

# Auf einen Blick

## TEIL I

Grundlagen ..... 71

## TEIL II

Aufgaben ..... 203

## TEIL III

Dienste ..... 273

## TEIL IV

Infrastruktur ..... 745

## TEIL V

Kommunikation ..... 879

## TEIL VI

Automatisierung ..... 1043

## TEIL VII

Sicherheit, Verschlüsselung und Zertifikate ..... 1189

# Inhalt

Vorwort .....	33
Über dieses Buch .....	45

## **1 Der Administrator** 49

---

<b>1.1 Der Beruf des Systemadministrators</b> .....	49
1.1.1 Berufsbezeichnung und Aufgaben .....	49
1.1.2 Job-Definitionen .....	50
1.1.3 Definitionen der Management-Level .....	55
<b>1.2 Nützliche Fähigkeiten und Fertigkeiten</b> .....	56
1.2.1 Soziale Fähigkeiten .....	57
1.2.2 Arbeitstechniken .....	57
<b>1.3 Das Verhältnis des Administrators zu Normalsterblichen</b> .....	59
1.3.1 Der Chef und andere Vorgesetzte .....	59
1.3.2 Benutzer .....	60
1.3.3 Andere Administratoren .....	60
<b>1.4 Unterbrechungsgesteuertes Arbeiten</b> .....	61
<b>1.5 Einordnung der Systemadministration</b> .....	62
1.5.1 Arbeitsgebiete .....	62
1.5.2 DevOps .....	65
<b>1.6 Ethischer Verhaltenskodex</b> .....	66
<b>1.7 Administration – eine Lebenseinstellung?</b> .....	68

## **TEIL I Grundlagen**

## **2 Bootvorgang** 73

---

<b>2.1 Einführung</b> .....	73
<b>2.2 Der Bootloader GRUB 2</b> .....	73
2.2.1 Funktionsweise .....	73
2.2.2 Installation .....	74
2.2.3 Konfiguration .....	74

<b>2.3</b>	<b>Bootloader Recovery</b> .....	80
<b>2.4</b>	<b>Der Kernel und die initrd</b> .....	81
2.4.1	initrd erstellen und modifizieren .....	82
2.4.2	initrd manuell modifizieren .....	86
<b>2.5</b>	<b>systemd</b> .....	87
2.5.1	Begrifflichkeiten .....	88
2.5.2	Kontrollieren von Diensten .....	89
2.5.3	Aktivieren und Deaktivieren von Diensten .....	91
2.5.4	Erstellen und Aktivieren eigener Service Units .....	92
2.5.5	Target Units .....	94
2.5.6	»systemd«- und Servicekonfigurationen .....	95
2.5.7	Anzeige von Dienstabhängigkeiten .....	97
2.5.8	Logs mit journald .....	98
2.5.9	Abschlussbemerkung .....	100
<b>3</b>	<b>Festplatten und andere Devices</b> .....	101
<b>3.1</b>	<b>RAID</b> .....	101
3.1.1	RAID-0 .....	102
3.1.2	RAID-1 .....	102
3.1.3	RAID-5 .....	102
3.1.4	RAID-6 .....	103
3.1.5	RAID-10 .....	103
3.1.6	Zusammenfassung .....	104
3.1.7	Weich, aber gut: Software-RAID .....	105
3.1.8	Software-RAID unter Linux .....	106
3.1.9	Abschlussbemerkung zu RAIDs .....	113
<b>3.2</b>	<b>Rein logisch: Logical Volume Manager (LVM)</b> .....	114
3.2.1	Grundlagen und Begriffe .....	116
3.2.2	Setup .....	117
3.2.3	Aufbau einer Volume Group mit einem Volume .....	118
3.2.4	Erweiterung eines Volumens .....	121
3.2.5	Eine Volume Group erweitern .....	121
3.2.6	Spiegelung zu einem Volume hinzufügen .....	123
3.2.7	Eine defekte Festplatte ersetzen .....	124
3.2.8	Backups mit Snapshots .....	125
3.2.9	Mirroring ausführlich .....	129

3.2.10	Thin Provisioning .....	133
3.2.11	Kommandos .....	136
<b>3.3</b>	<b>udev</b> .....	137
3.3.1	udev-Regeln .....	138
3.3.2	Eigene Regeln schreiben .....	138
<b>3.4</b>	<b>Alles virtuell? »/proc«</b> .....	141
3.4.1	CPU .....	141
3.4.2	RAM .....	143
3.4.3	Kernelkonfiguration .....	144
3.4.4	Kernelparameter .....	144
3.4.5	Gemountete Dateisysteme .....	145
3.4.6	Prozessinformationen .....	145
3.4.7	Netzwerk .....	147
3.4.8	Änderungen dauerhaft speichern .....	147
3.4.9	Abschlussbemerkung .....	148
<b>4</b>	<b>Dateisysteme</b> .....	149
<b>4.1</b>	<b>Dateisysteme: von Bäumen, Journalen und einer Kuh</b> .....	149
4.1.1	Bäume .....	150
4.1.2	Journalen .....	152
4.1.3	Und die Kühe? COW-fähige Dateisysteme .....	152
<b>4.2</b>	<b>Praxis</b> .....	153
4.2.1	Ext2/3-FS aufgebohrt: mke2fs, tune2fs, dumpe2fs, e2label .....	153
4.2.2	ReiserFS und seine Tools .....	156
4.2.3	XFS .....	157
4.2.4	Das Dateisystem vergrößern oder verkleinern .....	158
4.2.5	Btrfs .....	159
<b>4.3</b>	<b>Fazit</b> .....	166
<b>5</b>	<b>Berechtigungen</b> .....	167
<b>5.1</b>	<b>User, Gruppen und Dateisystemstrukturen</b> .....	167
<b>5.2</b>	<b>Dateisystemberechtigungen</b> .....	170
5.2.1	Spezialbits .....	171

<b>5.3</b>	<b>Erweiterte POSIX-ACLs</b> .....	174
5.3.1	Setzen und Anzeigen von einfachen ACLs .....	175
5.3.2	Setzen von Default-ACLs .....	177
5.3.3	Setzen von erweiterten ACLs .....	179
5.3.4	Entfernen von ACLs .....	181
5.3.5	Sichern und Zurückspielen von ACLs .....	182
<b>5.4</b>	<b>Erweiterte Dateisystemattribute</b> .....	183
5.4.1	Attribute, die jeder Benutzer ändern kann .....	183
5.4.2	Attribute, die nur »root« ändern kann .....	184
5.4.3	Weitere Attribute .....	185
<b>5.5</b>	<b>Quotas</b> .....	185
5.5.1	Installation und Aktivierung der Quotas .....	186
5.5.2	Journaling-Quotas .....	187
5.5.3	Quota-Einträge verwalten .....	188
<b>5.6</b>	<b>Pluggable Authentication Modules (PAM)</b> .....	192
5.6.1	Verschiedene PAM-Typen .....	193
5.6.2	Die PAM-Kontrollflags .....	193
5.6.3	Argumente zu den Modulen .....	194
5.6.4	Modulpfade .....	194
5.6.5	Module und ihre Aufgaben .....	195
5.6.6	Die neuere Syntax bei der PAM-Konfiguration .....	196
<b>5.7</b>	<b>Konfiguration von PAM</b> .....	198
<b>5.8</b>	<b>ulimit</b> .....	199
5.8.1	Setzen der ulimit-Werte .....	200
<b>5.9</b>	<b>Abschlussbemerkung</b> .....	201

