

Inhalt

Vorwort	21
Über dieses Buch	27
Formales	27
Linux-Distributionen	29

1 Der Administrator 31

1.1 Der Beruf des Systemadministrators	31
1.1.1 Berufsbezeichnung und Aufgaben	31
1.1.2 Job-Definitionen	32
1.2 Nützliche Fähigkeiten und Fertigkeiten	37
1.2.1 Soziale Fähigkeiten	37
1.2.2 Arbeitstechniken	38
1.3 Das Verhältnis vom Administrator zu Normalsterblichen	40
1.3.1 Der Chef und andere Vorgesetzte	40
1.3.2 Benutzer	41
1.3.3 Andere Administratoren	41
1.4 Unterbrechungsgesteuertes Arbeiten	42
1.5 Ethischer Verhaltenskodex	43

TEIL I: Grundlagen

2 Bootvorgang 47

2.1 Einführung	47
2.2 Der Bootloader GRUB	47
2.2.1 Installation	48
2.2.2 Konfiguration	50
2.2.3 Booten von einem Software-RAID-1	51
2.3 GRUB 2	52
2.3.1 Funktionsweise	52
2.3.2 Installation	52
2.3.3 Konfiguration	52
2.4 Bootloader Recovery	56
2.5 Der Kernel und die »initrd«	57
2.5.1 »initrd« erstellen und modifizieren	58
2.5.2 »initrd« manuell modifizieren	61
2.6 »Upstart«	62

2.6.1	Funktionsweise	62
2.6.2	Events im Detail	63
2.6.3	Prozessdefinitionen	64
2.6.4	Starten und Stoppen von Diensten	65
2.6.5	Abschlussbemerkung	66

3 Festplatten und andere Devices 67

3.1	RAID	67
3.1.1	RAID-0	68
3.1.2	RAID-1	68
3.1.3	RAID-5	68
3.1.4	RAID-6	69
3.1.5	RAID-10	69
3.1.6	Zusammenfassung	69
3.1.7	Weich, aber gut: Software-RAID	70
3.1.8	Software-RAID unter Linux	71
3.1.9	Abschlussbemerkung zu RAIDs	77
3.2	Rein logisch: LVM	78
3.2.1	Grundlagen und Begriffe	80
3.2.2	Setup	81
3.2.3	Aufbau einer Volume Group mit einem Volume	82
3.2.4	Erweiterung eines Volumes	85
3.2.5	Eine Volume Group erweitern	86
3.2.6	Aufbau eines gespiegelten Volumes	87
3.2.7	Eine defekte Festplatte ersetzen	89
3.2.8	Kommandos	89
3.3	udev	91
3.3.1	»udev«-Regeln	91
3.3.2	Eigene Regeln schreiben	92
3.4	Alles virtuell? »/proc«	95
3.4.1	CPU	95
3.4.2	RAM	96
3.4.3	Kernelkonfiguration	97
3.4.4	Kernelparameter	97
3.4.5	Gemountete Dateisysteme	97
3.4.6	Prozessinformationen	98
3.4.7	Netzwerk	99
3.4.8	Änderungen dauerhaft speichern	99
3.4.9	Abschlussbemerkung	100

4 Dateisysteme 101

4.1	Dateisysteme: Von Bäumen, Journalen und einer Kuh	101
4.1.1	Bäume	102
4.1.2	Journalen	104
4.1.3	Und die Kühe? COW-fähige Dateisysteme	104
4.2	Praxis	105
4.2.1	Ext2/3-FS aufgebohrt: mke2fs, tune2fs, dumpe2fs, e2label	105
4.2.2	ReiserFS und seine Tools	108
4.2.3	XFS	109
4.2.4	Das Dateisystem vergrößern oder verkleinern	110
4.2.5	Ausblick auf BtrFS	112

