Inhalt

Vorwort 23
Über dieses Buch 29
Formales 29
Linux-Distributionen 31

1 Der Administrator 33

1.1 Der Beruf des Systemadministrators 33
1.1.1 Berufsbezeichnung und Aufgaben 33
1.1.2 Job-Definitionen 34
1.2 Nützliche Fähigkeiten und Fertigkeiten 39
1.2.1 Soziale Fähigkeiten 39
1.2.2 Arbeitstechniken 40
1.3 Das Verhältnis vom Administrator zu Normalsterblichen 42
1.3.1 Der Chef und andere Vorgesetzte 42
1.3.2 Benutzer 43
1.3.3 Andere Administratoren 43
1.4 Unterbrechungsgesteuertes Arbeiten 44
1.5 Ethischer Verhaltenskodex 45

TEIL I: Grundlagen

2 Bootvorgang 49

2.1 Einführung 49
2.2 Der Bootloader GRUB 49
2.2.1 Installation 50
2.2.2 Konfiguration 52
2.2.3 Booten von einem Software-RAID-1 53
2.3 GRUB 2 54
2.3.1 Funktionsweise 54
2.3.2 Installation 54
2.3.3 Konfiguration 54
2.4 Bootloader Recovery 58
2.5 Der Kernel und die »initrd« 59
2.5.1 »initrd« erstellen und modifizieren 60
2.5.2 »initrd« manuell modifizieren 63

2.6 »Upstart« ... 64
2.6.1 Funktionsweise ... 64
2.6.2 Events im Detail ... 65
2.6.3 Prozessdefinitionen ... 66
2.6.4 Anzeige aller Upstart-Jobs ... 67
2.6.5 Anzeige und Überprüfung der Job-Konfigurationen ... 69
2.6.6 Starten, Stoppen und Neustarten von Diensten ... 70
2.6.7 Abschlussbemerkung ... 71

3 Festplatten und andere Devices ... 73

3.1 RAID ... 73
3.1.1 RAID-0 ... 74
3.1.2 RAID-1 ... 74
3.1.3 RAID-5 ... 74
3.1.4 RAID-6 ... 75
3.1.5 RAID-10 ... 75
3.1.6 Zusammenfassung ... 75
3.1.7 Weich, aber gut: Software-RAID ... 76
3.1.8 Software-RAID unter Linux ... 77
3.1.9 Abschlussbemerkung zu RAIDs ... 84
3.2 Rein logisch: Logical Volume Manager »LVM« ... 84
3.2.1 Grundlagen und Begriffe ... 86
3.2.2 Setup ... 87
3.2.3 Aufbau einer Volume Group mit einem Volume ... 88
3.2.4 Erweiterung eines Volumes ... 91
3.2.5 Eine Volume Group erweitern ... 92
3.2.6 Aufbau eines gespiegelten Volumes ... 94
3.2.7 Eine defekte Festplatte ersetzen ... 95
3.2.8 Backups mit Snapshots ... 95
3.2.9 Kommandos ... 99
3.3 »udev« ... 101
3.3.1 »udev«-Regeln ... 101
3.3.2 Eigene Regeln schreiben ... 102
3.4 Alles virtuell? »/proc« ... 105
3.4.1 CPU ... 105
3.4.2 RAM ... 106
3.4.3 Kernelkonfiguration ... 107
3.4.4 Kernelparameter ... 107
3.4.5 Gemountete Dateisysteme ... 108
3.4.6 Prozessinformationen ... 108

3.4.7 Netzwerk ... 109
3.4.8 Änderungen dauerhaft speichern ... 110
3.4.9 Abschlussbemerkung ... 110

4 Dateisysteme ... 111

4.1 Dateisysteme: von Bäumen, Journalen und einer Kuh ... 111
4.1.1 Bäume ... 112
4.1.2 Journale ... 114
4.1.3 Und die Kühe? COW-fähige Dateisysteme ... 115
4.2 Praxis ... 115
4.2.1 Ext2/3-FS aufgebohrt: mke2fs, tune2fs, dumpe2fs, e2label ... 115
4.2.2 ReiserFS und seine Tools ... 118
4.2.3 XFS ... 119
4.2.4 Das Dateisystem vergrößern oder verkleinern ... 120
4.2.5 Ausblick auf BtrFS ... 122
4.3 Fazit ... 124

