

Inhaltsverzeichnis

1	Vor dem Start	17
1.1	Der richtige Anbieter	17
1.1.1	Die lieben Finanzen	17
1.1.2	Klein, stark, schwarz?.....	19
1.2	Was Ihr PC können muss	21
1.2.1	Grundausstattung unter Windows	21
1.2.2	Versuchslabor im PC.....	22
1.2.3	Zugriff auf den Server.....	22
1.2.4	Dateien hochladen	23
2	Einführung in Linux	25
2.1	Grundlegende Eigenschaften.....	25
2.2	Unterschiede zu Windows	28
2.2.1	Einer für alle	28
2.2.2	Freie Namenswahl.....	28
2.2.3	Flexible Oberflächen.....	29
2.2.4	Das Client/Server-Konzept.....	29
2.2.5	Die zwei Dateitypen	30
2.3	Die wichtigsten Befehle	31
2.3.1	Woher und wohin	31
2.3.2	Linux-Verzeichnisstruktur.....	35
2.3.3	Dateioperationen	37
2.3.4	Suchen und Finden	41
2.3.5	Benutzer und Gruppen.....	43
2.3.6	Linux- und DOS-Befehle im Vergleich.....	46
2.3.7	Hilfe und Dokumentation	47
2.4	Programme, Prozesse und Dämonen.....	49
2.4.1	Allgemeines über Prozesse.....	49
2.4.2	Der Init-Prozess: Linux startet	51
2.4.3	Prozesse verwalten	54
2.4.4	Nützlich: Die Dämonen.....	56
2.5	Software installieren und deinstallieren.....	57
2.5.1	Programmpakete verwalten – Rpm, Yast, Apt	57
2.5.2	Programme selbst kompilieren – make, install	61
2.6	Oft benötigte Programme	64
2.6.1	Die Shell.....	64
2.6.2	Konfigurationsdateien bearbeiten – der Editor Vi	67

2.6.3	Eine Alternative zu Vi: Pico.....	69
2.6.4	Texte automatisch bearbeiten mit dem Editor Sed	70
2.6.5	Programme ausführen: Screen.....	71
2.6.6	Dateien archivieren und komprimieren – Tar und Gzip, Bzip2	73
2.6.7	Programme zeitgesteuert ausführen – Cron und Crontab	75
2.6.8	Programme downloaden – Wget.....	76
2.6.9	Im Textmodus im Internet surfen – Lynx	77

3	Die größten Anbieter.....	79
3.1	Die Anbieter	80
3.1.1	1&1 – Rootserver	80
3.1.2	IPX-Server	81
3.1.3	Hetzner	82
3.1.4	BSB Server4Free	83
3.1.5	Strato	85
3.1.6	MBBG Domainbox	85
3.1.7	Weitere Anbieter	86
3.2	In 10 Schritten zur eigenen Website	86
3.2.1	Schritt 1	87
3.2.2	Schritt 2	87
3.2.3	Schritt 3	88
3.2.4	Schritt 4	89
3.2.5	Schritt 5	89
3.2.6	Schritt 6	90
3.2.7	Schritt 7	92
3.2.8	Schritt 8	92
3.2.9	Schritt 9	92
3.2.10	Schritt 10	93
3.2.11	1&1 – Rootserver	94
3.2.12	IPX-Server	94
3.2.13	Server4free	94
3.2.14	MBBG Domainbox	95
3.2.15	Hetzner	98
4	Die wichtigste Serversoftware.....	101
4.1	Grundkonfiguration.....	101
4.1.1	1&1	101
4.1.2	IPX-Server	102
4.1.3	Hetzner	103
4.1.4	Server4Free	104
4.1.5	Strato	105
4.1.6	MBBG Domainbox	107
4.2	Apache, der Webserver.....	107
4.2.1	Apache auf den neuesten Stand bringen	108
4.2.2	Apache und seine Module	112
4.2.3	Die Apache-Konfigurationsdatei httpd.conf	117

4.2.4	Die .htaccess-Dateien	125
4.2.5	Verzeichnislistings verschönern mit mod_autoindex	128
4.2.6	Tippfehler der Anwender korrigieren: mod_speling	129
4.2.7	Das Schweizer Offiziersmesser: mod_rewrite	130
4.2.8	Apache lernt Fremdsprachen: mod_negotiate	133
4.2.9	Webseiten schrumpfen: mod_gzip	134
4.2.10	Apache und Server Side Includes (SSI): mod_include.....	136
4.2.11	Apache und CGI / Perl: mod_cgi	139
4.2.12	Apache und die Sicherheit.....	140
4.3	PHP	141
4.3.1	PHP benutzen.....	143
4.3.2	PHP und die Sicherheit.....	146
4.4	MySQL.....	147
4.4.1	phpMyAdmin.....	149
4.5	Perl.....	151
4.5.1	Perl installieren	151
4.5.2	Perl und mod_perl.....	152
4.5.3	Perl benutzen	153
4.5.4	Perl-Module	155
4.6	Mailserver & Co.	156
4.6.1	Mails senden und empfangen mit Postfix	157
4.6.2	Das Postbüro im Netz: Qpopper.....	162
4.6.3	Mails verarbeiten mit Procmail	164
4.6.4	Mails filtern mit SpamAssassin	164
4.6.5	Schwarzes Loch mit Ausgang: RBL.....	166
4.6.6	E-Mail ganz komfortabel: Courier IMAP	167
4.7	Bind, der Nameserver.....	168
4.7.1	Die named.conf.....	169
4.7.2	Die Reverse-Zone	170
4.7.3	Das eigentliche Zonefile	170
4.7.4	Die wichtigsten Records	172
4.7.5	Standard-Zonefile.....	172
4.7.6	Record testen	173
4.8	ProFTP, der FTP-Server	173
4.8.1	Installation von ProFTPd	173
4.8.2	Konfiguration des FTP-Servers	175
4.8.3	ProFTPd-Module	177
4.8.4	mod_sql.....	178
4.8.5	ProFTPd und TLS	179
4.9	Gameserver.....	180
4.9.1	Jedi Knight 2 – Jedi Outcast.....	180
4.9.2	Battlefield 1942.....	183
4.9.3	Half-Life (deutsche Version) & Co.....	185
4.9.4	Operation Flashpoint.....	190
4.9.5	Medal of Honor – Allied Assault	192
4.9.6	Star Trek Voyager: Elite Force	193

4.9.7	Command & Conquer: Renegade	196
4.9.8	Aliens vs. Predator 2	200
4.9.9	Neverwinter Nights	201
4.9.10	VoiceServer: TeamSpeak 2.....	207
5	Confixx, Visas, Webmin	211
5.1	Der Klassiker: Confixx.....	212
5.1.1	Confixx für Administratoren	213
5.1.2	Confixx-Design anpassen	224
5.1.3	Wichtige Konfigurationsdateien.....	225
5.1.4	Upgrade auf die Version 2	229
5.1.5	Serverumzug mit Confixx.....	232
5.1.6	Fehlersuche innerhalb von Confixx.....	233
5.2	Der Mächtige: Webmin	236
5.2.1	Installation	237
5.2.2	Das Webmin-Menü	238
5.2.3	Das Systemmenü.....	240
5.2.4	Das Servermenü	245
5.2.5	Praktische Funktionen.....	248
5.3	Der Neue: Visas	249
5.3.1	Serveradministrator-Level (root)	250
5.3.2	Kunden-Level (virtuelle Server)	254
5.4	Manuelle Benutzerverwaltung	255
5.4.1	Benutzer- und Gruppenlisten direkt bearbeiten	256
5.4.2	Nutzer per Kommandozeile hinzufügen	258
6	Wenn nichts mehr geht	261
6.1	Zur Vorsorge: Backups.....	261
6.1.1	Definition und Ziele eines Backups	262
6.1.2	Backup-Medien	262
6.1.3	Backup-Prinzipien und -Arten	264
6.1.4	Backup-Systeme	265
6.1.5	MySQL-Datenbanken sichern	270
6.1.6	Einrichten eines Backup-Systems für ein Vollbackup.....	271
6.1.7	Einrichten eines Systems für ein inkrementelles Backup	278
6.2	Logfile-Analyse	282
6.2.1	Einzelne Logfiles und ihr Inhalt.....	283
6.2.2	Handwerkszeug für die Logfile-Analyse.....	284
6.3	Neustart mit Optionen	284
7	Sicherheitsstrategien	287
7.1	Manueller Zugriff auf den Server	287
7.2	Die Macht des Superusers	288
7.2.1	»root« und sein Kennwort	288
7.2.2	Einloggen als »root« vermeiden.....	289

7.3	Grundkonfiguration absichern	292
7.3.1	Ein Account pro Nutzer	292
7.3.2	Sichere Kennwörter	292
7.3.3	Sichere Suchpfade	293
7.3.4	Sichere Dateiberechtigungen	293
7.3.5	Unsichere und unnötige Dienste deaktivieren	295
7.3.6	Zugriffsregeln definieren	298
7.3.7	Daten filtern	300
7.3.8	Startdateien aufräumen	306
7.3.9	Unnötige Programme entfernen	307
7.3.10	Anwendungen und Sicherheit, »chrooting«	307
7.3.11	Gameserver und Sicherheit	308
7.4	Prüfen	309
7.4.1	Nessus	309
7.4.2	Andere Tools	313
7.5	Vorsorgen	314
7.5.1	Tripwire	315
7.5.2	AIDE	315
7.6	Informieren	318
7.7	Reagieren	319
7.7.1	Die Kontrolle zurückgewinnen	319
7.7.2	Den Einbruch analysieren	322
7.7.3	Dritte kontaktieren	322
7.7.4	System neu einrichten und sichern	323
	Stichwortverzeichnis	325

2 Einführung in Linux

Lassen Sie sich nicht abschrecken: Linux ist schon lange nicht mehr das einsteigerfeindliche System, als das es früher verschrien war. Auf den folgenden Seiten lernen Sie, was Sie zur erfolgreichen Verwaltung Ihres Linux-Servers wissen müssen.

2.1 Grundlegende Eigenschaften

Was ein Betriebssystem ist, wissen Sie wahrscheinlich bereits: Es ist die in Software gegossene Komponente Ihres PCs, die für das reibungslose Zusammenspiel der Hardwarebestandteile sorgt, Ihre Eingaben entgegennimmt und Ergebnisse auf dem Bildschirm darstellt.

Im Vergleich zu Microsofts Windows-Betriebssystem, dessen allererste Version 1985 vorgestellt wurde, ist Linux noch vergleichsweise jung: Erst 1991 erschien die erste öffentliche Version 0.02 des ursprünglich von dem finnischen Studenten Linus Torvalds entwickelten Systems; bis tatsächlich von einer weltweiten Programmierergemeinde die Versionsnummer 1.0 erreicht wurde, vergingen weitere drei Jahre. Doch Linux steht in einer langen Ahnenreihe von UNIX-Systemen – deren erste Version wurde schon 1969 von Ken Thompson implementiert.

Linux profitierte fast von Beginn an stark vom GNU-Projekt (www.gnu.org (id15)), das seit 1984 bestrebt war, ein komplettes, freies, UNIX-kompatibles Betriebssystem zu schaffen. Insofern besteht die GNU-Gemeinde durchaus zu Recht darauf, statt von »Linux« besser von »GNU/Linux«-Systemen zu sprechen. Doch: eingebürgert hat sich inzwischen nun einmal Linux ohne Zusatz, deshalb bleibt auch dieses Buch dabei.



Bild 2.1: Tux, das Linux-Maskottchen

Wie andere Betriebssysteme auch, besteht Linux aus einem Kern (dem »Kernel«) und System- und Dienstprogrammen. Nur der Betriebssystemkern wird nach wie vor von Linus Torvalds verwaltet; Änderungen daran werden von ihm freigegeben. Jedermann kann die Linux-Quelltexte einsehen, die Codezeilen, aus denen sich System und Dienstprogramme erzeugen (kompilieren) lassen. Die Lizenz, unter der Linux freigegeben ist, die GPL, erlaubt es sogar, Quellcode in eigenen Projekten zu verwenden – vorausgesetzt, diese unterliegen derselben Lizenz, werden also auch wieder für jedermann freigegeben.

Dieser sehr weit gehenden Offenheit hat Linux einen großen Teil seiner Popularität zu verdanken – sie steht so ganz im Kontrast zu der Geheimniskrämerei, mit der Microsoft sein Windows umgibt, um Konkurrenten den Wettbewerb zu erschweren.

Verteilt wird Linux in Form so genannter Distributionen. Diese enthalten außer dem Betriebssystemkern, auf den alle »Linuxe« gleichermaßen zugreifen, jede Menge zusätzlicher Software und mehr oder weniger komfortable Installationsroutinen. Wenn Sie eine solche Distribution im Laden kaufen, merken Sie, dass »frei« und »offen« nicht unbedingt auch »kostenlos« heißen muss. Doch Sie bezahlen nicht das Betriebssystem an sich, sondern die spezifische Art und Weise der Kombination aus Anwendungssoftware, Dienstprogrammen, Installationsroutinen, umfangreichen Handbüchern und nicht zuletzt den immer mehr Datenträgern. Tatsächlich ist Linux heute nicht mehr das einsteigerfeindliche System, als das es früher verschrien war: Firmen wie SuSE (www.suse.de (id16)) und Mandrake (www.mandrakesoft.com (id17)) haben viel Hirnschmalz in einfache, auf fast jedem PC funktionierende Installationsroutinen gesteckt. Oft ist im Kaufpreis sogar ein zeitlich begrenzter telefonischer Installationssupport enthalten.

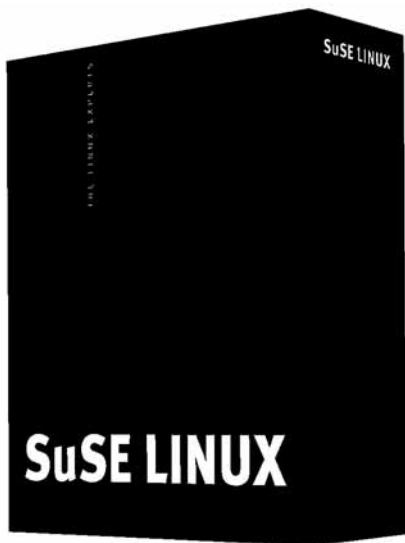


Bild 2.2: Die Einsteigervariante von SuSE Linux

Mittlerweile gehen die Firmen dazu über, spezialisierte Distributionen anzubieten – etwa für kleine Server oder für den Mittelstand. Daneben gibt es auch Linux-Pakete, die nicht von Unternehmen, sondern von Gruppen von Linux-Fans gepflegt werden. Die »Debian«-Distribution (www.debian.org (id18)) gehört zu dieser Kategorie. Sie ist vor allem unter Linux-Experten beliebt, weil sie großen Wert auf Stabilität legt. Ein weiteres Spezial-Linux ist »Knoppix« (www.knoppix.org (id19)), von dem im vorangegangenen Kapitel schon die Rede war. Dabei handelt es sich um ein Debian-System, das speziell darauf angepasst wurde, rein von CD aus zu funktionieren, ohne irgend etwas installieren zu müssen. Die Vielfalt zeigt, dass Distributionen nichts Statisches sind – jeder Linux-Anwender kann sich seine eigene zusammenstellen.

Bevor Sie eine Linux-Variante im Laden erwerben, sollten Sie prüfen, welche Distribution der von Ihnen präferierte Rootserver-Anbieter auf seinen Rechnern installiert.

Denn natürlich macht es sich im Fall des Falles besser, auf ein weitgehend identisches System zurückgreifen zu können. Allerdings unterscheiden sich die Distributionen auch nicht so gravierend wie etwa Windows und MacOS – wenn Sie mit SuSE Linux gut umgehen können, fällt Ihnen der Einstieg in RedHat nicht schwer. Nur – der Teufel steckt wie immer im Detail.

Sind Sie sich Ihrer Sache noch nicht sicher, probieren Sie doch einfach mal Knoppix – damit können Sie gar nichts falsch machen. Besorgen können Sie sich Knoppix entweder von der Heft-CD einer Computerzeitschrift oder per Online-Bestellung bei einem der unter www.knoppix.org (id19) registrierten Versender. Download-Links finden Sie hier auch – die sind zumindest bei einer flinken Internetanbindung eine Alternative. Später können Sie Knoppix dann auch fix auf der Festplatte installieren. Oder Sie kaufen eine Linux-Distribution im Softwarehandel. Mit einem großen Vorteil: den umfangreichen, inzwischen durchaus ausgereiften Handbüchern. Zudem ist der Lieferumfang dieser Varianten inzwischen auf fast zehn CDs angewachsen – da dauert der Download schon ein Weilchen.

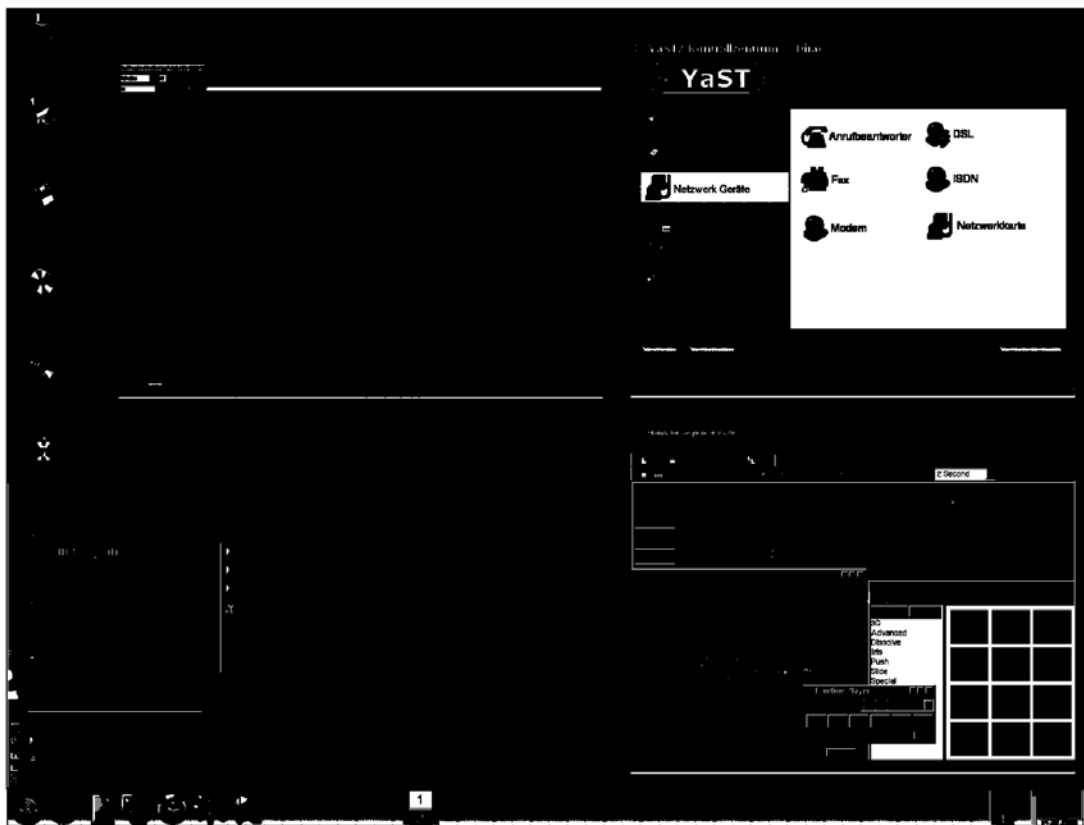


Bild 2.3: Schicker Schreibtisch: Linux-Oberfläche (SuSE)

Mit der Zeit werden Sie gar feststellen, dass Sie Windows immer seltener benötigen. Denn die Bedienung von Linux ist mindestens so komfortabel wie die von Microsofts Betriebssystem. Die Fenster sehen ebenso schick aus – und mit OpenOffice steht für Linux eine mächtige Bürosoftware zur Verfügung, die sich hinter MS-Office wahrlich nicht verstecken muss. Im technisch-wissenschaftlichen und im kommunikativen Bereich waren UNIXe schon traditionell stark, und auch im Grafikbereich kann etwa

GIMP auftrumpfen. Nur wenn Sie leidenschaftlicher PC-Spieler sind, sollten Sie Bill Gates' System nicht vorschnell von der Platte verbannen: Das Spieleangebot unter Linux bietet zwar aus allen Bereichen hübsche Kandidaten – Neuerscheinungen gibt's aber so gut wie immer zuerst unter Windows.

2.2 Unterschiede zu Windows

2.2.1 Einer für alle

Auch wenn sich Linux und Windows oberflächlich ähneln und natürlich auch dieselben Aufgaben zu erfüllen haben, so gibt es doch wichtige Unterschiede.

UNIX – und damit Linux – ist ein echtes Mehrbenutzersystem, während alle Windows-Versionen bis ME nur scheinbar für mehrere Nutzer ausgelegt waren. Sie benötigen also, um lokal oder auch aus der Ferne an einem Linux-Rechner arbeiten zu können, auf jeden Fall ein so genanntes Benutzerkonto – nämlich einen Benutzernamen und ein Passwort. Mehrere User können gleichzeitig und unabhängig voneinander an einem Unix-Rechner arbeiten, ohne sich ins Gehege zu kommen. Das macht zwar lokal wenig Sinn, weil in der Regel nur eine Tastatur und ein Monitor zur Verfügung stehen. Es ist aber für Internetserver ein essenzielles Feature. Dieses Konto kann Ihnen nur der Administrator eröffnen, er hat in der Regel den Benutzernamen »root«.

Eine Grundvoraussetzung für die Mehrbenutzerfähigkeiten ist die konsequente Rechtevergabe von Unix. Unter Windows 9x hingegen können sich zwar auch verschiedene Nutzer anmelden, diese haben aber dieselben Rechte: User A kann zum Beispiel problemlos die Dateien von User B ändern. Das kann unter Linux nicht passieren: Die Dokumente, die Nutzer A angelegt hat, gehören ihm allein. Allenfalls ein Administrator könnte daran etwas ändern. Das trifft ebenso auf die Installation (oder das Entfernen) von Programmen zu. Und natürlich auf das Löschen der Festplatte – während unter Windows (bis ME) jeder Anwender `FORMAT C:` ausführen kann. Außerdem können Sie unter Linux Teil einer Benutzergruppe sein, die der Administrator mit speziellen Rechten ausstatten darf. Auf einem Schulserver wären der Gruppe der Lehrer etwa andere Dateien und Bearbeitungsoptionen zugänglich als der Gruppe der Schüler.

Jedem Benutzerkonto ist unter Linux ein Heimatverzeichnis zugeordnet. Was Sie darin ablegen, kann kein anderer Nutzer einsehen, ändern oder löschen – es sei denn, Sie erlauben es explizit. Bei Windows 9x-Systemen gibt es solch ein Verzeichnis nicht wirklich. Sie können dort allenfalls Ihren Desktop oder das Startmenü anpassen.

2.2.2 Freie Namenswahl

Unterschiedlich ist bei beiden Systemen auch die Dateiverwaltung geregelt. Beschränkungen, wie Sie sie noch aus alten DOS-Zeiten kennen, wo etwa Dateinamen maximal acht Zeichen haben durften, gefolgt von einer drei Zeichen langen Dateiendung, hat es unter Unix nie gegeben. Wichtig: Linux unterscheidet in Dateinamen und Programmbefehlen zwischen Groß- und Kleinschreibung. So können sich in ein und demselben

Verzeichnis die Dateien test.txt, Test.txt und TEST.TXT befinden – das ist unter Windows verboten.

Frei wählen können Sie in Linux auch die Endung der Datei. Besser gesagt: Sie können auch ganz auf eine solche verzichten. Es empfiehlt sich allerdings aus Gründen der Übersicht, selbst erstellte Dateien systematisch zu benennen: etwa mit a.txt für einen Text und b.pic für ein Bild. Den oder die Punkt(e) im Dateinamen wertet Linux wie jedes andere Zeichen darin aus. Erlaubt sind aber auch alle anderen ASCII-Zeichen – bis zu 255 Zeichen darf ein Dateiname lang sein. Allerdings sollten Sie sich auf Punkt (.), Bindestrich (-) und Unterstrich (_) beschränken, wenn Sie beim Datenaustausch Probleme vermeiden wollen. Dateinamen mit Leerzeichen müssen in Shell-Kommandos (ähnlich wie unter Windows) in Anführungszeichen gesetzt werden, damit das System den Namen als Einheit erkennen kann.

2.2.3 Flexible Oberflächen

Als Windows erstmals vorgestellt wurde, war es noch ein reiner Betriebssystemaufsatz. DOS stellte das eigentliche Betriebssystem dar, das die grafische Benutzeroberfläche Windows erst startete. Das hat sich mit Windows 95 (zaghafte) und mit Windows NT ernsthaft geändert: Betriebssystem und Benutzeroberfläche sind eine Einheit.

Bei Linux ist das anders: Das System selbst ist vollkommen textorientiert. Denn gerade bei Servern, die eher Verteilungs- und Verwaltungsaufgaben übernehmen, schont das die Ressourcen des Systems zugunsten seines Hauptzwecks. In dieser Textumgebung, der so genannten Shell, kann der Benutzer sämtliche nötigen Programme und Funktionen ausführen. Der eigentliche Vorteil liegt hier in der Flexibilität: Linux-Anwender sind nicht auf eine bestimmte Shell angewiesen, je nach persönlichem Geschmack können Sie zwischen verschiedenen Shells wählen.

Eine grafische Oberfläche (genauer gesagt gleich mehrere verschiedene davon) besitzt Linux natürlich auch. Auch sie besteht wiederum aus zwei Komponenten: Das so genannte X-Window-System macht den Computer quasi grafikfähig. Darauf setzt der Fenstermanager auf: Er stellt Ihnen eine komfortable, Windows-ähnliche Benutzeroberfläche zur Verfügung. Beliebte Fenstermanager sind zum Beispiel »Gnome« und »KDE«. Damit werden Sie aber als Mieter eines Internetserverns weniger zu tun haben – es wäre viel zu bandbreitenaufwändig, ein grafisches System aus der Ferne per Maus zu steuern.

Das heißt aber auch, dass Sie sich wie in alten DOS-Zeiten wieder auf die Kommandozeile einstellen müssen. Diese stellt unter Linux nach wie vor ein sehr wichtiges Arbeitsmittel dar. Das liegt aber auch daran, dass sie ihrem DOS-Pendant nur äußerlich ähnelt – intern ist sie um vieles mächtiger.

2.2.4 Das Client/Server-Konzept

Dass Linux vor allem ein System für viele, in Netzwerken organisierte Anwender und Rechner ist (ein gutes Einzelplatzsystem ist es natürlich auch), ist an den unter Windows weniger gebräuchlichen Programmkonzepten zu erkennen. Eine Windows-Anwendung

ist meist monolithisch, sie bringt alles mit, was gebraucht wird, und ist für den lokalen Betrieb ausgelegt. Solche Programme gibt es unter Linux auch.

Wenn aber mehrere Nutzer auf dieselbe Software zugreifen wollen, ist es pure Platzverschwendung, diese auf den Festplatten aller Rechner zu installieren. Sinnvoller ist es da, solche Programme als Server zu konzipieren. Server laufen auf einem bestimmten Rechner und stellen den Anwendern im ganzen damit verbundenen Netz ihre Dienste zur Verfügung. Nun können User diese Dienste nicht direkt ansprechen – diese Aufgabe bleibt Client-Programmen überlassen. Die Clients kontaktieren den Server, übergeben ihm die nötigen Daten und Anforderungen und holen dann die Ergebnisse ab. Sehr wahrscheinlich arbeiten Sie bereits mit Client-Software: Ihr E-Mail-Programm ist zum Beispiel ein solcher Client.

Dieses Prinzip klingt kompliziert, ist aber durchaus vorteilhaft. Es erlaubt nämlich, dass sich Rechner kostengünstig spezialisieren. Wenn ein Programm zum Beispiel sehr viele Berechnungen in kurzer Zeit ausführen soll, benötigt man im Client/Server-Modell einen sehr flinken Server. Würde man nicht auf dieses Modell setzen, bräuchten alle User, die das Programm einsetzen sollen, entsprechend schnelle Computer. Zentralisieren lässt sich bei Client/Server-Systemen auch die Datenablage: Eine zentrale Datenbank ist viel einfacher zu verwalten und aktuell zu halten als auf allen möglichen Rechnern verteilte Bestände. Und schließlich wäre da auch noch der Faktor »Freiheit«: Sie brauchen nicht vor dem Firmenserver zu sitzen, um auf die Daten Ihres Unternehmens zuzugreifen.

