCP ermöglicht eine zentrale und einfache Verwaltung der IP-Adressen und der anderen Netzwerkparameter aller Clients. Ein lokaler Nameserver stellt sicher, dass die Clients gegenseitig ihre Namen kennen (Auflösung lokaler Namen in IP-Adressen). Außerdem fungiert das Programm als IP-Nummern-Cache, sodass wiederholte Internetzugriffe ein wenig beschleunigt werden.

  Zur Realisierung der DHCP- und DNS-Funktionen stelle ich zwei Varianten vor: Am einfachsten ist der Einsatz des Programms Dnsmasq, das beide Funktionen in sich vereint und einfach zu konfigurieren ist. Für gehobene Anforderungen bzw. große oder komplexe lokale Netzwerke empfiehlt sich dagegen die Aufteilung der Funktionen auf die beiden Programme `dhcpd` und `bind`. Das erhöht nicht nur die Konfigurationsmöglichkeiten, sondern auch den dafür erforderlichen Aufwand.

Hardware

Soweit das Internet-Gateway keine weiteren Aufgaben erfüllen soll, reicht ein minimal ausgestatteter, langsamer PC vollkommen aus. Eine wesentliche Voraussetzung sind aber zwei Netzwerkschnittstellen: eine, um den Rechner an den ADSL-Router bzw. an das ADSL-Modem anzuschließen, und eine zweite für das lokale Netzwerk.

Auf der Suche nach einem leisen, kostengünstigen und energiesparenden Rechner werden Sie rasch feststellen, dass die zweite Netzwerkschnittstelle die größte Hürde ist: Mini-PCs haben zumeist nur eine Netzwerkschnittstelle und lassen sich nicht durch Steckkarten (PCI, PCIe) erweitern. Ein möglicher Ausweg ist ein USB-Ethernet-Adapter. Vergewissern Sie sich aber vor dem Kauf, dass das Gerät Linux-kompatibel ist!

Eine interessante Alternative sind OpenWrt-kompabile WLAN-Router. Das besondere Merkmal dieser Geräte besteht darin, dass die Firmware durch eine Linux-Version ersetzt werden kann und darf. Im Internet gibt es gleich eine ganze Palette von geeigneten Distributionen (Tomato, DD-WRT, OpenWrt etc.). Natürlich erfordert die Inbetriebnahme etwas Bastelarbeit. Dafür erhalten Sie ein billiges, vollkommen lautloses Gerät, dessen Stromverbrauch wesentlich geringer ist als bei marktüblichen Mini-PCs.

https://openwrt.org

Für derartige Anwendungen sehr attraktive technische Daten und insbesondere zwei GBit-Ethernet-Schnittstellen hat auch der ARM-Computer Utilite. Das Gerät war im Sommer 2013 allerdings noch nicht lieferbar:

http://utilite-computer.com

Installation von Paketen

Bei den meisten Distributionen sind die Pakete der in diesem Kapitel beschriebenen Server-Dienste standardmäßig *nicht* installiert. Sie müssen die erforderlichen Pakete selbst installieren, z. B. mit `apt-get`, `yum` oder `zypper`.

Konfigurationshilfen

Dieses Kapitel richtet sich an fortgeschrittene Linux-Anwender. Es werden ausschließlich die Einstellungen der diversen Konfigurationsdateien beschrieben, nicht aber eventuell zur Verfügung stehende Benutzeroberflächen zur Konfiguration. Bei Fedora und Red Hat sind das diverse `system-config-xxx`-Kommandos, bei SUSE die NETZWERKDIENSTE-Module in YaST.

Der hier gewählte Ansatz – also die manuelle Veränderung von Konfigurationsdateien – mag altmodisch erscheinen, bewährt sich aber in der Praxis: Wenn Sie die Konfiguration manuell durchführen, wissen Sie auch, wo sich die Konfigurationsdateien befinden. Und nur damit gelingt es, eine fertige Konfiguration relativ rasch auf einen anderen Server zu übernehmen, beispielsweise bei einer Neuinstallation oder bei einem Distributionswechsel.

Sicherheit

Ein Router sollte das lokale Netzwerk durch eine Firewall gegen unerwünschte Zugriffe von außen absichern. Diesbezügliche Tipps gibt Kapitel 40.

Topologie des Beispielnetzwerks

Um Ihnen die Orientierung in diesem Kapitel zu erleichtern, fasst Abbildung 30.1 die Topologie des Beispielnetzwerks zusammen. Das lokale Netzwerk verwendet den Adressraum 192.168.0.* und den Domainnamen `sol`. Der Gateway-Rechner mit dem Hostnamen `mars` hat die fixe Adresse 192.168.0.1. Die Internetverbindung wird über einen ADSL-Router hergestellt. Die einfachste Form der WLAN-Anbindung erfolgt durch einen Access-Point, der mit dem Switch verbunden ist.

Die Clients im Netzwerk sind über einen Switch mit `mars` verbunden. Den Clients werden dynamische Adressen zugewiesen (192.168.0.2 bis 192.168.0.253). Einzige Ausnahme ist der Netzwerkdrucker `pluto`, dessen IP-Adresse statisch auf 192.168.0.254 eingestellt wurde.

Sicherheitsüberlegungen

Aus Sicherheitsgründen wäre es am besten, auf dem Rechner `mars` nur den Internetzugang und eine Firewall zu realisieren. Bei kleinen Netzen oder im Privatbereich sprechen Kosten- und Energiesparüberlegungen hingegen dafür, so wie hier beschrieben alle Server-Funktionen auf einem Rechner zu integrieren.

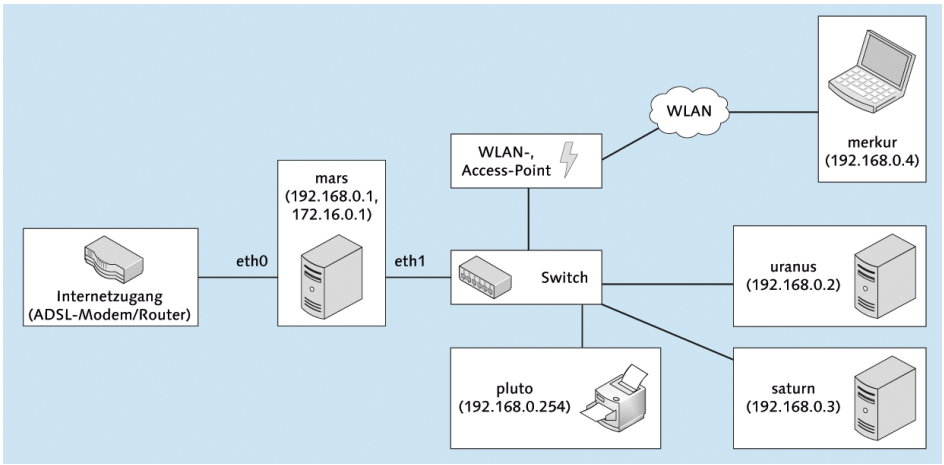


Abbildung 30.1 Topologie des Beispielnetzwerks

Auch die WLAN-Anbindung ließe sich mit etwas Konfigurationsaufwand sicherer gestalten: Eine Möglichkeit besteht darin, anstelle des Access-Points einen selbstständigen WLAN-Router einzusetzen. Eine andere Variante besteht darin, einen WLAN-Access-Point über eine dritte Netzwerkschnittstelle des Routers anzusteuern (siehe Abbildung 30.2).

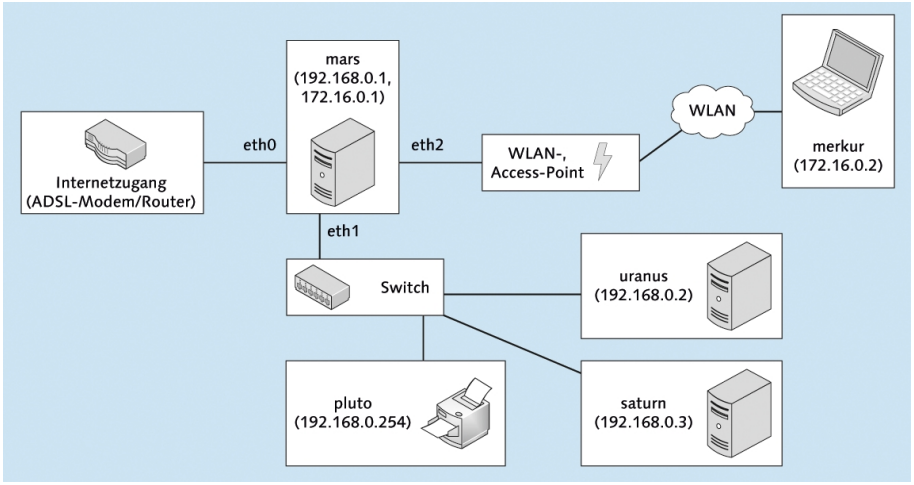


Abbildung 30.2 Variante mit Trennung zwischen LAN und WLAN

Damit nutzen das LAN und das WLAN nun zwei getrennte Netzadressbereiche – beispielsweise 192.168.0.* für das LAN und 172.16.0.* für das WLAN. Daraus ergibt sich die Möglichkeit, für die beiden Netzwerke unterschiedliche Netzwerkdienste anzu-

bieten – beispielsweise Internet- und SSH-Zugang per LAN und WLAN, aber Samba- oder MySQL-Zugang nur per LAN.

Richtig elegant wird diese Variante, wenn für die WLAN-Verbindung zwischen dem Netzwerk-Server und dem WLAN-Client ein Virtual Private Network (VPN) errichtet wird: Damit ist eine nahtlose Integration der WLAN-Clients in das gewöhnliche Netz möglich, ohne Abstriche bei der Sicherheit machen zu müssen.

30.2 Netzwerkkonfiguration

Die Netzwerkkonfiguration eines Internet-Gateways werden Sie in der Regel manuell durchführen, wie ich dies in Abschnitt 29.5 beschrieben habe. Davon abweichend besteht die einzige Besonderheit bei einem Internet-Gateway darin, dass es *zwei* Netzwerkschnittstellen gibt: Eine stellt die Verbindung zum Internet her, die andere die Verbindung zum lokalen Netzwerk.

Unter Debian oder Ubuntu muss die Konfigurationsdatei `/etc/network/interfaces` so ähnlich wie das folgende Beispiel aussehen: **Debian, Ubuntu**

```
# /etc/network/interfaces
auto lo
iface lo inet loopback

# dynamische Verbindung zu einem DHCP-Server,
# der die Eckdaten des Internetzugangs vermittelt
auto eth0
iface eth0 inet dhcp

# statische Konfiguration für die Verbindung zum LAN
auto eth1
iface eth1 inet static
  address 192.168.0.1
  netmask 255.255.255.0
```

Wenn die Verbindung in das Internet statisch konfiguriert wird, muss der `eth0`-Block in der `interfaces`-Datei wie folgt angepasst werden. Das Beispiel geht davon aus, dass der Internetzugang über einen ADSL-Router erfolgt, der die IP-Adresse 10.0.0.138 hat, so wie das SpeedTouch-Gerät, das bei mir zu Hause läuft. Diese Adresse ist gleichzeitig die Gateway-Adresse zum Internet (Schlüsselwort `gateway`).

```
# /etc/network/interfaces
...
# statische Verbindung zum ADSL-Router mit der IP-Adresse 10.0.0.138
auto eth0
iface eth0 inet static
```

```
address 10.0.0.1
netmask 255.255.255.0
gateway 10.0.0.138
```

Fedora, Red Hat

Bei Fedora bzw. Red Hat benötigen Sie je eine Konfigurationsdatei `ifcfg-xxx` im Verzeichnis `/etc/sysconfig/network-scripts`, wobei `xxx` jeweils der Name der Netzwerkschnittstelle ist. Die Datei für die Schnittstelle zum ADSL-Router richten Sie so ein wie in Abschnitt 29.5 beschrieben. Die folgende Datei beschreibt die Schnittstelle zum lokalen Netzwerk:

```
# Datei /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
HWADDR=xx:xx:xx:xx:xx:xx
NM_CONTROLLED=no
ONBOOT=yes
BOOTPROTO=none
TYPE=Ethernet
IPADDR=192.168.0.1
NETMASK=255.255.255.0
```

/etc/resolv.conf

Unabhängig von der Distribution müssen Sie außerdem sicherstellen, dass `/etc/resolv.conf` die IP-Adresse des Nameservers enthält.

30.3 Masquerading (NAT)

Der Ausgangspunkt für das Masquerading ist ein Rechner, der bereits mit dem Internet verbunden ist – in diesem Kapitel also der Rechner `mars`. Das Ziel ist es nun, auch allen anderen Rechnern im lokalen Netz den Zugang zum Internet zu ermöglichen.

Die Rechner im lokalen Netz verwenden private IP-Adressen: Diese Adressen liegen in den speziell dafür reservierten Adressbereichen (z. B. 10.*.*.* oder 192.168.*.*). Die Adressen sind nur innerhalb des LANs eindeutig, nicht aber darüber hinaus im Internet. Das Internet-Gateway kann deswegen die Internetanforderungen im LAN nicht einfach weiterleiten.

Masquerading

Das Prinzip des Masqueradings besteht darin, dass der Gateway-Rechner an das Internet adressierte Datenpakete der Clients annimmt und deren Absenderadresse so verändert, als würden sie vom ihm selbst stammen. Diese Adressänderung wird auch als *Network Address Translation* (NAT) bezeichnet.

Jetzt kann das Datenpaket in das Internet weitergeleitet werden. Im Regelfall kommt aus dem Internet nach einer Weile eine Antwort – beispielsweise die angeforderte Webseite. Das Gateway muss die Antwort an den richtigen Client weiterleiten. Dazu muss es die korrekte Zieladresse erraten. Das Datenpaket wurde ja (nach der Adress-

änderung) von ihm selbst abgesandt, daher ist auch die Antwort an das Gateway adressiert.

Um eine Adresszuordnung der Antwortpakete zu ermöglichen, verändert das Gateway nicht nur die Absenderadresse, sondern auch den Absender-Port. Für jede IP-Adresse innerhalb des lokalen Netzes wird eine bestimmte Port-Nummer verwendet. Linux-intern ist für das Masquerading `iptables` zuständig. Das ist ein in den Kernel integriertes System zur Verarbeitung von IP-Paketen.

Wenn der Gateway-Rechner über einen ADSL-Router mit dem Internet verbunden ist (also nicht über ein Modem), führt dieses Gerät nochmals Masquerading oder eine andere Form der Adressmanipulation durch. Daraus ergeben sich glücklicherweise keine Probleme.

Masquerading- und Firewall-Funktionen sind eng miteinander verwandt. In diesem Abschnitt gehe ich davon aus, dass der Rechner *nicht* schon als Firewall konfiguriert ist. Sollte das der Fall sein, müssen Sie die Masquerading-Funktionen mit dem Firewall-Konfigurationswerkzeug Ihrer Wahl einrichten oder aber einzelne Firewall-Funktionen abschalten, bevor Sie das Masquerading mit dem Kommando `iptables` manuell aktivieren können. Hintergrundinformationen darüber, was Firewalls sind und wie sie funktionieren, finden Sie in Kapitel 40.

Client/Server-Begriff

Im Folgenden wird der Rechner mit dem Internetzugang als Server bezeichnet, alle anderen Rechner als Clients, ganz unabhängig davon, welche Funktionen diese Rechner sonst erfüllen. Im Fall von Masquerading wird der Server oft auch als *Internet-Gateway* (korrekt) oder als *Internet-Router* bezeichnet.

Diese Unterscheidung zwischen Client und Server gilt für das gesamte Buch – aber immer nur für eine bestimmte Funktion! Ein Rechner, der bezüglich seines Internetzugangs ein Client ist, kann durchaus für eine andere Funktion (etwa NFS) ein Server sein. In der Praxis werden sehr oft mehrere Server-Funktionen auf einem einzigen Rechner konzentriert. Das ist aber nicht zwingend notwendig und aus Effizienzgründen – gerade in großen Netzen – auch nicht immer sinnvoll.

Masquerading ein- und ausschalten

Debian, Ubuntu

Bei Debian und Ubuntu stehen standardmäßig keine Konfigurationswerkzeuge für die Firewall und das Masquerading zur Verfügung. Sie können aber beispielsweise das Programm FireStarter installieren und damit eine Firewall und gleichzeitig auch das Masquerading aktivieren.

Fedora

Bei aktuellen Fedora-Versionen mit dem FirewallD-System ordnen Sie die Schnittstelle, mit der der Rechner mit dem Internet verbunden ist, der Firewall-Zone `exter-`

nal zu. Damit wird für diese Schnittstelle das Masquerading aktiviert. Gleichzeitig aktiviert Fedora auch das IP-Forwarding.

```
# Datei /etc/sysconfig/network-scripts/ifcfg-xxx (Schnittstelle zum Internet)
...
ZONE=external
```

RHEL 6 Unter RHEL 6 können Sie das Masquerading mit dem Programm system-config-firewall einschalten. Im Dialogblatt TRUSTED SCHNITTSTELLE markieren Sie die Schnittstelle zum LAN. Damit stellen Sie sicher, dass die Firewall den Netzwerkverkehr zum LAN nicht blockiert. Außerdem wählen Sie im Dialogblatt MASQUERADING die Schnittstelle aus, die mit dem Internet verbunden ist.

SUSE Bei SUSE ordnen Sie im YaST-Modul SICHERHEIT • FIREWALL die LAN-Schnittstelle dem internen Netzwerk zu. Anschließend aktivieren Sie im Dialogblatt MASQUERADING die gleichnamige Option.

Manuell aktivieren Wenn Sie das Masquerading ohne Firewall-Werkzeuge steuern möchten, führen Sie dazu zwei kurze Kommandos aus:

```
root#  sysctl -w net.ipv4.ip_forward=1
root#  iptables -A POSTROUTING -t nat -o eth0 -j MASQUERADE
```

Das sysctl-Kommando aktiviert die IP-Forwarding-Funktion des Kernels, die aus Sicherheitsgründen in der Standardeinstellung deaktiviert ist. Sollte sysctl bei Ihrer Distribution nicht zur Verfügung stehen, können Sie stattdessen das folgende Kommando ausführen:

```
root#  echo 1 > /proc/sys/net/ipv4/ip_forward
```

Das iptables-Kommando definiert eine Regel, gemäß der IP-Pakete, die das lokale Netzwerk verlassen sollen, über das Interface eth0 geleitet und dabei entsprechend den NAT-Regeln manipuliert werden. Je nachdem, wie Ihr Internetzugang konfiguriert ist, müssen Sie statt eth0 eine andere Schnittstelle angeben, etwa ppp0. (eth0 ist in diesem Kapitel die Schnittstelle, über die der Router mit dem Internet verbunden ist.)

Manuell deaktivieren Um die Masquerading-Funktionen zu deaktivieren, führen Sie folgende Kommandos aus:

```
root#  iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
root#  sysctl -w net.ipv4.ip_forward=0
```

Statt sysctl funktioniert auch dieses echo-Kommando:

```
root#  echo 0 > /proc/sys/net/ipv4/ip_forward
```

Masquerading automatisch aktivieren

Natürlich werden Sie das Masquerading nicht bei jedem Rechnerstart des Servers manuell aktivieren. Die übliche Vorgehensweise besteht darin, das Masquerading im Rahmen einer Firewall zu aktivieren. Sollten Sie Ihre Firewall manuell einrichten, aktivieren Sie die Firewall inklusive Masquerading durch ein Script, das während des Init-Prozesses ausgeführt wird (mehr dazu finden Sie in Kapitel 27, »Das Init-System«). Distributionsunabhängig funktioniert das in Abschnitt 27.4 vorgestellte Init-V-Script. Vergessen Sie aber nicht, das Script durch `chkconfig` (Red Hat), `insserv` (Debian, SUSE) bzw. `update-rc.d` (Ubuntu) zu aktivieren!

Unabhängig vom Firewall-System können Sie das IP-Forwarding bei den meisten Distributionen durch einen Eintrag in die Datei `/etc/systcl.conf` bleibend aktivieren. Diese Datei wird bei jedem Rechnerstart ausgewertet.

```
# in /etc/sysctl.conf
...
net.ipv4.ip_forward = 1
```

Probleme

Das Masquerading ist zwar eine elegante Lösung, um im lokalen Netzwerk einen Internetzugang gemeinsam zu nutzen; es kann aber auch Probleme geben:

- Bei einer ganzen Reihe von Internetprotokollen sind Schutzmechanismen vorgesehen, in denen die Zuordnung von IP-Adressen überprüft wird. Der durch das Masquerading nicht mehr eindeutige Zusammenhang zwischen IP-Adresse und einem Rechner kann Schwierigkeiten verursachen.
- Manche Protokolle sehen vor, dass IP-Adressen nicht nur in den IP-Paketen, sondern auch innerhalb der Datenpakete übertragen werden (als ASCII-Text oder auch verschlüsselt). Ein bekanntes Beispiel dafür ist FTP. Damit FTP trotz des Masqueradings funktioniert, muss der Masquerading-Server also nicht nur die Adressierung von IP-Paketen ändern, sondern in manchen Fällen auch deren Inhalt!

  Linux sieht für eine ganze Reihe von Internetdiensten entsprechende Masquerading-Module vor (z. B. `nf_nat_ftp` für FTP). Die Module werden automatisch geladen. Sollte das nicht der Fall sein, müssen Sie sie mit `modprobe` aktivieren:

  ```
  root#  modprobe nf_nat_ftp
  root#  modprobe nf_conntrack_ftp
  ```

  Wenn in FTP-Clients dennoch Verbindungsprobleme auftreten, lassen sich diese zumeist durch einen Betrieb im passiven Modus beheben. Die meisten FTP-Clients aktivieren diesen Modus automatisch oder bieten zumindest eine manuelle Einstellmöglichkeit.

- Wenn der Masquerading-Server via ADSL/PPPoE mit dem Internet verbunden ist, kann es Probleme mit der maximalen IP-Paketlänge geben. Die Abhilfe besteht darin, bei allen Clients die maximale Paketlänge (MTU) zu reduzieren oder auf dem Server ein sogenanntes *MSS-Clamping* durchzuführen. Dazu führen Sie bei der Aktivierung der Masquerading-Funktion das folgende `iptables`-Kommando aus. Es bewirkt, dass zu große Pakete gekennzeichnet werden.

```
root#  iptables -I FORWARD -p tcp --tcp-flags SYN,RST SYN \
         -j TCPMSS --clamp-mss-to-pmtu
```

Client-Konfiguration

Damit ein Client den vom Linux-Gateway zur Verfügung gestellten Internetzugang nutzen kann, müssen Sie bei der Netzwerkkonfiguration des Clients zwei Dinge beachten:

- Als Gateway-Adresse muss die IP-Adresse des Linux-Gateways angegeben werden (bei der Topologie laut Abbildung 30.1 also 192.168.0.1).
- Die Nameserver-Adresse muss mit der IP-Adresse des Nameservers für das Linux-Gateway übereinstimmen. Diese Adresse wird vom Internet Service Provider zugewiesen und kann der Datei `/etc/resolv.conf` des Linux-Gateways entnommen werden.

30.4 DHCP- und Nameserver-Grundlagen

DHCP

Natürlich können Sie in einem lokalen Netzwerk bei jedem Rechner die Netzwerkparameter separat einstellen. Das ist aber ebenso mühsam wie fehleranfällig. Außerdem handeln Sie sich jede Menge Zusatzarbeit ein, wenn Sie sich irgendwann dazu entschließen, die Topologie Ihres Netzwerks zu ändern.

Wesentlich intelligenter ist es, wenn *ein* Rechner sich darum kümmert, allen anderen Rechnern ihre IP-Adresse und andere Netzwerkparameter zuzuweisen. Dazu wird das *Dynamic Host Configuration Protocol* (DHCP) eingesetzt. Der Steuerungsrechner wird DHCP-Server genannt, die anderen Rechner DHCP-Clients. Es gibt zwei grundsätzliche Konfigurationsvarianten:

- **Dynamische Konfiguration:** Bei den Clients wird nur der Hostname eingestellt. Der DHCP-Server ist für alle anderen Konfigurationsparameter zuständig, weist den Clients also die IP-Adresse, die Gateway-Adresse, die Nameserver-Adresse etc. zu. Für die IP-Adressen gibt es einen Adresspool, aus dem der DHCP-Server für jeden Client dynamisch eine gerade freie Adresse wählt.

- **Statische Konfiguration:** Bei dieser Konfigurationsvariante identifiziert der DHCP-Server die Clients anhand der ID-Nummer der Netzwerkkarte. Damit kann er ihnen jedes Mal dieselbe IP-Adresse und optional auch den Hostnamen zuweisen. Diese Konfigurationsvariante ist mit etwas mehr Aufwand verbunden, ermöglicht dafür aber immer gleich bleibende IP-Adressen sowie eine zentrale Verwaltung der Hostnamen.

Einfacher ist in der Regel die erste Variante. Sie können beide Verfahren auch kombinieren, beispielsweise um sicherzustellen, dass ein Drucker immer dieselbe fixe IP-Adresse hat.

DHCP-Interna

Die Funktionsweise von DHCP sieht in etwa so aus: Wenn ein Rechner (also ein DHCP-Client) neu gestartet wird, schickt er eine Rundsendung an die Adresse 255.255.255.255. Durch diese Adressierung erreicht die Anfrage *alle* Rechner im lokalen Netz. Der DHCP-Server reagiert auf diese Anfrage und sendet als Antwort eine IP-Adresse aus der Liste der verfügbaren IP-Adressen.

Vielleicht fragen Sie sich, wohin der Server die Antwort sendet, denn der Client hat ja noch gar keine IP-Adresse. Zur Adressierung reicht die MAC-Adresse aus – und die ist aus der Anfrage bereits bekannt.

Der DHCP-Server vergibt IP-Adressen für eine bestimmte Zeitspanne (Lease Time). Diese Zeitspanne beträgt normalerweise einen Tag, kann aber beliebig eingestellt werden. Bevor diese Zeitspanne vergeht, muss der Client die Adresse beim DHCP-Server erneuern oder eine neue Adresse anfordern.

Nameserver

Ein *Domain-Nameserver* (kurz Nameserver, noch kürzer DNS) stellt den Zusammenhang zwischen Rechnernamen und IP-Adressen her. Jeder Internet Service Provider stellt einen DNS zur Verfügung, der zu Rechnernamen die passende IP-Nummer ermittelt. Statt auf diesen DNS zurückzugreifen, können Sie für Ihr lokales Netzwerk einen eigenen Nameserver einrichten. Das hat zwei Vorteile:

- **Höhere Geschwindigkeit:** Der DNS verwaltet einen Cache der zuletzt benutzten Internetadressen. Wenn Sie also zum zweiten Mal an einem Tag zu `www.yahoo.com` surfen, muss nicht wieder der DNS Ihres Internet-Providers gefragt werden, welches nun die IP-Adresse von Yahoo ist. Der lokale DNS hat sich die Adresse schon gemerkt.
- **Lokale Namensauflösung:** Der DNS verwaltet die Namen und IP-Adressen der Rechner des lokalen Netzes. Damit kennen sich alle Rechner im lokalen Netzwerk namentlich, und Sie können beispielsweise am Rechner `merkur` das Kommando `ping saturn` ausführen. `merkur` kontaktiert nun den lokalen Nameserver, der die IP-Adresse von `saturn` zurückgibt.

Die lokale Namensauflösung ist eine Grundvoraussetzung dafür, dass im lokalen Netzwerk Dienste wie NFS, FTP, SSH etc. komfortabel genutzt und konfiguriert werden können.

Weltweit sind unzählige DNS im Einsatz, die alle gegenseitig in Kontakt stehen. Wenn also ein DNS einen Namen nicht selbst kennt, gibt er die Anfrage an einen anderen DNS weiter. Die DNS sind hierarchisch organisiert.

30.5 Dnsmasq (DHCP- und Nameserver)

Dieser Abschnitt beschreibt das Programm Dnsmasq, das einen DHCP-Server und einen Nameserver in sich integriert und relativ einfach zu konfigurieren ist. Dnsmasq ist selbst für große lokale Netze ausreichend leistungsfähig.

Die populärste Alternative zu Dnsmasq sind die Programme `dhcpd` und `bind`, die jeweils eine dieser Aufgaben übernehmen. Insbesondere `bind` ist *das* dominierende Nameserver-Programm und damit ein zentraler Bestandteil der Infrastruktur des Internets. Es wird vor allem in den Knotenpunkten des Internets sowie von großen Internet-Providern und -Hostern eingesetzt. Als Nameserver für lokale Netze ist das Programm wegen seiner sehr unübersichtlichen Konfiguration aber weniger gut geeignet.

Voraussetzungen

Ich gehe im Folgenden davon aus, dass Sie das Paket `dnsmasq` installiert haben und dass `dhcpd` und `bind` *nicht* installiert sind – andernfalls kommen sich die Programme in die Quere.

Eine weitere wichtige Voraussetzung ist die korrekte Konfiguration der Datei `/etc/hosts` auf dem Gateway-Rechner. Ich habe die Erfahrung gemacht, dass diese Datei oft nicht den Anforderungen von Dnsmasq entspricht. Werfen Sie einen Blick auf diese Datei, wenn Sie die lokale Netzwerkkonfiguration Ihres Gateways ändern! `/etc/hosts` muss zumindest die beiden folgenden Zeilen enthalten. Entscheidend ist die Zeile für die Zuordnung zwischen dem lokalen Rechnernamen (hier `mars` bzw. `mars.sol`) und der IP-Adresse im LAN (hier 192.168.0.1).

```
# /etc/hosts auf dem Gateway-Rechner
127.0.0.1     localhost
192.168.0.1   mars        mars.sol
...
```

Tipp

Sollte es Probleme geben, werfen Sie auch einen Blick auf Ihre Firewall-Konfiguration! DNS-Anfragen werden über die TCP- und UDP-Ports 53 abgewickelt. DHCP benutzt die UDP-Ports 67 und 68. Diese Ports dürfen auf dem Gateway-Rechner nicht durch eine Firewall blockiert werden!

dnsmasq.conf

Die Konfiguration von Dnsmasq erfolgt durch die Datei `/etc/dnsmasq.conf`. Die standardmäßig mitgelieferte Datei dient gleichzeitig als Dokumentation und besteht aus rund 500 Kommentarzeilen. Sie können bei einzelnen schon vorgesehenen Anweisungen das Kommentarzeichen entfernen und die betreffende Zeile aktivieren. Übersichtlicher ist es aber zumeist, eine Sicherheitskopie von `dnsmasq.conf` zu erstellen und mit einer neuen, leeren Konfigurationsdatei zu beginnen.

```
root#  mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig
root#  touch /etc/dnsmasq.conf
```

Für die Konfiguration von Dnsmasq sind neben `/etc/dnsmasq.conf` auch `/etc/hosts` und `/etc/resolv.conf` entscheidend.

Bei aktuellen Debian- und Ubuntu-Versionen werden außerdem alle in `/etc/dnsmasq.d` enthaltenen Konfigurationsdateien berücksichtigt. Außerdem enthält die Datei `/etc/default/dnsmasq` einige Grundeinstellungen für Dnsmasq, unter anderem `ENABLED=1`, sodass Dnsmasq standardmäßig durch das Init-System gestartet wird.

Start/Neustart

Wie die meisten Programme, die in diesem und den folgenden Kapiteln vorgestellt werden, arbeitet Dnsmasq als sogenannter Dämon (Systemdienst). Bei einigen Distributionen wird das Programm sofort nach der Installation gestartet. Wenn das nicht der Fall ist, müssen Sie das Programm manuell starten. Auch Konfigurationsänderungen werden erst nach einem Neustart wirksam:

```
root#  service dnsmasq restart
```

Ebenfalls von der Distribution abhängig ist, ob das Programm in Zukunft beim Hochfahren des Rechners automatisch gestartet wird. Bei Fedora, Red Hat und SUSE ist das standardmäßig nicht der Fall. Abhilfe schaffen diese Kommandos:

```
root#  chkconfig --level 35 dnsmasq on      (RHEL)
root#  systemctl enable dnsmasq.service     (openSUSE, Fedora)
root#  insserv dnsmasq                      (Debian, ältere SUSE-Distributionen)
```

Minimalkonfiguration

Bereits in der folgenden Minimalkonfiguration funktioniert `dnsmasq.conf` zufriedenstellend. Das Programm arbeitet in dieser Konfiguration als Nameserver-Cache für das Internet und stellt den Clients IP-Adressen aus dem Bereich zwischen 192.168.0.2 und 192.168.0.250 zur Verfügung. Die Clients behalten ihren eigenen Hostnamen.

```
# /etc/dnsmasq.conf  (Minimalkonfiguration)
domain-needed
bogus-priv
interface=eth1
dhcp-range=192.168.0.2,192.168.0.250,24h
```

Kurz eine Erläuterung der Schlüsselwörter: `domain-needed` und `bogus-priv` verhindern, dass Dnsmasq lokale Hostnamen bzw. lokale IP-Adressen an den Nameserver Ihres Internet-Providers weitergibt. Der Nameserver des ISP ist nur für Internetnamen/-adressen zuständig, nicht für lokale Namen/Adressen.

`interface` gibt an, dass Dnsmasq in seiner Funktion als DHCP-Server nur auf Anfragen antworten soll, die von der Schnittstelle `eth1` kommen, die in der Beispieltopologie für das LAN zuständig ist. Wenn Dnsmasq auf die Anfragen von mehreren Schnittstellen reagieren soll, können Sie diese auflisten (`interfaces=eth1,eth2`). Alternativ besteht mit `except-interfaces=...` die Möglichkeit, die Schnittstellen anzugeben, die Dnsmasq *nicht* beachten soll.

`dhcp-range` gibt an, welchen Adressbereich der DHCP-Server zur Beantwortung von DHCP-Anfragen nutzen soll. Vergebene Adressen bleiben 24 Stunden lang gültig und müssen dann vom Client erneuert werden.

Nicht extra konfiguriert werden müssen die Nameserver- und Gateway-Adressen. Dnsmasq wertet selbstständig `/etc/resolv.conf` aus und greift auf den dort angegebenen Nameserver zurück. An DHCP-Clients wird als Nameserver- und Gateway-Adresse jeweils die lokale IP-Adresse übertragen.

Einsatz als lokaler Nameserver

In der obigen Minimalkonfiguration kann Dnsmasq lokale Adressen nur auflösen, wenn `/etc/hosts` entsprechende Informationen enthält. Dynamisch per DHCP zugewiesene Adressen kennt der Nameserver dagegen nicht. Damit Dnsmasq auch als Nameserver für die Clients im LAN funktioniert, fügen Sie die folgenden Zeilen zu `dnsmasq.conf` hinzu und weisen Dnsmasq an, die Konfigurationsdatei neu einzulesen. `sol` ist dabei der Domainname des Beispielnetzes.

```
# /etc/dnsmasq.conf  (Einsatz als Nameserver für lokale Adressen)
...
local=/sol/
domain=sol
expand-hosts
```

Das Schlüsselwort `local` gibt an, dass Adressanfragen aus dieser Domain direkt von Dnsmasq beantwortet werden sollen (nicht vom Nameserver des ISP).

`domain` gibt an, dass Dnsmasq den DHCP-Clients den angegebenen Domainnamen zuweisen soll. Dieser Name muss mit dem in `local` angegebenen Namen übereinstimmen.

`expand-hosts` bewirkt schließlich, dass bei Nameserver-Anfragen ohne Domain automatisch die in `domain` angegebene Domain hinzugefügt wird. Wenn Sie also `ping uranus` ausführen, liefert Dnsmasq die Adresse von `uranus.sol` zurück.

Dnsmasq kennt seine Clients – also die Rechner, die eine IP-Konfiguration via DHCP angefordert haben – nur dann namentlich, wenn diese im Rahmen der DHCP-Kommunikation ihren eigenen Hostnamen an Dnsmasq übermittelt haben. Das ist bei den meisten Distributionen bzw. LAN/WLAN-Konfigurationswerkzeugen standardmäßig der Fall, auch beim NetworkManager. Aufpassen müssen Sie aber, wenn Sie client-seitig Fedora, Red Hat oder alte Debian- und Ubuntu-Versionen einsetzen. Entsprechende Konfigurationstipps finden Sie in Abschnitt 30.5.

Statische Adressen und Hostnamen

Dnsmasq kann auch so konfiguriert werden, dass es die Hostnamen der Clients einstellt. Die statische Zuordnung des Hostnamens und der IP-Adresse erfolgt auf Basis der MAC-Adresse der Clients. Das ist vor allem für solche Geräte praktisch, bei denen sich nicht ohne Weiteres ein Hostname einstellen lässt – beispielsweise bei Netzwerkdruckern. Die Konfiguration erfolgt mit dem Schlüsselwort `dhcp-host`. Das folgende Listing zeigt den Eintrag für den Netzwerkdrucker `pluto`:

```
# /etc/dnsmasq.conf (statische Adresszuordnung)
...
dhcp-host=00:c0:ee:51:39:9f,pluto,192.168.0.254
```

Die mühsamste Aufgabe bei dieser Konfigurationsvariante ist es naturgemäß, die MAC-Adresse (*Media Access Control*) des Clients herauszufinden. Dabei handelt es sich um eine eindeutige ID-Nummer, mit der jeder Ethernet-Controller ausgestattet ist. Unter Linux zeigt `ifconfig` die MAC-Adresse an. Ansonsten verbinden Sie das Gerät einfach mit dem LAN und lassen Dnsmasq eine dynamische DHCP-Konfiguration durchführen. Das Programm protokolliert alle dynamisch zugewiesenen IP-Adressen samt Hostname und MAC-Adresse in der Datei `/var/lib/misc/dnsmasq.leases`. Sie können die MAC-Adresse also dieser Datei entnehmen.

Standardmäßig sind via DHCP zugewiesene IP-Adressen nur 24 Stunden lang gültig. Bei Netzwerkdruckern oder anderen Geräten mit automatischem Stand-by-Modus ist das oft zu kurz. Wenn ein Drucker mehr als 24 Stunden nicht genutzt wird, glaubt Dnsmasq, das Gerät sei ausgeschaltet, und »vergisst« es gewissermaßen. Um das zu verhindern, können Sie die Gültigkeit der Adresse durch eine zusätzliche Zeitangabe verlängern. `infinite` bewirkt, dass die Adresse nie verfällt.

```
# /etc/dnsmasq.conf (statische Adresszuordnung ohne Ablaufzeit)
...
dhcp-host=00:c0:ee:51:39:9f,pluto,192.168.0.254,infinite
```

`man dnsmaq` bzw. `/etc/dnsmasq.conf.orig` beschreibt eine Menge weiterer Syntaxvarianten für `dhcp-host`. Sie können damit beispielsweise eine Zuordnung zwischen dem Hostnamen und der IP-Adresse herstellen, bestimmte MAC-Adressen komplett blockieren etc.

DNS für den lokalen Rechner

Standardmäßig funktioniert Dnsmasq zwar für alle anderen Rechner im Netzwerk als Nameserver, nicht aber für den Gateway-Rechner selbst! Der Grund besteht darin, dass auf dem lokalen Rechner der in `/etc/resolv.conf` angegebene Nameserver verwendet wird. Diese Datei verweist in der Regel auf den Nameserver Ihres Internet-Providers oder Routers.

Falls auf dem Gateway weitere Server-Programme laufen sollen (ein Datei-Server, Kerberos etc.), ist es erforderlich, dass das Gateway die Clients namentlich kennt, also ebenfalls Dnsmasq als Nameserver verwendet. Damit das funktioniert, müssen Sie auf die folgenden Punkte achten:

- `/etc/resolv.conf` muss auf Dnsmasq (also auf `localhost`, Adresse 127.0.0.1) verweisen, nicht auf einen externen Nameserver. Vorsicht: Wenn Sie die Verbindung zum Internet dynamisch konfigurieren (LAN plus DHCP oder über ein Modem plus PPP), wird `resolv.conf` bei jedem Verbindungsaufbau überschrieben. Das müssen Sie verhindern: Konfigurieren Sie die Verbindung zum ADSL-Router statisch, bzw. verändern Sie die PPP-Konfiguration so, dass `resolv.conf` nicht angerührt wird.
- Dnsmasq kann nun nicht mehr `resolv.conf` auswerten, um die Adresse des externen Nameservers zu ermitteln. Deswegen müssen Sie dessen Adresse in `dnsmasq.conf` explizit mit dem Schlüsselwort `server` angeben.

Wie so oft macht ein Beispiel alles klarer. Nehmen wir an, der Gateway-Rechner `mars` mit der IP-Adresse 192.168.0.1 im LAN ist über die Ethernet-Schnittstelle `eth0` mit einem ADSL-Router verbunden. Der Router hat die IP-Adresse 10.0.0.138. Damit `mars` mit dem ADSL-Router kommunizieren kann, wird die Schnittstelle `eth0` statisch konfiguriert. (Auch wenn der ADSL-Router DHCP unterstützt, ist eine dynamische Konfiguration via DHCP nicht zweckmäßig, weil sonst `resolv.conf` bei jedem Rechnerstart mit den DHCP-Daten des ADSL-Routers überschrieben wird!)

```
# in /etc/network/interfaces
...
# statische Verbindung zum ADSL-Router bzw. in das Internet
auto eth0
iface eth0 inet  static
   address 10.0.0.1
   netmask 255.255.255.0
   gateway 10.0.0.138
...
```

Die Datei `/etc/resolv.conf` gibt den Namen der lokalen Domäne (`sol`) und die IP-Adresse des lokalen Nameservers an (also Dnsmasq):

```
# /etc/resolv.conf
search      sol
nameserver  192.168.0.1
```

Bleibt noch die Konfiguration von Dnsmasq: Dnsmasq kann die Adresse des externen Nameservers (für Internetzugriffe) nun nicht mehr als `resolv.conf` lesen. Vielmehr soll das Programm `resolv.conf` nun ignorieren (Option `no-resolv`) und als externen Nameserver die mit `server` angegebene Adresse kontaktieren:

```
# /etc/dnsmasq.conf
...
no-resolv
server=10.0.0.138
...
```

Alles zusammen

Falls Sie während dieser stückweisen Präsentation diverser Dnsmasq-Einstellungen den Überblick verloren haben, finden Sie hier die Zusammenfassung der endgültigen `dnsmasq.conf`-Datei:

```
# /etc/dnsmasq.conf

# Schnittstelle zum LAN
interface=eth1

# lokale Hosts nicht dem Upstream-Nameserver melden
domain-needed
bogus-priv

# Domainname sol im LAN
local=/sol/
domain=sol
expand-hosts
```

```
# Dnsmasq auch für das Gateway (Upstream-Nameserver = 10.0.0.138)
server=10.0.0.138
no-resolv

# dynamische Adressen
dhcp-range=192.168.0.2,192.168.0.250,24h

# statische Adressen
dhcp-host=00:c0:ee:51:39:9f,pluto,192.168.0.254,infinite
```

Konfiguration für mehrere Schnittstellen

Mitunter kommt es vor, dass Dnsmasq mehrere Netzwerkschnittstellen bedienen soll und diese mit IP-Adressen aus unterschiedlichen Netzwerksegmenten versorgen soll. In diesem Fall müssen Sie mit `interfaces` alle Schnittstellen angeben. Außerdem ist für jede Schnittstelle eine eigene `dhcp-range`-Anweisung erforderlich:

```
# /etc/dnsmasq.conf
interface=eth1,eth2
dhcp-range=192.168.0.2,192.168.0.250,24h
dhcp-range=172.16.0.2,172.16.0.250,12h
...
```

Das obige Beispiel geht davon aus, dass auf dem Gateway die Schnittstelle `eth1` mit der IP-Adresse 192.168.0.1 verbunden ist und die Schnittstelle `eth2` mit der IP-Adresse 172.16.0.1. Damit ist auch klar, welche `dhcp-range`-Anweisung für welche Schnittstelle gilt.

In Sonderfällen sieht Dnsmasq auch vor, dass die Schnittstelle in der `dhcp-range`-Anweisung explizit angegeben wird:

```
# /etc/dnsmasq.conf
interface=eth1,eth2
dhcp-range=interface:eth1,192.168.0.2,192.168.0.250,24h
dhcp-range=interface:eth2,172.16.0.2,172.16.0.250,12h
...
```

`man dnsmasq` weist im Abschnitt `NOTES` darauf hin, dass diese Konfigurationsvariante nur selten erforderlich ist.

Logging

Dnsmasq trägt automatisch alle dynamisch zugewiesenen IP-Adressen in die Datei `/var/lib/misc/dnsmasq.leases` oder `/var/lib/dnsmasq/dnsmasq.leases` ein. Statische Adressen werden dabei nicht berücksichtigt. Jeder Eintrag in dieser Datei enthält auch die MAC-Adresse und (soweit bekannt) den Hostnamen des Clients. Die Datei bietet somit eine gute Möglichkeit, um die MAC-Adresse neuer Clients herauszufinden.

Wenn Dnsmasq nicht wunschgemäß funktioniert, fügen Sie das Schlüsselwort `log-queries` in `dnsmasq.conf` ein. Das Programm protokolliert nun sämtliche Nameserver-Anfragen in `/var/log/syslog` oder `/var/log/messages`.

Client-Konfiguration

Die richtige Konfiguration eines Rechners, der seine IP-Konfiguration via DHCP beziehen soll, ist grundsätzlich ganz einfach. Jede Linux-Distribution und alle aktuellen Windows-Versionen bieten eine entsprechende Option im Netzwerkkonfigurationsdialog an – im Prinzip war's das schon! Auch der unter Linux immer öfter eingesetzte NetworkManager erkennt die DHCP-Daten einer LAN- oder WLAN-Verbindung selbstständig.

Der einzig kritische Punkt ist der Umgang mit dem Hostnamen: Normalerweise soll der auf dem Client fix eingestellte Hostname zurück an den DHCP-Server gesendet werden. Die meisten DHCP-Client-Tools tun das standardmäßig. Zu den Ausnahmen zählen Fedora und Red Hat. Bei diesen Distributionen wird ein statisch eingestellter Hostname *nicht* zurück an den DHCP-Server übertragen! Wenn Sie das möchten, müssen Sie den zu sendenden Namen extra einstellen. Dazu starten Sie das Programm `system-config-network`, öffnen mit BEARBEITEN den Eigenschaftsdialog der Netzwerkschnittstelle (üblicherweise `eth0`) und geben den Hostnamen bei den DHCP-Einstellungen an. Diese Einstellung ist auch erforderlich, wenn die Verbindung mit dem NetworkManager hergestellt wird!

DHCP-Daten neu einlesen

Zum Ausprobieren des DHCP-Servers müssen Sie die Clients natürlich nicht jedes Mal neu starten. Ein Neustart der Netzwerkfunktionen reicht vollkommen aus. Wenn Sie den NetworkManager verwenden, wählen Sie in dessen Menü einfach die betreffende Schnittstelle aus. Das Programm unterbricht dann die vorhandene Verbindung und stellt sie neu her.

Wenn Ihre Netzwerkkonfiguration ohne NetworkManager erfolgt, fordern Sie mit den folgenden Kommandos die DHCP-Informationen neu an:

```
root#  /etc/init.d/networking restart   (Debian, Ubuntu)
root#  service network restart          (Fedora, Red Hat, SUSE)
```

Anschließend vergewissern Sie sich mit `ifconfig` sowie durch einen Blick in die Datei `/etc/resolv.conf`, ob alles funktioniert hat. Wenn Sie unter KDE oder Gnome arbeiten, müssen Sie sich nach der Veränderung des Hostnamens oder anderer grundlegender Netzwerkparameter aus- und wieder neu einloggen!

Selbst unter Windows ist ein Neueinlesen der DHCP-Daten ohne Neustart möglich. Öffnen Sie einfach ein Kommandofenster, und führen Sie das folgende Kommando aus:

```
>  ipconfig /renew                    (Windows)
```

30.6 IPv6-Gateway

Wozu IPv6 im LAN?

Bevor Sie sich an die Arbeit machen, müssen Sie sich eine Frage gefallen lassen: Wozu soll das Ganze gut sein? Eine ausschließliche IPv6-Lösung kommt nicht infrage – bis auf Weiteres, vermutlich noch für viele Jahre, benötigen alle Geräte im LAN auch eine IPv4-Adresse, um vernünftig nutzbar sein. Die Karte des IPv6-Internets ist noch ziemlich weiß, denn die meisten Websites und Dienste funktionieren nur mit IPv4. IPv6 kann also nur eine Ergänzung sein.

Aus technischer Sicht ist die zusätzliche IPv6-Anbindung nicht besonders kompliziert, selbst dann, wenn Ihr Provider momentan nur IPv4 anbietet: Sie beziehen dann Ihre IPv6-Adressen eben von einem Tunnelbroker, z. B. von SixXs wie in der folgenden Anleitung; jeder Ihrer Rechner im lokalen Netzwerk hat dann sowohl eine IPv4- als auch eine IPv6-Adresse. Damit kann nun jeder im LAN bei Bedarf reine IPv6-Dienste nutzen, wenn diese in IPv4 nicht zur Verfügung stehen.

IPv6-Sicherheitsbedenken

Die zusätzliche IPv6-Verbindung erfordert auf jeden Fall auch zusätzliche Sicherheitsmaßnahmen, d. h. neue Firewall-Regeln (siehe Kapitel 40) und gegebenenfalls eine Aktivierung der Privacy Extensions. Außerdem sollten Sie sich im Klaren darüber sein, dass die IPv6-Funktionen im Kernel und in den diversen Netzwerkdiensten bei weitem noch nicht so gut getestet sind wie IPv4-Funktionen. Es kann gut sein, dass in den nächsten Jahren noch grundlegende Fehler und Sicherheitsmängel entdeckt werden.

Grundlagen

Neue Wege ohne Masquerading und NAT

Wie ich in den vorigen Abschnitten beschrieben habe, verwenden Privatanwender und kleine Firmen und Organisationen für lokale IPv4-Netze zumeist einen privaten Adressbereich in Kombination mit Masquerading und NAT. Keiner reflektiert mehr darüber, dass das eigentlich eine Notlösung ist, ein hässlicher Hack, um IPv4-Adressen zu sparen.

Ein lokales IPv6-Netz sieht ganz anders aus: Von Ihrem Provider oder von einem Tunnelbroker erhalten Sie nicht *eine* IPv6-Adresse, sondern gleich ein ganzes /64-Teilnetz, das aus IPv4-Sicht unvorstellbar riesig ist. Die Aufgabe des IPv6-Gateways besteht nun darin, allen Rechnern im lokalen Netzwerk eine eindeutige IPv6-Adresse in diesem Subnetz zuzuteilen. Dieser Aspekt der Gateway-Konfiguration unterscheidet sich also grundlegend von IPv4-Netzen.

IPv6 und NAT

Jetzt, da lokale Netzwerke endlich ohne NAT funktionieren, werden plötzlich auch die Vorteile von NAT deutlich. NAT ersetzt zwar keine Firewall, stellt aber doch einen gewissen Schutz des lokalen Netzwerks nach außen hin dar. Außerdem ist die Struktur des lokalen Netzwerks von außen nicht zu erkennen. Schließlich sind Netzwerkanfragen anonymer als unter IPv6. Aus all diesen Gründen hat man beschlossen, NAT auch für IPv6 zu implementieren. Diese Entscheidung war allerdings sehr umstritten, und persönlich glaube ich, dass die Nachteile von NAT schwerer wiegen als die Vorteile. Wie auch immer: Der Linux-Kernel unterstützt ab Version 3.7, also seit Dezember 2012, ein IPv6-NAT-Verfahren. Eine konkrete Anleitung, wie Sie NAT unter IPv6 einsetzen können, finden Sie hier:

http://atoomnet.net/howto-ipv6-nat-in-centos-6

Router Advertisement versus DHCP

Zur automatischen IPv4-Konfiguration benötigen Sie einen DHCP-Server. Für IPv6 ist das auch ein möglicher Weg, aber nicht der einzige. Der IPv6-Standard sieht nämlich im Neighbor Discovery Protocol (NDP) verschiedene Mechanismen zur selbstständigen Konfiguration der IP-Adresse durch den Client vor.

Ein wenig vereinfacht sieht die Vorgehensweise so aus: Sobald eine Netzwerkschnittstelle eine IPv6-Konfiguration durchführen möchte, sendet sie eine *Router Solicitation* aus, also eine ICMP-Nachricht, die an alle Geräte im lokalen Netzwerk geht und die um Antwort von Routern bittet. Ihr Gateway-Rechner bzw. alle anderen Router im Netz senden als Antwortpaket das sogenannte *Router Advertisement*.

Im Rahmen dieses Informationsaustausches erfährt die Netzwerkschnittstelle, in welchem Netzwerk sie sich befindet und welches die IP-Adresse des Routers ist. Diese Daten sind ausreichend, um selbst eine eindeutige IP-Adresse zu wählen und die Routing-Tabelle entsprechend einzurichten. Etwas detaillierter ist das Verfahren in der Wikipedia beschrieben:

http://de.wikipedia.org/wiki/Neighbor_Discovery_Protocol

In der einfachsten Form müssen Sie zur IPv6-Gateway-Konfiguration nur das Programm `radvd` einrichten. Dabei handelt es sich um ein Hintergrundprogramm zum Aussenden der Router Advertisements. Wie Sie im nächsten Abschnitt sehen werden, ist die Konfiguration sehr einfach. Das Verfahren hat aber den Nachteil, dass es den Nameserver-Aspekt ausblendet: Auf den Client-Rechnern muss deswegen eine manuelle Nameserver-Konfiguration erfolgen. Außerdem kennen sich die Rechner im lokalen IPv6-Netzwerk nicht namentlich, d. h. `ping6 jupiter` funktioniert nicht.

Um diese Einschränkungen zu vermeiden, werden auch für IPv6 DHCP-Server immer populärer. Bei meinen Tests hat sich allerdings ergeben, dass bei Weitem noch nicht alle Linux-Distributionen mit DHCPv6 problemlos zurechtkommen. Sie erkaufen sich den Vorteil einer umfassenderen Auto-Konfiguration also durch andere Probleme, sodass mir eine uneingeschränkte Empfehlung für einen DHCP-Server schwerfällt. Erste Experimente sollten Sie besser mit `radvd` durchführen!

Noch ein Punkt spricht gegen den DHCP-Einsatz: Wenn die IPv6-Adressen durch eine DHCP-Server dezidiert vorgegeben werden, können die in Abschnitt 30.6 beschriebenen Privacy Extensions nicht zum Einsatz kommen.

Voraussetzungen

Die folgenden Anleitungen setzen vier Dinge voraus:

- Die Konfiguration des Gateway-Rechners erfolgt statisch. Der Network Manager ist deaktiviert.
- Ihr Gateway-Rechner ist bereits für den IPv4-Betrieb konfiguriert und das lokale IPv4-Netzwerk funktioniert (siehe die vorherigen Abschnitte dieses Kapitels).
- Ihr Gateway-Rechner hat zusätzlich eine funktionierende IPv6-Verbindung, z. B. via SixXs (siehe Kapitel 29, »Netzwerkkonfiguration«). `ping6 google.com` darf keine Fehler liefern.
- Sie verfügen über ein /64-Netz, dessen Adressen Sie an die Computer im lokalen Netzwerk verteilen können.

SixXs-Subnetzdetails

In gehe in diesem Abschnitt davon aus, dass Sie keinen echten IPv6-Internetzugang haben und die IPv6-Konnektivität über einen Tunnelbroker beziehen. Besser wäre natürlich einen echter IPv6-Zugang, aber für den Testbetrieb ist ein SixXs-Tunnel absolut ausreichend. Allzu viele IPv6-Anwendungen gibt es ja ohnedies noch nicht, und die durch den Tunnel bedingte etwas schlechtere Geschwindigkeit stört zumeist nicht.

Wenn Sie sich bei SixXs um einen IPv6-Tunnel bewerben, wird im ersten Schritt nur ein Tunnel für *eine* IPv6-Adresse freigeschaltet. Nach der Konfiguration des `aiccu`-Clients auf einem Rechner hat dieser IPv6-Zugang (siehe Abschnitt 29.3).

Damit Sie nun ein ganzes Netzwerk mit IPv6 versorgen können, müssen Sie bei SixXs außerdem ein /64-Netz anfordern. Beachten Sie bei der weiteren Konfiguration unbedingt, dass sich Ihre Einzel-IPv6-Adresse *nicht* in diesem /64-Netz befindet. Die Eckdaten des zugewiesenen /64-Netzes müssen Sie nach einem Login auf der SixXs-Website nachlesen:

https://www.sixxs.net/home

Wenn Ihr IPv6-Gateway eine Weile aktiv ist und IPv6-Verkehr produziert, können Sie, quasi zur Belohnung, nach ein bis zwei Wochen sogar ein /48-Netz anfordern. Darin können Sie dann selbst mehrere /64-Netze einrichten. Das ist für die hier präsentierte Anleitung aber nicht erforderlich, *ein* /64-Netz reicht vollkommen.

Beispieladressen

Für diesen Abschnitt gelten beispielhaft die folgenden SixSs-Daten. Dabei handelt es sich natürlich nicht um gültige IP-Adressen, d. h., Sie müssen Ihre eigenen IP-Adressen verwenden!

IP-Adresse des SixXs-Tunnels:	2001:1234:789a:0471::1/64
Lokale IP-Adresse des Gateway-Rechners (`sixxs`):	2001:1234:789a:0471::2/64
Subnetz für das lokale Netzwerk (`eth1`):	2001:1234:789a:8471::/64

Vorbereitungsarbeiten auf dem Gateway-Rechner

IPv6-Konfiguration der Schnittstelle zum LAN

Die Schnittstelle zum lokalen Netzwerk bleibt in dieser Anleitung gemäß Abbildung 30.1 weiterhin `eth1`. Diese Schnittstelle ist bereits statisch für IPv4 konfiguriert. Jetzt muss diese Schnittstelle aber auch noch eine IPv6-Adresse innerhalb des IPv6-Bereichs erhalten, der für das lokale Netzwerk vorgesehen ist. Ich habe mich gleich für die erste mögliche Adresse entschieden, also für 2001:1234:789a:8471::1. Die beiden folgenden Listings zeigen die Konfiguration unter Fedora bzw. Ubuntu:

```
# Ergänzung in /etc/sysconfig/network-scripts/ifcfg-xxx (Fedora)
# (xxx ist die Schnittstelle zum LAN)
IPV6INIT=yes
IPV6ADDR=2001:1234:789a:8471::1/64
IPV6FORWARDING=yes
```

```
# Ergänzung in /etc/network/interfaces (Debian/Ubuntu)
auto eth1
iface eth1 inet6 static
  address 2001:1234:789a:8471::1
  netmask 64
  dns-nameservers 2001:4860:4860::8888
```

IPv6-Forwarding

Damit der Gateway-Rechner die eintreffenden IPv6-Datenpakete der anderen Rechner im lokalen Netzwerk weiterleiten kann, muss das IPv6-Forwarding aktiviert werden:

```
root#  sysctl -w net.ipv6.conf.all.forwarding=1
```

Damit das in Zukunft automatisch geschieht, ergänzen Sie die `sysctl.conf`-Datei um eine Zeile:

```
# Datei /etc/sysctl.conf ergänzen
net.ipv6.conf.all.forwarding=1
```

Beachten Sie, dass durch das Forwarding zwei ansonsten standardmäßig aktive IPv6-Funktionen deaktiviert werden: Die IPv6-Schnittstellen senden nun keine Soliciting-Pakete mehr aus, um andere Router im lokalen Netzwerk zu finden, und sie reagieren nicht mehr auf Router-Advertisement-Nachrichten, die normalerweise zur Durchführung der automatischen IPv6-Konfiguration verwendet werden. Mit anderen Worten: Sobald Sie IPv6-Forwarding aktivieren, müssen Sie die IPv6-Schnittstellen dieses Rechners statisch konfigurieren.

Gateway-Konfiguration mit radvd

radvd-Konfiguration

Nun muss auf dem Gateway-Rechner noch das Paket `radvd` installiert werden. Der Programmname `radvd` steht für *Router Advertisement Daemon*. Die Konfiguration befindet sich in der Datei `/etc/radvd.conf`. Die zumeist ausreichende Minimalkonfiguration sieht wie folgt aus:

```
interface eth0 {
  AdvSendAdvert on;
  prefix 2001:1234:789a:8471::/64
  {
  };
};
```

Dabei müssen Sie den Namen der Netzwerkschnittstelle und die Netzwerkadresse anpassen. Beachten Sie, dass der Start von `radvd` scheitert, wenn das IPv6-Forwarding nicht aktiviert ist.

Gateway aktivieren

Damit sind Sie schon fertig! Jetzt müssen Sie sich nur noch darum kümmern, dass der `radvd`-Dienst jetzt und in Zukunft gestartet wird.

```
root#  service radvd start
root#  systemctl enable radvd      (Fedora)
```

Eigentlich sollte von nun an alles wie von Zauberhand funktionieren: Beim nächsten Aufbau einer Netzwerkverbindung bzw. nach einiger Zeit vollkommen automatisch sollten die Client-Rechner eine IPv6-Adresse im angegebenen Netzwerk annehmen und die IPv6-Routing-Tabelle entsprechend aktualisieren. Einzig die DNS-Konfiguration müssen Sie manuell vornehmen, entweder durch eine direkte Veränderung von `/etc/resolv.conf` oder durch eine entsprechende Option im Dialogblatt der IPv6-Einstellungen des NetworkManagers (siehe Abbildung 30.3). Sofern Ihnen Ihr Internet-Provider keinen IPv6-Nameserver zur Verfügung stellt, verwenden Sie am besten den öffentlichen Nameserver von Google mit der Adresse 2001:4860:4860::8888.

Abbildung 30.3 IPv6-LAN-Konfiguration im NetworkManager

Fehlersuche auf dem Gateway-Rechner

Wenn es Probleme gibt, sollten Sie auf dem Gateway-Rechner und auf den Clients mit `ping6` und mit `ip` die einzelnen Teilfunktionen testen: Funktioniert ein `ping6` zwischen den Rechnern im lokalen Netzwerk? Funktioniert ein `ping6` nach außen, wenn Sie z. B. die oben erwähnte IP-Adresse der Google-DNS-Server angeben? Funktioniert der Nameserver, d. h., klappt auch ein `ping6 google.com`? Praktisch sind auch Testseiten wie *http://test-ipv6.com*, auf denen alle Eckdaten der bestehenden Internetverbindung in einem Webbrowser überprüft werden (siehe Abbildung 30.4).

Abbildung 30.4 IPv6-Testseite

Als Vergleichsbasis für die Fehlersuche sind hier noch die gekürzten Ergebnisse von `ip -6 addr` und `ip -6 route` abgedruckt:

```
root#  ip -6 addr
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000
    inet6 2001:1234:789a:8471::1/64 scope global
    inet6 fe80::a00:27ff:feac:1f24/64 scope link
5: sixxs: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1280 qlen 500
    inet6 2001:1234:789a:471::2/64 scope global
    inet6 fe80::4b8:2ff:471:2/64 scope link
root#  ip -6 route
2001:1234:789a:471::/64 dev sixxs  proto kernel  metric 256
2001:1234:789a:8471::/64 dev eth1  proto kernel  metric 256
default via 2001:1234:789a:471::1 dev sixxs  metric 1024
```

Mit `radvddump` können Sie in einem Terminalfenster verfolgen, welcher Rechner im LAN gerade IP-Daten anfordert und welche Antworten `radvd` sendet.

Fehlersuche auf den Client-Rechnern

Dieselben Tests führen Sie auch auf den Client-Rechnern durch. Als Vergleichsbasis sind im Folgenden auch die gekürzten Ergebnisse von `ip -6 addr` und `ip -6 route` auf einem der Client-Rechner im LAN abgedruckt. `ip -6 neigh` sollte zudem eine Liste der IPv6-Adressen aller anderen im lokalen Netzwerk bekannten Rechner liefen.

```
root#  ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ...
    link/ether 08:00:27:ab:ba:90 brd ff:ff:ff:ff:ff:ff
    inet6 2001:1234:789a:8471:a00:27ff:feab:ba90/64 scope global dynamic
root#  ip -6 route
2001:1234:789a:8471::/64 dev eth0  proto kernel  metric 256  expires 86392sec
default via fe80::a00:27ff:feac:1f24 dev eth0  proto static  metric 1
default via fe80::a00:27ff:feac:1f24 dev eth0  proto ra  metric 1024 ...
```

Gateway-Konfiguration mit Dnsmasq

Die oben beschriebene `radvd`-Konfiguration hat zwei Nachteile: Erstens muss die DNS-Konfiguration im LAN manuell erfolgen, und zweitens kennen sich die Rechner nicht mit ihren IPv6-Hostnamen. Wenn es also im LAN einen Rechner mit dem Hostnamen `jupiter` gibt, dann funktioniert zwar `ping jupiter`, nicht aber `ping6 jupiter`. Dieser Abschnitt zeigt, wie Sie diese Probleme mit `dnsmasq` lösen können. Das setzt voraus, dass Sie eine ausreichend aktuelle Version von `dnsmasq` besitzen! Die IPv6-Funktionen stehen erst ab Version 2.60 bzw. ab März 2012 zur Verfügung.

dnsmasq.conf

Nachdem Sie das Programm `dnsmasq` installiert und `radvd` deinstalliert haben, müssen Sie die Konfigurationsdatei `/etc/dnsmasq.conf` korrekt einstellen. Gegenüber der in Abschnitt 30.5 abgedruckten IPv4-Konfiguration sind nur zwei neue Zeilen erforderlich:

```
# Ergänzungen in /etc/dnsmasq.conf für eine IPv6-Erweiterung des LAN
...
dhcp-range=2001:1234:789a:8471::1,2001:1234:789a:8471::3ff,constructor:eth1,12h
enable-ra
```

Entscheidend ist dabei, dass die erste in `dhcp-range` angegebene IPv6-Adresse mit der Adresse der LAN-Schnittstelle, in diesem Kapitel also `eth1`, übereinstimmt! Das weicht von der sonst üblichen Regel ab, wonach statische Adressen gerade nicht im DHCP-Adressbereich sein sollten.

Die obige Konfiguration setzt voraus, dass `/etc/resolv.conf` bzw. bei Ubuntu `/etc/network/interfaces` die Adresse eines IPv6-Nameservers enthält. Alternativ können Sie die gewünschten Nameserver auch direkt in `dnsmasq.conf` angeben. In `dnsmasq.conf` sind mehrere `server`-Zeilen erlaubt, um mehrere Nameserver-Adressen anzugeben – z. B. eine für IPv4 und eine für IPv6.

```
# Ergänzungen in /etc/dnsmasq.conf, Google DNS verwenden
...
server=2001:4860:4860::8888
```

`/etc/resolv.conf` muss dann auch den Eintrag `nameserver ::1` enthalten, sodass der Gateway-Rechner selbst `dnsmasq` kontaktiert, um die IP-Adresse eines Hostnamen herauszufinden.

Nach einem Neustart von `dnsmasq` wird nun allen Rechnern im lokalen Netzwerk eine IPv6-Adresse aus dem angegebenen Adressbereich exklusive der ersten Adresse zugewiesen. Die Adressen bleiben 12 Stunden lang gültig und müssen dann erneuert werden.

Die Option `enable-ra` aktiviert die Router-Advertisement-Funktionen. Diese sind erforderlich, weil auch beim Einsatz von DHCPv6 ein Teil der IP-Adresskonfiguration über das Neighborhood Discovery Protocol (NDP) erfolgt. Wenn Sie auf die Option `enable-ra` verzichten, müssen Sie parallel zu `dnsmasq` auch `radvd` einsetzen, was die Konfiguration aber unübersichtlich macht.

Nameserver-Funktionen

Sofern Sie die schon bei der IPv4-Konfiguration beschriebenen Nameserver-Optionen in `/etc/dnsmasq.conf` belassen haben (siehe Abschnitt 30.5), agiert `dnsmasq.conf` als Nameserver-Cache für die IPv6-Clients. Die Hostnamen der Rechner im lokalen Netzwerk sind für `dnsmasq` allerdings nur dann bekannt, wenn die Rechner ihren eigenen Namen während der DHCP-Konfiguration zurück an `dnsmasq` melden. Was mittlerweile für IPv4 eine Selbstverständlichkeit ist, bereitet unter IPv6 leider bei vielen Distributionen noch Schwierigkeiten: Bei meinen Tests waren nur aktuelle Ubuntu- und Fedora-Versionen dazu in der Lage.

Protokollauswahl im Dual-Stack-Betrieb

Es gibt momentan recht wenige Webseiten, die sowohl via IPv4 als auch via IPv6 erreichbar sind, aber es gibt sie: *http://google.com*, *http://facebook.com* oder *http://heise.de* sind einige Beispiele und eignen sich gut als Testseiten.

Wenn Sie nun wie in diesem Kapitel beschrieben eine Dual-Stack-Konfiguration durchgeführt haben und eine Webseite beide Protokollvarianten kennt, kommt dann IPv4 oder IPv6 zum Einsatz? Diese Entscheidung fällt der Webbrowser. Bei der Namensauflösung treffen zwei Ergebnisse ein: eine IPv4- und eine IPv6-Adresse. Linux zieht in solchen Fällen IPv6 vor, sofern es sich dabei nicht um eine Tunnel-Lösung handelt. Bei Bedarf lässt sich das Verhalten durch die Datei `/etc/gai.conf` beeinflussen. Hintergrundinformationen finden Sie hier:

http://linux.die.net/man/5/gai.conf
http://biplane.com.au/blog/?p=122
https://isc.sans.edu/diary/IPv6+Focus+Month+IPv6+over+IPv4+Preference/15472

Wenn Sie Firefox verwenden und wissen möchten, welche IP-Adresse zur Kommunikation mit einer Website tatsächlich verwendet wird, sollten Sie das Add-on ShowIP installieren. Firefox zeigt dann in der Add-on-Leiste die IPv4- oder IPv6-Adresse zur aktuellen Seite an. Die Add-on-Leiste aktivieren Sie mit Ansicht • Symbolleisten.

Fehlersuche

Im Sommer 2013 hat sich die Konfiguration von `dnsmasq` als sehr fehleranfällig erwiesen. Die meisten Probleme hatten aber nicht direkt mit `dnsmasq` zu tun, sondern traten client-seitig auf. Deswegen ist es zweckmäßig, die `dnsmasq`-Konfiguration zuerst mit einem Client-Rechner zu testen, der eine aktuelle Linux-Distribution enthält – z. B. Ubuntu oder Fedora. Wenn das funktioniert, können Sie sich einigermaßen sicher sein, dass Sie den Gateway-Rechner richtig eingerichtet haben. Wenn andere Rechner im lokalen Netzwerk nun dennoch keine IPv6-Verbindung zustande bekommen, gibt es verschiedene Fehlerursachen:

- Die eingesetzte Version des NetworkManagers kommt mit DHCPv6 nicht zurecht. Bei meinen Tests war das z. B. unter RHEL 6.4 der Fall. Abhilfe schuf eine manuelle Konfiguration in `ifcfg-eth0`, also `NM_CONTROLLED=no` und `IPV6INIT=yes`.
- Wenn Sie mit dem NetworkManager arbeiten, achten Sie auf die richtige Einstellung der Optionen. Im Dialogblatt IPv6-Einstellungen muss die Methode Automatisch eingestellt sein. Falls Sie probeweise ein reines IPv6-Netz aufbauen, müssen Sie die Option Diese Verbindung benötigt IPv4 deaktivieren.
- Möglicherweise ist die Firewall schuld und blockiert DHCPv6-Pakete. Unter openSUSE 12.3 ist mir die Client-Konfiguration erst gelungen, nachdem ich die Firewall komplett abgeschaltet habe. Im YaST-Firewall-Modul habe ich keine andere Möglichkeit gefunden, den DHCPv6-Datenverkehr zuzulassen.

Zur Fehlersuche empfiehlt es sich, je nach Distribution sowohl auf dem Gateway-Rechner als auch auf dem Client-Rechner in einem Terminal-Fenster `tail -f /var/log/messages` bzw. `/var/log/syslog` auszuführen. Damit können Sie verzögerungsfrei alle Meldungen von `dnsmasq` auf der einen Seite und des NetworkManagers auf der anderen Seite mitverfolgen.

Die Sicherung der Privatsphäre

Das Problem

Das IPv6-Protokoll sieht eine weitgehend selbstständige Konfiguration der IP-Adressen auf dem Client vor. Diese Autokonfiguration kommt in Kombination mit dem Routing Advertisement zum Einsatz, bei den Konfigurationsvarianten dieses Kapitels also nur, wenn auf dem IPv6-Gateway `radvd` läuft. Der Client erfährt durch das Routing Advertisement die IPv6-Adresse seines Netzwerks und verwendet diese für die ersten 64 Bit seiner IPv6-Adresse (bei einem /64-Netz). In die restlichen 64 Bit bettet der Client die MAC-Adresse des Netzwerkadapters sowie den hexadezimalen Code `fffe` ein. Das folgende Listing verdeutlicht den Mechanismus der IPv6-Autokonfiguration:

```
MAC-Adresse:     08:00:27:ab:ba:90
Netzwerkadresse: 2001:1234:789a:471::
6 Stellen MAC:                    800:27
Hexcodes ff, fe:                        ff:fe
6 Stellen MAC:                               ab:ba90
Ergebnis:        2001:1234:789a:471:800:27ff:f2ab:ba89
```

Im Klartext bedeutet das: Wenn die Autokonfiguration aktiv ist, erhält jeder Rechner eine weltweit eindeutige IPv6-Adresse. Die IPv6-Entwickler sahen das vor 15 Jahren als Vorteil. Aus Datenschutzgründen sind eindeutige IPv6-Adressen für jedes Gerät aber nicht so glücklich: Die Werbewirtschaft freut sich, dass sie Ihre Webaktivität ohne Cookies und andere Hilfsmittel ganz bequem verfolgen und noch bessere Profile Ihrer persönlichen Interessen erstellen kann. Und die NSA und die anderen Geheimdienste ersparen sich auch eine Menge unnötiger Arbeit, um herauszufinden, welcher Datenverkehr wem zuzuordnen ist ...

Privacy Extensions

Noch lange, bevor IPv6 irgendeine praktische Relevanz hatte, wurden Datenschutzvereingungen aktiv und forderten eine Nachbesserung. Diese gibt es mittlerweile in Form der *Privacy Extensions*, einer Erweiterung zum IPv6-Standard. Die Idee ist einfach: Die lokale IPv6-Adresse wird regelmäßig, je nach Konfiguration z. B. täglich, geändert. An freien IPv6-Adressen herrscht ja kein Mangel.

Die bisherige IPv6-Adresse wird nicht sofort komplett deaktiviert, sondern bleibt für bereits existierende Verbindungen noch eine Weile gültig. Neue Verbindungen verwenden dann bereits die neue IPv6-Adresse. Dass dieses Konzept überhaupt

möglich ist, liegt daran, dass es bei IPv6 von Anfang an vorgesehen war, dass eine Schnittstelle mehrere IP-Adressen haben darf.

Was bringt's?

Über den Nutzen der Privacy Extensions gibt es geteilte Meinungen. Relativ gut funktionieren diese, wenn Ihnen Ihr IPv6-Provider bei jedem Verbindungsaufbau ein neues IPv6-Subnetz zuteilt oder wenn sich innerhalb Ihres eigenen Netzes viele Benutzer mit aktiven Privacy Extensions befinden. Weitgehend nutzlos sind die Privacy Extensions hingegen, wenn Sie einen IPv6-Internet-Zugang alleine nutzen oder nur mit wenigen Personen im Haushalt teilen und der IPv6-Provider bzw. das IPv6-Gateway Ihnen jedes Mal dasselbe Subnetz zuteilt: Dann reicht schon die Auswertung des Netzwerkteils der IPv6-Adresse, um den Datenverkehr zuzuordnen.

Einschränkungen und Probleme

Leider ist der Einsatz der Privacy Extensions mit Einschränkungen verbunden:

- Die Privacy Extensions sind inkompatibel zu DHCPv6, bei dem ein DHCP-Server jedem Rechner im lokalen Netzwerk eine IPv6-Adresse zuweist.
- Lange Downloads oder SSH-Sessions können durch den Adresswechsel gestört werden.

Trotz der Privacy Extensions behält der Computer zusätzlich eine weltweit gültige IPv6-Adresse. Diese wird standardmäßig zwar nicht genutzt, sie kann aber dazu verwendet werden, um von außen eine Verbindung aufzubauen. Das ist insbesondere dann praktisch, wenn auf dem Rechner auch Server-Dienste laufen, beispielsweise ein SSH-Server.

Aktivierung/ Deaktivierung

Die Privacy Extensions laufen auf den Client-Rechnern. Eine zentrale Aktivierung auf Router-Ebene ist daher nicht möglich. Unter Linux werden die Privacy Extensions durch verschiedene Kernelparameter `net.ipv6.conf.x.y` gesteuert, wobei `x` der Name der Schnittstelle ist und `y` der Name des Parameters (siehe Tabelle 30.1). Ausgenommen sind Loopback- und Point-to-Point-Schnittstellen, für die die Privacy Extensions immer deaktiviert sind.

Parameter	Bedeutung
`use_tempaddr`	gibt an, ob die Privacy Extensions aktiv sind oder nicht. Zulässige Werte sind 0 (deaktiviert), 1 (öffentliche Adressen vorziehen) oder 2 (temporäre Adressen verwenden).
`temp_prefered_lft`	steuert die aktive Nutzungszeit temporärer IP-Adressen (Default: 86.400 Sekunden, also einen Tag).
`temp_valid_lft`	bestimmt die passive Nutzungszeit temporärer IP-Adressen (Default: 604.800 Sekunden, also sieben Tage).

Tabelle 30.1 Kernelparameter zur Steuerung der Privacy Extensions

Die Defaulteinstellung von `use_tempaddr` variiert je nach Distribution. Im Sommer 2013 waren die Privacy Extensions unter Ubuntu standardmäßig aktiv:

```
root#  cat /proc/sys/net/ipv6/conf/all/use_tempaddr
2
```

Bei allen anderen Distributionen tragen Sie in `/etc/sysctl.conf` die folgenden zwei Zeilen ein:

```
# Datei /etc/sysctl.conf
net.ipv6.conf.all.use_tempaddr=2
net.ipv6.conf.default.use_tempaddr=2
```

`sysctl -f` aktiviert die Einstellungen. Anschließend müssen Sie für die betreffende Schnittstelle die Verbindung neu herstellen. Manuell gelingt das am einfachsten mit `ifdown xxx` und `ifup xxx`.

Möglicherweise werden in Zukunft auch die Einstellungsdialoge des NetworkManagers die Möglichkeit bieten, die Privacy Extensions zu steuern. Bei der KDE-Variante, die unter openSUSE zum Einsatz kommt, ist dies bereits der Fall.

Test

Nach der Aktivierung der Privacy Extensions können Sie sich mit `ip addr` vergewissern, dass alles geklappt hat:

```
root#  ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc ...
  link/ether 08:00:27:d1:31:09 brd ff:ff:ff:ff:ff:ff
  inet 192.168.0.159/24 brd 192.168.0.255 scope global eth0
     valid_lft forever preferred_lft forever
  inet6 2001:7b8:2ff:8471:dce6:4b6c:18f5:a6e9/64 scope global temporary dynamic
     valid_lft 86394sec preferred_lft 14394sec
  inet6 2001:7b8:2ff:8471:a00:27ff:fed1:3109/64 scope global dynamic
     valid_lft 86394sec preferred_lft 14394sec
  inet6 fe80::a00:27ff:fed1:3109/64 scope link
     valid_lft forever preferred_lft forever
```

`ip addr` zeigt, dass neben einer IPv4-Adresse gleichzeitig *drei* IPv6-Adressen aktiv sind! Die Adresse 2001:...:a6e9 ist die temporäre Adresse, die sich aus der Nutzung der Privacy Extensions ergibt. Die Adresse 2001:...:3109 enthält wie bisher die MAC-Daten. Es gibt also weiterhin eine weltweit gültige IPv6-Adresse. Vorrang hat nun aber die temporäre Adresse. Sie können sich davon durch einen Besuch der Seite *http://test-ipv6.com* vergewissern. Die Adresse fe80:...:3109 dient weiterhin ausschließlich zur Kommunikation innerhalb des lokalen Netzwerks.

Kapitel 31
Samba

Mit Samba stellen Sie Dateien bzw. Verzeichnisse ins lokale Netzwerk. Anwender mit Windows-, Linux- und Apple-Rechnern können darauf zugreifen. Ein fein differenziertes Authentifizierungs- und Rechtesystem steuert, wer welche Dateien lesen bzw. verändern darf. Samba ist somit der zentrale Knotenpunkt zum Datenaustausch in einem lokalen Netzwerk – sei es in einer Firma, einer Organisation oder zu Hause.

Der Name Samba ist von der Abkürzung SMB abgeleitet, die wiederum für das Protokoll *Server Message Block* steht. Die ersten SMB-Konzepte stammen von IBM, später wurde das Protokoll von mehreren Firmen erweitert, vor allem von Microsoft.

Samba wird oft als Verknüpfungselement zwischen der Linux- und der Windows-Welt betrachtet. Das greift aber zu kurz: SMB kommt selbst in reinen Linux- bzw. Unix-Umgebungen häufig zum Einsatz, weil es derart einfach zu nutzen ist: Die Dateimanager von Gnome und KDE unterstützen SMB standardmäßig, SMB-Verzeichnisse können dank CIFS direkt in den Linux-Verzeichnisbaum eingebunden werden etc. Wenn Sie nach einer Unix-typischen Alternative ohne Microsoft-Hintergrund suchen, bietet sich am ehesten NFS an (siehe Kapitel 32, »NFS und AFP«). Der Einsatz von NFS erfordert aber einheitliche Login-Namen auf allen Client-Rechnern oder den Einsatz von LDAP und ist zudem inkompatibel zur Windows-Welt.

Links

Dieses Kapitel beschreibt die Grundfunktionen von Samba 4 aus Server-Sicht. Wenn Sie die zahlreichen fortgeschrittenen Funktionen nutzen möchten, beispielsweise die Authentifizierung via LDAP oder die Verwendung von Samba als PDC, müssen Sie auf weiterführende Literatur zurückgreifen. Eine Menge Informationen finden Sie auf diesen Websites:

http://www.samba.org
https://help.ubuntu.com/community/Samba

31.1 Grundlagen und Glossar

Bevor Sie mit der Konfiguration eines Samba-Servers beginnen, sollten Sie die zugrunde liegenden Konzepte und das dazugehörende Vokabular verstehen. Dieser Abschnitt soll Ihnen dabei helfen.

NetBIOS

SMB basiert auf dem NetBIOS-Protokoll. NetBIOS steht für das ursprünglich von IBM entwickelte *Network Basic Input/Output System*. Mittlerweile bezieht sich NetBIOS allerdings auf ein mehrfach renoviertes Protokoll. NetBIOS besteht primär aus drei Diensten:

- **Name Service:** Dieses Verfahren zum Austausch der Rechnernamen ist mit DNS unter Unix/Linux vergleichbar. Die Verwaltung der Namen kann wahlweise zentral durch einen *NetBIOS-Nameserver* (NBNS) oder dezentral erfolgen. In diesem Fall sendet jeder Client beim Rechnerstart eine Meldung an alle anderen Clients im Netzwerk und teilt ihnen mit, unter welchem Namen er präsent ist.
- **Session Service:** Dieser Kommunikationsmechanismus ermöglicht ähnlich wie TCP einen geordneten Datenaustausch zwischen zwei Rechnern in Form von Paketen. Dabei wird die Integrität überprüft, und fehlerhafte oder verlorene Pakete werden neu angefordert.
- **Datagram Service:** Bei dieser Variante zum Session Service gibt es keine Überprüfung, ob die Daten ordnungsgemäß ankommen. Dafür hat der Datagram Service den Vorteil, dass Daten an mehrere Rechner gleichzeitig versandt werden können.

WINS

Unter Windows wird der NBNS durch den *Windows Internet Name Service* (WINS) realisiert. WINS-Server können mit Samba oder mit aktuellen Windows-Versionen eingerichtet werden.

Unter IPv4 sind die Rechnernamen für NetBIOS und für TCP/IP voneinander unabhängig. Theoretisch ist es also möglich, dass ein Rechner je nach Protokoll unter verschiedenen Namen konfiguriert ist. In der Praxis wird man das natürlich vermeiden. Unterschiedliche Namen stiften nicht nur Verwirrung, sondern machen auch die Nutzung mancher Funktionen unmöglich.

Der Netbios Name Service ist nur in IPv4-Netzen relevant. Wenn Samba in Kombination mit IPv6 zum Einsatz kommt, ist ein gewöhnlicher Linux-Nameserver zur Verwaltung der Rechnernamen erforderlich – beispielsweise das im vorigen Kapitel beschriebene Programm `dnsmasq`.

Browsing

Woher weiß ein Windows-Client, welche anderen Rechner sich im Netz befinden? Die Antwort lautet: durch Browsing. Mit diesem Begriff wird die Verwaltung der im Netz befindlichen Rechner bezeichnet. Damit sich nicht jeder Rechner selbst darum

kümmern muss, übernimmt ein sogenannter Master-Browser diese Verwaltungsaufgabe. In größeren Netzen wird er von einem oder mehreren Backup-Browser(n) unterstützt. Samba ist bei Bedarf ebenfalls in der Lage, als Browser aufzutreten.

Wer die Rolle als Browser übernimmt, ist nicht fest vorgeschrieben, sondern wird unter den im Netz befindlichen Rechnern dynamisch ausgehandelt – je nachdem, welche Rechner sich gerade im Netz befinden und welcher dieser Rechner am besten dazu geeignet ist. Oft kommt einfach der Rechner mit der neuesten Betriebssystemversion zum Zuge. Dabei muss es sich keineswegs automatisch um den WINS-Server handeln, sofern es im Netz überhaupt einen gibt. Der Browsing-Ansatz wird also sehr dezentral gehandhabt.

Leider gelingt es vor allem Windows-PCs nicht immer, die Browsing-Liste mit dem tatsächlichen Zustand des Netzwerks synchron zu halten. Das liegt auch daran, dass die Clients einen Cache mit dem zuletzt gültigen Zustand verwalten, um die Netzbelastung zu minimieren. Die Aktualisierung dieses Caches dauert oft geraume Zeit. Die schnellste Lösung ist übrigens – ganz Windows-typisch! – ein Neustart des betroffenen Rechners.

SMB-Versionen

Es gibt verschiedene Versionen des Protokolls Server Message Block (SMB): Beginnend mit Windows 7 bzw. Windows Server 2008 R2 kommt Version 2.1 zum Einsatz, und ab Windows 8 bzw. Windows Server 2012 Version 3. Alle Windows-Versionen sind natürlich abwärtskompatibel zu SMB 1. Samba 4 unterstützt SMB 2 vollständig und SMB 3 teilweise. Beachten Sie aber, dass auf manchen Distributionen standardmäßig Samba 3.6 oder sogar ältere Versionen zum Einsatz kommen, was für die Konfigurationsbeispiele in diesem Kapitel aber vollkommen ausreicht.

Zugriffsrechte und Sicherheitssysteme

Der Begriff *Shares* bezeichnet gleichermaßen Verzeichnisse oder Drucker, die anderen Rechnern zur Verfügung gestellt werden. Die deutsche Übersetzung lautet wenig elegant *Freigaben*. Es gibt verschiedene Formen der Zugriffssteuerung, die regeln, wer auf welche Freigaben zugreifen darf:

- **Share-Level-Sicherheit:** Bei der einfachsten Form der Zugriffssteuerung bekommt jedes Verzeichnis und jeder Drucker ein eigenes Passwort. Dieses Verfahren kommt aber kaum noch zum Einsatz. Der naheliegende Nachteil ist die große Anzahl erforderlicher Passwörter: Wenn auf zehn Rechnern jeweils drei Objekte freigegeben werden, ergeben sich daraus bereits 30 Passwörter. In größeren Netzen führt das naturgemäß zu chaotischen Zuständen.

- **Workgroup-Sicherheit:** Diese Erweiterung der Share-Level-Sicherheit erlaubt einen gegenseitigen Zugriff auf Objekte nur dann, wenn die Rechner derselben Arbeitsgruppe angehören. Das verbessert die Sicherheit noch nicht nennenswert: Jeder Rechner kann sich ohne zentrale Administration einer beliebigen Arbeitsgruppe zugehörig erklären. Share-Level-Sicherheit funktioniert also nach einem dezentralen Peer-to-Peer-Verfahren, im Gegensatz zu den zunehmend zentralistischeren Client/Server-Verfahren für User-Level und Domain-Level.
- **User-Level-Sicherheit:** Die User-Level-Sicherheit setzt auf der Client-Seite voraus, dass sich der Anwender mit Name und Passwort anmeldet. Wenn der Anwender nun irgendwelche Daten eines Samba-Servers bzw. eines anderen Windows-PCs nutzen möchte, gelten sein aktueller Name und sein Passwort als Zugangsberechtigung. Außerdem müssen beide Rechner zur selben Arbeitsgruppe gehören.

  Jedem Netzwerkobjekt ist also nicht einfach ein Passwort zugeordnet. Stattdessen ist es mit einem Benutzer verbunden oder mit einer Liste namentlich aufgezählter Benutzer oder mit allen Benutzern einer Gruppe. Wenn User-Level-Sicherheit mit Samba implementiert wird, ist eine eigene Datenbank mit Benutzernamen, Gruppenzugehörigkeiten und Passwörtern erforderlich.

  Dazu ein Beispiel: Anwender X arbeitet auf Rechner A. Damit X Daten vom Samba-Server S abrufen kann, muss X sowohl auf A als auch auf S als Benutzer registriert sein, und zwar jeweils mit dem gleichen Namen und Passwort. Nun geht Rechner A kaputt. X weicht auf Rechner B aus. Damit er auf seine Daten auf S zugreifen kann, muss auch auf B der Benutzer X (wieder mit Passwort) geschaffen werden.

  Wenn X sich entschließt, sein Passwort zu ändern, muss diese Änderung auf dem Server S und in der Folge auf jedem Client (A, B ...) durchgeführt werden. Die dezentrale Passwortverwaltung und Authentifizierung ist also ein immanentes Problem bei diesem Konzept.
- **Domain-Level-Sicherheit:** Mit Windows NT 4 hat Microsoft sogenannte *Domänen* in seine Netzwerkwelt eingeführt. Das Konzept der Zugriffsverwaltung ist ganz ähnlich wie bei der User-Level-Sicherheit. Die Unterschiede betreffen die Art und Weise, wie die Benutzerdatenbank verwaltet wird und wie die Authentifizierung erfolgt.

  Die Clients greifen beim Login auf die zentral vom Server verwaltete Benutzerdatenbank zurück. Die Zugriffsrechte werden durch eine Art Login-Token verwaltet. Der Client erhält beim Login eine Zugriffsinformation, die bis zum Logout im gesamten Netzwerk gilt. Dieser Unterschied ist für den Anwender zwar nicht sichtbar, stellt aber einen fundamentalen Unterschied bei der internen Verwaltung dar und ist für den Server deutlich effizienter zu handhaben.

Domain-Level-Sicherheit setzt voraus, dass es im Netzwerk einen *Primary Domain Controller* (PDC) gibt. In größeren Netzen können dem PDC einige *Backup Domain Controller* (BDC) zur Seite gestellt werden, damit nicht alles stillsteht, nur weil der PDC gerade ausgefallen ist.

- **Active Directories:** Um die Verwaltung großer Netzwerke zu vereinfachen, hat Microsoft die Domain-Level-Sicherheit um sogenannte Active Directories erweitert. Zur Authentifizierung wird das *Lightweight Directory Access Protocol* (LDAP) eingesetzt. Dabei können das Netzwerk und seine Domänen hierarchisch organisiert werden. Außerdem erfolgt die Verwaltung der Rechnernamen nun wie unter Linux üblich durch DNS, nicht durch WINS.

Samba versteht client-seitig schon lange alle fünf aufgezählten Sicherheitssysteme. Die Rolle eines Active-Directory-Domain-Servers kann Samba aber erst seit Version 4 übernehmen. Dieses Buch behandelt allerdings nur das User-Level-Sicherheitssystem. Man spricht in diesem Zusammenhang auch von einer Samba-Konfiguration als Stand-alone-Server. Wenn Sie Samba als PDC oder als Active-Directory-Server einsetzen möchten, benötigen Sie in jedem Fall weiterführende Literatur.

Zentrale oder dezentrale Server-Topologie?

Losgelöst vom Sicherheitssystem gibt es zwei fundamental unterschiedliche Strategien, wie Rechner in einem lokalen Netzwerk via Samba Daten austauschen:

- **Zentrale Topologie:** Ein zentraler Samba-Server stellt allen Benutzern Netzwerkverzeichnisse zur Verfügung. Es ist die Aufgabe des Administrators, die Zugriffsrechte der einzelnen Verzeichnisse so einzustellen, dass es sowohl private Verzeichnisse für individuelle Benutzer als auch mehr oder weniger öffentliche Verzeichnisse zum Datenaustausch in Benutzergruppen gibt. Anstelle eines selbst konfigurierten Windows- oder Linux-Rechner kann es sich bei dem Samba-Server auch ganz einfach um ein NAS-Gerät handeln.

  Die Vorteile dieser Konfiguration bestehen darin, dass alle Daten auf dem Server zentral gesichert werden können und dass sich die einzelnen Benutzer nicht selbst um das Einrichten von Netzwerkverzeichnissen kümmern müssen. Natürlich gibt es auch Nachteile: Das System ist relativ unflexibel, und jede Änderung muss von einem Administrator durchgeführt werden. Außerdem sind die Folgen eines Server-Ausfalls fatal für das ganze Netzwerk.
- **Dezentrale Topologie:** In diesem Fall stellt jeder Rechner, der im Netzwerk Daten für andere Benutzer zur Verfügung stellen will, diese selbst zur Verfügung. Sowohl Windows als auch Linux (genau genommen: Gnome bzw.

KDE) unterstützen den Anwender dabei durch relativ einfach zu nutzende Freigabedialoge.

Der Vorteil dieser Konfigurationsvariante ist der dezentrale Ansatz, bei dem jeder für sich selbst verantwortlich ist und kein Administrator erforderlich ist. Mit zunehmender Netzwerkgröße wird die Konfiguration naturgemäß unübersichtlich und zentrale Backups sind nahezu unmöglich.

Persönlich erscheint mir die zentrale Topologie im Unternehmenseinsatz zweckmäßiger. Wenn es aber nur darum geht, im privaten Umfeld rasch ein paar Dateien von einem Rechner zum nächsten zu kopieren, ist eine Ad-hoc-Konfiguration durch den entsprechenden KDE- oder Gnome-Dialog natürlich ausreichend. Das Hauptproblem besteht darin, dass die von KDE bzw. Gnome gebotenen Konfigurationsdialoge unausgereift sind und schlecht funktionieren.

31.2 Basiskonfiguration und Inbetriebnahme

Installation

Bei vielen Distributionen gibt es getrennte Pakete für die Client- und Server-Anwendung. Die Client-Pakete sind zumeist standardmäßig installiert, sodass ein Zugriff auf Netzwerkverzeichnisse auf Anhieb funktionieren sollte. Wenn Sie selbst Netzwerkverzeichnisse freigeben möchten, brauchen Sie auch die Server-Funktionen, die bei den meisten Distributionen im Paket `samba` verpackt sind.

Start

Samba stellt seine Dienste durch zwei Hintergrundprozesse zur Verfügung:

- `nmbd` dient zur internen Verwaltung und als Nameserver. Der Dämon kümmert sich auch um die Browsing-Funktionen. `nmbd` kann auch als Master-Browser oder als WINS-Server fungieren.
- `smbd` stellt die Schnittstelle für die Clients dar und gibt diesen Zugang zu Verzeichnissen, Druckern und zur aktuellen Browsing-Liste.

Die beiden Prozesse werden durch das Init-System gestartet. Die Namen der Init-Scripts bzw. -Konfigurationsdateien hängen von Ihrer Distribution ab. Tabelle 31.1 fasst für verschiedene Distributionen zusammen, welches Init-System und welche Dienstnamen verwendet werden. Bei Debian ist ein Init-Script für beide Prozesse verantwortlich. Falls Samba bei Ihrer Distribution nach der Installation nicht standardmäßig läuft, finden Sie in Abschnitt 16.5 Tipps, wie Sie die Scripts starten bzw. für einen automatischen Start konfigurieren.

smb.conf

Als zentrale Konfigurationsdatei für Samba dient `/etc/samba/smb.conf`. Die Datei setzt sich aus einem `[global]`-Abschnitt für die Grundeinstellungen sowie beliebig vielen weiteren Abschnitten für die Freigabe von Verzeichnissen, Druckern etc. zusammen. Jeder Abschnitt wird durch `[ressourcenname]` eingeleitet. Kom-

Distribution	Init-System	Dienstname
Debian	Init-V	samba **bzw.** samba4
Fedora	Systemd	smb, nmb
openSUSE	Init-V	smb, nmb
RHEL 6	Init-V	smb, nmb
Ubuntu	Upstart	smbd, nmbd

Tabelle 31.1 Samba-Dienste je nach Distribution und Init-System

mentare beginnen wahlweise mit den Zeichen ; oder #. Es ist aber nicht zulässig, im Anschluss an eine Parametereinstellung einen Kommentar hinzuzufügen. Kommentare beanspruchen also immer eine ganze Zeile.

Die folgenden Zeilen zeigen leicht gekürzt den globalen Abschnitt der Samba-Standardkonfiguration unter Ubuntu. Bei anderen Distributionen ist die Datei mitunter noch kürzer, weil darauf verzichtet wird, Defaulteinstellungen explizit zu wiederholen. Nicht abgedruckt sind hier die Abschnitte [printers] und [print$], die den Zugriff auf Drucker und Druckertreiber erlauben (siehe Abschnitt 33.4).

```
# Datei /etc/samba/smb.conf bei Ubuntu
[global]
   workgroup              = WORKGROUP
   server string          = %h server (Samba, Ubuntu)
   dns proxy              = no
   log file               = /var/log/samba/log.%m
   max log size           = 1000
   syslog                 = 0
   panic action           = /usr/share/samba/panic-action %d
   encrypt passwords      = true
   passdb backend         = tdbsam
   obey pam restrictions  = yes
   unix password sync     = yes
   passwd program         = /usr/bin/passwd %u
   passwd chat            = ...
   pam password change    = yes
   map to guest           = bad user
   usershare allow guests = yes
```

Kommentare aus smb.conf entfernen

Bei einigen Distributionen wird smb.conf gleichzeitig auch zur Dokumentation verwendet. Die resultierende Konfgurationsdatei ist dann endlos lang und unübersichtlich. Abhilfe schaffen die drei folgenden Kommandos:

```
root#  cd /etc/samba
root#  cp smb.conf smb.conf.org
root#  grep -Ev '^#|^;|^$' smb.conf.orig > smb.conf
```

Server-Identifizierung

Mit `workgroup` stellen Sie den Namen der Arbeitsgruppe ein. Das ist wahrscheinlich die erste Einstellung, die Sie ändern werden – um dort den Namen Ihrer eigenen Arbeitsgruppe einzustellen, innerhalb der Samba agieren soll.

`server string` gibt an, unter welchem Namen sich der Server identifiziert. `%h` wird dabei durch den Hostnamen ersetzt.

WINS

`dns proxy = no` bewirkt, dass Samba, wenn es als WINS-Server agiert, nicht auf DNS zurückgreift, um Windows-Hostnamen aufzulösen. Sofern es in Ihrem LAN einen lokalen Nameserver gibt, sollten Sie diesen Parameter auf `yes` einstellen. Die Standardeinstellung `no` ist nur zweckmäßig, wenn es keine lokalen bzw. schnell erreichbaren Nameserver gibt.

Logging

Die Parameter `log file`, `max log size` und `syslog` steuern, welche Daten Samba wo protokolliert. Details zum Logging folgen in Abschnitt 31.2.

Bei einem Absturz von Samba wird das Script `panic-action` ausgeführt. Es sendet eine E-Mail an `root`, die Informationen zum aufgetretenen Fehler enthält. `panic-action` bleibt wirkungslos, wenn auf dem Server kein E-Mail-System installiert ist.

Passwörter

`passdb backend` gibt an, wie die Samba-Passwörter verwaltet werden sollen. Zur Auswahl stehen `smbpasswd` (eine einfache Textdatei), `tdbsam` (TDB, ein relativ einfaches Datenbanksystem) oder `ldapsam` (LDAP). `tdbsam` ist zumeist die richtige Einstellung für kleine bis mittelgroße Netzwerke (bis ca. 250 Clients). Das früher populäre System `smbpasswd` sollte nicht mehr verwendet werden, weil damit keine erweiterten Attribute gespeichert werden können (*SAM Extended Controls*). Weitere Informationen zur Verwaltung der Samba-Passwörter folgen in Abschnitt 31.3.

Die Schlüsselwörter `unix password sync`, `passwd chat` und `pam password change` beschreiben, ob und wie Samba seine Passwörter mit den Linux-Passwörtern abgleichen soll. Details dieses Verfahrens sind in Abschnitt 31.3 beschrieben.

Gäste

`map to guest` und `usershare allow guests` regeln, wie Samba mit nicht authentifizierten Benutzern umgeht, also mit Benutzern, die sich mit einem ungültigen Namen oder Passwort anmelden. Die Bedeutung dieser und einiger weiterer `guest`-Parameter ist in Abschnitt 31.4 beschrieben.

Sicherheitsmodell

Vielleicht vermissen Sie im obigen Listing die Einstellung des Sicherheitsmodells: Standardmäßig gilt in Samba und somit auch bei der Ubuntu-Grundkonfiguration das User-Level-Sicherheitsmodell (`security = user`). Nur wenn ein anderes Sicherheitsmodell gewünscht ist, muss dieses mit dem Parameter `security` eingestellt werden.

Samba-Standards

Unter Debian und Ubuntu enthält `smb.conf` einige Anweisungen, die eigentlich überflüssig sind: Beispielsweise werden Passwörter schon seit vielen Jahren verschlüsselt. `encrypt passwords = true` dokumentiert daher nur eine Standardeinstellung. Irreführend ist `obey pam restrictions = yes`: Diese Einstellung hat nur dann Einfluss auf die Passwortverwaltung, wenn Passwörter nicht verschlüsselt werden. Da dies der Fall ist, wird die Einstellung ignoriert.

Im weiteren Verlauf dieses Kapitels werden Sie noch eine Menge weiterer Samba-Parameter kennenlernen, aber natürlich bei Weitem nicht alle. Detaillierte Informationen zu allen Einstellmöglichkeiten gibt `man smb.conf`.

SMB 2 und SMB 3

Die Samba-Versionen 3.5 und 3.6 unterstützen die Protokollversion SMB 2. Die entsprechenden Erweiterungen sind aber standardmäßig inaktiv und müssen explizit aktiviert werden. Dazu fügen Sie der Datei `smb.conf` im globalen Abschnitt die folgende Anweisung hinzu:

```
# in /etc/samba/smb.conf
[global]
  ...
  max protocol = SMB2
```

Beginnend mit Samba 4 können Sie auf diese Einstellung wieder verzichten. Nun gilt `SMB3` als Defaulteinstellung. Samba bleibt aber natürlich mit älteren Clients kompatibel. Es kommt automatisch das beste verfügbare Protokoll zum Einsatz.

Konfigurationsänderungen und Status

Damit Änderungen an `smb.conf` wirksam werden, müssen Sie Samba auffordern, die Konfigurationsdateien neu einzulesen:

```
root#  service samba[4] reload      (Debian)
root#  service smb[d] reload        (Fedora, openSUSE, Ubuntu)
```

testparam

Wenn Sie größere Änderungen an `smb.conf` durchführen möchten, sollten Sie die Datei zuerst mit `testparm` auf syntaktische Fehler überprüfen:

```
root#  testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions  <Return>
[global]
   server string = %h server (Samba, Ubuntu)
   ...
```

Wenn Sie `testparm` mit der Option `-v` ausführen, liefert das Kommando eine schier endlose Liste mit den Einstellungen aller möglichen `smb.conf`-Optionen. Das ist manchmal praktisch, wenn Sie sich nicht sicher sind, welche Einstellungen standardmäßig gelten – also bei Optionen, die Sie nicht selbst explizit eingestellt haben.

Den aktuellen Zustand des Samba-Servers ermitteln Sie mit `smbstatus`. Das Kommando liefert auch eine Liste aller zurzeit aktiven Verbindungen.

Samba absichern

Firewall

Unter Fedora, SUSE und RHEL blockiert die standardmäßig aktive Firewall Samba. Damit die Netzwerkdienste genutzt werden können, müssen Sie die Samba- bzw. Windows-spezifischen TCP-Ports 135, 139 und 445 sowie die UDP-Ports 137, 138 und 445 für die Schnittstelle zum lokalen Netzwerk freigeben!

Eine generelle Deaktivierung der Firewall ist nicht empfehlenswert! Jeder Samba-Server sollte unbedingt zum Internet hin durch eine Firewall abgesichert sein! Ist dies nicht der Fall, sind die freigegebenen Verzeichnisse für alle Welt zugänglich bzw. nur noch durch die Passwörter der Samba-Benutzerverwaltung abgesichert.

Schnittstellen

Unabhängig von der Firewall schadet es nicht, auch innerhalb der Samba-Konfiguration Vorsicht walten zu lassen: Dazu geben Sie mit `interfaces` explizit an, über welche Netzwerkschnittstellen Samba kommunizieren soll. Die Angabe der Schnittstellen erfolgt nicht über die Namen der Schnittstellen, sondern über den von diesen Schnittstellen genutzten Adressbereich. Sie können auch mehrere Bereiche angeben, wobei Sie diese einfach durch Leerzeichen trennen. Vergessen Sie `localhost` nicht – sonst funktionieren auf dem Server Administrationswerkzeuge wie `smbclient` nicht!

Die `interfaces`-Option ist nur relevant, wenn es auf Ihrem Rechner mehrere Netzwerkschnittstellen gibt. Auf vielen Rechnern gibt es nicht nur Schnittstellen zu physikalischen Netzwerkadaptern, sondern auch zu den virtuellen Netzwerkadaptern diverser Virtualisierungsprogramme! Standardmäßig bedient Samba *alle* Netzwerkschnittstellen.

Die Einstellungen durch `interfaces` werden nur wirksam, wenn Sie außerdem wie im folgenden Listing die Option `bind interfaces only` aktivieren.

Hosts

Des Weiteren können Sie mit `hosts allow` explizit aufzählen, welche Rechner mit Samba kommunizieren dürfen. Die Hostnamen, IP-Adressen oder IP-Adressbereiche müssen durch Leerzeichen voneinander getrennt werden. `hosts allow` erlaubt eine noch genauere Selektion als `interfaces`. Ergänzend können Sie mit `hosts deny` einzelnen Hosts oder Adressen die Nutzung von Samba verbieten.

IPv4 und IPv6

Grundsätzlich kommuniziert Samba sowohl über IPv4 als auch über IPv6. Bei einer Dual-Stack-Konfiguration im LAN ist es mitunter aus Sicherheitsgründen wünschenswert, dass Samba nur IPv4 spricht. Dazu geben Sie einfach bei `interfaces` und `host` ausschließlich IPv4-Adressen an. Sie sollten in solchen Fällen Hostnamen vermeiden und lieber die IP-Adressen angeben, weil bei der Auflösung der Hostnamen nicht immer vorhersehbar ist, ob das Ergebnis IPv4- oder IPv6-Adressen sind.

Diese Art der Konfiguration funktioniert auch umgekehrt: Wenn Sie mit `interfaces` ausschließlich IPv6-Adressen angeben, dann ist IPv4 gesperrt.