5 Berechtigungen ... 125

5.1 User, Gruppen und Dateisystemstrukturen ... 125
5.2 Dateisystemberechtigungen ... 128
5.2.1 Spezialbits ... 129
5.3 Erweiterte Posix-ACLs ... 132
5.3.1 Das Setzen und Anzeigen von einfachen ACLs ... 133
5.3.2 Setzen von Default-ACLs ... 135
5.3.3 Setzen von erweiterten ACLs ... 136
5.3.4 Entfernen von ACLs ... 139
5.3.5 Sichern und Zurückspielen von ACLs ... 140
5.4 Erweiterte Dateisystemattribute ... 140
5.4.1 Attribute, die jeder Benutzer ändern kann ... 141
5.4.2 Attribute, die nur »root« ändern kann ... 141
5.4.3 Weitere Attribute ... 142
5.5 Quotas ... 143
5.5.1 Installation und Aktivierung der Quotas ... 143
5.5.2 Journaling Quotas ... 145
5.5.3 Quota-Einträge verwalten ... 146
5.6 Pluggable Authentication Modules (PAM) ... 150
5.6.1 Verschiedene PAM-Typen ... 150
5.6.2 Die PAM-Kontrollflags ... 151
5.6.3 Argumente zu den Modulen ... 152

5.6.4 Modulpfade ... 152
5.6.5 Module und ihre Aufgaben ... 152
5.6.6 Die neuere Syntax bei der PAM-Konfiguration ... 154
5.7 Konfiguration von PAM ... 155
5.8 »ulimit« ... 157
5.8.1 Setzen der »ulimit«-Werte ... 158
5.9 Abschlussbemerkung ... 159

TEIL II: Aufgaben

6 Paketmanagement ... 163

6.1 Paketverwaltung ... 163
6.1.1 »rpm« oder »deb«? ... 164
6.1.2 »yum«, »yast« oder »apt«? ... 166
6.1.3 Außerirdische an Bord – »alien« ... 168
6.2 Pakete im Eigenbau ... 169
6.2.1 Am Anfang war das Makefile ... 169
6.2.2 Vom Fellknäuel zum Paket ... 172
6.2.3 Patchen mit »patch« und »diff« ... 176
6.2.4 Updates ohne Repository ... 179
6.2.5 »rpm«-Update-Paket ... 179
6.2.6 »deb«-Update-Pakete ... 182
6.2.7 Updatesicher konfigurieren ... 183

7 Backup und Recovery ... 187

7.1 Backup gleich Disaster Recovery? ... 187
7.2 Backupstrategien ... 188
7.3 Datensicherung mit »tar« ... 191
7.3.1 Weitere interessante Optionen für GNU-»tar« ... 192
7.3.2 Sicherung über das Netzwerk mit »tar« und »ssh« ... 193
7.4 Datensynchronisation mit »rsync« ... 194
7.4.1 Lokale Datensicherung mit »rsync« ... 194
7.4.2 Synchronisieren im Netzwerk mit »rsync« ... 195
7.4.3 Wichtige Optionen für »rsync« ... 195
7.4.4 Backupskript für die Sicherung auf einen Wechseldatenträger ... 197
7.4.5 Backupskript für Sicherungen auf einen Backupserver ... 197
7.4.6 Verwendung von »ssh« für die Absicherung von »rsync« ... 200

7.5 Imagesicherung mit »dd« ... 201
7.5.1 Sichern des Master Boot Records (MBR) ... 201
7.5.2 Partitionstabelle mithilfe von »dd« zurückspielen ... 202
7.5.3 Erstellen eines Images mit »dd« ... 202
7.5.4 Einzelne Dateien mit »dd« aus einem Image zurückspielen ... 203
7.5.5 Abschlussbemerkung zu »dd« ... 205
7.6 Disaster Recovery mit ReaR ... 205
7.6.1 ReaR installieren ... 206
7.6.2 ReaR konfigurieren ... 206
7.6.3 Die erste Konfiguration ... 208
7.6.4 ReaR aufrufen ... 208
7.6.5 Der erste Testlauf ... 209
7.6.6 Der Recovery-Prozess ... 212
7.6.7 Die ReaR-Konfiguration im Detail ... 214
7.6.8 Migrationen mit ReaR ... 215
7.6.9 Abschlussbemerkung ... 215
7.7 Fazit zur Datensicherung und Recovery ... 216

