

# Inhalt

Vorwort .....	33
Über dieses Buch .....	41

## **1 Der Administrator** 45

---

<b>1.1 Der Beruf des Systemadministrators</b> .....	45
1.1.1 Berufsbezeichnung und Aufgaben .....	45
1.1.2 Job-Definitionen .....	46
1.1.3 Definitionen der Management-Level .....	51
<b>1.2 Nützliche Fähigkeiten und Fertigkeiten</b> .....	52
1.2.1 Soziale Fähigkeiten .....	53
1.2.2 Arbeitstechniken .....	53
<b>1.3 Das Verhältnis des Administrators zu Normalsterblichen</b> .....	55
1.3.1 Der Chef und andere Vorgesetzte .....	55
1.3.2 Benutzer .....	56
1.3.3 Andere Administratoren .....	56
<b>1.4 Unterbrechungsgesteuertes Arbeiten</b> .....	57
<b>1.5 Einordnung der Systemadministration</b> .....	58
1.5.1 Arbeitsgebiete .....	58
1.5.2 DevOps .....	61
<b>1.6 Ethischer Verhaltenskodex</b> .....	63
<b>1.7 Administration – eine Lebenseinstellung?</b> .....	64

## TEIL I Grundlagen

## **2 Bootvorgang** 69

---

<b>2.1 Einführung</b> .....	69
<b>2.2 Der Bootloader GRUB 2</b> .....	69
2.2.1 Funktionsweise .....	69
2.2.2 Installation .....	70
2.2.3 Konfiguration .....	70

<b>2.3</b>	<b>Bootloader Recovery</b> .....	76
<b>2.4</b>	<b>Der Kernel und die »initrd«</b> .....	77
2.4.1	»initrd« erstellen und modifizieren .....	78
2.4.2	»initrd« manuell modifizieren .....	82
<b>2.5</b>	<b>»systemd«</b> .....	83
2.5.1	Begrifflichkeiten .....	84
2.5.2	Kontrollieren von Diensten .....	85
2.5.3	Aktivieren und Deaktivieren von Diensten .....	87
2.5.4	Erstellen und Aktivieren eigener Service Units .....	88
2.5.5	Target Units .....	90
2.5.6	»systemd«- und Servicekonfigurationen .....	91
2.5.7	Anzeige von Dienstabhängigkeiten .....	92
2.5.8	Logs mit »journald« .....	94
2.5.9	Abschlussbemerkung .....	95

## **3 Festplatten und andere Devices** 97

---

<b>3.1</b>	<b>RAID</b> .....	97
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 .....	110
<b>3.2</b>	<b>Rein logisch: Logical Volume Manager »LVM«</b> .....	110
3.2.1	Grundlagen und Begriffe .....	112
3.2.2	Setup .....	114
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 .....	120
3.2.7	Eine defekte Festplatte ersetzen .....	121
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> .....	134
3.3.1	»udev«-Regeln .....	134
3.3.2	Eigene Regeln schreiben .....	135
<b>3.4</b>	<b>Alles virtuell? »/proc«</b> .....	137
3.4.1	CPU .....	138
3.4.2	RAM .....	139
3.4.3	Kernelkonfiguration .....	140
3.4.4	Kernelparameter .....	141
3.4.5	Gemountete Dateisysteme .....	141
3.4.6	Prozessinformationen .....	142
3.4.7	Netzwerk .....	143
3.4.8	Änderungen dauerhaft speichern .....	144
3.4.9	Abschlussbemerkung .....	144

## **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 .....	149
<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 .....	156
<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 .....	190
5.6.3	Argumente zu den Modulen .....	190
5.6.4	Modulpfade .....	191
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> .....	196
5.8.1	Setzen der »ulimit«-Werte .....	197
<b>5.9</b>	<b>Abschlussbemerkung</b> .....	198

## 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	»yum«, »yast«, »zypper« oder »apt«? .....	204
6.1.3	Außerirdische an Bord – »alien« .....	206

<b>6.2</b>	<b>Pakete im Eigenbau</b> .....	207
6.2.1	Vorbereitungen .....	207
6.2.2	Am Anfang war das Makefile .....	208
6.2.3	Vom Fellknäuel zum Paket .....	211
6.2.4	Patchen mit »patch« und »diff« .....	214
6.2.5	Updates sicher konfigurieren .....	216
<b>6.3</b>	<b>Updates nur einmal laden: »Cache«</b> .....	219
6.3.1	»deb«-basierte Distributionen: »apt-cacher-ng« .....	219
6.3.2	Installation .....	219
6.3.3	Konfiguration .....	219
6.3.4	Clientkonfiguration .....	221
6.3.5	Fütterungszeit – bereits geladene Pakete dem Cache hinzufügen .....	221
6.3.6	Details: »Report-HTML« .....	222
6.3.7	»rpm«-basierte Distributionen .....	223
<b>6.4</b>	<b>Alles meins: »Mirror«</b> .....	223
6.4.1	»deb«-basierte Distributionen: »debmirror« .....	223
6.4.2	Konfiguration .....	223
6.4.3	Benutzer und Gruppe anlegen .....	224
6.4.4	Verzeichnisstruktur anlegen .....	224
6.4.5	Mirror-Skript erstellen (Ubuntu) .....	224
6.4.6	Cronjobs einrichten .....	227
6.4.7	Schlüssel importieren .....	228
6.4.8	Mirror erstellen .....	228
6.4.9	Mirror verfügbar machen – Webdienst konfigurieren .....	228
6.4.10	Clientkonfiguration .....	229
6.4.11	rpm-basierte Distributionen .....	230
6.4.12	Benutzer und Gruppe anlegen .....	230
6.4.13	Verzeichnisstruktur anlegen: »openSUSE Leap« .....	231
6.4.14	Verzeichnisstruktur anlegen: »CentOS« .....	231
6.4.15	Mirror-Skript erstellen .....	231
6.4.16	Cronjobs einrichten .....	232
6.4.17	Mirror erstellen .....	233
6.4.18	Mirror verfügbar machen – Webdienst konfigurieren .....	234
6.4.19	Clientkonfiguration: »openSUSE Leap« .....	235
6.4.20	Clientkonfiguration: »CentOS« .....	235

