Auf einen Blick

TEIL I
Grundlagen 61

TEIL II
Aufgaben 187

TEIL III
Dienste 279

TEIL IV
Infrastruktur 779

TEIL V
Kommunikation 841

TEIL VI
Automatisierung 991

TEIL VII
Sicherheit, Verschlüsselung und Zertifikate 1047

Bibliografische Informationen
http://d-nb.info/104990401X

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

Inhalt

Vorwort 29
Über dieses Buch 37

1 Der Administrator 41

1.1 Der Beruf des Systemadministrators 41
1.1.1 Berufsbezeichnung und Aufgaben 41
1.1.2 Job-Definitionen 42
1.2 Nützliche Fähigkeiten und Fertigkeiten 47
1.2.1 Soziale Fähigkeiten 47
1.2.2 Arbeitstechniken 48
1.3 Das Verhältnis vom Administrator zu Normalsterblichen 49
1.3.1 Der Chef und andere Vorgesetzte 50
1.3.2 Benutzer 50
1.3.3 Andere Administratoren 51
1.4 Unterbrechungsgesteuertes Arbeiten 52
1.5 Einordnung der Systemadministration 53
1.5.1 Arbeitsgebiete 53
1.5.2 DevOps 55
1.6 Ethischer Verhaltenskodex 57
1.7 Administration – eine Lebenseinstellung? 59

TEIL I Grundlagen

2 Bootvorgang 63

2.1 Einführung 63
2.2 Der Bootloader GRUB 63
2.2.1 Installation 64
2.2.2 Konfiguration 66
2.2.3 Booten von einem Software-RAID-1 68

2.3 GRUB 2 69
2.3.1 Funktionsweise 69
2.3.2 Installation 69
2.3.3 Konfiguration 70
2.4 Bootloader Recovery 75
2.5 Der Kernel und die »initrd« 77
2.5.1 »initrd« erstellen und modifizieren 77
2.5.2 »initrd« manuell modifizieren 80
2.6 »Upstart« 81
2.6.1 Funktionsweise 82
2.6.2 Events im Detail 83
2.6.3 Prozessdefinitionen 85
2.6.4 Anzeige aller »Upstart«-Jobs 85
2.6.5 Anzeige und Überprüfung der Job-Konfigurationen 87
2.6.6 Starten, Stoppen und Neustarten von Diensten 89
2.6.7 Abschlussbemerkung 89

3 Festplatten und andere Devices 91

3.1 RAID 91
3.1.1 RAID-0 92
3.1.2 RAID-1 92
3.1.3 RAID-5 92
3.1.4 RAID-6 93
3.1.5 RAID-10 93
3.1.6 Zusammenfassung 94
3.1.7 Weich, aber gut: Software-RAID 95
3.1.8 Software-RAID unter Linux 96
3.1.9 Abschlussbemerkung zu RAIDs 103
3.2 Rein logisch: Logical Volume Manager »LVM« 104
3.2.1 Grundlagen und Begriffe 106
3.2.2 Setup 107
3.2.3 Aufbau einer Volume Group mit einem Volume 108
3.2.4 Erweiterung eines Volumes 111

3.2.5 Eine Volume Group erweitern ... 112
3.2.6 Spiegelung zu einem Volume hinzufügen ... 113
3.2.7 Eine defekte Festplatte ersetzen ... 115
3.2.8 Backups mit Snapshots ... 115
3.2.9 Mirroring ausführlich ... 119
3.2.10 Kommandos ... 123

3.3 »udev« ... 124
3.3.1 »udev«-Regeln ... 125
3.3.2 Eigene Regeln schreiben ... 126

3.4 Alles virtuell? »/proc« ... 129
3.4.1 CPU ... 129
3.4.2 RAM ... 130
3.4.3 Kernelkonfiguration ... 131
3.4.4 Kernelparameter ... 132
3.4.5 Gemountete Dateisysteme ... 132
3.4.6 Prozessinformationen ... 133
3.4.7 Netzwerk ... 134
3.4.8 Änderungen dauerhaft speichern ... 135
3.4.9 Abschlussbemerkung ... 135

4 Dateisysteme 137

4.1 Dateisysteme: von Bäumen, Journalen und einer Kuh ... 137
4.1.1 Bäume ... 138
4.1.2 Journale ... 140
4.1.3 Und die Kühe? COW-fähige Dateisysteme ... 141

4.2 Praxis ... 141
4.2.1 Ext2/3-FS aufgebohrt: mke2fs, tune2fs, dumpe2fs, e2label ... 141
4.2.2 ReiserFS und seine Tools ... 144
4.2.3 XFS ... 145
4.2.4 Das Dateisystem vergrößern oder verkleinern ... 146
4.2.5 Ausblick auf BtrFS ... 148