Gäste

Die Einstellung `map to guest` verbietet schließlich allen Benutzern, die sich nicht richtig beim Server authentifizieren können, jeglichen Zugriff. Je nach Anwendung kann es zwar durchaus sinnvoll sein, auch für Gäste Verzeichnisse einzurichten, die ohne Authentifizierung gelesen oder sogar verändert werden dürfen; wenn dies aber nicht erforderlich ist, sollten Sie Gäste von vornherein aussperren.

```
# /etc/samba/smb.cnf
[global]
   ...
   bind interfaces only = yes
   interfaces           = 192.168.0.0/24 127.0.0.1
   hosts allow          = clientA clientB clientC
   map to guest         = never
```

SELinux

Unter Fedora und RHEL überwacht SELinux standardmäßig alle Samba-Aktivitäten. Damit die Freigabe von Heimatverzeichnissen unkompliziert funktioniert, müssen Sie den SELinux-Parameter `samba_enable_home_dirs` aktivieren.

```
root#  setsebool -P samba_enable_home_dirs on
```

Wenn Sie ein anderes Verzeichnis freigeben möchten, müssen Sie hierfür das Attribut `samba_share_t` setzen. Dazu führen Sie die beiden folgenden Kommandos aus, im folgenden Beispiel für das Verzeichnis `/data/samba`:

```
root#  semanage fcontext -a -t samba_share_t '/data/samba(/.*)?'
root#  restorecon -R /data/samba
```

SELinux-Konfiguration

Es gibt noch diverse weitere SELinux-Parameter, die steuern, was Samba alles (nicht) darf. Einen Überblick über all diese Parameter samt der Möglichkeit, deren Einstellung mit einem Mausklick zu verändern, gibt das Programm `system-config-selinux` aus dem Paket `policycoreutils-gui`. Suchen Sie nach dem Start im Dialogblatt Boolean nach *samba*! Weitere Tipps zu SELinux finden Sie in Kapitel 42.

Logging

Die beiden Samba-Dienste `smbd` und `nmbd` protokollieren globale Ereignisse in die Dateien `/var/log/samba/log.smbd` und `log.nmbd`. Weder der Name noch der Ort dieser beiden Logging-Dateien können durch `smb.conf` verändert werden.

Der Parameter `log file` im globalen Abschnitt von `smb.conf` gibt an, wohin client-spezifische Nachrichten protokolliert werden sollen. Die Voreinstellung `/var/log/samba/log.%m` bewirkt, dass für jeden Client, der auf Samba zugreift, eine eigene Logging-Datei mit dem Namen `log.`*`hostname`* erzeugt wird.

`max log size = 1000` limitiert die maximale Größe auf 1000 kByte. Wenn eine Logging-Datei größer wird, benennt Samba sie in *`name`*`.old` um. `syslog = 0` bedeutet nicht etwa, dass Syslog nicht verwendet wird, sondern dass in `/var/log/syslog` nur Fehlermeldungen protokolliert werden sollen. Alternative Einstellungen sind 1, 2, 3 etc., wenn Sie auch Warnungen, Notizen sowie Debugging-Nachrichten protokollieren möchten.

logrotate

Vorsicht ist beim Einsatz von `logrotate` geboten (siehe Abschnitt 21.7): Dieses Programm archiviert in der bei Debian, SUSE und Ubuntu üblichen Standardeinstellung einmal pro Woche `log.smbd` und `log.nmbd` und löscht gleichzeitig alle Archiv-Versionen, die älter als zwei Monate sind. `logrotate` ignoriert aber die viel schneller wachsenden client-spezifischen Logging-Dateien `log.`*`hostname`*.

Besser durchdacht ist hier die entsprechende Konfigurationsdatei bei Fedora und Red Hat, die sich um *alle* Logging-Dateien in `/var/log/samba` kümmert:

```
# /etc/logrotate.d/samba bei Fedora und Red Hat
/var/log/samba/*
{
    notifempty
    olddir /var/log/samba/old
    missingok
    sharedscripts
    copytruncate
}
```

Eine andere Lösung besteht darin, dass Sie in `smb.conf` die Einstellung `log file = /var/log/samba/log.smbd` verwenden. Damit erreichen Sie, dass `smbd` ebenso globale wie client-spezifische Nachrichten in derselben Datei protokolliert. Solange Sie nicht Fehler in der Samba-Konfiguration suchen müssen, ist das am praktischsten.

31.3 Passwortverwaltung

Standardmäßig gilt für Samba `security = user`, also User-Level-Sicherheit. Damit der Beispielnutzer `peter` ein Netzwerkverzeichnis nutzen kann, müssen die folgenden Voraussetzungen erfüllt sein:

- Auf dem Server muss es einen Linux-Account mit dem Namen `peter` geben. Dieser Account ist für die Verwaltung der Zugriffsrechte erforderlich. Samba greift also auf die Linux-Zugriffsrechte zu, um zu entscheiden, welcher Nutzer welche Datei lesen bzw. verändern darf.

  Der Linux-Account muss nicht aktiv sein. Oft ist es aus Sicherheitsgründen zweckmäßig, den Account mit einem ungültigen Passwort auszustatten. Sie verhindern damit, dass sich Samba-Benutzer auf dem Server einloggen können.

- `peter` und sein Passwort müssen in der Samba-Benutzerdatenbank enthalten sein. Aus technischen Gründen werden die Samba-Accounts (Benutzername, Passwort sowie weitere Daten) unabhängig von den Linux-Accounts verwaltet. Das Passwort des Linux-Accounts spielt für Samba keine Rolle.
- `smb.conf` muss Einträge für Netzwerkverzeichnisse enthalten, die `peter` benutzen darf (siehe Abschnitt 31.4).

Samba-Passwörter

Bevor ein Benutzer im lokalen Netzwerk auf ein Verzeichnis zugreifen kann, muss er sich beim Samba-Server identifizieren. Beim Verbindungsaufbau von einem Windows-Client werden dazu der Windows-Login-Name und eine verschlüsselte Zeichenkette für das Passwort übertragen. Bei Linux-Clients können diese Daten nicht aus dem Linux-Login übernommen werden, weswegen zumeist ein eigener Dialog zur Eingabe des Samba-Benutzernamens und -Passworts erscheint. Anschließend geht es wie bei Windows-Clients weiter: Auch in diesem Fall wird nicht das Passwort selbst, sondern ein verschlüsselter Code an den Samba-Server übertragen.

Aus Sicherheitsgründen kann das Passwort nicht aus der verschlüsselten Passwortzeichenkette rekonstruiert werden. Die Zeichenkette wird vielmehr vom Samba-Server mit einer gleichermaßen verschlüsselten Zeichenkette verglichen. Wenn beide Zeichenketten übereinstimmen, stimmen auch die Passwörter überein.

smbpasswd-Backend

Der Samba-Server braucht eine Benutzer- und Passwort-Datenbank, um die Authentifizierung durchzuführen. In der Vergangenheit kam hierfür oft eine simple Textdatei zum Einsatz (`passdb backend = smbpasswd`). SUSE verwendet dieses Backend noch immer und speichert Passwörter in `/etc/samba/smbpasswd`.

TDB-Backend

Bei den meisten anderen Distributionen hat sich für kleine Installationen das TDB-Backend durchgesetzt (`passdb backend = tdbsam`). Bei größeren Installationen ist es zweckmäßig, die Login-Daten via LDAP zu verwalten, worauf ich in diesem Buch aber nicht eingehe.

TDB steht für *Trivial Database* und ist ein binäres Format zur Speicherung von Datensätzen. Der wesentliche Vorteil im Vergleich zu den herkömmlichen `smbpasswd`-Dateien besteht darin, dass neben dem Login-Namen und dem Passwort weitere Daten und Attribute gespeichert werden. Dazu zählen insbesondere die sogenannten *SAM Extended Controls*, die die Kompatibilität mit aktuellen Windows-Versionen erhöhen. Wo die Passwörter physikalisch gespeichert werden, ist distributionsabhängig:

Debian, Ubuntu:	`/var/lib/samba/passdb.tdb`
Fedora, RHEL:	`/var/lib/samba/private/passdb.tdb`
SUSE:	`/etc/samba/passdb.tdb`

Bei Bedarf können Sie in `smb.conf` durch `passdb backend = tdbsam:dateiname` eine andere Datei angeben. Mit dem Kommando `smbpasswd` legen Sie einen neuen Samba-Account an bzw. verändern dessen Passwort. `pdbedit` gibt Zugriff auf alle Account-Informationen: `root`-Benutzer können damit eine Liste aller Samba-Benutzer erstellen (`pdbedit -L -v`), für jeden Account diverse Attribute einstellen etc. Beide Kommandos werten `smb.conf` aus und funktionieren für alle Passwort-Systeme, also `smbpasswd`, `tdbsam` und `ldapsam`.

smbpasswd

Damit `peter` also ein Samba-Verzeichnis nutzen kann, müssen Sie als Linux-Systemadministrator den Samba-Account `peter` anlegen. Dabei hilft Ihnen das Kommando `smbpasswd`. Als Passwort geben Sie dieselbe Zeichenkette an, die der Benutzer `peter` auch unter Windows hat. Um ein bereits vorhandenes Samba-Passwort zu verändern, verwenden Sie `smbpasswd` ohne die Option `-a`.

```
root#  smbpasswd -a peter
New SMB password:  ******
Retype new SMB password:  ******
Added user peter.
Password changed for user peter.
```

Beachten Sie, dass `sbmpasswd` nur funktioniert, wenn der Linux-Benutzer `peter` auch auf dem lokalen System existiert (Datei `/etc/passwd`)! Gegebenenfalls können neue Linux-Benutzer mit `useradd` oder `adduser` angelegt werden.

Synchronisation der Samba- und Linux-Passwörter

Bei manchen Installationen ist es wünschenswert, dass sich die Benutzer von Samba-Verzeichnissen direkt am Linux-Server anmelden können, beispielsweise um via SSH zu arbeiten und ihre Dateien mit Linux-Kommandos zu verarbeiten. In solchen Fällen wäre es natürlich zweckmäßig, wenn das Samba- und das Linux-Passwort immer übereinstimmen würden. Schließlich ist es ausgesprochen lästig, jede Passwort-Änderung mehrfach durchzuführen (im Extremfall gleich dreimal: auf dem Windows-Client, für den Samba-Server und für den Linux-Login).

Die Synchronisierung der Passwörter ist leider nicht ganz einfach zu bewerkstelligen, weil zur Verschlüsselung der Samba-Passwörter ein anderer Algorithmus als für Linux-Passwörter zum Einsatz kommt. Aus diesem Grund erfolgt die Verwaltung der Samba- und Linux-Passwörter getrennt. (Die Algorithmen sind zwar unterschiedlich, es gibt aber eine Gemeinsamkeit: Die gespeicherten Zeichenketten ermöglichen nur die Kontrolle der Passwörter, aber keine Rekonstruktion. Deswegen ist eine Umwandlung oder Konvertierung der gespeicherten Passwörter von einem System in ein anderes unmöglich.)

Die populärste Lösung dieses Problems besteht darin, bei jedem Client-Aufruf von `smbpasswd` zur Veränderung des eigenen Passworts parallel auch das Linux-Passwort zu verändern. Unter Ubuntu enthält `smb.conf` dafür bereits alle erforderlichen Einstellungen:

```
# /etc/samba/smb.conf
[global]
    ...
    unix password sync = yes
    pam password change = yes
    passwd chat = *Enter\snew\s*\spassword:* %n\n
                  *Retype\snew\s*\spassword:* %n\n
                  *password\supdated\ssuccessfully* .
```

`unix password sync = yes` aktiviert die Synchronisierung. Dabei wird wegen `pam password change` PAM eingesetzt. PAM steht für *Pluggable Authentication Modules* und bezeichnet eine Sammlung von Bibliotheken zur Administration von Passwörtern. Der früher erforderliche Parameter `passwd program`, der den Pfad des `passwd`-Programms angab, ist für PAM nicht relevant und wird ignoriert. `passwd chat` beschreibt die Kommunikation zwischen Samba und PAM. Die Zeichenkette wurde im obigen Listing über drei Zeilen verteilt, muss in `smb.conf` aber in einer Zeile angegeben werden.

Leider ist die Synchronisation mit vielen Einschränkungen verbunden:

- `smbpasswd` muss vom jeweiligen Benutzer ausgeführt werden, nicht von `root`! Der Grund: Wenn `smbpasswd` von `root` aufgerufen wird, manipuliert es direkt die Samba-Benutzerdatenbank. Das funktioniert auch, wenn der Samba-Server gar nicht läuft. Wenn das Kommando dagegen von einem gewöhnlichen Benutzer verwendet wird, kommuniziert es mit dem Samba-Server, der die eigentliche Arbeit inklusive der Passwort-Synchronisation erledigt.
- `smbpasswd` akzeptiert beliebig schlechte Passwörter, z. B. leere oder aus nur einem Buchstaben bestehende Passwörter. Das Linux-Passwortsystem bzw. PAM erzwingt dagegen eine minimale Passwortqualität und verweigert allzu einfache Passwörter. Das kann dazu führen, dass zwar das Samba-Passwort verändert wird, das Linux-Passwort aber nicht. Ab diesem Zeitpunkt sind die Passwörter nicht mehr synchron, weswegen nun jeder weitere Versuch scheitert, das Linux-Passwort neu einzustellen. Um die Passwörter wieder zu synchronisieren, muss `root` das Linux- und Samba-Passwort des betroffenen Benutzers neu einstellen.
- Die Synchronisation durch `unix password sync` funktioniert nur in eine Richtung: von Samba zu Linux. Wenn ein Benutzer dagegen sein Linux-Passwort durch `passwd` verändert, bleibt das Samba-Passwort unverändert. Abhilfe kann hier die weiter unten beschriebene Bibliothek `libpam-smbpass` schaffen.

Aus meiner persönlichen Erfahrung rate ich von der hier beschriebenen Passwort-Synchronisation ab. Sie ist fehleranfällig und verursacht vielfach mehr Probleme, als sie löst. Verwenden Sie die Einstellung `unix password sync = no`.

libpam-smbpass

Ubuntu sieht zur Passwort-Synchronisation von Linux nach Samba die Bibliothek `libpam-smbpass` vor. Die Installation des gleichnamigen Pakets führt dazu, dass die PAM-Konfigurationsdateien (siehe Abschnitt 21.4) so verändert werden, dass bei jedem erfolgreichen Login sowie bei jeder Veränderung eines Linux-Passworts das dazugehörende Samba-Passwort ebenfalls eingerichtet bzw. aktualisiert wird. Das setzt voraus, dass Sie Ihren Desktop nicht mit Auto-Login konfiguriert haben.

`libpam-smbpass` ist vor allem dann extrem praktisch, wenn mehrere Linux-Benutzer via Samba Dateien austauschen möchten. Durch `libpam-smbpass` ist sichergestellt, dass das Samba-Passwort jeweils mit dem gerade aktuellen Linux-Passwort des Benutzers übereinstimmt.

»libpam-smbpass« versus »[lib]pam_smb«

Verwechseln Sie die Bibliothek `libpam-smbpass` nicht mit `[lib]pam_smb`! Das Modul `pam_smb` ermöglicht die Login-Authentifizierung bei einem Samba- oder Windows-Server und hat nichts mit der Passwort-Synchronisation zu tun.

Zuordnung zwischen Windows- und Linux-Benutzernamen

Unter Windows ist als Benutzername beinahe jede Zeichenkette mit bis zu 128 Zeichen möglich, unter Linux dagegen nur eine Zeichenkette mit maximal 32 Zeichen ohne Sonderzeichen oder Leerzeichen. Wenn ein Windows-Benutzer einen Benutzernamen verwendet, der sich nicht unmittelbar einem Linux-Benutzernamen zuordnen lässt, muss die Zuordnung über eine Datei hergestellt werden. Der Name dieser Datei wird in `smb.conf` durch die Option `username map` angegeben:

```
# /etc/samba/smb.conf
[global]
    ...
    username map = /etc/samba/smbusers
```

Jede Zeile der Datei `smbusers` enthält zuerst einen Linux-Benutzernamen, dann das Zeichen = und schließlich einen oder mehrere Windows-Benutzernamen. Namen mit Leerzeichen stellen Sie in Anführungszeichen. Sie können die Datei auch benutzen, um mehreren Windows-Benutzern einen Linux-Benutzer zuzuordnen.

```
# /etc/samba/smbusers
peter  = "Peter Mayer"
...
```

Eine falsche Samba-Konfiguration kann das gesamte Linux-System gefährden

`/etc/samba/smbusers` kann das Sicherheitssystem von Samba bzw. Linux aushebeln, wenn `root` einem anderen Benutzer zugeordnet wird! Achten Sie darauf, dass nur `root` die Datei ändern darf:

```
root# chmod 644 /etc/samba/smbusers
```

Und jetzt alles zusammen

Nehmen wir an, in Ihrem lokalen Netzwerk gibt es einen Windows-PC für Peter Mayer, wobei der Login-Name auf diesem Rechner `Peter Mayer` lautet. Auf einem Linux-Server mit Samba gibt es den Account `peter`. `smbusers` stellt die Zuordnung zwischen `Peter Mayer` und `peter` her. Unter diesen Voraussetzungen gibt es nun folgende Kombinationen aus Login-Name und Passwort:

- **Login unter Windows:** `Peter Mayer` und das Windows-Passwort

  Das Windows-Passwort gilt für das lokale Arbeiten am Windows-Rechner. Peter kann sein Windows-Passwort unter Windows ändern.

- **Login auf dem Server (Linux):** `peter` und das Linux-Passwort

  Das Linux-Passwort gilt für einen direkten Login auf dem Server, sofern der Linux-Account aktiv und nicht gesperrt ist. Peter kann sein Linux-Passwort z. B. nach einem SSH-Login auf dem Server mit dem Kommando `passwd` ändern.

- **Zugriff auf Netzwerkverzeichnisse:** `Peter Mayer` oder `peter` und das Samba-Passwort

  Das Samba-Passwort gilt für die Nutzung der Netzwerkverzeichnisse. Es sollte mit dem Windows-Passwort übereinstimmen. Ist das nicht der Fall, erscheint unter Windows eine Login-Box, sobald Peter auf ein Netzwerkverzeichnis zugreifen möchte. Peter kann sein Samba-Passwort nach einem SSH-Login auf dem Server mit `smbpasswd` ändern.

Kurz und gut: Nur technisch versierte Benutzer sind in der Lage, ihre drei Passwörter selbst zu ändern – und das auch nur, wenn der Linux-Account aktiv ist. Für alle anderen gilt: Einmal definierte Passwörter werden nie wieder geändert. Vom Sicherheitsstandpunkt aus betrachtet, ist das natürlich alles andere als optimal.

31.4 Netzwerkverzeichnisse

Im vorigen Abschnitt habe ich erklärt, welche Voraussetzungen erfüllt sein müssen, damit sich ein Benutzer bei Samba anmelden kann – kurz zusammengefasst: Ein Linux-Account und ein Samba-Passwort müssen vorhanden sein. Offen ist nun nur noch, welche Ressourcen ein angemeldeter Benutzer sieht und verwenden kann. Entscheidend hierfür sind die `[resourcename]`-Abschnitte in `smb.conf`.

SELinux kann den Zugriff auf Verzeichnisse verhindern

Wenn Sie Ihren Samba-Server unter Fedora oder RHEL einrichten, sollten Sie auch an SELinux denken (siehe Abschnitt 31.2)! Sie müssen dem Verzeichnis das Attribut `samba_share_t` zuordnen oder den entsprechenden booleschen Parameter setzen, damit der Zugriff klappt!

Benutzerverzeichnisse

Die Definition eines Verzeichnisses, auf das ein bestimmter Benutzer zugreifen kann, sieht so aus:

```
# in /etc/samba/smb.conf
...
[verzeichnis1]
   user      = peter
   path      = /data/verz1
   writeable = yes
```

Mit dieser Einstellung können der Benutzer `peter` sowie alle Benutzer, die diesem Linux-Account durch `smbusers` zugeordnet sind, das Verzeichnis `/data/verz1` lesen und verändern. Im Datei-Manager hat diese Ressource den Namen `verzeichnis1`, also die in eckigen Klammern angegebene Zeichenkette.

Die Bedeutung der Schlüsselwörter ist leicht verständlich: `user` gibt den Benutzernamen an. Statt `user` können Sie auch die Synonyme `users` oder `username` verwenden. Es ist zulässig, mehrere durch Komma getrennte Benutzernamen anzugeben.

`path` gibt an, welches Verzeichnis des Servers freigegeben wird. Wenn `path` nicht explizit angegeben wird, gibt Samba standardmäßig das Heimatverzeichnis des angegebenen Benutzers frei. `writeable = yes` erlaubt Veränderungen im Verzeichnis. Ohne diese Option hat der Benutzer nur Lesezugriff.

Grundsätzlich gelten für alle Zugriffe die Linux-Zugriffsrechte. Wenn es in `/data/verz1` also eine Datei gibt, die `root` gehört, dann darf der Linux-Benutzer `peter` diese Datei normalerweise nur lesen, aber nicht verändern. Diese Einschränkung gilt ebenso für alle Benutzer des Netzwerkverzeichnisses.

Home-Verzeichnisse

Wenn ein Datei-Server für viele Benutzer eingerichtet wird, ist es das Einfachste, dass jeder angemeldete Samba-Benutzer direkt sein Linux-Heimatverzeichnis sieht und bearbeiten darf. Anstatt `smb.conf` nun durch unzählige Einträge der Form

```
[benuterzname]
   user      = benutzername
   writeable = yes
```

aufzublähen, sieht `smb.conf` die folgende Kurzschreibweise vor:

```
[homes]
   writeable  = yes
   browseable = no
```

Damit wird das Heimatverzeichnis des gerade aktiven Benutzers unter dessen Namen sichtbar. Die Option `browseable = no` bewirkt nicht, wie man vielleicht glauben könnte, dass der Benutzer sein Verzeichnis nicht sieht. Sie verhindert nur, dass das Verzeichnis doppelt sichtbar ist: einmal unter dem jeweiligen Benutzernamen (etwa `peter`) und einmal als `homes`.

Gruppenverzeichnisse

Benutzer- und Heimatverzeichnisse ermöglichen es dem Benutzer, seine Dateien zentral auf dem Server zu speichern, bieten aber keine Möglichkeit zum Datenaustausch. Die Verzeichnisse sind für andere Benutzer unsichtbar und unerreichbar. Abhilfe schaffen Gruppenverzeichnisse, die alle Mitglieder einer Gruppe verwenden dürfen. Die Gruppenzuordnung erfolgt durch die Linux-Benutzerverwaltung. Die Gruppe wird mit dem Schlüsselwort `user` in der Schreibweise `@gruppenname` angegeben.

```
# in /etc/samba/smb.conf
...
[salesdata]
   user           = @sales
   path           = /data/sales
   writeable      = yes
   force group    = +sales
   create mask    = 0660
   directory mask = 0770
```

Beim Zugriff auf Gruppenverzeichnisse ist die richtige Einstellung der Zugriffsrechte von Dateien und Verzeichnissen besonders wichtig. Das gilt auch für Dateien und Verzeichnisse, die neu erstellt werden. `force group = +sales` bewirkt, dass neu erzeugte Dateien oder Verzeichnisse der Gruppe `sales` zugeordnet werden und nicht wie sonst üblich der Standardgruppe des Benutzers. Wenn ein Benutzer nicht Mitglied der Gruppe `sales` ist, darf er nicht auf das Verzeichnis zugreifen.

Vorsicht mit »force group«

Verwenden Sie im obigen Fall auf keinen Fall die Einstellung `force group = sales`, also ohne vorangestelltes Plus! Das hätte zur Folge, dass Samba jeden Zugriff auf das Verzeichnis so durchführt, als wäre der gerade aktive Benutzer Mitglied der Gruppe `sales` – und zwar selbst dann, wenn der Benutzer auf Linux-Ebene gar kein Mitglied dieser Gruppe ist! Mit anderen Worten: Mit `force group = sales` geben Sie Benutzern, die der Gruppe `sales` gar nicht angehören, Lese- und Schreibrechte für das Verzeichnis. Bei Gruppenverzeichnissen ist das selten beabsichtigt und kann ein großes Sicherheitsproblem sein!

Die Parameter `create mask` und `directory mask` stellen sicher, dass von Gruppenmitgliedern neu erstellte Dateien und Verzeichnisse von allen anderen Gruppenmitgliedern gelesen und verändert werden können. Die oktale Zahl entspricht dem `chmod`-Wert – siehe `man chmod`. Wenn neue Dateien bzw. Verzeichnisse von anderen Gruppenmitgliedern nur gelesen, aber nicht verändert werden dürfen, verwenden Sie die Werte 0440 und 0550.

Frei zugängliche Verzeichnisse

Noch liberaler ist der Zugriff auf das `share`-Verzeichnis: Jeder Benutzer, der sich bei Samba authentifizieren kann, kann Dateien aus diesem Verzeichnis lesen. Der Schreibzugriff ist in diesem Beispiel deaktiviert:

```
# in /etc/samba/smb.conf
...
[share]
   path      = /data/share
   read only = yes
```

Sie können selbstverständlich auch frei zugängliche Verzeichnisse mit Schreibzugriff einrichten (`writable = yes`). Standardmäßig können alle Benutzer die von anderen Benutzern erzeugten Dateien lesen, aber nicht verändern. Abhilfe schafft die Einstellung von `force group` und der beiden `mask`-Parameter. Uneingeschränkte gegenseitige Schreib- und Leserechte erzielen Sie mit `create mask = 0666` und `directory mask = 0777`.

Zugriff für nicht authentifizierte Benutzer

Alle vorangegangenen Beispiele setzten voraus, dass sich der Benutzer bei Samba authentifizieren kann. Bei entsprechender Konfiguration sieht Samba auch einen Verzeichniszugriff für nicht authentifizierte Benutzer vor. Derartige Benutzer werden im Samba-Jargon als *Gäste* (`guest`-Benutzer) bezeichnet. Für den Umgang mit Gästen sind die im folgenden Listing zusammengefassten globalen Einstellungen verantwortlich:

```
# in /etc/samba/smb.conf
[global]
   ...
   map to guest           = bad user
   guest account          = nobody
```

`map to guest = bad user` bewirkt, dass Login-Versuche mit einem nicht existenten Benutzernamen automatisch dem virtuellen Samba-Benutzer `guest` zugeordnet werden. Standardmäßig gibt es allerdings keine Netzwerkverzeichnisse oder andere Ressourcen, die `guest` nutzen darf.

`guest account` gibt an, welchem Linux-Benutzer Gäste zugeordnet werden. Bei den meisten Linux-Distributionen inklusive Debian und Ubuntu ist hierfür der Benutzer `nobody` vorgesehen.

Verzeichnisse, die für Gäste benutzbar sein sollen, kennzeichnen Sie durch `guest ok = ok`. In aller Regel werden Sie solche Verzeichnisse mit dem Attribut `read only = yes` vor Schreibzugriffen schützen. Denken Sie daran, dass Gäste generell nur solche Dateien lesen bzw. verändern dürfen, die auch der Linux-Benutzer `nobody` lesen bzw. verändern darf.

```
[guest]
   path        = /data/guest
   guest ok    = yes
   read only   = yes
```

Eine Variante zu `guest ok` ist `guest only = yes`: Mit dieser Einstellung kann das Verzeichnis nur von Gästen, nicht aber von authentifizierten Benutzern verwendet werden. Wenn Sie Gästen generell keinen Zugang zu Samba-Ressourcen gewähren möchten, verwenden Sie im `[global]`-Abschnitt die Einstellung `map to guest = never`.

User Shares

Samba bietet gewöhnlichen Benutzern ohne `root`-Rechten die Möglichkeit, selbst Verzeichnisse, sogenannte User Shares, freizugeben. Die entsprechenden Konfigurationsdateien werden üblicherweise im Verzeichnis `/var/lib/samba/usershares` gespeichert, wobei jedes freigegebene Verzeichnis seine eigene Datei erhält. Die folgenden Zeilen geben dafür ein Beispiel.

```
# Datei /var/lib/samba/usershares/testdir
path          = /myhome/kofler/testdir
comment       =
guest_ok      = n
```

Details der User-Share-Konfiguration werden im globalen Abschnitt von `smb.conf` durch diverse `usershare`-Anweisungen gesteuert. `usershare allow guests` erlaubt die Freigabe von User Shares zur Benutzung durch den `guest`-Account, also ohne Passwortschutz. Das erfordert die Angabe von `guest ok` oder `guest only` bei der Definition des Verzeichnisses. `usershare max shares` limitiert die Anzahl der User Shares.

```
# in /etc/samba/smb.conf
[global]
   ...
   usershare allow guests = yes
   usershare max shares   = 100
```

Papierkorb für Samba-Verzeichnisse

Wenn Dateien in Netzwerkverzeichnissen gelöscht werden, sind sie in der Regel für immer verloren. Die Papierkorb-Funktionen, die Linux, Windows oder OS X anbieten, gelten jeweils nur für lokale Dateien. Um den ungewollten Verlust von Dateien zu vermeiden, können Sie aber auch auf Samba-Ebene einen Papierkorb einrichten. In der einfachsten Konfiguration reicht dazu eine einzige Zeile in `smb.conf`:

```
[global]
  vfs objects = recycle
```

Damit wird das Samba-VFS-Erweiterungsmodul `recycle` aktiviert, wobei VFS für *Virtual File System* steht. Gelöschte Dateien landen nun standardmäßig im Verzeichnis `.recycle` (relativ zum Share-Verzeichnis). Dieses Verzeichnis ist allerdings in den meisten Datei-Managern unsichtbar. Um den Vorgang transparenter zu machen, können Sie mit `recycle:repository` einen anderen Verzeichnisnamen für den Papierkorb angeben, z. B. so:

```
  recycle:repository = Papierkorb
```

Wirklich gelöscht werden Dateien nun erst, wenn sie auch im Papierkorb gelöscht werden. Unter Umständen kann es zweckmäßig sein, auf dem Samba-Server ein Script auszuführen, das alte Dateien nach einer gewissen Zeit automatisch aus dem Papierkorb löscht. Damit das funktioniert, müssen Sie aber das Änderungsdatum beim Verschieben in den Papierkorb aktualisieren (Option `recycle:touch = Yes`).

Diverse weitere `recycle:xxx`-Optionen sind hier dokumentiert:

http://linux.die.net/man/8/vfs_recycle

Die `recycle:xxx`-Optionen können wahlweise global oder für einzelne Verzeichnisse eingestellt werden. Ein Anwendungsbeispiel finden Sie hier:

http://www.redhat.com/advice/tips/sambatrash.html

Netzwerkverzeichnisse in Gnome und KDE freigeben

Wenn Desktop-Anwender rasch und unkompliziert ein Verzeichnis per Samba freigeben möchten, haben sie in der Regel keine Lust, manuell Änderungen an `smb.conf` durchzuführen. Deswegen sehen die Dateimanager von Gnome und KDE Dialoge vor, um Verzeichnisse freizugeben.

Hinter den Kulissen nutzen sowohl Nautilus (Gnome) als auch Dolphin (KDE) den User-Share-Mechanismus von Samba: Die Parameter für jedes freigegebene Verzeichnis werden dazu jeweils in einer eigenen Konfigurationsdatei im Verzeichnis `/var/lib/samba/usershares` gespeichert. Die Zugriffsrechte dieses Verzeichnisses sind so eingestellt, dass alle Benutzer, die einer bestimmten Gruppe angehören (bei Ubuntu `sambashare`), darin neue Dateien anlegen dürfen.

Vorbereitungen

Im Folgenden setze ich voraus, dass der Samba-Server installiert ist, also zumeist das Paket `samba`. Falls eine Firewall aktiv ist, müssen Sie dort die Samba-Ports öffnen.

Wenn Sie SUSE oder openSUSE verwenden, müssen Sie vor der Freigabe des ersten Verzeichnisses unter KDE oder Gnome eine Samba-Basiskonfiguration durchführen. Dazu können Sie das YaST-Modul NETZWERKDIENSTE • SAMBA-SERVER verwenden. Als Server-Typ wählen Sie KEIN DOMAIN CONTROLLER. Die anderen Varianten sind nur dann von Interesse, wenn Samba auch Login-Daten für Windows-Accounts verwalten soll. Im Dialogblatt START wählen Sie nun die Option BEIM SYSTEMSTART, um den Samba-Server in Zukunft automatisch zu starten. Damit andere Rechner im lokalen Netzwerk auf die Netzwerkverzeichnisse zugreifen können, müssen Sie außerdem die Option FIREWALL-PORT ÖFFNEN aktivieren.

Nautilus/Gnome

Sofern die Pakete `nautilus-share*` installiert sind, können Sie im Gnome-Dateimanager Verzeichnisse freigeben. Dazu klicken Sie das Verzeichnis mit der rechten Maustaste an und führen das Kontextmenükommando FREIGABEOPTIONEN aus (siehe Abbildung 31.1).

Fedora- und RHEL-Anwender müssen auf `nautilus-share` leider ganz verzichten, vermutlich weil diese Nautilus-Erweiterung nicht zur Red-Hat-spezifischen SELinux-

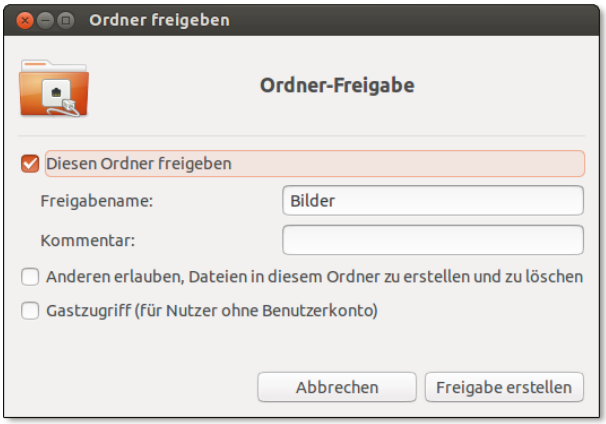


Abbildung 31.1 Verzeichnisfreigabe unter Ubuntu

Konfiguration kompatibel ist. Zur bequemen Konfiguration können Sie stattdessen das Programm `system-config-samba` einsetzen.

Dolphin/KDE

Unter KDE können Sie in den Dateimanagern Dolphin und Konqueror im FREIGABE-Blatt des Eigenschaftsdialogs ein Netzwerkverzeichnis einrichten. Dazu muss das Paket `kdenetwork-filesharing` installiert sein.

Passwort-verwaltung

Bleibt noch die Frage zu klären, wer die freigegebenen Verzeichnisse benutzen darf. Wenn Sie die Option GASTZUGRIFF aktiviert haben, hat jeder ohne Anmeldung Zugriff auf Ihr Netzwerkverzeichnis. Wenn Sie die Option dagegen nicht aktivieren, muss sich der Benutzer mit Name und Passwort anmelden. Das funktioniert aber nur für Benutzer, für die es auf dem aktuellen Rechner einen Account gibt, und nur dann, wenn für diese Benutzer mit `smbpasswd` oder via `libpam-smbpass` ein Samba-Passwort definiert wurde. Weder KDE noch Gnome kümmert sich darum. Gegebenenfalls müssen Sie Ihr Samba-Passwort mit `smbpasswd` in einem Terminal-Fenster festlegen.

31.5 Beispiel – Home- und Medien-Server

Dieser Abschnitt gibt ein einfaches Beispiel für die Konfiguration eines zentralen Samba-Servers. Ausgangspunkt ist ein computer-affiner Haushalt, in dem sich auf den drei Computern der Eltern bzw. der beiden Kinder immer mehr Daten anhäufen: Bilder von Digitalkameras, MP3s, Schuldokumente, die Buchhaltung etc. Die dezentrale Datenhaltung wirft einige Probleme auf:

- Es gibt keine ordentlichen Backups. Was passiert, wenn ein Notebook auf dem Weg zur Schule verloren geht oder das Zeitliche segnet?
- Es ist schwierig, auf gemeinsame Daten zuzugreifen. Oma soll zum nächsten Geburtstag ein Album der besten Familienfotos der letzten Jahre bekommen. Die digitalen Fotos sind aber über drei Rechner verteilt und in keiner Weise geordnet. Ähnliche Probleme gibt es auch bei Partys, wenn sich beim Abspielen von MP3-Dateien herausstellt, dass sich das gerade gewünschte Album auf einem anderen Rechner befindet.
- Der Datenaustausch zwischen den Rechnern ist umständlich und erfolgt zumeist mithilfe eines USB-Sticks.

Der Linux-begeisterte Sohn schlägt schließlich vor, diese Probleme durch einen zentralen Home- oder Medien-Server zu lösen. Der Server kann via WLAN in das Heimnetz integriert werden. Bei Bedarf kann der Rechner auch gleich als Internet-Router und Firewall genutzt werden.

An dieser Stelle ist nur die Samba-Konfiguration von Interesse: Jedes Familienmitglied bekommt ein eigenes Netzwerkverzeichnis, in dem es allein Daten schreiben und lesen darf. Die dort gespeicherten Daten sind also privat, wobei natürlich allen Familienmitgliedern klar sein muss, dass der Sohn als Administrator letztlich jede Datei lesen und verändern kann ...

Zum gemeinsamen Datenaustausch gibt es außerdem noch fünf weitere Verzeichnisse. Die Eltern dürfen auf `eltern` zugreifen, die Kinder auf `kinder` und alle Familienmitglieder auf die Verzeichnisse `familie`, `audio` und `fotos`. Natürlich wäre es möglich gewesen, die Verzeichnisse `audio` und `fotos` einfach als Unterverzeichnisse von `familie` einzurichten, die Definition eigener Netzwerkverzeichnisse macht die Anwendung aber ein wenig intuitiver. Bei Bedarf können natürlich beliebige weitere Benutzer und Verzeichnisse eingerichtet werden.

Linux-Benutzer und Gruppen einrichten

Als Benutzernamen verwende ich im Folgenden `mutter`, `vater`, `tochter`, `sohn`. In der Praxis werden Sie hier natürlich richtige Namen verwenden – aber darauf habe ich hier verzichtet, damit Sie nicht auch noch die Namen einer fiktiven Familie lernen müssen.

```
root#  groupadd eltern
root#  groupadd kinder
root#  groupadd familie
root#  useradd --create-home --groups eltern,familie vater
root#  useradd --create-home --groups eltern,familie mutter
root#  useradd --create-home --groups kinder,familie sohn
root#  useradd --create-home --groups kinder,familie tochter
```

Da useradd ohne Passwort ausgeführt wurde, werden die neuen Benutzer automatisch gesperrt, d. h., es ist kein Login möglich. Das ist beabsichtigt: Es ist weder erforderlich noch zweckmäßig, dass sich die Familienmitglieder direkt auf dem Server anmelden.

Zusammen mit jedem Benutzer wird automatisch auch eine neue, gleichnamige Gruppe erzeugt, die als Standardgruppe für den Benutzer gilt. Außerdem werden den neuen Benutzern auch die Gruppen familie und eltern oder kinder zugeordnet. vater gehört somit den Gruppen vater, eltern und familie an, mutter den Gruppen mutter, eltern und familie etc. Wenn Sie einem Benutzer später eine weitere Gruppe zuordnen möchten, verwenden Sie am einfachsten das folgende Kommando:

```
root#  usermod -a -G neuegruppe benutzer
```

Samba-Benutzer einrichten

Als Nächstes werden die Samba-Benutzer eingerichtet, diesmal jeweils mit einem Passwort:

```
root#  smbpasswd -a vater
root#  smbpasswd -a mutter
...
```

Verzeichnisse einrichten

Beim Einrichten der Verzeichnisse für die gemeinsamen Dateien ist es wichtig, Besitzer und Zugriffsrechte richtig einzustellen – sonst funktioniert später der Datenzugriff nicht. Das erste Kommando chmod 770 bewirkt, dass nur Gruppenmitglieder das Verzeichnis lesen und verändern dürfen. Das zweite Kommando verbietet den Zugriff auf die Home-Verzeichnisse durch andere Benutzer.

```
root#  mkdir /shared-data
root#  mkdir /shared-data/{eltern,kinder,familie,audio,fotos}
root#  cd /shared-data
root#  chown :eltern eltern/
root#  chown :kinder kinder/
root#  chown :famile familie/ audio/ fotos/
root#  chmod 770 *
root#  chmod 770 /home/{vater,mutter,sohn,tochter}
```

Ein Vorteil des gemeinsamen Datei-Servers ist die Möglichkeit, zentrale Backups zu machen. Dabei müssen Sie lediglich die Verzeichnisse /home und shared-data sichern.

Samba-Konfiguration

Die nachfolgenden Zeilen zeigen die Konfigurationsdatei smb.conf. Die Passwort-Synchronisierung und jeglicher Samba-Zugriff durch Gäste sind deaktiviert. Die Einstellungen für die diversen Verzeichnisse sollten nach der Lektüre von Abschnitt 31.4 ohne weitere Erklärung verständlich sein.

```
# /etc/samba/smb.conf für einen Home-Server
[global]
   workgroup           = home
   server string       = %h server (Samba, Ubuntu)
   security            = user
   passdb backend      = tdbsam
   unix password sync  = no
   invalid users       = root
   map to guest        = never
   log file            = /var/log/samba/log.%m
   max log size        = 1000
   syslog              = 0
   dns proxy           = no
   panic action        = /usr/share/samba/panic-action %d
[homes]
   browseable          = no
   writeable           = yes
[eltern]
   user                = @eltern
   path                = /shared-data/eltern
   writeable           = yes
   force group         = +eltern
   create mask         = 0660
   directory mask      = 0770
[kinder]
   user                = @kinder
   path                = /shared-data/kinder
   writeable           = yes
   force group         = +kinder
   create mask         = 0660
   directory mask      = 0770
[familie]
   user                = @familie
   path                = /shared-data/familie
   writeable           = yes
   force group         = +familie
   create mask         = 0660
   directory mask      = 0770
[fotos]
   user                = @familie
   path                = /shared-data/fotos
   ... wie bei [familie]

[audio]
   user                = @familie
   path                = /shared-data/audio
   ... wie bei [familie]
```

Die Konfiguration hat einen kleinen Schönheitsfehler: Alle Benutzer sehen *alle* Freigaben, auch die, die nicht für sie bestimmt sind und die sie nicht nutzen dürfen, z. B. sehen die Kinder das Verzeichnis `eltern`, die Eltern das Verzeichnis `kinder`. Eine tatsächliche Nutzung dieser Verzeichnisse scheitert wie geplant an den Zugriffsrechten, aber noch eleganter wäre es natürlich, wenn diese Verzeichnisse gar nicht erst sichtbar wären.

Samba bietet hierfür leider keine Konfigurationsmöglichkeiten. Sie können zwar einzelne Verzeichnisse durch `browseable = no` verstecken, aber dann sieht niemand die Verzeichnisse mehr, auch nicht die rechtmäßigen Nutzer. Die Verzeichnisse bleiben weiter benutzbar, allerdings muss der richtige Pfad manuell angegeben werden. Auch die Optionen `hide unreadable = yes` und `hide unwriteable = yes` helfen nicht weiter: Damit werden *innerhalb* eines Netzwerkverzeichnisses alle Dateien versteckt, die ein Benutzer nicht lesen bzw. nicht verändern kann. Das Netzwerkverzeichnis an sich bleibt aber weiter sichtbar.

31.6 Beispiel – Firmen-Server

Ein mittelständisches Unternehmen stellt Meßgeräte her. Vor allem im Hinblick auf zentrale Backups, aber auch zur Vereinfachung des Datenaustauschs, wird ein Samba-Server eingerichtet. Alle Mitarbeiter bekommen dort ein eigenes Verzeichnis. Außerdem gibt es mehrere gemeinsame Verzeichnisse, die Tabelle 31.2 zusammenfasst. Tabelle 31.3 zeigt, welchen Gruppen die Mitarbeiter je nach ihrer Position in der Firma angehören.

Netzwerkverzeichnis	Zugriff (Gruppen)
`strategie`	`leitung`
`buchhaltung`	`buchhaltung`, `leitung`
`entwicklung`	`entwicklung`, `leitung`
`vertrieb`	`vertrieb`, `buchhaltung`, `leitung`

Tabelle 31.2 Datenaustausch im Firmen-Server

Weniger ist mehr!

Wenn Sie selbst ein Gruppen- und Verzeichnisschema erstellen müssen, sollte Einfachheit das oberste Gebot sein. Je mehr Gruppen und Verzeichnisse es gibt, desto unübersichtlicher wird das System, desto unhandlicher seine Anwendung und desto mühsamer die Wartung.

Mitarbeiter	Gruppenzugehörigkeit
Unternehmensleitung	leitung, entwicklung, vertrieb, buchhaltung
Buchhaltung/Controlling	buchhaltung, vertrieb
Entwickler	entwicklung
Vertriebsteam, Marketing	vertrieb

Tabelle 31.3 Gruppenzugehörigkeit der Mitarbeiter je nach Position

Auch wenn Sie den Samba-Server mit hochwertiger Hardware realisieren und Gigabit-Netzwerkverbindungen verwenden, ist der Zugriff auf Netzwerkverzeichnisse langsamer als auf lokale Dateien. Deswegen werden manche Benutzer große Dateien aus Performance-Gründen weiterhin lokal speichern und bearbeiten. In diesem Fall sollte es unbedingt ein automatisches Script geben, das alle lokalen Dateien einmal täglich mit dem privaten Netzwerkverzeichnis des Benutzers snychronisiert. Alle Vorteile eines zentralen Backup-Systems gehen verloren, wenn einzelne Benutzer ihre Dateien auf der lokalen Festplatte speichern!

Linux-Benutzer und Gruppen einrichten

Als Benutzernamen verwende ich im Folgenden der Einfachheit halber `chefn`, `entwicklern` etc. In der Praxis werden Sie natürlich richtige Namen verwenden. Bis auf die Namen ähneln die Kommandos zum Einrichten der Gruppen und Benutzer sehr stark denen des vorigen Beispiels (Home-Server). Ein direkter Login der Mitarbeiter auf dem Server ist nicht vorgesehen, deswegen entfällt an dieser Stelle die Passwortangabe.

```
root#  groupadd leitung
root#  groupadd vertrieb
root#  groupadd buchhaltung
root#  groupadd entwicklung
root#  useradd --create-home \
         --groups leitung,vertrieb,buchhaltung,entwicklung chefin1
root#  useradd --create-home --groups vertrieb vertrieb1
root#  useradd --create-home --groups vertrieb vertrieb2
root#  useradd --create-home --groups entwicklung entwickler1
root#  useradd --create-home --groups entwicklung entwicklerin2
root#  useradd --create-home --groups buchhaltung,vertrieb buchhalter1
root#  useradd --create-home --groups buchhaltung,vertrieb controller1
root# ...
```

Samba-Benutzer einrichten

Als Nächstes werden die Samba-Benutzer eingerichtet, diesmal jeweils mit einem Passwort:

```
root#  smbpasswd -a chefin1
root#  smbpasswd -a vertrieb1
...
```

Verzeichnisse einrichten

Beim Einrichten der Verzeichnisse für die gemeinsamen Dateien ist es wichtig, Besitzer und Zugriffsrechte richtig einzustellen – sonst klappt später der Datenzugriff nicht. Das erste Kommando `chmod 770` bewirkt, dass nur Gruppenmitglieder das Verzeichnis lesen und verändern dürfen, und verhindert, dass andere Benutzer auf die Home-Verzeichnisse zugreifen dürfen.

```
root#  mkdir /firmendaten
root#  mkdir /firmendaten/{entwicklung,vertrieb,buchhaltung,strategie}
root#  cd /firmendaten
root#  chown :entwicklung entwicklung/
root#  chown :vertrieb    vertrieb/
root#  chown :buchhaltung buchhaltung/
root#  chown :leitung     strategie/
root#  chmod 770 /firmendaten/* /home/*
```

Samba-Konfiguration

Der globale Abschnitt von `smb.conf` sieht mit Ausnahme der `workgroup`-Zeichenkette exakt genauso aus wie beim Home-Server-Beispiel (siehe Abschnitt 31.5). Auch die Definition der Netzwerkverzeichnisse ähnelt dem vorigen Beispiel stark. Der Unterschied besteht darin, dass Mitglieder mehrerer Gruppen auf die Verzeichnisse zugreifen dürfen. Damit der Datenaustausch reibungslos funktioniert, ist insbesondere `force group` entscheidend. Alle Benutzer, die auf ein Verzeichnis zugreifen dürfen, müssen Mitglied dieser Gruppe sein. Vergessen Sie in `smb.conf` das Plus-Zeichen vor dem Gruppennamen nicht!

```
# /etc/samba/smb.conf für einen Firmen-Server (Stand-alone-Konfiguration)
[global]
   ... wie im vorigen Beispiel (Home-Server)
[homes]
   browseable     = no
   writeable      = yes
[strategie]
   user           = @leitung
   path           = /firmendaten/strategie
   writeable      = yes
   force group    = +leitung
   create mask    = 0660
   directory mask = 0770
[buchhaltung]
   user           = @buchhaltung, @leitung
   path           = /firmendaten/buchhaltung
   writeable      = yes
   force group    = +buchhaltung
   create mask    = 0660
   directory mask = 0770
```

```
[entwicklung]
   user           = @entwicklung, @leitung
   path           = /firmendaten/entwicklung
   writeable      = yes
   force group    = +entwicklung
   create mask    = 0660
   directory mask = 0770
[vertrieb]
   user           = @vertrieb, @buchhaltung, @leitung
   path           = /firmendaten/vertrieb
   writeable      = yes
   force group    = +vertrieb
   create mask    = 0660
   directory mask = 0770
```

31.7 Client-Zugriff

Dieser Abschnitt beschäftigt sich mit der Frage, wie ein Client-PC auf die von Samba zur Verfügung gestellten Verzeichnisse zugreift. Eine wichtige Voraussetzung besteht darin, dass die TCP-Ports 135, 139 und 445 sowie die UDP-Ports 137 und 138 nicht durch eine Firewall blockiert werden.

Linux-Clients

Bevor Sie unter Linux auf Windows- bzw. Samba-Netzwerkverzeichnisse zugreifen können, müssen Sie die Samba-Client-Tools installieren. Bei Ubuntu sind die erforderlichen Programme in `samba-common`, `smbclient` und `libsambaclient` verpackt, bei Fedora in `samba-common`, `samba-client` und `samba-libs`.

KDE, Gnome

Am einfachsten verwenden Sie zum Zugriff auf ein Netzwerkverzeichnis den Dateimanager von Gnome oder KDE. In beiden Programmen gibt es einen Netzwerk-Browser, der im ersten Schritt alle verfügbaren Windows-Netzwerke anzeigt. Ein paar Mausklicks und gegebenenfalls die Eingabe der Login-Daten (Benutzername und Passwort) führen in das gewünschte Verzeichnis.

Bisweilen ist der Dateimanager nicht in der Lage, die Netzwerkverzeichnisse selbstständig zu finden. In diesem Fall müssen Sie deren Ort explizit in der Adresszeile des Dateimanagers angeben. Dabei gilt die Schreibweise `smb://servername/verzeichnisname`.

LinNeighborhood und pyNeighborhood

KDE- und Gnome-Verweigerer, die dennoch grafische Unterstützung beim Zugriff auf Windows-Verzeichnisse suchen, sollten sich das Programm `LinNeighborhood` oder dessen neuere Variante `pyNeighborhood` ansehen.

CIFS

Eine weitere Vorgehensweise besteht darin, Netzwerkverzeichnisse mit dem *Common Internet File System* (CIFS) direkt in den lokalen Verzeichnisbaum einzubinden. Das ist freilich nur sinnvoll, wenn anzunehmen ist, dass das Verzeichnis über längere Zeit verfügbar bleibt, also auf einem stabilen Server läuft.

CIFS ist der Nachfolger von SMBFS (*SMB File System*). CIFS-kompatible Samba-Server geben Unix/Linux-kompatible Informationen über die Zugriffsrechte von Dateien weiter, was bei SMBFS nicht möglich ist.

CIFS setzt voraus, dass die Samba-Client-Werkzeuge und die CIFS-Unterstützung für `mount` und insbesondere das Kommando `mount.cifs` zur Verfügung stehen. Bei Debian und Ubuntu muss dazu das Paket `cifs-utils` installiert werden. Bei Fedora und openSUSE ist das Paket standardmäßig installiert.

Um ein externes Verzeichnis einzubinden, geben Sie eines der beiden folgenden Kommandos an, je nachdem, ob die Windows-Freigabe auf der Basis von Benutzernamen erfolgt oder nicht:

```
root#  mount -t cifs //jupiter/myshare /media/winshare
root#  mount -t cifs -o username=name //jupiter/myshare /media/winshare
```

Damit wird das auf dem Rechner `jupiter` unter dem Namen `myshare` freigegebene Verzeichnis in das Linux-Dateisystem eingebunden. Die Daten stehen jetzt unter dem Linux-Verzeichnis `/media/winshare` dem Benutzer `root` zur Verfügung. Dieses Verzeichnis muss vor dem Ausführen von `mount` natürlich schon existieren. Bei der Ausführung des Kommandos werden Sie nach dem Passwort gefragt. Sie können das Passwort aber auch direkt angeben, was aber weniger sicher ist:

```
root#  mount -t cifs -o username=name,password=xxxxxxxx \
        //jupiter/myshare /media/winshare
```

Weitere mount-Optionen

Damit Sie das Benutzerverzeichnis als gewöhnlicher Benutzer lesen und schreiben können, geben Sie beim `mount`-Kommando Ihre persönlichen Benutzer- und Gruppen-Identifikationsnummern an, die Sie mit dem Kommando `id` schnell ermitteln können.

```
root#  mount -t cifs -o username=name,password=xxxxxxxx,uid=1000,gid=1000 \
        //jupiter/myshare /media/winshare
```

Falls Dateinamen mit internationalen Zeichen falsch dargestellt werden, müssen Sie dem `mount`-Kommando die Option `iocharset=utf8` hinzufügen.

/etc/fstab

Um das Netzwerkverzeichnis immer automatisch in den Verzeichnisbaum einzubinden, fügen Sie `/etc/fstab` einen entsprechenden Eintrag hinzu, beispielsweise so:

```
# in /etc/fstab
//jupiter/myshare /media/winshare cifs username=u,password=p,...  0 0
```

Bei den meisten Distributionen werden alle in `/etc/fstab` genannten CIFS-Verzeichnisse während des Init-Prozesses eingebunden. Eine Ausnahme stellt SUSE dar: Hier ist für diesen Vorgang das Init-V-Script `cifs` zuständig, das explizit aktiviert werden muss:

```
root#  insserv cifs
```

Login-Daten auslagern

Aus Sicherheitsgründen ist die direkte Angabe des Passworts in `/etc/fstab` nicht empfehlenswert. Ein wenig besser ist es, diese Information in eine eigene Datei auszulagern, die nur `root` lesen kann. Richten Sie also die Datei `/etc/.winshare-pw` ein, die den Login-Namen, das Passwort und optional die Arbeitsgruppe (Domäne) für das Netzwerkverzeichnis enthält. Der Aufbau der Datei sieht so aus:

```
username=name
password=xxxx
domain=workgroup
```

Das folgende Kommando schränkt den Zugriff auf die Datei ein. Jetzt kann nur noch `root` die Datei lesen und verändern:

```
root#  chmod 600 /etc/.winshare-pw
```

Anschließend fügen Sie dem `fstab`-Eintrag die Option `credentials` hinzu. Beim Einbinden des Verzeichnisses werden die Authentifizierungsdateien aus `.winshare-pw` gelesen.

```
# Ergänzung in /etc/fstab
//jupiter/myshare    /media/winshare  cifs  credentials=/etc/.winshare-pw  0  0
```

smbclient und smbtree

smbclient

Freunde textorientierter Kommandos können Netzwerkverzeichnisse auch mit `smbclient` durchforschen. Das Kommando bietet zwar wenig Komfort, ist aber oft praktisch, um Samba-Problemen auf die Spur zu kommen.

`smbclient -L localhost` zeigt alle freigegebenen Ressourcen des lokalen Rechners an, listet alle sichtbaren Arbeitsgruppen des lokalen Netzwerks auf und gibt an, welcher Rechner in der jeweiligen Gruppe als Master fungiert. Die Passwortabfrage beantworten Sie bei passwortfreien Ressourcen einfach mit ↵. Falls auf dem lokalen Rechner kein Samba-Server läuft, geben Sie statt `localhost` den Rechnernamen an.

Wenn `smbclient` eine Login-Fehlermeldung liefert (*access denied*), stimmen die Benutzer- oder Workgroup-Namen Ihres Linux-Rechners zumeist nicht mit denen des Windows-Rechners oder Samba-Servers überein. Die einfachste Lösung besteht darin, diese Informationen als zusätzliche Parameter an `smbclient` zu übergeben:

```
user$  smbclient -U benutzername -W workgroupname -L jupiter
```

Sie können `smbclient` auch interaktiv zur Übertragung von Dateien einsetzen. Dazu stellen Sie zuerst eine Verbindung zum Windows-Rechner oder Samba-Server für das freigegebene Verzeichnis her. Das Verzeichnis müssen Sie in der Windows-typischen Schreibweise `\\servername\verzeichnisname` angeben. Damit die `\`-Zeichen nicht von der Shell verarbeitet werden, müssen diese verdoppelt werden.

Anschließend können Sie wie beim Kommando `ftp` Verzeichnisse mit `ls` ansehen, mit `cd` wechseln, mit `get` Dateien auf den lokalen Rechner übertragen (*download*) und mit `put` Dateien auf dem externen Rechner speichern (*upload*). Einen Überblick über die wichtigsten Kommandos bekommen Sie mit `help`. Eine ausführliche Beschreibung der Kommandos gibt `man smbclient`.

```
user$  smbclient -U name -W wgname \\\\jupiter\\myshare
Password:  xxxxxx
smb: >  ls
  .                   D        0  Thu Sep  7 17:38:02 2010
  ..                  D        0  Thu Sep  7 17:38:02 2010
  data                D        0  Wed Apr  5 18:17:11 2010
  file.xy            AR      226  Sat Dec 14 00:00:00 2010
```

Debugging mit »smbclient«

Zur Fehlersuche können Sie `smbtree` mit der Option `-d10` ausführen. Sie erhalten dann alle möglichen Debugging-Ausgaben. Mitunter scheitert der Samba-Zugriff daran, dass es im Netzwerk keinen Computer bzw. kein Gerät gibt, das als Master-Browser agiert. Abhilfe kann dann entweder ein echter Windows-Rechner schaffen oder natürlich ein Linux-Rechner, auf dem Samba läuft.

smbtree

Das Kommando `smbtree` liefert eine baumförmige Liste aller im Netzwerk zu findenden Windows- und Samba-Server inklusive aller von diesen Servern freigegebenen Objekte. Normalerweise verwendet `smbtree` den aktuellen Benutzernamen und fragt nach einem dazugehörenden Passwort. Mit `-user=name%passwort` können Sie diese Daten beim Aufruf des Kommandos einstellen. Um Ressourcen zu finden, die ohne Passwort zugänglich sind, verwenden Sie die Option `-N`. Das folgende Listing zeigt zwei Rechner (`kofler-desktop` und `ubuntu-test`), eine virtuelle Maschine (`merkurvm`) sowie eine NAS-Festplatte (`wd-nas`), die sich alle in der Arbeitsgruppe `WORKGROUP` befinden.

```
root#  smbtree
Enter kofler's password:  ********
WORKGROUP
        \\KOFLER-DESKTOP                    kofler-desktop server (Samba, Ubuntu)
                \\KOFLER-DESKTOP\mydata
                \\KOFLER-DESKTOP\IPC$       IPC Service (kofler-desktop server)
                \\KOFLER-DESKTOP\print$     Printer Drivers
        \\MERKURVM                          merkurvm
                \\MERKURVM\images
                \\MERKURVM\data
                \\MERKURVM\SharedDocs
        \\UBUNTU-TEST                       ubuntu-test server (Samba, Ubuntu)
                \\UBUNTU-TEST\IPC$          PC Service (ubuntu-test server ...)
                \\UBUNTU-TEST\print$        Printer Drivers
        \\WD-NAS                            My Book World Edition Network Storage
                \\WD-NAS\IPC$               IPC Service (My Book ...)
                \\WD-NAS\Configuration      System Configuration
                \\WD-NAS\multimedia
                \\WD-NAS\Download           Download Share
                \\WD-NAS\Public             Public Share
```

Windows-Clients

Bei älteren Windows-Versionen finden Sie sämtliche Samba-Server direkt in der Netzwerkansicht des Windows Explorers bzw. des Dateiauswahldialogs. Allerdings kann es mehrere Minuten lang dauern, bis ein neu installierter oder neu konfigurierter Samba-Server sichtbar wird. Am schnellsten und sichersten ist es, den Windows-Rechner einfach neu zu starten.

LLTD

Aktuelle Windows-Versionen ab Vista erkennen leider weder den Samba-Server noch ältere Windows-Server im lokalen Netzwerk. Schuld ist ein neues Protokoll zum Austausch der Netzwerkdaten, nämlich *Link Layer Topology Discovery* (kurz LLTD). Dieses Protokoll wäre an sich eine feine Sache, weil es wesentlich schneller als bisherige Verfahren funktioniert. Leider wird es momentan weder von Samba noch von älteren Windows-Versionen unterstützt. Weitere Informationen zu LLTD finden Sie hier:

http://support.microsoft.com/kb/922120
http://msdn.microsoft.com/en-us/windows/hardware/gg463099.aspx

Glücklicherweise ist auch ohne automatische Erkennung ein Zugriff auf nicht-LLTD-konforme Netzwerkgeräte möglich: Geben Sie in der Adresszeile des Windows Explorers einfach den Rechnernamen in der Form *\\name* manuell ein (siehe Abbildung 31.2).

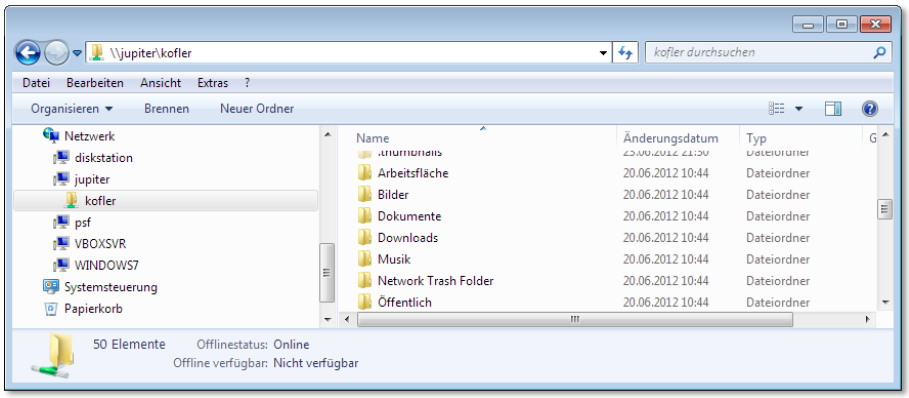


Abbildung 31.2 Unter Windows auf Samba-Verzeichnisse zugreifen

OS X

OS X ist grundsätzlich SMB-kompatibel. Bis OS X 10.6 (Snow Leopard) basierten die SMB-Funktionen auf Samba. Seit OS X 10.7 (Lion) verwendet das Apple-Betriebssystem hingegen eine eigene Implementierung. Leider sieht der OS X-Dateimanager *Finder* im lokalen Netzwerk verfügbare OS X-Server in der Regel nicht. Um einen Verbindungsaufbau durchzuführen, führen Sie im Finder GEHE ZU • MIT SERVER VERBINDEN aus bzw. drücken cmd+K. Anschließend geben Sie als Adresse `smb://hostname` an. In zwei weiteren Dialogen können Sie dann das gewünschte Verzeichnis auswählen und die Login-Daten angeben.

SMB versus AFP

Wenn ein Server Verzeichnisse sowohl über SMB als auch über das Apple-eigene Protokoll AFP anbietet, entscheidet sich OS X bis Version 10.8 standardmäßig für AFP, ab OS X 10.9 dagegen für SMB. Wie Sie einen AFP-Server auf der Basis von Netatalk einrichten, ist Thema des folgenden Kapitels.

Kapitel 32
NFS und AFP

Das im vorigen Kapitel vorgestellte Server-Message-Block-Protokoll bzw. das darauf basierende Programm Samba hat sich zum großen gemeinsamen Nenner beim Dateiaustausch zwischen allen Betriebssystemen entwickelt. Daneben gibt es aber noch andere Verfahren. Im Mittelpunkt dieses Kapitels stehen das »klassische« Unix-Protokoll NFS (Network File System) sowie das unter OS X bevorzugte AFP (Apple Filing Protocol).

32.1 NFS 4

Das *Network File System* (NFS) ermöglicht es, lokale Verzeichnisse anderen Rechnern im lokalen Netzwerk zur Verfügung zu stellen. Anders als bei SMB (Samba) wird das Netzwerkverzeichnis auf dem Client-Rechner durch `mount` bzw. durch eine entsprechende Zeile in `/etc/fstab` direkt in das Dateisystem eingebunden. Sie können ein NFS-Verzeichnis also nicht komfortabel im Dateimanager auswählen und mit ein paar Mausklicks darauf zugreifen. NFS ist vielmehr für eine selten wechselnde Netzwerkkonfiguration gedacht, wo die Client-Rechner ständigen Zugriff auf den NFS-Server benötigen.

Die Basisfunktionen für NFS werden direkt vom Kernel zur Verfügung gestellt, um auf diese Weise eine optimale Geschwindigkeit zu erzielen. Alternativ gibt es auch einen User-Space-NFS-Server, der aber kaum im Einsatz ist und auf den ich in diesem Kapitel nicht eingehe.

Die in den Kernel integrierten NFS-Funktionen unterstützen die NFS-Versionen 3 und 4. NFS 4 gilt mittlerweile als vollständig ausgereift und ist im Regelfall vorzuziehen. Nur in Sonderfällen, etwa wenn Sie es mit sehr alten Client-Rechnern zu tun haben, die NFS 4 nicht unterstützen, sollten Sie den Einsatz von NFS 3 in Betracht ziehen.

Server-Konfiguration

Der Linux-Kernel unterstützt NFS 4 standardmäßig. Dennoch müssen Sie zur Nutzung von NFS die Pakete `nfs-common` und `nfs-kernel-server` (Debian, Ubuntu) bzw. das Paket `nfs-utils` (Fedora, RHEL, SUSE) installieren: Die darin enthaltenen Programme und Scripts kümmern sich um den automatischen Start der erforderlichen Netzwerkdienste.

Eine entscheidende Voraussetzung für den Betrieb eines NFS-4-Servers besteht darin, dass der Dienst `rpc.idmapd` läuft. Dieses Programm stellt die Zuordnung zwischen NFS-Benutzernamen und UIDs/GIDs her. Wie der Dienst gestartet wird, variiert je nach Distribution:

- Unter Debian ist für den Start von `rpc.idmapd` das Init-V-Script `nfs-common` verantwortlich. Es startet den Dienst automatisch, wenn die Datei `/etc/exports` existiert (Server) oder wenn `/etc/fstab` die Zeichenkette `nfs4` enthält (Client). Bei Bedarf können Sie den Start auch erzwingen, indem Sie in `/etc/default/nfs-common` die Einstellung `NEED_IDMAPD=yes` verwenden.
- Unter Fedora führen Sie die beiden folgenden Systemd-Kommandos aus:

```
root#  systemctl start  nfs-idmap.service
root#  systemctl enable nfs-idmap.service
```

- Bei RHEL 6 wird `rpc.imapd` durch `/etc/init.d/nfs` standardmäßig gestartet. Es ist keine spezielle Konfiguration erforderlich.
- Unter SUSE stellen Sie sicher, dass `/etc/sysconfig/nfs` die Einstellung `NFS4_SUPPORT=yes` enthält. Standardmäßig ist das der Fall. `rpc.idmapd` wird dann durch das Init-System gestartet.
- Bei Ubuntu kümmert sich die Upstart-Datei `/etc/init/idmapd.conf` um den Start von `idmapd`.

Netzwerkverzeichnisse vorbereiten

Alle Verzeichnisse, die per NFS freigegeben bzw. »exportiert« werden, müssen einem Wurzelverzeichnis untergeordnet werden, das als Pseudo-Dateisystem dient. Am einfachsten ist das anhand eines Beispiels zu verstehen. Nehmen wir an, Sie wollen die bereits vorhandenen Verzeichnisse `/data/audio`, `/data/fotos` und `/iso-images` exportieren. Dazu erzeugen Sie vier neue Verzeichnisse, wobei `/nfsexport` als Wurzelverzeichnis dient. Der Name dieses Verzeichnisses ist willkürlich. Die Verzeichnisse `/nfsexport/audio`, `/data/fotos` und `/iso` sind leer. Sie dienen nur als Einhängepunkt (*mount point*).

```
root#  mkdir /nfsexport
root#  mkdir /nfsexport/audio
root#  mkdir /nfsexport/fotos
root#  mkdir /nfsexport/iso
```

Nun binden Sie /data/ und /data/fotos als neue nfsexports-Unterverzeichnisse ein. Damit ist der Inhalt von /data/audio nun auch unter /nfsexport/audio sichtbar; analog sehen Sie /data/fotos unter /nfsexport/fotos.

```
root#  mount -t none -o bind /data/audio/  /nfsexport/audio/
root#  mount -t none -o bind /data/fotos/  /nfsexport/fotos/
root#  mount -t none -o bind /iso-images/  /nfsexport/iso/
```

Damit das Einbinden des NFS-Verzeichnisses in Zukunft automatisch erfolgt, fügen Sie in /etc/fstab auf dem Server die folgenden drei Zeilen hinzu:

```
# /etc/fstab
...
/data/audio    /nfsexport/audio  none  bind 0 0
/data/fotos    /nfsexport/fotos  none  bind 0 0
/iso-images    /nfsexport/iso    none  bind 0 0
```

/etc/exportfs

/etc/exports ist die zentrale Konfigurationsdatei für den NFS-Server. Diese Datei steuert, welcher Rechner auf welche Verzeichnisse wie zugreifen darf. Die Rechner können wahlweise durch IP-Nummern oder durch Namen angegeben werden. Subnetze können in der Präfix-Notation angegeben werden, z. B. 192.168.0.0/24. Auch IPv6-Adressen sind zulässig. Rechnernamen dürfen außerdem das Jokerzeichen * enthalten (z. B. *.sol), IP-Adressen aber nicht!

Achten Sie darauf, dass Sie zwischen den IP-Adressen bzw. Hostnamen und den Optionen kein Leerzeichen eingeben! Wenn Sie ein Verzeichnis ohne Einschränkungen für alle Rechner freigeben möchten, die eine Verbindung zum NFS-Server herstellen können, geben Sie einfach das Zeichen * an.

Die folgende Beispieldatei gibt an, dass alle Clients mit IP-Nummern im Netz 192.168.0.* oder mit dem Namen *.lan auf die Verzeichnisse /nfsexport/audio und /nfsexport/fotos zugreifen dürfen. Außerdem dürfen alle Rechner im Netzwerk ohne Einschränkungen bezüglich IP-Adresse oder Hostname auf /nfsexport/iso zugreifen. In den Verzeichnissen audio und iso sind nur Lesezugriffe erlaubt. Die langen Exportdefinitionen wurden hier durch \ über zwei Zeilen verteilt.

```
# Datei /etc/exports für NFS 4
/nfsexport        192.168.0.0/24(rw,async,no_subtree_check,fsid=0,crossmnt) \
                          *.lan(rw,async,no_subtree_check,fsid=0,crossmnt)
/nfsexport/audio  192.168.0.0/24(ro,async,no_subtree_check) \
                          *.lan(ro,async,no_subtree_check)
/nfsexport/fotos  192.168.0.0/24(rw,async,no_subtree_check) \
                          *.lan(rw,async,no_subtree_check)
/nfsexport/iso                *(ro,async,no_subtree_check)
```

IPv6

Wenn Sie den NFS-Server in einem IPv6-Netz verwenden möchten, geben Sie in `/etc/exports` einfach das entsprechende IPv6-Netz an, z. B. 2001:7b8:2ff:8471::/64. Im Gegensatz zu manchen anderen Programmen dürfen IPv6-Adressen nicht in eckige Klammern gesetzt werden!

Optionen in /etc/exports

Die Syntax von `/etc/exports` geht aus dem obigen Listing hervor. Dem Verzeichnis und den Hostnamen bzw. IP-Adressen folgen in Klammern diverse NFS-Optionen, von denen die wichtigsten im Folgenden kurz erläutert werden. Einige weitere Optionen beschreibt `man exports`.

- `ro` (read-only) bzw. `rw` (read-write) geben an, ob nur ein Lese- oder auch ein Schreibzugriff erlaubt ist.
- `sync` bzw. `async` bestimmen den Zeitpunkt, zu dem der NFS-Server die Änderungen von Dateien bestätigt. Standardmäßig gilt `sync`. Das bewirkt, dass eine Bestätigung erst erfolgt, wenn die Datei tatsächlich gespeichert wurde. Viel effizienter, aber weniger sicher ist `async`. Der Geschwindigkeitsunterschied zwischen `sync` und `async` ist bei Schreibzugriffen dramatisch (bis zu Faktor 10), weswegen `async` in der Praxis häufig zum Einsatz kommt.
- `no_subtree_check` bzw. `subtree_check` geben an, ob der NFS-Server den Subtree-Test durchführen soll. Dazu kurz einige Hintergrundinformationen: Wenn ein Verzeichnis eines Dateisystems (nicht aber ein gesamtes Dateisystem) per NFS exportiert wird, stellt der NFS-Server durch den Subtree-Test fest, ob sich die Datei innerhalb des exportierten Verzeichnisses befindet. Der NFS-Server gibt dann Informationen über den tatsächlichen Ort der Datei an den Client weiter. Wird die Datei später auf dem Server umbenannt, führt das oft zu Problemen auf dem Client.

  Aus diesem Grund ist der Subtree-Test in aktuellen NFS-Server-Versionen standardmäßig deaktiviert. Die Option `no_subtree_check` sollte aber dennoch angegeben werden, um eine diesbezügliche Warnung des Servers beim Start zu verhindern.

  Wenn Sie möchten, können Sie den Subtree-Test durch `subtree_check` explizit aktivieren. `man exports` empfiehlt dies vor allem für Verzeichnisse, in denen selten Dateien umbenannt werden und die im Read-Only-Modus exportiert werden.
- `root` darf zwar wie jeder andere Benutzer NFS nutzen, hat aber aus Sicherheitsgründen in den importierten Verzeichnissen nur die Rechte des Benutzers `nobody` (UID=65534 und GID=65534). Wenn Sie `root` die üblichen Rechte geben möchten, müssen Sie in `/etc/exports` die Option `no_root_squash` angeben.

- Das NFS-4-Wurzelverzeichnis muss durch die Option `fsid=0` gekennzeichnet werden. Es darf nur ein Wurzelverzeichnis geben! Es ist mit NFS 4 nicht möglich, Verzeichnisse zu exportieren, die sich außerhalb des Wurzelverzeichnisses befinden.
- Die `crossmnt`-Option wird ebenfalls nur beim Wurzelverzeichnis angegeben. Sie bewirkt, dass beim Einbinden von Unterverzeichnissen deren Inhalt bei den Clients auch dann sichtbar ist, wenn das Wurzelverzeichnis auf dem Client nicht eingebunden ist. Statt der `crossmnt`-Option beim Wurzelverzeichnis können Sie auch die `nohide`-Option bei allen Unterverzeichnissen angeben – Sie erzielen damit denselben Effekt.

exportfs -a

Wenn der NFS-Server bereits läuft, müssen Sie nach jeder Änderung in `/etc/exports` das Kommando `exportfs -a` ausführen. Es stellt sicher, dass der NFS-Server die geänderten neuen Einträge berücksichtigt.

```
root#  exportfs -a
```

Distributionsspezifische Einstellungen

Neben den standardisierten Konfigurationsdateien können Sie je nach Distribution zusätzlich individuelle Einstellungen vornehmen:

Debian, Ubuntu: `/etc/defaults/nfs-common`, `/etc/defaults/nfs-kernel-server`
Fedora, SUSE, RHEL: `/etc/sysconfig/nfs`

Start

Debian und Ubuntu starten den NFS-Server nach der Installation standardmäßig. Bei Fedora, Red Hat und SUSE müssen Sie wie bei anderen Init-Diensten durch die folgenden Kommandos nachhelfen (siehe auch Abschnitt 16.5):

```
root#  systemctl start  nfs-server.service   (Fedora)
root#  systemctl enable nfs-server.service
root#  chkconfig --level 35 nfs on           (RHEL)
root#  service nfs start
root#  insserv nfs                           (SUSE)
root#  service nfs start
```

UID- und GID-Mapping

NFS 4 verwendet standardmäßig Benutzer- und Gruppennamen zum ID-Mapping. Eine Datei, die auf dem NFS-Server dem Benutzer `hofer` gehört, darf auf dem NFS-Client-Rechner ebenfalls vom Benutzer `hofer` gelesen und verändert werden. Server-Benutzer und -Gruppen, die auf dem Client nicht existieren, werden dort dem Benutzer und der Gruppe `nobody` zugeordnet.

Grundsätzlich ist das ID-Mapping von NFS 4 zwar wesentlich intelligenter als jenes von NFS 3, wo einzig die UID- und GID-Nummern als Grundlage verwendet werden. Dennoch ist das Mapping auch unter NFS 4 nicht frei von Tücken: Sie müssen unbedingt sicherstellen, dass Benutzer im gesamten Netzwerk auf allen Rechnern exakt dieselben Account-Namen haben!

Für das UID- und GID-Mapping ist der bereits erwähnte Dämon `rpc.idmapd` verantwortlich. Dessen Konfiguration erfolgt durch `/etc/idmapd.conf`. Für die in diesem Kapitel beschriebene Minimalkonfiguration von NFS 4 können Sie die Datei so lassen, wie sie von Ihrer Distribution vorgegeben ist.

Firewall

Bei NFS 4 erfolgt die gesamte Kommunikation über den TCP-Port 2049. Wenn Ihr Server durch eine Firewall abgesichert ist, müssen Sie diesen Port im lokalen Netzwerk freigeben.

NFS 4 mit LDAP und Kerberos

In diesem Abschnitt habe ich die Server-Konfiguration ohne ein Authentifikationssystem beschrieben – also den einfachsten Weg, um NFS 4 in Betrieb zu nehmen. In großen Netzwerken mit vielen Benutzern werden Sie NFS 4 zumeist mit LDAP und Kerberos verbinden wollen. Auf diese ziemlich komplexe Konfiguration kann ich hier aus Platzgründen nicht eingehen. Sie finden entsprechende Anleitungen im Internet, beispielsweise hier:

http://www.itp.uzh.ch/~dpotter/howto/kerberos
http://wiki.debian.org/nfs4-kerberos-ldap
http://www.danbishop.org/2012/06/02/ubuntu-12-04-ultimate-server-guide

Client-Konfiguration

Damit NFS 4 auf einem Client-Rechner genutzt werden kann, muss je nach Distribution das Paket `nfs-common` (Debian, Ubuntu), `nfs-utils` (Fedora, RHEL) oder `nfsclient` (SUSE) installiert sein. Außerdem muss der Dämon `rcp.idmapd` laufen.

mount und umount

Damit Sie das Netzwerkverzeichnis nutzen können, müssen Sie es mit `mount` in den Verzeichnisbaum integrieren. Die folgenden Kommandos integrieren den gesamten `nfsexport`-Verzeichnisbaum an der Stelle `/media/nfsdata` in das lokale Dateisystem. Dabei müssen Sie `jupiter` durch den Hostnamen des NFS-Servers ersetzen. Beachten Sie, dass Sie das NFS-Wurzelverzeichnis einfach mit `/` adressieren müssen, nicht mit `/nfsexport`!

```
root#  mkdir /media/nfsdata
root#  mount -t nfs4 jupiter:/ /media/nfsdata
root#  ls /media/nfsdata
audio  fotos iso
```

Alternativ können Sie auch nur ein Teilverzeichnis importieren:

```
root#  mkdir /media/fotos
root#  mount -t nfs4 jupiter:/fotos /media/fotos
```

Mit `umount` wird das NFS-Verzeichnis wieder aus dem lokalen Dateisystem entfernt. Wenn die Netzwerkverbindung gerade unterbrochen ist, sollten Sie `umount` mit der Option `-f` ausführen. Sonst müssen Sie sehr lange warten, bis `umount` ausgeführt wird!

```
root#  umount /media/fotos
root#  umount /media/nfsdata
```

Tipp

Unter openSUSE verwenden Sie zum Einrichten von NFS-Verzeichnissen am besten das YaST-Modul Netzwerkdienste • NFS-Client.

/etc/fstab

Um NFS-Verzeichnisse beim Rechnerstart automatisch in das Dateisystem zu integrieren, ergänzen Sie `/etc/fstab` um eine Zeile nach dem folgenden Muster. In der vierten Spalte können Sie die NFS-spezifische Option `bg` verwenden. Sie erreichen damit, dass `mount` im Hintergrund versucht, das Netzwerkverzeichnis einzubinden, wenn dieses nicht sofort zur Verfügung steht. Das ist vor allem beim Einbinden von Netzwerkverzeichnissen während des Rechnerstarts praktisch.

```
# Ergänzung in /etc/fstab
jupiter:/fotos    /media/fotos  nfs4  bg  0  0
```

automount/ autofs

Wenn es in einem großen Netzwerk viele NFS-Verzeichnisse gibt, ist es selten zweckmäßig, einfach alle per `/etc/fstab` zu aktivieren. Das kostet Zeit und Ressourcen, auch wenn die meisten Verzeichnisse dann gar nicht verwendet werden. Viel besser ist es, die Verzeichnisse erst bei der ersten Benutzung automatisch in den Verzeichnisbaum einzubinden. Diese Aufgabe übernimmt bei vielen Distributionen das Paket `autofs` bzw. `autofs4`.

Fehlersuche

Wenn das `mount`-Kommando auf dem Client scheitert, sollten Sie zur Fehlersuche die folgenden Punkte abarbeiten:

- Die Verbindung zwischen Server und Client darf nicht durch eine Firewall blockiert werden. Relevant für NFS 4 ist der TCP-Port 2049.
- Der Dämon `rpc.idmapd` muss sowohl auf dem Server als auch auf dem Client laufen. Überzeugen Sie sich davon mit `ps ax | grep idmapd`.
- Auf dem Server muss der NFS-Server laufen. Das stellen Sie mit `rpcinfo -p` fest. Die folgenden Zeilen beweisen, dass der NFS-Server für die NFS-Versionen 2, 3 und 4 läuft:

```
root#  rpcinfo -p | grep nfs
   program vers proto   port  service
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    ...
```

- Überprüfen Sie mit `showmount -e`, welche Verzeichnisse für NFS freigegeben sind. Lassen Sie sich dabei von den Angaben `*` bzw. `everyone` nicht irritieren – `showmount` ist nicht in der Lage, detaillierte Zugriffsregeln auszuwerten:

  ```
  user@nfsserver$  showmount -e
  /nfsexport       (everyone)
  /nfsexport/audio (everyone)
  /nfsexport/fotos (everyone)
  /nfsexport/iso   *
  ```

  Sie können `showmount` auch auf dem Client-Rechner ausführen, müssen dann aber den Hostnamen des NFS-Servers angeben:

  ```
  user$client#  showmount -e <nfsserver>
  ```

- Stellen Sie sicher, dass sich Client und Server im selben Netzwerksegment befinden.

32.2 NFS 3

Obwohl es NFS 4 schon seit vielen Jahren gibt, ist NFS 3 noch immer weit verbreitet. Das hat nicht zuletzt mit der äußerst einfachen Konfiguration zu tun. Gegen NFS 3 sprechen aber eine ganze Reihe von Gründen:

- Die Zuordnung von Dateibesitzern und -gruppen erfolgt auf Basis der ID-Nummern. Eine Datei, die auf dem Server dem Benutzer mit der UID 1000 gehört, hat auch auf dem Client diese UID-Nummer – selbst dann, wenn der Account-Name der UID 1000 auf dem Server ein ganz anderer ist als der Account-Name der UID 1000 auf dem Client. Der Einsatz von NFS 3 setzt somit voraus, dass auf allen Rechnern im lokalen Netzwerk dieselben UID- und GID-Nummern verwendet werden!
- Die Absicherung durch eine Firewall ist wesentlich schwieriger. NFS 3 verwendet die Protokolle TCP und UDP auf den Ports 111 (`portmap`) und 2049 (`nfsd`) sowie auf zufällig freien Ports (`rpc.*d`).
- Die Locking- und Mounting-Funktionen sind nicht direkt in NFS 3 integriert, sondern müssen von Zusatzprogrammen übernommen werden (`portmap` und `rpc.mountd`).

- NFS 3 kümmert sich nicht um den Zeichensatz der Dateinamen. Wenn auf dem Server und den Clients unterschiedliche Zeichensätze gelten, werden die Dateinamen falsch dargestellt. Unter Linux ist das in der Regel kein Problem, weil alle gängigen Linux-Distributionen seit vielen Jahren den Unicode-Zeichensatz UTF8 verwenden.
- NFS 3 unterstützt weder ACLs noch die Authentifizierung durch Kerberos oder SPKM-3.

Links

Ein ausgezeichnetes HOWTO zum Thema NFS 3 mit vielen Tuning- und Sicherheitstipps finden Sie auf der folgenden Webseite. Beachten Sie aber, dass NFS 4 dort nicht berücksichtigt wird.

http://nfs.sourceforge.net/nfs-howto

Server-Konfiguration

/etc/exports

Die Konfiguration eines Servers für NFS 3 ist einfacher als bei NFS 4: Es ist nicht erforderlich, alle zu exportierenden Verzeichnisse zuerst in einem eigenen Verzeichnis per `mount` zu sammeln. Stattdessen können Sie die Verzeichnisse ohne lange Vorbereitungsarbeiten direkt in `/etc/exports` aufzählen. Davon abgesehen ist die Syntax nahezu die gleiche wie bei NFS 4.

Einzig bei den Export-Optionen gibt es zwei Unterschiede:

- Die Optionen `fsid` und `crossmnt` sind für NFS 3 nicht relevant.
- Dafür muss die Option `insecure` verwendet werden, wenn der NFS-Server auch für Apple-Rechner unter OS X zugänglich sein soll. Die Option bewirkt, dass der NFS-Server auch auf Client-Anfragen reagiert, die von einem IP-Port größer 1024 stammen. Bei NFS-Clients unter OS X ist das der Fall.

Das folgende `exports`-Beispiel exportiert dieselben drei Verzeichnisse wie beim NFS-4-Beispiel:

```
# Datei /etc/exports für NFS 3
/data/audio  192.168.0.0/24(ro,async,no_subtree_check) \
                    *.lan(ro,async,no_subtree_check)
/data/fotos  192.168.0.0/24(rw,async,no_subtree_check) \
                    *.lan(rw,async,no_subtree_check)
/data/iso-images          *(ro,async,no_subtree_check)
```

exportfs -a

Wie bei NFS 4 müssen Sie auch bei NFS 3 nach Änderungen in der `exports`-Datei das Kommando `exportfs -a` ausführen:

```
root#  exportfs -a
```

UIDs und GIDs

NFS 3 verwendet UIDs und GIDs zur Verwaltung der Zugriffsrechte auf Dateien und Verzeichnisse. Das ist einfach, funktioniert aber nur dann zufriedenstellend, wenn es auf dem Server und auf allen Clients eine einheitliche Zuordnung zwischen Benutzern, Gruppen und deren ID-Nummern gibt.

Bei einer manuellen Benutzerverwaltung lassen sich einheitliche UIDs und GIDs nur mit großer Sorgfalt erreichen: Beim Anlegen jedes neuen Benutzers auf jedem Rechner müssen UIDs und GIDs manuell festgelegt werden; außerdem brauchen Sie eine zentrale Referenz über alle bereits vergebenen UIDs und GIDs. Fehler oder Schlampereien bei der Benutzerverwaltung führen sofort zu unerwünschten Konsequenzen: Wenn beispielsweise der Benutzer `peter@merkur` und die Benutzerin `birgit@neptun` auf ihren Rechnern jeweils die UID 1234 haben, haben beide Benutzer im NFS-Verzeichnis dieselben Zugriffsrechte. Das ist selten gewollt!

Die früher übliche Lösung bestand darin, die Dateien `/etc/passwd`, `/etc/group` und `/etc/shadow` mittels NIS (*Network Information Services*) auf allen Rechnern im lokalen Netzwerk zu synchronisieren. NIS war zwar relativ leicht einzurichten, gilt aber als veraltet und unsicher.

Wesentlich besser ist es, die Benutzerdaten (Login-Name, Passwort, Gruppenzugehörigkeiten, UIDs und GIDs etc.) mit einem LDAP-Dienst zentral zu verwalten. LDAP steht für *Lightweight Directory Access Protocol*, ein Protokoll zur Verwaltung hierarchischer Daten. Als LDAP-Server kommt unter Linux in der Regel openLDAP zum Einsatz. Leider ist die Konfiguration und die Verwaltung eines LDAP-Servers relativ aufwendig.

Firewall

Um den Zugriff auf einen NFS-3-Server zu sperren, müssen Sie nur die Ports 111 und 2049 für die Protokolle TCP und UDP blockieren. Umgekehrt ist es leider unmöglich, ein vollständig blockiertes System nur für NFS 3 freizuschalten: NFS 3 verwendet neben den Ports 111 und 2049 nämlich auch zufällige, gerade freie Ports. Abhilfe schafft die fixe Zuordnung von Ports für die Dienste `statd`, `lockd` und `mountd`, in RHEL z. B. in der Datei `/etc/sysconfig/nfs`:

http://www.gotdoug.com/?p=3
https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Storage_Administration_Guide/s2-nfs-nfs-firewall-config.html

/etc/hosts.allow, /etc/hosts.deny

Die Dateien `hosts.allow` und `hosts.deny` geben an, welche Rechner auf den NFS-3-Server zugreifen dürfen. Die Informationen in `/etc/exports` sind nur für die Benutzer relevant, die den NFS-Server überhaupt kontaktieren können. Insofern stehen `hosts.allow` und `hosts.deny` in der Hierarchie des Zugriffsschutzes an erster Stelle. Die Syntax der Dateien ist in Abschnitt 40.2 beschrieben. Für den NFS-Server sind die Einträge `portmap` und `mountd` relevant.

Beachten Sie, dass `/etc/hosts.allow` und `-.deny` nur von NFS-3-Servern berücksichtigt werden, nicht aber von NFS-4-Servern!

Mit dem Kommando `showmount -a` ermitteln Sie eine Liste aller aktiven NFS-Clients. Beachten Sie, dass dieses Kommando nur für NFS-3 gilt! Verzeichnisse, die der Server per NFS 4 freigibt, erscheinen nicht im Ergebnis. mount-Status

Client-Konfiguration

Die Client-Konfiguration für NFS 3 unterscheidet sich nur minimal von der für NFS 4. Als Grundvoraussetzung müssen Sie je nach Distribution auf dem Client die Pakete `nfs-common` (Debian, Ubuntu), `nfs-utils` (Fedora, RHEL) oder `nfsclient` (SUSE) installieren. Wenn Sie `mount` manuell ausführen, geben Sie als Dateisystemtyp `nfs` anstelle von `nfs4` an. Außerdem müssen Sie den vollständigen Pfad des Verzeichnisses auf dem NFS-Server angeben:

```
root#  mount -t nfs jupiter:/data/fotos /media/fotos
```

Dieselben Regeln gelten auch für Einträge in `/etc/fstab`:

```
# Ergänzung in /etc/fstab
jupiter:/data/fotos    /media/fotos  nfs  bg  0  0
```

32.3 Apple Filing Protocol

Das *Apple Filing Protocol* (kurz AFP) ist ein Netzwerkprotokoll zum Zugriff auf Dateien und Verzeichnisse über das Netzwerk. AFP kommt standardmäßig zum Einsatz, wenn mehrere Apple-Computer in einem lokalen Netzwerk Dateien austauschen möchten.

Vielleicht fragen Sie sich: »Wozu AFP, OS X unterstützt doch auch SMB?« Prinzipiell stimmt das, und ab Herbst 2013 wird SMB in OS X 10.9 sogar zum bevorzugten Protokoll für Netzwerkverzeichnisse. Bei älteren OS X-Versionen war AFP aber zumeist deutlich schneller als SMB. Außerdem ist AFP das einzige Protokoll, um Backups mit der *Time Machine* in Netzwerken durchzuführen.

Für die Nachbildung des Apple Filing Protocols ist das Open-Source-Programm Netatalk verantwortlich. Entsprechende Pakete stehen in allen gängigen Distributionen zur Verfügung. Netatalk kommt auch in nahezu allen NAS-Geräten (Network Attached Storage) zum Einsatz. Netatalk

In diesem Abschnitt erfahren Sie, wie Sie Netatalk so einrichten, dass OS X-Rechner im lokalen Netzwerk Dateien lesen und speichern und Ihren Linux-Server als Backup-Medium verwenden können. Netatalk bietet darüber hinaus unzählige

Optionen und Konfigurationsvarianten, die nur in Sonderfällen relevant sind und auf die ich deswegen nicht eingehe. Werfen Sie gegebenenfalls einen Blick in das eher dürftige Online-Handbuch auf der Netatalk-Website:

http://netatalk.sourceforge.net

Versionen

Dieses Kapitel bezieht sich auf die Netatalk-Versionen 2.*n*, die momentan die größte Verbreitung haben. Version 3.0 wurde zwar schon im Juli 2012 fertiggestellt, im Sommer 2013 verwendeten aber alle in diesem Buch behandelten Distributionen Netatalk 2.2, sogar Fedora und Ubuntu, die sonst oft die neuesten Software-Versionen einsetzen.

afpd.conf

Die Konfigurationsdateien für Netatalk befinden sich im Verzeichnis `/etc/netatalk`. Von zentraler Bedeutung ist die Datei `afpd.conf`. In ihr werden zeilenweise die Server definiert, die Netatalk abbilden soll. Netatalk kann also prinzipiell mehrere virtuelle Server ausführen; in meinen Tests hat das aber nicht funktioniert.

Der erste Server gilt als Default-Server. Sein Name wird durch einen einfachen Bindestrich angegeben. Auf den Apple-Clients wird in diesem Fall der Hostname des Servers angezeigt. Die Namen aller weiteren Server geben Sie am besten in Anführungszeichen an.

```
# Syntax in /etc/netatalk/afpd.conf
-         [optionen]
"server2" [optionen]
"server3" [optionen]
...
```

Im Regelfall brauchen Sie nur einen virtuellen Server. Für erste Experimente ist es zweckmäßig, einfach die am Ende der Konfigurationsdatei bereits vorgesehene Zeile zu aktivieren. Dazu müssen Sie lediglich das Kommentarzeichen entfernen:

```
# Default-Einstellung für /etc/netatalk/afpd.conf
- -tcp -noddp -uamlist uams_dhx.so,uams_dhx2.so
```

Ab der Netatalk-Version 2.2.3 sehen die Defaulteinstellungen so aus:

```
# Default-Einstellung für /etc/netatalk/afpd.conf
- -tcp -noddp -uamlist uams_dhx_passwd.so,uams_dhx2_passwd.so
```

Diese Standardkonfiguration gilt auch dann, wenn `afpd.conf` leer ist bzw. ausschließlich aus Kommentarzeilen besteht. Netatalk kommuniziert mit diesen Einstellungen nur über das TCP/IP-Protokoll, nicht aber über das veraltete AppleTalk-Protokoll (Option `-noddp`).

`-uamlist` zählt auf, welche Authentifizierungsmethoden (User Authentication Modules) akzeptiert werden sollen, nämlich das Diffie-Hellman-eXchange-Verfahren in

den Versionen 1 und 2. Das Verfahren DHX2 ist ab OS X 10.7 zwingend erforderlich! Noch sicherer wird Netatalk, wenn Sie `uams_dhx.so` aus der Liste der Authentifizierungsmodule entfernen. OS X unterstützt bereits seit Version 10.2 das DHX2-Verfahren.

Fedora- und Ubuntu-Eigenheiten

Fedora und Ubuntu ignorieren die Option `-uamlist` in `afpd.conf`! Stattdessen sind die Authentifizierungsmodule fix eingestellt, in Ubuntu durch die Variable `AFPD_UAMLIST` im Init-V-Script `/etc/init.d/netatalk` und in Fedora durch die gleiche Variable im Script `/usr/libexec/netatalk/netatalk.sh`.

In Fedora 18 und 19 ist die Defaulteinstellung zu allem Überfluss falsch! Dort kommt Netatalk 2.2.3 zum Einsatz. In dieser Version wurden die UAMS-Module umbenannt. Netatalk funktioniert erst, wenn Sie die folgende Änderung in `/usr/libexec/netatalk/netatalk.sh` durchführen:

```
ADPD_UAMLIST="-U uams_dhc_passwd.so,uams_dhx2_passwd.so"
```

Zur Authentifizierung greift Netatalk auf die Linux-Benutzerverwaltung zurück. Sie müssen also für jeden Benutzer, der von einem Apple-Computer aus auf den Netatalk-Server zugreifen darf, einen entsprechenden Linux-Benutzer einrichten. Dessen Passwort gilt dann gleichermaßen für Linux und Netatalk. Falls Sie Linux-Benutzer nur für Netatalk einrichten, sollten Sie aus Sicherheitsgründen einen direkten Login auf dem Linux-Rechner unterbinden:

```
root#  useradd loginname
root#  passwd loginname
root#  usermod -s /bin/false loginname
```

Avahi und Netatalk

Anders als bei älteren Netatalk-Versionen ist es nicht mehr erforderlich, in einer `*.service`-Datei im Verzeichnis `/etc/avahi/services/` auf die Existenz des Time-Machine-Mediums hinzuweisen. Netatalk kümmert sich seit Version 2.2 selbst um die Bonjour-Kommunikation. Ein zusätzlicher Avahi-Eintrag führt zu Hostname-Kollisionen und dazu, dass der Server nicht als Time-Machine-Medium verwendet werden kann!

AppleVolumes-.default

In der Datei `/etc/netatalk/AppleVolumes.default` werden die via AFP erreichbaren Netzwerkverzeichnisse für den Default-Server zeilenweise aufgezählt. Es ist zulässig, sehr lange Definitionen mit \ über mehrere Zeilen zu verteilen. Default-Einstellungen, die für alle Verzeichnisse gelten sollen, können in einer Zeile angegeben werden, die mit `:DEFAULT:` beginnt.

```
# Syntax in /etc/netatalk/AppleVolumes.default
:DEFAULT: [default-optionen]
pfad1 ["volume-name1"] [optionen]
pfad2 ["volume-name2"] [optionen]
...
```

In den Pfad- und Namensangaben können vordefinierte Variablen verwendet werden, z. B. `$h` für den Hostnamen oder `$u` für den Benutzernamen. Eine vollständige Liste aller Variablen liefert `man AppleVolumes.default`. Standardmäßig sieht Netatalk die folgende Default-Konfiguration vor:

```
# Default-Einstellung in /etc/netatalk/AppleVolumes.default
:DEFAULT: options:upriv,usedots
~/   "Home Directory"
```

Damit kann jeder Benutzer auf das dazugehörende Linux-Heimatverzeichnis zugreifen. Wenn sich ein Mac-Benutzer bei Netatalk also als *huber* mit dem dazugehörenden Linux-Passwort anmeldet, kann er `/home/huber` als Netzwerkverzeichnis nutzen, wobei im Finder (also dem OS X-Dateimanager) als Verzeichnisname *Home Directory* angezeigt wird.

Die Option `upriv` bedeutet, dass für den Zugriff auf die Dateien die Linux-Zugriffsrechte gelten, also die eingestellten rwx-Bits für Benutzer, Gruppe und Andere. Die Option `usedots` bedeutet, dass Punkte in Dateinamen unverändert gespeichert werden. Wenn diese Option aktiv ist, sind der Dateiname `.Parent` sowie alle Dateinamen, die mit `.Apple.` beginnen, nicht zulässig. (Diese Dateien haben unter OS X eine besondere Bedeutung.)

Um zusätzliche Verzeichnisse im Apple-Netzwerk freizugeben, müssen Sie `AppleVolumes.default` um weitere Zeilen ergänzen und Netatalk dann mit `service netatalk restart` neu starten. Dabei können Sie mit `allowXxx`- und `denyXxx`-Optionen steuern, wer die Verzeichnisse benutzen darf und wer nicht. Wenn Sie keine derartigen Optionen angeben, ist das Verzeichnis für jeden sichtbar, der sich authentifizieren kann! Achten Sie darauf, dass im Linux-Dateisystem die Zugriffsrechte für die Verzeichnisse korrekt eingestellt sind! Die folgenden Zeilen geben einige Beispiele:

```
# Definition weiterer Netzwerkverzeichnisse
# in /etc/netatalk/AppleVolumes.default
...
/data/iso-images  "iso"        allow:benutzer1,benutzer2
/data/multimedia  "Multimedia" allow:@gruppe1,@gruppe2
/data/verz1       "verz1"      allow:peter allowed_host:peters_mac
```

Der Name des Netzwerkverzeichnisses, also der zweite Parameter in `AppleVolumes.default`, darf maximal 27 Zeichen lang sein und keinen Doppelpunkt enthalten.

Mit den Optionen `preexec` und `postexec` besteht die Möglichkeit, vor dem Verbindungsaufbau bzw. nach dessen Ende ein Script auszuführen. Mit `dperm` und `fperm` können Sie einstellen, welche Zugriffsbits neu erzeugte Verzeichnisse oder Dateien haben sollen. `options:ro` bewirkt, dass Dateien im Netzwerkverzeichnis nur gelesen, aber nicht verändert werden können. In einem heterogenen Netzwerk spricht nichts dagegen, ein und dasselbe Verzeichnis sowohl mit Samba via SMB als auch mit Netatalk via AFP freizugeben.

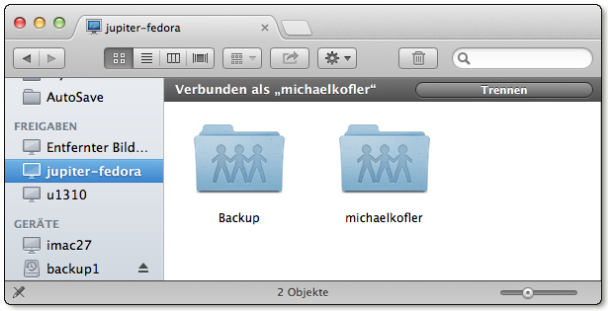


Abbildung 32.1 Auswahl eines AFP-Verzeichnisses im Finder

Wenn Sie in `afpd.conf` mehrere virtuelle Server definieren, sollten Sie für jeden Server eine eigene `AppleVolumes`-Konfigurationsdatei vorsehen. In `afpd.conf` geben Sie in der Server-Zeile mit der Option `-defaultvol` an, welche Konfigurationsdatei für welchen virtuellen Server gilt. Bei meinen Tests ist es mir allerdings nicht gelungen, mehrere virtuelle Server einzurichten. Unter OS X war immer nur ein Server sichtbar.

Time Machine

Damit ein Netatalk-Verzeichnis als Backup-Medium für die Time Machine verwendet werden kann, müssen einige besondere Optionen gesetzt werden. Entscheidend ist insbesondere die `tm`-Option. Die restlichen Optionen gelten normalerweise per Default und sind nur dann wichtig, wenn Sie abweichende Default-Einstellungen verwenden.

```
# Definition eines Backup-Verzeichnisses in /etc/netatalk/AppleVolumes.default
...
/data/tm  "Backup"  allow:benutzer1234  cnidscheme:dbd  options:usedots,upriv,tm
```

Das Time-Machine-Verzeichnis kann grundsätzlich von mehreren Macs parallel genutzt werden, d. h., jeder Mac kann dort Backups ablegen. Für jeden Rechner, der Ihren Linux-Rechner als Backup-Medium verwendet, wird ein Unterverzeichnis mit dem Rechnernamen angelegt. Darin werden dann sogenannte Sparse-Bundle-Dateien erzeugt, die zusammen als Image für ein Apple-Dateisystem (HFS) dienen. Wenn viele kleine Dateien gesichert werden müssen, spart diese Vorgehensweise eine Menge Platz. Außerdem können Apple-Rechner auf diese Weise unabhängig

vom Linux-Dateisystem alle HFS-spezifischen Attribute und Zusatzmerkmale speichern. Der offensichtliche Nachteil besteht aber darin, dass es ohne einen Mac unmöglich ist, auf den Inhalt des Backups zuzugreifen.

Verwenden Sie möglichst eine eigene Partition für Time-Machine-Backups

Im Laufe der Zeit füllt die Time Machine jede noch so große Festplatte vollständig mit Backup-Dateien. Alte Versionen von Backup-Dateien werden erst dann automatisch gelöscht, wenn kein Platz mehr auf der Festplatte ist. Um den Speicherplatz für die Time Machine zu limitieren, ist es daher zweckmäßig, das Time-Machine-Verzeichnis in einer eigenen Partition bzw. einem Logical Volume einzurichten.

Gastzugriff ohne Authentifizierung

Das zusätzliche Authentifizierungsmodul `uams_guest.so` erlaubt den unauthentifizierten Zugriff auf Netzwerkverzeichnisse:

```
# Default-Einstellung für /etc/netatalk/afpd.conf
- -tcp -noddp -uamlist uams_dhx.so,uams_dhx2.so,uams_guest.so -nosavepassword
```

Beachten Sie aber, dass nun alle Verzeichnisse, auf die der Zugriff nicht durch `allowXxx`-Optionen limitiert ist, für jederman frei zugänglich sind! Falls Sie ein öffentliches Verzeichnis nur für den Lesezugriff schaffen möchten, geben Sie in `AppleVolumes.default` zusätzlich `options:ro` an:

```
# Definition eines öffentlichen Verzeichnisses
# in /etc/netatalk/AppleVolumes.default
...
/data/public      "Public"
/data/public-ro   "Public Read-only"   options:ro
```

Firewall, atalkd.conf

Wenn Ihr LAN-Server durch eine Firewall geschützt ist, müssen Sie zur Nutzung von AFP die Ports 427 und 548 freigeben!

Netatalk erkennt normalerweise selbstständig die richtige Netzwerkschnittstelle (zumeist `eth0`). Bei Servern mit mehreren Netzwerkschnittstellen kann es aber erforderlich sein, dass Sie die gewünschte Schnittstelle explizit in `/etc/netatalk/atalkd.conf` angeben müssen:

```
# in /etc/netatalk/atalkd.conf
eth0
```

Kapitel 33
CUPS

Das *Common UNIX Printing System* (kurz CUPS) ist unter Linux für die Verarbeitung und Zwischenspeicherung von Druckjobs und für die Umwandlung der Druckdaten in das Format des Druckers zuständig. Deswegen ist auf jedem Desktop-Rechner standardmäßig CUPS installiert. Dieses Kapitel geht auf einige CUPS-Grundlagen ein und zeigt, wie Sie einen mit dem Server verbundenen Drucker für die anderen Rechner im lokalen Netzwerk zugänglich machen.

Das Drucksystem CUPS steht unter der Lizenz GPL. Der Hauptentwickler von CUPS, Michael Sweet, ist seit einigen Jahren bei Apple angestellt. Apple hat bei dieser Gelegenheit die Rechte an CUPS erworben und kümmert sich um dessen Weiterentwicklung. CUPS kommt also nicht nur unter Linux, sondern auch unter OS X zum Einsatz.

http://www.cups.org

33.1 Grundlagen

Auf einem Desktop-Rechner kommen Sie mit CUPS zumeist nur über die Drucker-Konfigurationsdialoge der Systemeinstellungen in Berührung. Sofern Ihr Drucker CUPS-kompatibel ist, bereitet dessen Konfiguration und Verwendung kaum Probleme. Die folgenden Seiten richten sich in erster Linie an Anwender, die die Grundlagen und Hintergründe des Linux-Drucksystems verstehen möchten.

Generell erfolgt die Druckerverwaltung unter Linux durch einen Netzwerkdienst – auch auf Desktop-Rechnern. Jeder unter Linux eingerichtete Drucker kann daher bei entsprechender Konfiguration auch von allen anderen Rechnern im lokalen Netzwerk genutzt werden.

Ablauf des Druckprozesses

PostScript und PDF

Die gesamte Druckphilosophie unter Unix/Linux basiert auf PostScript-Druckern. PostScript ist eine Programmiersprache zur Beschreibung von Seiteninhalten. PostScript-Drucker erwarten Druckdaten in diesem Format. Fast alle Linux-Programme mit Druckfunktionen senden PostScript-Daten an das Drucksystem.

Seit einigen Jahren vollzieht sich ein Wandel vom PostScript- zum PDF-Format. Salopp formuliert ist PDF eine komprimierte Darstellung einer PostScript-Datei mit einigen Zusatzfunktionen. Da mittlerweile immer mehr Programme PDF-Dateien erzeugen können und immer mehr Drucker PDF-Dateien direkt verarbeiten können, versucht CUPS zunehmend, den Zwischenschritt PostScript zu vermeiden.

