

# Auf einen Blick

<b>TEIL I</b>	
Grundlagen .....	67
<b>TEIL II</b>	
Aufgaben .....	199
<b>TEIL III</b>	
Dienste .....	269
<b>TEIL IV</b>	
Infrastruktur .....	745
<b>TEIL V</b>	
Kommunikation .....	871
<b>TEIL VI</b>	
Automatisierung .....	1041
<b>TEIL VII</b>	
Sicherheit, Verschlüsselung und Zertifikate .....	1181

# Inhalt

Vorwort .....	33
Über dieses Buch .....	43

## 1 Der Administrator 47

---

1.1 Der Beruf des Systemadministrators .....	47
1.1.1 Berufsbezeichnung und Aufgaben .....	47
1.1.2 Job-Definitionen .....	48
1.1.3 Definitionen der Management-Level .....	52
1.2 Nützliche Fähigkeiten und Fertigkeiten .....	54
1.2.1 Soziale Fähigkeiten .....	54
1.2.2 Arbeitstechniken .....	55
1.3 Das Verhältnis des Administrators zu Normalsterblichen .....	57
1.3.1 Der Chef und andere Vorgesetzte .....	57
1.3.2 Benutzer .....	58
1.3.3 Andere Administratoren .....	58
1.4 Unterbrechungsgesteuertes Arbeiten .....	59
1.5 Einordnung der Systemadministration .....	60
1.5.1 Arbeitsgebiete .....	60
1.5.2 DevOps .....	62
1.6 Ethischer Verhaltenskodex .....	64
1.7 Administration – eine Lebenseinstellung? .....	65

## TEIL I Grundlagen

## 2 Der Bootvorgang 69

---

2.1 Der Bootloader GRUB 2 .....	69
2.1.1 Funktionsweise .....	69
2.1.2 Installation .....	70
2.1.3 Konfiguration .....	70
2.2 Bootloader Recovery .....	76

<b>2.3</b>	<b>Der Kernel und die initrd .....</b>	<b>77</b>
2.3.1	initrd erstellen und modifizieren .....	78
2.3.2	initrd manuell modifizieren .....	82
<b>2.4</b>	<b>systemd .....</b>	<b>83</b>
2.4.1	Begriffe .....	84
2.4.2	Kontrollieren von Diensten .....	85
2.4.3	Aktivieren und Deaktivieren von Diensten .....	87
2.4.4	Erstellen und Aktivieren eigener Service Units .....	88
2.4.5	Target Units .....	90
2.4.6	»systemd«- und Servicekonfigurationen .....	91
2.4.7	Anzeige von Dienstabhängigkeiten .....	92
2.4.8	Logs mit journald .....	94
2.4.9	Abschlussbemerkung .....	95

3

Festplatten und andere Devices

97

---

<b>3.1</b>	<b>RAID .....</b>	<b>97</b>
3.1.1	RAID-0 .....	98
3.1.2	RAID-1 .....	98
3.1.3	RAID-5 .....	98
3.1.4	RAID-6 .....	99
3.1.5	RAID-10 .....	99
3.1.6	Zusammenfassung .....	100
3.1.7	Weich, aber gut: Software-RAID .....	101
3.1.8	Software-RAID unter Linux .....	102
3.1.9	Abschlussbemerkung zu RAIDs .....	109
<b>3.2</b>	<b>Rein logisch: Logical Volume Manager (LVM) .....</b>	<b>110</b>
3.2.1	Grundlagen und Begriffe .....	112
3.2.2	Setup .....	113
3.2.3	Aufbau einer Volume Group mit einem Volume .....	114
3.2.4	Erweiterung eines Volumes .....	117
3.2.5	Eine Volume Group erweitern .....	118
3.2.6	Spiegelung zu einem Volume hinzufügen .....	119
3.2.7	Eine defekte Festplatte ersetzen .....	120
3.2.8	Backups mit Snapshots .....	121
3.2.9	Mirroring ausführlich .....	125

3.2.10	Thin Provisioning .....	129
3.2.11	Kommandos .....	132
<b>3.3</b>	<b>udev</b> .....	133
3.3.1	udev-Regeln .....	133
3.3.2	Eigene Regeln schreiben .....	134
<b>3.4</b>	<b>Alles virtuell? »/proc«</b> .....	137
3.4.1	CPU .....	137
3.4.2	RAM .....	138
3.4.3	Kernelkonfiguration .....	139
3.4.4	Kernelparameter .....	140
3.4.5	Gemountete Dateisysteme .....	140
3.4.6	Prozessinformationen .....	141
3.4.7	Netzwerk .....	142
3.4.8	Änderungen dauerhaft speichern .....	143
3.4.9	Abschlussbemerkung .....	143

---

## 4 Dateisysteme 145

---

<b>4.1</b>	<b>Dateisysteme: von Bäumen, Journalen und einer Kuh</b> .....	145
4.1.1	Bäume .....	146
4.1.2	Journale .....	148
4.1.3	Und die Kühe? COW-fähige Dateisysteme .....	148
<b>4.2</b>	<b>Praxis</b> .....	149
4.2.1	Ext2/3-FS aufgebohrt: mke2fs, tune2fs, dumpe2fs, e2label .....	149
4.2.2	ReiserFS und seine Tools .....	152
4.2.3	XFS .....	153
4.2.4	Das Dateisystem vergrößern oder verkleinern .....	154
4.2.5	Btrfs .....	155
<b>4.3</b>	<b>Fazit</b> .....	162

---

## 5 Berechtigungen 163

---

<b>5.1</b>	<b>User, Gruppen und Dateisystemstrukturen</b> .....	163
<b>5.2</b>	<b>Dateisystemberechtigungen</b> .....	166
5.2.1	Spezialbits .....	167

<b>5.3</b>	<b>Erweiterte POSIX-ACLs</b>	170
5.3.1	Setzen und Anzeigen von einfachen ACLs	171
5.3.2	Setzen von Default-ACLs	173
5.3.3	Setzen von erweiterten ACLs	175
5.3.4	Entfernen von ACLs	177
5.3.5	Sichern und Zurückspielen von ACLs	178
<b>5.4</b>	<b>Erweiterte Dateisystemattribute</b>	179
5.4.1	Attribute, die jeder Benutzer ändern kann	179
5.4.2	Attribute, die nur »root« ändern kann	180
5.4.3	Weitere Attribute	181
<b>5.5</b>	<b>Quotas</b>	181
5.5.1	Installation und Aktivierung der Quotas	182
5.5.2	Journaling-Quotas	183
5.5.3	Quota-Einträge verwalten	184
<b>5.6</b>	<b>Pluggable Authentication Modules (PAM)</b>	188
5.6.1	Verschiedene PAM-Typen	189
5.6.2	Die PAM-Kontrollflags	189
5.6.3	Argumente zu den Modulen	190
5.6.4	Modulpfade	190
5.6.5	Module und ihre Aufgaben	191
5.6.6	Die neuere Syntax bei der PAM-Konfiguration	192
<b>5.7</b>	<b>Konfiguration von PAM</b>	194
<b>5.8</b>	<b>ulimit</b>	195
5.8.1	Setzen der ulimit-Werte	196
<b>5.9</b>	<b>Abschlussbemerkung</b>	197