2.2.5 Die zwei Dateitypen

Zwei Dateitypen? Tatsächlich: Die Tausende unterschiedlicher Dateitypen in Windows sind genau genommen Dokumenttypen. Wenn Betriebssysteme hingegen zwischen Dateitypen unterscheiden, sind damit ASCII- und Binärdateien gemeint. Letztere enthalten Daten im Binärcode, dabei handelt es sich oft um Programme, doch auch Bilder oder Audiodaten werden als Binärfile übertragen. Lesbar (oder ausführbar) sind sie nur für den Computer selbst. ASCII-Dateien hingegen enthalten Zeichen, die auch Menschen interpretieren können. Man kann sie in einem so genannten Editor öffnen und bearbeiten.

Sie sind in Zeilen aufgeteilt – und hier beginnt das Problem: Der Computergemeinde ist es bisher nicht gelungen, sich auf ein bestimmtes Zeichen zu einigen, das das Zeilenende definiert. Unter Linux genügt (wie unter allen Unixen) LF (»Linefeed«, also Zeilenvorschub). Windows hingegen möchte danach noch ein »CR« (»Carriage Return«, das heißt Wagenrücklauf – die Namen der Zeichen stammen noch aus Schreibmaschinenzeiten) sehen. Wenn Sie nun eine mit Linux erzeugte Textdatei mit einem Windows-Editor betrachten, sehen Sie nur eine endlos lange Zeile.

Das Problem ist natürlich nicht ganz neu und lässt sich einfach lösen, indem man betroffene Dateien programmgesteuert umwandelt. Diese Konvertierung kann auf Wunsch zum Beispiel ein FTP-Programm übernehmen: Binärdateien überträgt es unverändert, bei ASCII-Files fügt es je nach System CR-Zeichen hinzu oder löscht sie. Sie

müssen der Software lediglich verraten, welche Dateien sie im ASCII-Modus übertragen soll.

2.3 Die wichtigsten Befehle

Sich mit Hilfe der Linux-Shell durch das Dateisystem zu bewegen, ist für Maus-Akroba-ten durchaus eine Umstellung. Wer hingegen regelmäßig am DOS-Prompt gearbeitet hat, wird mit den Linux-Befehlen wenig Probleme haben. Allerdings steckt der Teufel im Detail – auch ähnlich lautende Kommandos verfügen oft über unterschiedliche Parameter. Bei der Erläuterung der wichtigsten Befehle lassen wir all diejenigen aus, die nur von Bedeutung sind, wenn Sie persönlich vor dem Server sitzen (das Partitionieren von Festplatten zum Beispiel).

2.3.1 Woher und wohin

Nachdem Sie sich erstmals an Ihrem Server angemeldet haben (wie das geht, lesen Sie in Kapitel 3), erwartet Sie ein spartanischer Prompt, der je nach Anbieter ein wenig anders aussehen kann:

Der Befehl »pwd« (»print work directory«) verrät Ihnen immer, in welchem Ordner Sie sich zurzeit befinden.

Das aktuelle Verzeichnis heißt root. Das ist keine Überraschung, denn nach dem Login landen Sie stets zunächst in Ihrem Heimatverzeichnis. Und da Sie den Rootserver eben erstmals »betreten« haben, mussten Sie sich als Anwender »root« einloggen. Das sollten Sie übrigens nicht zur Gewohnheit erheben – »root« darf einfach alles, machen Sie unter diesem Usernamen Fehler, bestraft das System dies unter Umständen schmerzhaft. Jetzt, am Anfang, müssten Sie allerdings allenfalls eine Neuinstallation in Kauf nehmen (die viele Anbieter nicht kostenlos ausführen).

Erforschen Sie am besten zunächst die Verzeichnisstruktur Ihres Servers. Sie, als »root«, haben zunächst überall Zutritt. In andere Ordner wechseln Sie mit dem Kommando »cd« (change directory):

Die zwei Punkte (Leerzeichen nicht vergessen!) nach dem cd-Befehl sorgen dafür, dass Sie eine Verzeichnisebene höher gelangen.

Wie der Zufall so spielt, sind Sie nun im Hauptverzeichnis / angekommen. Dass Sie hier kein C:\ sehen, liegt an einem ganz wichtigen Unterschied zwischen Windows und

Linux: Das Konzept der Laufwerke oder Laufwerksbuchstaben gibt es in Linux nicht. Festplatten, CD-ROMs und so weiter werden gleichberechtigt und flexibel im Dateisystem aufgehängt – »gemountet«. Ob ein Ordner sich auf der einen oder anderen Festplattenpartition befindet, ist für das Linux-System unerheblich. Da Sie Ihren Server nur aus der Ferne sehen, ist das für Sie aber nicht so bedeutsam.

Dass an dieser Stelle auch die Tilde verschwunden ist, erklärt sich aus ihrer Bedeutung: sie steht für das Heimatverzeichnis des Anwenders. Das haben Sie verlassen – und korrekt ist das neue Verzeichnis / im Prompt aufgeführt. Zurück in Ihr Heimatverzeichnis kommen Sie übrigens stets, indem Sie einfach »cd« ohne weitere Parameter eingeben.

In welche Verzeichnisse Sie direkt aus / wechseln können, müssen Sie natürlich nicht erraten. Konsultieren Sie den ls-Befehl (»list«):

So sieht etwa das Hauptverzeichnis eines jungfräulichen SuSE-Servers der Firma Hetzner aus. ls verschweigt Ihnen aber etwas: Dateien, die mit einem Punkt beginnen, zeigt es nur an, wenn Sie die Option -a verwenden:

Jetzt probieren Sie das Ganze doch mal im Ordner dev:

Ihr Bildschirm ist in Sekunden vollgeschrieben – keine Chance, alle Einträge mitzulesen. Doch es gibt Hilfe in Form von »more« oder »less«. »more« ist überraschenderweise simpler gestrickt als »less«, aber trotzdem effektiv:

Jetzt bekommen Sie den Inhalt des Verzeichnisses Zeile für Zeile auf den Bildschirm. Sie können mit den Cursorstasten scrollen oder über die Leertaste seitenweise durch die Bildschirmausgabe springen. Wenn Sie am Ende angelangt sind, drücken Sie einfach (für »quit«).

Bei dieser Gelegenheit haben Sie gleich noch ein weiteres Unix-Konzept kennen gelernt: die so genannten Pipes. Das Zeichen | (finden Sie normalerweise mit auf der Taste) sorgt dafür, dass die Ausgabe des links von ihm stehenden Befehls (hier also »ls«) als Eingabe des rechts davon notierten Kommandos (hier more) verwendet wird. Solche Pipes können Sie auch beliebig verketteten – die more-Ergebnisse könnte man zum Beispiel noch speziell sortieren und formatieren. Außerdem kann Unix Ein- und Ausgaben auch in Dateien umlenken:

In diesem Beispiel schreibt der `ls`-Befehl – dafür steht das `>>` – seine Ergebnisse in die Datei `inhalt.txt` (die »Dateiendung« `txt` ist nur der guten Ordnung halber gewählt, siehe Abschnitt 2.2.2). Anschließend sorgt der Platzhalter `*` dafür, dass `»ls«` nur noch Dateien aufspürt, deren Namen mit `»inh«` beginnen. Das ist zufällig nur `»inhalt.txt«`. Deren Inhalt bringt `»more«` schließlich auf den Bildschirm. Allerdings hätten Sie das `<<` nach `»more«` auch weglassen können, denn der Befehl liest standardmäßig aus der Datei, die ihm als Parameter übergeben wurde. Wenn Sie `>>` durch `>>>` ersetzen, werden die neuen Zeichen an die so verknüpfte Datei nur angehängt.

Das Sternchen `*`, das immer für beliebig viele Zeichen steht, ist beileibe nicht der einzige in Linux verfügbare Platzhalter (auch Wildcard genannt): Das Fragezeichen `?` etwa symbolisiert genau einen fehlenden Buchstaben, in eckigen Klammern können Sie Alternativen angeben: `inhalt[12].txt` steht sowohl für `inhalt1.txt`, als auch für `inhalt2.txt`. Die Alternativen können sogar ganze Bereiche sein: `inhalt[1-5].txt` zum Beispiel meint die Dateien `inhalt1.txt`, `inhalt2.txt` bis `inhalt5.txt`.

Wenn Sie zu einem Befehl mal etwas Genaueres wissen wollen (und im Englischen nicht ganz unbewandert sind), steht Hilfe natürlich auch auf der Kommandozeile bereit. Oft geben die Programme selbst kleine Hilfetexte aus, wenn Sie sie dazu überreden:



Bild 2.4: Hilfetext zum Befehl `»ls«` (Ausschnitt)

Noch beredter ist im Allgemeinen die Online-Hilfe man (`»manual«`), die so genannten man-Pages. Um sie zu konsultieren, verwendet man den gleichnamigen Befehl und setzt als Parameter dahinter das Kommando, über das man mehr erfahren will:

```

NAME

SYNOPSIS
    ls

DESCRIPTION

        --sort

    -a  --all

    -A  --almost-all

        --author

```

Bild 2.5: Man-Pages zum Befehl »ls« (Ausschnitt)

Durch die seitenlangen Erklärungen bewegen Sie sich wie beim `more`-Befehl mit Hilfe der Cursortasten und der Leertaste, `q` beendet das Programm. Während man sich auf das Vorhandensein eines `man`-Eintrags weitgehend verlassen kann, ist das Vorhandensein eines `-help`-Parameters nicht sicher.

Bisher war »ls« gerade im Hinblick auf die Eigenschaften einer Datei recht schweigsam. Erst mit dem Parameter »-l« wird die Darstellung ausführlicher:

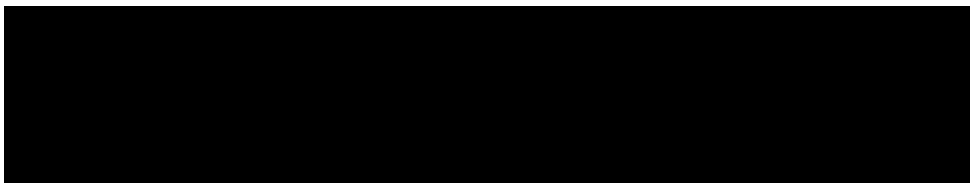


Bild 2.6: Ausführliche Directory-Anzeige

Jede Datei verbraucht nun eine Zeile. Den Anfang jedes Eintrags bilden die Zugriffsrechte – darüber erfahren Sie im übernächsten Abschnitt mehr. Die folgende Zahl gibt an, wie viele Verweise es auf diese Datei gibt. Dann folgen Angaben zum Besitzer und zur Gruppe der Datei (ebenfalls im Kapitel 2.3.3 erläutert). Die nächste Zahl stellt die Dateigröße in Byte dar, gefolgt vom Datum ihrer letzten Änderung.

Natürlich sind Sie nicht darauf beschränkt, sich Schritt für Schritt durch die Ordner zu hangeln. Sie können dem `cd`-Befehl auch direkt den Namen Ihres Zielverzeichnisses übergeben. Dabei gibt es zwei Möglichkeiten:

Zum einen können Sie einen **absoluten** Pfadnamen übergeben. Dieser beschreibt, vom Hauptverzeichnis ausgehend, den kompletten Weg zum Zielordner, etwa so:

Alternativ können Sie einen **relativen** Pfadnamen verwenden. Dieser geht nicht von /, sondern vom aktuellen Ordner aus. Wenn Sie sich beispielsweise gerade in /home befinden (und nur dann!), können Sie mit

in den Unterordner meier/texte/2003 wechseln. Ist hingegen /dev Ihr Ziel, benutzen Sie

Die zwei Punkte .. versetzen Sie eine Verzeichnisebene höher, so dass Sie dev auch tatsächlich erreichen können. Das aktuelle Verzeichnis müssen Sie übrigens nie komplett eintippen: Es wird durch den Punkt (».«) symbolisiert. Wenn Sie zum Beispiel das Programm »programm« aus dem aktuellen Directory starten wollen, funktioniert der Befehl

in der Regel auch dann nicht, wenn »programm« als ausführbar gekennzeichnet ist. Denn »/home« liegt nicht im Suchpfad, und Linux beschränkt sich bei der Suche tatsächlich auf diesen. Geben Sie deshalb das Verzeichnis mit an:

Das entspricht dem Befehl

ist aber deutlich schneller einzutippen.

2.3.2 Linux-Verzeichnisstruktur

Damit Sie bei den folgenden Operationen nicht ziellos durch die Ordner Ihres Servers wandeln, verraten wir im Folgenden, in welchen Verzeichnissen Sie welche Inhalte erwarten dürfen. Denn die meisten Systemen halten sich an einen Standard, den »File System Hierarchy Standard«, der unter www.pathname.com/fhs/ (id20) komplett beschrieben ist.

/

Das Haupt- oder Wurzelverzeichnis, das Sie schon kennen gelernt haben.

/bin

Dieser Ordner enthält wichtige Anwender- und Systemprogramme, etwa die Shells, die Ihre Befehle entgegennehmen, oder die Editoren.

/boot

Hierin finden Sie die zum Systemstart benötigten Dateien. Das sind unter anderem der Kernel (Datei `vmlinuz`) und seine Einstellungen (`vmlinuz.config` – eine Textdatei, die Sie aber nicht direkt ändern sollten).

/dev

Eine der Spezialitäten von Linux: Schnittstellen zur Hardware stellt Ihnen das System in Form von Dateien zur Verfügung, so genannten Gerätedateien. Sie finden hier unter anderem Einträge für all Ihre Festplatten.

/etc

In diesem Ordner stapeln sich vor allem die Konfigurationsfiles, sowohl von Anwendungssoftware als auch des Systems. Sie sind oft an Endungen wie ».ini« oder ».conf« erkennbar.

/home

Nomen est omen: Hier bekommen üblicherweise die Benutzer des Systems ihr Heimatverzeichnis.

/lib

Was in Windows die DLLs sind, stellen unter Linux die Libraries dar – allerdings ohne die typischen DLL-Konflikte. Sie werden in der Regel hier abgelegt und sollten weitgehend sich selbst überlassen bleiben.

/opt

In diesem Verzeichnis sind Programme untergebracht, die nicht unmittelbar zum System gehören – typischerweise KDE, Netscape oder OpenOffice. Diese Anwendungen werden Sie auf Ihrem Server eher selten benötigen.

/proc

Und noch eine Linux-Spezialität: `/proc` ist nicht wirklich ein Verzeichnis, sondern vielmehr ein Interface zum Linux-Kernel. In seinen Unterverzeichnissen finden Sie alle aktuell laufenden Programme, inklusive wichtiger Informationen zu ihrem Zustand, aufgelistet. Außerdem lassen sich hier Daten zum Kernel und zur Hardware abrufen.

/root

Auch der Systemverwalter »root« besitzt ein Heimatverzeichnis.

/sbin

Dieser Ordner ähnelt /bin, allerdings sind die in ihm enthaltenen Tools vor allem für Administratoren gedacht.

/tmp

Der Müllhaufen des Systems: Hier dürfen alle Nutzer und Anwendungen temporäre Dateien speichern. Damit sie sich dabei nicht ins Gehege kommen, ist für /tmp das »Sticky Bit« (siehe spätere Erläuterungen zur Rechtvergabe) gesetzt.

/usr

Dieses Verzeichnis beherbergt den Großteil der auf Ihrem Server eingerichteten Programme.

/var

Wie der Name schon verrät, enthält /var vor allem Dateien, die sich regelmäßig ändern. Dazu gehören zum Beispiel Ordner für das System verlassende E-Mails, noch nicht ausgeführte Druckjobs und die für Fehlersuche und Sicherheitschecks wichtigen Logdateien.

2.3.3 Dateioperationen

Für ein übersichtliches und ordentliches Linux-System kommen Sie ohne die wichtigsten Dateibefehle nicht aus.

Ordner erstellen und löschen

Der Ordner »test« etwa ist mit dem simplen Kommando »mkdir« (make directory) fix erstellt:

```
[REDACTED]
```

Ebenso schnell verschwindet er wieder von der Festplatte:

```
[REDACTED]
```

Der Befehl »rmdir« (remove directory) löscht allerdings nur komplett geleerte Verzeichnisse. Probieren Sie doch mal

```
[REDACTED]
```

das System verweigert die Arbeit (und das ist auch gut so). Wenn Sie ein Verzeichnis inklusive all seiner Elternverzeichnisse löschen wollen, benutzen Sie den Parameter »-p«:

Hätten Sie an dieser Stelle »-p« weggelassen, würde »rmdir« nur den Unterordner test3 löschen, der Ordner test mit dem Unterverzeichnis test2 bliebe aber erhalten. Die Befehlsfolge hätten Sie im Übrigen auch abkürzen können, denn »mkdir« kennt »-p« ebenfalls:

Preisfrage: Wie verhält sich Linux, wenn Sie bei »mkdir« den Schalter »-p« vergessen? Korrekt: Es gibt eine Fehlermeldung aus, weil es versucht, den Ordner test3 in test/test2 anzulegen – test/test2 gibt es aber noch gar nicht.

Dateien löschen

Wenn das zu löschende Verzeichnis noch nicht leer ist, müssen Sie auf »rm« (»remove«) zurückgreifen. Der ist eigentlich für das Entfernen von Dateien vorgesehen. Bevor Sie ihn ausprobieren können, müssen Sie erst einmal eine Spielwiese mit Testdateien schaffen:

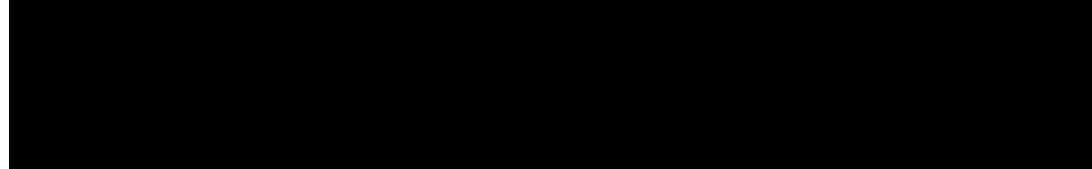
Dann genügt ein

und die Datei verschwindet auf Nimmerwiedersehen. Das heißt – fast: Mit den richtigen Werkzeugen lässt sie sich wiederherstellen. Wollen Sie eine Datei wirklich und endgültig in den Mülleimer befördern, hilft »shred«.

Damit »rm« auch mit Verzeichnissen arbeitet, müssen Sie ihm den Parameter »-r« (recursive) mitgeben. Achtung, Sie arbeiten – wenn Sie noch immer als »root« eingeloggt sind – dann mit einem durchaus gefährlichen Werkzeug: Während »rmdir /lib« überhaupt nichts ändert, könnte ein »rm -r /lib« Ihrem Server den Garaus machen. Probieren Sie es deshalb besser mit einem Testverzeichnis:

Dateien kopieren

Weniger obstruktiv, aber unter Umständen auch noch gefährlich, ist der cp-Befehl (copy). Er dient dazu, Dateien zu kopieren (gut), überschreibt vorhandene Files gleichen Namens aber (ohne zusätzliche Parameter) rücksichtslos (schlecht):



Im mit »ls -l« aufgerufenen ausführlichen Directorylisting sehen Sie, dass die Dateien t.txt und u.txt unterschiedlich groß sind. Jetzt geht »cp« ans Werk:



Tatsächlich, u.txt ist jetzt mit t.txt identisch. Solche Ärgernisse passieren Ihnen nicht, wenn Sie »cp« mit dem Parameter »-i« aufrufen – Linux fragt dann ausdrücklich nach, ob es eine schon vorhandene Datei überschreiben darf.

Übergeben Sie »cp« statt des Zieldateinamens ein Verzeichnis, versucht das Programm, die Quelldatei dorthin zu kopieren. In jedem Fall ist »cp« so flexibel, dass es mit den vorn schon beschriebenen Platzhaltern umgehen kann. Zudem können Sie auch die Namen der Spezialverzeichnisse verwenden. Der Befehl



kopiert zum Beispiel alle auf ».conf« endenden Dateien aus /etc ins aktuelle (».«) Verzeichnis – wie der Linux-Prompt verrät also /test.

Soft-Links

Doch müssen Sie die Dateien wirklich kopieren? Zwei identische Dateien auf der Festplatte, das macht unter Linux höchstens für Backup-Zwecke Sinn. Wenn Sie lediglich wollen, dass ein File auch in einem anderen Verzeichnis für Sie erreichbar ist, dann legen Sie lieber einen Link an.

Linux kennt sogar gleich zwei Sorten von Links. Die erste, auch »soft link« oder »symbolic link« genannt, ist im Prinzip eine Datei, die nichts weiter als einen Pfad zu einer anderen Datei enthält. Einen solchen Link legen Sie so an:



Statt zum Beispiel test.txt von /etc nach /bin zu kopieren, könnten Sie diesen Befehl verwenden:



Von der unteren Zeile haben wir der Verdeutlichung halber einen Teil weggelassen – Sie sehen, dass der symbolische Link auf die Originaldatei verweist. Die Soft-Links ähneln

insofern den von Windows bekannten Links (oder Verknüpfungen), als sie nichts davon bemerken, wenn das Ziel des Verweises gelöscht oder verschoben werden sollte. Das liegt daran, dass die Shell erst dann versucht, den Link aufzulösen, wenn Sie das Verzeichnis öffnen, in dem er sich befindet. Immerhin wird der ungültige Soft-Link dann (zumindest von der Bash) rot gefärbt dargestellt. Dazu passt, dass Sie Soft-Links auch zu Dateien erstellen können, die gar nicht vorhanden sind.

Hard-Links

Sie ahnen es sicher schon: Wenn es weiche Links gibt, muss Linux auch harte Vertreter dieser Art kennen. Das Prinzip der so genannten »hard links« besteht darin, der zu verlinkenden Datei im Dateisystem einfach einen zweiten Namen zuzuordnen. Beide Namen sprechen aber ein und dieselbe Datei an. Original und Kopie zu unterscheiden, ist nicht möglich. Anlegen können Sie Hard-Links wie ihre weichen Vettern mit dem `ln`-Befehl, allerdings ohne den »-s«-Parameter:

Um zur Datei `/etc/test.txt` einen Link in `/bin` anzulegen, verwenden Sie also:

Wenn Sie nun nachsehen, was sich in `/etc` getan hat, sehen Sie (in `/bin` erhalten Sie ein identisches Ergebnis!):

Hier kommt es auf die »2« an – das ist der so genannte Link-Counter. Er verrät, unter wie vielen unterschiedlichen Namen Sie dieselbe Datei ansprechen können. Wenn Sie `test.txt` in `/bin` nun löschen

und sich erneut `/etc` ansehen, hat der Link-Counter um 1 heruntergezählt:

Natürlich hätten Sie `test.txt` auch in `/etc` löschen können – danach wäre die Datei noch immer in `/bin` zu finden gewesen.

Dateien verschieben

Gleich doppelt nützlich ist der Befehl »mv« (»move«): Damit können Sie Dateien oder Verzeichnisse entweder umbenennen oder auch verschieben. Testen wir zunächst das Umbenennen:

macht aus der Datei t.txt die Datei test.txt. Achtung: So wie »cp«, überschreibt auch »mv« vorhandene Dateien gleichen Namens gnadenlos. Und wie bei »cp«, können Sie dies durch den Parameter »-i« verhindern. Ähnlich reibungslos funktioniert das Verschieben:

Sie haben eben die Datei test.txt in den (vorher im Hauptverzeichnis angelegten) Ordner test2 verschoben.

2.3.4 Suchen und Finden

Da Sie im Textmodus nicht wirklich mit einem rechten Mausklick auf Dateisuche gehen können, gehören die »Such&Find«-Kommandos zu den wichtigsten Werkzeugen. Tatsächlich bieten sie äußerst mächtige Funktionen, die weit über ein Auflisten der Fundstellen hinausgehen.

Locate

Doch zunächst zu den einfacheren Optionen – beginnend mit dem locate-Befehl. Probieren Sie es mit

Sie erhalten eine sehr lange Liste mit Dateinamen, in denen (inklusive Pfad) irgendwo das Wörtchen »test« auftaucht. Wenn es Sie interessiert, wie viele das sind, können Sie gleich Ihre Kenntnisse über Pipes (siehe Kapitel 2.3.1) testen. Denn Linux kennt das nützliche Programmchen »wc«. Die Abkürzung steht für »wordcount«: wc zählt Zeichen, Wörter und Zeilen. Darum übergeben Sie ihm einfach das, was »locate« aufgespürt hat:

Das Ergebnis sind zwei Zahlen, die nacheinander die Menge der enthaltenen Zeilen, Wörter und Zeichen angeben. Doch vielleicht wollten Sie ja gar nicht 3000 und mehr Dateien aufspüren, sondern nur eine: Dann müssen Sie den Suchstring mit den schon oben erwähnten Platzhaltern enger fassen. Mit

(beachten Sie die einfachen Hochkommas) können Sie die Zahl der angezeigten Dateien schon deutlich reduzieren. In diesem Beispiel listet Linux nur noch Files auf, die auf »test« enden. Ebenso wirksam sind ? (steht für ein Zeichen) und [] (markiert Alternativen). Mit dem Parameter »-i« weisen Sie »locate« an, Groß- und Kleinschreibung nicht zu beachten.

Find

Wesentlich mehr können Sie bei »locate« auch nicht einstellen – da ist sein Konkurrent »find« schon raffinierter. Wenn Sie damit bloß nach vorgegebenen Dateinamen suchen,

ist es definitiv unterfordert, außerdem ist für diesen simplen Zweck »locate« schneller einsetzbar. Vergleichen Sie selbst: Der folgende Befehl findet dieselben Ergebnisse wie das locate-Beispiel im vorigen Absatz.

Was das find-Kommando so wertvoll macht, sind zum einen seine mächtigen Suchparameter. In diesem Beispiel haben wir schon »-path« verwendet, das zur Suche in kompletten Pfadnamen auffordert. Interessieren Sie nur die eigentlichen Dateinamen, verwenden Sie »-name«:

Der Slash / gleich nach dem Befehl gibt »find« das Verzeichnis vor, bei dem es mit der Wühlarbeit starten soll – in diesem Fall das Hauptverzeichnis. Wenn Sie diese Angabe weglassen, beschränkt sich das Programm auf das aktuelle Arbeitsverzeichnis. Mit »-maxdepth« und »-mindepth« können Sie »find« veranlassen, nur bis zu einer bestimmten Verzeichnistiefe (maxdepth) oder ab einer bestimmten Verzeichnistiefe zu suchen. Mit dem String

durchforsten Sie zum Beispiel nur die zweite bis vierte Ebene. Sehr umfangreich sind auch die Möglichkeiten, die Suche zeitlich einzuschränken:

In diesem Beispiel beschränkt sich »find« durch den »mtime«-Parameter auf Dateien, die höchstens drei Tage alt sind. Das Minus vor der 3 steht für »heute minus drei Tage«.

Grep

Ein drittes sehr nützliches Suchprogramm ist »grep«. Es dient dazu (unter anderem), die Ausgabe anderer, beliebiger Befehle nach bestimmten Kriterien zu durchwühlen. So lässt sich zum Beispiel eine lange Dateiliste auf die wirklich interessanten Files reduzieren. Zwar haben viele Linux-Kommandos selbst die Fähigkeit, ihre Ausgabe zu beschränken – grep hat aber den Vorteil, dass Sie nur die Suchparameter dieses einen Programms kennen lernen müssen. Und die sind zudem so mächtig, dass sie die Möglichkeiten anderer Programme oft in den Schatten stellen.

Grundsätzlich benötigt grep ein Suchmuster. Optional können Sie diesem – welche Überraschung – Optionen voranstellen. Danach können Dateinamen (oder auch Verzeichnisse) folgen, mit denen grep arbeiten soll. Wenn kein Dateiname erwähnt ist, liest das Programm aus der Standardeingabe – so kann ihm auch das Ergebnis anderer Befehle per Pipe (|) übermittelt werden. Ein paar praktische Beispiele:

Dieser Befehl sucht in allen txt-Dateien im aktuellen Verzeichnis nach »test«.

Damit wird rekursiv der Inhalt des kompletten /dev-Verzeichnisbaums nach »test« abgesehen. Wenn Ihnen der Vorgang zu lange dauert, brechen Sie ihn einfach mit `[Strg]-C` ab.