## TEIL II Aufgaben

### **6 Paketmanagement** 205

---

<b>6.1</b>	<b>Paketverwaltung</b> .....	205
6.1.1	rpm oder deb? .....	206
6.1.2	yum, yast, zypper oder apt? .....	208
6.1.3	Außerirdische an Bord – alien .....	210

<b>6.2</b>	<b>Pakete im Eigenbau</b>	211
6.2.1	Vorbereitungen	211
6.2.2	Am Anfang war das Makefile	212
6.2.3	Vom Fellknäuel zum Paket	215
6.2.4	Patchen mit patch und diff	218
6.2.5	Updates sicher konfigurieren	220
<b>6.3</b>	<b>Updates nur einmal laden: Cache</b>	223
6.3.1	deb-basierte Distributionen: apt-cacher-ng	223
6.3.2	Installation	223
6.3.3	Konfiguration	223
6.3.4	Clientkonfiguration	225
6.3.5	Fütterungszeit – bereits geladene Pakete dem Cache hinzufügen	225
6.3.6	Details: Report-HTML	226
6.3.7	rpm-basierte Distributionen	227
<b>6.4</b>	<b>Alles meins: Mirror</b>	227
6.4.1	deb-basierte Distributionen: debmirror	227
6.4.2	Konfiguration	227
6.4.3	Benutzer und Gruppe anlegen	228
6.4.4	Verzeichnisstruktur anlegen	228
6.4.5	Mirror-Skript erstellen (Ubuntu)	228
6.4.6	Cronjobs einrichten	231
6.4.7	Schlüssel importieren	232
6.4.8	Mirror erstellen	232
6.4.9	Mirror verfügbar machen – Webdienst konfigurieren	232
6.4.10	Clientkonfiguration	233
6.4.11	rpm-basierte Distributionen	234
6.4.12	Benutzer und Gruppe anlegen	234
6.4.13	Verzeichnisstruktur anlegen: openSUSE Leap	235
6.4.14	Verzeichnisstruktur anlegen: CentOS	235
6.4.15	Mirror-Skript erstellen	235
6.4.16	Cronjobs einrichten	236
6.4.17	Mirror erstellen	237
6.4.18	Mirror verfügbar machen – Webdienst konfigurieren	238
6.4.19	Clientkonfiguration: openSUSE Leap	239
6.4.20	Clientkonfiguration: CentOS	239

<b>7</b>	<b>Backup und Recovery</b>	241
<b>7.1</b>	<b>Backup gleich Disaster Recovery?</b>	241
<b>7.2</b>	<b>Backupstrategien</b>	242
<b>7.3</b>	<b>Datensicherung mit tar</b>	245
7.3.1	Weitere interessante Optionen für GNU-tar	246
7.3.2	Sicherung über das Netzwerk mit tar und ssh	247
<b>7.4</b>	<b>Datensynchronisation mit rsync</b>	248
7.4.1	Lokale Datensicherung mit rsync	248
7.4.2	Synchronisieren im Netzwerk mit rsync	249
7.4.3	Wichtige Optionen für rsync	249
7.4.4	Backupskript für die Sicherung auf einen Wechseldatenträger	251
7.4.5	Backupskript für die Sicherung auf einen Backupserver	252
7.4.6	Verwendung von ssh für die Absicherung von rsync	254
<b>7.5</b>	<b>Imagesicherung mit dd</b>	255
7.5.1	Sichern des Master Boot Records (MBR)	255
7.5.2	Partitionstabelle mithilfe von dd zurückspielen	256
7.5.3	Images mit dd erstellen	256
7.5.4	Einzelne Dateien mit dd aus einem Image zurückspielen	257
7.5.5	Abschlussbemerkung zu dd	259
<b>7.6</b>	<b>Disaster Recovery mit ReaR</b>	259
7.6.1	ReaR installieren	261
7.6.2	ReaR konfigurieren	261
7.6.3	Aufrufparameter von ReaR	263
7.6.4	Der erste Testlauf	264
7.6.5	Der Recovery-Prozess	268
7.6.6	Die ReaR-Konfiguration im Detail	270
7.6.7	Migrationen mit ReaR	271

## TEIL III Dienste

<b>8</b>	<b>Webserver</b>	275
<b>8.1</b>	<b>Apache</b>	275
8.1.1	Installation	275
8.1.2	Virtuelle Hosts einrichten	276

---

8.1.3	Debian/Ubuntu: Virtuelle Hosts aktivieren .....	279
8.1.4	HTTPS konfigurieren .....	280
8.1.5	Benutzer-Authentifizierung mit Kerberos .....	284
8.1.6	Apache-Server mit ModSecurity schützen .....	285
8.1.7	Tuning und Monitoring .....	290
<b>8.2</b>	<b>nginx</b> .....	295
8.2.1	Installation .....	295
8.2.2	Grundlegende Konfiguration .....	295
8.2.3	Virtuelle Hosts .....	296
8.2.4	HTTPS mit nginx .....	298
<b>8.3</b>	<b>Logfiles auswerten</b> .....	299
<b>9</b>	<b>FTP-Server</b> .....	303

---

<b>9.1</b>	<b>Einstieg</b> .....	303
9.1.1	Das File Transfer Protocol .....	303
9.1.2	vsftpd .....	304
<b>9.2</b>	<b>Download-Server</b> .....	304
<b>9.3</b>	<b>Zugriff von Usern auf ihre Homeverzeichnisse</b> .....	306
<b>9.4</b>	<b>FTP über SSL (FTPS)</b> .....	307
<b>9.5</b>	<b>Anbindung an LDAP</b> .....	309
<b>10</b>	<b>Mailserver</b> .....	311

---

<b>10.1</b>	<b>Postfix</b> .....	311
10.1.1	Installation der Postfix-Pakete .....	312
10.1.2	Grundlegende Konfiguration .....	312
10.1.3	Postfix als Relay vor Exchange, Dovecot oder anderen Backends .....	315
10.1.4	Die Postfix-Restrictions: Der Schlüssel zu Postfix .....	317
10.1.5	Weiterleitungen und Aliasse für Mailadressen .....	326
10.1.6	SASL/SMTP-Auth .....	327
10.1.7	SSL/TLS für Postfix einrichten .....	329
<b>10.2</b>	<b>POP3/IMAP-Server mit Dovecot</b> .....	331
10.2.1	Installation der Dovecot-Pakete .....	331
10.2.2	Vorbereitungen im Linux-System .....	332