TEIL III: Dienste

8 Webserver ... 219

8.1 Apache ... 219
8.1.1 Virtuelle Hosts einrichten ... 219
8.1.2 HTTPS konfigurieren ... 221
8.1.3 Benutzer-Authentisierung mit Kerberos ... 224
8.1.4 Apache-Server mit ModSecurity schützen ... 226
8.1.5 Tuning und Monitoring ... 229
8.2 LightHttpd ... 233
8.2.1 Virtuelle Hosts mit »mod_simple_vhost« einrichten ... 233
8.2.2 Virtuelle Hosts ohne »mod_simple_vhost« einrichten ... 234
8.2.3 HTTPS konfigurieren ... 235
8.3 Logfiles auswerten ... 237

9 FTP-Server ... 241

9.1 Einstieg ... 241
9.1.1 Das File Transfer Protocol ... 241
9.1.2 vsftpd ... 242
9.2 Download-Server ... 242

9.3 Zugriff von Usern auf ihre Home-Verzeichnisse 244
9.4 FTP über SSL (FTPS) 245
9.5 Anbindung an LDAP 246

10 Mailserver 247

10.1 Postfix 247
10.1.1 Grundlegende Konfiguration 247
10.1.2 Integrierte Sicherheitsmechanismen 249
10.1.3 Antivirus- und Spamfilter mit Amavisd-new, ClamAV und SpamAssassin 252
10.2 Exim 262
10.2.1 Grundlegende Konfiguration 262
10.2.2 Viren erkennen 263
10.2.3 Spam abwehren 264
10.3 Monitoring und Logfile-Auswertung 266
10.3.1 Logfile-Auswertung mit »Lire« 266
10.4 Dovecot 269
10.4.1 POP3 269
10.4.2 IMAP 271
10.4.3 Konfiguration 273

11 Datenbank 277

11.1 MySQL in der Praxis 277
11.1.1 Installation und grundlegende Einrichtung 277
11.1.2 Replikation 278
11.1.3 Master-Master-Replikation 285
11.2 Tuning 288
11.2.1 Tuning des Speichers 289
11.2.2 Tuning von Indizes 295
11.3 Backup und Point-In-Time-Recovery 299
11.3.1 Restore zum letztmöglichen Zeitpunkt 300
11.3.2 Restore zu einem bestimmten Zeitpunkt 301

12 Syslog 303

12.1 Aufbau von Syslog-Nachrichten 303
12.2 Der Klassiker: »SyslogD« 304
12.3 Syslog-ng 306

12.3.1 Der »options«-Abschnitt ... 306
12.3.2 Das »source«-Objekt ... 308
12.3.3 Das »destination«-Objekt ... 308
12.3.4 Das »filter«-Objekt ... 310
12.3.5 Das »log«-Objekt ... 311
12.4 Rsyslog ... 312
12.4.1 Eigenschaftsbasierte Filter ... 312
12.4.2 Ausdrucksbasierte Filter ... 313
12.5 Loggen über das Netz ... 314
12.5.1 SyslogD ... 314
12.5.2 Syslog-ng ... 315
12.5.3 Rsyslog ... 315
12.6 Syslog in eine Datenbank schreiben ... 316
12.6.1 Anlegen der Log-Datenbank ... 316
12.6.2 In die Datenbank loggen ... 317

13 Proxyserver ... 321

13.1 Einführung des Stellvertreters ... 321
13.2 Proxys in Zeiten des Breitbandinternets ... 322
13.3 Herangehensweisen und Vorüberlegungen ... 323
13.4 Grundkonfiguration ... 323
13.4.1 Aufbau des Testumfelds ... 324
13.4.2 Netzwerk ... 324
13.4.3 Cache ... 325
13.4.4 Logging ... 326
13.4.5 Handhabung des Dienstes ... 329
13.4.6 Objekte ... 330
13.4.7 Regeln ... 332
13.4.8 Anwendung von Objekten und Regeln ... 334
13.5 Authentifizierung ... 336
13.5.1 Benutzerbasiert ... 338
13.5.2 Gruppenbasiert ... 349
13.6 Helferlein ... 353
13.6.1 squidGuard ... 353
13.6.2 Antiviren-Check: ClamAV mit HAVP einbinden ... 355
13.6.3 Dansguardian ... 358
13.7 Log-Auswertung: »Calamaris« und »Sarg« ... 362
13.7.1 Calamaris ... 362
13.7.2 Sarg ... 363
13.8 Unsichtbar: »transparent proxy« ... 364