## 7 Backup und Recovery 237

---

<b>7.1</b>	<b>Backup gleich Disaster Recovery?</b> .....	237
<b>7.2</b>	<b>Backupstrategien</b> .....	238
<b>7.3</b>	<b>Datensicherung mit »tar«</b> .....	241
7.3.1	Weitere interessante Optionen für GNU-»tar« .....	242
7.3.2	Sicherung über das Netzwerk mit »tar« und »ssh« .....	243
<b>7.4</b>	<b>Datensynchronisation mit »rsync«</b> .....	244
7.4.1	Lokale Datensicherung mit »rsync« .....	244
7.4.2	Synchronisieren im Netzwerk mit »rsync« .....	245
7.4.3	Wichtige Optionen für »rsync« .....	245
7.4.4	Backupskript für die Sicherung auf einen Wechseldatenträger .....	247
7.4.5	Backupskript für die Sicherung auf einen Backupserver .....	248
7.4.6	Verwendung von »ssh« für die Absicherung von »rsync« .....	250
<b>7.5</b>	<b>Imagesicherung mit »dd«</b> .....	251
7.5.1	Sichern des Master Boot Records (MBR) .....	251
7.5.2	Partitionstabelle mithilfe von »dd« zurückspielen .....	252
7.5.3	Images mit »dd« erstellen .....	252
7.5.4	Einzelne Dateien mit »dd« aus einem Image zurückspielen .....	253
7.5.5	Abschlussbemerkung zu »dd« .....	255
<b>7.6</b>	<b>Disaster Recovery mit ReaR</b> .....	255
7.6.1	ReaR installieren .....	257
7.6.2	ReaR konfigurieren .....	257
7.6.3	Aufrufparameter von ReaR .....	259
7.6.4	Der erste Testlauf .....	260
7.6.5	Der Recovery-Prozess .....	264
7.6.6	Die ReaR-Konfiguration im Detail .....	266
7.6.7	Migrationen mit ReaR .....	267

## TEIL III Dienste

## 8 Webserver 271

---

<b>8.1</b>	<b>Apache</b> .....	271
8.1.1	Installation .....	271
8.1.2	Virtuelle Hosts einrichten .....	272

8.1.3	Debian/Ubuntu: Virtuelle Hosts aktivieren .....	275
8.1.4	HTTPS konfigurieren .....	275
8.1.5	Benutzer-Authentifizierung mit Kerberos .....	280
8.1.6	Apache-Server mit ModSecurity schützen .....	281
8.1.7	Tuning und Monitoring .....	286
<b>8.2</b>	<b>nginx</b> .....	<b>291</b>
8.2.1	Installation .....	291
8.2.2	Grundlegende Konfiguration .....	291
8.2.3	Virtuelle Hosts .....	292
8.2.4	HTTPS mit nginx .....	294
<b>8.3</b>	<b>Logfiles auswerten</b> .....	<b>295</b>
<b>9</b>	<b>FTP-Server</b> .....	<b>299</b>
<hr/>		
<b>9.1</b>	<b>Einstieg</b> .....	<b>299</b>
9.1.1	Das File Transfer Protocol .....	299
9.1.2	vsftpd .....	300
<b>9.2</b>	<b>Download-Server</b> .....	<b>300</b>
<b>9.3</b>	<b>Zugriff von Usern auf ihre Homeverzeichnisse</b> .....	<b>302</b>
<b>9.4</b>	<b>FTP über SSL (FTPS)</b> .....	<b>303</b>
<b>9.5</b>	<b>Anbindung an LDAP</b> .....	<b>305</b>
<b>10</b>	<b>Mailserver</b> .....	<b>307</b>
<hr/>		
<b>10.1</b>	<b>Postfix</b> .....	<b>307</b>
10.1.1	Grundlegende Konfiguration .....	308
10.1.2	Postfix als Relay vor Exchange, Dovecot oder anderen Backends .....	310
10.1.3	Die Postfix-Restrictions: Der Schlüssel zu Postfix .....	312
10.1.4	Weiterleitungen und Aliasse für Mailadressen .....	321
10.1.5	SASL/SMTP-Auth .....	322
10.1.6	SSL/TLS für Postfix einrichten .....	324
<b>10.2</b>	<b>Antivirus- und Spam-Filter mit Amavisd-new, ClamAV und SpamAssassin</b> .....	<b>326</b>
10.2.1	Installation .....	328
10.2.2	ClamAV konfigurieren .....	328
10.2.3	Updates für SpamAssassin konfigurieren .....	329

10.2.4	Amavisd-new konfigurieren .....	330
10.2.5	Eine Quarantäne mit Amavis betreiben .....	335
10.2.6	Postfix für die Verwendung mit Amavisd-new konfigurieren .....	337
<b>10.3</b>	<b>POP3/IMAP-Server mit Dovecot .....</b>	<b>338</b>
10.3.1	Vorbereitungen im Linux-System .....	338
10.3.2	Log-Meldungen und Debugging .....	339
10.3.3	User-Authentifizierung .....	340
10.3.4	Aktivierung des LMTP-Servers von Dovecot .....	341
10.3.5	Einrichten von SSL/TLS-Verschlüsselung .....	342
<b>10.4</b>	<b>Der Ernstfall: Der IMAP-Server erwacht zum Leben .....</b>	<b>344</b>
<b>10.5</b>	<b>Dovecot im Replikations-Cluster .....</b>	<b>346</b>
10.5.1	Einrichtung der Replikation .....	347
10.5.2	Hochverfügbare Service-IP .....	350
<b>10.6</b>	<b>Monitoring und Logfile-Auswertung .....</b>	<b>351</b>
10.6.1	Logfile-Auswertung mit »Pflogsumm« .....	352

## **11 Datenbank** 355

---

<b>11.1</b>	<b>MariaDB in der Praxis .....</b>	<b>355</b>
11.1.1	Installation und grundlegende Einrichtung .....	355
11.1.2	Replikation .....	357
11.1.3	Master-Master-Replikation .....	365
<b>11.2</b>	<b>Tuning .....</b>	<b>368</b>
11.2.1	Tuning des Speichers .....	369
11.2.2	Tuning von Indizes .....	375
<b>11.3</b>	<b>Backup und Point-In-Time-Recovery .....</b>	<b>380</b>
11.3.1	Restore zum letztmöglichen Zeitpunkt .....	380
11.3.2	Restore zu einem bestimmten Zeitpunkt .....	381

## **12 Syslog** 383

---

<b>12.1</b>	<b>Aufbau von Syslog-Nachrichten .....</b>	<b>383</b>
<b>12.2</b>	<b>Der Klassiker: »SyslogD« .....</b>	<b>385</b>



<b>12.3</b>	<b>Syslog-ng</b> .....	387
12.3.1	Der »options«-Abschnitt .....	387
12.3.2	Das »source«-Objekt .....	389
12.3.3	Das »destination«-Objekt .....	389
12.3.4	Das »filter«-Objekt .....	391
12.3.5	Das »log«-Objekt .....	392
<b>12.4</b>	<b>Rsyslog</b> .....	393
12.4.1	Eigenschaftsbasierte Filter .....	393
12.4.2	Ausdrucksbasierte Filter .....	394
<b>12.5</b>	<b>Loggen über das Netz</b> .....	395
12.5.1	SyslogD .....	395
12.5.2	Syslog-ng .....	396
12.5.3	Rsyslog .....	396
<b>12.6</b>	<b>Syslog in eine Datenbank schreiben</b> .....	397
12.6.1	Anlegen der Log-Datenbank .....	397
12.6.2	In die Datenbank loggen .....	398
<b>12.7</b>	<b>»systemd« mit »journalctl«</b> .....	400
12.7.1	Erste Schritte mit dem »journalctl«-Kommando .....	401
12.7.2	Filtern nach Zeit .....	403
12.7.3	Filtern nach Diensten .....	405
12.7.4	Kernelmeldungen .....	406
<b>12.8</b>	<b>Fazit</b> .....	407