5 Berechtigungen 113

5.1	User, Gruppen und Dateisystemstrukturen	113
5.2	Dateisystemberechtigungen	116
5.2.1	Spezialbits	117
5.3	Erweiterte Posix-ACLs	120
5.3.1	Das Setzen und Anzeigen von einfachen ACLs	121
5.3.2	Setzen von Default-ACLs	123
5.3.3	Setzen von erweiterten ACLs	124
5.3.4	Entfernen von ACLs	127
5.3.5	Sichern und Zurückspielen von ACLs	128
5.4	Erweiterte Dateisystemattribute	128
5.4.1	Attribute, die jeder Benutzer ändern kann	129
5.4.2	Attribute, die nur »root« ändern kann	129
5.4.3	Weitere Attribute	130
5.5	Quotas	131
5.5.1	Installation und Aktivierung der Quotas	131
5.5.2	Journaling Quotas	133
5.5.3	Quota-Einträge verwalten	134
5.6	PAM	138
5.6.1	Verschiedene PAM-Typen	138
5.6.2	Die PAM-Kontrollflags	139
5.6.3	Argumente zu den Modulen	140
5.6.4	Modulpfade	140
5.6.5	Module und ihre Aufgaben	140
5.6.6	Konfiguration von PAM	142

5.7	Ulimit	143
5.7.1	Setzen der »ulimit«-Werte	144
5.8	Zusammenfassung	145

TEIL II: Aufgaben

6 Paketmanagement 149

6.1	Paketverwaltung	149
6.1.1	»rpm« oder »deb«?	150
6.1.2	»yum«, »yast« oder »apt«?	152
6.1.3	Außerirdische an Bord – »alien«	154
6.2	Pakete im Eigenbau	155
6.2.1	Am Anfang war das Makefile	155
6.2.2	Vom Fellknäuel zum Paket	158
6.2.3	Patchen mit »patch« und »diff«	162
6.2.4	Updates ohne Repository	165
6.2.5	»rpm«-Update-Paket	165
6.2.6	»deb«-Update-Pakete	168
6.2.7	Update-sicher konfigurieren	169

7 Backup und Recovery 173

7.1	Backup gleich Disaster Recovery?	173
7.2	Backupstrategien	174
7.3	Datensicherung mit »tar«	176
7.3.1	Weitere interessante Optionen für GNU-»tar«	178
7.3.2	Sicherung über das Netzwerk mit »tar« und »ssh«	179
7.4	Datensynchronisation mit »rsync«	179
7.4.1	Lokale Datensicherung mit »rsync«	180
7.4.2	Synchronisieren im Netzwerk mit »rsync«	180
7.4.3	Wichtige Optionen für »rsync«	181
7.4.4	Backupsript für die Sicherung auf einen Wechseldatenträger	183
7.4.5	Backupsript für Sicherungen auf einen Backupserver	183
7.4.6	Verwendung von »ssh« für die Absicherung von »rsync«	185
7.5	Imagesicherung mit »dd«	186
7.5.1	Sichern des MBR	187
7.5.2	Partitionstabelle mithilfe von »dd« zurückspielen	188
7.5.3	Erstellen eines Images mit »dd«	188
7.5.4	Einzelne Dateien mit »dd« aus einem Image zurückspielen	189
7.5.5	Abschlussbemerkung zu »dd«	191

7.6	Disaster Recovery mit ReaR	191
7.6.1	ReaR installieren	192
7.6.2	ReaR konfigurieren	192
7.6.3	Die erste Konfiguration	194
7.6.4	ReaR aufrufen	194
7.6.5	Der erste Testlauf	195
7.6.6	Der Recovery-Prozess	198
7.6.7	Die ReaR-Konfiguration im Detail	199
7.6.8	Migrationen mit ReaR	200
7.6.9	Abschlussbemerkung	201
7.7	Fazit zur Datensicherung und Recovery	202

TEIL III: Dienste

8 Webserver 205

8.1	Apache	205
8.1.1	Virtuelle Hosts einrichten	205
8.1.2	HTTPS konfigurieren	207
8.1.3	Apache-Server mit ModSecurity schützen	210
8.1.4	Tuning und Monitoring	213
8.2	LightHttpd	217
8.2.1	Virtuelle Hosts mit »mod_simple_vhost« einrichten	217
8.2.2	Virtuelle Hosts ohne »mod_simple_vhost« einrichten	218
8.2.3	HTTPS konfigurieren	219
8.3	Logfiles auswerten	221