13.9 Ab in den Pool – Verzögerung mit »delay_pools« 366
13.9.1 Funktionsweise – alles im Eimer! 366
13.9.2 Details – Klassen, Eimer und ACLs richtig wählen 367

14 Kerberos 371

14.1 Begriffe im Zusammenhang mit Kerberos 372
14.2 Funktionsweise von Kerberos 373
14.3 Installation und Konfiguration des Kerberos-Servers 373
14.3.1 Konfiguration der Datei »/etc/krb5.conf« 374
14.3.2 Konfiguration der Datei »kdc.conf« 376
14.4 Initialisierung und Testen des Kerberos-Servers 379
14.4.1 Verwalten der Principals 380
14.5 Kerberos und PAM 384
14.5.1 Konfiguration der PAM-Dateien auf dem SLES11 384
14.5.2 Testen der Anmeldung 385
14.6 Neue Benutzer mit Kerberos-Principal anlegen 385
14.7 Hosts und Dienste 386
14.7.1 Entfernen von Einträgen 388
14.8 Konfiguration des Kerberos-Clients 389
14.8.1 PAM und Kerberos auf dem Client 390
14.9 Replikation des Kerberos-Servers 390
14.9.1 Bekanntmachung aller KDCs im Netz 391
14.9.2 Konfiguration des KDC-Masters 394
14.9.3 Konfiguration des KDC-Slaves 395
14.9.4 Replikation des KDC-Masters auf den KDC-Slave 396
14.10 Kerberos Policies 398

15 Samba 401

15.1 Kurze Einführung in die Protokolle SMB und NetBIOS 402
15.1.1 Das Protokoll SMB 402
15.1.2 Das Protokoll NetBIOS 403
15.1.3 Möglichkeiten mit NetBIOS 404
15.1.4 Grundeinstellung der »smb.conf« 404
15.1.5 Verwendung von WINS zur Namensauflösung 406
15.1.6 Parameter für den »nmbd«in der »smb.conf« 407
15.1.7 Clientkonfiguration 409
15.2 Samba als Fileserver 410
15.2.1 Erstellen einfacher Freigaben 410
15.2.2 Spezielle Freigaben 413

15.2.3 Zusammenfassung mehrerer Freigaben ... 414
15.2.4 Kopieren von Freigabeeinstellungen ... 415
15.2.5 Ablauf des Zugriffs auf eine Freigabe ... 416
15.3 Benutzerverwaltung ... 419
15.3.1 Anlegen der Benutzer in der »smbpasswd« ... 420
15.3.2 Umwandeln der »smbpasswd« in »tdbsam« ... 422
15.4 Verschiedene »passdb backends« ... 423
15.4.1 »smbpasswd« ... 423
15.4.2 »tdbsam« ... 424
15.4.3 »ldapsam« ... 425
15.5 Samba als Domänencontroller ... 427
15.5.1 Grundeinstellung des Domänencontrollers ... 428
15.5.2 Weitere Möglichkeiten mit »rpcclient« ... 429
15.5.3 Einrichten eines Domänenadministrators ... 435
15.5.4 Kennwortrichtlinien mit »pdbedit« erstellen ... 437
15.5.5 Einrichten von Benutzern und Hosts in der Domäne ... 439
15.5.6 Benutzeranmeldung ... 446
15.6 Winbind ... 446
15.6.1 Verschachtelte Gruppen ... 450
15.6.2 Mitgliedschaft in einer Windows-Domäne ... 452
15.6.3 Konfiguration des Kerberos-Clients ... 453
15.6.4 Einstellung in der »smb.conf« ... 455
15.6.5 Beitritt zur Windows-Domäne ... 457
15.6.6 Testen der Domänenmitgliedschaft ... 459
15.6.7 Freigaben und Berechtigungen als Domänenmitglied ... 461
15.7 Samba als Printserver ... 464
15.7.1 Freigaben für Druckertreiber und Spooling ... 465
15.7.2 Einrichtung eines Printeradmins ... 466
15.7.3 Installation von Windows-Druckertreibern ... 466
15.7.4 Druckertreiber unter Windows-Server 2000/2003 und Windows XP ... 467
15.7.5 Druckertreiber unter Windows-Server 2008 R2 und Windows 7 ... 468
15.8 Samba und Kerberos ... 471
15.9 Virtuelle Server und virtuelle Domänen ... 474
15.9.1 Zusammenführung der Server in jeder Arbeitsgruppe ... 475
15.9.2 Zusammenführen der zwei Arbeitsgruppen auf einer Maschine ... 477
15.10 Distributed File System mit Samba ... 480
15.10.1 Samba als DFS-Proxy ... 481
15.10.2 Samba als DFS-Link-Server ... 481