10.2.3	Log-Meldungen und Debugging .....	333
10.2.4	User-Authentifizierung .....	334
10.2.5	Aktivierung des LMTP-Servers von Dovecot .....	335
10.2.6	Einrichten von SSL/TLS-Verschlüsselung .....	336
10.2.7	Der Ernstfall: Der IMAP-Server erwacht zum Leben .....	337
10.2.8	Dovecot im Replikations-Cluster .....	339
10.2.9	Einrichtung der Replikation .....	340
10.2.10	Hochverfügbare Service-IP .....	343
<b>10.3</b>	<b>Anti-Spam/Anti-Virus mit Rspamd .....</b>	<b>344</b>
10.3.1	Mails ablehnen oder in die Quarantäne filtern? .....	345
10.3.2	Installation von Rspamd, ClamAV und Redis .....	346
10.3.3	Update der Virensignaturen und Start der Dienste .....	347
10.3.4	Die Architektur von Rspamd .....	348
10.3.5	Einbindung von Rspamd an Ihren Postfix-Mailserver .....	349
10.3.6	Konfiguration des Rspamd .....	351
10.3.7	Konfiguration von Upstream-Quellen .....	353
10.3.8	Redis als schnelle Datenbank an der Seite von Rspamd .....	354
10.3.9	Die Definition auszulösender Aktionen .....	355
10.3.10	Statistik und Auswertung im Webinterface .....	356
10.3.11	ClamAV in Rspamd einbinden .....	357
10.3.12	Späteres Filtern über Mail-Header .....	359
10.3.13	RBLs in Rspamd .....	360
10.3.14	Bayes in Rspamd .....	361
10.3.15	Eigene White- und Blacklists führen .....	362
10.3.16	Einrichtung von DKIM zur Mailsignierung .....	364
10.3.17	Ausblick: Einbindung weiterer Prüfungsmethoden .....	367
<b>10.4</b>	<b>Monitoring und Logfile-Auswertung .....</b>	<b>367</b>
<b>11</b>	<b>Datenbank .....</b>	<b>369</b>
<hr/>		
<b>11.1</b>	<b>MariaDB in der Praxis .....</b>	<b>369</b>
11.1.1	Installation und grundlegende Einrichtung .....	369
11.1.2	Replikation .....	371
11.1.3	Master-Master-Replikation .....	379
<b>11.2</b>	<b>Tuning .....</b>	<b>382</b>
11.2.1	Tuning des Speichers .....	383
11.2.2	Tuning von Indizes .....	389

<b>11.3 Backup und Point-In-Time-Recovery</b> .....	393
11.3.1 Restore zum letztmöglichen Zeitpunkt .....	393
11.3.2 Restore zu einem bestimmten Zeitpunkt .....	394

---

## **12 Syslog** .....

---

<b>12.1 Der Aufbau von Syslog-Nachrichten</b> .....	397
<b>12.2 systemd mit journalctl</b> .....	399
12.2.1 Erste Schritte mit dem journalctl-Kommando .....	401
12.2.2 Filtern nach Zeit .....	402
12.2.3 Filtern nach Diensten .....	403
12.2.4 Kernelmeldungen .....	405
12.2.5 Einrichten eines Log-Hosts .....	405
<b>12.3 Der Klassiker: Syslogd</b> .....	409
<b>12.4 Syslog-ng</b> .....	410
12.4.1 Der »options«-Abschnitt .....	411
12.4.2 Das »source«-Objekt .....	413
12.4.3 Das »destination«-Objekt .....	413
12.4.4 Das »filter«-Objekt .....	415
12.4.5 Das »log«-Objekt .....	416
<b>12.5 Rsyslog</b> .....	417
12.5.1 Eigenschaftsbasierte Filter .....	417
12.5.2 Ausdrucksbasierte Filter .....	418
<b>12.6 Loggen über das Netz</b> .....	419
12.6.1 SyslogD .....	419
12.6.2 Syslog-ng .....	420
12.6.3 Rsyslog .....	420
<b>12.7 Syslog in eine Datenbank schreiben</b> .....	421
12.7.1 Anlegen der Log-Datenbank .....	421
12.7.2 In die Datenbank loggen .....	422
<b>12.8 Fazit</b> .....	424

---

## **13 Proxy-Server** .....

---

<b>13.1 Einführung des Stellvertreters</b> .....	425
--	-----

<b>13.2</b>	<b>Proxys in Zeiten des Breitbandinternets</b> .....	426
<b>13.3</b>	<b>Herangehensweisen und Vorüberlegungen</b> .....	427
<b>13.4</b>	<b>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</b>	<b>Authentifizierung</b> .....	440
13.5.1	Benutzerbasiert .....	443
13.5.2	Gruppenbasiert .....	452
<b>13.6</b>	<b>Log-Auswertung: Calamaris und Sarg</b> .....	455
13.6.1	Calamaris .....	455
13.6.2	Sarg .....	457
<b>13.7</b>	<b>Unsichtbar: »transparent proxy«</b> .....	458
<b>13.8</b>	<b>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</b>	<b>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: always_direct .....	465
<b>13.10</b>	<b>Cache-Konfiguration</b> .....	466
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 Kerberos</b>	471
<b>14.1 Begriffe im Zusammenhang mit Kerberos</b>	472
<b>14.2 Die Funktionsweise von Kerberos</b>	472
<b>14.3 Installation und Konfiguration des Kerberos-Servers</b>	473
14.3.1 Starten und Stoppen der Dienste	474
14.3.2 Konfiguration der Datei »/etc/krb5.conf«	475
14.3.3 Konfiguration der Datei »kdc.conf«	477
<b>14.4 Initialisierung und Testen des Kerberos-Servers</b>	481
14.4.1 Verwalten der Principals	483
<b>14.5 Kerberos und PAM</b>	487
14.5.1 Konfiguration der PAM-Dateien auf einem openSUSE-System	488
14.5.2 Testen der Anmeldung	489
<b>14.6 Neue Benutzer mit Kerberos-Principal anlegen</b>	489
<b>14.7 Hosts und Dienste</b>	490
14.7.1 Einträge entfernen	493
<b>14.8 Konfiguration des Kerberos-Clients</b>	494
14.8.1 PAM und Kerberos auf dem Client	496
<b>14.9 Replikation des Kerberos-Servers</b>	496
14.9.1 Bekanntmachung aller KDCs im Netz	496
14.9.2 Konfiguration des KDC-Masters	500
14.9.3 Konfiguration des KDC-Slaves	502
14.9.4 Replikation des KDC-Masters auf den KDC-Slave	502
<b>14.10 Kerberos-Policys</b>	505
<b>14.11 Kerberos in LDAP einbinden</b>	507
14.11.1 Konfiguration des LDAP-Servers	508
14.11.2 Zurücksichern der alten Datenbank	518
14.11.3 Erstellung der Service-Keys in der Standard-»keytab«-Datei	521
14.11.4 Erstellung der Service Keys in einer eigenen Datei	523
14.11.5 Bestehende LDAP-Benutzer um Kerberos-Principal erweitern	524
<b>14.12 Neue Benutzer im LDAP-Baum</b>	529
<b>14.13 Authentifizierung am LDAP-Server über »GSSAPI«</b>	530
14.13.1 Authentifizierung einrichten	530
14.13.2 Den zweiten KDC an den LDAP-Server anbinden	535
<b>14.14 Konfiguration des LAM Pro</b>	536