Jetzt geht's schon schneller: `grep` ignoriert (-I) nun Binärfiles (also Programme und Ähnliches).

Diesmal dauert es wieder etwas länger: Das Programm gibt nur Dateien aus, die die Suchbedingung nicht erfüllen (»-L«).

Wenn Sie nur die Anzahl der entsprechenden Dateien erfahren wollen, hilft der Parameter »-c«.

Mit »-i« haben Sie `grep` dazu aufgefordert, Groß- und Kleinschreibung zu ignorieren.

`Grep` besitzt zahlreiche weitere Optionen, über die Sie bei Bedarf »man `grep`« aufklärt. Ein ganz besonderes Kapitel darin sind auch die Suchmuster – mit simplen Suchwörtern ist `grep` nämlich geradezu unterfordert. Das Stichwort heißt »reguläre Ausdrücke«, eine Beinahe-Wissenschaft, die sich nur durch regelmäßigen Gebrauch erschließt. Wenn Sie sich damit auseinandersetzen, hat das aber einen Vorteil: die »regexpressions« sind auch anderswo beliebt, etwa in den Skriptsprachen Perl und PHP, die Sie zur Erstellung dynamischer Websites benötigen.

2.3.5 Benutzer und Gruppen

Wir hatten die Benutzer- und Rechteverwaltung schon als einen der Vorzüge von Linux hervorgehoben. Es bleibt nicht aus, dass sie auch den Verwaltungsaufwand etwas erhöht. Denn jede Datei und jedes Verzeichnis kennt zunächst mal drei verschiedene Sorten von Nutzern, nämlich ihren Eigentümer, die Gruppe, der sie zugeordnet ist, sowie den Rest der Welt. Den verschiedenen Nutzern lassen sich abgestuft bestimmte Rechte erteilen: eine Datei zu lesen (»read«, Abkürzung `r`), sie zu verändern (»write«, Abkürzung `w`) und sie auszuführen (»execute«, Abkürzung `x`). Wenn Sie die Eigenschaften einer Datei mit »`ls -l`« anzeigen lassen, verrät Ihnen der Textstring am linken Rand alles über die Benutzerrechte. Probieren Sie's aus:



Bild 2.7: Zugriffsrechte (linke Spalte)

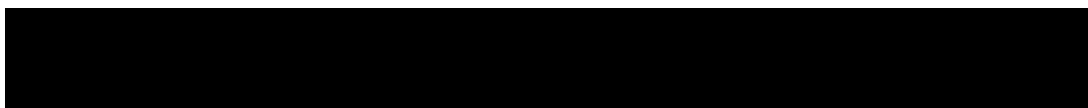
Der erste Buchstabe verrät, um welche Art von Eintrag es sich handelt. Das »d« steht dabei für ein Verzeichnis, der Bindestrich für eine normale Datei. Das »l« symbolisiert einen Verweis (»link«) – die betreffende Datei liegt in Wirklichkeit in einem anderen Ordner, kann aber auch vom aktuellen Verzeichnis aus angesprochen werden.

Anschließend folgen drei Dreiergruppen, die nacheinander für die Rechte der Eigentümer, der Gruppe und der sonstigen Nutzer stehen. In jeder Dreiergruppe sind Lese-, Schreib- und Ausführbarkeits-Recht hintereinander angegeben. Ist die Berechtigung erteilt, steht an dieser Stelle der entsprechende Buchstabe. Fehlt sie, findet sich nur ein »-«.

Ein Beispiel: Die Datei »arch« oben im Bild darf von ihrem Besitzer (root) gelesen (r), geschrieben (w) und ausgeführt (x) werden. Ihre Gruppe (ebenfalls root) darf sie nur lesen (r) und ausführen (x), aber nicht ändern (-). Die anderen Nutzer haben dieselben Rechte wie die Gruppe. Es ergibt sich also der Rechtecode `rwxr-xr-x`.

Manchmal ist, wenn es um die Rechtevergabe geht, auch von Zahlen wie »666« die Rede. Dabei handelt es sich nur um eine andere Erscheinungsform desselben Phänomens. Die Benutzerrechte lassen sich nämlich auch binär – mit Einsen und Nullen – ausdrücken. »r«, »w« und »x« ersetzen wir dabei durch Einsen, die »-« durch Nullen. Aus `rwx r-x r-x` werden so die drei Zahlen 111, 101 und 101 – also im Dezimalsystem 7, 5 und 5 – kurz: 755. Anders herum wird aus der drohenden 666 zunächst 110 110 110 und mit Buchstaben `rw- rw- rw-`. Eine solche Datei dürfen also alle Nutzer lesen und ändern, aber nicht ausführen. Das eben Gesagte gilt komplett auch für Verzeichnisse – mit der klitzekleinen Änderung, die die Bedeutung von »Ausführen« betrifft: Hat ein Nutzer das »x«-Recht für ein Verzeichnis, darf er in dieses wechseln.

Wenn Sie ein Verzeichnis erstellen, können zunächst nur Sie als Eigentümer darauf schreibend zugreifen – alle anderen Nutzer können es aber lesen und zum Arbeitsverzeichnis machen. Bei einer von Ihnen erzeugten Datei haben Sie alle Rechte, andere Anwender dürfen sie nur lesen. Mit dem Befehl »chmod« können Sie alle Zugriffsrechte anpassen:



Sie erstellen eine Datei `bsp.txt` und zeigen danach ihre Eigenschaften an. In der unteren Zeile vorn finden Sie die Zugriffsrechte: Nur Sie als Eigentümer dürfen auch schreiben (»rw-«).

Jetzt folgt das chmod-Kommando:

Damit haben nun alle am Server angemeldeten Nutzer Schreibrechte für die Datei. Wem Sie was erlauben, regeln Sie über den Parameter nach »chmod«. Dieses Wort beginnt mit bis zu drei Zeichen, die festlegen, wessen Fähigkeiten Sie modifizieren wollen. Das »u« steht dabei für den Besitzer (user), das »g« für die Gruppe und das »o« für die anderen Nutzer (others). Die Buchstaben lassen sich auch kombinieren, etwa zu »go« (group und others) wie im Beispiel oben. Der Maximalfall tritt bei »ugo« ein – er lässt sich auch mit »a« (all) abkürzen.

Nach der »Wer«-Frage teilen Sie »chmod« die Art der Operation mit, die es durchführen soll. »Chmod« kann Rechte hinzufügen (»+«), wegnehmen (»-«) oder definieren (»=«). Im Beispiel oben soll also ein Recht hinzugefügt werden.

Zum Abschluss müssen Sie noch verraten, um welche Rechte es Ihnen überhaupt geht: ums Lesen (»r«), Schreiben (»w«) oder Ausführen (»x«). Auch hier können Sie die Zeichen wieder kombinieren, zum Beispiel zu »rw« oder »rwx« (Letzteres lässt sich nicht abkürzen). Im oben genannten Exempel würde also für die Gruppe (»g«) und die anderen Nutzer (»o«) das Schreibrecht (»w«) hinzugefügt (»+«). Dabei ist es unerheblich, ob der w-Schalter eventuell schon gesetzt ist. Außer »r«, »w« und »x« taucht auch noch ab und zu das Recht »t« auf: Das so genannte Sticky Bit sorgt dafür – wenn es für ein Verzeichnis gesetzt ist – dass Nutzer in diesem Ordner nur Dateien ändern können, die sie selbst angelegt haben.

Ein Spezialfall ist die »=«-Operation: Sie bewirkt, dass die nach ihr genannten Rechte hinzugefügt, alle anderen aber gelöscht werden. Zur Veranschaulichung noch zwei Beispiele:

Allen Nutzern (»a«) wird das Ausführungsrecht (»x«) für bsp.txt entzogen. Dabei ist irrelevant, ob sie es je besaßen.

Der Gruppe (»g«) und den anderen Nutzern (»o«) wird für bsp.txt das Leserecht (»r«) erteilt, alle anderen Rechte werden für diese User gelöscht.

Übrigens können Sie die zu vergebenden Rechte auch schon dem mkdir-Befehl mitteilen – der Option »-m« stellen Sie dasselbe Konstrukt nach wie dem chmod-Befehl. So erzeugen Sie zum Beispiel einen neuen Ordner, den alle Nutzer außer Ihnen lesen und schreiben können, in den aber niemand außer Ihnen wechseln darf:

Mit welchen Rechten neue Dateien standardmäßig ausgestattet werden, ist in Linux nicht ein für alle Mal festgelegt. Stattdessen wird ständig die so genannte Maske (»umask«) als Schablone herangezogen. Sie legt fest, welche Werte von den Standard-

werten abgezogen werden müssen, um die tatsächlichen Zugriffsrechte zu ermitteln. Mit dem Befehl

können Sie sich die aktuelle Einstellung anzeigen lassen. Wir hatten oben schon erklärt, wie sich diese Binärzahl in einen Zeichenstring umwandeln lässt: 022 ergibt --- -w- -w-: Es wird vom Standardwert rw- rw- rw- also jeweils für Gruppe und andere Nutzer das »w« abgezogen.

Wichtig: Sonderrechte nur, wenn nötig

Wenn Sie an Ihrem Mietserver arbeiten, sollten Sie sich stets als normaler Nutzer ohne weitere Privilegien anmelden. Wie Sie einen solchen Account anlegen, erfahren Sie im Abschnitt »Benutzerverwaltung«. Stellt sich eine Aufgabe, die Superuser-Privilegien erfordert, benutzen Sie den Befehl »su« (»super user«):

Das Programm startet eine neue Shell, in der Sie alle Genehmigungen des Superusers besitzen.

2.3.6 Linux- und DOS-Befehle im Vergleich

Alle, die sich noch gut an alte DOS-Zeiten erinnern können, finden vielleicht die folgende Tabelle nützlich, in der die wichtigsten Befehle noch einmal mit ihrem DOS-Äquivalent aufgeführt sind.

chmod	Dateiattribute und -rechte ändern	attrib
cd	Verzeichnis wechseln	cd
pwd	Aktuelle Position zeigen	cd
cp	Dateien kopieren	copy
date	Zeit und Datum ändern	date / time
rm	Dateien löschen	del
rm -r	Verzeichnisbaum löschen	deltree
ls	Verzeichnisinhalt anzeigen	dir
df	Verwendeten Speicher anzeigen	dir
echo	Text ausgeben	echo
diff	Dateien vergleichen	fc
grep	Dateien durchsuchen	find
mkdir	Verzeichnis erstellen	md
more, less	Inhalt einer Datei zeigen	more
mv	Datei oder Verzeichnis verschieben / umbenennen	move / rename

rmdir	Verzeichnis löschen	rd
sort	Datei oder Verzeichnis sortieren	sort
cat	Inhalt einer Datei zeigen	type
cp -a	Mehrere Dateien oder Verzeichnisse kopieren	xcopy

2.3.7 Hilfe und Dokumentation

Auf ein sehr nützliches Linux-Programmchen haben wir schon hingewiesen: Auf man nämlich, das die Handbuch-Einträge zu vielen Befehlen und Programmen ausgibt. Wussten Sie schon, dass Sie im Inhalt der man-Seite auch suchen können? Mit /Suchwort fahnden Sie vorwärts, mit ?Suchwort hingegen rückwärts.

man und Kollegen

Auch noch nicht erwähnt haben wir, dass man-Files aus so genannten Sektionen bestehen. Der Sinn dahinter: So lässt sich dasselbe Stichwort je nach Zusammenhang unterscheidlich darstellen. Was einen Administrator interessiert, ist zum Beispiel für den simplen Anwender schon zu viel des Guten. Sektion 1 behandelt denn auch Programme, die von der Kommandozeile aufrufbar sind. Sektion 2 kümmert sich um Kernelroutinen, Nr. 3 um die C-Systembibliotheken. In Sektion 4 erfahren Sie alles über die »special files«, die oft die angeschlossene Hardware (in /dev) repräsentieren. In Sektion 5 geht es um Datenformate und Konfigurationsdateien, 6 befasst sich mit Spielen, 7 enthält alle den anderen Sektionen nicht zuzuordnenden Themen und Sektion 8 schließlich erklärt Interna für Systemadministratoren. In den man-Pages selbst sind bei Verweisen auf andere man-Einträge die betreffenden Sektionen in Klammern angegeben. Die gewünschte Sektion setzen Sie gleich als ersten Parameter ein:

Dadurch wird Ihnen der normale Umgang mit man erklärt. Wenn Sie aber Sektion 7 wählen

erfahren Sie, wie Sie eigene man-Pages erstellen. Sehr nützlich in diesem Zusammenhang ist der Befehl »whatis«. Damit können Sie sich nämlich eine Kurzbeschreibung der man-Einträge ausgeben lassen – und zwar aller verfügbaren Sektionen:

Noch ein nützliches Kommando zum Umgang mit man-Dateien: »apropos« durchsucht die Kurzbeschreibungen aller man-Einträge nach einem bestimmten Stichwort. So liefert

eine lange Liste mit Kommandos, in deren Beschreibung das Wörtchen »man« vorkommt. Wenn Sie nun wissen wollen, wo ein Programm, sein Quellcode und seine Beschreibung physisch residieren, können Sie »whereis« befragen:



Das Programm gibt Ihnen nacheinander die betreffenden Dateipfade aus.

Einen Minibefehl wollen wir noch nachreichen: Wenn Sie sich mal wundern sollten, warum Sie zwar »cd« ausführen können, dieses Programm aber nirgends finden, dann klärt Sie »type« auf:

Oder für »ls«:

Info

Ein weiterer wichtiger Teil der Linux-Dokumentation steckt in so genannten »info«-Files, die der gleichnamige Befehl auf den Bildschirm bringt. Infoseiten enthalten vor allem Details zu Kommando- und Befehlsaufrufen. Wenn Sie den Befehl ohne Parameter aufrufen

erscheint ein Inhaltsverzeichnis aller Infotexte. Falls Sie nur eine Fehlermeldung erhalten, müssen Sie »info« erst noch nachinstallieren (»yast -i texinfo« oder »apt-get install texinfo«). Infoseiten funktionieren so ähnlich wie Webseiten: Mit  und  bewegen Sie sich durch die Hyperlinks, mit »p« (previous) und »n« (next) durch die Kapitel. Mit »d« (directory) kommen Sie wieder zum Inhaltsverzeichnis. »info info« führt Sie noch ausführlicher in die Geheimnisse von »info« ein.

Beschreibungen, How-Tos und FAQs

Wenn Sie ein neues Programmpaket installieren, stecken in der Regel auch ein paar »So geht's«-Dateien im Archiv. README informiert Sie ganz allgemein über die Anwendung und weist meist auch auf andere lesenswerte Files hin. INSTALL erklärt, wie Sie

das Programm kompilieren und installieren. Zudem gibt es zu sehr vielen Anwendungen so genannte »How-tos«, die mehr oder weniger detailliert vorführen, wie Sie eine bestimmte Aufgabe erledigen. Solche How-tos sammelt zum Beispiel das Linux Documentation Project (www.tldp.org (id21)). Und dann gibt es da noch die FAQs: die beliebten Listen häufig gestellter Fragen. Bevor Sie selbst in einem Online-Forum eine Frage stellen, ist es quasi obligatorisch, sich zuerst die entsprechende FAQ zu Gemüte zu führen. Zu finden sein könnte diese zum Beispiel im FAQ-Archiv unter www.faqs.org (id22). Abschließend noch ein paar Hinweise auf deutschsprachige Linux-Anleitungen: Die »Linux-Fibel« (<http://fibel.org/linux/> (id23)) gibt eine gute Einführung. »SelfLinux« (<http://www.selflinux.org> (id24)) ist eine nach dem Vorbild von »SelfHTML« entstandene (und immer noch in Gemeinschaftsarbeit entstehende) Linux-Referenz und -Schulung. Das Linux-Wiki (www.linuxwiki.de (id25)) ist eine von den Anwendern zusammengestellte Datenbank mit nützlichen Erklärungen, Tipps und Tricks.

2.4 Programme, Prozesse und Dämonen

2.4.1 Allgemeines über Prozesse

Was ein Programm ist, scheint auf den ersten Blick klar: Word ist ein Programm ebenso wie Excel oder Solitaire. Allgemeiner gesehen, ist ein Programm einfach eine Folge von maschinenverständlichen Anweisungen, eine Art Rezept also, das von der CPU des Computers abgearbeitet wird. Eine Maschine, die immer nur ein einziges Programm auf einmal ausführt, muss auch nichts weiter beachten.

Anders ist es, wenn auf einem Computer verschiedene Benutzer unterschiedliche (oder auch identische) Programme in beliebiger Abfolge starten dürfen. Das System muss ständig den Überblick behalten, für welchen Nutzer gerade welches Programm läuft, in welchem Programmschritt es sich befindet und wo es im Hauptspeicher abgelegt ist. Die Zusammenfassung dieser Merkmale heißt unter Linux »Prozess«. Innerhalb eines Prozesses verwaltet das Betriebssystem also den aktuellen Zustand eines Programms mit allen nötigen Informationen.

Linux ist – als Multi-Tasking-System – in der Lage, mehrere Prozesse quasi gleichzeitig zu bearbeiten. »Quasi gleichzeitig« heißt, dass tatsächlich immer nur eine Anweisung ausgeführt wird. Allerdings wird den Einzelschritten eines Prozesses zyklisch Arbeitszeit zugeteilt. Das hat zum Beispiel den Vorteil, dass in einzelnen Programmen nötige Wartezeiten effizient von den anderen Programmen genutzt werden können. Außerdem ist der Vorgang für den Anwender transparent – die Umschaltung zwischen den Prozessen erfolgt meist in so kurzen Abständen, dass alle gleichzeitig aktiv erscheinen.

Die ersten Prozesse startet Linux schon beim Systemstart. Die Shell, unter der Sie zuvor Dateisystembefehle getestet haben, ist zum Beispiel ein solcher Prozess. Um die einzelnen Prozesse voneinander unterscheiden zu können, nummeriert Linux sie fortlaufend – der »Name« eines Prozesses ist damit die Prozessnummer oder PID (»process identification«).

3 Die größten Anbieter

Zum Redaktionsschluss dieses Buches buhlten die unterschiedlichsten Anbieter um die Gunst der Servereinsteiger. Dieses Kapitel zählt zunächst deren Gemeinsamkeiten und Unterschiede auf, um Sie dann in konkreten, auf die Anbieter angepassten Schritten zum Erfolg zu führen. Dabei gehen wir vom schwierigsten Fall aus – auch Kunden anderer, möglicherweise neuere Anbieter kommen deshalb in dieser Anleitung zum Zuge.

Ein eigener Server im Internet ist eine gute Sache – vorausgesetzt Sie haben sich vorher alles reiflich überlegt. Derzeit gibt es fünf große Anbieter von dedizierten Servern im Einsteigerbereich: 1&1, IPX-Server, Hetzner, BSB »Server4free«, Domainbox und – ganz neu – Strato.

Als Einstiegspreis haben sich 29 Euro pro Monat für die günstigste Variante durchgesetzt, doch es gibt erhebliche Leitungsunterschiede.

Bevor wir nun in den folgenden Kapiteln die Unterschiede herausarbeiten, sollten Sie sich ein paar grundsätzliche Fragen stellen. Ein beliebter Irrtum besteht darin zu glauben, dass ein Internetserver so läuft, wie er geliefert wird. Zeit für Administration plant kaum jemand ein. Das ist grundlegend falsch. Wer keine Zeit hat, sich tageweise mit Linux, Confixx, Apache & Co. herumzuschlagen, lässt besser die Finger von der Sache. Ein Server ist nie fertig, es gibt immer etwas zu tun.

Egal, ob es neue Sicherheits-Updates sind, Programme angepasst werden müssen, neue Programmversionen erschienen sind oder irgendein böser Zeitgenosse versucht, in den Rechner einzubrechen: Falsche Handhabung oder unterlassene Pflege kann nicht nur sehr teuer werden, sondern unter Umständen sogar strafbar sein. Falls Sie wenig Zeit mitbringen, sollten Sie besser zu einem »Managed Server« greifen, bei dem erfahrene Administratoren die Serverwartung übernehmen. Sie haben dann zwar etwas weniger Möglichkeiten, schlafen aber wesentlich ruhiger.

Ein eigener Server ist vor allem dann wirklich interessant, wenn Sie Leistungen oder Dienste benötigen, die Sie auf einer normalen Web-Präsenz nicht erhalten (zum Beispiel Chat-Funktionen, Game-Server oder Streaming Media). Haben Sie keine besonderen Wünsche, dann vergessen Sie einen eigenen Server besser. Der Aufwand, den Sie treiben müssen, lohnt die Arbeit nicht.

Auch wenn Sie sehr wenig Erfahrung mit Linux haben, sollten Sie erst einmal zu Hause auf einem kleinen Bastelsystem üben. Für blutige Einsteiger empfiehlt sich SuSE, für den etwas erfahreneren Anwender ist Debian/GNU-Linux eine gute Wahl.

Wichtig ist, viel zu lesen. Gerade was Linux-Know-how angeht. Sind Sie bereit, sich um Datensicherheit zu kümmern? Kein Rootserver besitzt gespiegelte Festplatten. Verabschiedet sich eine Festplatte ins Datennirwana, was einigen Anwendern schon passiert ist, sind alle Daten verloren. Wer sicherer gehen will, sollte daher entweder regelmäßige

Sicherungskopien anlegen oder einen zweiten Server besitzen, auf den täglich alle Daten kopiert werden.

3.1 Die Anbieter

Ihre Entscheidung ist gefallen, niemand kann Sie abhalten? Herzlich willkommen im Club der Administratoren – jetzt muss nur noch der passende Server her. Wozu Sie greifen, hängt nicht zuletzt von Ihren Einsatzwünschen ab.

3.1.1 1&1 – Rootserver

Neben Windows- und Managed Servern hat 1&1 drei Linux-Grundkonfigurationen im Programm: L, XL und XXL. Die Varianten unterscheiden sich in der Hardwareausstattung – primär Prozessor, Speicher und Festplatte. Datensicherheit in Form von gespiegelten Festplatten gibt es im Low-Budget-Segment noch nicht.

Über Sinn und Unsinn von schnellen Prozessoren bei Internetservern, die nur eine 100-MBit-Anbindung besitzen, lässt sich diskutieren. Um eine reguläre Netzwerkkarte auszureizen, genügt sicher schon ein 800-Megahertz-Computer. Auf CPU-Leitung zu sehen lohnt also nur bei aufwändigen dynamischen Angeboten, bei denen im Hintergrund viel gerechnet werden muss.

Auch der erlaubte Traffic unterscheidet sich erheblich. Deshalb sollten Sie vorher unbedingt möglichst exakt abschätzen, wie viele Daten Ihr Server übertragen soll. Besonders bei Filesharing, Kommunikationsplattformen und Tauschbörsen werden die Grenzen schnell erreicht. Dagegen werden Server, die nur Webseiten anbieten, die Minimalgrenze von 75 Gigabyte pro Monat sicher nicht überschreiten. Ist es wahrscheinlich, dass Sie die maximal erlaubte Transfermenge nicht einhalten können, sollten Sie sich andere Anbieter ansehen. Denn bei 1&1 kommt Sie das sehr teuer: zwischen 5 und 15 Euro pro Gigabyte.

Etwas Zeit müssen Sie bei der Bestellung eines Rootservers bei 1&1 schon mitbringen. Je nach Bestellzeitpunkt und Auftragslage kann es ein paar Wochen dauern, bis der Server bereitgestellt wird.

The screenshot displays the 1&1 website's server configuration page. The main content area is titled 'Root Server - maximale Freiheit für Linux-Profis'. It lists several features:

- Erhältlich in drei Hardware-Leistungsklassen ab 16 GB / 20 TB Server
- Conflix 2.0 Professional Vollversion, kostenlos inklusive (vorinstalliert)
- Linux 9.3 Betriebssystem
- Leistungstauglicher Server mit vollem Root-Zugriff und lokalem Mail-Server
- Ideal für Gameserver geeignet

Below this list, three server configurations are shown with their respective prices:

- 16 GB / 20 TB: 149,-
- 16 GB / 20 TB: 99,-
- 16 GB / 20 TB: 49,-

A note at the bottom of the main panel states: 'Einmalige Einrichtungsgebühr für 4900 EUR'. To the right, a sidebar highlights a discount: 'Einrichtungsgebühr: Dreifach gesenkt, Sie zahlen hier nicht 49,- EUR, sondern 99,- EUR!'.

Bild 3.1: Drei Grundkonfigurationen bei 1&1. Zu wenig Speicher rächt sich später

3.1.2 IPX-Server

Neu im Einsteigerbereich ist IPX-Server. Bisher setzte der Anbieter ausschließlich auf teure Systeme, hohe Verfügbarkeit und Reputation, aber das Geschäft mit den Einsteigern will die IP Partner AG nicht der Konkurrenz überlassen. Der Nürnberger Anbieter überlässt dem Kunden die Qual der Wahl. Fest definierte Systeme gibt es nicht. Jeder kann sich den Server so zusammenstellen, wie er es gerne hätte.

Etwas verwirrend ist allerdings, dass Sie gleich zwei Verträge mit dem Unternehmen abschließen müssen: einen über die gemietete Hardware, einen über den Stellplatz (inklusive Traffic). Das erschwert die Kostenrechnung, denn sowohl monatliche Kosten als auch Einrichtungsgebühren fallen für beide Verträge an.

AMD Athlon XP 2000+, satte 512 MByte Arbeitsspeicher und 80 GByte Traffic zu bieten.

Sie kümmern sich nur um die Software. Wir bieten Ihnen die aktuelle und aushändler abgestimmte Hardware mit vorinstalliertem Betriebssystem. Sie verfügen über **vollen Rootzugriff**. Typischerweise installieren wir ein Minimalsystem mit SSH-Zugriff. Danach können Sie von unseren zentralen Distributionsservern die von Ihnen benötigten Softwarepakete nachinstallieren. Besonders einfach kann dies z. B. bei Suse über Yast2 erfolgen. Der Zugriff auf die Distributions-CDs erfolgt im lokalen Netzwerk. Das ermöglicht schnellen Zugriff und generiert keinen Traffic, der von Ihnen bezahlt werden muss.

Bestellung nur in Unterteilung möglich.

	30€	79€	69€	149€	139€	149€
Grundpreis	30€	79€	69€	149€	139€	149€
Server unsere aktuel. Hardwarekonfiguration	AMD Athlon XP 2000+ 512 MB RAM 40 GB schnelle HDD	AMD Athlon XP 2200+ 512 MB RAM 80 GB schnelle HDD	AMD Athlon XP 2200+ 512 MB RAM 80 GB schnelle HDD	Motherboard: MCH74 Ultra AMD Athlon XP 2600+ 1 GB DDR-RAM 80 GB schnelle HDD		
Vorinstalliertes Betriebssystem	SUSE 8.1 Standard inkl. LAMP und Webmin oder Debian 3.0	SUSE oder Redhat Linux Version + Partitionierung nach Absprache	SUSE oder Redhat Linux Version + Partitionierung nach Absprache	SUSE oder Redhat Linux Version + Partitionierung nach Absprache		
Traffic	80 GB	100 GB	100 GB	150 GB		

Bild 3.3: Hetzner bietet viel Freiheit für erfahrene Admins

Viel Freiheit: Besonders positiv ist, dass Hetzner seine Kunden nicht mit langen Vertragslaufzeiten an sich bindet. Beschließt ein Kunde zu wechseln, so ist das jederzeit zum Monatsende möglich. Ein weiterer Pluspunkt: Wer sich den Server »zerschießt«, kann zum Nulltarif eine Neuinstallation bekommen. USV, Rebootservice und Server-Monitoring kosten bei allen Paketen extra.

3.1.4 BSB Server4Free

Ende 2001 schlug die Stunde der günstigen Einstiegsserver: Die Intergenia AG (PlusServer, Server4free und Onlinekosten.de) eröffnete mit damals sensationellen 49 Euro pro Monat den Preiskrieg. Das genügte für einen 800-Megahertz-Computer, 256 Megabyte Speicher und eine dauerhafte Internetanbindung. Dass die häufig Leistungsengpässen oder gar Totalausfällen zum Opfer fiel, war allen Admins bei dem Preis völlig logisch. Heute wirken die 6 GByte Traffic, die es damals dazu gab, geradezu altertümlich. Jedes weitere GByte schockierte mit 15 Euro. Dennoch: Es war ein Schnäppchen. Server4free mauserte sich innerhalb kürzester Zeit zu einem echten Konkurrenten zu 1&1. Heute

bietet Server4free, die mittlerweile zur BSB Service GmbH gehört, dedizierte Einstiegs-server ab knapp 30 Euro – 100 Gigabyte Traffic inklusive. Und wer mehr Traffic braucht: 89 Cent pro Gigabyte schlägt kaum ein anderer Anbieter.