## TEIL II Aufgaben

<b>6</b>	<b>Paketmanagement</b>	201
<b>6.1</b>	<b>Paketverwaltung</b>	201
6.1.1	rpm oder deb?	202
6.1.2	dnf, yast, zypper oder apt?	204
6.1.3	Außerirdische an Bord – alien	205

<b>6.2</b>	<b>Pakete im Eigenbau .....</b>	<b>206</b>
6.2.1	Vorbereitungen .....	207
6.2.2	Am Anfang war das Makefile .....	207
6.2.3	Vom Fellknäuel zum Paket .....	210
6.2.4	Patchen mit patch und diff .....	214
6.2.5	Updates sicher konfigurieren .....	217
<b>6.3</b>	<b>Updates nur einmal laden: Cache .....</b>	<b>219</b>
6.3.1	deb-basierte Distributionen: apt-cacher-ng .....	219
6.3.2	Installation .....	219
6.3.3	Konfiguration .....	220
6.3.4	Clientkonfiguration .....	222
6.3.5	Fütterungszeit – bereits geladene Pakete dem Cache hinzufügen .....	222
6.3.6	Details: Report-HTML .....	223
6.3.7	rpm-basierte Distributionen .....	223
<b>6.4</b>	<b>Alles meins: Mirror .....</b>	<b>224</b>
6.4.1	deb-basierte Distributionen: debmirror .....	224
6.4.2	Konfiguration .....	224
6.4.3	Benutzer und Gruppe anlegen .....	224
6.4.4	Verzeichnisstruktur anlegen .....	225
6.4.5	Mirror-Skript erstellen (Ubuntu) .....	225
6.4.6	Cronjobs einrichten .....	228
6.4.7	Schlüssel importieren .....	228
6.4.8	Mirror erstellen .....	229
6.4.9	Mirror verfügbar machen – Webdienst konfigurieren .....	229
6.4.10	Clientkonfiguration .....	230
6.4.11	rpm-basierte Distributionen .....	230
6.4.12	Benutzer und Gruppe anlegen .....	231
6.4.13	Verzeichnisstruktur anlegen: openSUSE Leap .....	231
6.4.14	Verzeichnisstruktur anlegen: CentOS .....	231
6.4.15	Mirror-Skript erstellen .....	232
6.4.16	Cronjobs einrichten .....	233
6.4.17	Mirror erstellen .....	234
6.4.18	Mirror verfügbar machen – Webdienst konfigurieren .....	234
6.4.19	Clientkonfiguration: openSUSE Leap .....	235
6.4.20	Clientkonfiguration: CentOS .....	236

7

Backup und Recovery

237

---

7.1

Backup gleich Disaster Recovery?

237

7.2

Backupstrategien

238

7.3

Datensicherung mit tar

241

7.3.1

Weitere interessante Optionen für GNU-tar

242

7.3.2

Sicherung über das Netzwerk mit tar und ssh

243

7.4

Datensynchronisation mit rsync

243

7.4.1

Lokale Datensicherung mit rsync

244

7.4.2

Synchronisieren im Netzwerk mit rsync

244

7.4.3

Wichtige Optionen für rsync

245

7.4.4

Backupskript für die Sicherung auf einen Wechseldatenträger

246

7.4.5

Backupskript für die Sicherung auf einen Backupserver

247

7.4.6

Verwendung von ssh für die Absicherung von rsync

249

7.5

Imagesicherung mit dd

250

7.5.1

Sichern des Master Boot Records (MBR)

251

7.5.2

Die Partitionstabelle mithilfe von dd zurückspielen

251

7.5.3

Images mit dd erstellen

252

7.5.4

Einzelne Dateien mit dd aus einem Image zurückspielen

252

7.5.5

Abschlussbemerkung zu dd

254

7.6

Disaster Recovery mit ReaR

255

7.6.1

ReaR installieren

256

7.6.2

ReaR konfigurieren

256

7.6.3

Aufrufparameter von ReaR

258

7.6.4

Der erste Testlauf

259

7.6.5

Der Recovery-Prozess

263

7.6.6

Die ReaR-Konfiguration im Detail

265

7.6.7

Migrationen mit ReaR

266

TEIL III Dienste

8

Webserver

271

---

8.1

Apache

271

8.1.1

Installation

271

8.1.2

Virtuelle Hosts einrichten

272

8.1.3

Debian/Ubuntu: Virtuelle Hosts aktivieren

274

8.1.4	HTTPS konfigurieren .....	275
8.1.5	Apache-Server mit ModSecurity schützen .....	280
8.1.6	Tuning und Monitoring .....	285
<b>8.2</b>	<b>nginx</b> .....	289
8.2.1	Installation .....	289
8.2.2	Grundlegende Konfiguration .....	290
8.2.3	Virtuelle Hosts .....	290
8.2.4	HTTPS mit nginx .....	293
<b>8.3</b>	<b>PHP</b> .....	294
8.3.1	Installation .....	294
8.3.2	PHP in den Webseitenkonfigurationen aktivieren .....	297
8.3.3	Funktionstest .....	299
8.3.4	Tipps und Tricks .....	299
<b>8.4</b>	<b>Fortgeschrittene TLS-Konfiguration und Sicherheitsfunktionen</b> .....	301
8.4.1	SSL/TLS .....	301
8.4.2	Konfiguration in Apache2 .....	302
8.4.3	Konfiguration in nginx .....	304
8.4.4	Informationen und Anregungen .....	305

## 9 FTP-Server 307

---

<b>9.1</b>	<b>Einstieg</b> .....	307
9.1.1	Das File Transfer Protocol .....	307
9.1.2	vsftpd .....	308
<b>9.2</b>	<b>Download-Server</b> .....	308
<b>9.3</b>	<b>Zugriff von Usern auf ihre Homeverzeichnisse</b> .....	310
<b>9.4</b>	<b>FTP über SSL (FTPS)</b> .....	311
<b>9.5</b>	<b>Anbindung an LDAP</b> .....	313

## 10 Mailserver 315

---

<b>10.1</b>	<b>Postfix</b> .....	315
10.1.1	Installation der Postfix-Pakete .....	316
10.1.2	Grundlegende Konfiguration .....	316
10.1.3	Postfix als Relay vor Exchange, Dovecot oder anderen Backends .....	319