4.3 Fazit ... 150

5 Berechtigungen 151

5.1 User, Gruppen und Dateisystemstrukturen 151

5.2 Dateisystemberechtigungen 154

5.2.1 Spezialbits 155

5.3 Erweiterte Posix-ACLs 158

5.3.1 Das Setzen und Anzeigen von einfachen ACLs 159

5.3.2 Setzen von Default-ACLs 161

5.3.3 Setzen von erweiterten ACLs 162

5.3.4 Entfernen von ACLs 165

5.3.5 Sichern und Zurückspielen von ACLs 166

5.4 Erweiterte Dateisystemattribute 166

5.4.1 Attribute, die jeder Benutzer ändern kann 167

5.4.2 Attribute, die nur »root« ändern kann 168

5.4.3 Weitere Attribute 169

5.5 Quotas 169

5.5.1 Installation und Aktivierung der Quotas 169

5.5.2 Journaling-Quotas 171

5.5.3 Quota-Einträge verwalten 172

5.6 Pluggable Authentication Modules (PAM) 176

5.6.1 Verschiedene PAM-Typen 177

5.6.2 Die PAM-Kontrollflags 177

5.6.3 Argumente zu den Modulen 178

5.6.4 Modulpfade 178

5.6.5 Module und ihre Aufgaben 179

5.6.6 Die neuere Syntax bei der PAM-Konfiguration 180

5.7 Konfiguration von PAM 182

5.8 »ulimit« 183

5.8.1 Setzen der »ulimit«-Werte 184

5.9 Abschlussbemerkung 185

TEIL II Aufgaben

6 Paketmanagement 189

6.1 Paketverwaltung 189

6.1.1 »rpm« oder »deb«? 190

6.1.2 »yum«, »yast« oder »apt«? ... 192
6.1.3 Außerirdische an Bord – »alien« ... 194

6.2 Pakete im Eigenbau ... 195
6.2.1 Am Anfang war das Makefile ... 195
6.2.2 Vom Fellknäuel zum Paket ... 198
6.2.3 Patchen mit »patch« und »diff« ... 202
6.2.4 Updates ohne Repository ... 205
6.2.5 »rpm«-Update-Paket ... 205
6.2.6 »deb«-Update-Pakete ... 208
6.2.7 Updatesicher konfigurieren ... 209

6.3 Updates nur einmal laden: »Cache« ... 211
6.3.1 deb-basierte Distributionen: »apt-cacher-ng« ... 212
6.3.2 Installation ... 212
6.3.3 Konfiguration ... 212
6.3.4 Fütterungszeit – bereits geladene Pakete dem Cache hinzufügen ... 214
6.3.5 Aufräumen – Zweige aus dem Cache entfernen ... 215
6.3.6 Clientkonfiguration ... 216
6.3.7 Details: »Report-HTML« ... 216
6.3.8 rpm-basierte Distributionen ... 217

6.4 Alles meins: »Mirror« ... 217
6.4.1 deb-basierte Distributionen: »debmirror« ... 217
6.4.2 Konfiguration ... 218
6.4.3 Benutzer und Gruppe anlegen ... 218
6.4.4 Verzeichnisstruktur anlegen ... 219
6.4.5 Mirror-Skript erstellen (Ubuntu) ... 219
6.4.6 Cronjobs einrichten ... 222
6.4.7 Schlüssel importieren ... 222
6.4.8 Mirror erstellen ... 223
6.4.9 Mirror verfügbar machen – Webdienst konfigurieren ... 223
6.4.10 Clientkonfiguration ... 224
6.4.11 rpm-basierte Distributionen ... 225
6.4.12 Benutzer und Gruppe anlegen ... 225
6.4.13 Verzeichnisstruktur anlegen ... 226
6.4.14 Mirror-Skript erstellen ... 226
6.4.15 Cronjobs einrichten ... 227
6.4.16 Mirror erstellen ... 228
6.4.17 Mirror verfügbar machen – Webdienst konfigurieren ... 229
6.4.18 Clientkonfiguration ... 229

7 Backup und Recovery 231

7.1 Backup gleich Disaster Recovery? ... 231

7.2 Backupstrategien ... 232

7.3 Datensicherung mit »tar« ... 235

7.3.1 Weitere interessante Optionen für GNU-»tar« ... 236

7.3.2 Sicherung über das Netzwerk mit »tar« und »ssh« ... 237

7.4 Datensynchronisation mit »rsync« ... 238

7.4.1 Lokale Datensicherung mit »rsync« ... 238

7.4.2 Synchronisieren im Netzwerk mit »rsync« ... 239

7.4.3 Wichtige Optionen für »rsync« ... 239

7.4.4 Backupskript für die Sicherung auf einen Wechseldatenträger ... 241

7.4.5 Backupskript für die Sicherung auf einen Backupserver ... 242

7.4.6 Verwendung von »ssh« für die Absicherung von »rsync« ... 244

7.5 Imagesicherung mit »dd« ... 245

7.5.1 Sichern des Master Boot Records (MBR) ... 245

7.5.2 Partitionstabelle mithilfe von »dd« zurückspielen ... 246

7.5.3 Erstellen eines Images mit »dd« ... 246

7.5.4 Einzelne Dateien mit »dd« aus einem Image zurückspielen ... 247

7.5.5 Abschlussbemerkung zu »dd« ... 249

7.6 Disaster Recovery mit ReaR ... 249

7.6.1 ReaR konfigurieren ... 251

7.6.2 Aufrufparameter von ReaR ... 253

7.6.3 Der erste Testlauf ... 253

7.6.4 Der Recovery-Prozess ... 258

7.6.5 Die ReaR-Konfiguration im Detail ... 260

7.6.6 Migrationen mit ReaR ... 261

7.7 Backup und Recovery mit Bacula/Bareos ... 262

7.7.1 Das erste Backup: Der Bareos-Server sichert sich selbst ... 264

7.7.2 Einrichtung eines zu sichernden externen Clients ... 274

7.7.3 Sichern von MySQL und LDAP ... 277

7.7.4 Bareos und ReaR als Dreamteam ... 277

7.7.5 Bacula/Bareos für Fortgeschrittene ... 278

TEIL III Dienste

8 Webserver 281

8.1 Apache ... 281
8.1.1 Virtuelle Hosts einrichten ... 281
8.1.2 HTTPS konfigurieren ... 283
8.1.3 Benutzer-Authentisierung mit Kerberos ... 287
8.1.4 Apache-Server mit ModSecurity schützen ... 288
8.1.5 Tuning und Monitoring ... 291