9 Mailserver 225

9.1	Postfix	225
9.1.1	Grundlegende Konfiguration	225
9.1.2	Integrierte Sicherheitsmechanismen	227
9.1.3	Antivirus- und Spamfilter mit Amavisd-new, ClamAV und SpamAssassin	230
9.2	Exim	239
9.2.1	Grundlegende Konfiguration	240
9.2.2	Viren erkennen	241
9.2.3	Spam abwehren	241
9.3	Monitoring und Logfile-Auswertung	244
9.3.1	Logfile-Auswertung mit »Lire«	244

10 Datenbank 249

10.1	MySQL in der Praxis	249
10.1.1	Installation und grundlegende Einrichtung	249
10.1.2	Replikation	250
10.1.3	Master-Master-Replikation	257
10.2	Tuning	260
10.2.1	Tuning des Speichers	261
10.2.2	Tuning von Indizes	267
10.3	Backup und Point-In-Time-Recovery	271
10.3.1	Restore zum letzten möglichen Zeitpunkt	272
10.3.2	Restore zu einem bestimmten Zeitpunkt	273

11 Syslog 275

11.1	Aufbau von Syslog-Nachrichten	275
11.2	Der Klassiker: »SyslogD«	276
11.3	Syslog-ng	278
11.3.1	Der »options«-Abschnitt	278
11.3.2	Das »source«-Objekt	279
11.3.3	Das »destination«-Objekt	280
11.3.4	Das »filter«-Objekt	282
11.3.5	Das »log«-Objekt	283
11.4	Rsyslog	284
11.4.1	Eigenschaftsbasierte Filter	284
11.4.2	Ausdrucksbasierte Filter	285
11.5	Loggen über das Netz	286
11.5.1	SyslogD	286
11.5.2	Syslog-ng	286
11.5.3	Rsyslog	287
11.6	Syslog in eine Datenbank schreiben	288
11.6.1	Anlegen der Log-Datenbank	288
11.6.2	In die Datenbank loggen	289

12 Proxyserver 291

12.1	Einführung des Stellvertreters	291
12.2	Proxys in Zeiten des Breitbandinternets	292
12.3	Herangehensweisen und Vorüberlegungen	293
12.4	Grundkonfiguration	293
12.4.1	Netzwerk	294

12.4.2	Cache	294
12.4.3	Logging	296
12.4.4	Handhabung des Dienstes	298
12.4.5	Objekte	300
12.4.6	Regeln	301
12.4.7	Konfiguration des Testumfeldes	304
12.5	Authentifizierung	307
12.5.1	Benutzerbasiert	309
12.5.2	Gruppenbasiert	315
12.6	Helferlein	317
12.6.1	squidGuard	317
12.6.2	Antiviren-Check: ClamAV mit HAVP einbinden	319
12.6.3	Dansguardian	322
12.7	Log-Auswertung: »Calamaris« und »Sarg«	326
12.7.1	Calamaris	326
12.7.2	Sarg	327
12.8	Unsichtbar: »transparent proxy«	328

13 Samba 331

13.1	Kurze Einführung in die Protokolle SMB und NetBIOS	332
13.1.1	Das Protokoll SMB	332
13.1.2	Das Protokoll NetBIOS	333
13.1.3	Möglichkeiten mit NetBIOS	334
13.1.4	Grundeinstellung der »smb.conf«	334
13.1.5	Verwendung von WINS zur Namensauflösung	336
13.1.6	Parameter für den »nmbd« in der »smb.conf«	337
13.1.7	Clientkonfiguration	339
13.2	Samba als Fileserver	340
13.2.1	Erstellen einfacher Freigaben	340
13.2.2	Spezielle Freigaben	343
13.2.3	Zusammenfassung mehrerer Freigaben	344
13.2.4	Kopieren von Freigabeeinstellungen	345
13.2.5	Ablauf des Zugriffs auf eine Freigabe	346
13.3	Benutzerverwaltung	349
13.3.1	Anlegen der Benutzer in der »smbpasswd«	350
13.3.2	Umwandeln der »smbpasswd« in »tdsam«	352
13.4	Verschiedene »passwd backends«	353
13.4.1	»smbpasswd«	353
13.4.2	»tdbsam«	354
13.4.3	»ldapsam«	355