10.1.4	Die Postfix-Restrictions: Der Schlüssel zu Postfix .....	321
10.1.5	Weiterleitungen und Aliasse für Mailadressen .....	330
10.1.6	SASL/SMTP-Auth .....	331
10.1.7	SSL/TLS für Postfix einrichten .....	333
<b>10.2</b>	<b>POP3/IMAP-Server mit Dovecot .....</b>	<b>335</b>
10.2.1	Installation der Dovecot-Pakete .....	335
10.2.2	Vorbereitungen im Linux-System .....	336
10.2.3	Log-Meldungen und Debugging .....	336
10.2.4	User-Authentifizierung .....	337
10.2.5	Aktivierung des LMTP-Servers von Dovecot .....	339
10.2.6	Einrichten von SSL/TLS-Verschlüsselung .....	340
10.2.7	Der Ernstfall: Der IMAP-Server erwacht zum Leben .....	341
10.2.8	Dovecot im Replikations-Cluster .....	342
10.2.9	Einrichtung der Replikation .....	343
10.2.10	Hochverfügbare Service-IP .....	346
<b>10.3</b>	<b>Anti-Spam/Anti-Virus mit Rspamd .....</b>	<b>348</b>
10.3.1	Mails ablehnen oder in die Quarantäne filtern? .....	348
10.3.2	Installation von Rspamd, ClamAV und Redis .....	349
10.3.3	Update der Virensignaturen und Start der Dienste .....	350
10.3.4	Die Architektur von Rspamd .....	351
10.3.5	Einbindung von Rspamd an Ihren Postfix-Mailserver .....	352
10.3.6	Konfiguration des Rspamd .....	354
10.3.7	Konfiguration von Upstream-Quellen .....	356
10.3.8	Redis als schnelle Datenbank an der Seite von Rspamd .....	357
10.3.9	Die Definition auszulösender Aktionen .....	357
10.3.10	Statistik und Auswertung im Webinterface .....	359
10.3.11	ClamAV in Rspamd einbinden .....	360
10.3.12	Späteres Filtern über Mail-Header .....	361
10.3.13	RBLs in Rspamd .....	362
10.3.14	Bayes in Rspamd .....	364
10.3.15	Eigene White- und Blacklists führen .....	365
10.3.16	Einrichtung von DKIM zur Mailsignierung .....	367
10.3.17	Ausblick: Einbindung weiterer Prüfungsmethoden .....	370
<b>10.4</b>	<b>Monitoring und Logfile-Auswertung .....</b>	<b>370</b>

11.1

MariaDB in der Praxis

371

11.1.1

Installation und grundlegende Einrichtung

371

11.1.2

Replikation

373

11.1.3

Master-Master-Replikation

380

11.2

Tuning

384

11.2.1

Tuning des Speichers

384

11.2.2

Tuning von Indizes

390

11.3

Backup und Point-In-Time-Recovery

394

11.3.1

Restore zum letztmöglichen Zeitpunkt

395

11.3.2

Restore zu einem bestimmten Zeitpunkt

395

12.1

Der Aufbau von Syslog-Nachrichten

397

12.2

systemd mit journalctl

399

12.2.1

Erste Schritte mit dem journalctl-Kommando

400

12.2.2

Filtern nach Zeit

402

12.2.3

Filtern nach Diensten

403

12.2.4

Kernelmeldungen

404

12.2.5

Einrichten eines Log-Hosts

405

12.3

Der Klassiker: Syslogd

408

12.4

Syslog-ng

410

12.4.1

Der »options«-Abschnitt

410

12.4.2

Das »source«-Objekt

412

12.4.3

Das »destination«-Objekt

412

12.4.4

Das »filter«-Objekt

414

12.4.5

Das »log«-Objekt

416

12.5

Rsyslog

416

12.5.1

Eigenschaftsbasierte Filter

416

12.5.2

Ausdrucksbasierte Filter

417

12.6

Loggen über das Netz

418

12.6.1

SyslogD

418

12.6.2

Syslog-ng

419

12.6.3

Rsyslog

420

<b>12.7 Syslog in eine Datenbank schreiben</b>	420
12.7.1 Anlegen der Log-Datenbank	420
12.7.2 In die Datenbank loggen	421
<b>12.8 Fazit</b>	423

## **13 Proxy-Server** 425

---

<b>13.1 Einführung des Stellvertreters</b>	425
<b>13.2 Proxys in Zeiten des Breitbandinternets</b>	426
<b>13.3 Herangehensweisen und Vorüberlegungen</b>	427
<b>13.4 Grundkonfiguration</b>	427
13.4.1 Aufbau des Testumfelds	428
13.4.2 Netzwerk	428
13.4.3 Cache	429
13.4.4 Logging	430
13.4.5 Handhabung des Dienstes	432
13.4.6 Objekte	433
13.4.7 Objekttypen	435
13.4.8 Objektlisten in Dateien	435
13.4.9 Regeln	436
13.4.10 Überlagerung mit »first match«	438
13.4.11 Anwendung von Objekten und Regeln	439
<b>13.5 Authentifizierung</b>	440
13.5.1 Benutzerbasiert	443
13.5.2 Gruppenbasiert	452
<b>13.6 Log-Auswertung: Calamaris und Sarg</b>	455
13.6.1 Calamaris	455
13.6.2 Sarg	457
<b>13.7 Unsichtbar: transparent proxy</b>	458
<b>13.8 Ab in den Pool – Verzögerung mit delay_pools</b>	459
13.8.1 Funktionsweise – alles im Eimer!	459
13.8.2 Details – Klassen, Eimer und ACLs richtig wählen	460
<b>13.9 Familienbetrieb: Sibling, Parent und Co.</b>	462
13.9.1 Grundlagen	463
13.9.2 Eltern definieren	464
13.9.3 Geschwister definieren	464

13.9.4	Load Balancing .....	465
13.9.5	Inhalte eigenständig abrufen: <code>always_direct</code> .....	465
<b>13.10</b>	<b>Cache-Konfiguration .....</b>	<b>466</b>
13.10.1	Cache-Arten: Hauptspeicher und Festplatten .....	466
13.10.2	Hauptspeicher-Cache .....	467
13.10.3	Festplatten-Cache .....	467
13.10.4	Tuning .....	470
<b>14</b>	<b>Kerberos .....</b>	<b>471</b>
<b>14.1</b>	<b>Begriffe im Zusammenhang mit Kerberos .....</b>	<b>472</b>
<b>14.2</b>	<b>Die Funktionsweise von Kerberos .....</b>	<b>472</b>
<b>14.3</b>	<b>Installation und Konfiguration des Kerberos-Servers .....</b>	<b>473</b>
14.3.1	Starten und Stoppen der Dienste .....	474
14.3.2	Konfiguration der Datei <code>»etc/krb5.conf«</code> .....	475
14.3.3	Konfiguration der Datei <code>»kdc.conf«</code> .....	477
<b>14.4</b>	<b>Initialisierung und Testen des Kerberos-Servers .....</b>	<b>481</b>
14.4.1	Verwalten der Principals .....	483
<b>14.5</b>	<b>Kerberos und PAM .....</b>	<b>487</b>
14.5.1	Konfiguration der PAM-Dateien auf einem openSUSE-System .....	488
14.5.2	Testen der Anmeldung .....	488
<b>14.6</b>	<b>Neue Benutzer mit Kerberos-Principal anlegen .....</b>	<b>489</b>
<b>14.7</b>	<b>Hosts und Dienste .....</b>	<b>490</b>
14.7.1	Einträge entfernen .....	493
<b>14.8</b>	<b>Konfiguration des Kerberos-Clients .....</b>	<b>494</b>
14.8.1	PAM und Kerberos auf dem Client .....	495
<b>14.9</b>	<b>Replikation des Kerberos-Servers .....</b>	<b>496</b>
14.9.1	Bekanntmachung aller KDCs im Netz .....	496
14.9.2	Konfiguration des KDC-Masters .....	499
14.9.3	Konfiguration des KDC-Slaves .....	501
14.9.4	Replikation des KDC-Masters auf den KDC-Slave .....	502
<b>14.10</b>	<b>Kerberos-Policies .....</b>	<b>504</b>
<b>14.11</b>	<b>Kerberos in LDAP einbinden .....</b>	<b>507</b>
14.11.1	Konfiguration des LDAP-Servers .....	508
14.11.2	Zurücksichern der alten Datenbank .....	517