Wer mal eben eine eigene Root-Umgebung ausprobieren will, ohne sich gleich einen kompletten Server zuzulegen, kann mit den so genannten vServern für unter 10 Euro pro Monat ins Adminleben reinschnuppern. Viel mehr aber auch nicht – auf einem Server, der per Software in viele kleine Serverchen geteilt wird, sind die Ressourcen schnell aufgebraucht. Außerdem gibt es viele Einschränkungen, zusätzlicher Traffic kostet hier zum Beispiel gleich 5 Euro pro Gigabyte. Da ist der Preisunterschied zum echten Rootserver schnell erarbeitet.

Der günstige Preis bei Server4free hat allerdings versteckte Haken: Zum Beispiel ist die installierte Confixx-Version »Confixx-Premium Edition 2003« lediglich eine optisch aufgewertete 1-er Pro-Version (1.6.5, um genau zu sein). Herkömmlicherweise wird von den Anbietern dedizierter Server aber die Version 2 installiert, die einige Funktionen mehr bietet. Vorbildlich ist dagegen das Administrationsmenü.

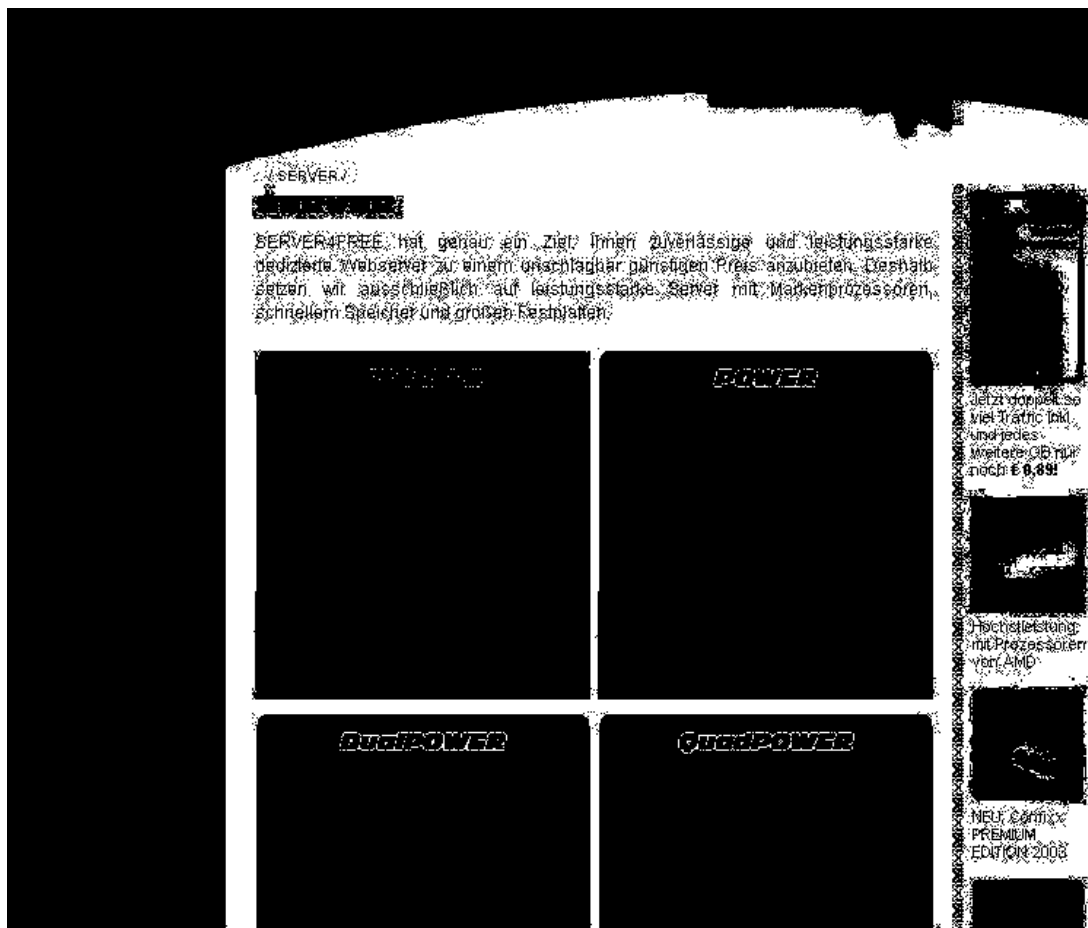


Bild 3.4: Server4free führt im Preiskrieg der großen Anbieter

3.1.5 Strato

Spät, aber immerhin: Strato – bisher nur für Wunschnamen-Adressen und kleinere Webangebote bekannt – liefert jetzt auch Rootserver. Und davon gleich einen ordentlichen Schwung: drei Rootserver und drei Managed Server.

Preislich attackiert Strato den Erzrivalen 1&1. Aber besonders in Sachen Ausstattung (Grundversion mit Pentium 4 – 2,4 GHz, 60 GByte Festplatte, 75 GByte Traffic – jedes weitere GByte kostet 6 Euro) setzt Strato mit dem so genannten »Highend Server SR« seine Mitbewerber unter Zugzwang. Als Serverkonfigurationssystem verwenden die Berliner als einziger Anbieter Visas (<http://www.visas.de> (id40)). Das ist zwar optisch noch nicht so durchgestylt wie Confixx 2 und wirkt auf den ersten Blick etwas verwirrend – aber die ein oder andere clevere Funktion, die Admins in der Kombination Webmin/Usermin/Virtualmin lieben, findet sich auch in Visas wieder.

Übrigens hat auch Strato ein ladbares Notbetriebssystem wie 1&1, aber zusätzlich gibt es die Remote-Console, die (über die serielle Schnittstelle) selbst dann noch SSH-Zugriff auf den Rechner erlaubt, wenn sich die Netzwerkkarte verabschiedet hat. Das ist ein unscheinbares, aber sehr nützliches Feature für alle, die gern an ihrem Server herumbasteln und zum Beispiel selbst neue Linux-Kernel-Versionen einspielen wollen. Mit der Remote-Console können Sie Ihrem Server quasi beim Booten zuschauen, wenn noch gar keine Netzverbindung möglich ist.

Außerdem stellt Strato einen Real-Media-Server bereit, der bis zu 50 MByte Streaming-Dateien akzeptiert.

3.1.6 MBBG Domainbox

Domainbox hat gleich vier dedizierte Servertypen im Programm: »Spirit«, »Basic«, »Real« und »Hyper«. Die günstigste Version (Spirit) kostet 45 Euro, dafür gibt es einen AMD Duron mit 1200 MHz, 256 MByte RAM und einer 40-GByte-Festplatte. Auch beim Frei-Traffic geht's sparsam zu: 30 GByte sind inklusive, jedes weitere kostet zwischen 2,60 und 2,80 Euro, je nach Datenmenge. Softwareseitig ist auf allen Systemen Debian installiert (andere Distributionen gibt es aber auf Wunsch auch) – wahlweise mit oder ohne Confixx Pro 2.0. Dazu gibt's einen Domainnamen. Fair: Die Mindestvertragslaufzeit beträgt nur einen Monat.

Über das klar gegliederte und umfangreiche Kundenmenü namens »S-Tool« können Sie die Kommunikation mit Domainbox (Ticketsystem) und eigenen Kunden abwickeln, Domains bestellen, DNS-Einträge direkt vornehmen und vieles mehr. Mithilfe der Kombination aus S-Tool und Confixx 2 Pro können auch Einsteiger leicht die ersten Schritte zum eigenen Server nehmen.

DomainBOX.de

home | produkte | bestellen | service | agb | impressum | Intoline: 01805 808 400

Produkt Übersicht
Über uns

Webhosting

- ▶ startBOX.1
- ▶ startBOX.2
- ▶ startBOX.3
- ▶ profiBOX.1
- ▶ profiBOX.2
- ▶ profiBOX.3
- ▶ ntBOX.1
- ▶ ntBOX.2
- ▶ ntBOX.3
- ▶ shopBOX.1
- ▶ shopBOX.2
- ▶ shopBOX.3

Virtualhosting

- ▶ virtualBOX.1
- ▶ virtualBOX.2
- ▶ virtualBOX.3

Serverhosting

- ▶ serverBOX.Spirit
- ▶ serverBOX.Basic
- ▶ serverBOX.Real
- ▶ serverBOX.Hyper

Der Anfang muss nicht...

serverBOX.Spirit

Unser **serverBOX.Spirit** Angebot können Sie sowohl nur als Linux Server bekommen aber auch mit Confixx 2.0 Prof. Zudem ist es jederzeit möglich, das System mit mehr Leistung auszustatten. Sollten Sie noch Fragen haben, beantworten wir Ihnen diese gern per Telefon oder auch per Email. Sprechen Sie mit uns !

Hardware:

- MSI MS-6378 ATX Sockel A
- AMD Duron 1200 MHz 128/64 KB Sockel A
- 40 GB IBM Festplatten U-100 IDE (UDMA)
- 256 MB SDRAM Arbeitsspeicher / Kingsten oder Samsung

Leistungen:

- Inkl. einer Domain nach Ihrer Wahl (de / com / net / org)
- Root / Adminrechte; Sie haben vollen Zugriff auf Ihren Server
- **Inkl. Confixx 2.0 Prof. !!**

Bild 3.5: Den »Spirit« dedizierter Server bietet das Domainbox-Einsteigerangebot

3.1.7 Weitere Anbieter

Es gibt aber auch eine ganze Reihe weiterer Anbieter, die wir Ihnen nicht verschweigen möchten. Sie alle vermieten dedizierte Server für unter 20 bis 100 Euro pro Monat. Die Ausstattung mit Prozessoren, Arbeitsspeicher und nicht zuletzt Traffic ist jedoch sehr unterschiedlich. Exemplarisch haben wir Ihnen ein paar Firmen herausgepickt: DS-Media, Greatnet, Host Europe, Keyweb, Kos-Online, Networx-Internet, Oscram-Service, Power-Netz, Serv4you, Server-Service, Web-Jansen, Webplus24. Gerade bei diesen (mit wenigen Ausnahmen) kleineren Firmen ist häufig noch eine Verhandlung über Zusatzausstattung möglich. Und: Fragen kostet nichts.

3.2 In 10 Schritten zur eigenen Website

Grundsätzlich ist die Vorgehensweise, um die erste Website ins Internet zu stellen, bei allen Anbietern ähnlich: Sie benötigen einen Domainnamen, eine statische IP-Adresse für den Rootserver, einen Nameserver-Eintrag und einen eingerichteten Webserver, der auf die Browseranfragen Ihrer Nutzer reagiert und die entsprechenden Seitendaten zurückschickt. Allerdings unterscheidet sich die Vorgehensweise von Anbieter zu Anbieter auch ein wenig. Besitzt Ihr Server ein einfaches Konfigurationsinterface (wie zum Beispiel Confixx oder PD-Admin), haben Sie ein leichtes Spiel.

Wir zeigen Ihnen anhand der wichtigsten Anbieter, wie Sie in zehn einfachen Schritten ein erstes »Hello World« von Ihrem dedizierten Server auf den heimischen Monitor

übermittelt bekommen. Die hier dargestellte Vorgehensweise beruht auf einem System mit Confixx. Dabei ist es egal, welche Confixx-Version Sie einsetzen – die Schritte sind zumindest ähnlich. Anschließend erklären wir, wie sich einzelne Details von Anbieter zu Anbieter unterscheiden.

3.2.1 Schritt 1

Zuallererst benötigen Sie einen Domainnamen und einen Nameserver-Eintrag. Um einen passenden Namen zu finden, lohnt sich der Besuch der DENIC-Internet-Site (www.denic.de (id41)). Hier können Sie schnell und sicher unter »Whois« abfragen, ob ein Name für eine Internet-Site schon vergeben ist – allerdings nur für die Endung ».de« für Deutschland. Sind Sie auf der Suche nach einer CNO-Adresse (die branchenübliche Abkürzung für Com/Net/Org), dann werfen Sie bitte einen Blick auf die WhoIs-Abfrage bei NetworkSolutions (www.networksolutions.com (id42)).

3.2.2 Schritt 2

Haben Sie Ihre Wunschadresse überprüft und ist diese nicht vergeben, dann bedienen Sie sich eines Domain-Registrierdienstes. Zwei typische Vertreter sind Providerdomain (heißen jetzt Schlundtechnologies: www.schlundtechnologies.com (id44)) und http.net (www.http.net (id45)). Bei beiden Anbietern müssen Sie sich registrieren und einen Rahmenvertrag unterschreiben. Nachdem das erledigt ist, beantragen Sie über das Web-Interface den Domainnamen. Als Beispiel zeigen wir Ihnen die Vorgehensweise bei Schlundtechnologies.



Bild 3.6: So beantragen Sie bei Schlundtec eine Domain

4 Die wichtigste Serversoftware

Ihr Server ist eingerichtet – war's das schon? Nicht wirklich – die für die einzelnen Anwendungen Ihres Rootservers zuständigen Programme haben Sie bisher garantiert nicht ausgereizt. Das vorliegende Kapitel geht für die wichtigste Serversoftware ins Detail.

4.1 Grundkonfiguration

Wenn Ihr neuer Server von Providerseite erfolgreich eingerichtet wurde, erhalten Sie in der Regel eine kurze E-Mail, die Sie auf die nun nötigen nächsten Schritte verweist und anführt, was Sie über ein Web-Interface des Anbieters noch einstellen und konfigurieren können. Etwa eine Traffic-Warnung wie: Bei Überschreiten einer von Ihnen einstellbaren Datenmenge erhalten Sie dann eine Warnmail. Ein anderer Punkt ist das Beantragen von Domain-Namen. Was genau möglich ist, variiert von Provider zu Provider.

4.1.1 1&1

1&1 stellt seinen Kunden ein recht umfangreiches Konfigurationsmenü zur Verfügung, das Sie unter <https://login.1und1.de/> (id46) erreichen (https beachten!). Nachdem Sie sich eingeloggt und den zu bearbeitenden Vertrag ausgewählt haben, betreten Sie über »Serververwaltung« den wichtigsten der Unterbereiche.

- Konfiguration & Verwaltung

Hier können Sie zum Beispiel die Serverdaten abrufen (zumindest diejenigen, die bei der Bestellung und Ersteinrichtung des Servers vergeben wurden). Im Notfall können Sie Ihren Server neu booten oder im Recovery-Modus starten lassen. Zudem können Sie wählen, ob Sie lieber einen Mailserver auf Ihrem eigenen Server verwenden (sinnvoll, wenn Sie zum Beispiel Bereiche Ihres Servers vermieten) oder auf das 1&1-Mailsystem zurückgreifen (macht Sinn, wenn Sie Ihren Server nur privat einsetzen, zum Beispiel als Gameserver – um den Mailserver müssen Sie sich dann nicht kümmern) wollen. Zusätzliche Domainnamen verschaffen Sie sich bequem über die Domain-Verwaltung. Dort können Sie sich zum Beispiel auch schon für Domains mit Umlauten vormerken lassen (ohne Garantie, dass Sie diese auch erhalten). Die E-Mail-Verwaltung ermöglicht es Ihnen – für den Fall, dass Sie auf das 1&1-Mailsystem setzen –, neue Mailadressen zu definieren und bestehende umzuleiten. Weniger nützlich sind die Performance-Tools. Unter diesem Menü finden Sie lediglich einen Link zu webmasterplan.de, einem nur teilweise kostenlosen Service zur Website-Optimierung.

- Software & Lizenzen

Bei »Software & Lizenzen« finden Sie die Option, nachträglich für 6 Euro Porto die 1&1-Software-CD anzufordern. Wenn Sie die darauf enthaltenen Programme benötigen (zum Beispiel Netobjects Fusion MX) und nicht schon für ein anderes Webspace-Paket bekommen haben, ist das ein durchaus lohnendes Schnäppchen. Die nötigen Registrierschlüssel erhalten Sie ebenfalls im Softwaremenü.

- Zusatzleistungen / Tune-up bestellen

Nützlich sind außerdem noch ein paar der Einträge im »Zusatzleistungen«-Menü: Dort ordern Sie Domainnamen oder bestellen eine mit 49 Euro pro Monat recht teure Backup-Lösung.

- Rund um diesen Vertrag

Einen Blick (oder zwei, oder drei...) sollten Sie unbedingt auf »Rund um diesen Vertrag« werfen. Dort haben Sie nämlich (von der Rechnungseinsicht abgesehen) die Möglichkeit, die Traffic-Kontrolle zu aktivieren. Besonders praktisch: bei 1&1 können Sie auch ein echtes Kostenlimit setzen, das alle zu Ihrem Vertrag anfallenden Gebühren umfasst. So können Sie sich vor unliebsamen Überraschungen schützen.

Für weitere, servernahe Einstellungen können Sie von der Serververwaltung aus übrigens auch direkt ins Confifix-Menü auf Ihrem Rootserver springen.

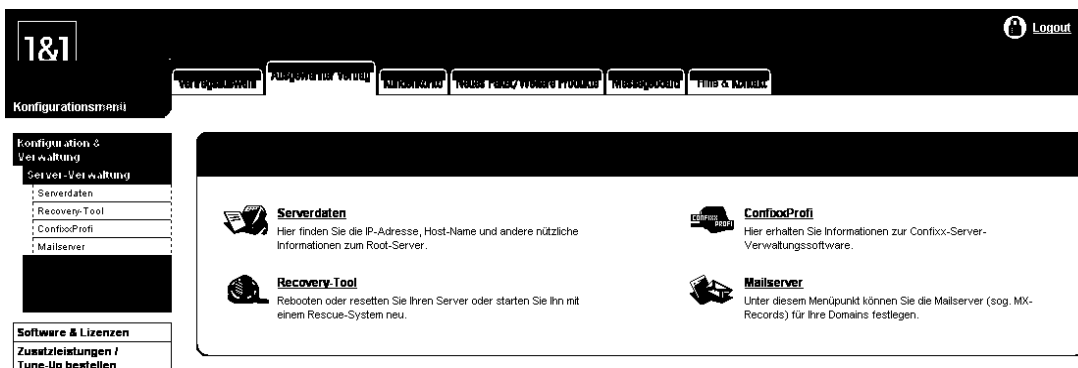


Bild 4.1: Die Serververwaltung bei 1&1

4.1.2 IPX-Server

IPX-Server besitzt für seine Server wie 1&1 ein Kunden-Interface, über das Sie die wichtigsten Einstellungen verändern können. Einstellen lässt sich dort unter anderem die Traffic-Überwachung (sehr wichtig), Sie können per Weboberfläche einen Hardware-Reset ebenso anfordern wie ein Rescue-System, das Ihren Server bootet, ohne seine Festplatte zu benutzen.

Support-Anfragen werden Sie natürlich auch online los. Kleiner Nachteil: Wir können Ihnen dieses System hier noch nicht detailliert beschreiben, da es erst nach Redaktionsschluss dieses Buches (geplant ist der September) in Betrieb geht. Allerdings macht die uns zugänglich gemachte Vorabversion einen durchaus viel versprechenden Eindruck.

4.1.3 Hetzner

Hetzner bietet unter <https://www.hetzner.de/robot/> (id47) ein knappes, aber durchaus nützliches Grundmenü, das auch noch funktioniert, wenn Ihr Server nicht mehr erreichbar ist. Nicht erschrecken, wenn Sie den Robot zum ersten Mal aufrufen: Was da auf der Titelseite prangt, ist nicht Ihre aktuelle Rechnung, sondern die Preisliste. Immerhin wissen Sie damit stets, woran Sie sind. Der Registration-Robot erledigt fast nur Verwaltungsaufgaben: Sie können Rechnungen einsehen und unterschiedlichste Traffic-Reports abrufen.

Sehr nützlich ist unter Umständen die Traffic-Begrenzung, die Sie hier einstellen können. Sie legen dazu Grenzwerte pro Stunde, Tag und Monat fest, bei deren Überschreiten Sie eine Warnmail erhalten. Wenn Sie diese noch an ein E-Mail-Konto mit SMS-Benachrichtigung schicken lassen, sind Sie auch mobil stets gewarnt. Speichern Sie am besten noch die Telefonnummer des Supports in Ihrem Adressbuch, dann können Sie den Server notfalls vom Netz nehmen lassen.

Wenn mal nichts mehr funktioniert, probieren Sie es doch zunächst mit einem Reset-Auftrag, den Sie ebenfalls hier absetzen können. Allerdings müssen Sie, wenn Sie außerhalb der Hetzner-Geschäftszeiten das Bedürfnis nach einem manuellen Reset verspüren, eine E-Mail an server_down@hetzner.de schicken. Auch für Support-Anfragen über das Service-Menü gilt Ähnliches: Diese werden kostenfrei beantwortet, wenn sie während der Geschäftszeiten eintreffen.



Bild 4.2: Der Registration-Robot bei Hetzner

Schließlich bietet Ihnen der Registration-Robot auch noch die Möglichkeit, Reverse-DNS-Einträge anzulegen, die bestimmen, welcher Name Ihrer IP-Nummer zugeordnet wird. Domainnamen selbst können Sie bei Hetzner <http://www.hetzner.de/robot.htm> (id48) beantragen. Alle weiteren Einstellungen können Sie übrigens mithilfe von Webmin (<https://xxx.xxx.xxx.xxx:10000/>) treffen. Die »xxx« müssen Sie dabei durch Ihre IP-Nummer ersetzen, beachten Sie auch das »s« hinter http.

4.1.4 Server4Free

Server4Free bietet seinen Rootserver-Kunden unter www.server4free.de/admin/ (id49) ein recht umfangreiches Admin-Interface.

- Verwaltung

Hier können Sie zum Beispiel Vertrags- und Serverdaten einsehen, inklusive aller Kennwörter, wobei nur das zum Start vergebene Server-Root-Passwort angezeigt wird, das Sie selbstverständlich schon auf der Linux-Kommandozeile geändert haben. Ändern können Sie hier direkt nur Ihr Passwort für den Administrationsbereich selbst. Sie können zudem Ihre Rechnungen einsehen und Kontakt- und Kontoinformationen aktualisieren. Der Punkt »Kündigung« ist allerdings nicht wirklich nützlich – ein Klick darauf gibt Ihnen lediglich zu verstehen: »Um Ihren Vertrag mit uns zu kündigen, schicken Sie uns bitte Ihre schriftliche Kündigung per Fax oder Post.«

- Support

Ein sehr nützlicher Bereich: Hier können Sie unter anderem Support-Anfragen stellen, aber auch die Antworten aktueller und früherer Anfragen abrufen. Zudem können Sie eine wenig ausführliche Traffic-Statistik abrufen.

- Tools

Diesen Bereich benötigen Sie vor allem, wenn mal nichts mehr funktioniert. Dazu kennt S4F verschiedene Werkzeuge: Nur bevor etwas passiert, ist das FTP-Backup (letzter Punkt im Tools-Menü) nützlich. Um dies durchzuführen, müssen Sie sich von Ihrem Server aus auf dem Backup-Server einloggen – das nötige Passwort können Sie hier ändern. Der Reboot-Service drückt quasi den Reset-Knopf Ihres Servers – ein Hardware-Reboot, der oft auch noch hilft, wenn Sie sich ausgesperrt haben. Falls das Ihren Fehler nicht beseitigt hat, können Sie auf das Recovery-System ausweichen: Das bootet ein minimales RedHat-System, ohne die Festplatten Ihres Rootservers zu nutzen. Es steht zurzeit allerdings nur wochentags tagsüber zur Verfügung. Das Mittel der Wahl, wenn jemand in Ihren Server eingedrungen ist. Schließlich bietet S4F auch noch eine komplette Neuinstallation an, die Sie ebenfalls hier anfordern können.

- DNS & Domain

Dieser Abschnitt ist für alles zuständig, was die für Sie verfügbaren Domainnamen betrifft. Sie können neue Domainnamen ordern, einen KK-Antrag für den Umzug einer Ihrer Domains zu S4F stellen, Sie können festlegen, was der Nameservice antworten soll, wenn nach dem Namen zu Ihrer IP-Nummer gefragt wird (»Reverse-DNS«), können für all Ihre Domains zum Beispiel Subdomains definieren oder auf eigene Nameserver ver-

weisen. Schließlich können Sie auch noch zusätzliche IP-Nummern bestellen (zum Beispiel für Kunden).

- Service

Schließlich findet sich auch noch der Servicebereich, der allerdings nur FAQs (immerhin wichtiger Lesestoff) und ein paar Links enthält.

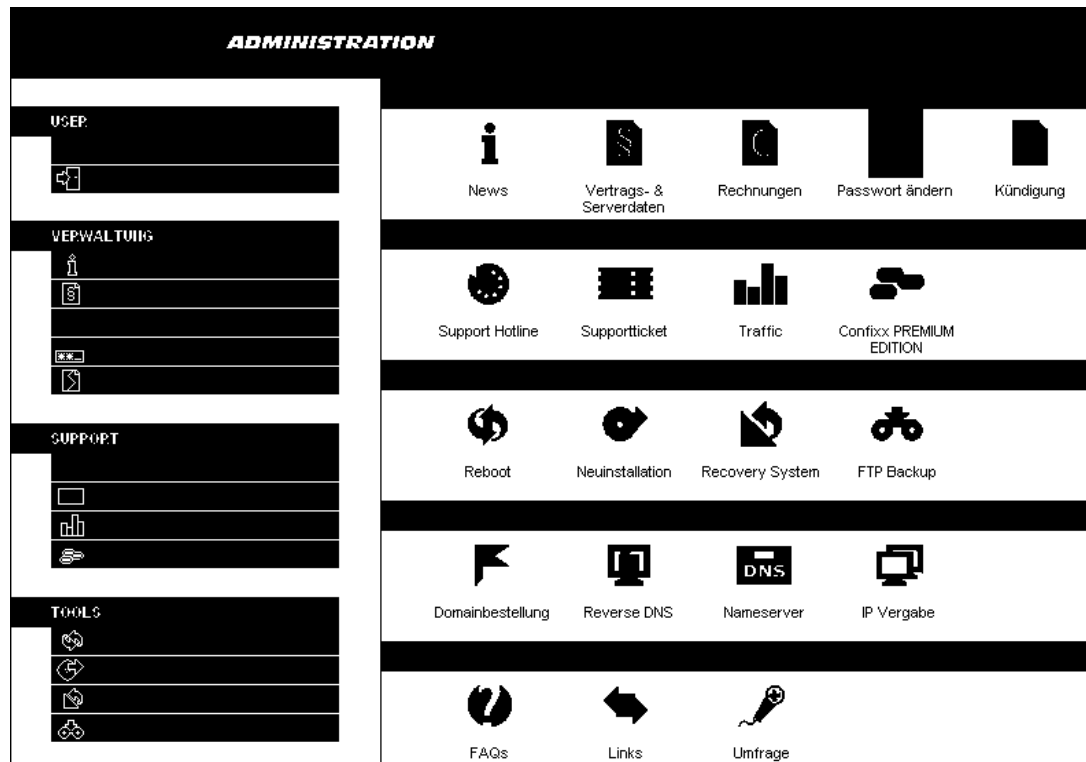


Bild 4.3: Admin-Interface von Server4Free

4.1.5 Strato

Das Kundenmenü der Strato-Rootserver ist unter der Adresse <https://config.strato.de> erreichbar. Den Login-Namen und das passende Kennwort hat Ihnen Strato mitgeteilt. Hier die wichtigsten zur Verfügung stehenden Bereiche:

- Traffic-Statistik: Sie verrät Ihnen (allerdings im Tagesrhythmus), wie viel Ihres Inklusiv-Traffics Sie bereits verbraucht haben. Außerdem können Sie hier eine Warngrenze festlegen (in Prozent des Inklusivverbrauchs), bei deren Überschreiten Ihnen eine E-Mail zugeschickt wird. Wenn Sie hier »0 %« eingeben, bekommen Sie täglich eine Traffic-Übersicht per E-Mail.
- Zugangsdaten: Hier können Sie Ihr nicht ganz unwichtiges Passwort für den Zugang zum Konfigurationsmenü ändern (hat mit Ihrem Root-Passwort für den Server allerdings nichts zu tun).