---

## **13 Proxy-Server** 409

<b>13.1</b>	<b>Einführung des Stellvertreters</b> .....	409
<b>13.2</b>	<b>Proxys in Zeiten des Breitbandinternets</b> .....	410
<b>13.3</b>	<b>Herangehensweisen und Vorüberlegungen</b> .....	411
<b>13.4</b>	<b>Grundkonfiguration</b> .....	411
13.4.1	Aufbau des Testumfelds .....	412
13.4.2	Netzwerk .....	412
13.4.3	Cache .....	413
13.4.4	Logging .....	414
13.4.5	Handhabung des Dienstes .....	416
13.4.6	Objekte .....	418
13.4.7	Objekttypen .....	419

13.4.8	Objektlisten in Dateien .....	419
13.4.9	Regeln .....	420
13.4.10	Überlagerung mit »first match« .....	422
13.4.11	Anwendung von Objekten und Regeln .....	423
<b>13.5</b>	<b>Authentifizierung</b> .....	<b>424</b>
13.5.1	Benutzerbasiert .....	427
13.5.2	Gruppenbasiert .....	437
<b>13.6</b>	<b>Log-Auswertung: »Calamaris« und »Sarg«</b> .....	<b>440</b>
13.6.1	Calamaris .....	440
13.6.2	Sarg .....	442
<b>13.7</b>	<b>Unsichtbar: »transparent proxy«</b> .....	<b>443</b>
<b>13.8</b>	<b>Ab in den Pool – Verzögerung mit »delay_pools«</b> .....	<b>444</b>
13.8.1	Funktionsweise – alles im Eimer! .....	444
13.8.2	Details – Klassen, Eimer und ACLs richtig wählen .....	445
<b>13.9</b>	<b>Familienbetrieb: »Sibling, Parent und Co.«</b> .....	<b>448</b>
13.9.1	Grundlagen .....	448
13.9.2	Eltern definieren .....	449
13.9.3	Geschwister definieren .....	449
13.9.4	Load Balancing .....	450
13.9.5	Inhalte eigenständig abrufen: »always_direct« .....	451
<b>13.10</b>	<b>Cache-Konfiguration</b> .....	<b>451</b>
13.10.1	Cache-Arten: »Hauptspeicher« und »Festplatten« .....	451
13.10.2	Hauptspeicher-Cache .....	452
13.10.3	Festplatten-Cache .....	452
13.10.4	Tuning .....	455
<b>14</b>	<b>Kerberos</b> .....	<b>457</b>
<hr/>		
<b>14.1</b>	<b>Begriffe im Zusammenhang mit Kerberos</b> .....	<b>458</b>
<b>14.2</b>	<b>Funktionsweise von Kerberos</b> .....	<b>459</b>
<b>14.3</b>	<b>Installation und Konfiguration des Kerberos-Servers</b> .....	<b>460</b>
14.3.1	Konfiguration der Datei »/etc/krb5.conf« .....	461
14.3.2	Konfiguration der Datei »kdc.conf« .....	462
<b>14.4</b>	<b>Initialisierung und Testen des Kerberos-Servers</b> .....	<b>465</b>
14.4.1	Verwalten der Principals .....	468

<b>14.5</b>	<b>Kerberos und PAM</b> .....	471
14.5.1	Konfiguration der PAM-Dateien auf einem openSUSE-System .....	472
14.5.2	Testen der Anmeldung .....	472
<b>14.6</b>	<b>Neue Benutzer mit Kerberos-Principal anlegen</b> .....	473
<b>14.7</b>	<b>Hosts und Dienste</b> .....	474
14.7.1	Einträge entfernen .....	476
<b>14.8</b>	<b>Konfiguration des Kerberos-Clients</b> .....	477
14.8.1	PAM und Kerberos auf dem Client .....	478
<b>14.9</b>	<b>Replikation des Kerberos-Servers</b> .....	479
14.9.1	Bekanntmachung aller KDCs im Netz .....	479
14.9.2	Konfiguration des KDC-Masters .....	482
14.9.3	Konfiguration des KDC-Slaves .....	485
14.9.4	Replikation des KDC-Masters auf den KDC-Slave .....	485
<b>14.10</b>	<b>Kerberos-Policies</b> .....	487
<b>14.11</b>	<b>Kerberos in LDAP einbinden</b> .....	490
14.11.1	Konfiguration des LDAP-Servers .....	490
14.11.2	Umstellung des Kerberos-Servers .....	493
14.11.3	Zurücksichern der alten Datenbank .....	497
14.11.4	Erstellung der Service-Keys in der Standard-»keytab«-Datei .....	498
14.11.5	Erstellung der Service Keys in einer eigenen Datei .....	499
14.11.6	Bestehende LDAP-Benutzer um Kerberos-Principal erweitern .....	500
<b>14.12</b>	<b>Neue Benutzer im LDAP-Baum</b> .....	502
<b>14.13</b>	<b>Authentifizierung am LDAP-Server über »GSSAPI«</b> .....	504
14.13.1	Authentifizierung unter Debian und Ubuntu einrichten .....	504
14.13.2	Authentifizierung unter openSUSE und CentOS einrichten .....	509
14.13.3	Den zweiten KDCs an den LDAP-Server anbinden .....	513
<b>14.14</b>	<b>Konfiguration des LAM Pro</b> .....	514

## **15 Samba 4** 517

---

<b>15.1</b>	<b>Vorüberlegungen</b> .....	517
15.1.1	Installation der Pakete unter Ubuntu und Debian .....	519
<b>15.2</b>	<b>Konfiguration von Samba 4 als Domaincontroller</b> .....	519
15.2.1	Konfiguration des Bind9 .....	524