14.11.3	Erstellung der Service-Keys in der Standard-»keytab«-Datei .....	520
14.11.4	Bestehende LDAP-Benutzer um Kerberos-Principal erweitern .....	521
<b>14.12</b>	<b>Neue Benutzer in den LDAP-Baum aufnehmen .....</b>	<b>526</b>
<b>14.13</b>	<b>Authentifizierung am LDAP-Server über »GSSAPI« .....</b>	<b>527</b>
14.13.1	Authentifizierung einrichten .....	527
14.13.2	Den zweiten KDC an den LDAP-Server anbinden .....	533
<b>14.14</b>	<b>Konfiguration des LAM Pro .....</b>	<b>533</b>

---

## 15 Samba 4 537

---

<b>15.1</b>	<b>Vorüberlegungen .....</b>	<b>537</b>
<b>15.2</b>	<b>Konfiguration von Samba 4 als Domaincontroller .....</b>	<b>538</b>
15.2.1	Das Provisioning .....	541
15.2.2	Konfiguration des Bind9 .....	542
<b>15.3</b>	<b>Testen des Domaincontrollers .....</b>	<b>546</b>
15.3.1	Testen des DNS-Servers .....	548
15.3.2	Test des Verbindungsaufbaus .....	549
15.3.3	Einrichtung des Zeitservers .....	551
<b>15.4</b>	<b>Benutzer- und Gruppenverwaltung .....</b>	<b>552</b>
<b>15.5</b>	<b>Benutzer- und Gruppenverwaltung über die Kommandozeile .....</b>	<b>553</b>
15.5.1	Verwaltung von Gruppen über die Kommandozeile .....	553
15.5.2	Verwaltung von Benutzern über die Kommandozeile .....	558
15.5.3	Setzen der Passwortsrichtlinien .....	562
15.5.4	Passwortsrichtlinien mit Password Settings Objects (PSO) .....	563
<b>15.6</b>	<b>Die Remote Server Administration Tools (RSAT) .....</b>	<b>564</b>
15.6.1	Die RSAT einrichten .....	564
15.6.2	Beitritt eines Windows-Clients zur Domäne .....	565
15.6.3	Einrichten der RSAT .....	566
15.6.4	Benutzer- und Gruppenverwaltung mit den RSAT .....	566
<b>15.7</b>	<b>Gruppenrichtlinien .....</b>	<b>567</b>
15.7.1	Verwaltung der GPOs mit den RSAT .....	567
15.7.2	Erste Schritte mit der Gruppenrichtlinienverwaltung .....	568
15.7.3	Eine Gruppenrichtlinie erstellen .....	569
15.7.4	Die Gruppenrichtlinie mit einer OU verknüpfen .....	572
15.7.5	GPOs über die Kommandozeile .....	576

<b>15.8</b>	<b>Linux-Clients in der Domäne</b>	577
15.8.1	Bereitstellen von Freigaben	583
15.8.2	Mounten über »pam_mount«	584
15.8.3	Umstellen des grafischen Logins	587
<b>15.9</b>	<b>Zusätzliche Server in der Domäne</b>	588
15.9.1	Einen Fileserver einrichten	589
15.9.2	Ein zusätzlicher Domaincontroller	594
15.9.3	Konfiguration des zweiten DC	596
15.9.4	Einrichten des Nameservers	596
15.9.5	Testen der Replikation	599
15.9.6	Weitere Tests	601
15.9.7	Einrichten des Zeitservers	601
<b>15.10</b>	<b>Die Replikation der Freigabe »sysvol« einrichten</b>	602
15.10.1	Einrichten des rsync-Servers	602
15.10.2	Einrichten von rsync auf dem PDC-Master	603
<b>15.11</b>	<b>Was geht noch mit Samba 4?</b>	607
<b>16</b>	<b>NFS</b>	609
<hr/>		
<b>16.1</b>	<b>Unterschiede zwischen NFSv3 und NFSv4</b>	609
<b>16.2</b>	<b>Funktionsweise von NFSv4</b>	610
<b>16.3</b>	<b>Einrichten des NFSv4-Servers</b>	611
16.3.1	Konfiguration des Pseudodateisystems	611
16.3.2	Anpassen der Datei »/etc/exports«	612
16.3.3	Tests für den NFS-Server	614
<b>16.4</b>	<b>Konfiguration des NFSv4-Clients</b>	616
<b>16.5</b>	<b>Konfiguration des idmapd</b>	617
<b>16.6</b>	<b>Optimierung von NFSv4</b>	619
16.6.1	Optimierung des NFSv4Servers	619
16.6.2	Optimierung des NFSv4-Clients	620
<b>16.7</b>	<b>NFSv4 und Firewalls</b>	621
<b>16.8</b>	<b>NFS und Kerberos</b>	622
16.8.1	Erstellung der Principals und der keytab-Dateien	622
16.8.2	Kerberos-Authentifizierung unter Debian und Ubuntu	624
16.8.3	Kerberos-Authentifizierung auf openSUSE und CentOS	624

16.8.4	Anpassen der Datei »/etc/exports« .....	624
16.8.5	Einen NFS-Client für Kerberos unter Debian und Ubuntu konfigurieren .	625
16.8.6	Einen NFS-Client für Kerberos unter openSUSE und CentOS konfigurieren .....	625
16.8.7	Testen der durch Kerberos abgesicherten NFS-Verbindung .....	625
16.8.8	Testen der Verbindung .....	626

## 17 LDAP 629

---

<b>17.1</b>	<b>Einige Grundlagen zu LDAP .....</b>	<b>630</b>
17.1.1	Was ist ein Verzeichnisdienst? .....	630
17.1.2	Der Einsatz von LDAP im Netzwerk .....	631
17.1.3	Aufbau des LDAP-Datenmodells .....	632
17.1.4	Objekte .....	632
17.1.5	Attribute .....	633
17.1.6	Das Schema .....	634
17.1.7	Das LDIF-Format .....	637
<b>17.2</b>	<b>Zu den hier verwendeten Distributionen .....</b>	<b>638</b>
<b>17.3</b>	<b>Installation der Symas-Pakete .....</b>	<b>639</b>
17.3.1	Die zwei Konfigurationsarten .....	643
17.3.2	Die Datenbank-Backends .....	644
17.3.3	Grundkonfiguration des LDAP-Servers (statisch) .....	645
17.3.4	Grundkonfiguration des LDAP-Servers (dynamisch) .....	646
17.3.5	Anlegen der ersten Objekte .....	654
<b>17.4</b>	<b>Die Verbindung zum LDAP-Server über TLS absichern .....</b>	<b>656</b>
17.4.1	Erstellen der Zertifizierungsstelle .....	656
17.4.2	Erstellen des Serverzertifikats .....	657
17.4.3	Signieren des Zertifikats .....	657
17.4.4	Zertifikate in die »slapd.conf« eintragen .....	658
17.4.5	Zertifikate in die dynamische Konfiguration eintragen .....	658
17.4.6	Konfiguration des LDAP-Clients .....	659
<b>17.5</b>	<b>Einrichtung des sssd .....</b>	<b>660</b>
17.5.1	Anlegen eines Testbenutzers .....	665
<b>17.6</b>	<b>Grafische Werkzeuge für die LDAP-Verwaltung .....</b>	<b>666</b>
<b>17.7</b>	<b>Änderungen mit »ldapmodify« .....</b>	<b>667</b>
17.7.1	Interaktive Änderung mit »ldapmodify« .....	668
17.7.2	Änderungen über eine LDIF-Datei mit »ldapmodify« .....	668