Drucker-Devices

Wenn Ihr PostScript-Drucker mit einem USB-Kabel angeschlossen ist, können Sie die PostScript-Datei einfach mit `cp` an das Device der Schnittstelle übertragen:

```
root#  cp datei.ps /dev/usb/lp0     (USB-Schnittstelle)
```

Spooling-Systeme

Nun wollen normalerweise außer `root` auch gewöhnliche Benutzer drucken – möglicherweise auch solche, die an einem anderen Rechner im Netzwerk arbeiten. Und keiner von ihnen möchte sich dabei mit Device-Namen herumärgern. Aus diesem Grund gibt es sogenannte Spooling-Systeme. Sie haben mehrere Aufgaben:

- Sie stellen einfach zu bedienende Kommandos zum Drucken zur Verfügung, dank derer beim Ausdruck kein Device-Name, sondern einfach der Druckername angegeben werden muss.
- Sie erlauben je nach Konfiguration allen Benutzern das Drucken, bei Bedarf auch in einem Netzwerk.
- Sie ermöglichen es, an einen Rechner mehrere Drucker anzuschließen und diese zu verwalten.
- Wenn mehrere Druckaufträge gleichzeitig eintreffen, werden die Aufträge in sogenannten Warteschlangen (Print Queues) zwischengespeichert, bis der Drucker frei ist.
- Außerdem können Spooling-Systeme diverse Zusatzfunktionen übernehmen, etwa eine Protokollierung, wer wie viel druckt etc.

Das modernste und populärste Spooling-System für Linux ist CUPS. In der Vergangenheit kamen statt CUPS beispielsweise BSD-LPD oder LPRng zum Einsatz. Unabhängig vom Spooling-System sieht das Kommando zum Ausdruck einer Datei immer gleich aus:

```
user$  lpr -Pname datei
```

Dabei ist *name* der Name des Druckers (genau genommen: der Name der Druckerwarteschlange). Wenn Sie auf die Option `-P` verzichten, erfolgt der Ausdruck auf dem Standarddrucker.

Drucker-Filter (Ghostscript)

Bis jetzt habe ich vorausgesetzt, dass Sie einen Drucker einsetzen, der PostScript oder möglicherweise sogar PDF direkt unterstützt. In der Praxis kommen aber häufig Drucker zur Anwendung, die nicht PostScript- oder PDF-kompatibel sind. Damit auch solche Drucker unter Linux funktionieren, ist eine Umwandlung der PostScript- oder PDF-Daten in das jeweilige Druckerformat erforderlich. Intern kommt dabei das Programm Ghostscript zum Einsatz (Kommando `gs`).

Um den Aufruf von `gs` kümmert sich ein sogenannter Filter. Das ist ein Programm (ein Script), das Eingabedaten verarbeitet und Ausgabedaten liefert. Der Filter für den Druckprozess muss insbesondere die richtigen Parameter an `gs` weitergeben, also den Namen des Druckermodells, die gewünschte Auflösung, die gewünschte Seitengröße etc. Er wandelt die PostScript-Daten seitenweise in Bitmaps um und gibt diese – zusammen mit den Druckbefehlen des jeweiligen Druckers – weiter.

Ghostscript greift bei seiner Arbeit auch auf externe Druckertreiber zurück. Das wichtigste Treiberprojekt für Linux ist Gutenprint (ehemals Gimp-Print):

http://gimp-print.sourceforge.net

Dokument-Filter

Nun sind PostScript und PDF zwar die bevorzugten Formate aller CUPS-Druckdateien – aber manchmal soll einfach nur eine Text- oder Grafikdatei gedruckt werden. Natürlich können Sie die Textdatei in einen Editor laden, der die Datei dann im PostScript- oder PDF-Format an das Drucksystem weitergibt. Ebenso können Sie die Grafikdatei mit einem Grafikprogramm oder -konverter in die Formate PostScript oder PDF umwandeln.

Noch bequemer ist es aber, auch für derartige Dateien einfach nur `lpr datei` auszuführen. Damit das funktioniert, versucht das Spooling-System, den Typ der zu druckenden Datei zu erkennen. Wenn das gelingt, wird die Datei mit geeigneten Programmen in das PostScript- oder PDF-Format umgewandelt.

Alles zusammen

Sie haben auf Ihrem Rechner einen Tintenstrahldrucker richtig konfiguriert. Der Druckername sei `pluto`. Nun möchten Sie die Grafikdatei `mypicture.png` ausdrucken und führen das folgende Kommando aus:

```
user$ lpr -Ppluto mypicture.png
```

Jetzt laufen die folgenden Operationen ab:

- `lpr` gibt die Datei an das Spooling-System CUPS weiter.
- Dieses gibt die Datei an das Filtersystem weiter.

- Der Filter erkennt den Dateityp (PNG) und wandelt die Bitmap je nach CUPS-Version in eine PostScript- oder PDF-Datei um.
- Diese Datei wird an Ghostscript weitergegeben, das sie in das herstellerspezifische Format des Druckers `pluto` umwandelt.
- Nachdem der Drucker `pluto` alle zuvor gestarteten Druckjobs verarbeitet hat, druckt er `mypicture.png` aus.

33.2 CUPS-Interna

Konfigurationsdateien

Wie die meisten anderen Netzwerkfunktionen ist CUPS als Hintergrundprozess (Dämon) realisiert. Der Drucker-Dämon `cupsd` wird durch das Init-System gestartet. Bei älteren Drucksystemen erfolgte beinahe die gesamte Druckerkonfiguration durch die Datei `/etc/printcap`. Bei CUPS spielt diese Datei dagegen so gut wie keine Rolle mehr. Sie steht zwar aus Kompatibilitätsgründen noch immer zur Verfügung, enthält aber nur eine Liste aller bekannten Warteschlangen (ohne irgendwelche weiteren Parameter). Die eigentliche CUPS-Konfiguration erfolgt durch die Dateien des Verzeichnisses `/etc/cups`. Tabelle 33.1 gibt einen Überblick über die wichtigsten Dateien.

Datei	Inhalt
`classes.conf`	Definition aller Klassen
`cupsd.conf`	zentrale CUPS-Konfigurationsdatei
`lpoptions`	Veränderungen gegenüber der Grundkonfiguration
`printers.conf`	Definition aller Drucker
`ppd/name.ppd`	Konfiguration für die Warteschlange `name`
`.cups/lpoptions`	persönliche Einstellungen (KDE)

Tabelle 33.1 Konfigurationsdateien in /etc/cups

In `cupsd.conf` werden diverse Installationsverzeichnisse eingestellt, der Port des CUPS-Dämons für das *Internet Printing Protocol* (IPP), die Optionen für das Printerbrowsing, Sicherheitsparameter, Zugriffsrechte für Clients im Netzwerk (*allow/deny*) etc.

Das Verzeichnis `/etc/cups/ppd` enthält für jeden in `printers.conf` angeführten Druckernamen die dazugehörende PPD-Datei. Darin sind alle Druckparameter gespeichert, also Druckermodell und -treiber, Einstellungen wie Papiergröße und Auflösung etc.

Wenn der Systemadministrator `root` Druckeroptionen oder Einstellungen verändert, also die Blattgröße, die Druckauflösung, Längs- oder Querformat etc., dann werden diese Veränderungen in der Datei `lpoptions` gespeichert. Die Veränderungen gelten für alle Benutzer, die nicht schon selbst Veränderungen durchgeführt haben. Diese benutzerspezifischen Veränderungen werden in `.cups/lpoptions` gespeichert.

»If it ain't broke, don't fix it.«

CUPS ist ein sehr komplexes System. Verwenden Sie zur Konfiguration nach Möglichkeit die dazu vorgesehenen Werkzeuge. Manuelle Änderungen an der Konfiguration sind nur für CUPS-Profis empfehlenswert. Die in diesem Abschnitt zusammengefassten Informationen sind keinesfalls ausreichend! Mehr Details zur CUPS-Konfiguration finden Sie hier:

http://www.cups.org/documentation.php

MIME

`/usr/share/cups/mime/mime.types` enthält eine Liste aller Dokumenttypen, die von CUPS automatisch erkannt und in PostScript- oder PDF-Dateien umgewandelt werden. Die im gleichen Verzeichnis gespeicherte Datei `mime.convs` gibt an, welcher Filter verwendet werden soll. Die angegebenen Filter müssen sich als ausführbare Dateien in `/usr/lib/cups/filter` befinden.

Nicht erreichbare Drucker

Wenn ein Drucker vorübergehend nicht erreichbar ist, z. B. weil er gerade ausgeschaltet ist, wird er von CUPS *angehalten*. CUPS merkt sich also, dass der Drucker nicht verwendet werden kann. Das Problem: Wird der Drucker später wieder eingeschaltet bzw. verbunden, erkennt CUPS das nicht immer selbstständig. Sie müssen den Drucker explizit reaktivieren. Diese Möglichkeit bieten alle CUPS-Benutzeroberflächen sowie die Kommandos `cupsenable` *druckername* bzw. `lpadmin -E -p` *druckername*.

Um dem Problem ganz aus dem Weg zu gehen, empfiehlt es sich, in `/etc/cups/printers.conf` bei der Beschreibung des Druckers die Zeile `ErrorPolicy retry-job` hinzuzufügen. Einige CUPS-Konfigurationswerkzeuge verwenden diese Einstellung standardmäßig.

PPD-Dateien (PostScript Printer Definition)

Für CUPS sieht jeder Drucker wie ein PostScript- oder PDF-Drucker aus. Druckerspezifische Details wie die Größe des nicht bedruckbaren Seitenrands, die Druckerauflösung, Kommandos für bestimmte Zusatzfunktionen wie den Papiereinzug, Besonderheiten wie der Duplex-Druck etc. werden in PPD-Dateien gespeichert (PostScript Printer Definition). Das PPD-Format wurde von Adobe definiert und kommt auch unter Windows und OS X zum Einsatz.

Da natürlich nicht jeder Drucker tatsächlich ein PostScript- oder PDF-Drucker ist, enthalten CUPS-PPD-Dateien in Form von Kommentaren auch das erforderliche Ghostscript-Kommando inklusive aller Optionen, damit `gs` die Druckdaten in das

Format des Druckers umwandeln kann. Die folgenden Zeilen zeigen einige Auszüge aus einer PPD-Datei für den Tintenstrahldrucker HP DeskJet 6980:

```
*PPD-Adobe: "4.3"
...
*Manufacturer: "HP"
*ModelName: "HP Deskjet 6980 Series hpijs"
*FoomaticIDs: "HP-DeskJet_6980 hpijs"
*FoomaticRIPCommandLine: "gs -q -dBATCH -dPARANOIDSAFER -dQUIET -dNOPAUSE
  -sDEVICE=ijs -sIjsServer=hpijs%A%B%C -dIjsUseOutputFD%Z -sOutputFile=- -"
...
```

Diese Informationen stammen aus der Datenbank `ppds.dat`, die PPD-Einträge für alle Drucker enthält, die CUPS bekannt sind. Die binäre Datei `ppds.dat` befindet sich je nach Distribution z. B. im Verzeichnis `/var/cache/cups`. Wenn Ihr Drucker in dieser Datenbank fehlt und Sie auch kein kompatibles Modell finden, hilft vielleicht eine passende `*.ppd`-Datei aus dem Internet weiter.

Beim Ausdruck extrahiert CUPS aus der `*.ppd`-Datei die Ghostscript-Parameter für den gewünschten Drucker, ruft damit `gs` auf und wandelt so die PostScript-Daten in das Format des jeweiligen Druckers um. Die resultierenden Daten werden dann an das Drucker-Device gesendet.

HPLIP

HP entwickelt im Rahmen des Projekts *HP Linux Imaging and Printing* (kurz HPLIP) selbst freie Druckertreiber für viele seiner Drucker, Scanner und Multifunktionsgeräte. Als Lizenz kommt überwiegend die GPL zum Einsatz, teilweise auch die MIT- oder BSD-Lizenz. HP ist mit dieser aktiven Open-Source-Unterstützung ein leuchtendes Vorbild in der Computer-Industrie. Da viele HP-Drucker auch ohne HPLIP direkt von CUPS unterstützt werden, ist der Einsatz der HPLIP-Funktionen zumeist optional. Weitere Informationen zu HPLIP finden Sie hier:

http://hplipopensource.com

Zu HPLIP gibt es die grafische Benutzeroberfläche `hplip-toolbox`, die sich bei vielen Distributionen in einem eigenen Paket befindet (z. B. `hplip-gui` bei Ubuntu) und extra installiert werden kann. Das Programm erkennt selbstständig angeschlossene HP-Geräte und hilft bei deren Konfiguration und Anwendung. `hp-toolbox` kann unter anderem den Füllstand der Tintenpatronen vieler HP-Tintenstrahldrucker anzeigen – eine Funktion, die CUPS von sich aus nicht bietet.

Klassen

Klassen helfen dabei, in großen Netzwerken einen Drucker-Pool einzurichten. Ein an eine Klasse geleiteter Ausdruck erfolgt dann auf dem ersten freien Drucker dieses Pools.

IPP

CUPS unterstützt das *Internet Printing Protocol* (IPP). Dieses Protokoll vereinfacht die Nutzung von Druckern im Netzwerk über die Grenzen von Linux hinweg ganz erheblich (siehe auch ab Abschnitt 33.4). IPP wird von allen gängigen Betriebssystemen unterstützt. Detaillierte Informationen zu IPP finden Sie unter:

http://www.pwg.org/ipp

Spooling

Alle an den Drucker gesandten Daten werden im Verzeichnis `/var/spool/cups/*` zwischengespeichert, bis der Ausdruck abgeschlossen ist. Beachten Sie, dass Spool-Daten auch bei einem Neustart von Linux nicht verloren gehen. `cupsd` stellt nach dem Neustart fest, dass es noch nicht ausgedruckte Dateien gibt, und wird weiterhin versuchen, die Daten an den Drucker zu übertragen.

TCP-Wrapper

Der Zugriff auf CUPS wird normalerweise durch `/etc/cups/cupsd.conf` gesteuert. CUPS kann aber auch so kompiliert sein, dass zusätzlich die TCP-Wrapper-Bibliothek zum Einsatz kommt. Das überprüfen Sie mit `ldd`:

```
user$  ldd /usr/sbin/cupsd | grep wrap
...
libwrap.so.0 => /lib64/libwrap.so.0 (0x00007fa6e5c6a000)
```

Aus dem obigen Test geht hervor, dass die TCP-Wrapper-Bibliothek verwendet wird. CUPS kann somit nur genutzt werden, wenn dies in `/etc/hosts.deny` nicht verboten oder in `/etc/hosts.allow` explizit erlaubt ist. Standardmäßig sind beide Dateien leer, das Drucken ist also erlaubt. Details zur Konfiguration von `/etc/hosts.allow` und `hosts.deny` finden Sie in Abschnitt 40.2.

CUPS-Webschnittstelle

Grundsätzlich ist es möglich, die CUPS-Konfigurationsdateien mit einem Texteditor zu verändern. Für manche Basiseinstellungen mag das praktikabel sein, ansonsten rate ich davon wegen der großen Komplexität aber ab. Vernünftiger ist es zumeist, lokale Konfigurationswerkzeuge zu nutzen, also die Systemeinstellungen von KDE oder Gnome oder das SUSE-spezifische Programm YaST. Auf Server-Installationen ohne grafische Benutzeroberfläche können Sie zur Konfiguration auch die CUPS-Webschnittstelle verwenden (siehe Abbildung 33.1). Aus Sicherheitsgründen steht diese Schnittstelle nur auf dem lokalen Rechner zur Verfügung. Die folgende Adresse führt zur Startseite:

http://localhost:631

Etwas schwieriger ist es, die Webschnittstelle auf einem anderen Rechner zu nutzen. Es ist möglich, die Konfigurationsdatei `/etc/cups/cupsd.conf` entsprechend anzupassen, was in der Praxis aber oft zu Problemen und Sicherheitslücken führt.

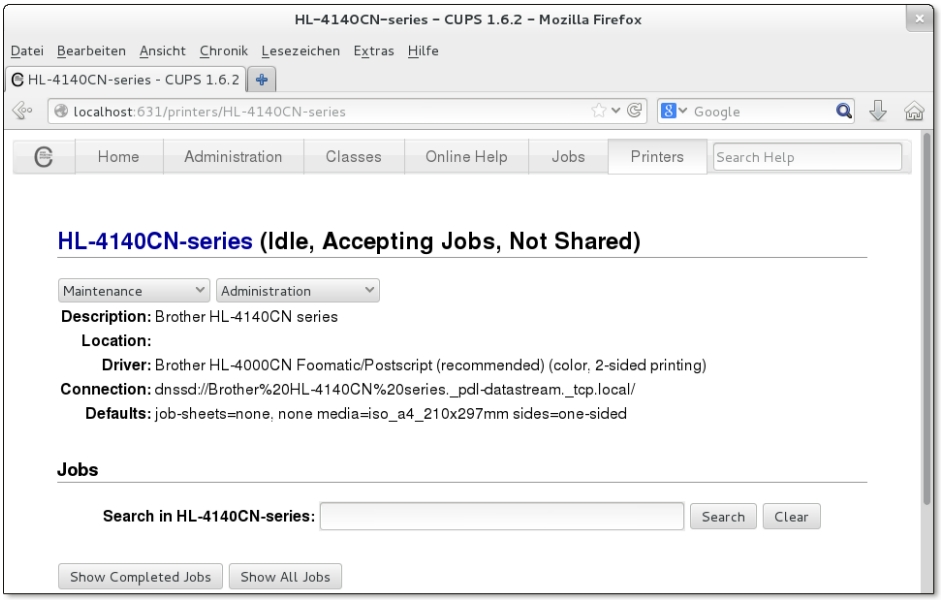


Abbildung 33.1 CUPS-Konfiguration im Webbrowser

Einen wesentlich einfacheren Weg bietet das Kommando `ssh`, das Sie in einem Terminalfenster auf dem lokalen Rechner ausführen: Mit der Option `-L` können Sie den Port 631 des Rechners, auf dem CUPS läuft, auf einen beliebigen Port des lokalen Rechners umleiten.

Solange die SSH-Verbindung besteht, können Sie auf dem lokalen Rechner in einem Webbrowser die CUPS-Webschnittstelle nutzen, wobei Sie die im SSH-Kommando angegebene Portnummer verwenden. Im folgenden Beispiel wird also der Port 631 des CUPS-Rechners auf den Port 6310 des lokalen Rechners (`localhost`) umgeleitet:

```
user@local-machine#  ssh -L 6310:localhost:631 user@cups-hostname
```

Im Webbrowser auf Ihrem lokalen Rechner geben Sie nun die folgende Adresse ein:

http://localhost:6310

Um die administrativen Teile der Webschnittstelle zu nutzen müssen Sie sich mit einem Benutzernamen des CUPS-Rechners und dem dazugehörigen Passwort einloggen. Sie können nun neue Drucker einrichten, Druckjobs verwalten etc. Wenn Sie damit fertig sind, beenden Sie die SSH-Verbindung mit Strg+D.

CUPS-Administration per Kommando

In der Regel werden Sie zum Drucken die Dialoge des jeweiligen Programms verwenden und zur Verwaltung der Druckjobs die entsprechenden Werkzeuge von Gnome oder KDE. Für Freunde der Kommandozeile stehen alternativ diverse Kommandos zur Auswahl, um Dateien zu drucken bzw. Druckjobs zu verwalten. Diese Kommandos sind vor allem dann hilfreich, wenn Sie Druckaufgaben durch Script-Dateien automatisieren möchten.

Die Kommandos `lpr`, `lpq`, `lprm` und `lpc` stehen nicht nur bei CUPS, sondern auch bei BSD-LPD und LPRng zur Verfügung. Das ist gewissermaßen ein gemeinsamer Nenner aller Spooling-Systeme. Beachten Sie aber, dass es Unterschiede bei den unterstützten Optionen gibt.

lpr

Mit `lpr` drucken Sie eine Datei aus. Falls Sie mehrere Drucker eingerichtet haben, geben Sie mit der Option `-P` ohne Leerzeichen den Namen der Warteschlange an. Für den Standarddrucker können Sie auf `-P` verzichten.

```
user$ lpr -Pname datei
```

Falls eine Druckdatei bereits im druckerspezifischen Format vorliegt, übergeben Sie an `lpr` die zusätzliche Option `-l`. Das Kommando umgeht nun das sonst übliche Filtersystem und sendet die Druckerdaten unverändert an den Drucker. Wenn Sie z. B. eine PostScript-Datei auf einem PostScript-Drucker ausdrucken wollen, kann das eine Menge Zeit sparen.

Durch eine Pipe kann `lpr` auch dazu verwendet werden, die Ausgabe eines anderen Kommandos auszudrucken. Das folgende Kommando druckt die mit `ls` ermittelte Dateiliste auf dem Standarddrucker aus:

```
user$ ls -l *.png | lpr
```

Statt `lpr` können Sie auch das Kommando `lp` verwenden (Syntax siehe `man 1 lp`). Dieses Kommando soll Umsteigern von herkömmlichen Unix-Drucksystemen das Leben erleichtern.

lpq, lprm

Alle Druckaufträge, die nicht sofort ausgeführt werden können, werden zwischengespeichert, wobei es für jeden eingerichteten Drucker eine eigene Warteschlange gibt. Den Inhalt der Warteschlange sehen Sie sich mit `lpq -P`*name* an.

Druckjobs, die Sie selbst initiiert haben, können Sie mit `lprm -P`*name* `id` wieder löschen, wobei Sie den Namen der Warteschlange und die ID-Nummer des Jobs angeben müssen. Die richtige Nummer ermitteln Sie vorher mit `lpq`.

```
user$  lpq
FS-1800+ ist nicht bereit
Rang    Besitz  Auftrag Datei(en)                       Gesamtgröße
1st     kofler  20      evince-print                    17408 Byte
2nd     kofler  21      evince-print                    16384 Byte
user$  lprm 20
user$  lprm 21
```

lpc

`lpc` gestattet eine feinere Kontrolle über den Druckvorgang. Nach dem Start dieses Kommandos befinden Sie sich in einer interaktiven Arbeitsumgebung, in der Sie Kommandos wie `status`, `help` etc. ausführen. `topq` verändert die Position eines Druckjobs in der Warteliste. Als Parameter geben Sie den Druckernamen und die Jobnummer an. Ein Teil der Kommandos in `lpc` (so auch `topq`) darf nur von `root` ausgeführt werden. `exit`, `bye` oder `quit` beenden `lpc`.

lpstat, lpinfo, lpadmin, lpoptions

`lpstat` liefert Informationen über alle für CUPS verfügbaren Drucker. `lpinfo` ermittelt eine Liste aller verfügbaren Druck-Devices und Druckertreiber. Mit `lpadmin` richten Sie einen neuen Drucker ein bzw. löschen eine vorhandene Druckerkonfiguration. `lpoptions` zeigt die Optionen von CUPS-Druckern an bzw. verändert sie.

```
user$  lpoptions -o PageSize=A4
```

CUPS deaktiviert Drucker, die nicht erreichbar sind. Um den Drucker wieder zu aktivieren, führen Sie eines der beiden folgenden Kommandos aus:

```
user$  lpadmin -E  druckername
user$  accept  druckername
```

Um einen Drucker explizit zu deaktivieren, nutzen Sie das Kommando `reject`:

```
user$  reject  druckername
```

33.3 Druckerkonfiguration

Bei der Konfiguration des Druckers helfen wahlweise die in Gnome bzw. KDE integrierten Werkzeuge, die CUPS-eigene Webkonfiguration oder spezielle Konfigurationsprogramme Ihrer Distribution.

Druckertreiber

Die entscheidende Frage bei der Druckerkonfiguration ist natürlich, ob Ihr Drucker kompatibel zu Linux bzw. zur Kombination aus CUPS, Ghostscript und dessen Druckertreibern ist. Die folgende Aufzählung fasst zusammen, wie gut verschiedene Druckerkategorien unterstützt werden:

- **Laser-Drucker:** Die meisten Laser-Drucker sind PostScript- oder HP-kompatibel (Druckersprache PCL). Sie sind optimal für den Betrieb unter Linux geeignet. Das gilt auch für die meisten Netzwerkmodelle.
- **GDI-Drucker/Windows-Drucker:** Diese zumeist billigen Laser-Drucker wurden speziell für den Einsatz unter Windows entwickelt. Die Grundidee besteht darin, dass ein Windows-Programm die gesamte zu druckende Seite zuerst vorbereitet und dann an den Drucker überträgt. Beim Seitenaufbau kommt die von Microsoft entwickelte Grafikschnittstelle GDI zum Einsatz. Leider ist das Format zur Datenübertragung zum Drucker zumeist nicht öffentlich dokumentiert. Daher werden viele derartige Drucker unter Linux nicht unterstützt.
- **Tintenstrahl- und Fotodrucker:** Bei Tintenstrahldruckern ist das Ausmaß der Linux-Unterstützung sehr stark vom jeweiligen Modell abhängig. Relativ gut klappt es bei vielen HP-Modellen. Neue Drucker fehlen aber mitunter in der CUPS-Druckerdatenbank noch. Mehr Probleme bereiten in der Regel Tintenstrahldrucker anderer Hersteller.

Wenn Sie vor dem Kauf eines neuen Druckers stehen, lohnt auf jeden Fall ein Blick auf die folgende Website, die zahllose Informationen zum Thema Linux und Drucken enthält. Dazu zählt auch eine umfassende Datenbank der von Linux unterstützten Modelle:

http://www.openprinting.org/printers

TurboPrint

Manche Drucker, zu denen es keinen Open-Source-Treiber gibt, werden vom kommerziellen Druckertreiber der Firma TurboPrint unterstützt. Außerdem können Sie mit TurboPrint bei manchen Fotodruckern bessere Ergebnisse erzielen als mit den Standardtreibern von CUPS. Sie finden den relativ preisgünstigen Treiber auf der folgenden Website:

http://www.turboprint.de

Konfigurationstipps

Unabhängig davon, welches Konfigurationsprogramm Sie einsetzen, sollten die folgenden Tipps weiterhelfen:

- Die automatische Druckererkennung kann nur funktionieren, wenn der Drucker eingeschaltet ist.
- Die Druckerkonfiguration in den Gnome-Systemeinstellungen bietet nur noch ganz wenige Einstellungsmöglichkeiten. Bei vielen Distributionen können Sie alternativ auch das alte Programm `system-config-printer` installieren. Es bietet mehr Optionen und ist wesentlich ausgereifter. Alternativ können Sie die Konfiguration auch im Webbrowser auf der Seite *http://localhost:631* vornehmen.

- Zur manuellen Konfiguration müssen Sie zumindest die Schnittstelle (USB, Netzwerk etc.) und das Druckermodell angeben. Das Druckermodell wählen Sie aus einer riesigen Datenbank aus.

  Falls Ihr Gerät nicht enthalten ist, versuchen Sie ein kompatibles Modell zu finden. Bei PostScript- und HP-kompatiblen Laserdruckern können Sie als Hersteller GENERIC wählen und dann den Standard angeben, z. B. PostScript oder PCL.

  Zu manchen neuen Druckern, die in der CUPS-Modelldatenbank noch nicht enthalten sind, finden Sie im Internet passende `*.ppd`-Dateien. Sie können eine derartige Datei während der Konfiguration laden. Beachten Sie aber, dass nicht jede `*.ppd`-Datei CUPS-kompatibel ist bzw. unter Umständen eine ganz bestimmte CUPS-Version voraussetzt.
- Bei vielen Druckermodellen stehen mehrere Treiber zur Auswahl. Dafür kann es zwei Gründe geben: Erstens unterstützen viele Drucker verschiedene Standards. Zweitens enthält CUPS Druckertreiber aus verschiedenen Projekten (Ghostscript, Gutenprint etc.). Wenn Sie unsicher sind, welcher Treiber die besten Ergebnisse erzielt, richten Sie den Drucker mehrfach unter verschiedenen Namen ein. Anschließend können Sie die verschiedenen Treiber bequem ausprobieren. Die Qualität des Ausdrucks hängt auch davon ab, was Sie drucken möchten – Text, technische Zeichnungen, Fotos etc. Die Druckqualität wird zudem durch die Einstellung der Treiberparameter beeinflusst, z. B. der DPI-Auflösung.
- Fast alle PostScript-Laserdrucker können auch in einem Kompatibilitätsmodus betrieben werden, sodass sie sich wie ein HP-Laserjet-Drucker verhalten. Sie können also Ihren PostScript-Drucker zumeist auch als HP-Laserjet-kompatiblen Drucker konfigurieren. Das bewirkt, dass die Druckdaten von Ihrem Computer in das HP-Laserjet-Format umgewandelt und dann an den Drucker gesandt werden. Das wirkt umständlich, kann aber bei älteren Druckern zu einer deutlichen Geschwindigkeitssteigerung führen.

33.4 Drucken in lokalen Netzwerken

Dieser Abschnitt gibt einige Tipps zur Konfiguration eines Druckers, der über das Netzwerk mit dem Rechner verbunden ist. Dabei gibt es ziemlich viele Varianten, je nachdem, welche Protokolle der Netzwerkdrucker selbst versteht bzw. wie ein selbst nicht netzwerkfähiger Drucker mit einem Rechner im LAN verbunden ist:

- IPP-Drucker: Verwaltung z. B. durch Linux/Unix/OS X mit CUPS, Internet Printing Protocol
- Unix-Drucker: Verwaltung durch Linux/Unix, LPD-Protokoll

- Windows-Drucker: Verwaltung durch einen Windows-Rechner oder Samba-Server
- Socket-API: z. B. JetDirect von HP am IP-Port 9100
- herstellerspezifische Protokolle

Konfiguration eines Netzwerkdruckers (Client-Sicht)

IPP-Drucker verwenden

Die Details der Konfiguration hängen davon ab, über welches Protokoll die Kommunikation erfolgt. Am einfachsten funktioniert das Drucken im Netzwerk, wenn auf beiden Seiten CUPS bzw. das Protokoll IPP zum Einsatz kommt. Derartige Drucker sind ohne weitere Konfigurationsarbeiten auf der Client-Seite sichtbar und können sofort verwendet werden.

`lpstat -v` liefert eine Liste aller verfügbaren Drucker. Das folgende Kommando wurde auf dem Rechner `merkur` ausgeführt. Dort ist lokal ein Drucker mit dem Namen `DeskJet-5940` konfiguriert. Außerdem sind auf den Rechnern `mars` und `saturn` zwei weitere Drucker mit den Namen `pluto` und `kyocera` verfügbar:

```
user@uranus$  lpstat -v
Gerät für DeskJet-5940: parallel:/dev/lp0
Gerät für pluto:        ipp://mars.sol:631/printers/pluto
Gerät für kyocera:      ipp://saturn.sol:631/printers/kyocera
```

Sie können alle drei Drucker sofort mit `lpr -P`*`name`* benutzen. Falls mehrere Drucker im Netzwerk denselben Namen haben, müssen deren Namen in der Form *`drucker-name@hostname`* angegeben werden, also z. B. als `lpr -Plp@jupiter`.

Drucker im Netzwerk teilen

Damit die CUPS-Drucker anderer Rechner auf dem lokalen Rechner sichtbar sind, muss CUPS auf den externen Rechnern so konfiguriert sein, wie dies im nächsten Abschnitt beschrieben wird. Port 631 darf nicht durch eine Firewall blockiert sein!

Ein IPP-Drucker kann so konfiguriert sein, dass er zwar im Netz genutzt werden kann, aber nicht automatisch sichtbar ist. In diesem Fall müssen Sie den Drucker auf dem lokalen Rechner zuerst konfigurieren. Dabei wählen Sie den Druckertyp IPP-Drucker und geben als Adresse `ipp://hostname/printers/druckername` an. Sofern der externe Drucker via Linux/CUPS verwaltet wird, geben Sie als Hersteller und Modell Raw und Queue an. Das bedeutet, dass PostScript-Daten ohne Veränderung an den externen Rechner weitergeleitet werden; dieser kümmert sich dann um die Aufbereitung der Daten für den Drucker.

Andere Netzwerkdrucker konfigurieren

Wenn der externe Netzwerkdrucker nicht IPP-kompatibel ist, muss er vor der ersten Verwendung client-seitig konfiguriert werden. Dazu setzen Sie dieselben Programme wie bei der Konfiguration eines lokalen Druckers ein, wählen als Druckertyp aber NETZWERKDRUCKER. Die weitere Konfiguration hängt vom Protokoll ab:

- LPD (Unix-LPD): Hier geben Sie den Hostnamen des Rechners/Druckers sowie den Namen der Warteschlange an, im Zweifelsfall einfach `lp` oder `lp0`.
- SMB (Windows/Samba): Sie müssen den Hostnamen des Rechners, den Druckernamen sowie eventuell Benutzername und Passwort angeben. Bevor Sie einen Windows-Drucker verwenden können, müssen Sie das Samba-Client-Paket installieren.
- SOCKET-PROTOKOLL BZW. HP JETDIRECT: Hier geben Sie den Hostnamen oder die IP-Adresse des Druckers sowie die Port-Nummer an, in der Regel 9100.

Manche Konfigurationsprogramme erwarten die obigen Angaben auch in Form einer URI-Adresse (siehe die Tabelle 33.2). Detailinformationen für die Netzwerkdrucker – also Protokoll, Login-Name etc. – werden in der Datei `/etc/cups/printers.conf` gespeichert. Die folgenden Zeilen zeigen auszugsweise die Konfiguration eines JetDirect-kompatiblen Netzwerkdruckers:

```
# in /etc/cups/printers.conf
<DefaultPrinter Kyocera-Mita-FS-1800+>
UUID urn:uuid:000fee34-7f9c-3836-63e1-1c924ed63b7b
Info Kyocera Mita FS-1800+
Location 10.0.0.57
MakeModel Kyocera Mita FS-1800+
DeviceURI socket://10.0.0.57:9100
State Idle
StateTime 1340700228
Accepting Yes
Shared Yes
OpPolicy default
ErrorPolicy retry-job
Attribute marker-names TK-60,Waste Toner Bottle
...
</Printer>
```

Das entscheidende Schlüsselwort in `printers.conf` ist `DeviceURI`. Diesem Schlüsselwort folgt die URI-Adresse, aus der das Protokoll und die Netzwerkadresse hervorgehen. Tabelle 33.2 gibt einige Beispiele dafür, wie diese Adresse zusammengesetzt werden kann.

Adresse	Bedeutung
usb:/dev/usb/lp0	lokaler USB-Drucker
parallel:/dev/lp0	lokaler Drucker an der parallelen Schnittstelle
serial:/dev/ttyS0?baud=115200	lokaler Drucker an der seriellen Schnittstelle
lpd://hostname/printername	LPD-Netzwerkdrucker
socket://hostname:9100	Drucker mit Socket-Protokoll, z. B. HP JetDirect
smb://hostname/printername	Windows-Drucker
smb://workgroup/hostname/printer	Windows-Drucker
smb://user:xxx@wg/host/printer	Windows-Drucker
ipp://hostname/printers/printername	IPP-Drucker

Tabelle 33.2 CUPS-URI-Adressen

Konfiguration eines CUPS-Netzwerkdruckers (Server-Sicht)

Immer mehr Drucker sind selbst netzwerkfähig. Sie verbinden derartige Drucker einfach mit dem lokalen Netzwerk, und schon kann jeder Rechner im LAN auf den Drucker zugreifen. Das Thema dieses Abschnitts ist aber ein anderes: Wie können Sie einen lokalen Drucker *ohne* Netzwerkschnittstelle im Netzwerk nutzen?

Sicherlich haben Sie es schon erraten – via CUPS. Auf dem Rechner, der mit dem Drucker verbunden ist, konfigurieren Sie CUPS so, dass der Drucker-Server allen anderen Rechnern im Netzwerk Zugang zum lokalen Drucker gibt. Anschließend können Sie den Drucker von allen gängigen Betriebssystemen aus über IPP ansprechen.

Server-Konfiguration

Normalerweise kann ein via CUPS eingerichteter Drucker nur vom lokalen Rechner aus genutzt werden. Damit der Drucker auch von anderen Rechnern aus genutzt werden kann, wählen Sie in der Webschnittstelle das Dialogblatt VERWALTUNG aus, aktivieren dort die Option FREIGABE VON DRUCKERN, WELCHE MIT DIESEM SYSTEM VERBUNDEN SIND und klicken dann auf den Button EINSTELLUNGEN ÄNDERN. Wenn Sie die Konfigurationsdateien lieber selbst verändern, müssen Sie die folgenden Einstellungen in `cupsd.conf` durchführen und CUPS anschließend neu starten (`service cups restart`):

```
# Änderungen in /etc/cups/cupsd.conf
Port 631
Browsing On
BrowseOrder allow,deny
BrowseAddress @LOCAL
```

```
<Location />
  ...
  Allow @LOCAL
</Location>
```

`Port 631` bedeutet, dass CUPS über den Netzwerk-Port 631 kommuniziert. `BrowseAddress @LOCAL` bewirkt, dass die CUPS-Informationen an alle lokalen Netzwerkschnittstellen gesendet werden (Broadcast), nicht aber an Internetschnittstellen wie PPP. Alternativ kann mit `BrowseAddress @IF(eth0)` auch eine bestimmte Netzwerkschnittstelle angegeben werden.

`cupsd.conf` sieht eine Reihe weiterer `Browse`-Schlüsselwörter vor. Beispielsweise steuern `BrowseAllow` und `BrowseDeny`, von welchen Rechnern CUPS-Informationen *empfangen* werden. Standardmäßig gibt es keine Empfangseinschränkungen, und es ist selten notwendig oder sinnvoll, diese oder die anderen `BrowseXxx`-Einstellungen zu ändern. `Allow @LOCAL` bewirkt, dass andere Rechner im lokalen Netzwerk die von CUPS angebotenen Drucker tatsächlich nutzen dürfen.

Client-Konfiguration

Damit andere Linux-Rechner im Netz den externen CUPS-Drucker automatisch erkennen, müssen Sie die Option Freigegebenen Drucker anderer Systeme anzeigen oder eine ähnlichlautende Einstellung aktivieren.

Alternativ ist es auch möglich, den Drucker manuell einzurichten. Dazu starten Sie den Dialog zur Konfiguration eines neuen Druckers, wählen als Gerätetyp Internet Printing Protocol und geben den Hostnamen des Servers an. Der Konfigurationsdialog zeigt dann eine Liste aller auf dem Server verfügbaren Drucker an.

Auch unter Windows können CUPS-Drucker genutzt werden. Dazu wählen Sie im Druckerkonfigurationsdialog die Option Verbindung mit einem Drucker im Internet oder Netzwerk herstellen und geben die folgende Adresse an:

```
http://mars.sol:631/printers/pluto
```

Dabei müssen Sie natürlich `mars.sol` durch den Hostnamen des CUPS-Servers ersetzen und `pluto` durch den Namen des Druckers. Als Treiber geben Sie nach Möglichkeit den tatsächlichen Druckertreiber an; wenn es unter Windows keinen Treiber für Ihren Drucker gibt (was unwahrscheinlich ist), können Sie auch einen beliebigen PostScript-Druckertreiber verwenden.

Probleme

Wenn der Ausdruck statt des erwarteten Ergebnisses nur wirren Text bzw. undefinierbare Grafikmuster enthält, ist zumeist eine doppelte Verarbeitung der Druckdaten schuld: Zuerst wandelt der Windows-Treiber den Ausdruck in das Format des Druckers um. Diese Daten kommen dann bei CUPS an und werden dort ein zweites

Mal formatiert (in der CUPS-Nomenklatur: »gefiltert«). Das kann natürlich nicht gut gehen.

Abhilfe: Richten Sie nur unter Windows den für den Drucker erforderlichen Treiber ein! Am CUPS-Server konfigurieren Sie den Drucker in Form einer sogenannten Raw-Warteschlange, die die empfangenen Daten ohne Veränderung einfach an den Drucker weiterleitet. Dazu wählen Sie bei der Druckerkonfiguration als Gerätetyp RAW und als Modell RAW QUEUE.

AirPrint

Grundsätzlich unterstützt CUPS *AirPrint*. Das ist eine von Apple entwickelte Funktion, damit iPhones und iPads über das WLAN drucken können. Damit AirPrint funktioniert, müssen sich Ihr Linux-Rechner und das iOS-Gerät im selben Funknetz befinden. Außerdem müssen CUPS und Avahi richtig konfiguriert sein. Avahi ist ein Hintergrundprogramm, das eine automatische Nutzung des Netzwerks mittels Zeroconf ermöglicht (siehe Abschnitt 29.6).

Leider funktioniert AirPrint bei den wenigsten Distributionen auf Anhieb. Die folgende Anleitung zeigt, wie Sie AirPrint unter Fedora und Ubuntu zum Laufen bringen. Bei anderen Distributionen ist die Vorgehensweise analog.

Netzwerkdruck erlauben

Der erste Schritt besteht darin, das Drucken im Netzwerk zu erlauben. Dazu öffnen Sie im Webbrowser die Seite *http://localhost:631/admin*, aktivieren die Optionen SHARE PRINTER CONNECTED TO THIS SYSTEM und speichern diese mit dem Button CHANGE SETTINGS. Bei der Login-Aufforderung geben Sie unter Ubuntu Ihren Loginnamen, bei anderen Distributionen `root` und das dazu passende Passwort an.

AirPrint-Beschreibung des Druckers

Als Nächstes laden Sie das winzige Python-Script `airprint-generate` von der folgenden Website herunter:

https://github.com/tjfontaine/airprint-generate

Dieses Script führen Sie nun aus:

```
user$  python ~/Downloads/airprint-generate.py
```

Das Script speichert im lokalen Verzeichnis Dateien mit der Avahi-Beschreibung aller konfigurierten Drucker. Für den designierten AirPrint-Drucker verschieben Sie diese Datei in das Verzeichnis `/etc/avahi/services`:

```
root#  mv druckername.service /etc/avahi/services
```

Unter Fedora müssen Sie auf die korrekten SELinux-Attribute achten:

```
root#  mv druckername.service /etc/avahi/services
```

Firewall

Unter Fedora müssen Sie in den Firewall-Einstellungen die Dienste IPP und IPP CLIENT freischalten (Port 631).

Neustart von CUPS und Avahi

Nach einem Neustart von Avahi und CUPS sollten iOS-Geräte den Drucker erkennen:

```
root#  service avahi-daemon restart
root#  service cups restart
```

Weitere Informationen können Sie auf den folgenden Seiten nachlesen:

http://confoundedtech.blogspot.co.at/2012/12
http://blog.mornati.net/2012/09/22/linux-airprint-server-for-ios6-devices

Konfiguration eines Samba-Netzwerkdruckers (Server-Sicht)

Anstatt den Drucker direkt via CUPS im lokalen Netzwerk anzubieten, kann auch Samba diese Aufgabe übernehmen, wobei dann Samba wiederum auf CUPS zurückgreift. Standardmäßig ist Samba bei den meisten Distributionen bereits entsprechend vorkonfiguriert. Das folgende Listing fasst die relevanten Zeilen aus `/etc/samba/smb.conf` zusammen:

```
# Datei /etc/samba/smb.conf
...
# alle CUPS-Drucker via Samba nutzen
[printers]
   comment     = All Printers
   browseable  = no
   path        = /var/spool/samba
   printable   = yes
   guest ok    = no
   read only   = yes
   create mask = 0700
```

Der `[printers]`-Abschnitt ist für den eigentlichen Zugriff auf die Drucker verantwortlich. `browseable = no` bewirkt, dass nur die Drucker sichtbar sind, nicht aber das Verzeichnis `printers`. Der Pfad gibt den Ort für temporäre Druckdateien an.

Wenn Sie nicht alle Drucker, sondern nur einen bestimmten Drucker freigeben möchten, verwenden Sie die folgenden Zeilen anstelle des `[printers]`-Abschnitts. Das Beispiel geht davon aus, dass die Warteschlange dieses Druckers den Namen `pluto` hat, auf den Samba-Clients aber unter dem Namen `Hp_pluto` sichtbar sein soll:

```
# Datei /etc/samba/smb.conf
...
# Zugriff nur auf den CUPS-Drucker pluto unter dem Namen HP_pluto
[HP_pluto]
   printer     = pluto
   browseable  = no
   path        = /var/spool/samba/
   printable   = yes
   guest ok    = no
   read only   = yes
   create mask = 0700
```

Samba bietet die Möglichkeit, den Windows-Clients Druckertreiber anzubieten. Die folgenden Zeilen in der Samba-Standardkonfiguration sehen hierfür das Verzeichnis `/var/lib/samba/printers` vor:

```
# Datei /etc/samba/smb.conf
...
[print$]
   comment     = Printer Drivers
   path        = /var/lib/samba/printers
   browseable  = yes
   read only   = yes
   guest ok    = no
```

Das Problem an der Sache ist: Das Verzeichnis mit den Druckertreibern ist leer. Die Beschaffung und das Einrichten der Druckertreiber in einem Format, das alle gängigen Windows-Versionen verstehen, ist schwierig und lohnt sich nur, wenn der Drucker von sehr vielen Windows-Clients genutzt werden soll. Andernfalls ist es einfacher, die Treiberinstallation manuell unter Windows durchzuführen und dabei auf den Fundus der mitgelieferten Druckertreiber zurückzugreifen. Weitere Informationen zu diesem Thema geben `man cupsaddsmb` sowie die folgende Webseite:

http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/CUPS-printing.html

TEIL VI

Root-Server

Kapitel 34
Secure Shell (SSH)

Server, die nicht physikalisch vor Ihnen stehen, können Sie nur über eine Netzwerkverbindung administrieren. Das bevorzugte Werkzeug hierfür ist SSH (*Secure Shell*). Es ermöglicht sowohl die einfache Ausführung von Kommandos als auch die Bedienung grafischer Programme über eine sichere Netzwerkverbindung. Die einzige Voraussetzung besteht darin, dass auf dem Server ein SSH-Server installiert ist.

Das Kommando `ssh` ist der Nachfolger von `telnet` und `rlogin` und ist erheblich sicherer. Der Client-Einsatz dieses Kommando wurde bereits in Abschnitt 18.2 beschrieben. Dieses kurze Kapitel gibt einige Tipps, wie Sie einen SSH-Server so sicher wie möglich einrichten. Außerdem geht das Kapitel auf die Verwendung von Schlüsseln zur Authentifizierung ein.

Root-Server

Dieses SSH-Kapitel ist das erste von mehreren Kapiteln, in denen Netzwerkdienste beschrieben werden, die üblicherweise auf einem Root-Server laufen. Als »Root-Server« wird ein externer Rechner in einem Rechenzentrum bezeichnet, den Sie ohne Einschränkungen selbst administrieren dürfen, eben mit `root`-Rechten. Für erfahrene Linux-Administratoren stellen Root-Server eine preisgünstige Möglichkeit dar, eigene Webauftritte einzurichten, einen eigenen E-Mail-Server zu betreiben etc. Das ist vor allem für kleine und mittelgroße Unternehmen interessant, deren Internetzugang auf ADSL basiert und damit ungeeignet für Server-Dienste mit einem eigenen Domainnamen ist.

Bei der Auswahl eines Root-Servers sollten Sie vor allem auf die Seriosität des Hosting-Unternehmens achten. Nichts ist ärgerlicher als ein nicht funktionierender Support bei einem Rechner, zu dem Sie selbst keinen physikalischen Zugang haben. Wichtig sind auch administrative Hilfen, z. B. eine Webschnittstelle, um nach einem Absturz einen Server-Reboot auszulösen oder ein Rettungssystem zu starten.

Achten Sie schließlich darauf, welche Linux-Distributionen installiert werden können – nicht jeder Provider unterstützt alle gängigen Distributionen. Gut geeignet für den Root-Server-Einsatz sind neben den teuren Enterprise-Distributionen vor allem Debian, Ubuntu LTS und CentOS. Aufgrund des zu kleinen Wartungszeitraums sind Fedora und openSUSE nicht empfehlenswert.

34.1 Installation

Bei vielen Distributionen wandert der SSH-Server bereits während der Erstinstallation auf die Festplatte. Nur wenn der SSH-Server noch nicht installiert ist, müssen Sie selbst Hand anlegen.

Debian, Ubuntu Unter Debian und Ubuntu installieren Sie das Paket `openssh-server`. Der Dämon `sshd` wird sofort automatisch gestartet.

```
root#  apt-get install openssh-server
```

Fedora, RHEL Unter Fedora und RHEL führen Sie die Installation analog mit `yum` durch.

```
root#  yum install openssh-server
```

Unter Fedora wird der SSH-Server sofort automatisch ausgeführt; unter RHEL muss hingegen sowohl der erstmalige Start als auch die Aktivierung des automatischen Starts manuell durchgeführt werden.

```
root#  service sshd start          (SSH-Server erstmalig starten, nur RHEL)
root#  service --add sshd          (SSH-Server zukünftig automatisch starten, nur RHEL)
```

openSUSE Unter openSUSE lautet der Paketname `openssh`. Bei aktuellen openSUSE-Versionen mit Systemd-Unterstützung wird `openssh` sofort automatisch gestartet.

```
root#  zypper install openssh
```

Firewall Der Zugriff auf den SSH-Server scheitert, wenn eine Firewall den Port 22 blockiert. Unter Fedora, openSUSE und RHEL müssen Sie gegebenenfalls die Firewall-Konfiguration entsprechend ändern (siehe auch Kapitel 40).

34.2 Konfiguration und Absicherung

Die Konfigurationsdateien zu `sshd` befinden sich im Verzeichnis `/etc/ssh`. Für die Server-Konfiguration ist `sshd_config` zuständig. Normalerweise kann diese Datei unverändert bleiben, d. h., der SSH-Server sollte auf Anhieb funktionieren. Die Kommunikation erfolgt standardmäßig über den IP-Port 22. Wenn Sie besondere Anforderungen stellen, finden Sie in den `man`-Seiten zahlreiche weitere Informationen.

Secure FTP Ein Bestandteil des SSH-Servers ist der `sftp`-Server. Dabei handelt es sich um eine sichere Alternative zu einem normalen FTP-Server. Die `sftp`-Funktionen stehen normalerweise automatisch zur Verfügung, sobald der SSH-Server läuft; werfen Sie gegebenenfalls einen Blick auf die Zeile `Subsystem sftp` in `sshd_config`. Sie können mit `sftp`-kompatiblen Clients genutzt werden, z. B. mit dem Programm `sftp`. `sftp` sieht lediglich User-Logins vor, aber kein Anonymous FTP.

Absicherung

Grundsätzlich läuft der SSH-Server auf Anhieb ohne Konfigurationsarbeit. Das ist allerdings ein nicht zu unterschätzendes Sicherheitsrisiko: Jeder, der eine gültige Kombination aus Benutzername und Passwort errät, kann sich auf Ihrem Rechner anmelden! Cracker verwenden automatisierte Tools, die im Internet nach Servern suchen und sich dort einzuloggen versuchen. Alle derartigen Aktivitäten werden in der Datei `/var/log/auth.log` vermerkt. Auf öffentlich erreichbaren Servern finden Sie darin täglich Tausende von Einlog-Versuchen!

Sie tun also gut daran, alle Benutzer durch nichttriviale Passwörter abzusichern! Verwenden Sie beispielsweise das Kommando `makepasswd` aus dem gleichnamigen Paket, um sichere Passwörter zu erzeugen.

Die Datei `/etc/shadow`, in der in verschlüsselter Form alle Benutzerpasswörter gespeichert sind, darf auf keinen Fall Einträge ohne Passwort enthalten! Sie erkennen derartige Einträge daran, dass in einer Zeile zwischen dem ersten und dem zweiten Doppelpunkt kein Text enthalten ist. Üblicherweise befindet sich dort entweder ein verschlüsseltes Passwort oder bei System-Accounts ein Sonderzeichen (zumeist * oder !), das Logins vollständig unmöglich macht. Sollten Sie in dieser Datei tatsächlich einen Eintrag ohne Passwort finden, beheben Sie den Missstand mit `password name`.

Die folgenden Maßnahmen reduzieren jeweils die Wahrscheinlichkeit eines Crack-Angriffs auf Ihren SSH-Server. Sie können einzeln oder in Kombination angewendet werden.

Kein root-Login

Ein Angreifer möchte `root`-Rechte erzielen – und am einfachsten gelingt das natürlich durch einen `root`-Login. Dabei muss nur ein Parameter (das `root`-Passwort) erraten werden. Wesentlich sicherer ist es, einen direkten `root`-Login via SSH zu verbieten. Sie müssen sich also unter einem anderen Benutzernamen einloggen und dann mit `su` oder `sudo` in den `root`-Modus wechseln. Wenn Sie einen root-Server administrieren, sollten Sie das unbedingt testen, bevor Sie die folgende Änderung durchführen – sonst sperren Sie sich womöglich selbst aus!

```
# Änderung in /etc/ssh/sshd_config
...
PermitRootLogin = no
```

Damit die Änderung wirksam wird, müssen Sie `sshd` dazu auffordern, die Konfigurationsdateien neu einzulesen:

```
root# service ssh reload
```

Für den Angreifer hat das die Konsequenz, dass nun zwei Parameter unbekannt sind: der Login-Name *und* das Passwort!

Eine sinnvolle Alternative zu `PermitRootLogin = no` ist die Einstellung `without-password`:

```
# Änderung in /etc/ssh/sshd_config
...
PermitRootLogin =  without-password
```

Keine Angst, diese Einstellung erlaubt keineswegs einen `root`-Login mit leerem Passwort! `without-password` meint vielmehr, dass ein Login weiterhin möglich ist, dass aber die Authentifizierung durch ein sichereres Verfahren als durch die simple Passworteingabe erfolgen muss – in aller Regel durch den Austausch von Schlüsseln (siehe den folgenden Abschnitt).

IPv6-Zugang sperren

Wenn Rechner im lokalen Netzwerk über IPv4 kommunizieren, außerdem aber eine IPv6-Konfiguration oder ein IPv6-Tunnel vorliegt, ist es zweckmäßig, den IPv6-Zugang auf den SSH-Server zu blockieren. Damit können Sie im lokalen Netzwerk via SSH auf Ihren Rechner zugreifen, nicht aber von außen. Genau das erreichen Sie durch die Einstellung `AddressFamily inet`. Andere zulässige Einstellungen sind `inet6` (nur IPv6) und `any` (sowohl IPv4 als auch IPv6, gilt per Default).

```
# Änderung in /etc/ssh/sshd_config, nur IPv4 akzeptieren
...
AddressFamily inet
```

SSH-Port ändern

Der SSH-Server kommuniziert standardmäßig über den Port 22. Mit der `Port`-Zeile können Sie mühelos einen anderen, momentan unbenutzten Port einstellen. Da viele automatisierte Crack-Tools nur den Port 22 berücksichtigen, vermeiden Sie auf einen Schlag viele Sicherheitsprobleme.

Bei der Verwendung von `ssh` müssen Sie nun jedes Mal mit `-p` den Port Ihres SSH-Servers explizit angeben. Beachten Sie, dass Sie beim Kommando `scp` die Option `-P` verwenden müssen, weil `-p` dort die Bedeutung *preserve* hat und bewirkt, dass Zeit- und Zugriffsinformationen der zu kopierenden Datei erhalten bleiben!

Sie sollten sich freilich im Klaren darüber sein, dass der Schutz durch den Port-Wechsel nur begrenzte Wirkung hat: Wer Ihren Server ernsthaft angreifen will und nicht nur auf der Suche nach dem nächstbesten schlecht konfigurierten Server zur Installation eines Root-Kits ist, der wird einen Port-Scan durchführen. Damit bleibt Ihr SSH-Server nicht lange unentdeckt, egal auf welchem Port er läuft.

Die Veränderung des SSH-Ports hat zudem einen nicht unerheblichen Nachteil: Während die meisten Firewalls so konfiguriert sind, dass sie Verkehr über den Port 22 zulassen, wird dies für Ihren neuen Port wahrscheinlich nicht zutreffen. Wenn Sie vom Unternehmen Xy, wo Sie gerade ein paar Tage arbeiten, schnell via SSH auf Ihren Server zugreifen möchten, scheitern Sie womöglich bereits an der Firmen-Firewall.

TCP-Wrapper

Der SSH-Server verwendet die sogenannte TCP-Wrapper-Bibliothek. Deswegen können Sie auch durch die Konfigurationsdateien `/etc/hosts.allow` und `/etc/hosts.deny` steuern, von welchen Netzwerkadressen der SSH-Server genutzt werden kann. Bei einem SSH-Server auf einem Root-Server ist diese Art der Absicherung selten zweckmäßig – SSH soll ja gerade aus dem ganzen Internet verwendbar sein. Wenn Sie dagegen einen SSH-Server auf einem LAN-Server installiert haben und die Administration nur innerhalb des LANs erfolgen soll, ist es durchaus sinnvoll, die Zugriffsmöglichkeiten entsprechend einzuschränken. Details zur TCP-Wrapper-Bibliothek und den dazugehörigen Konfigurationsdateien finden Sie in Abschnitt 40.2.

DenyHosts (nur für IPv4!)

Das Python-Script DenyHosts überwacht SSH-Login-Versuche. Sobald es feststellt, dass es von einer IPv4-Adresse mehrere vergebliche Logins gibt, wird diese IP-Adresse automatisch der Datei `/etc/hosts.deny` hinzugefügt. Je nach Konfiguration bleibt die IP-Adresse nun für immer in `hosts.deny` oder wird nach einer bestimmten Zeit wieder entfernt, z. B. nach einem Tag oder einer Woche.

DenyHosts verhindert automatisierte Login-Versuche wirksam (es sei denn, es handelt sich um einen Angriff, der gleichzeitig von sehr vielen unterschiedlichen Rechnern erfolgt) und hat sich auf den von mir betreuten Servern sehr gut bewährt. Für viele Distributionen gibt es fertige Pakete. Weitere Informationen und die gerade aktuelle Version finden Sie unter:

http://denyhosts.sourceforge.net

DenyHosts wird durch ein Init-Script gestartet und wertet die Konfigurationsdatei `/etc/denyhosts.conf` aus. Entscheidend ist, dass `denyhost` die richtige Logging-Datei überwacht (Parameter `SECURE_LOG`). Das folgende Listing zeigt einige Zeilen der Konfiguration auf meinem Webserver *http://kofler.info*:

```
# Datei /etc/denyhosts.conf
SECURE_LOG = /var/log/auth.log
HOSTS_DENY = /etc/hosts.deny

# blockierte IP-Adressen nach 24h wieder freigeben
PURGE_DENY = 1d
# blockieren nach drei vergeblichen Versuchen für einen falschen Login-Namen
DENY_THRESHOLD_INVALID = 3
# blockieren nach fünf vergeblichen Versuchen für einen richtigen Login-Namen
DENY_THRESHOLD_VALID = 5
# blockieren nach einem vergeblichen Versuch für root
DENY_THRESHOLD_ROOT = 1
```

DenyHosts bietet keinen Schutz vor Angriffen aus dem IPv6-Netz! Sofern Sie den SSH-Zugriff via IPv6 nicht unbedingt benötigen, sollten Sie ihn einfach komplett sperren oder nur einen Login mit Schlüsseln zulassen.

34.3 Authentifizierung mit Schlüsseln

Schlüssel erzeugen

Am sichersten ist die Verwendung des SSH-Servers, wenn Sie sich nicht mit einem Passwort authentifizieren, sondern mit einem Schlüssel. Dazu erzeugen Sie auf dem lokalen Rechner mit `ssh-keygen` ein Schlüsselpaar. Diesen Schlüssel sollten Sie durch eine Passphrase selbst verschlüsseln. Als *Passphrase* wird ein aus mehreren Wörtern bestehendes Passwort bezeichnet. Anschließend fügen Sie – noch per Passwort-Authentifizierung – den öffentlichen Schlüssel mit dem Kommando `ssh-copy-id` in die Datei `.ssh/authorized_keys` auf dem Server ein:

```
user@client$  ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_rsa):  <Return>
Enter passphrase (empty for no passphrase):  ********
Enter same passphrase again:  ********
Your identification has been saved in /home/user/.ssh/id_rsa.
Your public key has been saved in /home/user/.ssh/id_rsa.pub.
user@client$  ssh-copy-id -i user@server
user@server's password:  *******
```

Wenn Sie die Passphrase-Frage einfach mit ↵ oder mit der Eingabe `empty` beantworten, verzichtet `ssh-keygen` auf die Verschlüsselung. Das ist bequem, weil es eine SSH-Nutzung ohne Passwort-Rückfrage ermöglicht. Sie gehen damit aber ein Sicherheitsrisiko ein: Jeder, dem Ihr Schlüssel auf dem Client-Rechner in die Hände gerät, kann sich ohne Weiteres auf allen Rechnern anmelden, auf denen Sie den öffentlichen Teil des Schlüssels installiert haben!

Das Kommando `ssh-copy-id` scheitert, wenn der Server nur eine Authentifizierung per Schlüssel zulässt. Zur Lösung dieses Henne-Ei-Problems müssen Sie die Schlüsselübertragung von einem anderen Client aus durchführen, der sich beim Server authentifizieren kann. Sie müssen in diesem Fall Ihre öffentliche Schlüsseldatei `.ssh/id_rsa.pub` über einen dritten Rechner zum Server übertragen und dort manuell am Ende der Datei `.ssh/authorized_keys` einfügen.

Wenn Sie nun eine Verbindung zum Zielrechner erstellen, tauscht `ssh` die Schlüsselinformationen aus. Ein Login ist nicht mehr erforderlich, Sie müssen aber die Passphrase der privaten Schlüsseldatei eingeben.

ssh-agent

Sofern Ihre Schlüssel durch ein Passwort bzw. eine Passphrase abgesichert sind, haben Sie durch die Verwendung von Schlüsseln nur an Sicherheit, aber nicht an Komfort gewonnen. Eine sichere und doch einigermaßen bequeme Lösung bietet `ssh-agent`. Dieses Programm verwaltet alle privaten Schlüssel des Anwenders. Das Programm wird folgendermaßen gestartet:

```
user$  eval $(ssh-agent)
```

Dadurch werden einige Umgebungsvariablen der aktuellen Konsole geändert. `ssh-agent` läuft als Hintergrundprozess weiter. Durch `ssh-add` können Sie nun Ihre privaten Schlüssel hinzufügen:

```
user$  ssh-add ~/.ssh/id_rsa
Enter passphrase for /home/user/.ssh/id_rsa:  ******
```

Von nun an verwendet `ssh` die von `ssh-agent` verwalteten Schlüsseldateien. Das heißt, Sie werden nie mehr nach dem Passwort für die Schlüsseldatei gefragt. Anstatt das Passwort bei jedem `ssh`-Kommando einzugeben, ist dies nur noch einmal erforderlich. Der große Nachteil von `ssh-agent` besteht darin, dass die Wirkung der Umgebungsvariablen auf eine einzige Konsole beschränkt ist.

gnome-keyring

Unter Gnome kümmert sich standardmäßig der `gnome-keyring-daemon` um Passwörter und SSH-Schlüssel. Der erstmalige Zugriff auf die Daten erfordert zumeist einen richtigen Login (vermeiden Sie Auto-Logins durch den Display Manager!) oder die Angabe des Master-Passworts. Zur Administration der gespeicherten Schlüssel und Passwörter verwenden Sie das Programm `seahorse`.

Login-Probleme

Nicht immer funktioniert der passwortfreie Login beim SSH-Server auf Anhieb. Schuld sind diverse Sicherheitseinstellungen. Falls der SSH-Server im `STRICT_MODE` läuft, was standardmäßig der Fall ist, wird die Datei `authorized_keys` nur berücksichtigt, wenn deren Zugriffsrechte sehr restriktiv eingestellt sind. Wurde die Schlüsseldatei von `ssh-copy-id` erstellt, ist das zumeist nicht der Fall. Abhilfe schaffen die beiden folgenden Kommandos:

```
user@server$  chmod 700 ~/.ssh
user@server$  chmod 600 ~/.ssh/authorized_keys
```

Bei Fedora- und RHEL-Servern tritt häufig ein weiteres Problem auf: Der von `ssh-copy-id` erzeugten Schlüsseldatei fehlen die erforderlichen SELinux-Kontextinformationen. Abhilfe:

```
root@server#  /sbin/restorecon -r /root/.ssh          (für root)
root@server#  /sbin/restorecon -r /home/user/.ssh     (für andere Benutzer)
```

Fehlersuche

Wenn der SSH-Login nicht wie erwartet funktioniert, führen Sie das `ssh`-Kommando mit der zusätzlichen Option `-v` aus. `ssh` liefert dann eine Menge Debugging-Meldungen. Die Option kann bis zu dreimal angegeben werden, also `-v -v -v`. `ssh` protokolliert dann entsprechend detaillierter.

Passwort-Login ganz abstellen

Sobald der Aufbau einer SSH-Verbindung mit dem Schlüssel funktioniert und keine Login-Aufforderung mehr erscheint, können Sie sich überlegen, den Passwort-Login ganz zu deaktivieren. Dazu verändern Sie auf dem Server die Konfigurationsdatei `sshd_config`. Entscheidend sind zwei Zeilen:

```
# in /etc/ssh/sshd_config
...
PasswordAuthentication  no
UsePAM                  no
```

Damit ist von nun an eine SSH-Authentifizierung *nur* noch mit Schlüsseln möglich. Passen Sie aber auf, dass Sie sich nicht selbst aus Ihrem System aussperren! Wenn Sie den Schlüssel auf Ihrem Client-Rechner verlieren, beispielsweise weil Ihnen Ihr Notebook gestohlen wird und Sie kein Backup haben, können Sie sich auf dem Server nicht mehr einloggen! Es ist wie so oft: Jede zusätzliche Sicherheit bezahlen Sie durch geringere Flexibilität …

Mehrere Schlüssel

Bis jetzt bin ich davon ausgegangen, dass Sie nur einen einzigen, selbst erzeugten Schlüssel verwenden. Aber vielleicht haben Sie mehrere Schlüssel, die Sie in der Vergangenheit auf unterschiedlichen Rechnern eingesetzt haben; oder Sie wollen unterschiedliche Schlüssel für unterschiedliche externe Server verwenden; oder es übergibt Ihnen jemand eine Schlüsseldatei, damit Sie einen weiteren Rechner administrieren können.

Die einfachste Lösung besteht darin, auf dem Client-Rechner im Verzeichnis `.ssh` die Datei `config` einzurichten. Vergessen Sie `chmod 600` nicht! Diese Datei enthält mit dem Schlüsselwort `IdentityFile` Referenzen auf alle Schlüsseldateien, beispielsweise so:

```
# Datei .ssh/config
IdentityFile ~/.ssh/id_rsa
IdentityFile ~/.ssh/id_rsa.my-other-server
IdentityFile ~/.ssh/id_rsa.fh-xen-server
...
```

In dieser Konfiguration testet das `ssh`-Kommando einfach alle Schlüssel, bis einer passt. Sie können der `config`-Datei noch mehr »Intelligenz« verleihen, wenn Sie die Einträge nach Hosts gruppieren. Damit können Sie für jeden Host zusätzlich angeben, welcher Port, welcher Benutzer etc. verwendet werden soll. Die folgenden Zeilen veranschaulichen die Syntax; mehr Details gibt `man ssh_config`.

```
# Datei .ssh/config
Host kofler.info
  IdentityFile ~/.ssh/id_rsa
  User strenggeheim
Host my-other-server.com
  IdentityFile ~/.ssh/id_rsa.my-other-server
  User otheradmin
  Port 22022
```

Kapitel 35
Apache

Dieses Kapitel beschreibt, wie Sie Ihren eigenen Webserver aufsetzen. Außer auf Apache und seine Basiskonfiguration geht das Kapitel auch auf einige beliebte Erweiterungen ein, unter anderem auf PHP, Webalizer und Awstats. Das Kapitel endet mit einigen Informationen zu FTP – und der Empfehlung, auf einen FTP-Server zu verzichten. Ich gehe in diesem Kapitel davon aus, dass Sie einen öffentlichen Webserver im Internet betreiben möchten.

Grundsätzlich ist es natürlich auch möglich, Apache nur innerhalb eines LANs einzusetzen, beispielsweise als firmeninternes Kommunikationszentrum mit einem Wiki und Seiten zur Projektplanung, Zeiterfassung etc. In diesem Fall müssen Sie aber unbedingt sicherstellen, dass die hier gesammelten Daten tatsächlich intern bleiben und kein ungeschützter Webzugriff aus dem Internet möglich ist (siehe auch Abschnitt 35.2).

Generell gilt: Dieses Kapitel ist lediglich eine Einführung in die Konfiguration von Apache und beschreibt bestenfalls ein Prozent der Schlüsselwörter zur Apache-Konfiguration. Der professionelle Einsatz von Apache setzt das Studium weiterführender Dokumentation voraus, sei es in Buchform oder aus dem Internet.

35.1 Apache

Apache ist *der* Webserver der Open-Source-Welt. Im Juli 2013 liefen laut *http://netcraft.com* ca. 52 Prozent aller Websites unter Apache. Wird nur die Million der am meisten besuchten Websites betrachtet, steigt der Marktanteil sogar auf 58 Prozent. Aktuelle Informationen sowie eine umfassende Dokumentation zu Apache finden Sie auf der Apache-Website:

http://httpd.apache.org

Version 2.2 versus 2.4

Anfang 2012 wurde Apache 2.4 fertiggestellt. Viele Distributionen und insbesondere alle im Sommer 2013 verfügbaren Enterprise-Distributionen verwenden aber noch Apache 2.2. Dieses Kapitel berücksichtigt beide Versionen. Apache 2.4 können Sie unkompliziert mit aktuellen Fedora- oder Ubuntu-Versionen ausprobieren.

Installation

Eine typische Apache-Installation besteht aus zahlreichen zusammengehörenden Paketen: dem Server an sich, diversen Bibliotheken, Plugins, Programmiersprachen etc. Um Ihnen die Installation zu erleichtern, können Sie bei einigen Distributionen jeweils eine ganze Gruppe von Paketen zur Installation auswählen. Damit werden neben Apache auch die wichtigsten MySQL- und PHP-Pakete installiert.

```
root#  tasksel install web-server                (Debian)
root#  yum groupinstall 'Web-Server'             (Fedora, RHEL)
root#  zypper intall -t pattern lamp_server      (SUSE)
root#  tasksel install lamp-server               (Ubuntu)
```

Das richtige Multi-Processing-Modul (MPM)

Seit Version 2 unterstützt Apache drei unterschiedliche Multi-Processing-Module, nämlich `perchild`, `prefork` und `worker`. Mit Apache 2.4 ist als vierte Variante `event` hinzugekommen. Diese Multi-Threading-Verfahren haben Einfluss darauf, wie effizient Apache mehrere Anfragen gleichzeitig verarbeiten kann. Beim Einrichten von Apache müssen Sie sich für eine dieser Varianten entscheiden, indem Sie das entsprechende `apache2-mpm-xxx`-Paket installieren.

Wenn Sie zusammen mit Apache die Programmiersprache PHP einsetzen möchten, ist das Verfahren `prefork` die sicherste Wahl. Bei den beiden anderen Varianten sind Fehler aufgrund von nicht thread-sicheren Bibliotheken möglich:

http://www.php.net/manual/en/faq.installation.php

Start/Stopp

Apache ist ein Dämon, der je nach Distribution explizit gestartet werden muss. Eine Zusammenfassung der erforderlichen Kommandos finden Sie in Abschnitt 16.5. Der Name des Init-Scripts variiert je nach Distribution: Er lautet `apache2` bei Debian, SUSE und Ubuntu bzw. `httpd` bei Fedora und Red Hat.

Firewall

Unter Fedora, RHEL und (open)SUSE blockiert die standardmäßig aktive Firewall den Zugriff auf den Webserver von außen. Sie können Apache also vorerst nur direkt auf dem Rechner ausprobieren, auf dem der Webserver läuft (`http://localhost`). Damit der Webserver auch von außen erreichbar ist, müssen Sie in der Firewall Ausnahmeregeln für die Protokolle HTTP und HTTPS definieren, also für die Port-Nummern 80 und 443.

Name und Account

Der Service-Name für das Init-System variiert je nach Distribution. Aus Sicherheitsgründen wird der Webserver wie die meisten anderen Netzwerk-Dämonen nicht unter dem Account `root` ausgeführt, sondern unter einem anderen Account. Dessen Namen stellen Sie am einfachsten mit `ps axu` fest. Tabelle 35.1 fasst zusammen, unter welchem Namen Apache dem Init-System bekannt ist, unter welchem Account das Programm läuft und wo sich standardmäßig die HTML-Dateien befinden.

Distribution	Prozessname	Account	DocumentRoot
Debian, Ubuntu	apache	www-data	/var/www
Fedora, Red Hat	httpd	apache	/var/www/html
SUSE	httpd2-*threadverfahren*	wwwrun	/srv/www/htdocs

Tabelle 35.1 Programmname, Account und DocumentRoot-Verzeichnis von Apache

Test

Um zu testen, ob alles funktioniert, starten Sie auf dem lokalen Rechner einen Webbrowser und geben als Adresse `http://localhost/` oder `http://servername/` ein. Sie sollten nun eine Testseite des Webservers sehen (siehe Abbildung 35.1).

Abbildung 35.1 Apache-Testseite eines Fedora-Rechners

Eigene HTML-Seiten

Damit statt der Testseite die Startseite Ihres eigenen Webauftritts erscheint, müssen Sie Ihre HTML-Dateien in das Dokumentverzeichnis von Apache speichern. Auch dieses Verzeichnis ist distributionsabhängig (Schlüsselwort `DocumentRoot` in den Konfigurationsdateien, siehe Tabelle 35.1). Ihre HTML-Dateien müssen für den Account des Apache-Webservers lesbar sein!

SELinux

Wenn Sie unter Fedora oder RHEL arbeiten, müssen Sie außerdem darauf achten, dass alle HTML-Dateien mit dem SELinux-Attribut `httpd_sys_content_t` ausgestattet sind. Für Dateien innerhalb von `/var/www/html` erreichen Sie das am einfachsten durch das folgende Kommando:

```
root#  restorecon -R -v /var/www/html/*
```

Wenn Sie Ihre HTML-Dateien in einem anderen Verzeichnis ablegen, ist hingegen das folgende Kommando erforderlich:

```
root#  chcon -R system_u:object_r:httpd_sys_content_t:s0 /mein-web-verzeichnis
```

Beachten Sie, dass für CGI-, Webalizer- und Konfigurationsdateien andere Attribute vorgesehen sind. Details zum SELinux-Modul für Apache können Sie hier nachlesen:

http://fedoraproject.org/wiki/SELinux/apache

Konfiguration

In diesem Buch fehlt der Platz, um detailliert auf alle Konfigurationsoptionen und -varianten einzugehen. Ich möchte an dieser Stelle aber zumindest einen Überblick darüber geben, wo sich die Konfigurationsdateien je nach Distribution befinden und wie ganz elementare Einstellungen durchgeführt werden.

Früher erfolgte die Konfiguration von Apache durch eine einzige Datei `httpd.conf`, wobei deren genauer Ort distributionsabhängig war. Diese Konfigurationsdatei wurde im Laufe der Zeit immer unübersichtlicher.

Aus diesem Grund sind die meisten Distributionen dazu übergegangen, die Einstellungen auf diverse Dateien zu verteilen, die durch `Include`-Anweisungen aus verschiedenen Verzeichnissen gelesen werden (siehe die Tabellen 35.2 bis 35.4). Das macht jede einzelne Datei übersichtlicher und ermöglicht eine automatisierte Wartung – also beispielsweise das Aktivieren oder Deaktivieren von Plugins durch Kommandos oder Scripts. Wenn Sie ein bestimmtes Schlüsselwort in den Konfigurationsdateien suchen, gehen Sie am besten so vor:

```
user$  cd /etc/httpd (bzw.) cd /etc/apache2
user$  find -type f -exec grep -i -q Schlüsselwort {} ^; -print
```

Bei Debian/Ubuntu enthält das Verzeichnis `mods-available` eine Kollektion von `*.load`- und `*.conf`-Dateien für diverse Apache-Module. Um weitere Module zu aktivieren, richten Sie in `mods-enabled` Links auf diese Dateien ein. Bei der Verwaltung der Links helfen die Debian-spezifischen Kommandos `a2enmod` und `a2dismod`.

Des Weiteren können Sie mit `a2ensite` und `a2dissite` virtuelle Hosts aktivieren bzw. deaktivieren. Standardmäßig enthält `sites-available` nur die Dateien `000-default.conf` und `default-ssl.conf`: Dort befinden sich diverse Grundeinstellungen für das Verzeichnis `/var/www`. Der Mechanismus funktioniert wie bei den Modulen: Das Verzeichnis `sites-available` enthält die Konfigurationsdateien für alle Hosts, in `sites-enabled` befinden sich die entsprechenden Links.

Dateien	Inhalt
/etc/apache2/apache2.conf	Startpunkt
/etc/apache2/httpd.conf	benutzerspezifische Konfiguration
/etc/apache2/ports.conf	überwachte Ports, normalerweise Port 80
/etc/apache2/conf.d/*	weitere Konfigurationsdateien
/etc/apache2/mods-available/	verfügbare Erweiterungsmodule
/etc/apache2/mods-enabled/*.conf	Links auf aktive Erweiterungsmodule
/etc/apache2/conf-available/	verfügbare Konfigurationsdateien
/etc/apache2/conf-enabled/*.conf	Links auf aktive Konfigurationsdateien
/etc/apache2/sites-available/	verfügbare Websites (virtuelle Hosts)
/etc/apache2/sites-enabled/*.conf	Links auf aktive Websites
/etc/apache2/envvars	Umgebungsvariablen für das Init-Script

Tabelle 35.2 Apache-Konfiguration bei Debian und Ubuntu

Dateien	Inhalt
/etc/httpd/conf/httpd.conf	Startpunkt
/etc/httpd/conf/magic	MIME-Konfiguration (für mod_mime)
/etc/httpd/conf.d/*.conf	sonstige Konfigurationsdateien

Tabelle 35.3 Apache-Konfiguration bei Fedora und Red Hat

Dateien	Inhalt
/etc/apache2/httpd.conf	Startpunkt
/etc/apache2/*.conf	globale Konfigurationsdateien
/etc/apache2/sysconf.d/*.conf	automatisch erzeugte Systemkonfigurationsdateien
/etc/apache2/conf.d/*.conf	sonstige Konfigurationsdateien
/etc/apache2/vhosts.d/*.conf	Websites (virtuelle Hosts)
/etc/sysconfig/apache2	Grundeinstellungen

Tabelle 35.4 Apache-Konfiguration bei SUSE

Bei aktuellen Ubuntu-Versionen mit Apache 2.4 wurde dieser Mechanismus auch auf sonstige Konfigurationsdateien ausgeweitet. Die Dateien befinden sich in `conf-available`. Mit den Kommandos `a2enconf` bzw. `a2disconf` werden im Verzeichnis `conf-enabled` entsprechende Links darauf eingerichtet bzw. wieder entfernt. Bei älteren Ubuntu-Versionen sowie bei Debian werden derartige Konfigurationsdateien in `conf.d` gespeichert. Die Verwaltung erfolgt manuell ohne Kommandos.

Bei SUSE werden sämtliche `*.conf`-Dateien im Verzeichnis `sysconf.d` bei jedem Apache-Start durch das Init-V-Script `/etc/init.d/apache2` neu erstellt! Änderungen in diesen Dateien sind daher zwecklos! Vielmehr müssen Sie die Variablen in `/etc/sysconfig/apache2` ändern. In dieser Datei ist auch festgelegt, welche Module beim Apache-Start geladen werden (Variable `APACHE_MODULES`). Wenn Sie den SUSE-Konfigurationsdateien eine eigene Datei hinzufügen möchten, geben Sie deren Dateinamen in der Variable `APACHE_CONF_INCLUDE_FILES` an.

Konfiguration testen

Nach Änderungen an der Syntax können Sie mit `httpd -t`, `httpd2 -t` bzw. `apache2 -t` testen, ob die Konfiguration frei von Syntaxfehlern ist. Bei Debian und Ubuntu müssen Sie vorher einige Umgebungsvariablen aus `envvars` einlesen:

```
root#  . /etc/apache2/envvars
root#  apache2 -t
Syntax OK
```

Anschließend fordern Sie Apache dazu auf, die Konfigurationsdateien neu einzulesen:

```
root#  service apache2|httpd reload
```

ServerName

Der Webserver Apache funktioniert zwar im Regelfall auf Anhieb. Je nach Netzwerkkonfiguration müssen Sie aber zumindest eine Zeile in den Konfigurationsdateien ändern bzw. zu ihnen hinzufügen: `ServerName` sollte den Namen Ihres Rechners enthalten. Falls diese Einstellung nicht wirksam wird, müssen Sie außerdem die Einstellung `UseCanonicalName Off` verwenden.

```
# in   /etc/apache2/httpd.conf     (Debian/Ubuntu)
# bzw. /etc/httpd/conf/httpd.conf  (Fedora/Red Hat)
ServerName mars.sol     # geben Sie hier den Namen Ihres Rechners an
```

Bei SUSE stellen Sie den Rechnernamen in `/etc/sysconfig/apache2` mit der Variablen `APACHE_SERVERNAME` ein.

IPv6 blockieren

Sofern der Root-Server über eine IPv6-Adresse verfügt, beantwortet Apache auch IPv6-Webanfragen. Dafür verantwortlich ist die Standardeinstellung `Listen 80`, mit der Apache den Port 80 überwacht, unabhängig von der IP-Version. Wenn Sie IPv6 deaktivieren möchten, fügen Sie die Anweisung `Listen 0.0.0.0:80` in die passende Konfigurationsdatei ein. Falls Apache auch HTTPS-Seiten liefern soll, benötigen Sie eine weitere `Listen`-Anweisung für den Port 443:

```
# Datei   /etc/apache2/ports.conf (Debian, Ubuntu)
# Dateien /etc/httpd/conf/httpd.conf und conf.d/ssl.conf (Fedora, Red Hat)
# Datei   /etc/apache2/listen.conf (SUSE)
Listen 0.0.0.0:80
Listen 0.0.0.0:443 https
```

Standardzeichensatz

Bei allen gängigen Linux-Distributionen gilt automatisch der Unicode-Zeichensatz UTF-8. Wenn Sie also mit einem Texteditor eine Textdatei erstellen, die die deutschen Buchstaben ä, ö, ü oder ß enthält, werden diese in der UTF-8-Codierung gespeichert.

Apache ist die Codierung der HTML-Dateien grundsätzlich egal. Das Programm überträgt die Dateien einfach Byte für Byte an den Webbrowser, der die Seite angefordert hat. Allerdings sendet Apache zusätzlich einen sogenannten Header mit, der unter anderem Informationen darüber enthält, in welchem Zeichensatz die Seite codiert ist. Der Webbrowser wertet diese Information aus und verwendet den angegebenen Zeichensatz zur Darstellung der Seite.

Zeichensatz einstellen

Der springende Punkt ist nun, dass Apache den richtigen Zeichensatz angibt: Wenn das schiefgeht, sieht der Benutzer in seinem Webbrowser statt ä oder ü irgendwelche merkwürdigen Zeichenkombinationen. Aus diesem Grund bietet Apache diverse Möglichkeiten zur Zeichensatzkonfiguration:

- **`AddDefaultCharset off`:** Bei dieser Einstellung wertet Apache das `<meta>`-Tag in der zu übertragenden HTML-Datei aus und sendet den dort angegebenen Zeichensatz an den Browser. Wenn die HTML-Datei wie folgt beginnt, kommt der Zeichensatz Unicode UTF-8 zur Anwendung:

  ```
  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
  "http://www.w3.org/TR/html4/loose.dtd">
  <html><head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
  ...
  ```

- **`AddDefaultCharset zeichensatz`:** Apache überträgt den hier angegebenen Zeichensatz für alle Seiten an den Browser. Die Einstellung gilt sowohl für HTML- als auch für PHP-Dateien. Das `<meta>`-Tag im HTML-Code wird ignoriert.
- **`AddCharset zeichensatz kennung`:** Damit wird ein Zeichensatz für Dateien mit einer bestimmten Kennung eingestellt. `AddCharset utf-8 .utf8` bewirkt also, dass für alle Dateien, deren Name auf `.utf8` endet, als Zeichensatz Unicode UTF-8 an den Browser gesendet wird. `AddCharset` setzt das Apache-Modul `mod_mime` voraus.

Debian, Ubuntu

Natürlich gilt je nach Distribution eine unterschiedliche Standardkonfiguration. Für die globale Voreinstellung des Zeichensatzes ist unter Debian die Konfigurationsdatei `/etc/apache2/conf.d/charset` vorgesehen, bei aktuellen Ubuntu-Versionen die Datei `/etc/apache2/conf-enabled/charset.conf`. Normalerweise sind diese Dateien leer, d. h., es gilt `AddDefaultCharset off`.

Sie können `AddDefaultCharset` und `AddCharset` auch in den Konfigurationsdateien für virtuelle Hosts (Verzeichnis `sites-available`) sowie in `.htaccess`-Dateien einsetzen, wenn Sie eine host- bzw. verzeichnisspezifische Konfiguration wünschen. Beachten Sie aber, dass die Zeichensatzeinstellungen in `.htaccess` nur berücksichtigt werden, wenn für das Webverzeichnis `AllowOverride All` oder `FileInfo` gilt.

Fedora, Red Hat

Bei Fedora und Red Hat gilt `AddDefaultCharset UTF-8`. Die Einstellung befindet sich in `/etc/httpd/conf/httpd.conf`. In derselben Datei ist auch `AllowOverride None` für das Verzeichnis `/var/www/html` eingestellt.

SUSE

Bei SUSE fehlt in den Konfigurationsdateien eine explizite Zeichensatzeinstellung. Damit gilt `AddDefaultCharset off`, d. h., die `<meta>`-Informationen in den HTML-Dateien sind für die richtige Zeichensatzerkennung entscheidend. Ein geeigneter Ort zur Einstellung von `AddDefaultCharset` ist die Datei `/etc/apache2/mod_mime-defaults.conf`. Auch bei SUSE gilt `AllowOverride None` für das Verzeichnis `/srv/www/htdocs`. Sie können die Einstellung in `/etc/apache2/default-server.conf` verändern.

Logrotate

Die Logging-Dateien von Apache zählen bei vielen Servern zu den Dateien, die am schnellsten wachsen. Deswegen müssen Sie sich darum kümmern, dass die Logging-Dateien regelmäßig umbenannt, komprimiert und schließlich gelöscht werden. Genau diese Aufgabe erledigt das Programm Logrotate (siehe Abschnitt 21.7), das auf Linux-Servern in der Regel standardmäßig installiert ist.

Das Programm wird üblicherweise einmal täglich durch `/etc/cron.daily/logrotate` gestartet. In der Standardkonfiguration verarbeitet es die Apache-Logging-Dateien `/var/log/httpd/*.log` (Fedora/RHEL) bzw. `/var/log/apache2/*.log` (Debian/Ubuntu) einmal pro Woche, benennt sie in *name*`.`*nn* um und komprimiert sie. Die komprimierten Dateien werden für 52 Wochen archiviert und dann gelöscht.

Falls Sie bei der Konfiguration virtueller Hosts eigene Logging-Verzeichnisse definieren, müssen Sie in der Konfigurationsdatei `/etc/logrotate.d/apache2` die erste Zeile anpassen und dort die Orte der zusätzlichen Logging-Dateien angeben. Dabei sind auch Muster wie `/home/*/www-log/*.log` erlaubt.

```
# Datei /etc/logrotate.d/apache2
/var/log/apache2/*.log /home/meinefirma/www-log/*.log {
  weekly
  missingok
  rotate 52
  ...
}
```

35.2 Webverzeichnisse einrichten und absichern

Nach der Grundkonfiguration von Apache werden Sie in der Regel verschiedene Webverzeichnisse einrichten, die jene HTML- und PHP-Dateien enthalten, aus der sich Ihre Website zusammensetzt. Auf den folgenden Seiten gehe ich dabei von der Apache-Standardkonfiguration aus, wie Sie sie unter Ubuntu bzw. Debian vorfinden. Wenn Sie mit einer anderen Distribution arbeiten, gibt es bei der Standardkonfiguration kleine Variationen. Die hier präsentierten Schlüsselwörter und Arbeitstechniken gelten aber auch dort.

Ubuntu-Standardkonfiguration

Unter Ubuntu ist Apache so vorkonfiguriert, dass für die Standard-Website Dateien aus dem Verzeichnis `/var/www` verwendet werden. Die erforderlichen Einstellungen befinden sich in der Datei `/etc/apache2/sites-available/000-default.conf`.

```
# Datei /etc/apache2/sites-available/000-default.conf (Ubuntu)
<VirtualHost *:80>
  ServerAdmin      webmaster@localhost
  DocumentRoot     /var/www/
  ErrorLog         ${APACHE_LOG_DIR}/error.log
  CustomLog        ${APACHE_LOG_DIR}/access.log combined
<VirtualHost>
```

Eine Debian- bzw. Ubuntu-spezifische Besonderheit der Defaultkonfiguration besteht darin, dass alle Einstellungen in einer `<VirtualHost>`-Gruppe gebündelt sind. `<VirtualHost>`-Gruppen dienen dazu, Einstellungen für mehrere eigenständige Hosts (Websites) voneinander zu trennen (siehe Abschnitt 35.3). Der Host in der Datei `default` ist allerdings weder an eine IP-Adresse noch an einen Hostnamen gekoppelt und gilt aus diesem Grund für alle Webzugriffe, die nicht einem speziellen virtuellen Host zugeordnet werden können.

Host-Konfiguration

Mit den im Folgenden beschriebenen Schlüsselwörtern zur Konfiguration einer `<VirtualHost>`-Gruppe werden die Details des Hosts festgelegt – also die Herkunft der Daten, die E-Mail-Adresse des Administrators, der Ort der Logging-Dateien etc.

- `DocumentRoot` gibt an, in welchem Verzeichnis sich die HTML-Dateien befinden.
- `ServerAdmin` gibt die E-Mail-Adresse des Administrators des virtuellen Hosts an. Die Adresse wird z. B. bei Fehlermeldungen angezeigt. Sie sollten hier eine E-Mail-Adresse angeben, die tatsächlich aktiv ist. Üblich ist `webmaster@hostname`.
- `ServerSignatur` steuert, ob Apache bei selbst generierten Dokumenten (Fehlermeldungen, Verzeichnislisten etc.) am Ende eine Signatur hinzufügen soll. Die Signatur besteht aus der Apache-Version und dem Hostnamen. Mit `ServerSignatur=EMail` wird auch die E-Mail-Adresse des Administrators hinzugefügt.
- `LogLevel` bestimmt, in welchem Ausmaß Webserver-Probleme protokolliert werden sollen. Mögliche Werte reichen von `emerg` (nur kritische Fehler protokollieren, die zum Ende von Apache führen) bis `debug` (alles protokollieren, selbst Debugging-Texte). Sinnvolle Einstellungen sind in der Regel `error` oder `warn`. Letztere Einstellung gilt per Default.
- `ErrorLog` gibt den Dateinamen der Protokolldatei für Fehlermeldungen an.
- `CustomLog` gibt den Dateinamen des Zugriffsprotokolls an. In dieser Datei protokolliert Apache jede erfolgreiche Übertragung einer Datei. An den zweiten Parameter übergeben Sie entweder den Namen eines vordefinierten Loggingformats oder eine Zeichenkette mit eigenen Formatanweisungen. Die erlaubten Formatcodes sind hier beschrieben:

  http://httpd.apache.org/docs/2.4/de/mod/mod_log_config.html

  Unter Ubuntu sind in `apache2.conf` einige Formate vorkonfiguriert, z. B. `combined` oder `common`.
- `ErrorDocument` gibt an, wie Apache auf Fehler reagieren soll. Als ersten Parameter geben Sie die Fehlernummer an (z. B. 404 für *not found*), im zweiten Parameter den Namen einer lokalen Datei bzw. die Adresse einer externen Seite, die in diesem Fall angezeigt werden soll. Der Dateiname muss relativ zu `DocumentRoot` angegeben werden. Die wichtigsten Fehlercodes sind:

  400 *Bad Request*
  401 *Authorization Required*
  403 *Forbidden*
  404 *Not Found*
  500 *Internal Server Error*

  Eine Liste aller Apache-Statuscodes finden Sie hier:

  http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

  Standardmäßig ist `ErrorDocument` nicht konfiguriert. Um unschöne Fehlermeldungen zu vermeiden, sollten Sie sich die Mühe machen, eine Fehlerseite einzurichten und deren Ort mit `ErrorDocument` anzugeben.

- `Alias` stellt eine Zuordnung zwischen einem Webverzeichnis und einem beliebigen Verzeichnis der Festplatte (auch außerhalb von `DocumentRoot`) her. Beispielsweise bewirkt `Alias /mytool /usr/local/mytool`, dass bei Zugriffen auf *http://meinserver.de/mytool* die Dateien aus dem Verzeichnis `/urs/local/mytool` gelesen werden.

  In der Regel müssen Sie für jedes `alias`-Verzeichnis in einer `<Directory>`-Gruppe die Zugriffsrechte einstellen (siehe den folgenden Abschnitt). Zu `Alias` gibt es die Variante `ScriptAlias`, die zur Definition von Verzeichnissen mit CGI-Scripts dient.

Verzeichniskonfiguration

Im Anschluss an diese Einstellungen, die für den gesamten virtuellen Host gelten, können Sie in einer oder mehreren `<Directory "/verzeichnis/">`-Gruppen die Eigenschaften für einzelne Verzeichnisse Ihres Hosts einstellen. Die folgende Liste nennt hierfür nur die wichtigen Schlüsselwörter:

- `DirectoryIndex` gibt an, welche Datei Apache senden soll, wenn eine Adresse mit `/` endet und somit ein ganzes Verzeichnis betrifft (standardmäßig `index.html`). Es dürfen auch mehrere Dateien angegeben werden. In diesem Fall arbeitet Apache alle Angaben der Reihe nach bis zum ersten Treffer ab (z. B. `DirectoryIndex index.php index.html`).
- `Options` ermöglicht die Angabe diverser Optionen, die für das Verzeichnis gelten. Dazu zählen:

`ExecCGI`	CGI-Scripts ausführen
`FollowSymLinks`	symbolische Links verfolgen
`Includes`	Include-Dateien hinzufügen (Modul `mod_include`)
`Indexes`	Dateiliste anzeigen, wenn `index.html` fehlt
`MultiViews`	automatische Sprachauswahl (Modul `mod_negotiation`)

  Standardmäßig gilt in Apache die Einstellung `All`. Damit sind alle Optionen mit der Ausnahme von `MultiViews` aktiv. Die Ubuntu-Konfiguration ist etwas restriktiver: Für das gesamte Dateisystem gilt `Options FollowSymLinks`, für das `/var/www`-Verzeichnis gilt `Options Indexes FollowSymLinks MultiViews`.

  Um einzelne Optionen gegenüber den Voreinstellungen eines übergeordneten Verzeichnisses wieder zu deaktivieren, muss ein Minuszeichen vorangestellt werden. Ein vorangestelltes Pluszeichen ist ebenfalls erlaubt, hat aber keine Wirkung: Die Option ist genau so aktiviert, als wäre sie ohne Pluszeichen angegeben.

  Aus Sicherheitsgründen sollte für `Options` die Devise »Weniger ist mehr« gelten: Die Option `Indexes` verrät neugierigen Websurfern die Namen aller Dateien, die sich in einem Verzeichnis befinden, sofern Sie einmal `index.html` vergessen. Das

ist ein potenzielles Sicherheitsrisiko. `MultiView` brauchen Sie nur für mehrsprachige Websites mit automatischer Sprachauswahl. Bietet Ihre Seite so etwas nicht, können Sie auch auf diese Option verzichten.

- **`AllowOverride`** gibt an, welche Einstellungen verzeichnisspezifisch durch eine `.htaccess`-Datei verändert werden dürfen. Zur Auswahl stehen:

`AuthConfig`	Authentifizierungsverfahren einstellen
`FileInfo`	Datei- und Dokumenttypen einstellen
`Indexes`	Verzeichnisindex modifizieren
`Limit`	Zugriffsrechte ändern (`Allow`, `Deny`, `Order`)
`Options`	Verzeichnisoptionen ändern

  Standardmäßig sind in Apache alle Möglichkeiten aktiv, d. h., jede Option kann verändert werden. Ubuntu-spezifisch ist allerdings `None` voreingestellt (siehe `/etc/apache2/sites-available/default`).

Verzeichnisse absichern

Auf einen zentralen Punkt bin ich bisher noch nicht eingegangen: auf die Steuerung der Zugriffsrechte für Verzeichnisse. Die Apache-Versionen 2.2 und 2.4 unterscheiden sich hierbei deutlich.

Zugriffsrechte für Verzeichnisse (Apache 2.2)

In Apache 2.2 können Sie innerhalb der `<Directory>`-Gruppe mit `Order`, `Allow` und `Deny` einstellen, unter welchen Umständen Apache Dateien aus dem jeweiligen Verzeichnis lesen und weitergeben darf.

Zugriffsregeln gelten auch für alle Unterverzeichnisse, sofern nicht explizit in einer weiteren `<Directory>`-Gruppe andere Regeln definiert werden. Die Zugriffsregeln für das Verzeichnis `/` geben daher Standardregeln für das gesamte Dateisystem vor!

- **`Order Allow,Deny`** bedeutet, dass zuerst alle `Allow`- und dann alle `Deny`-Regeln ausgewertet werden. Wenn auf einen Seitenzugriff keine Regel angewendet werden kann, wird der Zugriff blockiert.
- **`Order Deny,Allow`** dreht die Reihenfolge der Regeln um. Beachten Sie aber: Wenn bei einem Seitenzugriff keine Regel passt, ist der Zugriff erlaubt! Diese Regel gilt in Apache standardmäßig.
- **`Allow from`** gibt an, von welchen Hostnamen bzw. IP-Adressen Zugriffe erlaubt sind – also beispielsweise `Allow from 213.214.215.216 bekannteseite.de`. IP-Adressbereiche können Sie in der Form 213.214 oder 213.214.0.0/255.255.0.0 oder 213.214.0.0/16 (für 213.214.*.*) angeben. Bei Hostnamen gilt `site.de` auch für `www.site.de`, `sub.site.de` etc. Die Regel `Allow from all` erlaubt jeden Zugriff.
- **`Deny from`** funktioniert gerade umgekehrt und blockiert den Zugriff für die angegebenen Hosts bzw. Adressen.

Per Default gilt `Order Deny,Allow`, und mangels anderer Regeln ist somit der gesamte Zugriff auf alle Verzeichnisse blockiert! Wenn Sie Webdateien in anderen Verzeichnissen unterbringen, vergessen Sie nicht, den Zugriff darauf zu erlauben.

Zugriffsrechte für Verzeichnisse (Apache 2.4)

Unter Apache 2.4 gelten die drei Schlüsselwörter `Order`, `Allow` und `Deny` als obsolet. Die Schlüsselwörter werden aber weiterhin vom Modul `mod_access_compat` verarbeitet. Dieses Modul steht bei den meisten Apache-2.4-Installationen zur Verfügung und stellt sicher, dass ein Apache-2.4-Update nicht die gesamte bisherige Konfiguration über den Haufen wirft.

Bei einer Neukonfiguration wird der Einsatz des neuen Schlüsselworts `Require` empfohlen. Die folgenden Beispiele zeigen verschiedene Anwendungsformen:

```
# erlaubt den Zugriff vom Rechner mit der IP-Adresse 192.168.0.2
Require ip 192.168.0.2

# erlaubt den Zugriff aus dem Adressbereich 10.0.*.*
Require ip 10.0

# erlaubt den Zugriff aus einem IPv6-Adressbereich
Require ip 2001:1234:789a:0471::/64

# erlaubt den Zugriff für einen bestimmten Hostnamen
Require host intern.meine-firma.de

# erlaubt den Zugriff für *.meine-firma.de
Require host meine-firma.de

# erlaubt den Zugriff von localhost (IPv4 und IPv6)
Require local

# erlaubt den Zugriff für authentifizierte Benutzer
Require valid-user

# erlaubt den Zugriff von überall
Require all granted

# blockiert jeden Zugriff
Require all denied
```

Wenn Sie für ein `<Directory>` mehrere Bedingungen formulieren, dann reicht es, wenn *eine* dieser Bedingungen erfüllt ist:

```
<Directory /var/www/cms>
  Require local
  Require ip 192.168
  Require host meine-firma.de
</Directory>
```

Mit `<RequireAll>` können Sie mehrere Bedingungen durch ein logisches Und kombinieren. Apache liefert die angeforderte Seite nur, wenn *alle* Bedingungen gleichzeitig zutreffen.

```
<Directory /var/www/internal-wiki>
  <RequireAll>
    Require valid-user
    Require ip 192.168.17
  </RequireAll>
</Directory>
```

Internet-Zugriff blockieren

Wenn Sie Apache zur firmeninternen Kommunikation einrichten, können Sie den Webzugriff auf das lokale Netzwerk beschränken. Wenn das lokale Netzwerk den Adressbereich 192.168.1.* und die lokale Domain `.sol` nutzt, sieht die richtige Konfiguration für `/var/www` so aus:

```
<Directory /var/www/>
  Options        Indexes FollowSymLinks MultiViews
  AllowOverride  None
  Order          Deny,Allow
  Deny           from all
  Allow          from 192.168.1
  Allow          from localhost
  Allow          from .sol
</Directory>
```

Zugriffsschutz durch Listen

Eine alternative Vorgehensweise besteht darin, mit `Listen` die IP-Adresse der lokalen Netzwerkschnittstelle anzugeben. Das setzt voraus, dass die IP-Adresse statisch ist. Nehmen wir an, der Server hat zwei Netzwerkschnittstellen: eine für die Verbindung in das Internet und eine zweite für das LAN mit der IP-Adresse 192.168.1.17. Dann bewirkt `Listen 192.168.1.17`, dass Apache nur noch auf Anfragen aus dem lokalen Netzwerk reagiert. `Listen` gilt allerdings für die gesamte Apache-Konfiguration, nicht nur für einzelne Verzeichnisse oder virtuelle Hosts.

Zugriffsschutz durch eine Firewall

Eine dritte Variante ist die Verwendung einer Firewall: Die Firewall muss den Empfang von Paketen verweigern, die von außen (also aus dem Internet) kommen und an die Ports 80 und 443 (`https`) gerichtet sind. Die Verwendung einer Firewall ist generell eine gute Idee, weil sie vollkommen unabhängig von Apache funktioniert.

Passwortschutz für Webverzeichnisse

Häufig sollen Webverzeichnisse nur nach einer Authentifizierung durch einen Benutzernamen und das dazugehörende Passwort freigegeben werden. Apache sieht hierfür ein einfaches Verfahren vor, das gleichermaßen in den Versionen 2.2 und 2.4 funktioniert.

Passwortdatei

Der erste Schritt hin zum Passwortschutz ist eine Passwortdatei. Die Datei sollte aus Sicherheitsgründen außerhalb aller Webverzeichnisse angelegt werden, um einen Zugriff per Webadresse auszuschließen. Das folgende Beispiel geht davon aus, dass die Passwortdatei im Verzeichnis `/var/www-private` gespeichert wird. Wenn Sie ein neues Verzeichnis einrichten, achten Sie darauf, dass Apache hierfür Leserechte hat.

Um eine neue Passwortdatei anzulegen, verwenden Sie das Kommando `htpasswd` mit der Option `-c` (*create*). Das Passwort wird selbstverständlich verschlüsselt.

```
root#  cd /var/www-private
root#  htpasswd -c passwords.pwd username
New password:  ********
Re-type new password:  ********
Adding password for user username
```

Weitere Benutzername/Passwort-Paare werden mit `htpasswd` ohne die Option `-c` hinzugefügt:

```
root#  cd /var/www-private
root#  htpasswd passwords.pwd name2
New password:  ********
Re-type new password:  ********
Adding password for user username
```

Konfiguration

Es gibt nun zwei Varianten, um Apache so zu konfigurieren, dass die Passwortdatei tatsächlich berücksichtigt wird. Die erste Variante setzt voraus, dass Sie die Konfiguration direkt in einer Apache-Konfigurationsdatei durchführen, unter Debian oder Ubuntu also in `/etc/apache2/sites-available/default` für die Standard-Website des Servers bzw. in `.../sitename` für einen virtuellen Host. Bei der zweiten Variante erfolgt die Konfiguration in der Datei `.htaccess`, die sich innerhalb des Webverzeichnisses befindet.

Damit die Passwortdatei von Apache berücksichtigt wird, müssen Sie in die `<Directory>`-Gruppe diverse Authentifizierungsoptionen einfügen. Wenn es für das zu schützende Verzeichnis noch keine eigene `<Directory>`-Gruppe gibt, legen Sie eine neue Gruppe an. Dabei werden automatisch alle Optionen vom übergeordneten Verzeichnis übernommen. Sie müssen also nur die Authentifizierungsoptionen hinzufügen. Die folgenden Zeilen geben hierfür ein Muster:

```
# in /etc/apache2/sites-available/xxx (Debian/Ubuntu)
...
# passwortgeschütztes Verzeichnis
<Directory "/var/www/admin/">
    AuthType     Basic
    AuthUserFile /var/www-private/passwords.pwd
    AuthName     "admin"
    Require      valid-user
</Directory>
```

Kurz eine Erklärung der Schlüsselwörter:

- `AuthType` gibt den Authentifizierungstyp an. Ich gehe hier nur auf den `Basic`-Typ ein.
- `AuthUserFile` gibt den Ort der Passwortdatei an.
- `AuthName` bezeichnet den Bereich (Realm), für den der Zugriff gültig ist. Der Sinn besteht darin, dass Sie nicht jedes Mal einen Login durchführen müssen, wenn Sie auf unterschiedliche Verzeichnisse zugreifen möchten, die durch dieselbe Passwortdatei geschützt sind. Sobald Sie sich mit einer bestimmten `AuthName`-Bezeichnung eingeloggt haben, gilt dieser Login auch für alle anderen Verzeichnisse mit diesem `AuthName`.
- `Require valid-user` bedeutet, dass als Login jede gültige Kombination aus Benutzername und Passwort erlaubt ist. Alternativ können Sie hier auch angeben, dass ein Login nur für ganz bestimmte Benutzer erlaubt ist:

  ```
  Require user name1 name2
  ```

.htaccess-Datei

Die oben skizzierte Vorgehensweise ist nur möglich, wenn Sie Zugang zu den Apache-Konfigurationsdateien haben, d. h., wenn Sie selbst der Webadministrator sind. Ist das nicht der Fall, kann eine gleichwertige Absicherung auch durch die Datei `.htaccess` erfolgen, die sich im zu schützenden Verzeichnis befindet. In dieser Datei müssen sich dieselben Anweisungen befinden, die vorhin innerhalb der `<Directory>`-Gruppe angegeben wurden, also `AuthType`, `AuthUserFile`, `AuthName` und `Require`.

.htaccess erfordert AllowOverride AuthConfig

`.htaccess`-Dateien werden nur beachtet, wenn innerhalb des Webverzeichnisses eine Veränderung der Authentifizierungsinformationen zulässig ist! Die (übergeordnete) `<Directory>`-Gruppe muss `AllowOverride AuthConfig` oder `AllowOverride All` enthalten.

35.3 Virtuelle Hosts

Für jede Website (für jeden Host) ein eigener Webserver – das wäre angesichts der Leistungsfähigkeit aktueller Rechner eine Verschwendung von Ressourcen! Mit Apache können Sie dank sogenannter virtueller Hosts nahezu beliebig viele Websites parallel einrichten. Solange die Gesamtzugriffszahlen nicht an die Limits des Rechners gehen, bemerkt kein Anwender, dass die Websites in Wirklichkeit alle auf demselben Rechner laufen.

Aus technischer Sicht gibt es drei Verfahren, wie Apache entscheidet, an welchen virtuellen Host eine Webanfrage gerichtet ist. Als Ausgangspunkt dient in jedem Fall der vom Browser an den Server übertragene HTTP-Header.