15.11 Vertrauensstellung ... 483
15.11.1 Der Samba-Server als vertrauende Domäne ... 484
15.11.2 Der Samba-Server als vertraute Domäne ... 484
15.12 Sicherung der Konfigurationen ... 486
15.13 Ausblick auf Samba 4 ... 487

16 NFS ... 489

16.1 Unterschiede zwischen »NFSv3«und »NFSv4« ... 489
16.2 Funktionsweise von »NFSv4« ... 490
16.3 Einrichten des »NFSv4«-Servers ... 491
16.3.1 Konfiguration des Pseudodateisystems ... 491
16.3.2 Anpassen der Datei »/etc/exports« ... 492
16.3.3 Tests für den NFS-Server ... 495
16.4 Konfiguration des »NFSv4«-Clients ... 496
16.5 Konfiguration des »idmapd« ... 497
16.6 Optimierung von »NFSv4« ... 499
16.6.1 Optimierung des »NFSv4«-Servers ... 499
16.6.2 Optimierung des »NFSv4«-Clients ... 500
16.7 »NFSv4« und Firewalls ... 501
16.8 NFS und Kerberos ... 502
16.8.1 Erstellung der Principals und der »keytab«-Dateien ... 503
16.8.2 Kerberos-Authentifizierung unter Debian und Ubuntu ... 506
16.8.3 Kerberos-Authentifizierung auf einem SLES11 ... 506
16.8.4 Anpassen der Datei »/etc/exports« ... 506
16.8.5 NFS-Client für Kerberos unter Debian und Ubuntu konfigurieren ... 507
16.8.6 NFS-Client für Kerberos auf SLES11 konfigurieren ... 507
16.8.7 Testen der durch Kerberos abgesicherten NFS-Verbindung ... 507
16.8.8 Testen der Verbindung ... 508

17 LDAP ... 511

17.1 Einige Grundlagen zu LDAP ... 512
17.1.1 Was ist ein Verzeichnisdienst? ... 512
17.1.2 Der Einsatz von LDAP im Netzwerk ... 513
17.1.3 Aufbau des LDAP-Datenmodells ... 513
17.1.4 Objekte ... 514
17.1.5 Attribute ... 515
17.1.6 Schema ... 515
17.1.7 Das LDIF-Format ... 519

17.2 Unterschiede in den einzelnen Distributionen 520
17.2.1 Umstellung auf die statische Konfiguration unter SLES11 520
17.2.2 Umstellung auf die statische Konfiguration unter Ubuntu-Server und Debian 521
17.2.3 Pfade und Benutzer 521
17.2.4 Die Datenbank-Backends 521
17.2.5 Grundkonfiguration des LDAP-Servers 521
17.3 Konfiguration des LDAP-Clients 524
17.3.1 Konfiguration des Clients auf dem SLES11 524
17.3.2 Konfiguration des Clients unter Debian »Squeeze« 525
17.3.3 Konfiguration des LDAP-Clients unter Ubuntu-Server 527
17.3.4 Erster Zugriff auf den LDAP-Server 527
17.4 Grafische Werkzeuge für die LDAP-Verwaltung 528
17.4.1 Konfiguration des »LAM« 530
17.4.2 Konfiguration des Lamdaemons 531
17.5 Änderungen mit »ldapmodify« 534
17.5.1 Interaktive Änderung mit »ldapmodify« 534
17.5.2 Änderungen über eine »ldif«-Datei mit »ldapmodify« 535
17.6 Absichern der Verbindung zum LDAP-Server über TLS 536
17.6.1 Erstellen der Zertifizierungsstelle 537
17.6.2 Erstellen des Serverzertifikats 537
17.6.3 Signieren des Zertifikats 537
17.6.4 Zertifikate in die »slapd.conf«eintragen 538
17.6.5 Konfiguration des LDAP-Clients 538
17.7 Absichern des LDAP-Baums mit ACLs 539
17.7.1 Eine eigene Datei für die ACLs einbinden 540
17.7.2 Erste ACLs zur Grundsicherung des DIT 541
17.7.3 ACLs mit regulären Ausdrücken 542
17.7.4 ACLs für den Einsatz von Samba in LDAP 544
17.7.5 Testen von ACLs vor dem Einsatz 544
17.8 Filter zur Suche im LDAP-Baum 546
17.8.1 Testen der Fähigkeiten des LDAP-Servers 546
17.8.2 Einfache Filter 548
17.8.3 Filter mit logischen Verknüpfungen 548
17.8.4 Einschränkung der Suchtiefe 549
17.9 Verwendung von Overlays 550
17.9.1 Overlays am Beispiel von »dynlist« 551
17.9.2 Weitere Overlays 552
17.10 Replikation des DIT 553
17.10.1 Konfiguration des Providers 554
17.10.2 Konfiguration des Consumers 556