<b>15.3</b>	<b>Testen des Domaincontrollers</b> .....	527
15.3.1	Testen des DNS-Servers .....	529
15.3.2	Test des Verbindungsaufbaus .....	530
15.3.3	Test des Kerberos-Servers .....	530
15.3.4	Einrichtung des Zeitservers .....	532
<b>15.4</b>	<b>Benutzer- und Gruppenverwaltung</b> .....	533
<b>15.5</b>	<b>Benutzer- und Gruppenverwaltung über die Kommandozeile</b> .....	534
15.5.1	Verwaltung von Gruppen über die Kommandozeile .....	534
15.5.2	Verwaltung von Benutzern über die Kommandozeile .....	538
15.5.3	Setzen der Passwortrichtlinien .....	542
<b>15.6</b>	<b>Die »Remote Server Administration Tools« (RSAT)</b> .....	543
15.6.1	Die »RSAT« einrichten .....	543
15.6.2	Beitritt eines Windows-Clients zur Domäne .....	544
15.6.3	Benutzer- und Gruppenverwaltung mit den »RSAT« .....	546
<b>15.7</b>	<b>Gruppenrichtlinien</b> .....	547
15.7.1	Verwaltung der GPOs mit den RSAT .....	547
15.7.2	Erste Schritte mit der Gruppenrichtlinienverwaltung .....	548
15.7.3	Eine Gruppenrichtlinie erstellen .....	550
15.7.4	Die Gruppenrichtlinie mit einer OU verknüpfen .....	553
15.7.5	Benutzer und Gruppen verschieben .....	555
15.7.6	GPOs über die Kommandozeile .....	556
<b>15.8</b>	<b>Linux-Client in der Domäne</b> .....	558
15.8.1	Konfiguration der Authentifizierung .....	564
15.8.2	Mounten über »pam_mount« .....	565
15.8.3	Umstellen des grafischen Logins .....	568
<b>15.9</b>	<b>Zusätzliche Server in der Domäne</b> .....	569
15.9.1	Einen Fileservers einrichten .....	569
15.9.2	Ein zusätzlicher Domaincontroller .....	572
15.9.3	Konfiguration des zweiten DC .....	573
15.9.4	Einrichten des Nameservers .....	575
15.9.5	Testen der Replikation .....	579
15.9.6	Weitere Tests .....	584
15.9.7	Einrichten des Zeitservers .....	584
<b>15.10</b>	<b>Die Replikation der Freigabe »sysvol« einrichten</b> .....	585
15.10.1	Einrichten des »rsync«-Servers .....	585
15.10.2	Einrichten von »rsync« auf dem »PDC-Master« .....	585
<b>15.11</b>	<b>Was geht noch mit Samba 4?</b> .....	590

<b>16</b>	<b>NFS</b>	591
<hr/>		
<b>16.1</b>	<b>Unterschiede zwischen »NFSv3« und »NFSv4«</b>	591
<b>16.2</b>	<b>Funktionsweise von »NFSv4«</b>	592
<b>16.3</b>	<b>Einrichten des »NFSv4«-Servers</b>	593
16.3.1	Konfiguration des Pseudodateisystems	593
16.3.2	Anpassen der Datei »/etc/exports«	594
16.3.3	Tests für den NFS-Server	596
<b>16.4</b>	<b>Konfiguration des »NFSv4«-Clients</b>	598
<b>16.5</b>	<b>Konfiguration des »idmapd«</b>	599
<b>16.6</b>	<b>Optimierung von »NFSv4«</b>	601
16.6.1	Optimierung des »NFSv4«-Servers	601
16.6.2	Optimierung des »NFSv4«-Clients	602
<b>16.7</b>	<b>»NFSv4« und Firewalls</b>	603
<b>16.8</b>	<b>NFS und Kerberos</b>	604
16.8.1	Erstellung der Principals und der »keytab«-Dateien	605
16.8.2	Kerberos-Authentifizierung unter Debian und Ubuntu	607
16.8.3	Kerberos-Authentifizierung auf SUSE und CentOS	608
16.8.4	Anpassen der Datei »/etc/exports«	608
16.8.5	Einen NFS-Client für Kerberos unter Debian und Ubuntu konfigurieren	608
16.8.6	Einen NFS-Client für Kerberos unter SUSE und CentOS konfigurieren	609
16.8.7	Testen der durch Kerberos abgesicherten NFS-Verbindung	609
16.8.8	Testen der Verbindung	609
<b>17</b>	<b>LDAP</b>	611
<hr/>		
<b>17.1</b>	<b>Einige Grundlagen zu LDAP</b>	612
17.1.1	Was ist ein Verzeichnisdienst?	612
17.1.2	Der Einsatz von LDAP im Netzwerk	613
17.1.3	Aufbau des LDAP-Datenmodells	613
17.1.4	Objekte	614
17.1.5	Attribute	615
17.1.6	Schema	615
17.1.7	Das LDIF-Format	619
<b>17.2</b>	<b>Unterschiede in den einzelnen Distributionen</b>	620
17.2.1	Umstellung auf die statische Konfiguration unter SUSE	620

17.2.2	Umstellung auf die statische Konfiguration unter Ubuntu-Server und Debian .....	621
17.2.3	Pfade und Benutzer .....	621
17.2.4	Die Datenbank-Backends .....	621
17.2.5	Grundkonfiguration des LDAP-Servers .....	621
<b>17.3</b>	<b>Konfiguration des LDAP-Clients .....</b>	<b>624</b>
<b>17.4</b>	<b>Absichern der Verbindung zum LDAP-Server über TLS .....</b>	<b>624</b>
17.4.1	Erstellen der Zertifizierungsstelle .....	625
17.4.2	Erstellen des Serverzertifikats .....	625
17.4.3	Signieren des Zertifikats .....	625
17.4.4	Zertifikate in die »slapd.conf« eintragen .....	626
17.4.5	Konfiguration des LDAP-Clients .....	626
<b>17.5</b>	<b>Einrichtung des »sssd« .....</b>	<b>627</b>
17.5.1	Erster Zugriff auf den LDAP-Server .....	630
<b>17.6</b>	<b>Grafische Werkzeuge für die LDAP-Verwaltung .....</b>	<b>631</b>
<b>17.7</b>	<b>Änderungen mit »ldapmodify« .....</b>	<b>632</b>
17.7.1	Interaktive Änderung mit »ldapmodify« .....	632
17.7.2	Änderungen über eine LDIF-Datei mit »ldapmodify« .....	633
<b>17.8</b>	<b>Absichern des LDAP-Baums mit ACLs .....</b>	<b>634</b>
17.8.1	Eine eigene Datei für die ACLs einbinden .....	635
17.8.2	Erste ACLs zur Grundsicherung des DIT .....	636
17.8.3	ACLs mit regulären Ausdrücken .....	637
17.8.4	ACLs vor dem Einsatz testen .....	638
<b>17.9</b>	<b>Filter zur Suche im LDAP-Baum .....</b>	<b>640</b>
17.9.1	Die Fähigkeiten des LDAP-Servers testen .....	640
17.9.2	Einfache Filter .....	642
17.9.3	Filter mit logischen Verknüpfungen .....	643
17.9.4	Einschränkung der Suchtiefe .....	643
<b>17.10</b>	<b>Verwendung von Overlays .....</b>	<b>644</b>
17.10.1	Overlays am Beispiel von »dynlist« .....	645
17.10.2	Weitere Overlays .....	646
<b>17.11</b>	<b>Partitionierung des DIT .....</b>	<b>647</b>
17.11.1	Einrichtung von »subordinate«-Datenbanken .....	647
17.11.2	Verwaltung von »Referrals« .....	649
17.11.3	Konfiguration des Hauptnamensraums .....	649
17.11.4	Die untergeordneten Datenbank einrichten .....	652
17.11.5	Testen der Referrals .....	654