- **Namensbasierte virtuelle Hosts:** Apache erkennt die gewünschte Website anhand des im HTTP-Header enthaltenen Hostnamens. Diese Variante ist am einfachsten zu realisieren und am weitesten verbreitet.
- **IP-basierte virtuelle Hosts:** Apache erkennt die gewünschte Website anhand der IP-Adresse im Header. Diese Vorgehensweise ist mit einem gravierenden Nachteil verbunden: Jeder virtuelle Host erfordert eine eigene IP-Adresse, und die sind für IPv4 Mangelware. Dennoch gibt es Gründe, IP-basierte Hosts einzurichten: So ist eine eigene IP-Adresse zwingend erforderlich, wenn die Website Daten auch verschlüsselt übertragen soll (`https`). Auch wenn Sie für Ihre Website Funktionen zur Bandbreitenregulierung realisieren möchten bzw. müssen, brauchen Sie zumeist eine eindeutige IP-Adresse.
- **Port-basierte virtuelle Hosts:** Apache erkennt aufgrund der Port-Nummer die gewünschte Website. Diese Variante ist in der Praxis unüblich, weil die Port-Nummer als Teil der Webadresse angegeben werden muss. Das sieht unübersichtlich aus und eignet sich bestenfalls für eine technisch versierte Zielgruppe , z. B. für Administratoren.

Ich beziehe mich in diesem Abschnitt wiederum auf die Default-Konfiguration von Debian bzw. Ubuntu. Dort ist es üblich, für jeden virtuellen Host eine eigene Konfigurationsdatei zu verwenden.

Wenn Sie Ihren Webserver unter Fedora oder RHEL einrichten, kommen naturgemäß dieselben Apache-Schlüsselwörter zum Einsatz. Allerdings erfolgen sämtliche Einstellungen wahlweise in `/etc/httpd/conf/httpd.conf` oder in `/etc/httpd/conf.d/sitename.conf`.

Virtuelle Hosts einrichten

NameVirtualHost (Apache 2.2)

In Apache 2.2 muss die Konfiguration an einer Stelle die Anweisung `NameVirtualHost *:80` enthalten. Das ist die Voraussetzung dafür, dass Apache 2.2 namensbasierte Hosts unterstützt. Das *-Zeichen bedeutet, dass Apache alle hereinkommenden Webanfragen im Hinblick auf virtuelle Hosts auswertet. Wenn Ihr Server mit mehreren IP-Adressen ausgestattet ist und nur eine IP-Adresse für namensbasierte virtuelle Hosts gedacht ist, müssen Sie bei `NameVirtualHost` diese Adresse explizit angeben.

Ab Apache 2.4 ist das Schlüsselwort `NameVirtualHost` nicht mehr erforderlich. Apache erkennt bei der Analyse der Konfigurationsdateien automatisch, dass namensbasierte virtuelle Hosts verwendet werden.

Host-Dateien (Debian, Ubuntu)

Unter Debian und Ubuntu ist die Standard-Website in `/etc/apache2/sites-available/default` als virtueller Host definiert. Um einen neuen virtuellen Host zu definieren, legen Sie unter Debian oder Ubuntu eine neue Datei im Verzeichnis `/etc/apache2/sites-available/` an. Diese Datei sollte genau eine `<VirtualHost>`-Gruppe enthalten. Die drei folgenden Listings geben je ein Beispiel für einen namens-, IP- und port-basierten Host.

Namensbasierte virtuelle Hosts

`ServerName` gibt den Namen des Hosts an. Dieser Hostname muss in den Header-Informationen einer Webanfrage enthalten sein, damit Apache darauf reagiert. Optional können Sie mit `ServerAlias` weitere Namen nennen. Beispielsweise empfiehlt sich zur Einstellung `ServerName www.meinserver.de` die Ergänzung `ServerAlias meinserver.de`, damit ein virtueller Host mit oder ohne die vorangestellten Buchstaben `www.` verwendet werden kann.

```
# /etc/apache2/sites-available/beispiel-named-host (Debian/Ubuntu)
<VirtualHost *:80>
  DocumentRoot /var/verzeichnis1/
  ServerName   www.firma-1.de
  ServerAlias  firma-1.de
  ...
</VirtualHost>
```

Unter Apache 2.2 müssen Sie außerdem darauf achten, dass die Adressangabe in `<VirtualHost>` mit der von `NameVirtualHost` übereinstimmt.

IP- und port-basierte virtuelle Hosts

Bei IP- und port-basierten Hosts muss die IP-Adresse mit einer der IP-Adressen des Servers übereinstimmen:

```
# /etc/apache2/sites-available/beispiel-IP-host  (Debian/Ubuntu)
<VirtualHost 213.214.215.216:80>
  DocumentRoot /var/verzeichnis2/
  ServerName   www.firma-2.com
  ...
</VirtualHost>
# /etc/apache2/sites-available/beispiel-port-host  (Debian/Ubuntu)
<VirtualHost 213.214.215.216:12001>
  DocumentRoot /var/verzeichnis3/
  ServerName   www.admin-firma3.de
  ...
</VirtualHost>
```

Vergessen Sie nicht, Zusatzports mit listen anzugeben!

Die Adress- und Port-Angaben in `<VirtualHost>` haben keinen Einfluss darauf, welche IP-Adressen und Ports Apache überwacht. In der Ubuntu-Standardkonfiguration verarbeitet Apache Anfragen von beliebigen Adressen für die Ports 80 und 443 (`https`). Die entsprechende Konfiguration erfolgt in `/etc/apache2/ports.conf`. Wenn Apache weitere Ports überwachen soll, müssen Sie `ports.conf` entsprechend erweitern. Weitere Informationen zur Apache-Konfiguration für virtuelle Hosts finden Sie hier:

http://httpd.apache.org/docs/2.2/de/vhosts
http://httpd.apache.org/docs/2.4/de/vhosts

Virtuelle Hosts aktivieren

Um einen virtuellen Host zu aktivieren bzw. später wieder zu deaktivieren, führen Sie nun unter Debian/Ubuntu `a2ensite name` bzw. `a2dissite name` aus und fordern Apache dann zum Neuladen der Konfigurationsdateien auf:

```
root# a2ensite beispiel-named-host    (Debian/Ubuntu)
root# service apache2 reload
```

Theoretisch ist es möglich, mit `a2dissite` auch die Standard-Website des Servers zu deaktivieren. Das sollten Sie aber nicht tun, weil die Datei `/etc/apache2/sites-available/default` diverse Standardeinstellungen für Apache enthält!

Sobald Sie virtuelle Hosts eingerichtet haben, wird die in `sites-available/default` definierte Standard-Website nur noch angezeigt, wenn Webanfragen für keine der virtuellen Hosts zutreffen.

Unter Fedora bzw. RHEL entfallen die Kommandos `a2ensite`/`a2dissite`, weil sich alle Angaben zu den virtuellen Hosts in der zentralen Konfigurationsdatei `httpd.conf` oder in eigenen Dateien im Verzeichnis `conf.d` befinden. Dort durchgeführte Änderungen aktivieren Sie mit dem folgenden Kommando:

```
root# service httpd reload                    (RHEL, Fedora)
```

Beispiel

Dieser Abschnitt beschreibt, wie Sie auf einem Debian- oder Ubuntu-Server den neuen virtuellen Host `firma-123.de` einrichten – zusammen mit einem neuen Login `firma123`, sodass Ihr Kunde, Freund etc. den virtuellen Host selbst administrieren kann. Dabei gehe ich davon aus, dass die Web- und Logdateien des virtuellen Hosts innerhalb des Heimatverzeichnisses des neuen Benutzers `firma123` angeordnet werden. Ebenso gut ist es möglich, zu diesem Zweck ein neues Verzeichnis `/var/www-firma123` einzurichten und dem Benutzer hierfür Schreibrechte zu geben.

Der erste Schritt besteht darin, einen neuen Account einzurichten, ein Passwort zuzuweisen und die erforderlichen Verzeichnisse zu erzeugen. In den folgenden Kommandos müssen Sie natürlich `firma123` durch den tatsächlichen Benutzernamen ersetzen!

```
root#  adduser firma123
root#  passwd firma123
Enter new UNIX password:   ********
Retype new UNIX password:  ********
passwd: password updated successfully
root#  mkdir                  ~firma123/www
root#  chown firma123:firma123 ~firma123/www
root#  mkdir           ~firma123/www-log
root#  chown root:root ~firma123/www-log
root#  chmod go-w      ~firma123/www-log
```

Im zweiten Schritt erzeugen Sie eine neue Datei im Verzeichnis `sites-available`, die so ähnlich wie das folgende Muster aufgebaut ist. Abermals müssen Sie `firma123` durch den tatsächlichen Benutzernamen ersetzen und außerdem statt `firma-123.de` den tatsächlichen Hostnamen angeben. Mit `AllowOverride AuthConfig File` geben Sie Ihrem Kunden relativ weitreichende Möglichkeiten, die Konfiguration der Website durch eine `.htaccess`-Datei anzupassen. Wenn Sie das nicht möchten, müssen Sie diverse Konfigurationsdetails absprechen und fix einstellen.

```
# /etc/apache2/sites-available/firma-123.de
<VirtualHost * >
  DocumentRoot   /home/firma123/www/
  ServerName     firma-123.de
  ServerAlias    www.firma-123.de
  ErrorLog       /home/firma123/www-log/error.log
  CustomLog      /home/firma123/www-log/access.log combined
  ServerAdmin    webmaster@firma-123.de
  ErrorDocument  404 /not-found.html
  <Directory  "/home/firma123/www/" >
    AllowOverride AuthConfig File
  </Directory>
</VirtualHost>
```

Zur Aktivierung der Website führen Sie die folgenden Kommandos aus:

```
root#  a2ensite firma-123.de
root#  service apache2 reload
```

Ihr Kunde muss nun nur noch die DNS-Konfiguration seiner Domain anpassen: Die zugeordnete IP-Adresse muss mit der Ihres Servers übereinstimmen. Sobald das der Fall ist, beantwortet Ihr Webserver alle Anfragen, die an *www.firma-123.de* gerichtet sind.

Zugriffsrechte

Wie ich bereits erwähnt habe, läuft Apache aus Sicherheitsgründen nicht mit `root`-Rechten, sondern unter einem Account mit eingeschränkten Rechten (`www-data` bei Debian/Ubuntu, `apache` bei Fedora/RHEL bzw. `wwwrun` bei SUSE). Stellen Sie die Zugriffsrechte der Webdateien so ein werden, dass Apache diese lesen kann!

Wenn Apache einzelne Dateien auch verändern soll (z. B. über ein PHP-Script), ordnen Sie den Verzeichnissen und Dateien die Gruppe `www-data`/`apache`/`wwwrun` zu und geben den Gruppenmitgliedern Schreibrechte (`chmod g+w`). Unter Fedora und RHEL müssen Sie außerdem den SELinux-Kontext korrekt einstellen (siehe Abschnitt 35.1).

Logging

Im obigen Beispiel werden alle Fehler- und Zugriffsmeldungen in eigenen Dateien für den virtuellen Host gespeichert. Diese Vorgehensweise erleichtert die Auswertung der Logging-Dateien. Allerdings ist die Anzahl der offenen Datei-Handles für Apache (wie für jeden anderen Linux-Prozess) beschränkt. Wenn Sie sehr viele virtuelle Hosts einrichten, müssen Sie alle Zugriffe in einer zentralen Datei protokollieren und diese Datei dann durch ein anderes Programm in kleinere Dateien je nach Host zerlegen. Weitere Informationen zu diesem Thema finden Sie hier:

http://httpd.apache.org/docs/2.4/vhosts/fd-limits.html

Test

Virtuelle Hosts setzen voraus, dass die DNS-Konfiguration stimmt! Um die im vorigen Abschnitt beschriebene Website *firma-123.de* zu testen, muss der DNS-Eintrag der Domain *firma-123.de* auf die IP-Adresse Ihres Webservers zeigen. Änderungen am DNS-Eintrag kann nur der Eigentümer der Domain durchführen. Die meisten Domain-Händler bieten dazu entsprechende Werkzeuge an. Beachten Sie, dass DNS-Änderungen nicht sofort gelten. Die Synchronisation der vielen, weltweit verteilten Nameserver kann etliche Stunden dauern (auch wenn es oft schneller geht).

Bei Serverumbauten oder -umzügen besteht oft der Wunsch, den neuen Server zuerst in Ruhe zu testen, bevor die DNS-Änderung tatsächlich durchgeführt wird. Der einfachste Weg besteht darin, den neuen virtuellen Host anfänglich nicht namensbasiert, sondern port-basiert zu konfigurieren. Dazu entfernen Sie die `ServerName`- und `ServerAlias`-Anweisungen und geben im `<VirtualHost>`-Tag statt des Sterns die IP-Adresse des Servers sowie eine freie Port-Nummer an, beispielsweise so:

```
<VirtualHost 213.214.215.216:12001 >
```

Standardmäßig verarbeitet Apache nur Anfragen, die an die Ports 80 und 443 (für `https`) gerichtet sind. Damit Apache auch den hier eingesetzten Port 12001 berücksichtigt, müssen Sie in `/etc/apache2/ports.conf` eine weitere Zeile mit `Listen 12001` einfügen. Nun ist noch das Kommando `service apache2 reload` erforderlich, damit Apache die veränderte Konfiguration berücksichtigt. Jetzt können Sie den neuen Webauftritt mit Ihrem Webbrowser testen, indem Sie die IP-Adresse des Servers samt der Port-Nummer 12001 angeben, also beispielsweise *http://213.214.215.216:12001*.

35.4 Verschlüsselte Verbindungen (HTTPS)

Für den gewöhnlichen Austausch von Daten zwischen Webserver und Browser kommt das Protokoll HTTP zum Einsatz. Es ist einfach, überträgt aber alle Daten unverschlüsselt. Damit ist es ungeeignet, um Kreditkartennummern oder andere vertrauliche Daten zu übermitteln. Für diesen Zweck kommt das Protokoll HTTPS zum Einsatz. HTTPS vereint die Protokolle *Hypertext Transfer Protocol* (HTTP) mit *Secure Sockets Layer* (SSL) und fügt HTTP so Verschlüsselungsfunktionen hinzu. Dieser Abschnitt erklärt, wie Sie Apache für HTTPS-Verbindungen konfigurieren.

Zertifikate

Bevor Sie nun mit den Konfigurationsarbeiten beginnen, brauchen Sie nur noch ein Server-Zertifikat. Und an dieser Stelle muss ich etwas ausholen ...

Grundlagen

Die Verschlüsselung der Daten erfolgt auf der Basis asymmetrischer Verschlüsselungsverfahren. Die Grundidee besteht darin, dass es ein Schlüsselpaar gibt, das aus einem privaten (geheimen) und einem öffentlichen Schlüssel besteht. Der öffentliche Schlüssel eignet sich nur zum *Ver*schlüsseln von Daten. Zum *Ent*schlüsseln ist der private Schlüssel erforderlich. Auf die Details dieser Verfahren gehe ich hier nicht ein – sie wurden schon unzählige Male beschrieben und erklärt, unter anderem auch in der Wikipedia.

Beim Verbindungsaufbau zwischen dem Client (also einem Webbrowser) und dem Server (Apache) wird zuerst auf der Basis einer Zufallszahl vom Client und des öffentlichen Schlüssels vom Server ein gemeinsamer Schlüssel ausgehandelt (Handshake-Verfahren). Dieser *Session Key* wird dann zur Verschlüsselung der gesamten weiteren Kommunikation eingesetzt.

Der nach heutigem Wissensstand nahezu abhörsichere Datenaustausch ist aber nur *ein* Punkt zur Verbesserung der Sicherheit. Der ebenso wichtige zweite Punkt besteht darin, dass der Anwender Gewissheit haben muss, dass er mit dem richtigen Partner kommuniziert. Was nützt es, wenn die Daten für das Online-Banking zwar abhörsicher übertragen werden, aber statt zur Bank direkt in die Hände eines Betrügers gelangen?

Aus diesem Grund enthält ein Server-Zertifikat nicht nur den öffentlichen Schlüssel des Servers, sondern auch Daten über die Website sowie eine Art Unterschrift einer Zertifizierungseinrichtung. Deren Aufgabe ist es, die Identität des Zertifikatbewerbers anhand einer Passkopie, eines Gewerbescheins etc. zu überprüfen. Dieser Kontrollprozess macht Server-Zertifikate leider relativ teuer.

Wie vertrauenswürdig ein Zertifikat ist, hängt von der Vertrauenswürdigkeit der Authentifizierungsstelle ab. Bekannte Webbrowser wie Firefox oder Internet Explorer akzeptieren nur Zertifikate, die von etablierten Authentifizierungseinrichtungen ausgestellt wurden (z. B. Verisign oder Thawte). Bei anderen Zertifikaten werden unübersehbare Warnungen angezeigt. Mit etwas Hartnäckigkeit kann man den Webbrowser zwar dennoch dazu bringen, auch unsichere Zertifikate zu akzeptieren, ein florierendes Online-Geschäft ist auf dieser Basis aber unmöglich. Mit anderen Worten: Für ernsthafte Geschäftsanwendungen ist ein autorisiertes Zertifikat unabdingbar.

Ein eigenes Zertifikat erstellen

Nachdem ich Sie gerade zu überzeugen versucht habe, ein »richtiges« Zertifikat zu erwerben, erkläre ich Ihnen jetzt, wie Sie ein Zertifikat selbst erstellen können. Es gibt gute Gründe für diesen scheinbaren Sinneswandel: Für erste Experimente reicht ein selbst erstelltes Zertifikat vollkommen aus. Außerdem lässt sich ein eigenes Zertifikat in wenigen Minuten erstellen, während die Erteilung eines autorisierten Zertifikats erfahrungsgemäß tage-, wenn nicht wochenlang dauert. Diese Wartezeit nutzen Sie am besten, indem Sie sich mit den wichtigsten Stolperfallen vertraut machen. Wenn grundsätzlich alles funktioniert, können Sie Ihr eigenes Zertifikat mühelos durch ein »richtiges« ersetzen.

Als Erstes installieren Sie das Paket `openssl`. Es enthält das gleichnamige Kommando, mit dem Sie unter anderem Schlüssel und Zertifikate erstellen können.

```
root#  apt-get install openssl  bzw.  yum install openssl
```

Das folgende Kommando erzeugt eine Datei, die sowohl den privaten als auch den öffentlichen Schlüssel enthält. Damit der private Schlüssel nicht im Klartext gelesen werden kann, wird die Schlüsseldatei selbst verschlüsselt. Dazu müssen Sie eine sogenannte *Passphrase* angeben, also eine möglichst lange bzw. aus mehreren Wörtern bestehende Zeichenkette. Im Folgenden kehre ich dennoch zum gebräuchlicheren Begriff »Passwort« zurück, auch wenn es sich vielleicht um mehrere Wörter handelt.

```
root#  openssl genrsa -des3 -out server.key 1024
...
Enter pass phrase for server.key:  ******************
Verifying - Enter pass phrase for server.key:  ******************
```

In Zukunft müssen Sie jedes Mal, wenn Sie den privaten Schlüssel einsetzen möchten, das Passwort angeben. Da auch Apache den privaten Schlüssel benötigt, müssten Sie das Passwort auch bei jedem Start von Apache angeben. Das ist für den Server-Betrieb natürlich inakzeptabel. Das folgende Kommando entfernt daher die Verschlüsselung. `server.csr` enthält jetzt den privaten und den öffentlichen Schlüssel im Klartext. Achten Sie darauf, dass nur `root` diese Datei lesen kann! Wenn diese

Datei in fremde Hände gerät, ist Ihr Serverzertifikat wertlos, und Sie müssen es widerrufen!

```
root#  openssl rsa -in server.key -out server.pem
Enter pass phrase for server.key:  ******************
writing RSA key
root#  chmod 400 server.pem
```

Schon etwas mehr Arbeit macht es, das Zertifikat zu erstellen. Sie müssen dabei unter anderem angeben, in welchem Land und in welchem Ort Sie wohnen, wie Sie heißen etc. Entscheidend ist die Frage nach dem *Common Name*: Hier ist nicht Ihr Name gefragt, sondern der exakte Name Ihrer Website in der Form, in der er für verschlüsselte Verbindungen verwendet wird. Manche Websites verwenden für verschlüsselte Verbindungen eine eigene Subdomain (z. B. `banking.ing-diba.de`), andere nicht (z. B. `www.amazon.de`). Wie auch immer, das Zertifikat gilt nur für eine bestimmte Schreibweise. Sie können also beispielsweise ein Zertifikat für `www.firma-abc.de` nicht auch für `firma-abc.de` verwenden (oder umgekehrt)!

In das Zertifikat fließt auch der öffentliche Schlüssel ein, den das `openssl`-Kommando aus `server.key` extrahiert:

```
root#  openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:  ******************
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN. There are quite a few fields but you can leave
some blank. For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:             DE
State or Province Name (full name) [...]:      .
Locality Name (eg, city) []:                   Berlin
Organization Name (eg, company) [Sample Ltd]:  Max Muster
Organizational Unit Name (eg, section) []:     .
Common Name (eg server FQDN or YOUR name) []:  www.firma-abc.de
Email Address []:                              webmaster@firma-abc.de

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:                       .
An optional company name []:                   .
```

Mit dem nächsten Kommando unterschreiben Sie Ihr Zertifikat selbst. Bei einem »richtigen« Zertifikat erfolgt dieser Vorgang – natürlich nach einer Kontrolle der von Ihnen vorgelegten Dokumente – durch die Authentifizierungseinrichtung. Zur Unterschrift wird dann der Schlüssel der Authentifizierungsstelle verwendet.

Standardmäßig gilt das fertige Zertifikat nur für 30 Tage. Die Option `-days 1900` verlängert den Gültigkeitszeitraum auf circa fünf Jahre.

```
root#  openssl x509 -req -days 1900 -in server.csr -signkey server.key \
                    -out server.crt
Signature ok
subject=/C=DE/L=Berlin/O=Max Muster/CN=www.firma-abc.de/
  emailAddress=webmaster@firma-abc.de
Getting Private key
Enter pass phrase for server.key:  ******************
```

Physikalisch gesehen, handelt es sich bei den erzeugten Schlüsseln und Zertifikaten um relativ kleine Textdateien. Um die in einem Zertifikat enthaltenen Daten im Klartext anzuzeigen, verwenden Sie das Kommando `openssl x509 -text`. Die folgenden Ausgaben sind aus Platzgründen gekürzt.

```
root#  ls -l
...   696 ... server.csr   (Zertifikat ohne Unterschrift)
...   963 ... server.key   (verschlüsselter privater Schlüssel)
...   887 ... server.pem   (unverschlüsselter privater Schlüssel)
...   936 ... server.crt   (Zertifikat mit Unterschrift)
root#  cat server.crt
-----BEGIN CERTIFICATE-----
MIICWTCCAcICCQCL6ExhrQiELDANBgkqhkiG9w0BAQUFADBxMQswCQYDVQQGEwJB ...
-----END CERTIFICATE-----
root#  openssl x509 -text -in server.crt
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number:
      8b:e8:4c:61:ad:08:84:2c
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=DE, L=Berlin, O=Max Muster, CN=www.firma-abc.de/
            emailAddress=webmaster@firma-abc.de
    Validity
     Not Before: Oct 28 14:03:18 2013 GMT
     Not After : Jan 10 14:03:18 2019 GMT
    Subject: C=DE, L=Berlin, O=Max Muster, CN=www.firma-abc.de/
             emailAddress=webmaster@firma-abc.de
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
            00:ed:1f:08:cb:f4:4d:ef:a6:f6:0a:be:b3:c2:92: ...
        Exponent: 65537 (0x10001)
  Signature Algorithm: sha1WithRSAEncryption
      05:46:af:5c:12:84:28:59:e4:8f:db:2d:2d:0f:4a:3c:0e:84: ...
```

Kostenlose Zertifikate

Anbieter wie *https://www.startssl.com* oder *http://www.cheapssls.com* bieten kostenlose bzw. sehr preisgünstige Zertifikate an. Die Besucher Ihrer Website bekommen damit die Gewissheit, dass sie wirklich mit *http://ihre-website.de* kommunizieren und nicht mit einem anderen Host. Bei derartigen Zertifikaten findet nur eine Domain-Validierung statt. Es wird nicht überprüft, wer für diese Website wirklich verantwortlich ist. Es kann sich also auch jeder Betrüger mühelos ein derartiges Zertifikat beschaffen. Ein weiterer Nachteil ist die begrenzte Gültigkeitsdauer, z. B. maximal ein Jahr bei StartSSL.

Trotz dieser Einschränkungen sind Zertifikate von Firmen wie StartSSL oder CheapSSLs einem selbst erzeugten Zertifikat oft vorzuziehen: Die meisten Webbrowser akzeptieren die Zertifikate ohne die abschreckenden Warnungen, die bei selbst erstellten Zertifikaten üblich sind. Die vom Webbrowser angezeigte Sicherheitsstufe ist zwar gering und es wird kein grüner Balken mit dem Firmennamen in der Adressleiste angezeigt, aber immerhin gelingt eine verschlüsselte Kommunikation bei den meisten Webbrowsern auf Anhieb.

Kostenlose bzw. preisgünstige Domain-Zertifikate sind damit ein Kompromiss zwischen vollwertigen, aber teueren Zertifikaten mit Identitätsüberprüfung und selbst erstellten Zertifikaten. Erwarten Sie aber nicht, dass das Erstellen der Zertifikatdateien einfacher ist als mit dem `openssl`-Kommando: Gerade die StartSSL-Website ist ausgesprochen unübersichtlich zu bedienen. Um die Kommunikation zwischen StartSSL und dem Browser abzusichern, wird ein eigener Schlüssel auf Ihrem Computer installiert. Dieser Schlüssel ist die Voraussetzung für jeden weiteren Login. Verwenden Sie nach Möglichkeit Firefox; damit bereitet StartSSL nach meinen Erfahrungen die geringsten Probleme.

Apache-Konfiguration für den HTTPS-Betrieb

mod_ssl

Die für das Protokoll HTTPS erforderlichen Apache-Funktionen befinden sich im Modul `mod_ssl`. Unter Debian oder Ubuntu ist dieses Modul standardmäßig installiert und muss nur aktiviert werden:

```
root#  a2enmod ssl
root#  service apache2 restart
```

Unter Fedora bzw. RHEL müssen Sie das SSL-Modul zuerst installieren:

```
root#  yum install mod_ssl
root#  service httpd restart
```

HTTPS-VirtualHost

Apache muss die Schlüssel- und Zertifikatdatei lesen – daher liegt es nahe, die beiden Dateien in das Apache-Konfigurationsverzeichnis zu kopieren:

```
root#  cp server.pem server.crt /etc/apache2
```

Als Nächstes müssen Sie `httpd.conf` (Fedora, RHEL) um einen `VirtualHost`-Eintrag erweitern bzw. die entsprechenden Zeilen in eine neue Datei in `/etc/apache2/sites-available` einfügen. Bei Debian und Ubuntu wird eine entsprechende Musterdatei gleich mitgeliefert (`default-ssl`). Sie können diese Datei als Ausgangsbasis für eine eigene Site-Datei verwenden, der Sie zur besseren Unterscheidbarkeit von anderen Site-Dateien `ssl` oder `https` voranstellen, also beispielsweise `ssl.firma-abc.de`.

Die folgenden Zeilen zeigen eine minimale Konfiguration, bei der parallel zur Default-Website (HTTP) eine HTTPS-Seite eingerichtet wird. Für beide Seiten kommt dieselbe IP-Adresse zum Einsatz. Die Unterscheidung erfolgt durch die in der `VirtualHost`-Zeile eingestellte Port-Nummer 443.

`SSLEngine on` aktiviert die Verschlüsselungsfunktionen. `SSLxxxFile` gibt an, wo sich die Dateien mit dem Zertifikat und dem privaten Schlüssel befinden. `SSLProtocol` und `SSLCipherSuite` bestimmen, welche Version des SSL-Protokolls bzw. welcher Mechanismus zur Erzeugung des gemeinsamen Session Keys eingesetzt werden soll. In der Regel tauschen Apache und der Webbrowser Informationen darüber aus, welche Protokolle sie jeweils unterstützen, und verwenden dann das sicherste Verfahren, das beide beherrschen. Nur wenn es gute Gründe dafür gibt – etwa, weil Sie bestimmte ältere Protokolle/Verfahren nicht akzeptieren möchten –, sollten Sie hier explizite Vorgaben machen.

```
# z.B. in /etc/httpd/conf/httpd.conf (Fedora/RHEL)
# oder in /etc/apache2/sites-available/ssl.firma-abc.de
<VirtualHost _default_:443>
  ServerName             www.firma-abc.de
  DocumentRoot           /var/www/
  SSLEngine              on
  SSLCertificateFile     /etc/apache2/server.crt
  SSLCertificateKeyFile  /etc/apache2/server.pem
  SSLProtocol            all -SSLv2
  SSLCipherSuite         HIGH:MEDIUM
  <Directory /var/www/>
    AllowOverride  None
    # Apache 2.2
    Order          allow,deny
    Allow          from all
    # Apache 2.4
    Require all granted
  </Directory>
</VirtualHost>
```

Zur Aktivierung der HTTPS-Site müssen Sie Apache dazu auffordern, die Konfiguration neu einzulesen. Falls Sie die HTTPS-Datei unter Debian/Ubuntu in einer eigenen Konfigurationsdatei in `/etc/apache2/sites-available` durchgeführt haben, müssen Sie diese Datei aktivieren:

```
root#  service httpd restart          (Fedora/RHEL)
root#  a2ensite ssl.firma-abc.de      (Debian/Ubuntu)
root#  service apache2 restart        (Debian/Ubuntu)
```

Wenn Sie erstmals von einem Betrieb ohne SSL auf einen Betrieb mit SSL umstellen, reicht ein Neueinlesen der Konfigurationsdateien nicht aus. Damit das SSL-Modul geladen wird, müssen Sie `restart` angeben, nicht `reload`!

SSLCertificate-ChainFile

Die beiden in der vorhin abgedruckten Apache-Konfiguration verwendeten `SSLCertificate`-Schlüsselwörter sind sowohl für selbst erstellte Zertifikate als auch für Zertifikate von großen, anerkannten Zertifizierungsstellen (Thawte, VeriSign) ausreichend.

Wenn Sie hingegen ein Zertifikat einer Zertifizierungsstelle verwenden, die dem Webbrowser nicht standardmäßig bekannt ist, müssen Sie an den Browser Zusatzinformationen übergeben, wie er Ihre Zertifikate überprüfen kann. Das ist vor allem bei vielen kleineren Zertifizierungsstellen der Fall, unter anderem auch bei StartSSL. Genau genommen geht es hier um Informationen, welche anerkannte Zertifizierungsstelle wiederum Ihrer Zertifizierungsstelle vertraut. Der Browser muss in der Lage sein, eine Vertrauenskette bis zu einer Zertifizierungsstelle herzustellen, die ihm bekannt ist. Vergessen Sie diese Zusatzfunktionen, beklagt sich der Webbrowser beim Besuch Ihrer Seite, dass der Verbindung nicht vertraut wird, weil keine Zertifikatsausstellerkette angegeben wurde.

Abhilfe schaffen die Schlüsselwörter `SSLCertificateChainFile` und `SSLCACertificateFile`, mit denen Sie an Apache Zertifikate Ihrer Zertifizierungsstelle übergeben (Certification Authority, daher die Abkürzung CA). Die erforderlichen Zertifikatdateien stellt Ihnen Ihre Zertifizierungsstelle zum Download zur Verfügung. Nachdem Sie die Dateien so auf Ihrem Rechner eingerichtet haben, dass Apache sie lesen kann, ändern Sie die Konfiguration wie folgt und führen dann `service apache2/httpd reload` aus.

```
...
SSLCertificateFile      /etc/apache2/server.crt
SSLCertificateKeyFile   /etc/apache2/server.pem
SSLCertificateChainFile /etc/apache2/sub.class1.server.ca.pem
SSLCACertificateFile    /etc/apache2/ca.pem
...
```

Diese Zusatzinformationen ermöglichen es dem Webbrowser, die Korrektheit der von Ihnen benutzten Zertifikate zu überprüfen.

Mehrere HTTPS-Sites

Ein wesentlicher Nachteil von HTTPS besteht darin, dass Sie bei mehreren HTTPS-Websites für jede Site eine eigene IP-Adresse benötigen. Sie müssen die IP-Adressen beim `VirtualHost`-Schlüsselwort explizit angeben. Apache kontrolliert dies

bereits beim Einlesen der Konfigurationsdateien und warnt gegebenenfalls vor Adresskollisionen.

```
<VirtualHost 1.2.3.4:443>
  ServerName              www.noch-eine-firma.de
  DocumentRoot            /var/www-secure
  SSLEngine               on
  ...
</VirtualHost>
```

35.5 Awstats und Webalizer

Wenn Sie eine Website betreiben, wollen Sie in der Regel auch wissen, wie viele Besucher Sie haben. Die beiden populärsten Programme zur Ermittlung einer Zugriffsstatistik sind Awstats und Webalizer. Diese beiden Programme zur Webanalyse werten die Apache-Logging-Dateien aus. Die Auswertungsergebnisse können Sie dann mit einem Webbrowser ansehen.

Eine Empfehlung für eines der beiden Programme ist schwierig: Awstats ist eigentlich das modernere Programm. Es liefert ausführlichere und häufig auch genauere Ergebnisse. Andererseits ist der Konfigurationsaufwand relativ hoch, außerdem sind die Sicherheitsrisiken bei einer Standardkonfiguration nicht unerheblich.

Webalizer ist im Vergleich zu Awstats ein Urgestein aus der Geschichte des Webs. Das Programm wird zwar noch gewartet, aber schon seit Jahren nicht mehr weiterentwickelt. Seine anhaltende Popularität verdankt Webalizer vor allem seiner Einfachheit, sowohl bei der Konfiguration als auch bei der Präsentation der Ergebnisse.

Welche Ergebnisse sind korrekt?

Sollten Sie Awstats und Webalizer probeweise parallel einsetzen, werden Sie feststellen, dass beide Programme zu unterschiedlichen Ergebnissen gelangen: Beide Programme versuchen mehr oder weniger erfolgreich, nicht relevante Zugriffe auszufiltern. Es lässt sich trefflich darüber streiten, welches Ergebnis nun »richtiger« ist. Fakt ist, dass beide Werkzeuge eine Menge Zugriffe mitzählen, die von Suchrobotern und automatisierten Download-Scripts stammen.

Alternativen

Anstelle von Awstat oder Webalizer können Sie das OpenSource-System Piwik oder Google Analytics einsetzen. Dazu müssen Sie auf den Seiten Ihrer Website JavaScript-Code einbauen, der jeden Seitenzugriff an einen zentralen Server weiterleitet. Diese Vorgehensweise erleichtert die Unterscheidung zwischen »echten« Besuchern und Suchrobotern und führt zu genaueren Ergebnissen, die in Echtzeit beobachtet wer-

den können. Beachten Sie aber, dass der Einsatz beider Dienste unter Einhaltung der deutschen Datenschutzgesetze problematisch ist!

http://de.piwik.org
https://www.datenschutzzentrum.de/tracking/piwik
http://www.google.com/intl/de/analytics
http://de.wikipedia.org/wiki/Google_Analytics

Awstats

Die Grundidee von Awstats besteht darin, dass die Apache-Logging-Dateien regelmäßig ausgewertet werden, z. B. stündlich. Die Ergebnisse werden in einer einfachen Datenbank in Textform im Verzeichnis `/var/lib/awstats` gespeichert. Die grafische bzw. statistische Aufbereitung der Daten erfolgt in der Regel dynamisch durch ein CGI-Perl-Script, das unter einer Adresse nach dem folgenden Muster aufgerufen werden kann (siehe Abbildung 35.2):

http://ihre-website.de/awstats/awstats.pl
http://ihre-website.de/awstats/awstats.pl?config=zweite-seite.de

Grundsätzlich ist es auch möglich, die Ergebnisseiten einmal täglich durch ein Cron-Script zu generieren. Das ist sicherer, aber für den Betrachter weniger komfortabel.

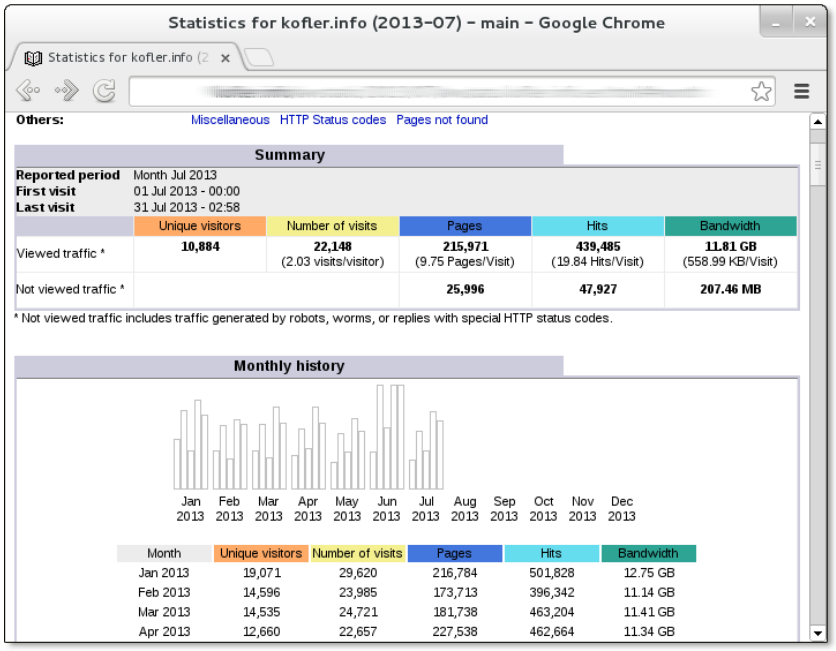


Abbildung 35.2 Awstats-Zugriffsstatistik

Awstats funktioniert nach der Installation des `awstats`-Pakets nicht auf Anhieb! Sie müssen vorher eine Awstat-Konfigurationsdatei für jeden virtuellen Host erstellen, die statischen Awstat-Seiten oder das Awstat-CGI-Script in die Apache-Konfiguration aufnehmen und außerdem einige distributionsspezifische Konfigurationsarbeiten erledigen.

Awstats-Konfiguration

Bei der Arbeit an diesem Abschnitt habe ich leider den Eindruck gewonnen, dass die Awstats-Konfigurationsunterschiede zwischen Debian/Ubuntu und Fedora/RHEL größer sind als die Gemeinsamkeiten. Einen gemeinsamen Nenner gibt es aber: Awstats setzt voraus, dass es für jeden virtuellen Host eine eigene Konfigurationsdatei im Verzeichnis `/etc/awstats` gibt. Der Dateiname hat die Form `awstats.`*`hostname`*`.conf`, also z. B. `awstats.firma123.de.conf`. Als Ausgangspunkt beim Erstellen neuer Konfigurationsdateien verwenden Sie die Musterdatei `awstats.conf` (Debian/Ubuntu) bzw. `awstats.model.conf` (Fedora/RHEL):

```
root#  cd /etc/awstats
root#  cp awstats.conf       awstats.firma123.de.conf   (Debian/Ubuntu)
root#  cp awstats.model.conf awstats.firma123.de.conf   (Fedora/RHEL)
```

Jede Konfigurationsdatei ist ca. 1500 Zeilen lang, enthält aber fast nur Kommentare. In der Regel müssen Sie lediglich drei Angaben ändern: einmal den Ort der Access-Logging-Datei und zweimal den Hostnamen:

```
# Änderungen in /etc/awstats/awstats.<hostname>.conf
...
LogFile="/home/firma123/www-log/access.log"
SiteDomain="firma123.de"
HostAliases="localhost 127.0.0.1 firma123.de"
```

Standardmäßig verarbeitet Awstats nur die Zugriffsdaten für einen Monat. Wenn Sie die Daten für ein ganzes Jahr betrachten möchten, ist eine weitere Änderung erforderlich:

```
# Änderungen in /etc/awstats/awstats.<hostname>.conf
...
AllowFullYearView=3
```

Beachten Sie aber, dass die Erzeugung einer Jahresstatistik nur dynamisch erfolgen kann und dass das Awstats-Script dabei eine Menge Speicherplatz und CPU-Ressourcen beansprucht. Die statischen Ergebnisseiten enthalten immer nur die Ergebnisse eines Monats.

Unter Debian und Ubuntu müssen Sie schließlich der Musterdatei einen neuen Namen geben, damit diese Datei nicht ebenfalls wie eine aktive Konfigurationsdatei verarbeitet wird:

```
root#  mv /etc/awstats/awstats.conf \
          /etc/awstats/awstats.conf.orig     (Debian/Ubuntu)
```

Falls Sie einige gemeinsame Einstellungen für *alle* Awstats-Konfigurationsdateien verändern möchten, verwenden Sie die hierfür vorgesehene Datei `/etc/awstats/awstats.conf.local`.

Awstats und Debian/Ubuntu

Unter Debian und Ubuntu kümmert sich die Datei `/etc/cron.d/awstats` darum, dass alle 10 Minuten das Script `/usr/share/awstats/tools/update.sh` ausgeführt wird. Dieses Script ruft wiederum für alle `/etc/awstats/awstats.*conf`-Konfigurationsdateien das Perl-Script `awstats.pl` auf und aktualisiert so die Awstats-Statistikdatenbank. Damit nicht auch die Musterdatei `awstats.conf` als Konfigurationsdatei berücksichtigt wird, müssen Sie diese umbenennen (siehe oben).

Anfänglich scheitert der Zugriff auf die Apache-Logging-Dateien an den Zugriffsrechten: Die Apache-Logging-Dateien sind nur für `root` und `adm`-Gruppenmitglieder lesbar. Die Awstats-Scripts werden dagegen unter dem Account `www-data` ausgeführt.

Wenn Sie im Internet nach *ubuntu|debian awstat permission denied* suchen, finden Sie unzählige Lösungsvorschläge, von denen aber viele sicherheitstechnisch unbrauchbar sind. Mit relativ geringen Sicherheitskomplikationen ist eine Veränderung der Gruppenzugehörigkeit der Apache-Logging-Dateien verbunden. Mit den beiden folgenden Kommandos ordnen Sie das Verzeichnis `/var/log/apache2` und alle darin enthaltenen Dateien der Gruppe `www-data` zu und stellen sicher, dass auch neu erzeugte Dateien dieser Gruppe zugeordnet werden:

```
root#  chgrp -R www-data /var/log/apache2/
root#  chmod 2755 /var/log/apache2/
```

Außerdem müssen Sie sicherstellen, dass auch `logrotate` von nun an die Gruppe `www-data` nutzt. Dazu ändern Sie eine Zeile in der `logrotate`-Konfiguration für Apache:

```
# in der Datei /etc/logrotate.d/apache2
...
create 640 root www-data
```

Schließlich sollten Sie dafür sorgen, dass die Logging-Dateien durch Awstats ausgewertet werden, bevor `logrotate` diese umbenennt:

```
# in der Datei /etc/logrotate.d/apache2
...
prerotate
  if [ -x /usr/share/awstats/tools/update.sh ]; then
    su -l -c /usr/share/awstats/tools/update.sh www-data
  fi
endscript
```

Sobald die automatische Auswertung der Logging-Dateien gelingt, werden Sie sich die Ergebnisse auch ansehen wollen. Standardmäßig erzeugt das Cron-Script `/etc/cron.d/awstats` einmal täglich eine statische Version der Ergebnisdateien. Diese

werden im Verzeichnis `/var/cache/awstats/`*`domainname`* gespeichert. Damit dieses Verzeichnis über einen Webbrowser betrachtet werden kann, fügen Sie die folgenden Zeilen in die Virtual-Host-Datei von Apache ein:

```
# in /etc/apache2/sites-available/firma123.de
...
Alias       /awstatic       "/var/cache/awstats/kofler.info"
<Directory /var/cache/awstats/kofler.info>
  Options +Indexes
</Directory>
```

Awstats richtet für jedes Jahr und für jeden Monat eigene Verzeichnisse ein. Eine zentrale Startdatei fehlt aber. Um die Auswertung für einen bestimmten Monat anzusehen, muss im Webbrowser die folgende Adresse angegeben werden:

http://firma123.de/awstatic/2012/09/awstats.firma123.de.en.html

Die Option `+Indexes` ermöglicht ein bequemes Navigieren durch die Ergebnisverzeichnisse und erspart die mühsame Eingabe der vollständigen Adresse. Damit nicht jeder Besucher der Website *firma123.de*, der die Adresse errät, die Seitenstatistiken lesen kann, sollten Sie das Verzeichnis durch ein Passwort absichern (siehe Abschnitt 35.2).

Für die dynamische Präsentation der Awstats-Ergebnisseiten ist das CGI-Script `awstats.pl` vorgesehen. Damit dieses Script von Apache ausgeführt werden kann, müssen Sie die folgenden Zeilen in eine Apache-Konfigurationsdatei einfügen:

```
# in /etc/apache2/sites-available/default
...
Alias       /awstatsclasses "/usr/share/awstats/lib/"
Alias       /awstats-icon/  "/usr/share/awstats/icon/"
Alias       /awstatscss     "/usr/share/doc/awstats/examples/css"
ScriptAlias /awstats/       "/usr/lib/cgi-bin/"
```

Die Awstats-Auswertungen können nun im Webbrowser über die Seiten

http://hostname/awstats/awstats.pl
http://hostname/awstats/awstats.pl?config=zweite-seite.de

angesehen werden. Wie bei der statischen Konfiguration sollten Sie auch die dynamische Konfiguration mit einem Passwort absichern. Die Absicherung betrifft nun das `cgi-bin`-Verzeichnis. Fügen Sie die entsprechenden `AuthXxx`-Anweisungen einfach in der Datei `/etc/apache2/sites-available/default` in den `Directory`-Block für das Verzeichnis `/usr/lib/cgi-bin` ein!

Weitere Informationen zur Debian- und Ubuntu-spezifischen Konfiguration von Awstats finden Sie in der folgenden Datei:

```
/usr/share/doc/awstats/README.Debian.gz
```

Fedora/RHEL-Eigenheiten

Während für Fedora ein Awstats-Paket zur Installation bereitsteht, trifft dies für RHEL nicht zu. Sie müssen also vor der Installation eine zusätzliche Paketquelle einrichten. Gut geeignet ist EPEL (Extra Packages for Enterprise Linux).

Bei Awstats-Installationen unter Fedora oder RHEL kümmert sich die Cron-Datei `/etc/cron.hourly/awstats` darum, einmal pro Stunde das Script `/usr/share/awstats/tools/awstats_updateall.pl` auszuführen. Dieses Script aktualisiert wiederum die Awstats-Datenbanken für alle Konfigurationsdateien `/etc/awstats/awstats.*conf`, wobei die Musterdatei `awstats.model.conf` nicht berücksichtigt wird.

Bei der Awstats-Installation versuchen die Paket-Scripts, automatisch geeignete Konfigurationsdateien für den Host einzurichten. Das gelingt aber nur, wenn Sie keine Änderungen am Ort der Logging-Dateien vorgenommen haben. Falls die Apache-Konfiguration Einstellungen für weitere virtuelle Hosts enthält, müssen Sie die entsprechenden erforderlichen Awstats-Konfigurationsdateien selbst einrichten.

Anders als unter Debian bzw. Ubuntu hat Awstats keine Probleme beim Zugriff auf die Apache-Logging-Dateien. Diese sind unter Fedora und RHEL generell für alle lesbar.

Damit `logrotate` die Logging-Dateien nicht umbenennt, bevor Awstats diese auswerten kann, sollten Sie die beiden Dienste synchronisieren. Dazu fügen Sie in die Datei `/etc/logrotate.d/httpd` die folgenden `prerotate`-Zeilen ein:

```
# in /etc/logrotate.d/httpd
...
prerotate
  /usr/bin/awstats_updateall.pl now -configdir=/etc/awstats/ \
    --awstatsprog=/var/www/awstats/awstats.pl >/dev/null
endscript
```

Für den Zugriff auf die dynamisch erzeugten Awstats-Auswertungen ist die Konfigurationsdatei `/etc/httpd/conf.d/awstats.conf` vorgesehen. Dabei gelten für die Ergebnisseiten die folgenden Adressen:

http://hostname/awstats/awstats.pl
http://hostname/awstats/awstats.pl?config=zweite-seite.de

Aus Sicherheitsgründen können diese Seiten aber anfänglich nur von `localhost` aus betrachtet werden. Abhilfe: Ersetzen Sie `Allow from 127.0.0.1` durch `Allow from all`. Damit machen Sie das Awstats-Verzeichnis allerdings für jedermann öffentlich, was in der Regel auch nicht erwünscht ist. Sie sollten deswegen im `Directory`-Block für das Verzeichnis `/usr/share/awstats/wwwroot` die üblichen `AuthXxx`-Anweisungen einfügen, um das Verzeichnis durch ein Passwort abzusichern (siehe Abschnitt 35.2).

```
# in /etc/httpd/conf.d/awstats.conf
...
<Directory "/usr/share/awstats/wwwroot">
    Options None
    AllowOverride None
    Order allow,deny
    Allow from all
    AuthType     Basic
    AuthUserFile /etc/httpd/awstat-passwords.pwd
    AuthName     "awsuser1 awuser2 ..."
    Require      valid-user
</Directory>
```

Die Erzeugung statischer Awstats-Ergebnisseiten ist unter Fedora/RHEL nicht vorgesehen. Wenn Sie aus Sicherheitsgründen die dynamische Ansicht der Awstats-Statistiken vermeiden möchten, müssen Sie eine Cron-Datei in `/etc/cron.daily` einrichten, die das Perl-Script `/usr/share/awstats/tools/awstats_buildstaticpages.pl` aufruft. Die Parameter dieses Scripts sind hier dokumentiert:

http://awstats.sourceforge.net/docs/awstats_tools.html

Webalizer

Eine nach wie vor populäre Alternative zu Awstats ist das steinzeitliche Programm Webalizer. Die Funktionsweise ist ähnlich wie bei Awstats: Webalizer wird in der Regel einmal täglich durch Cron ausgeführt, wertet die Apache-Logging-Dateien aus und erzeugt dann einige statische Seiten mit den Auswertungsergebnissen (siehe Abbildung 35.3). Anders als bei Awstats ist eine dynamische Darstellung der Ergebnisse ist nicht vorgesehen. Damit sind eine Menge potenzieller Sicherheitsprobleme von vorne herein ausgeschlossen.

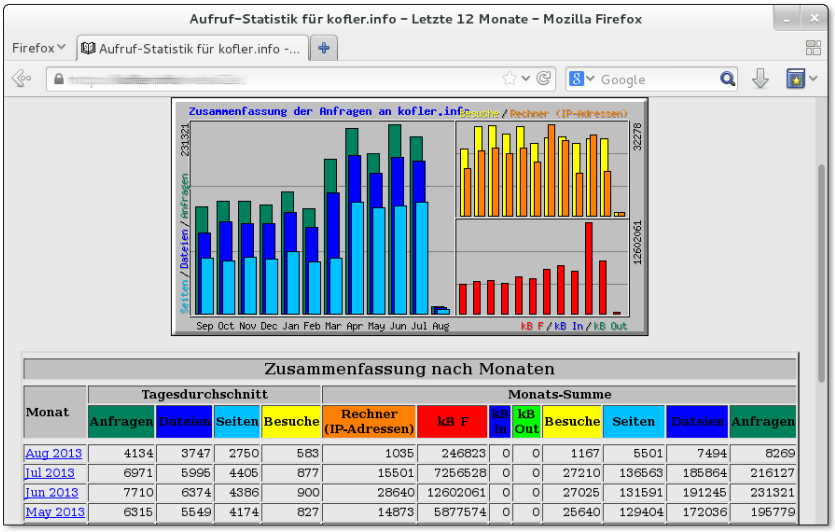
Webalizer steht bei allen gängigen Distributionen als fertiges Paket zur Verfügung:

```
root#  apt-get install webalizer   (Debian/Ubuntu)
root#  yum install webalizer       (Fedora/RHEL)
```

Konfiguration unter Debian/Ubuntu

Bei der Konfiguration gibt es je nach Distribution erhebliche Unterschiede. Unter Debian und Ubuntu wird Webalizer durch `*.conf`-Dateien im Verzeichnis `/etc/webalizer` gesteuert. Die gut dokumentierte Beispieldatei `webalizer.conf` gilt dabei als Muster.

Wenn Sie auf Ihrem Server nur eine einzige Website betreiben und diese die Standard-Logging-Dateien verwendet, müssen Sie keinerlei Änderungen durchführen. Webalizer wertet dann die Datei `/var/log/apache2/access.log.1` aus und speichert die Ergebnisse im Verzeichnis `/var/www/webalizer`.



Zusammenfassung nach Monaten

Monat	Tagesdurchschnitt				Monats-Summe							
	Anfragen	Dateien	Seiten	Besuche	Rechner (IP-Adressen)	kB F	kB In	kB Out	Besuche	Seiten	Dateien	Anfragen
Aug 2013	4134	3747	2750	583	1035	246823	0	0	1167	5501	7494	8269
Jul 2013	6971	5995	4405	877	15501	7256528	0	0	27210	136563	185864	216127
Jun 2013	7710	6374	4386	900	28640	12602061	0	0	27025	131591	191245	231321
May 2013	6315	5549	4174	827	14873	5877574	0	0	25640	129404	172036	195779

Abbildung 35.3 Zugriffsstatistik mit Webalizer

Möglicherweise wird es Sie irritieren, dass Webalizer `access.log.1` auswertet und nicht die aktuellere Datei `access.log`. Das hat den Vorteil, dass sich Webalizer und Logrotate nicht in die Quere kommen. Allerdings benennt Logrotate die Apache-Logging-Dateien nur wöchentlich um. Die Webalizer-Statistiken erscheinen deswegen mit einer Verzögerung von bis zu einer Woche.

Die einfachste Lösung für dieses Problem besteht darin, dass Sie Logrotate so konfigurieren, dass die Logging-Dateien täglich umbenannt werden (`daily` statt `weekly` in `/etc/logrotate.d/apache2`).

Eine andere Lösung besteht darin, in `webalizer.conf` doch auf `access.log` zuzugreifen. Dann müssen Sie aber mit `Incremental=yes` sicherstellen, dass sich Webalizer bei jedem Durchlauf merkt, wie weit es die Logging-Datei bereits gelesen hat.

```
# in /etc/webalizer/webalizer.conf
...
LogFile=/var/log/apache2/access.log
Incremental=yes
```

Gleichzeitig müssen Sie nun dafür sorgen, dass Webalizer von Logrotate ausgeführt wird, bevor die Logging-Datei umbenannt wird:

```
# in /etc/logrotate.d/apache2
...
prerotate
  /etc/cron.daily/webalizer
endscript
```

Der Zugriff auf die Webalizer-Statistiken erfolgt im Webbrowser über die folgende Adresse:

http://hostname/webalizer

In der Regel werden Sie kein Interesse daran haben, dass jeder die statistischen Daten Ihres Webservers lesen kann. Deswegen ist es eine gute Idee, den Zugriff auf das Verzeichnis `/var/www/webalizer` mit den Webalizer-Daten durch ein Passwort abzusichern (siehe Abschnitt 35.2).

Falls Sie auf Ihrem Server mehrere virtuelle Hosts eingerichtet haben, müssen Sie für jeden Host, der eigene Logging-Dateien hat, auch eine eigene Webalizer-Konfigurationsdatei einrichten. Das folgende Beispiel gilt für die Website *firma-123.de*, deren Log-Dateien im Verzeichnis des Benutzers `firma123` gespeichert werden.

```
# Datei /etc/webalizer/firma-123.de.conf

# Grundeinstellungen
LogFile         /home/firma123/www-log/access.log
OutputDir       /home/firma123/www/webalizer

# Beschriftung
ReportTitle     Zugriffsstatistik firma-123.de
HostName        firma-123.de

# Anzahl der Top-n-Einträge
TopURLs         50
TopKURLs        30
TopReferrers    50

# in der Top-n-Liste der URLs nicht berücksichtigen
HideURL         *.gif
HideURL         *.jpg
HideURL         *.png

# Zugriffe von localhost sowie Verweise von firma-123.de ignorieren
IgnoreSite      localhost
IgnoreReferrer  localhost
IgnoreReferrer  firma-123.de
IgnoreReferrer  www.firma-123.de
```

Noch einige Anmerkungen zu dieser Konfiguration: Die `TopXxx`-Optionen vergrößern die Anzahl der Einträge in den Listen *Top n ... URLs*, *Top n ... URLs by kByte* und *Top n ... referrers*. Diese Listen finde ich persönlich am interessantesten. Die `HideURL`-Zeilen stellen sicher, dass Bilddateien in Top-n-Listen ignoriert werden. Die `Ignore`-Zeilen bewirken, dass Zugriffe vom lokalen Rechner sowie Querverweise von der eigenen Website nicht mitgezählt werden.

Damit Webalizer die Ergebnisse speichern kann, muss natürlich noch das Verzeichnis `/home/firma123/www/webalizer` erzeugt werden:

```
root#  mkdir /home/firma123/www/webalizer
root#  chown firma123:firma123 /home/kofler/www/webalizer
```

Der für die Website verantwortliche Benutzer – hier also `firma123` – sollte den Zugriff auf das Webalizer-Verzeichnis nun noch durch eine `.htaccess`-Datei absichern.

Das richtige Logging-Format ist entscheidend

Webalizer kann nur dann die Liste *Top n ... referrers* bilden, wenn die Apache-Log-Datei die entsprechenden Informationen enthält. Dazu müssen Sie in der Apache-Konfigurationsdatei `/etc/apache2/sites-available/*` in der Zeile `CustomLog` die Formatierung `combined` angeben (nicht `common`)!

Konfiguration unter Fedora/RHEL

Unter Fedora und RHEL wertet Webalizer nur die Konfigurationsdatei `/etc/webalizer.conf` aus. Die Ergebnisse werden im Verzeichnis `/var/www/usage` gespeichert und sind somit unter der folgenden Adresse zu finden:

http://hostname/usage

Wenn Sie getrennte Statistiken für mehrere virtuelle Hosts benötigen, müssen Sie nicht nur die entsprechenden Webalizer-Konfigurationsdateien selbst einrichten, sondern auch Cron-Scripts für den Webalizer-Aufruf.

Wesentlich simpler als unter Debian und Ubuntu sind dafür die Konflikte zwischen Webalizer und Logrotate gelöst: Webalizer wird dank der vorangestellten Nullen in `/etc/cron.daily/00webalizer` immer *vor* Logrotate ausgeführt, weil Cron die Scripts in `cron.daily` in alphabetischer Reihenfolge verarbeitet.

35.6 PHP

Dynamische Webseiten

Apache an sich kann nur statische Webseiten übertragen. Alle modernen Websites nutzen aber dynamische Seiten. Jedes Mal, wenn eine derartige Seite angefordert wird, startet Apache ein externes Programm, verarbeitet den Code der Seite und liefert als Ergebnis eine Seite, die individuell angepasst ist. Damit kann die Seite beispielsweise die aktuelle Uhrzeit enthalten oder das Ergebnis einer Datenbankabfrage oder eine ständig wechselnde Werbeeinblendung etc.

PHP

Zur Programmierung dynamischer Webseiten eignen sich zahllose Programmiersprachen – z. B. Perl, PHP oder Java. Die Grundidee einer PHP-Webseite besteht darin, dass die Datei mit der Kennung `*.php` sowohl HTML- als auch PHP-Code enthält. PHP-Code wird mit dem Tag `<?php` eingeleitet und endet mit `?>`. Wenn ein Webnutzer eine

PHP-Seite anfordert, übergibt Apache die Seite an den PHP-Interpreter. Dort wird der PHP-Code ausgeführt. Das Ergebnis des Codes wird direkt in die HTML-Datei eingebettet. Der PHP-Interpreter übergibt die resultierende Seite zurück an Apache, und dieser sendet sie dem Webnutzer. Der Webbrowser des Nutzers sieht also nie den PHP-Code, sondern immer nur die resultierende HTML-Seite.

Hello World!

Der Platz reicht hier nicht für eine Einführung in die Programmiersprache PHP. Stattdessen soll das folgende Minibeispiel das Konzept von PHP veranschaulichen. Die folgende Datei liefert nach der Verarbeitung durch den PHP-Interpreter eine HTML-Seite mit der aktuellen Uhrzeit:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0//EN">
<html><head>
  <meta http-equiv="Content-Type"
        content="text/html; charset=iso-8859-1" />
  <title>PHP-Beispiel</title>
</head><body>

<p>Die aktuelle Uhrzeit auf diesem Server:
    <?php echo date("G:i:s"); ?>
</p>
</body></html>
```

Installation

Sofern PHP nicht bereits mit Apache mitinstalliert wurde, installieren Sie mit Ihrem Paketverwaltungsprogramm die erforderlichen `php5`-Pakete. Was »erforderlich« ist, ist allerdings gar nicht so einfach festzustellen: Ähnlich wie bei Apache ist auch PHP zumeist auf zahlreiche Pakete verteilt, die die Sprache an sich sowie diverse Erweiterungen enthalten. Für erste Experimente reichen üblicherweise `php5`, `php5-common` sowie `libapache2-mod-php5`. Soweit sich nicht die Paketverwaltung darum kümmert, müssen Sie Apache nach der Installation neu starten, damit der Webserver neu hinzugekommene PHP-Module berücksichtigt.

Konfiguration

Zahllose Optionen des PHP-Interpreters werden durch die Datei `php.ini` gesteuert. Im Regelfall können Sie die Grundeinstellungen einfach beibehalten. Der Ort dieser Datei sowie weiterer PHP-Konfigurationsdateien ist wieder einmal distributionsabhängig:

Debian, Ubuntu:	`/etc/php5/apache2/php.ini`, `/etc/php5/apache2/conf.d/*.ini`
Fedora, Red Hat:	`/etc/php.ini`, `/etc/php.d/*.ini`
SUSE:	`/etc/php5/apache2/php.ini`

Test

Um zu testen, ob die PHP-Installation funktioniert, erstellen Sie die Datei `phptest.php`, die aus nur einer einzigen Zeile Code besteht:

```
<?php phpinfo(); ?>
```

Kopieren Sie diese Datei in das `DocumentRoot`-Verzeichnis (siehe Abschnitt 35.1), und stellen Sie sicher, dass Apache die Datei lesen darf. Obwohl es sich bei PHP-Dateien eigentlich um Script-Dateien handelt, reichen Leserechte. Zugriffsrechte zum Ausführen (x-Zugriffsbits) sind nicht erforderlich.

Mit einem Webbrowser sehen Sie sich nun die Seite `http://localhost/phptest.php` an. Das Ergebnis ist eine sehr umfangreiche Seite, die alle möglichen Optionen und Einstellungen von Apache und PHP enthält. Aus Sicherheitsgründen ist es nicht empfehlenswert, eine derartige Seite frei zugänglich ins Internet zu stellen. Sie enthält eine Menge Informationen über Ihre Konfiguration.

Wenn es nicht funktioniert

Wenn Sie statt der Testseite den PHP-Code sehen oder die PHP-Datei zum Download angeboten bekommen, ist die wahrscheinlichste Fehlerursache die, dass Sie als Webadresse den Dateinamen (z. B. `/srv/www/htdocs/phpinfo.php`) angegeben haben. In diesem Fall wird die Datei direkt aus dem lokalen Dateisystem gelesen, anstatt von Apache und PHP verarbeitet zu werden. Die Webadresse muss mit `http://` beginnen!

Eine weitere Fehlerursache ist die Apache-Konfiguration: Haben Sie Apache nach der Installation von PHP bzw. nach der Veränderung von Konfigurationsdateien neu gestartet?

Wenn es einmal nicht geklappt hat, kann Ihnen in der Folge der Cache Ihres Webbrowsers einen Strich durch die Rechnung machen. Anstatt die Seite neu von Apache anzufordern, was nun vielleicht funktionieren würde, liest der Browser die Seite aus dem internen Cache. Starten Sie das Programm sicherheitshalber neu bzw. löschen Sie den Cache!

35.7 FTP-Server (vsftpd)

Vielen Webservern gesellt sich ein FTP-Server hinzu, der je nach Website zwei Aufgaben erfüllt: Einerseits ermöglicht er den Download großer Dateien, die auf der Website zur Verfügung gestellt werden; andererseits hilft er bei der Wartung bzw. Aktualisierung der Website, indem er eine einfache Möglichkeit zum Upload von Dateien zulässt.

Sicherheit

FTP ist ein sehr altes Programm. Sein Protokoll führt in Kombination mit Firewalls bzw. mit Masquerading oft zu Problemen. Noch problematischer ist der Umstand, dass beim Verbindungsaufbau zwischen einem FTP-Client und dem -Server der Benutzername und das Passwort unverschlüsselt übertragen werden. Da stehen jedem sicherheitsbewussten Anwender die Haare zu Berge!

Natürlich gibt es schon längst sichere Alternativen zu FTP. Unter anderem stellt der in Kapitel 34 beschriebene SSH-Server mit SFTP (*Secure FTP*) auch Dienste zur

Dateiübertragung zur Verfügung. Das Problem liegt hier mehr auf der Client-Seite: Es gibt nur relativ wenige benutzerfreundliche Programme, die SFTP beherrschen. Aus diesem Grund wird FTP trotz aller Sicherheitsmängel noch immer recht häufig eingesetzt.

Eine andere Alternative ist der WebDAV-Standard, der das HTTP-Protokoll erweitert und die Datenübertragung in beide Richtungen erleichtert. Beispielsweise unterstützt Apache in Kombination mit dem Modul `mod_dav` WebDAV:

http://httpd.apache.org/docs/2.4/mod/mod_dav.html
http://wiki.ubuntuusers.de/Apache/webdav

Wenn Sie auf einen traditionellen FTP-Server nicht verzichten möchten, können Sie diesen auch als reinen Anonymous-FTP-Server konfigurieren. Dabei werden beim Login keine kritischen Daten übertragen. Allerdings schränkt das auch die Anwendung von FTP stark ein. Zur einfachen Wartung einer Website lässt sich FTP dann nicht mehr verwenden.

vsftpd

Es gibt unzählige verschiedene FTP-Server. Das populärste Programm ist momentan `vsftpd`. Alle gängigen Distributionen stellen hierfür ein Paket zur Verfügung. `vsftpd` steht für *Very Secure FTP Daemon*. Das Attribut *Very Secure* ist aber unter dem Vorbehalt zu sehen, dass auch der beste FTP-Server die Sicherheitsmängel des FTP-Protokolls aufweist.

Start als Dämon

`vsftpd` kann auf zwei Arten gestartet werden: entweder als eigenständiger Dämon durch das Init-System oder über `xinetd`. Bei den meisten Distributionen ist die Dämon-Variante vorkonfiguriert. Die Konfigurationsdatei `vsftpd.conf` muss dazu die Anweisung `listen=YES` enthalten. Um den FTP-Server zu starten bzw. zu stoppen, verwenden Sie je nach Distribution die üblichen Kommandos (siehe Abschnitt 16.5).

Konfiguration

Die Konfiguration von `vsftpd` erfolgt durch die Datei `/etc/vsftpd.conf` bzw. `/etc/vsftpd/vsftpd.conf`. Standardmäßig ist oft nur ein Read-Only-Zugang per Anonymous FTP zugelassen. FTP-Clients können also nur einen Download, aber keinen Upload durchführen. Wenn Sie neben Anonymous FTP auch Benutzer-Logins benötigen, müssen Sie `locale_enable` auf `YES` stellen. Wenn Sie bei dieser FTP-Form auch einen Daten-Upload zulassen möchten, müssen Sie zusätzlich `write_enable` auf `YES` stellen. Wenn `vsftpd.conf` die Zeile `tcp_wrappers=Yes` enthält, wertet `vsftpd` wie `xinetd` die Dateien `/etc/hosts.allow` und `/etc/hosts.deny` aus (siehe Abschnitt 40.2). Die folgenden Zeilen fassen die wichtigsten Einstellungen in `vsftpd.conf` zusammen:

```
# /etc/vsftpd.conf bzw. /etc/vsftpd/vsftpd.conf
...
local_enable=YES / NO        # FTP-Login zulassen
write_enable=YES / NO        # Daten-Upload grundsätzlich zulassen
...
```

```
anonymous_enable=YES / NO    # Anonymous FTP zulassen
anon_upload_enable=YES / NO  # Daten-Upload auch bei Anonymous FTP
...
listen=YES / NO              # Start als Init-Dämon (YES) oder durch xinetd (NO)
tcp_wrapper=YES / NO         # hosts.allow und hosts.deny auswerten
```

FTP ausprobieren

FTP müsste jetzt eigentlich auf Anhieb funktionieren. Führen Sie auf dem Server-Rechner `ftp localhost` aus, um zu testen, ob der FTP-Server ordnungsgemäß gestartet wird. Beachten Sie dabei, dass `root` grundsätzlich keinen FTP-Login durchführen darf.

Anonymous FTP

Wenn Anonymous FTP in `vsftpd.conf` zugelassen ist, akzeptiert `vsftpd` als Login die Namen `anonymous` und `ftp` in Kombination mit einem beliebigen Passwort. Es ist üblich, als Passwort die E-Mail-Adresse anzugeben. `vsftpd` kontrolliert das aber nicht.

Nach dem Login kann der FTP-Client auf die Dateien des Home-Verzeichnisses des Linux-Benutzers `ftp` zugreifen. Der Ort dieses Verzeichnisses wird in `/etc/passwd` angegeben:

Debian, Ubuntu:	`/home/ftp`
Fedora, Red Hat:	`/var/ftp/`
SUSE:	`/srv/ftp/`

Upload per Anonymous FTP

Wenn Sie den Upload von Dateien per Anonymous FTP zulassen, sollten Sie darauf achten, dass es nur ein einziges Verzeichnis innerhalb des FTP-Datenverzeichnisses gibt, das Schreibrechte hat – z. B. `/var/ftp/upload` bei Fedora oder Red Hat. Dieses Verzeichnis sollte dem Benutzer `ftp` gehören und aus Sicherheitsgründen keine Leserechte haben:

```
root#  mkdir /var/ftp/upload
root#  chown ftp upload
root#  chmod 730 upload
```

Somit kann jeder einen Upload durchführen und dem FTP-Administrator anschließend eine E-Mail mit Instruktionen senden, wofür die Datei dient. Andere FTP-Nutzer können die Datei aber aus dem `upload`-Verzeichnis weder sehen noch herunterladen. Wenn Sie auf derartige Sicherheitsmaßnahmen verzichten, kann es passieren, dass das FTP-Upload-Verzeichnis zum Austausch illegaler Dateien missbraucht wird.

FTP für root und andere Spezialbenutzer

Aus Sicherheitsgründen sind `root` und einige andere Spezialbenutzer (wie `daemon`, `lp` oder `nobody`) von der FTP-Benutzung ausgeschlossen. Die dazu erforderliche Konfiguration variiert von Distribution zu Distribution.

Bei Fedora und Red Hat erfolgt der Login-Schutz doppelgleisig. Einerseits greift `vsftpd` für die Login-Kontrolle auf PAM zurück (*Pluggable Authentication Modules*).

PAM wertet die Datei `/etc/pam.d/vsftpd` aus, die auf die Datei `etc/vsftpd/ftpusers` verweist. Diese Datei enthält eine Liste aller Login-Namen, die FTP *nicht* benutzen dürfen.

Andererseits wendet `vsftpd` auch eine interne Login-Kontrolle an und sperrt alle Benutzer, die in `/etc/vsftpd.user_list` genannt sind. Diese Login-Kontrolle wird in `vsftpd.conf` durch `userlist_enable=YES` und `userlist_deny=YES` (gilt standardmäßig) aktiviert.

Bei Debian, SUSE und Ubuntu greift `vsftpd` für den Login ebenfalls auf PAM zurück. `/etc/pam.d/vsftpd` verweist hier allerdings auf `/etc/ftpusers`. Diese Datei enthält eine Liste aller Login-Namen, die FTP nicht benutzen dürfen.

Kapitel 36
MySQL und MariaDB

MySQL ist seit vielen Jahren das populärste Datenbanksystem der Open-Source-Welt. Auch wenn Sie nicht vorhaben, selbst irgendwelche Datenbanken zu verwalten, gibt es unzählige Webanwendungen, die den MySQL-Server voraussetzen – beispielsweise Wikis, Diskussionsforen wie phpBB, Content-Management-Systeme wie TYPO3 oder Fehlerverwaltungssysteme wie Bugzilla.

In diesem Kapitel zeige ich Ihnen, wie Sie den MySQL- oder MariaDB-Server auf Ihrem Rechner installieren und wie Sie grundlegende Administrationsaufgaben durchführen. Auf das Design von Datenbanken, auf den Einsatz von SQL zur Abfrage bzw. zur Manipulation von Daten sowie auf die Entwicklung von Datenbankanwendungen gehe ich hingegen nicht ein – das würde hier den Rahmen sprengen.

MySQL versus MariaDB

MySQL wurde ursprünglich von der MySQL AB entwickelt, einer eigenständigen schwedischen Firma. Diese wurde von Sun aufgekauft. Später kaufte Oracle Sun, und so ist nun Oracle der Eigentümer von MySQL. Leider klappt die Zusammenarbeit zwischen Oracle und den Distributoren nicht besonders gut. Insbesondere beklagen viele Distributoren, dass sie die Informationen zur Behebung von Sicherheitsproblemen nicht bzw. zu spät erhalten und es daher unmöglich sei, Sicherheitslücken rasch zu beheben.

Dieser Ärger führte dazu, dass Fedora und openSUSE mittlerweile standardmäßig MariaDB anstelle von MySQL installieren. Im Sommer 2013 war noch nicht klar, ob RHEL 7 auch diesen Weg einschlagen würde – einiges deutete aber darauf hin. MariaDB entstand als Fork des MySQL-Codes und ist daher weitestgehend zu MySQL kompatibel. MariaDB enthält allerdings einige Zusatzfunktionen. Es ist abzusehen, dass sich MySQL und MariaDB in Zukunft weiter auseinanderentwickeln werden.

In der Praxis werden die meisten Linux-Anwender gar nicht bemerken, ob das CMS, Wiki etc. hinter den Kulissen mit einem originalen MySQL-Server oder mit einem MariaDB-Server kommuniziert. Auch die in diesem Kapitel beschriebenen Konfigurationsdateien sowie die Administrationswerkzeuge und -techniken gelten gleichermaßen für MySQL und für MariaDB. Insbesondere heißen auch bei MariaDB der

Dienstname `mysqld` und das Steuerungskommando `mysql`. Wenn ich in diesem Kapitel ohne weitere Erläuterungen von »MySQL« schreibe, gelten diese Informationen gleichermaßen für MySQL und MariaDB.

Lizenz

MySQL und die dazugehörenden Treiber für diverse Programmiersprachen unterstehen der GPL. Die firmeninterne Nutzung von MySQL, der Einsatz auf einem Webserver sowie die Nutzung in GPL-Projekten ist grundsätzlich kostenlos. Beachten Sie aber, dass die Weitergabe kommerzieller Projekte (Closed Source, keine GPL), die auf MySQL aufbauen, eine kommerzielle Lizenz des MySQL-Servers erfordert! Details zu den Lizenzbedingungen von MySQL finden Sie hier:

http://www.mysql.com/about/legal

MariaDB kann ausschließlich gemäß den Regeln der GPL verwendet werden.

36.1 Installation und Inbetriebnahme

Installation

Bei allen gängigen Distributionen werden MySQL- und/oder MariaDB-Pakete mitgeliefert. Fedora und openSUSE stellen sogar Pakete für beide Varianten zur Verfügung. Der Datenbank-Server selbst, seine Bibliotheken und Administrationswerkzeuge befinden sich üblicherweise in unterschiedlichen Paketen. Tabelle 36.1 fasst zusammen, welche Pakete Sie üblicherweise benötigen (Stand: Sommer 2013). Diese Pakete installieren Sie je nach Distribution mit `apt-get`, `yum` oder `zypper`.

Distribution	Datenbanksystem	Pakete
Debian	MySQL 5.5	`mysql-server`, `mysql-client`, `mysql-common`
Fedora	MariaDB 5.5	`mariadb-server`, `mariadb`, `mariadb-libs`
Fedora	MySQL 5.5	`community-mysql-server`, `community-mysql`, `community-mysql-libs`
openSUSE	MariaDB 5.5	`mariadb`, `mariadb-client`, `libmysqlclient18`
openSUSE	MySQL 5.5	`mysql-community-server`, `mysql-community-server-client`, `libmysql55client`
RHEL 6	MySQL 5.1	`mysql-server`, `mysql`, `mysql-libs`
Ubuntu	MySQL 5.5	`mysql-server`, `mysql-client`, `mysql-common`

Tabelle 36.1 MySQL- und MariaDB-Pakete je nach Distribution

Bei Fedora ist es zweckmäßig, statt der Einzelpakete gleich die vordefinierte Paketgruppe `mysql` zu installieren. Obwohl man anderes vermuten möchte, werden dadurch MariaDB-Pakete installiert! Die Fedora-Entwickler wollen offensichtlich unbedingt vermeiden, dass Sie »aus Versehen« MySQL-Pakete installieren.

```
root#  yum groupinstall mysql
```

Start/Stopp

MySQL ist ein Dämon, der bei Fedora, RHEL und openSUSE explizit gestartet werden muss (siehe auch Abschnitt 16.5). Fedora und openSUSE verwenden auch für MariaDB den Dienstnamen `mysqld` bzw. `mysql`, d. h., das Startkommando ist unabhängig davon, ob Sie den originalen MySQL-Server oder MariaDB verwenden.

```
root#  systemctl start mysqld              (Fedora, einmalig starten)
root#  systemctl enable mysqld             (Fedora, immer starten)
root#  service mysql start                 (openSUSE, einmalig starten)
root#  insserv mysql                       (openSUSE, immer starten)
root#  service mysqld start                (RHEL 6, einmalig starten)
root#  chkconfig --level 35 mysqld on      (RHEL 6, immer starten)
```

Die Datenbankdateien des MySQL- bzw. MariaDB-Servers werden im Verzeichnis `/var/lib/mysql` gespeichert. Der Ort der Logging-Dateien variiert je nach Distribution. Üblich sind `/var/log/syslog` (Debian, Ubuntu), `/var/lib/mysql/`*hostname* (SUSE) bzw. `/var/log/mysql*`.

Konfiguration

Die Konfiguration des MySQL- bzw. MariaDB-Servers erfolgt durch die Datei `/etc/my.cnf` bzw. `/etc/mysql/my.cnf` (Debian, Ubuntu). Unter Fedora werden außerdem die Dateien `/etc/my.conf.d/*.conf` berücksichtigt.

`my.cnf` ist für den gewöhnlichen Betrieb vorkonfiguriert. Aus Platzgründen kann ich nicht auf alle Schlüsselwörter für diese Datei eingehen. Einige sicherheitsrelevante Details möchte ich aber doch herausgreifen.

Grundsätzlich ist die Konfigurationsdatei durch `[`*name*`]` in mehrere Abschnitte gegliedert. Im Folgenden beziehe ich mich ausschließlich auf den Abschnitt `[mysqld]`, der den MySQL- bzw. MariaDB-Server an sich betrifft. Änderungen an diesem Abschnitt werden nur wirksam, wenn Sie den Datenbank-Server neu starten. Die anderen Abschnitte dienen zur Konfiguration diverser Client-Programme.

- **`bind-address = 127.0.0.1`:** Diese Einstellung bewirkt, dass Netzwerkverbindungen zum Datenbank-Server ausschließlich vom lokalen Rechner aus möglich sind, nicht aber von anderen Rechnern im lokalen Netzwerk oder aus dem Internet. Wenn MySQL/MariaDB ohnedies nur von lokalen Programmen genutzt werden soll, z. B. von PHP-Scripts des auf dem gleichen Rechner installierten Webservers, vergrößert diese Einstellung die Sicherheit. Bei Debian und Ubuntu gilt diese Einstellung standardmäßig, bei anderen Distributionen sollte sie nach Möglichkeit hinzugefügt werden.
- **`skip-networking`:** Diese Einstellung verhindert jeglichen Netzwerkzugang zum MySQL- bzw. MariaDB-Server. Selbst lokale Netzwerkverbindungen sind damit verboten. Die Einstellung ist noch restriktiver als `bind-address = 127.0.0.1`. Ein

Verbindungsaufbau ist nur noch für lokale Programme möglich, die über eine sogenannte Socket-Datei mit dem Datenbank-Server kommunizieren. Das trifft z. B. für PHP-Scripts und C-Programme zu. Programme, die via TCP/IP mit dem Datenbank-Server kommunizieren, können den MySQL-Server nicht nutzen. Diese Einschränkung betrifft insbesondere alle Java-Programme. Aus diesem Grund sollten Sie im Zweifelsfall `bind-address = 127.0.0.1` vorziehen.

IPv6

MySQL und MariaDB unterstützen ab Version 5.5 IPv6. Allerdings ist der Datenbank-Server standardmäßig so vorkonfiguriert, dass IPv6-Verbindungen abgelehnt werden. Wenn Sie sowohl IPv4- als auch IPv6-Verbindungen zulassen möchten, müssen Sie in `my.cnf` die Einstellung `bind-address=::` verwenden. `bind-address=::1` lässt ausschließlich IPv6-Verbindungen durch `localhost` zu. Beachten Sie, dass ein IPv6-Verbindungsaufbau nur gelingt, wenn Sie die betreffende IP-Adresse vorher mit dem SQL-Kommando `GRANT` oder durch eine direkte Änderung an der `host`-Spalte der Tabelle `mysql.user` zugelassen haben.

root-Passwort

Bei Debian und Ubuntu müssen Sie während der Installation des MySQL-Servers ein `root`-Passwort angeben. `root` hat nicht nur in Linux, sondern auch in MySQL eine besondere Bedeutung und verfügt über uneingeschränkte Administrationsrechte.

Debian und Ubuntu richten außerdem den MySQL-Benutzer `debian-sys-main` ein und versehen diesen mit einem zufälligen Passwort, das sich im Klartext in der Datei `/etc/mysql/debian.cnf` befindet, die nur Linux-`root` lesen kann. Das für den Start von MySQL erforderliche Script `/etc/mysql/debian-start` greift auf diesen Benutzer zurück. Deswegen darf der Benutzer `debian-sys-maint` nicht deaktiviert werden! Nach einer Passwortänderung müssen Sie auch `debian.cnf` entsprechend aktualisieren.

Fedora, Red Hat und SUSE verzichten auf die Absicherung von MySQL bzw. MariaDB. Deswegen kann nach der Installation jeder unter Verwendung des Benutzernamens `root` ohne Passwort eine Verbindung zu MySQL herstellen. Abhilfe schaffen die folgenden Kommandos:

```
user$   mysql -u root
mysql>  UPDATE mysql.user SET password=PASSWORD('xxx') WHERE user='root';
mysql>  FLUSH PRIVILEGES;
mysql>  exit
```

Von nun an müssen Sie sich beim Start von `mysql` anmelden:

```
user$  mysql -u root -p
Enter password:  ******
```

Die Verwaltung der Benutzernamen und Passwörter in MySQL und in Linux ist vollkommen voneinander getrennt. Aus Sicherheitsgründen sollten Sie auf keinen Fall für MySQL-Benutzer und für Linux-Benutzer dieselben Passwörter verwenden!

MySQL-Passwörter müssen oft im Programmcode gespeichert werden und sind daher wesentlich schwerer zu schützen als gewöhnliche Linux-Passwörter.

Anonyme MySQL-Benutzer

Der MySQL-Benutzer `root` ist nun durch ein Passwort abgesichert. Je nach Distribution kann es aber sein, dass es einen anonymen MySQL-Benutzer gibt. Das bedeutet, dass sich jeder mit einem beliebigen Benutzernamen beim MySQL-Server anmelden kann. Der anonyme Benutzer hat zwar nach dem MySQL-Login nur wenige Rechte, dennoch stellt dieser Benutzer ein Sicherheitsrisiko dar und sollte eliminiert werden.

Ob es anonyme Benutzer gibt, stellen Sie mit dem Kommando `mysql` fest. Sie erkennen anonyme Benutzer daran, dass im `SELECT`-Ergebnis die Spalte `user` leer ist. Mit dem `DELETE`-Kommando löschen Sie diese Benutzer. `FLUSH PRIVILEGES` macht die Änderung in der Benutzerdatenbank sofort wirksam.

```
user$  mysql -u root -p
Enter password:  *******
mysql>  SELECT user, host, password FROM mysql.user;
+------+---------------+-------------------------------------------+
| user | host          | password                                  |
+------+---------------+-------------------------------------------+
| root | localhost     | *AFCF054603403E6863B8DCFC1BEAC269746E8720 |
| root | <hostname>    | *AFCF054603403E6863B8DCFC1BEAC269746E8720 |
| root | 127.0.0.1     | *AFCF054603403E6863B8DCFC1BEAC269746E8720 |
| root | ::1           | *AFCF054603403E6863B8DCFC1BEAC269746E8720 |
|      | localhost     |                                           |
|      | <hostname>    |                                           |
+------+---------------+-------------------------------------------+
mysql>  DELETE FROM mysql.user WHERE user='';
mysql>  FLUSH PRIVILEGES;
mysql>  exit
```

Erste Tests

Neue Datenbank, neuer Benutzer

Um MySQL zu testen, müssen Sie die Datenbanksprache SQL kennen, was ich hier voraussetze. Das Ziel der folgenden Kommandos besteht darin, die neue Datenbank `mydatabase` und einen neuen Nutzer `newuser` zu schaffen, der auf diese Datenbank zugreifen darf. Für derartige Arbeiten setzen Sie am einfachsten das Programm `mysql` ein. Es hat eine vergleichbare Aufgabe wie eine Linux-Shell: Es nimmt SQL-Kommandos entgegen, leitet diese an den MySQL- oder MariaDB-Server weiter und zeigt schließlich das Ergebnis an. Dabei müssen alle SQL-Kommandos mit einem Strichpunkt enden.

```
user$  mysql -u root -p
Enter password:  ******
...
```

```
mysql>  CREATE DATABASE mydatabase;
mysql>  GRANT ALL ON mydatabase.* TO newuser@localhost
        IDENTIFIED BY 'xxxxxxxxx';
mysql>  exit
```

Alle weiteren Tests mit der neuen Datenbank kann nun der MySQL-Benutzer `newuser` durchführen. Wie unter Linux ist es auch in MySQL zweckmäßig, so wenig wie möglich als `root` zu arbeiten.

Tabelle erzeugen und mit Daten füllen

Mit den folgenden Kommandos erzeugt `newuser` eine neue Tabelle (`CREATE TABLE`), fügt darin einige Datensätze ein (`INSERT`) und sieht sich schließlich alle Datensätze an (`SELECT`). Bei der Tabelle spielt die Spalte `id` eine besondere Rolle: Der MySQL-Server fügt dort für jeden neuen Datensatz selbstständig eine eindeutige Zahl ein. Diese Zahl dient zur Identifizierung des Datensatzes.

```
user$  mysql -u newuser -p
Enter password:  ******
mysql>  USE mydatabase;
mysql>  CREATE TABLE mytable (
          id INT NOT NULL AUTO_INCREMENT,
          txt VARCHAR(100),
          n  INT,
          PRIMARY KEY(id));
mysql>  INSERT INTO mytable (txt, n) VALUES('abc', 123);
mysql>  INSERT INTO mytable (txt, n) VALUES('efgsd', -4);
mysql>  INSERT INTO mytable (txt, n) VALUES(NULL, 0);
mysql>  SELECT * FROM mytable;
+----+-------+------+
| id | txt   | n    |
+----+-------+------+
|  1 | abc   |  123 |
|  2 | efgsd |   -4 |
|  3 | NULL  |    0 |
+----+-------+------+
mysql>  exit
```

36.2 Administrationswerkzeuge

Zu MySQL und MariaDB gibt es unzählige Administrationswerkzeuge. Standardmäßig stehen die Kommandos `mysql`, `mysqldump` sowie einige weitere, textbasierte Werkzeuge zur Verfügung. Optional können Sie diverse weitere Programme installieren, die aber teilweise einen grafischen Desktop voraussetzen. Dieser Abschnitt gibt einen kurzen Überblick über die wichtigsten Werkzeuge. Nicht enthalten sind die speziell für Backups konzipierten Kommandos `mysqldump` und `mylvmbackup`, die ich in Abschnitt 36.3 zum Thema Backup beschreibe.

mysql

Hinter dem Programm `mysql` verbirgt sich nicht etwa der MySQL-Server (der hat den Programmnamen `mysqld`), sondern ein Kommandozeilen-Client. Damit können Sie eine Verbindung zum MySQL- oder MariaDB-Server herstellen und dann SQL-Kommandos ausführen. Soweit es sich dabei um SELECT-Kommandos handelt, zeigt das Programm die Abfrageergebnisse im Textmodus an.

Beim Start von `mysql` geben Sie normalerweise mit `-u` den MySQL-Benutzernamen an. Die Option `-p` bewirkt, dass Sie nach dem Start das dazugehörende Passwort angeben können. Wenn der MySQL-Server nicht auf dem lokalen Rechner läuft, geben Sie den Hostnamen mit `-h` an. Optional können Sie auch eine Standarddatenbank angeben, die als Datengrundlage für alle weiteren SQL-Kommandos gilt.

```
user$  mysql -u root -p meinedatenbank
Enter password:  *******
```

Anschließend können Sie interaktiv SQL-Kommandos eingeben, die Sie durch einen Strichpunkt abschließen. Das `mysql`-spezifische Kommando `status`, das auch ohne Strichpunkt ausgeführt werden kann, zeigt Informationen zur aktuellen Verbindung sowie Eckdaten des MySQL-Servers an. Strg+D beendet das Programm.

```
mysql>  status
mysql  Ver 14.14 Distrib 5.5.22, for debian-linux-gnu (x86_64)
...
Connection id:          48097
Server version:         5.5.22-0ubuntu1 (Ubuntu)
Protocol version:       10
Connection:             Localhost via UNIX socket
Server characterset:    latin1
Db     characterset:    latin1
Client characterset:    utf8
Conn.  characterset:    utf8
UNIX socket:            /var/run/mysqld/mysqld.sock
Uptime:                 7 days 13 hours 31 min 33 sec
...
```

UTF8-Zeichensatz

Bei älteren MySQL-Versionen lautet die Ausgabe von `status` beim Eintrag `Client characterset` oft `latin1`. Dann werden internationale Sonderzeichen in Linux-Textkonsolen falsch dargestellt, weil dort standardmäßig der UTF8-Zeichensatz gilt. Abhilfe schafft das folgende SQL-Kommando:

```
mysql>  SET NAMES utf8;
```

»Intelligentere« Client-Programme kümmern sich selbst um die korrekte Einstellung des Zeichensatzes. MySQL selbst kommt mit allen erdenklichen Zeichensätzen zurecht. Sie müssen nur darauf achten, dass Sie beim Einrichten neuer Tabellen den richtigen Zeichensatz für Textspalten wählen.

mysql im Batch-Modus

Für administrative Zwecke und insbesondere zum Einspielen von Backups kann `mysql` auch SQL-Kommandos aus einer `*.sql`-Datei verarbeiten:

```
user$  mysql -u root -p meinedatenbank < kommandos.sql
Enter password:  *******
```

mysqladmin

`mysqladmin` ermöglicht es, verschiedene administrative Aufgaben in Form eines Kommandos auszuführen. Zu allen `mysqladmin`-Kommandos gibt es auch gleichwertige SQL-Kommandos (z. B. `CREATE DATABASE`). Der Vorteil von `mysqladmin` besteht darin, dass es dabei hilft, wiederkehrende Aufgaben durch Scripts zu automatisieren.

Wie bei `mysql` geben Sie mit der Option `-u` den Benutzernamen und mit `-h` den Hostnamen (standardmäßig `localhost`) an. `-p` ohne weitere Angaben führt zur einer interaktiven Passwortabfrage. Die können Sie durch `-p`*`password`* ohne ein Leerzeichen nach `-p` vermeiden. Diese Bequemlichkeit hat aber den Nachteil, dass das Passwort im Klartext übertragen wird. Eine alternative Vorgehensweise besteht darin, die Login-Daten in einer Passwortdatei zu speichern bzw. auf den unter Debian und Ubuntu bereits vordefinierten MySQL-Benutzer `debian-sys-maint` zurückzugreifen. Dessen Passwortdatei `/etc/mysql/debian.cnf` ist allerdings nur für den Linux-`root` lesbar. Der Aufruf von `mysqladmin` sieht dann so aus:

```
root#  mysqladmin --defaults-file=/etc/mysql/debian.cnf kommando ...
```

Einen Überblick über die für `mysqladmin` verfügbaren Kommandos gibt `mysqladmin --help`. Die folgenden Zeilen geben einige Beispiele: Das erste Kommando erzeugt eine neue Datenbank, das zweite liefert eine Liste aller MySQL-Statusvariablen, das dritte gibt eine Liste aller aktiven MySQL-Threads (Verbindungen) zurück.

```
user$  mysqladmin -u root -p create  neuedatenbank
Enter password:  *******
user$  mysqladmin -u root -p extended-status
...
user$  mysqladmin -u root -p processlist
...
```

MySQL Workbench

MySQL stellt mit der MySQL Workbench ein hochwertiges Administrationsprogramm mit grafischer Benutzeroberfläche zur Verfügung. Sie können damit den Datenbank-Server überwachen, seine Einstellungen ändern, Benutzerrechte einstellen, neue Datenbanken einrichten, vorhandene Datenbanken auslesen, verändern und sichern, Datenbankschemas entwickeln etc. Die MySQL Workbench funktioniert gleichermaßen für MySQL und MariaDB, das Programm kennt aber keine MariaDB-spezifischen Optionen.

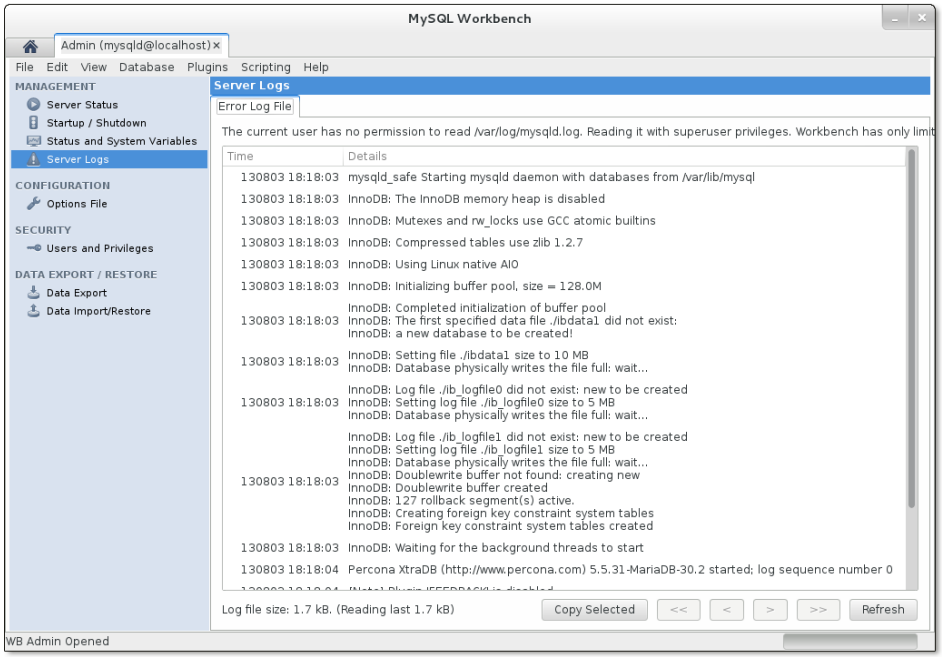


Abbildung 36.1 Die MySQL Workbench

Die meisten Distributionen stellen für die MySQL Workbench eigene Pakete zur Verfügung. Zu den prominenten Ausnahmen zählt leider RHEL. Um die MySQL Workbench auf Red-Hat-basierten Distributionen einzusetzen, müssen Sie die Pakete direkt von der MySQL-Website herunterladen:

http://dev.mysql.com/downloads/tools/workbench

phpMyAdmin

Das bekannteste MySQL-Administrationsprogramm ist phpMyAdmin. Sein größter Vorteil besteht darin, dass das Programm über einen Webbrowser bedient wird. Der eigentliche phpMyAdmin-Code läuft direkt auf dem Server. Das funktioniert auch dann, wenn der MySQL-Server aus Sicherheitsgründen so konfiguriert ist, dass keine Verbindungen über das Netzwerk zulässig sind.

Bei vielen Distributionen gibt es fertige phpMyAdmin-Pakete. Sollte das bei Ihrer Distribution nicht der Fall sein, laden Sie phpMyAdmin von der folgenden Website herunter und installieren die PHP-Dateien in ein Verzeichnis, auf das der Webserver Apache zugreifen kann.

http://www.phpmyadmin.net/home_page

Debian, Ubuntu

Beachten Sie noch Folgendes zur Ubuntu- bzw. Debian-spezifischen Konfiguration von phpMyAdmin: Alle Konfigurationsdateien befinden sich in `/etc/phpmyadmin`. Sofern Sie Apache als Webserver verwenden, kümmert sich `apache.conf` darum, das tatsächliche Installationsverzeichnis `/usr/share/phpmyadmin` durch einen Alias auf das Webverzeichnis `phpmyadmin` abzubilden. Die Sicherheitseinstellungen in `apache.conf` betreffen standardmäßig nur das Setup-Script von phpMyAdmin, das Sie normalerweise aber gar nicht brauchen.

`apache.conf` wird durch einen symbolischen Link in `/etc/apache2/conf.d` in die Apache-Konfiguration integriert. Wenn Sie über das Protokoll HTTPS mit phpMyAdmin kommunizieren möchten, löschen Sie diesen Link und fügen dann eine Include-Anweisung für `apache.conf` in Ihre HTTPS-Konfigurationsdatei ein:

```
<VirtualHost _default_:443>
  ...
  Include /etc/phpmyadmin/apache.conf
</VirtualHost>
```

Konfiguration

Für phpMyAdmin-Konfigurationsdetails ist die Datei `config.inc.php` verantwortlich. Hier müssen Sie nur Veränderungen vornehmen, wenn Sie einige phpMyAdmin-Spezialfunktionen benutzen möchten. Diese Funktionen setzen allerdings voraus, dass Sie vorher eine neue MySQL-Datenbank einrichten, in der phpMyAdmin Daten speichern kann. Weitere Informationen finden Sie hier:

https://phpmyadmin.readthedocs.org/en/latest/setup.html

phpMyAdmin absichern

phpMyAdmin ist ein beliebtes Einfallstor für Cracker. Es gibt im Internet zahllose automatisierte Tools, die Webserver nach schlecht abgesicherten oder veralteten phpMyAdmin-Installationen absuchen. Ein fehlendes oder leicht erratbares MySQL-`root`-Passwort gibt dem Angreifer MySQL-Administratorrechte! Ergreifen Sie daher die folgenden Vorsichtsmaßnahmen:

- Sichern Sie die MySQL-Installation ab, bevor Sie phpMyAdmin installieren (siehe Abschnitt 36.1).
- Geben Sie dem phpMyAdmin-Verzeichnis einen Alias, der nicht ganz leicht erraten werden kann. *http://mysite.de/pMa1* ist sicherer als *http://mysite.de/phpmyadmin*.
- Akzeptieren Sie für das phpMyAdmin-Verzeichnis nach Möglichkeit nur das sichere `https`-Protokoll, nicht `http`.
- Sichern Sie das phpMyAdmin-Verzeichnis auch auf Apache-Ebene durch ein Passwort ab, z. B. durch eine `.htaccess`-Datei (siehe Abschnitt 35.2).

36.3 Backups

Auch wenn Sie nicht vorhaben, sich auf die Datenbankadministration zu spezialisieren, sollten Sie wissen, wie Sie ein fehlerfreies Backup einer MySQL- oder MariaDB-Datenbank durchführen. Dabei gibt es mehr Varianten und Spielarten, als man es für möglich halten möchte. Dieser Abschnitt stellt die Kommandos `mysqldump` und `mylvmbackup` vor. Wenn Sie außer den zu bestimmten Zeiten durchgeführten Backups auch kontinuierliche Backups benötigen, aktivieren Sie das (binäre) Logging. Damit wird jede Änderung an der Datenbank in einer Logging-Datei festgehalten. Die Logging-Dateien können auch als Basis für die Replikation der Datenbank auf einen zweiten Server verwendet werden.

Tabellentypen

Die Vielfalt der MySQL-Backup-Verfahren hat unter anderem damit zu tun, dass MySQL verschiedene Tabellentypen kennt: Beim Anlegen einer Tabelle kann der Datenbankentwickler bzw. das Programm zwischen verschiedenen Tabellentypen wählen. Es ist sogar möglich, innerhalb einer Datenbank Tabellen mit unterschiedlichen Typen zu verwenden. Die beiden wichtigsten Typen sind momentan MyISAM und InnoDB, außerdem Aria bei MariaDB. Je nach Tabellentyp stehen nicht nur unterschiedliche Zusatzfunktionen zur Verfügung (Transaktionen, Foreign-Key-Regeln, Volltextsuche), auch das zugrunde liegende Dateiformat und das optimale Backup-Verfahren variieren.

Wenn Sie nicht wissen, welche Datenbanken Ihr MySQL-Server verwaltet und welchen Typ die darin enthaltenen Tabellen aufweisen, führen Sie im Kommandozeilen-Client `mysql` das folgende SQL-Kommando aus. Das resultierende Ergebnis listet alle Tabellen auf. Die Spalte `table_schema` gibt dabei den Datenbanknamen an, `engine` den Tabellentyp.

```
mysql>  SELECT table_schema, table_name, engine
        FROM information_schema.tables
        WHERE table_type='BASE TABLE'
        ORDER BY table_schema, table_name;

table_schema  table_name     engine
-----------------------------------
mylibrary     authors        InnoDB
mylibrary     categories     InnoDB
mylibrary     counters       MyISAM
mylibrary     fulltitles     MyISAM
mylibrary     languages      InnoDB
...
```

mysqldump

Das zum Lieferumfang von MySQL zählende Kommando `mysqldump` erstellt ein Backup einer MySQL-Datenbank in Form von SQL-Anweisungen. Die resultierende Datei kann später mit `mysql` wieder in eine bereits vorhandene Datenbank eingespielt werden. Die prinzipielle Syntax sieht so aus:

```
user$ mysqldump -u root -p [optionen] datenbankname > backup.sql
```

Details des Backups können Sie durch zahllose Optionen steuern (siehe auch `mysqldump --help`). Die optimale Kombination von Optionen hängt unter anderem davon ab, in welchem Format die Tabellen Ihrer MySQL-Datenbank vorliegen, also im MyISAM- oder im InnoDB-Format.

Backup von MyISAM-Tabellen

Bei MyISAM-Tabellen reicht die Option `--lock-all-tables`. Sie bewirkt, dass `mysqldump` am Beginn des Backups *alle* Tabellen durch ein `LOCK`-Kommando blockiert und erst am Ende des Backups wieder freigibt. Standardmäßig führt `mysqldump` das Locking hingegen Tabelle für Tabelle aus, also immer nur für die Tabelle, die gerade bearbeitet wird. Das kann aber zur Folge haben, dass sich einzelne Tabellen während des Backups verändern und dass die Verknüpfungen zwischen den Tabellen letztlich nicht mehr stimmen.

```
user$ mysqldump -u root -p --lock-all-tables dbname > backup.sql
```

Backup von InnoDB-Tabellen

Wesentlich mehr Optionen brauchen Sie für ein Backup einer Datenbank mit InnoDB-Tabellen: Mit `--skip-opt` deaktivieren Sie einige, speziell für MyISAM gedachte Standardoptionen. `--single-transaction` bewirkt, dass das gesamte Backup im Rahmen einer Transaktion durchgeführt wird. Damit ist ausgeschlossen, dass sich während des Backups Daten ändern, was zu inkonsistenten Verknüpfungen zwischen den Tabellen führen kann. `--disable-keys` bewirkt, dass beim späteren Einlesen der Daten vorübergehend die Indexaktualisierung deaktiviert wird. Der Index wird erst zum Schluss vollständig neu erzeugt, was wesentlich schneller ist. Dank `--create-options` verwendet `mysqldump` bei der Ausgabe alle MySQL-spezifischen Optionen des `CREATE-TABLE`-Kommandos.

`--quick` bewirkt, dass `mysqldump` die Tabellen Datensatz für Datensatz vom Server abholt, anstatt sie alle auf einmal zu lesen. Das ist bei großen Tabellen effizienter. Aufgrund von `--extended-insert` erzeugt `mysqldump` `INSERT`-Kommandos, die mehrere Datensätze auf einmal einfügen, was einerseits die Größe der Backup-Datei ein wenig reduziert und später das Wiedereinspielen der Daten beschleunigt. `--add-drop-table` bewirkt, dass `mysqldump` jedem `CREATE-TABLE`-Kommando ein `DROP-TABLE`-Kommando voranstellt. Das vermeidet Fehler, wenn – z. B. aufgrund eines unvollständig eingespielten Backups – einzelne Tabellen bereits in der Datenbank existieren.

```
user$  mysqldump -u root -p --skip-opt --single-transaction  \
         --disable-keys --create-options --quick  \
         --extended-insert --add-drop-table dbname >  backup.sql
```

Bleibt noch die naheliegende Frage, wie Sie am besten vorgehen, wenn eine Datenbank sowohl MyISAM- als auch InnoDB-Tabellen enthält. In diesem Fall verwenden Sie `mysqldump` einfach ohne weitere Optionen. Falls die Datenbank während des Backups genutzt wird, kann es nun aber passieren, dass sich während des Backups Tabellen verändern. Wenn Sie Pech haben, ist das Backup dann inkonsistent, d. h., miteinander verknüpfte Tabellen enthalten Verweise auf nicht mehr existente Datensätze. Dieses Problem lässt sich mit `mysqldump` nicht umgehen. Am besten verwenden Sie stattdessen ein anderes Backup-Verfahren (siehe den folgenden Abschnitt zu `mylvmbackup`).

Wenn Sie ein Backup *aller* Datenbanken erstellen (nicht ein Backup einer bestimmten Datenbank), geben Sie die Option `--all-databases` an.

SPs und Trigger

Beachten Sie, dass `mysqldump` standardmäßig weder Stored Procedures (SPs) noch Trigger speichert. Wenn Sie das wünschen, geben Sie zusätzlich die Optionen `--routines` und `--triggers` an.

Datenbank wiederherstellen

Um eine Datenbank aus einem Backup wiederherzustellen, erzeugen Sie zuerst die betreffende Datenbank (falls es sie noch nicht gibt). Anschließend übergeben Sie die Backup-Datei an `mysql`. Dabei stellt die Option `-default-character-set` sicher, dass die im UTF8-Format gespeicherten Zeichenketten auch tatsächlich in diesem Format gelesen werden.