- **Domainverwaltung:** Dieses Menü dient zum Bestellen neuer Domainnamen. Die Preise variieren zwischen 99 Cent (.de) und 1,45 Euro (andere) monatlich.
- **SSL-Verwaltung:** Wenn Sie den Aufwand zur Installation eines eigenen SSL-Zertifikats scheuen, können Sie hier einen von Strato zugeschalteten SSL-Proxy aktivieren.
- **Media-Server:** Über diesen Menüpunkt können Sie Accounts auf einem Strato-Realmedia-Server anlegen. Das gibt Ihnen die Möglichkeit, später unter *http://www.ihredomain.de/realmediafile.ram* Streaming Media zum Download anzubieten. Dadurch bleibt Ihnen erspart, einen eigenen Streaming-Media-Server auf Ihrem Server einzurichten.
- **Serverkonfiguration:** Das wohl wichtigste Menü im Kundenbereich. Einerseits finden Sie hier Ihre Erstzugangsdaten (inklusive Root-Passwort). Andererseits erreichen Sie hier Stratos Recovery-Modus: Per Mausclick können Sie wählen, ob Ihr Server resettet oder neu gebootet wird – und in welchem Modus das passiert: »normal« oder per Rettungssystem. Übrigens können Sie bei Strato über die Reset-Option sogar einen irrtümlich komplett heruntergefahrenen Rechner wieder aktivieren. Schließlich können Sie hier auch die serielle Konsole ein- und ausschalten, mit der Sie Ihrem Server sogar beim Booten zusehen können. Bei der seriellen Konsole arbeiten Sie fast wie mit einer Tastatur direkt am Server. Sie greifen per SSH-Programm auf die Remote-Console zu und diese leitet Ihre Eingaben als Tastatureingabe an Ihren Server weiter.

The screenshot shows the Strato customer interface. At the top right, it says 'European Multimedia Forum 02 2001'. Below that is a navigation bar with links: 'Produkte', 'Kundenservice', 'Wir über uns', 'Kontakt', 'Presse', 'Übersicht', 'FAQ'. The main content area is divided into two parts. On the left is a vertical navigation tree under the heading 'Kundenservicebereich'. The tree includes: 'News und Infos' (Aktuelle Meldungen, Technische News), 'Anleitungen' (Anleitungen), 'Trafikstatistik' (Datentransfer, E-Mail-Benachrichtigung, Kurzanleitung), 'Zugangsdaten', 'Domainverwaltung' (Domainübersicht, Neue Domain bestellen, Kurzanleitung), 'SSL-Verwaltung' (SSL-Proxy, Kurzanleitung), 'Media-Server' (RealMedia, Kurzanleitung), and 'Serverkonfiguration' (Serverdaten, RecoveryManager, RemoteConsole). On the right is the 'SSL-Proxy' page. The text on this page reads: 'Hier können Sie für Ihre Domain einen SSL-Proxy einrichten. So ist Ihre Präsenz auch dann mittels SSL erreichbar, wenn Sie kein eigenes SSL. Ihre Präsenz ist dann unter der URL `https://ssl-id1.de/<IhrDomainname>/` erreichbar. Bitte aktivieren Sie nachfolgend die Domainnamen, für die Sie entsprechend den :'. Below this text are three empty rectangular boxes for input.

Bild 4.4: Kundenmenü der Strato-Rootserver

4.1.6 MBBG Domainbox

Domainbox besitzt sowohl einen Kundenbereich (mit Kundennummer und separat zugeteiltem Kennwort) als auch das schon in früheren Kapiteln erwähnte S-Tool. Im Kundenbereich (<https://www.domainbox.de/Kundenbereich/>) finden Sie vor allem Anleitungen und die Möglichkeit, Support-Anfragen zu stellen. Außerdem können Sie dort Domainnamen ordern.

Das S-Tool ist noch ein Stück nützlicher. Darüber können Sie die Kommunikation mit Domainbox (Ticketsystem) und eigenen Kunden abwickeln, Domains bestellen und DNS-Einträge direkt vornehmen und vieles mehr. Die wichtigsten Features von S-Tool haben wir bereits in Kapitel 3 erläutert.

4.2 Apache, der Webserver

Die wohl wichtigste Komponente Ihres Servers – wenn Sie es nicht gerade auf ein nur als Gameserver laufendes System abgesehen haben. Apache läuft weltweit auf deutlich mehr als der Hälfte aller Webserver. Das hat auch seinen Grund: Apache ist kostenlos erhältlich, es wird von einer Vielzahl von Programmierern auf freiwilliger Basis weiterentwickelt. Gleichzeitig läuft es sehr stabil und ist auf den verschiedensten Betriebssystemversionen verfügbar. Zurzeit sind die Versionen 1 und 2 im Ablauf. Allerdings konnte sich die neuere Programmvariante noch nicht durchsetzen – teils wohl wegen der Devise »never change a running system«, teils auch, weil die wichtigsten Module noch nicht vollständig dafür erhältlich sind. Das Programm liefert, kurz gesagt, Webseiten aus – kann aber noch einiges mehr, wie Sie im Folgenden erfahren werden.

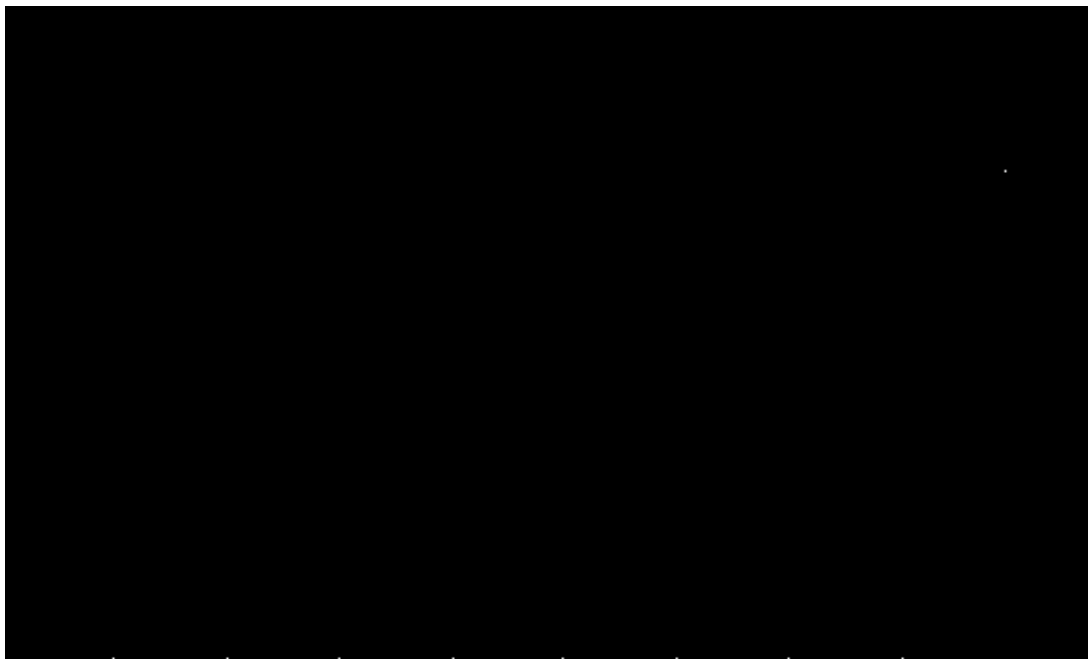


Bild 4.5: Marktanteile des Apache-Webserver

4.2.1 Apache auf den neuesten Stand bringen

Schon aus Sicherheitsgründen ist es immer angeraten, die verwendeten Programme zunächst auf den allerneuesten Stand zu bringen – so sind zumindest die bis dato bekannten Schlupflöcher (es gibt keine fehlerfreie Software) beseitigt. Wenn wir im folgenden Programmversionen nennen, dann sind das diejenigen, die zum Redaktionsschluss des Buches aktuell waren. Wir geben deshalb zusätzlich jeweils eine Webseite an, auf der Sie sich über den gegenwärtigen Versionsstand informieren können.

Zunächst überprüfen Sie, ob die nötigen Pakete womöglich schon installiert sind. Wenn Sie irgendwelche sicheren (also verschlüsselten) Transaktionen anbieten (etwa E-Mail oder ein Shoppingsystem), benötigen Sie zunächst SSL (»Secure Sockets Layer«), und zwar in seiner freien (und kostenlosen) Variante OpenSSL. Geben Sie auf einem RPM-basierten System (alles außer Debian) diesen Befehl ein:

```
rpm -qa --queryformat '%{NAME} %{VERSION}' | grep openssl
```

erscheinen. Wenn die unter www.openssl.org angegebenen Versionsnummern größer als die auf Ihrem System vorhandenen sind oder der Bildschirm ganz leer bleibt, sorgen Sie mit

```
rpm -Uvh http://www.openssl.org/openssl-0.9.7c-1.i386.rpm
```

für aktualisierten Nachschub, zumindest unter SuSE 8.1. Bei 8.2 ändern Sie die Versionsnummer in der Adresse entsprechend. RedHat-Anwender finden ein für ihre Version aktualisiertes RPM unter <http://www.redhat.com/apps/download/> (id52).

Debian-Besitzer können über diese umständlichen Befehle nur lächeln: Hier reicht ein

```
apt-get update
```

```
dpkg-query -f='${Package} ${Version} ${Architecture}\n'
```

Jetzt geht es Apache an den Kragen – zunächst den dafür installierten Modulen, kleinen Helferlein, die sich in den Server quasi einklinken. Wieder prüfen Sie zunächst, welche Module vorhanden sind:

```
apache2ctl -M
```

Daraufhin könnte folgende Liste erscheinen:

Sehr wahrscheinlich ist die Liste noch länger, aber diese vier werden später noch benötigt. Welche Apache-Version auf dem Server läuft, erfahren Sie mit

Es sollten nun wenigstens drei Files gelistet werden:

Anschließend entfernen Sie die insgesamt sieben Module. Dazu benutzen Sie zum Beispiel

Das heißt, die Versionsnummern hinter dem Namen sind nicht mit anzugeben. Achtung: Bei Debian nutzen Sie statt Rpm natürlich Dpkg. War die Operation erfolgreich, müssen Sie zunächst die aktuelleren Versionen auf Ihren Server holen. Wechseln Sie zunächst das Verzeichnis:

Dann benutzen Sie das wget-Programm wie folgt:

Nun geht's ans Auspacken:

und zwar wieder mit der oben in Erfahrung gebrachten Versionsnummer. Allerdings wird Ihnen Apache nicht fertig geliefert. Sie haben bisher nur den Quellcode auf der Festplatte und müssen diesen noch nach Ihren Anforderungen kompilieren, also in lauffähigen Code übersetzen. Die dafür nötigen Werkzeuge sind in jeder Linux-Variante bereits enthalten und können sogar das komplette System selbst neu übersetzen. In Bezug auf Apache können Sie wählen, ob Sie die Zusatzmodule statisch oder dynamisch einbinden wollen – beides hat Vor- und Nachteile.

Wenn Sie sich fürs statische Kompilieren entschieden haben, teilen Sie das dem System über

mit. Soll die Einbindung lieber dynamisch erfolgen, wählen Sie die Variante

Falls der Apache nicht in `/usr/local/apache` installiert werden soll, können Sie auch noch diese Parameter benutzen:

Das `prefix`-Argument steht hierbei für den Hauptordner der Installation. Der `sysconfdir`-Parameter sagt Apache, dass die Konfigurationsdateien (z.B. `httpd.conf`) in diesem Ordner abgelegt werden sollen. `»Htdocsdir«` steht für den Standardvirtualhost. Dieser ist nicht so besonders wichtig, da es meist besser ist, jedem Programm und jedem Anwender seinen eigenen Virtualhost zu verpassen. Ähnlich verhält es sich mit dem Standard `»cgi-bin«`, wo CGI-Programme abgelegt werden. Im `»runtimedir«` finden sich die dem Apache-Prozess zugeordnete PID-Datei bei der Ausführung und im `»logfiledir«` legt das Programm logischerweise die Logdateien ab.

Jetzt geht es ans eigentliche Übersetzen, das der `»make«`-Befehl startet:

Nun müssen wir noch dafür sorgen, dass Apache bei jedem Systemstart automatisch startet. Dazu legen wir eine Verknüpfung von `/usr/local/apache/bin/apachectl` (falls Sie ein anderes Präfix gewählt haben, müssen Sie den Pfad gegebenenfalls anpassen) nach `/etc/init.d` an:

Nun legen wir noch eine Verknüpfung nach `/etc/rc.d/rc3.d` (Runlevel 3, normalerweise Standard):

(das gilt für SuSE – bei Debian: `/etc/rc3.d/` und bei RedHat: `/etc/rc.d/rc3.d`) Abschließend fügen wir noch den Pfad `/usr/local/apache/bin` zur `PATH`-Variable hinzu:

WebDAV-Modul

WebDAV oder kurz DAV ist eine Technologie, mit der sich Webinhalte aus der Ferne bearbeiten lassen – quasi eine moderne Variante von FTP. Immer mehr Programme unterstützen WebDAV. Wenn Sie oder Ihre Anwender oder Kunden die Technik nutzen

wollen, müssen Sie Apache das WebDAV-Modul zur Verfügung stellen. Das bekommen Sie hier:

Danach entpacken Sie das Sourcecode-Paket:

Am praktischsten ist es nun, wenn Sie Apache zur Verwendung dynamischer Module überredet haben. Dann kompilieren Sie WebDAV so:

Statisch dauert's etwas länger. Dafür müssen Sie zuerst das Modul selbst kompilieren:

Danach wechseln Sie in Apaches Quellcodeverzeichnis und sagen dem System, dass es ein neues Modul mit einbinden muss:

Zum Schluss müssen Sie den kompletten Webserver neu übersetzen:

SSL-Modul

Wir haben schon am Anfang der Apache-Installation OpenSSL eingeführt. Damit der Webserver auch darüber kommunizieren kann, müssen Sie nun auch das SSL-Modul einbinden. Das ist ein recht komplizierter Vorgang, weil es hierbei auf die Reihenfolge ankommt. Mod_ssl sollte immer vor den anderen Modulen installiert werden. Am besten, Sie holen sich zunächst das Quelltextarchiv auf Ihren Server:

Dann folgt wie immer der Entpackvorgang:

Jetzt öffnen Sie mit

die Installationsanweisungen. Denn praktischerweise haben die mod_ssl-Programmierer darin für die unterschiedlichsten Konfigurationen (etwa Apache mit Perl oder Apache mit PHP und MySQL) Beispielablaufpläne erfasst (ziemlich am Dateiende zu finden), die wir hier nicht in aller Ausführlichkeit wiederholen wollen.

4.2.2 Apache und seine Module

Einer der Hauptgründe für die Popularität des Apache-Webservers ist zweifellos die Möglichkeit, ihn mithilfe von Modulen auszubauen. Natürlich wird auch schon eine ganze Reihe dieser Erweiterungen mitgeliefert. Die große Auswahl führt allerdings fast zwangsläufig dazu, dass sich Einsteiger zunächst im Modulschunzel verirren. Zudem gibt es für viele der Module keine deutsche Beschreibung, von einer Installations- und Konfigurationshilfe in Deutsch ganz zu schweigen.

Dass der Apache-Server zwei Verfahrensweisen kennt, Module einzubinden, haben wir Ihnen bereits weiter vorn erläutert. Wenn Sie ein Modul nur einmal ausprobieren wollen, binden Sie es am besten zuerst dynamisch ein. Das ist normalerweise recht einfach, weil Sie ja nicht den kompletten Webserver neu übersetzen müssen. Kompilieren Sie, wenn nötig, das Modul, indem Sie den Anweisungen der mitgelieferten INSTALL-Textdatei folgen. Dann kopieren Sie die .so-Datei in den /modules-Ordner des Apache. Schließlich müssen Sie den Server auch noch veranlassen, das Modul zu laden. Das erledigen Sie über die LoadModule-Direktive in der httpd.conf (siehe folgender Abschnitt).

Um Ihnen einen Überblick über die Module und ihre Funktionen zu geben, führen wir im Folgenden die meisten der mitgelieferten Erweiterungen auf und empfehlen zusätzlich einige wichtige Fremdmodule. Eine genauere Erklärung würde den Rahmen des Buches sprengen, deshalb finden Sie zu jedem Modul nur eine kurze Beschreibung und können sich so einen Eindruck davon verschaffen, ob es für Ihre Zwecke nützlich ist. Eine ausführliche Liste mit Suchfunktion, finden Sie in der Apache Module Registry (<http://modules.apache.org/>).

Auf **fett** markierte Module kommen wir etwas später noch separat zu sprechen – im Abschnitt zur Apache-Konfigurationsdatei httpd.conf zum Beispiel.

- **mod_access**

Ein sehr wichtiges Modul, das den Zugriff auf Teile des Servers, bestimmte Verzeichnisse und Dateien regelt.

- **mod_actions**

Dieses Modul erlaubt es, immer dann ein CGI-Programm zu starten, wenn ein bestimmter Dateityp angefordert wird oder die Anforderung von einem bestimmten Typ ist.

- **mod_alias**

Damit lassen sich Anforderungen weiterleiten – nützlich, wenn Internetseiten zum Beispiel umgezogen sind.

- **mod_asis**

Dieses Modul erlaubt es, Dateien zu senden, wie sie sind (»as is«), das heißt auch ohne den normalerweise von Apache hinzugefügten HTTP-Header.

- **mod_auth**

Damit lässt sich eine Benutzerauthentifizierung basierend auf einfachen Textdateien mit Namen und Passwörtern realisieren.

- **mod_autoindex**

Dieses Modul sorgt dafür, dass Apache bei Verzeichnissen, die keine Indexdatei (etwa index.html) enthalten, selbst einen Index anlegt und an den User schickt. Das kann zum Beispiel für einfache Download-Abteilungen sinnvoll sein, da zum Beispiel je nach Dateityp auch kleine Icons erzeugt werden.

- **mod_cgi**

Die Voraussetzung, um von Apache aus CGI-Skripts zu starten (»Common Gateway Interface«) – etwa Perl-Programme.

- **mod_dir**

Dieses Modul verrät dem Webserver, welche Datei er liefern soll, wenn ein Anwender statt eines Dateinamens den Namen eines Verzeichnisses anfordert. Zum Beispiel index.html oder index.php.

- **mod_env**

Mithilfe dieses Moduls können Sie die Umgebungsvariablen ändern, die CGI-Skripts zur Verfügung stehen. Normalerweise gelten für Skripts dieselben Umgebungsvariablen wie für die Shell, aus der der Webserver gestartet wurde. Das kann unter Umständen ein Sicherheitsproblem sein.

- **mod_expires**

Bestimmt, wie lange eine Seite (zum Beispiel im Cache oder in Proxys) zwischengespeichert werden soll.

- **mod_imap**

Zum Erstellen von serverseitigen Imagemaps (.map-Dateien), zum Beispiel für grafische Menüs.

- **mod_include**

Wenn Ihr Apache die so genannten Server Side Includes (SSI) verstehen soll, müssen Sie dieses Modul aktivieren. Apache führt dann speziell formatierte SSI-Befehle (`<!--#element attribute=value attribute=value ... -->`) aus und fügt deren Ausgaben in den HTML-Text ein.

- **mod_info**

Zum Anzeigen von installierten Modulen und Direktiven in der Konfigurationsdatei. Die Informationen sind über *http://your.host.tld/server-info* abrufbar. Dieses Modul sollten Sie aus Sicherheitsgründen nicht statisch einbinden und auch nur vorsichtig einsetzen.

- **mod_log_config**

Umfassendes Standardmodul zum Mitschreiben aller Anforderungen, inklusive Cookys, Browsertypen, Referrer und so weiter.

- **mod_mime**

Ein sehr wichtiges Modul, das – von Dateierweiterungen ausgehend – die zugehörigen MIME-Dateitypen festlegt. Browser müssen den MIME-Typ eines Dokuments kennen, um es korrekt anzeigen zu können.

- **mod_mime_magic**

Mod_mime_magic ergänzt mod_mime, indem es zusätzlich die ersten paar Bytes einer Datei betrachtet und daraus ihren Typ zu bestimmen versucht. Die Informationen, welche Datenbytes welchem Dateityp entsprechen könnten, bezieht es aus einer Datei.

- **mod_negotiation**

Haben Sie sich auch schon gewundert, dass beim Aufruf von *google.com* die deutsche Google-Seite erscheint? Dieses Modul ermöglicht diesen Trick. Es gestattet Webserver und Browser, über die Art der gelieferten Inhalte zu entscheiden, zum Beispiel nach der Sprache des Anwenders oder nach den Fähigkeiten des aufrufenden Browsers. So könnten auf einem Handy zum Beispiel anders formatierte Seiten erscheinen als auf einem PC.

- **mod_proxy**

Dieses Modul aktiviert auf Ihrem Server einen so genannten Proxy, der Dateien aus dem Web zwischenspeichert. Da offene Proxys sich leicht missbrauchen lassen und ein Proxy auf Ihrem Rootserver nur in Sonderfällen sinnvoll ist, empfehlen wir, das Modul zu deaktivieren, zumindest aber die Direktive ProxyRequests auf »off« zu stellen.

- **mod_rewrite**

Das »Schweizer Offiziersmesser« der URL-Manipulation. Ein sehr komplex anzuwendendes Modul, das die vielfältigsten Funktionen erfüllt, indem es Internetadressen nach bestimmten Regeln umformt.

- **mod_setenvif**

Mit diesem Modul können Sie Umgebungsvariablen von Parametern der Anforderung abhängig machen. So könnten Sie zum Beispiel Suchmaschinen-Roboter anders behandeln als normale Browser.

- `mod_so`

Modul zum dynamischen Laden anderer Module. Ohne dieses Modul lassen sich keine dynamischen Module einbinden.

- `mod_speling`

Kein Schreibfehler: Dieses sehr praktische Modul hilft Ihren Usern beim »Spelling«, also wenn sie mal einen Tippfehler fabriziert haben, zum Beispiel durch falsche Groß- und Kleinschreibung. Es sucht nach Dateien, die der Anforderung weitgehend entsprechen. Findet es gar nichts, folgt der übliche Error 404. Findet es genau ein ähnlich geschriebenes Dokument, leitet es darauf weiter. Tauchen sogar mehrere ähnliche Dateinamen auf, bekommt der Anwender eine Auswahlliste.

- `mod_status`

Mit `mod_info` verwandt, gibt dieses Modul Informationen zum Serverstatus aus. Auch damit sollten Sie eher vorsichtig umgehen.

- `mod_unique_id`

Damit lässt sich jeder Anforderung eine eindeutige Kennzeichnung zuordnen.

- `mod_userdir`

Erlaubt es, Anwendern eigene Heimatverzeichnisse zuzuordnen. Mithilfe dieses Moduls entstehen die »beliebten« Verzeichnisse mit der Tilde: `www.bla.tld/~otto` kann zum Beispiel in das Unterverzeichnis `/usr/web/otto` »übersetzt« werden.

- `mod_usertrack`

Für Datensammler interessant: Mit `mod_usertrack` können Sie den Weg Ihrer User durch Ihr Webangebot verfolgen (den so genannten »Clickstream«). Diese Daten könnte man zum Beispiel auswerten, um die Benutzerführung der Site zu verbessern.

- `mod_vhost_alias`

Dieses Modul lässt sich dazu einsetzen, eine große Zahl ähnlich konfigurierter virtueller Hosts bereitzustellen.

Externe Module

- `mod_backhand`

http://www.backhand.org/mod_backhand/ (id56)

Wenn Sie mindestens zwei Server betreiben, ermöglicht Ihnen dieses Modul ein relativ simples Load-Balancing, das heißt, wenn ein Server stark ausgelastet ist, können Anfragen an einen zweiten Server weitergeleitet werden.

- `mod_bandwidth`

http://www.cohprog.com/mod_bandwidth.html (id57)

5 Confixx, Visas, Webmin

Für viele Routineaufgaben müssen Sie nicht die Linux-Kommandozeile bemühen: Programme mit Web-Interface erleichtern die Arbeit, wenn es um Einstellungsparameter und Ähnliches geht. Dieses Kapitel führt Sie in die Arbeit mit den beliebtesten Vertretern dieser Softwaregattung ein – allen voran Confixx.

Server konfigurieren ist eine ziemlich mühsame Angelegenheit. Wenn Sie sich nicht mit den Dateien wie der `httpd.conf`, SSH-Logins, Konfigurationsskripts, Cronjobs und ähnlichem herumschlagen möchten, dann werden Sie für ein paar nützliche Programme zur Serververwaltung dankbar sein. Am bekanntesten im Rootserverbereich ist sicher das Programm Confixx von Swsoft (früher yippi-yeah-Software). Etwas weniger bekannt ist Visas, das Strato für seine Rootserver einsetzt und das recht günstig zu haben ist.

Sollte auf Ihrem Rootserver keines der beiden Verwaltungssysteme installiert sein, dann gibt es den Webmin – ein sehr mächtiges Konfigurationstool, das in weiten Teilen Confixx & co. in den Schatten stellt, dafür aber andererseits wesentlich mehr Wissen voraussetzt und in puncto Userverwaltung gar nicht oder nur mit Erweiterungen wie Usermin zum Einsatz kommen kann. Alle drei Varianten (Confixx, Visas und Webmin) werden wir uns ansehen.

Neben diesen drei Tools gibt es noch eine Fülle weiterer, zum Teil guter und günstiger Konfigurationstools, beispielsweise PD-Admin (www.pd-admin.de (id145)), SeCoTo (www.secoto.org (id146)), Providertool-Server-Admin (www.providertool.de (id147)) und viele mehr.

Alle gängigen Tools haben mehrere Dinge gemeinsam: Die Konfiguration des Webserver geschieht mit einem herkömmlichen Browser. Die Seiten sind passwortgeschützt und sie unterteilen die Serveranwender in drei Gruppen (mit Ausnahme von Webmin): Administratoren, Wiederverkäufer/Anbieter und Anwender/User.

Das Beste an den Konfigurationslösungen ist aber: Sie sind wirklich kinderleicht zu bedienen, selbst für völlig Linux-unerfahrene Anwender. Das ist allerdings auch ihr größter Nachteil. Verlassen Sie sich nicht drauf, dass Sie Ihren Server ausschließlich mit den Konfigurationsprogrammen in den Griff bekommen. Das wird ganz sicher schief gehen. Viele Aufgaben und nette Effekte lassen sich nur händisch lösen. Einige Beispiele, wie Sie Confixx komplett in den Griff bekommen, zeigen wir Ihnen im Confixx-Kapitel.



Bild 5.1: Die S4f-Premium-Edition hat fast die gleichen Funktionen wie Confixx 2

5.1 Der Klassiker: Confixx

Confixx gilt derzeit sicher als das Referenzprodukt in der Klasse der Serverkonfigurationsprogramme – sowohl in puncto Anzahl der installierten Versionen als auch im Preis. Um so erfreulicher ist, dass der hohe Confixx-Preis bei den Rootserver-Anbietern wie 1&1, IP-Exchange und Server4free so gut wie nicht zu Buche schlägt. Allerdings unterscheiden sich die Versionen der Server-Vermieter. Während 1&1, Domainbox und IP-Exchange die aktuellen Versionen (derzeit Pro 2.0, ab Spätherbst 3.0) einsetzen, erhalten Sie bei Server4free eine leicht erweiterte Version 1, die optisch etwas anders als die herkömmlichen Versionen erscheint. Inhaltlich unterscheiden sich die Versionen gar nicht mal so dramatisch, weshalb wir hier die aktuelle Version 2 Pro besprechen. Sind Sie Server4free-Kunde und finden bestimmte Funktionen nicht (zum Beispiel die DNS- und DNR-Verwaltung), dann ignorieren Sie es einfach. In den meisten Fällen weisen wir im Text darauf hin.

5.1.1 Confixx für Administratoren

Den Confixx-Administrationsbereich erreichen Sie über Ihren Webbrowser. Ist Ihr Server bereits vorkonfiguriert, erhalten Sie eine Adresse, die so aussehen könnte wie diese

Das unterscheidet sich nur geringfügig zwischen den Providern. Während bei 1&1, Domainbox und Server4free der Dienst über den Port 80 (http) zu erreichen ist, müssen Sie bei IP-Exchange den Port 8080 (also https) verwenden. Anschließend werden Sie nach Ihren Zugangsdaten gefragt. In der Regel heißt der Benutzer »Administrator« (achten Sie auf die Groß- und Kleinschreibung!), als Passwort verwenden Sie das Ihnen zugesendete Administratorpasswort. Bei 1&1 und S4f können Sie es im Kundenkonfigurationsmenü einsehen.