<b>17.12</b>	<b>Einrichtung mit Chaining</b> .....	655
17.12.1	Die untergeordneten Datenbank einrichten .....	656
17.12.2	Konfiguration der Server .....	660
17.12.3	Erste Tests .....	663
17.12.4	Das Overlay »chain« .....	667
17.12.5	Der sssd-Zugriff .....	668
17.12.6	Auf dem untergeordneten Namensraum .....	671
<b>17.13</b>	<b>Testen der Umgebung</b> .....	673
17.13.1	Auf dem Master von »dc=exampe,dc=net« .....	673
17.13.2	Auf dem Master von »dc=referral,dc=example,dc=net« .....	675
<b>17.14</b>	<b>Replikation des DIT</b> .....	677
17.14.1	Konfiguration des Providers .....	679
17.14.2	Konfiguration des Consumers .....	681
<b>17.15</b>	<b>Die dynamische Konfiguration</b> .....	683
17.15.1	Umstellung auf die dynamische Konfiguration am Provider .....	683
17.15.2	Umstellung auf die dynamische Konfiguration am Consumer .....	687
<b>17.16</b>	<b>Verwaltung von Weiterleitungen für den Mailserver Postfix</b> .....	689
<b>17.17</b>	<b>Benutzerauthentifizierung von Dovecot über LDAP</b> .....	692
<b>17.18</b>	<b>Benutzerauthentifizierung am Proxy »Squid« über LDAP</b> .....	694
17.18.1	Die Authentifizierung über LDAP aktivieren .....	695
17.18.2	Benutzerbezogene Authentifizierung .....	696
17.18.3	Gruppenbezogene Authentifizierung .....	697
<b>17.19</b>	<b>Benutzerauthentifizierung am Webserver Apache über LDAP</b> .....	698
17.19.1	Konfiguration der Cache-Parameter .....	698
17.19.2	Konfiguration der Zugriffsparameter .....	699
<b>17.20</b>	<b>Und was geht sonst noch alles mit LDAP?</b> .....	701
<b>18</b>	<b>Druckserver</b> .....	703
<hr/>		
<b>18.1</b>	<b>Grundkonfiguration des Netzwerkzugriffs</b> .....	704
<b>18.2</b>	<b>Policies</b> .....	707
18.2.1	Location-Policies .....	708
18.2.2	Operation Policies .....	709
18.2.3	Weitere Konfigurationsmöglichkeiten .....	710
18.2.4	Browsing .....	712

<b>18.3 Drucker und Klassen einrichten und verwalten</b> .....	713
18.3.1 Drucker einrichten .....	713
18.3.2 Klassen einrichten .....	714
<b>18.4 Druckerquotas</b> .....	715
<b>18.5 CUPS über die Kommandozeile</b> .....	716
18.5.1 Einstellen eines Standarddruckers .....	716
18.5.2 Optionen für einen Drucker verwalten .....	717
<b>18.6 PPD-Dateien</b> .....	719
<b>18.7 CUPS und Kerberos</b> .....	720
18.7.1 Erstellen des Kerberos-Principals und der »keytab«-Datei .....	720
18.7.2 Umstellung der Authentifizierung am CUPS-Server .....	721
<b>18.8 Noch mehr Druck</b> .....	722

## TEIL IV Infrastruktur

### 19 Hochverfügbarkeit 725

---

<b>19.1 Das Beispiel-Setup</b> .....	725
<b>19.2 Installation</b> .....	726
19.2.1 Debian 9 und Ubuntu 18.04 LTS .....	726
19.2.2 CentOS 7.5 .....	726
19.2.3 openSUSE Leap .....	727
<b>19.3 Einfache Vorarbeiten</b> .....	727
<b>19.4 Shared Storage mit DRBD</b> .....	727
19.4.1 Grundlegende Konfiguration .....	728
19.4.2 Die wichtigsten Konfigurationsoptionen .....	729
19.4.3 Die DRBD-Ressource in Betrieb nehmen .....	730
<b>19.5 Grundkonfiguration der Clusterkomponenten</b> .....	733
19.5.1 Pacemaker und Corosync: das Benachrichtigungssystem .....	733
19.5.2 Pacemaker: der Ressourcenmanager .....	735
19.5.3 Quorum deaktivieren .....	737
<b>19.6 Dienste hochverfügbar machen</b> .....	739
19.6.1 Die erste Ressource: eine hochverfügbare IP-Adresse .....	741
19.6.2 Hochverfügbarkeit am Beispiel von Apache .....	744
19.6.3 DRBD integrieren .....	747
19.6.4 Fencing .....	751



## 20 Virtualisierung 753

---

<b>20.1</b>	<b>Einleitung</b> .....	753
<b>20.2</b>	<b>Für den »Sysadmin«</b> .....	754
<b>20.3</b>	<b>Servervirtualisierung</b> .....	758
20.3.1	KVM .....	759
20.3.2	Xen .....	761
<b>20.4</b>	<b>Netzwerkgrundlagen</b> .....	762
<b>20.5</b>	<b>Management und Installation</b> .....	763
20.5.1	Einheitlich arbeiten: »libvirt« .....	764
20.5.2	Konsolenbasiertes Management: »virsh« .....	767
20.5.3	Virtuelle Maschinen installieren .....	770
20.5.4	»virt-install« .....	772
20.5.5	Alleskönner: »Virtual Machine Manager« .....	775
20.5.6	Zusätzliche Konsolentools .....	779
<b>20.6</b>	<b>Umzugsunternehmen: Live Migration</b> .....	780
20.6.1	Vorbereitungen .....	781
20.6.2	Konfiguration im »Virtual Machine Manager« .....	781

## 21 Docker 783

---

<b>21.1</b>	<b>Einführung, Installation und wichtige Grundlagen</b> .....	783
21.1.1	Was ist Docker? .....	783
21.1.2	Was ist ein Container? .....	783
21.1.3	Container vs. VM .....	784
21.1.4	Docker: Entstehung und Geschichte .....	785
21.1.5	Docker-Versionen .....	785
21.1.6	Funktionale Übersicht .....	786
21.1.7	Installation .....	786
21.1.8	Ergänzungen zur Installation, erster Systemtest .....	788
21.1.9	Etwas Terminologie .....	790
21.1.10	Konfigurationsmöglichkeiten des Docker-Daemons .....	791
21.1.11	Betrieb hinter einem Proxy .....	791
21.1.12	Image-Schichten und Storage Driver .....	792
21.1.13	Einrichtung von devicemapper/direct-lvm .....	795

