

# Der eigene Server mit FreeBSD 9

Konfiguration, Sicherheit und Pflege

von  
Benedikt Nießen

1. Auflage

Der eigene Server mit FreeBSD 9 – Nießen

schnell und portofrei erhältlich bei [beck-shop.de](http://beck-shop.de) DIE FACHBUCHHANDLUNG

Thematische Gliederung:

[UNIX Betriebssysteme](http://UNIX-Betriebssysteme)

dpunkt.verlag 2012

Verlag C.H. Beck im Internet:

[www.beck.de](http://www.beck.de)

ISBN 978 3 89864 814 1

**Benedikt Nießen**

# **Der eigene Server mit FreeBSD 9**

**Konfiguration, Sicherheit und Pflege**



**dpunkt.verlag**

Benedikt Nießen  
buch@niessen.ch

Lektorat: Dr. Michael Barabas  
Copy-Editing: Friederike Daenecke  
Herstellung: Frank Heidt  
Umschlaggestaltung: Helmut Kraus, [www.exclam.de](http://www.exclam.de)  
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek  
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;  
detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN:  
Buch 978-3-89864-814-1  
PDF 978-3-86491-122-4  
ePub 978-3-86491-123-1

Copyright © 2012 dpunkt.verlag GmbH  
Ringstraße 19 B  
69115 Heidelberg

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

# Inhaltsverzeichnis

<b>Vorwort und Typografie</b>	<b>xiii</b>
<b>1 Eine Einführung</b>	<b>1</b>
1.1 Was bedeutet es, Administrator zu sein? .....	1
1.2 Warum FreeBSD? .....	2
1.3 Das Ziel dieses Buchs .....	3
1.4 Neuerungen in FreeBSD 9 .....	4
1.5 Der neue Installer .....	4
1.6 High Availability Storage .....	4
1.7 Ressourcenbeschränkungen .....	5
1.8 Kernel-Dumps auf andere Systeme .....	6
1.9 Das Sandbox-Framework Capiscum .....	6
<b>2 FreeBSD installieren</b>	<b>7</b>
<b>3 Erste Schritte im neuen System</b>	<b>23</b>
3.1 Arbeiten mit dem Server .....	23
3.2 Das richtige Passwort .....	24
3.3 Die Verzeichnisstruktur von FreeBSD .....	25
3.4 Die Editoren »vi« und »ee« .....	27
3.4.1 vi .....	27
3.4.2 ee .....	28
3.5 »sudo« – weil es nicht immer root sein muss .....	28
3.6 Die Shell anpassen .....	30
3.7 SSH absichern .....	32
3.7.1 Gefühlte Sicherheit erhöhen .....	33
3.7.2 Tatsächliche Sicherheit erhöhen .....	33

3.8	Zeitsynchronisation per NTP . . . . .	34
3.9	E-Mails für root an ein Postfach weiterleiten . . . . .	36
3.10	Zusammenfassung . . . . .	37
<b>4</b>	<b>Erste Gedanken zur Sicherheit</b>	<b>39</b>
4.1	Die Benutzerverwaltung . . . . .	39
4.2	Das Berechtigungsmodell . . . . .	40
4.3	Der Systemaufbau in diesem Buch . . . . .	42
4.4	Zusammenfassung . . . . .	42
<b>5</b>	<b>Das System aktuell halten</b>	<b>45</b>
5.1	System-Updates installieren . . . . .	46
5.2	Release-Wechsel durchführen . . . . .	46
5.3	Zusammenfassung . . . . .	47
<b>6</b>	<b>Software installieren</b>	<b>49</b>
6.1	Der Portstree . . . . .	49
6.1.1	Den Portstree installieren . . . . .	49
6.1.2	Den Portstree aktualisieren . . . . .	50
6.1.3	Den Portstree durchsuchen . . . . .	50
6.1.4	Ports installieren . . . . .	50
6.1.5	Der Compiler-Cache ccache . . . . .	51
6.1.6	Installierte Software verändern . . . . .	53
6.1.7	Ports aktualisieren . . . . .	53
6.1.8	Ports deinstallieren . . . . .	53
6.1.9	Unsichere Ports erkennen . . . . .	54
6.2	pkg als Alternative zum Portstree . . . . .	54
6.2.1	Ein Paket installieren . . . . .	55
6.2.2	Ein Paket aktualisieren . . . . .	55
6.2.3	Ein Paket deinstallieren . . . . .	55
6.3	Überflüssige Ports aufspüren . . . . .	55
6.4	Zusammenfassung . . . . .	56