8.2 LightHttpd ... 295
8.2.1 Virtuelle Hosts mit »mod_simple_vhost« einrichten ... 295
8.2.2 Virtuelle Hosts ohne »mod_simple_vhost« einrichten ... 296
8.2.3 HTTPS konfigurieren ... 297

8.3 Nginx ... 299
8.3.1 Grundlegende Konfiguration ... 299
8.3.2 Virtuelle Hosts ... 300
8.3.3 HTTPS mit Nginx ... 302

8.4 Logfiles auswerten ... 303

9 FTP-Server 307

9.1 Einstieg ... 307
9.1.1 Das File Transfer Protocol ... 307
9.1.2 vsftpd ... 308

9.2 Download-Server ... 308

9.3 Zugriff von Usern auf ihre Homeverzeichnisse ... 310

9.4 FTP über SSL (FTPS) ... 311

9.5 Anbindung an LDAP ... 313

10 Mailserver 315

10.1 Postfix ... 315
10.1.1 Grundlegende Konfiguration ... 316
10.1.2 Postfix als Relay vor Exchange, Dovecot oder anderen Backends ... 318

10.1.3 Die Postfix-Restrictions: der Schlüssel zu Postfix ... 320
10.1.4 Weiterleitungen und Aliase für Mailadressen ... 328
10.1.5 SASL/SMTP-Auth ... 329
10.1.6 SSL/TLS für Postfix einrichten ... 331

10.2 Antivirus- und Spam-Filter mit Amavisd-new, ClamAV und SpamAssassin ... 333
10.2.1 Installation ... 334
10.2.2 ClamAV konfigurieren ... 335
10.2.3 Updates für SpamAssassin konfigurieren ... 336
10.2.4 Amavisd-new konfigurieren ... 336
10.2.5 Eine Quarantäne mit Amavis betreiben ... 341
10.2.6 Postfix für die Verwendung mit Amavisd-new konfigurieren ... 343

10.3 POP3/IMAP-Server mit Dovecot ... 345
10.3.1 Vorbereitungen im Linux-System ... 345
10.3.2 Log-Meldungen und Debugging ... 346
10.3.3 User-Authentifizierung ... 347
10.3.4 Aktivierung des LMTP-Servers von Dovecot ... 348
10.3.5 Einrichten von SSL/TLS-Verschlüsselung ... 349

10.4 Der Ernstfall: Der IMAP-Server erwacht zum Leben ... 350

10.5 Monitoring und Logfile-Auswertung ... 352
10.5.1 Logfile-Auswertung mit »Lire« ... 353
10.5.2 Logfile-Auswertung mit »Pflogsumm« ... 356

11 Datenbank 359

11.1 MySQL in der Praxis ... 359
11.1.1 Installation und grundlegende Einrichtung ... 359
11.1.2 Replikation ... 360
11.1.3 Master-Master-Replikation ... 368

11.2 Tuning ... 371
11.2.1 Tuning des Speichers ... 371
11.2.2 Tuning von Indizes ... 378

11.3 Backup und Point-In-Time-Recovery ... 382
11.3.1 Restore zum letztmöglichen Zeitpunkt ... 382
11.3.2 Restore zu einem bestimmten Zeitpunkt ... 383

12 Syslog 385

12.1 Aufbau von Syslog-Nachrichten 385

12.2 Der Klassiker: »SyslogD« 387

12.3 Syslog-ng 388

12.3.1 Der »options«-Abschnitt 388

12.3.2 Das »source«-Objekt 390

12.3.3 Das »destination«-Objekt 390

12.3.4 Das »filter«-Objekt 392

12.3.5 Das »log«-Objekt 393

12.4 Rsyslog 394

12.4.1 Eigenschaftsbasierte Filter 394

12.4.2 Ausdrucksbasierte Filter 395

12.5 Loggen über das Netz 396

12.5.1 SyslogD 396

12.5.2 Syslog-ng 397

12.5.3 Rsyslog 397

12.6 Syslog in eine Datenbank schreiben 398

12.6.1 Anlegen der Log-Datenbank 398

12.6.2 In die Datenbank loggen 399

13 Proxy-Server 403

13.1 Einführung des Stellvertreters 403

13.2 Proxys in Zeiten des Breitbandinternets 404

13.3 Herangehensweisen und Vorüberlegungen 405

13.4 Grundkonfiguration 405

13.4.1 Aufbau des Testumfelds 406

13.4.2 Netzwerk 406

13.4.3 Cache 407

13.4.4 Logging 408

13.4.5 Handhabung des Dienstes 410

13.4.6 Objekte 412

13.4.7 Objekttypen 413

13.4.8 Objektlisten in Dateien 413

13.4.9 Regeln ... 414
13.4.10 Überlagerung mit »first match« ... 416
13.4.11 Anwendung von Objekten und Regeln ... 417

13.5 Authentifizierung ... 418
13.5.1 Benutzerbasiert ... 421
13.5.2 Gruppenbasiert ... 431

13.6 Helferlein ... 434
13.6.1 squidGuard ... 435
13.6.2 Antiviren-Check: ClamAV mit HAVP einbinden ... 437
13.6.3 Dansguardian ... 439