<b>21.2</b>	<b>Management von Images und Containern</b>	797
21.2.1	Das Docker-CLI (Command Line Interface)	797
21.2.2	Erste Schritte	798
21.2.3	Löschen von Containern und Images	799
21.2.4	Handling von Containern	800
21.2.5	Prozessverwaltung	802
21.2.6	Umgebungsvariablen	803
21.2.7	(Zentralisiertes) Logging	804
21.2.8	Verteilung von Images über Dateiversand	805
21.2.9	Der Docker Hub	805
21.2.10	Image-Tags und Namenskonventionen	806
21.2.11	Informationen über Images gewinnen	807
21.2.12	Go-Templates	808
21.2.13	Erstellen eigener Base-Images	809
21.2.14	Container limitieren	810
21.2.15	Packungsdichte	811
<b>21.3</b>	<b>Docker-Networking</b>	811
21.3.1	Grundlagen	811
21.3.2	Docker und iptables	812
21.3.3	/etc/hosts-Einträge beim Containerstart	812
21.3.4	User Defined Networks	812
21.3.5	Portmapping	813
<b>21.4</b>	<b>Datenpersistenz</b>	814
21.4.1	Bind Mounts und Volumes	814
21.4.2	Weitere Möglichkeiten zur Datenpersistenz	817
<b>21.5</b>	<b>Erstellen eigener Images mit Dockerfiles</b>	817
21.5.1	Einfaches Commmitten von Anpassungen	817
21.5.2	Dockerfiles und docker build: Basics	818
21.5.3	Dangling Images	819
21.5.4	Den Build-Cache umgehen	821
21.5.5	Fehler(-Suche) im Buildprozess	821
21.5.6	Die Dockerfile-Direktiven: Ein Überblick	822
21.5.7	Ein Beispiel mit COPY, VOLUME, EXPOSE, USER, CMD	823
21.5.8	CMD und ENTRYPOINT, CMD vs. ENTRYPOINT	825
21.5.9	.dockerignore-Files	826
21.5.10	Healthchecks	827
21.5.11	Multistage-Builds	828
21.5.12	Best Practices	829

<b>21.6</b>	<b>Multi-Container-Rollout mit Docker Compose</b> .....	829
21.6.1	Einleitung und Installation .....	829
21.6.2	Basics .....	830
21.6.3	Ein erstes Beispiel mit docker-compose .....	831
21.6.4	Build and Run .....	832
21.6.5	Netzwerke, Volumes, Environment .....	833
21.6.6	Flexible Compose-Konfigurationen durch Umgebungsvariablen .....	834
21.6.7	Integration in systemd .....	835
<b>21.7</b>	<b>Betrieb einer eigenen Registry</b> .....	836
21.7.1	Basis-Setup und erster Test .....	836
21.7.2	Registry mit TLS .....	838
21.7.3	Registry-Authentifizierung .....	840
21.7.4	Suchen oder Löschen in der privaten Registry .....	841
21.7.5	Der Docker Registry Manager .....	842
<b>21.8</b>	<b>Container-Cluster mit dem Docker Swarm Mode</b> .....	843
21.8.1	Swarm-Konzepte .....	843
21.8.2	Unser Beispielszenario .....	844
21.8.3	Cluster-Setup .....	845
21.8.4	Swarm Services .....	845
21.8.5	Skalierung .....	847
21.8.6	Netzwerken im Schwarm: Overlay-Netzwerke .....	847
21.8.7	Ausfallsicherheit .....	847
21.8.8	Ausrollen von Services .....	848
21.8.9	Labels und Constraints .....	850
21.8.10	Noch mal Healthchecks .....	851

## TEIL V Kommunikation

### **22 Netzwerk** 855

---

<b>22.1</b>	<b>Vorwort zu »Predictable Network Interface Names«</b> .....	855
<b>22.2</b>	<b>Netzwerkkonfiguration mit »iproute2«</b> .....	856
22.2.1	Erste Schritte .....	856
22.2.2	Die Syntax von »ip« .....	859
22.2.3	Links ansehen und manipulieren: »ip link« .....	859
22.2.4	IP-Adressen ansehen und manipulieren: »ip address« .....	861
22.2.5	Manipulation von ARP-Einträgen: »ip neighbour« .....	865

<b>22.3</b>	<b>Routing mit »ip«</b> .....	867
22.3.1	Routing-Informationen anzeigen .....	867
22.3.2	Da geht noch mehr: »Advanced Routing« .....	869
22.3.3	Die vorhandenen Regeln ansehen .....	870
22.3.4	Eine neue Routing-Tabelle anlegen .....	871
22.3.5	Ändern der »Policy Routing Database« .....	871
22.3.6	Routing über mehrere Uplinks .....	873
22.3.7	Fazit bis hierher .....	878
<b>22.4</b>	<b>Bonding</b> .....	878
22.4.1	Bonding-Konfiguration .....	879
22.4.2	Bonding unter Debian .....	882
22.4.3	Bonding unter Ubuntu .....	882
22.4.4	Bonding unter CentOS .....	883
22.4.5	Bonding unter openSUSE Leap .....	884
<b>22.5</b>	<b>IPv6</b> .....	884
22.5.1	Die Vorteile von IPv6 .....	886
22.5.2	Notation von IPv6-Adressen .....	886
22.5.3	Die Netzmasken .....	887
22.5.4	Die verschiedenen IPv6-Adressarten .....	887
22.5.5	Es geht auch ohne »ARP« .....	889
22.5.6	Feste Header-Länge .....	890
22.5.7	IPv6 in der Praxis .....	892
<b>22.6</b>	<b>Firewalls mit »netfilter« und »iptables«</b> .....	893
22.6.1	Der Weg ist das Ziel – wie Pakete durch den Kernel laufen .....	894
22.6.2	Einführung in »iptables« .....	895
22.6.3	Regeln definieren .....	897
22.6.4	Die klassischen Targets .....	899
22.6.5	Ein erster Testlauf .....	899
22.6.6	Rein wie raus: »Stateful Packet Inspection« .....	900
22.6.7	Das erste Firewallskript .....	902
22.6.8	Externe Firewall .....	904
22.6.9	Logging .....	910
22.6.10	Network Address Translation und Masquerading .....	912
22.6.11	Weitere nützliche Module für »iptables« .....	913
22.6.12	Abschlussbemerkung .....	916
<b>22.7</b>	<b>DHCP</b> .....	916
22.7.1	Funktionsweise .....	916
22.7.2	Konfiguration .....	917