17.11 Die dynamische Konfiguration 558
17.11.1 Umstellung auf die dynamische Konfiguration am Provider 559
17.11.2 Umstellung auf die dynamische Konfiguration am Consumer 563
17.12 Verwaltung von Mail-Aliasen für den Mailserver Postfix 565
17.12.1 Einrichten der »alias«-Tabelle 565
17.12.2 Einrichten der »virtual«-Tabelle 566
17.13 Cyrus und »saslauthd«über LDAP 567
17.14 Benutzerauthentifizierung am Proxy Squid über LDAP 568
17.14.1 Aktivierung der Authentifizierung über LDAP 568
17.14.2 Benutzerbezogene Authentifizierung 570
17.14.3 Gruppenbezogene Authentifizierung 570
17.15 Benutzerauthentifizierung am Webserver Apache über LDAP 572
17.15.1 Konfiguration der Cache-Parameter 572
17.15.2 Konfiguration der Zugriffsparameter 573
17.16 LDAP und Kerberos 574
17.17 Authentifizierung am LDAP-Server über »GSSAPI« 576
17.17.1 Einrichtung der Authentifizierung unter Debian und Ubuntu 577
17.17.2 Einrichten der Authentifizierung unter SLES11 582
17.18 Und was geht sonst noch alles mit LDAP? 586

18 Druckserver 587

18.1 Policies 588
18.1.1 Grundkonfiguration des Netzwerkzugriffs 588
18.1.2 Location policies 589
18.1.3 Operation policies 591
18.1.4 Weitere Konfigurationsmöglichkeiten 592
18.1.5 Browsing 594
18.2 Drucker und Klassen einrichten und verwalten 595
18.2.1 Drucker einrichten 595
18.2.2 Klassen einrichten 596
18.3 Druckerquotas 597
18.4 CUPS über die Kommandozeile 598
18.4.1 Einstellen eines Standarddruckers 598
18.4.2 Optionen für einen Drucker verwalten 599
18.5 PPD-Dateien 601
18.6 CUPS und Kerberos 602
18.6.1 Erstellen des Kerberos-Principals und der »keytab«-Datei 602
18.6.2 Umstellung der Authentifizierung am CUPS-Server 603
18.7 Noch mehr Druck 604

TEIL IV: Infrastruktur

19 Hochverfügbarkeit 607

19.1 Das Beispiel-Setup 607
19.2 Installation 608
19.2.1 Ubuntu 12.04 LTS »Precise Pangolin« 608
19.2.2 Debian 6.0 »Squeeze« 608
19.2.3 Debian 5.0 »Lenny« 608
19.2.4 openSUSE 609
19.2.5 SUSE Linux Enterprise Server 11 609
19.3 Einfache Vorarbeiten 610
19.4 Shared Storage mit DRBD 610
19.4.1 Grundlegende Konfiguration unter Debian und SUSE 611
19.4.2 Grundlegende Konfiguration unter Ubuntu LTS 611
19.4.3 Die wichtigsten Konfigurationsoptionen 612
19.4.4 Die DRBD-Ressource in Betrieb nehmen 614
19.5 Grundkonfiguration der Clusterkomponenten 617
19.5.1 OpenAIS und Corosync: das Benachrichtigungssystem 617
19.5.2 Pacemaker: der Ressourcen-Manager 619
19.5.3 Quorum deaktivieren 620
19.6 Dienste hochverfügbar machen 622
19.6.1 Die erste Ressource: eine hochverfügbare IP-Adresse 623
19.6.2 Hochverfügbarkeit am Beispiel von Apache 625
19.6.3 DRBD integrieren 628
19.6.4 Fencing 631