```
user$ mysqladmin create dbname
user$ mysql -u root -p --default-character-set=utf8 dbname < backup.sql
```

Komprimierte Backups

Mit `mysqldump` erzeugte Backup-Dateien sind aufgrund des Textformats sehr groß. Dieses Problem umgehen Sie am einfachsten dadurch, dass Sie die Backups sofort komprimieren bzw. beim Wiedereinspielen direkt dekomprimieren. Die entsprechenden Kommandos sehen so aus:

```
user$ mysqldump [optionen] dbname | gzip -c > backup.sql.gz
user$ gunzip -c backup.sql.gz | mysql [optionen] dbname
```

Die Komprimierung durch `gzip` kostet allerdings eine Menge CPU-Ressourcen. Wenn Sie Rechenzeit sparen möchten und sich dafür mit etwas größeren Backup-Dateien abfinden können, empfiehlt sich der Einsatz des Komprimierkommandos `lzop` aus dem gleichnamigen Paket:

```
user$ mysqldump [optionen] dbname | lzip -c > backup.sql.lzo
user$ lzop -c -d backup.sql.lzo | mysql [optionen] dbname
```

mylvmbackup

Das Kommando `mysqldump` funktioniert für kleine Datenbanken ausgezeichnet. Allerdings sind die betroffenen Tabellen während des Backups nur eingeschränkt verwendbar – bei MyISAM-Tabellen aufgrund des Lockings, bei InnoDB-Tabellen aufgrund einer lang andauernden Transaktion. Für Datenbanksysteme, die im 24-Stunden-Betrieb unterbrechungsfrei laufen sollen, wird das mit zunehmender Datenbankgröße zu einem echten Problem.

Die optimale Lösung für dieses Problem wäre ein Hot-Backup-Verfahren, das störungsfrei im laufenden Betrieb funktioniert. Für InnoDB-Tabellen gibt es ein entsprechendes Backup-Programm, es ist aber nur im Rahmen einer kostenpflichtigen MySQL-Enterprise-Lizenz verfügbar.

Wenn Sie dafür kein Geld ausgeben möchten, haben Sie mit dem hier vorgestellten Kommando `mylvmbackup` eine gute Alternative: `mylvmbackup` minimiert die Zeit, während der die Datenbank blockiert ist, auf ein tolerierbares Minimum (im Regelfall wenige Sekunden, unabhängig von der Datenbankgröße!). Es setzt allerdings voraus, dass sich sämtliche Datenbankdateien in einem Logical Volume.

Das Perl-Script `mylvmbackup` kann bei vielen Distributionen als Paket installiert werden. Wenn Ihre Distribution kein entsprechendes Paket anbietet, laden Sie das Script von dieser Seite herunter:

http://www.lenzg.net/mylvmbackup

Grundlagen

Ich setze im Folgenden voraus, dass Sie mit LVM bereits vertraut sind (siehe die Abschnitte 2.7 und 25.15). Worauf es hier ankommt, ist die Möglichkeit, sogenannte LVM-Snapshots zu erstellen: Damit können Sie den Inhalt eines Logical Volumes (LV) gewissermaßen einfrieren und in diesem Zustand als neues LV in das Dateisystem einbinden.

Das ursprüngliche LV kann weiter verändert werden. Allerdings bleibt das Snapshot-LV nur verwendbar, solange es genug Platz für Kopien aller geänderten Datenblöcke gibt. Diese Datenblöcke werden in einen Snapshot-Puffer kopiert, dessen Größe Sie beim Erzeugen des Snapshots angeben. LVM-intern wird jeder Datenblock vor seiner Veränderung kopiert. Der Snapshot sieht so den alten Zustand, während das ursprüngliche LV den geänderten Datenblock verwendet.

`mylvmbackup` nutzt einen LVM-Snapshot, um alle Datenbankdateien aus dem Verzeichnis `/var/lib/mysql` zu sichern. Im Detail sieht die Vorgehensweise des Scripts so aus:

- Das SQL-Kommando `FLUSH TABLES WITH READ LOCK` bewirkt, dass alle MyISAM-Dateien physikalisch auf der Festplatte gespeichert werden und dass danach alle Veränderungen durch andere Clients blockiert werden. Es kann sein, dass die Ausführung dieses Kommandos eine Zeit lang dauert, weil der MySQL-Server alle anderen, früher eingetroffenen `LOCK`-Kommandos abschließen muss.
- `lvcreate -s` erzeugt einen LVM-Snapshot und bindet diesen in das Dateisystem ein. Der Snapshot enthält zumindest das Verzeichnis `/var/lib/mysql`.
- `SHOW MASTER STATUS` ermittelt die gerade aktuelle binäre Logging-Datei und deren Position. Diese Informationen landen in der Backup-Datei `backup-pos/*_mysql.pos`. Sie sind wichtig, wenn das Backup später zum Einrichten eines Replikationssystems verwendet werden soll oder wenn inkrementelle Backups aus den binären Logging-Dateien verwendet werden sollen.
- `UNLOCK TABLES` gibt die MyISAM-Tabellen wieder frei. Der MySQL-Server ist nun wieder uneingeschränkt verfügbar. (InnoDB-Tabellen wurden zu keinem Zeitpunkt blockiert und müssen daher auch nicht freigegeben werden.)
- Nun wird der LVM-Snapshot in das Dateisystem eingebunden und ein Backup aller Dateien aus dem Verzeichnis `/var/lib/mysql` in ein `tar`-Archiv geschrieben. Bei großen Datenbanksystemen dauert das natürlich einige Zeit, deren Dauer auch davon abhängt, wie stark die Festplatte gerade durch andere Operationen beansprucht wird.
- Auch eine Kopie von `/etc/mysql/my.cnf` wird in das `tar`-Archiv eingebunden.
- Zu guter Letzt wird der LVM-Snapshot wieder aus dem Dateisystem gelöst und anschließend gelöscht.

Vielleicht wundern Sie sich darüber, dass es keinerlei Maßnahmen gibt, um die InnoDB-Dateien zu synchronisieren. Das ist nicht notwendig, weil Transaktionen für InnoDB-Tabellen ACID-konform ausgeführt werden. Aus den sogenannten Masterspace-Dateien, die alle Tabellen enthalten, und den dazugehörigen InnoDB-Logging-Dateien kann der InnoDB-Treiber zu jedem Zeitpunkt alle bereits abgeschlossenen Transaktionen vollständig wiederherstellen, auch wenn die Änderungen im Masterspace noch gar nicht gespeichert wurden. Diese Sicherheitsmaßnahme schützt primär gegen Datenverluste bei einem Absturz oder Stromausfall, vereinfacht aber auch das Backup. Wichtig ist nur, dass der InnoDB-Masterspace und die Logging-Dateien exakt zum gleichen Zeitpunkt für das Backup eingefroren werden – und das ist durch den LVM-Snapshot sichergestellt.

Das so erstellte Backup unterscheidet sich in zwei Punkten von `mysqldump`-Resultaten: Erstens erfasst es grundsätzlich *alle* Datenbanken inklusive aller Zusatzdaten wie Stored Procedures, Trigger, Zugriffsrechte etc. Und zweitens liegt es in binärer Form vor. Das hat zur Folge, dass nur alle Datenbanken zusammen wiederhergestellt werden können und dass zum Wiedereinspielen des Backups ein MySQL-Server in derselben Konfiguration und möglichst auch mit derselben MySQL-Versionsnummer erforderlich ist.

Konfiguration

Die Konfiguration erfolgt in der Datei `/etc/mylvmbackup.conf`. Die folgenden Zeilen zeigen eine Beispielkonfiguration. Dabei setze ich voraus, dass es für das Verzeichnis `/var/lib/mysql` eine eigene LVM-Partition mit dem Namen `/dev/vg1/mysql` gibt.

```
# /etc/mylvmbackup.conf
[mysql]
user      =  root
password  =  *******
host      = localhost
port      = 3306
socket    =
mycnf     = /etc/mysql/my.cnf

[lvm]
vgname    =  vg1
lvname    =  mysql
backuplv  =
lvsize    = 5G

[fs]
xfs=0
mountdir  = /var/cache/mylvmbackup/mnt/
backupdir = /var/cache/mylvmbackup/backup/
relpath   =

[tools]
... (normalerweise keine Änderungen)

[misc]
backuptype     = tar
prefix         = backup
tararg         = cvzf
tarsuffixarg   =
rsyncarg       = -avWP
datefmt        = %Y%m%d_%H%M%S
innodb_recover =  1
pidfile        = /var/tmp/mylvmbackup_recoverserver.pid
```

Dazu einige Anmerkungen: `vgname` und `lvname` geben den VG- und LV-Namen an. Daraus wird der LVM-Device-Name `/dev/vgname/lvname` zusammengesetzt. Mit `backuplv` können Sie der Snapshot-Partition einen bestimmten Namen geben. Standardmäßig verwendet das Backup-Script `mysql_snapshot`. `lvsize` gibt die Größe des Snapshot-Puffers für geänderte Datenblöcke an. Der Puffer muss so groß sein, dass darin alle Datenblöcke der MySQL-Partition Platz finden, die sich während des Backups ändern. 5 GByte ist schon recht großzügig bemessen. `mylvmbackup` verrät zum Schluss, wie viel Speicher während des Backups tatsächlich verwendet wurde. Mit dieser Information können Sie die Einstellung optimieren.

`backupdir` gibt an, wo `mylvmbackup` die Backup-Dateien speichern soll. Das Verzeichnis sollte sich möglichst in einem anderen LV befinden als `/var/lib/mysql`. `relpath` gibt an, wo sich das Verzeichnis `/var/lib/mysql` *relativ* zum LV-Mount-Punkt befindet. Wenn es ein eigenes LV für `/var/lib/mysql` gibt, ist `relpath` leer. Wenn das LV dagegen das gesamte `/var`-Verzeichnis erfasst, müssen Sie `relpath=lib/mysql/` verwenden.

`innodb_recover` gibt an, ob schon während des Backups getestet werden soll, ob der InnoDB-Masterspace und die dazugehörenden Logging-Dateien synchron sind. Ist das nicht der Fall, erfolgt im Rahmen des Backups ein InnoDB-Recovery-Durchlauf, um in der Logging-Datei aufgezeichnete Transaktionen auch im Masterspace auszuführen. Das verlängert die Zeit, die für das Backup erforderlich ist, verkürzt aber die Zeit, um später ein neues System auf der Basis des Backups einzurichten.

Backup erstellen

Das eigentliche Backup führen Sie nun so durch:

```
root#  mylvmbackup
```

Anschließend finden Sie im Verzeichnis `/var/cache/mylvmbackup/backup` ein mit dem aktuellen Datum versehenes `*.tar.gz`-Archiv, das außer den eigentlichen Datenbankdateien auch eine Kopie von `my.cnf` sowie Logging- und Replikationsinformationen enthält (Datei `backup-pos/*.pos`).

Datenbank wiederherstellen

Die folgenden Kommandos zeigen, wie Sie das Backup wieder einspielen. Das erste `tar`-Kommando ist ein wenig unübersichtlich: Es extrahiert nur jene Dateien, die sich innerhalb des Archivs im Verzeichnis `backup` befinden, und schreibt sie – ohne vorangestelltes `backup`-Verzeichnis – in das Verzeichnis `/var/lib/mysql`. Das zweite `tar`-Kommando extrahiert analog die Archivdateien `backup-pos/*` direkt in das Verzeichnis `/etc/mysql`.

```
root#  /etc/init.d/mysql stop
root#  rm -rf /var/lib/mysql/*  oder  mv /var/lib/mysql/* /bak/
root#  mv /etc/mysql/my.cnf /etc/mysql/my.cnf.bak
root#  tar -x -f backup.tar.gz -C /var/lib/mysql --strip 1 backup
root#  tar -x -f backup.tar.gz -C /etc/mysql --strip 1 backup-pos
root#  mv /etc/mysql/backup-*_my.cnf /etc/mysql/my.cnf
root#  /etc/init.d/mysql start
```

Inkrementelle Backups durch binäres Logging

Über ein Script können Sie Backups mit `mysqldump` automatisieren und so täglich oder wöchentlich ein Backup erstellen. Um einen möglichen Datenverlust im Katastrophenfall weiter zu minimieren, können Sie außerdem inkrementelle Backups aktivieren. Dazu fügen Sie in `/etc/mysql/my.cnf` die folgende Zeile ein und starten den MySQL-Server dann neu:

```
# Änderung in /etc/mysql/my.cnf
log_bin = /var/log/mysql/mysql-bin.log
```

Der MySQL-Server protokolliert nun alle SQL-Kommandos, die Daten verändern. Die Logging-Dateien werden automatisch durchnummeriert (`mysql-bin.000001`, `.000002` etc.). Da sich immer nur die letzte Datei ändert, ist es relativ einfach, diese Dateien in kurzen Abständen in ein Backup-Verzeichnis zu übertragen (z. B. mit `rsync`).

Wenn Sie Ihre Datenbanken wiederherstellen müssen, führen Sie zuerst die oben beschriebenen Restore-Schritte für das letzte Komplett-Backup aus. Anschließend spielen Sie mit `mysqlbinlog` alle Änderungen ein, die seither aufgetreten sind. Die Kommandoabfolge sieht so aus:

```
root# mysqlbinlog --start-position=<p> mysql-bin.<n> | mysql -u root -p
root# mysqlbinlog mysql-bin.<n+1> | mysql -u root -p
root# mysqlbinlog mysql-bin.<n+2> | mysql -u root -p
..
```

Bevor Sie loslegen können, brauchen Sie noch zwei Informationen: Welche Nummer hat die erste Logging-Datei, die Sie berücksichtigen müssen (`<n>`)? Und mit welcher Position innerhalb der ersten Datei beginnen Sie (`<p>`)? `mylvmbackup` hat diese Informationen zum Glück im Backup-Archiv gespeichert. Wenn Sie die Daten wie oben beschrieben extrahiert haben, finden Sie die erforderlichen Informationen in den ersten zwei Zeilen der Datei `/etc/mysql/*_msql.pos`:

```
root# less /etc/mysql/backup-20101128_145023_mysql.pos
Master:File=mysql-bin.000016
Master:Position=98
...
```

Replikation

Ist das binäre Logging einmal aktiviert, ist es nur noch ein kleiner Schritt zur Replikation: Damit synchronisieren Sie einen zweiten MySQL-Server mit dem ersten und haben so jederzeit ein aktives zweites Datenbanksystem, das im Notfall das Hauptsystem ersetzen kann. Eine Einführung in die Replikation von MySQL-Datenbanken gibt das MySQL-Handbuch:

http://dev.mysql.com/doc/refman/5.5/en/replication.html

Kapitel 37
Postfix und Dovecot

Dieses Kapitel beschreibt, wie Sie auf einem Root-Server einen E-Mail-Server einrichten. Damit können Sie alle Mitarbeiter einer Firma oder Organisation mit eigenen E-Mail-Adressen ausstatten. Jeder Mitarbeiter kann E-Mails per SMTP versenden und per POP/IMAP abholen/lesen. Als SMTP-Server kommt dabei das Programm Postfix zum Einsatz, als POP/IMAP-Server und zur SMTP-Authentifizierung das Programm Dovecot.

Zur Eindämmung der Spam-Flut können Sie SpamAssassin einsetzen. Wenn Ihre Mitarbeiter (bzw. die Ihrer Auftraggeber) mit Windows-PCs arbeiten, lohnt sich eventuell auch die Installation des Virenschutzprogramms ClamAV. Bevor Sie an die Arbeit gehen können, brauchen Sie einen Server mit einem international gültigen Hostnamen. Sie müssen in der Lage sein, dessen DNS-Einträge selbst zu konfigurieren (MX-Eintrag, Reverse DNS).

Ich gehe in diesem Kapitel davon aus, dass Ihr Server unter Ubuntu oder Debian läuft. Selbstverständlich stehen die hier vorgestellten Programme Postfix, Dovecot, SpamAssassin etc. auch für andere Distributionen zur Verfügung, ich habe die Installation und Konfiguration aber nicht im Detail getestet. Beachten Sie, dass bei Fedora und RHEL standardmäßig das Programm Sendmail als Mail-Server installiert ist. Wenn Sie bei diesen Distributionen Postfix verwenden möchten, müssen Sie Sendmail vorher deinstallieren (`yum remove sendmail`)!

E-Mail ist ein wesentlich komplexeres Thema, als viele Einsteiger in diese Materie vermuten. Für jede Teilaufgabe stehen unterschiedliche Programme und Kommandos zur Auswahl, und es existieren schier unendlich viele Konfigurationsmöglichkeiten. Dieses Kapitel beschreibt deswegen zuerst die wesentlichen Grundlagen der E-Mail-Kommunikation und gibt Ihnen einen ersten Überblick über die zur Auswahl stehenden Werkzeuge.

37.1 Einführung und Grundlagen

E-Mail ist ganz einfach, oder? Aus der Sicht des Endanwenders stimmt das – zumindest, solange alles funktioniert. Hinter den Kulissen ist das E-Mail-System wesentlich komplexer, als es den Anschein hat. Es gibt viele Konfigurationsmöglichkeiten, die alle unter bestimmten Umständen ihre Berechtigung haben. Gute Bücher über E-Mail-Server wie Sendmail, Postfix oder Exim umfassen oft mehr als 1000 Seiten! Es liegt auf der Hand, dass ich hier nur auf die Grundkonfiguration eingehen kann.

Komponenten eines E-Mail-Servers – Glossar

Ein vollständiger E-Mail-Server besteht aus drei Komponenten:

- **MTA:** Der *Mail Transfer Agent* ist das, was umgangssprachlich als E-Mail-Server bezeichnet wird. Der MTA kümmert sich darum, E-Mails über das Internet zu versenden bzw. zu empfangen, wobei das Protokoll SMTP eingesetzt wird.

  Die meisten Einsteiger in die Interna der E-Mail-Welt sind sich nicht darüber im Klaren, dass sich die Zuständigkeit des MTAs auf den Netzwerkverkehr beschränkt und am Server endet. Empfangene E-Mails werden an den MDA weitergegeben, der sich um die lokale Speicherung kümmert. Es ist *nicht* Aufgabe des MTAs, E-Mails zu einem Benutzer zu bringen, der in der Regel auf einem anderen Rechner arbeitet!

  Beispiele: Courier, Cyrus, Exim, Postfix, Qmail, Sendmail

- **MDA:** Der *Mail Delivery Agent* kümmert sich um die lokale Zustellung von E-Mails, also um die Speicherung der beim MTA eintreffenden E-Mails in lokalen Postfächern. Ein »Postfach« meint in diesem Zusammenhang einfach ein Verzeichnis bzw. eine Datei auf dem Server.

  Beispiele: Maildrop, Procmail

  In einige MTAs ist ein MDA integriert bzw. wird mitgeliefert, z. B. das Kommando `local` bei Postfix. Die Programme Maildrop bzw. Procmail sind dennoch sehr populär, weil sie in der Regel noch mehr Konfigurationsmöglichkeiten bieten.

- **POP/IMAP-Server:** E-Mails werden selten direkt auf dem Server gelesen. Damit ein extern arbeitender Benutzer die E-Mails auf seinen lokalen Rechner übertragen bzw. von dort aus verwalten kann, haben sich die Protokolle POP und IMAP durchgesetzt. Zur Unterstützung dieser Protokolle muss auf dem Server ein POP- und/oder IMAP-Server eingerichtet werden. Bisweilen werden POP- und IMAP-Server zu den MDAs hinzugerechnet, was der ursprünglichen Bedeutung eines MDAs aber widerspricht und somit falsch ist.

  Beispiel: Dovecot

In diesem Zusammenhang werden Sie häufig auf eine weitere Abkürzung stoßen: E-Mail-Programme (Clients), wie der Benutzer sie sieht und verwendet, heißen in der Nomenklatur der E-Mail-Welt MUAs (*Mail User Agents*). Diese Programme holen E-Mails beim E-Mail-Server ab (Protokoll POP) bzw. helfen beim Lesen und bei der Verwaltung der externen E-Mails (IMAP). Zum Versenden kommuniziert der MUA direkt mit dem MTA (Protokoll SMTP). Populäre Vertreter dieser Gattung sind Thunderbird, Evolution, KMail, Microsoft Outlook, Apple Mail sowie das textbasierte Programm `mutt`. Anstelle eines lokalen Mail-Clients werden immer häufiger Webanwendungen eingesetzt, z. B. Google Mail.

Damit Sie den Überblick über die vielen Abkürzungen nicht verlieren, fasst Tabelle 37.1 die wichtigsten Abkürzungen aus dem E-Mail-Umfeld zusammen. Einige Abkürzungen sind im Text noch nicht vorgekommen, tauchen aber auf den nächsten Seiten auf.

Abkürzung	Bedeutung
IMAP	Internet Message Access Protocol
MDA	Mail Delivery Agent
MTA	Mail Transfer Agent
MUA	Mail User Agent
POP	Post Office Protocol
SASL	Simple Authentication and Security Layer
SMTP	Simple Mail Transfer Protocol

Tabelle 37.1 Wichtige E-Mail-Abkürzungen

E-Mail einst und jetzt

In der Anfangszeit des Internets war *jeder* Rechner direkt mit dem Internet verbunden und hatte – bei Bedarf – seinen eigenen E-Mail-Server. POP oder IMAP waren überflüssig, weil die Anwender die E-Mails direkt auf ihren Rechner = Server serviert bekamen. Die zu diesem Zeitpunkt üblichen textbasierten Mail-Clients (`elm`, `mail`, `pine`) konnten die lokalen Postfächer direkt auslesen – eine Fähigkeit, die den meisten modernen Mail-Clients mit grafischer Benutzeroberfläche abhanden gekommen ist. Herkömmliche Mail-Clients kommunizierten mit dem MTA auch nicht via SMTP, sondern übergaben die zu sendende E-Mail ganz einfach an das Kommando `sendmail`. Wenn Sie einen modernen textbasierten E-Mail-Client suchen, sollten Sie `mutt` ausprobieren (siehe Abschnitt 8.8).

Der Nachrichtenfluss im Detail

Anhand von Abbildung 37.1 können Sie nun verfolgen, wie eine E-Mail von Herrn Huber von Firma-Abc an `schmiedt@ziel.de` gesendet wird bzw. wie eine E-Mail von `irgendwer@absender.de` zurück zu `huber@firma-abc.de` kommt.

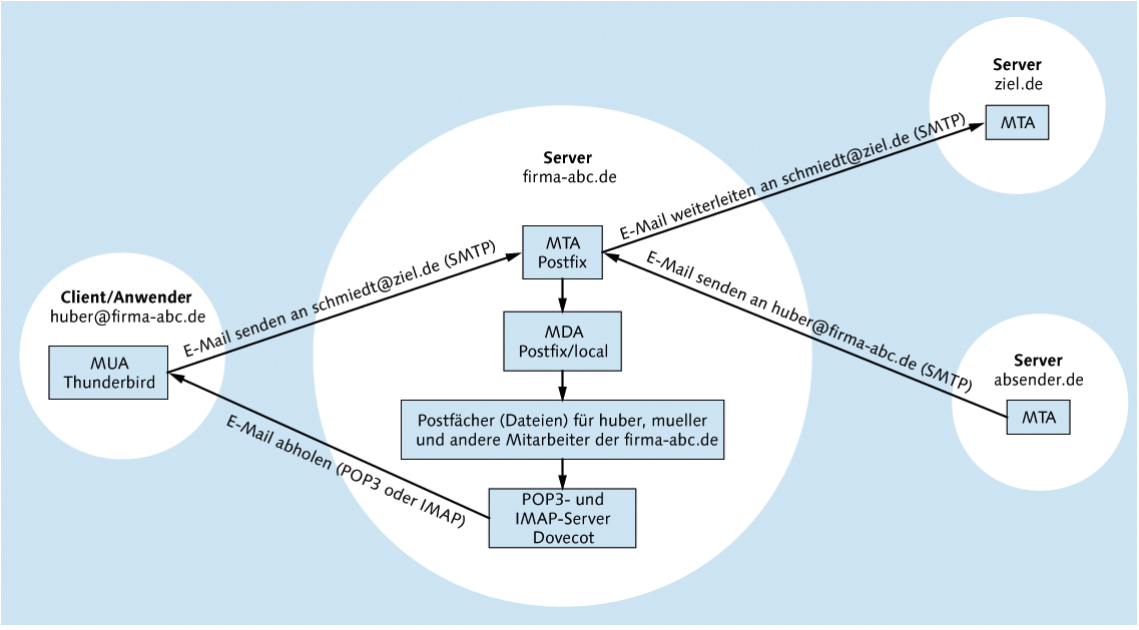


Abbildung 37.1 E-Mail-Kommunikationsfluss

Beginnen wir mit dem ersten Fall: Ein Mitarbeiter der Firma-Abc verfasst in seinem E-Mail-Client Thunderbird eine E-Mail an `schmiedt@ziel.de` und sendet diese ab. Thunderbird nimmt nun über das Protokoll SMTP Kontakt mit dem Mail-Server der Firma auf, also mit dem Programm Postfix, das auf dem Server `firma-abc.de` läuft. Postfix übernimmt die E-Mail, stellt fest, an welche Domain sie adressiert ist, und nimmt Kontakt mit dem Mail-Server von `ziel.de` auf. Der MTA von `ziel.de` vergewissert sich, dass der angegebene Benutzer `schmiedt` tatsächlich einen E-Mail-Account auf `ziel.de` hat, und nimmt die E-Mail entgegen.

Währenddessen hat `irgendwer@absender.de` eine E-Mail für Herrn Huber verfasst und diese versendet. Der MTA von `absender.de` tritt nun mit dem MTA von `firma-abc.de` in Verbindung und leitet die E-Mail weiter. Auf dem Server `firma-abc.de` stellt Postfix fest, dass es einen E-Mail-Account für `huber` gibt. Postfix akzeptiert die E-Mail und übergibt sie an das zu Postfix gehörende Kommando `local`, das die E-Mail im Postfach von Herrn Huber speichert. Das »Postfach« ist eine Datei oder ein Verzeichnis, das sich auf dem Server `firma-abc.de` befindet.

Dort bleibt die E-Mail liegen, bis der E-Mail-Client von Herrn Huber über das Protokoll POP oder IMAP mit dem Programm Dovecot auf dem Rechner `firma-abc.de` in Kontakt tritt. Die meisten E-Mail-Programme sind so eingestellt, dass sie das alle paar Minuten automatisch tun. Wenn Herr Huber gerade offline ist, kann es aber natürlich Stunden oder Tage dauern, bis es so weit ist. Nun muss die E-Mail nur noch in das E-Mail-Programm übertragen werden und kann dann dort gelesen werden.

Varianten und Optionen

Um Sie nicht zu sehr mit Details zu erschlagen, habe ich die obige Darstellung ein wenig verkürzt: Beispielsweise bin ich nicht auf den Umgang mit vorübergehend unzustellbaren E-Mails eingegangen. Ein E-Mail-Server unternimmt über mehrere Stunden Zustellversuche, bevor er den Versand aufgibt. Wenn die Zustellung definitiv scheitert, bekommt der Absender die E-Mail mit einer kurzen Beschreibung der Fehlerursache zurück.

Authentifizierung

Auch das Thema Authentifizierung ist außen vor geblieben: Nicht jeder darf einfach mit einem beliebigen MTA in Kontakt treten und E-Mails versenden. Um einen derart unkontrollierten E-Mail-Versand zu verhindern, dürfen E-Mails in der Basiskonfiguration nur lokal losgesandt werden. Damit auch ein externer E-Mail-Client E-Mails versenden darf, bedarf es einer Authentifizierung. Das in diesem Kapitel präsentierte Programm Postfix unterstützt zwar das Protokoll SASL (*Simple Authentication and Security Layer*), kann die Authentifizierung aber nicht selbst durchführen. In der Beispielkonfiguration dieses Kapitels übernimmt das Programm Dovecot diese Aufgabe.

Verschlüsselung

Damit der Inhalt der E-Mails nicht im Klartext übertragen wird, muss die Verbindung zwischen Client und Mail-Server verschlüsselt werden. Die meisten Mail-Server unterstützen dazu das Protokoll *Transport Layer Security* (TLS, ehemals SSL). Beim Verbindungsaufbau wird die Verschlüsselung zumeist mit STARTTLS eingeleitet: Die Kommunikation beginnt unverschlüsselt; Client und Server vereinbaren dann das bestmögliche Verschlüsselungsverfahren und setzen die Kommunikation verschlüsselt fort. Das funktioniert mit den meisten aktuellen Mail-Clients ausgezeichnet.

Relaying

Ein weiterer Punkt ist die Nachrichtenübertragung von einem MTA zum nächsten: Nicht immer ist der Weg so direkt wie in Abbildung 37.1. Bisweilen erfolgt der Versand über mehrere Stationen. Die dazwischenliegenden MTAs geben die Nachricht nur weiter (Relaying). Das ist vor allem dann zweckmäßig, wenn es für eine Mail-Domäne einen Haupt- und einen oder mehrere Backup-Server gibt. Wenn der Haupt-Server gerade nicht erreichbar ist, nehmen die Backup-Server die E-Mails entgegen und leiten sie später an den Haupt-Server weiter. Diese Art der Konfigu-

ration mindert das Risiko, dass das E-Mail-System während Wartungsarbeiten nicht erreichbar ist.

Sichern Sie Ihren Mail-Server ab, sonst landet er auf einer Blacklist!

Das Schlimmste, was bei der Konfiguration eines E-Mail-Servers passieren kann, ist die mangelnde oder fehlerhafte Absicherung des Relaying: Dann kann jeder ohne Authentifizierung Nachrichten zur Weiterleitung an Ihren E-Mail-Server übergeben.

Spam-Versender durchsuchen das Internet beständig nach solchen Servern und missbrauchen sie für die allgegenwärtige Werbeflut. Das zieht unangenehme Konsequenzen nach sich: Innerhalb weniger Tage landet Ihr Server in Blacklists, die gefährliche bzw. falsch konfigurierte E-Mail-Server auflisten. Viele E-Mail-Server akzeptieren zur Vermeidung von Spam keine E-Mails von derartigen Servern. Es ist wesentlich schwieriger, aus solchen Blacklists wieder gelöscht zu werden, als darin zu landen. Seien Sie bei der Konfiguration also vorsichtig! Wenn Sie den Verdacht haben, dass Ihr Server (genau genommen: dessen IP-Adresse) auf einer Blacklist gelandet ist, können Sie das sehr einfach auf der folgenden Seite verifizieren:

http://www.mxtoolbox.com/blacklists.aspx

Spam- und Virenschutz, Web-Oberfläche

Schließlich lässt sich das in Abbildung 37.1 dargestellte Szenario noch durch einen serverseitigen Spam- und Virenschutz erweitern. Wenn Sie möchten, dass Ihre Anwender E-Mails auch ohne Mail-Client direkt auf einer Webseite lesen können, brauchen Sie außerdem eine Web-Oberfläche, z. B. das Programm RoundCube oder Horde.

DNS-Konfiguration

Um nochmals auf Abbildung 37.1 zurückzukommen: Woher kennt der MTA auf dem Rechner `firma-abc.de` die IP-Adresse des Mail-Servers für `ziel.de`? Dank DNS natürlich, werden Sie antworten. Grundsätzlich ist das richtig, allerdings sind für den E-Mail-Verkehr nicht gewöhnliche DNS-Einträge (sogenannte A-Records) zuständig, sondern spezielle MX-Einträge. Ein MX-Eintrag gibt den Hostnamen und nicht die IP-Adresse des Rechners an, der für die E-Mail einer Domain zuständig ist. Das ermöglicht es, die E-Mail-Dienste auf einem anderen Rechner zu realisieren als die restlichen Internetdienste wie Web, SSH, FTP etc. Wenn Ihr Mail-Server auch IPv6 unterstützt, benötigen Sie einen AAAA-Eintrag mit der IPv6-Adresse des Mail-Hosts. Am MX-Eintrag ändert sich nichts.

Außerdem enthält jeder MX-Eintrag eine Prioritätsnummer. Wenn mehrere E-Mail-Server mit unterschiedlicher Priorität eingerichtet werden, erhält normalerweise der Server mit der höchsten Priorität alle E-Mails. Ist dieser Server vorübergehend

nicht erreichbar, kommen die niedriger priorisierten Server zum Zuge. Diese Server dienen normalerweise nur als Backup-System und leiten die E-Mails an den Haupt-Server weiter (Relaying), sobald dieser wieder online ist.

Tabelle 37.2 fasst eine typische DNS-Konfiguration für einen einfachen Server zusammen. Alle Internetdienste inklusive Mail laufen auf demselben Rechner, es gibt keinen Backup-E-Mail-Server. Da beim MX-Eintrag ein Domainname (keine IP-Adresse) angegeben werden muss, muss der dort angegebene Domainname – üblicherweise `mail.`*`domain`* – ebenfalls durch einen A-Eintrag definiert werden. Neben den in Tabelle 37.2 angegebenen Einträgen hat jede Domain diverse weitere DNS-Einträge, die unter anderem auf die zugrunde liegenden Nameserver verweisen.

Häufig werden bei der DNS-Konfiguration zusätzlich A- und AAAA-Einträge für `smtp.firma-abc.de` und `imap.firma-abc.de` eingerichtet, jeweils mit derselben IP-Adresse wie bei `mail.firma-abc.de`. Diese Hostnamen sind für den Mail-Server-Betrieb nicht erforderlich, erleichtern aber oft die Client-Konfiguration: Manche Mail-Clients gehen standardmäßig davon aus, dass es mit `smtp`, `imap` und eventuell auch `pop` oder `pop3` beginnende Hostnamen für die entsprechenden Protokolle gibt.

Typ	Name	Wert	Priorität
A	firma-abc.de	213.214.215.216	
A	www.firma-abc.de	213.214.215.216	
A	mail.firma-abc.de	213.214.215.216	
A	smtp.firma-abc.de	213.214.215.216	
A	imap.firma-abc.de	213.214.215.216	
AAAA	firma-abc.de	2001:1234:789a:0471::1234	
AAAA	www.firma-abc.de	2001:1234:789a:0471::1234	
AAAA	mail.firma-abc.de	2001:1234:789a:0471::1234	
AAAA	smtp.firma-abc.de	2001:1234:789a:0471::1234	
AAAA	imap.firma-abc.de	2001:1234:789a:0471::1234	
MX	–	mail.firma-abc.de	10

Tabelle 37.2 DNS-Konfiguration eines einfachen Web- und Mail-Servers mit IPv4 und IPv6

DNS-Konfiguration

Bleibt zuletzt noch die Frage, wie bzw. wo Sie die DNS-Konfiguration durchführen. In der Regel verwenden Sie dazu eine Web-Oberfläche, die Ihnen der Service-Provider zur Verfügung stellt, bei dem Sie Ihren Domainnamen registriert haben (siehe z. B. Abbildung 37.2).

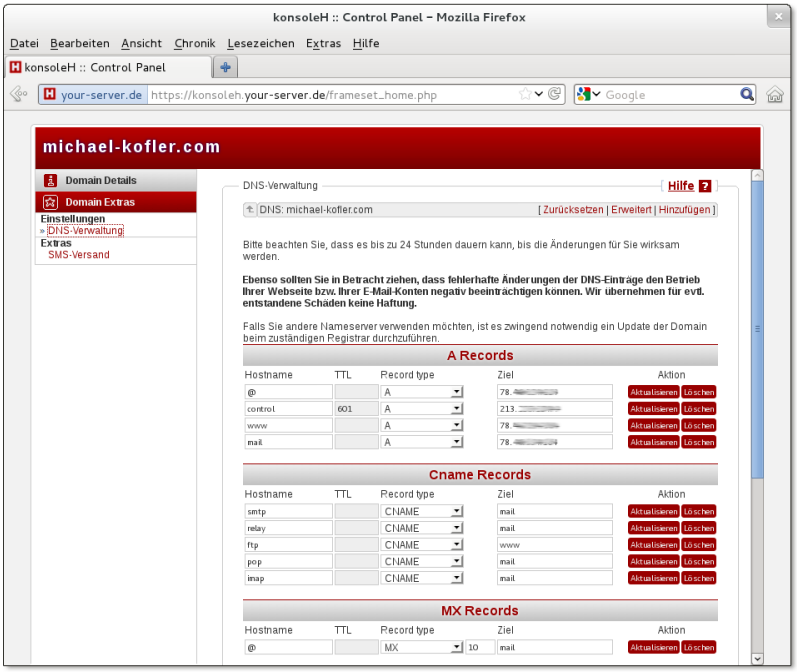


Abbildung 37.2 DNS-Konfiguration bei einem Domain-Name-Registrar

host-Kommando

Wenn Sie die DNS-Mail-Konfiguration überprüfen möchten, ist das Kommando `host` hilfreich, das je nach Distribution im Paket `bind9-host` versteckt ist. Die folgenden Zeilen zeigen, wie Sie zuerst den oder die Hostname(n) der Mail-Server ermitteln und dann deren IP-Adresse abfragen:

```
user$  host -t MX firma-abc.de
firma-abc.de mail is handled by 10 mail.firma-abc.de
user$  host mail.firma-abc.de
mail.firma-abc.de has address 213.214.215.216
```

Führen Sie `host` nicht direkt auf dem Root-Server, sondern auf einem externen Rechner aus! Andernfalls können ein eigener Nameserver sowie der Nameserver Ihres Providers das Ergebnis beeinflussen. Das erschwert die Suche nach eventuell vorhandenen eigenen Konfigurationsfehlern.

Reverse-DNS-Eintrag

Normalerweise liefern Domain Name Server (DNS) die IP-Adresse, die zu einem Hostnamen gehört. Wenn ein fremder Rechner mit `firma-abc.de` in Kontakt treten möchte – sei es mit einem Webbrowser, via SSH oder per E-Mail –, kontaktiert er zuerst den nächsten DNS. Dieser liefert die IP-Nummer der Servers von `firma-abc.de`.

Reverse DNS funktioniert gerade umgekehrt: Die IP-Nummer ist bekannt, dafür wird nun der Hostname gesucht. Damit das funktioniert, muss ein Reverse-DNS-Eintrag vorhanden sein. Wenn Sie einen Root-Server gemietet haben, muss Ihr Provider diesen Reverse-DNS-Eintrag durchführen. Viele Provider stellen ihren Kunden ein entsprechendes Konfigurationswerkzeug zur Verfügung. Der Reverse-DNS-Eintrag hat nichts mit den übrigen DNS-Einträgen zu tun! Die Einstellung erfolgt deswegen nicht auf der DNS-Konfigurationsseite Ihres Domainnamens, sondern im Rahmen der Root-Server-Konfiguration.

Auch Reverse DNS testen Sie am einfachsten mit dem Kommando `host`. Beachten Sie, dass zwar mehrere Hostnamen zur selben IP-Adressse führen können (etwa, wenn dank *Virtual Hosting* mehrere Websites auf einem Server laufen), dass die umgekehrte IP-Auflösung aber immer nur einen eindeutigen Hostnamen liefert:

```
user$  host firma-abc.de
firma-abc.de has address 213.214.215.216
firma-abc.de mail is handled by 10 mail.firma-abc.de.
user$  host 213.214.215.216
216.215.214.213.in-addr.arpa domain name pointer firma-abc.de.
```

An sich sind Reverse-DNS-Einträge für den Internet-Verkehr nicht zwingend erforderlich. Es gibt keinen Internet-Standard, der derartige Einträge vorschreibt. Bei E-Mail-Servern haben sich Reverse-DNS-Einträge dennoch durchgesetzt: Viele MTAs akzeptieren nämlich den Empfang von E-Mails von externen MTAs nur, wenn für den Hostnamen des Servers, auf dem der MTA läuft, ein Reverse-DNS-Eintrag existiert und dieser vermutlich nicht dynamisch generiert ist. Diese Schutzmaßnahme richtet sich gegen durch Schadsoftware infizierte (Windows-)PCs, die – oft ohne das Wissen des Eigentümers – zum Spam-Versand missbraucht werden.

Auch wenn der Reverse-DNS-Test keinen zuverlässigen Schutz gegen Spam bietet, wird er oft eingesetzt. Und das bedeutet: Damit andere MTAs Mails von Ihrem Server nicht als Spam klassifizieren, braucht der Server einen Reverse-DNS-Eintrag und gegebenenfalls für die IPv6-Adresse einen zweiten.

37.2 Postfix (MTA)

Dieser Abschnitt beschreibt die Installation und Konfiguration des MTAs Postfix unter Ubuntu. Postfix zählt momentan zu den populärsten MTAs und ist sehr gut dokumentiert – sowohl auf *http://postfix.org* als auch in unzähligen Artikeln und einigen Büchern.

Dennoch ist die Wahl von Postfix keineswegs selbstverständlich: Während es für manche Aufgaben nur ein weit verbreitetes Programm gibt (beispielsweise den Web-

server Apache), stellt die Open-Source-Welt gleich mehrere ausgezeichnete MTAs zur Auswahl. Ob Postfix oder Exim, Qmail oder Sendmail – alle genannten Programme sind weitverbreitet und erfüllen ihren Zweck. Wenn Sie mit Administratoren sprechen, wird vermutlich jeder den MTA empfehlen, den er selbst einsetzt und gut kennt. Einen relativ neutralen und gut fundierten Vergleich verschiedener MTAs finden Sie hier:

http://shearer.org/MTA_Comparison

Voraussetzungen

Bevor Sie mir auf den nächsten Seiten durch diverse Konfigurationsdetails folgen, sollten einige Voraussetzungen erfüllt sein:

- Sie brauchen einen von Ihrem Server unabhängigen E-Mail-Account – beispielsweise bei GMX, Google oder Yahoo –, um Ihr neues E-Mail-System zu testen.
- Die DNS-Konfiguration Ihrer Domain muss korrekt sein. Das betrifft insbesondere den in Abschnitt 37.1 beschriebenen MX-Eintrag.
- Der Hostname Ihres Rechners sollte korrekt eingestellt sein. Die Kommandos `hostname` und `cat /etc/hostname` sollten jeweils den richtigen Namen Ihres Servers liefern (also z. B. `firma-abc.de`).
- Für Ihren Root-Server sollte es einen Reverse-DNS-Eintrag geben (siehe Abschnitt 37.1).
- Zu guter Letzt ist die Installation eines kleinen textbasierten E-Mail-Clients empfehlenswert, um den MTA direkt zu testen (siehe Abschnitt 8.8).

Installation

Bei Debian und Ubuntu erscheint nach der Installation des `postfix`-Pakets ein Konfigurationsprogramm. Dort müssen Sie angeben, welche Art von Grundinstallation Sie wünschen. Auf einem Root-Server ist INTERNET SITE die richtige Wahl: Sie wollen Postfix einsetzen, um auf dem Server E-Mails per SMTP zu versenden und zu empfangen.

Im nächsten Punkt müssen Sie den Namen des E-Mail-Servers angeben (standardmäßig einfach den Hostnamen des Rechners, also beispielsweise `firma-abc.de`). Dieser Name wird dazu verwendet, um E-Mail-Adressen ohne Domainnamen zu vervollständigen. Aus einer E-Mail an `name` wird also eine an `name@firma-abc.de`.

Grundfunktionen

Nach dieser Minimalkonfiguration wird Postfix sofort gestartet. Das Programm erfüllt in der Grundkonfiguration die folgenden Funktionen:

- Postfix empfängt via SMTP E-Mails an `name@firma-abc.de`. Sofern es auf dem Server den Login `name` gibt, wird die E-Mail akzeptiert und gespeichert. Das gilt für alle Accounts, die in `/etc/passwd` definiert sind: Sofern Apache installiert ist,

ist beispielsweise auch `www-data@firma-abc.de` eine gültige E-Mail-Adresse. Wenn `name` nicht bekannt ist, wird die E-Mail zurückgewiesen (*user unknown*).

- Akzeptierte E-Mails werden vom Postfix-eigenen MDA im Mbox-Format in der Datei `/var/mail/name` gespeichert. Die Dateien in `/var/mail` sind also die »Postfächer« (Mailboxes) der verschiedenen E-Mail-Benutzer des Rechners. Das Mbox-Format bedeutet vereinfacht gesagt, dass die E-Mails in einer immer größer werdenden Datei aneinandergefügt werden. Da E-Mails in der Regel in einem Textformat codiert sind, können Sie die Mbox-Datei zur Not sogar mit `cat` oder `less` ansehen. Eine Alternative zum Mbox-Format ist das Maildir-Format, in dem es für jedes Postfach ein eigenes Verzeichnis und für jede E-Mail eine eigene Datei gibt.
- Lokale Benutzer können E-Mails versenden – sowohl intern an alle Accounts auf dem Server als auch extern an beliebige andere E-Mail-Adressen.

Test

Als ersten Test senden Sie von einem externen Account eine E-Mail an *name*`@firma-abc.de`, wobei *name* ein aktiver Linux-Account auf dem Root-Server ist. Die E-Mail sollte nach kurzer Zeit in `/var/mail/`*name* auftauchen. Wenn Sie sich als *name* anmelden, können Sie die E-Mail mit `mutt` lesen. Ebenfalls mit `mutt` testen Sie als Nächstes das Versenden einer E-Mail an Ihre externe E-Mail-Adresse. Sollten bei den beiden Tests Probleme auftreten, ist die wahrscheinlichste Fehlerursache eine falsche bzw. fehlende DNS-Konfiguration.

Konfiguration

Die grundlegenden Postfix-Konfigurationsdateien befinden sich in `/etc/postfix`. Innerhalb der Konfigurationsdateien können Sie bereits eingestellte Optionen wie Variablen verwenden – also `option1 = wert1` und dann `option2 = $option1`. Anweisungen in der Konfigurationsdatei dürfen über mehrere Zeilen reichen, wobei der Text ab der zweiten Zeile eingerückt sein muss.

Lookup Tables

In den Konfigurationsdateien wird oft auf Tabellen oder Listen verwiesen, die in der englischen Dokumentation *Lookup Tables* oder *Mappings* heißen. Dabei gilt die Syntax `option=type:name`. Der gebräuchlichste Dateityp ist `hash`. In diesem Fall wertet Postfix die Datei `name.db` aus, d. h., es fügt dem angegebenen Dateinamen die Endung `.db` hinzu. `*.db`-Dateien sind Tabellen in einem binären Format (*Berkeley Database*, kurz BDB). Zur Manipulation solcher Dateien verwenden Sie das Kommando `postmap`.

Tabellen im Textformat sind aus Effizienzgründen nicht vorgesehen. Eine Ausnahme ist lediglich die Textdatei `/etc/aliases`, deren Format kompatibel zu Sendmail ist. Aber auch in diesem Fall greift Postfix auf die dazugehörende BDB-Datei `aliases.db` zurück. Deswegen muss `aliases.db` nach jeder Änderung an `aliases` durch das

Kommando `newaliases` synchronisiert werden. Was Mail-Aliase sind und wie sie konfiguriert werden, ist in Abschnitt 37.2 beschrieben.

Externe Datenbanken

Postfix kann aber auch mit externen Datenbanken (MySQL, PostgreSQL, LDAP) kommunizieren, sofern die entsprechenden Postfix-Erweiterungspakete installiert sind. Die in der Konfigurationsdatei genannte Datei enthält nun nicht die eigentlichen Daten, sondern die Verbindungsinformationen und eine (SQL-)Abfrage. Der Einsatz externer Datenbanken bietet sich vor allem dann an, wenn Sie sehr viele, also Hunderte oder Tausende von E-Mail-Accounts verwalten müssen.

```
virtual_mailbox_domains=mysql:/etc/postfix/mysql-virt-domains.cf
```

main.cf

Die wichtigste Konfigurationsdatei für Postfix ist `/etc/postfix/main.cf`. Das folgende Listing gibt die wichtigsten Zeilen dieser Datei in der Grundeinstellung (Typ INTERNET SITE) wieder:

```
# Datei /etc/postfix/main.cf (auszugsweise)
# so meldet sich Postfix bei anderen MTAs
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)

# keine automatische Adressvervollständigung durch .firma-abc.de
append_dot_mydomain = no

# Hostname
myhostname = firma-abc.de

# Domain für lokale E-Mails ohne explizite Domain-Angabe
# /etc/mailname enthält in der Beispielkonfiguration firma-abc.de
myorigin = /etc/mailname

# Ort der Alias-Datei
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases

# Versand neuer E-Mails nur vom lokalen Rechner zulassen
mydestination = firma-abc.de, localhost
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128

# keine E-Mail-Weitergabe an andere Hosts (kein Relaying)
relayhost =

# E-Mail-Empfang über alle Netzwerkschnittstellen
inet_interfaces = all

# keine Beschränkung der E-Mail- und Postfach-Größe
mailbox_size_limit = 0
```

Neben den im obigen Listing enthaltenen Schlüsselwörtern gibt es unzählige weitere, die in `man 5 postconf` dokumentiert sind. Für alle nicht explizit eingestellten Optionen gelten Defaulteinstellungen. Wie diese aussehen, verrät das Kommando `postconf -d`. Im Folgenden stelle ich Ihnen einige besonders wichtige Einstellungen kurz vor:

- **`myhostname`** sollte den Hostnamen des Servers enthalten. `myhostname` gilt als Standardeinstellung für viele andere Optionen.
- **`myorigin`** gibt an, welcher Domain lokal versandte E-Mails zugeordnet werden sollen. Standardmäßig hat `myorigin` denselben Wert wie `myhostname`, und bei der hier vorgestellten Konfiguration sollten Sie es auch dabei belassen! Bei der mit Ubuntu bzw. Debian mitgelieferten Konfigurationsdatei wird `myorigin` aus der Datei `/etc/mailname` gelesen. Stellen Sie sicher, dass dort der richtige Name enthalten ist (für unser Beispiel also `firma-abc.de`), oder ändern Sie die Einstellung in der Datei `main.cf` in `myorigin=$myhostname`!
- **`mydestination`** listet Domänen auf, für die empfangene E-Mails lokal in ein Postfach zugestellt (also gespeichert) werden sollen. Nach der Basiskonfiguration hat diese Zeile bei mir auch `localhost.de` enthalten; diesen Eintrag habe ich wieder entfernt.

  Vorsicht: Auch wenn Postfix für mehrere Domänen zuständig ist, darf `mydestination` nur Einträge für die Hauptdomäne enthalten. Virtuelle Domänen geben Sie mit der Option `virtual_alias_domains` an (siehe Abschnitt 37.2).
- **`mynetworks`** gibt an, von welchen Adressen Postfix E-Mails ohne Authentifizierung via SMTP entgegennimmt. Die hier angegebenen Adressen bzw. Adressbereiche bezeichnen also die Rechner, denen Postfix »vertraut« (*Trusted SMTP Clients*).

  Bei der hier präsentierten Konfiguration (also für einen eigenständigen E-Mail-Server auf einem Root-Server) darf `mynetworks` nur `localhost` (oben in IP4- und IP6-Schreibweise) enthalten! Wenn Sie `mynetworks` falsch (zu liberal) konfigurieren, können fremde Benutzer Ihren Mail-Server dazu verwenden, ohne Authentifizierung E-Mails zu versenden. Vorsicht, Spam-Versender lieben solche Rechner!
- **`relayhost`** gibt an, an welchen MTA E-Mails weitergeleitet werden sollen, die *nicht* für die lokale Zustellung gedacht sind. Bei der hier vorgestellten Konfiguration muss `relayhost` leer bleiben. Wenn Postfix dagegen auf einem Rechner im LAN läuft und zu versendende E-Mails an einen externen MTA im Internet weitergeben soll, ist `relayhost` der entscheidende Parameter.

Eine Beschreibung diverser weiterer Optionen folgt im weiteren Verlauf dieses Kapitels.

Änderungen an der Konfiguration

Postfix besteht aus einer Menge Einzelprogramme, von denen viele bei Bedarf jedes Mal neu gestartet und wenig später gleich wieder beendet werden. Diese Programme lesen die für sie relevanten Konfigurationsdateien jedes Mal neu ein.

Allerdings gibt es auch Postfix-Komponenten, die Konfigurationsänderungen nicht selbstständig bemerken. Postfix-Einsteiger, denen oft unklar ist, welche Änderungen Postfix selbstständig bemerkt, sollten nach Konfigurationsänderungen grundsätzlich `service postfix reload` ausführen. Das gilt insbesondere für Änderungen an `master.cf` und `main.cf`. Postfix-Profis werden `reload` dagegen wegen des damit verbundenen Geschwindigkeitsverlusts möglichst vermeiden, besonders bei großen aktiven Systemen.

Anstatt `main.cf` mit einem Editor zu ändern und anschließend ein `reload`-Kommando auszuführen, können Sie die Änderung auch mit `postconf -e option=wert` durchführen. Das Kommando `postconf` benachrichtigt dann auch gleich Postfix über die Änderung.

IPv6

Postfix unterstützt zwar IPv6, standardmäßig ist aber nur IPv4 aktiv. Wenn Sie IPv6 nutzen möchten, sind in der Regel zwei Änderungen in `main.cf` erforderlich:

```
# in /etc/postfix/main.cf
...
inet_protocols = all
smtp_address_preference = any
```

Diese Änderungen werden erst nach einem Neustart von Postfix wirksam. Weitere Informationen zu den IPv6-Funktionen von Postfix können Sie hier nachlesen:

http://www.postfix.org/IPV6_README.html

Verschlüsselung (TLS/STARTTLS)

Postfix unterstützt das Protokoll *Transport Layer Security* (TLS) und das Verfahren STARTTLS zum Aufbau einer verschlüsselten Verbindung. Je nachdem, wie Postfix vorkonfiguriert ist, ist STARTTLS allerdings nicht aktiv. Abhilfe schafft die folgende Einstellung in `main.cf` sowie ein Neustart von Postfix:

```
# Datei /etc/postfix/main.cf, TLS und STARTTLS aktivieren
...
smtpd_tls_security_level = may
```

Diese Einstellung bewirkt, dass Postfix STARTTLS anbietet und die Kommunikation nach Möglichkeit TLS-verschlüsselt durchführt. Bei einer falschen Konfiguration des Mail-Clients bzw. für alte Mail-Clients ist allerdings weiterhin eine Authentifizierung im Klartext möglich.

Unter Debian und Ubuntu wird bei der Postfix-Installation standardmäßig ein sogenanntes SnakeOil-Zertifikat samt Schlüssel eingerichtet. Die Parameter `smtpd_tls_cert_file` und `-key_file` in `main.cf` geben die Orte der Zertifikat- und Schlüsseldateien an:

```
# Datei /etc/postfix/main.cf
...
smtpd_tls_cert_file = /etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file  = /etc/ssl/private/ssl-cert-snakeoil.key
```

Wenn Sie bereits von Ihrer Webserver-Konfiguration über zertifizierte Schlüssel verfügen, verändern Sie die Pfadangaben entsprechend. Gegebenenfalls können Sie mit `smtpd_tls_CAfile` zusätzlich einen Schlüssel der Certification Authority angeben. Alternativ können Sie mit den folgenden Kommandos selbst ein eigenes, für 10 Jahre gültiges Zertifikat erzeugen. Entscheidend ist, dass Sie bei der Ausführung von `openssl` als Common Name den Hostnamen Ihres Servers angeben, also z. B. `firma-abc.de` (siehe Abschnitt 35.4).

```
root#  openssl req -new -x509 -days 3650 -nodes \
         -out /etc/ssl/certs/postfix.pem \
         -keyout /etc/ssl/private/postfix.pem
...
Common Name (eg server FQDN or YOUR name) []:  firma-abc.de
root#  chmod 600 /etc/ssl/private/postfix.pem
```

Anschließend verändern Sie `main.cf` wie folgt:

```
# Datei /etc/postfix/main.cf, selbst erzeugtes Zertifikat verwenden
...
smtpd_tls_cert_file = /etc/ssl/certs/postfix.pem
smtpd_tls_key_file  = /etc/ssl/private/postfix.pem
```

Änderungen an der TLS-Konfiguration werden erst mit einem Neustart von Postfix wirksam. Weitere Informationen zur TLS-Unterstützung von Postfix finden Sie hier:

http://www.postfix.org/TLS_README.html

Client-Konfiguration

Beim Einrichten eines neuen Mail-Kontos in Ihrem Mail-Client wählen Sie die SMTP-Verschlüsselungsmethode STARTTSL aus (siehe auch Abbildung 37.3). Beim ersten Verbindungsaufbau durch einen Mail-Client müssen Sie das Zertifikat akzeptieren.

mbox- oder Maildir-Format

Standardmäßig speichert Postfix eintreffende E-Mails im mbox-Format in der Datei `/var/mail/name`. Wenn E-Mails stattdessen in einer lokalen Datei im Benutzerverzeichnis gespeichert werden sollen (weiterhin im mbox-Format), geben Sie den gewünschten Dateinamen relativ zum Homeverzeichnis mit `home_mailbox` an:

```
# in /etc/postfix/main.cf
...
# E-Mails im mbox-Format in der Datei /home/name/Mailbox speichern
home_mailbox = Mailbox
```

Wenn Sie vorhaben, die Mails überwiegend via IMAP abzurufen, sollten Sie das Maildir-Format vorziehen. Die korrekte Einstellung von `home_mailbox` sieht nun so aus:

```
# in /etc/postfix/main.cf
...
# E-Mails im maildir-Format im Verzeichnis /home/name/Maildir speichern
home_mailbox = Maildir/
```

Der Verzeichnisname muss mit `/` enden, damit Postfix das Maildir-Format verwendet! Falls `main.cf` eine `mailbox_command`-Anweisung enthält, müssen Sie diese auskommentieren. Neu eintreffende E-Mails werden nun in eigenen Dateien im Verzeichnis `/homename/Maildir` gespeichert.

Vergessen Sie nicht, auch Ihrem lokalen Mail-Client bzw. Dovecot den Ort und das Format Ihres Postfachs mitzuteilen (siehe Abschnitt 37.3)! Wenn Sie `mutt` einsetzen, müssen Sie das Programm entsprechend konfigurieren, damit es die E-Mails aus dem `Maildir`-Verzeichnis liest (siehe Abschnitt 8.8).

Mail-Aliase

Ein Mail-Alias ist ein zusätzlicher Mail-Name zum Empfang von E-Mail. Die E-Mail wird aber tatsächlich an einen bereits vorhandenen Account weitergeleitet. Aliase werden in der Datei `/etc/aliases` definiert. Diese Datei sieht üblicherweise so ähnlich wie das folgende Muster aus:

```
# Datei /etc/aliases
postmaster:      root
webmaster:       huber
Bernhard.Huber:  huber
...
```

Die erste Spalte gibt den Alias-Namen ohne Domäne an. Der Name gilt für die in `myhostname` definierte Domäne, also beispielsweise `postmaster@firma-abc.de`. Die zweite Spalte enthält den lokalen Empfänger. Im obigen Beispiel werden an `postmaster`

adressierte E-Mails an root weitergeleitet, E-Mails an webmaster und an Bernhard.Huber an huber. Es ist zulässig, in /etc/aliases für jeden Alias mehrere, durch Kommas getrennte Empfänger anzugeben.

Als Empfänger können Sie statt eines lokalen E-Mail-Account-Namens auch eine externe E-Mail-Adresse angeben, oder eine Datei, an die die E-Mail angefügt wird, oder ein Programm in der Schreibweise |kommando, an das die E-Mail weitergegeben wird. Das Weiterleiten an externe E-Mail-Adressen funktioniert zwar problemlos, scheitert in der Praxis aber oft am Spam-Schutz des Ziel-MTAs. Wenn Sie also beispielsweise E-Mails an webmaster an name@gmx.de weiterleiten, erkennt der Spam-Filter von GMX, dass die E-Mail nicht direkt an gmx.de übertragen wurde, sondern indirekt über firma-abc.de. Das reicht für einen misstrauischen Spam-Filter, um die E-Mail als Spam zu klassifizieren.

Damit geänderte Aliase wirksam werden, müssen Sie das Kommando newaliases ausführen. Dieses Kommando synchronisiert die Textdatei /etc/aliases mit der BDB-Datei /etc/aliases.db.

alias_database und alias_maps

In /etc/postfix/main.cf stoßen Sie in der Regel auf zwei alias-Optionen, was bisweilen Verwirrung stiftet:

```
# in /etc/postfix/main.cf
...
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```

alias_database gibt an, welche Datenbankdatei durch das Kommando newaliases aktualisiert werden soll. Die hier angegebene Datei (deren Name durch .db ergänzt wird) enthält die in /etc/aliases angegebenen Aliase in einem binären Format.

alias_maps gibt an, welche Alias-Datenbanken Postfix berücksichtigen soll. Normalerweise geben Sie hier dieselbe Datei an wie bei alias_database. Es ist aber zulässig, darüber hinaus weitere Quellen für Alias-Definitionen anzugeben. Der entscheidende Unterschied zwischen den beiden Parametern besteht darin, dass alias_database für newaliases gilt, alias_maps dagegen für Postfix!

.forward

Auch als lokaler Benutzer, der keinen Zugriff auf /etc/aliases hat, können Sie Ihre E-Mail an eine andere Adresse umleiten: Dazu erzeugen Sie die Datei .forward und speichern darin die neue Zieladresse. Fertig!

Wie ich oben bereits erwähnt habe, funktioniert diese simple Form der E-Mail-Umleitung zumeist nur bei lokalen Adressen wunschgemäß. Bei externen Zieladressen kann es dagegen passieren, dass sich die umgeleiteten E-Mails im Spam-Schutz des Ziel-MTAs verfangen.

Explizite Empfängerliste

Standardmäßig kann jeder Linux-Account E-Mails empfangen. Es ist aber selten wünschenswert, dass System-Accounts wie `daemon`, `sys` oder `man` E-Mails erhalten. Um diesen Missstand zu beheben, müssen Sie am Parameter `local_recipient_maps` drehen. Die Standardeinstellung lautet:

```
local_recipient_maps = proxy:unix:passwd.byname $alias_maps
```

Das bedeutet, dass alle in der Unix-Datei `/etc/passwd` aufgezählten Benutzer sowie alle in den Alias-Datenbanken genannten Benutzer E-Mails empfangen können. Wenn Sie möchten, dass nur `fischer`, `huber`, `schmidt` sowie `root` (für System-Benachrichtigungen) E-Mails empfangen sollen, gehen Sie wie folgt vor: Zuerst erzeugen Sie eine Textdatei, die zeilenweise die Account-Namen enthält. Die Datei muss in einer zweiten Spalte einen beliebigen Wert enthalten, weil Postfix und das Kommando `postmap` generell Schlüssel/Wert-Paare (*Key/Value Pairs*) erwarten – auch bei Listen, bei denen eigentlich nur die Existenz eines Schlüssels relevant ist, der dazugehörige Wert aber gar nicht berücksichtigt wird.

```
# Datei /etc/postfix/local-recips
fischer    x
huber      x
schmidt    x
root       x
```

Aus dieser Datei erstellen Sie nun mit `postmap` eine für Postfix lesbare Datenbankdatei `local-recips.db`:

```
root#  cd /etc/postfix
root#  postmap local-recips
```

Mit `postmap -s` können Sie überprüfen, dass die Datei korrekt erstellt wurde:

```
root#  postmap -s hash:local-recips
huber   x
root    x
schmidt x
fischer x
```

Anschließend fügen Sie in `/etc/postfix/main.cf` eine Zeile zur Einstellung von `local_recipient_maps` ein:

```
# in /etc/postfix/main.cf
local_recipient_maps = hash:/etc/postfix/local-recips $alias_maps
```

Mapping-Dateien ganz sicher aktualisieren

Nach jeder Änderung an `local-recips` müssen Sie `postmap` ausführen, um die für Postfix relevante Datenbankdatei `local-recips.db` zu aktualisieren. Diese Akualisierung ist allerdings ein kritischer Vorgang: `postmap` löscht dabei `local-recips.db` und schreibt die Datei anschließend neu. Wenn Postfix gerade während dieses Zeitpunkts auf `local-recips.db` zugreift, erhält es falsche bzw. unvollständige Daten.

Eine sichere Vorgehensweise sieht deswegen so aus: Sie geben der zugrunde liegenden Textdatei einen anderen Namen (z. B. `local-recips1`), wenden `postmap` auf diese Datei an und führen dann `mv local-recips1.db local-recips.db` aus. Somit enthält `local-recips.db` zu jedem Zeitpunkt konsistente Daten – entweder in der alten oder in der neuen Version. Diesen Vorgang können Sie durch eine Script- oder `make`-Datei automatisieren, wie es hier beschrieben ist:

http://www.postfix.org/DATABASE_README.html#safe_db

Dieser Hinweis gilt für *alle* in diesem Kapitel vorkommenden Mapping-Dateien.

Linux-Accounts einrichten

Von nun an akzeptiert Postfix nur noch E-Mails an die in `local-recips` genannten Empfänger. Es gibt allerdings noch eine Einschränkung: Es werden nur dann E-Mails zugestellt (also lokal gespeichert), wenn der Benutzer einen Account auf dem Rechner hat. Ist das nicht der Fall, müssen Sie mit `adduser` einen neuen Account erstellen.

Im folgenden Beispiel bewirkt die Option `--shell /bin/false`, dass dem Account statt einer Shell das Programm `/bin/false` zugeordnet ist. Das macht ein interaktives Arbeiten unmöglich. `--gecos ,,,` unterdrückt die Fragen nach dem vollständigen Namen und weiteren überflüssigen Kontaktinformationen. Wichtig ist hingegen das Passwort, und das, obwohl sich der Benutzer gar nicht einloggen kann. Der Grund: Das Passwort gilt für die in Abschnitt 37.3 beschriebene POP- und SMTP-Authentifizierung.

```
root#  adduser  --shell /bin/false --gecos ,,, huber
Geben Sie ein neues UNIX-Passwort ein:         ********
Geben Sie das neue UNIX-Passwort erneut ein:   ********
```

Tipp

Sichere Passwörter können Sie komfortabel mit `makepasswd` (Debian, Ubuntu) oder `mkpasswd` (Fedora, RHEL, Paket `expect`) erzeugen.

Wenn Sie mit virtuellen Domänen arbeiten (siehe den übernächsten Abschnitt), können Sie darauf verzichten, für jeden Benutzer einen eigenen Linux-Account einzurichten. Postfix unterstützt dann sogenannte virtuelle Postfächer, die ganz real sind, aber keinem gültigen Benutzernamen entsprechen.

Vom Linux-Account abweichende E-Mail-Adressen

In vielen Firmen sind E-Mail-Adressen der Form `Vorname.Nachname@firma.de` üblich. Linux sieht jedoch derart lange Benutzernamen – noch dazu mit einem Punkt – nicht vor. Das hindert Sie aber nicht daran, dennoch lange E-Mail-Namen zu verwenden:

- Legen Sie einen Linux-Account mit einem Linux-typischen, kurzen Benutzernamen an, z. B. `huber`.
- Definieren Sie eine Alias-Regel, die E-Mails an `Bernhard.Huber` an `huber` weiterleitet.
- Verwenden Sie bei der Konfiguration des E-Mail-Clients als Absenderadresse die Langform, also `Bernhard.Huber@firma-abc.de`. Beachten Sie aber, dass Sie zur POP- und SMTP-Authentifizierung den Linux-Account-Namen angeben müssen!
- Damit auch lokal (z. B. durch `mutt`) versandte E-Mails die richtige Absenderadresse in der Langform enthalten, richten Sie eine neue Tabelle in der Textdatei `/etc/postfix/canonical` ein. Diese Tabelle gibt an, wie Postfix E-Mail-Adressen verändern soll:

  ```
  # /etc/postfix/canonical
  huber     Bernhard.Huber@firma-abc.de
  ...
  ```

  Diese Tabelle wandeln Sie mit `postmap` in eine für Postfix lesbare Tabelle um.
- Anschließend stellen Sie in `main.cf` den Parameter `canonical_maps` ein und führen dann `service postfix reload` aus.

  ```
  # in /etc/postfix/main.cf
  ...
  canonical_maps = hash:/etc/postfix/canonical
  ```

Neben den Canonical- und Alias-Tabellen bietet Postfix diverse weitere Möglichkeiten, um E-Mail-Adressen in verschiedenen Phasen des E-Mail-Verkehrs zu manipulieren, also beim Empfang, vor dem Versenden etc. Einen guten Überblick gibt die folgende Seite:

http://www.postfix.org/ADDRESS_REWRITING_README.html

Virtuelle Domänen mit gemeinsamen E-Mail-Benutzern

Im einfachsten Fall ist Postfix nur für E-Mails an den Hostnamen des Rechners zuständig, z. B. `xxx@firma-abc.de`. Oft ist es aber wünschenswert, dass *ein* MTA für mehrere E-Mail-Domänen zuständig ist, also `xxx@noch-eine-firma.de`. Alle Domänen, die nicht mit dem Hostnamen des Rechners übereinstimmen, werden in der Postfix-Nomenklatur »virtuell« genannt (auf Englisch oft auch *Hosted Domains*).

Postfix sieht mehrere Möglichkeiten zur Realisierung virtueller Domänen vor. Der einfachste Weg besteht darin, beim Parameter `mydestination` einfach mehrere Domänen einzustellen, etwa so:

```
# in /etc/postfix/main.cf
...
mydestination = firma-abc.de, localhost, noch-eine-firma.de
```

Selbstverständlich müssen Sie auch die DNS-Konfiguration von `noch-eine-firma.de` entsprechend anpassen. Dem MX-Hostnamen muss also die IP-Adresse Ihres Servers zugeordnet sein (siehe auch Abschnitt 37.1).

Sie erreichen damit, dass Mails an `noch-eine-firma.de` genauso behandelt werden wie Mails an `firma-abc.de`. Es spielt also keine Rolle, ob eine E-Mail an `huber@firma-abc.de` oder an `huber@noch-eine-firma.de` adressiert wird: Postfix stellt die E-Mail auf jeden Fall dem lokalen Benutzer `huber` zu. Für manche Fälle ist das ausreichend – insbesondere dann, wenn eine Firma oder Organisation mehrere Webauftritte hat, aber in Wirklichkeit immer dieselben Personen dafür verantwortlich sind.

Virtuelle Domänen mit getrennten E-Mail-Benutzern

Wenn Sie zwischen gleichnamigen Benutzern je nach Domäne differenzieren möchten, geben Sie die betroffenen Domänen nicht in `mydestination` an, sondern mit dem Schlüsselwort `virtual_alias_domains`.

Außerdem brauchen Sie nun eine Tabelle, die die Zuordnung zwischen den E-Mail-Adressen der virtuellen Domänen und realen Linux-Accounts herstellt. Weiterhin ist also für jede E-Mail-Adresse ein Linux-Account erforderlich. Um beim Beispiel der `huber`-Adressen zu bleiben: Der Account für `huber@firma-abc.de` ist weiterhin `huber`. Für `huber@noch-eine-firma.de` müssen Sie einen neuen Account anlegen, z. B. `huberNEF`. Der Aufbau der Tabelle für die virtuellen E-Mail-Benutzer sieht so aus:

```
# Textdatei /etc/postfix/virtual
huber@noch-eine-firma.de      huberNEF
mueller@noch-eine-firma.de    muellerNEF
...
```

Die Tabelle kann wie die Alias-Tabelle mehreren E-Mail-Adressen denselben Benutzer zuordnen, also etwa:

```
# in /etc/postfix/virtual
...
webmaster@noch-eine-firma.de  huberNEF
```

Mit `postmap` machen Sie aus dieser Datei eine für Postfix lesbare Datenbankdatei:

```
root#  postmap /etc/postfix/virtual
```

Jetzt müssen Sie noch `main.cf` anpassen. `virtual_alias_domains` zählt alle virtuellen Domänen auf (aber nicht die Hauptdomäne, die geben Sie weiterhin mit `mydestination` an!). `virtual_alias_maps` gibt den Dateinamen der virtuellen Alias-Tabelle an.

```
# in /etc/postfix/main.cf
...
mydestination         = firma-abc.de, localhost
virtual_alias_domains = noch-eine-firma.de, firma-xyz.de, ...
virtual_alias_maps    = hash:/etc/postfix/virtual
```

Virtuelle Domänen mit virtuellen Postfächern

Bis jetzt war es immer erforderlich, dass jeder E-Mail-Adresse ein Linux-Account gegenüberstand. Postfix weigert sich, E-Mails in einem Postfach zu speichern, wenn es nicht einen gleichnamigen Linux-Account gibt. Bei sehr vielen E-Mail-Adressen wird es aber zunehmend unpraktisch, jedes Mal auch einen neuen Account anzulegen. Postfix sieht zur Lösung dieses Problems virtuelle Postfächer vor. Das sind ganz gewöhnliche Postfachdateien; die Bezeichnung »virtuell« bezieht sich nur darauf, dass es keine dazugehörenden Linux-Accounts gibt.

Freilich müssen auch die virtuellen Postfächer jemandem gehören. Dazu erzeugen Sie eine neue Gruppe und einen neuen Benutzer mit jeweils noch unbenutzten GIDs und UIDs, im folgenden Beispiel jeweils 5000:

```
root#  groupadd -g 5000 vmail
root#  useradd -g vmail -u 5000 vmail -d /home/vmail -m
```

Nun ändern Sie `main.cf` wie im folgenden Beispiel-Listing. `virtual_mailbox_domains` gibt die virtuellen Domänen an, deren E-Mails in virtuellen Postfächern gespeichert werden sollen. `virtual_mailbox_base` gibt das Verzeichnis an, in dem die virtuellen Postfächer angelegt werden sollen. Die Tabelle `virtual_mailbox_maps` stellt die Zuordnung zwischen den E-Mail-Adressen und den Postfächern her. `virtual_uid_maps` und `_gid_maps` gibt die UID und GID der Postfachdateien an. Theoretisch ist es hier möglich, eigene UIDs und GIDs für jedes Postfach anzugeben, aber das ist selten zweckmäßig.

```
# in /etc/postfix/main.cf
...
mydestination           = firma-abc.de, localhost
virtual_mailbox_domains = noch-eine-firma.de, firma-xyz.de, ...
virtual_mailbox_base    = /var/mail
```

```
virtual_mailbox_maps    = hash:/etc/postfix/virtual-mboxes
virtual_uid_maps        = static:5000
virtual_gid_maps        = static:5000
```

Die Datei `virtual-mboxes` gibt für jede E-Mail-Adresse die dazugehörende Postfachdatei relativ zum Pfad `virtual_mailbox_base` an. Dieses Beispiel verwendet für jede Domain ein eigenes Verzeichnis und innerhalb dieses Verzeichnisses dann einfach den Benutzernamen. Grundsätzlich können Sie hier aber nach Belieben verfahren. Für die eigentliche Zustellung ist das Postfix-Kommando `virtual` zuständig. Es speichert die E-Mails standardmäßig im mbox-Format. Wenn Sie das Maildir-Format vorziehen, geben Sie in `virtual-mboxes` einfach im Anschluss an den Dateinamen einen Schrägstrich an, also beispielsweise `noch-eine-firma.de/huber/`.

```
# Datei /etc/postfix/virtual-mboxes
huber@noch-eine-firma.de      noch-eine-firma.de/huber
mueller@noch-eine-firma.de    noch-eine-firma.de/mueller
webmaster@firma-xyz.de        firma-xyz.de/webmaster
...
```

`postmap` macht aus `virtual-mboxes` eine Datenbankdatei:

```
root#  postmap /etc/postfix/virtual-mboxes
```

Ein letzter Schritt besteht nun darin, dass Sie für jede Domain das Postfachverzeichnis erzeugen müssen. Entscheidend sind dabei die Zugriffsrechte.

```
root#  mkdir /var/mail/noch-eine-firma.de
root#  chown mail:mail /var/mail/noch-eine-firma.de
root#  chmod g+w /var/mail/noch-eine-firma.de
```

`postfix reload` aktiviert die Konfiguration. Nun senden Sie eine Testnachricht an `huber@noch-eine-firma.de` und werfen danach einen Blick in das Verzeichnis `/var/mail/noch-eine-firma.de/`. Dort sollte nun die Datei `huber` mit der neuen E-Mail auftauchen.

Wenn Sie *alle* Domänen virtuell verwalten möchten, also auch die Domäne des Hostnamens Ihres Rechners, entfernen Sie den Hostnamen aus der `mydestination`-Zeile und fügen ihn der `virtual_mailbox_domains`-Zeile hinzu:

```
# in /etc/postfix/main.cf
...
mydestination           = localhost
virtual_mailbox_domains = firma-abc.de, noch-eine-firma.de, ...
```

Virtuelle Postfächer mit MySQL-Tabellen verwalten

Virtuelle Postfächer ersparen Ihnen es zwar, für jede E-Mail-Adresse einen Account einzurichten, machen dafür aber die Konfiguration von Dovecot zur Abholung der E-Mails (POP) sowie zur SMTP-Authentifizierung komplizierter (siehe Abschnitt 37.3): Sie müssen nun eine weitere Tabelle administrieren, die für jeden Benutzer einen Login-Namen und ein Passwort enthält.

Virtuelle Postfächer reduzieren den Verwaltungsaufwand nur dann, wenn Sie gleichzeitig sämtliche Daten der E-Mail-Accounts in einer Datenbank oder in einem LDAP-System speichern und Postfix und Dovecot gleichermaßen auf diese Datenbank zugreifen können. Eine ausführliche Anleitung, wie Sie dies mit MySQL bewerkstelligen, gibt die folgende Seite, die auch sonst eine Menge ausgezeichneter Informationen enthält:

https://workaround.org/ispmail/squeeze

Postfix als lokaler E-Mail-Server

Einige Programme versenden Statusberichte oder Fehlermeldungen per E-Mail an `root`. Dazu zählen z. B. Logwatch, das RAID-System und SMART. Wenn auf dem Rechner – wie auf den vorangegangenen Seiten beschrieben – ein vollwertiger E-Mail-Server läuft, kümmert sich dieser um den Versand derartiger Benachrichtigungs-Mails. Sie sollten allerdings in `/etc/aliases` eine Zeile einfügen, die die an `root` gerichteten E-Mails an Ihren lokalen E-Mail-Account umleitet:

```
# in /etc/aliases
root:        username
```

Vergessen Sie nicht, dass Sie nach Änderungen an der `aliases`-Datei das Kommando `newaliases` ausführen müssen!

Postfix nur für den lokalen Bedarf

Der Empfang von lokalen E-Mails ist freilich auch dann wünschenswert, wenn auf dem Rechner *kein* vollwertiger E-Mail-Server installiert ist. Für solche Fälle sieht Postfix die Konfigurationsvariante NUR LOKAL vor, die Sie unmittelbar nach der Installation auswählen. Wenn Sie die Postfix-Grundkonfiguration zu einem späteren Zeitpunkt nochmals wiederholen möchten, führen Sie unter Debian/Ubuntu `dpkg-reconfigure postfix` aus.

Die Konfigurationsvariante NUR LOKAL bewirkt, dass nur innerhalb des Servers E-Mails verarbeitet werden. Programme können also E-Mails an `root` oder an andere Benutzer versenden. Diese werden in den Postfächern `/var/spool/mail/`*`benutzername`* gespeichert und können z. B. mit Mutt gelesen werden (siehe Abschnitt 8.8).

Postfix akzeptiert in dieser Konfiguration weder E-Mails von anderen Rechnern noch versendet es E-Mails an andere Rechner. Die resultierende Datei `/etc/postfix/main.cf` sieht wie folgt aus. Entscheidend ist die Zeile `inet_interfaces = loopback-only`, die den E-Mail-Empfang über reale Netzwerkschnittstellen von vornherein ausschließt.

```
# /etc/postfix/main.cf für eine lokale Konfiguration
...
myhostname          = michaels-computer
alias_maps          = hash:/etc/aliases
alias_database      = hash:/etc/aliases
mydestination       = michaels-computer, localhost.localdomain, localhost
relayhost           =
mynetworks          = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit  = 0
recipient_delimiter = +
inet_interfaces     = loopback-only
default_transport   = error
relay_transport     = error
```

E-Mails per SMTP weiterleiten

Die Installation eines lokalen Postfix-Servers ist also trivial, ein Problem bleibt aber ungelöst: Wie kommen die lokalen E-Mails aus `/var/spool/mail/`*username* zum Administrator? Dieser muss sich ja in der Regel um mehrere Rechner kümmern und wird sich nicht ständig auf allen Rechnern einloggen, nur um nachzusehen, ob auf dem Rechner interessante lokale E-Mails zu finden sind.

An dieser Stelle wird es kompliziert: Der erste Schritt besteht darin, in `/etc/aliases` statt eines lokalen Benutzers die gewünschte Empfängeradresse für `root`-E-Mails anzugeben. Nach der Änderung führen Sie das Kommando `newaliases` aus.

```
# in /etc/aliases
root:        mein.name@anderer-host.de
```

Als Nächstes müssen Sie `main.cf` ändern, damit Postfix E-Mails auch weiterleitet. `relayhost` gibt an, an welchen Server nicht-lokale E-Mails weitergeleitet werden. Achten Sie darauf, den Hostnamen in eckige Klammern zu setzen!

Die `smtp`-Optionen geben an, dass sich Postfix beim externen Server authentifizieren soll. Die Passwortinformationen befinden sich in der Datei `sasl-passwd`, wobei die dazugehörende Datenbank wie üblich nach jeder Änderung durch `postmap` aktualisiert werden muss.

Zu guter Letzt müssen die beiden Einstellungen für `default_transport` und `relay_transport` auskommentiert werden. Dabei handelt es sich um eine Vorsichtsmaßnahme der lokalen Konfigurationsvariante, die verhindert, dass Postfix zum Relaying verwendet werden kann.

```
# Änderungen in /etc/postfix/main.cf
...
relayhost                  = [anderer-host.de]
smtp_sasl_auth_enable      = yes
smtp_sasl_password_maps    = hash:/etc/postfix/sasl-passwd
smtp_always_send_ehlo      = yes
smtp_sasl_security_options = noanonymous
# default_transport = error
# relay_transport = error
```

Die Datei `sasl-passwd` hat den folgenden Aufbau:

```
# /etc/postfix/sasl-passwd
anderer-host.de  loginname:passwort
```

Viele E-Mail-Server werden den Empfang von E-Mails von Ihrem Server verweigern, weil die Absenderadresse der E-Mail nicht mit der Adresse des in `sasl-passwd` spezifizierten E-Mail-Accounts übereinstimmt. Um auch diese dem Spam-Schutz dienende Hürde zu überwinden, wird Postfix so konfiguriert, dass es die Absenderadresse `root@...` durch die E-Mail-Adresse Ihres Accounts ersetzt.

```
# noch eine Änderung in /etc/postfix/main.cf
...
canonical_maps = hash:/etc/postfix/canonical
```

`canonical` muss nun den folgenden Eintrag enthalten. Vergessen Sie anschließend `postmap /etc/postfix/canonical` nicht!

```
# /etc/postfix/canonical
root  mein.name@andere-firma.de
```

Logging, Administration

Postfix protokolliert alle seine Tätigkeiten – und das sind viele – via Syslog in den Logging-Dateien `/var/log/mail.*` (siehe Abschnitt 21.7).

`mail.warn` enthält in erster Linie Warnungen vor DNS-Problemen. Die Datei kann im Regelfall ignoriert werden, Schuld an den Warnungen haben zumeist die Betreiber externer MTAs. Viele MTAs sind auch ganz bewusst falsch konfiguriert, weil sie ausschließlich zum Spam-Versand dienen.

Fehler beim Start von Postfix, die oft durch eine syntaktisch falsche Konfiguration verursacht sind, werden in `mail.err` aufgezeichnet. Ein Blick in diese Datei lohnt, wenn einzelne Komponenten nicht funktionieren oder gar nicht starten.

Wenn Sie wissen möchten, welche E-Mails auf den Versand warten, führen Sie `postqueue -p` oder `mailq` aus. Die beiden Kommandos liefern eine Liste aller E-Mails, die – aus welchen Gründen auch immer – bisher nicht versandt werden konnten.

37.3 Dovecot (POP- und IMAP-Server)

Das aus mehreren Komponenten bestehende Programm Dovecot arbeitet je nach Installationsumfang (Pakete `dovecot-pop3d` und `dovecot-imapd`) als POP- und IMAP-Server. Im einfachsten Fall funktioniert das Programm ohne jede Konfigurationsarbeiten – man würde es nicht für möglich halten, dass es so etwas überhaupt noch gibt!

Konfiguration

Für die Konfiguration von Dovecot 2.0 sind eine Menge Dateien vorgesehen: `/etc/dovecot/dovecot.conf` und `/etc/dovecot/conf.d/*.conf`. Die Datei `10-auth.conf` enthält zudem einige `include`-Anweisungen für `auth-*.ext`-Dateien mit Ergänzungen; die meisten `include`-Anweisungen sind aber standardmäßig auskommentiert und daher nicht aktiv.

```
user$  cd /etc/dovecot/conf.d
user$  ls
10-auth.conf       10-ssl.conf    90-plugin.conf            auth-static.conf.ext
10-director.conf   15-lda.conf    90-quota.conf             auth-system.conf.ext
10-logging.conf    20-imap.conf   auth-deny.conf.ext        auth-vpopmail.conf.ext
10-mail.conf       20-pop3.conf   auth-master.conf.ext
10-master.conf     90-acl.conf    auth-passwdfile.conf.ext
```

Die `*.conf`-Dateien dienen auch zur Dokumentation von Dovecot. Das ist einerseits praktisch, andererseits aber auch sehr unübersichtlich: Standardmäßig umfassen die `*.conf`-Dateien rund 1100 Zeilen Code! Die tatsächlich relevanten Anweisungen befinden sich in ganz wenigen Zeilen, der Rest sind Kommentare.

Mit den folgenden Kommandos können Sie sich einen Überblick verschaffen. Die beiden verschachtelten `grep`-Kommandos eliminieren alle Kommentare und leere Zeilen:

```
user$  cd /etc/dovecot
user$  grep -h -v '^[[:space:]]*\#' dovecot.conf conf.d/*.conf |  \
          grep -v '^[[:space:]]*$' | less
```

Die folgenden Zeilen präsentieren die Einstellungen der wichtigsten Konfigurationsdateien. Auf den Abdruck der Dateien, die nur Kommentare, aber keinen aktiven Code enthalten, habe ich aus Platzgründen verzichtet.

```
# Datei dovecot.conf
!include_try /usr/share/dovecot/protocols.d/*.protocol
dict {
}
!include conf.d/*.conf
!include_try local.conf
```

```
# Datei conf.d/10-auth.conf
auth_mechanisms = plain
!include auth-system.conf.ext

# Datei conf.d/10-director.conf
service director {
  unix_listener login/director {
  }
  fifo_listener login/proxy-notify {
  }
  unix_listener director-userdb {
  }
  inet_listener {
  }
}
service imap-login {
}
service pop3-login {
}
protocol lmtp {
}


# Datei conf.d/10-master.conf
service imap-login {
  inet_listener imap {
  }
  inet_listener imaps {
  }
}
service pop3-login {
  inet_listener pop3 {
  }
  inet_listener pop3s {
  }
}

service lmtp {
  unix_listener lmtp {
  }
}
service imap {
}
service pop3 {
}
```

```
service auth {
  unix_listener auth-userdb {
  }
}
service auth-worker {
}
service dict {
  unix_listener dict {
  }
}

# Datei conf.d/10-ssl.conf
ssl_cert = </etc/ssl/certs/dovecot.pem
ssl_key = </etc/ssl/private/dovecot.pem

# Datei conf.d/15-lda.conf
protocol lda {
}

# Datei conf.d/20-imap.conf
protocol imap {
}

# Datei conf.d/20-pop3.conf
protocol pop3 {
}
```

Beachten Sie, dass Sie die geschwungenen Klammern in einer eigenen Zeile schließen müssen. Die Anweisung `protocol imap { }` in nur einer Zeile ist syntaktisch nicht erlaubt.

Dovecot braucht deswegen so wenige Einstellungen, weil es für alle Optionen Defaultwerte gibt. `dovecot -a` liefert eine Liste aller Einstellungen, `dovecot -n` eine Liste mit allen Optionen, die von der Defaulteinstellung abweichen.

IPv6

Dovecot ist zwar IPv6-tauglich, kommuniziert aber standardmäßig nur über das IPv4-Protokoll. Um auch IPv6 zuzulassen, müssen Sie in `dovecot.conf` den Parameter `listen` einstellen. `*` bedeutet, dass alle IPv4-Schnittstellen berücksichtigt werden, `::` gilt analog für IPv6-Schnittstellen. Alternativ können Sie auch explizit die IPv4- und IPv6-Adressen der für den Mail-Verkehr vorgesehenen Schnittstellen angeben.

```
# Datei dovecot.conf, IPv6 aktivieren
...
listen = *, ::
```

Ort der Mailbox-Dateien

Dovecot kommt sowohl mit dem Maildir- als auch mit dem mbox-Format zurecht, ganz egal, ob Sie das Programm als POP- oder IMAP-Server verwenden (oder beides). Wenn Sie Dovecot allerdings überwiegend als IMAP-Server einsetzen, ist das Maildir-Format aus Effizienzgründen vorzuziehen.

Dovecot versucht die Postfächer automatisch zu entdecken, was bei meinen Tests auch problemlos funktioniert hat. Es durchsucht dabei in dieser Reihenfolge die folgenden Verzeichnisse:

```
/home/username/Maildir                          (Maildir-Format)
/home/username/mail   und  /var/mail/username   (mbox-Format)
/home/username/Mail   und  /var/mail/username   (mbox-Format)
```

Die automatische Mailbox-Suche kann allerdings scheitern, wenn ein Benutzer noch keine Mail erhalten hat und sein Postfach somit leer ist, die Postfachdatei also noch gar nicht existiert. Deswegen empfiehlt es sich, den Mailbox-Ort in `10-mail.conf` explizit einzustellen. Für Postfächer in `/var/mail/`*`username`* lautet die richtige Einstellung:

```
# in /etc/dovecot/conf.d/10-mail.conf
...
# mbox-Postfächer in /var/mail
mail_location = mbox:~/Mail:INBOX=/var/mail/%u
```

Damit weiß Dovecot, dass Ihr Server das mbox-Format verwendet und dass sich neue E-Mails in `/var/mail/`*`username`* befinden. Die zusätzliche Angabe des Verzeichnisses `Mail` ist für diverse Zusatzfunktionen von Dovecot erforderlich – auch dann, wenn sich in diesem Verzeichnis keine E-Mails befinden! Falls Dovecot als IMAP-Server verwendet wird, werden dort alle anderen IMAP-Postfächer gespeichert. Sie können natürlich ein beliebiges anderes Benutzerverzeichnis angeben, `mail` oder `Mail` sind aber die übliche Wahl. Das Benutzerverzeichnis muss vor der `INBOX`, also dem Postfach für neue E-Mails, angegeben werden.

Falls Sie Postfix so konfiguriert haben, dass der MTA die E-Mails im Maildir-Format an das lokale Verzeichnis `Maildir` zustellt, sieht die korrekte Einstellung von `mail_location` so aus:

```
# in /etc/dovecot/conf.d/10-mail.conf
...
# mbox-Postfächer in /var/mail
mail_location = maildir:~/Maildir
```

Wenn Postfix so konfiguriert ist, dass es E-Mail-Adressen aus diversen Domänen in virtuellen Postfächern speichert, wird die Konfiguration komplizierter: Zum einen müssen Sie Dovecot verraten, wo sich die Postfächer befinden; und zum anderen brauchen Sie nun eine eigene Tabelle, die für alle E-Mail-Adressen Login-Namen und

Passwörter für die POP- und SMTP-Authentifizierung enthält. Konfigurationstipps und ein konkretes Beispiel finden Sie auf den folgenden Webseiten:

http://wiki2.dovecot.org/VirtualUsers
https://workaround.org/ispmail/squeeze

Betrieb als POP- bzw. IMAP-Server

Dovecot funktioniert auf Anhieb als POP- oder IMAP-Server. Um Ihre E-Mails von einem externen Rechner mit einem E-Mail-Client herunterzuladen, richten Sie darin ein neues Konto ein und geben als Verschlüsselungsverfahren STARTTLS an. Der Benutzername entspricht dem Namen Ihres Linux-Accounts auf dem Server. Auch das Passwort ist dasselbe wie auf dem Server.

Verschlüsselung (TLS/STARTTLS)

Dovecot unterstützt das Protokoll *Transport Layer Security* (TLS) und das Verfahren STARTTLS zum Aufbau einer verschlüsselten Verbindung. Standardmäßig verwendet Dovecot das selbst generierte Zertifikat `/etc/ssl/certs/dovecot.pem`, das Sie beim ersten Verbindungsaufbau im Mail-Client akzeptieren müssen. Wenn Sie ein eigenes Zertifikat und einen eigenen Schlüssel verwenden möchten, müssen Sie die Orte der Zertifikats- und Schlüsseldateien in `10-ssl.conf` anpassen.

Im folgenden Beispiel kommen Dateien zum Einsatz, die auch für die HTTPS-Konfiguration von Apache verwendet wurden (siehe Abschnitt 35.4). Das zusätzliche CA-Zertifikat ist nur erforderlich, wenn Ihr Zertifikat von einer Zertifizierungsstelle stammt, die dem E-Mail-Client nicht bekannt ist. Der E-Mail-Client kann damit überprüfen, ob Ihre Zertifizierungsstelle befugt ist, Zertifikate auszustellen.

```
# in /etc/dovecot/conf.d/10-ssl.conf
...
ssl_cert = </etc/apache2/firma-abc.de.crt
ssl_key = </etc/apache2/firma-abc.de.key
ssl_ca = </etc/apache2/ca.pem
```

Die folgenden Kommandos zeigen, wie Sie selbst ein neues, für 10 Jahre gültiges Zertifikat für Dovecot erzeugen (siehe auch Abschnitt 35.4):

```
root#  openssl req -new -x509 -days 3650 -nodes \
         -out /etc/ssl/certs/dovecot.pem \
         -keyout /etc/ssl/private/dovecot.pem
root#  chmod 600 /etc/ssl/private/dovecot.pem
```

Die dazu passende Dovecot-Konfiguration sieht wie folgt aus:

```
# in /etc/dovecot/conf.d/10-ssl.conf
...
ssl_cert = </etc/ssl/certs/dovecot.pem
ssl_key  = </etc/ssl/private/dovecot.pem
```

SMTP-Authentifizierung für Postfix

Im Postfix-Abschnitt habe ich bereits erwähnt, dass Postfix zwar das Protokoll SASL (Simple Authentication and Security Layer) unterstützt, die Authentifizierung aber nicht selbst durchführen kann. Dovecot kann Postfix in dieser Angelegenheit unter die Arme greifen.

Dovecot-Konfiguration

Der erforderliche Konfigurationsaufwand ist minimal. Zum Ersten müssen Sie in der Dovecot-Konfigurationsdatei `10-master.conf` den im Abschnitt `service auth` bereits vorgesehenen Code zur Authentifizierung über die Socket-Datei `/var/spool/postfix/private/auth` aktivieren:

```
# Ergänzungen in /etc/dovecot/conf.d/10-master.conf
...
service auth {
  unix_listener auth-userdb {
    mode  = 0600
    user  = postfix
    group = postfix
  }

  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
  }

  # Auth process is run as this user.
  user = $default_internal_user
}
```

Zum Zweiten fügen Sie in `10-auth.conf` den Authentifizierungsmechanismus `login` hinzu. Diese Ergänzung ist erforderlich, damit die Authentifizierung auch mit Outlook Express bzw. Windows Mail funktioniert.

```
# Ergänzungen in /etc/dovecot/conf.d/10-auth.conf
...
auth_mechanisms = plain  login
```

Postfix-Konfiguration

Zuletzt müssen Sie am Ende der Postfix-Konfigurationsdatei `/etc/postfix/main.cf` einige Zeilen einfügen. Beachten Sie, dass die Pfadangabe für `smtpd_sasl_path` relativ zum Verzeichnis `/var/spool/postfix` erfolgen muss. Der Grund: Postfix läuft aus Sicherheitsgründen in einer `chroot`-Umgebung und interpretiert *alle* Pfadangaben in `main.cf` relativ zum Postfix-Queue-Verzeichnis.

```
# Ergänzung in /etc/postfix/main.cf
...
smtpd_sasl_auth_enable       = yes
smtpd_sasl_type              = dovecot
```

```
smtpd_sasl_path              = private/auth
smtpd_recipient_restrictions = permit_mynetworks,
                               permit_sasl_authenticated,
                               reject_unauth_destination
```

Konfiguration aktivieren

Anschließend fordern Sie beide Dienste dazu auf, ihre Konfigurationsdateien neu einzulesen:

```
root#  service dovecot restart
root#  service postfix reload
```

Client-Konfiguration

Beim Einrichten eines E-Mail-Kontos für Ihren eigenen E-Mail-Server wählen Sie im Mail-Client die Verschlüsselungsmethode STARTTLS aus (siehe Abbildung 37.3). Bei der Authentifizierung kommen Klartextpasswörter zum Einsatz. Das klingt unsicher, ist es aber nicht, weil die Passwortübertragung innerhalb einer TLS-Sitzung erfolgt, also bereits auf einer höheren Ebene verschlüsselt wird.

Abbildung 37.3 Beispielhafte Konfiguration eines Mail-Kontos in Thunderbird

Fehlersuche

Sollte es bei der SMTP-Authentifizierung Probleme geben, ist erstaunlicherweise das veraltete Programm `telnet` ein wertvolles Hilfsmittel zur Fehlersuche. Sie können dieses Kommando auf einem beliebigen Rechner ausführen. Es muss sich dabei nicht um den Mail-Server handeln.

Der Verbindungsaufbau über Port 25 beginnt mit Textnachrichten. Die Willkommensnachricht der Servers müssen Sie mit `EHLO hostname` beantworten. Postfix gibt nun bekannt, dass die weitere Kommunikation gemäß dem STARTTLS-Verfahren verschlüsselt werden kann und dass die Authentifizierung durch ein Klartext-Passwort erfolgen darf. Mit `quit` beenden Sie nun das »Gespräch« mit dem Mail-Server.

```
user  telnet mail.firma-abc.de 25
Trying 211.212.213.214...
Connected to mail.firma-abc.de
Escape character is '^]'.
220 firma-abc.de ESMTP Postfix (Ubuntu)
EHLO firma-abc.de
250-firma-abc.de
250-PIPELINING
250-SIZE 50480000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
Connection closed by foreign host.
```

37.4 SpamAssassin (Spam-Abwehr)

Das bekannteste Open-Source-Programm zur Spam-Bekämpfung ist SpamAssassin. Es versucht aufgrund diverser Kriterien zu entscheiden, ob eine E-Mail Spam enthält oder nicht. Gründe, die zu einer Spam-Klassifizierung führen, sind fehlende Reverse-DNS-Einträge, offensichtlich falsche DNS-Angaben oder die Herkunft der E-Mails von bekannten »Spam-Schleudern«, also von Rechnern, die aufgrund von massenhaftem Spam-Versand auf sogenannten Blacklists gelandet sind.

SpamAssassin berücksichtigt auch den *Inhalt* der E-Mail. Letzteres erfordert eine relativ aufwendige Analyse, die auf stark frequentierten E-Mail-Servern eine hohe CPU-Last verursacht. Die Ergebnisse der verschiedenen Spam-Erkennungsregeln werden addiert. Überschreitet die Summe einen Grenzwert, wird die E-Mail als Spam gekennzeichnet.

Umgang mit spam-verdächtigen E-Mails

Standardmäßig verpackt SpamAssassin als Spam erkannte E-Mails neu. Die E-Mail enthält einen Hinweis auf den Spam-Verdacht. Die originale Nachricht wird im Anhang mitgeliefert, sodass der Anwender eine irrtümlich als Spam klassifizierte E-Mail problemlos lesen kann.

Jetzt bleibt noch die Frage offen, wie der Endanwender am besten mit spam-verdächtigen E-Mails verfährt: SpamAssassin fügt in jede E-Mail eine Zeile der Form `X-Spam-Flag: YES` ein. Außerdem bekommt jede von SpamAssassin kontrollierte E-Mail eine Zeile `X-Spam-Level: ********`, wobei die Anzahl der Sterne die Spam-Bewertungs-

summe wiedergibt: Je mehr Sterne, desto höher ist die Spam-Wahrscheinlichkeit. Standardmäßig betrachtet SpamAssassin E-Mails ab fünf Sternen als Spam.

Aufgrund der `X-Spam`-Zeilen im E-Mail-Header können Sie bei den meisten E-Mail-Clients eine Filterregel aufstellen, sodass derart gekennzeichnete E-Mails automatisch in einen Junk- oder Spam-Ordner verschoben werden.

SpamAssassin ist lernfähig

Zu den Besonderheiten von SpamAssassin zählt der Umstand, dass das Programm dazulernen kann: Wenn ein Benutzer bei der Klassifizierung der E-Mails hilft, versucht SpamAssassin, Merkmale dieser E-Mails zu extrahieren und neue E-Mails aufgrund dieser Merkmale selbst richtig zu klassifizieren. Die zugrunde liegenden Techniken basieren auf einem sogenannten Bayesschen Filter, deren Grundlagen in der Wikipedia gut beschrieben sind.

Die Lernfunktionen haben den Nachteil, dass sie eine manuelle Kontrolle der Spam-Klassifizierung voraussetzen – und die ist beim Betrieb von SpamAssassin auf einem Server selten gegeben. SpamAssassin funktioniert erfreulicherweise auch ohne dieses Training, wenn auch mit einer etwas niedrigeren Trefferquote.

Installation und Konfiguration

Es gibt verschiedene Möglichkeiten, SpamAssassin mit Postfix zu kombinieren. Dieser Abschnitt beschreibt, wie Sie SpamAssassin über die Milter-Schnittstelle von Postfix aufrufen. Milter steht für *Mail Filter* und ist eigentlich eine von Sendmail definierte Schnittstelle, um E-Mail-Filterprogramme einzubinden. Postfix unterstützt diese Schnittstelle in aktuellen Versionen ebenfalls und vereinfacht so die Integration von Spam- und Virenfiltern im Vergleich zu anderen Verfahren ganz erheblich.

Alle gängigen Distributionen stellen Pakete für SpamAssassin zur Verfügung. Unter Debian und Ubuntu führen Sie zur Installation das folgende Kommando aus:

```
root#  apt-get install spamassassin spamass-milter
```

Um SpamAssassin als Dämon zu aktivieren, führen Sie zwei Änderungen in `/etc/default/spamassassin` durch:

```
# Änderungen in /etc/default/spamassassin
...
# den SpamAssassin-Dämon spamd starten
ENABLED=1
...
# regelmäßige Updates der SpamAssassin-Regeln durchführen
CRON=1
```

Die Basiskonfiguration von SpamAssassin erfolgt durch diverse `*.cf`-Dateien im Verzeichnis `/usr/share/spamassassin`. Davon abweichende Einstellungen führen Sie am besten in der Datei `/etc/spamassassin/local.cf` durch. Die wahrscheinlich interessanteste Einstellung ist `required_score` (Defaultwert 5.0): Sie gibt an, ab welcher

Punkteanzahl eine E-Mail als Spam klassifiziert wird. Ebenfalls oft praktisch ist die Einstellung `rewrite_header Subject *****SPAM*****`: Damit wird die Subject-Zeile aller spam-verdächtigen E-Mails verändert. Das erleichtert die Spam-Erkennung für E-Mail-Anwender, die mit der Definition von Filterregeln in ihrem E-Mail-Client überfordert sind.

Nach diesen Vorbereitungsarbeiten starten Sie SpamAssassin:

```
root#  service spamassassin start
```

Die Milter-Erweiterung zu SpamAssassin, also das Programm `spamass-milter`, ist bereits aktiv. Es wurde unmittelbar nach der Installation gestartet und kommuniziert direkt mit dem SpamAssassin-Dämon `spamd`. Die Konfiguration erfolgt durch die Datei `/etc/default/spamass-milter`, Änderungen sind in der Regel aber nicht erforderlich. Die Kommunikation zwischen `spamass-milter` und Postfix erfolgt über die Socket-Datei `/var/spool/postfix/spamass/spamass.sock`.

Postfix-Konfiguration

Jetzt müssen Sie Postfix noch dazu bringen, dass es alle eintreffenden E-Mails durch den SpamAssassin-Filter leitet. Dazu fügen Sie die folgende Zeile in `main.cf` ein. Beachten Sie, dass der Pfad zur Socket-Datei relativ zum Postfix-Queue-Verzeichnis `/var/spool/postfix` angegeben werden muss!

```
# Ergänzung in /etc/postfix/main.cf
...
smtpd_milters = unix:spamass/spamass.sock
```

Anschließend laden Sie die Postfix-Konfiguration neu:

```
root#  service postfix reload
```

Test

Um SpamAssassin auszuprobieren, senden Sie von einem externen E-Mail-Account eine speziell für SpamAssassin konzipierte Testnachricht an Ihren Server. Diese Nachricht muss die folgende Zeichenkette enthalten. Anstatt die Zeichenkette abzutippen, können Sie in Wikipedia nach GTUBE (*Generic Test for Unsolicited Bulk Email*) suchen und die Zeichenkette von dort kopieren.

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Wenn alles funktioniert, wird die Nachricht als Spam erkannt. Der Adressat erhält die als Spam markierte E-Mail zusammen mit einer Information, warum es sich vermutlich um Spam handelt. Der Text der Nachricht sollte in etwa so aussehen:

```
Software zur Erkennung von "Spam" auf dem Rechner kofler.info hat die
eingegangene E-mail als mögliche "Spam"-Nachricht identifiziert.  Die
ursprüngliche Nachricht wurde an diesen Bericht angehängt, so dass Sie sie
anschauen können (falls es doch eine legitime E-Mail ist) oder ähnliche
unerwünschte Nachrichten in Zukunft markieren können.  Bei Fragen zu diesem
```

```
Vorgang wenden Sie sich bitte an

   @@CONTACT_ADDRESS@@

Vorschau: XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
  test [...]

Inhaltsanalyse im Detail:   (1000.0 Punkte, 5.0 benötigt)

Pkte Regelname              Beschreibung
---- ---------------------- --------------------------------------------------
-0.0 RCVD_IN_DNSWL_NONE     RBL: Sender listed at http://www.dnswl.org/, no
                            trust
                            [213.165.64.42 listed in list.dnswl.org]
0.0 FREEMAIL_FROM           Sender email is commonly abused enduser mail
                            provider
-0.0 T_RP_MATCHES_RCVD      Envelope sender domain matches handover relay
                            domain
-0.0 SPF_PASS               SPF: Senderechner entspricht SPF-Datensatz
0.0 UNPARSEABLE_RELAY       Informational: message has unparseable relay lines
1000 GTUBE                  BODY: Test zur Prüfung von Anti-Spam-Software
0.0 T_TO_NO_BRKTS_FREEMAIL  T_TO_NO_BRKTS_FREEMAIL
```

37.5 ClamAV (Virenabwehr)

Mit Spam ist es leider noch nicht getan: Wenn sich in Ihrem Netzwerk Windows-Rechner befinden, müssen Sie auch dafür sorgen, dass die E-Mails frei von Viren eintreffen. Nun sind per E-Mail verbreitete Viren für Windows-PCs heute nicht mehr das ganz große Thema, das sie vor ein paar Jahren waren. E-Mail-Viren sind aber noch immer ein sporadisches Risiko, das es zu minimieren gilt. Deswegen empfiehlt es sich, auf dem E-Mail-Server ein weiteres Programm zu installieren, das E-Mails bzw. deren Anhänge auf bekannte Viren untersucht und befallene E-Mails löscht. Technisch funktioniert ein E-Mail-Filter ähnlich wie ein Spam-Filter, wobei aber vor allem Anhänge auf Muster bekannter E-Mails durchsucht werden müssen. Das kostet eine Menge CPU-Zeit und ist nur dann zielführend, wenn eine aktuelle Virendatenbank zur Verfügung steht.

ClamAV ist das populärste Open-Source-Programm zur Erkennung von Viren in Dateien oder E-Mails. Dabei geht es primär um Schadsoftware für Windows-Rechner. E-Mail-Viren für Linux und Mac OS X gibt es ja glücklicherweise noch nicht. Im Vergleich zu kommerziellen Virenschutzprogrammen war ClamAV in der Vergangenheit selten Testsieger, hat sich aber in der Regel einigermaßen gut geschlagen. Eine Garantie, die allerneuesten Viren von der ersten Stunde an korrekt zu erkennen, gibt es aber nicht.

Installation

Ähnlich wie bei SpamAssassin gibt es auch bei ClamAV verschiedene Möglichkeiten zur Integration in Postfix. Ich stelle Ihnen hier wieder die Milter-Variante vor, die am einfachsten zu konfigurieren ist. Entsprechende Pakete finden Sie in allen gängigen Distributionen. Unter Debian und Ubuntu heißen sie `clamav`, `clamav-daemon` und `clamav-milter`. Zusammen mit ClamAV wird in der Regel auch das Programm `freshclam` installiert. Es kümmert sich darum, die initiale Virendatenbank herunterzuladen und in der Folge regelmäßig zu aktualisieren. Werfen Sie einen Blick in das Verzeichnis `/var/lib/clamav` (es darf nicht leer sein!) bzw. lesen Sie die `man`-Seite zu `freshclam`.

Konfiguration

Damit Sie ClamAV über die Postfix-Milter-Schnittstelle benutzen können, sind einige Vorbereitungsarbeiten erforderlich: Als Erstes entfernen Sie in `/etc/default/clamav-milter` das Kommentarzeichen für die bereits vorgesehene Zeile zur Postfix-Konfiguration. Die Variable `SOCKET_RWGROUP` gibt an, welcher Gruppe die ClamAV-Socket-Datei zugeordnet werden soll.

```
# in /etc/default/clamav-milter
...
SOCKET_RWGROUP=postfix
```

In `/etc/clamav/clamav-milter.conf` geben Sie an, an welchem Ort die ClamAV-Socket-Datei erzeugt werden soll:

```
# in /etc/clamav/clamav-milter.conf
...
MilterSocket /var/spool/postfix/clamav/clamav-milter.ctl
```

Anschließend erzeugen Sie das Verzeichnis für die Socket-Datei so, dass sowohl Postfix als auch ClamAV darin lesen und schreiben dürfen:

```
root#  mkdir -p /var/spool/postfix/clamav/
root#  chown clamav:postfix /var/spool/postfix/clamav/
root#  chmod g+s /var/spool/postfix/clamav/
```

Ein Neustart von `clamd` und `clamav-milter` stellt sicher, dass ClamAV diese Änderungen übernimmt:

```
root#  service clamav-daemon restart
root#  service clamav-milter restart
```

Nun müssen Sie noch `/etc/postfix/main.cf` so anpassen, dass Postfix alle eintreffenden E-Mails zur Kontrolle an ClamAV weiterleitet. Wenn Sie nur ClamAV, nicht aber SpamAssassin verwenden, lassen Sie die Socket-Datei für SpamAssassin einfach weg. Die Pfadangaben der Socket-Dateien sind relativ zum Postfix-Queue-Verzeichnis `/var/spool/postfix`.

```
# Ergänzung in /etc/postfix/main.cf
...
smtpd_milters = unix:spamass/spamass.sock unix:clamav/clamav-milter.ctl
```

Dank `postfix reload` übernimmt Postfix die Konfigurationsänderung sofort:

```
root#  service postfix reload
```

ClamAV fügt nun in den Header jeder überprüften E-Mail den folgenden Text ein: Test

```
X-Virus-Scanned: clamav-milter 0.96.1 at firma-abc.de
X-Virus-Status: Clean
```

Wenn ClamAV tatsächlich einen Virus feststellt, wird die E-Mail nicht weitergeleitet. Weder der Absender noch der Empfänger wird davon informiert. Diese Vorgehensweise kann in `/etc/clamav/clamav-milter.conf` verändert werden. Die dort eingesetzten Schlüsselwörter sind in `/usr/share/doc/clamav-milter/examples/clamav-milter.conf` dokumentiert.