13.7 Log-Auswertung: »Calamaris« und »Sarg« ... 443
13.7.1 Calamaris ... 443
13.7.2 Sarg ... 444

13.8 Unsichtbar: »transparent proxy« ... 445

13.9 Ab in den Pool – Verzögerung mit »delay_pools« ... 447
13.9.1 Funktionsweise – alles im Eimer! ... 447
13.9.2 Details – Klassen, Eimer und ACLs richtig wählen ... 448

13.10 Familienbetrieb: »Sibling, Parent und Co.« ... 450
13.10.1 Grundlagen ... 450
13.10.2 Eltern definieren ... 452
13.10.3 Geschwister definieren ... 452
13.10.4 Load Balancing ... 453
13.10.5 Inhalte eigenständig abrufen: »always_direct« ... 453

13.11 Cache-Konfiguration ... 454
13.11.1 Cache-Arten: »Hauptspeicher« und »Festplatten« ... 454
13.11.2 Hauptspeicher-Cache ... 454
13.11.3 Festplatten-Cache ... 455
13.11.4 Tuning ... 458

14 Kerberos ... 459

14.1 Begriffe im Zusammenhang mit Kerberos ... 460

14.2 Funktionsweise von Kerberos ... 461

14.3 Installation und Konfiguration des Kerberos-Servers ... 461
14.3.1 Konfiguration der Datei »/etc/krb5.conf« ... 462
14.3.2 Konfiguration der Datei »kdc.conf« ... 464

14.4 Initialisierung und Testen des Kerberos-Servers 466
14.4.1 Verwalten der Principals 468
14.5 Kerberos und PAM 472
14.5.1 Konfiguration der PAM-Dateien auf dem SLES11 472
14.5.2 Testen der Anmeldung 473
14.6 Neue Benutzer mit Kerberos-Principal anlegen 473
14.7 Hosts und Dienste 474
14.7.1 Entfernen von Einträgen 475
14.8 Konfiguration des Kerberos-Clients 477
14.8.1 PAM und Kerberos auf dem Client 478
14.9 Replikation des Kerberos-Servers 478
14.9.1 Bekanntmachung aller KDCs im Netz 478
14.9.2 Konfiguration des KDC-Masters 482
14.9.3 Konfiguration des KDC-Slaves 483
14.9.4 Replikation des KDC-Masters auf den KDC-Slave 484
14.10 Kerberos Policies 486
14.11 Kerberos im LDAP einbinden 488
14.11.1 Konfiguration des LDAP-Servers 488
14.11.2 Umstellung des Kerberos-Servers 491
14.11.3 Zurücksichern der alten Datenbank 494
14.11.4 Bestehende LDAP-Benutzer um Kerberos-Principal erweitern 495
14.11.5 Anbinden des zweiten KDCs an den LDAP 500

15 Samba 501

15.1 Kurze Einführung in die Protokolle SMB und NetBIOS 502
15.1.1 Das Protokoll SMB 504
15.1.2 Das Protokoll NetBIOS 504
15.1.3 Möglichkeiten mit NetBIOS 505
15.1.4 Grundeinstellung der »smb.conf« 505
15.1.5 Verwendung von WINS zur Namensauflösung 507
15.1.6 Parameter für den »nmbd«in der »smb.conf« 508
15.1.7 Clientkonfiguration 510
15.2 Samba als Fileserver 511
15.2.1 Erstellen einfacher Freigaben 511
15.2.2 Spezielle Freigaben 514

15.2.3 Zusammenfassung mehrerer Freigaben ... 516
15.2.4 Kopieren von Freigabeeinstellungen ... 517
15.2.5 Freigaben in der Registry verwalten ... 517
15.2.6 Erstellen einer Freigabe in der Registry ... 520
15.2.7 Zugriff auf eine Freigabe aus der Registry ... 520
15.2.8 Erweitern einer Freigabe in der Registry ... 521
15.2.9 Sichern der Freigabeeinstellungen aus der Registry ... 521
15.2.10 Löschen einer Freigabe aus der Registry ... 522
15.2.11 Wiederherstellen von Freigaben in der Registry ... 522
15.2.12 Ablauf des Zugriffs auf eine Freigabe ... 523

15.3 Benutzerverwaltung ... 526
15.3.1 Anlegen der Benutzer in der »smbpasswd« ... 527
15.3.2 Umwandeln der »smbpasswd« in »tdbsam« ... 529

15.4 Verschiedene »passdb backends« ... 530
15.4.1 »smbpasswd« ... 530
15.4.2 »tdbsam« ... 531
15.4.3 »ldapsam« ... 532

15.5 Samba als Domänencontroller ... 534
15.5.1 Grundeinstellung des Domänencontrollers ... 535
15.5.2 Weitere Möglichkeiten mit »rpcclient« ... 536
15.5.3 Einrichten eines Domänenadministrators ... 542
15.5.4 Kennwortrichtlinien mit »pdbedit« erstellen ... 544
15.5.5 Einrichten von Benutzern und Hosts in der Domäne ... 546
15.5.6 Benutzeranmeldung ... 553

15.6 Winbind ... 554
15.6.1 Verschachtelte Gruppen ... 557
15.6.2 Mitgliedschaft in einer Windows-Domäne ... 560
15.6.3 Konfiguration des Kerberos-Clients ... 561
15.6.4 Einstellung in der »smb.conf« ... 563
15.6.5 Beitritt zur Windows-Domäne ... 565
15.6.6 Testen der Domänenmitgliedschaft ... 567
15.6.7 Freigaben und Berechtigungen als Domänenmitglied ... 569