---

<b>15</b>	<b>Samba 4</b>	539
<b>15.1</b>	<b>Vorüberlegungen</b>	539
15.1.1	Installation der Pakete unter Ubuntu und Debian	541
<b>15.2</b>	<b>Konfiguration von Samba 4 als Domaincontroller</b>	542
15.2.1	Das Provisioning	544
15.2.2	Konfiguration des Bind9	545
<b>15.3</b>	<b>Testen des Domaincontrollers</b>	551
15.3.1	Testen des DNS-Servers	552
15.3.2	Test des Verbindungsaufbaus	553
15.3.3	Einrichtung des Zeitserver	555
<b>15.4</b>	<b>Benutzer- und Gruppenverwaltung</b>	556
<b>15.5</b>	<b>Benutzer- und Gruppenverwaltung über die Kommandozeile</b>	557
15.5.1	Verwaltung von Gruppen über die Kommandozeile	557
15.5.2	Verwaltung von Benutzern über die Kommandozeile	562
15.5.3	Setzen der Passworrichtlinien	566
15.5.4	Passworrichtlinien mi Password Settings Objects (PSO)	567
<b>15.6</b>	<b>Die Remote Server Administration Tools (RSAT)</b>	568
15.6.1	Die RSAT einrichten	568
15.6.2	Beitritt eines Windows-Clients zur Domäne	569
15.6.3	Einrichten der RSAT	570
15.6.4	Benutzer- und Gruppenverwaltung mit den RSAT	570
<b>15.7</b>	<b>Gruppenrichtlinien</b>	571
15.7.1	Verwaltung der GPOs mit den RSAT	572
15.7.2	Erste Schritte mit der Gruppenrichtlinienverwaltung	572
15.7.3	Eine Gruppenrichtlinie erstellen	574
15.7.4	Die Gruppenrichtlinie mit einer OU verknüpfen	577
15.7.5	GPOs über die Kommandozeile	580
<b>15.8</b>	<b>Linux-Clients in der Domäne</b>	582
15.8.1	Bereitstellen von Freigaben	588
15.8.2	Mounten über »pam_mount«	589
15.8.3	Umstellen des grafischen Logins	592
<b>15.9</b>	<b>Zusätzliche Server in der Domäne</b>	592
15.9.1	Einen Fileserver einrichten	592
15.9.2	Ein zusätzlicher Domaincontroller	597
15.9.3	Konfiguration des zweiten DC	598
15.9.4	Einrichten des Nameservers	598

15.9.5	Testen der Replikation .....	602
15.9.6	Weitere Tests .....	604
15.9.7	Einrichten des Zeitserverns .....	604
<b>15.10</b>	<b>Die Replikation der Freigabe »sysvol« einrichten .....</b>	<b>605</b>
15.10.1	Einrichten des rsync-Servers .....	605
15.10.2	Einrichten von rsync auf dem PDC-Master .....	606
<b>15.11</b>	<b>Was geht noch mit Samba 4? .....</b>	<b>609</b>
<b>16</b>	<b>NFS .....</b>	<b>611</b>
<hr/>		
<b>16.1</b>	<b>Unterschiede zwischen NFSv3 und NFSv4 .....</b>	<b>611</b>
<b>16.2</b>	<b>Funktionsweise von NFSv4 .....</b>	<b>612</b>
<b>16.3</b>	<b>Einrichten des NFSv4-Servers .....</b>	<b>613</b>
16.3.1	Konfiguration des Pseudodateisystems .....	613
16.3.2	Anpassen der Datei »/etc/exports« .....	614
16.3.3	Tests für den NFS-Server .....	616
<b>16.4</b>	<b>Konfiguration des NFSv4-Clients .....</b>	<b>618</b>
<b>16.5</b>	<b>Konfiguration des idmapd .....</b>	<b>619</b>
<b>16.6</b>	<b>Optimierung von NFSv4 .....</b>	<b>621</b>
16.6.1	Optimierung des NFSv4Servers .....	621
16.6.2	Optimierung des NFSv4-Clients .....	622
<b>16.7</b>	<b>NFSv4 und Firewalls .....</b>	<b>623</b>
<b>16.8</b>	<b>NFS und Kerberos .....</b>	<b>624</b>
16.8.1	Erstellung der Principals und der keytab-Dateien .....	624
16.8.2	Kerberos-Authentifizierung unter Debian und Ubuntu .....	626
16.8.3	Kerberos-Authentifizierung auf openSUSE und CentOS .....	626
16.8.4	Anpassen der Datei »/etc/exports« .....	626
16.8.5	Einen NFS-Client für Kerberos unter Debian und Ubuntu konfigurieren	627
16.8.6	Einen NFS-Client für Kerberos unter openSUSE und CentOS konfigurieren .....	627
16.8.7	Testen der durch Kerberos abgesicherten NFS-Verbindung .....	627
16.8.8	Testen der Verbindung .....	628

---

<b>17 LDAP</b>	631
<b>17.1 Einige Grundlagen zu LDAP</b>	632
17.1.1 Was ist ein Verzeichnisdienst?	632
17.1.2 Der Einsatz von LDAP im Netzwerk	633
17.1.3 Aufbau des LDAP-Datenmodells	633
17.1.4 Objekte	634
17.1.5 Attribute	635
17.1.6 Schema	635
17.1.7 Das LDIF-Format	638
<b>17.2 Zu den hier verwendeten Distributionen</b>	640
17.2.1 Die zwei Konfigurationsarten	640
17.2.2 Die Datenbank-Backends	641
17.2.3 Grundkonfiguration des LDAP-Servers (statisch)	642
17.2.4 Grundkonfiguration des LDAP-Servers (dynamisch)	644
<b>17.3 Absichern der Verbindung zum LDAP-Server über TLS</b>	650
17.3.1 Erstellen der Zertifizierungsstelle	651
17.3.2 Erstellen des Serverzertifikats	651
17.3.3 Signieren des Zertifikats	651
17.3.4 Zertifikate in die »slapd.conf« eintragen	652
17.3.5 Zertifikate in die dynamische Konfiguration eintragen	652
17.3.6 Konfiguration des LDAP-Clients	653
<b>17.4 Einrichtung des sssd</b>	654
17.4.1 Anlegen eines Testbenutzers	658
<b>17.5 Grafische Werkzeuge für die LDAP-Verwaltung</b>	660
<b>17.6 Änderungen mit ldapmodify</b>	661
17.6.1 Interaktive Änderung mit ldapmodify	662
17.6.2 Änderungen über eine LDIF-Datei mit ldapmodify	662
<b>17.7 Absichern des LDAP-Baums mit ACLs</b>	663
<b>17.8 Grundlegende ACLs in der statischen Konfiguration</b>	668
17.8.1 Eine eigene Datei für die ACLs einbinden	668
17.8.2 Erste ACLs zur Grundsicherung des DIT	669
<b>17.9 Grundlegende ACLs in der dynamischen Konfiguration</b>	671
<b>17.10 Der neue LDAP-Admin</b>	674
17.10.1 Anlegen der Objekte	674
17.10.2 ACLs für die statische Konfiguration	675
17.10.3 ACLs für die dynamische Konfiguration	675