Um die korrekte Funktion von ClamAV zu testen, senden Sie von einem externen E-Mail-Account eine Testnachricht mit dem folgenden Text an Ihren Server:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Sie müssen den Text nicht abtippen, sondern können ihn auch von der folgenden Wikipedia-Seite kopieren:

http://en.wikipedia.org/wiki/EICAR_test_file

Kapitel 38
ownCloud

ownCloud ermöglicht es, Dateien, Adressen, Kalender, Musikstücke und andere Daten auf einem eigenen Server abzulegen und diese Daten über alle erdenklichen Client-Geräte hinweg zu synchronisieren. Unterstützt werden unter anderem Rechner unter Linux, Windows und OS X sowie Smartphones und Tablets unter Andoid und iOS. Damit bietet ownCloud auf den ersten Blick ähnliche Funktionen wie Dropbox, Ubuntu One und zahllose andere Cloud-Dienste.

Demgegenüber hat ownCloud einige wesentliche Vorteile:

- Sie geben die Daten nicht aus der Hand, sondern speichern sie auf Ihrem eigenen Server. Wer die Datensammelwut von Apple, Google & Co. sowie der NSA kennt, wird das zu schätzen wissen.
- Es fallen unabhängig von der Datenmenge keine zusätzlichen Kosten an. Speicher- und Synchronisationsdienste wie Dropbox sind ja nur für kleine Datenmengen kostenlos, üblicherweise 2 bis 5 GByte. Das macht ownCloud vor allem dann attraktiv, wenn Sie ohnedies einen eigenen Root-Server betreiben und noch freie Speicher- und Traffic-Ressourcen haben.
- Neben der Synchronisation von Dateien bietet ownCloud eine Menge Zusatzfunktionen: eine Kontakt- und Terminverwaltung, einen integrierten Audio-Player für MP3-Dateien, die direkte Anzeige von Bildern, PDF-Dateien, Office-Dateien etc.
- Wenn Ihnen das noch nicht genug ist, können Sie ownCloud durch Zusatzprogramme (Apps) erweitern. Neben den mitgelieferten Apps wird es in Zukunft vermutlich auch Apps von anderen Entwicklern geben: Eine öffentliche API macht die App-Entwicklung relativ einfach.

ownCloud bietet sich damit als Komplettlösung zur Speicherung und Synchronisation nahezu aller gängigen Daten zwischen mehreren Computern und iOS- oder Android-Geräten an.

Das *Cloud* im Namen ownCloud ist allerdings trotz vieler Ähnlichkeiten zu populären Cloud-Diensten irreführend. ownCloud ist in der gegenwärtigen Form in keiner Weise dahingehend optimiert, auf mehreren Servern zu laufen, die Daten redun-

dant zu speichern, Datenzugriffe gleichmäßig zu verteilen etc. Das alles sind aber Merkmale, die mit Cloud-Diensten assoziiert werden. ownCloud richtet sich also primär an Privatanwender oder kleine Firmen, die eine zentrale Datei-, Kontakt- und Terminverwaltung mit Synchronisationsfunktionen wünschen. Wer selbst einen Dienst wie DropBox gründen möchte, wird mit ownCloud hingegen nicht glücklich werden.

Eine Stärke von ownCloud im Vergleich zu anderen Open-Source-Projekten mit ähnlicher Zielsetzung ist die breite Client-Unterstützung: Clients für Linux, Windows und OS X sind kostenlos verfügbar, daneben gibt es Apps für iOS und Android. Außerdem können viele ownCloud-Funktionen auch über deren Weboberfläche sowie über standardisierte Protokolle genutzt werden, unter anderem WebDAV, CalDAV, CardDAV und Ampache.

Praxiserfahrungen

ownCloud ist noch nicht frei von Kinderkrankheiten! Die Synchronisation von Dateien funktioniert normalerweise gut, aber nicht so problemlos wie mit Dropbox. Brauchbare Informationen über den Stand der Synchronisation fehlen ganz. Zuletzt brachte eine Veränderung des Synchronisationsverhaltens einiges Durcheinander in meine Dateisammlung bei ownCloud: Während ältere ownCloud-Clients das lokale Verzeichnis `ownCloud` auf dem Server mit dem Unterverzeichnis `clientsync` abgleichen, werden bei neueren ownCloud-Clients *alle* ownCloud-Dateien synchronisiert.

Die Synchronisation von Terminen, Adressen etc. klappt zumeist einwandfrei, die Konfiguration der Client-Geräte ist aber mitunter mühsam. Das gilt insbesondere für Android-Smartphones.

Versionen

Für dieses Kapitel habe ich ownCloud in der Version 5.0 unter Ubuntu 12.04 als Server getestet. Aktuelle Informationen zu ownCloud lesen Sie am besten auf der Projektwebsite *http://owncloud.org* nach.

38.1 Installation

Voraussetzungen

Sofern Sie eine aktuelle Distribution als Basis verwenden, ist die Installation eines ownCloud-Servers unkompliziert. Zu den Voraussetzungen zählen Apache, PHP (mindestens in Version 5.3), das Datenbanksystem SQLite sowie diverse PHP-Module. Unter Ubuntu 12.04 installieren Sie einfach die folgenden Pakete:

```
root#  apt-get install apache2 php5 php5-common php5-gd php5-sqlite php5-curl \
         php-xml-parser curl libcurl3 libcurl3-dev php5-curl php-pdo
```

ownCloud-Paket installieren

ownCloud wird nur unter wenigen Distributionen als fertiges Paket mitgeliefert – und wenn, dann in der Regel in einer veralteten Version. Von der Website *http://owncloud.org/install* führt aber ein Link auf Paketquellen für fast alle gängigen Distributionen. Damit können Sie ownCloud mit wenigen Kommandos installieren – und haben zusätzlich einen Update-Service. Die Ubuntu-Version wird in das Verzeichnis `/var/www/owncloud` installiert. Die Apache-Konfigurationsdatei `/etc/apache2/conf.d/owncloud.conf` enthält für dieses Verzeichnis den Eintrag `AllowOverride All`.

ownCloud-manuell installieren

Zur manuellen Installation laden Sie ownCloud als TAR-Archiv von der Webseite *http://owncloud.org/install* herunter. Das Archiv packen Sie unter Debian und Ubuntu im Verzeichnis `/var/www` aus, bei anderen Distributionen in einem für Apache zugänglichen Verzeichnis. Anschließend machen Sie mit `chown` die Dateien für den Apache-Account les- und schreibbar, bei Debian und Ubuntu also für `www-data`.

```
root#  cd /var/www
root#  tar xjf download-verz/owncloud-n.n.n.tar.bz2
root#  chown -R www-data.www-data owncloud/
```

Apache-Konfiguration

ownCloud greift auf die Apache-Module `rewrite` und `headers` zurück. Um diese zu aktivieren, führen Sie das folgende Kommando aus:

```
root#  a2enmod rewrite headers
```

Damit die diversen `.htaccess`-Einstellungen von ownCloud wirksam werden, muss die Apache-Konfiguration für das Verzeichnis `/var/www/owncloud` den Eintrag `AllowOverride All` enthalten.

```
# in einer Apache-Konfigurationsdatei
...
<Directory /var/www/owncloud/>
  AllowOverride  All
  ...
</Directory>
```

ownCloud und HTTPS

Wenn Sie Apache für den HTTPS-Einsatz konfiguriert haben, sollten Sie das ownCloud-Verzeichnis nur über HTTPS verfügbar machen, also innerhalb einer `VirtualHost`-Gruppe für den Port 443. Das stellt eine verschlüsselte Übertragung Ihrer Daten sicher.

Leider sind manche Client-Programme nicht HTTPS-kompatibel. Wenn z. B. die Synchronisation von Adressen und Kontakten oder das Hören von Musik via HTTPS nicht funktioniert, ist ein HTTP/HTTPS-Parallelbetrieb unumgänglich.

Damit alle veränderten Einstellungen wirksam werden, auch die vorhin aktivierten Module `rewrite` und `headers`, müssen Sie Apache neu starten:

```
root# service apache2 restart
```

Administrator-Konto

Die ownCloud-Installation können Sie nun in Ihrem Webbrowser unter der folgenden Adresse abschließen:

http://ihr-hostname/owncloud oder *https://ihr-hostname/owncloud*

Sie müssen lediglich ein Admin-Konto einrichten, also einen Namen und ein Passwort angeben. Optional können Sie auch den Ort des Datenverzeichnisses einstellen. Standardmäßig verwendet ownCloud das Verzeichnis `/var/www/owncloud/data`. Falls Sie ein eigenes ownCloud-Datenverzeichnis einstellen – z. B. in einem eigenen Logical Volume oder auf einer eigenen Festplattenpartition –, müssen Sie sicherstellen, dass der Apache-Account dieses Verzeichnis lesen und verändern darf. Unter Fedora und RHEL müssen Sie außerdem den SELinux-Kontext korrekt einstellen.

Außerdem können Sie das Datenbanksystem wählen, in dem ownCloud diverse Einstellungen und Metadaten speichert. Standardmäßig kommt SQLite zum Einsatz, und dabei sollten Sie es im Regelfall auch belassen. Wenn Sie stattdessen MySQL verwenden möchten, müssen Sie sicherstellen, dass neben dem MySQL-Server selbst auch das Paket `php5-mysql` installiert ist. Außerdem müssen Sie eine leere MySQL-Datenbank und einen dazu passenden Benutzer für ownCloud einrichten und die entsprechenden MySQL-Parameter (Benutzername, Passwort, Datenbankname) angeben.

ownCloud-Benutzerverwaltung

So wie Sie unter Linux nur in Ausnahmefällen als `root` arbeiten, werden Sie auch bei ownCloud das Admin-Konto nicht zur Speicherung gewöhnlicher Daten verwenden. Sie sollten deswegen nach dem ersten Login bei ownCloud im Einstellungspunkt NUTZER im Login-Menü rechts oben (siehe Abbildung 38.1) einen gewöhnlichen Benutzer einrichten. An dieser Stelle können Sie auch ownCloud-Konten für Familienmitglieder, Firmenmitarbeiter etc. anlegen.

Im Dialog zur Benutzerverwaltung können Sie ein Standard-Quota festlegen, z. B. 5 GByte. Damit geben Sie den maximalen Speicherplatz vor, den ein Benutzer beanspruchen darf. Davon abweichend können Sie die maximale Speichermenge individuell für jeden Benutzer einstellen. Leider verrät ownCloud nicht, wie viel Speicherplatz jeder Benutzer tatsächlich beansprucht. Eine Liste aller Datenverzeichnisse mit dem Platzbedarf in MByte liefert das folgende Kommando:

```
root# du -m --max 1 /var/www/owncloud/data | sort -rn
```

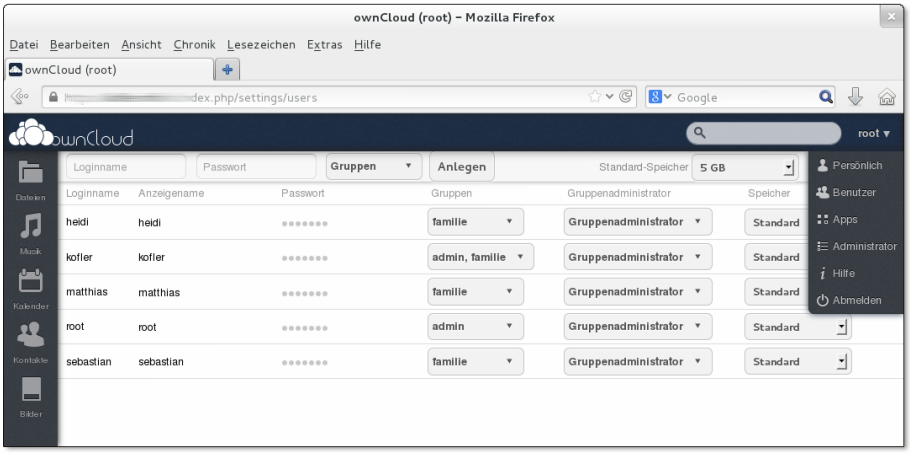


Abbildung 38.1 ownCloud-Benutzerverwaltung

ownCloud gibt Ihnen auch die Möglichkeit, die Benutzer in Gruppen zu organisieren. Es gibt aber nur wenige Funktionen, bei denen die Gruppenzugehörigkeit relevant ist.

Benutzer löschen

Um einen Benutzer zu löschen, klicken Sie einfach auf den x-Button am rechten Ende der Zeile des Benutzers. Beachten Sie aber, dass die Dateien des Benutzers aus Sicherheitsgründen *nicht* gelöscht werden! Wenn Sie sicher sind, dass Sie die Dateien nicht mehr brauchen, müssen Sie das entsprechende Verzeichnis manuell löschen. Der Konfiguration dieses Kapitels folgend ist das `/var/www/owncloud/data/benutzername`.

Benutzer-einstellungen

Jeder Benutzer kann nach dem Login in der ownCloud-Weboberfläche seine persönlichen Einstellungen inklusive des Passworts ändern. Dazu wählen Sie im Login-Menü den Eintrag PERSÖNLICH. Hier können Sie auch die gewünschte Sprache einstellen. Empfehlenswert ist schließlich die Angabe einer E-Mail-Adresse, an die gegebenenfalls ein Login-Link versandt wird, falls Sie Ihr Passwort vergessen sollten. Diese Funktion setzt voraus, dass auf dem ownCloud-Server ein Mail-Server zur Verfügung steht.

Sonstige Einstellungen

Apps

Der Einstellungspunkt APPS führt in eine Liste von Zusatzprogrammen (Plugins), die in ownCloud zur Verfügung stehen. Diese können bei Bedarf aktiviert oder deaktiviert werden. Standardmäßig aktiviert sind beispielsweise Viewer für verschiedene Dateitypen. Daneben stehen einige weitere Apps für ausgefallenere Aufgaben zur Auswahl, z. B. für ein LDAP-Backend.

Der Button Weitere Anwendungen führt auf eine Website mit Apps aus der ownCloud-Community. Damit Sie diese Apps verwenden können, müssen Sie die betreffende TAR-Datei im Verzeichnis `/var/www/owncloud/apps` auspacken und für Apache lesbar machen.

Administrator

Der Menüeintrag Administrator führt auf eine Seite mit diversen ownCloud-Grundeinstellungen. Hier können Sie z. B. die maximale Dateigröße verändern oder ganze ownCloud-Instanzen als Backup exportieren.

Verschlüsselung

Wenn Sie möchten, dass die Daten verschlüsselt zwischen Ihren Clients und ownCloud übertragen werden, müssen Sie ownCloud auf einer HTTPS-Site einrichten. Auf der Seite Administrator können Sie sogar einstellen, dass ownCloud ausschließlich via HTTPS verwendet werden darf.

Wünschen Sie darüber hinaus auch, dass alle Dateien innerhalb der ownCloud-Verzeichnisse verschlüsselt gespeichert werden, müssen Sie die App Encryption aktivieren. Die App verschlüsselt nur den Inhalt von Dateien, nicht aber Dateinamen, Kontakte, Termine etc. Interna zur Encryption-App, die für ownCloud 5 komplett neu implementiert wurde, können Sie hier nachlesen:

http://blog.schiessle.org/2013/05/28

Versionen

Standardmäßig erstellt ownCloud Backups aller Dateien, die geändert oder gelöscht werden. Verantwortlich ist dafür die App Versions, die standardmäßig aktiviert ist. ownCloud-Anwender können also wie unter Dropbox bei Bedarf auch auf ältere Versionen von synchronisierten Dateien zurückgreifen. Der Zugriff auf die Backup-Versionen von Dateien erfolgt in der Web-Oberfläche von ownCloud bei der jeweiligen Datei mit dem Link Versionen. Beachten Sie auch, dass Backups ausschließlich für reguläre Dateien erstellt werden, nicht aber für Kontakte und Termine!

ownCloud speichert aktuelle Änderungen einer Datei in der ersten Stunde minütlich, am ersten Tag stündlich, im ersten Monat täglich, dann wöchentlich. Außerdem werden alte Backups automatisch entfernt, wenn sie mehr als 50 Prozent des für den Benutzer vorgesehenen Speicherplatzes beanspruchen.

Interna

Tabelle 38.1 fasst die Speicherorte von ownCloud-Daten relativ zum ownCloud-Datenverzeichnis zusammen. Wenn Sie der obigen Anleitung gefolgt sind, hat dieses Verzeichnis den Pfad `/var/www/owncloud/data`.

In der SQLite-Datenbank werden unter anderem die Programmeinstellungen, die ownCloud-Benutzer und Gruppen, Sharing-Informationen, Kontakt- und Kalender-Daten sowie die Metadaten von Audio-Dateien und Fotos gespeichert. Wenn Sie

Pfad und Dateiname	Inhalt
owncloud.db	SQLite-Datenbank
loginname/files/*	Dateien
loginname/files/clientsync/*	Dateien der Desktop-Clients
loginname/files_versions/*	Backups alter Dateien (Versioning-App)
loginname/gallery/*	Vorschau-Bilder (Thumbnails)

Tabelle 38.1 ownCloud-Speicherorte

einen Blick in die Datenbank werfen möchten, installieren Sie das Paket `sqlite3` und führen dann `sqlite3 owncloud.db` aus. In der SQLite-Shell liefert das Kommando `.tables` eine Liste aller Tabellen. `select * from tablename` zeigt den Inhalt einer Tabelle an.

Umgang mit großen Dateien

In den Defaulteinstellungen erlaubt PHP nur den Upload von relativ kleinen Dateien (z. B. 2 MByte). Damit Sie in ownCloud auch größere Dateien übertragen können, befinden sich in der Datei `.htaccess` die folgenden Anweisungen:

```
# in /var/www/owncloud/.htaccess
php_value upload_max_filesize 512M
php_value post_max_size 512M
php_value memory_limit 512M
```

Damit ist ein Upload bis zu einer Größe von 512 MByte möglich. Gegebenenfalls müssen Sie diese Einstellungen verändern, wenn Sie noch größere Dateien übertragen wollen. Beachten Sie, dass die Angaben in `.htaccess` nur wirksam werden, wenn die Apache-Konfiguration für das Verzeichnis die Zeile `AllowOverride All` enthält. Sie können die PHP-Einstellungen natürlich auch systemweit verändern – unter Ubuntu in der Datei `/etc/php5/apache2/php.ini`. Weitere Tipps zum Umgang mit sehr großen Dateien finden Sie hier:

http://owncloud.org/support/big-files

ownCloud-Updates

Wenn Sie ownCloud aus einer Paketquelle beziehen, erfolgen Updates automatisch. Beim ersten Login nach einem Update werden eventuell erforderliche Umstellungsarbeiten automatisch erledigt.

Zur manuellen Durchführung eines ownCloud-Updates laden Sie das aktuelle TAR-Archiv herunter und extrahieren es im selben Apache-Verzeichnis wie die vorige Version. Vergessen Sie nicht, anschließend die Zugriffsrechte auf die Dateien wieder richtig einzustellen. Generell ist es natürlich eine gute Idee, vor jedem Update zuerst eine Kopie des gesamten ownCloud-Verzeichnisses zu erstellen – sicher ist sicher!

```
root#  cp -a owncloud owncloud-backup
root#  cd /var/www
root#  tar xjf download-verz/owncloud-n.n.n.tar.bz2
root#  chown -R www-data.www-data owncloud/
```

Mit welcher ownCloud-Version Sie gerade arbeiten, können Sie in der Weboberfläche im Punkt PERSÖNLICH der Einstellungen nachschauen. Bei Upgrades auf eine neue ownCloud-Hauptversion, also z. B. von Version 4 auf Version 5, beinhaltet der Update-Prozess mitunter weitere Schritte, die auf der folgenden Seite beschrieben sind:

http://owncloud.org/support/upgrade

38.2 Betrieb

Synchronisation von Dateien

Weboberfläche

Sie können ownCloud ohne die Installation irgendwelcher Client-Werkzeuge sofort nutzen. Dazu öffnen Sie in einem Webbrowser die ownCloud-Seite und loggen sich mit Ihrem Benutzernamen und Passwort ein.

Im Dialogblatt DATEIEN (siehe Abbildung 38.2) können Sie mit den meisten Webbrowsern Dateien direkt per Drag&Drop hochladen. Für ganze Verzeichnisse funktioniert dies aber nicht. Mit dem NEU-Button können Sie neue Verzeichnisse einrichten sowie Dateien aus dem lokalen Dateisystem zum Hochladen auswählen, falls Ihr Browser keine Drag&Drop-Funktionen bietet.

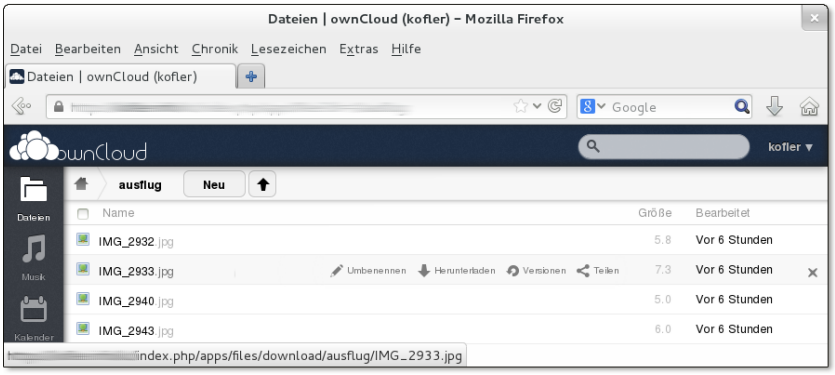


Abbildung 38.2 Dateien in der ownCloud-Benutzeroberfläche verwalten

Sync-Client für Linux

Immer mehr Distributionen stellen den ownCloud-Client im Paket `owncloud-client` oder `mirall` zur Verfügung, das Sie unkompliziert mit `apt-get`, `yum` oder `zypper` installieren können. Sollte das bei Ihrer Distribution nicht der Fall sein bzw. sollte die mitgelieferte Version veraltet sein, führt *http://owncloud.org/sync-clients* zu

Paketquellen für CentOS, Debian, Fedora, openSUSE und Ubuntu. Das Einrichten dieser Paketquelle hat den Vorteil, dass der ownCloud-Client in Zukunft automatisch aktualisiert wird.

Nach der Installation starten Sie den ownCloud-Client im Startmenü bzw. mit Alt+F2 `owncloud`. Im Verbindungsassistenten geben Sie die HTTP- oder HTTPS-Adresse Ihres ownCloud-Servers sowie den Loginnamen und das Passwort an (siehe Abbildung 38.3).

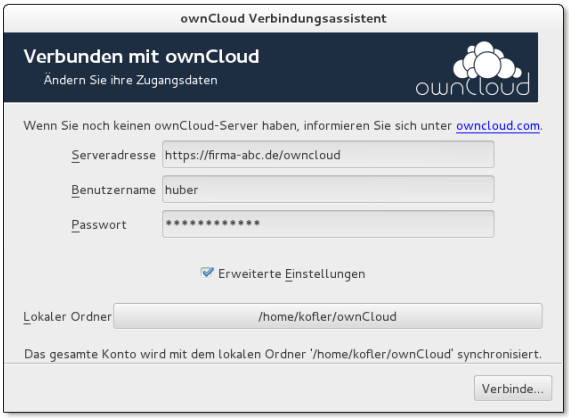


Abbildung 38.3 ownCloud-Linux-Client einrichten

Der Installationsassistent richtet automatisch das Verzeichnis `ownCloud` ein. Seit der im Frühjahr 2013 fertiggestellten Client-Version 1.3 wird das lokale `ownCloud`-Verzeichnis mit *allen* auf dem ownCloud-Server gespeicherten Dateien synchronisiert; in älteren Versionen wurde hingegen serverseitig das Unterverzeichnis `client-sync` verwendet. Ein wolkenförmiges Icon im Panel oder in der Statusleiste liefert Statusinformationen und bietet weitere Einstellmöglichkeiten.

Damit der ownCloud-Client in Zukunft automatisch gestartet wird, müssen Sie `/usr/bin/owncloud` manuell als Autostart-Programm einrichten. Unter Gnome und Unity führen Sie dazu Alt+F2 `gnome-session-properties` aus; unter KDE verwenden Sie stattdessen das Systemsteuerungsmodul STARTEN UND BEENDEN.

Die Einstellungen des ownCloud-Clients sind im Verzeichnis `.local/share/data/ownCloud` gespeichert, globale Einstellungen in `/etc/owncloud`. Der ownCloud-Client ist desktop-unabhängig implementiert und funktioniert unter Gnome, KDE und anderen Desktop-Systemen. Damit fehlt leider eine direkte Integration in Nautilus oder Dolphin: Anders als bei Dropbox oder Ubuntu One geben die Icons im Dateimanager keinen Rückschluss auf den Synchronisationsstatus.

Sync-Client für OS X

Der Sync-Client für OS X läuft wie unter Linux als Hintergrundprogramm und ist nur in Form eines kleinen Icons im rechten Teil der Menüleiste sichtbar. Die Bedienung erfolgt ganz ähnlich wie beim Linux-Client.

Damit der ownCloud-Client bei jedem Login automatisch gestartet wird, müssen Sie das Programm zu den Startprogrammen hinzufügen. Dazu öffnen Sie das Modul Benutzer & Gruppen der Systemeinstellungen und fügen das Programm den Anmeldeobjekten hinzu. Die Einstellungen des ownCloud-Clients werden im Verzeichnis `Library/Application Support/ownCloud` gespeichert.

Sync-Client für Windows

Der Sync-Client für Windows bietet im Vergleich zu den Programmen für Linux und OS X keine Überraschungen. Die Bedienung ist identisch. Die Einstellungen des Programms werden im Verzeichnis `C:\Users\`*name*`\AppData\Local\ownCloud` gespeichert.

Wie bei den anderen Betriebssystemen müssen Sie sich selbst um den automatischen Start des ownCloud-Clients kümmern. Unter Windows 7 suchen Sie dazu im Startmenü den Eintrag Alle Programme • Autostart und öffnen das entsprechende Verzeichnis mit der rechten Maustaste. Anschließend fügen Sie das ownCloud-Icon per Drag&Drop in dieses Verzeichnis ein.

Dateizugriff unter Android und iOS

Für Android- und iOS-Geräte gibt es im Play Store bzw. im App Store eine kostengünstige ownCloud-App. Damit können Sie unkompliziert auf Ihre ownCloud-Dateien zugreifen und – momentan nur unter Android – Ihre Fotos mit ownCloud synchronisieren.

WebDAV

Anstelle der Client-Apps können Sie zur Verwaltung der Dateien auch jedes Programm verwenden, das das WebDAV-Protokoll unterstützt. Unter Linux zählen dazu z. B. die Dateimanager von Gnome und KDE, also Nautilus und Dolphin. In Nautilus klicken Sie in der Seitenleiste auf den Eintrag Mit Server verbinden oder drücken Strg+L und geben dann eine Adresse nach dem folgenden Muster an:

```
dav://loginname@hostname/owncloud/remote.php/webdav   (HTTP)
davs://loginname@hostname/owncloud/remote.php/webdav  (HTTPS)
```

Dateien teilen

In der ownCloud-Weboberfläche können Sie einzelne Dateien »teilen«, also öffentlich zugänglich machen. Dabei gibt es zwei Varianten:

- Zum einen können Sie Dateien mit anderen Benutzern Ihres ownCloud-Servers austauschen. Bei der Eingabe wird der Name automatisch vervollständigt.
- Zum anderen können Sie mit der Option Über einen Link freigeben einen öffentlich zugänglichen Link erzeugen, den Sie dann per E-Mail versenden (siehe Abbildung 38.4). Bei dieser Variante benötigt der Empfänger selbst kein ownCloud-Konto, allerdings muss auf dem ownCloud-Server auch ein E-Mail-Server installiert sein.

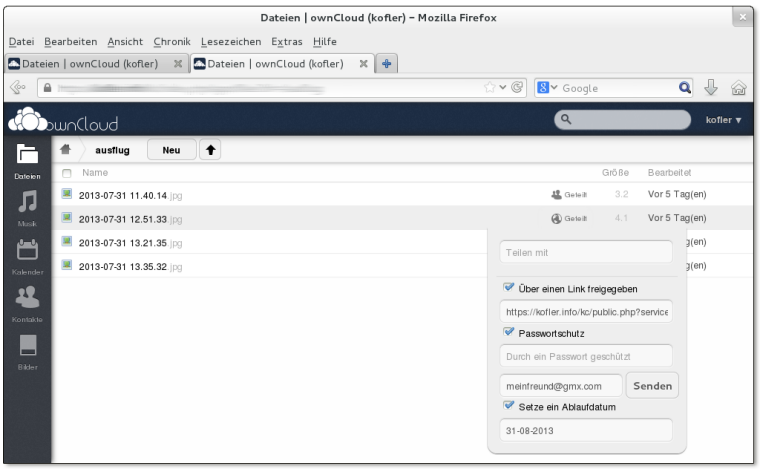


Abbildung 38.4 Dateien öffentlich zugänglich machen

Musik

In der Musik-Ansicht können Sie alle MP3-Dateien, die Sie in Ihr ownCloud-Verzeichnis (egal, in welches Unterverzeichnis) hochgeladenen haben, mit SAMMLUNG ERNEUT SCANNEN erfassen und anschließend abspielen. Die Wiedergabe funktioniert allerdings nicht in jedem Webbrowser.

Probleme hatte ich bei meinen Tests auch mit dem Einscannen der Musik: Gelöschte MP3-Dateien wurden nicht aus der Sammlung entfernt. Grundsätzlich berücksichtigt ownCloud ausschließlich die ID3-Tags in den MP3-Dateien, nicht deren Dateinamen. Alle MP3-Dateien werden nach Interpreten sortiert. Der ownCloud-Audio-Player kann zwar nicht mit Amarok oder Banshee mithalten, aber die Funktion ist durchaus praktisch, um unterwegs einige in der ownCloud gespeicherte Musikstücke abzuspielen.

Ampache

Anstatt des ownCloud-eigenen Audio-Players können Sie die Audio-Dateien unter Umständen sogar mit Ihrem eigenen Audio-Player abspielen. Die einzige Voraussetzung besteht darin, dass der Audio-Player die Ampache-API unterstützt. Ampache ist ein bereits mehr als 10 Jahre altes Programm für einen webbasierten Medien-Server. Hintergrundinformationen zu Ampache sowie eine Liste der dazu kompatiblen Audio-Player finden Sie in der Wikipedia.

Geeignete Audio-Player sind unter anderem Amarok, Rhythmbox und Banshee, wobei Sie bei den beiden letzteren Programmen je nach Distribution zuerst das dazugehörende Ampache-Plugin installieren müssen. Der Zugriff auf die Ampache-Daten erfolgt über die folgende Adresse:

http://<hostname>/owncloud/remote.php/ampache

Leider kommen viele Ampache-Player nicht mit HTTPS-Adressen zurecht. Auch in den ownCloud-Foren klagen viele Benutzer diverser Ampache-Clients, dass zwar die Übertragung der Titelliste funktioniert, nicht aber das Abspielen der Musik.

Kalender

Mit ownCloud können Sie einen oder mehrere Kalender verwalten. Zur Termineingabe können Sie sowohl die ownCloud-Weboberfläche als auch externe Kalenderprogramme verwenden. Zur Datenübertragung wird das weit verbreitete CalDAV-Protokoll verwendet.

Weniger ist mehr ...

Vermeiden Sie es, Ihre Termine über allzu viele Kalender zu verteilen! Bei vielen Client-Programmen müssen Sie jeden Kalender extra einrichten.

Im Dialogblatt KALENDER können Sie sofort Termine eintragen. Ein einzelner Mausklick auf einen Tag führt nach einer kurzen Wartezeit in den Dialog NEUES EREIGNIS, in dem Sie die Details des Termins eingeben können. Vorhandene Termine können Sie per Drag&Drop verschieben bzw. ebenfalls durch einen Mausklick bearbeiten.

Der Zahnrad-Button rechts oben führt in einen Einstellungsdialog. Dort können Sie vorhandene Kalender löschen, neue Kalender einrichten, diese mit anderen ownCloud-Benutzern teilen oder veröffentlichen sowie diverse Kalendereigenschaften ändern, z. B. die Farbe.

Externe Clients

Viele Kalenderprogramme sind CalDAV-kompatibel. Damit diese auf Ihre ownCloud-Kalender zugreifen können, müssen Sie normalerweise die folgende Adresse angeben:

http[s]://<hostname>/owncloud/remote.php/caldav/calendars/<benutzername>/<kalendername>

Im Kalender-Einstellungsdialog, den Sie durch einen Klick auf den Zahnrad-Button rechts oben in der ownCloud-Website öffnen, gibt es für jeden Kalender einen Link-Button. Damit ersparen Sie sich das fehleranfällige Abtippen der obigen Adresse.

Thunderbird

Auch das E-Mail-Programm Thunderbird kommt mit ownCloud-Terminen zurecht. Allerdings müssen Sie zuerst das Add-on Lightning installieren. Danach führen Sie EINSTELLUNGEN • KALENDER EINRICHTEN • ALLGEMEIN • KALENDER aus und wählen den Kalendertyp DAV-GROUPWARE-RESSOURCE.

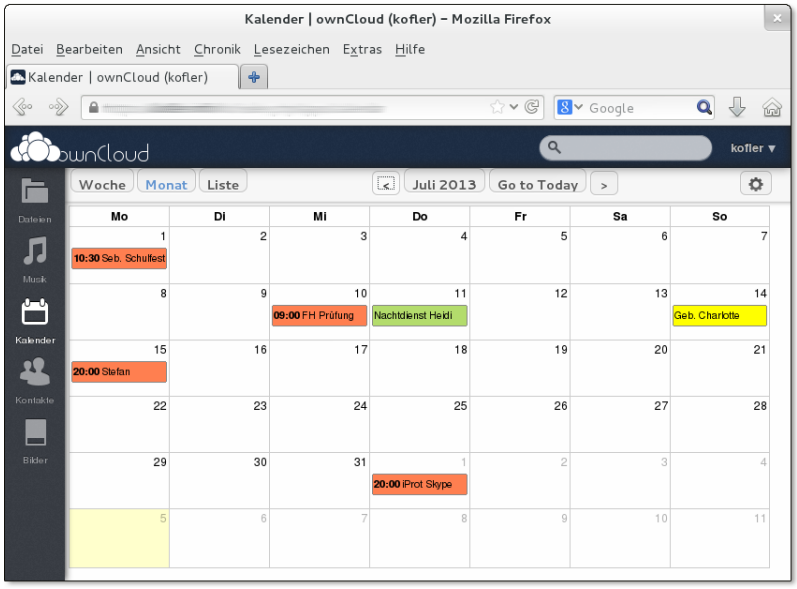


Abbildung 38.5 Kalenderverwaltung

Bei den Apple-Programmen iCal bzw. Kalender geben Sie diese Adresse an: Mac, iPhone, iPad

http[s]://<hostname>/owncloud/remote.php/caldav/principals/<benutzername>

Damit ersparen Sie sich die Definition jedes einzelnen Kalenders. Die Kalender-Programme von OS X bzw. iOS ermitteln selbstständig alle verfügbaren ownCloud-Kalender und übernehmen dabei sogar die in ownCloud definierten Farben.

Android unterstützt das CalDAV-Format leider nicht. Abhilfe schafft die App CalDAV-Sync, die zuletzt ca. drei Euro kostete. Nach der Installation richten Sie Ihren Kalender in den Android-Systemeinstellungen im Punkt KONTEN ein, wo jetzt der neue Kontentyp CALDAV zur Auswahl steht. Nach meinen Erfahrungen funktioniert die Synchronisation gut. Allerdings ist es auf Android-Geräten unmöglich, den Google-Kalender zu deaktivieren. Deswegen passiert es immer wieder, dass neue Termine versehentlich im falschen Kalender landen. Android

Kontakte

ownCloud eignet sich auch zur Verwaltung und Synchronisation von Kontakten. Die Kommunikation mit externen Kalenderprogrammen erfolgt dabei über das CardDAV-Protokoll. Dieses Protokoll wird auch von manchen Programmen zur Kontakt- bzw. Adressverwaltung unterstützt, aber leider bei Weitem noch nicht von allen.

Im Dialogblatt KONTAKTE der ownCloud-Weboberfläche können Sie mit dem Zahnrad-Button ein neues, leeres Adressbuch einrichten oder eine vorhandene Kalenderdatei im `*.vcf`-Format importieren. Bei modernen Browsern funktioniert dies auch per Drag&Drop.

Die Verwendung des Adressbuchs in der ownCloud-Benutzeroberfläche funktioniert zufriedenstellend, wenn Sie lediglich Kontakte suchen bzw. lesen möchten. Das Eingeben neuer Kontakte bzw. die Veränderung vorhandener Daten ist aber recht umständlich. In dieser Hinsicht kann ownCloud externe Adressbuchprogramme nicht ersetzen.

Externe Clients

Wenn Sie Ihr Adressbuchprogramm oder Ihren E-Mail-Client mit ownCloud synchronisieren möchten, müssen Sie zuerst einmal feststellen, ob das Programm das CardDAV-Protokoll unterstützt. Das ist unter anderem beim Gnome-Adressbuch und beim KDE-Programm Kontact der Fall.

Thunderbird

Wenn Sie mit Thunderbird arbeiten, benötigen Sie den *SOGo-Connector*. Das Add-on müssen Sie im Internet herunterladen und manuell installieren:

http://www.sogo.nu/downloads/frontends.html

Damit steht nun im Adressbuchfenster das neue Menükommando DATEI • NEU • REMOTE-ADRESSBUCH zur Verfügung. Im Konfigurationsdialog müssen Sie die Adresse Ihres Adressbuchs angeben. Diese ermitteln Sie am einfachsten in der Weboberfläche von ownCloud, indem Sie zuerst auf den Zahnrad-Button klicken, dann auf das neben dem Adressbuch angezeigte Link-Icon. Der Link hat die folgende Form:

http[s]://<hostname>/owncloud/remote.php/carddav/addressbooks/<name>/
<adressbuch>

Die Synchronisation müssen Sie per Kontextmenü explizit starten. Dabei werden Sie aufgefordert, den ownCloud-Login-Namen und das dazugehörige Passwort anzugeben.

Mac, iPhone, iPad

Die Adressbücher unter OS X und iOS sind CardDAV-kompatibel; die Synchronisation mit ownCloud gelingt problemlos.

Android

Auf Android-Geräten hilft die App CardDAV-Sync bei der Synchronisation. iPhones und iPads und das Adressbuch von OS X sind erfreulicherweise von Haus aus CardDAV-kompatibel.

Bilder

Die Ansicht BILDER der ownCloud-Weboberfläche (siehe Abbildung 38.6) hilft dabei, rasch durch die mit einem Desktop-Client hochgeladenen Bilder zu navigieren. Es ist nicht erforderlich, die Bilddateien in ein spezielles Verzeichnis hochzuladen.

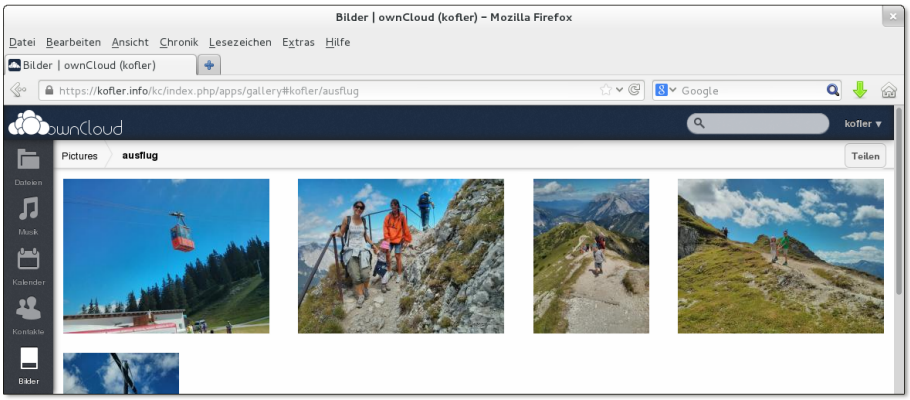


Abbildung 38.6 ownCloud-Bildansicht

Die Navigation durch die Bilder ist gewöhnungsbedürftig: Anfänglich zeigt ownCloud nur ein Bild für jedes Grundverzeichnis in ownCloud an. Wenn Sie dieses Verzeichnis anklicken, erscheinen alle direkt in diesem Verzeichnis enthaltenen Bilder, außerdem je ein Vorschaubild für jedes Unterverzeichnis. Wenn Sie die Maus über eine Verzeichnisvorschau bewegen, werden mehrere darin enthaltene Bilder nebeneinandergestellt. Leider können Sie in der Bildansicht keine Bilder per Drag&Drop hochladen. Das funktioniert nur in der Dateiansicht, also im Dialogblatt DATEIEN.

TEIL VII

Sicherheit

Kapitel 39
Backups

Ich mache hier gar nicht erst den Versuch, Sie von der Notwendigkeit von Backups zu überzeugen. Vielmehr konzentriert sich dieses Kapitel darauf, einige Backup-Tools vorzustellen. Welche Werkzeuge Sie in welcher Kombination einsetzen, bleibt Ihnen überlassen – dafür gibt es kein allgemeingültiges Rezept. Zu sehr hängt die optimale Backup-Strategie von der Natur der Daten, von der Art des Rechners (Desktop-PC/Notebook/Server), vom Backup-Medium (externe Festplatte, Netzwerkverzeichnis, Cloud) und vielen anderen Faktoren ab.

39.1 Backup-Benutzeroberflächen

Apple hat mit seiner Time Machine bewiesen, dass selbst ein Backup-Programm Begeisterung hervorrufen kann. Linux kann in dieser Hinsicht leider nicht mithalten: Das Angebot an Backup-Kommandos und -Tools ist zwar groß, aber auf das geniale, einfach zu nutzende Backup-Werkzeug warten Desktop-Anwender noch immer. In diesem Abschnitt stelle ich Ihnen die folgenden drei Programme kurz vor:

Déjà Dup: *https://launchpad.net/deja-dup*
Grsync: *http://www.opbyte.it/grsync*
Back in Time: *http://backintime.le-web.org*

Das populärste dieser Programme ist momentan Déjà Dup: Es wird von vielen Distributionen als Default-Backup-Programm eingerichtet. Auch mit Grsync können Sie nichts falsch machen – es synchronisiert Ihre Dateien einfach in ein anderes Verzeichnis, sodass das Backup ohne Zusatzwerkzeuge gelesen werden kann.

Déjà Dup

Déjà Dup ist dahingehend konzipiert, das Heimatverzeichnis möglichst unkompliziert in einem lokalen oder via SSH erreichbaren Backup-Verzeichnis zu sichern. Unter Ubuntu ist Déjà Dup in die Systemeinstellungen eingebettet und kann aus diesen heraus gestartet werden. Unter Fedora suchen Sie in der Gnome-Programmübersicht nach dem Programm DATENSICHERUNG.

Konfiguration

Die Konfiguration von Déjà Dup erfolgt in den drei Dialogblättern SPEICHER, ORDNER und ZEITPLAN. Im Dialogblatt SPEICHER geben Sie an, wo die Backups abgelegt werden sollen. Im Regelfall wählen Sie als Ort der Datensicherung den Eintrag LOKALER ORDNER und können dann ein beliebiges Verzeichnis auswählen, in dem Sie Dateien lesen und schreiben dürfen. Wenn Sie eine externe Festplatte oder einen USB-Stick nicht ausschließlich für Backups nutzen möchten, ist es zweckmäßig, dort ein eigenes Backup-Verzeichnis einzurichten. Als Backup-Ziel kann auch ein FTP-Verzeichnis, ein via SSH erreichbarer Server, ein WebDAV-Verzeichnis oder ein Windows- bzw. Samba-Netzwerkverzeichnis dienen.

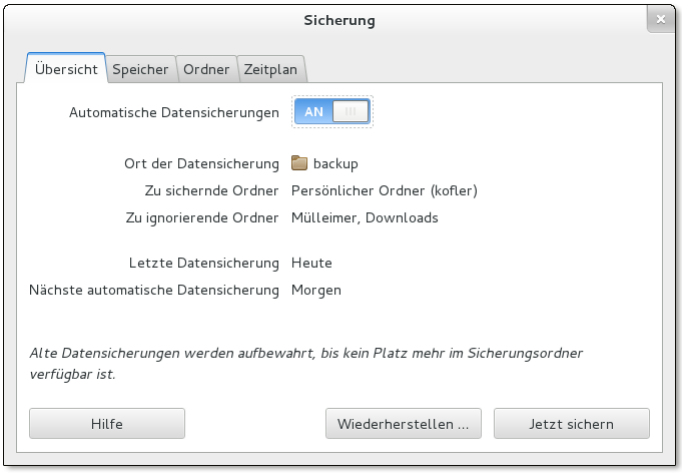


Abbildung 39.1 Backup-Konfiguration in Déjà Dup

Im Dialogblatt ORDNER geben Sie an, welche Verzeichnisse vom Backup-Programm gesichert werden sollen. Standardmäßig wird der Inhalt Ihres gesamten persönlichen Verzeichnisses mit Ausnahme des Mülleimers und des Verzeichnisses `Downloads` gesichert. Oft ist es sinnvoll, außerdem Verzeichnisse mit sehr großen Dateien von den regelmäßigen Backups auszunehmen, z. B. Videos oder den Speicherort virtueller Maschinen, falls Sie VirtualBox einsetzen.

Im Dialogblatt ZEITPLAN bestimmen Sie, ob die Backups täglich oder wöchentlich ausgeführt werden sollen. Déjà Dup wird in Zukunft immer automatisch gestartet, sobald Sie sich einloggen, und kümmert sich um die Backups. Falls das Backup-Medium gerade nicht erreichbar ist, verschiebt Déjà Dup das Backup auf später und startet die Sicherung automatisch, sobald die externe Festplatte wieder erreichbar ist. Das ist ausgesprochen bequem: Sie müssen sich nur darum kümmern, dass regelmäßig ein Backup-Medium zur Verfügung steht – um alles andere kümmert sich das Backup-Programm selbst.

Außerdem können Sie einstellen, über welchen Zeitraum das Backup-Programm sich ändernde Dateien sichern soll. Die Standardeinstellung FÜR IMMER ist am sichersten, führt aber unweigerlich dazu, dass selbst das größte Backup-Medium irgendwann voll sein wird. Mit der Einstellung MINDESTENS SECHS MONATE erreichen Sie, dass *alle* Dateien im Backup gesichert werden, wobei aber bei sich ändernden Dateien nur die Versionen der letzten sechs Monate aufbewahrt werden.

Das Dialogblatt ÜBERSICHT fasst alle Einstellungen zusammen. Dort können Sie nun wahlweise *ein* Backup manuell durchführen (Button JETZT SICHERN) oder die Option AUTOMATISCHE SICHERUNGEN aktivieren, wenn sich das Backup-Programm eigenständig um die regelmäßige Sicherung kümmern soll.

Beim ersten Backup müssen Sie außerdem angeben, ob die Backups verschlüsselt werden sollen, und falls ja, mit welchem Passwort. Beachten Sie aber, dass das Verschlüsseln eine Menge zusätzlicher CPU-Leistung erfordert!

Das erste mit Déjà Dup durchgeführte Backup dauert unverhältnismäßig lange. Das liegt daran, dass das Backup komprimiert wird. Bei weiteren Backups werden nur noch die Änderungen gespeichert, was den Vorgang stark beschleunigt.

Déjà Dup unter Ubuntu

Déjà Dup kann auch Backups im Amazon-S3-System durchführen. Unter Ubuntu steht diese Variante aber standardmäßig nicht zur Auswahl. Abhilfe: Installieren Sie das Paket `python-boto`. Eigenartig sind auch die Déjà-Dup-Voreinstellungen unter Ubuntu: Als Speicherort für die Backups ist standardmäßig ein Verzeichnis innerhalb des Ubuntu-One-Ordners vorgesehen. Das ist jedoch nur dann eine zweckmäßige Voreinstellung, wenn Sie geringe Datenmengen sichern möchten und über eine Internetverbindung mit hoher Upload-Geschwindigkeit verfügen.

Daten wiederherstellen

Mit dem Button WIEDERHERSTELLUNG stellen Sie ein vollständiges Backup wieder her. Dabei können Sie die gewünschte Backup-Version auswählen und angeben, wohin die Backup-Dateien kopiert werden sollen.

Wenn Sie eine ältere Version einer einzelnen Datei wiederherstellen möchten, ist es gar nicht notwendig, das Modul DATENSICHERUNG der Systemeinstellungen zu starten. Stattdessen klicken Sie die Datei bzw. das Verzeichnis im Dateimanager Nautilus an und führen das Kontextmenükommando AUF FRÜHERE VERSION ZURÜCKSETZEN aus. Im Dateimanager können Sie auch gelöschte Dateien wiederherstellen: Das Kommando VERSCHWUNDENE DATEIEN WIEDERHERSTELLEN öffnet einen Dialog, der alle im Backup gesicherten Dateien anzeigt, die es im aktuellen Verzeichnis *nicht* mehr gibt.

Déjà Dup basiert auf dem in Python entwickelten Backup-Script Duplicity. Das hat den Nachteil, dass die Backup-Dateien in einem sehr speziellen Format vorliegen, sodass die Daten nur mit Déjà Dup selbst oder mit Duplicity wiederhergestellt werden können.

Grsync

Eigentlich ist es übertrieben, Grsync als Backup-Werkzeug zu bezeichnen. In Wirklichkeit handelt es sich um eine simple Benutzeroberfläche zum Kommando `rsync` (siehe Abbildung 39.2). Nach der Installation verbinden Sie eine externe Festplatte oder einen USB-Stick mit Ihrem Computer, starten Grsync und kopieren den Inhalt Ihres Heimatverzeichnisses in ein Verzeichnis der externen Festplatte. Beim ersten Mal müssen dabei alle Dateien kopiert werden, in der Folge nur noch geänderte oder neue Dateien.

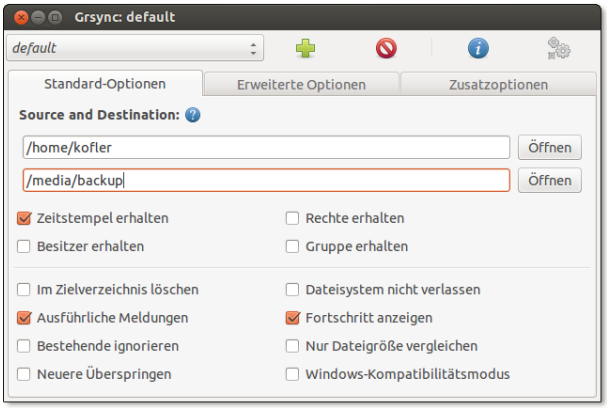


Abbildung 39.2 Verzeichnisse synchronisieren mit Grsync

Die zahlreichen Optionen können Sie im Wesentlichen so lassen, wie sie voreingestellt sind. Zwei Optionen bedürfen aber einer genaueren Erläuterung:

- IM ZIELVERZEICHNIS LÖSCHEN gibt an, ob Grsync auch Löschvorgänge synchronisieren soll. Wenn Sie nach dem ersten Backup in Ihrem Heimatverzeichnis eine Datei löschen, wird diese Datei beim nächsten Mal auch im Backup-Verzeichnis gelöscht. Wenn Ihr Backup vor versehentlichen Löschvorgängen geschützt sein soll, dürfen Sie diese Option nicht aktivieren. Das ist auch die Grundeinstellung. Wenn es Ihnen hingegen wichtig ist, dass das Backup exakt den gleichen Inhalt hat wie das zu sichernde Verzeichnis, sollten Sie die Option aktivieren.
- DATEISYSTEM NICHT VERLASSEN bedeutet, dass Grsync nur solche Dateien synchronisiert, die sich im Dateisystem des Quellverzeichnisses befinden. Zumeist ist es zweckmäßig, diese Option zu aktivieren.

Die größten Vorteile von Grsync sind die einfache Bedienung und der Umstand, dass Ihre Dateien 1:1 in ein zweites Verzeichnis kopiert werden. Sollten Sie je auf Ihr Backup zurückgreifen müssen, brauchen Sie dazu keine speziellen Werkzeuge.

Back In Time

Back In Time ist ein Backup-Programm für persönliche Daten, wobei es sowohl für KDE als auch für Gnome eine eigene Benutzeroberfläche gibt. Die meisten aktuellen Distributionen stellen fertige Back-in-Time-Pakete zur Verfügung. Nach deren Installation führen Sie zur erstmaligen Konfiguration Alt+F2 `backintime-kde` bzw. `backintime-gnome` aus.

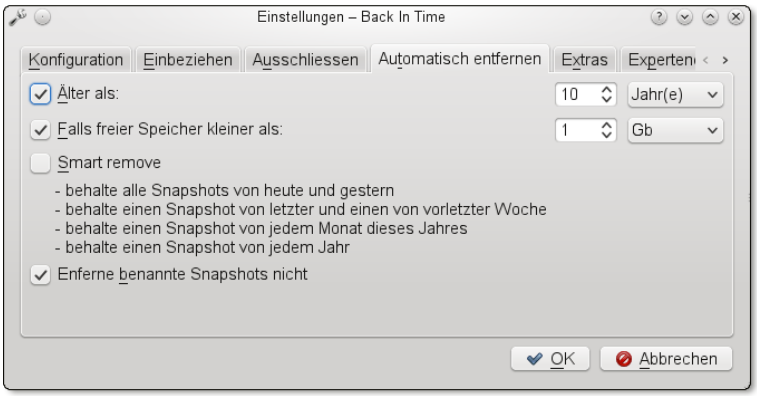


Abbildung 39.3 Konfiguration von Back In Time

Die Konfiguration erfolgt in sechs Dialogblättern:

- KONFIGURATION: Hier geben Sie an, in welchem Verzeichnis die Backups gespeichert werden sollen. Es kann sich dabei auch um einen externen Datenträger handeln, wenn dieser ständig mit Ihrem Rechner verbunden ist. Sie müssen für das Backup-Verzeichnis Schreibrechte haben.

  Außerdem stellen Sie in diesem Dialogblatt ein, wie oft die Backups durchgeführt werden sollen. Sinnvolle Einstellungen sind in der Regel STÜNDLICH oder TÄGLICH. Sie können auch den Listeneintrag DEAKTIVIERT angeben – dann müssen Sie jedes Backup manuell starten. Das ist z. B. dann sinnvoll, wenn Sie eine externe Festplatte für Ihre Backups verwenden, die Festplatte aber nicht immer an den Rechner angeschlossen ist.
- EINBEZIEHEN: Hier wählen Sie aus, welche Verzeichnisse gesichert werden sollen. Üblicherweise werden Sie hier einfach Ihr Heimatverzeichnis angeben. Sie können aber auch eine differenzierte Auswahl treffen und beispielsweise nur Ihre Verzeichnisse `Dokumente` und `Bilder` sichern.

- AUSSCHLIESSEN: Hier geben Sie an, welche Verzeichnisse und Dateimuster vom Backup ausgenommen sind, z. B. `Downloads`. Standardmäßig sieht Back In Time vor, dass versteckte Dateien und Verzeichnisse *nicht* gesichert werden. Das ist eine gefährliche Voreinstellung, weil sich gerade in versteckten Verzeichnissen oft wichtige Anwendungsdaten befinden – in `.thunderbird` z. B. Ihre E-Mails, wenn Sie Thunderbird als E-Mail-Client verwenden.
- AUTOMATISCH ENTFERNEN: Damit das Backup-Volumen nicht grenzenlos wächst, können Sie angeben, welche Backup-Daten automatisch gelöscht werden sollen. Zumeist ist SMART REMOVE eine sinnvolle Option: Damit werden Backups von gestern und heute nie angerührt. Ältere Backups werden größtenteils gelöscht, wobei aber sichergestellt wird, dass es je ein Backup für die letzten zwei Wochen, für jeden Monat des laufenden Jahres sowie für jedes vergangene Jahr gibt.
- EXTRAS und EXPERTENOPTIONEN: Hier finden Sie einige Optionen für fortgeschrittene Benutzer, die in der Regel nicht verändert werden müssen.

Nach Abschluss der Konfiguration erscheint die Benutzeroberfläche von Back In Time. Hier können Sie jederzeit manuell ein Backup starten, also außerhalb der eingestellten Backup-Periode. Außerdem können Sie vorhandenen Backups Namen geben.

Daten wiederherstellen

Die wichtigste Funktion der Benutzeroberfläche besteht aber darin, dass Sie in einem einfachen Verzeichnis-Browser zu jedem gewünschten Zeitpunkt Zugriff auf alle gesicherten Dateien haben. Mit dem Button WIEDERHERSTELLEN können Sie eine irrtümlich gelöschte oder veränderte Datei wiederherstellen. KOPIEREN kopiert die ausgewählten Dateien. Sie können die Dateien nun in einem Datei-Manager an einer beliebigen Stelle einfügen.

Standardmäßig kann Back In Time nur persönliche Dateien sichern. Wenn Sie Back In Time zur Sicherung von Systemdateien einsetzen möchten, müssen Sie es im root-Modus starten. Sowohl KDE als auch Gnome sehen entsprechende Starteinträge vor.

Interna

Hinter den Kulissen kümmert sich Cron um die automatische Durchführung der Backups durch das Kommando `backintime`. Dabei wird die Konfigurationsdatei `.config/backintime/config` ausgewertet. Die Benutzeroberfläche von Back In Time muss für die automatischen Backups nicht laufen! Die Cron-Steuerung erfolgt durch die Datei `/var/spool/cron/tabs/`*`loginname`*.

Im Backup-Verzeichnis werden alle Dateien unkomprimiert gespeichert. (Es gibt leider keine Komprimieroption.) Dateien, die sich von einem Backup zum nächsten nicht ändern, werden nur durch sogenannte *Hardlinks* miteinander verbunden, was eine Menge Platz auf der Festplatte spart. Das funktioniert allerdings nur auf Datenträgern, die derartige Links unterstützen, also nicht auf FAT-formatierten Festplatten oder Memory-Sticks!

39.2 Backups auf NAS-Geräten

Wenn Sie nur einen einzelnen Computer besitzen, ist das ideale Backup-Medium in der Regel eine externe Festplatte oder ein USB-Stick. Sobald aber mehrere Rechner im Einsatz sind, besteht oft der Wunsch nach einem zentralen Platz für Backups und nach dem Austausch gemeinsamer Daten. Ideal geeignet für diesen Zweck sind NAS-Geräte. Die Abkürzung NAS steht für *Network Attached Storage* und bezeichnet Datenspeicher, die über das Netzwerk zugänglich sind.

Auf fast allen marktüblichen NAS-Geräten laufen ein Linux-System, der Datei-Server Samba und ein Webserver, der über eine mehr oder weniger komfortable Webschnittstelle bei der Konfiguration des Geräts hilft. Viele Modelle stellen außerdem einen NFS-Server, einen FTP-Server, einen AFP-Server (für Apple), einen SSH-Server, Multimedia-Streaming-Clients, Download-Werkzeuge etc. zur Verfügung.

Backups in Netzwerkverzeichnissen

Auch wenn NAS-Systeme intern in aller Regel Linux-Rechner sind – nach außen verhalten sie sich dank Samba wie ein Windows-Rechner, der Netzwerkverzeichnisse freigibt. Und genau hier liegt das Problem: Linux-Backup-Werkzeuge setzen in der Regel voraus, dass das Ziel des Backups ein Linux- bzw. Unix-kompatibles Dateisystem ist. In einem Windows-Netzwerkverzeichnis ist es aber unmöglich, die Unix-typischen Zugriffsrechte zu speichern. Außerdem können Linux-Backup-Werkzeuge in der Regel nicht direkt auf ein Windows-Netzwerkverzeichnis zugreifen.

Es gibt verschiedene Möglichkeiten, diese Probleme zu umgehen:

- Damit Backup-Werkzeuge in ein Windows-Netzwerkverzeichnis schreiben können, muss dieses vorher in das Dateisystem des Linux-Rechners eingebunden werden. Das kann wahlweise über einen Dialog des Dateimanagers oder durch die Veränderung der Systemdatei `/etc/fstab` erfolgen.
- Um zu vermeiden, dass Linux-Zugriffsrechte beim Backup verloren gehen, können die zu sichernden Dateien verpackt werden, z. B. in ein komprimiertes `tar`-Archiv. Das auf den vorangegangenen Seiten vorgestellte Programm Déjà Dup geht auf diese Weise vor.
- Sie können versuchen, die zu sichernden Dateien direkt im Windows-Netzwerkverzeichnis zu speichern, z. B. mit dem Kommando `rsync` oder mit Grsync. Mit etwas Glück bleiben dabei sogar die Zugriffsbits der Dateien erhalten, also z. B. das Execute-Bit für ausführbare Programme oder Scripts. Das ist dann der Fall, wenn das Netzwerkverzeichnis nicht von einem Windows-Rechner, sondern von einem einigermaßen aktuellen Samba-Server zur Verfügung gestellt wird, der die POSIX-Erweiterungen unterstützt und via CIFS (Common Internet File System) weitergibt. Nach meinen Erfahrungen funktioniert das aber leider häufig nicht, weil auf vielen NAS-Geräten uralte Samba-Versionen laufen.

- Zu guter Letzt bieten manche NAS-Geräte die Möglichkeit, auch NFS-Verzeichnisse oder einen Rsync-Server als Backup-Medium zu verwenden. Je nach Gerät ist die korrekte Konfiguration aber oft schwierig.

mount bzw. /etc/fstab

Der meiner Ansicht nach zuverlässigste Weg zu einem Backup auf einem NAS-Gerät führt über ein `mount`-Kommando bzw. einen Eintrag in `/etc/fstab`. Das Ziel besteht darin, ein Verzeichnis des NAS-Geräts in den Verzeichnisbaum des lokalen Rechners einzubinden. Die Vorgehensweise ist im Detail in Abschnitt 31.7 beschrieben. Die Anleitung setzt allerdings voraus, dass das NAS-Gerät ständig läuft, das Netzwerkverzeichnis also immer zur Verfügung steht.

Netzwerkverzeichnis unter Gnome nutzen

Anstatt manuell `mount` auszuführen oder `/etc/fstab` zu ändern, können Sie das Netzwerkverzeichnis auch unter Gnome in das lokale Dateisystem einbinden. Dazu führen Sie MIT SERVER VERBINDEN aus und geben das gewünschte Verzeichnis wie im folgenden Beispiel an:

```
smb://benutzername@nas-hostname/verzeichnisname
```

Damit Sie diese Angaben in Zukunft nicht jedes Mal wiederholen müssen, setzen Sie nach dem Verbindungsaufbau mit Strg+D ein Lesezeichen. Hinter den Kulissen verwendet Gnome das GVFS (Gnome Virtual File System) für den Zugriff auf Netzwerkverzeichnisse. Die Netzwerkverzeichnisse werden im unsichtbaren Verzeichnis `.gvfs` in den Verzeichnisbaum integriert. In Nautilus sind die eingebundenen Verzeichnisse leicht zu finden und zu nutzen, das gilt aber leider nicht für alle Backup-Programme: Während Déjà Dup die Netzwerkverzeichnisse direkt im Dateiauswahldialog anzeigt, müssen Sie das Netzwerkverzeichnis bei Grsync explizit als Unterverzeichnis von `.gvfs` öffnen.

39.3 Dateien komprimieren und archivieren

In den folgenden Abschnitten stelle ich eine ganze Palette von Kommandos vor, die in unterschiedlicher Form bei der Archivierung und Sicherung von Dateien helfen: `tar`, `zip`, `rsync`, `rdiff-backup`, `rsnapshot` etc. Dieser Abschnitt beginnt mit Kommandos zum Komprimieren und Archivieren. Einen ersten Überblick gibt Tabelle 39.1.

Kommando	Bedeutung
`gzip`	komprimiert eine Datei.
`gunzip`	dekomprimiert die Datei wieder.
`bzip2`	komprimiert eine Datei (höhere Kompression als `gzip`, aber langsamer).

Tabelle 39.1 Werkzeuge zum Komprimieren und Archivieren von Dateien

Kommando	Bedeutung
bunzip2	dekomprimiert die Datei wieder.
xz	komprimiert eine Datei (höhere Kompression als bzip2, noch langsamer).
unxz	dekomprimiert die Datei wieder.
lzop	komprimiert/dekomprimiert deutlich schneller als gzip.
tar	erstellt bzw. extrahiert ein Dateiarchiv.
zip	erzeugt ein Windows-kompatibles ZIP-Archiv.
unzip	extrahiert ein ZIP-Archiv.
zipinfo	zeigt Informationen über ein ZIP-Archiv an.

Tabelle 39.1 Werkzeuge zum Komprimieren und Archivieren von Dateien (Forts.)

Dateien komprimieren (gzip, bzip2, xz, lzop)

gzip und gunzip

gzip komprimiert die als Parameter angegebenen Dateien und benennt sie in name.gz um. gunzip funktioniert in die umgekehrte Richtung. Die beiden Kommandos verwenden den sogenannten LZ77-Lempel-Ziv-Algorithmus, der sich besonders für Textdateien eignet, nicht aber für Audio- oder Video-Dateien. Die Komprimierung ist selbstverständlich verlustlos, d. h., nach dem Dekomprimieren steht die ursprüngliche Datei wieder unverändert zur Verfügung. Die folgenden Kommandos demonstrieren die Anwendung:

```
user$  ls -l filesystem.tex
... 178794  1. Aug 17:43 filesystem.tex
user$  gzip filesystem.tex
user$  ls -l filesystem.tex.gz
...  57937  1. Aug 17:43 filesystem.tex.gz
user$  gunzip filesystem.tex.gz
```

bzip2 und bunzip2

bzip2 und bunzip2 sind Alternativen zu gzip/gunzip. Der Vorteil dieser Kommandos besteht in der etwas besseren Komprimierung, der Nachteil in der etwas langsameren Ausführung. Die Dateiendung derart komprimierter Dateien ist .bz2.

```
user$  bzip2 filesystem.tex
user$  ls -l filesystem.tex.bz2
...  47105  1. Aug 17:43 filesystem.tex.bz2
user$  bunzip2 filesystem.tex.bz2
```

xz und unxz

Anstelle von gzip und bzip2 können Sie zum Komprimieren auch xz verwenden. Das Ergebnis sind in den meisten Fällen noch kleinere Dateien, das Komprimieren erfordert dafür noch mehr Zeit bzw. CPU-Ressourcen. Wenn die kleinstmögliche Komprimierung das vorrangige Ziel ist, können Sie auch das Kommando 7zr aus dem Paket p7zip ausprobieren.

lzop

Ganz anders ist die Zielsetzung von `lzop`: Dieses Komprimierkommando arbeitet *viel* schneller als alle bisher genannten Kommandos. Dafür sind die resultierenden Dateien aber vergleichsweise groß (bei meinen Tests ca. 50 Prozent größer als bei `gzip`). Der Einsatz von `lzop` ist vor allem dann empfehlenswert, wenn Sie *on the fly* mit möglichst geringer CPU-Belastung komprimieren möchten, z. B. zur Übertragung einer großen Datei über eine Netzwerkverbindung.

Im folgenden Beispielkommando wird ein Logical Volume mit `cat` ausgelesen und mit `lzop` komprimiert. Das dauert nur unwesentlich länger als das direkte Kopieren des Logical Volumes in eine Image-Datei.

```
root#  cat /dev/vg1/lv3 | lzop -c > lv3.img.lzo    (55 Sekunden)
root#  cat /dev/vg1/lv3 > lv3.img                   (50 Sekunden)
```

Komprimierte Archive erstellen (tar, zip)

tar

`tar` ist das bevorzugte Kommando, um unter Linux mehrere Dateien in einem Archiv zusammenzufassen, wobei das Archiv üblicherweise mit `gzip` oder `bzip2` komprimiert wird. `tar` war ursprünglich dazu konzipiert, Dateien auf einen Streamer zu schreiben bzw. von dort zu lesen. Da derartige Streamer nur noch relativ selten eingesetzt werden, beschreibe ich an dieser Stelle nur die Anwendung für Dateiarchive.

Das folgende Kommando fügt sämtliche Dateien aus dem Verzeichnis `buch` in die komprimierte Archivdatei `buch.tgz` ein. Kurz eine Erklärung zu den Optionsbuchstaben: `c` steht für *create*, d. h., `tar` soll ein Archiv erzeugen. `z` steht *zip*, d. h., das Archiv soll mit `gzip` komprimiert werden. `f` steht für *file*, d. h., `tar` soll eine Archivdatei erzeugen, anstatt das Archiv auf eine Streamer-Kassette zu schreiben. Den gewünschten Dateinamen geben Sie im Anschluss an die Option an. Die übliche Dateikennung für derartige Archive lautet `.tar.gz` oder kurz `.tgz`.

```
user$  tar -czf meinarchiv.tgz buch/
```

`tar -tzf` liefert ein Inhaltsverzeichnis des Archivs. Die Dateien innerhalb des Archivs sind willkürlich geordnet. Bei den meisten Distributionen ist `less` so konfiguriert, dass Sie den Archivinhalt einfach mit `less name.tgz` ansehen können.

```
user$  tar -tzf meinarchiv.tgz
linuxbuch/
linuxbuch/lanserver.tex
linuxbuch/security.tex~
```

```
linuxbuch/buch.tex
linuxbuch/u4.txt~
...
```

`tar -xzf` packt das Archiv aus und extrahiert alle enthaltenen Dateien.

```
user$  cd anderes-verzeichnis/
user$  tar -xzf meinarchiv.tgz
```

Beim folgenden Beispiel extrahiert `tar` nur `*.tex`-Dateien aus dem Archiv. Achten Sie auf die Apostrophe für das Dateimuster, um eine sofortige Auswertung durch die Shell zu vermeiden!

```
user$  tar -xzf meinarchiv.tgz '*.tex'
```

Wenn Sie Archive mit `bzip2` statt mit `gzip` komprimieren möchten, ersetzen Sie die Option `z` durch `j`.

zip

In der Unix/Linux-Welt sind `tar`-Dateien das bevorzugte Format zur Weitergabe von Dateiarchiven. Wenn Sie mit Windows-Anwendern kommunizieren, sind ZIP-Archive aber die bessere Wahl. Das folgende Kommando fügt alle als Parameter übergebenen HTML-Dateien in `meinarchiv.zip` ein:

```
user$  zip meinarchiv.zip *.html
```

Wenn Sie den Inhalt ganzer Verzeichnisse archivieren möchten, geben Sie die Option `-r` an:

```
user$  zip -r meinarchiv.zip mywebsite/
```

Den Inhalt einer ZIP-Datei sehen Sie sich mit `zipinfo` an:

```
user$  zipinfo meinarchiv.zip
Archive:  test.zip   143677915 bytes   1899 files
-rw-r--r--  2.3 unx    78039 tx defN 10-Jul-06 11:27 linuxbuch/lanserver.tex
-rw-r--r--  2.3 unx   115618 tx defN  7-Apr-05 15:58 linuxbuch/security.tex~
-rw-r--r--  2.3 unx     3899 tx defN 28-Jul-06 16:38 linuxbuch/buch.tex
-rw-r--r--  2.3 unx      752 tx defN 11-Feb-04 12:06 linuxbuch/u4.txt~
...
```

Zum Extrahieren des Archivs verwenden Sie `unzip`:

```
user$  cd anderes-verzeichnis/
user$  unzip meinarchiv.zip
```

39.4 Verzeichnisse synchronisieren (rsync)

Das Kommando `rsync` synchronisiert Verzeichnisbäume. Sie können damit im ersten Durchlauf alle Dateien von einem Verzeichnis in ein neues Verzeichnis kopieren. Bei den weiteren Durchläufen werden nur noch geänderte Dateien kopiert und (auf Wunsch) auch Löschvorgänge repliziert. `rsync` eignet sich damit ausgezeichnet, um z. B. täglich oder wöchentlich eine vollständige Kopie eines Verzeichnisses auf einer externen Festplatte zu synchronisieren.

`rsync` kann auch über Netzwerkverbindungen eingesetzt werden. Standardmäßig erfolgt die Kommunikation via `ssh`. Damit ist die Datenübertragung auch gleich verschlüsselt. Alternativ kann auch ein anderes externes Shell-Programm eingesetzt werden, oder es muss auf der Gegenseite ein `rsync`-Server konfiguriert werden.

Tabelle 39.2 zeigt die Syntax zur Angabe der Quell- und Zielverzeichnisse. Tabelle 39.3 fasst die wichtigsten Optionen zur Steuerung von `rsync` zusammen.

Schreibweise	Bedeutung
`datei1 datei2`	lokale Dateien
`verzeichnis`	lokales Verzeichnis
`host:verz`	Verzeichnis auf dem Rechner `host`
`user@host:verz`	wie oben mit SSH-Login unter dem Namen `user`
`rsync://user@host/verz`	Kommunikation mit RSYNC-Server
`rsync://user@host:port/verz`	RSYNC-Server am angegebenen Port

Tabelle 39.2 Angabe von Quell- und Zielverzeichnissen in rsync

Option	Wirkung
`-a` bzw. `--archive`	kopiert rekursiv und erhält alle Dateiinformationen.
`--delete`	löscht im Zielverzeichnis Dateien bzw. Verzeichnisse, die im Quellverzeichnis nicht mehr existieren.
`-D`	berücksichtigt auch Device- und Spezialdateien.
`--exclude=`*`muster`*	überspringt die angegebenen Dateien.
`-g` bzw. `--group`	erhält die Gruppenzugehörigkeit.
`-l` bzw. `--links`	dupliziert symbolische Links.
`-o` bzw. `--owner`	erhält die Besitzerinformationen.
`-p` bzw. `--perms`	erhält die Zugriffsrechte.

Tabelle 39.3 rsync-Optionen

Option	Wirkung
`-r` bzw. `--recursive`	kopiert rekursiv auch alle Unterverzeichnisse.
`-t` bzw. `--times`	erhält die Änderungszeit.
`-u` bzw. `--update`	ignoriert bereits vorhandene, ältere Dateien.
`-v` bzw. `--verbose`	zeigt an, was gerade passiert.
`-W` bzw. `--whole-file`	kopiert bei Änderungen die gesamte Datei.
`-z`	komprimiert die via SSH übertragenen Daten.

Tabelle 39.3 rsync-Optionen (Forts.)

Lokale Anwendung

Um ein ganzes Verzeichnis inklusive aller Unterverzeichnisse zu synchronisieren, verwenden Sie die Option `-a`, die als Kurzschreibweise für eine ganze Reihe anderer Optionen gilt (`-rlptgoD`). Die Option bewirkt eine rekursive Verarbeitung aller Unterverzeichnisse und stellt sicher, dass möglichst alle Dateiinformationen erhalten bleiben, also Besitzer, Gruppenzugehörigkeit, Zeitpunkt der letzten Änderung etc. Falls `verz2` noch nicht existiert, wird das Verzeichnis erzeugt. Anders als bei `cp` werden bereits vorhandene Dateien, die seit dem letzten Kopieren unverändert geblieben sind, nicht neuerlich kopiert.

```
user$  rsync -a verz1/ verz2/
```

Standardmäßig kopiert bzw. aktualisiert `rsync` alle neuen bzw. geänderten Dateien, löscht aber nichts. Wenn Sie möchten, dass aus `verz1` gelöschte Dateien oder Verzeichnisse auch in `verz2` gelöscht werden, geben Sie zusätzlich die Option `--delete` an. Es sollte klar sein, dass diese Option gefährlich ist: Wenn Sie versehentlich ein Verzeichnis löschen, wird genau dieses Verzeichnis beim nächsten Backup-Vorgang auch auf der Backup-Festplatte gelöscht!

Anwendung im Netzwerk

Bei der Anwendung von `rsync` zur Synchronisation von Verzeichnissen auf unterschiedlichen Rechnern müssen Sie das Quell- und das Zielverzeichnis in der Schreibweise `hostname:verzeichnis` bzw. `username@hostname:verzeichnis` angeben. Im ersten Fall verwendet `rsync` den aktuellen Benutzernamen.

Durch das folgende Kommando wird das Verzeichnis `verz1` des lokalen Benutzers `username` auf dem Rechner `saturn.sol` mit dem Verzeichnis `verz2` auf dem Rechner `mars.sol` synchronisiert. Für die Passworteingabe ist `ssh` verantwortlich. Sie müssen also das Login-Passwort des Benutzers `username` auf dem Rechner `mars.sol` eingeben.

```
username@saturn.sol$  rsync -e ssh -az verz1/ mars.sol:verz2/
username@mars.sol's password:  ******
```

`rsync` kann Dateien auch von einem entfernten Rechner auf den lokalen übertragen. Das folgende Kommando synchronisiert also in die umgekehrte Richtung:

```
username@saturn.sol$  rsync -e ssh -az mars.sol:verz2/ verz3/
username@mars.sol's password:  ******
```

Wenn `rsync` durch ein automatisches Backup-Script aufgerufen werden soll, stört natürlich die interaktive Passworteingabe. Die Lösung besteht darin, auf dem lokalen Rechner eine private Schlüsseldatei einzurichten und auf dem Partnerrechner den dazu passenden öffentlichen Schlüssel (siehe Abschnitt 34.3). Wenn Sie bei der Erzeugung der Schlüssel auf die sogenannte *Passphrase* verzichten, ist nun ein SSH-Login ohne Passwort möglich. Aus Sicherheitsgründen sollten Sie für das Backup-Script einen eigenen Account vorsehen.

rsync-Server

Neben der hier vorgestellten Anwendung von `rsync` in Kombination mit SSH besteht auch die Möglichkeit, dass das lokale `rsync`-Kommando mit einem `rsync`-Server auf dem entfernten Rechner kommuniziert. Das setzt voraus, dass auf dem Partnerrechner ein `rsync`-Server eingerichtet wurde. Dessen Konfiguration erfolgt durch die Datei `/etc/rsyncd.conf`. Die Kommunikation zwischen dem `rsync`-Client und dem `rsync`-Server erfolgt dann über den Port 873. Dieser Port darf daher nicht durch eine Firewall blockiert sein.

In der Praxis ist die Konfiguration eines `rsync`-Servers zumeist nur empfehlenswert, wenn der Server regelmäßig von verschiedenen Clients gespiegelt wird, also als Mirror-Server dient:

http://unix.stackexchange.com/questions/26182
http://serverfault.com/questions/100707/rsync-daemon-is-it-really-useful

39.5 Inkrementelle Backups (rdiff-backup)

Eine interessante Alternative zu `rsync` ist das Kommando `rdiff-backup`. Der wichtigste Unterschied zu `rsync` besteht darin, dass `rdiff-backup` bei veränderten Dateien auch die alte Version im Backup-Verzeichnis archiviert. Um Platz zu sparen, können statt einer Kopie der betreffenden Datei auch nur die Änderungen gespeichert werden, optional in komprimierter Form. `rdiff-backup` liefert also ohne viel Mühe ein inkrementelles Backup, aus dem Sie auch ältere Versionen einer Datei wiederherstellen können. Im Prinzip bietet `rdiff-backup` dieselben Funktionen wie die »Time Machine« von Apples OS X – nur ohne spektakuläre Benutzeroberfläche.

Backups durchführen

In der einfachsten Form wenden Sie `rdiff-backup` auf zwei lokale Verzeichnisse an. Wenn das Zielverzeichnis noch nicht existiert, wird es erzeugt.

```
root#  rdiff-backup /home /home-backup
```

`rdiff-backup` erzeugt im Backup-Verzeichnis das Unterverzeichnis `rdiff-backup-data`. Darin speichert es diverse statistische Daten und Statusinformationen. Außerdem

enthält das Verzeichnis `increments` alte Versionen von Dateien, die sich mittlerweile geändert haben oder die gelöscht wurden. Dabei werden nur die Änderungen gespeichert (`.diff`) und zusätzlich komprimiert. Außerdem wird in den Dateinamen das Datum der letzten Version integriert. Daraus ergeben sich dann unübersichtliche Dateinamen in der Form `dateiname.2010-04-03T08:37:58+02:00.diff.gz`.

Zugriff auf Backups

Wenn Sie auf das Backup zurückgreifen möchten, enthält `/home-backup` den Zustand des `/home`-Verzeichnisses zum Zeitpunkt des letzten Backups mit Ausnahme des `rdiff-backup-data`-Verzeichnisses genau so, als hätten Sie das Backup mit `cp -a` oder `rsync -a --delete` ausgeführt. Der Zugriff auf das letzte Backup ist also ganz einfach. Natürlich können Sie das Backup auch mit `rdiff-backup` wiederherstellen. Dazu verwenden Sie die Option `-r` und die Zeitangabe `now`. Das folgende Kommando stellt das Backup probeweise in einem temporären Verzeichnis wieder her:

```
root#  rdiff-backup -r now /home-backhup /tmp/home-aktuell
```

Wenn Sie auf eine ältere Version einer Datei bzw. auf eine mittlerweile gelöschte Datei zugreifen möchten, wird es komplizierter: Sie müssen der Reihe nach alle `.diff`-Dateien anwenden (die neueste zuerst), bis Sie den gewünschten Zeitpunkt in der Vergangenheit wiederhergestellt haben. Natürlich müssen Sie das nicht manuell tun – `rdiff-backup` hilft Ihnen dabei. Das folgende Kommando stellt den Zustand des `/home`-Verzeichnisses so wieder her, wie er vor zehn Tagen war:

```
root#  rdiff-backup -r 10D /home-backup/ /tmp/home-historisch
```

Den Backup-Zeitpunkt können Sie wahlweise absolut (z. B. `2013-12-31`) oder relativ in Stunden (`h`), Tagen (`D`), Wochen (`W`) etc. angeben – siehe auch `man rdiff-backup` im Abschnitt `TIME FORMATS`. Beachten Sie, dass die Wiederherstellung alter Dateien mit zunehmender Versionsanzahl einen erheblichen CPU-Aufwand verursacht und entsprechend langsam ist!

Oft wollen Sie nur eine einzelne Datei oder ein Unterverzeichnis in einer alten Version wiederherstellen. Dabei können Sie auch eine gar nicht mehr existierende Datei bzw. ein mittlerweile gelöschtes Verzeichnis angeben:

```
root#  rdiff-backup -r 10D /home-backup/datei  datei-historisch
root#  rdiff-backup -r 10D /home-backup/verz/  verz-historisch
```

Alte Backups löschen

Wenn Sie `rdiff-backup` regelmäßig ausführen, wächst das Backup-Verzeichnis im Laufe der Zeit immer stärker an. Um alle Backup-Dateien zu löschen, die älter als vier Monate sind, gehen Sie so vor:

```
root#  rdiff-backup --remove-older-than 4M --force /home-backup/
```

Statt eines konkreten Zeitpunkts können Sie auch angeben, wie viele Backup-Versionen maximal archiviert bleiben sollen. Das folgende Kommando reduziert die Backup-Versionen auf drei:

```
root#  rdiff-backup --remove-older-than 3B --force /home-backup/
```

Netzwerk-Backup

In allen bisherigen Beispielen bin ich davon ausgegangen, dass sich das Quell- und das Zielverzeichnis im lokalen Dateisystem befinden. `rdiff-backup` kann aber über das Netzwerk auch auf externe Verzeichnisse zugreifen. Anders als bei `rsync` muss dazu `rdiff-backup` auch auf dem externen Rechner installiert sein! Die Kommunikation erfolgt über SSH. Eine spezielle Konfiguration von `rdiff-backup` ist nicht erforderlich.

Bei der Angabe externer Verzeichnisse gilt nahezu dieselbe Syntax wie bei `rsync`. Der einzige Unterschied besteht darin, dass nach dem Hostnamen *zwei* Doppelpunkte angegeben werden müssen:

```
root#  rdiff-backup user@firma-abc.de::/home /home-backup
```

Noch mehr Details und Beispiele zum Umgang mit `rdiff-backup` bietet die folgende Webseite:

http://www.nongnu.org/rdiff-backup

Duplicity

Wenn Ihnen die Idee von `rdiff-backup` zusagt, Sie sich aber außerdem noch die Verschlüsselung des Backups sowie ein Upload via SSH oder FTP auf einen externen Server wünschen, lohnt sich vielleicht ein Blick auf das Python-Programm Duplicity. Es ist ähnlich wie `rdiff-backup` zu bedienen, erzeugt allerdings `tar`-Archive. Duplicity befindet sich allerdings nun schon seit mehreren Jahren im Beta-Stadium. Nichtsdestotrotz dient es als Basis für die Backup-Benutzeroberfläche Déjà Dup, die ich Ihnen am Beginn dieses Kapitels vorgestellt habe.

http://duplicity.nongnu.org

39.6 Inkrementelle Backups (rsnapshot)

Auch das Perl-Script `rsnapshot` aus dem gleichnamigen Paket baut auf `rsync` auf. Im Unterschied zum gerade beschriebenen Kommando `rdiff-backup` verwendet es Hardlinks, um auf bereits gesicherte Dateien früherer Backups zurückzugreifen. Das macht den Zugriff auf ältere Backup-Versionen (»Snapshots«) einfacher als bei `rdiff-backup`. Eine Komprimierung der Backups ist hingegen nicht vorgesehen.

`rsnapshot` ist dahingehend konzipiert, dass das Script regelmäßig automatisch ausgeführt wird. `rsnapshot` sichert bei entsprechender Konfiguration sowohl lokale Verzeichnisse als auch via SSH Verzeichnisse von anderen Rechnern im lokalen Netzwerk. Alle Backups werden auf dem lokalen Rechner gespeichert, auf dem `rsnapshot` ausgeführt wird. Dieser Denkansatz ist genau umgekehrt als bei vielen anderen

Backup-Tools: `rsnapshot` ist nicht dazu gedacht, ein Backup der lokalen Dateien auf einem anderen Rechner zu speichern. Vielmehr sichert das Kommando den die Daten mehrerer via SSH oder RSYNC erreichbarer Rechner im lokalen Dateisystem.

Konfiguration

Anstatt an `rsnapshot` zahlreiche Optionen zu übergeben, wird das Kommando durch die Konfigurationsdatei `/etc/rsnapshot.conf` gesteuert. Für diese Datei gelten zwei wichtige Syntaxregeln: Verzeichnisse müssen mit einem Slash enden (also `/verzeichnis/`, nicht `/verzeichnis`), und die Elemente der Konfigurationsdatei müssen durch Tabulatorzeichen (nicht Leerzeichen) voneinander getrennt werden!

Für erste Experimente können Sie die zusammen mit `rsnapshot` mitgelieferte Konfigurationsdatei bis auf wenige Details unverändert lassen. Die drei wichtigsten Parameter, die Sie kennen und gegebenenfalls selbst einstellen müssen, sind `snapshot_root`, `backup` und `interval`.

snapshot_root

`snapshot_root` gibt an, in welchem Verzeichnis die Backups gespeichert werden sollen. Standardmäßig kommt das Verzeichnis `/var/cache/rsnapshot` zum Einsatz, das bei der Installation von `rsnapshot` automatisch eingerichtet wurde.

backup

`backup` gibt an, welches Verzeichnis wo gesichert werden soll. `backup` kann mehrfach jeweils in einer eigenen Zeile angegeben werden, um mehrere Verzeichnisse an unterschiedlichen Orten zu sichern. Für Backups innerhalb des lokalen Dateisystems sehen die `backup`-Einstellungen wie folgt aus:

```
# in /etc/rsnapshot.conf
...
backup  /home/    localhost/
backup  /etc/     localhost/
```

Um ein Verzeichnis `/home/user/Mail` des externen, via SSH erreichbaren Rechners `mars.sol` zu sichern, müssen Sie in der bereits vorhandenen Zeile `cmd_ssh` das Kommentarzeichen # entfernen. In der `backup`-Zeile geben Sie den Login-Namen, den Hostnamen sowie das gesamte zu sichernde Verzeichnis an. Damit das funktioniert, müssen Sie vor dem ersten Backup einen mit `root`-Rechten eingerichteten SSH-Schlüssel ohne Passphrase in die Datei `/home/user/.ssh/authorized_keys` des Rechners `mars.sol` kopieren (siehe Abschnitt 34.3). Vorsicht: Die auf dem lokalen Rechner im Verzeichnis `/root/.ssh` gespeicherte Schlüsseldatei darf nicht in falsche Hände geraten!

```
# in /etc/rsnapshot.conf
...
cmd_ssh /usr/bin/ssh
...
backup  user@mars.sol:/home/user/Mail/  mars.sol/
```

Optional besteht die Möglichkeit, während des Backups einen LVM-Snapshot durchzuführen oder Scripts auszuführen, bestimmte Dateimuster vom Backup auszuschließen etc. Details können Sie in der mitgelieferten Konfigurationsdatei sowie in der `man`-Seite zu `rsnapshot` nachlesen.

interval

`interval` definiert, wie viele Backup-Versionen für ein bestimmtes Zeitintervall gespeichert werden sollen. Die Standardeinstellungen sehen so aus:

```
# in /etc/rsnapshot.conf
...
interval        hourly  6
interval        daily   7
interval        weekly  4
#interval       monthly 3
```

Das bedeutet, dass von Backups, die durch das Kommando `rsnapshot hourly` ausgeführt werden, sechs Versionen gespeichert werden. Des Weiteren werden sieben Backups von `rsnapshot daily` archiviert sowie vier Backups von `rsnapshot weekly`. Das Intervall `monthly` ist standardmäßig nicht definiert.

Die Einstellung `interval hourly 6` ist dann zweckmäßig, wenn das Kommando `rsnapshot hourly` nicht stündlich, sondern nur alle vier Stunden ausgeführt wird, wie dies in `/etc/cron.d/rsnapshot` vorgesehen ist. Wenn Sie `rsnapshot hourly` hingegen wirklich jede Stunde ausführen möchten, wäre die Einstellung `interval hourly 24` zweckmäßiger.

Sie können nach Bedarf beliebige weitere Intervalle definieren. `rsnapshot` speichert die Backups für jedes Intervall in einem jeweils eigenen Verzeichnis und verlinkt nicht geänderte Backups nur innerhalb des Verzeichnisses eines Intervalls. Das bedeutet, dass der Speicherbedarf mit jedem zusätzlichen Intervall stark steigt.

Manueller Aufruf

`rsnapshot` kann manuell aufgerufen werden. Das erfordert `root`-Rechte. Als Parameter müssen Sie dabei ein in der Konfigurationsdatei mit `interval` definiertes Zeitintervall angeben:

```
root#  rsnapshot daily
```

Nach dem Backup finden Sie die gesicherten Daten im folgenden Verzeichnis:

```
/var/cache/rsnapshot/<interval.n>/<hostname>/<verzeichnis>
```

Dabei gibt `interval` das Intervall an, standardmäßig `hourly`, `daily`, `weekly` oder `monthly`. `n` gibt die Backup-Version an: 0 für das aktuellste Backup, 1 für die letzte Version, 2 für die vorletzte Version etc. `hostname` gibt an, von welchem Rechner die gesicherten Daten stammen, wobei `localhost` den lokalen Rechner bezeichnet.

Das aktuellste stündliche Backup des lokalen Verzeichnisses `/etc` befindet sich also im folgenden Verzeichnis:

```
/var/cache/rsnapshot/hourly.0/localhost/etc
```

Das aktuellste monatliche Backup des Verzeichnisses `/home/user/Mail` des Servers `mars.sol` befindet sich in diesem Verzeichnis:

```
/var/cache/rsnapshot/monthly.0/mars.sol/home/user/Mail
```

Automatischer Aufruf

Um die Backups zu automatisieren, ist ein regelmäßiger Aufruf von `rsnapshot` durch die Cron-Konfigurationsdatei `/etc/cron.d/rsnapshot` vorgesehen. Sie müssen dazu nur die Kommentarzeilen vor den vier bereits vorgesehenen Cron-Zeilen entfernen:

```
# /etc/cron.d/rsnapshot
0 */4         * * *           root    /usr/bin/rsnapshot hourly
30 3          * * *           root    /usr/bin/rsnapshot daily
0  3          * * 1           root    /usr/bin/rsnapshot weekly
30 2          1 * *           root    /usr/bin/rsnapshot monthly
```

Damit wird `rsnapshot` alle vier Stunden, also um 0:00, 4:00, 8:00 etc., täglich um 3:30, wöchentlich montags um 3:00 sowie monatlich am ersten Tag des Monats um 2:30 mit den Parametern `hourly`, `daily`, `weekly` und `monthly` ausgeführt. Natürlich können Sie die Zeiten nach eigenem Gutdünken variieren. Beachten Sie, dass alle in der Cron-Datei verwendeten Zeitintervalle auch in `/etc/rsnapshot.conf` definiert sein müssen! Für das Intervall `monthly` ist das standardmäßig nicht der Fall.

39.7 Backup-Scripts

Im letzten Abschnitt dieses Kapitels stehen praktische Beispiele im Vordergrund.

rsync mit Cron automatisieren

Das folgende Script synchronisiert den Inhalt des lokalen Verzeichnisses `data` mit dem gleichnamigen Verzeichnis auf einer externen Festplatte mit dem Namen `backup`. Das Script testet, ob die externe Festplatte zur Verfügung steht. Sollte das nicht der Fall sein, wird auf die Durchführung des Backups verzichtet.

```
#!/bin/bash
if [ -d /media/backup/ ]; then
  rsync -avW --delete /home/kofler/data /media/backup/
fi
```

In aller Regel werden Sie Backup-Scripts regelmäßig automatisch ausführen. Dazu richten Sie am einfachsten einen Cron-Job ein. Am einfachsten ist es, das Script direkt in einem Cron-Verzeichnis zu speichern, z. B. unter dem Dateinamen `/etc/cron.daily/mybackup`. Achten Sie darauf, dass der Dateiname keinen Punkt enthalten darf und dass die Datei ausführbar sein muss (`chmod a+x`).

Die andere Variante besteht darin, dass Sie das Backup-Script in einem beliebigen Verzeichnis speichern, z. B. in `/etc/myscripts`. Zum automatischen Aufruf des Scripts richten Sie eine neue Datei in `/etc/cron.d` ein, z. B. nach diesem Muster:

```
# Datei /etc/cron.d/mybackup
15 2 * * * root /etc/myscripts/mybackup
```

Das Backup-Script `mybackup` wird damit täglich um 2:15 ausgeführt.

Tägliche und monatliche Sicherheitskopien

Das folgende Script erzeugt ein komprimiertes `tar`-Archiv des Verzeichnisses `data`. Das Archiv wird unter zwei Dateinamen gespeichert: `mydata-day-`*`dd`*`.tar.gz` und `mydata-month-`*`mm`*`.tar.gz`. Dabei gibt `dd` den Tag (01 bis 31) und *`mm`* den Monat an (01 bis 12). Wenn das Script täglich ausgeführt wird, haben Sie mit der Zeit 43 Backup-Versionen, die den Zustand des Backup-Verzeichnisses für die letzten 28 bis 31 Tage sowie für die letzten 12 Monate widerspiegeln.

```
#!/bin/bash
fname1=/backup/mydata-day-$(date "+%d").tar.gz
fname2=/backup/mydata-month-$(date "+%m").tar.gz
tar czf $fname1 /home/kofler/data
cp $fname1 $fname2
chmod 600 $fname1 $fname2
```

Backups mit LVM

Wenn sich Dateien während der Durchführung eines Backups ändern, ist die resultierende Sicherheitskopie inkonsistent. Nicht immer ist es aber möglich, für das Backup die betreffenden Programme oder Server-Dienste zu stoppen. Eine mögliche Lösung für dieses Problem besteht darin, zu Beginn des Backups einen LVM-Snapshot zu erstellen und diesen als Basis für das Backup zu verwenden. Das setzt natürlich voraus, dass sich das Verzeichnis mit den zu sichernden Daten in einem Dateisystem befindet, das in einem Logical Volume gespeichert wird (und nicht direkt auf einer Festplattenpartition).

Zum Erzeugen eines Snapshots verwenden Sie das Kommando `lvcreate` mit der Option `-s`. Mit `-L` geben Sie an, wie viele Daten sich während der Lebensdauer des Snapshots – also während der Zeit, in der das Backup durchgeführt wird – maximal verändern dürfen. Im LVM-Speicherpool (also im PV) muss dafür ausreichend freier Platz sein. Die erforderliche Größe des Pufferspeichers ist anfänglich schwer abzuschätzen. Wenn Sie mit dem Backup fertig sind, können Sie mit `lvdisplay` feststellen, wie viel Prozent des Puffers bis jetzt beansprucht wurden.

Beim folgenden Beispiel-Script gehe ich davon aus, dass sich das Verzeichnis `/home` im LV `/dev/vg1/myhome` befindet. Um vom `/home`-Verzeichnis ein konsistentes Backup durchzuführen, während dessen sich keine Dateien ändern, erstellen Sie mit `lvcreate` den Snapshot `homesnap`. Als Pufferspeicher sehen Sie 2 GByte vor.

Diesen Snapshot binden Sie beim Verzeichnis `/var/homesnap` in den Verzeichnisbaum ein und verwenden ihn anschließend als Datenquelle für Ihr Backup-Kommando oder -Script. Zuletzt lösen Sie `homesnap` wieder aus dem Dateisystem und entfernen den Snapshot mit `lvremove`. Die Option `-f` unterbindet die Rückfrage, ob Sie das wirklich wollen.

```
#!/bin/bash
mkdir -p /var/homesnap
lvcreate -s -L 2G -n homesnap /dev/vg1/home
mount -t ext4 /dev/vg1/homesnap /var/homesnap
tar czf /backup/mybackup.tgz /var/homesnap
lvdisplay /dev/vg1/homesnap > /tmp/backup.log
umount /var/homesnap
lvremove -f /dev/vg1/homesnap
```

Das Kommando `lvdisplay` dient zur Kontrolle, ob Sie den Pufferspeicher für den LVM-Snapshot richtig dimensioniert haben:

```
root#  cat /var/homesnap
  ...
  COW-table size         2.00 GB
  Allocated to snapshot  5.23%
```

Im obigen Beispiel wurden also nur fünf Prozent des Pufferspeichers beansprucht. Das ist natürlich keine Garantie dafür, dass das beim nächsten Mal auch so sein wird. Vielleicht verursacht dann gerade irgendein Benutzer oder ein Prozess große Änderungen im `/home`-Verzeichnis.

Logical Volume als Image auslesen

Auch wenn Sie Logical Volumes verwenden, um darin den Datenträger einer virtuellen Maschine zu speichern (siehe Kapitel 43), können Sie LVM-Snapshots verwenden, um das Logical Volume sicher in eine komprimierte Image-Datei zu kopieren. Das folgende Script benennt zuerst das eventuell schon vorhandene Backup `image.lzo` in `old-image.lzo` um. Anschließend erstellt es den Snapshot `snap` des Logical Volumes `/dev/vg1/lv1`, das den virtuellen Datenträger enthält.

Das Image wird nun mit `cat` ausgelesen und mit `lzop` komprimiert. Dank `ionice -c 3` wird dieses IO- und CPU-intensive Kommando ausgeführt, ohne alle anderen laufenden Prozesse allzu stark zu beeinträchtigen.

Das komprimierte Image wird anschließend mit `curl` auf einen Backup-Server hochgeladen. Die Option `--limit-rate` limitiert dabei die Übertragungsgeschwindigkeit. Das stellt sicher, dass die Netzwerkkapazitäten des Servers nicht vollständig durch das Backup-Script blockiert werden.

```
#!/bin/bash
mv /backup/image.lzo /backup/old-image.lzo
lvcreate -s -L 2G -n snap /dev/vg1/lv1
ionice -c 3 cat /dev/vg1/snap | lzop -c > /backup/image.lzo
lvremove -f /dev/vg1/snap

# Image per FTP auf einen Backup-Server hochladen
pw=u12345:2n34jkj546wqdsr
ftp=u12345.backup-server.de
curl --limit-rate 8m -T /backup/image.lzo -u $pw ftp://$ftp/image.lzo
```

Tartarus

Wozu das Rad neu erfinden, wenn es im Internet fertige Backup-Scripts gibt? Eine Internet-Suche nach *linux backup script* liefert unzählige Ergebnisse. Das Problem besteht allerdings darin, die Spreu vom Weizen zu trennen. Viele Scripts sind für eine ganz spezifische Aufgabenstellung konzipiert und kaum allgemeingültig verwendbar. Aber zum Glück gibt es auch positive Ausnahmen: Bei meiner Arbeit bewährt hat sich beispielsweise das `bash`-Script Tartarus. Es verpackt in ca. 600 Zeilen Code die folgenden Funktionen:

- `tar`-Archivformat
- Speicherung der Backups wahlweise im lokalen Dateisystem, auf einem FTP-Server oder über ein eigenes Kommando (z. B. mit `ssh`)
- inkrementelle Backups (optional)
- LVM-Snapshots (optional)
- Verschlüsselung mit GPG (optional)

Tartarus wird unter anderem vom Webhosting- und Root-Server-Provider Hetzner empfohlen. Sie finden das Script sowie eine brauchbare Dokumentation hier:

http://wertarbyte.de/tartarus.shtml

Kapitel 40
Firewalls

Die Überschrift für dieses Kapitel ist ein wenig plakativ – ganz einfach deswegen, weil fast jeder etwas mit dem Begriff »Firewall« anfangen kann. Tatsächlich geht es in diesem Kapitel aber nicht nur darum, einen Filter für Netzwerkpakete einzurichten, sondern auch um Netzwerkgrundlagen und um andere Techniken zur Absicherung. Daher lernen Sie in diesem Kapitel auch einige elementare Werkzeuge kennen, um den aktuellen Zustand des Netzwerks zu analysieren, z. B., um offene Ports zu finden. Ein Abschnitt zur TCP-Wrapper-Bibliothek zeigt zudem, wie der Zugriff auf bestimmte Netzwerkdienste durch einfache Regeln eingeschränkt werden kann.

40.1 Netzwerkgrundlagen und -analyse

Bevor Sie Ihren Rechner absichern können, müssen Sie eine Vorstellung davon gewinnen, wie die Netzwerkdienste funktionieren, welche Dienste gerade laufen, welche Ports offen sind etc. Dieser Abschnitt beschäftigt sich daher mit TCP/IP-Grundlagen und beschreibt einige Programme, um den aktuellen Netzwerkstatus zu analysieren und beispielsweise alle gerade aktiven Netzwerkverbindungen aufzulisten. Vorweg fasst Tabelle 40.1 die wichtigsten Abkürzungen zusammen.

Abkürzung	Bedeutung
DNS	Domain Name Service
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
NFS	Network File System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Tabelle 40.1 Netzwerk-Glossar

Internet Protocol

Praktisch alle gängigen Netzwerkdienste basieren auf IP-Paketen. Wenn beispielsweise ein Internetbenutzer per FTP auf Ihren Rechner zugreifen möchte, startet er dazu auf seinem Rechner einen FTP-Client. Dieser sendet ganz spezielle IP-Pakete an Ihren Rechner. Wenn auf Ihrem Rechner ein FTP-Server installiert ist, erhält dieser die IP-Pakete und reagiert auf die Anfrage, indem er selbst IP-Pakete an den Client zurücksendet.

Neben den eigentlichen Daten enthalten IP-Pakete unter anderem vier wesentliche Informationen: die Absender-IP-Adresse, den Absender-Port, die Zieladresse und den Ziel-Port. Diese Daten geben an, woher das Paket kommt und wohin es gehen soll.

IP-Adressen und -Ports

Die Bedeutung der IP-Adresse sollte klar sein (siehe auch Kapitel 29). IP-Ports werden dazu verwendet, um verschiedene Dienste zu identifizieren. Beispielsweise wird zur Anforderung eines WWW-Dokuments üblicherweise der Port 80 verwendet. Bei Port-Nummern handelt es sich um 16-Bit-Zahlen. Die Ports bis 1024 gelten als privilegiert und sind für Server-Dienste reserviert, z. B. für den HTTP-Server. Die verbleibenden Ports können an sich von Clients eingesetzt werden, allerdings gibt es auch hier eine Reihe von Nummern, die nicht verwendet werden sollten, weil sie oft schon für bestimmte Zwecke reserviert sind.

Zu vielen IP-Port-Nummern sind in `/etc/services` Alias-Namen definiert. Tabelle 40.2 führt die wichtigsten Port-Nummern mit den üblicherweise gültigen Namen und einer kurzen Erklärung auf.

Name	Port	Funktion
`ftp`	20, 21	FTP
`ssh`	22	SSH
`telnet`	23	Telnet
`smtp`	25	E-Mail
`domain`	53	DNS
`bootps` und `bootpc`	67, 68	DHCP
`http`	80	Web
`pop3`	110	E-Mail
`portmap`	111	Portmap (für NFS)
`ntp`	123	Zeit (Network Time Protocol)
`netbios-ns`	137	Microsoft/NetBIOS Name Service
`netbios-dgm`	138	Microsoft/NetBIOS Datagram Service

Tabelle 40.2 Wichtige IP-Ports

Name	Port	Funktion
netbios-ssn	139	Microsoft File Sharing (SMB, Samba)
imap	143	E-Mail
ldap	389	LDAP
–	427	Apple Filing Protocol (AFP)
https	443	Web (verschlüsselt)
microsoft-ds	445	CIFS-Dateisystem (SMB, Samba)
printer	515	Drucken mit LPD/LPR
–	548	Apple Filing Protocol (AFP)
ipp	631	Drucken mit IPP/CUPS
rmi	1099	Remote Method Incovation (Java)
pptp	1723	PPTP/VPN
nfs	2049	NFS
–	3128	Squid (Web-Proxy)
mysql	3306	MySQL Datenbank-Server
–	5353	Netzkonfiguration durch Zeroconf/Bonjour
–	5999–6003	X-Display
–	9100	HP-JetDirect-Netzwerkdrucker

Tabelle 40.2 Wichtige IP-Ports (Forts.)

IP-Protokolle

Es gibt unterschiedliche Protokolle für IP-Pakete: Die meisten Internetdienste verwenden TCP. Dieses Protokoll verlangt eine Bestätigung des Empfangs. Es gibt aber auch Protokolle, die keine derartige Bestätigung erwarten, nämlich ICMP (wird z. B. von `ping` verwendet) und UDP (wird z. B. von DNS und NFS verwendet).

IP-Paketfilter

IP-Pakete können durch lokale Programme erzeugt werden oder von außen – also über Netzwerk-Schnittstellen – in den Rechner kommen. Der Kernel muss nun entscheiden, was mit den Paketen passieren soll. Er kann die Pakete verwerfen oder an laufende Programme bzw. an andere Schnittstellen weiterleiten. Dabei können alle oben beschriebenen Paketmerkmale als mögliche Entscheidungskriterien dienen. Um einen Paketfilter zu realisieren, brauchen Sie also eine Möglichkeit, dem Kernel Regeln mitzuteilen, wie er mit bestimmten IP-Paketen verfahren soll. Dazu dient seit Kernel 2.4 das Kommando `iptables`, dessen Anwendung Thema des Abschnitts 40.5 ist.

Aktive Netzwerk-Ports ermitteln

Das Funktionsprinzip der meisten Netzwerkdienste sieht so aus, dass diese einen bestimmten Port überwachen. Treffen für diesen Port IP-Pakete ein, kümmert sich der Dienst um deren Verarbeitung und Beantwortung. Pakete, die an nicht überwachte Ports adressiert sind, werden einfach ignoriert und stellen insofern auch keine Gefahr dar. Um die Gefährdung eines Rechners abzuschätzen, ist es daher zweckmäßig, eine Liste der überwachten Ports zu ermitteln. Umgekehrt wird auch ein Angreifer als Erstes versuchen, die aktiven Ports herauszufinden.

netstat

Um festzustellen, welche Netzwerkaktivitäten auf dem lokalen Rechner stattfinden, ist das Kommando `netstat` ein großes Hilfsmittel. Je nachdem, mit welchen Optionen es aufgerufen wird, liefert es eine Fülle unterschiedlicher Informationen.