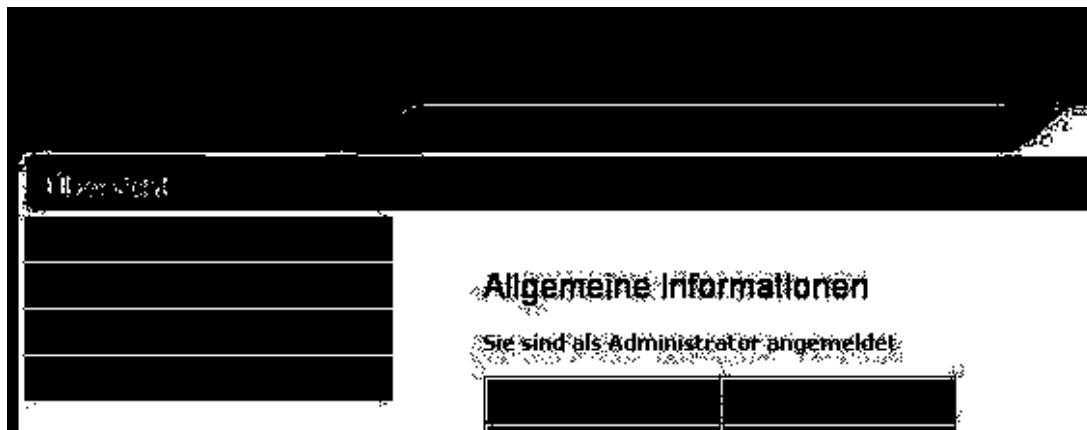


Bild 5.2: Die Administration von Confixx gliedert sich in vier Punkte

Auf der ersten Seite erhalten Sie eine erste Übersicht über den Zustand Ihres Servers. Sollten hier Einträge rot gefärbt sein, dann überprüfen Sie die Einstellungen für Ihre Anbieter.

Passwort ändern

Einer der ersten Schritte, die Sie mit Confixx unternehmen sollten, ist die Vergabe eines neuen Administratorpassworts. Im Menü links finden Sie dazu den entsprechenden Eintrag. Wählen Sie eine lange, nicht erratbare Zahlen-Ziffern-Kombination – am besten mit zwei oder mehr Sonderzeichen, zum Beispiel »od3n.we7\$1«. Dann können Sie recht sicher sein, dass kaum jemand (selbst mit einer Brute Force Attack) Ihr Passwort herausfindet. Übrigens: Das Passwort, das Sie hier vergeben, gilt nur für Confixx. Für den SSH-Zugriff haben Sie ein anderes Passwort.

Allerdings ist dieses Administrator-Kennwort der Generalschlüssel zu allen Confixx- und Webalizer-Türen! Wenn Sie später Anbieter oder Kunden angelegt haben, können Sie als Administrator einfach unter zu Hilfenahme Ihres Kennworts in alle Bereiche des Systems gelangen. Also noch ein Grund, ein schwer erratbares Kennwort zu benutzen. In keinem Fall sollten Sie wie im Handbuch angedeutet das Passwort-Feld leer lassen – also kein Passwort verwenden. Das wäre grob fahrlässig, denn jeder könnte dann schnell

Ihren Server zum Beispiel zum Raubkopieren missbrauchen. Am Monatsende bekommen Sie garantiert eine saftige Traffic-Abrechnung präsentiert. Auch das strafrechtliche Risiko sowie mögliche Imageschäden sind in ihrer Bedeutung nicht zu unterschätzen. Dabei sind Raubkopien noch beinahe als »Kavaliersdelikte« anzusehen. Stellen Sie sich die Folgen vor, wenn der Rootserver zur Verbreitung von Kinderpornografie missbraucht würd.

Sprache/Design

Hier finden Sie eine schnelle Möglichkeit, die Farbgestaltung von Confixx ein wenig zu ändern und die bevorzugte Sprache auszuwählen.

Für Fortgeschrittene gibt es auch die Möglichkeit, das Design von Confixx komplett an die eigenen Wünsche anzupassen. Dazu müssen Sie sich allerdings als »root« per SSH in den Server einloggen und anschließend am einfachsten mit dem Midnight-Commander (mc) drei Vorlagenverzeichnisse, zum Beispiel

in das confixx-Hauptverzeichnis

kopieren. In diesen Verzeichnissen finden Sie CSS-Dateien, die die grundsätzlichen Formatierungen enthalten und jeweils ein Unterverzeichnis namens pics, in dem sich alle Grafiken befinden. Erstellen Sie sich nun einfach unter skins ein neues Verzeichnis, in das Sie die Vorlagen kopieren. Ohne den Midnight-Commander kopieren Sie mit folgenden Zeilen:

Entsprechend natürlich in anderen Verzeichnissen, wenn Ihr Confixx zum Beispiel unter /srv/www/confixx angelegt ist. Im Kapitel zur Confixx-Designanpassung gehen wir noch einmal speziell auf diesen Punkt ein.

Servermeldungen

Eine der wichtigen Informationsquellen sind so genannte LOG-Dateien. In diesen werden von unterschiedlichen Programmen erwähnenswerte Ereignisse eingetragen. Unter Servermeldungen finden Sie Fehler, Warnungen und Hinweise. Die Hinweise können Sie getrost ignorieren. Sie dienen lediglich der Information, zum Beispiel, ob und wann ein neuer Anbieter oder Kunde angelegt wurde. Schon etwas interessanter ist die Liste mit Warnungen. Häufig verstecken sich hinter Warnungen spätere Fehler.

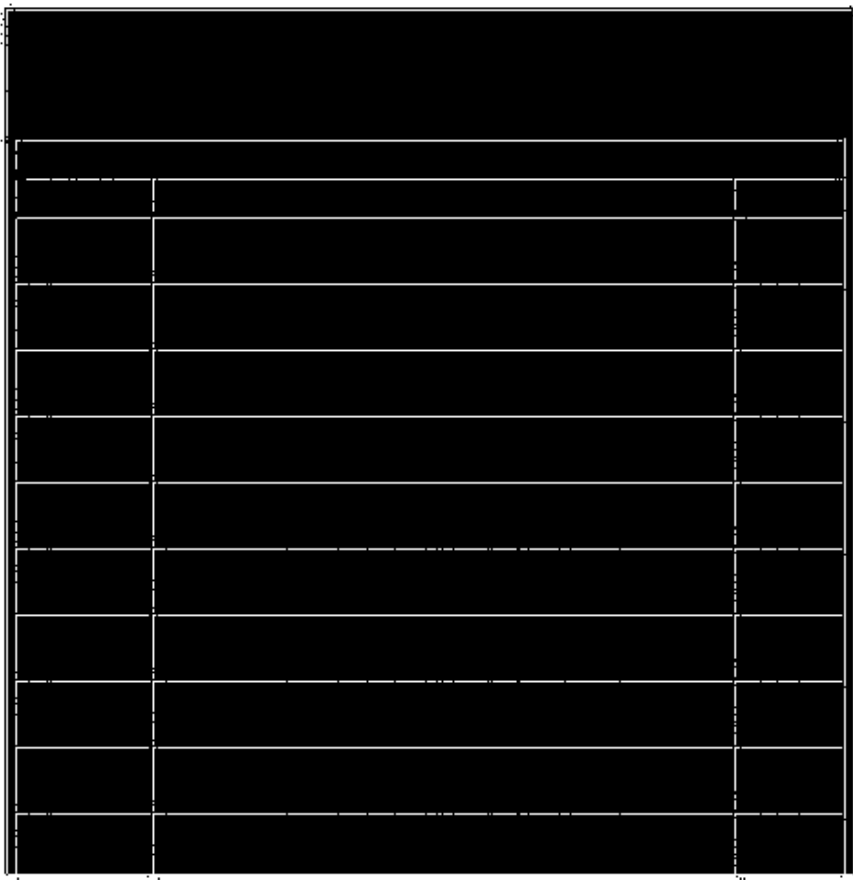


Bild 5.3: Hinter einer harmlosen Warnung kann ein dicker Fehler stecken

Oft ist nicht die letzte Warnung die ausschlaggebende, in unserem Beispiel konnte Confixx eine Tabelle aufgrund eines falschen Leerzeichens in einer Konfigurationsdatei nicht anlegen. Die darauf folgenden Fehler sind nur das Ergebnis des vorangegangenen Problems. In einem solchen Fall wenden Sie sich lieber an den Support Ihres Hosters, außer Sie wissen genau, wo der Fehler zu suchen ist.

Eintragungen in der dritten Kategorie »Fehler« sollten Sie in jedem Fall versuchen, schnell zu klären oder klären zu lassen. Taucht hier eine Meldung auf, dann betrifft das wichtige Funktionen von Confixx, die unter ungünstigen Umständen zu einem Serverabsturz führen können. Ein Fehlereintrag bedeutet auch immer, dass Confixx keine weiteren Änderungen durchführt, um sich selbst zu schützen. Fehler müssen behoben werden.

Im zweiten großen Oberpunkt »Anbieter« erstellen Sie Ihre Wiederverkäufer/Anbieter. Freilich ist ein gewöhnlicher Rootserver kein professionelles System, das für den Weiterverkauf ausgelegt ist, aber Sie können ja auch einigen guten Freunden die Freude machen und ihnen die Möglichkeit eröffnen, mehrere »Kunden« (sprich Internetadressen) bei Ihnen unterzustellen.



Bild 5.4: Hier können Sie Ihre Anbieter verwalten

E-Mail-Setup

Nach dem Anlegen eines Anbieters (siehe unten unter »Anbieter anlegen«) haben Sie die Möglichkeit, die Zugangsdaten sowie weitere Informationen per E-Mail an den neuen Anbieter zu verschicken. Hier erstellen Sie die E-Mail-Vorlage dazu. Interessant sind die Platzhalter, die Sie verwenden können. Damit lassen sich E-Mails personalisieren. Diese werden später automatisch durch die entsprechenden Inhalte ersetzt, vorausgesetzt, Sie haben sie beim Einrichten angegeben. Die E-Mail-Vorlage lohnt sich aber nur, wenn Sie planen, vielen Anbietern einen Zugang zu Ihrem Server einzurichten.

Index-Setup

Das kennen Sie: Sie erraten wild eine Website und rufen diese auf. Doch statt der Site erscheint ein freundlicher Hinweis, dass an dieser Stelle bald eine neue Website entsteht. Diesen Platzhalter können Sie hier beim Index-Setup erstellen. Gestalten Sie sich einfach in einem HTML-Programm (wie beispielsweise Dreamweaver) die gewünschte Seite und kopieren Sie den entstandenen Code in dieses Fenster. Zum Personalisieren können Sie dann die bekannten Platzhalter einfügen. Achtung: Wenn Sie auf der Site Grafik verwenden möchten, dann achten Sie darauf, dass die Grafikdaten mit einer absoluten Adresse angesprochen werden, sonst erscheinen nur unschöne Kästchen mit fehlenden Bildern.

Die Datei kann später vom Endkunden überschrieben werden, wenn er seine eigene Internetseite auf den Server lädt.

Rundschreiben

Hier können Sie schlicht eine E-Mail an alle Ihre Anbieter schreiben. Nachdem Sie auf »Weiter« geklickt haben, werden alle Anbieter aufgelistet. Entfernen Sie nun die Empfänger aus der Liste, die Ihre Mail nicht erhalten sollen.

Anbieter anlegen

Zentraler Punkt des Administrationsbereichs ist das Anlegen eines neuen Anbieters. Im ersten Schritt legen Sie die Leistungen fest, über die Ihr zukünftiger Anbieter verfügen kann.



Bild 5.5: Ressourcenzuweisung an Anbieter

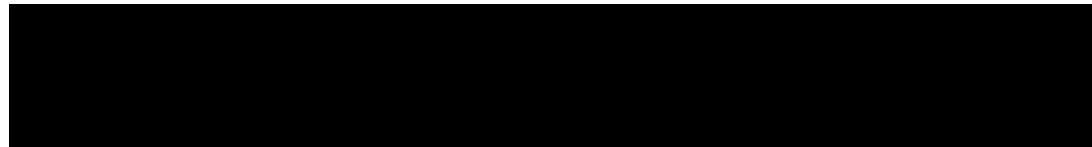
Was Sie hier angeben, unterliegt ganz Ihrem Geschick für interessante Wiederverkaufsprodukte. Bedenken Sie, dass bei Gigabyte-Angaben immer 1024 Megabyte gemeint sind. Und denken Sie daran, dass ein Server nicht unendlich leistungsfähig ist. In Sachen Sicherheit gibt es einige Punkte, die Sie fremden Anbietern besser nicht zu Verfügung stellen: Dazu gehört der externe MySQL-Zugriff und das DirectoryListing. Die Standard-CGI-Skripts sollten Sie nur freigeben, wenn Sie sich ganz sicher sind, dass keines der Skripts zum Beispiel für den SPAM-Versand zu gebrauchen ist (ältere formmail-Skripts sind anfällig und werden von SPAM-Versendern in allen erdenklichen Schreibweisen aktiv gesucht!).

Im zweiten Schritt geben Sie die Daten des Anbieters ein. In der Regel können Sie sich diese Arbeit sparen – außer Sie vermieten Ihren Server wirklich (entgegen all unseren Warnungen) weiter. Die Angaben erschienen dann alle auf der Anbieter-Startseite. Unten finden Sie übrigens (wie später bei den Endkunden auch) drei Felder, die Sie

beliebig benennen können. Bei den »Kunden« bietet sich in diesen Feldern die Angabe der Zahlungsmodalitäten an.

Im dritten Einrichtungsschritt können Sie jedem Anbieter eine eigene IP-Adresse zuordnen. Unter dieser IP-Nummer sind dann gewöhnlich die Kunden des Anbieters zu erreichen. Das ist insbesondere dann sinnvoll, wenn Sie als Server-Anbieter im Hintergrund bleiben möchten. Um für den Anbieter die Illusion eines eigenen Servers perfekt zu machen, sollte seine IP-Nummer noch mit einem entsprechenden Reverse-DNS-Eintrag versehen werden. Ebenfalls nicht ganz unwichtig: Sie können jedem Anbieter ein eigenes Confixx-Design zuordnen. Dieses Design erhalten auch seine Kunden (dieses Feature gibt es nur in der Version 2 Pro – Server4free-Premium-Edition-Nutzer können das nicht). Sobald Sie nun auf »Weiter« klicken, wird der Anbieter angelegt.

Im vierten und letzten Schritt erhalten Sie die Anbieterkennung (res1..resX) und das Zugangskennwort. Beides könnten Sie – dazu verleitet das E-Mail-Formular darunter – gleich per E-Mail an den neuen Anbieter schicken. Lassen Sie das! Ihre Mail wird als offener Text versendet. Wie leicht sich eine ungeschützte Mail auslesen lässt, wissen Sie mittlerweile selbst. Wenn nicht, dann lässt Sie sicher ein kurzer Blick in das Verzeichnis `//var/spool/mail` erschauern. Hier finden Sie alle Mails unverschlüsselt vor.



Anbieter ändern

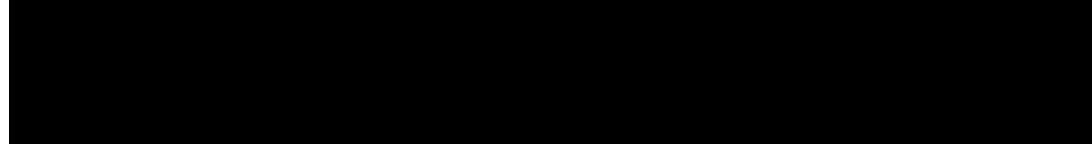
Schnell erläutert: Hier können Sie alle Einstellungen ändern, die Sie vorher unter »Anbieter anlegen« getroffen haben. Zusätzlich lassen sich Anbieter löschen oder sperren. Das Sperren eines Anbieters hat allerdings weitreichende Folgen:

- Ihr Anbieter kann keine weiteren Einstellungen in Confixx vornehmen,
- seine Kunden werden von Confixx ausgeschlossen,
- die Kunden-Webseiten sind nicht mehr erreichbar,
- die Kunden haben keinen FTP-Zugriff mehr,
- E-Mails können nicht abgeholt werden, werden aber nach wie vor empfangen und nicht gelöscht.
- Heben Sie die Sperrung auf, kann der Betrieb sofort ohne Einschränkungen aufgenommen werden. Das Sperren und Entsperren eines Anbieters kann (je nach Einstellung der Update-Intervalle – dazu etwas später) einige Minuten dauern.

Kundenzuordnung

Jeder Anbieter »besitzt« seine Kunden. Diese Zuordnung können Sie auf zwei Arten verändern. Entweder Sie ordnen alle Kunden eines Anbieters einem anderen zu, oder Sie

»verschieben« einzelne Kunden. Da beim Ändern der Zuordnung sein Zugang erhalten bleibt (alle Kennwörter und Benutzernamen bleiben), merkt der Kunde nichts – außer der neue Anbieter hätte ein anderes Design der Confixx-Oberfläche oder eine andere IP-Adresse. Das kann nur dann zu kleineren Problemen führen, wenn Ihre Kunden den Server direkt über die IP-Adresse und nicht über den Domainnamen ansprechen.



MySQL

- Ihre Anbieter können Kunden MySQL-Datenbanken freigeben. Diese sollten von vornherein nur für den lokalen Zugriff freigegeben sein, denn hier gilt die Regel: Je weniger Freigaben nach außen, um so sicherer der Server. Es gibt allerdings eine Ausnahme: Haben Sie mehrere Server und einer davon ist als Datenbankserver ausgewählt (meist wegen höherer Datensicherheit oder besserer Backupmöglichkeit), dann müssen Sie die Datenbanken freigeben.



Bild 5.6: Datenbanken für den externen Zugriff freigeben

In wenigen Fällen kann es vorkommen, dass der externe MySQL-Zugriff trotzdem nicht funktioniert. Dann loggen Sie sich per SSH in Ihren Server ein und sehen nach, ob im Verzeichnis `/etc/MySQL/my.cnf` ein Eintrag `skip-networking` existiert. Wenn dem so ist, kommentieren Sie ihn aus – d.h. setzen Sie ein `#` davor. Dann müssen Sie nur noch

MySQL neu starten und der externe Zugriff sollte möglich sein – allerdings für alle Datenbanken.

Bis jetzt haben wir nur oberflächliches erledigt – nun wird's spannender: Unter dem Oberpunkt »Einstellungen« sind die wichtigsten Serverparameter zusammengefasst. Falsche Werte können hier unter ungünstigen Umständen zu erheblichen Funktionsstörungen oder sogar zum Stillstand des Servers führen.

Datenbanken

Wenn Telnet oder SSH auf dem Server freigegeben ist, kann sich ein Endkunde mit einem entsprechenden Telnet- oder SSH-Client in die MySQLKonsole einloggen. Die Zugangsdaten, User, Passwort und Host, geben Sie auf dieser Seite an. Diese Daten werden beim Endkunden angezeigt. Wenn es keinen besonders dringenden Bedarf für einen SSH- oder Telnet-Zugriff gibt, sollen Sie hier nichts eintragen, denn alle Arbeiten am MySQL können die Kunden bequemer mit PhpMyAdmin erledigen.

Auf den meisten Servern ist phpMyAdmin bereits installiert. Unter diesem Punkt können Sie bequem einstellen, welcher verwendet werden soll. Das ist besonders praktisch, wenn Sie auf eine neuere Version umstellen. Installieren Sie einfach die neue Version in einem parallelen Verzeichnis und stellen Sie dann erst mit einem Eintrag um, wenn alles funktioniert.

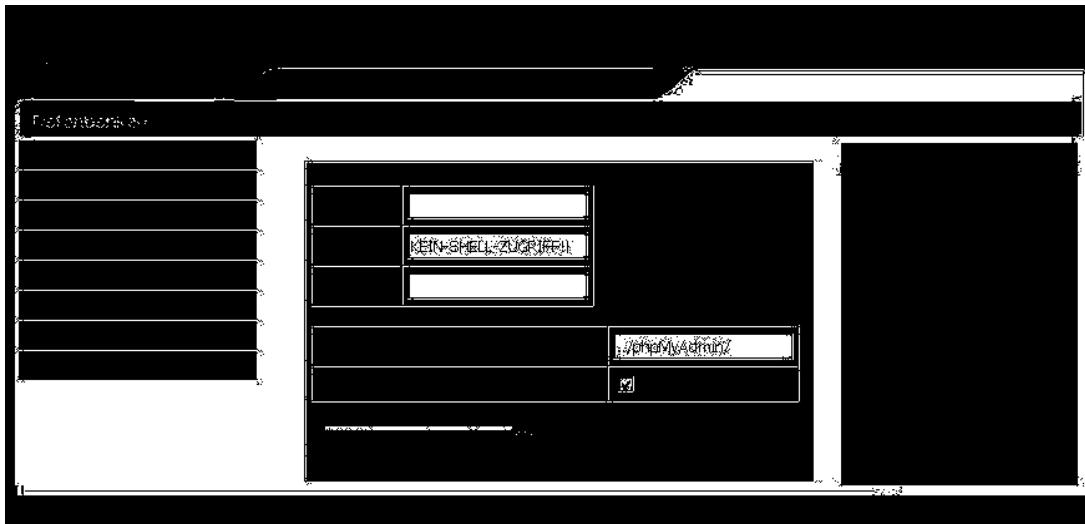


Bild 5.7: Vergeben Sie keinen Shell-Zugriff auf die MySQL-Datenbank

IP-Adressen

Jeder Internetserver hat eine IP-Nummer. Mit so genannten virtuellen Servern, wie sie Apache bereitstellt, können sich mehrere Internetpräsenzen eine IP teilen. Unter Confixx heißt diese Nummer »Standard-IP«. Allerdings können Sie auf einem Server auch mehrere IP-Adressen verwalten. Weitere IP-Nummern können nützlich sein, um mehrere Anbieter zu unterscheiden oder den Server-Anbieter zu verschleiern. Wie dem auch sei: Unter Confixx/Einstellungen/IP-Adressen können Sie einem Anbieter weitere IP-

6 Wenn nichts mehr geht

Trotz aller Vorsicht – irgendwann kommt garantiert der Zeitpunkt, wo Ihr System nicht mehr das tut, was Sie von ihm verlangen. Dazu müssen Sie nicht einmal offensichtliche Fehler begehen. Denn das übernehmen die auf dem Server laufenden Programme gern für Sie. Software ohne Bugs gibt es bekanntlich nicht. Deshalb verrät Ihnen das folgende Kapitel, wie Sie für den Fall des Falles vorsorgen, was im Ernstfall zu tun ist und wie Sie aus den Fehlern (aus Ihren oder denen der Software) lernen.

6.1 Zur Vorsorge: Backups

In den bisherigen Kapiteln des Buches haben Sie eine Menge über Linux im Rootserver-Einsatz gelernt und Ihre Kenntnisse schon eingesetzt. Das hat Ihnen vielleicht sogar Spaß gemacht. Wie viele Stunden haben Sie daran gearbeitet? Stellen Sie sich nun vor, aus irgendwelchen Gründen würde all Ihre Arbeit vernichtet. Wie reagieren Sie? »Macht nichts, dann mal wieder alles von Anfang an, denn schließlich macht ja die Übung den Meister«? Nun, bei den meisten werden sich Unmut und sogar vielleicht ein wenig Verzweiflung breit machen.

Doch der potenzielle Verlust bei einem Server-Crash geht ja über die in die Konfiguration des Servers investierte Arbeitszeit hinaus. Stellen Sie sich den Verlust vor, den Sie ertragen müssten, wenn der Daten-GAU irgendwann in der Zukunft passiert. Neben der zerstörten Konfiguration könnten dann auch Daten verloren gehen, die für Sie einen wirtschaftlichen oder persönlichen Wert haben.

Leider gibt es viele Ursachen für einen Datenverlust. Am häufigsten ist ein Hardwaredefekt. Stirbt die Festplatte, sind mit einem Schlag alle Daten verschwunden. Stirbt sie einen langsamen Tod, gehen Daten oft auch bruchstückweise und schleichend verloren. In diesem Fall kommt es meist irgendwann zu einem Systemabsturz. Dagegen gibt es nur einen Schutz: ein gutes Backup.

Selbst der Einsatz von Hochverfügbarkeits-Hardware wie zum Beispiel eines RAID-Festplattenverbunds ersetzt auf gar keinen Fall ein gutes Backup. Selbst gespiegelte Festplatten können – so es Murphy und der Teufel wollen – gleichzeitig sterben. Das haben wir schon erlebt. Das System wollte einfach nicht mehr starten. Selten war ein gutes Backup so wertvoll.

Damit Sie auch auf der sicheren Seite sind, stellen wir Ihnen neben den Grundbegriffen einige intelligente Konzepte für Backup-Strategien vor. Schließlich werden wir noch mehrere Möglichkeiten im Detail erklären, wie Sie für Ihren Rootserver eine ideale Backup-Lösung erarbeiten. Denn mit einem guten Backup schläft es sich einfach ruhiger.

6.1.1 Definition und Ziele eines Backups

Backup ist nicht gleich Backup. Ein einmaliges Sichern aller Daten gilt nicht als Datensicherung. Bemühen wir doch einmal eine akademische Definition des Backup-Begriffes:

»Backup ist ein in regelmäßigen Intervallen wiederholtes Archivieren von Daten auf einem logisch, physikalisch und örtlich unabhängigen Medium, mit dem Ziel, einen möglichen Datenverlust und Ausfallzeiten eines Systems oder Dienstes so gering wie möglich zu halten«

Wie die Definition besagt, müssen Sie sich Gedanken machen, wann und in welchen Intervallen ein Backup durchzuführen ist, um den Datenverlust so gering wie möglich zu halten. Es nutzt Ihnen nichts, wenn Sie zum Beispiel ein Backup nur alle zwei Tage durchführen, Sie aber täglich wichtige Daten geändert haben, vor allem weil ein Datenverlust immer zum ungünstigsten Zeitpunkt zu erwarten ist.

Ziel bei der Durchführung eines Backups ist das Archivieren von Daten so zeitnah wie möglich an deren Erstellung oder Veränderung. Daraus ergibt sich der Wunsch, das Backup möglichst stündlich durchzuführen. Aber das kommt in der Praxis wirklich nur in besonderen Ausnahmefällen vor und wäre ausgesprochen schwierig – technisch und logistisch – durchzuführen. Wählen Sie ein geeigneteres Intervall: In der Regel genügt ein tägliches oder 12-stündliches Backup.

Außerdem müssen Sie sich überlegen, wann im Laufe eines Tages das Backup durchgeführt werden soll. Sie sollten einen Backup-Lauf nur starten, wenn der Server am wenigstens von anderen Diensten beansprucht wird.

Des Weiteren müssen Sie das Medium, auf dem die archivierten Daten abgelegt werden sollen, sorgfältig nach mehreren Aspekten auswählen. Denn es nutzt ihnen nichts, wenn Sie zwar ein einwandfreies Backup haben, aber die Backup-Daten bei einem Daten-GAU gleich mit verloren gehen – oder, was noch frustrierender ist, wenn Sie ein vorhandenes Backup nicht wiederherstellen können. Doch was ist überhaupt ein Backup-System?

»Ein Backup-System ist die Gesamtheit der Software und Hardware, die das Backup durchführt und bei Bedarf die Wiederherstellung von Daten ermöglicht.«

6.1.2 Backup-Medien

Wie schon erwähnt, ist die Wahl des Backup-Mediums von essenzieller Bedeutung. Folglich ist eine Reihe von Kriterien wichtig, nach denen ein Backup-Medium ausgewählt werden sollte.

- Logische, physikalische und örtliche Unabhängigkeit
- Ausreichend Speicherplatz

- Geringe Kosten
- Ausreichende Übertragungsrate, auch für die Wiederherstellung von Daten
- Zugriffssicherheit gegenüber Dritten

Die am häufigsten verwendeten Backup-Medien sind nach wie vor Wechselmedien wie zum Beispiel Tapes, CD-R oder neuerdings auch wiederbeschreibbare DVD. Diese erfüllen prinzipiell alle oben genannten Kriterien – aber die dafür erforderliche Hardware ist bei den meisten Rootservern nicht verfügbar. Was noch schwerwiegender ist: Sie müssen die Wechselmedien auch wechseln, damit sie ihrem Namen gerecht werden. Die wenigsten Rootserver-Admins haben ihre Provider aber direkt vor der Haustür.