<b>17.11 Absichern der Passwörter</b> .....	677
<b>17.12 ACLs mit regulären Ausdrücken</b> .....	679
17.12.1 ACLs vor dem Einsatz testen .....	686
<b>17.13 Filter zur Suche im LDAP-Baum</b> .....	688
17.13.1 Die Fähigkeiten des LDAP-Servers testen .....	688
17.13.2 Einfache Filter .....	690
17.13.3 Filter mit logischen Verknüpfungen .....	691
17.13.4 Einschränkung der Suchtiefe .....	691
<b>17.14 Verwendung von Overlays</b> .....	692
17.14.1 Overlays am Beispiel von dynlist .....	693
17.14.2 Weitere Overlays .....	697
<b>17.15 Replikation des DIT</b> .....	698
Vorbereitungen unabhängig von der Konfigurationsart .....	699
17.15.1 Replikation mit statischer Konfiguration .....	701
17.15.2 Replikation mit dynamischer Konfiguration .....	705
<b>17.16 Umstellung auf die dynamische Konfiguration</b> .....	711
17.16.1 Umstellung auf die dynamische Konfiguration am Provider .....	712
17.16.2 Umstellung auf die dynamische Konfiguration am Consumer .....	713
<b>17.17 Verwaltung von Weiterleitungen für den Mailserver Postfix</b> .....	714
<b>17.18 Benutzerauthentifizierung von Dovecot über LDAP</b> .....	717
<b>17.19 Benutzerauthentifizierung am Proxy Squid über LDAP</b> .....	720
17.19.1 Die Authentifizierung über LDAP aktivieren .....	720
17.19.2 Benutzerbezogene Authentifizierung .....	721
17.19.3 Gruppenbezogene Authentifizierung .....	722
<b>17.20 Benutzerauthentifizierung am Webserver Apache über LDAP</b> .....	723
17.20.1 Konfiguration der Cache-Parameter .....	724
17.20.2 Konfiguration der Zugriffsparameter .....	725
<b>17.21 Und was geht sonst noch alles mit LDAP?</b> .....	726

---

## 18 Druckserver 727

---

<b>18.1 Grundkonfiguration des Netzwerkzugriffs</b> .....	728
<b>18.2 Policys</b> .....	731
18.2.1 Location-Policys .....	732
18.2.2 Operation Policys .....	733



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

## TEIL IV Infrastruktur

### 19 Hochverfügbarkeit 747

---

<b>19.1</b>	<b>Das Beispiel-Setup .....</b>	<b>747</b>
<b>19.2</b>	<b>Installation .....</b>	<b>748</b>
19.2.1	Debian 10 und Ubuntu 20.04 LTS .....	748
19.2.2	CentOS Stream .....	748
19.2.3	openSUSE Leap .....	749
<b>19.3</b>	<b>Einfache Vorarbeiten .....</b>	<b>749</b>
<b>19.4</b>	<b>Shared Storage mit DRBD .....</b>	<b>749</b>
19.4.1	Grundlegende Konfiguration .....	750
19.4.2	Die wichtigsten Konfigurationsoptionen .....	751
19.4.3	Die DRBD-Ressource in Betrieb nehmen .....	752
<b>19.5</b>	<b>Grundkonfiguration der Clusterkomponenten .....</b>	<b>755</b>
19.5.1	Pacemaker und Corosync: das Benachrichtigungssystem .....	755
19.5.2	Pacemaker: der Ressourcenmanager .....	758
19.5.3	Quorum deaktivieren .....	760
<b>19.6</b>	<b>Dienste hochverfügbar machen .....</b>	<b>762</b>
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 .....	774

<b>20</b>	<b>Virtualisierung</b>	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: 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
<b>21</b>	<b>Docker</b>	805
<b>21.1</b>	<b>Einführung, Installation und wichtige Grundlagen</b>	805
21.1.1	Was ist Docker? Und was ist ein Container?	805
21.1.2	Docker: Entstehung und Geschichte	807
21.1.3	Funktionale Übersicht	808
21.1.4	Installation	808
21.1.5	Ergänzungen zur Installation, erster Systemtest	812
21.1.6	Etwas Terminologie	813
21.1.7	Konfigurationsmöglichkeiten des Docker-Daemons	814
21.1.8	Betrieb hinter einem Proxy	815
21.1.9	Image-Schichten und Storage Driver	816
<b>21.2</b>	<b>Management von Images und Containern</b>	820
21.2.1	Das Docker-CLI (Command Line Interface)	820
21.2.2	Erste Schritte	821
21.2.3	Löschen von Containern und Images	822
21.2.4	Handling von Containern	823

21.2.5	Prozessverwaltung .....	825
21.2.6	Restart Polycys und Live Restore .....	827
21.2.7	Umgebungsvariablen .....	827
21.2.8	(Zentralisiertes) Logging .....	828
21.2.9	Verteilung von Images über Dateiversand .....	829
21.2.10	Der Docker Hub .....	830
21.2.11	Image-Tags und Namenskonventionen .....	831
21.2.12	Informationen über Images gewinnen .....	832
21.2.13	Erstellen eigener Base-Images .....	833
21.2.14	Go-Templates .....	834
21.2.15	Container limitieren .....	835
21.2.16	Packungsdichte .....	838
21.2.17	Systeminformationen und Aufräumarbeiten .....	838
<b>21.3</b>	<b>Docker-Networking .....</b>	<b>838</b>
21.3.1	Grundlagen .....	838
21.3.2	User Defined Networks .....	840
21.3.3	Portmapping .....	841
21.3.4	»etc/hosts«-Einträge beim Containerstart .....	842
<b>21.4</b>	<b>Datenpersistenz .....</b>	<b>842</b>
21.4.1	Bind Mounts und Volumes .....	842
21.4.2	Weitere Möglichkeiten .....	845
21.4.3	Volumes identifizieren .....	846
<b>21.5</b>	<b>Erstellen eigener Images mit Dockerfiles .....</b>	<b>846</b>
21.5.1	Einfaches Committen von Anpassungen .....	846
21.5.2	Dockerfiles und »docker build«: Basics .....	847
21.5.3	Der Build-Cache und docker build --pull .....	849
21.5.4	Dangling Images .....	850
21.5.5	Fehler(-Suche) im Buildprozess .....	851
21.5.6	Die Dockerfile-Direktiven: Ein Überblick .....	852
21.5.7	Ein komplexeres Beispiel mit ENV, COPY und CMD .....	853
21.5.8	CMD und ENTRYPOINT, CMD vs. ENTRYPOINT .....	854
21.5.9	Verwendung eigener Entrypoint-Skripte .....	856
21.5.10	».dockerignore«-Files .....	857
21.5.11	Healthchecks .....	857
21.5.12	Multistage-Builds .....	859
21.5.13	Best Practices .....	860
<b>21.6</b>	<b>Multi-Container-Rollout mit Docker Compose .....</b>	<b>860</b>
21.6.1	Basics .....	861
21.6.2	Ein erstes Beispiel .....	862