Das erste Beispiel auf dem Server `mars` zeigt alle aktiven Verbindungen (`ESTAB`) bzw. überwachten Ports (`LISTEN`). Kurz zu den Optionen: `a` zeigt auch nichtaktive Ports, `tu` schränkt die Ausgabe auf die Protokolle TCP und UDP ein, `pe` zeigt zusätzlich die Prozessnummer und den Account, unter dem das Programm ausgeführt wird. Die Ausgabe wurde aus Platzgründen gekürzt.

```
root#  netstat -atupe
Active Internet connections (servers and established)
Proto Local Address           Foreign Addr   State    User     PID/Prog name
tcp   *:nfs                   *:*            LISTEN   root     -
tcp   *:54980                 *:*            LISTEN   root     -
tcp   *:ldap                  *:*            LISTEN   root     5842/slapd
tcp   *:3142                  *:*            LISTEN   root     5904/perl
tcp   localhost:mysql         *:*            LISTEN   mysql    5785/mysqld
...
tcp6  [::]:ssh                [::]:*         LISTEN   root     5559/sshd
tcp6  mars.sol:ssh            merkur.so...   ESTAB    root     7729/0
udp   *:nfs                   *:*                     root     -
udp   mars.local:netbios-ns   *:*                     root     6231/nmbd
udp   mars.sol:netbios-ns     *:*                     root     6231/nmbd
udp   *:netbios-ns            *:*                     root     6231/nmbd
udp   mars.local:netbios-dgm  *:*                     root     6231/nmbd
udp   mars.sol:netbios-dgm    *:*                     root     6231/nmbd
udp   *:netbios-dgm           *:*                     root     6231/nmbd
udp   *:domain                *:*                     root     5537/dnsmasq
udp   *:55350                 *:*                     avahi    5604/avahi-...
...
```

Eine kurze Zusammenfassung des obigen Ergebnisses: Auf dem Testrechner laufen unter anderem ein Samba-Server, ein NFS-Server, Kerberos, LDAP, Dnsmasq, CUPS, MySQL und ein SSH-Server. Wenn der Rechner so ohne Firewall direkt mit dem Internet verbunden ist, freut sich jeder potenzielle Angreifer. Es gibt eine Menge Programme, bei denen sich vielleicht irgendwelche Sicherheitslücken finden lassen.

Das folgende Kommando liefert die Liste der aktiven TPC- und UDP-Verbindungen samt Benutzer- und Prozessname:

```
root#  netstat -tuep
Active Internet connections (w/o servers)
Proto Local Address    Foreign Address   State       User     PID/Program name
tcp   localhost:57450  localhost:ldap    ESTABLISHED root     6233/smbd
tcp   localhost:ldap   localhost:57450   ESTABLISHED openldap 5842/slapd
tcp6  mars.sol:ssh     merkur.sol:45368  ESTABLISHED root     7729/0
```

lsof

Wenn Sie herausfinden möchten, welche Programme TCP- bzw. UDP-Ports nutzen, hilft auch das Kommando `lsof`. In der Form `lsof -i [protokoll]@[hostname][:port]` liefert es eine Liste von Prozessen, die die angegebenen Netzwerkressourcen nutzen. Die beiden folgenden Kommandos zeigen alle Prozesse, die das Protokoll UDP bzw. den Port 22 nutzen:

```
root#  lsof -i udp
ntpd      3696     ntp   16u  IPv4   9026       UDP *:ntp
ntpd      3696     ntp   17u  IPv6   9028       UDP *:ntp
ntpd      3696     ntp   18u  IPv6   9031       UDP ip6-localhost:ntp
portmap   4745  daemon    3u  IPv4  12931       UDP *:sunrpc
rpc.statd 4764   statd    5u  IPv4  12962       UDP *:700
rpc.statd 4764   statd    7u  IPv4  12970       UDP *:39146
...
root#  lsof -i :22
COMMAND  PID USER   FD   TYPE DEVICE SIZE NODE NAME
sshd    5559 root    3u  IPv6  14097       TCP *:ssh (LISTEN)
sshd    7729 root    3r  IPv6  33146       TCP mars.sol:ssh->merkur.sol:45368
                                                        (ESTABLISHED)
```

nmap

`netstat` und `lsof` können nur auf dem lokalen Rechner ausgeführt werden und stehen einem Angreifer normalerweise nicht zur Verfügung. Dieser greift stattdessen auf sogenannte Port-Scanner zurück. Solche Programme senden Pakete an die wichtigsten Ports eines Rechners und finden anhand der Antwort heraus, welche Dienste in welcher Programmversion dort laufen. Das hier vorgestellte Kommando `nmap` ist das bekannteste, aber keineswegs das einzige derartige Programm. Bei den meisten Distributionen muss es vor der ersten Verwendung installiert werden.

Die folgenden Zeilen zeigen, welche Ergebnisse `nmap` für den Rechner `mars` liefert. `nmap` wurde auf einem anderen Rechner innerhalb des lokalen Netzwerks ausgeführt. Die Ausgabe wurde aus Platzgründen gekürzt.

```
root#  nmap -v -A mars
Scanning 192.168.0.1 [1 port]
...
Discovered open port 53/tcp on 192.168.0.1
Discovered open port 21/tcp on 192.168.0.1
```

```
...
Completed SYN Stealth Scan at 09:43, 0.29s elapsed (1715 total ports)
Initiating Service scan at 09:43
Scanning 9 services on mars.sol (192.168.0.1)
...
Host mars.sol (192.168.0.1) appears to be up ... good.
Interesting ports on mars.sol (192.168.0.1):
Not shown: 1706 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.0.6
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
53/tcp   open  domain      dnsmasq 2.41
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: SOL)
389/tcp  open  ldap        OpenLDAP 2.2.X
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: SOL)
749/tcp  open  rpcbind
2049/tcp open  rpcbind
...
```

Zu `nmap` existiert auch eine grafische Benutzeroberfläche, die sich je nach Distribution im Paket `zenmap` oder `nmap-frontend` befindet.

Führen Sie keine Port-Scans für fremde Server durch!

Ein Port-Scan wird von vielen Administratoren als Einbruchsversuch gewertet. Adressieren Sie mit Programmen wie `nmap` nie ungefragt einen fremden Rechner! `nmap` ist aber ein praktisches Hilfsmittel, um Schwächen im eigenen Netzwerk zu erkennen.

40.2 Basisabsicherung von Netzwerkdiensten

Der vorige Abschnitt hat gezeigt, wie Sie sich rasch einen Überblick über die laufenden Netzwerkdienste verschaffen. Der nächste Schritt besteht nun darin, die Dienste möglichst gut abzusichern:

- Deinstallieren Sie alle Netzwerkdienste, die Sie nicht brauchen. Nicht installierte Programme laufen nicht und können daher keine Gefahr darstellen.
- Bei den erforderlichen Netzwerkdiensten reicht es vielfach aus, ihren Zugriff auf bestimmte Clients einzuschränken, z. B. aus dem lokalen Netzwerk. Es ist beispielsweise selten notwendig, dass ein Drucker-Server seine Dienste im Internet anbietet!

  Bei Apache, Samba, MySQL und zahlreichen weiteren »großen« Diensten muss die Absicherung in der jeweiligen Konfigurationsdatei erfolgen. Erfreulicherwei-

se gibt es aber auch eine Reihe von Netzwerkdiensten, die für die Zugriffskontrolle auf die TCP-Wrapper-Bibliothek zurückgreifen. Das ermöglicht eine zentrale Konfiguration (siehe den folgenden Abschnitt).

- Notwendige Netzwerkdienste sollten mit minimalen Rechten ausgeführt werden. Darum kümmert sich das Init-System Ihrer Distribution. Soweit es möglich und sinnvoll ist, startet das Init-System die Dienste ohne `root`-Rechte in einem für den Dienst konzipierten Account oder in einer `chroot`-Umgebung, die den Zugriff auf Dateien außerhalb des `chroot`-Verzeichnisses verhindert.
- Als zusätzliche Schutzebene empfiehlt sich eine Paketfilter-Firewall, die durch Regeln aus dem Internet kommende Pakete für diverse Dienste von vornherein blockiert (siehe Abschnitt 40.3).
- Kein Programm ist fehlerfrei. Programmfehler können es einem Angreifer ermöglichen, durch die gezielte Übertragung manipulierter Netzwerkpakete das Programm zum Absturz zu bringen oder gar eigene Befehle auszuführen. Um das daraus entstehende Risiko zu minimieren, kann der Kernel die Ausführung von Programmen anhand von Regeln überwachen. Diese Vorgehensweise wird als *Mandatory Access Control* bezeichnet, kurz MAC. Unter Linux sind zu diesem Zweck die Verfahren SELinux und AppArmor populär, die ich Ihnen in Kapitel 42 vorstelle.

Updates, Logging

Die sichere Konfiguration eines Rechners ist keine einmalige Arbeit, sondern ein stetiger Prozess. Nur regelmäßige Software-Updates halten die Software auf Ihrem Rechner auf dem aktuellen Stand. Empfehlenswert ist auch ein regelmäßiger Blick in die Logging-Dateien Ihres Rechners.

TCP-Wrapper-Bibliothek

Gerade auf einem LAN-Server ist es selten zweckmäßig, alle Netzwerkdienste global verfügbar zu machen. Es reicht aus, wenn die Dienste im lokalen Netzwerk verwendet werden können. Eine Reihe von Netzwerkdiensten greifen für diese Basisabsicherung auf die sogenannte TCP-Wrapper-Bibliothek zurück. Dazu zählen insbesondere der SSH- und der NFS-Server. Auch Dienste, die über einen Internet Service Daemon gestartet werden, profitieren von der TCP-Wrapper-Bibliothek (siehe Abschnitt 27.9).

/etc/hosts.allow und hosts.deny

Die Dateien `/etc/hosts.allow` und `/etc/hosts.deny` steuern, von welchem Rechner aus welche Dienste verwendet werden dürfen. Die Einstellungen gelten nur für Netzwerkdienste, die die TCP-Wrapper-Bibliothek bzw. das Kommando `tcpd` für die Zugriffskontrolle verwenden. Standardmäßig sind beide Dateien leer, d. h., es gelten keinerlei Einschränkungen.

Die TCP-Wrapper-Bibliothek wertet zuerst `hosts.allow` aus: Wenn der Zugriff dort explizit gestattet wird, ist die Kontrolle erledigt. Andernfalls wird auch `hosts.deny` ausgewertet: Ist der Zugriff dort verwehrt, erhält der Client eine Fehlermeldung. Vorsicht: In allen Fällen, die weder durch `allow`- noch durch `deny`-Regeln erfasst sind, wird der Zugang gewährt!

Eine möglichst sichere Konfiguration erreichen Sie dadurch, dass Sie als Erstes in `/etc/hosts.deny` durch `all:all` generell den Start jedes Netzwerkdienstes verbieten. Die `spawn`-Anweisung bewirkt darüber hinaus, dass jeder Versuch, irgendeinen Dienst zu starten, in der Datei `/var/log/deny.log` protokolliert wird.

`/var/log/deny.log` verrät Ihnen von nun an, wer wann versucht, einen Netzwerkdienst des Rechners zu nutzen. Nicht jeder Versuch muss zwangsläufig einen Angriff darstellen. Es kann auch sein, dass sich jemand bei der Eingabe des Hostnamens oder der IP-Adresse vertippt hat.

```
# /etc/hosts.deny
# standardmäßig alles verbieten, jeden Verbindungsversuch
# protokollieren
ALL : ALL : spawn (echo Attempt from %h %a to %d at $(date) \
                   >> /var/log/deny.log)
```

Im zweiten Schritt lassen Sie nun in `/etc/hosts.allow` die Nutzung bestimmter Dienste zu. Die unten gezeigte Beispielkonfiguration erlaubt die folgenden IPv4-Zugriffe:

- vom lokalen Rechner aus (`localhost`) den Zugriff auf alle Dienste
- von jedem Rechner aus den `ssh`-Zugriff, also auch aus dem Internet
- innerhalb des lokalen Netzes die Nutzung von NFS (`portmap` und `mountd`) und SWAT

Das Beispiel geht davon aus, dass der Server unter den Namen `mars` und `mars.sol` erreichbar ist, dass das lokale Netz im Adressraum 192.168.0.* betrieben wird und dass alle Rechner die Domain `*.sol` nutzen. Nach demselben Muster können Sie natürlich auch andere Netzwerkdienste, die Sie zuerst global abgeschaltet haben, für das lokale Netz oder für einen beliebigen Adressbereich aktivieren:

```
# /etc/hosts.allow
# einzelne Dienste erlauben
ALL     : localhost mars mars.sol  : ALLOW
sshd    : 0.0.0.0                  : ALLOW
portmap : 192.168.0.0/24 *.sol     : ALLOW
mountd  : 192.168.0.0/24 *.sol     : ALLOW
swat    : 192.168.0.0/24 *.sol     : ALLOW
```

Die Syntax innerhalb von `hosts.allow` bzw. `hosts.deny` sollte aus den Beispielen klar werden. Jeder Eintrag besteht aus drei Teilen, die durch Doppelpunkte getrennt sind.

Der erste Teil gibt den Dienst an, der zweite Teil die IP-Adresse bzw. den Netzwerknamen, der dritte Teil die resultierende Aktion. Eine genauere Syntaxbeschreibung erhalten Sie mit `man 5 hosts_access`.

IPv6

Aktuelle Versionen der TCP-Wrapper-Bibliothek kommen auch mit IPv6 zurecht. Die IPv6-Adressen müssen in `hosts.allow` und `hosts.deny` in eckige Klammern gestellt werden. Die folgenden Zeilen erlauben jede IPv6-Verbindung von `localhost` sowie SSH-Verbindungen aus dem lokalen IPv6-Netz.

```
# /etc/hosts.allow
ALL     : [::1]                       : ALLOW
sshd    : [2001:1234:789a:0471::1/64] : ALLOW
```

TCP-Wrapper-Unterstützung feststellen

Mit `ldd` können Sie leicht selbst feststellen, ob ein bestimmtes Programm die TCP-Wrapper-Bibliothek (`libwrap`) nutzt. Die Ergebnisse für `cupsd` und `sshd` unter Ubuntu sehen wie folgt aus:

```
user$  ldd /usr/sbin/cupsd | grep wrap
user$  ldd /usr/sbin/sshd  | grep wrap
        libwrap.so.0 => /lib/libwrap.so.0 (0x00007f1a5f7f0000)
```

`cupsd` verwendet die Wrapper-Bibliothek also nicht, `ssh` schon.

Start von Netzwerkdiensten ohne root-Rechte

Damit Programme wie Apache oder MySQL ihre Arbeit erledigen können, ist es nicht erforderlich, dass die Programme mit `root`-Rechten laufen. Deswegen sehen die meisten Distributionen für derartige Dienste eigene Accounts vor, deren Namen von Distribution zu Distribution variieren. Unter Ubuntu wird beispielsweise Apache im Account `www-data` ausgeführt und darf daher nur auf Dateien zugreifen, die für diesen Account lesbar sind. Sie können sich davon mit `ps axu` überzeugen. *Eine* Instanz von Apache läuft übrigens doch mit `root`-Rechten. Sie ist aber nur für den Start der anderen Instanzen verantwortlich und erfüllt sonst keine Aufgaben.

```
root#  ps axu | grep apache2
root     ... /usr/sbin/apache2 -k start
www-data ... /usr/sbin/apache2 -k start
www-data ... /usr/sbin/apache2 -k start
...
```

Da die Scripts des Init-Systems grundsätzlich mit `root`-Rechten ausgeführt werden, ist ein spezieller Mechanismus erforderlich, um den Netzwerkdämon in einem anderen Account zu starten. Im einfachsten Fall wird der Prozess dazu in der Form `su accountname -c daemon` gestartet.

Die meisten Netzwerkprozesse sehen allerdings ausgefeiltere Mechanismen vor, bei denen das Programm die Initialisierung mit `root`-Rechten durchführt und erst dann

in einen Account mit weniger Rechten wechselt. Bei manchen Programmen wie `syslogd` gibt es eine eigene Option, um den gewünschten Account anzugeben. Bei Apache, MySQL und einigen weiteren Server-Diensten, die mehrere Instanzen starten, läuft außerdem ein Steuerungsprozess mit `root`-Rechten. Dieser Prozess erfüllt zumeist nur ganz wenige Aufgaben, in der Regel den Start bzw. das Beenden von Instanzen.

Start von Netzwerkdiensten in einer chroot-Umgebung

Das Kommando `chroot rootdir kommando` startet das angegebene Kommando, wobei es `rootdir` als Wurzelverzeichnis verwendet. Das Kommando kann nun nur auf Dateien zugreifen, die sich innerhalb dieses Verzeichnisses befinden. Um sicherzustellen, dass das Programm aus seinem »`chroot`-Gefängnis« nicht ausbrechen kann, muss es zudem in einem Account mit eingeschränkten Rechten ausgeführt werden, also nicht als `root`.

In der Praxis werden Netzwerkdienste allerdings selten mit `chroot` gestartet. Vielmehr sehen viele Dienste eine spezielle Option vor, um das `chroot`-Verzeichnis direkt anzugeben. Dieses Verzeichnis muss dann alle erforderlichen Bibliotheken, Konfigurationsdateien etc. enthalten. Gegebenenfalls kopiert ein Init-Script alle erforderlichen Dateien vor dem Start dorthin.

Wenn ein Netzwerkdienst durch SELinux oder AppArmor überwacht wird und die Regeln korrekt formuliert sind, ist die Verwendung einer `chroot`-Umgebung überflüssig bzw. bietet keine zusätzliche Sicherheit. Fedora und Red Hat verzichten deswegen standardmäßig auf `chroot`-Verzeichnisse und verlassen sich stattdessen auf die SELinux-Regeln.

40.3 Firewalls – eine Einführung

Der Begriff »Firewall« ist zwar in aller Munde, es gibt aber keine allgemein akzeptierte Definition dafür. Eine »Firewall« kann sich auf die Hardware beziehen: Dann ist damit meist ein Rechner gemeint, der zwischen dem lokalen Netz und dem Internet steht. Viele ADSL-Router enthalten elementare Firewall-Funktionen.

Oft wird mit Firewall aber auch ein Programm bezeichnet, das auf dem Rechner installiert wird und das bei korrekter Konfiguration die Sicherheit verbessern soll. Manche Distributionen enthalten Werkzeuge zur Konfiguration der Firewall.

In diesem Buch bezeichne ich mit dem Begriff Firewall die Absicherung des TCP/IP-Verkehrs durch einen Paketfilter. Ein derartiger Filter analysiert alle Netzwerkpakete, die in den Rechner kommen bzw. diesen wieder verlassen. Je nachdem, ob dabei

alle Regeln eingehalten werden, dürfen die Pakete passieren oder werden blockiert. Details zur Konfiguration eines solchen Paketfilters folgen im nächsten Abschnitt. Hier geht es vorerst darum, die Terminologie zu klären.

Firewalls für private Rechner

Die Notwendigkeit von Firewalls auf privaten Rechnern ist umstritten. Die Ubuntu-Entwickler sind beispielsweise der Ansicht, dass bei einer Desktop-Installation von Ubuntu ohnedies keine Netzwerkdienste laufen, die zu schützen sind. Bei einer Minimalinstallation ist das an sich korrekt, aber dabei bleibt es selten: Sobald der Benutzer Samba installiert, um eigene Dateien über ein Netzwerkverzeichnis anderen Benutzern zur Verfügung zu stellen, gibt es den ersten von außen angreifbaren Dienst.

Solange der Computer zu Hause betrieben wird und den Internet-Zugang durch einen ADSL-Router bezieht, sorgt der Router für einen gewissen Schutz von außen – einerseits durch das üblicherweise eingesetzte NAT-Verfahren, andererseits vielleicht auch durch eine Firewall, die auf dem Router läuft. Ganz anders sieht die Sache aus, wenn Sie mit Ihrem Notebook im ungesicherten WLAN eines Hotels E-Mails abrufen. Spätestens dann sollte eine Firewall auch auf Privat-PCs selbstverständlich sein.

Firewalls für lokale Netzwerke

Bei einem Firmen-LAN ist der Wunsch nach einer guten Absicherung noch stärker ausgeprägt. Gleichzeitig bestehen auch bessere Voraussetzungen, was die Infrastruktur betrifft. In der Praxis kümmert sich oft ein eigener Rechner um den Internetzugang für die Firma und um dessen Absicherung. Alle weiteren Netzwerkdienste laufen auf anderen Rechnern. Abbildung 40.1 veranschaulicht das Konzept.

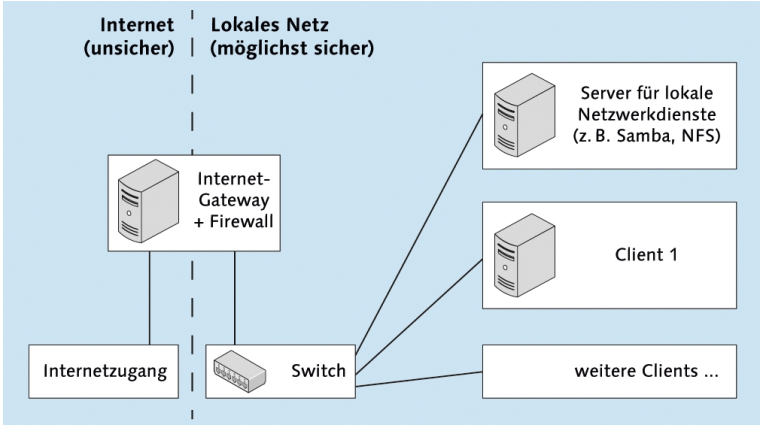


Abbildung 40.1 Firewall für lokale Netzwerke

Bei sehr kleinen Netzen dient manchmal *ein* Rechner gleichzeitig als Firewall und als Netzwerk-Server. Sicherheitstechnisch ist das nicht optimal, weil auf diesem Rech-

ner zwangsläufig eine ganze Menge Netzwerkdienste laufen, die alle ein gewisses Sicherheitsrisiko darstellen.

Bei sehr großen Netzwerken gibt es oft sogar zwei Firewalls: Die erste Firewall dient nur zur Basisabsicherung, ist aber durchlässig für gewöhnliche Internetprotokolle wie HTTP oder FTP. Der Netzwerkbereich dahinter wird als *Demilitarized Zone* (DMZ) bezeichnet; das soll zum Ausdruck bringen, dass in diesem Bereich nur eine eingeschränkte Sicherheit gegeben ist. In dieser Zone befinden sich in der Regel der Webserver sowie andere Netzwerk-Server, die öffentlich (also über das Internet) zugänglich sein müssen.

Die DMZ wird vom eigentlichen lokalen Netzwerk durch eine zweite Firewall getrennt. Erst dahinter befinden sich alle weiteren Server-Dienste, die nur für das lokale Netzwerk zuständig sind und die von außen absolut unzugänglich sein sollen. Die Konfiguration einer mehrstufigen Firewall geht allerdings weit über die Bandbreite dieses Buchs hinaus. Konfigurationsanleitungen finden Sie in speziellen Firewall-Büchern.

Netfilter

Kernelintern kümmert sich das Netfilter-System um die Verarbeitung von Firewall-Regeln. Abbildung 40.2 veranschaulicht stark vereinfacht, welche Wege IP-Pakete innerhalb des Paketfiltersystems gehen können. Eine detailliertere Abbildung finden Sie unter:

http://open-source.arkoon.net/kernel/kernel_net.png

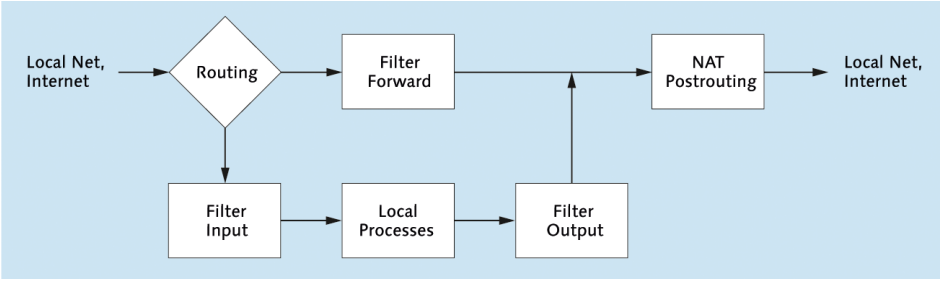


Abbildung 40.2 Vereinfachte Darstellung des iptables/netfilter-Systems

Die folgende Liste beschreibt ganz kurz die Stationen eines IP-Pakets im Kernel:

- **Routing:** Anhand der IP- und Port-Adresse entscheidet der Kernel, ob das Paket lokal bearbeitet werden soll oder ob es an eine Netzwerkschnittstelle und damit an einen anderen Rechner weitergeleitet werden soll. Dieser Mechanismus ist

unabhängig davon, ob sich der andere Rechner im lokalen Netz oder im Internet befindet.

- **Filter Input:** Anhand einer Reihe von Regeln wird getestet, ob das Paket zur weiteren Verarbeitung durch lokale Programme akzeptiert wird oder nicht.
- **Local Process:** Diese Box symbolisiert alle Programme, die IP-Pakete auf dem lokalen Rechner verarbeiten bzw. die selbst neue IP-Pakete erzeugen. Dazu zählen Programme wie Apache, MySQL, Samba oder der NFS-Server.
- **Filter Output:** Anhand einer Reihe von Regeln wird getestet, ob das Paket den Kernel wieder verlassen darf.
- **Filter Forward:** Dieser Filter entscheidet, welche der Pakete, die nur weitergeleitet, aber nicht bearbeitet werden sollen, den Kernel passieren dürfen.
- **NAT Postrouting:** Falls der lokale Rechner via Masquerading anderen Rechnern einen Zugang ins Internet gewähren soll, kümmert sich diese Station um die erforderliche Manipulation der IP-Pakete.

Einem Paketfilter sind in Abbildung 40.2 nur die Boxen *Filter Input*, *Filter Output*, *Filter Forward* und eventuell auch *NAT Postrouting* zuzuordnen. Alle anderen Teile der Abbildung beschreiben die Netzwerkfunktionen des Kernels bzw. gewöhnliche Netzwerkdienste, die auf dem lokalen System laufen und mit dem Paketfilter nichts zu tun haben.

Firewall-Abbildungen

Bei vielen Firewall-Abbildungen sehen Sie links das gefährliche Internet, dann die Firewall und rechts das vergleichsweise sichere lokale Netz. Abbildung 40.2 entspricht nicht diesem Schema! Die Pakete, die links in den Rechner kommen, stammen sowohl aus dem lokalen Netz als auch aus dem Internet. Dasselbe gilt auch für die Pakete, die die Firewall rechts verlassen.

Aktionen

Für die Weiterleitung von Paketen – egal, ob diese von einer Netzwerkschnittstelle kommen oder von einem lokalen Programm erzeugt wurden – ist der Kernel zuständig. Dieser hat dabei in den unterschiedlichen Stufen des Filtersystems jeweils drei Alternativen:

- **Deny:** Die Weiterleitung des Pakets wird ohne Rückmeldung abgelehnt. Das Paket wird damit gewissermaßen gelöscht. Es existiert nicht mehr weiter. Der Sender erfährt nie, was mit seinem Paket passiert ist.
- **Reject:** Die Weiterleitung wird mit einer Rückmeldung abgelehnt. Die Folgen für das Paket sind dieselben, allerdings bekommt der Sender durch ein anderes ICMP-Paket die Nachricht, dass sein Paket abgelehnt wurde.
- **Accept:** Das Paket wird weitergeleitet.

Tabellen

Die Grundidee eines Netfilter-Systems sieht so aus: Jedes IP-Paket durchläuft verschiedene Orte im Kernel, an denen anhand von Regeln überprüft wird, ob das Paket zulässig ist. Wenn das der Fall ist, wird es weitergeleitet, sonst wird es gelöscht oder zurückgesandt. Mehrere Tabellen steuern den Netfilter:

- **Filter-Tabelle:** Diese Tabelle enthält üblicherweise das gesamte Regelsystem für den eigentlichen Paketfilter, also die »Firewall«.
- **NAT-Tabelle:** Diese Tabelle ist nur aktiv, wenn die Masquerading-Funktion des Kernels aktiviert ist. Sie ermöglicht verschiedene Formen der Adressveränderung (Network Address Translation) bei Paketen, die von außen in den Kernel eintreten bzw. diesen wieder verlassen.
- **Mangle-Tabelle:** Auch mit dieser Tabelle können IP-Pakete manipuliert werden. Die Tabelle dient Spezialaufgaben. Ein Anwendungsbeispiel folgt im nächsten Kapitel bei der Konfiguration eines transparenten HTTP-Proxys.

Daneben gibt es noch die Raw- und die Security-Tabelle, auf die ich in diesem Buch aber nicht eingehe.

Regelketten (Chains)

Jede dieser Tabellen sieht wiederum mehrere Regelketten (Chains) vor:

- **Filter-Tabelle:** Input, Forward und Output
- **NAT-Tabelle:** Prerouting, Input, Output und Postrouting
- **Mangle-Tabelle:** Prerouting, Input, Forward, Output und Postrouting

Von diesen insgesamt zwölf Regelketten sind in Abbildung 40.2 nur die vier wichtigsten dargestellt.

Unterschiedliche Regelketten gleichen Namens

Alle Regelketten sind voneinander unabhängig! Es gibt also zwei verschiedene Prerouting- und sogar drei Output-Regelketten.

Dennoch ist in der `iptables`-Dokumentation oft einfach von der Output-Regelkette die Rede, ohne genaue Angabe, auf welche Tabelle sich diese Regelkette eigentlich bezieht. Gemeint sind in derartigen Fällen immer die Regelketten der Filter-Tabelle, die bei Weitem am wichtigsten ist.

Diese Sprachregelung gilt auch für das Kommando `iptables`: Dort kann die gewünschte Tabelle mit der Option `-t` angegeben werden. Entfällt diese Option, gilt das Kommando automatisch für die Filter-Tabelle.

Wenn ein IP-Paket bei seiner Wanderung durch den Kernel auf eine Regelkette stößt, überprüft der Kernel der Reihe nach sämtliche Regeln. Sobald eine Regel auf das Paket zutrifft, wird die in der Regel vorgesehene Aktion durchgeführt und das Paket weitergeleitet, gelöscht oder zurückgesendet. Nur wenn keine einzige der Regeln auf das Paket zutrifft, kommt das Standardverhalten des Filters zur Anwendung. Dieses lautet je nach Konfiguration abermals: weiterleiten, löschen oder zurücksenden.

Grundzustand

Im Grundzustand des Kernels ist nur die Filter-Tabelle mit ihren drei Regelketten Input, Forward und Output aktiv. Keine dieser drei Regelketten enthält eine Regel, und das Standardverhalten lautet für alle drei Regelketten: weiterleiten.

IPv6

Die Regelsysteme für IPv4 und IPv6 sind vollkommen voneinander getrennt. Es gibt also gewissermaßen eine Firewall für IPv4 und eine zweite für IPv6. Im Regelfall ist es zweckmäßig, das Firewall-System parallel für IPv4 und IPv6 aufzubauen. Wenn Sie also einkommende Pakete für den Port 23456 sperren wollen, sind dazu zwei nahezu gleichlautende Regeln für IPv4 und IPv6 erforderlich.

Nicht jede IPv4-Firewallregel ist auch für IPv6 geeignet: Beispielsweise ist NAT unter IPv4 ein wichtiges Thema, während NAT für IPv6 gänzlich unüblich ist und erst seit der Kernelversion 3.7 überhaupt unterstützt wird.

iptables und ip6tables

Die Kunst, einen Paketfilter zu erstellen, besteht nun darin, für jede relevante Filterkette das Standardverhalten sowie eine Reihe von Regeln zu definieren. Auf Kommandoebene verwalten Sie diese Regeln mit `iptables` für IPv4 und `ip6tables` für IPv6.

Das manuelle Einrichten einer Firewall erfordert eine Menge Fachwissen. Besser ist es zumeist, eine Konfigurationshilfe in Anspruch zu nehmen. Im folgenden Abschnitt stelle ich Ihnen dazu einige distributionsspezifische Programme vor. Wenn Sie die Firewall doch lieber manuell konfigurieren möchten, gibt Abschnitt 40.5 ein Einführungsbeispiel. Weitere Informationen und Details gibt es wie üblich im Internet:

http://www.netfilter.org
http://people.netfilter.org/rusty/unreliable-guides

nftables

Das Netfilter-System ist seit 2001 Bestandteil des Kernels. Mittlerweile haben sich einige grundlegende Mängel herausgestellt, weswegen bereits am Nachfolgesystem `nftables` gearbeitet wird. Es ist momentan aber nicht abzusehen, wann und in welcher Form `nftables` Netfilter ablösen wird.

http://lwn.net/Articles/324989

40.4 Firewall-Konfigurationshilfen

Viele Distributionen helfen ihren Anwendern bei der Firewall-Konfiguration mit komfortablen Benutzeroberflächen. Damit können Sie quasi per Mausklick eine einfache Firewall einrichten oder verändern. Hinter der recht einfachen Konfiguration verbirgt sich in der Regel eine Menge Paketfilter-Know-how. Das Resultat ist also oft ein besserer Schutz als eine selbst gebastelte Lösung.

Der Nachteil vorgegebener Firewalls ist deren Blackbox-Verhalten: Wenn die Wirkung des Filters überhaupt dokumentiert ist, dann sehr dürftig. Sie wissen weder, wogegen der Filter Sie schützt, noch, welche Nebenwirkungen der Filter hat. Da kann es schon passieren, dass Linux-Einsteiger nach tagelangem Suchen, warum das Drucken im Netzwerk unmöglich ist, schließlich die Firewall als Schuldigen ausmachen. Der Versuch, den Paketfilter nun entsprechend anzupassen, wird vermutlich scheitern, vor allem dann, wenn ein Firewall-Grundwissen fehlt. Das vorauszusehende Ergebnis: Die Firewall wird einfach ausgeschaltet!

IPv6

Alle im Folgenden beschriebenen Programme richten auch Regeln für IPv6 ein. Debian sieht standardmäßig keine Firewall vor und kennt auch keine distributionsspezifischen Konfigurationswerkzeuge.

Anzahl der Filterregeln

Mit dem Kommando `iptables -L | wc -l` können Sie abschätzen, aus wie vielen Regeln die aktuelle Firewall besteht. Die resultierende Zahl ist ein Maß für die Komplexität der Firewall, aber nicht für ihre Sicherheit! Am sichersten wäre es, den Netzwerkverkehr ganz lahmzulegen – und das gelingt mit einer oder mit zwei Regeln.

Links

Neben den hier beschriebenen Programmen finden Sie im Internet unzählige weitere Konfigurationshilfen. Populär und seit vielen Jahren erprobt sind:

http://www.fwbuilder.org
http://www.shorewall.net

Fedora

FirewallD

Fedora verwendet das 2012 neu entwickelte FirewallD-System. Sein Hauptvorteil besteht darin, dass Änderungen dynamisch, also im laufenden Betrieb, durchgeführt werden. Im Gegensatz dazu war es beim bisherigen statischen System erforderlich, zur Aktivierung von Änderungen die Firewall vorübergehend abzuschalten und dann neu zu errichten. Das war nicht nur ein Sicherheitsrisiko, sondern führte auch dazu, dass vorhandene Netzwerkverbindungen unterbrochen wurden.

Zonen

Für die Verwaltung der Firewall ist der neue Hintergrundprozess `firewalld` verantwortlich. Konfigurationswerkzeuge kommunizieren via D-BUS mit dem Dämon.

Eine zentrale Grundidee von FirewallD besteht darin, dass jeder Netzwerkschnittstelle eine sogenannnte Zone zugeordnet wird. Eine »Zone« im Sinne von FirewallD ist eine Sammlung von Regeln für einen bestimmten Anwendungszweck. Die folgende Liste beschreibt ganz kurz einige Zonen:

- `block`: blockiert jeden Netzwerkverkehr, der Absender erhält eine ICMP-Fehlermeldung.
- `drop`: blockiert jeden Netzwerkverkehr, der Absender wird nicht informiert.
- `trusted`: erlaubt jeden Netzwerkverkehr. Diese Zone ist für gut gesicherte lokale Netzwerke gedacht, aber nicht für WLAN-Verbindungen.
- `external`: blockiert die meisten Ports und aktiviert Masquerading (IPv4). Bei einem Router ist diese Zone für die Schnittstelle vorgesehen, die die Verbindung zum Internet herstellt.
- `home` und `internal`: blockiert die meisten Ports, akzeptiert aber Samba (nur als Client), CUPS und Zeroconf/Avahi/mdns. Beide Zonen sind für Rechner in einem als einigermaßen sicher geltenden lokalen Netzwerk gedacht. Wenn Sie diese Zone nutzen und selbst Windows-Netzwerkverzeichnisse freigeben möchten, müssen Sie außerdem den Dienst SAMBA freischalten.
- `public`: ähnlich wie `home`, blockiert aber auch CUPS und Samba-Client-Funktionen. Die Zone ist für die Internet-Nutzung in unsicheren Netzwerken gedacht, z. B. in einem öffentlichen WLAN.

Standardmäßig ordnet Fedora alle Schnittstellen der Zone `public` zu. Die Zonenregeln mit der Ausnahme von `block`, `drop` und `trusted` können verändert werden. Bei Bedarf können Sie auch selbst eigene Zonen definieren.

Benutzeroberfläche

Zur Firewall-Konfiguration steht eine neue Benutzeroberfläche zur Verfügung (Kommando `firewall-config`, siehe Abbildung 40.3). Das Programm ist leider äußerst unübersichtlich zu bedienen. Nach dem Start sehen Sie die sogenannte RUNTIME-KONFIGURATION der diversen Zonen. Hier durchgeführte Änderungen gelten sofort für die betreffende Zone, sie werden aber nicht gespeichert und gehen somit beim Neustart des Rechners verloren.

Mit OPTIONS • STANDARDZONE ÄNDERN können Sie einstellen, welche Zone standardmäßig gilt, also für alle Netzwerkschnittstellen, bei denen nicht explizit eine andere Zone eingestellt ist.

Die Benutzeroberfläche verrät unbegreiflicherweise nicht, welche Zone nun tatsächlich aktiv ist! Um das herauszufinden, führen Sie OPTIONEN • CHANGE ZONES OF CONNECTIONS aus. Damit gelangen Sie in einen Dialog mit einer Liste aller vom Network Manager verwalteten Schnittstellen. BEARBEITEN führt in den Detaildialog dieser Schnittstelle, und erst dessen Dialogblatt ALLGEMEIN gibt die Zone an. Die Ein-

stellung VORGABE bedeutet, dass diese Schnittstelle der Standardzone zugeordnet ist, also normalerweise `public`.

Um die Definition einer Zone dauerhaft zu ändern, wechseln Sie im Konfigurationsprogramm in die Ansicht DAUERHAFTE KONFIGURATION. Ärgerlicherweise müssen Änderungen, die Sie zuvor in der RUNTIME-Ansicht ausprobiert haben, jetzt wiederholt werden.

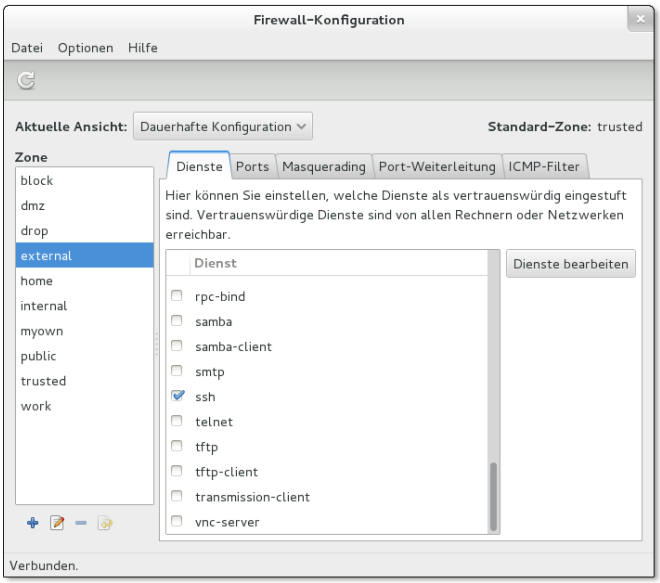


Abbildung 40.3 Fedoras FirewallD-Konfigurationsprogramm

Firewall deaktivieren

Das Konfigurationsprogramm bietet keine Möglichkeit, die Firewall zu deaktivieren. Abhilfe: Führen Sie OPTIONS • STANDARDZONE ÄNDERN aus, und wählen Sie die Zone `trusted`. Beachten Sie aber, dass diese Einstellung nur für solche Schnittstellen gilt, die nicht explizit einer anderen Zone zugewiesen sind. Sollte es bei Ihnen derartige Schnittstellen geben, müssen Sie diese mit OPTIONEN • CHANGE ZONES OF CONNECTIONS extra bearbeiten. In der Standardkonfiguration ist das aber nicht erforderlich.

Wenn Sie eine eigene Firewall einrichten möchten, müssen Sie das Paket `firewalld` deinstallieren.

firewall-cmd

Im Terminal führen Sie Konfigurationsänderungen mit `firewall-cmd` durch. Standardmäßig werden die Änderungen dabei nur dynamisch durchgeführt, aber nicht gespeichert. Wenn die Änderungen dauerhaft gelten sollen, müssen Sie zusätzlich die Option `--permanent` angeben. Die Regeln werden im Verzeichnis `/etc/firewalld` gespeichert. FirewallD wird durch Systemd gestartet.

Sollten Sie die Netzwerkkonfiguration statisch in `/etc/sysconfig/network-scripts` durchführen, also ohne den Network Manager, dann können Sie in der Konfigurationsdatei `ifcfg-xxx` die gewünschte Firewall-Zone angeben. `xxx` ist dabei der Name der Schnittstelle.

```
# Datei /etc/sysconfig/network-scripts/ifcfg-xxx
...
ZONE=trusted
```

Eine umfassende Dokumentation zu FirewallD sowie eine Menge Anwendungsbeispiele zu `firewall-cmd` finden Sie hier:

https://fedoraproject.org/wiki/FirewallD

RHEL 6, CentOS 6

Während der Installation von RHEL 6 und seinen Varianten wird standardmäßig eine Firewall eingerichtet, die alle von außen kommenden Verbindungsversuche blockiert. Zur Konfiguration starten Sie das Programm `system-config-firewall` (siehe Abbildung 40.4). Sie können nun einzelne Dienste und Netzwerkschnittstellen als sicher definieren und so vom Schutz ausnehmen. Wenn der Rechner als Gateway dient, können Sie zudem eine Schnittstelle für das Masquerading angeben.

Die Einstellungen werden in `/etc/sysconfig/iptables` gespeichert. Für den Start der Firewall ist das Init-V-Script `/etc/init.d/iptables` verantwortlich.

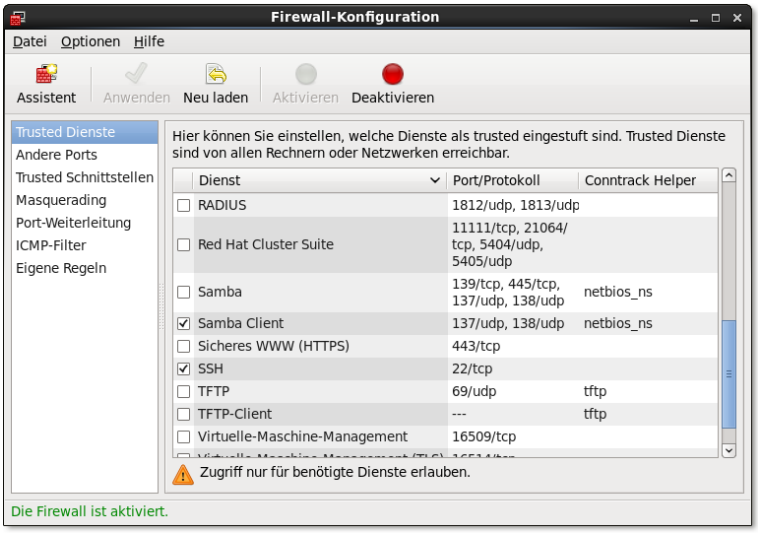


Abbildung 40.4 Firewall-Konfiguration in Red Hat Enterprise Linux

SUSE

SUSE-Distributionen richten standardmäßig eine Firewall ein, wobei die Schnittstelle zum Internet automatisch der externen Zone zugeordnet wird. Die Konfiguration erfolgt durch das YaST-Modul SICHERHEIT • FIREWALL. Dabei werden – abweichend vom sonst dialogorientierten YaST-Konzept – die einzelnen Dialogblätter durch Einträge im linken Teil des YaST-Fensters ausgewählt. Falls der Rechner als Gateway zu einem LAN dient, ordnen Sie im Dialogblatt SCHNITTSTELLEN die LAN-Schnittstelle der internen Zone zu und aktivieren im Dialogblatt MASQUERADING die gleichnamige Option.

Die Firewall-Einstellungen werden in `/etc/sysconfig/SuSEfirewall` gespeichert. Um den Start der Firewall kümmern sich bei älteren SUSE-Versionen die Init-V-Scripts `SuSEfirewall2*`. Aktuelle openSUSE-Versionen verwenden stattdessen Systemd.

Ubuntu

ufw

Bei Ubuntu wird standardmäßig keine Firewall eingerichtet, und es gibt auch keine grafischen Konfigurationswerkzeuge. Dafür enthält Ubuntu das Kommando `ufw` (Uncomplicated Firewall). Es ermöglicht die Definition von Firewall-Regeln in einer wesentlich einfacheren Syntax als `iptables`. Zudem sollen in zukünftigen Ubuntu-Versionen bei der Installation von Netzwerkdiensten die entsprechenden `ufw`-Regeln zur Absicherung gleich mitinstalliert werden. Das ist freilich noch Zukunftsmusik: `ufw` hat bislang nur eine geringe Akzeptanz gefunden.

Wenn Sie schon Erfahrung mit Paketfiltern haben, werden Sie mit `ufw` rasch zum Ziel kommen: `ufw enable` aktiviert die Firewall. Die Firewall wird sofort und in Zukunft auch bei jedem Rechnerstart aktiviert. `ufw disable` deaktiviert die Firewall wieder. `ufw default allow` bzw. `ufw default deny` gibt an, ob eintreffende Pakete grundsätzlich akzeptiert oder abgewiesen werden. Normalerweise gilt `deny`.

Zusätzlich definieren Sie mit `ufw allow/deny` *n* bzw. `ufw allow/deny` *dienst* Regeln, die für spezielle IP-Ports bzw. Protokolle gelten. `ufw status` gibt Informationen zum aktuellen Zustand der Firewall. `ufw` kümmert sich standardmäßig sowohl um IPv4 als auch um IPv6. Wenn Sie IPv6-Verkehr ganz blockieren möchten, verwenden Sie in `/etc/sysconfig/ufw` die Einstellung `IPV6=no`.

```
user$  sudo -s
root#  ufw enable
root#  ufw allow ssh
root#  ufw status
Status: Aktiv
```

```
Zu     Aktion    Von
--     ------    ----
22     ALLOW     Anywhere
22     ALLOW     Anywhere (v6)
```

Eigene Regeln werden in `/lib/ufw/user.rules` und `user6.rules` (für IPv6) gespeichert. Außerdem berücksichtigt `ufw` die Regeldateien aus dem Verzeichnis `/etc/ufw/`. Weitere Informationen und Beispiele zu `ufw` erhalten Sie mit `man ufw` bzw. auf den folgenden Seiten:

http://wiki.ubuntuusers.de/ufw
https://help.ubuntu.com/12.04/serverguide/firewall.html
https://wiki.ubuntu.com/UncomplicatedFirewall

Gufw

Zu `ufw` gibt es mit Gufw eine grafische Benutzeroberfläche, die bei aktuellen Ubuntu-Versionen als `universe`-Paket zur Verfügung steht, also ohne offiziellen Support.

40.5 Firewall mit iptables selbst gebaut

Minimale Client-Absicherung (IPv4 und IPv6)

Die meisten Rechner genießen zu Hause oder in einer Firma in lokalen IPv4-Netzwerken dank NAT eine gewisse Sicherheit. Damit ist es vorbei, wenn Sie unterwegs in einem öffentlichen WLAN E-Mails abrufen: Sie wissen nicht, wer sich sonst noch im Funknetz befindet!

Ein ähnliches Sicherheitsproblem haben Sie, wenn Sie (wie in Abschnitt 29.3 beschrieben) einen Tunnel-Dienst wie Gogo oder SixXs einrichten. Damit hat Ihr Rechner eine zusätzliche IPv6-Adresse. NAT spielt nun keine Rolle mehr: Weltweit kann nun jeder, der über eine IPv6-Verbindung verfügt, IP-Pakete zu Ihrem Rechner senden! Diese Datenpakete können z. B. dazu dienen, um einen SSH-Login zu versuchen oder um über Samba freigegebene Netzwerkverzeichnisse auszulesen.

Idee

Die folgende Mini-Firewall verbessert die Sicherheit in beiden Fällen ganz erheblich. Sie verbietet grundsätzlich jeden Datenverkehr, der nicht von Ihrem Rechner initiiert wird. Mit anderen Worten: Sie können z. B. via SSH einen externen Rechner administrieren, umgekehrt kann aber niemand auch nur versuchen, sich via SSH bei Ihnen einzuloggen. Analog funktioniert dieser Schutz auch für alle anderen Netzwerkdienste.

Das Beispiel wurde unter Ubuntu entwickelt und getestet. Wenn Sie eine andere Distribution verwenden, müssen Sie unbedingt vorher die distributionsspezifische Firewall deaktivieren bzw. unter Fedora das Paket `firewalld` deinstallieren!

Reset

Der erste Teil des Firewall-Scripts führt eine Art `iptables`-Reset durch. `iptables -P` stellt dann das Standardverhalten aller Filter auf `ACCEPT`. `iptables -F` löscht alle vorhandenen Regeln, wobei für die NAT-Tabelle ein eigenes Kommando erforderlich ist. `iptables -X` löscht alle benutzerdefinierten Regelketten. Analog werden all diese Kommandos auch für IPv6 ausgeführt. Netfilter erlaubt nun jeglichen IP-Verkehr.

```
#!/bin/bash
# Mini-Firewall (Teil 1)
IPT4=$(which iptables)
IPT6=$(which ip6tables)

# reset iptables
for IPT in $IPT4 $IPT6; do
  $IPT -P INPUT ACCEPT
  $IPT -P OUTPUT ACCEPT
  $IPT -P FORWARD ACCEPT
  $IPT -F
  $IPT -X
done
```

ICMPv6

Damit IPv6-Funktionen zur Autokonfiguration funktionieren, ist es erforderlich, ICMPv6-Pakete passieren zu lassen. Dazu dienen die zwei abschließenden Kommandos im ersten Teil des Listings:

```
# Mini-Firewall (Teil 2): ICMPv6 zulassen
$IPT6 -A INPUT   -p ipv6-icmp -j ACCEPT
$IPT6 -A FORWARD -p ipv6-icmp -j ACCEPT
```

wall-Regelkette für IPv4

Die folgenden Zeilen definieren eine neue Regelkette mit dem Namen `wall`. Sie stellt einen ebenso eleganten wie wirkungsvollen Schutz vor neuen Verbindungen von außen dar. Die erste `wall`-Regel besagt, dass alle Pakete akzeptiert werden, die zu einer bereits vorhandenen Verbindung gehören.

Die zweite Regel akzeptiert Pakete, die eine neue Verbindung initiieren, sofern die Verbindung *nicht* über die Internetschnittstelle hergestellt wird. Die Inversion wird syntaktisch durch das Ausrufezeichen vor der Option `-i` ausgedrückt. Im Klartext bedeutet die Regel, dass es beispielsweise möglich ist, aus dem lokalen Netz heraus eine HTTP-Kommunikation mit dem Rechner zu starten, nicht aber aus dem Internet.

Die dritte Regel lautet: Alle Pakete, die nicht den vorigen Regeln entsprechen, werden abgewiesen. Diese letzte Regel entspricht also dem Motto: Alles verbieten, was nicht explizit erlaubt ist! Einem potenziellen Angreifer aus dem Internet wird es daher nicht gelingen, eine SSH-Session auch nur zu starten. Das Gleiche gilt natürlich auch für alle anderen Netzwerkdienste – HTTP, FTP, Telnet etc.

Die zwei abschließenden Kommandos des Scripts geben an, dass für alle Pakete, die die Input- oder Forward-Filter durchlaufen, die `wall`-Regeln zur Anwendung kommen:

```
# Mini-Firewall (Teil 3): wall-Regelkette für IPv4
INET=eth0
$IPT4 -N wall
$IPT4 -A wall -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT4 -A wall -m state --state NEW ! -i $INET -j ACCEPT
$IPT4 -A wall -j DROP

# die Regelkette für INPUT und FORWARD anwenden
$IPT4 -A INPUT -j wall
$IPT4 -A FORWARD -j wall
```

wall-Regelkette für IPv6

Der letzte Teil der Mini-Firewall definiert dieselbe `wall`-Regelkette für IPv6. Dabei müssen Sie beachten, dass bei Tunnelverbindungen eine andere Netzwerkschnittstelle aktiv ist: Während IPv4-Verkehr nach `eth0` fließt, geht IPv6-Verkehr über die Tunnelschnittstelle, im folgenden Beispiel `sixxs`:

```
# Mini-Firewall (Teil 4): wall-Regelkette für IPv6
INET6=sixxs
$IPT6 -N wall
$IPT6 -A wall -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT6 -A wall -m state --state NEW ! -i $INET6 -j ACCEPT
$IPT6 -A wall -j DROP
$IPT6 -A INPUT -j wall
$IPT6 -A FORWARD -j wall
```

Internet-Gateway für lokales Netzwerk absichern (IPv4 und IPv6)

Aufgabenstellung

Das zweite Beispiel baut auf den obigen Ideen auf, ist aber schon etwas anspruchsvoller. Es geht darum, ein Gateway abzusichern, das anderen Rechnern im LAN Internetzugang gibt (siehe Kapitel 30). Abbildung 40.1 zeigt die Ausgangssituation.

Die Aufgabe der Firewall besteht darin, gefährliche Ports nach außen hin ganz zu blockieren und bei den restlichen Ports eine Kommunikation nur dann zu erlauben, wenn die Kommunikation von innen initiiert wurde. Der Schutz gilt nun auch für alle IPv4- und IPv6-Clients im lokalen Netzwerk. Das Firewall-Script kümmert sich außerdem um die Aktivierung der Masquerading- und Forwarding-Funktionen.

Überblick

Die Firewall besteht aus den beiden Script-Dateien `myfirewall-start` und `myfirewall-stop`. Die Grundeinstellungen der Firewall werden in der Konfigurationsdatei `myfirewall` gespeichert.

`/etc/myfirewall/myfirewall-start`	(Firewall-Start)
`/etc/myfirewall/myfirewall-stop`	(Firewall-Stopp)
`/etc/default/myfirewall`	(Grundeinstellungen)

Basiskonfiguration (myfirewall)

Die Variable `MFW_ACTIVE` in `/etc/default/myfirewall` steuert, ob die Firewall während des Systemstarts aktiviert werden soll. `MFW_MASQ` gibt an, ob Masquerading und Forwarding aktiviert werden soll. Die restlichen Variablen geben die Schnittstellen und Adressen des lokalen Netzwerks bzw. der Internetverbindung an.

```
# Datei /etc/default/myfirewall
# Firewall starten: yes/no
MFW_ACTIVE=yes
# Masquerading und Forwarding aktivieren: yes/no
MFW_MASQ=yes
# Lokales Netzwerk
MFW_LAN=eth1
MFW_LAN_IP=192.168.0.0/24
# Schnittstelle zum Internet (IPv4 und IPv6)
MFW_INET=eth0
MFW_INET6=sixxs
```

Firewall stoppen (myfirewall-stop)

Das Script `myfirewall-stop` stellt den `iptables`-Grundzustand her und deaktiviert die Firewall – wie in den ersten Zeilen der Mini-Firewall. Ergänzend dazu werden diesmal auch die `nat`-Regelketten zurückgesetzt.

```
#!/bin/bash
# Datei /etc/myfirewall/myfirewall-stop

# Konfigurationseinstellungen lesen
. /etc/default/myfirewall
IPT4=$(which iptables)
IPT6=$(which ip6tables)
SYS=$(which sysctl)

# Firewall-Reset (IPv4 und IPv6)
for IPT in $IPT4 $IPT6; do
  $IPT -P INPUT ACCEPT
  $IPT -P OUTPUT ACCEPT
  $IPT -P FORWARD ACCEPT
  $IPT -F
  $IPT -X
done

# NAT-Reset nur für IPv4
$IPT4 -F -t nat
$IPT4 -P POSTROUTING ACCEPT -t nat
$IPT4 -P PREROUTING ACCEPT -t nat
$IPT4 -P OUTPUT ACCEPT -t nat
```

```
# Forwarding stoppen
$SYS -q -w net.ipv4.ip_forward=0
$SYS -q -w net.ipv6.conf.all.forwarding=0
```

Vergessen Sie nicht, die Script-Datei mit `chmod u+x` als ausführbar zu kennzeichnen!

Firewall starten (myfirewall-start)

Wesentlich interessanter ist naturgemäß `myfirewall-start`. Das Script beginnt damit, die Stopp-Regeln auszuführen. Das bewirkt gleichsam ein Reset des Netfilter-Systems. Alle weiteren `iptables`-Kommandos können sich somit darauf verlassen, dass vorher keine anderen Regeln definiert wurden.

SSH öffnen, ICMPv6 zulassen

Die ersten drei `iptables`-Kommandos lassen den Zugriff auf SSH-Server aus dem Internet zu. Diese Kommandos zeigen beispielhaft, wie Sie trotz Firewall einzelne Dienste nach außen zugänglich machen. Beachten Sie, dass das Absichern eines SSH-Servers im IPv6-Netz schwierig ist; sicherer ist es, SSH zumindest für IPv6 zu sperren.

```
#!/bin/bash
# Datei /etc/myfirewall/myfirewall-start (Teil 1)

# Konfigurationseinstellungen lesen
. /etc/default/myfirewall
IPT=$(which iptables)
SYS=$(which sysctl)

if [ $MFW_ACTIVE != "yes" ]; then
  echo "Firewall disabled in /etc/default/myfirewall"
  exit 0
fi

# Reset aller Firewall-Regeln
. /etc/myfirewall/myfirewall-stop

# Zugriff auf den SSH-Server (Port 22) aus dem Internet erlauben
$IPT4 -A INPUT    -i $MFW_INET -p tcp --dport 22 -j ACCEPT
$IPT6 -A INPUT    -i $MFW_INET6 -p tcp --dport 22 -j ACCEPT
$IPT6 -A FORWARD  -i $MFW_INET6 -p tcp --dport 22 -j ACCEPT

# ICMPv6 erlauben
$IPT6 -A INPUT   -p ipv6-icmp -j ACCEPT
$IPT6 -A FORWARD -p ipv6-icmp -j ACCEPT
```

Ports sperren

In der `for`-Schleife werden nun einige Ports gegenüber dem Internet vollständig blockiert. Sie können die Port-Liste bei Bedarf selbst ergänzen.

```
# Datei /etc/myfirewall/myfirewall-start (Teil 2)
# einige Ports komplett sperren
#   23 (telnet)
#   69 (tftp)
#  135 (Microsoft DCOM RPC)
#  139 (NetBIOS/Samba/etc.)
#  445 (CIFS-Dateisystem für Samba/SMB)
#  631 (ipp/CUPS)
# 1433 (Microsoft SQL Server)
# 2049 (NFS)
# 3306 (MySQL)
# 5999-6003 (X-Displays)
for PORT in 23 69 135 139 445 631 1433 2049 3306 \
            5999 6000 6001 6002 6003; do
  $IPT4 -A INPUT  -i $MFW_INET -p tcp --dport $PORT -j DROP
  $IPT4 -A OUTPUT -o $MFW_INET -p tcp --dport $PORT -j DROP
  $IPT4 -A INPUT  -i $MFW_INET -p udp --dport $PORT -j DROP
  $IPT4 -A OUTPUT -o $MFW_INET -p udp --dport $PORT -j DROP
  $IPT6 -A INPUT  -i $MFW_INET -p tcp --dport $PORT -j DROP
  $IPT6 -A OUTPUT -o $MFW_INET -p tcp --dport $PORT -j DROP
  $IPT6 -A INPUT  -i $MFW_INET -p udp --dport $PORT -j DROP
  $IPT6 -A OUTPUT -o $MFW_INET -p udp --dport $PORT -j DROP
done
```

wall-Regelkette

Die Idee der `wall`-Regelkette habe ich schon im Rahmen der Mini-Firewall beschrieben. Bei diesem größeren Beispiel kommt sie nur zur Anwendung, wenn nicht schon vorher eine der `DROP`- oder `ACCEPT`-Regeln zutraf. Die Reihenfolge der Regeln ist also beim Aufbau einer Firewall entscheidend!

```
# Datei /etc/myfirewall/myfirewall-start (Teil 3)
# wall-Regelkette für IPv4 ..
$IPT4 -N wall
$IPT4 -A wall -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT4 -A wall -m state --state NEW ! -i $MFW_INET -j ACCEPT
$IPT4 -A wall -j DROP
$IPT4 -A INPUT -j wall
$IPT4 -A FORWARD -j wall

# ... und für IPv6
$IPT6 -N wall
$IPT6 -A wall -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT6 -A wall -m state --state NEW ! -i $MFW_INET6 -j ACCEPT
$IPT6 -A wall -j DROP
$IPT6 -A INPUT -j wall
$IPT6 -A FORWARD -j wall
```

Masquerading und Forwarding

Zu guter Letzt müssen auf einem Gateway das Masquerading und das Forwarding aktiviert werden (siehe Abschnitt 30.3):

```
# Datei /etc/myfirewall/myfirewall-start (Teil 4)
if [ $MFW_MASQ = 'yes' ]; then
  $IPT4 -A POSTROUTING  -t nat -o $MFW_INET -s $MFW_LAN_IP -j MASQUERADE
  $SYS -q -w net.ipv4.ip_forward=1
  $SYS -q -w net.ipv6.conf.all.forwarding=1
fi
```

Init-V-Integration

Zum Start der Firewall bietet sich ein Init-V-Script an. Das funktioniert auf fast allen Distributionen, da sowohl Upstart als auch Systemd dazu kompatibel sind. Details des Scripts müssen Sie dennoch an die Besonderheiten der jeweiligen Distribution anpassen.

```
#!/bin/sh -e
# eigenes Init-V-Script /etc/init.d/myfirewall
### BEGIN INIT INFO
# Provides:          firewall
# Required-Start:    networking
# Required-Stop:
# Default-Start:     S
# Short-Description: Start firewall and masquerading
### END INIT INFO

# Grundfunktionen
. /lib/lsb/init-functions

# Funktionen für start, stop und restart
case "$1" in
  start|restart)
        log_begin_msg "Starting firewall and masquerading ..."
        . /etc/myfirewall/myfirewall-start
        log_end_msg 0
        ;;
  stop)
        log_begin_msg "Stopping firewall and masquerading ..."
        . /etc/myfirewall/myfirewall-stop
        log_end_msg 0
        ;;

  status)
        /sbin/iptables -L -v -n
        ;;
```

```
  *)
        log_success_msg "Usage: xxx {start|stop|restart|status}"
        exit 1
        ;;
esac
exit 0
```

Damit dieses Script beim Systemstart automatisch ausgeführt wird, richten Sie unter Debian und Ubuntu den folgenden Link ein:

```
root#  cd /etc/rcS.d
root#  ln -s ../init.d/myfirewall S41myfirewall
```

Upstart-Integration

Um die Firewall durch Upstart automatisch während des Rechnerstarts vor den Netzwerkschnittstellen zu aktivieren bzw. beim Herunterfahren des Rechners nach den Netzwerkschnittstellen zu deaktivieren, müssen Sie eine eigene Konfigurationsdatei in `/etc/init` erstellen:

```
# Datei /etc/init/myfirewall.conf
description "myfirewall"
start on (starting network-interface
          or starting network-manager
          or starting networking)
stop on runlevel [!023456]
pre-start exec /etc/myfirewall/myfirewall-start
post-stop exec /etc/myfirewall/myfirewall-stop
```

Mit `service` können Sie die Firewall auch manuell starten, stoppen und neu starten:

```
root#  service myfirewall start
root#  service myfirewall stop
root#  service myfirewall restart
```

Kapitel 41
Squid und DansGuardian (Webfilter)

Squid ist ein sogenannter Proxy-Cache. Das bedeutet, dass das Programm Webseiten lokal zwischenspeichert und den Zugriff darauf reguliert. Squid kann drei Funktionen übernehmen:

- **Zugriffskontrolle:** Squid kann bestimmte Seiten für manche Nutzer ganz blockieren, den Webzugang auf bestimmte Zeiten beschränken etc. Zur Erkennung »gefährlicher« Seiten wird Squid oft mit dem Webfilter DansGuardian kombiniert. Squid und DansGuardian sind damit eine Hilfe, um den Internetzugang zu Hause, in Schulen oder in öffentlichen Einrichtungen einzuschränken bzw. abzusichern.
- **Cache:** Wenn mehrere Personen über einen Proxy-Cache auf dieselbe Webseite zugreifen, vermeidet das die mehrfache Übertragung derselben Datei. Das macht das Lesen häufig benötigter Webseiten schneller und reduziert den Datenverkehr zum Provider. Im Zeitalter des Web 2.0 mit seinen vielen dynamisch generierten Inhalten dürfen Sie davon allerdings weder einen nennenswerten Geschwindigkeitsgewinn noch eine spürbare Download-Ersparnis erwarten.
- **Logging/Überwachung:** Mit Squid können Sie für das gesamte lokale Netzwerk zentral überwachen, wer welche Seiten wann und wie oft besucht. Das klingt sehr nach *big brother is watching you*, mag aber in manchen Firmen mit hohen Sicherheitsanforderungen notwendig sein.

Dieses Kapitel konzentriert sich auf den ersten Punkt und geht auf die Cache- und Logging-Funktionen nur am Rande ein. Um Enttäuschungen zu vermeiden, möchte ich bereits an dieser Stelle darauf hinweisen, dass Squid und DansGuardian weder Wunder vollbringen noch Erziehungs- und Aufklärungsarbeit ersetzen können!

Links

Auf der Squid-Webseite finden Sie ein Konfigurationshandbuch sowie ein sehr ausführliches FAQ-Dokument. Lesenswert ist auch das deutschsprachige Squid-Handbuch von Dirk Dithardt, das sowohl online als auch in gedruckter Form verfügbar ist.

http://www.squid-cache.org
http://www.squid-handbuch.de/hb

41.1 Squid

Minimalkonfiguration

Das Verhalten von Squid wird durch `/etc/squid[3]/squid.conf` gesteuert. Bei manchen Distributionen ist die mit Squid mitgelieferte Konfigurationsdatei zwar ausgezeichnet dokumentiert, aus diesem Grund aber auch erschreckend lang. Um die Orientierung zu vereinfachen, sollten Sie eine Sicherheitskopie der originalen Konfigurationsdatei erzeugen und dann alle Kommentare entfernen. `grep` filtert mit der Option `-v` alle Zeilen heraus, die mit dem Kommentarzeichen # beginnen. `cat` entfernt leere Zeilen. Damit schrumpft die Konfigurationsdatei auf ca. 50 Zeilen.

```
root#  cd /etc/squid3
root#  mv squid.conf squid.conf.orig
root#  grep -v '^#' squid.conf.orig | cat -s > squid.conf
```

Standardmäßig ist `squid.conf` zumeist so eingestellt, dass der Cache nur vom Rechner `localhost` verwendet werden darf, dass für den Zwischenspeicher 8 MByte im RAM und 100 MByte auf der Festplatte reserviert werden und dass jeder Zugriff in `/var/spool/squid` protokolliert wird. Die Größe des RAM-Cache können Sie mit `cache_mem` einstellen. Wenn Sie keinen Festplatten-Cache wünschen, stellen Sie sicher, dass `squid.conf` keine `cache_dir`-Anweisungen enthält.

Wenn Sie Squid in erster Linie als Webfilter einsetzen möchten, können Sie den Festplatten-Cache und das Logging deaktivieren. Außerdem müssen Sie allen Rechnern im LAN den Zugriff auf Squid erlauben. Dazu definieren Sie mit `acl localnet` die Variable `localnet`, die den Adressraum des lokalen Netzes angibt. Wenn Sie im lokalen Netzwerk auch IPv6 verwenden, benötigen Sie zwei derartige Definitionen: eine für das IPv4- und die zweite für das IPv6-Netz. Bei manchen Distributionen versucht das Squid-Installations-Script, lokale Netze selbstständig zu entdecken, und fügt diese Anweisungen gleich hinzu.

In Kombination mit `http_access localnet` erlaubt Squid allen Rechnern aus dem lokalen Netz, den Cache zu benutzen. Sie können statt `localnet` einen beliebigen anderen Namen verwenden. In den folgenden Zeilen sind die Änderungen gegenüber der mit Ubuntu mitgelieferten Konfigurationsdatei fett hervorgehoben:

```
# /etc/squid/squid.conf
# Beispielkonfiguration zur Verwendung als Webfilter

# Hostname des Rechners, auf dem squid läuft
visible_hostname mars.sol

# Definitionen
acl manager      proto cache_object
acl localhost    src   127.0.0.1/32 ::1
acl to_localhost dst   127.0.0.0/8 0.0.0.0/32 ::1
```

```
acl localnet     src   192.168.0.0/255.255.255.0
acl localnet     src   192.168.0.0/255.255.255.0
acl localnet     src   fc00::/7       # IPv6 local private network range (RFC 4193)
acl localnet     src   fe80::/10      # IPv6 link-local (RFC 4291)
acl localnet     src   2001:7b8:2ff:8471::/64

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

# Zugriffsregeln
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access allow localnet
http_access deny all

# kein Logging
access_log none

# Standard-Port
http_port 3128

# Abstürze hier speichern
coredump_dir /var/spool/squid3

# Lebensdauer von Dateien ohne expiry-Datum
refresh_pattern ^ftp:                   1440    20%     10080
refresh_pattern ^gopher:                1440    0%      1440
refresh_pattern (Release|Packages(.gz)*)$  0       20%     2880
refresh_pattern  .                      0       20%     4320

# Cache-Größe limitieren
cache_mem 256 MB

# kein Festplatten-Cache:
# alle cache_dir-Anweisungen auskommentieren oder löschen
```

Um die Änderungen zu aktivieren, starten Sie Squid neu:

```
root#  service squid[3] restart
```

Externen Proxy-Cache verwenden

Falls Ihr Provider selbst einen Proxy-Cache anbietet und Sie diesen verwenden möchten oder müssen, geben Sie dessen IP-Adresse und -Port wie im folgenden Beispiel mit dem Schlüsselwort `cache_peer` an. Wenn der ICP-Port nicht bekannt ist, versuchen Sie es mit 0 oder 7. Wenn das nicht klappt, geben Sie zusätzlich die Option `default` oder `no-query` an.

```
# übergeordneter Proxy-Cache (z.B. vom Internet-Provider)
# cache_peer <hostname> <type> <proxy-port> <icp-port> <options>
cache_peer  www-proxy.provider.de  parent  8080  7  default
```

Cache selektiv deaktivieren

Wenn Sie möchten, dass die Webseiten eines lokalen Servers nicht zwischengespeichert werden, verwenden Sie das Schlüsselwort `no_cache`. Das Beispiel geht davon aus, dass auf `uranus` ein lokaler Webserver läuft:

```
# direkter Zugang zum lokalen Webserver uranus.sol
acl      mars  dstdomain .uranus .uranus.sol
no_cache deny  uranus
```

IPv6

Squid ist seit der 2010 veröffentlichten Version 3.1 IPv6-kompatibel. IPv6 ist standardmäßig aktiv. Sofern das lokale Netzwerk korrekt konfiguriert ist und jeder Rechner im lokalen Netzwerk den Hostnamen des Squid-Servers korrekt auflösen kann (also `ping6 hostname-des-squid-rechners`), sollte Squid auf Anhieb auch als IPv6-Proxy funktionieren. Vergessen Sie nicht, in `squid.conf` eine `localnet`-Zeile für Ihr lokales IPv6-Netz einzubauen!

Es gibt Hunderte weiterer Optionen, mit denen Sie das Verhalten von Squid bzw. dessen Logging-Funktionen steuern können. Wenn Sie spezielle Wünsche haben, werfen Sie einen Blick in die Dokumentation bei *ww.squid-cache.org*!

Erster Test

Standardmäßig verwendet Squid den Port 3128. Damit die Benutzer in Ihrem lokalen Netz den Proxy tatsächlich nutzen, muss die Proxy-Konfiguration auch auf deren Webbrowsern geändert werden! Bei Firefox führen Sie dazu BEARBEITEN • EINSTELLUNGEN • ERWEITERT • NETZWERK aus, klicken auf den Button EINSTELLUNGEN und aktivieren die Option MANUELLE PROXY-KONFIGURATION. Als Proxy-Server geben Sie den Namen des Rechners an, auf dem Squid läuft (z. B. `mars.sol`), als Port-Nummer 3128.

Sofern Sie die Logging-Funktionen von Squid nicht deaktiviert haben, können Sie anhand der Datei `/var/log/squid[3]/access.log` kontrollieren, ob Squid ordnungsgemäß funktioniert. Wenn alles funktioniert, werden dort alle übertragenen Dateien protokolliert.

Konfiguration als transparenter Proxy-Cache (NAT-Variante)

Bis jetzt erfolgt die Benutzung des Proxy-Cache auf freiwilliger Basis. Nur wenn die Clients (also die Surfer) die Proxy-Einstellungen ihres Browsers anpassen, kommt Squid tatsächlich zur Anwendung. Ohne die Veränderung der Proxy-Einstellungen surfen die Anwender aber quasi am Cache vorbei.

Diese Situation ist aus zwei Gründen unbefriedigend: Viele Endanwender sind ganz einfach damit überfordert, die Proxy-Einstellung selbst zu ändern. Außerdem wird Squid als Filter wirkungslos bleiben, solange die Anwender nur die Proxy-Einstellung zurücksetzen müssen, um Squid zu umgehen.

Um dem abzuhelfen, kann der Linux-Kernel so eingerichtet werden, dass der gesamte HTTP-Verkehr, der üblicherweise über den IP-Port 80 läuft, automatisch zum Proxy-Cache umgeleitet wird. Der Cache wird dann als »transparent« bezeichnet. Das bedeutet, dass der Cache ohne irgendwelchen Konfigurationsaufwand durch den Anwender automatisch bei jedem HTTP-Zugriff verwendet wird.

Es gibt zwei Konfigurationsvarianten:

- **NAT (IPv4):** Die in diesem Abschnitt beschriebene Variante setzt voraus, dass Squid auf dem Rechner (Server) installiert ist, der im lokalen Netzwerk das Internet-Gateway darstellt. Sie ist einfacher, funktioniert aber nur für IPv4. Wenn Sie das im folgenden Abschnitt beschriebene Programm DansGuardian verwenden möchten, kommt nur diese Variante infrage.
- **TPROXY (IPv4 und IPv6):** Im folgenden Abschnitt stelle ich Ihnen eine zweite Variante vor, deren Konfiguration aufwendiger ist. Dafür funktioniert die TPROXY-Variante gleichermaßen für IPv4 und IPv6. Aus technischer Sicht ist sie zudem die elegantere Variante, weil sie die Manipulation von Paketen vollständig vermeidet.

Einschränkungen

Prinzipbedingt funktioniert ein transparenter Proxy nur für alle Clients im lokalen Netzwerk, nicht aber für den Squid-Host selbst. Um den Proxy auch dort zu nutzen, müssen Sie weiterhin die Proxy-Einstellung des Webbrowsers ändern. Dieser Umstand ist vor allem beim Testen irritierend: Sie können den transparenten Proxy nur auf einem Client im lokalen Netzwerk ausprobieren, nicht aber auf dem Rechner, auf dem Squid läuft!

HTTPS-Seiten können nicht durch einen transparenten Proxy geleitet werden. Einerseits ist es erfreulich, dass immer mehr Websites wie Facebook standardmäßig auf HTTPS setzen, andererseits macht es aber die Sperre derartiger Seiten durch einen Proxy unmöglich.

squid.conf

Bei der NAT-Variante muss in `squid.conf` nur eine einzige Zeile geändert werden. Bei `http_port` geben Sie nun im Anschluss an die Port-Nummer auch das Schlüsselwort `transparent` an und starten Squid dann neu.

```
# Änderung in /etc/squid/squid.conf
...
http_port 3128 transparent
```

Forwarding aktivieren

Falls nicht ohnedies schon aufgrund einer Masquerading-Konfiguration der Fall ist, müssen Sie die Forwarding-Funktion des Kernels aktivieren:

```
root#  sysctl -q -w net.ipv4.ip_forward=1
root#  sysctl -q -w net.ipv6.conf.all.forwarding=1
```

Port-Umleitung

Jetzt müssen Sie nur noch die Umleitung von IP-Paketen aktivieren: Alle IP-Pakete, die den Rechner verlassen sollen und an Port 80 adressiert sind, sollen an den IP-Port von Squid geleitet werden. Das Kommando ist hier nur aus Platzgründen auf zwei Zeilen verteilt. `eth1` müssen Sie durch den Namen der Schnittstelle ersetzen, die das Gateway mit dem LAN verbindet.

```
root#  iptables -A PREROUTING -t nat -i eth1 -p tcp \
               --dport 80 -j REDIRECT --to-port 3128
```

Wenn alles funktioniert, nutzt nun jeder Client im lokalen Netz ohne Konfiguration automatisch Squid zur Übertragung von Webseiten. Überprüfen Sie, ob beim Webzugriff von einem Client-Rechner tatsächlich neue Einträge in `/var/log/squid[3]/access.log` auftauchen!

Zum Abschluss fügen Sie das `iptables`-Kommando in ein Init-Script ein, das beim Rechnerstart automatisch ausgeführt wird. Auf meinem Server ist das Kommando ein Bestandteil des in Kapitel 40 vorgestellten Scripts:

```
# in /etc/myfirewall/myfirewall
...
if [ $MFW_MASQ = 'yes' ]; then
  # Masquerading
  $IPT4 -A POSTROUTING  -t nat -o $MFW_INET -s $MFW_LAN_IP \
        -j MASQUERADE

  # transparenter Proxy-Cache
  $IPT4 -A PREROUTING -t nat -i $MFW_LAN -p tcp --dport 80 \
        -j REDIRECT --to-port 3128

  # Forward-Funktion des Kernels
  $SYS -q -w net.ipv4.ip_forward=1
fi
```

Konfiguration als transparenter Proxy-Cache (TPROXY-Variante)

Die TPROXY-Variante basiert auf der gleichnamigen Netfilter-Funktion. Die Grundidee besteht darin, dass die durch den Router zu transportierenden HTTP-Datenpakete zuerst markiert und dann über den Squid-Port umgeleitet werden. Die technischen Hintergründe können Sie hier nachlesen:

http://wiki.squid-cache.org/Features/Tproxy4
http://www.mjmwired.net/kernel/Documentation/networking/tproxy.txt

squid.conf

Die Änderungen für Squid fallen abermals minimal aus. Üblicherweise lassen Sie den üblichen Squid-Port 3128 unverändert. Außerdem definieren Sie aber einen zweiten Port mit dem Schlüsselwort `tproxy`:

```
# Datei squid.conf
...
http_port 3128
http_port 3129 tproxy
```

Wenn Sie unter Fedora oder RHEL arbeiten, verhindert SELinux nun den Start von Squid. Abhilfe schafft das Setzen des booleschen SELinux-Parameters `squid_use_tproxy`:

```
root# setsebool -P squid_use_tproxy 1
```

IPv4

In Ihrem Firewall-Script bauen Sie nun die folgenden Kommandos ein, um IPv4-Verkehr mittels TPROXY auf den Port 3129 umzuleiten. Die `iptables`-Anweisungen betreffen dabei die Mangle-Tabelle, für die die neue Regel `DIVERT` definiert wird.

```
# Firewall-Script (Teil 1, IPv4)
iptables -t mangle -N DIVERT
iptables -t mangle -A PREROUTING -p tcp -m socket -j DIVERT
iptables -t mangle -A DIVERT -j MARK --set-mark 1
iptables -t mangle -A DIVERT -j ACCEPT
ip rule add fwmark 1 lookup 100
ip route add local 0.0.0.0/0 dev lo table 100
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j TPROXY \
  --tproxy-mark 0x1/0x1 --on-port 3129
```

IPv6

Die für IPv6 verantwortlichen Kommandos sehen ganz ähnlich aus:

```
# Firewall-Script (Teil 2, IPv6)
ip6tables -t mangle -N DIVERT
ip6tables -t mangle -A PREROUTING -p tcp -m socket -j DIVERT
ip6tables -t mangle -A DIVERT -j MARK --set-mark 1
ip6tables -t mangle -A DIVERT -j ACCEPT
ip6tables -t mangle -A PREROUTING -p tcp --dport 80 -j TPROXY \
  --tproxy-mark 0x1/0x1 --on-port 3129
ip -6 rule add fwmark 1 lookup 100
ip -6 route add local ::/0 dev lo table 100
```

Nach dem Neustart von Squid und der Ausführung des Scripts ist der transparente Proxy aktiv. Wie üblich ist es zweckmäßig, in Squid das Logging zumindest vorübergehend zu aktivieren, um die Funktion zu testen.

Aufräumarbeiten

Wenn Sie den transparenten Proxy wieder abschalten möchten, sind einige Aufräumarbeiten notwendig. Es ist zweckmäßig, die Kommandos in einem eigenen Script zu speichern:

```
# Aufräum-Script
iptables  -F -t mangle
iptables  -X -t mangle
ip6tables -F -t mangle
ip6tables -X -t mangle
ip    rule del fwmark 1 lookup 100
ip    route del local 0.0.0.0/0 dev lo table 100
ip -6 rule del fwmark 1 lookup 100
ip -6 route del local ::/0 dev lo table 100
```

41.2 DansGuardian

Grundsätzlich ist es möglich, durch Regeln in `squid.conf` einzelne Websites zu blockieren. Auf dieser Basis einen echten Webfilter zu realisieren, wäre aber zu aufwendig. Wozu auch das Rad neu erfinden? Mit dem Programm DansGuardian erreichen Sie einen einigermaßen kindersicheren Webzugang viel einfacher.

Die Grundfunktion des Programms besteht darin, dass es den Text von Webseiten auf pornografische Schlüsselwörter analysiert und die Weiterleitung der Seite bei Überschreitung eines bestimmten Grenzwerts blockiert. Der Mechanismus ist intelligent genug, dass nicht jede Seite, die Wörter wie *sex* oder *breast* enthält, blockiert wird. Da DansGuardian den »Inhalt« der Seiten verarbeitet, ist das Programm zugleich unabhängig von zumeist veralteten Listen blockierter Websites. Einen Überblick über weitere Merkmale des Programms finden Sie auf der folgenden Website:

http://dansguardian.org

IPv6

DansGuardian ist leider weder IPv6-fähig noch unterstützt es die vorhin vorgestellte `TPROXY`-Funktion, um es als transparenten Proxy in IPv6-Netzen einzusetzen. DansGuardian kann daher nur IPv4-Netze mit NAT schützen. Generell verläuft die Entwicklung von DansGuardian seit einigen Jahren äußerst schleppend. Es gibt mittlerweile einige Forks des Programms, aber leider keine echten Alternativen.

Installation

DansGuardian kann bei den meisten Distributionen direkt als Paket installiert werden. Da es auch den Download bekannter Windows-Viren blockiert, wird zusammen mit DansGuardian der Virenfilter ClamAV installiert.

DansGuardian ist ein Dämon, der durch das Init-System gestartet und gestoppt wird. Standardmäßig erwartet das Programm Webanfragen am Port 8080. Es kontaktiert dann das Programm Squid (Port 3128) und analysiert die Webseite. Wird die Seite für in Ordnung befunden, wird sie über Port 8080 zurück an den Webbrowser geleitet. Noch eleganter ist die hier vorgestellte Konfigurationsvariante, bei der DansGuardian transparent alle Webanfragen an Port 80 verarbeitet, sodass an den Clients keinerlei Proxy-Konfiguration erforderlich ist.

dansguardian.conf

Die primäre Konfigurationsdatei ist `/etc/dansguardian/dansguardian.conf`. In der Regel können Sie diese Datei weitestgehend so lassen, wie sie ist. Je nach Distribution enthält die Datei die Zeile `UNCONFIGURED`, der Sie ein Kommentarzeichen voranstellen müssen.

Wenn Sie möchten, dass die Meldung »access denied« in deutscher Sprache erscheint, nutzen Sie außerdem die Einstellung `language = 'german'`. Falls sich in Ihrem Netzwerk ausschließlich Linux-Rechner befinden, deaktivieren Sie durch `virusscan = off` den Virus-Scanner, der standardmäßig alle Downloads auf Viren überprüft. Für das Zusammenspiel mit dem Proxy Squid müssen Sie dessen IP-Adresse und Port-Nummer angeben.

```
# /etc/dansguardian/dansguardian.conf (auszugsweise)
# UNCONFIGURED (diese Zeile muss auskommentiert werden!)
reportinglevel = 3
languagedir = '/etc/dansguardian/languages'
language = 'german'
loglevel = 1
logexceptionhits = 2
logfileformat = 1
filterport = 8080
proxyip = 127.0.0.1
proxyport = 3128
...
```

Nach der Konfiguration starten Sie DansGuardian erstmalig:

```
root#  service dansguardian start
```

Transparenter Schutz

Standardmäßig funktioniert DansGuardian nur für Zugriffe über den Port 8080. Um einen transparenten Schutz für alle Webzugriffe auf Port 80 zu erreichen, müssen Sie Ihr Firewall-Script nochmals ein wenig verändern: Anstatt HTTP-Zugriffe auf den Port 3128 (Squid) umzuleiten, leiten Sie sie auf den Port 8080 um (DansGuardian). Diese Konfiguration funktioniert nur für die NAT-Variante, also nur für IPv4-Netze.

```
# Ergänzung im Firewall-Script
#
# alle an Port 80 adressierten Pakete zu DansGuardian (Port 8080)
# umleiten (transparenter Webfilter)
```

```
iptables -t nat -A PREROUTING -i $MFW_LAN -p tcp --dport 80 \
         -j REDIRECT --to-port 8080
```

Squid muss als gewöhnlicher Proxy-Cache konfiguriert sein, nicht als transparenter Cache. Außerdem müssen Sie den Zugriff auf Squid nun so einschränken, dass nur der Rechner, auf dem DansGuardian läuft, mit Squid kommunizieren darf. Wenn Squid und DansGuardian auf demselben Rechner laufen und Sie die in diesem Kapitel beschriebene Konfiguration verwenden, müssen Sie dazu die Zeile `http_access allow localnet` entfernen. Andernfalls wäre es für die Benutzer im LAN möglich, die Proxy-Konfiguration ihrer Webbrowser so einzurichten, dass die Webbrowser über den Port 3128 direkt mit Squid kommunizieren und so DansGuardian umgehen!

```
# Datei squid.conf
...
# alle acl localnet-Zeilen für das lokale Netzwerk auskommentieren
# acl localnet src 10.0.0.0/8

# Squid agiert als gewöhnlicher Proxy
http_port 3128
```

Webfilter-Konfiguration

Die eigentlichen Filterfunktionen von DansGuardian werden durch `/etc/dansguardian/dansguardianf1.conf` gesteuert. Die Datei verweist zuerst auf diverse vorkonfigurierte Dateien mit Schlüsselwörtern, blockierten Websites etc. Der Parameter `naughtynesslimit` steuert, ab welchem Grenzwert eine Seite blockiert wird. Dieser Wert ist umso höher, je mehr Schlüsselwörter bzw. Schlüsselwortkombinationen im Text gefunden werden.

```
# /etc/dansguardian/dansguardianf1.conf (auszugsweise)
# Content filtering files location
bannedphraselist       = '/etc/dansguardian/lists/bannedphraselist'
weightedphraselist     = '/etc/dansguardian/lists/weightedphraselist'
exceptionphraselist    = '/etc/dansguardian/lists/exceptionphraselist'
bannedsitelist         = '/etc/dansguardian/lists/bannedsitelist'
greysitelist           = '/etc/dansguardian/lists/greysitelist'
exceptionsitelist      = '/etc/dansguardian/lists/exceptionsitelist'
bannedurllist          = '/etc/dansguardian/lists/bannedurllist'
greyurllist            = '/etc/dansguardian/lists/greyurllist'
exceptionurllist       = '/etc/dansguardian/lists/exceptionurllist'
exceptionregexpurllist = '/etc/dansguardian/lists/exceptionregexpurllist'
bannedregexpurllist    = '/etc/dansguardian/lists/bannedregexpurllist'
picsfile               = '/etc/dansguardian/lists/pics'
contentregexplist      = '/etc/dansguardian/lists/contentregexplist'
urlregexplist          = '/etc/dansguardian/lists/urlregexplist'
```

```
# Naughtyness limit
# As a guide:
# 50 is for young children,  100 for old children,  160 for young adults.
naughtynesslimit = 50
...
```

Wenn DansGuardian eine Seite blockiert, zeigt der Webbrowser einen entsprechenden Hinweis an (siehe Abbildung 41.1). Das Aussehen und den Inhalt der Blockadeseite können Sie in der folgenden Datei einstellen:

```
/etc/dansguardian/languages/german/template.html
```

Tabelle 41.1 fasst die Funktion der wichtigsten Dateien des Verzeichnisses `/etc/dansguardian/list` zusammen. In diesen Dateien bzw. in dort genannten Include-Dateien können Sie weitere erwünschte und oder unerwünschte Begriffe, Websites bzw. Dateitypen aufzählen.

Datei	Inhalt
`bannedextensionlist`	Dateien mit diesen Kennungen blockieren
`bannedmimetypelist`	diese Dateitypen blockieren
`bannedphraselist`	verbotene Schlüsselwörter
`weightedphraselist`	negative Schlüsselwörter
`bannedsitelist`	diese Websites komplett blockieren
`bannedurllist`	diese Seiten blockieren
`exceptioniplist`	Anfragen von diesen Rechnern nie blockieren (ermöglicht Administratorzugriff auf fragwürdige Seiten)
`exceptionsitelist`	diese Websites ohne weitere Kontrolle akzeptieren
`exceptionurllist`	diese Webseiten ohne weitere Kontrolle akzeptieren
`exceptionphraselist`	positive Schlüsselwörter
`greysitelist`	diese Websites prinzipiell akzeptieren, aber Textinhalt kontrollieren

Tabelle 41.1 DansGuardian-Konfigurationsdateien

Bei der Textanalyse unterscheidet DansGuardian zwischen verbotenen Schlüsselwörtern (`bannedphraselist`), deren Vorkommen den Zugriff auf eine Seite sofort verbietet, und gewichteten Schlüsselwörtern (`weightedphraselist` und `exceptionphraselist`). In der Grundkonfiguration gibt es kaum verbotene Schlüsselwörter, weil diese oft auch in harmlosen Seiten vorkommen. Stattdessen verwendet DansGuardian relativ umfangreiche Wortlisten (siehe `/etc/dansguardian/list/phraselists`). Anhand dieser Listen bildet DansGuardian eine Summe über das Vorkommen aller negativen und positiven Schlüsselwörter. Überschreitet diese Summe einen Grenzwert,

wird der Zugriff blockiert. Details darüber, wie die Bewertungssummen blockierter Seiten zustande kommen, finden Sie in der Logging-Datei `/var/log/dansguardian/access.log`.

Abbildung 41.1 DansGuardian und Squid blockieren den Zugriff auf eine Webseite.

Das DansGuardian-Paket enthält *keine* Listen von Webadressen, die blockiert werden sollen! Die Dateien `bannedsitelist` und `bannedurllist` dokumentieren nur die prinzipielle Syntax. Es gibt aber Firmen, die gegen Bezahlung den regelmäßigen Download aktueller Listen ermöglichen. Am bekanntesten ist URLblacklist, die in diversen Squid-kompatiblen Textdateien Links auf problematische Webseiten sammelt. Die Listen sind nach diversen Kategorien geordnet (z. B. `drugs`, `porn`, `violence`). Die Filterlisten dürfen zu Testzwecken einmalig kostenlos heruntergeladen werden, regelmäßige Updates sind aber kostenpflichtig:

http://urlblacklist.com

In der Standardkonfiguration blockiert DansGuardian den Download von komprimierten Dateien, MP3-Dateien, ISO-Dateien etc. Diese Einstellungen sind für den Linux-Alltag entschieden zu restriktiv und verhindern bei manchen Distributionen sogar ein korrektes Funktionieren der Paketverwaltung. Werfen Sie einen Blick auf `bannedmimetypelist` und `bannedextensionlist`, und stellen Sie allen erlaubten Dateitypen ein Kommentarzeichen voran! Alternativ können Sie in `dansguardianf1.conf` bei der Einstellung der Variablen `bannedextensionlist` und `bannedmimetypelist` auch einfach eine leere Datei angeben.

Um auf Anfragen der Art *DansGuardian blockiert Seite xxx, die ist aber OK* zu reagieren, müssen Sie als Administrator in der Lage sein, DansGuardian zu umgehen. Am einfachsten erreichen Sie das dadurch, dass Sie in der Konfigurationsdatei `exceptionip` die fixe IP-Adresse Ihres Rechners im lokalen Netzwerk angeben.

Einschränkungen

Machen Sie sich keine Illusionen über die Wirksamkeit von DansGuardian! Selbst die Einstellung `naughtynesslimit = 50` (*for young children*) bietet keinen vollständigen Schutz vor pornografischen Webseiten und Abbildungen. Unter anderem gelten die folgenden Einschränkungen:

- Die Standardkonfiguration berücksichtigt überwiegend englischsprachige Schlüsselwörter. Für die meisten pornografischen Seiten mag das ausreichen, wenn Sie aber auch rechtsextreme oder gewaltverherrlichende Seiten blockieren möchten, ist Handarbeit erforderlich. Der richtige Startpunkt ist die Datei `/etc/dansguardian/list/weightedphraselist`.
- Davon unabhängig lässt sich der Filter durch dynamisch von JavaScript oder Flash erzeugten Text oder durch PDF-Dateien leicht umgehen.
- Der Zugriff auf Bilder und Videos ist gänzlich ungeschützt.
- Squid und DansGuardian gelten nur für gewöhnliche Webseiten. Andere Kommunikationsformen wie E-Mail, News, Chat, Skype etc. bleiben ungeschützt.
- Auch HTTPS-Seiten sind ungeschützt. Squid kann prinzipbedingt HTTPS-Seiten nicht verarbeiten.
- Die Kombination aus Squid und DansGuardian kann zurzeit nicht in IPv6-Netzen verwendet werden.

Kapitel 42
SELinux und AppArmor

SELinux und AppArmor sind Kernelerweiterungen, die laufende Prozesse überwachen und sicherstellen, dass diese bestimmte Regeln einhalten. SELinux kommt standardmäßig unter Fedora und RHEL zum Einsatz, AppArmor unter Ubuntu und teilweise in SUSE-Distributionen.

Dieses Kapitel gibt eine Einführung in die Funktionsweise und Konfiguration von SELinux und AppArmor. Es zeigt auch, wie Sie Regelverstöße feststellen und wie Sie darauf reagieren können.

42.1 SELinux

Unter Linux gilt normalerweise das traditionelle System zur Verwaltung von Zugriffsrechten: Jedes Programm läuft in einem Benutzer-Account. Dieser Account bestimmt, auf welche (Device-)Dateien das Programm zugreifen darf.

Gewöhnliche Programme verwenden den Account des Benutzers, der das Programm gestartet hat. Netzwerkdienste, Datenbank-Server etc. werden mit `root`-Rechten gestartet, wechseln aber aus Sicherheitsgründen zumeist unmittelbar nach dem Start in einen anderen Account mit eingeschränkten Rechten.

Das Unix-Rechtesystem ist zwar ausgesprochen einfach, bietet aber nur eingeschränkte Konfigurationsmöglichkeiten. Wenn es einem Angreifer gelingt, die Steuerung eines Programms zu übernehmen, kann er auf zahllose Dateien zugreifen, die das Programm normalerweise gar nicht benötigt. Besonders schlimm ist es, wenn der Angreifer die Kontrolle über ein Programm mit `root`-Rechten erhält bzw. wenn er über Umwege erreichen kann, dass eigener Code mit `root`-Rechten ausgeführt wird: Damit kann er den Rechner uneingeschränkt manipulieren, eigene Programme installieren und starten etc.

Vielleicht fragen Sie sich, wie ein Angreifer die Kontrolle über ein Programm erlangen kann. Fast immer werden dabei Fehler im Programmcode ausgenutzt. Beispielsweise wird durch das Übersenden manipulierter Daten ein sogenannter Pufferüberlauf ausgelöst. Dieser Fehler wird wiederum dazu genutzt, um dem Pro-

gramm eigenen Code unterzujubeln und diesen auszuführen. Natürlich gibt es auch andere Verfahren – aber immer geht es darum, Sicherheitslücken des Programms zu missbrauchen, um das Programm zweckentfremdet zu nutzen bzw. zu manipulieren.

Sicherheitsmaßnahmen

Fehlerfreie Programme gibt es nicht und wird es wohl auch in Zukunft nie geben, wenn man einmal von winzigen Trivialprogrammen absieht. Deswegen wurden im Laufe der Zeit alle möglichen Verfahren entwickelt, um die durch Programmfehler verursachten Risiken zu minimieren: Zu den etablierten Sicherheitsmaßnahmen zählt, möglichst auf Dämonen mit `root`-Rechten zu verzichten, möglichst wenige Programme bzw. Scripts mit `setuid`-Bit zu installieren (siehe Abschnitt 15.6) und die Ausführung von Code im Stack durch die von Red Hat entwickelte Kernelerweiterung Exec Shield zu verbieten.

SELinux

Noch einen Schritt weiter geht die ursprünglich von der NSA als Open-Source-Code entwickelte Kernelerweiterung SELinux. Der Zweck dieser Erweiterung ist es, dass der Kernel die Ausführung von Programmen anhand von Regeln überwacht. Diese Vorgehensweise wird als *Mandatory Access Control* bezeichnet, kurz MAC. Wird eine Regel verletzt, verhindert SELinux die Operation oder protokolliert eine Warnung. Das regelverletzende Programm wird durch SELinux nicht beendet. Es hängt vom Programm ab, wie es darauf reagiert, dass es auf eine bestimmte Datei nicht zugreifen kann oder eine Netzwerkschnittstelle nicht nutzen kann.

MAC-Regeln ermöglichen eine sehr viel engmaschigere Sicherheitskontrolle als das Unix-Zugriffssystem. Mit ihnen kann man einem Programm unabhängig von Unix-Zugriffsrechten bzw. -Accounts den Zugriff auf bestimmte Verzeichnisse oder Netzwerkfunktionen generell verbieten. Da diese Regeln auf Kernelebene überwacht werden, gelten sie selbst dann noch, wenn das Programm aufgrund eines Fehlers bzw. Sicherheitsmangels außer Kontrolle gerät.

SELinux ist sauber, obwohl der Code von der NSA entwickelt wurde

Die *National Security Agency* ist ein Nachrichtendienst der USA, der zuletzt aufgrund der umfassenden Überwachung des gesamten Internet-Verkehrs eine Menge negative Presse auf sich zog. Obwohl SELinux also gewissermaßen aus Geheimdienstkreisen stammt, besteht keine Gefahr, dass Linux auf diese Weise um Überwachungsfunktionen erweitert wurde: Der SELinux-Code ist öffentlich, wurde von vielen unabhängigen Experten kontrolliert und verbessert und ist Bestandteil des offiziellen Kernels. Wenn die NSA Sie und andere überwacht, dann sicher nicht durch eine Hintertür in SELinux.

SELinux-Regeln

Ohne entsprechende Regeln ist SELinux wirkungslos. Ob ein System durch SELinux sicherer wird, hängt somit vor allem von der Qualität der Regeln ab. Von den gängigen Distributoren hat bisher nur Red Hat intensiv Zeit und Mühe in die Entwicklung derartiger Regeln investiert. Dabei dient Fedora gewissermaßen als Testvehikel. Was sich dort bewährt, findet schließlich Eingang in die Red-Hat-Enterprise-Versionen (RHEL).

Kritik an SELinux

SELinux ist nicht unumstritten. Die zwei wichtigsten Kritikpunkte sind:

- Dateien müssen mit erweiterten Attributen (EAs, siehe Abschnitt 15.7) gekennzeichnet werden, um ein Zusammenspiel mit SELinux zu gewährleisten. Das erfordert EA-kompatible Dateisysteme (NFS ist ungeeignet!) und führt zu Problemen bei Updates und Backups.
- Das größte Problem von SELinux ist seine riesige Komplexität. Bereits die Absicherung der wichtigsten Netzwerkdienste erfordert Tausende von Regeln. Nur wenige Experten sind in der Lage, die Wirksamkeit dieser Regeln zu beurteilen. Den aktuellen Regelwerken fehlt zudem eine schlüssige Dokumentation. Aus diesem Grund sind durchschnittliche Linux-Anwender nicht in der Lage, SELinux-Regeln an eigene Erfordernisse anzupassen.

  SELinux wird deswegen von der Mehrheit seiner Anwender zu Recht als »Blackbox« betrachtet. Die Komplexität führt beinahe zwangsläufig zu Implementierungsfehlern und verleitet dazu, das System beim ersten Problem komplett auszuschalten.

Alternativen

Die populärste Alternative zu SELinux ist das von SUSE und Ubuntu eingesetzte System AppArmor (siehe Abschnitt 42.2). Daneben hat mit Version 2.6.25 ein weiteres MAC-System namens Smack Einzug in den Kernel gefunden. Smack kommt primär in Embedded-Linux-Systemen zum Einsatz.

SELinux-Interna und -Praxis

SELinux steht auf zwei Fundamenten: Einerseits setzt es die richtige Kennzeichnung aller Dateien und Prozesse durch einen sogenannten Sicherheitskontext voraus, andererseits beruht es auf Regeln, die von den überwachten Prozessen eingehalten werden müssen.

Sicherheitskontext

SELinux basiert darauf, dass jedes Objekt (z. B. Dateien) und jedes Subjekt (z. B. Prozesse) mit einem Sicherheitskontext verbunden ist. Bei Dateien wird der Dateikontext in Form von erweiterten Attributen gespeichert (EAs, siehe Abschnitt 15.7). Die Sicherheitsinformationen sind damit unmittelbar mit der Datei verbunden und unabhängig vom Namen der Datei. Den Sicherheitskontext einer Datei ermitteln Sie

am einfachsten mit `ls -Z`. Alternativ funktioniert auch `getfattr -n security.selinux -d` *dateiname*.

```
user$  ls -Z /usr/sbin/httpd
... system_u:object_r:httpd_exec_t:s0   /usr/sbin/httpd
user$  ls -Z /etc/httpd/conf/httpd.conf
... system_u:object_r:httpd_config_t:s0 /etc/httpd/conf/httpd.conf
user$  getfattr -n security.selinux -d /etc/httpd/conf/httpd.conf
getfattr: Removing leading '/' from absolute path names
# file: etc/httpd/conf/httpd.conf
security.selinux="system_u:object_r:httpd_config_t:s0\000"
```

chcon und restorecon

SELinux steht und fällt damit, dass zu allen Dateien der richtige Kontext gespeichert ist. Damit dies auch funktioniert, wenn Sie nach der Installation neue Dateien erzeugen, gibt es für viele Verzeichnisse SELinux-Regeln, die den darin erzeugten neuen Dateien automatisch den passenden Kontext zuweisen. Wenn dieser Automatismus versagt, z. B. beim Verschieben von Dateien aus einem anderen Verzeichnis, können Sie den Kontext korrigieren bzw. neu einstellen.

Sofern sich Ihre Dateien in den von SELinux vorgesehenen Verzeichnissen befinden, führt `restorecon` am schnellsten zum Ziel. Durch das folgende Kommando wird der Kontext aller im `DocumentRoot`-Verzeichnis von Apache gespeicherten Dateien richtig eingestellt:

```
root#  restorecon -R -v /var/www/html/*
```

Wenn Sie Dateien an einem anderen Ort gespeichert haben, z. B. HTML-Dateien im Verzeichnis `/var/myotherserver`, müssen Sie hingegen mit `chcon` den richtigen Kontext einstellen:

```
root#  chcon -R system_u:object_r:httpd_sys_content_t:s0 /var/myotherserver
```

Jetzt bleibt noch eine Frage offen: Woher wissen Sie, welcher Kontext erforderlich ist? Die Antwort geben `man`-Seiten, die die SELinux-Regeln für diverse Programme dokumentieren. `man apache_selinux` beschreibt beispielsweise die Regeln und vorgesehenen Kontexte für Apache. Eine lange Liste aller derartigen `man`-Seiten liefert das folgende Kommando:

```
root#  rpm -qd selinux-policy-devel
```

Prozesskontext (Domäne)

Bei Prozessen wird der Kontext oft als »Domäne« bezeichnet. Den Sicherheitskontext eines Prozesses (einer Domäne) ermitteln Sie mit `ps axZ`. Im Regelfall übernimmt ein Prozess den Kontext des Accounts, aus dem er gestartet wird. Der Kontext kann aber auch automatisch nach dem Start durch eine SELinux-Regel verändert werden. Das ist notwendig, wenn ein bestimmtes Programm (z. B. Firefox) unabhängig davon, von wem bzw. wie es gestartet wird, einen bestimmten Kontext erhalten soll.

```
user$  ps axZ | grep httpd
unconfined_u:system_r:httpd_t:s0 2373 ?    Ss     0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 2376 ?    S      0:00 /usr/sbin/httpd
...
```

Der Sicherheitskontext besteht aus drei oder vier Teilen, die durch Doppelpunkte getrennt sind:

benutzer:rolle:typ:mls-komponente

Am wichtigsten ist der dritte Teil, der den Typ der Datei bzw. des Prozesses angibt. Die meisten SELinux-Regeln werten diese Information aus. Eine detaillierte Beschreibung aller vier Teile des Sicherheitskontexts finden Sie hier:

https://fedoraproject.org/wiki/Security_context

Regeln

Die allgemeine Syntax einer typischen SELinux-Regel sieht so aus:

```
allow type1_t type2_t:class { operations };
```

Dazu ein konkretes Beispiel: Die folgende Regel erlaubt es Prozessen, deren Kontexttyp `httpd_t` lautet, in Verzeichnissen mit dem Kontexttyp `httpd_log_t` neue Dateien zu erzeugen:

```
allow httpd_t httpd_log_t:dir create;
```

SELinux-Regelwerke

Ein typisches SELinux-Regelwerk besteht aus Zehntausenden solcher Regeln! Aus Geschwindigkeitsgründen erwartet SELinux die Regeln nicht als Text, sondern in einem binären Format. In einer Analogie zum Programmieren kann man dabei auch von einem Kompilat sprechen. Eine Zusammenfassung der Schritte, wie Sie dem vorhandenen Regelwerk ein eigenes Regelmodul hinzufügen, finden Sie in der SELinux-FAQ:

http://docs.fedoraproject.org/en-US/Fedora/13/html/SELinux_FAQ

Unter aktuellen Fedora- und RHEL-Versionen kommt standardmäßig das Regelwerk `targeted` zum Einsatz. Es überwacht ausgewählte Programme und Server-Dienste und ist in den unzähligen `man`-Seiten des Pakets `selinux-policy-devel` dokumentiert.