15.7 Samba als Printserver ... 572
15.7.1 Freigaben für Druckertreiber und Spooling ... 573
15.7.2 Einrichtung eines Printeradmins ... 574
15.7.3 Installation von Windows-Druckertreibern ... 574
15.7.4 Zuordnung des Druckertreibers ... 577

15.8 Samba und Kerberos ... 578

15.9 Virtuelle Server und virtuelle Domänen 582
15.9.1 Zusammenführung der Server in jeder Arbeitsgruppe 583
15.9.2 Zusammenführen der zwei Arbeitsgruppen auf einer Maschine 584
15.10 Distributed File System mit Samba 588
15.10.1 Samba als DFS-Proxy 588
15.10.2 Samba als DFS-Link-Server 589
15.11 Vertrauensstellung 590
15.11.1 Der Samba-Server als vertrauende Domäne 592
15.11.2 Der Samba-Server als vertraute Domäne 592
15.12 Sicherung der Konfigurationen 594

16 Samba 4 597

16.1 Vorbereitung für die Installation 597
16.1.1 Installation der Pakete unter Debian und Ubuntu 598
16.1.2 Installation der Pakete auf einem SLES11 598
16.2 Konfiguration von Samba 4 als Domaincontroller 599
16.2.1 Erster Start des DC unter Debian und Ubuntu 603
16.2.2 Erster Start des DC auf dem SLES11 603
16.3 Testen des Domaincontrollers 604
16.3.1 Testen der Serverports 604
16.3.2 Testen des DNS-Servers 605
16.3.3 Test des Verbindungsaufbaus 606
16.3.4 Test des Kerberos-Servers 606
16.4 Benutzer- und Gruppenverwaltung 607
16.5 Benutzer- und Gruppenverwaltung über die Kommandozeile 608
16.5.1 Verwaltung von Gruppen über die Kommandozeile 608
16.5.2 Verwaltung von Benutzern über die Kommandozeile 612
16.6 Die »Remote Server Administration Tools«(RSAT) 617
16.6.1 Einrichtung der »RSAT« 617
16.6.2 Beitritt eines Windows-Clients zur Domäne 617
16.6.3 Benutzer- und Gruppenverwaltung mit den »RSAT« 620
16.7 Gruppenrichtlinien 621
16.7.1 Verwaltung der GPOs mit den RSAT 621
16.7.2 Erste Schritte mit dem Gruppenrichtlinieneditor 621
16.7.3 Erstellen einer Gruppenrichtlinie 623

16.7.4 Verknüpfung der Gruppenrichtlinie mit einer OU 626
16.7.5 Verschieben der Benutzer und Gruppen 628
16.7.6 GPOs über die Kommandozeile 629

16.8 Linux-Client in der Domäne 630
16.8.1 Konfiguration der Authentifizierung 636
16.8.2 Mounten über »pam_mount« 637
16.8.3 Vorbereitung auf dem SLES11 638

16.9 Zusätzliche Server in der Domäne 640
16.9.1 Einrichtung eines Fileservers 640
16.9.2 Ein zusätzlicher Domaincontroller 641
16.9.3 Konfiguration des zweiten DC 642

16.10 Was geht noch mit Samba 4? 650

17 NFS 651

17.1 Unterschiede zwischen »NFSv3«und »NFSv4« 651

17.2 Funktionsweise von »NFSv4« 652

17.3 Einrichten des »NFSv4«-Servers 653
17.3.1 Konfiguration des Pseudodateisystems 653
17.3.2 Anpassen der Datei »/etc/exports« 654
17.3.3 Tests für den NFS-Server 656

17.4 Konfiguration des »NFSv4«-Clients 658

17.5 Konfiguration des »idmapd« 659

17.6 Optimierung von »NFSv4« 661
17.6.1 Optimierung des »NFSv4«-Servers 661
17.6.2 Optimierung des »NFSv4«-Clients 662

17.7 »NFSv4« und Firewalls 663

17.8 NFS und Kerberos 664
17.8.1 Erstellung der Principals und der »keytab«-Dateien 665
17.8.2 Kerberos-Authentifizierung unter Debian und Ubuntu 667
17.8.3 Kerberos-Authentifizierung auf einem SLES11 667
17.8.4 Anpassen der Datei »/etc/exports« 668
17.8.5 NFS-Client für Kerberos unter Debian und Ubuntu konfigurieren 668
17.8.6 NFS-Client für Kerberos auf SLES11 konfigurieren 668
17.8.7 Testen der durch Kerberos abgesicherten NFS-Verbindung 669
17.8.8 Testen der Verbindung 669

18 LDAP 671

18.1 Einige Grundlagen zu LDAP ... 672
18.1.1 Was ist ein Verzeichnisdienst? ... 672
18.1.2 Der Einsatz von LDAP im Netzwerk ... 673
18.1.3 Aufbau des LDAP-Datenmodells ... 673
18.1.4 Objekte ... 674
18.1.5 Attribute ... 675
18.1.6 Schema ... 675
18.1.7 Das LDIF-Format ... 679

18.2 Unterschiede in den einzelnen Distributionen ... 680
18.2.1 Umstellung auf die statische Konfiguration unter SLES11 ... 680
18.2.2 Umstellung auf die statische Konfiguration unter Ubuntu-Server und Debian ... 681
18.2.3 Pfade und Benutzer ... 681
18.2.4 Die Datenbank-Backends ... 681
18.2.5 Grundkonfiguration des LDAP-Servers ... 681