<b>17.8</b>	<b>Absichern des LDAP-Baums mit ACLs</b>	669
<b>17.9</b>	<b>Grundlegende ACLs</b>	673
<b>17.10</b>	<b>Der neue LDAP-Admin</b>	676
17.10.1	Anlegen der Objekte	677
<b>17.11</b>	<b>Absichern der Passwörter</b>	678
<b>17.12</b>	<b>ACLs mit regulären Ausdrücken</b>	679
17.12.1	ACLs vor dem Einsatz testen	683
<b>17.13</b>	<b>Filter zur Suche im LDAP-Baum</b>	685
17.13.1	Die Fähigkeiten des LDAP-Servers testen	686
17.13.2	Einfache Filter	687
17.13.3	Filter mit logischen Verknüpfungen	688
17.13.4	Einschränkung der Suchtiefe	689
<b>17.14</b>	<b>Verwendung von Overlays</b>	690
17.14.1	Overlays am Beispiel von »dynlist«	690
17.14.2	Weitere Overlays	694
<b>17.15</b>	<b>Replikation des DIT</b>	696
17.15.1	Vorbereitungen für die Replikation	697
17.15.2	Einrichtung der Replikation	698
17.15.3	Einrichtung einer Multiprovider-Replikation	706
<b>17.16</b>	<b>Weiterleitungen für den Mailserver Postfix</b>	712
<b>17.17</b>	<b>Benutzerauthentifizierung von Dovecot über LDAP</b>	714
<b>17.18</b>	<b>Benutzerauthentifizierung am Proxy Squid über LDAP</b>	717
17.18.1	Die Authentifizierung über LDAP aktivieren	717
17.18.2	Benutzerbezogene Authentifizierung	719
17.18.3	Gruppenbezogene Authentifizierung	719
<b>17.19</b>	<b>Benutzerauthentifizierung am Webserver Apache über LDAP</b>	720
17.19.1	Konfiguration der Cache-Parameter	721
17.19.2	Konfiguration der Zugriffsparameter	722
<b>17.20</b>	<b>Und was geht sonst noch alles mit LDAP?</b>	723

## 18 Druckserver

725

---

<b>18.1</b>	<b>CUPS administrieren</b>	726
<b>18.2</b>	<b>Policies</b>	731
18.2.1	Location-Policies	732
18.2.2	Operation Policies	733



- 18.2.3 Weitere Konfigurationsmöglichkeiten ..... 734
  - 18.2.4 Browsing ..... 736
- 18.3 Drucker und Klassen einrichten und verwalten ..... 736
  - 18.3.1 Drucker einrichten ..... 737
  - 18.3.2 Klassen einrichten ..... 738
- 18.4 Druckerquotas ..... 739
- 18.5 CUPS über die Kommandozeile ..... 740
  - 18.5.1 Einstellen eines Standarddruckers ..... 740
  - 18.5.2 Optionen für einen Drucker verwalten ..... 741
- 18.6 PPD-Dateien ..... 743
- 18.7 Noch mehr Druck ..... 744

TEIL IV Infrastruktur

- 19 Hochverfügbarkeit ..... 747
- 19.1 Das Beispiel-Setup ..... 747
- 19.2 Installation ..... 748
  - 19.2.1 Debian 11 und Ubuntu 22.04 LTS ..... 748
  - 19.2.2 CentOS Stream ..... 748
  - 19.2.3 openSUSE Leap ..... 749
- 19.3 Einfache Vorarbeiten ..... 749
- 19.4 Shared Storage mit DRBD ..... 749
  - 19.4.1 Grundlegende Konfiguration ..... 750
  - 19.4.2 Die wichtigsten Konfigurationsoptionen ..... 751
  - 19.4.3 Die DRBD-Ressource in Betrieb nehmen ..... 752
- 19.5 Grundkonfiguration der Clusterkomponenten ..... 755
  - 19.5.1 Pacemaker und Corosync: das Benachrichtigungssystem ..... 755
  - 19.5.2 Pacemaker: der Ressourcenmanager ..... 758
  - 19.5.3 Ein Quorum deaktivieren ..... 760
- 19.6 Dienste hochverfügbar machen ..... 762
  - 19.6.1 Die erste Ressource: eine hochverfügbare IP-Adresse ..... 763
  - 19.6.2 Hochverfügbarkeit am Beispiel von Apache ..... 766
  - 19.6.3 DRBD integrieren ..... 769
  - 19.6.4 Fencing ..... 773

## 20 Virtualisierung 775

---

<b>20.1</b>	<b>Einleitung</b>	775
<b>20.2</b>	<b>Für den Sysadmin</b>	776
<b>20.3</b>	<b>Servervirtualisierung</b>	780
20.3.1	KVM	781
20.3.2	Xen	783
<b>20.4</b>	<b>Netzwerkgrundlagen</b>	784
<b>20.5</b>	<b>Management und Installation</b>	785
20.5.1	Einheitlich arbeiten: »libvirt«	786
20.5.2	Konsolenbasiertes Management: virsh	789
20.5.3	Virtuelle Maschinen installieren	792
20.5.4	virt-install	794
20.5.5	Alleskönner: Der Virtual Machine Manager	797
20.5.6	Zusätzliche Konsolentools	801
<b>20.6</b>	<b>Umzugsunternehmen: Live Migration</b>	802
20.6.1	Vorbereitungen	803
20.6.2	Konfiguration im Virtual Machine Manager	803

## 21 Containervirtualisierung mit Docker und Podman 805

---

<b>21.1</b>	<b>Einführung, Installation und Grundlagen für den Betrieb</b>	805
21.1.1	Was ist ein Container?	805
21.1.2	Container vs. VM	806
21.1.3	Entstehung und Geschichte	806
21.1.4	Versionen	807
21.1.5	Docker oder Podman?	808
21.1.6	Installation von Docker	809
21.1.7	Installation von Podman	811
21.1.8	Ergänzungen zur Installation, erster Systemtest	811
21.1.9	Betrieb hinter einem Proxy	813
21.1.10	Konfiguration der Laufzeitumgebung	814
<b>21.2</b>	<b>Management von Images und Containern</b>	815
21.2.1	Etwas Terminologie	815
21.2.2	Das Command Line Interface	816
21.2.3	Erste Schritte: hello-world	817