Alternativ kann das speziell für Server konzipierte Regelwerk MLS (*Multilevel Security*) installiert werden. Es befindet sich im Paket `selinux-policy-mls`. Das Ziel dieses Regelwerks ist es, mit RHEL eine Zertifizierung der Klasse EAL 4 zu erreichen. Diese Zertifizierung wird in den USA für bestimmte, oft militärische Anwendungen verlangt:

http://fedoraproject.org/wiki/SELinux/FedoraMLSHowto

SELinux-Parameter (Booleans)

Mittlerweile ist Ihnen wahrscheinlich klar, dass Änderungen am Regelwerk schwierig sind. Um ein gewisses Maß der Anpassung auch ohne Regeländerungen zu ermöglichen, enthält das Regelwerk `targeted` diverse boolesche Parameter, die Sie im laufenden Betrieb verändern können. Unter Fedora/Red Hat verwenden Sie dazu am einfachsten die grafische Benutzeroberfläche `system-config-selinux` (siehe Abbildung 42.1), die im Paket `policycoreutils-gui` versteckt ist. Dieses Paket ist standardmäßig nicht installiert.

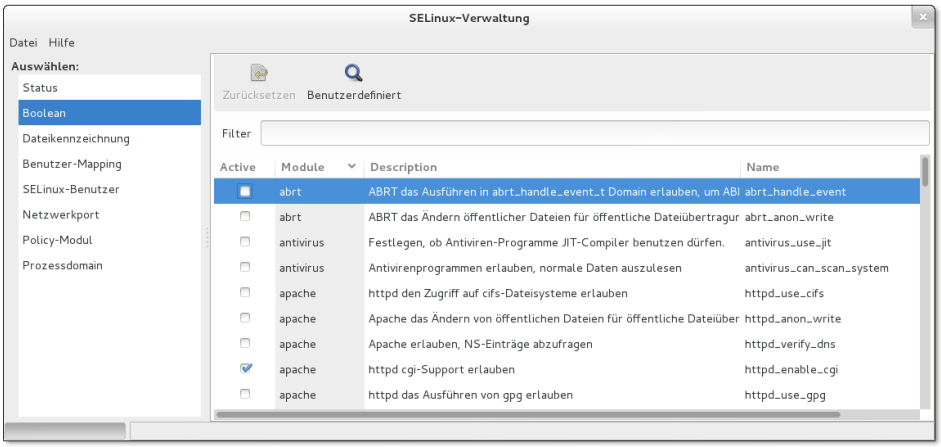


Abbildung 42.1 SELinux-Boolean-Parameter ändern

Alternativ ermittelt `getsebool` den Wert boolescher Konfigurationsparameter. `setsebool` verändert derartige Parameter und erlaubt im folgenden Beispiel, dass Apache CGI-Scripts ausführen darf:

```
root#  setsebool -P httpd_enable_cgi 1
```

Start und Konfiguration

SELinux ist als Teil des Kernels implementiert. Ein expliziter Start durch das Init-System ist daher nicht erforderlich. Ebenso wenig gibt es einen SELinux-Dämon oder andere Hintergrundprozesse.

Die Konfiguration erfolgt durch die Dateien im Verzeichnis `/etc/selinux`. Von zentraler Bedeutung ist `/etc/selinux/config`. Die Datei gibt an, in welchem Modus SELinux läuft (*Enforcing*, *Permissive* oder *Disabled*) und welches Regelwerk gilt. Änderungen an dieser Datei werden allerdings nur durch einen Neustart wirksam.

```
# /etc/selinux/config
SELINUX=enforcing
SELINUXTYPE=targeted
```

Status

`sestatus` ermittelt den aktuellen Status von SELinux. Auf dem Testrechner ist SELinux mit dem Regelwerk *Targeted* aktiv:

```
root#  sestatus
SELinux status:           enabled
SELinuxfs mount:          /sys/fs/selinux
SELinux root directory:   /etc/selinux
Loaded policy name:       targeted
Current mode:             enforcing
...
```

SELinux-Probleme beheben

Grundsätzlich bestehen die folgenden Möglichkeiten, auf SELinux-Regelverstöße zu reagieren:

- Sie suchen nach einem für Ihr Problem passenden Boolean-Parameter im Regelwerk und stellen diesen mit `system-config-selinux` oder `setsebool` richtig ein.
- Sie ändern die Kontextinformationen der betroffenen Dateien.
- Sie ändern bzw. erweitern das Regelwerk. Das erfordert allerdings wesentlich mehr SELinux-Kenntnisse, als in diesem Abschnitt vermittelt werden.
- Sie schalten SELinux ganz aus.

Nicht immer sind durch SELinux verursachte Probleme auf den ersten Blick zu erkennen. Wenn Sie beispielsweise einen Verzeichnisbaum mit HTML-Dateien mit `cp -a` in das Verzeichnis `/var/www/html` kopieren, können die HTML-Dateien anschließend nicht von Apache gelesen werden. Der Grund: Die `cp`-Option `-a` bewirkt, dass auch die Extended Attributes und damit die SELinux-Kontextinformationen mitkopiert werden. Dieser Umstand verhindert, dass die kopierten Dateien in `/var/www/html` durch eine SELinux-Regel automatisch die richtigen Kontextinformationen erhalten. Diese Probleme vermeiden Sie, wenn Sie statt `cp -a` die Variante `cp -r` einsetzen.

Apache selbst weiß nichts von SELinux. Das Programm bemerkt nur, dass es nicht auf die Dateien zugreifen kann, und liefert die in die Irre führende Fehlermeldung *You don't have permission to access <filename>*. Erst ein Blick in `/var/log/messages` macht klar, dass die Zugriffsprobleme von SELinux verursacht wurden:

```
root#  less /var/log/messages
...
Aug 31 12:45:45 fedora setroubleshoot: SELinux is preventing /usr/sbin/httpd
  from read access on the file tst. For complete SELinux messages run
  sealert -l dccb472d-6dd8-49d2-b7d7-2658e082c805
```

Wenn Sie nun, wie in der Protokolldatei angegeben, `sealert` ausführen, erhalten Sie einen fast 100-zeiligen Text, aus dem die wichtigsten Passagen hier wiedergegeben sind. Die Mischung von Deutsch und Englisch ist wahrlich lesenswert!

```
root#  sealert -l dccb472d-6dd8-49d2-b7d7-2658e082c805
SELinux is preventing /usr/sbin/httpd from read access on the file index.html.
```

```
*****  Plugin catchall_boolean (89.3 confidence) suggests  ******************
If sie möchten allow httpd to read user content Then you must tell SELinux
about this by enabling the 'httpd_read_user_content' boolean. You can read
'user_selinux' man page for more details.  Do setsebool -P
httpd_read_user_content 1

*****  Plugin catchall (11.6 confidence) suggests  **************************
If sie denken, dass httpd standardmässig erlaubt sein sollte, read Zugriff auf
index.html file zu erhalten.  Then sie sollten dies als Fehler melden.  Um
diesen Zugriff zu erlauben, können Sie ein lokales Richtlinien-Modul erstellen.
Do zugriff jetzt erlauben, indem Sie die nachfolgenden Befehle ausführen:
# grep httpd /var/log/audit/audit.log | audit2allow -M mypol
# semodule -i mypol.pp
...
```

Nicht nur die sprachliche Qualität lässt zu wünschen übrig, auch der Inhalt der Lösungsvorschläge ist unbrauchbar. Um das Problem tatsächlich zu beheben, müssen Sie die Kontextinformationen der betroffenen Dateien mit `restorecon` richtig einstellen:

```
root#  restorecon -R -v /var/www/html/*
```

SELinux deaktivieren

Um SELinux vorübergehend zu aktivieren, starten Sie `system-config-selinux` und aktivieren den Modus PERMISSIVE. Damit läuft SELinux weiter und protokolliert Regelverstöße in `/var/log/messages`. SELinux lässt den Regelverstoß aber zu und blockiert das betroffene Programm nicht. Dieselbe Wirkung hat auch das Kommando `setenforce 0`.

Natürlich können Sie SELinux in `system-config-selinux` auch ganz abschalten (Einstellung DISABLED). Das ist aber nur empfehlenswert, wenn Sie SELinux auch in Zukunft nicht mehr nutzen möchten. Der Grund: Wenn SELinux deaktiviert wird, sind auch alle Regeln außer Kraft, die neuen Dateien die SELinux-Kontextinformationen zuordnen. Wird SELinux später wieder aktiviert, verursachen die Dateien mit fehlenden Kontextinformationen Probleme. Bei der späteren Richtigstellung der Kontextdaten hilft das Kommando `restorecon`, der Prozess ist aber mühsam und fehleranfällig.

Sollte SELinux bereits während des Systemstarts Probleme verursachen, verhindert der Kernelparameter `selinux=0`, dass das SELinux-System gestartet wird. Eine Reaktivierung ist dann aber erst beim nächsten Neustart möglich. Alternativ bewirkt der Parameter `enforcing=0`, dass SELinux zwar gestartet wird, Regelübertritte aber nur protokolliert.

42.2 AppArmor

Anstatt das komplexe SELinux-System für die eigenen Distributionen zu adaptieren, kaufte Novell 2005 die Firma Immunix, gab dessen Sicherheitslösung Subdomain den neuen Namen AppArmor, stellte sie unter die GPL und entwickelte einige YaST-Module zur Administration. Mit Kernelversion 2.6.36 erhielt AppArmor gewissermaßen den Ritterschlag der Kernelentwickler und wurde offiziell in den Kernel integriert. Danach ist bei SUSE rund um AppArmor Stille eingekehrt. AppArmor ist zwar weiter im Einsatz, in den letzten Jahren sind aber weder an den Regeln noch an den Administrationswerkzeugen merkbare Verbesserungen durchgeführt worden. Um die AppArmor-Weiterentwicklung kümmern sich seither vor allem von Canonical angestellte Entwickler.

AppArmor ist wie SELinux ein MAC-Sicherheitssystem (*Mandatory Access Control*). Im Unterschied zu SELinux basieren AppArmor-Regeln auf absoluten Dateinamen. Daher ist eine eigene Kennzeichnung aller Dateien durch EAs nicht erforderlich; zudem funktioniert AppArmor auch für Dateisysteme, die keine EAs unterstützen. In den AppArmor-Regeln sind Jokerzeichen erlaubt. Aus diesem Grund kommt AppArmor für typische Anwendungsfälle mit wesentlich weniger Regeln aus als SELinux.

Kritik

Naturgemäß gibt es auch Argumente, die gegen AppArmor sprechen:

- Sicherheitsexperten von Red Hat sind der Meinung, dass absolute Pfade in den Regeln ein inhärentes Sicherheitsrisiko sind. Der Schutz von AppArmor kann durch das Umbenennen von Dateien oder Verzeichnissen umgangen werden – was natürlich nur gelingt, wenn ein Angreifer dazu bereits ausreichende Rechte hat.
- Das Regelwerk für AppArmor ist nicht so umfassend wie das von SELinux. Standardmäßig werden weniger Programme geschützt. Zwar ist es einfacher als bei SELinux, selbst Regeln zu erstellen bzw. zu ändern, aber diese Art der Do-it-yourself-Sicherheit hinterlässt einen wenig professionellen Eindruck.

Links

Dieser Abschnitt gibt nur eine Einführung zu AppArmor. Weitere Informationen finden Sie hier:

https://www.suse.com/documentation/apparmor
https://help.ubuntu.com/community/AppArmor
https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/AppArmorProfiles

AppArmor unter Ubuntu

Die folgenden Ausführungen beziehen sich auf AppArmor, wie es unter Ubuntu aktiv ist. SUSE-spezifische Anmerkungen folgen am Ende dieses Abschnitts.

AppArmor ist unter Ubuntu standardmäßig im Kernel integriert. Das Sicherheitssystem wird durch das Init-V-Script `/etc/init.d/apparmor` gestartet. Es berücksichtigt die Grundkonfiguration aus dem Verzeichnis `/etc/apparmor` und lädt alle Regeldateien aus dem Verzeichnis `/etc/apparmor.d`. Das Init-Script greift auf Funktionen zurück, die in `/etc/apparmor/rc.apparmor.functions` definiert sind.

Das Kommando `aa-status` gibt einen Überblick über den gegenwärtigen Zustand von AppArmor. Das Kommando liefert sowohl eine Liste aller Profile als auch eine Liste der tatsächlich überwachten Prozesse. Die folgende Liste zeigt an, welche Dienste eines Ubuntu-Root-Servers überwacht werden:

```
root#  aa-status
apparmor module is loaded.
23 profiles are loaded.
23 profiles are in enforce mode.
   /sbin/dhclient
   ...
   /usr/sbin/mysqld
   /usr/sbin/tcpdump
3 processes are in enforce mode.
   /sbin/dhclient (2251)
   /usr/sbin/cupsd (527)
   /usr/sbin/mysqld (1045)
```

Beim Start von AppArmor wird das Dateisystem `securityfs` in das Verzeichnis `/sys/kernel/security` eingebunden. Seine Dateien geben Auskunft über aktive Profile, die Anzahl der aufgetretenen Regelverletzungen etc.

Regeln (Profile)

Die Wirkung von AppArmor steht und fällt mit den Überwachungsregeln. Diese Regeln werden auch »Profile« genannt und befinden sich in den Dateien des Verzeichnisses `/etc/apparmor.d/`. Beispielsweise enthält die Datei `usr.sbin.cupsd` die Profile für CUPS und den CUPS-PDF-Treiber.

Die offiziell gewarteten Regelprofile werden üblicherweise vom jeweiligen Paket zur Verfügung gestellt. Das Regelprofil `user.sbin.cupsd` steht also nur dann zur Verfügung, wenn Sie das Druckersystem CUPS installiert haben. Aus diesem Grund ist `/etc/apparmor.d` nach einer Ubuntu-Server-Installation anfänglich fast leer und füllt sich erst in dem Ausmaß, in dem Sie Server-Dienste installieren.

Außerdem können Sie das Paket `apparmor-profiles` aus der `universe`-Paketquelle installieren. Es enthält zahlreiche weitere Profile, die aber nicht offiziell unterstützt

und gewartet werden. Die meisten Profile laufen nur im sogenannten `complain`-Modus: In diesem Modus werden Regelverstöße zwar protokolliert, aber nicht geahndet. Mit den Kommandos `aa-enforce` und `aa-complain` aus dem Paket `apparmor-utils` können Sie den Modus eines Profils ändern. An die beiden Kommandos übergeben Sie den vollständigen Pfad des zu überwachenden Programms:

```
root#  aa-enforce /usr/sbin/dnsmasq
Setting /usr/sbin/dnsmasq to enforce mode.
root#  aa-complain /usr/sbin/dnsmasq
Setting /usr/sbin/dnsmasq to complain mode.
```

Alternativ können Sie an `aa-enforce` und `aa-complain` auch die Dateinamen der Profildateien übergeben. Das macht es einfach, den Modus mehrerer Profile auf einmal zu verändern:

```
root#  cd /etc/apparmor.d
root#  aa-enforce usr.lib.dovecot*
```

Bei Server-Diensten müssen Sie nach einer Aktivierung eines AppArmor-Profils auch das jeweilige Programm neu starten:

```
root#  service <name> restart
```

Losgelöst vom AppArmor-Modus sind Profile natürlich nur dann relevant, wenn das betreffende Programm tatsächlich ausgeführt wird. Welche Programme momentan aktiv überwacht werden, verrät das oben erwähnte Kommando `aa-status`.

Aufbau von Regeldateien

Regeldateien, die bei AppArmor *Profile* heißen, liegen in einem einfachen Textformat vor. Die folgenden Zeilen zeigen die AppArmor-Regeln für `mysqld`:

```
#include <tunables/global>

/usr/sbin/mysqld {
  #include <abstractions/base>
  #include <abstractions/nameservice>2007
  #include <abstractions/user-tmp>
  #include <abstractions/mysql>
  #include <abstractions/winbind>
  #include <abstractions/base>
  capability dac_override,ameservice>
  capability sys_resource,ser-tmp>
  capability setgid,ions/mysql>
  capability setuid,ions/winbind>

  network tcp,ac_override,
  capability sys_resource,
  /etc/hosts.allow r,
  /etc/hosts.deny r,
```

```
  /etc/mysql/*.pem r,
  /etc/mysql/conf.d/ r,
  /etc/mysql/conf.d/* r,
  /etc/mysql/*.cnf r,
  /usr/lib/mysql/plugin/ r,
  /usr/lib/mysql/plugin/*.so* mr,
  /usr/sbin/mysqld mr,,
  /usr/share/mysql/** r,
  /var/log/mysql.log rw,
  /var/log/mysql.err rw, r,
  /var/lib/mysql/ r,gin/*.so* mr,
  /var/lib/mysql/** rwk,
  /var/log/mysql/ r,* r,
  /var/log/mysql/* rw,w,
  /var/run/mysqld/mysqld.pid rw,
  /var/run/mysqld/mysqld.sock w,
  /run/mysqld/mysqld.pid rw,
  /run/mysqld/mysqld.sock w,
  /var/log/mysql/* rw,
  /sys/devices/system/cpu/ r,rw,
:
  # Site-specific additions and overrides. See local/README for details.
  #include <local/usr.sbin.mysqld>
}
```

In den Regeldateien werden zuerst einige Include-Dateien gelesen und dann grundlegende Merkmale (siehe `man capabilities`) des Programms festgelegt. Die weiteren Regeln geben an, welche Dateien das Programm wie nutzen darf.

In den AppArmor-Regeldateien gilt das Jokerzeichen `*` als Platzhalter für eine beliebige Anzahl von Zeichen. `**` hat eine ähnliche Bedeutung, schließt aber das Zeichen `/` ein und umfasst damit auch Dateien in allen Unterverzeichnissen. Die Zugriffsrechte werden durch Buchstaben oder Buchstabenkombinationen ausgedrückt, deren Bedeutung im AppArmor-Administration-Manual genau beschrieben ist. Tabelle 42.1 beschreibt die wichtigsten Buchstaben. Die `?x`-Kombinationen steuern die Rechte von Sub-Prozessen, die das Hauptprogramm startet.

Regelparameter (tunables)

AppArmor sieht einen Mechanismus vor, um einzelne Parameter der Regeln auf eine einfache Weise zu verändern. Diese Parameter sind in den Dateien des Verzeichnisses `/etc/apparmor.d/tunables` definiert. In der aktuellen Implementierung gibt es allerdings nur wenige Parameter, mit denen Sie beispielsweise den Ort der Heimatverzeichnisse individuell einstellen können. Wenn Ihr Server außer `/home` auch andere Orte für Heimatverzeichnisse vorsieht, müssen Sie die Variable `@{HOMEDIRS}` verändern.

Kürzel	Bedeutung
r	erlaubt Lesezugriffe (read).
w	erlaubt Schreibzugriffe (write).
a	erlaubt es, die Datei zu erweitern (append).
l	wendet auf harte Links dieselben Regeln wie für die Ursprungsdatei an (link).
k	erlaubt es, die Datei zu blockieren (lock).
m	lässt die mmap-Funktion zu (allow executable mapping).
ix	Das Programm erbt die Regeln des Basisprogramms (inherent execute).
px	Das Programm hat ein eigenes AppArmor-Profil (discrete profile execute).
ux	führt das Programm ohne AppArmor-Regeln aus (unconstrained execute).

Tabelle 42.1 Elementare AppArmor-Zugriffsrechte

```
# Datei /etc/apparmor.d/tunables/home
@{HOME}=@{HOMEDIRS}/*/ /root/
@{HOMEDIRS}=/home/ /home1/ /myhome/
```

Logging und Wartung

Details über stattgefundene Regelverletzungen im complain- oder enforce-Modus werden in Form von Kernelmeldungen weitergegeben und standardmäßig in den Dateien /var/log/kern.log und /var/log/syslog aufgezeichnet. Sie erkennen AppArmor-Meldungen am Schlüsselwort audit.

```
root#  grep audit /var/log/kern.log
[...] audit(1238580174.435:3): type=1503 operation="inode_permission"
        requested_mask="a::" denied_mask="a::" name="/dev/tty"
        pid=6345 profile="/usr/sbin/cupsd" namespace="default"
[...] audit(1238580174.435:4): type=1503 operation="inode_permission"
        requested_mask="w::" denied_mask="w::" name="/etc/krb5.conf"
        pid=6345 profile="/usr/sbin/cupsd" namespace="default"
```

Oft sind die Audit-Meldungen ein Indikator dafür, dass die AppArmor-Regeln unvollständig sind. Ein Fehlverhalten des Programms ist natürlich auch möglich, aber eher unwahrscheinlich. Mit Sicherheit kann das nur ein Experte für das jeweilige Programm beurteilen. Insofern ist eine angemessene Reaktion auf Regelübertretungen schwierig.

Wenn Sie vermuten, dass das betroffene Programm ordnungsgemäß funktioniert, sollten Sie das Profil in den complain-Modus umschalten und die Audit-Meldung im Ubuntu-Bug-System melden (*https://bugs.launchpad.net*). Sie können auch versuchen, das Profil um eine Regel zu erweitern, die den gemeldeten Vorgang erlaubt. Oder Sie ignorieren die Meldung einfach, sofern das betroffene Programm anstandslos weiterläuft.

AppArmor unter SUSE

Konfiguration und Start

Seit openSUSE 12.1 ist AppArmor nicht mehr standardmäßig installiert. Wenn Sie AppArmor verwenden möchten, müssen Sie zuerst die AppArmor-Pakete installieren. Am einfachsten aktivieren Sie dazu im YaST-Modul SOFTWARE INSTALLIEREN das Schema APPARMOR.

AppArmor wird am Beginn des Init-V-Prozesses durch das Script `/etc/init.d/boot.apparmor` gestartet. Dieses Script greift auf Funktionen zurück, die in `/lib/apparmor/rc.apparmor.functions` definiert sind. `boot.apparmor` liest die Grundkonfiguration aus dem Verzeichnis `/etc/apparmor` und lädt alle Regeldateien aus dem Verzeichnis `/etc/apparmor.d`.

Änderungen an der Konfiguration werden erst wirksam, wenn Sie AppArmor neu starten bzw. die Regeldateien neu einlesen:

```
root# /etc/init.d/boot.apparmor restart    (AppArmor neu starten)
root# /etc/init.d/boot.apparmor reload     (AppArmor-Regeln neu laden)
```

YaST

Zur Steuerung von AppArmor sieht YaST das gleichnamige Modul vor. Die Bedienung dieses Moduls ist leider unübersichtlich, manche Dialoge funktionieren gar nicht. Als ich das Modul zuletzt unter openSUSE 12.3 getestet habe, gelang damit nicht einmal die Aktivierung bzw. Deaktivierung einzelner Profile. Dazu setzen Sie besser die Kommandos `aa-enforce` und `aa-complain` ein.

Kapitel 43
KVM

Seit KVM (*Kernel-based Virtual Machine*) 2007 in den offiziellen Kernelcode integriert wurde, hat sich diese Linux-spezifische Virtualisierungstechnik vor allem im Server- und Enterprise-Segment etabliert. Red Hat Enterprise Linux 6 setzt voll auf KVM, aktuelle Versionen des SUSE Linux Enterprise Servers bieten KVM als gleichwertige Option zu Xen an. Debian und Ubuntu enthalten standardmäßig KVM-Pakete.

Dieses Kapitel führt zuerst in die Grundlagen von KVM ein und konzentriert sich dann auf die Server-Virtualisierung mit KVM: Damit können auf einem Rechner mehrere virtuelle Linux-Server laufen. In der Praxis wird das häufig gemacht, um die Server-Funktionen so gut wie möglich voneinander zu trennen und so die Sicherheit zu maximieren. Aber auch praktische Gründe sprechen oft für die Server-Virtualisierung: Während der eine Anwender für seine Website spezielle Apache-Module braucht, will ein anderer die neueste MySQL-Version einsetzen. Wenn viele derartige Sonderwünsche auf *einem* System erfüllt werden, führt das rasch zu unerwünschten Nebenwirkungen und Instabilitäten.

KVM ist prinzipiell auch zur Desktop-Virtualisierung geeignet, dieser Aspekt steht hier aber im Hintergrund. Für den Desktop-Einsatz empfehle ich Ihnen VirtualBox, das einfacher zu bedienen ist. Sollten Sie dennoch KVM auf Desktop-Systemen einsetzen wollen, können Sie einen Blick auf das Gnome-Programm »Boxes« werfen: Gnome-typisch ist die Bedienung sehr einfach, allerdings bietet das Programm selbst für einfache Anwendungen zu wenige Konfigurationsmöglichkeiten.

Links

Dieses Kapitel kann nur eine Einführung in KVM geben. Weitere Informationen finden Sie hier:

http://www.linux-kvm.org	(offizielle Website)
http://www.linux-kvm.com	(News, Blog, Forum)
https://help.ubuntu.com/community/KVM	
http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux	

43.1 Grundlagen

KVM versus QEMU

Das Programm QEMU emuliert verschiedene CPUs und elementare Hardware-Komponenten eines Rechners, also seine Netzwerkkarte, das CD-Laufwerk etc. QEMU ist auch in der Lage, zur Wirts-CPU inkompatible Prozessoren zu emulieren (ARM, Sparc, PowerPC, MIPS etc.).

KVM ist ein Kernelmodul, das seine Wirkung erst in Kombination mit QEMU entfaltet. KVM setzt eine CPU mit Funktionen zur Hardware-Virtualisierung voraus und macht aus dem Emulator QEMU ein Hardware-Virtualisierungssystem. Die Eleganz von KVM besteht darin, dass es typische Hypervisor-Aufgaben nicht selbst ausführt, sondern dazu auf Speicher- und Prozessverwaltungsfunktionen des Linux-Kernels zurückgreift. Die Nutzung der KVM-Funktionen erfolgt über die Device-Datei `/dev/kvm`.

Hardware-Voraussetzungen

KVM funktioniert nur, wenn der Prozessor des Host-Systems Virtualisierungsfunktionen unterstützt (Intel-VT bzw. AMD-V). Das ist bei den meisten aktuellen Prozessoren der Fall. Zu den Ausnahmen zählen sehr preisgünstige CPUs für Billig-PCs bzw. -Notebooks sowie die Atom-Prozessoren von Intel. Um festzustellen, ob Ihre CPU bei der Hardware-Virtualisierung hilft (Intel-VT oder AMD-V), führen Sie das folgende `egrep`-Kommando aus. Wenn das Ergebnis leer ist, unterstützt Ihre CPU keine Virtualisierung oder die Funktion wurde im BIOS/EFI deaktiviert.

```
user$  egrep '^flags.*(vmx|svm)' /proc/cpuinfo
flags :...  vmx ...
```

Bei Ubuntu-Systemen können Sie noch einfacher das Kommando `kvm-ok` aus dem Paket `cpu-checker` ausführen:

```
user$  kvm-ok
INFO: Your CPU supports KVM extensions
INFO: /dev/kvm exists
KVM acceleration can be used
```

Im weiteren Verlauf dieses Kapitels setze ich voraus, dass Ihre CPU KVM-kompatibel ist. Sollte das nicht der Fall sein, funktioniert KVM scheinbar auch. Tatsächlich werden die virtuellen Maschinen aber nur durch QEMU und somit ohne KVM-Unterstützung ausgeführt und laufen dann wesentlich langsamer.

Virtualisierungsfunktionen im BIOS/EFI aktivieren

Erstaunlich sind die vorhandenen Virtualisierungsfunktionen der CPU durch das BIOS oder EFI deaktiviert. Abhilfe: Öffnen Sie beim Rechnerstart die BIOS/EFI-Dialoge, und suchen Sie nach der betreffenden Einstellung.

Kernelmodule

KVM stellt seine Funktionen in drei Kernelmodulen zur Verfügung: Die Grundfunktionen befinden sich im Modul `kvm`, die Intel-VT-spezifischen Funktionen in `kvm-intel`, die AMD-V-spezifischen Funktionen in `kvm-amd`. Damit Sie KVM nutzen können, muss das zu Ihrer Hardware passende KVM-Modul geladen werden. Das Modul `kvm` wird dabei gleich mitgeladen. Bei den meisten Distributionen kümmert sich das Init-System darum. Sollte das nicht funktionieren, greifen Sie manuell ein:

```
root#  modprobe kvm-intel  (für Intel-VT-Prozessoren)
root#  modprobe kvm-amd    (für AMD-V-Prozessoren)
```

KVM-Kommando

Um eine virtuelle Maschine mit QEMU oder KVM auszuführen, können Sie direkt das KVM-Kommando ausführen. Es wird je nach Distribution unterschiedlich angesprochen (siehe Tabelle 43.1).

Distribution	Paket	KVM-Kommando
Debian	qemu-kvm	kvm
Fedora	qemu-kvm	qemu-kvm
openSUSE	kvm	qemu-kvm
RHEL 6	qemu-kvm	/usr/libexec/qemu-kvm
Ubuntu	qemu-system-x86	kvm -enable-kvm

Tabelle 43.1 KVM-Paketname und -Kommandoname

Nach dem Start des KVM-Kommandos wird die virtuelle Maschine in einem Fenster angezeigt oder muss durch einen VNC-Client gesteuert werden. Generell ist der direkte Einsatz des KVM-Kommandos aber selten zu empfehlen: Sie müssen die Hardware-Komponenten der virtuellen Maschine durch unzählige Optionen einstellen. Das macht den Einsatz von KVM unübersichtlich und fehleranfällig.

libvirt-Werkzeuge

Der Einsatz der diversen libvirt-Werkzeuge vereinfacht die Administration virtueller Maschinen erheblich:

- Der Virtual Machine Manager (Programm- bzw. Paketname `virt-manager`) hilft mit einer grafischen Benutzeroberfläche beim Einrichten und Ausführen virtueller Maschinen.
- Wenn Sie lieber im Terminal arbeiten, können Sie mit der Shell `virsh` virtuelle Maschinen erzeugen, starten und wieder stoppen sowie andere Administrationsarbeiten durchführen.
- Daneben gibt es diverse Kommandos für Spezialaufgaben: `virt-install` richtet eine neue virtuelle Maschine ein, `virt-clone` kopiert eine virtuelle Maschine, `virt-top` liefert ähnlich wie `top` eine Auflistung aller virtuellen Maschinen samt RAM- und CPU-Nutzung etc.

Distributionen

Mittlerweile stellen alle gängigen Distributionen KVM- und libvirt-Pakete zur Verfügung. Da die Entwicklung von KVM aber in einem sehr hohen Ausmaß von Red Hat betrieben wird, eignen sich RHEL oder RHEL-Clones wie CentOS besonders gut für den KVM-Einsatz. Wenn Sie die allerneuesten KVM-Features testen möchten, ist Fedora die ideale Spielwiese.

Natürlich können Sie auch mit anderen Distributionen arbeiten, Sie müssen sich dann aber damit abfinden, dass neue KVM-Funktionen nicht oder nur eingeschränkt nutzbar sind. Beispielsweise sind die libvirt-Werkzeuge in Ubuntu 12.04 nicht Spice-kompatibel, obwohl dieses besonders effiziente virtuelle Grafiksystem in wesentlich älteren RHEL-Versionen problemlos läuft, auch im Virtual Machine Manager.

Beachten Sie, dass Red Hat KVM-Pakete nur mit der 64-Bit-Version seiner Enterprise-Distribution ausliefert. Auf einem Virtualisierungs-Host sollte der Einsatz einer 64-Bit-Installation aber ohnedies selbstverständlich sein.

Erforderliche Pakete

Um virtuelle KVM-Maschinen auszuführen und mit den libvirt-Werkzeugen steuern zu können, müssen Sie die folgenden Pakete installieren:

```
root#  yum install qemu-kvm virt-manager python-virtinst   (Fedora, RHEL)
root#  apt-get install qemu-kvm virt-manager virtinst      (Ubuntu)
```

Unter Fedora und RHEL benötigen Sie `root`-Rechte zur Nutzung der libvirt-Werkzeuge. Unter Ubuntu müssen Sie hingegen ein Mitglied der Gruppe `libvirtd` sein. Das erreichen Sie mit dem folgenden Kommando, das allerdings erst nach einem Login wirksam wird:

```
root#  adduser loginname libvirtd                          (Ubuntu)
```

libvirt-Interna

`libvirt` ist eine Schnittstelle zur Verwaltung von virtuellen Maschinen und der dazugehörigen virtuellen Netzwerk- und Festplatten-Devices. Eine Voraussetzung für die Nutzung der libvirt-Werkzeuge besteht darin, dass auf dem Hostsystem der Dämon `libvirtd` läuft. Dieses Programm wird beim Hochfahren des Hostrechners durch das Init-System gestartet.

Die Steuerung der virtuellen Maschinen erfolgt wahlweise durch die Shell `virsh`, den Virtual Machine Manager oder durch andere libvirt-Kommandos. Jedes dieser Programme muss vorher eine Verbindung zum libvirt-Dämon herstellen. Der libvirt-Dämon erlaubt auch Netzwerkverbindungen, die üblicherweise durch SSH getunnelt werden.

Die libvirt-Werkzeuge können neben KVM auch das Virtualisierungssystem Xen steuern. In diesem Kapitel beziehe ich mich aber ausschließlich auf KVM.

KVM-Maschinen können via libvirt auf zwei verschiedenen Ebenen ausgeführt werden:

System- versus Benutzerebene

- **Benutzerebene** (`qemu:///session`): Diese Variante ist vor allem für die Desktop-Virtualisierung gedacht und gibt den virtuellen Maschinen weniger Zugriffsmöglichkeiten auf die Hardware des Hostrechners. Intern wird beim ersten Aufruf eines libvirt-Werkzeugs auf Benutzerebene ein eigener `libvirtd`-Prozess gestartet, dem nur die Rechte des aktuellen Benutzers zukommen. KVM-Maschinen auf Benutzerebene minimieren also die Sicherheitsrisiken durch die Virtualisierung.
- **Systemebene** (`qemu:///system`): Virtuelle Maschinen auf Systemebene sind besser für die Server-Virtualisierung geeignet, weil sie direkt auf Hardware-Komponenten des Hostrechners zugreifen können und mehr Möglichkeiten zur Integration der virtuellen Maschinen in das Netzwerk bestehen. Die libvirt-Prozesse kommunizieren dabei mit dem Dämon `libvirtd`, der mit `root`-Rechten läuft.

Fedora, RHEL 6

Bei der Kommunikation zwischen den libvirt-Werkzeugen und dem Dämon `libvirtd` bestehen starke Konfigurationsunterschiede zwischen den Distributionen. Ganz einfach ist es bei Fedora und RHEL: Wenn Sie mit `libvirtd` auf Systemebene kommunizieren möchten, benötigen Sie `root`-Rechte. Der Virtual Machine Manager kann zwar mit Benutzerrechten gestartet werden, das Programm erwartet aber unmittelbar nach dem Start die Angabe des `root`-Passworts.

Beachten Sie dabei, dass zwar die libvirt-Werkzeuge mit `root`-Rechten ausgeführt werden, nicht aber das eigentliche Virtualisierungskommando! Vielmehr starten die libvirt-Werkzeuge das Kommando `qemu-kvm` unter dem Benutzeraccount `qemu`. Auf diese Feinheit müssen Sie vor allem bei der richtigen Einstellung der Zugriffsrechte für Image- oder ISO-Dateien achten!

Ubuntu

Auch unter Ubuntu kommunizieren libvirt-Werkzeuge, die mit `root`-Rechten ausgeführt werden, mit `libvirtd` auf Systemebene. Aber auch libvirt-Kommandos, die nur mit Benutzerrechten ausgeführt werden, dürfen mit `libvirtd` auf Systemebene kommunizieren, sofern der Benutzer der Gruppe `libvirtd` angehört! Genau genommen ist entscheidend, ob der Benutzer auf die Datei `/var/run/libvirt/libvirt-sock` zugreifen darf. Diese Datei gehört `root` und der Gruppe `libvirtd`.

Die Zuordnung zur Gruppe `libvirtd` wird bei der Installation des Pakets `libvirt-bin` automatisch für den Benutzer hergestellt, der die Installation durchführt. Weitere Benutzer können mit dem folgenden Kommando der `libvirtd`-Gruppe hinzugefügt werden:

```
root# adduser loginname libvirtd      (Ubuntu)
```

Konfiguration

Die Konfigurationsdateien des libvirt-Systems befinden sich im Verzeichnis `/etc/libvirt`. Besonders interessant ist die in diesem Verzeichnis enthaltene Datei `qemu.conf`: Sie gibt diverse Grundeinstellungen für das KVM-Kommando vor. Die Datei steuert unter anderem die Defaulteinstellungen des VNC- bzw. Spice-Servers der virtuellen Maschine. Dabei kommt standardmäßig die IP-Adresse 127.0.0.1 zum Einsatz. Somit sind nur lokale Verbindungen zulässig, wobei eine Weiterleitung via SSH Port Forwarding möglich ist.

Außerdem werden die Eigenschaften jeder virtuellen Maschine in einer XML-Datei im Verzeichnis `/etc/libvirt/qemu` festgehalten. Die meisten Einstellungen sind ohne weitere Erklärung verständlich und korrespondieren direkt mit entsprechenden KVM- oder `virt-install`-Optionen. Im Detail ist das Format der libvirt-XML-Dateien auf folgender Seite dokumentiert:

http://libvirt.org/format.html

Ändern Sie die Beschreibung virtueller Maschinen immer durch »virsh edit«!

Sie sollten die XML-Dateien mit den Eckdaten einer virtuellen Maschine nicht direkt mit einem Editor ändern – sonst kann es passieren, dass ein anderes libvirt-Werkzeug Ihre Änderungen überschreibt. Verwenden Sie stattdessen das `virsh`-Kommando `edit`!

Image-Dateien

Wenn Sie beim Einrichten virtueller Maschinen auf Disk Images zur Abbildung der virtuellen Datenträger zurückgreifen, werden diese standardmäßig im Verzeichnis `/var/lib/libvirt/images` gespeichert. Wenn Sie Disk Images in einem anderen Verzeichnis speichern möchten oder Logicial Volumes, Festplattenpartitionen oder Netzwerkgeräte zur Speicherung der Datenträger nutzen möchten, müssen Sie vorher einen sogenannten Storage Pool einrichten. Am einfachsten gelingt das im Virtual Machine Manager. Alternativ führen Sie die entsprechenden `pool`-Kommandos innerhalb von `virsh` aus.

Verhalten beim Neustart des Hostsystems

Was passiert mit den virtuellen Maschinen, wenn Sie das Hostsystem herunterfahren? In diesem Punkt gibt es grundlegende Unterschiede zwischen den Distributionen:

- Fedora und RHEL 6 sichern mit dem `virsh`-Kommando `save` den Speicherinhalt aller durch `libvirtd` auf Systemebene ausgeführten virtuellen Maschinen. Beim nächsten Start des Rechners wird der Zustand der virtuellen Maschinen automatisch wiederhergestellt (`restore`), d. h., die virtuellen Maschinen laufen weiter, als wäre in der Zwischenzeit nichts passiert.

Verantwortlich für diesen Mechanismus ist unter RHEL das Init-V-Script `/etc/init.d/libvirt-guests`, unter Fedora das Script `/usr/libexec/libvirt-guests.sh`, das vom Systemd-Service `libvirt-guests` aufgerufen wird. Einige Konfigurationsparameter können Sie in `/etc/sysconfig/libvirt-guests` einstellen.

Bei der Sicherung bzw. Wiederherstellung mehrerer virtueller Maschinen muss jeweils deren gesamtes RAM auf der Festplatte gespeichert bzw. von dort gelesen werden. Das setzt ausreichend freien Speicherplatz im Verzeichnis `/var/lib/libvirt/qemu/save` voraus und dauert natürlich einige Zeit.

- Ubuntu versucht beim Herunterfahren, alle laufenden virtuellen Maschinen durch das `virsh`-Kommando `shutdown` herunterzufahren. Wenn das nicht gelingt bzw. wenn die virtuellen Maschinen sich für ein geordnetes Ende zu viel Zeit nehmen, werden sie gewaltsam durch das `virsh`-Kommando `destroy` beendet. Der dafür verantwortliche Code befindet sich in der Upstart-Konfigurationsdatei `/etc/init/libvirt-bin.conf`.

Virtuelle Hardware

Beim Einrichten einer neuen virtuellen Maschine haben Sie eine Menge Wahlmöglichkeiten: Disk-Images im RAW- oder im QCOW2-Format, IDE- oder virtio-Festplattenadapter, Grafiksystem auf der Basis von SDL, VNC oder Spice etc. Dieser Abschnitt fasst dazu die wichtigsten Informationen zusammen.

virtio-Treiber und Paravirtualisierung

Grundsätzlich führt KVM eine vollständige Virtualisierung durch. Das in der virtuellen Maschine laufende Gastsystem benötigt also keine besonderen Treiber.

Das Gastsystem kann freilich noch effizienter ausgeführt werden, wenn zur Kommunikation zwischen KVM und der virtuellen Maschine die optionalen virtio-Treiber zum Einsatz kommen. In der Fachsprache ist dann von »Paravirtualisierung« die Rede, d. h., das Gastsystem hilft gewissermaßen bei der Virtualisierung mit.

Bei Linux-Gästen stehen standardmäßig drei virtio-Treiber zur Beschleunigung von Festplatten-, Speicher- und Netzwerkzugriffen zur Verfügung. Es geht also nur darum, beim Einrichten der virtuellen Maschine die entsprechenden virtio-Komponenten auszuwählen.

Ein wenig diffiziler ist die Angelegenheit, wenn Sie Windows in einer KVM-Maschine ausführen möchten: In diesem Fall richten Sie die virtuelle Maschine zuerst mit traditionellen Hardware-Komponenten ein, also z. B. mit einer virtuellen IDE-Schnittstelle. Nach der Installation von Windows installieren Sie die virtio-Treiber, und erst dann können Sie die virtio-Komponenten durch eine nachträgliche Veränderung der virtuellen Maschine aktivieren.

Virtuelle Datenträger

Um einem Gast eine virtuelle Festplatte anzubieten, wird häufig auf dem KVM-Host eine Image-Datei verwendet. Dabei unterstützen QEMU/KVM drei Image-Formate:

- **RAW-Format:** Beim RAW-Format werden die Blöcke der virtuellen Festplatte einfach 1:1 abgebildet. Sofern das Dateisystem des Hostrechners sogenannte *Sparse Files* unterstützt, werden Blöcke, die ausschließlich Nullen enthalten, nicht physikalisch gespeichert. Das funktioniert so unter anderem bei `ext-`, `xfs-` und `btrfs`-Dateisystemen und spart anfänglich eine Menge Platz. Das RAW-Format ist das einfachste und schnellste Image-Format für virtuelle Maschinen.
- **QCOW2-Format:** QCOW2 steht für *Qemu Copy-on-Write, Version 2*. Dieses Format bietet gegenüber RAW eine Menge Zusatzfunktionen: Die Datenblöcke werden erst bei Bedarf reserviert, ohne ein Sparse-kompatibles Dateisystem vorauszusetzen. Außerdem kann das virtuelle Dateisystem komprimiert und verschlüsselt werden. Außerdem bieten QCOW2-Images die Möglichkeit, Snapshots zu verwalten. QCOW2-Images sind etwas langsamer als RAW-Images, der Geschwindigkeitsnachteil ist aber nicht mehr so groß wie in der Vergangenheit.
- **QED-Format:** QEMU/KVM unterstützt seit Mitte 2011 das neue *QEMU Enhanced Disk Format*, kurz QED. Dieses Format bietet eine etwas höhere Geschwindigkeit als QCOW2, enthält dafür aber weniger Funktionen. Insbesondere fehlt die praktische Snapshot-Funktion. QED hat noch keine große Verbreitung gefunden.

Anstelle von Image-Dateien können Sie auch Festplattenpartitionen, Logical Volumes oder iSCSI-Devices als virtuelle Festplatten nutzen. Diese Varianten bieten in großen Virtualisierungssystemen administrative Vorteile, aber keine nennenswert höhere Geschwindigkeit im Vergleich zu RAW-Images.

Netzwerkanbindung

Um die virtuelle Maschine mit dem lokalen Netzwerk oder dem Internet zu verbinden, muss diese mit einem Netzwerkadapter ausgestattet werden. Bei Linux-Gästen ist der virtio-Treiber die erste Wahl. Bei Windows-Gästen haben Sie unter anderem die Wahl zwischen einem RTL-8139- oder einem Intel-E1000-Netzwerkadapter.

Die zweite Frage ist, wie Sie den Adapter mit Ihrem Netzwerk verbinden:

- **NAT:** Standardmäßig entscheiden sich das KVM-Kommando bzw. die libvirt-Werkzeuge für die NAT-Variante, also für Network Address Translation. Damit wird der Internetzugang des Hosts an den Gast weitergeleitet. Der Gast ist aber weder im lokalen Netzwerk noch im Internet sichtbar.
- **Netzwerkbrücken:** Für den Server-Einsatz müssen Sie die virtuelle Maschine durch eine Netzwerkbrücke oder durch Routing mit dem Netzwerk bzw. Internet verbinden. Das erfordert eine spezielle Netzwerkkonfiguration des KVM-Hosts.

- **MacVTap:** Aktuelle Versionen der libvirt-Werkzeuge unterstützen mit MacVTap-Devices eine dritte Variante, bei der ein virtueller Netzwerkadapter mit einem physischen verbunden wird.

Grafik

Zumindest während der Installation müssen Sie die Ausgaben der virtuellen Maschine sehen. Der Gast braucht also ein eigenes Grafiksystem. Dazu wird eine VGA-kompatible Grafikkarte emuliert, deren Ausgaben dann via VNC oder Spice in einem Fenster angezeigt werden. Für den 2D-Einsatz funktioniert dies selbst in hoher Auflösung gut. KVM bietet zurzeit aber keine Unterstützung für 3D-Funktionen.

VNC und Spice sind netzwerktauglich. Für die relativ neue Spice-Architektur sprechen die etwas höhere Geschwindigkeit und der Umstand, dass auch Audio-Ausgaben der virtuellen Maschine über das Netzwerk an den lokalen Spice-Client weitergeleitet werden können. Gegen Spice spricht die schlechte Verfügbarkeit von Spice-Clients für andere Betriebssysteme als Linux.

43.2 KVM ohne libvirt

Grundsätzlich rate ich Ihnen davon ab, KVM ohne die libvirt-Werkzeuge zu benutzen. Dass ich Ihnen in diesem Abschnitt dennoch zeige, wie Sie eine virtuelle Maschine ohne libvirt-Overhead zum Laufen bringen, hat primär didaktische Gründe: Es ist immer gut zu wissen, was hinter den Kulissen vor sich geht. Außerdem werden Sie die libvirt-Werkzeuge mehr schätzen, wenn Sie sehen, mit wie vielen Optionen Sie sich beim KVM-Kommando auseinandersetzen müssen.

Image-Datei erstellen

Bevor Sie mit dem Kommando `qemu-kvm` oder `kvm` eine virtuelle Maschine starten können, müssen Sie mit dem Kommando `qemu-img` eine Image-Datei für die virtuelle Festplatte einrichten. Beim Aufruf von `qemu-img` geben Sie mit `-f raw` oder `-f qcow2` das Image-Format an. Die Größe der Datei geben Sie in MByte (*n*`M`) oder GByte (*n*`G`) an.

```
user$  qemu-img create -f qcow2 datei.img 10G
```

Das KVM-Kommando

KVM starten Sie nun mit dem Kommando `qemu-kvm` (Fedora), `/usr/libexec/qemu-kvm` (RHEL) oder `kvm -enable-kvm` (Ubuntu). Es gilt die folgende Syntax:

```
user$  qemu-kvm [optionen] [image-datei]
```

Im einfachsten Fall können Sie eine bereits installierte virtuelle Maschine so ausführen:

```
root#  qemu-kvm disk.img
```

Damit stattet das KVM-Kommando die virtuelle Maschine einfach mit einigen standardmäßig vorgesehenen Hardware-Komponenten aus: mit einem CPU-Core, 128 MByte RAM, mit einer IDE-Festplatte ohne Caching und mit einem RTL-8139-Netzwerkadapter mit der immer gleichen MAC-Adresse 52:54:00:12:34:56 etc.

Die Warnung *failed to find romfile pxe_rtl8139.bin*, die beim Start von KVM unter Ubuntu angezeigt wird, können Sie ignorieren. Sie bedeutet nur, dass KVM keine Dateien findet, um die virtuelle Maschine über das Netzwerk zu booten Das war hier aber gar nicht beabsichtigt; wenn doch, installieren Sie das Paket `kvm-pxe`.

In der Praxis reichen KVM-Kommandos deswegen oft über mehrere Zeilen, in denen alle erdenklichen Hardware-Details eingestellt werden. Das folgende Kommando startet die Installation einer Linux-Distribution. Die virtuelle Maschine wird mit zwei CPUs und 1024 MByte RAM ausgestattet. Die virtuelle Festplatte und der Netzwerkadapter werden über die virtio-Treiber des Gasts angesteuert. Als Installationsquelle dient eine ISO-Datei, die im Gast als virtuelles DVD-Laufwerk sichtbar ist und beim ersten Start als Boot-Medium gilt.

Zur Steuerung der virtuellen Maschine startet das KVM-Kommando einen nur für localhost erreichbaren VNC-Server (Display 0, also IP-Port 5900). Dank `-k de` gilt das deutsche Tastaturlayout. `-usbdevice tablet` ist erforderlich, damit die Mausbedienung funktioniert und die Zeigerposition des VNC-Clients mit der Zeigerposition der virtuellen Maschine synchronisiert werden kann.

```
root#  kvm -enable-kvm -m 1024 -smp 2 -boot once=d -cdrom linux.iso \
         -drive file=disk.img,if=virtio,format=qcow2 \
         -net user -net nic,macaddr=52:54:00:12:e4:4e,model=virtio \
         -vga cirrus -vnc 127.0.0.1:0 -k de -usb -usbdevice tablet
```

Bei virtuellen Maschinen, die vom Virtual Machine Manager bzw. von den libvirt-Werkzeugen gestartet werden, ist die KVM-Optionenliste übrigens noch viel länger. Davon können Sie sich mit `ps ax | grep kvm` überzeugen.

Um die virtuelle Maschine zu bedienen, müssen Sie nun noch einen VNC-Client starten. Bei Gnome-basierten Distributionen ist häufig das Programm Vinagre vorinstalliert. Eine gute Alternative ist das Programm TightVNC, das Sie unter Fedora/RHEL im Paket `tigervnc` finden, unter Ubuntu in `xtightvncviewer`. Wenn dieses Program installiert ist, stellen Sie die Verbindung zum auf dem KVM-Host laufenden VNC-Server so her:

```
user@client$  vncviewer localhost:0
```

Gegebenenfalls müssen Sie den VNC-Viewer neu starten, wenn dieser nach dem Wechsel vom Text- in den Grafikmodus einen Teil des Bildschirms abschneidet.

Gastsystem installieren

Nachdem Sie die virtuelle Maschine gestartet haben, führen Sie im VNC-Client eine ganz gewöhnliche Installation durch. Wenn Sie die virtuelle Maschine nach Abschluss der Installation später neuerlich starten, können Sie auf die Optionen `-cdrom linux.iso -boot once=d` verzichten.

Für die Installation von Windows müssen Sie KVM mit etwas anderen Optionen starten: ohne virtio-Adapter, mit einem Standard-VGA-Adapter und mit der Option `-localtime`, weil Windows annimmt, dass die Uhr der virtuellen Maschine die lokale Zeit enthält:

```
root#  kvm -enable-kvm -m 1024 -smp 2 -boot once=d -cdrom windows.iso \
         -drive file=disk.img,format=qcow2 \
         -net user -net nic,macaddr=52:54:00:12:e4:4e \
         -vga std -vnc 127.0.0.1:0 -k de -usb -usbdevice tablet
```

43.3 Der Virtual Machine Manager

Der Virtual Machine Manager (Programm- und Paketname `virt-manager`) ist für KVM-Einsteiger sicherlich der beste Weg, um mit diesem Virtualisierungssystem vertraut zu werden. Das Programm hat auch für Profis eine Menge zu bieten und ist für die meisten Automatisierungsaufgaben absolut ausreichend.

Damit Sie das Programm benutzen können, müssen Sie eine Verbindung zum libvirt-Dämon herstellen. Unter Fedora und RHEL ist dazu ein Doppelklick auf den bereits vorgesehenen Eintrag LOCALHOST (QEMU) erforderlich. Der Verbindungsaufbau erfordert die Eingabe des `root`-Passworts.

Bei aktuellen Ubuntu-Versionen erfolgt der Verbindungsaufbau zum libvirt-Dämon auf Systemebene automatisch, sofern der Benutzer zur Gruppe `libvirtd` gehört. Ist das nicht der Fall, führen Sie `sudo adduser` *`loginname`* `libvirtd` aus und loggen sich aus und neu ein.

Virtuelle Maschinen ausführen

Das Hauptfenster des Virtual Maschine Managers enthält eine Liste aller libvirt-Verbindungen (siehe Abbildung 43.1). Standardmäßig besteht diese Liste nur aus einem Eintrag, nämlich LOCALHOST (QEMU). Sie können aber mit DATEI • VERBINDUNG HINZUFÜGEN die Eckdaten weiterer KVM-Hosts angeben.

Ein Doppelklick auf einen Eintrag dieser Liste stellt die Verbindung zum KVM-Host her und zeigt dann alle virtuellen Maschinen dieses Hosts an. Bei jeder virtuellen Maschine zeigt ein Icon, ob die Maschine heruntergefahren ist, läuft oder pausiert.

Um eine virtuelle Maschine zu starten, klicken Sie deren Eintrag mit der rechten Maustaste an und führen AUSFÜHREN aus. Ein Doppelklick auf den Eintrag öffnet ein neues Fenster, das in zwei Ansichten den Zustand der virtuellen Maschine zeigt:

- **Die Konsolenansicht** zeigt das Grafiksystem der virtuellen Maschine. Hier sehen Sie die Ausgaben der virtuellen Maschine und können per Tastatur und Maus Eingaben durchführen. Bei virtuellen Maschinen, die im Textmodus laufen, wird der Mauscursor durch einen Klick in der virtuellen Maschine gleichsam eingefangen. Strg+Alt löst den Cursor wieder.
- **Die Detailansicht** zeigt die Eckdaten der virtuellen Maschine an. Hier können Sie die Hardware-Ausstattung der virtuellen Maschine verändern. Die meisten Änderungen können allerdings nur durchgeführt werden, wenn die virtuelle Maschine gerade nicht läuft.

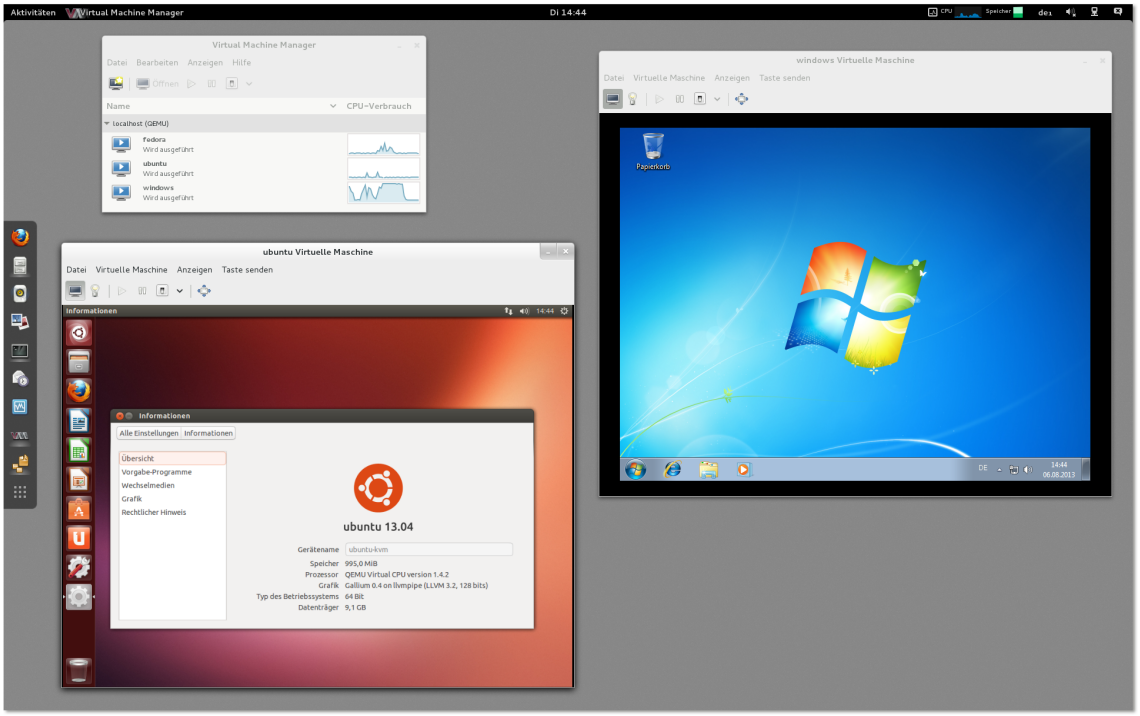


Abbildung 43.1 Der Virtual Machine Manager auf einem Fedora-Host mit virtuellen Ubuntu- und Windows-Installationen

Um zwischen den beiden Ansichten umzuschalten, führen Sie ANZEIGEN • KONSOLE bzw. ANZEIGEN • DETAILS aus bzw. klicken in der Symbolleiste auf die entsprechenden Buttons. Unter RHEL werden die Fenster zur Darstellung virtueller Maschinen standardmäßig ohne Symbolleiste angezeigt. ANZEIGEN • WERKZEUGLEISTE behebt dieses Manko und ermöglicht dann ein wesentlich komfortableres Wechseln zwischen der Konsolen- und der Detailansicht.

Virtuelle Maschinen stoppen

Die virtuellen Maschinen laufen vollkommen unabhängig vom Virtual Machine Manager! Sie können also die Fenster des Virtual Machine Managers schließen und später wieder öffnen – die virtuellen Maschinen laufen in der Zwischenzeit weiter. Sie können sich sogar aus- und neu einloggen, ohne die Ausführung von virtuellen Maschinen zu beeinträchtigen.

Es gibt vier Möglichkeiten, eine virtuelle Maschine zu stoppen:

- HERUNTERFAHREN • NEUSTART sendet ein entsprechendes ACPI-Ereignis an die virtuelle Maschine. Wenn die virtuelle Maschine ACPI-Ereignisse verarbeitet, leitet sie einen Shutdown und anschließend einen Neustart ein. In Linux-Gästen ist dazu das Paket `acpid` erforderlich, das bei Desktop-Systemen automatisch installiert wird.
- HERUNTERFAHREN • HERUNTERFAHREN leitet via ACPI einen Shutdown ein.
- HERUNTERFAHREN • FORCIERTES AUSSCHALTEN beendet die Ausführung der virtuellen Maschine sofort – so, als würden Sie bei einem realen Rechner das Stromkabel ziehen. Naturgemäß sollten Sie versuchen, diese Variante des Ausschaltens zu vermeiden, da sie mit Datenverlusten verbunden sein kann.
- HERUNTERFAHREN • SPEICHERN speichert den Inhalt des virtuellen RAMs der Maschine in einer Datei und beendet dann die Ausführung. Wird die virtuelle Maschine später wieder gestartet, befindet sie sich exakt im selben Zustand wie beim Herunterfahren.

Administration im Netzwerk via SSH

Sie können den Virtual Machine Manager auch verwenden, um einen via SSH erreichbaren externen KVM-Host zu administrieren. Dazu definieren Sie zuerst mit DATEI • VERBINDUNG HINZUFÜGEN eine Verbindung zu diesem Server, wobei Sie als Verbindungsmethode SSH auswählen (siehe Abbildung 43.2). Beim Verbindungsaufbau müssen Sie zudem das entsprechende Login-Passwort angeben.

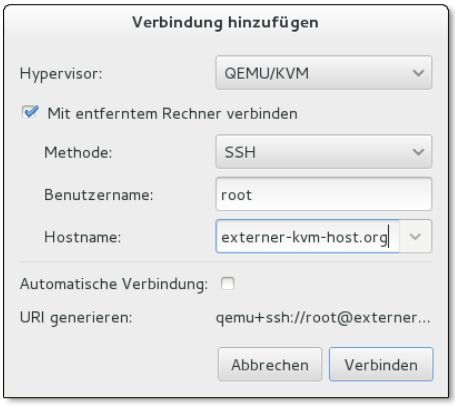


Abbildung 43.2 Verbindungsaufbau via SSH

Wenn der externe KVM-Host unter RHEL oder Fedora läuft, erfordert die `libvirt`-Administration root-Rechte und somit einen `root`-Login via SSH. Aus Sicherheitsgründen sind SSH-Server aber häufig so konfiguriert, dass ein direkter `root`-Login unmöglich ist. Ein Kompromiss kann so aussehen, dass Sie den SSH-Server so konfigurieren, dass ein `root`-Login nur bei einer Authentifizierung durch einen Schlüssel akzeptiert wird, nicht aber per Passwort. Generell funktioniert die Administration externer KVM-Hosts nur mit einem SSH-Schlüssel komfortabel.

Unter Fedora blockiert SELinux das Port Forwarding

Unter Fedora wird SSH Port Forwarding aber durch eine SELinux-Regel blockiert. Das verhindert eine VNC- oder Spice-Bedienung der virtuellen Maschinen über das Netzwerk. Abhilfe: Sie müssen auf dem KVM-Host das Port-Forwarding explizit erlauben. Dazu führen Sie dieses Kommando aus:

```
root@fedora-kvm-host# setsebool -P sshd_forward_ports 1
```

Die Hintergründe dieses Problems können Sie hier nachlesen:

https://bugzilla.redhat.com/show_bug.cgi?id=653579

Merkwürdigerweise gibt es die SELinux-Regel `sshd_forward_ports` nur unter Fedora, aber nicht unter RHEL.

Eine neue virtuelle Maschine einrichten

Das Einrichten einer neuen virtuellen Maschine beginnt jetzt mit dem Button Neue virtuelle Maschine erstellen. Bei der Einstellung der Eckdaten hilft ein Assistent in fünf Schritten:

- Im ersten Schritt geben Sie den Namen der virtuellen Maschine und deren Installationsquelle an. Bei einer Linux-Installation handelt es sich üblicherweise um eine ISO-Datei. Es ist aber auch möglich, die Installationsdaten vom DVD-Laufwerk des Hostrechners zu lesen. Die Option Vorhandenes Festplatten-Abbild importieren erzeugt eine Kopie einer bereits vorhandenen Image-Datei mit einer virtuellen Maschine.
- Wenn Sie im ersten Schritt ein ISO-Abbild oder eine CD/DVD als Installationsquelle ausgewählt haben, können Sie im zweiten Schritt den Dateinamen einer ISO-Datei oder das CD/DVD-Laufwerk angeben. Der Button Durchsuchen führt in einen Dialog, der vorerst nur die dem Virtual Machine Manager bekannten Storage Pools anzeigt. Um eine ISO-Datei direkt auszuwählen, müssen Sie in diesem Dialog den Button Lokal durchsuchen anklicken.

Außerdem stellen Sie im zweiten Schritt des Assistenten den Typ des Betriebssystems und die Version des Gastsystems ein, also z. B. Linux und Fedora 19. Diese Einstellungen sind erforderlich, damit der Assistent die für das Gastsystem optimalen virtuellen Hardware-Komponenten einrichtet!

- Im dritten Schritt geben Sie an, wie viel Speicher (RAM) und wie viele CPU-Cores Sie der virtuellen Maschine zuweisen möchten.
- Im vierten Schritt richten Sie die virtuelle Festplatte ein. Normalerweise werden Sie die bereits vorselektierte Option Plattenabbild auf Festplatte des Systems erstellen nutzen. Die neue Image-Datei wird standardmäßig im Verzeichnis `/var/lib/libvirt/images` angelegt. Wählen Sie die Größe der virtuellen Festplatte nicht zu klein – eine nachträgliche Vergrößerung ist mit großem Aufwand verbunden.

  Neben der Größe können Sie auch auswählen, ob der virtuelle Festplattenspeicher sofort zugewiesen wird oder ob die virtuelle Festplatte erst bei Bedarf wachsen soll. Ersteres ist effizienter und schließt aus, dass zu einem späteren Zeitpunkt vielleicht zu wenig Platz auf der Festplatte ist, um dem steigenden Platzbedarf der virtuellen Maschine gerecht zu werden.

  Die Alternative Verwalteten oder anderen Speicher wählen ist nur dann von Relevanz, wenn Sie vorher mit Bearbeiten • Verbindungsdetails im Dialogblatt Speicher weitere Speicherpools eingerichtet haben.
- Im fünften Schritt können Sie schließlich in den Erweiterten Optionen die Netzwerkschnittstelle konfigurieren. Der Assistent weist dem Netzwerkadapter jeder virtuellen Maschine eine eindeutige MAC-Adresse der Form 52:54:00:nn:nn:nn zu. Standardmäßig wird die virtuelle Maschine mittels Network Address Translation mit dem Hostsystem verbunden. Damit kann die virtuelle Maschine den Internetzugang des Hostrechners nutzen, aber keine Verbindungen zu anderen Rechnern in Ihrem lokalen Netzwerk herstellen.

  Mit dem Button Abschliessen wird die Konfiguration beendet und die neue virtuelle Maschine sofort gestartet. Wenn Sie das nicht wünschen, aktivieren Sie im letzten Dialogblatt des Assistenten die Option Konfiguration bearbeiten vor der Installation. Damit gelangen Sie nach dem Ende des Assistenten in einen Dialog, der die Hardware-Komponenten der virtuellen Maschine zusammenfasst (siehe Abbildung 43.3).

Mit dem Abschluss der Konfiguration der virtuellen Maschine wird diese gestartet. Die Ausgaben der virtuellen Maschine sehen Sie in einem neuen Fenster des Virtual Machine Managers. Hinter den Kulissen agiert dieses Fenster als VNC- oder Spice-Client.

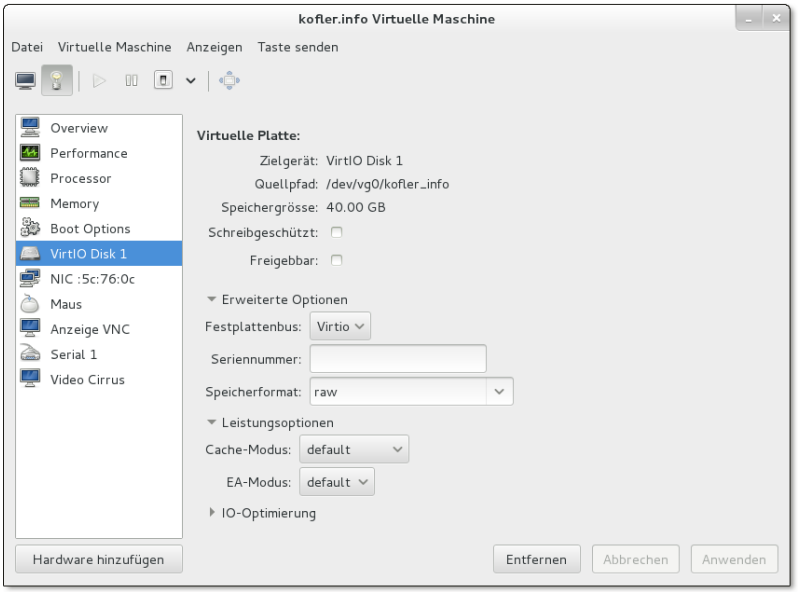


Abbildung 43.3 Hardware-Verwaltung im Virtual Machine Manager

RHEL- oder Fedora-Minimalinstallation

Für Server-Aufgaben reicht oft eine Minimalinstallation ohne grafische Benutzeroberfläche. Bei Fedora-Gästen stellen Sie dazu während der Installation bei der Software-Auswahl anstelle der vorgegebenen Option GRAFISCHE OBERFLÄCHE die Option MINIMAL ein. Bei RHEL-Distributionen ist diese Option bereits voreingestellt.

Außer `root` werden keine Benutzer eingerichtet. Immerhin wird standardmäßig ein SSH-Server installiert und eine Firewall eingerichtet. Auch SELinux ist aktiv. Die gesamte weitere Administration muss nun mit textbasierten Werkzeugen erfolgen und setzt daher gute Fedora- oder RHEL-Grundlagenkenntnisse voraus. Das betrifft auch die Netzwerkkonfiguration – standardmäßig ist nur die Loopback-Schnittstelle aktiv.

Manuelle Netzwerkkonfiguration

Somit ist als Nächstes eine manuelle Netzwerkkonfiguration notwendig. Wenn die virtuelle Maschine ihre Netzwerkparameter via DHCP bezieht, richten Sie die Datei `/etc/sysconfig/network-scripts/ifcfg-eth0` wie folgt ein:

```
# Datei /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=52:54:00:xx:xx:xx      (eigene MAC-Adresse)
NM_CONTROLLED=no
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
```

```
USERCTL=no
PEERDNS=yes
IPV6INIT=no
```

Die MAC-Adresse des Netzwerkadapters der virtuellen Maschine können Sie entweder der XML-Datei mit der Beschreibung der virtuellen Maschine entnehmen (`/etc/libvirt/qemu/name.xml`) oder in der virtuellen Maschine mit `ip addr` ermitteln.

Bei einer statischen Konfiguration muss die Datei dem folgenden Muster entsprechen, wobei Sie die IP-Adressen und -Masken durch eigene Werte ersetzen müssen:

```
# Datei /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=52:54:00:xx:xx:xx      (eigene MAC-Adresse)
NM_CONTROLLED=no
ONBOOT=yes
BOOTPROTO=none
TYPE=Ethernet
USERCTL=no
IPV6INIT=no
IPADDR=10.0.17.33
NETMASK=255.255.255.0
NETWORK=10.0.17.0
BROADCAST=10.0.17.255
GATEWAY=10.0.17.1
```

Die Gateway-Adresse können Sie auch in `/etc/sysconfig/network` einstellen. Das ist dann zweckmäßig, wenn es ein zentrales Gateway für alle Netzwerkschnittstellen gibt. Den oder die Nameserver tragen Sie in `/etc/resolv.conf` ein:

```
# /etc/resolv.conf
nameserver 10.0.17.1    # erster DNS
nameserver 10.0.17.2    # zweiter DNS
```

Falls Sie den Hostnamen verändern möchten, finden Sie den entsprechenden Parameter in der Datei `/etc/sysconfig/network`. Im Regelfall ist es zweckmäßig, die Zuordnung der IP-Adresse des Rechners zu seinem Hostnamen auch in `/etc/hosts` einzutragen:

```
# /etc/hosts
...
10.0.17.33      myhostname.mydomainname myhostname
```

Das folgende Kommando aktiviert die Netzwerkeinstellungen:

```
root#  service network restart
```

Ad-hoc-Netzwerkkonfiguration zur Installation von Paketen

Während dieser Konfigurationsarbeiten steht Ihnen als einziger Editor `vi` zur Verfügung. Wenn Sie einen anderen Editor vorziehen, können Sie die Netzwerkschnittstelle `eth0` vorweg durch das Kommando `dhclient eth0` aktivieren – einmal vorausgesetzt, dass die virtuelle Maschine in einem Netzwerk mit DHCP-Server läuft. Anschließend können Sie mit `yum` einen anderen Editor installieren.

ACPI-Dämon installieren

Damit Sie virtuelle Maschinen via `virsh shutdown` oder über den Virtual Machine Manager herunterfahren können, muss der ACPI-Dämon laufen. Bei Minimalinstallationen ist das nicht der Fall. Abhilfe schaffen die folgenden Kommandos:

```
root#  yum install acpid
root#  service acpid start
```

Ubuntu-Minimalinstallation

Wenn Sie in einer virtuellen Maschine eine minimale Ubuntu-Installation durchführen möchten, sollten Sie als Installationsquelle das ISO-Image der Server-CD verwenden, nicht die ISO-Datei zur Desktop-Installation. Am Beginn einer Ubuntu-Server-Installation können Sie mit F4 die Installationsvariante Eine minimale virtuelle Maschine installieren auswählen. Der Vorteil gegenüber einer herkömmlichen Server-Installation besteht darin, dass ein spezieller Kernel eingesetzt wird, der für den Einsatz in virtuellen Maschinen optimiert ist und mit wenig zusätzlichem Ballast auskommt.

Netzwerkkonfiguration

Anders als bei RHEL kümmert sich das Installationsprogramm um die Netzwerkkonfiguration. Wenn Sie die Konfiguration später ändern möchten, ist der zentrale Dreh- und Angelpunkt die Datei `/etc/network/interfaces`. Bezieht die virtuelle Maschine ihre Netzwerkparameter von einem DHCP-Server, muss diese Datei so aussehen:

```
# /etc/network/interfaces
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

Bei einer statischen Konfiguration können Sie sich am folgenden Muster orientieren:

```
# /etc/network/interfaces
auto lo
iface lo inet loopback
```

```
auto eth0 inet static
  address 10.0.17.33
  netmask 255.255.255.0
  gateway 10.0.17.1
```

Den oder die Nameserver tragen Sie in `/etc/resolv.conf` ein. Damit Änderungen an der Konfiguration wirksam werden, führen Sie das folgende Kommando aus:

```
root#  /etc/init.d/networking restart
```

ACPI-Dämon installieren

Um virtuelle Ubuntu-Maschinen via `virsh shutdown` oder über den Virtual Machine Manager herunterfahren zu können, muss der ACPI-Dämon laufen. Bei einer Minimalinstallation ist das nicht der Fall. Abhilfe schafft `apt-get install acpid`.

Windows-Installation

KVM ist Windows-kompatibel, und prinzipiell unterscheidet sich eine Windows-Installation nur unwesentlich von einer Linux-Installation. Sie beginnen abermals damit, dass Sie eine neue virtuelle Maschine einrichten. Achten Sie darauf, dass Sie im zweiten Schritt des Assistenten den Betriebssystemtyp WINDOWS und die entsprechende Windows-Version auswählen! Nur dann verwendet der Virtual Machine Manager für Windows geeignete virtuelle Hardware-Komponenten. Um Zeit zu sparen, sollten Sie vor Beginn der Installation in den Hardware-Einstellungen für die IDE-Festplatte den Cache-Modus WRITEBACK aktivieren.

Uhrzeit

Bei älteren KVM-Versionen hatte ich Probleme mit der Uhr, die im Windows-Gast zu schnell lief. Unter Windows 7 bzw. Windows Server 2008 beheben Sie dieses Problem, indem Sie die Uhr von Time Stamp Counter (TSC) auf Real-Time Clock (RTC) umstellen. Dazu öffnen Sie im Windows-Gast das Startmenü, klicken den Eintrag ALLE PROGRAMME • ZUBEHÖR • EINGABEAUFFORDERUNG mit der rechten Maustaste an und wählen ALS ADMINISTRATOR AUSFÜHREN. Im Kommandofenster führen Sie die folgende Anweisung aus:

```
>  bcdedit /set default USEPLATFORMCLOCK on
```

Die geänderte Uhr wird erst mit einem Neustart aktiv. Mit aktuellen KVM-Versionen trat das Problem gar nicht erst auf, der Fix ist dann überflüssig.

virtio-Treiber

Standardmäßig kommen die folgenden Hardware-Komponenten zum Einsatz:

- eine CPU mit einem Core
- ein RTL-8139-Netzwerkadapter im NAT-Netzwerk
- eine IDE-Festplatte
- eine Grafikkarte mit nahezu beliebiger Auflösung, wobei Windows aber anfänglich nur 800×600 Pixel nutzt

Um Netzwerk- und Festplattenzugriffe effizienter zu gestalten, sollten Sie nun unbedingt virtio-Treiber unter Windows installieren und anschließend die Hardware-Einstellungen der virtuellen Maschine entsprechend ändern.

Auf der folgenden Website finden Sie Download-Links für eine ISO-Datei mit signierten Treibern für alle gängigen Windows-Versionen von Windows XP bis Windows 7:

http://www.linux-kvm.org/page/WindowsGuestDrivers/Download_Drivers

Diese ISO-Datei laden Sie auf das Hostsystem herunter, also nicht in der virtuellen Maschine. Anschließend fahren Sie Ihren Windows-Gast hinunter. Mit ANZEIGEN • DETAILS wechseln Sie in die Hardware-Ansicht der virtuellen Maschine. Dort geben Sie die ISO-Datei als Quelle für das virtuelle CD-Laufwerk an. Außerdem fügen Sie der virtuellen Maschine zusätzlich zu den vorhandenen Netzwerk- und Festplattenadaptern eine neue `virtio`-Netzwerkkarte und eine `virtio`-Festplatte hinzu. Die Image-Datei für die neue Festplatte muss nicht groß sein – es geht nur darum, dass Windows beim nächsten Start die neuen Hardware-Komponenten bemerkt.

Anschließend starten Sie den Windows-Gast neu und starten im Windows-Menü das Programm GERÄTE-MANAGER. Dort erscheinen die noch unbekannten Hardware-Komponenten als ETHERNET- und SCSI-CONTROLLER. Bei beiden Komponenten öffnen Sie nun per Doppelklick den Eigenschaftendialog, klicken auf EINSTELLUNGEN ÄNDERN, dann auf TREIBER AKTUALISIEREN und schließlich auf AUF DEM COMPUTER NACH TREIBERSOFTWARE SUCHEN. Bei dieser Suche müssen Sie mithelfen. Sie geben als Ort der Treibersoftware das DVD-Laufwerk an, also üblicherweise »D:«.

Abbildung 43.4 virtio-Treiberinstallation unter Windows 7

Nun fahren Sie Windows herunter und entfernen in der Hardware-Übersicht des Virtual Machine Managers die IDE-Festplatte, die virtio-Festplatte und den RTL-8139-Netzwerkadapter. Außerdem richten Sie eine neue virtio-Festplatte ein, wobei Sie die ursprüngliche Image-Datei auswählen – also die, die bisher mit der IDE-Festplatte verbunden war. Das Ergebnis ist eine virtuelle Maschine mit einem virtio-Netzwerkadapter und einer virtio-Festplatte. Vergewissern Sie sich mit einem Blick in den Geräte-Manager!

virtio-Treiberprobleme

In der Vergangenheit hat die Treiberinstallation klaglos funktioniert – nicht aber beim jüngsten Test für die Neuauflage dieses Buchs: Während der virtio-Festplattentreiber anstandslos lief, beklagte sich der Geräte-Manager darüber, dass der virtio-Netzwerktreiber beschädigt sei. Es ist zu hoffen, dass dieses Problem bei zukünftigen Versionen der virtio-Treiber behoben wird. Für meine Tests habe ich die seit Juni 2013 verfügbare ISO-Datei `virtio-win-0.1-65.iso` verwendet. Ich habe daher den virtuellen Netzwerkadapter wohl oder übel auf das Modell RTL-8139 zurücksetzen müssen.

43.4 libvirt-Kommandos

Nachdem ich Ihnen im vorigen Abschnitt recht ausführlich den Virtual Machine Manager als wichtigsten Vertreter der libvirt-Werkzeuge präsentiert habe, folgen in diesem Abschnitt einige Kommandos, deren Nutzung keine grafische Benutzeroberfläche voraussetzt.

virsh

Mit dem Kommando `virsh` starten Sie die libvirt-Shell. Darin können Sie Kommandos zur Verwaltung aller virtuellen Maschinen ausführen, die libvirt bekannt sind.

```
root#  virsh
virsh#  list --all
 Id Name                 Status
----------------------------------
 13 fedora          laufend
  - ubuntu          ausschalten
  - windows         ausschalten
virsh#  start windows
Domain windows gestartet
virsh#  vncdisplay windows
:1
virsh#  exit
```

Mit der `virsh` können Sie virtuelle Maschinen mit `start`, `suspend`/`resume`, `shutdown`, `destroy`, `save`/`restore` bzw. `undefine` starten, vorübergehend anhalten und wieder fortsetzen, geordnet herunterfahren (ACPI Shutdown), sofort ausschalten, speichern und wieder fortsetzen oder aus der Liste der `libvirt`-Definitionen löschen.

`edit` ermöglicht es, die XML-Datei mit der Beschreibung der virtuellen Maschine direkt in einem Editor zu bearbeiten. Als Editor kommt üblicherweise `vi` zum Einsatz. Wenn Sie mit einem anderen Editor arbeiten möchten, müssen Sie die Umgebungsvariable `EDITOR` entsprechend einstellen.

Bei allen oben aufgezählten `virsh`-Kommandos müssen Sie den Namen der virtuellen Maschine, deren UUID-Nummer oder bei laufenden virtuellen Maschinen die ID-Nummer angeben. Die UUID-Nummer geht aus der XML-Definitionsdatei hervor. Auskunft über die ID-Nummern laufender virtueller Maschinen gibt das `virsh`-Kommando `list`.

Verbindungsaufbau

Sofern `virsh` erkennt, dass der Rechner ein KVM-Host ist, stellt es nach Möglichkeit eine Verbindung zu dem auf Systemebene laufenden Dämon `libvirtd` her. Wenn `virsh` nur mit Benutzerrechten ausgeführt wird, erfordert eine Verbindung auf Systemebene unter Ubuntu die Zugehörigkeit zur Gruppe `libvirtd`. Unter RHEL und Fedora müssen Sie das Kommando als `root` starten, wenn Sie auf Systemebene arbeiten möchten.

Es ist möglich, innerhalb der `virsh`-Shell die Verbindung mit dem Kommando `connect` zu verändern: `qemu:///session` bezeichnet dabei eine Verbindung auf Benutzerebene, `qemu:///system` eine Verbindung auf Systemebene.

```
virsh#  connect qemu:///system
```

Via SSH können Sie auch eine Verbindung zum Dämon `libvirtd` auf einem anderen Rechner herstellen. Wenn es sich beim KVM-Host um einen RHEL- oder Fedora-Rechner handelt, müssen Sie als Benutzername `root` angeben, weil auf diesen Systemen nur `root` eine Verbindung zum libvirt-Systemdämon herstellen darf. Beachten Sie, dass nach `qemu+ssh:` nur zwei Schrägstriche folgen, nicht drei! Wenn auf dem KVM-Host aus Sicherheitsgründen ein `root`-Login mit Passwortangabe via SSH unmöglich ist, müssen Sie vor dem ersten Verbindungsaufbau Ihren öffentlichen SSH-Schlüssel auf dem KVM-Host einrichten.

```
virsh#  connect qemu qemu+ssh://user@hostname/system
user@hostname's password:  *******
```

Anstatt `virsh` interaktiv zu verwenden, können Sie ein einzelnes `virsh`-Kommando in der Form `virsh kommando` ausführen:

```
root#  virsh  list --all
...
```

Wenn Sie dabei nicht die von `virsh` standardmäßig vorgesehene Verbindung verwenden möchten, geben Sie die Verbindungszeichenkette mit der Option `-c` an:

```
root#  virsh -c qemu:///session list --all
...
```

Ausgewählte virsh-Kommandos

Zum Abschluss stelle ich Ihnen einige ausgewählte `virsh`-Kommandos vor. `man virsh` dokumentiert mindestens hundert weitere Kommandos. Innerhalb der Shell erhalten Sie mit `help name` eine ausführliche Beschreibung des jeweiligen Kommandos.

- `connect qemu:///session`: stellt eine gewöhnliche Benutzerverbindung zu `libvirtd` her. Auf diese Weise können eigene virtuelle Maschinen verwaltet werden.
- `connect qemu:///system`: stellt eine `root`-Verbindung zu `libvirtd` her. Das ist nur erforderlich, wenn globale KVM-Optionen oder virtuelle Netzwerke verändert werden sollen.
- `list [--inactive` oder `--all]`: listet alle laufenden virtuellen Maschinen auf. Wenn Sie nur die gerade nicht aktiven oder überhaupt alle Maschinen auflisten möchten, geben Sie die Optionen `--inactive` oder `--all` an.
- `start` *`name`*: startet die angegebene virtuelle Maschine. Wenn Sie mit der Maschine im Grafikmodus kommunizieren möchten, verwenden Sie dazu entweder das Programm `virt-viewer` oder einen VNC-Client. Die Verbindungsdaten ermittelt das `virsh`-Kommando `vncdisplay`.
- `suspend/resume` *`name`*: stoppt die angegebene virtuelle Maschine vorübergehend bzw. setzt die Ausführung wieder fort. Die gestoppte virtuelle Maschine beansprucht weiterhin RAM! Es wird also nur die virtuelle CPU angehalten.
- `shutdown/reboot` *`name`*: fährt die virtuelle Maschine herunter bzw. startet sie neu. Die virtuelle Maschine erhält via ACPI ein Shutdown-Signal. Es ist allerdings der virtuellen Maschine überlassen, ob sie auch darauf reagiert. Wenn das nicht der Fall ist, hilft in der Regel die Installation des Pakets `acpid` in der virtuellen Maschine.
- `save` *`name dateiname`*: speichert den Zustand der virtuellen Maschine in einer Datei und stoppt dann die Ausführung der Maschine.
- `restore` *`dateiname`*: aktiviert die zuvor gespeicherte virtuelle Maschine wieder. Die Zustandsdatei kann anschließend gelöscht werden.
- `destroy` *`name`*: beendet die virtuelle Maschine sofort. Das ist so, als würden Sie bei Ihrem Rechner das Stromkabel ausstecken, und es kann dieselben Folgen haben.
- `undefine` *`name`*: löscht die XML-Datei, die die virtuelle Maschine beschreibt. Die Image-Datei mit der virtuellen Festplatte bleibt erhalten.
- `autostart [--disable]` *`name`*: gibt an, dass die virtuelle Maschine während des Bootprozesses des Hostrechners automatisch gestartet werden soll. Mit der Option `--disable` wird der automatische Start wieder abgestellt. Der automatische Start funktioniert nur für Maschinen, die auf Systemebene eingerichtet werden.

Auf Session-Ebene werden `autostart`-Maschinen dagegen erst gestartet, wenn mit `virsh` zum ersten Mal eine Verbindung zu `libvirtd` hergestellt wird.

- `console` *name*: ermöglicht die Bedienung der angegebenen virtuellen Maschine direkt in der Konsole. Das setzt voraus, dass in der virtuellen Maschine ein `getty`-Prozess für die serielle Schnittstelle `/dev/ttyS0` läuft. Um die Verbindung zu beenden, drücken Sie Strg+].
- `ttyconsole` *name*: gibt an, über welches Device des Host-Computers die serielle Schnittstelle des Gastsystems zugänglich ist (z. B. `/dev/pts/5`). Sie können nun in einem Terminalfenster `socat - /dev/pts/5` ausführen und dann mit der virtuellen Maschine kommunizieren (ganz ähnlich wie beim oben beschriebenen `console`-Kommando). Vorher muss in der Regel das Paket `socat` installiert werden.
- `vncdisplay` *name*: liefert die IP-Adresse (leer für `localhost`) und Portnummer für die VNC-Anzeige der virtuellen Maschine. Sie können nun einen beliebigen VNC-Client (z. B. Vinagre) starten, um mit der virtuellen Maschine zu interagieren. Am KVM-Host können Sie stattdessen auch `virt-viewer` *name* ausführen. Aus Sicherheitsgründen funktioniert der VNC-Zugang nur von `localhost`.
- `edit` *name*: lädt die XML-Datei zur Beschreibung der virtuellen Maschine in den Editor, den Sie in der Umgebungsvariablen `$EDITOR` eingestellt haben.

virt-install

Mit dem Kommando `virt-install` richten Sie eine neue virtuelle Maschine ein. `virt-install` kann wahlweise mit oder ohne `root`-Rechte ausgeführt werden. Im ersten Fall wird die virtuelle Maschine auf Benutzerebene eingerichtet (`qemu:///session`), im zweiten Fall auf Systemebene (`qemu:///system`). Dementsprechend finden Sie nach der Installation die XML-Konfigurationsdatei in den Verzeichnissen `.virtlib/qemu/` oder `/etc/libvirt/qemu/`.

Im folgenden Beispiel gehen wir davon aus, dass Sie auf Systemebene arbeiten. Bevor Sie `virt-install` ausführen, müssen Sie eine Image-Datei für die virtuelle Festplatte erzeugen. Damit die Image-Datei wie die virtuelle Maschine unter der Verwaltung der libvirt-Werkzeuge steht, richten Sie diese am besten mit `virsh vol-create-as` ein. Der erste Parameter dieses Kommandos gibt den gewünschten Speicherpool an, der zweite Parameter den Namen der Image-Datei, der dritte Parameter die Größe. Mit `--format` geben Sie das gewünschte Image-Format an.

```
root#  virsh
virsh#  vol-create-as default disk.qcow2 10G --format qcow2
virsh#  exit
```

Mit dem Kommando `virt-install` richten Sie nun eine neue virtuelle Maschine ein. An das Kommando müssen zumindest die Größe des virtuellen RAMs, der

gewünschte Name der virtuellen Maschine, der Ort der Image-Datei sowie die gewünschte Installationsart angefügt werden, in der Regel z. B. `--cdrom`.

Für alle anderen Eckdaten der virtuellen Maschine wählt `virt-install` selbst geeignete Einstellungen. Hilfreich ist dabei die Option `--os-variant`: Damit kann `virt-install` die für das installierte Betriebssystem optimalen virtuellen Hardware-Komponenten einsetzen, z. B. einen virtio-Netzwerkadapter. Die Einstellungen können Sie nach der Installation in der Datei `/etc/libvirt/qemu/name.xml` nachlesen. Eine Liste der `virt-install` bekannten Betriebssystembezeichnungen liefert `virt-install --os-variant list`.

```
root#  virt-install --name myvmname --ram 1024 --cdrom install.iso \
          --os-variant rhel6  --disk vol=default/disk.qcow2 --graphics vnc \
          --noreboot
```

SELinux erfordert ISO-Images in lokalen Dateisystemen

Wenn Sie unter Fedora oder Red Hat arbeiten, müssen sich die Image-Datei für die virtuelle Festplatte und die ISO-Datei mit der Installations-DVD in einem von libvirt verwalteten Speicherpool im lokalen Dateisystem befinden. Andernfalls reklamiert SELinux ein verdächtiges Verhalten und blockiert den Zugriff.

Die eigentliche Installation des Betriebssystems erfolgt in einem Fenster des Programms `virt-viewer` via VNC. Stellen Sie sicher, dass das Paket `virt-viewer` installiert ist! Sollte der `virt-viewer` nicht zur Verfügung stehen, können Sie die VNC-Verbindungsdaten mit dem `virsh`-Kommando `vncdisplay` ermitteln und die Installation mit einem beliebigen anderen VNC-Client durchführen.

```
root#  virsh
virsh#  list
 Id Name                 Status
----------------------------------
  2 myvmname          laufend
virsh#  vncdisplay 2
10.0.0.44:0
```

Sollte während der Installation etwas schiefgehen, können Sie möglicherweise noch laufende virtuelle Maschinen mit `virsh` beenden und löschen. Die Image-Datei der virtuellen Festplatte bleibt dabei erhalten.

```
root#  virsh
virsh#  list
 Id Name                 Status
----------------------------------
  2 myvmname          laufend
virsh#  destroy  myvmname
virsh#  undefine myvmname
virsh#  quit
```

virt-clone

Das Einrichten einer neuen virtuellen Maschine mit `virt-install` nimmt geraume Zeit in Anspruch. Wenn Sie eine virtuelle Maschine wünschen, die im Wesentlichen dieselben Eckdaten wie eine bereits vorhandene virtuelle Maschine hat, ist es wesentlich schneller, diese einfach zu kopieren bzw. zu »klonen«. Dabei hilft das Kommando `virt-clone`: Standardmäßig erzeugt es eine neue XML-Definitionsdatei, kopiert die Image-Datei für die virtuelle Festplatte und gibt dem Netzwerkadapter eine neue, zufällige MAC-Adresse. Die restlichen Hardware-Komponenten bleiben unverändert. Die virtuelle Maschine muss vor dem Kopieren heruntergefahren werden.

Das folgende Kommando kopiert eine Ubuntu-Server-Installation. Die neue virtuelle Maschine erhält den Namen `userver6`, die neue Image-Datei wird in der Datei `/var/lib/libvirt/images/userver6.img` gespeichert. Achten Sie darauf, die neue Image-Datei in einem libvirt-Speicherpool anzulegen: So verhindern die SELinux-Regeln unter RHEL/Fedora die Ausführung der virtuellen Maschine.

```
root#  virt-clone --original userver5 --name userver6 \
                  --file /var/lib/libvirt/images/userver6.img
```

Nach dem Kopieren müssen Sie in der virtuellen Maschine diverse Anpassungen vornehmen. Beispielsweise müssen Sie die Netzwerkkonfiguration ändern, damit es keine IP-Adresskonflikte gibt. Je nach Konfiguration ist es erforderlich, auch die Dateien `/etc/hosts` und `/etc/hostname` zu aktualisieren. Wenn es in der ursprünglichen virtuellen Maschine einen SSH-Server gab, sollten Sie in der virtuellen Maschine unbedingt einen neuen SSH-Schlüssel erzeugen:

```
root#  service ssh stop                    (Debian/Ubuntu)
root#  rm /etc/ssh/ssh_host_*
root#  dpkg-reconfigure openssh-server

root#  service sshd stop                   (Fedora/Red Hat)
root#  rm /etc/ssh/ssh_host_*
root#  service sshd start
```

virt-viewer

`virt-viewer` ist ein VNC-Client zur Darstellung des Bildschirminhalts sowie zur Kommunikation mit einer virtuellen Maschine. `virt-viewer` *vm-name* stellt die Verbindung zu einer laufenden virtuellen Maschine her. Das setzt voraus, dass die virtuelle Maschine VNC nutzt. Bei virtuellen Maschinen, die mit `virt-install` eingerichtet werden, ist das standardmäßig der Fall.

```
root#  virt-viewer  vm-name
```

Wenn Sie `virt-viewer` ohne `root`-Rechte ausführen, aber die Verbindung zu einer auf Systemebene laufenden virtuellen Maschine herstellen möchten, geben Sie die Verbindungszeichenkette mit der Option `-c` an:

```
user$  virt-viewer -c qemu:///system  vm-name
```

Statt `virt-viewer` können Sie jeden beliebigen anderen VNC-Client einsetzen. Der einzige Unterschied besteht darin, dass Sie zuerst mit dem `virsh`-Kommando `vncdisplay` die Verbindungsdaten ermitteln müssen.

virt-top

Das Kommando `virt-top` aus dem gleichnamigen Paket liefert ähnlich wie `top` eine Auflistung aller virtuellen Maschinen. Zu jeder virtuellen Maschine werden deren Speicher- und CPU-Bedarf sowie diverse andere Parameter angezeigt.

```
user$  virt-top
virt-top 10:41:40 - x86_64 4/4CPU 1600MHz 1586OMB 0,6%
6 domains, 2 active, 2 running, 0 sleeping, 0 paused, 4 inactive D:0 O:0 X:0
CPU: 25,0%  Mem: 2048 MB (2048 MB von Gast)

   ID S RDRQ WRRQ RXBY TXBY %CPU %MEM    TIME   NAME
   15 R    0    0    0    0 24,8  6,0   0:07.57 ubuntu
   13 R    0    0  104    0  0,2  6,0   1:24.07 centos
    -                                           (debian)
    -                                           (windows)
```

43.5 Integration der virtuellen Maschinen in das LAN (Netzwerkbrücke)

Standardmäßig verwendet libvirt ein sogenanntes Usermode-Networking. Den virtuellen Maschinen wird dabei via DHCP eine IP-Adresse im Bereich 192.168.122.* zugewiesen. Der Hostrechner dient mit der IP-Adresse 192.168.122.1 als Gateway ins Internet. Die Gäste können zudem mit dem Host über dessen Adresse 192.168.122.1 kommunizieren. Davon abgesehen, können die KVM-Gäste aber nicht auf Netzwerkdienste im lokalen Netzwerk zugreifen, und umgekehrt können auch die Rechner im LAN nicht mit KVM-Gästen kommunizieren.

Damit Sie auf KVM-Gästen Server-Dienste für das lokale Netzwerk anbieten können, brauchen Sie eine virtuelle Netzwerkbrücke (Bridge), die die virtuellen Netzwerkadapter der KVM-Maschinen mit dem physikalischen Netzwerkadapter des Hostrechners verbindet.

Um die Brücke zu bauen, verwenden Sie die Werkzeuge aus dem Paket `bridge-utils`. Die Konfigurationsdetails variieren aber wie üblich von Distribution zu Distribution.

Im Folgenden beziehe ich mich auf Ubuntu. Ganz egal, mit welcher Distribution Sie arbeiten: Stellen Sie sicher, dass der Network Manager deaktiviert ist!

Konfiguration der Netzwerkbrücke (Ubuntu)

Bei Ubuntu erfolgt die Konfiguration durch die Datei `/etc/network/interfaces`. Die dort vorhandenen Zeilen zur manuellen Konfiguration der Schnittstelle zum LAN (in diesem Beispiel also `eth1`) müssen dahingehend geändert werden, dass diese Schnittstelle nun manuell gesteuert werden kann. Dafür wandern die entsprechenden Konfigurationseinstellungen nun in die Beschreibung des Interfaces `br0` (oder wie auch immer Sie die Brücke nennen). In diesem Beispiel ist 10.0.0.138 das Gateway und der DHCP-Server des lokalen Netzwerks. Der Bridge selbst wird die IP-Adresse zugewiesen, die bisher der Hostrechner innehatte (10.0.0.120). Vergessen Sie nicht, dass `/etc/resolv.conf` die Adresse des Nameservers enthalten muss!

```
# Datei /etc/interfaces/network (Ubuntu)
# Loopback-Netzwerkschnittstelle (unverändert)
auto lo
iface lo inet loopback

# Schnittstelle zum LAN (manuell)
auto eth1
# Brücke zu eth1
iface eth1 inet manual
auto br0
iface br0 inet static
       address 10.0.0.120
       network 10.0.0.0
       netmask 255.255.255.0
       broadcast 10.0.0.255
       gateway 10.0.0.138
       bridge_ports eth1
```

Mit `/etc/init.d/networking restart` starten Sie das Netzwerk neu. Die Brücke `br0` hat nun die IP-Adresse 10.0.0.120 und überträgt die IP-Pakete an den physikalischen Netzwerkadatper `eth1`. Falls die Brücke ihre IP-Adresse via DHCP beziehen soll, vereinfacht sich die Konfiguration der Schnittstelle `br0`:

```
# Datei /etc/interfaces/network
# Loopback-Netzwerkschnittstelle (unverändert)
auto lo
iface lo inet loopback
# Schnittstelle zum LAN (manuell)
auto eth1
iface eth1 inet manual
# Brücke zu eth1
auto br0
iface br0 inet dhcp
       bridge_ports eth1
```

Konfiguration der virtuellen Maschine

Beim Einrichten der virtuellen Maschine verwenden Sie die Option `--net bridge:br0`, wobei Sie statt `br0` den Device-Namen der Netzwerkbrücke angeben:

```
root#  qemu-img create image.raw 10G
root#  virt-install --name vmname --ram 384 --cdrom install.iso \
                    --disk image.raw --net bridge:br0
```

Entscheidend ist, dass `virt-install` mit `root`-Rechten ausgeführt und die virtuelle Maschine auf KVM-Systemebene eingerichtet wird. Der Grund: Die Netzwerkkommunikation zwischen dem Hostrechner und dem KVM-Gast erfolgt durch sogenannte TUN/TAP-Devices. Dabei handelt es sich um vom Kernel simulierte Netzwerkschnittstellen, die sowohl bei der erstmaligen Installation als auch bei jedem nachfolgenden Start eingerichtet werden müssen. Die `libvirt`-Werkzeuge kümmern sich zum Glück um alle Details, können ihre Arbeit aber nur mit `root`-Rechten verrichten.

43.6 Direkter Zugriff auf den Inhalt einer Image-Datei

In diesem Abschnitt geht es um die Frage, wie Sie den Inhalt eines virtuellen Datenträgers auslesen oder verändern können, ohne die virtuelle Maschine selbst zu starten. Das ist beispielsweise praktisch, um von außen Reparaturen durchzuführen oder um Konfigurationsdateien durch ein Script zu verändern.

Für den Zugriff auf den virtuellen Datenträger gibt es verschiedene Vorgehensweisen:

- Sie können den Inhalt der virtuellen Datenträger direkt im Hostsystem lesen oder verändern,
- Sie können auf diverse `libguestfs`-Werkzeuge zurückgreifen, oder
- Sie können ein Linux-Live-System zu Hilfe nehmen, also die virtuelle Maschine vom ISO-Image einer Linux-Distribution starten und von dort aus auf die virtuellen Festplatten zugreifen.

In diesem Abschnitt gehe ich nur auf die beiden ersten Varianten ein. Manche der hier vorgestellten Werkzeuge können ausschließlich RAW-Images bearbeiten. Gegebenenfalls müssen Sie eine in einem anderen Format vorliegende Image-Datei in dieses Format umwandeln:

```
user$  qemu-img convert -f qcow2 image.qcow2 -O raw image.raw
```

Mit dem folgenden Kommando erzeugen Sie aus einem Logical Volume oder einer Festplattenpartition ein äquivalentes RAW-Image:

```
root#  dd if=/dev/mapper/vg830-lv2 of=copy.raw bs=64M
312+1 Datensätze ein
312+1 Datensätze aus
20971520000 Bytes (21 GB) kopiert, 133,462 s, 157 MB/s
```

Ein Schreibzugriff auf einen virtuellen Datenträger ist nur zulässig, wenn die virtuelle Maschine vollkommen heruntergefahren ist! Andernfalls riskieren Sie ein kaputtes Dateisystem!

Zugriff auf partitionierte RAW-Images im Hostsystem

kpartx

Mit dem Kommando `kpartx` aus dem gleichnamigen Paket verbinden Sie alle in einer RAW-Datei enthaltenen Partitionen mit Loop-Devices:

```
root#  kpartx -av image.raw
add map loop0p1 (252:12): 0 1024000 linear /dev/loop0 2048
add map loop0p2 (252:13): 0 19945472 linear /dev/loop0 1026048
```

Bei unseren Tests hat dies auch funktioniert, wenn die Image-Datei eine GUID Partition Table enthält (also keine traditionelle Partitionstabelle im Master Boot Record). Soweit es sich um normale Partitionen handelt, können Sie diese nun direkt mit `mount` in das Dateisystem einbinden:

```
root#  mkdir /repair1
root#  mount /dev/mapper/loop0p1 /repair1
```

LVM

Wenn Sie innerhalb der virtuellen Maschine LVM konfiguriert haben, stehen die resultierenden Physical und Logical Volumes sowie Volume Groups direkt zur Verfügung. Listen der LVM-Elemente liefern `lvscan`, `pvscan` und `vgscan`. Der Zugriff auf die LVs setzt voraus, dass auf dem Hostsystem die LVM-Werkzeuge installiert sind.

```
root#  lvscan
ACTIVE            '/dev/VolGroup/lv_root' [7,56 GiB] inherit
ACTIVE            '/dev/VolGroup/lv_swap' [1,94 GiB] inherit
...
root#  mkdir /repair2
root#  mount /dev/VolGroup/lv_root /repair2
```

Nun können Sie über die Verzeichnisse `repair`*n* auf die Dateisysteme der virtuellen KVM-Festplatte zugreifen. Wenn Sie damit fertig sind, müssen Sie aufräumen:

```
root#  umount /repair1
root#  umount /repair2
root#  kpartx -dv image.raw
```

libguestfs-Werkzeuge

Anstatt die Image-Datei selbst zu analysieren und die relevanten Partitionen in das lokale Dateisystem zu integrieren, können Sie diese Aufgaben diversen Werkzeugen überlassen, die auf der `libguestfs`-Bibliothek aufbauen.

Die Bibliothek `libguestfs` erlaubt den direkten Zugriff auf die Dateisysteme, die sich innerhalb einer Image-Datei befinden. `libguestfs` unterstützt alle erdenklichen Image-Formate, Partitionen, LVM sowie alle gängigen Dateisysteme. Die Bedienung der `libguestfs`-Werkzeuge ist auf der folgenden Website sowie auf der `man`-Seite `libguestfs` umfassend dokumentiert:

http://libguestfs.org

Installation

RHEL und Fedora liefern alle erforderlichen Pakete gleich mit (`yum install *guestf*`), bei Ubuntu müssen Sie auf das folgende Download-Verzeichnis zurückgreifen:

http://libguestfs.org/download/binaries/ubuntu1204-packages

Unter Ubuntu müssen Sie außerdem die Kerneldateien in `/boot/` für alle Benutzer lesbar machen:

```
user$  sudo chmod a+r /boot/vmlinuz*
```

virt-df

Das Paket `libguestfs-tools` enthält diverse Kommandos zur Manipulation von Image-Dateien. Die zu bearbeitende oder zu analysierende Image-Datei geben Sie in der Regel mit `-a image-datei` an. Alternativ können Sie mit `-d vmname` den `libvirt`-Namen der virtuellen Maschine angeben.

`virt-df` gibt einen raschen Überblick über die Auslastung aller Dateisysteme aller virtuellen Maschinen, die den libvirt-Werkzeugen bekannt sind. Das Kommando kommt auch mit Logical Volumes innerhalb von virtuellen Datenträgern zurecht.

```
root#  virt-df
Filesystem                            1K-blocks       Used  Available  Use%
centos-mini:/dev/sda1                    495844      52091     418153   11%
centos-mini:/dev/sdb1                  20157836     253468   18880396    2%
centos-mini:/dev/vg_centosmini/lv_root
                                        9571132    1051104    8033836   11%
centos64-vm2:/dev/sdb                   4319464    4319464          0  100%
centos64-vm2:/dev/sda1                   495844      32918     437326    7%
centos64-vm2:/dev/vg_vm2/lv_root        7539088    2369932    4786180   32%
...
```

Wenn Sie nur an den Ergebnissen einer einzelnen virtuellen Maschine interessiert sind, geben Sie den Dateinamen der Image-Datei mit `-a` oder den libvirt-Namen der virtuellen Maschine mit `-d` an.

virt-filesystems

`virt-filesystems` verrät, welche Dateisysteme sich in einer Image-Datei befinden. Mit den Optionen `--all`, `--long` und `--uuid` listet das Kommando auch LVM- und Swap-Partitionen auf und gibt die UUID-Nummern der Dateisysteme an.

```
root#  virt-filesystems -a vm2.img --all --long --uuid
Name                Type       VFS  Label Size        Parent      UUID
/dev/sda1           filesystem ext4 -     524288000   -           7a95...
/dev/vg_vm2/lv_root filesystem ext4 -     7843348480  -           e69f...
/dev/vg_vm2/lv_swap filesystem swap -     2113929216  -           e0f4...
...
```

virt-inspector

`virt-inspector` wirft einen Blick in die Dateisysteme einer Image-Datei und verrät, welche Distribution darin installiert ist, welche Partitionen es gibt, welche Kernelversion und welche Pakete installiert sind etc. `virt-inspector` kennt sowohl das RPM- als auch das Debian-Paketsystem.

```
root#  virt-inspector disk.img
linux centos x86_64 6.4 (CentOS release 6.4 (Final)) on /dev/vg_vm2/lv_root:
  Mountpoints:
    /dev/vg_vm2/lv_root            /
    /dev/sda1                      /boot
    /dev/vg_vm2/lv_swap            swap
  Filesystems:
    /dev/sda1:
      label:
      UUID: 7a95ebf4-4a3d-4a87-888f-93c08505156c
      type: ext4
      content: linux-grub
...
```

virt-cat

`virt-cat` gibt eine Datei einer virtuellen Maschine aus:

```
root#  virt-cat -d centos64 /etc/fstab
LABEL=79d3d2d4  / ext4    defaults,noatime 0 0
...
```

Um die Datei in einem Editor zu verändern, verwenden Sie anstelle von `virt-cat` das Kommando `virt-edit`. Es darf nur für ausgeschaltete virtuelle Maschinen verwendet werden! Abweichend von den anderen Kommandos wird der Name der Image-Datei bzw. der virtuellen Maschine ohne die Optionen `-a` bzw. `-d` angegeben. `virt-edit` berücksichtigt bei der Wahl des Editors die Umgebungsvariable `EDITOR`. Standardmäßig wird der Editor `vi` ausgeführt.

```
root#  virt-edit centos64 /etc/fstab
```

virt-tar

Mit `virt-tar` können Sie ein Archiv von Dateien aus dem Dateisystem der virtuellen Maschine lesen oder dorthin schreiben – Letzteres aber nur, wenn die virtuelle Maschine ausgeschaltet ist. Das folgende Kommando liest das Verzeichnis `/root` der virtuellen Maschine `vm1` aus und speichert es in einem tar-Archiv.

```
root#  virt-tar -z -x vm1 /root root-backup.tar.gz
```

`virt-make-fs` erzeugt eine neue Image-Datei und speichert darin den Inhalt eines Verzeichnisses oder eines tar-Archivs: virt-make-fs

```
root#  virt-make-fs mydata.tar.gz new-disk.img
```

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z