<b>7</b>	<b>Die Firewall konfigurieren</b>	<b>57</b>
7.1	Brauche ich eine Firewall auf dem Server? . . . . .	57
7.2	Firewall mit pf . . . . .	58
7.2.1	Der Firewall-Airbag . . . . .	58
7.2.2	Grundlegende Optimierungen . . . . .	59
7.2.3	Firewallregeln . . . . .	59
7.2.4	Eine Beispielkonfiguration . . . . .	60
7.2.5	pf aktivieren . . . . .	62
7.2.6	pf steuern . . . . .	62
7.3	Spezielle pf-Konfigurationen . . . . .	63
7.3.1	Dienste mit sshguard schützen . . . . .	63
7.3.2	Brute-Force-Schutz mit expire-Table . . . . .	64
7.4	Firewall-Monitoring mit pftop . . . . .	66
7.5	Packet Queueing und Priorisierung . . . . .	66
7.5.1	Priority Based Queueing . . . . .	68
7.5.2	Class Based Queueing . . . . .	68
7.5.3	Scheduler-Optionen . . . . .	69
7.5.4	Queues zuweisen . . . . .	69
7.6	Zusammenfassung . . . . .	69
<b>8</b>	<b>Arbeiten mit Jails</b>	<b>71</b>
8.1	Was sind Jails? . . . . .	71
8.2	Das System für Jails vorbereiten . . . . .	72
8.2.1	IP-Aliase anlegen . . . . .	72
8.2.2	Firewallregeln anpassen . . . . .	74
8.2.3	FreeBSD-Quellcode auschecken . . . . .	75
8.3	Das Jail-Framework ezJail . . . . .	75
8.4	Jails anlegen, starten und konfigurieren . . . . .	76
8.4.1	Jail-Vorlage anpassen . . . . .	77
8.4.2	Jail anlegen . . . . .	77
8.4.3	Jail starten . . . . .	78
8.4.4	Jail betreten und verlassen . . . . .	78
8.4.5	Jail stoppen . . . . .	79
8.4.6	Jail löschen . . . . .	79
8.4.7	Jail deaktivieren und aktivieren . . . . .	79
8.4.8	Portstree in eine Jail mounten . . . . .	79
8.5	Backup einer Jail anlegen und wiederherstellen . . . . .	80
8.6	ccache-Konfiguration anpassen . . . . .	81
8.7	Binary-Update für die Basejail . . . . .	81

8.8	Ressourcenbeschränkungen für Jails .....	81
8.8.1	RCTL-Unterstützung aktivieren .....	82
8.8.2	Obergrenzen festlegen .....	82
8.8.3	Ressourcennutzung anzeigen .....	83
8.8.4	Einschränkungen entfernen .....	83
8.9	Zusammenfassung .....	83
<b>9</b>	<b>Appliances konfigurieren</b>	<b>85</b>
9.1	Datenbankserver .....	86
9.1.1	MySQL .....	86
9.1.2	MySQL-Server-Tuning .....	88
9.1.3	MariaDB .....	89
9.1.4	Drizzle .....	90
9.1.5	Replikation von MySQL- und MariaDB-Datenbanken .....	90
9.1.5.1	Master/Slave-Replikation .....	91
9.1.5.2	Master/Master-Replikation .....	95
9.1.6	Zusammenfassung .....	98
9.2	Webserver .....	98
9.2.1	nginx .....	99
9.2.1.1	Installation und Konfiguration .....	99
9.2.1.2	vHosts anlegen .....	102
9.2.1.3	Die location-Direktive .....	103
9.2.1.4	Ein vollständiger vHost .....	105
9.2.1.5	Berechtigungen richtig setzen .....	106
9.2.1.6	Passwortschutz für Verzeichnisse .....	106
9.2.1.7	SSL-Verschlüsselung für vHosts .....	108
9.2.1.8	nginx gegen (D)DoS-Attacken rüsten .....	109
9.2.2	PHP 5 per FastCGI .....	111
9.2.2.1	Installation .....	111
9.2.2.2	PHP-FPM als FastCGI-Manager .....	113
9.2.2.3	Benutzer und Gruppe anlegen .....	113
9.2.2.4	PHP 5 absichern .....	115
9.2.2.5	PHP 5-Prozesse konfigurieren und starten .....	115
9.2.2.6	PHP 5 im vHost konfigurieren .....	118
9.2.3	Webapplication-Firewall mit nginx .....	118
9.2.3.1	Das NAXSI-Modul installieren .....	119
9.2.3.2	Den vHost für NAXSI konfigurieren .....	119
9.2.3.3	Die Whitelist erstellen .....	121
9.2.3.4	Die Whitelist aktivieren .....	122
9.2.4	Zusammenfassung .....	123
9.3	FTP-Server mit Pure-FTPd .....	124
9.3.1	FTP-Benutzer anlegen .....	127
9.3.2	Firewall anpassen .....	128