13.5	Samba als Domänencontroller	357
13.5.1	Grundeinstellung des Domänencontrollers	358
13.5.2	Weitere Möglichkeiten mit »rpcclient«	359
13.5.3	Einrichten eines Domänenadministrators	364
13.5.4	Kennwortrichtlinien mit »pdbedit« erstellen	367
13.5.5	Einrichten von Benutzern und Hosts in der Domäne	368
13.5.6	Benutzeranmeldung	374
13.6	Winbind	375
13.6.1	Mitgliedschaft in einer Windows-Domäne	378
13.6.2	Konfiguration des Kerberos-Clients	379
13.6.3	Einstellung in der »smb.conf«	381
13.6.4	Beitritt zur Windows-Domäne	383
13.6.5	Testen der Domänenmitgliedschaft	385
13.6.6	Freigaben und Berechtigungen als Domänenmitglied	386
13.7	Samba als Printserver	389
13.7.1	Freigaben für Druckertreiber und Spooling	390
13.7.2	Einrichtung eines Printeradmins	391
13.7.3	Installation von Windows-Druckertreibern	392
13.8	Virtuelle Server und virtuelle Domänen	393
13.8.1	Zusammenführung der Server in jeder Arbeitsgruppe	394
13.8.2	Zusammenführen der zwei Arbeitsgruppen auf einer Maschine	396
13.9	DFS mit Samba	399
13.9.1	Samba als DFS-Proxy	399
13.9.2	Samba als DFS-Link-Server	400
13.10	Vertrauensstellung	402
13.10.1	Der Samba-Server als vertrauende Domäne	403
13.10.2	Der Samba-Server als vertraute Domäne	403
13.11	Sicherung der Konfigurationen	405
13.12	Ausblick auf Samba4	406

14 LDAP 407

14.1	Einige Grundlagen zu LDAP	408
14.1.1	Was ist ein Verzeichnisdienst?	408
14.1.2	Einsatz von LDAP im Netzwerk	409
14.1.3	Aufbau des LDAP-Datenmodells	409
14.1.4	Objekte	410
14.1.5	Attribute	411
14.1.6	Schema	411
14.1.7	LDIF-Format	414
14.2	Unterschiede in den einzelnen Distributionen	416

14.2.1	Umstellung auf die statische Konfiguration unter SLES11	416
14.2.2	Umstellung auf die statische Konfiguration unter Ubuntu-Server	417
14.2.3	Pfade und Benutzer	417
14.2.4	Die Datenbank-Backends	417
14.2.5	Grundkonfiguration des LDAP-Servers	417
14.3	Konfiguration des LDAP-Clients	420
14.3.1	Konfiguration des Clients auf dem SLES11	420
14.3.2	Konfiguration des Clients unter Debian »Lenny«	420
14.3.3	Konfiguration des LDAP-Clients unter Ubuntu-Server	423
14.3.4	Erster Zugriff auf den LDAP-Server	424
14.4	Grafische Werkzeuge für die LDAP-Verwaltung	425
14.4.1	Konfiguration des LAM	426
14.5	Änderungen mit »ldapmodify«	428
14.5.1	Interaktive Änderung mit »ldapmodify«	428
14.5.2	Änderungen über eine »ldif«-Datei mit »ldapmodify«	428
14.6	Absichern der Verbindung zum LDAP-Server über TLS	430
14.6.1	Erstellen der Zertifizierungsstelle	430
14.6.2	Erstellen des Serverzertifikates und des Requests	431
14.6.3	Signieren des Zertifikats	431
14.6.4	Zertifikate in die »slapd.conf« eintragen	431
14.6.5	Konfiguration des LDAP-Clients	432
14.7	Absichern des LDAP-Baums mit ACLs	432
14.7.1	Eine eigene Datei für die ACLs einbinden	433
14.7.2	Erste ACLs zur Grundsicherung des DIT	434
14.7.3	ACLs mit regulären Ausdrücken	436
14.7.4	ACLs für den Einsatz von Samba in LDAP	437
14.7.5	Testen von ACLs vor dem Einsatz	437
14.8	Filter zur Suche im LDAP-Baum	439
14.8.1	Testen der Fähigkeiten des LDAP-Servers	439
14.8.2	Einfache Filter	441
14.8.3	Filter mit logischen Verknüpfungen	441
14.8.4	Einschränkung der Suchtiefe	442
14.9	Verwendung von Overlays	443
14.9.1	Overlays am Beispiel von »dynlist«	444
14.9.2	Weitere Overlays	445
14.10	Replikation des DIT	445
14.10.1	Konfiguration des Providers	447
14.10.2	Konfiguration des Consumers	449
14.11	Die dynamische Konfiguration	451
14.11.1	Umstellung auf die dynamische Konfiguration am Provider	452
14.11.2	Umstellung auf die dynamische Konfiguration am Consumer	456