21.2.4	Löschen von Containern und Images .....	818
21.2.5	Image-Namen, Docker Hub und weitere Registrys .....	819
21.2.6	Handling von Containern .....	820
21.2.7	Prozessverwaltung .....	822
21.2.8	Umgebungsvariablen .....	823
21.2.9	Logging .....	824
21.2.10	Verteilung von Images über Dateiversand .....	825
21.2.11	Ausgaben filtern und/oder formatieren .....	825
21.2.12	Restart-Policies: Verhalten beim Host-Restart .....	827
21.2.13	Container limitieren .....	828
21.2.14	Packungsdichte .....	831
21.2.15	Systeminformationen und Aufräumarbeiten .....	831
<b>21.3</b>	<b>Docker-Networking .....</b>	<b>832</b>
21.3.1	User Defined Networks .....	833
21.3.2	Portmapping .....	834
21.3.3	»/etc/hosts«-Einträge beim Containerstart .....	835
<b>21.4</b>	<b>Containerdaten und Persistenz .....</b>	<b>836</b>
21.4.1	Aufbau von Images und Containern .....	836
21.4.2	Bind Mounts und Volumes .....	837
21.4.3	Weitere Möglichkeiten .....	840
21.4.4	Informationsbeschaffung .....	840
<b>21.5</b>	<b>Erstellen eigener Images mit Dockerfiles .....</b>	<b>842</b>
21.5.1	Einfaches Comitten von Anpassungen .....	842
21.5.2	Dockerfiles und »docker build«: Basics .....	844
21.5.3	Der Build-Cache und »docker build --pull« .....	844
21.5.4	Dangling Images .....	845
21.5.5	Die Dockerfile-Direktiven: Ein Überblick .....	846
21.5.6	Ein komplexeres Beispiel mit ENV, COPY und CMD .....	847
21.5.7	CMD und/oder ENTRYPOINT .....	848
21.5.8	Verwendung eigener Entrypoint-Skripte .....	850
21.5.9	».dockerignore«-Files .....	851
21.5.10	Healthchecks .....	851
21.5.11	Multistage-Builds .....	853
21.5.12	Best Practices .....	854
<b>21.6</b>	<b>Multi-Container-Rollout mit Docker Compose .....</b>	<b>855</b>
21.6.1	Installation .....	855
21.6.2	Basics .....	856
21.6.3	Ein erstes Beispiel .....	857
21.6.4	Build and Run .....	858

21.6.5	Environment und Portmappings .....	859
21.6.6	Volumes in Compose .....	860
21.6.7	Flexible Compose-Konfigurationen durch Umgebungsvariablen .....	861
21.6.8	Noch mal Restart-Policys .....	862
<b>21.7</b>	<b>Betrieb und Verwendung einer eigenen Registry .....</b>	<b>862</b>
21.7.1	Vorbereitungen in einer (virtuellen) Test-/Schulungsumgebung .....	863
21.7.2	Heute mal kein TLS/HTTPS .....	864
21.7.3	Harbor .....	866
21.7.4	Docker Registry .....	867
21.7.5	Arbeiten mit einer privaten Registry .....	869

## TEIL V Kommunikation

<b>22</b>	<b>Netzwerk .....</b>	<b>873</b>
<b>22.1</b>	<b>Vorwort zu Predictable Network Interface Names .....</b>	<b>873</b>
<b>22.2</b>	<b>Netzwerkkonfiguration mit iproute2 .....</b>	<b>874</b>
22.2.1	Erste Schritte .....	874
22.2.2	Die Syntax von ip .....	877
22.2.3	Links ansehen und manipulieren: ip link .....	877
22.2.4	IP-Adressen ansehen und manipulieren: ip address .....	879
22.2.5	Manipulation von ARP-Einträgen: ip neighbour .....	883
<b>22.3</b>	<b>Routing mit ip .....</b>	<b>885</b>
22.3.1	Routing-Informationen anzeigen .....	885
22.3.2	Da geht noch mehr: »Advanced Routing« .....	887
22.3.3	Die vorhandenen Regeln ansehen .....	888
22.3.4	Eine neue Routing-Tabelle anlegen .....	889
22.3.5	Ändern der Policy Routing Database .....	889
22.3.6	Routing über mehrere Uplinks .....	891
22.3.7	Fazit bis hierher .....	896
<b>22.4</b>	<b>Bonding .....</b>	<b>896</b>
22.4.1	Bonding-Konfiguration .....	897
22.4.2	Bonding unter Debian .....	900
22.4.3	Bonding unter Ubuntu .....	900
22.4.4	Bonding unter CentOS .....	901
22.4.5	Bonding unter openSUSE Leap .....	902

<b>22.5</b>	<b>IPv6</b>	902
22.5.1	Die Vorteile von IPv6	904
22.5.2	Notation von IPv6-Adressen	904
22.5.3	Die Netzmasken	905
22.5.4	Die verschiedenen IPv6-Adressarten	905
22.5.5	Es geht auch ohne ARP	907
22.5.6	Feste Header-Länge	908
22.5.7	IPv6 in der Praxis	910
<b>22.6</b>	<b>Firewalls mit netfilter und iptables</b>	911
22.6.1	Der Weg ist das Ziel – wie Pakete durch den Kernel laufen	912
22.6.2	Einführung in iptables	913
22.6.3	Regeln definieren	915
22.6.4	Die klassischen Targets	917
22.6.5	Ein erster Testlauf	917
22.6.6	Rein wie raus: Stateful Packet Inspection	918
22.6.7	Das erste Firewallskript	920
22.6.8	Externe Firewall	922
22.6.9	Logging	928
22.6.10	Network Address Translation und Masquerading	930
22.6.11	Weitere nützliche Module für iptables	931
22.6.12	Abschlussbemerkung	934
<b>22.7</b>	<b>DHCP</b>	934
22.7.1	Funktionsweise	934
22.7.2	Konfiguration	935

**23**

**DNS-Server**

939

---

<b>23.1</b>	<b>Funktionsweise</b>	939
23.1.1	Unterschied: rekursiv und autoritativ	941
23.1.2	Einträge im DNS: Resource Records	941
23.1.3	Die Grundkonfiguration	942
23.1.4	Zonendefinitionen	944
23.1.5	Die erste vollständige Zone	949
23.1.6	Die hint-Zone	950
23.1.7	Reverse Lookup	952
23.1.8	Secondary-Server	954
23.1.9	DNS-Server und IPv6	956

<b>23.2</b>	<b>Vertrauen schaffen mit DNSSEC</b>	957
23.2.1	Die Theorie: »Wie arbeitet DNSSEC?«	957
23.2.2	Anpassungen am Server	959
23.2.3	Schlüssel erzeugen	960
23.2.4	Schlüssel der Zone hinzufügen und die Zone signieren	961
23.2.5	Signierte Zone aktivieren	963
23.2.6	Signierung prüfen	963
23.2.7	Die Signierung veröffentlichen	965
23.2.8	Weniger anstrengend: Mehr Automatismus!	966
23.2.9	Fazit	967
<b>23.3</b>	<b>Client-Anfragen absichern mit »DNS over HTTPS (DoH)«</b>	967
23.3.1	Installation	967
23.3.2	Vorbereitungen	968
23.3.3	Konfiguration	969
23.3.4	Funktionstest	970
23.3.5	Client-Konfiguration	971