21.6.3	Build and Run .....	863
21.6.4	Environment und Portmappings .....	864
21.6.5	Volumes in Compose .....	865
21.6.6	Flexible Compose-Konfigurationen durch Umgebungsvariablen .....	866
21.6.7	Autostart-Integration .....	867
<b>21.7</b>	<b>Betrieb einer eigenen Registry .....</b>	<b>868</b>
21.7.1	Basis-Setup ohne TLS und erster Test .....	869
21.7.2	Registry mit TLS .....	871
21.7.3	Registry-Authentifizierung .....	873
21.7.4	Suchen oder Löschen in der privaten Registry .....	875
21.7.5	Sonstiges / Ausblick .....	877
21.7.6	Der Docker Registry Manager .....	877

## TEIL V Kommunikation

### 22 Netzwerk 881

---

<b>22.1</b>	<b>Vorwort zu Predictable Network Interface Names .....</b>	<b>881</b>
<b>22.2</b>	<b>Netzwerkkonfiguration mit iproute2 .....</b>	<b>882</b>
22.2.1	Erste Schritte .....	882
22.2.2	Die Syntax von ip .....	885
22.2.3	Links ansehen und manipulieren: ip link .....	885
22.2.4	IP-Adressen ansehen und manipulieren: ip address .....	887
22.2.5	Manipulation von ARP-Einträgen: ip neighbour .....	891
<b>22.3</b>	<b>Routing mit ip .....</b>	<b>893</b>
22.3.1	Routing-Informationen anzeigen .....	893
22.3.2	Da geht noch mehr: »Advanced Routing« .....	895
22.3.3	Die vorhandenen Regeln ansehen .....	896
22.3.4	Eine neue Routing-Tabelle anlegen .....	897
22.3.5	Ändern der Policy Routing Database .....	897
22.3.6	Routing über mehrere Uplinks .....	899
22.3.7	Fazit bis hierher .....	904
<b>22.4</b>	<b>Bonding .....</b>	<b>904</b>
22.4.1	Bonding-Konfiguration .....	905
22.4.2	Bonding unter Debian .....	908
22.4.3	Bonding unter Ubuntu .....	908
22.4.4	Bonding unter CentOS .....	909
22.4.5	Bonding unter openSUSE Leap .....	910

<b>22.5</b>	<b>IPv6</b> .....	910
22.5.1	Die Vorteile von IPv6 .....	912
22.5.2	Notation von IPv6-Adressen .....	912
22.5.3	Die Netzmasken .....	913
22.5.4	Die verschiedenen IPv6-Adressarten .....	913
22.5.5	Es geht auch ohne ARP .....	915
22.5.6	Feste Header-Länge .....	916
22.5.7	IPv6 in der Praxis .....	918
<b>22.6</b>	<b>Firewalls mit netfilter und iptables</b> .....	919
22.6.1	Der Weg ist das Ziel – wie Pakete durch den Kernel laufen .....	920
22.6.2	Einführung in iptables .....	921
22.6.3	Regeln definieren .....	923
22.6.4	Die klassischen Targets .....	925
22.6.5	Ein erster Testlauf .....	925
22.6.6	Rein wie raus: Stateful Packet Inspection .....	926
22.6.7	Das erste Firewallskript .....	928
22.6.8	Externe Firewall .....	930
22.6.9	Logging .....	936
22.6.10	Network Address Translation und Masquerading .....	938
22.6.11	Weitere nützliche Module für iptables .....	939
22.6.12	Abschlussbemerkung .....	942
<b>22.7</b>	<b>DHCP</b> .....	942
22.7.1	Funktionsweise .....	942
22.7.2	Konfiguration .....	943
<b>22.8</b>	<b>DNS-Server</b> .....	946
22.8.1	Funktionsweise .....	946
22.8.2	Unterschied: rekursiv und autoritativ .....	948
22.8.3	Einträge im DNS: Resource Records .....	948
22.8.4	Die Grundkonfiguration .....	949
22.8.5	Zonendefinitionen .....	952
22.8.6	Die erste vollständige Zone .....	956
22.8.7	Die hint-Zone .....	958
22.8.8	Reverse Lookup .....	960
22.8.9	Slave-Server .....	961
22.8.10	DNS-Server und IPv6 .....	963
<b>22.9</b>	<b>Vertrauen schaffen mit DNSSEC</b> .....	965
22.9.1	Die Theorie: »Wie arbeitet DNSSEC?« .....	965
22.9.2	Anpassungen am Server .....	967
22.9.3	Schlüssel erzeugen .....	968

22.9.4	Schlüssel der Zone hinzufügen und die Zone signieren .....	969
22.9.5	Signierte Zone aktivieren .....	970
22.9.6	Signierung prüfen .....	971
22.9.7	Die Signierung veröffentlichen .....	973
22.9.8	Fazit .....	974
<b>22.10</b>	<b>Nachwort zum Thema Netzwerk .....</b>	<b>974</b>

---

## 23 OpenSSH 975

---

<b>23.1</b>	<b>Die SSH-Familie .....</b>	<b>975</b>
23.1.1	Die Clients: ssh, scp, sftp .....	976
23.1.2	Der Server: sshd .....	978
<b>23.2</b>	<b>Schlüssel statt Passwort .....</b>	<b>980</b>
23.2.1	Schlüssel erzeugen .....	980
23.2.2	Passwortloses Login .....	981
23.2.3	Der SSH-Agent merkt sich Passphrasen .....	982
<b>23.3</b>	<b>X11-Forwarding .....</b>	<b>983</b>
<b>23.4</b>	<b>Portweiterleitung und Tunneling .....</b>	<b>984</b>
23.4.1	SshFS: Entfernte Verzeichnisse lokal einbinden .....	985