<b>22.8</b>	<b>DNS-Server</b> .....	920
22.8.1	Funktionsweise .....	920
22.8.2	Unterschied: rekursiv und autoritativ .....	922
22.8.3	Einträge im DNS: »Resource Records« .....	922
22.8.4	Die Grundkonfiguration .....	923
22.8.5	Zonendefinitionen .....	926
22.8.6	Die erste vollständige Zone .....	930
22.8.7	Die »hint«-Zone .....	932
22.8.8	Reverse Lookup .....	934
22.8.9	Slave-Server .....	935
22.8.10	DNS-Server und IPv6 .....	937
<b>22.9</b>	<b>Vertrauen schaffen mit »DNSSEC«</b> .....	939
22.9.1	Die Theorie: »Wie arbeitet DNSSEC?« .....	939
22.9.2	Anpassungen am Server .....	941
22.9.3	Schlüssel erzeugen .....	942
22.9.4	Schlüssel der Zone hinzufügen und die Zone signieren .....	943
22.9.5	Signierte Zone aktivieren .....	944
22.9.6	Signierung prüfen .....	945
22.9.7	Die Signierung veröffentlichen .....	947
22.9.8	Fazit .....	948
<b>22.10</b>	<b>Nachwort zum Thema Netzwerk</b> .....	948

## **23 OpenSSH** 949

---

<b>23.1</b>	<b>Die SSH-Familie</b> .....	949
23.1.1	Die Clients: »ssh«, »scp«, »sftp« .....	950
23.1.2	Der Server: »sshd« .....	952
<b>23.2</b>	<b>Schlüssel statt Passwort</b> .....	954
23.2.1	Schlüssel erzeugen .....	954
23.2.2	Passwortloses Login .....	955
23.2.3	Der SSH-Agent merkt sich Passphrasen .....	956
<b>23.3</b>	<b>X11-Forwarding</b> .....	957
<b>23.4</b>	<b>Portweiterleitung und Tunneling</b> .....	957
23.4.1	SshFS: entfernte Verzeichnisse lokal einbinden .....	959

## 24 Administrationstools 961

---

<b>24.1 Was kann dies und jenes noch?</b>	961
24.1.1 Der Rsync-Daemon	961
24.1.2 Wenn's mal wieder später wird: »screen«	963
24.1.3 Anklopfen mit »nmap«	963
24.1.4 Netzwerkinspektion: »netstat«	967
24.1.5 Zugreifende Prozesse finden: »lsof«	969
24.1.6 Was macht mein System? »top«!	973
24.1.7 Wenn gar nichts mehr geht – Debugging mit »strace«	977
24.1.8 Prüfung der Erreichbarkeit mit »my traceroute«	982
24.1.9 Subnetzberechnung mit »ipcalc«	983
<b>24.2 Aus der Ferne – Remote-Administrationstools</b>	984
24.2.1 PuTTY	985
24.2.2 WinSCP	988
24.2.3 Synergy	989
24.2.4 Eine für immer: »mosh«	991

## 25 Versionskontrolle 993

---

<b>25.1 Philosophien</b>	994
25.1.1 Lokal	994
25.1.2 Zentral	995
25.1.3 Dezentral	996
<b>25.2 Versionskontrollsysteme</b>	997
25.2.1 CVS	997
25.2.2 Apache Subversion	1000
25.2.3 GNU Bazaar	1002
25.2.4 Mercurial	1004
25.2.5 Git	1006
<b>25.3 Kommandos</b>	1009
<b>25.4 Serverdienste</b>	1010
25.4.1 Git-Server mit Gitolite	1010
25.4.2 Git-Server mit Gitea	1014

## TEIL VI Automatisierung

### 26 Scripting 1019

---

<b>26.1</b>	<b>Aufgebohrte Muscheln</b>	1019
<b>26.2</b>	<b>Vom Suchen und Finden: ein kurzer Überblick</b>	1020
26.2.1	Die Detektive: »grep«, »sed« und »awk«	1020
26.2.2	Reguläre Ausdrücke verstehen und anwenden	1021
<b>26.3</b>	<b>Fortgeschrittene Shell-Programmierung</b>	1024
26.3.1	Expansionsschemata	1024
26.3.2	Umgebungsvariablen	1028
26.3.3	»Back to bash«: ein tieferer Blick in die Muschel	1029
26.3.4	Logging in Skripten	1034
<b>26.4</b>	<b>Tipps und Tricks aus der Praxis</b>	1037
26.4.1	Aufräumkommando	1037
26.4.2	IFS	1038
26.4.3	Datumsmagie	1038
26.4.4	E-Mails aus einem Skript versenden	1039
26.4.5	Interaktive Programme steuern	1039

### 27 Ansible 1041

---

<b>27.1</b>	<b>Einführung, Überblick und Installation</b>	1041
27.1.1	Geschichte und Versionen	1041
27.1.2	Was bedeutet »Ansible«?	1041
27.1.3	Merkmale	1042
27.1.4	Beispielszenario	1042
27.1.5	Installation auf dem Control Host	1043
27.1.6	Installation auf den Target Hosts	1045
27.1.7	Einrichten der SSH-Public-Key-Authentifizierung	1046
27.1.8	Ein Ad-hoc-Test ohne jegliche Konfiguration	1046
27.1.9	Noch ein Hinweis zur Migration von älteren Versionen	1047
<b>27.2</b>	<b>Basiseinrichtung und Ad-hoc-Kommandos</b>	1047
27.2.1	Verzeichnisstruktur einrichten	1047
27.2.2	Grundkonfiguration (ansible.cfg)	1048
27.2.3	Erstellen und Verwalten eines Inventorys	1050
27.2.4	Ad-hoc-Kommandos	1053