---

<b>24</b>	<b>OpenSSH</b>	973
-----------	----------------	-----

---

<b>24.1</b>	<b>Die SSH-Familie</b>	973
24.1.1	Die Clients: ssh, scp, sftp	974
24.1.2	Der Server: sshd	976
<b>24.2</b>	<b>Schlüssel statt Passwort</b>	978
24.2.1	Schlüssel erzeugen	978
24.2.2	Passwortloses Login	979
24.2.3	Der SSH-Agent merkt sich Passphrasen	980
<b>24.3</b>	<b>X11-Forwarding</b>	981
<b>24.4</b>	<b>Portweiterleitung und Tunneling</b>	982
24.4.1	SshFS: Entfernte Verzeichnisse lokal einbinden	983

---

<b>25</b>	<b>Administrationstools</b>	985
-----------	-----------------------------	-----

---

<b>25.1</b>	<b>Was kann dies und jenes noch?</b>	985
25.1.1	Der Rsync-Daemon	985
25.1.2	Wenn's mal wieder später wird: screen	987

25.1.3	Anklopfen mit nmap .....	987
25.1.4	Netzwerkinspektion: netstat .....	991
25.1.5	Zugreifende Prozesse finden: lsof .....	993
25.1.6	Was macht mein System? top .....	997
25.1.7	Wenn gar nichts mehr geht – Debugging mit strace .....	1001
25.1.8	Prüfung der Erreichbarkeit mit my traceroute .....	1006
25.1.9	Subnetzberechnung mit ipcalc .....	1007
<b>25.2</b>	<b>Aus der Ferne – Remote-Administrationstools .....</b>	<b>1008</b>
25.2.1	PuTTY .....	1009
25.2.2	WinSCP .....	1012
25.2.3	Synergy .....	1013
25.2.4	Eine für immer: mosh .....	1015

## 26 Versionskontrolle 1017

---

<b>26.1</b>	<b>Philosophien .....</b>	<b>1018</b>
26.1.1	Lokal .....	1018
26.1.2	Zentral .....	1019
26.1.3	Dezentral .....	1020
<b>26.2</b>	<b>Versionskontrollsysteme .....</b>	<b>1020</b>
26.2.1	CVS .....	1021
26.2.2	Apache Subversion .....	1024
26.2.3	GNU Bazaar .....	1026
26.2.4	Mercurial .....	1028
26.2.5	Git .....	1030
<b>26.3</b>	<b>Kommandos .....</b>	<b>1032</b>
<b>26.4</b>	<b>Serverdienste .....</b>	<b>1033</b>
26.4.1	Git-Server mit Gitolite .....	1033
26.4.2	Git-Server mit Gitea .....	1037

TEIL VI    Automatisierung

27    Scripting 1043

---

27.1	Aufgebohrte Muscheln .....	1043
27.2	Vom Suchen und Finden: ein kurzer Überblick .....	1044
27.2.1	Die Detektive: grep, sed und awk .....	1044
27.2.2	Reguläre Ausdrücke verstehen und anwenden .....	1045
27.3	Fortgeschrittene Shell-Programmierung .....	1048
27.3.1	Expansionsschemata .....	1048
27.3.2	Umgebungsvariablen .....	1052
27.3.3	»Back to bash«: ein tieferer Blick in die Muschel .....	1053
27.3.4	Logging in Skripten .....	1057
27.4	Tipps und Tricks aus der Praxis .....	1060
27.4.1	Aufräumkommando .....	1061
27.4.2	IFS .....	1061
27.4.3	Datumsmagie .....	1062
27.4.4	E-Mails aus einem Skript versenden .....	1062
27.4.5	Interaktive Programme steuern .....	1063

28    Konfigurationsmanagement mit Ansible 1065

---

28.1	Einführung und Installation .....	1065
28.1.1	Was ist Ansible? .....	1065
28.1.2	Geschichte und Versionen .....	1067
28.1.3	Setup/Laborumgebung .....	1067
28.1.4	Ansible-Installation auf dem Control Host .....	1068
28.1.5	Authentifizierung und Autorisierung auf den Target Hosts .....	1071
28.1.6	Einrichten der SSH-Public-Key-Authentifizierung .....	1072
28.1.7	Ein Ad-hoc-Test ohne jegliche Konfiguration .....	1072
28.2	Basiseinrichtung und erstes Inventory-Management .....	1074
28.2.1	Verzeichnisstruktur einrichten .....	1074
28.2.2	Grundkonfiguration (»ansible.cfg«) .....	1075
28.2.3	Erstellen und Verwalten eines statischen Inventorys .....	1076
28.2.4	Inventory-Aliasse und Namensbereiche .....	1078
28.2.5	Jenseits von Ping .....	1079
28.2.6	Ein etwas komplexeres Beispiel .....	1081
28.2.7	Alternative bzw. mehrere Inventorys .....	1082



<b>28.3</b>	<b>Ad-hoc-Kommandos und Patterns</b>	1084
28.3.1	Ad-hoc-Kommandos	1084
28.3.2	Use Cases jenseits von »command« und »shell«	1085
28.3.3	Idempotenz	1086
28.3.4	Interne Funktionsweise	1086
28.3.5	Die Ansible-Konsole	1088
28.3.6	Patterns zum Adressieren von Hosts	1089
<b>28.4</b>	<b>Die Konfigurations- und Serialisierungssprache YAML</b>	1090
28.4.1	Syntax und Struktur	1090
28.4.2	YAML-Files editieren	1091
28.4.3	Listen und Maps	1092
28.4.4	Verschachtelte Strukturen	1093
28.4.5	Textpassagen und Block-Ausdrücke	1094
28.4.6	Das Nichts in YAML	1095
<b>28.5</b>	<b>Playbooks und Tasks: die Grundlagen</b>	1095
28.5.1	Hallo Ansible – das allererste Playbook	1096
28.5.2	Formulierung von Tasks	1099
28.5.3	Beenden von Plays	1100
28.5.4	Fehlerbehandlung, Retry-Files	1101
28.5.5	Tags	1102
28.5.6	Das Kommando »ansible-playbook«	1103
28.5.7	Eine exemplarische Apache-Installation	1104
28.5.8	Handler: Tasks nur bei Changes durchführen	1108
<b>28.6</b>	<b>Playbooks und Tasks: fortgeschrittene Methoden</b>	1112
28.6.1	Variablen	1112
28.6.2	Registrierte Variablen	1118
28.6.3	Facts und implizite Variablen	1122
28.6.4	Bedingte Ausführung mit »when«	1124
28.6.5	Jinja und Templates	1125
28.6.6	Schleifen	1128
28.6.7	Fehlerbehandlung mit »failed_when« und »ignore_errors«	1133
28.6.8	Blocks	1134
28.6.9	Lookup-Plug-ins	1134
28.6.10	Umgebungsvariablen setzen	1136
<b>28.7</b>	<b>Module und Collections verwenden</b>	1137
28.7.1	Collections	1137
28.7.2	Module	1141
28.7.3	Module zur Kommandoausführung	1142
28.7.4	Module zur Paketverwaltung	1143