18.3 Konfiguration des LDAP-Clients ... 684
18.3.1 Konfiguration des Clients auf dem SLES11 ... 684
18.3.2 Konfiguration des Clients unter Debian »Squeeze« ... 685
18.3.3 Konfiguration des LDAP-Clients unter Ubuntu-Server ... 686
18.3.4 Erster Zugriff auf den LDAP-Server ... 687

18.4 Grafische Werkzeuge für die LDAP-Verwaltung ... 688
18.4.1 Konfiguration des »LAM« ... 690
18.4.2 Konfiguration des Lamdaemons ... 691

18.5 Änderungen mit »ldapmodify« ... 694
18.5.1 Interaktive Änderung mit »ldapmodify« ... 694
18.5.2 Änderungen über eine »ldif«-Datei mit »ldapmodify« ... 695

18.6 Absichern der Verbindung zum LDAP-Server über TLS ... 696
18.6.1 Erstellen der Zertifizierungsstelle ... 697
18.6.2 Erstellen des Serverzertifikats ... 697
18.6.3 Signieren des Zertifikats ... 697
18.6.4 Zertifikate in die »slapd.conf«eintragen ... 698
18.6.5 Konfiguration des LDAP-Clients ... 698

18.7 Absichern des LDAP-Baums mit ACLs ... 699
18.7.1 Eine eigene Datei für die ACLs einbinden ... 700
18.7.2 Erste ACLs zur Grundsicherung des DIT ... 701
18.7.3 ACLs mit regulären Ausdrücken ... 702

18.7.4 ACLs für den Einsatz von Samba im LDAP ... 703
18.7.5 Testen von ACLs vor dem Einsatz ... 704

18.8 Filter zur Suche im LDAP-Baum ... 706
18.8.1 Testen der Fähigkeiten des LDAP-Servers ... 706
18.8.2 Einfache Filter ... 707
18.8.3 Filter mit logischen Verknüpfungen ... 708
18.8.4 Einschränkung der Suchtiefe ... 709

18.9 Verwendung von Overlays ... 710
18.9.1 Overlays am Beispiel von »dynlist« ... 710
18.9.2 Weitere Overlays ... 712

18.10 Partitionierung des DIT ... 712
18.10.1 Einrichtung von »subordinate«-Datenbanken ... 713
18.10.2 Verwaltung von »Referrals« ... 715
18.10.3 Automatisierung des »chaining« ... 719
18.10.4 Administration der beiden Teilbäume ... 721

18.11 Replikation des DIT ... 723
18.11.1 Konfiguration des Providers ... 724
18.11.2 Konfiguration des Consumers ... 726

18.12 Die dynamische Konfiguration ... 728
18.12.1 Umstellung auf die dynamische Konfiguration am Provider ... 729
18.12.2 Umstellung auf die dynamische Konfiguration am Consumer ... 733

18.13 Verwaltung von Weiterleitungen für den Mailserver Postfix ... 735

18.14 Benutzerauthentifizierung von Dovecot über LDAP ... 738

18.15 Benutzerauthentifizierung am Proxy Squid über LDAP ... 740
18.15.1 Aktivierung der Authentifizierung über LDAP ... 741
18.15.2 Benutzerbezogene Authentifizierung ... 742
18.15.3 Gruppenbezogene Authentifizierung ... 742

18.16 Benutzerauthentifizierung am Webserver Apache über LDAP ... 744
18.16.1 Konfiguration der Cache-Parameter ... 744
18.16.2 Konfiguration der Zugriffsparameter ... 745

18.17 LDAP und Kerberos ... 747

18.18 Authentifizierung am LDAP-Server über »GSSAPI« ... 749
18.18.1 Einrichtung der Authentifizierung unter Debian und Ubuntu ... 749
18.18.2 Einrichten der Authentifizierung unter SLES11 ... 755

18.19 Und was geht sonst noch alles mit LDAP? ... 759

19 Druckserver 761

19.1 Policies 762
19.1.1 Grundkonfiguration des Netzwerkzugriffs 762
19.1.2 Location policies 763
19.1.3 Operation policies 765
19.1.4 Weitere Konfigurationsmöglichkeiten 766
19.1.5 Browsing 768

19.2 Drucker und Klassen einrichten und verwalten 769
19.2.1 Drucker einrichten 769
19.2.2 Klassen einrichten 770

19.3 Druckerquotas 771

19.4 CUPS über die Kommandozeile 772
19.4.1 Einstellen eines Standarddruckers 772
19.4.2 Optionen für einen Drucker verwalten 773

19.5 PPD-Dateien 775

19.6 CUPS und Kerberos 776
19.6.1 Erstellen des Kerberos-Principals und der »keytab«-Datei 776
19.6.2 Umstellung der Authentifizierung am CUPS-Server 777

19.7 Noch mehr Druck 778

TEIL IV Infrastruktur

20 Hochverfügbarkeit 781

20.1 Das Beispiel-Setup 781

20.2 Installation 782
20.2.1 Ubuntu 12.04 LTS und 14.04 LTS 782
20.2.2 Debian 6 und 7 (»Squeeze« und »Wheezy«) 782
20.2.3 Debian 5.0 (»Lenny«) 782
20.2.4 openSUSE 783
20.2.5 SUSE Linux Enterprise Server 783

20.3 Einfache Vorarbeiten 783

20.4 Shared Storage mit DRBD 784
20.4.1 Grundlegende Konfiguration unter Debian und SUSE 785
20.4.2 Grundlegende Konfiguration unter Ubuntu LTS 785