27.2.5	Patterns zum Adressieren von Hosts .....	1054
27.2.6	Die Ansible-Konsole .....	1055
27.2.7	Idempotenz .....	1055
27.2.8	Parallele Ausführung .....	1056
27.2.9	»Hängende« Verbindungen .....	1056
27.2.10	Exkurs: Versionskontrolle mit Git .....	1057
<b>27.3</b>	<b>Die Konfigurations- und Serialisierungssprache YAML .....</b>	<b>1058</b>
27.3.1	YAML-Files editieren .....	1059
27.3.2	Listen und Hashes .....	1060
27.3.3	Verschachtelte Strukturen .....	1060
27.3.4	Block-Ausdrücke .....	1062
<b>27.4</b>	<b>Playbooks .....</b>	<b>1063</b>
27.4.1	Playbooks, Tasks und Plays .....	1063
27.4.2	Das Kommando ansible-playbook .....	1067
27.4.3	Tags .....	1068
27.4.4	Variablen .....	1069
27.4.5	Facts und implizite Variablen .....	1075
27.4.6	Jinja2 und Templates .....	1079
27.4.7	Bedingte Ausführung .....	1082
27.4.8	Schleifen .....	1082
27.4.9	Das Verhalten von command und shell .....	1086
27.4.10	Fehlerbehandlung und Retry-Files .....	1086
27.4.11	Blocks (und noch mal Fehlerbehandlung) .....	1088
27.4.12	Die Vault .....	1089
27.4.13	Handler .....	1091
27.4.14	Asynchrone Ausführung .....	1093
27.4.15	Lokale Tasks .....	1094
27.4.16	Hosts in einer definierten Reihenfolge abarbeiten .....	1095
27.4.17	Dynamische Gruppen .....	1096
27.4.18	Lookups .....	1098
27.4.19	Logging und no_log .....	1099
27.4.20	Die Kuh spricht: cowsay .....	1100
<b>27.5</b>	<b>Die Modul-Bibliothek .....</b>	<b>1101</b>
27.5.1	Module zur Kommandoausführung .....	1101
27.5.2	Module zur Paketverwaltung .....	1102
27.5.3	Module zur Verwaltung von Dateien und Dateiinhalten .....	1102
27.5.4	Module für weitere typische Verwaltungsaufgaben .....	1105
27.5.5	Spezialmodule (Kontrollflusssteuerung etc.) .....	1106



<b>27.6</b>	<b>Modularisierung von Playbooks mit Rollen oder Includes</b>	1107
27.6.1	Erstellung und Verwendung von Rollen	1107
27.6.2	Ansible Galaxy	1111
27.6.3	Verwendung von Imports/Includes	1112
<b>27.7</b>	<b>Webinterfaces</b>	1113
27.7.1	Ansible Tower / AWX	1113
27.7.2	Ansible Configuration Management Database (ansible-cmdb)	1115
27.7.3	Ansible Run Analysis (ARA)	1115
27.7.4	nci ansible ui	1116
<b>27.8</b>	<b>Was könnte noch besser sein bzw. was fehlt noch?</b>	1118
27.8.1	Skip/End auf Rollenebene	1118
27.8.2	Locking bei konkurrierenden Playbook-Aufrufen	1119
27.8.3	Schleifen über Blöcke	1120
27.8.4	Konfigurierbarer Logging-Output	1121
27.8.5	Standardisierte Vorgaben für die Rollen-Dokumentation	1121
27.8.6	Fazit	1123

## **28 Monitoring – wissen, was läuft** 1125

---

<b>28.1</b>	<b>Monitoring mit Naemon</b>	1127
28.1.1	Allgemeine Konfiguration	1128
28.1.2	Konfiguration der Objekte	1129
28.1.3	Eigene Hosts und Services konfigurieren	1138
28.1.4	Benachrichtigungen	1140
28.1.5	NRPE – Partitionsfüllstand und andere lokale Werte remote überprüfen	1142
<b>28.2</b>	<b>Monitoring mit Munin</b>	1145
<b>28.3</b>	<b>Fazit</b>	1147

## **TEIL VII Sicherheit, Verschlüsselung und Zertifikate**

### **29 Sicherheit** 1151

---

<b>29.1</b>	<b>Weniger ist mehr</b>	1152
<b>29.2</b>	<b>»chroot«</b>	1153
29.2.1	Dienste	1153

<b>29.3</b>	<b>Selbstabsicherung: »AppArmor«</b>	1155
29.3.1	Status und Betriebsarten	1156
29.3.2	Eigene Profile erstellen	1158
<b>29.4</b>	<b>Gotcha! Intrusion-Detection-Systeme</b>	1161
29.4.1	»snort« und Co.	1162
<b>29.5</b>	<b>Installation und Konfiguration</b>	1164
29.5.1	Vorbereitungen	1164
29.5.2	Kompilieren und installieren	1165
29.5.3	Basiskonfiguration	1167
29.5.4	Ein erster Test: »ICMP«	1168
29.5.5	Start-Skript erstellen: »systemd«	1169
<b>29.6</b>	<b>Performante Log-Speicherung mit »Barnyard2« und »MySQL«</b>	1170
29.6.1	Vorbereitungen	1170
29.6.2	Kompilieren und installieren	1171
29.6.3	Einbinden in Snort	1172
<b>29.7</b>	<b>Das Neueste vom Neuen: »pulledpork«</b>	1175
<b>29.8</b>	<b>Klein, aber oho: »fail2ban«</b>	1177
29.8.1	Konfiguration	1177
29.8.2	Aktive Sperrungen	1180
29.8.3	Reguläre Ausdrücke	1182
<b>29.9</b>	<b>OpenVPN</b>	1183
29.9.1	Serverinstallation – OpenVPN, PKI und Co.	1184
29.9.2	CentOS/openSUSE Leap: »easy-rsa«	1190
29.9.3	Gemeinsam weiter	1193
29.9.4	Roadwarrior	1194
29.9.5	Start-Skript?	1197
29.9.6	Site-to-site	1201
29.9.7	Simple-HA	1203
29.9.8	Tipps und Tricks	1204

## **30 Verschlüsselung und Zertifikate** 1211

---

<b>30.1</b>	<b>Definition und Historie</b>	1211
<b>30.2</b>	<b>Moderne Kryptologie</b>	1213
30.2.1	Symmetrische Verschlüsselung	1213
30.2.2	Asymmetrische Verschlüsselung	1214

<b>30.3</b>	<b>Den Durchblick behalten</b>	1215
30.3.1	Das Grundproblem	1215
30.3.2	Verwendungszwecke	1216
30.3.3	Umsetzung mithilfe einer PKI	1216
30.3.4	X.509	1217
30.3.5	Ein anderer Ansatz: PGP (Web-of-Trust)	1219
<b>30.4</b>	<b>Einmal mit allem und kostenlos bitte: »Let's Encrypt«</b>	1220
30.4.1	Wie funktioniert das?	1220
30.4.2	Einschränkungen	1221
30.4.3	Der Client »certbot«	1221
<b>30.5</b>	<b>In der Praxis</b>	1223
30.5.1	Einrichtung einer PKI mit Server- und E-Mail-Zertifikaten	1223
30.5.2	E-Mail-Verschlüsselung	1234
<b>30.6</b>	<b>Neben der Kommunikation – Dateiverschlüsselung</b>	1241
30.6.1	Dateien	1241
30.6.2	Devices	1242
30.6.3	Festplatten/System	1244
<b>30.7</b>	<b>Rechtliches</b>	1249
30.7.1	Fortgeschrittene elektronische Signatur	1249
30.7.2	Qualifiziertes Zertifikat	1250
30.7.3	Qualifizierte elektronische Signatur	1250
30.7.4	Sichere Signaturerstellungseinheit (SSEE)	1250
Die Autoren		1253
Index		1255