Die erste Idee für einen Backup-Platz könnte deshalb die eigene Festplatte des Rootservers sein. Die verfügt über genügend Kapazität, ist sehr schnell und verursacht keine Zusatzkosten. Irrtum! Stirbt Ihre Festplatte (was leider gar nicht so selten ist), können Sie Ihr Backup auch gleich vergessen.

Daneben gibt es natürlich eine Reihe anderer Möglichkeiten, Ihr Backup tatsächlich sicher zu verwahren. Da wäre zum Beispiel die zweite Festplatte im Server. Dumm nur: die meisten Rootserver werden nur mit einer Festplatte ausgestattet und in puncto Sicherheit wäre eine Zwei-Festplatten-Lösung auch nicht wirklich optimal. Da beide Platten im Dauerbetrieb laufen, ist es ziemlich wahrscheinlich, dass beide Platten im gleichen Zeitraum ausfallen. Murphy eben: Das passiert tatsächlich! Und dann ist auch das schöne Backup schon wieder weg.

Eine weitere Lösung wäre, sich die gesicherten Daten via E-Mail nach Hause zu schicken. Allerdings: Haben Sie genügend Speicherplatz auf Ihrem E-Mail-Account? Holen Sie Ihre E-Mails regelmäßig ab, und wer holt die Post, wenn Sie im Urlaub sind? Außerdem: Möchten Sie wirklich ab und an ein paar Gigabyte als Mail bekommen? Selbst mit 1,5-MBit-DSL – das macht die Leitung unter Umständen für Stunden dicht. Alles in allem: richtig unpraktisch!

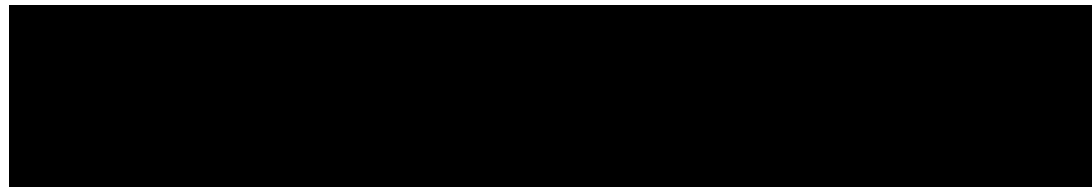
Rekapitulieren wird kurz: Kein Wechselmedienlaufwerk ist verfügbar, das System verfügt nur über eine Festplatte, das Zumailen des Backups nach Hause ist ab einer gewissen Größenordnung Unfug – da bleibt wohl nur noch der schwere Gang zum professionellen (und teuren) Backup-Anbieter.

Es sei denn, Sie können auf eine besonders interessante Lösung für Ihr Problem ausweichen: einen netten Backup-Partner. Mit etwas Glück kennen Sie jemanden, der auch einen Rootserver betreibt, zum Beispiel aus dem Freundes- oder Bekanntenkreis, oder Sie finden jemandem in einem Forum, das sich speziell mit Rootservern beschäftigt und dem Sie nach ein paar persönlichen Treffen vertrauen. Sie können sich dann gegenseitig einen Zugang und ausreichend Speicherplatz zur Verfügung stellen, um Backups zu speichern. Hält Ihr Bekannter oder Freund nichts von Backups, dann sollten Sie ihn –

auch um seinetwegen – dringend dazu überreden (am besten, Sie schenken ihm dieses Buch).

Es gibt allerdings einen Haken an der Sache: Die Durchführung der Backups erzeugt Traffic und der kostet richtig Geld. Haben Sie das Glück, dass Ihr Backup-Partner seinen Rootserver im gleichen Rechenzentrum hostet, so fragen Sie bei Ihrem Betreiber, ob der Traffic, im Rechenzentrum (interner Traffic) berechnet wird. Die meisten Firmen verrechnen nur externen Traffic, also den Traffic, der nach außen geht.

Abgesehen vom Problem mit den Traffic-Kosten – haben Sie schon daran gedacht, dass ihr Backup-Partner Zugriff auf die gesicherten Daten hat? Es könnte aus Versehen oder mutwillig Ihr Backup löschen. Was noch schlimmer ist, Ihr Backup-Partner kann Ihre Daten einsehen. Es ist zwar technisch bei der Backup-Erstellung kein Problem, die Daten zu verschlüsseln. Aber wenn Sie einen Totalausfall erleiden und alle Daten für die Entschlüsselung des Backups mit ins Nirwana katapultiert werden, haben Sie ein vorbildliches Backup, auf das Sie nicht mehr zugreifen können. Schöne Pleite! Dagegen hilft es nur eins: im Vertrauen auf den Backup-Partner auf Verschlüsselung zu verzichten.



Wer selbst für internen Traffic zahlen muss, hat trotzdem keinen Grund zu verzweifeln. Es gibt Möglichkeiten, den Datenverkehr durch Wahl der richtigen Backup-Art sehr gering zu halten.

6.1.3 Backup-Prinzipien und -Arten

Es gibt zwei Prinzipien, nach denen ein Backup durchgeführt werden kann: Pull- oder Push-Backup. Das Pull-Backup wird oft von professionellen Backup-Anbietern eingesetzt. Auf Ihrem Server läuft dann ein kleines Programm, Backup-Agent genannt. Der Backup-Anbieter baut eine Verbindung zum Backup-Agent auf und holt alle zu sichern Daten von Ihrem Server ab. Somit liegt es im Verantwortungsbereich des Backup-Anbieters, das Backup komplett durchzuführen. Der Nachteil: Sie haben keine direkte Möglichkeit, die Originaldaten wiederherzustellen. Sie müssen dazu erst bei Ihrem Backup-Anbieter anrufen und um eine Wiederherstellung bitten. Richtig: Der Wiederherstellungs-Service kostet natürlich zusätzlich Geld.

Wir beschränken uns daher hier auf das Push-Backup, bei dem Sie die Kopie selbst erstellen und auf ein Backup-Medium »schieben« (= push) – und bei Bedarf die gesicherten Daten wiederherstellen.

Nun müssen Sie noch entscheiden, welche Daten wann zu sichern sind. Diese Überlegung ist wichtig, wenn Sie drauf angewiesen sind, so wenig Traffic wie möglich zu erzeugen. Mit dem Vollbackup werden zwar alle Daten vollständig gesichert, aber es erzeugt mächtig viel Traffic, und keine noch so gute Komprimierung kann die falsche Wahl der Backup-Art wettmachen.

Begrenzen Sie das Backup besser auf die Serverkonfiguration und die Anwenderdaten, die geändert oder neu angelegt wurden. Das ist der kleine Bruder des Vollbackups, denn es ist ausgesprochen verschwenderisch und manchmal auch recht schwierig, alle Daten auf einer Festplatte automatisiert zu sichern (zum Beispiel bei gerade geöffneten Dateien). Wenn Sie aber der Daten-GAU erwischt, muss der Rootserver ohnehin neu installiert werden, und damit ist die Sicherung der Programme ohnehin überflüssig. Was Sie aber brauchen, um einen neu installierten Rootserver schnellstmöglich in Betrieb zu nehmen, sind Konfigurations-Files und die Anwenderdaten.

Ein geringeres Traffic-Volumen wird vom differenziellen Backup erzeugt. Das Verfahren bietet ebenfalls den maximalen Schutz im Falle eines Daten-GAUs. Bei diesem Verfahren machen Sie zum Beispiel nur einmal pro Woche ein Vollbackup – an den übrigen Tagen werden aber nur die Daten gesichert, die seit dem Vollbackup geändert wurden. Der Vorteil: Die tägliche Datenmenge ist erheblich geringer. Sie müssen aber genau überlegen, welche Backup-Teile wie lange aufzubewahren sind. Die einzelnen Teile sind nur brauchbar, wenn Sie auch ein Vollbackup als Basis dafür haben.

Die tägliche Datenmenge eines differenziellen Backups lässt sich noch weiter senken, wenn Sie ein inkrementelles Backup durchführen. Beim inkrementellen Backup werden nur die Daten gesichert, die sich seit dem letzten Backup verändert haben, und nicht alle Daten, die seit dem letzten Vollbackup verändert wurden. Diese Backup-Art, gekoppelt mit einem leistungsfähigen Kompressionsverfahren, erzeugt ein Minimum an Traffic. Einen Nachteil gibt es aber: Müssen alle gesicherten Dateien wiederhergestellt werden, müssen Sie zuerst das Vollbackup wiederherstellen und danach in chronologischer Reihenfolge jedes einzelne Teilbackup. Dies ist zwar aufwändig, kommt dafür aber selten vor.

6.1.4 Backup-Systeme

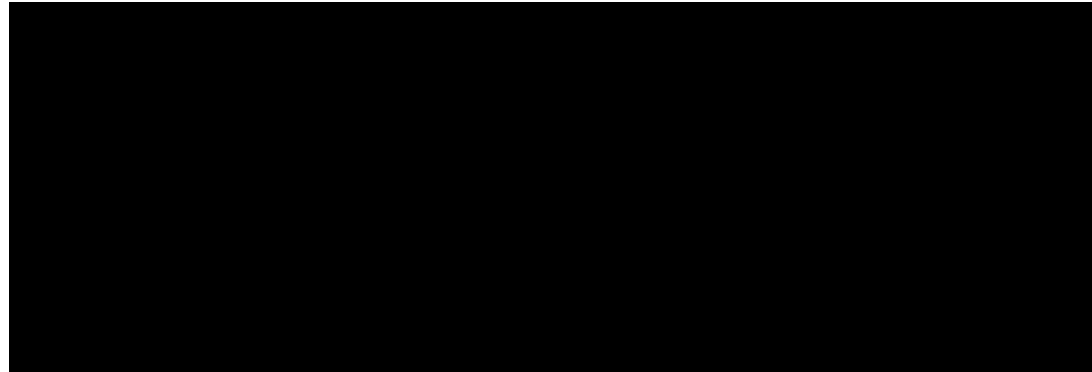
Genug der grauen Theorie: Kümmern wir uns um die Planung, Einrichtung und Durchführung eines auf Sie zugeschnittenen Backup-Systems.

Welche Dateien sichern?

Als Erstes müssen Sie festlegen, welche Daten gesichert werden sollen. Bei Linux ist das einfach: Alle Konfigurationsdateien jeder Standardsoftware sollten sich in /etc und darunter liegenden Verzeichnissen befinden. Haben Sie eine Software installiert, bei der Sie sich nicht sicher sind, ob ihre Konfigurationsdateien sich auch an den Standard halten, können Sie dies sehr schnell mit dem rpm-Befehl herausfinden. Der rpm-Befehl ist nur unter SuSE und RedHat verfügbar.

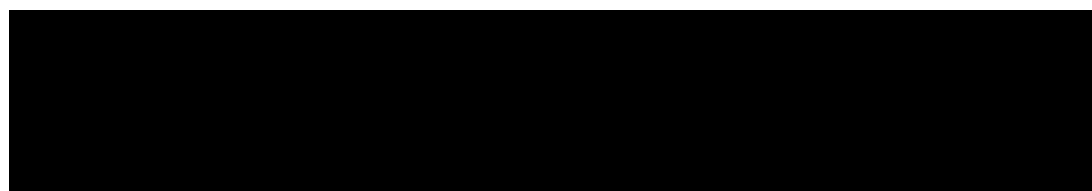
Als Beispiel betrachten wir das apache2-Paket, dabei handelt es sich um Ihren Webserver. Sie können natürlich auch jedes andere Rpm-Paket so überprüfen. Geben Sie unter der Shell das folgende Kommando ein.

Wenn das apache-Paket richtig installiert ist, bekommen Sie folgende Ausgabe:



Wie Sie sehen, befinden sich alle Konfigurationsdateien, die Ihren Webserver betreffen, im /etc-Verzeichnis. Leider gibt es unter Debian bei dem Kommando »apt« (Advanced Package Tool) nicht die Möglichkeit, sich die Konfigurationsdateien eines Paketes anzeigen zu lassen. Sie können aber beruhigt davon ausgehen, dass auch unter Debian alle Konfigurationsdateien sich brav im /etc-Verzeichnis befinden.

Außerdem müssen Sie natürlich auch die Anwenderdaten sichern, diese befinden sich in der Regel im /home-Verzeichnis. Benutzen Sie eine abweichende Konfiguration (zum Beispiel als Server4free-Kunde), müssen Sie die abweichenden Verzeichnisse auch mit in das Backup aufnehmen. Dann sollten Sie auch nicht vergessen, die Daten des Users »root« mitzunehmen. Denn der User »root« hat sein eigenes Homeverzeichnis /root.



Klar, man könnte noch viel mehr Interessantes über ein Backup sichern, aber vieles ist weder den Speicherplatz noch den Traffic wert: temporäre Dateien zum Beispiel (Endung .tmp). Bei Logdateien scheiden sich schon wieder die Geister (Verzeichnis /var/log). Zur reinen Serverfunktion sind sie nicht wirklich nötig, aber wenn der Speicherplatz ausreicht und Traffic kostenlos ist, kann ein Backup der Logdateien (_log oder .log) schon Sinn machen, um später eventuell auf die Ursache des Crashes zu schließen oder Crack-Aktivitäten nachzuweisen (wenn es ein schlechter Cracker war).

Backups erzeugen mit Tar

Eine Kleinigkeit bleibt noch. Stellen Sie sich nur mal kurz vor, Sie müssen ein Backup mit Tausenden von Dateien wiederherstellen. Sie können alle Dateien restaurieren und

stellen dann fest, dass die Attribute der Files nicht mehr stimmen. Sie müssten nun bei allen Dateien von Hand den Besitzer, die Besitzergruppe und die Zugriffsrechte setzen.

So – jetzt kann es aber losgehen. Sie fragen sich bereits, mit welchem Programm man allen Anforderungen gerecht werden kann? Sie kennen das Programm wahrscheinlich schon: Allen Anforderungen genügt nämlich das Programm mit dem schlicht klingenden Namen Tar (Tape Archive). Bandarchive? Der Name kommt aus den frühen Computerzeiten, als nur Bänder (Tapes) als Massenspeicher zur Verfügung standen.

Tar ist ein mächtiges Werkzeug, wenn es um Datensicherung geht, und es besitzt eine Unmenge an Optionen und Parametern. Die für Sie interessantesten Parameter sind:

- c = erzeuge ein neues Archiv
- x = extrahiere eine Datei oder ein Verzeichnis aus dem Archiv
- p = sichere alle Rechte der Dateien (damit werden Besitzer, Besitzergruppen usw. mit in das Backup aufgenommen)
- z = komprimiere das Backup mit dem gzip-Algorithmus
- v = liste alle gesicherten Dateien ausführlich mit ihrem absoluten Dateinamen. Sie können sich die Auflistung per Mail zusenden lassen, damit Sie wissen, welche Dateien gesichert wurden.
- f = gibt das erzeugte Backup nicht auf den Bildschirm aus, sondern schreibe es in eine Datei
- totals = die Größe des Backups auf den Bildschirm aus

Wenn Sie mehr über Tar erfahren wollen, lesen Sie doch mit dem Befehl »man tar« die Manpage.

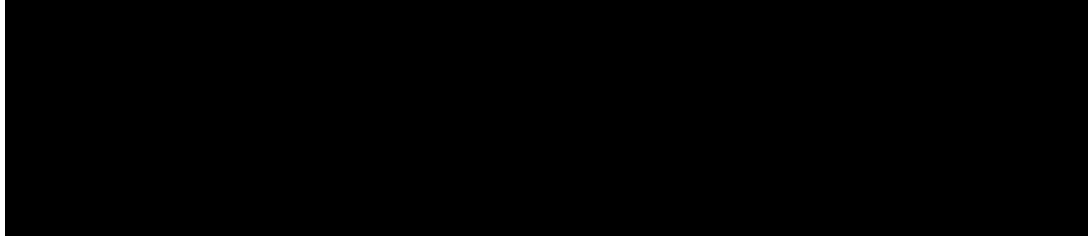
Mit diesem Kommando erstellen Sie ein Vollbackup:

(\$Backup-Datei: Die Backup-Datei muss die Endung .tar.gz haben, \$Verzeichnisse: die Liste der Verzeichnisse, die gesichert werden sollen, zum Beispiel: /etc /root /home)

Dateien wiederherstellen mit Tar

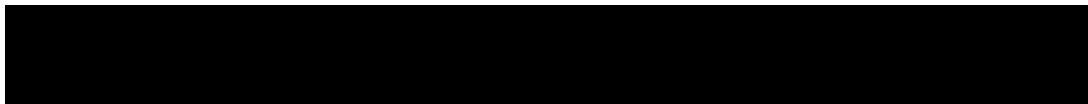
Haben Sie bereits ein Backup mit Tar erstellt, sollten Sie überprüfen, ob sich Ihr Backup eignet, um Daten auch wiederherzustellen. Sie haben bereits analysiert, welche Dateien zu restaurieren sind. Deshalb müssen Sie nun in erster Linie herausfinden, ob die gewünschten Dateien sich auch in einem Backup-File befinden. Prinzipiell brauchen Sie also eine Möglichkeit, alle in einem Backup gesicherten Dateien aufzulisten.

Dies bewerkstelligt der folgende Befehl:



Die Liste aller Dateien in einem Backup-File ist gewöhnlich sehr lang. Da wäre doch ein Werkzeug ganz praktisch, mit dem Sie schneller herausfinden können, ob sich die gewünschte Datei tatsächlich in Ihrem Backup-File befindet. Am besten nutzen Sie dazu das Kommando »grep«. Sie leiten einfach die vollständige Bildschirmausgabe des obigen tar-Befehls mit Hilfe einer Pipe (|) an Grep um.

Grep untersucht jede Zeile der tar-Ausgabe nach einem Muster. Sobald Grep eine Zeile findet, deren Inhalt dem Suchmuster ganz oder teilweise entspricht, gibt das Tool die Zeile unverändert auf den Bildschirm aus. Im folgenden Beispiel suchen wir nach der Datei fstab:



Damit haben Sie nun erfolgreich festgestellt, dass sich die gewünschte Datei wirklich im Backup-File befindet. Es kann also jetzt ans Extrahieren gehen. Um eine Datei aus dem Backup-File zu restaurieren, benötigen Sie den vollen Dateinamen (inklusive Pfad), unter dem die Datei im Archiv abgelegt ist (in unserem Beispiel etc/fstab). Mit dem folgenden Kommando sind Sie nun in der Lage, die gewünschte Datei wiederherzustellen:



Als \$Dateinamen müssen Sie hier den vollen Namen angeben, also etc/fstab. Aber Vorsicht: Eine bereits existierende Datei gleichen Namens wird gnadenlos überschrieben.

Sie können mit diesem Kommando übrigens auch mehrere Dateien gleichzeitig wiederherstellen, indem Sie die durch Leerzeichen getrennten Dateinamen nacheinander dem tar-Kommando übergeben.

Wurden auf Ihrem Server ganze Verzeichnisse unbrauchbar gemacht, ermöglicht es Ihnen das folgende Kommando, ganze Verzeichnisbäume wiederherzustellen. Dabei werden alle Dateien und Unterverzeichnisse mit deren Inhalt restauriert.



\$Verzeichnis muss mit vollem Namen angegeben werden (etwa etc/zebra/). Auch hier gilt: Alle existierenden Dateien und Unterverzeichnisse im Zielverzeichnis werden von den Dateien aus dem Backup ohne Rückfrage überschrieben. Existieren Dateien im Zielverzeichnis, die sich nicht im Backup befinden, bleiben diese immerhin unangetastet. Freilich haben Sie auch hier die Möglichkeit, mehrere Verzeichnisse auf einmal zurückzuholen, indem Sie die gewünschten Verzeichnisse durch Leerzeichen getrennt hintereinander angeben.

Hat Sie trotz aller Vorsichtsmaßnahmen der komplette Daten-GAU ereilt, weil die Festplatte zum Beispiel mit einem lauten Pfeifen das Zeitliche gesegnet hat, muss Ihr Rootserver neu installiert werden. Das System wird Ihnen dann nach einer Neuinstallation ohne jegliche Konfiguration übergeben. Nun können Sie aus dem Vollen schöpfen, sofern Sie vorher wirklich alles kopiert haben. Sie brauchen nur das Vollbackup wiederherzustellen und schon sollte sich Ihr System wieder im ursprünglichen Zustand befinden. Um ein Vollbackup zu restaurieren, starten Sie dieses Kommando:

Ein bisschen Vorsicht ist allerdings geboten: Nur wenn die Neuinstallation mit der gleichen Linux-Distribution und -Version durchgeführt wurde, können Sie wie oben beschrieben verfahren. Allerdings sollten Sie vorher fehlende Programme nachinstallieren.

Erfolgt die Neuinstallation mit der gleichen Distribution, aber auf einem anderen Versionsstand (altes System war zum Beispiel SuSE 7.3, neues System ist SuSE 8.1), ist ein derart schnelles Wiederherstellen nicht möglich. Genauso verhält es sich, wenn die Neuinstallation mit einer anderen Distribution durchgeführt wird. Das einzige, was Sie dann getrost restaurieren können, ist das /home-Verzeichnis mit den Anwenderdaten.

Die Ursache dafür ist simpel: Art und der Ort der Konfiguration unterscheiden sich zwischen den Linux-Distributionen in kleinen, aber feinen Details. Zum Beispiel wird der Start von Diensten unter SuSE 7.3 noch über die Datei /etc/rc.config geregelt. In SuSE 8.1 werden Sie das File einfach nicht mehr finden.

Ein anderes Szenario: Sie haben Ihr System neu installiert, weil die alte Installation nicht mehr funktioniert hatte. Sie können aber nicht eindeutig ausschließen, dass dies nicht an einer fehlerhaften oder defekten Konfiguration lag. Wenn Sie in diesem Fall eine Wiederherstellung per Vollbackup durchführen, kann das dazu führen, dass auch die Neuinstallation im Schnelldurchlauf wieder unbrauchbar wird.

Nun gehen wir mal davon aus, dass Sie das Vollbackup nicht an seinem ursprünglichen Ort wiederherstellen wollen, weil dies zu Konflikten mit einem neuen Betriebssystem führen könnte. Sie können sich trotzdem viel Zeit und Mühe sparen, wenn Sie auf die Konfigurationsdateien aus dem Backup zugreifen. Stellen Sie dazu das /etc-Verzeichnis einfach zum Beispiel innerhalb des /root-Verzeichnisses her. Das Kommando dazu lautet:

Nach diesem Schritt finden Sie im Verzeichnis /root/etc/ alle extrahierten Konfigurationsdateien.

6.1.5 MySQL-Datenbanken sichern

Ein paar Besonderheiten ergeben sich, wenn es um die Sicherung von MySQL-Datenbanken geht. Wie Sie vielleicht bereits wissen, befinden sich die Daten der Datenbank in keinem der oben genannten Verzeichnisse. Sie lagern normalerweise in `/var/lib/mysql`.

Die einfachste Lösung wäre es nun, einfach das Verzeichnis mit ins Backup aufzunehmen. Dies funktioniert aber aus zwei Gründen nicht: Zum einen sind die Dateien der MySQL-Datenbank exklusiv vom MySQL-Server geöffnet und können deshalb nicht kopiert werden. Zum anderen können die gesicherten Dateien nur von der gleichen MySQL-Version verwendet werden. Haben Sie einen Daten-GAU erlitten und Ihr Rootserver muss neu installiert werden, wird es Ihnen aber mit Sicherheit passieren, dass Sie nach dem Neuaufsetzen des Systems auch eine neuere MySQL-Version vorfinden. Somit haben Sie wieder ein einwandfreies Backup mit dem winzigen Makel, dass Sie darauf nicht mehr zugreifen können.

Eine mögliche Lösung zu Problem 1 besteht darin, während des Backups den MySQL-Server zu stoppen und anschließend wieder zu starten. Der Haken: Während des Sicherungsvorgangs steht MySQL dann nicht zur Verfügung. Dabei geht es zwar täglich nur um ein paar Minuten, aber wenn Ihre Website auf MySQL aufbaut und ständig verfügbar sein muss, ist dies keine passende Option.

Der Weg, der gleich beide Probleme löst, besteht darin, alle Daten aus der Datenbank zu extrahieren und nur die derart erhaltenen Daten zu sichern. Das Extrahieren belastet zwar den Server, der Dienst muss aber nicht gestoppt werden. Ein weiterer Vorteil dieser Methode: Sie ist flexibler, denn nicht immer müssen Sie alle Datenbanken aus MySQL wiederherstellen. Es geschieht viel häufiger, dass Daten einer bestimmten Tabelle gelöscht oder beschädigt werden. Hätten Sie nur die Dateien aus dem `/var/lib/mysql`-Verzeichnis gesichert, müssten Sie alle Datenbanken und Tabellen restaurieren – oder keine.

Das Programm, das Daten aus einer MySQL-Datenbank zusammenstellt, heißt `Mysqldump`. Es erzeugt eine Datei, die alle Einträge der Datenbank enthält. Und mehr als das: Es werden auch alle zum Neuaufbau der Datenbank nötigen SQL-Befehle mitgesichert. Haben Sie nur in einer Tabelle Datenverlust erlitten, müssen Sie die durch `Mysqldump` erzeugte Datei nur so verkürzen, dass Sie einzig die gewünschten Daten enthält. Die Wiederherstellung geschieht dann mit den `mysql`-Befehl.

So verwenden Sie `Mysqldump`:

```
($Zieldatei: absoluter Pfad der Sicherungsdatei, zum Beispiel /backup/sqldump.bak)
```

Möchten Sie testen, ob diese Methode bei Ihnen einwandfrei funktioniert, müssen Sie nur den Befehl ohne `»» $Zieldatei«` eingeben. Der Inhalt der Datenbank wird somit auf den Bildschirm ausgegeben und Sie haben einen kurzen Einblick in die Struktur der Sicherungsdatei.

7 Sicherheitsstrategien

Schon in den vorangegangenen Kapiteln haben wir Ihnen gezeigt, wie Sie Ihren Server möglichst sicher konfigurieren. Sicherheit ist aber nicht statisch – neue Programm-lücken werden entdeckt, weiter entwickelte Software bringt garantiert auch bisher unbe-kannte Fehler mit sich. Als Administrator gehört es deshalb zu Ihrem Verantwortungsbereich, grundlegende Sicherheitsstrategien zu beachten und anzuwenden. Das gilt auch, wenn Sie den Server nur als Hobby betreiben, denn ein zu lasches Verhältnis zu diesem Thema kann Ihnen und anderen durchaus erheblichen finanziellen Schaden zufügen. Überlegen Sie nur einmal, was passiert, wenn es einem Hacker gelingt, Ihr System unbemerkt zu einem Großangriff auf Dritte zu missbrauchen. Oder welche Reaktionen Sie erfahren werden, wenn Spammer über Ihren Mailserver Millionen von Werbemails für ihre neue »Teen Sex«-Webpage versenden. In diesem Abschnitt wollen wir Ihnen helfen, der Verantwortung gerecht zu werden.

Auch wenn das nicht beruhigend klingt: Absolute Sicherheit und die Funktionalität Ihres Rootservers, der anderen Dienste im Internet bereitstellen soll, schließen sich leider aus. Sie müssen nun einmal anderen Menschen gewisse Rechte auf Ihrem Server erteilen. Zwar gehört Linux zweifellos dank der offen gelegten Quellcodes zu den am besten studierten Betriebssystemen, doch fehlerfrei ist es damit noch lange nicht. Es kommt hinzu, dass Sie eigentlich nur zwei Klassen von User definieren können: die praktisch rechtlosen Anwender, und die übermächtigen Superuser. Beiden User-Sorten werden wir im Folgenden eigene Abschnitte widmen.

7.1 Manueller Zugriff auf den Server

Am schwierigsten abzusichern ist tatsächlich der physische Zugriff auf Ihren Rootserver: Es handelt sich ja dabei in der Regel um einen Standard-PC mit der üblichen Hardware. Eine bootfähige Diskette oder CD-ROM einlegen, ein kurzer Eingriff ins BIOS, und schon hat ein Angreifer das System unter Kontrolle. Diese Art des Crackens können Sie nicht wirklich verhindern – Sie müssen einfach den Beteuerungen Ihres Providers glauben, dass er sein Rechenzentrum ordentlich absichert (umso wichtiger sind die im vorigen Kapitel besprochenen Vorsorgestrategien).

