

Courier Mail Server

7. Juni 2004

Note légale

Dieser Beitrag ist lizenziert unter der UVM Lizenz für die freie Nutzung unveränderter Inhalte.

Zusammenfassung

Der Courier-Mailserver ist eine integrierte und zugleich modulare Mail- und Groupwarelösung, die sich zunehmender Beliebtheit erfreut. Besondere Merkmale sind u.a. die konsequente Unterstützung des Maildir++-Formats für die Speicherung der Emails, Authentifizierung mittels eines speziellen Dienstes für System- und virtuelle Konten, sowie geteilte Konten.

Courier bietet die Dienste ESMTP, IMAP, POP3, Webmail und Mailinglisten in einem konsistenten Framework an. Die einzelnen Dienste sind unabhängig von einander und können je nach Wunsch aktiviert bzw. deaktiviert werden. Ein häufiges Einsatzszenario ist die Verwendung eines anderen MTA wie z.B. Exim oder Postfix zusammen mit dem Courier IMAP-Server.

Die Konfiguration erfolgt durch Textdateien, die auch mit dem mitgelieferten Administrationsfrontend bearbeitet werden können.

Der Schwerpunkt dieses Vortrag liegt auf der Architektur und Konfiguration des Systems. Zusätzlich wird die Benutzung einiger Besonderheiten von Courier erläutert.

1 Courier-Mailserver

Der Courier-Mailserver ist eine integrierte und zugleich modulare Mail- und Groupwarelösung, die sich zunehmender Beliebtheit erfreut.

Das Courier-Framework stellt den einzelnen Komponenten die folgenden Funktionalitäten zur Verfügung:

- Postfächer im **Maildir++-Format**
- virtuelle Postfächer
- **gemeinsame Ordner**
- **Authentifizierung** mittels eines speziellen Dienstes
- **SSL/TLS**
- Unterstützung von IPv6

Courier entstand aus verschiedenen Projekten von Sam Varshavchik, der auch heute noch den größten Anteil an der Weiterentwicklung dieser Software hat.

2 Pro und Contra

Courier zeichnet sich dadurch aus, dass es sowohl als umfassendes Paket aus Maildiensten verwendet werden kann als auch in Kombinationen von verschiedenen Softwarepaketen, z.B. mit Exim oder Postfix als SMTP-Server.

Ein weiterer wichtiger Pluspunkt ist die kontinuierliche Weiterentwicklung und der umfangreiche Support auf den Mailinglisten vom Autor und anderen Interessierten.

Für den Einsatz von Courier ist eine gewisse Einarbeitung erforderlich, zumal die Standardkonfiguration nicht für den typischen Kundenkreis eines ISP geeignet ist. Dazu sind einige Einstellungen wie die maximale Anzahl der Verbindungen pro IP beim IMAP-Server und der Umgang mit nicht MIME-konformer Email zu konservativ.

3 Komponenten im Überblick

Der Courier-Mailserver setzt sich aus den folgenden Komponenten zusammen:

- SMTP-Server (Courier)
- IMAP-Server (Courier-IMAP)
- POP3-Server (Courier-POP)
- Webmail (SqWebMail)
- Mailinglisten-Server (couriermlm)
- MDA mit Filterfähigkeiten (Maildrop)
- Webadministration (courierwebadmin)

Neben dem kompletten Quellpaket sind auch ausgewählte Komponenten als gesonderte Distributionen erhältlich. Dies sind Courier-IMAP, SqWebMail und Maildrop. Allerdings bestehen mitunter subtile Unterschiede zwischen den aus dem Gesamtpaket erstellten Kompilaten und den Einzelpaketen.

4 Maildir++

Courier benutzt das sogenannte Maildir++-Format zur Speicherung und zum Zugriff auf Emails. Dabei werden die einzelnen Emails in einer Hierarchie von Verzeichnisse abgelegt. Die Vorteile dieses Verfahrens gegenüber Mailboxdateien sind geringerer Ressourcenbedarf, keine Lockingprobleme (auch wenn sich die Postfächer auf einem NFS-Dateisystem befinden) und gleichzeitiger Lese- und Schreibzugriff durch mehrere Mailclients.

Maildir++ erweitert das durch qmail eingeführten Maildir-Format (<http://www.qmail.org/man/man5/maildir.html>) um Ordner und Platzbeschränkungen (Quota) unabhängig vom Dateisystem.

Mailboxdateien werden zwar z.T. unterstützt, z.B. für die Auslieferung von Emails durch Maildrop, empfehlenswert ist jedoch nur der Einsatz der Maildir-Formate.

Andere SMTP-Server wie Exim beherrschen die Auslieferung in Maildirs entweder von Haus aus oder es existieren entsprechende Patches. Ist beides nicht möglich, kann zur lokalen Auslieferung von Emails entweder `maildrop` oder `deliverquota` verwendet werden.