20 Virtualisierung 633

20.1 Einleitung 633
20.2 Für den »Sysadmin« 634
20.3 Servervirtualisierung 638
20.3.1 KVM 639
20.3.2 Xen 641
20.4 Netzwerkgrundlagen 642
20.5 Management und Installation 645
20.5.1 Einheitlich arbeiten: »libvirt« 645
20.5.2 Konsolenbasiertes Management: »virsh« 649
20.5.3 Virtuelle Maschinen installieren 652
20.5.4 »virt-install« 654
20.5.5 Alleskönner: »Virtual Machine Manager« 657

20.5.6 Zusätzliche Konsolentools ... 661
20.6 Umzugsunternehmen: Live Migration ... 663
20.6.1 Vorbereitungen ... 663
20.6.2 Konfiguration im »Virtual Machine Manager« ... 664

TEIL V: Kommunikation

21 Netzwerk ... 669

21.1 Netzwerkkonfiguration mit »iproute2« ... 669
21.1.1 Erste Schritte ... 669
21.1.2 »iproute2« im Detail ... 672
21.1.3 Links ansehen und manipulieren ... 673
21.1.4 IP-Adressen mit »iproute2« ... 675
21.1.5 »ip« zur Manipulation von ARP-Einträgen ... 678
21.2 Routing mit »ip« ... 679
21.2.1 Routing-Informationen anzeigen ... 680
21.2.2 Advanced Routing ... 681
21.2.3 Die vorhandenen Regeln ansehen ... 682
21.2.4 Neue Routing-Tabelle anlegen ... 683
21.2.5 Policy Routing Database ändern ... 683
21.2.6 Routing über mehrere Uplinks ... 685
21.2.7 Abschlussbemerkung ... 690
21.3 Bonding ... 690
21.3.1 Bonding-Konfiguration ... 690
21.3.2 Bonding bei Debian und Ubuntu ... 693
21.3.3 Bonding bei SLES ... 693
21.4 IPv6 ... 693
21.4.1 Die Vorteile von IPv6 ... 695
21.4.2 Notation von IPv6-Adressen ... 695
21.4.3 Die Netzmasken ... 696
21.4.4 Die verschiedenen IPv6-Adressarten ... 696
21.4.5 Es geht auch ohne »ARP« ... 698
21.4.6 Feste Header-Länge ... 699
21.4.7 IPv6 in der Praxis ... 702
21.5 Firewalls mit »netfilter« und »iptables« ... 703
21.6 Firewall mit »iptables« ... 703
21.6.1 Der Weg der Pakete durch den Kernel ... 704
21.6.2 Einführung in »iptables« ... 705
21.6.3 Regeln definieren ... 707

21.6.4 Die klassischen Targets ... 708
21.6.5 Ein erster Testlauf ... 708
21.6.6 Stateful Packet Inspection ... 709
21.6.7 Das erste Firewallskript ... 711
21.6.8 Externe Firewall ... 712
21.6.9 Logging ... 717
21.6.10 Network Address Translation und Masquerading ... 719
21.6.11 Weitere nützliche Module für »iptables« ... 720
21.7 Abschlussbemerkung ... 722
21.8 DHCP ... 723
21.8.1 Funktionsweise ... 723
21.8.2 Konfiguration ... 723
21.9 DNS-Server ... 726
21.9.1 Funktionsweise ... 726
21.9.2 Die Grundkonfiguration ... 727
21.9.3 Zonendefinitionen ... 729
21.9.4 Die erste vollständige Zone ... 734
21.9.5 Die »hint«-Zone ... 736
21.9.6 Reverse Lookup ... 738
21.9.7 Slave-Server ... 739
21.9.8 DNS-Server und IPv6 ... 741
21.10 Nachwort zum Thema Netzwerk ... 743

22 OpenSSH ... 745

22.1 Die SSH-Familie ... 745
22.1.1 Die Clients: »ssh«, »scp«, »sftp« ... 746
22.1.2 Der Server: »sshd« ... 748
22.2 Schlüssel statt Passwort ... 750
22.2.1 Schlüssel erzeugen ... 750
22.2.2 Passwortloses Login ... 751
22.2.3 Der SSH-Agent merkt sich Passphrasen ... 752
22.3 X11-Forwarding ... 753
22.4 Portweiterleitung und Tunneling ... 753

23 Administrationstools ... 755

23.1 Was kann dies und jenes noch? ... 755
23.1.1 Der Rsync-Daemon ... 755
23.1.2 Wenn's mal wieder später wird: »screen« ... 757
23.1.3 Anklopfen mit »nmap« ... 757

