

# Apache Kochbuch

*Ken Coar & Rieh Bowen*

*Deutsche Übersetzung von  
Jochen Wiedmann*

**O'REILTT**

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

# Inhalt

<b>Vorwort</b> .....	<b>XI</b>
<b>Installation</b> .....	<b>1</b>
1.1 Installation eines RPM-Archivs unter Red Hat Linux .....	2
1.2 Installation des Apache unter Windows .....	3
1.3 Download der Apache-Quelltexte .....	10
1.4 Übersetzung der Apache-Quelltexte .....	12
1.5 Installation mit der ApacheToolbox .....	13
1.6 Start, Stopp und Neustart des Apache .....	16
1.7 Deinstallation des Apache .....	18
<b>Einbau der wichtigsten Module</b> .....	<b>21</b>
2.1 Installation eines generischen Moduls .....	22
2.2 Installation von mod_dav unter Linux oder Unix .....	23
2.3 Installation von mod_dav unter Windows .....	25
2.4 Installation von mod_perl unter Linux oder Unix .....	28
2.5 Installation von mod_php unter Linux oder Unix .....	30
2.6 Installation von mod_php unter Windows .....	31
2.7 Installation des Python-Moduls mod_snake .....	32
2.8 Installation von mod_ssl .....	33
<b>Logging</b> .....	<b>35</b>
3.1 Weitere Details in Logdateien aufnehmen .....	39
3.2 Ausführlichere Fehlermeldungen .....	40
3.3 Protokollierung des Inhalts von POST-Requests .....	42
3.4 Protokollierung der IP-Adresse eines Proxy-Clients .....	43
3.5 Protokollierung der MAC-Adresse des Clients .....	43

3.6	Protokollierung von Cookies. . . . .	44
3.7	Unterdrückung von Requests nach Bildern auf lokalen Seiten. . . . .	46
3.8	Pro Tag oder Stunde neue Protokolldateien erzeugen. . . . .	47
3.9	Rotation von Logdateien am Monatsersten. . . . .	48
3.10	Protokollierung von Hostnamen statt IP-Adressen. . . . .	49
3.11	Separate Logdateien für jeden virtuellen Host. . . . .	50
3.12	Protokollierung von Proxy-Requests. . . . .	51
3.13	Fehlermeldungen virtueller Hosts auf mehrere Dateien verteilen. . . . .	52
3.14	Protokollierung der IP-Adresse des Servers. . . . .	53
3.15	Protokollierung der referenzierenden URL. . . . .	54
3.16	Protokollierung der verwendeten Browser-Software. . . . .	55
3.17	Protokollieren beliebiger Felder im Header des HTTP-Requests. . . . .	56
3.18	Protokollierung beliebiger Felder im Header der HTTP-Response. . . . .	57
3.19	Protokollierung in eine MySQL-Datenbank. . . . .	57
3.20	Protokollierung in syslog. . . . .	58
3.21	Protokolle für Anwenderverzeichnisse. . . . .	60
<b>Virtuelle Hosts. . . . .</b>		<b>63</b>
4.1	Einrichtung eines namensbasierten virtuellen Hosts. . . . .	64
4.2	Auswahl eines namensbasierten virtuellen Hosts als Defaultserver. . . . .	66
4.3	Einrichtung IP-basierter virtueller Hosts. . . . .	67
4.4	Einrichtung eines Defaulthosts für IP-basierte virtuelle Hosts. . . . .	68
4.5	Kombination von IP-basierten und namensbasierten virtuellen Hosts. . . . .	69
4.6	Einrichtung einer großen Anzahl virtueller Hosts mit mod_vhost_alias. . . . .	70
4.7	Einrichtung einer großen Anzahl virtueller Hosts mit mod_rewrite. . . . .	72
4.8	SSL und namensbasierte virtuelle Hosts. . . . .	73
4.9	Logdateien pro virtuellem Host. . . . .	74
4.10	Aufteilung einer Logdatei. . . . .	75
4.11	Portbasierte virtuelle Hosts. . . . .	76
4.12	Präsentation desselben Inhalts auf mehreren IP-Adressen. . . . .	77
<b>Aliase, Redirect und Rewrite. . . . .</b>		<b>79</b>
5.1	Ausgabe kolorierter PHP-Quelltexte ohne die Verwendung symbolischer Links. . . . .	79
5.2	Abbildung einer URL auf ein Verzeichnis. . . . .	81
5.3	Vorhandene Dateien unter einer neuen URL zugänglich machen. . . . .	82
5.4	Zuteilung eigener Webverzeichnisse. . . . .	83
5.5	Einrichtung eines Alias für mehrere URLs. . . . .	86
5.6	Einrichtung eines Alias für CGI-Verzeichnisse und mehrere URLs. . . . .	87