20.4.3 Die wichtigsten Konfigurationsoptionen ... 786
20.4.4 Die DRBD-Ressource in Betrieb nehmen ... 787

20.5 Grundkonfiguration der Clusterkomponenten ... 790
20.5.1 OpenAIS und Corosync: das Benachrichtigungssystem ... 791
20.5.2 Pacemaker: der Ressourcen-Manager ... 792
20.5.3 Quorum deaktivieren ... 794

20.6 Dienste hochverfügbar machen ... 796
20.6.1 Die erste Ressource: eine hochverfügbare IP-Adresse ... 797
20.6.2 Hochverfügbarkeit am Beispiel von Apache ... 799
20.6.3 DRBD integrieren ... 801
20.6.4 Fencing ... 804

21 Virtualisierung 807

21.1 Einleitung ... 807

21.2 Für den »Sysadmin« ... 808

21.3 Servervirtualisierung ... 812
21.3.1 KVM ... 813
21.3.2 Xen ... 815

21.4 Netzwerkgrundlagen ... 816

21.5 Management und Installation ... 819
21.5.1 Einheitlich arbeiten: »libvirt« ... 819
21.5.2 Konsolenbasiertes Management: »virsh« ... 823
21.5.3 Virtuelle Maschinen installieren ... 827
21.5.4 »virt-install« ... 829
21.5.5 Alleskönner: »Virtual Machine Manager« ... 831
21.5.6 Zusätzliche Konsolentools ... 835

21.6 Umzugsunternehmen: Live Migration ... 837
21.6.1 Vorbereitungen ... 837
21.6.2 Konfiguration im »Virtual Machine Manager« ... 839

TEIL V Kommunikation

22 Netzwerk 843

22.1 Netzwerkkonfiguration mit »iproute2« 843

22.1.1 Erste Schritte 844
22.1.2 Syntax von »ip« 846
22.1.3 Links ansehen und manipulieren: »ip link« 846
22.1.4 IP-Adressen ansehen und manipulieren: »ip address« 849
22.1.5 Manipulation von ARP-Einträgen: »ip neighbour« 853

22.2 Routing mit »ip« 855

22.2.1 Routing-Informationen anzeigen 855
22.2.2 Da geht noch mehr: »Advanced Routing« 857
22.2.3 Die vorhandenen Regeln ansehen 857
22.2.4 Eine neue Routing-Tabelle anlegen 859
22.2.5 Ändern der »Policy Routing Database« 859
22.2.6 Routing über mehrere Uplinks 861
22.2.7 Fazit bis hierher 866

22.3 Bonding 866

22.3.1 Bonding-Konfiguration 867
22.3.2 Bonding bei Debian und Ubuntu 870
22.3.3 Bonding bei SLES 870

22.4 IPv6 871

22.4.1 Die Vorteile von IPv6 872
22.4.2 Notation von IPv6-Adressen 873
22.4.3 Die Netzmasken 874
22.4.4 Die verschiedenen IPv6-Adressarten 874
22.4.5 Es geht auch ohne »ARP« 876
22.4.6 Feste Header-Länge 877
22.4.7 IPv6 in der Praxis 879

22.5 Firewalls mit »netfilter« und »iptables« 881

22.5.1 Der Weg ist das Ziel – wie Pakete durch den Kernel laufen 881
22.5.2 Einführung in »iptables« 882
22.5.3 Regeln definieren 884
22.5.4 Die klassischen Targets 886
22.5.5 Ein erster Testlauf 886

22.5.6 Rein wie raus: »Stateful Packet Inspection« ... 887
22.5.7 Das erste Firewallskript ... 889
22.5.8 Externe Firewall ... 891
22.5.9 Logging ... 897
22.5.10 Network Address Translation und Masquerading ... 899
22.5.11 Weitere nützliche Module für »iptables« ... 900
22.6 Abschlussbemerkung ... 903
22.7 DHCP ... 903
22.7.1 Funktionsweise ... 903
22.7.2 Konfiguration ... 904
22.8 DNS-Server ... 907
22.8.1 Funktionsweise ... 907
22.8.2 Unterschied: rekursiv und autoritativ ... 909
22.8.3 Einträge im DNS: »Resource Records« ... 909
22.8.4 Die Grundkonfiguration ... 910
22.8.5 Zonendefinitionen ... 913
22.8.6 Die erste vollständige Zone ... 917
22.8.7 Die »hint«-Zone ... 919
22.8.8 Reverse Lookup ... 921
22.8.9 Slave-Server ... 922
22.8.10 DNS-Server und IPv6 ... 924
22.9 Nachwort zum Thema Netzwerk ... 926

23 OpenSSH 927

23.1 Die SSH-Familie ... 927
23.1.1 Die Clients: »ssh«, »scp«, »sftp« ... 928
23.1.2 Der Server: »sshd« ... 930
23.2 Schlüssel statt Passwort ... 932
23.2.1 Schlüssel erzeugen ... 932
23.2.2 Passwortloses Login ... 933
23.2.3 Der SSH-Agent merkt sich Passphrasen ... 934
23.3 X11-Forwarding ... 935
23.4 Portweiterleitung und Tunneling ... 936
23.4.1 SshFS: entfernte Verzeichnisse lokal einbinden ... 937