---

## 24 Administrationstools 987

---

<b>24.1</b>	<b>Was kann dies und jenes noch? .....</b>	<b>987</b>
24.1.1	Der Rsync-Daemon .....	987
24.1.2	Wenn's mal wieder später wird: screen .....	989
24.1.3	Anklopfen mit nmap .....	989
24.1.4	Netzwerkinspektion: netstat .....	993
24.1.5	Zugreifende Prozesse finden: lsof .....	995
24.1.6	Was macht mein System? top .....	999
24.1.7	Wenn gar nichts mehr geht – Debugging mit strace .....	1003
24.1.8	Prüfung der Erreichbarkeit mit my traceroute .....	1008
24.1.9	Subnetzberechnung mit ipcalc .....	1009
<b>24.2</b>	<b>Aus der Ferne – Remote-Administrationstools .....</b>	<b>1010</b>
24.2.1	PuTTY .....	1011
24.2.2	WinSCP .....	1014

24.2.3	Synergy .....	1015
24.2.4	Eine für immer: mosh .....	1017

## 25 Versionskontrolle 1019

---

<b>25.1</b>	<b>Philosophien .....</b>	<b>1020</b>
25.1.1	Lokal .....	1020
25.1.2	Zentral .....	1021
25.1.3	Dezentral .....	1022
<b>25.2</b>	<b>Versionskontrollsysteme .....</b>	<b>1023</b>
25.2.1	CVS .....	1023
25.2.2	Apache Subversion .....	1026
25.2.3	GNU Bazaar .....	1028
25.2.4	Mercurial .....	1030
25.2.5	Git .....	1032
<b>25.3</b>	<b>Kommandos .....</b>	<b>1035</b>
<b>25.4</b>	<b>Serverdienste .....</b>	<b>1036</b>
25.4.1	Git-Server mit Gitolite .....	1036
25.4.2	Git-Server mit Gitea .....	1039

## TEIL VI Automatisierung

## 26 Scripting 1045

---

<b>26.1</b>	<b>Aufgebohrte Muscheln .....</b>	<b>1045</b>
<b>26.2</b>	<b>Vom Suchen und Finden: ein kurzer Überblick .....</b>	<b>1046</b>
26.2.1	Die Detektive: grep, sed und awk .....	1046
26.2.2	Reguläre Ausdrücke verstehen und anwenden .....	1047
<b>26.3</b>	<b>Fortgeschrittene Shell-Programmierung .....</b>	<b>1050</b>
26.3.1	Expansionsschemata .....	1050
26.3.2	Umgebungsvariablen .....	1054
26.3.3	»Back to bash«: ein tieferer Blick in die Muschel .....	1055
26.3.4	Logging in Skripten .....	1060
<b>26.4</b>	<b>Tipps und Tricks aus der Praxis .....</b>	<b>1063</b>
26.4.1	Aufräumkommando .....	1063
26.4.2	IFS .....	1064

26.4.3	Datumsmagie .....	1064
26.4.4	E-Mails aus einem Skript versenden .....	1065
26.4.5	Interaktive Programme steuern .....	1065

## **27 Ansible** 1067

---

<b>27.1</b>	<b>Einführung und Installation .....</b>	<b>1067</b>
27.1.1	Was ist Ansible? .....	1067
27.1.2	Beispielszenario/Laborumgebung .....	1069
27.1.3	Ansible-Installation auf dem Control Host .....	1070
27.1.4	Einrichten der SSH-Public-Key-Authentifizierung .....	1073
27.1.5	Ein Ad-hoc-Test ohne jegliche Konfiguration .....	1073
<b>27.2</b>	<b>Basiseinrichtung und erstes Inventory-Management .....</b>	<b>1075</b>
27.2.1	Verzeichnisstruktur einrichten .....	1075
27.2.2	Grundkonfiguration (ansible.cfg) .....	1076
27.2.3	Erstellen und Verwalten eines statischen Inventorys .....	1077
27.2.4	Inventory-Aliase .....	1079
27.2.5	Jenseits von Ping .....	1079
27.2.6	Alternative Inventorys .....	1082
<b>27.3</b>	<b>Ad-hoc-Kommandos und Patterns .....</b>	<b>1083</b>
27.3.1	Ad-hoc-Kommandos .....	1083
27.3.2	Use cases .....	1084
27.3.3	Idempotenz .....	1085
27.3.4	Interne Funktionsweise .....	1086
27.3.5	Die Ansible-Konsole .....	1088
27.3.6	Patterns zum Adressieren von Hosts .....	1088
<b>27.4</b>	<b>Die Konfigurations- und Serialisierungssprache YAML .....</b>	<b>1089</b>
27.4.1	Syntax und Struktur .....	1090
27.4.2	YAML-Files editieren .....	1090
27.4.3	Listen und Maps .....	1092
27.4.4	Verschachtelte Strukturen .....	1092
27.4.5	Block-Ausdrücke .....	1094
27.4.6	Das Nichts in YAML .....	1095
<b>27.5</b>	<b>Playbooks und Tasks: die Grundlagen .....</b>	<b>1095</b>
27.5.1	Hallo Ansible – das allererste Playbook .....	1095
27.5.2	Formulierung von Tasks .....	1099
27.5.3	Beenden von Plays .....	1100



27.5.4	Kommandoaufrufe mit den Modulen <code>command</code> und <code>shell</code> .....	1100
27.5.5	Fehlerbehandlung .....	1104
27.5.6	Tags .....	1105
27.5.7	Das Kommando <code>ansible-playbook</code> .....	1107
27.5.8	Eine exemplarische Apache-Installation .....	1108
27.5.9	Handler: Tasks nur bei Changes durchführen .....	1112
<b>27.6</b>	<b>Playbooks und Tasks: fortgeschrittene Methoden</b> .....	<b>1115</b>
27.6.1	Variablen .....	1115
27.6.2	Facts und implizite Variablen .....	1121
27.6.3	Bedingte Ausführung mit <code>when</code> .....	1123
27.6.4	Jinja und Templates .....	1124
27.6.5	Schleifen .....	1127
27.6.6	Fehlerbehandlung mit <code>failed_when</code> und <code>ignore_errors</code> .....	1130
27.6.7	Blocks (und noch mal Fehlerbehandlung) .....	1131
27.6.8	Lookup-Plugins .....	1133
27.6.9	Umgebungsvariablen setzen .....	1135
<b>27.7</b>	<b>Modularisierung mit Rollen und Includes</b> .....	<b>1136</b>
27.7.1	Erstellung und Verwendung von Rollen .....	1136
27.7.2	Ansible Galaxy .....	1141
27.7.3	Verwendung von Imports/Includes .....	1142
<b>27.8</b>	<b>Die Modul-Bibliothek</b> .....	<b>1143</b>
27.8.1	Module zur Kommandoausführung .....	1143
27.8.2	Module zur Paketverwaltung .....	1145
27.8.3	Module zur Verwaltung von Dateien und Dateiinhalten .....	1146
27.8.4	Module für weitere typische Verwaltungsaufgaben .....	1151
<b>27.9</b>	<b>Ansible Vault</b> .....	<b>1153</b>
27.9.1	Erste Schritte .....	1153
27.9.2	Mehrere Vault-Passwörter und weitere Vault-Kommandos .....	1155
27.9.3	Ein Trick zum Wiederfinden von Variablen .....	1156
27.9.4	Mehr Bequemlichkeit bzw. Automatisierbarkeit .....	1156
27.9.5	Bequem und (möglichst) sicher mit GPG + pass .....	1157