14.12 Verwaltung von Mail-Aliasen für den Mailserver Postfix	458
14.12.1 Einrichten der »alias«-Tabelle	458
14.12.2 Einrichtung der »virtual«-Tabelle	459
14.13 Cyrus und »sasauthd« über LDAP	460
14.14 Benutzerauthentifizierung am Proxy Squid über LDAP	461
14.14.1 Aktivierung der Authentifizierung über LDAP	461
14.14.2 Benutzerbezogene Authentifizierung	463
14.14.3 Gruppenbezogene Authentifizierung	463
14.15 Benutzerauthentifizierung am Webserver Apache über LDAP	465
14.15.1 Konfiguration der Cache-Parameter	465
14.15.2 Konfiguration der Zugriffsparameter	466
14.16 Und was geht sonst noch alles mit LDAP?	467

15 Druckserver 469

15.1 Policies	470
15.1.1 Grundkonfiguration des Netzwerkzugriffs	470
15.1.2 Location policies	471
15.1.3 Operation policies	473
15.1.4 Weitere Konfigurationsmöglichkeiten	474
15.1.5 Browsing	476
15.2 Drucker und Klassen einrichten und verwalten	477
15.2.1 Drucker einrichten	477
15.2.2 Klassen einrichten	478
15.3 Druckerquotas	479
15.4 CUPS über die Kommandozeile	480
15.4.1 Einstellen eines Standarddruckers	480
15.4.2 Optionen für einen Drucker verwalten	481
15.5 PPD-Dateien	483
15.6 Noch mehr Druck	484

TEIL IV: Infrastruktur

16 Hochverfügbarkeit 487

16.1 Das Beispiel-Setup	487
16.2 Installation	488
16.2.1 Ubuntu 10.04 LTS »Lucid Lynx«	488
16.2.2 Debian 5.0 »Lenny«	488
16.2.3 OpenSUSE	489
16.2.4 SUSE Linux Enterprise Server 11	489

16.3	Einfache Vorarbeiten	489
16.4	Shared Storage mit DRBD	490
16.4.1	Grundlegende Konfiguration unter Debian und SUSE	490
16.4.2	Grundlegende Konfiguration unter Ubuntu LTS	491
16.4.3	Die wichtigsten Konfigurationsoptionen	492
16.4.4	Die DRBD-Ressource in Betrieb nehmen	493
16.5	Grundkonfiguration der Cluster-Komponenten	496
16.5.1	OpenAIS und Corosync: das Benachrichtigungssystem	496
16.5.2	Pacemaker: der Ressourcen-Manager	498
16.5.3	Quorum deaktivieren	500
16.6	Dienste hochverfügbar machen	502
16.6.1	Die erste Ressource: eine hochverfügbare IP-Adresse	503
16.6.2	Hochverfügbarkeit am Beispiel von Apache	505
16.6.3	DRBD integrieren	507
16.6.4	Fencing	510