Was jedoch oft unbeachtet bleibt: Ein böswilliger Schelm muss sich nicht in persona in die Serverräume einschleichen – es genügt allzu oft, dass er dortselbst ebenfalls einen Server besitzt oder sich auf welchem Wege auch immer die Macht über einen dort platzierten Rootserver verschaffen konnte. Denn wenn der Provider sein internes Netz, an dem alle Mietserver angeschlossen sind, nicht genügend abgesichert hat, ist es möglich, den Netzwerkverkehr der anderen Maschinen zu belauschen. Insofern hat es zu Recht zu

Aufsehen geführt, als sich herausstellte, dass eben dies bei einem größeren Anbieter über längere Zeit der Fall war.

Das Problem: Normalerweise reagieren Computer nur auf Netzwerkpakete, die tatsächlich an sie adressiert sind. Mithilfe bestimmter Software, so genannter Sniffer, ist es aber möglich, die Netzwerkschnittstelle des Rechners in einen speziellen Modus zu versetzen, der ganz passend mit »promiscuous mode« betitelt ist. In diesem Modus kann der Computer den kompletten Netzwerkverkehr analysieren und zum Beispiel auf bestimmte Schlüsselwörter lauschen. Wir können nun nicht empfehlen, sich selbst probeweise mit einem Sniffer auf Datenfang zu begeben (unter Umständen verletzen Sie damit auch die AGB Ihres Providers), aber Sie sollten sich des potenziellen Problems bewusst sein und, sollte es tatsächlich auftauchen, Ihrem Anbieter das Vertrauen kündigen. Zumindest können Sie die Fähigkeiten eines Sniffers (etwa »Hunt« oder »Sniffit«) auf Ihrem lokalen Linux-System austesten.

7.2 Die Macht des Superusers

7.2.1 »root« und sein Kennwort

Es gibt einen ganz besonderen Linux-Account: den Superuser, auch »root« genannt. Er hat derartig viele Privilegien, dass Sie mit allen Mitteln verhindern müssen, dass jemand anders in seinen Besitz gelangt.

Als Superuser gelten alle Nutzer mit der speziellen User-ID »0«. Damit wären wir schon bei der ersten potenziellen Sicherheitslücke: Es ist prinzipiell möglich, sowohl den Namen des Superusers zu ändern als auch weitere Superuser hinzuzufügen. Davon sollten Sie tunlichst Abstand nehmen, denn erfahrungsgemäß schmälert das nur die Systemsicherheit. Denken Sie nur an Dritte (etwa Mitarbeiter Ihres Providers), die sich womöglich (zum Beispiel im Fall eines Hardwaredefekts) mit Ihrem System auseinandersetzen müssen und Benutzern außer »root« keine Superuser-Fähigkeiten zutrauen.

Bequemlichkeit versus Sicherheit: Auch wenn Sie des Öfteren als »root« an Ihrem System arbeiten müssen, lassen Sie sich nicht dazu verleiten, ein zu kurzes und damit unsicheres Kennwort zu verwenden. Das Passwort sollte acht Zeichen lang sein, nicht weniger, damit es nicht einfach zu »errechnen« ist. Natürlich sollte sich das Kennwort auch nicht einfach erraten oder ausprobieren lassen – Wörter aus dem Duden scheiden damit schon einmal aus.

Am sichersten sind die geheimen Codes, wenn Sie ganz zufällig aus groß- und kleingeschriebenen Buchstaben, Zeichen und Ziffern zusammengesetzt sind. Solche Passwörter haben nur den kleinen Nachteil, dass sie schwer zu merken sind. Das führt dann oft dazu, dass sich Administratoren aus Bequemlichkeit einfacher Merkhilfen bedienen, des berühmten Post-It auf dem Bildschirm zum Beispiel. Wenn man nun weiß, dass die vielen »Angriffe« aus dem Kollegen- oder Bekanntenkreis kommen (sind Sie sicher, dass Ihr Sohn nicht mal aus reiner Neugier in Ihren Rootserver schauen möchte?), wird die Gefährlichkeit solcher Hilfen wohl erst bewusst.

Wenn Sie kein Gehirnakrobat sind, brauchen Sie also eine Alternative. Bis vor nicht allzu langer Zeit galten Kombinationen aus zwei zufällig gewählten Wörtern, durch ein Sonderzeichen verknüpft, noch als sicher. Frühere Compuserve-Nutzer erinnern sich womöglich noch an derartige Konstruktionen. Inzwischen sind Passwortcracker aber zu ausgereift, sich davon abschrecken zu lassen. Die Fachliteratur rät deshalb inzwischen zu Passwörtern, die aus Sätzen voll »schockierendem Unsinn« konstruiert werden. Den kompletten Satz reduzieren Sie auf ein Wort, indem Sie jeweils einen bestimmten (zum Beispiel den dritten oder den letzten) Buchstaben jedes Wortes verwenden. Der schockierende Teil des Inhalts soll Ihnen helfen, sich den kompletten Satz zu merken. Weil niemand außer Ihnen den Satz jemals lesen wird, sollten Sie das »schockierend« durchaus ernst nehmen – etwa im Sinne von obszön oder in anderer Weise extrem. Weil der Satz insgesamt völlig unsinnig ist, ist er aber kaum zu erraten. Ein sehr gemäßigtes Beispiel wäre etwa »Mama sticht der grün gestreiften Mietze die Knopfaugen aus«, das sich daraus ergebende Kennwort könnte dann »MsdggMdKa« sein. Wenn Sie darin noch eine Ziffer oder ein Sonderzeichen einstreuen, erhöht das die Sicherheit weiter.

7.2.2 Einloggen als »root« vermeiden

Wenn Sie an Ihrem Mietserver arbeiten, sollten Sie sich stets als normaler Nutzer ohne weitere Privilegien anmelden. Wie Sie einen solchen Account anlegen, haben Sie im Abschnitt »Benutzerverwaltung« erfahren. Stellt sich eine Aufgabe, die Superuser-Privilegien erfordert, benutzen Sie den Befehl »su« (super user):

Das Programm startet eine neue Shell, in der Sie alle Genehmigungen des Superusers besitzen. Kleiner Nachteil: Das Kommando sorgt nicht dafür, die als »root« ausgeführten Befehle aufzuzeichnen. Außerdem vergessen Sie womöglich Ihren besonderen Status, denn er bleibt so lange in Kraft, bis Sie die Shell mit

beenden. Dass Sie für den Aufruf nicht einfach nur »su« verwendet haben, ist eine zusätzliche Sicherheitsmaßnahme, die Sie ähnlich auch bei anderen kritischen Programmen anwenden sollten. Der komplette Pfadname garantiert nämlich, dass Sie nicht zufällig ein in den Pfad geschmuggeltes, ebenfalls »su« genanntes Programm aufrufen, das etwa als Password-Sniffer dienen könnte.

Übrigens können Sie sich mit »su« auch unter jedem anderen Benutzernamen einloggen – Sie müssen dem Befehl nur als Parameter den gewünschten Namen übergeben. Voraussetzung ist natürlich, dass Sie das Passwort des Users kennen. Diese Fähigkeit dient nicht zum Spionieren in fremden Accounts, vielmehr ist es oft so, dass Sie bestimmte Fehler nur nachvollziehen können, wenn Sie unter dem richtigen Benutzerkonto eingeloggt sind.

Weniger nützlich ist »su«, wenn Sie auch anderen Nutzern erlauben wollen, ganz bestimmte Befehle oder Programme mit Superuser-Rechten auszuführen. Denn Sie kön-

nen dabei die Rechte der Anwender nicht beschränken – einmal zum Superuser gemacht, können Sie es, wenn Sie es darauf anlegen, auch für immer bleiben.

Für solche Zwecke gibt es aber eine praktische Alternative: »sudo« (super user do). Das Programm konsultiert nämlich die Textdatei `/etc/sudoers`. Darin ist notiert, welche User welche Befehle mit Superuser-Privilegien ausführen dürfen. Nachdem sudo anhand der Liste geprüft hat, ob der Anwender das geforderte Kommando ausführen darf, fragt es sicherheitshalber zunächst nach seinem Kennwort (nicht nach dem Administratorpasswort). Danach hat der Nutzer fünf Minuten Zeit, ihm erlaubte Kommandos auszuführen, erst danach muss er wieder sein Kennwort eingeben. Das soll dazu dienen, die Gefahr durch einen »mal eben« verlassenen Rechner mit gültigem Login zu minimieren. Auf Ihrem Rootserver ist dieser Aspekt weniger wichtig.

Die sudoers-Liste können Sie **nicht** mit dem Texteditor Ihrer Wahl bearbeiten. Das heißt, im Prinzip können Sie das durchaus, es handelt sich um eine ganz normale Textdatei. Allerdings ist das, was sie enthält, unter Umständen recht brisant. Aus diesem Grund gibt es das kleine Tool Visudo, das es erlaubt, das sudoers-File auf sichere Art und Weise zu bearbeiten. Es handelt sich dabei um eine Art Erweiterung, die sich um den Texteditor (in der Regel Vi) herumlegt und Ihre Änderungen in sudoers vor dem Speichern auf syntaktische Richtigkeit prüft. Allerdings kann Visudo wirklich nur testen, ob Sie alle Regeln eingehalten haben – wenn Sie (technisch korrekt) all Ihren Nutzern sämtliche Freiheiten geben, akzeptiert Visudo dies ohne Murren.

Gestartet wird das Programm einfach über

Dazu **müssen** Sie als Root eingeloggt sein. Beschwerst sich das Programm darüber, den Editor nicht finden zu können, müssen Sie ihm zunächst über eine Umgebungsvariable den Weg weisen:

Vorausgesetzt, Vi beziehungsweise Vim befindet sich auf Ihrem System im Verzeichnis `/bin`.

Wenn Sie alle nötigen Änderungen eingearbeitet haben, überprüft Visudo die Syntax. Falls das Programm dabei einen Fehler ausfindig macht, gibt es eine entsprechende Meldung aus, die die betroffenen Zeilennummern enthält. Danach stellt es Sie vor die Wahl, mit »e« wieder in den Editiermodus zu springen, mit »x« das Programm ohne Speichern zu verlassen oder mit »Q« die Änderungen trotz der Fehler zu sichern. Allerdings können Sie sich darauf verlassen, dass auch Sudo an der fehlerhaften Datei Anstoß nimmt.

Die Datei sudoers enthält (unter anderem) zwei wichtige Bereiche. Zunächst können Sie der Einfachheit halber den Aktionen, die Ihre Benutzer ausführen dürfen, Namen geben:

Doch nicht nur den Aktionen dürfen Sie (wie im Beispiel eben mit dem Schlüsselwort `Cmnd_Alias`) eigene Namen verpassen. Das funktioniert auch mit Usernamen (Keyword `User_Alias`), dem Benutzer, unter dessen Berechtigung das Programm ausgeführt

werden soll (Runas_Alias) oder dem Hostsystem (Host_Alias – dieses Schlüsselwort brauchen Sie auf einem einzelnen Server nicht). Ein User-Alias könnte zum Beispiel so aussehen:

In der Liste können auch Gruppennamen enthalten sein, diesen müssen Sie lediglich ein % voranstellen (ohne Anführungszeichen). Dann können Sie Ihren Nutzern die zuvor definierten Aktionen (oder auch weitere ohne eigenen Alias) zuordnen:

Der Nutzer »verwalter« darf damit die oben als »SHELLS« definierten Shells als Superuser ausführen. Und zwar auf allen (»ALL«) Maschinen – in diesem Fall also auf dem einen zur Verfügung stehenden Server. »verwalter« könnte damit zum Beispiel während Ihres Urlaubs Ihren Stellvertreter spielen, ohne dass Sie ihm Ihr Root-Passwort verraten müssen. Außerdem notiert das System, was »verwalter« unter sudo-Kontrolle tut. Statt des konkreten Usernamens können Sie selbstverständlich auch einen Alias verwenden:

In diesem Fall dürfen tom, martin und horst die grundlegenden Kommandos zum Anlegen und Löschen anderer User ausführen. Noch nicht zur Sprache kam bisher der Parameter »Run as«. Das hatte seinen Grund: Wenn Sie ihn nicht angeben, wird der betreffende Befehl immer als »root« ausgeführt, und das ist ja der Hauptzweck von Sudo. Wenn Sie aber zum Beispiel erreichen wollen, dass die Skatbrüder heinz und karl gegenseitig Zugriff auf ihre Heimatverzeichnisse haben sollen, dann hilft diese Zeile:

heinz darf also auf allen Maschinen (das erste ALL) alle Befehle (das zweite ALL) mit den Rechten von karl ausführen. Der Username, mit dessen Rechten ein Programm gestartet wird, muss also in Klammern noch vor dem eigentlichen Befehl angegeben werden.

Weil sowohl heinz als auch karl gewöhnliche User sind, ist »alle Befehle« nicht wörtlich zu nehmen – gemeint sind »alle Befehle, auf die der jeweilige Benutzer Zugriff hat«. Die zweite Zeile sorgt dafür, dass karl dieselben Privilegien zustehen. Wenn heinz nun in karls Verzeichnis Dateien löscht, ist ihm das zwar erlaubt, Sudo führt aber darüber Buch.

Welche Befehle ein Nutzer mit Hilfe von Sudo ausführen kann, erfährt er übrigens von Sudo selbst:

Ein Nachteil von Sudo sei nicht verschwiegen: Wenn der Account eines der beteiligten Anwender kompromittiert wird, ist es mit der Sicherheit von Sudo dahin. Sie sollten also wirklich genau überlegen, wem Sie zumindest zeitweise Superuser-Rechte ver-

schaffen. Immerhin hat Sudo im Fall des Falles den Vorteil gegenüber »su«, dass es alle ausgeführten Befehle aufzeichnet.

7.3 Grundkonfiguration absichern

7.3.1 Ein Account pro Nutzer

Vermeiden Sie es immer, Sammelzugänge für ganze Gruppen von Nutzern zu vergeben. Etwas, was allen gehört, gehört niemandem wirklich. Wenn Sie allen Mitgliedern Ihres Skatclubs den Zugang »club« zuteilen, wird sich keins der Clubmitglieder wirklich dafür verantwortlich fühlen, wer welche Dateien ablegt, welches Kennwort verwendet wird und so weiter. Niemand wird sich darüber wundern, wenn plötzlich bisher nicht vorhandene Verzeichnisse erscheinen – die könnten ja von den anderen »club«-Logins kommen.

Es ist dann auch rein technisch nicht mehr möglich, im Nachhinein herauszubekommen, wer ein bestimmtes Programm auf den Server geschmuggelt oder sein Kennwort schludrig behandelt hat. Deshalb richten Sie besser einzelne Logins ein – über die Gruppenverwaltung können Sie Ihren Usern trotzdem ermöglichen, Dateien gemeinsam zu verwalten.

7.3.2 Sichere Kennwörter

Wenn Sie anderen Nutzern den Zugang zu Ihrem Server erlauben, können Sie sich nicht darauf verlassen, dass diese genauso verantwortungsbewusst wie Sie mit dem System umgehen. Oft ist den »normalen« Anwendern gar nicht klar, welche Gefahren sie womöglich heraufbeschwören. Das Problem: Natürlich kann sich niemand 25 Kennwörter für alle möglichen Server, Dienste und Anwendungen merken. Deshalb ist es durchaus üblich, Kennwörter quasi zu recyceln und mehrfach zu nutzen (selbst wir Buchautoren müssen zugeben, das bisweilen so zu halten – obwohl wir eigentlich genau wissen, dass das die Sicherheit mindert).

Die Folge: Hat ein Hacker erst einmal zum Beispiel das Login-Passwort des Nutzers herausbekommen, hält er womöglich auch gleich das Homebanking-Kennwort desselben Anwenders in den Händen. Insofern kann es ratsam sein, die Auswahl schlechter Passwörter von vornherein zu vereiteln. Dazu versuchen Sie einfach, die Kennwörter Ihrer Benutzer selbst zu knacken. Das passende Tool dafür heißt, *nomen est omen*, »crack«. Sie bekommen es unter *ftp.cert.org* (id179) im Verzeichnis XXX. Das Programm nutzt mehrere verschiedene Algorithmen, um Passwörter zu errechnen, und teilt Ihnen mit, welche es herausbekommen konnte.

Eine oft empfohlene Sicherheitsmaßnahme besteht darin, die Nutzer in regelmäßigen Abständen zu zwingen, ihre Kennwörter zu wechseln. Nach unseren Erfahrungen erhöht das jedoch oft die Sicherheit nicht, denn sich ständig neue, sichere, aber leicht zu merkende Passwörter ausdenken zu müssen, geht Ihren Usern schnell auf die Nerven. Die Folge: Entweder variieren sie die Codes nur minimal, wechseln ständig zwischen zwei

Kennwörtern hin und her oder achten nicht mehr darauf, ob das gewählte Passwort auch schwer zu erraten ist. Es handelt sich dabei um den typischen Konflikt zwischen Sicherheit und Bequemlichkeit, und wenn es sich nicht durchgängig um sehr sicherheitsbewusste Nutzer handelt (Sie verwalten nicht zufällig den Webserver des BND?), gewinnt diesen Kampf meist das Komfortbedürfnis.

7.3.3 Sichere Suchpfade

Ein weiteres Bequemlichkeits-Problem: Suchpfade sind eine sehr praktische Sache, wenn es darum geht, Programme schnell zu starten. Wenn sich das gewünschte Kommando im Suchpfad befindet, müssen Sie sich den tatsächlichen Pfadnamen nicht merken. Sicherheitsrelevant wird die Sache dann, wenn Sie gar nicht mehr genau wissen, welches Programm Sie überhaupt aufrufen. Es könnte einem böswilligen Anwender gelingen, Ihnen im Suchpfad ein Tool unterzujubeln, das zwar so heißt wie ein Systemprogramm (etwa »su«), aber durchaus unchristliche Absichten hegt.

Das machen Sie dem Angreifer besonders einfach, wenn Sie das aktuelle Verzeichnis (.) in den Suchpfad mit aufnehmen. Gerade als Administrator bewegen Sie sich ja durchaus in prinzipiell unsicheren Gegenden – Verzeichnissen nämlich, auf die andere Anwender regulär Zugriff haben. Im Suchpfad sollten deshalb nur Ordner enthalten sein, auf die einzig und allein der Administrator zugreifen darf. So können Sie die Pfade einsehen:

Die Pfadnamen werden also durch einen Doppelpunkt getrennt. Ändern können Sie den Pfad mit dem folgenden Befehl. Merken Sie sich dabei den ursprünglichen Inhalt der Variablen und lassen Sie nur den Teil mit dem Punkt (.) weg.

7.3.4 Sichere Dateiberechtigungen

Was ein Eindringling mit einer Systemdatei anstellen kann, wird ihm (solange es ihm noch nicht gelungen ist, sich Superuser-Status zu verschaffen) immer durch die von Ihnen vergebenen Dateiberechtigungen vorgeschrieben. Besonders wichtig sind in diesem Zusammenhang natürlich die Dateien mit den Nutzer- und Gruppenlisten.

Eigentümer und Gruppe von `/etc/passwd`, `/etc/groups` und `/etc/shadow` sollten immer »root« sein (wenn nicht – Kommando »chown« benutzen).

Die `passwd`- und `groups`-Datei muss von allen Nutzern einsehbar sein, allerdings dürfen diese keine Schreibrechte besitzen.

Demzufolge müssen Sie diese beiden Files auf den Modus »644« einstellen (»chmod«-Befehl, siehe Kapitel 3)

Die Datei mit den verschlüsselten Kennwörtern darf niemand außer »root« einsehen – ihr Modus muss also »640« lauten.

Ebenfalls eine Schwachstelle: die Festplattenpartitionen, die Sie in /dev finden. Wer zum Beispiel auf irgendeine Weise Lese- und Schreibrecht für /dev/hda1 erwirbt, hat damit Rechte an allen auf dieser Partition liegenden Files. Anderen Nutzern sollten Sie deshalb für diese Gerätedateien keinerlei Berechtigungen erteilen.

Nicht ganz so offensichtlich ist die Gefahr, die von Programmen mit SGID- oder SUID-Rechten ausgeht. Diese speziellen Dateiberechtigungen, die so genannten S-Bits, bewirken, dass ein Programm stets mit den Rechten seines Eigentümers ausgeführt wird, nicht mit denen seines Benutzers. Das ist dann eine offene Hintertür, wenn der Eigentümer »root« ist und das unter seinen Rechten gestartete Programm eine Schwachstelle besitzt. Mit dem Befehl

(in einer Zeile eingeben) verschaffen Sie sich einen Überblick, welche Dateien überhaupt betroffen sind. In diesem Fall nimmt ein »s« den Platz ein, den normalerweise »x« innehat.

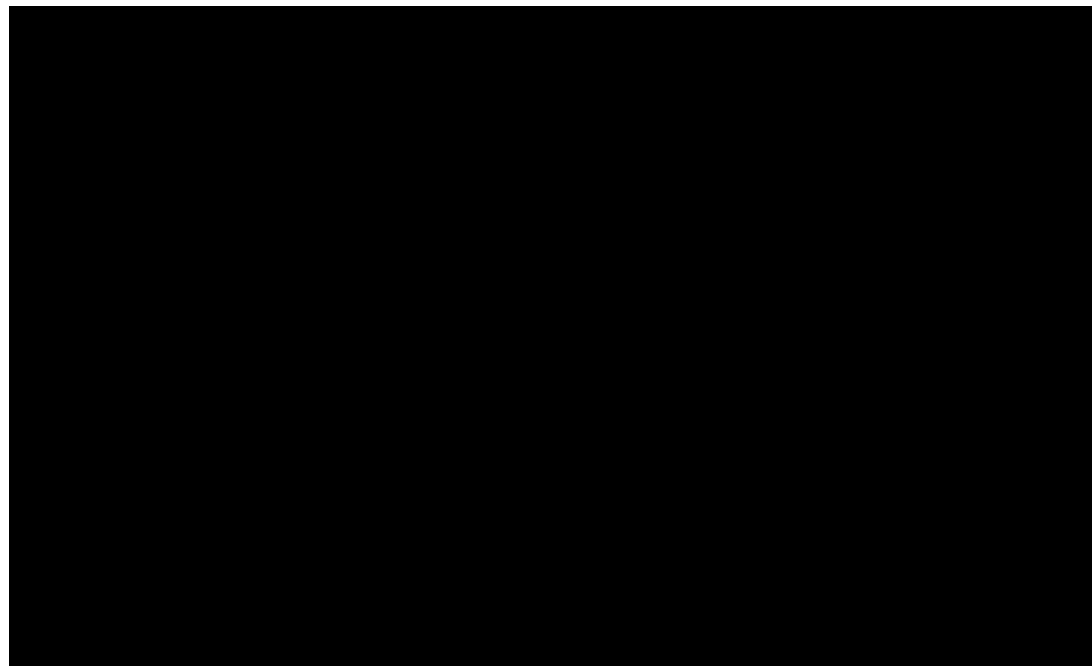


Bild 7.1: Dateien mit gesetztem S-Bit

Meist müssen Programme dann Root-Rechte bekommen, wenn sie auf geschützte Systemdateien zugreifen müssen (um ihren Zweck zu erfüllen), aber trotzdem für jeden User nutzbar sein sollen. So wie zum Beispiel der `passwd`-Befehl: Anwender müssen ja in der Lage sein, ihr Kennwort zu ändern. Dazu muss das Programm aber in der nur dem Root zugänglichen Datei `/etc/shadow` schreiben können. Es lässt sich leider kein Universalrezept angeben, welche Programme das S-Bit denn nun haben dürfen. Von Ihnen selbst installierte Software, Gameserver zum Beispiel, sollten das S-Bit aber nicht benötigen. Entfernen Sie es in diesem Fall mit

für das SUID-Bit und

für das SGID-Bit.

7.3.5 Unsichere und unnötige Dienste deaktivieren

Eine Grundregel der Serversicherheit lautet, auf das Anbieten unnötiger und vor allem unsicherer Dienste zu verzichten. Als unsicher gelten dabei nicht nur Services mit bekannten Sicherheitslücken, sondern strikt alle Programme, die die Übertragung von Kennwörtern im Klartext vorsehen. Dazu gehören zum Beispiel `Rshd` und `Rexecd`, die die Ausführung extern gestarteter Befehle ermöglichen, oder der `rlogind`-Dämon, der zur (unverschlüsselten) Anmeldung von Fernnutzern dient. Der `Telnet`-Dämon `Telnetd` ermöglicht ebenfalls das Einloggen über eine ungesichere Verbindung. Der Trivial FTP-Service `Tftpd` ermöglicht plattenlosen Systemen, bestimmte zum Booten nötige Dateien aus dem Netzwerk zu beziehen. Auf einem Rootserver hat er nichts zu suchen. Der `Finger`-Dämon `Fingerd` verarbeitet Anforderungen des `finger`-Kommandos, das (für Hacker womöglich interessante) Informationen über am System eingeloggte User bereitstellt.

All diese Dienste werden meist vom `Inet`- beziehungsweise `Xinet`-Dämon aufgerufen. Wie Sie vorgehen müssen, um einen Dienst auszuschalten, hängt darum vom verwendeten Netzwerkdienst-Dämon ab. Sie müssen also zunächst einmal herausfinden, welcher dieser Dämonen auf Ihrem System überhaupt aktiv ist. Das verrät Ihnen der Befehl `»ps«` – im folgenden Beispiel haben wir die Ausgabe noch zusätzlich mit Hilfe von `»grep«` gefiltert:

Hier ist also `Xinetd` am Werke. Falls Sie überhaupt kein Ergebnis erhalten, ist das auch nicht schlimm: Dann werden auf Ihrem System Server offensichtlich nicht von dritter Seite gestartet. Das muss nicht prinzipiell ein sicherheitsrelevanter Nachteil sein. Einerseits entgeht Ihnen dadurch die Möglichkeit, mit Hilfe der TCP-Wrappers (siehe folgender Abschnitt) Zugriffe zentral zu regulieren. Andererseits sind in modernen Servern ähnliche Regelmöglichkeiten stets auch eingebaut. Sie müssen dann allerdings jeden Server auch einzeln absichern. `Inetd` beziehungsweise `Xinetd` nicht zu verwenden, hat den Vorteil, dass die entsprechenden Serverprogramme sofort reagieren können und

nicht erst auf das Signal von Inetd warten müssen. Bei Programmen, die sowieso ständig Daten zugeschickt bekommen (zum Beispiel dem Webserver), verzichtet man deshalb darauf, sie über Inetd und Konsorten starten zu lassen.

Inetd

Inetd besitzt eindeutig die einfachere Konfigurationsdatei. Sie befindet sich in der Regel in /etc, falls nicht, hilft ein

auf jeden Fall weiter. Öffnen Sie die Datei zunächst mit

Jede Zeile in der Datei folgt demselben Schema (wenn sie nicht durch ein # auskommentiert ist):

Beim FTP-Dienst könnte das dann folgendermaßen aussehen:

Übersetzung: Wenn auf dem Port, der in der Datei /etc/services für den ftp-Dienst eingetragen ist (also 21), tcp-Daten eintreffen, soll Inetd unter dem Usernamen root das Programm /usr/sbin/tcpd (die so genannten TCP-Wrapper) mit dem Parameter vsftpd (das ist der eigentliche FTP-Server) aufrufen. Wenn Sie diese Zeile auskommentieren, indem Sie ein # an ihren Anfang setzen, wird Inetd in Zukunft alle tcp-Datenpakete an Port 21 ignorieren.

Eine besondere Rolle spielt übrigens der hier in der »flags«-Spalte vertretene Eintrag »nowait«. Mit seinem Gegenstück »wait« entscheidet er darüber, wie sich Inetd bei weiteren auf demselben Port eintreffenden Anforderungen verhält. Bei »wait« geht der Inetd-Dämon davon aus, dass der aufgerufene Server sich um alles weitere kümmert, und lauscht auf dem entsprechenden Port erst wieder, wenn der Server sich beendet hat. »nowait« sorgt für entgegengesetztes Verhalten: Inetd startet bei neuen Anforderungen den angesprochenen Server (das heißt eine Kopie davon) erneut.

Wenn Sie an inetd.conf irgendwelche Änderungen durchgeführt haben, vergessen Sie nicht, den Dämon auch darauf aufmerksam zu machen:

Xinetd

Doch auch die Konfigurationsdatei von Xinetd ist durchaus lesbar. Sie befindet sich normalerweise in /etc und heißt xinetd.conf. Ein

verräät Ihnen stets ihren aktuellen Ablageplatz. Öffnen Sie die Datei zunächst mit