23.1.4 Netzwerkinspektion: »netstat« 761
23.1.5 Zugreifende Prozesse finden: »lsof« 763
23.1.6 Was macht mein System? »top«! 767
23.1.7 Wenn gar nichts mehr geht – Debugging mit »strace« 772
23.2 Aus der Ferne – Remote-Administrationstools 777
23.2.1 PuTTY 777
23.2.2 WinSCP 780
23.2.3 Synergy 781

TEIL VI: Automatisierung

24 Scripting 787

24.1 Aufgebohrte Muscheln 787
24.2 Vom Suchen und Finden: ein kurzer Überblick 788
24.2.1 Die Detektive: »grep«, »sed« und »AWK« 788
24.2.2 Reguläre Ausdrücke verstehen und anwenden 789
24.3 Fortgeschrittene Shell-Programmierung 792
24.3.1 Expansionsschemata 792
24.3.2 *Umgebungsvariablen* 796
24.3.3 »Back to bash«: ein tieferer Blick in die Muschel 797
24.3.4 Logging in Skripten 801
24.4 Tipps und Tricks aus der Praxis 804
24.4.1 Aufräumkommando 804
24.4.2 IFS 805
24.4.3 Datumsmagie 805
24.4.4 E-Mails aus einem Skript versenden 806
24.4.5 Interaktive Programme steuern 806

25 Monitoring – wissen, was läuft 809

25.1 Nagios 809
25.1.1 Installation 810
25.1.2 Nagios selbst kompilieren 810
25.1.3 Nagios-Plugins kompilieren 812
25.1.4 Die Verzeichnisstruktur 813
25.1.5 Das Webinterface 813
25.1.6 Die Hauptkonfigurationsdatei 814
25.1.7 Die Objekte 815
25.1.8 Die Ressourcendatei 824

25.1.9 CGI-Konfiguration ... 824
25.1.10 Plugins zu Nagios ... 825
25.1.11 Benachrichtigungen ... 831
25.1.12 Performance-Datenanalyse ... 833
25.1.13 Das Web-Frontend ... 836
25.2 Monitoring mit Munin ... 836

TEIL VII: Sicherheit, Verschlüsselung und Zertifikate

26 Sicherheit ... 841

26.1 Weniger ist mehr ... 842
26.2 »chroot« ... 842
26.2.1 Dienste ... 843
26.2.2 »jailkit« ... 845
26.3 Selbstabsicherung: »AppArmor« ... 849
26.4 Gotcha! Intrusion-Detection-Systeme ... 855
26.4.1 »snort« und Co. ... 856
26.4.2 Installation ... 858
26.4.3 Regeln – »oinkmaster« ... 860
26.4.4 Anwendung von Intrusion-Detection-Systemen in der Praxis ... 865
26.5 Klein, aber oho: »fail2ban« ... 867
26.6 Einmalpasswörter mit OPIE ... 872
26.7 OpenVPN ... 875
26.7.1 Serverinstallation – OpenVPN, PKI und Co. ... 876
26.7.2 Roadwarrior ... 883
26.7.3 Site-to-site ... 889
26.7.4 Simple-HA ... 891
26.7.5 Tipps und Tricks ... 892

27 Verschlüsselung und Zertifikate ... 897

27.1 Definition und Historie ... 897
27.2 Moderne Kryptologie ... 899
27.2.1 Symmetrische Verschlüsselung ... 899
27.2.2 Asymmetrische Verschlüsselung ... 900
27.3 Den Durchblick behalten ... 901
27.3.1 Das Grundproblem ... 901
27.3.2 Verwendungszwecke ... 902
27.3.3 Umsetzung mithilfe einer PKI ... 902

27.3.4 X.509 903
27.3.5 Ein anderer Ansatz: PGP (Web-of-Trust) 905
27.4 In der Praxis 906
27.4.1 Einrichtung einer PKI mit Server- und E-Mail-Zertifikaten 906
27.4.2 E-Mail-Verschlüsselung 916
27.5 Neben der Kommunikation – Dateiverschlüsselung 924
27.5.1 Dateien 924
27.5.2 Devices 925
27.5.3 Festplatten/System 928
27.6 Rechtliches 931
27.6.1 Fortgeschrittene elektronische Signatur 932
27.6.2 Qualifiziertes Zertifikat 932
27.6.3 Qualifizierte elektronische Signatur 932
27.6.4 Sichere Signaturerstellungseinheit (SSEE) 933

Die Autoren 935

Index 937