Für das Anlegen von Maildirs wird das Courier-Programm `maildirmake` empfohlen,

```
maildirmake /home/racke/Maildir
```

4.1 Quotas

Die bevorzugte Methode, um Platzbeschränkungen (Quotas) auf Benutzerpostfächer zu erzwingen, sind Quotas pro Benutzer, basierend auf dem Dateisystem (<http://www.tldp.org/HOWTO/Quota.html>).

Diese Lösung ist offensichtlich ungeeignet für virtuelle Postfächer, wo viele Postfächer die gleiche Benutzererkennung verwenden. Für diesen Fall kann der Speicherplatz in Maildir++-Postfächer durch sogenannte freiwillige Quotas eingeschränkt werden. Diese funktionieren jedoch nur, wenn alle Anwendungen, die Emails in diese Postfächer ausliefern, sich an diese Konvention halten. Außerdem dürfen die Benutzer keinen direkten Zugriff auf das Dateisystem haben, ansonsten können sie die Beschränkungen einfach umgehen.

Beim Anlegen eines Maildir++-Postfachs kann die Quota mit der Kommandozeilenoption `-q` des `maildirmake`-Kommandos eingerichtet werden:

```
maildirmake -q 1000000S /var/local/mail/linuxia.de/racke
```

In diesem Beispiel wurde auf dem Postfach ein Quota von ungefähr 10 Megabyte gesetzt.

Gelöschte Email und der Inhalt des Trash-Ordners werden bei der Berechnung des verbrauchten Speicherplatz nicht berücksichtigt, außer Courier wurde mit der Option `--with-trashquota` kompiliert.

4.2 Interne Struktur

Ist für ein Postfach Quota gesetzt, wird diese in der Datei `maildirsize` verwaltet.

Das Verzeichnis `courierimapkeywords` enthält die Schlagwörter für die Emails in einem Maildir++-Ordner. Diese können mit `maildirkw -L .` angezeigt werden.

5 Authentifizierung

Die Authentifizierung für die einzelnen Komponenten wird durch Authentifizierungsmodule realisiert. Dabei wird die Authentifizierung durch die folgenden beiden Aufgaben charakterisiert:

1. Zu einer Emailadresse das lokale Benutzerkonto mit Heimatverzeichnis, Benutzerkennung (UID) und Gruppenkennung (GID) bestimmen.
2. Zu einem Benutzernamen und einem Passwort das lokale Benutzerkonto mit Heimatverzeichnis, Benutzerkennung (UID) und Gruppenkennung (GID) bestimmen

In den Konfigurationsdateien der einzelnen Dienste können die gewünschten Authentifizierungsmodule angegeben werden. Dabei werden die Module nacheinander durchlaufen. Signalisiert eines der Module eine erfolgreiche Authentifizierung, steht der Dienst dem Benutzer zur Verfügung. Dieses Daisy-Chaining erlaubt z.B. PAM-Authentifizierung für Systembenutzer und Authentifizierung gegen eine MySQL-Datenbank für virtuelle Mailkonten ohne Systembenutzer.

Die wichtigsten Authentifizierungsmodule neben dem Authentifizierungsdaemon (`authdaemon`) sind:

authpam PAM-Authentifizierung

authuserdb Authentifizierung anhand einer Unix-Datenbank (GDBM oder DB)

authmysql Authentifizierung anhand einer MySQL-Datenbank

authpgsql Authentifizierung anhand einer PostgreSQL-Datenbank

authldap Authentifizierung anhand eines LDAP-Verzeichnisses

authvchkpw Authentifizierung anhand von virtuelle Domains von vpopmail

Der Authentifizierungsdaemon ist ein als Daemon laufender Proxy, der dauerhafte Verbindungen zu der Authentifizierungsdatenbank herstellt und dadurch eine deutliche schneller Authentifizierung ermöglicht, als mit den oben genannten Authentifizierungsmodulen. `authdaemon` kann ebenfalls mehrere Authentifizierungsmodule nacheinander befragen.

Normale Module sind in dem Standardprogramm `authdaemond.plain` für den Authentifizierungsdaemon enthalten. Module, die externe Bibliotheken erfordern wie `authmysql`, `authpgsql` und `authldap` benötigen angepaßte Programme für den Authentifizierungsdaemon (`authdaemond.mysql`) etc.

Die Konfiguration für den Authentifizierungsdaemon befindet sich der Datei `authdaemonrc`, die wichtigsten Variablen sind:

Tabelle 1: Konfiguration Authentifizierungsdaemon

Variable	Beschreibung	Standardwert
<code>authmodulelist</code>	Liste der Authentifizierungsmodule	-
<code>daemons</code>	Anzahl der zu startenden Dämonen	5
<code>version</code>	Programm für den Authentifizierungsdaemon	-

6 Gemeinsame Ordner

Courier-IMAP und SqWebMail können zwei Typen von gemeinsamen Ordner (shared folders) verwenden:

1. Basierend auf Dateizugriffsrechten, für Systeme mit traditionellen Shellbenutzerkonten
2. Virtuelle gemeinsame Ordner, für geschlossene Systeme mit gemeinsamen Benutzer- und Gruppenkennungen

Virtuelle gemeinsame Ordner basieren auf Zugangskontrolllisten (ACL), die nicht dem gleichnamigen Dateisystem-ACL verwechselt werden sollten. Jeder Benutzer kann einem anderen Benutzer oder einer anderen Benutzergruppen den Zugriff auf einen Ordner gewähren. Durch die Zugangskontrolllisten ist ein fein abgestufte Kontrolle der Zugriffsrechte möglich.