---

## 28 Monitoring – wissen, was läuft 1161

<b>28.1</b>	<b>Monitoring mit Checkmk</b> .....	<b>1161</b>
<b>28.2</b>	<b>Installation der Pakete</b> .....	<b>1161</b>
28.2.1	Installation von Checkmk unter openSUSE Leap .....	1162

28.2.2	Installation von Checkmk unter Debian/Ubuntu .....	1163
28.2.3	Installation von Checkmk unter CentOS .....	1163
28.2.4	Die erste Kontrolle – klappt alles? .....	1163
<b>28.3</b>	<b>Einrichtung der ersten Monitoring-Instanz .....</b>	<b>1163</b>
<b>28.4</b>	<b>Server, Geräte und Dienste überwachen .....</b>	<b>1166</b>
<b>28.5</b>	<b>Installation des Checkmk-Agenten .....</b>	<b>1167</b>
<b>28.6</b>	<b>Anlegen eines Hosts .....</b>	<b>1168</b>
<b>28.7</b>	<b>Betriebs- und Fehlerzustände von Host und Services im Überblick .....</b>	<b>1169</b>
<b>28.8</b>	<b>Konfiguration durch Regelsätze .....</b>	<b>1171</b>
28.8.1	Arbeiten in Host-Ordnern .....	1172
28.8.2	Keine Alarme für Testsysteme .....	1173
28.8.3	Unterschiedliche Alarmschwellen bei Dateisystemen .....	1174
28.8.4	Service Discovery Rules: Gezielt Prozesse überwachen .....	1177
28.8.5	HTTP, TCP und E-Mail: Netzwerkdienste überwachen .....	1178
<b>28.9</b>	<b>Notifications .....</b>	<b>1179</b>
28.9.1	Anlegen weiterer Kontaktgruppen .....	1180
28.9.2	Test der E-Mail-Zustellung .....	1181
28.9.3	Alarmierung per SMS .....	1181
28.9.4	Wann wird ein Fehler zum HARD STATE? .....	1182
28.9.5	Definieren von Notification Periods .....	1183
<b>28.10</b>	<b>Alarme managen .....</b>	<b>1183</b>
28.10.1	Die mächtige Suche von Checkmk .....	1184
<b>28.11</b>	<b>Weitere Fähigkeiten von Checkmk .....</b>	<b>1186</b>
<b>28.12</b>	<b>Fazit .....</b>	<b>1187</b>

## TEIL VII Sicherheit, Verschlüsselung und Zertifikate

<b>29</b>	<b>Sicherheit .....</b>	<b>1191</b>
<b>29.1</b>	<b>Weniger ist mehr .....</b>	<b>1192</b>
<b>29.2</b>	<b>»chroot« .....</b>	<b>1193</b>
29.2.1	Dienste .....	1193
<b>29.3</b>	<b>Selbstabsicherung: AppArmor .....</b>	<b>1195</b>
29.3.1	Status und Betriebsarten .....	1196
29.3.2	Eigene Profile erstellen .....	1198

<b>29.4</b>	<b>Gotcha! Intrusion-Detection-Systeme</b> .....	1201
29.4.1	snort und Co. ....	1202
<b>29.5</b>	<b>Installation und Konfiguration</b> .....	1204
29.5.1	Vorbereitungen .....	1204
29.5.2	Kompilieren und installieren .....	1205
29.5.3	Basiskonfiguration .....	1207
29.5.4	Ein erster Test: ICMP .....	1208
29.5.5	Start-Skript erstellen: systemd .....	1209
<b>29.6</b>	<b>Das Neueste vom Neuen: pulledpork</b> .....	1210
<b>29.7</b>	<b>Klein, aber oho: fail2ban</b> .....	1212
29.7.1	Konfiguration .....	1212
29.7.2	Aktive Sperrungen .....	1215
29.7.3	Reguläre Ausdrücke .....	1216
<b>29.8</b>	<b>OpenVPN</b> .....	1217
29.8.1	Serverinstallation – OpenVPN, PKI und Co. ....	1218
29.8.2	CentOS/openSUSE Leap: easy-rsa .....	1224
29.8.3	Gemeinsam weiter .....	1226
29.8.4	Roadwarrior .....	1227
29.8.5	Start-Skript? .....	1230
29.8.6	Site-to-site .....	1234
29.8.7	Simple-HA .....	1236
29.8.8	Tipps und Tricks .....	1237

---

## **30 Verschlüsselung und Zertifikate** 1241

---

<b>30.1</b>	<b>Definition und Historie</b> .....	1241
<b>30.2</b>	<b>Moderne Kryptologie</b> .....	1243
30.2.1	Symmetrische Verschlüsselung .....	1243
30.2.2	Asymmetrische Verschlüsselung .....	1244
<b>30.3</b>	<b>Den Durchblick behalten</b> .....	1245
30.3.1	Das Grundproblem .....	1245
30.3.2	Verwendungszwecke .....	1246
30.3.3	Umsetzung mithilfe einer PKI .....	1246
30.3.4	X.509 .....	1247
30.3.5	Ein anderer Ansatz: PGP (Web-of-Trust) .....	1249
<b>30.4</b>	<b>Einmal mit allem und kostenlos bitte: Let's Encrypt</b> .....	1250

---

30.4.1	Wie funktioniert das? .....	1250
30.4.2	Einschränkungen .....	1251
30.4.3	Der Client »certbot« .....	1251
<b>30.5</b>	<b>In der Praxis</b> .....	<b>1253</b>
30.5.1	Einrichtung einer PKI mit Server- und E-Mail-Zertifikaten .....	1253
30.5.2	E-Mail-Verschlüsselung .....	1264
<b>30.6</b>	<b>Neben der Kommunikation – Dateiverschlüsselung</b> .....	<b>1271</b>
30.6.1	Dateien .....	1271
30.6.2	Devices .....	1272
30.6.3	Festplatten/System .....	1274
<b>30.7</b>	<b>Rechtliches</b> .....	<b>1278</b>
30.7.1	Fortgeschrittene elektronische Signatur .....	1279
30.7.2	Qualifiziertes Zertifikat .....	1279
30.7.3	Qualifizierte elektronische Signatur .....	1279
30.7.4	Sichere Signaturerstellungseinheit (SSEE) .....	1280
Die Autoren .....		1281
Index .....		1283