---

9.4	Mailserver mit IMAP und POP3 . . . . .	129
9.4.1	Die Mailserverkomponenten . . . . .	130
9.4.2	Der MTA: Postfix . . . . .	130
9.4.2.1	sendmail deaktivieren . . . . .	131
9.4.2.2	Postfix installieren . . . . .	131
9.4.2.3	Die MySQL-Datenbank pflegen . . . . .	132
9.4.2.4	Postfix konfigurieren . . . . .	134
9.4.2.5	Weitere Verzeichnisse und Zertifikate erstellen . . . . .	138
9.4.3	Der MDA: Dovecot . . . . .	139
9.4.4	Berechtigungen setzen . . . . .	141
9.4.5	Firewall anpassen . . . . .	142
9.4.6	Postfächer und E-Mail-Adressen verwalten . . . . .	142
9.4.6.1	SQL-Befehle zur Benutzerverwaltung . . . . .	143
9.4.6.2	PostfixAdmin installieren . . . . .	145
9.4.7	E-Mail-Clients konfigurieren . . . . .	145
9.4.8	Spam- und Virenabwehr . . . . .	146
9.4.8.1	Blacklists . . . . .	147
9.4.8.2	Spam-Filter und Virenschanner per DSPAM integrieren . . . . .	148
9.4.8.3	Sender Policy Framework . . . . .	163
9.4.8.4	Dovecot-Antispam . . . . .	164
9.4.8.5	Spam-Bekämpfung auf Firewallebene . . . . .	166
9.4.8.6	Greylisting mit SQLgrey . . . . .	169
9.4.9	E-Mails mit Sieve sortieren . . . . .	173
9.4.9.1	Was ist Sieve? . . . . .	173
9.4.9.2	Die Syntax von Sieve . . . . .	173
9.4.9.3	Sieve-Plug-in installieren . . . . .	176
9.4.10	Jails anpassen . . . . .	176
9.4.11	DNS-Einstellungen vornehmen . . . . .	178
9.4.12	Zusammenfassung . . . . .	178
9.5	Cache-Server . . . . .	179
9.5.1	Memcached . . . . .	179
9.5.2	Redis . . . . .	181
9.6	Subversion-Server . . . . .	182
9.6.1	Repositories anlegen . . . . .	183
9.6.2	Repositories sichern . . . . .	184
9.6.3	Repositories wiederherstellen . . . . .	185
9.7	Virtual Private Network (VPN) . . . . .	185
9.7.1	Client/Server-Verbindung . . . . .	185
9.7.2	Server/Server-Verbindung . . . . .	189
9.7.2.1	Die Funktionsweise von tinc . . . . .	189
9.7.2.2	Tinc installieren . . . . .	190
9.7.2.3	Den VPN-Server konfigurieren . . . . .	190
9.7.2.4	Den VPN-Client konfigurieren . . . . .	192