5.7	Einrichtung eines persönlichen CGI-Verzeichnisses für alle Anwender ...	88
5.8	Redirect auf eine andere URL. ....	88
5.9	Redirect verschiedener URLs an dasselbe Ziel. ....	90
5.10	Groß- und Kleinschreibung in URLs ignorieren. ....	91
5.11	Text in URLs ersetzen. ....	92
5.12	Ändern von Pfadinformationen, die CGI-Skripten zur Verfügung gestellt werden. ....	93
5.13	Zugriffe aus fremden Dokumenten verbieten. ....	94
5.14	Rewrite der URL anhand des Query-Strings. ....	95
5.15	Redirect einer URL oder des ganzen Servers auf SSL. ....	95
5.16	Verzeichnisnamen in Hostnamen umwandeln. ....	96
5.17	Redirect aller Requests auf einen einzigen Host. ....	97
5.18	Umwandlung von Dokumentnamen in Argumente. ....	98
<b>Sicherheit. ....</b>		<b>99</b>
6.1	Verwendung der Systemdaten zur Authentifizierung. ....	100
6.2	Einrichtung von Passwörtern zum einmaligen Gebrauch. ....	102
6.3	Passwörter mit Verfallsdatum. ....	103
6.4	Limitierung der Größe eines Uploads. ....	105
6.5	Zugriffe aus fremden Dokumenten verbieten. ....	107
6.6	Erzwingen von schwacher und starker Authentifizierung. ....	108
6.7	Administration von .htpasswd-Dateien. ....	109
6.8	Erzeugen von Passwortdateien zur Authentifizierung per Digest. ....	112
6.9	Lockerung der Sicherheitsrichtlinien in einem Unterverzeichnis. ....	113
6.10	Selektive Zugriffsrestriktionen. ....	115
6.11	Authentifizierung über Eigentumsrechte des Betriebssystems. ....	116
6.12	Speicherung von Benutzerdaten in einer MySQL-Datenbank. ....	117
6.13	Zugriff auf den Namen des authentifizierten Benutzers. ....	119
6.14	Zugriff auf das zur Authentifizierung benutzte Passwort. ....	120
6.15	Unterbindung massenhafter Versuche zur Auskundshaftung von Passwörtern. ....	120
6.16	Authentifizierungsmodus Digest oder Basic. ....	121
6.17	Zugriff auf Benutzerdaten in URLs. ....	123
6.18	Einrichten von Sicherheitsrichtlinien für WebDAV. ....	123
6.19	WebDAV ohne Update-Möglichkeiten durch unbefugte Anwender ....	124
6.20	Einschränkung des Zugriffs per Proxy auf bestimmte URLs. ....	126
6.21	Sperrung des Zugriffs mit Hilfe eines Wrappers. ....	127
6.22	Zugriffsschutz für alle Dateien mit Ausnahme bestimmter. ....	129
6.23	Schutz des Servers vor böswilligen Skripten. ....	130