17 Virtualisierung 513

17.1	Einleitung	513
17.2	Für den »Sysadmin«	514
17.3	Server-Virtualisierung	518
17.3.1	KVM	519
17.3.2	»Xen«	521
17.4	Netzwerkgrundlagen	522
17.5	Management und Installation	525
17.5.1	Einheitlich arbeiten: »libvirt«	525
17.5.2	Konsolenbasiertes Management: »virsh«	529
17.5.3	Virtuelle Maschinen installieren	533
17.5.4	virt-install	535
17.5.5	Alleskönner: »Virtual Machine Manager«	537
17.5.6	Zusätzliche Konsolen-Tools	541
17.6	Umzugsunternehmen: Live Migration	543
17.6.1	Vorbereitungen	544
17.6.2	Konfiguration im »Virtual Machine Manager«	545

TEIL V: Kommunikation

18 Netzwerk 549

18.1	Netzwerkkonfiguration mit »iproute2«	549
18.1.1	Erste Schritte	549

18.1.2	»iproute2« im Detail	552
18.1.3	Links ansehen und manipulieren	553
18.1.4	IP-Adressen mit »iproute2«	555
18.1.5	»ip« zur Manipulation von ARP-Einträgen	558
18.2	Routing mit »ip«	559
18.2.1	Routinginformationen anzeigen	560
18.2.2	Advanced Routing	561
18.2.3	Die vorhandenen Regeln ansehen	562
18.2.4	Neue Routingtabelle anlegen	563
18.2.5	Policy Routing Database ändern	563
18.2.6	Routing über mehrere Uplinks	565
18.2.7	Abschlussbemerkung	569
18.3	Bonding	570
18.3.1	Bonding-Konfiguration	570
18.3.2	Bonding bei Debian und Ubuntu	572
18.3.3	Bonding bei SLES	573
18.4	IPv6	573
18.4.1	Die Vorteile von IPv6	574
18.4.2	Notation von IPv6-Adressen	575
18.4.3	Die Netzmasken	576
18.4.4	IPv6 in der Praxis	576
18.5	Firewalls mit »netfilter« und »iptables«	578
18.5.1	Der Weg der Pakete durch den Kernel	578
18.5.2	Einführung in »iptables«	580
18.5.3	Regeln definieren	581
18.5.4	Die klassischen Targets	582
18.5.5	Ein erster Testlauf	583
18.5.6	Stateful Packet Inspection	583
18.5.7	Das erste Firewallskript	585
18.5.8	Externe Firewall	587
18.5.9	Logging	592
18.5.10	Network Address Translation und Masquerading	594
18.5.11	Weitere nützliche Module für »iptables«	595
18.6	Abschlussbemerkung	597
18.7	DHCP	597
18.7.1	Funktionsweise	598
18.7.2	Konfiguration	598
18.8	DNS-Server	601
18.8.1	Funktionsweise	601
18.8.2	Die Grundkonfiguration	602
18.8.3	Zonendefinitionen	604

18.8.4	Die erste vollständige Zone	609
18.8.5	Die »hint«-Zone	610
18.8.6	Reverse Lookup	612
18.8.7	Slave-Server	614
18.9	Nachwort zum Thema Netzwerk	616

19 OpenSSH 617

19.1	Die SSH-Familie	617
19.1.1	Die Clients: ssh, scp, sftp	618
19.1.2	Der Server: sshd	620
19.2	Schlüssel statt Passwort	622
19.2.1	Schlüssel erzeugen	622
19.2.2	Passwortloses Login	623
19.2.3	Der SSH-Agent merkt sich Passphrasen	624
19.3	X11-Forwarding	625
19.4	Port-Weiterleitung und Tunneling	625

20 Administrationstools 627

20.1	Was kann dies und jenes noch?	627
20.1.1	Der Rsync-Daemon	627
20.1.2	Wenn's mal wieder später wird: »screen«	629
20.1.3	Anklopfen mit »nmap«	630
20.1.4	Netzwerkinspektion: »netstat«	633
20.1.5	Zugreifende Prozesse finden: »lsof«	635
20.1.6	Was macht mein System – »top«	639
20.1.7	Wenn gar nichts mehr geht – Debugging mit »strace«	644
20.2	Aus der Ferne – Remote-Administrationstools	649
20.2.1	PuTTY	649
20.2.2	WinSCP	652
20.2.3	Synergy	653