28.7.5	Module zur Verwaltung von Dateien und Dateiinhalten .....	1145
28.7.6	Module für weitere typische Verwaltungsaufgaben .....	1148
28.7.7	Spezialmodule (Kontrollflusssteuerung etc.) .....	1151
<b>28.8</b>	<b>Nächste Schritte .....</b>	<b>1153</b>

## 29 Monitoring – wissen, was läuft 1155

<b>29.1</b>	<b>Monitoring mit Checkmk .....</b>	<b>1155</b>
<b>29.2</b>	<b>Installation der Pakete .....</b>	<b>1155</b>
29.2.1	Installation von Checkmk unter openSUSE .....	1156
29.2.2	Installation von Checkmk unter Debian/Ubuntu .....	1156
29.2.3	Installation von Checkmk unter CentOS .....	1156
29.2.4	Die erste Kontrolle – klappt alles? .....	1156
<b>29.3</b>	<b>Einrichtung der ersten Monitoring-Instanz .....</b>	<b>1157</b>
<b>29.4</b>	<b>Server, Geräte und Dienste überwachen .....</b>	<b>1160</b>
<b>29.5</b>	<b>Installation des Checkmk-Agenten .....</b>	<b>1161</b>
<b>29.6</b>	<b>Anlegen eines Hosts .....</b>	<b>1162</b>
<b>29.7</b>	<b>Betriebs- und Fehlerzustände von Host und Services im Überblick .....</b>	<b>1163</b>
<b>29.8</b>	<b>Konfiguration durch Regelsätze .....</b>	<b>1164</b>
29.8.1	Arbeiten in Host-Ordern .....	1165
29.8.2	Keine Alarme für Testsysteme .....	1167
29.8.3	Unterschiedliche Alarmschwellen bei Dateisystemen .....	1168
29.8.4	Service Discovery Rules: Gezielt Prozesse überwachen .....	1170
29.8.5	HTTP, TCP und E-Mail: Netzwerkdienste überwachen .....	1172
<b>29.9</b>	<b>Notifications .....</b>	<b>1173</b>
29.9.1	Anlegen weiterer Kontaktgruppen .....	1173
29.9.2	Test der E-Mail-Zustellung .....	1174
29.9.3	Alarmierung per SMS .....	1174
29.9.4	Wann wird ein Fehler zum HARD STATE? .....	1175
29.9.5	Definieren von Notification Periods .....	1176
<b>29.10</b>	<b>Alarme managen .....</b>	<b>1176</b>
29.10.1	Die mächtige Suche von Checkmk .....	1178
<b>29.11</b>	<b>Weitere Fähigkeiten von Checkmk .....</b>	<b>1179</b>
<b>29.12</b>	<b>Fazit .....</b>	<b>1180</b>

TEIL VII    Sicherheit, Verschlüsselung und Zertifikate

<b>30</b>	<b>Sicherheit</b>	1183
<hr/>		
<b>30.1</b>	<b>Weniger ist mehr</b>	1184
<b>30.2</b>	<b>chroot</b>	1184
30.2.1	Dienste	1185
<b>30.3</b>	<b>Selbstabsicherung: AppArmor</b>	1187
30.3.1	Status und Betriebsarten	1188
30.3.2	Eigene Profile erstellen	1190
<b>30.4</b>	<b>Gotcha! Intrusion-Detection-Systeme</b>	1193
30.4.1	snort und Co.	1194
<b>30.5</b>	<b>Installation und Konfiguration</b>	1195
30.5.1	Vorbereitungen	1196
30.5.2	Kompilieren und installieren	1197
30.5.3	Basiskonfiguration	1198
30.5.4	Ein erster Test: ICMP	1199
30.5.5	Start-Skript erstellen: systemd	1200
<b>30.6</b>	<b>Immer das Neueste vom Neuen: pulledpork</b>	1201
<b>30.7</b>	<b>Klein, aber oho: fail2ban</b>	1204
30.7.1	Konfiguration	1204
30.7.2	Aktive Sperrungen	1207
30.7.3	Reguläre Ausdrücke	1209
<b>30.8</b>	<b>OpenVPN</b>	1210
30.8.1	Serverinstallation – OpenVPN, PKI und Co.	1211
30.8.2	CentOS/openSUSE Leap: easy-rsa	1215
30.8.3	Gemeinsam weiter	1218
30.8.4	Für den Roadwarrior	1220
30.8.5	Start-Skript?	1222
30.8.6	Site-to-site	1226
30.8.7	Simple-HA	1228
30.8.8	Tipps und Tricks	1229
<b>30.9</b>	<b>Schnell, Modern, Sicher: WireGuard</b>	1232
30.9.1	Schnell einen Tunnel einrichten	1233
30.9.2	Die dunkle Seite des Mondes	1235
30.9.3	Dauerhafte Tunnel mit »systemd«	1235

30.9.4	Alle machen mit: »Hub and Spoke« .....	1237
30.9.5	Tipps und Tricks .....	1238
<b>30.10</b>	<b>Fazit .....</b>	<b>1239</b>

## **31 Verschlüsselung und Zertifikate** 1241

---

<b>31.1</b>	<b>Definition und Historie .....</b>	<b>1241</b>
<b>31.2</b>	<b>Moderne Kryptologie .....</b>	<b>1243</b>
31.2.1	Symmetrische Verschlüsselung .....	1243
31.2.2	Asymmetrische Verschlüsselung .....	1244
<b>31.3</b>	<b>Den Durchblick behalten .....</b>	<b>1245</b>
31.3.1	Das Grundproblem .....	1245
31.3.2	Verwendungszwecke .....	1246
31.3.3	Umsetzung mithilfe einer PKI .....	1246
31.3.4	X.509 .....	1247
31.3.5	Ein anderer Ansatz: PGP (Web-of-Trust) .....	1249
<b>31.4</b>	<b>Einmal mit allem und kostenlos bitte: Let's Encrypt .....</b>	<b>1249</b>
31.4.1	Wie funktioniert das? .....	1250
31.4.2	Einschränkungen .....	1251
31.4.3	Der Client certbot .....	1251
<b>31.5</b>	<b>In der Praxis .....</b>	<b>1253</b>
31.5.1	Einrichtung einer PKI mit Server- und E-Mail-Zertifikaten .....	1253
31.5.2	Lokale Zertifikatsausstellung wie Let's Encrypt: acme2certifier .....	1264
31.5.3	E-Mail-Verschlüsselung .....	1271
<b>31.6</b>	<b>Neben der Kommunikation – Dateiverschlüsselung .....</b>	<b>1279</b>
31.6.1	Dateien .....	1279
31.6.2	Devices .....	1280
31.6.3	Festplatten/System .....	1282

Die Autoren .....	1287
-------------------	------

Index .....	1289
-------------	------