24 Administrationstools 939

24.1 Was kann dies und jenes noch? 939
24.1.1 Der Rsync-Daemon 939
24.1.2 Wenn's mal wieder später wird: »screen« 941
24.1.3 Anklopfen mit »nmap« 941
24.1.4 Netzwerkinspektion: »netstat« 945
24.1.5 Zugreifende Prozesse finden: »lsof« 947
24.1.6 Was macht mein System? »top«! 951
24.1.7 Wenn gar nichts mehr geht – Debugging mit »strace« 956
24.1.8 Prüfung der Erreichbarkeit mit »My traceroute« 961
24.1.9 Subnetzberechnung mit »ipcalc« 961

24.2 Aus der Ferne – Remote-Administrationstools 963
24.2.1 PuTTY 963
24.2.2 WinSCP 966
24.2.3 Synergy 967
24.2.4 Eine für immer: »mosh« 970

25 Versionskontrolle 973

25.1 Philosophien 974
25.1.1 Lokal 974
25.1.2 Zentral 975
25.1.3 Dezentral 976

25.2 Versionskontrollsysteme 977
25.2.1 CVS 977
25.2.2 Apache Subversion 980
25.2.3 GNU Bazaar 982
25.2.4 Mercurial 984
25.2.5 Git 986

25.3 Kommandos 989

TEIL VI Automatisierung

26 Scripting 993

26.1 Aufgebohrte Muscheln ... 993

26.2 Vom Suchen und Finden: ein kurzer Überblick ... 994

26.2.1 Die Detektive: »grep«, »sed« und »AWK« ... 994

26.2.2 Reguläre Ausdrücke verstehen und anwenden ... 995

26.3 Fortgeschrittene Shell-Programmierung ... 998

26.3.1 Expansionsschemata ... 998

26.3.2 Umgebungsvariablen ... 1003

26.3.3 »Back to bash«: ein tieferer Blick in die Muschel ... 1004

26.3.4 Logging in Skripten ... 1008

26.4 Tipps und Tricks aus der Praxis ... 1011

26.4.1 Aufräumkommando ... 1011

26.4.2 IFS ... 1012

26.4.3 Datumsmagie ... 1012

26.4.4 E-Mails aus einem Skript versenden ... 1013

26.4.5 Interaktive Programme steuern ... 1013

27 Monitoring – wissen, was läuft 1015

27.1 Nagios ... 1016

27.1.1 Installation ... 1017

27.1.2 Allgemeine Konfiguration ... 1020

27.1.3 Konfiguration der Objekte ... 1021

27.1.4 Eigene Hosts und Services konfigurieren ... 1030

27.1.5 Benachrichtigungen ... 1032

27.1.6 NRPE – Partitionsfüllstand und andere lokale Werte remote überprüfen 1035

27.1.7 PNP4Nagios – grafische Aufbereitung der Messwerte ... 1039

27.2 Monitoring mit Munin ... 1043

27.3 Fazit ... 1045

TEIL VII Sicherheit, Verschlüsselung und Zertifikate

28 Sicherheit 1049

28.1 Weniger ist mehr ... 1050

28.2 »chroot« ... 1051

28.2.1 Dienste ... 1051

28.2.2 »jailkit« ... 1053

28.3 Selbstabsicherung: »AppArmor« ... 1056

28.3.1 Status und Betriebsarten ... 1057

28.3.2 Eigene Profile erstellen ... 1060

28.4 Gotcha! Intrusion-Detection-Systeme ... 1064

28.4.1 »snort« und Co. ... 1064

28.4.2 Installation ... 1066

28.4.3 Regeln – »oinkmaster« ... 1068

28.4.4 Anwendung von Intrusion-Detection-Systemen in der Praxis ... 1073

28.5 Klein, aber oho: »fail2ban« ... 1075

28.5.1 Konfiguration ... 1075

28.5.2 Aktive Sperrungen ... 1078

28.5.3 Reguläre Ausdrücke ... 1079

28.6 OpenVPN ... 1080

28.6.1 Serverinstallation – OpenVPN, PKI und Co. ... 1081

28.6.2 Roadwarrior ... 1088

28.6.3 Site-to-site ... 1093

28.6.4 Simple-HA ... 1095

28.6.5 Tipps und Tricks ... 1097

29 Verschlüsselung und Zertifikate 1103

29.1 Definition und Historie ... 1103

29.2 Moderne Kryptologie ... 1105

29.2.1 Symmetrische Verschlüsselung ... 1105

29.2.2 Asymmetrische Verschlüsselung ... 1106

29.3 Den Durchblick behalten ... 1107

29.3.1 Das Grundproblem ... 1107

29.3.2 Verwendungszwecke ... 1108

29.3.3 Umsetzung mithilfe einer PKI ... 1108
29.3.4 X.509 ... 1109
29.3.5 Ein anderer Ansatz: PGP (Web-of-Trust) ... 1111

29.4 In der Praxis ... 1112
29.4.1 Einrichtung einer PKI mit Server- und E-Mail-Zertifikaten ... 1112
29.4.2 E-Mail-Verschlüsselung ... 1123

29.5 Neben der Kommunikation – Dateiverschlüsselung ... 1130
29.5.1 Dateien ... 1130
29.5.2 Devices ... 1131
29.5.3 Festplatten/System ... 1133

29.6 Rechtliches ... 1137
29.6.1 Fortgeschrittene elektronische Signatur ... 1138
29.6.2 Qualifiziertes Zertifikat ... 1138
29.6.3 Qualifizierte elektronische Signatur ... 1138
29.6.4 Sichere Signaturerstellungseinheit (SSEE) ... 1139

Die Autoren ... 1141

Index ... 1143