TEIL VI: Automatisierung

21 Scripting 659

21.1	Aufgebohrte Muscheln	659
21.2	Vom Suchen und Finden: Ein kurzer Überblick	660
21.2.1	Die Detektive: »grep«, »sed« und »AWK«	660
21.2.2	Reguläre Ausdrücke verstehen und anwenden	661

21.3	Fortgeschrittene Shell-Programmierung	664
21.3.1	Expansionsschemata	664
21.3.2	Umgebungsvariablen	668
21.3.3	»Back to bash«: Ein tieferer Blick in die Muschel	669
21.3.4	Logging in Skripten	673
21.4	Tipps und Tricks aus der Praxis	676
21.4.1	Aufräumkommando	676
21.4.2	IFS	677
21.4.3	Datumsmagie	677
21.4.4	E-Mails aus einem Skript versenden	678
21.4.5	Interaktive Programme steuern	678

22 Monitoring – wissen, was läuft 681

22.1	Nagios	681
22.1.1	Installation	682
22.1.2	Nagios selbst kompilieren	682
22.1.3	Nagios Plugins kompilieren	684
22.1.4	Die Verzeichnisstruktur	685
22.1.5	Das Webinterface	685
22.1.6	Die Hauptkonfigurationsdatei	686
22.1.7	Die Objekte	687
22.1.8	Die Ressourcen-Datei	696
22.1.9	CGI-Konfiguration	696
22.1.10	Plugins zu Nagios	697
22.1.11	Benachrichtigungen	703
22.1.12	Performancedatenanalyse	704
22.1.13	Das Webfrontend	707
22.2	Monitoring mit Munin	708

TEIL VII: Sicherheit, Verschlüsselung und Zertifikate

23 Sicherheit 713

23.1	Weniger ist mehr	714
23.2	»chroot«	714
23.2.1	Dienste	715
23.2.2	»jailkit«	717
23.3	Selbstabsicherung: »AppArmor«	721
23.4	Gotcha! IDS-Systeme	727
23.4.1	»snort« und Co.	728

23.4.2	Installation	730
23.4.3	Regeln – »oinkmaster«	732
23.4.4	Anwendung von Intrusion-Detection-Systemen in der Praxis	736
23.5	Klein, aber oho: »fail2ban«	739
23.6	Einmalpasswörter mit OPIE	744
23.7	OpenVPN	747
23.7.1	Server-Installation – OpenVPN, PKI und Co.	748
23.7.2	Roadwarrior	756
23.7.3	Site-to-site	761

24 Verschlüsselung und Zertifikate 765

24.1	Definition und Historie	765
24.2	Moderne Kryptologie	767
24.2.1	Symmetrische Verschlüsselung	767
24.2.2	Asymmetrische Verschlüsselung	768
24.3	Den Durchblick behalten	769
24.3.1	Das Grundproblem	769
24.3.2	Verwendungszwecke	770
24.3.3	Umsetzung mithilfe einer PKI	770
24.3.4	X.509	771
24.3.5	Ein anderer Ansatz: PGP (Web-of-Trust)	773
24.4	In der Praxis	774
24.4.1	Einrichtung einer PKI mit Server- und E-Mail-Zertifikaten	774
24.4.2	E-Mail-Verschlüsselung	785
24.5	Neben der Kommunikation – Dateiverschlüsselung	793
24.5.1	Dateien	793
24.5.2	Devices	794
24.5.3	Festplatten/System	796
24.6	Rechtliches	800
24.6.1	Fortgeschrittene elektronische Signatur	800
24.6.2	Qualifiziertes Zertifikat	800
24.6.3	Qualifizierte elektronische Signatur	801
24.6.4	Sichere Signaturerstellungseinheit (SSEE)	801

Die Autoren	803
Index	805