9.8	Samba-Server für Intranets .....	194
9.8.1	Öffentliche Freigaben .....	195
9.8.2	Geschützte Freigaben .....	195
9.8.3	Benutzer verwalten .....	196
9.8.4	Samba starten .....	196
<b>10</b>	<b>Daten sichern</b>	<b>197</b>
10.1	Backups erstellen .....	197
10.1.1	Backup-Profil anlegen .....	197
10.1.2	GPG-Verschlüsselung konfigurieren .....	198
10.1.3	Backup-Profil konfigurieren .....	198
10.1.4	Verzeichnisse ausschließen .....	199
10.1.5	Befehle vor oder nach dem Backup-Prozess ausführen .....	200
10.1.6	Backup anlegen .....	200
10.1.7	Dateien wiederherstellen .....	201
10.1.8	Backup-Speicher bereinigen .....	201
10.2	Datensicherung mit Snapshots .....	202
10.2.1	Snapshot erstellen .....	202
10.2.2	Snapshots anzeigen .....	203
10.2.3	Snapshots mounten .....	203
10.2.4	Snapshots automatisieren .....	203
10.3	Datenbanken sichern mit AutoMySQLBackup .....	204
10.4	Zusammenfassung .....	205
<b>11</b>	<b>Serverüberwachung</b>	<b>207</b>
11.1	Hardware-Monitoring .....	207
11.1.1	Festplatten überwachen .....	207
11.1.2	Die CPU überwachen .....	208
11.2	Service-Monitoring .....	208
11.2.1	Monitoring mit monit .....	209
11.2.1.1	Allgemeine Einstellungen .....	209
11.2.1.2	Überwachungsaufgaben konfigurieren .....	210
11.2.1.3	Überwachung von Services in einer Jail .....	211
11.2.1.4	Webinterface für monit .....	211
11.2.2	Der Logfile-Parser logwatch .....	212
11.2.3	Der Logging-Daemon rsyslog .....	213
11.2.3.1	syslog ersetzen .....	213
11.2.3.2	MySQL-Server konfigurieren .....	214
11.2.3.3	rsyslog konfigurieren .....	215

---

11.3	Kombinierte Überwachung mit munin . . . . .	215
11.3.1	Den Master konfigurieren . . . . .	216
11.3.2	Clients konfigurieren . . . . .	217
11.4	Einbruchsversuche erkennen und abwehren . . . . .	218
11.4.1	Ports überwachen mit portsentry . . . . .	219
11.4.2	Einfache Integritätsprüfung mit freebsd-update . . . . .	220
11.5	Zusammenfassung . . . . .	221
<b>12</b>	<b>Für Fortgeschrittene</b>	<b>223</b>
12.1	Software-RAID1 mit gmirror . . . . .	223
12.1.1	Partitionstabellen abgleichen . . . . .	224
12.1.2	Partitionen spiegeln . . . . .	225
12.1.3	RAID-Verbund wiederherstellen . . . . .	226
12.2	Loadbalancer und Reverse Proxies . . . . .	227
12.2.1	pound (ohne Caching) . . . . .	228
12.2.2	HAproxy (ohne Caching) . . . . .	230
12.2.2.1	Session-Persistence . . . . .	232
12.2.2.2	Access Control Lists (ACL) . . . . .	233
12.2.2.3	HAproxy starten . . . . .	233
12.2.3	nginx (mit Caching) . . . . .	234
12.2.3.1	Installation . . . . .	234
12.2.3.2	Konfiguration mit Festplatten-Cache . . . . .	235
12.2.3.3	Konfiguration mit Memcached . . . . .	237
12.3	Loadbalancing mit Failover für TCP-Verbindungen . . . . .	239
12.4	Port-Knocking . . . . .	240
12.5	FreeBSD abhärten . . . . .	243
12.5.1	Zugriffsrechte beschränken . . . . .	243
12.5.2	Sysctl-Flags setzen . . . . .	244
12.5.3	Sicherheitsstufen anpassen . . . . .	246
12.5.4	Dateien vor Veränderung schützen . . . . .	247
12.5.5	Sicherheitsstufe per Passwort heruntersetzen . . . . .	248
12.5.6	Sicherheitsstufen in Jails . . . . .	250
12.5.7	Logrotation trotz »append-only«-Markierung . . . . .	250
12.6	Device-Polling für Netzwerkkarten aktivieren . . . . .	251
12.6.1	Den Kernel konfigurieren und installieren . . . . .	251
12.6.2	Konfiguration der Netzwerkkarten anpassen . . . . .	252
12.7	IPv6 auf dem Hostsystem konfigurieren . . . . .	252

12.8	Einen eigenen Kernel kompilieren . . . . .	254
12.8.1	Den Quellcode aktualisieren . . . . .	254
12.8.2	Den Kernel konfigurieren . . . . .	254
12.8.3	Den Kernel kompilieren . . . . .	255
12.8.4	Den neuen Kernel testen . . . . .	256
12.8.5	Den neuen Kernel installieren . . . . .	256
12.9	Zusammenfassung . . . . .	256
<b>13</b>	<b>Server läuft – was jetzt?</b>	<b>259</b>
	<b>Index</b>	<b>261</b>