6.24	Setzen korrekter Dateirechte . . . . .	131
6.25	Limitierung der vorhandenen Module . . . . .	134
6.26	Zugriff auf Dateien außerhalb des Dokumentverzeichnisses unterbinden	136
6.27	Einschränkung der verwendbaren GET-Methoden . . . . .	137
6.28	Verbot partieller Downloads . . . . .	138
<b>7</b>	<b>SSL . . . . .</b>	<b>141</b>
7.1	Installation von SSL . . . . .	141
7.2	Generierung eines SSL-Zertifikats . . . . .	143
7.3	Generierung einer Zertifizierungsstelle . . . . .	146
7.4	Umstellung eines Teils Ihrer Site auf SSL . . . . .	148
7.5	Authentifizierung mit Client-Zertifikaten . . . . .	150
<b>8</b>	<b>Dynamische Inhalte . . . . .</b>	<b>151</b>
8.1	Einrichtung eines CGI-Verzeichnisses . . . . .	151
8.2	Aktivieren von CGI-Skripten in Verzeichnissen mit statischen Inhalten .	152
8.3	Dateiendungen von Windows zur Erkennung von CGI-Skripten nutzen.	153
8.4	Verwendung von Dateiendungen zur Identifikation von CGI-Skripten . .	155
8.5	Test der Funktion einer CGI-Umgebung . . . . .	155
8.6	Lesen von Formularinhalten . . . . .	158
8.7	Aufrufeines CGI-Skripts zur Behandlung eines Content-Type. . . . .	161
8.8	Konfiguration von SSL . . . . .	162
8.9	Ausgabe des Änderungsdatums von Dokumenten . . . . .	164
8.10	Einbindung eines Standardseitenkopfs . . . . .	165
8.11	Ausgabe eines CGI-Skripts in HTML-Seiten einbinden . . . . .	166
8.12	Start eines CGI-Skripts unter einer anderen User-ID mit suexec. . . . .	166
8.13	Installation eines mod_perl-Handlers aus dem CPAN . . . . .	169
8.14	Schreiben eines eigenen mod_perl-Handlers . . . . .	170
8.15	Aktivieren von PHP-Skripten . . . . .	172
8.16	Prüfung der PHP-Installation . . . . .	172
<b>9</b>	<b>Fehlerbehandlung . . . . .</b>	<b>175</b>
9.1	Fehlerbehandlung bei fehlendem Host-Header . . . . .	175
9.2	Fehlerbehandlung durch CGI-Skripten . . . . .	176
9.3	Individuelle Fehlermeldungen . . . . .	177
9.4	Ausgabe von Fehlern in mehreren Sprachen . . . . .	178
9.5	Redirect ungültiger URLs auf eine andere Seite . . . . .	180
9.6	Ausgabe der individuellen Fehlermeldung im Internet Explorer. . . . .	181
9.7	Benachrichtigung im Falle von Fehlermeldungen . . . . .	182

<b>10</b>	<b>Proxyserver.</b>	<b>185</b>
10.1	Sicherheitsrelevante Maßnahmen	186
10.2	Verhindern, dass ein Proxyserver zum Verschicken von Spam-Mail missbraucht wird	187
10.3	Weiterleitung von Requests an einen anderen Server	188
10.4	Sperren bestimmter URLs im Proxy	189
10.5	Der Proxy als Frontend eines mod_perl-Servers	190
10.6	Beschleunigung des Proxy durch einen Cache	190
10.7	Filtern der vom Proxy gelieferten Inhalte	191
10.8	Schutz des Proxyservers durch Authentifikation	192
<b>11</b>	<b>Performance.</b>	<b>195</b>
11.1	Schätzung des erforderlichen Hauptspeichers	196
11.2	Durchführung eines Benchmarks mit ab	197
11.3	Tuning der Keepalive-Einstellungen	198
11.4	Anzeige des Serverstatus	200
11.5	Vermeidung von DNS-Lookups	201
11.6	Optimierung symbolischer Links	203
11.7	Minimierung der Performance-Nachteile von .htaccess-Dateien	204
11.8	Verbot von Content Negotiation	206
11.9	Die Erzeugung neuer Prozesse optimieren	208
11.10	Die Erzeugung von Threads optimieren	209
11.11	Verwaltung eines Cache häufig gelesener Dateien	211
11.12	Lastverteilung zwischen verschiedenen Servern mit mod_proxy	213
11.13	Last gleichmäßig auf mehrere Server verteilen	214
11.14	Ausgabe von Verzeichnislisten aus einem Cache	215
11.15	Beschleunigung von in Perl geschriebenen CGI-Skripten mit mod_perl	216
<b>12</b>	<b>Verschiedenes.</b>	<b>219</b>
12.1	Anweisungen richtig platzieren	219
12.2	Einen anderen Namen für .htaccess-Dateien wählen	221
12.3	Erzeugen eines Inhaltsverzeichnisses	222
12.4	Das Problem mit dem »abschließenden Slash«	224
12.5	Setzen des Content-Type abhängig von den Fähigkeiten des Browsers	225
12.6	Fehlerbehandlung bei einem fehlenden Host-Header	226
12.7	Wahl einer anderen Indexseite	227
12.8	Einrichtung eines Defaults für das »Favicon«	227

A Einsatz regulärer Ausdrücke im Apache.....	229
B Fehlerdiagnose.....	235
Index.....	245