7 SMTP-Server (Courier)

Die Konfiguration des SMTP-Servers erfolgt über eine Anzahl von Konfigurationsdateien, die sich im Konfigurationsverzeichnis von Courier befinden. Der genaue Ort dieses Verzeichnisse wird während der Kompilierung von Courier festgelegt. Im folgenden wählen wir als Konfigurationsverzeichnis, auch für die anderen Komponenten, `/etc/courier`.

Einige Konfigurationsdateien können anstatt als einfache Textdatei auch als Sammlung von Textdateien in einem Unterverzeichnis von `/etc/courier` zur Verfügung gestellt werden. Dies ist sogar erforderlich, wenn man das Web-Administrationsfrontend verwenden möchte.

Damit Änderungen an der Konfiguration wirksam werden, ist in vielen Fällen ein Kommando aufzurufen, wie z.B. das auch von `sendmail` bekannte `makealiases`. Diese Kommandos sind in der folgenden Tabelle zusammengefaßt:

Tabelle 2: Konfigurationskommandos SMTP-Server

Datei	Kommando
<code>aliases</code>	<code>makealiases</code>
<code>esmtacceptmailfor</code>	<code>makeacceptmailfor</code>
<code>hosteddomains</code>	<code>makehosteddomains</code>
<code>smtaccess</code>	<code>makesmtaccess</code>

7.1 Lokale Domains

Lokale Domains sind in `locals` und `hosteddomains` konfiguriert. Der einzige Unterschied zwischen Domains in `locals` und `hosteddomains` ist die Methode zum Auffinden der lokalen Postfächer. Bei Domains in `locals` wird dazu die Domain aus der Emailadresse entfernt (aus `racke@linuxia.de` wird `racke`), bei `hosteddomains` nicht.

Weitere Domains, für die Courier Emails via ESMTP annimmt, können in der Datei `esmtppacceptmailfor` angegeben werden.

7.2 Aliase

Systemaliase können z.B. in `/etc/courier/aliases/system` abgelegt werden:

```
root: postmaster
mailer-daemon: postmaster
MAILER-DAEMON: postmaster
postmaster: racke
```

7.3 MIME-Konformität

Emails, die nicht den MIME-Konventionen entsprechen, können vom Courier-Mailserver akzeptiert, als nicht auslieferbar zurückgeschickt werden oder als Attachment an den Empfänger weitergeleitet werden. Diese Emails nicht zu akzeptieren ist bei der minderen Qualität vieler Emailclients oft problematisch. Die Prüfung kann in der Datei `/etc/courier/bofh` deaktiviert werden:

```
opt BOFHBADMIME=accept
```

7.4 Mailfilter

Courier stellt zwei verschiedene Mechanismen zur Filterung von Emails zur Verfügung, globale und lokale Mailfilter.

Globale Mailfilter sind im Hintergrund laufende Dämonen, die jede eingehende Email filtern. Sie können nicht die Email selbst verändern.

Lokale Mailfilter filtern Emails an lokale Benutzer, die eigene Filterregeln verwenden können. Dies wird gewöhnlich von Maildrop erledigt.

8 IMAP-Server (Courier-IMAP)

Neben den Features, die sich durch das **Courier-Framework** ergeben, zeichnet sich Courier-IMAP u.a. durch geringen Speicherverbrauch, und Unterstützung verschiedener IMAP-Erweiterungen aus:

- NAMESPACE (RFC 2342 <<http://www.rfc-editor.org/rfc/rfc2342.txt>>)
- serverseitiges Sortieren und Threading
- IMAP Schlagwörter

8.1 Namespaces

Namespaces sind die Anordnung der Ordner auf dem Server. Courier-IMAP verwendet `INBOX.` als Namespace für private Ordner und `shared.` bzw. `#shared.` als Namespace für gemeinsame Ordner. Die von Courier-IMAP unterstützte NAMESPACE IMAP-Erweiterung erlaubt es IMAP-Clients diese NAMESPACE-Konfiguration abzufragen:

```
racke#~ > telnet localhost 143
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCING]
a login racke@linuxia.de secret
a OK LOGIN Ok.
b namespace
* NAMESPACE (("INBOX." ".") NIL ("#shared." "")("shared." "."))
b OK NAMESPACE completed.
```

8.2 Typische Probleme

Einige moderne IMAP-Clients öffnen für jeden Ordner eine Verbindung zum IMAP-Server. Bei einer konservativen Einstellung für `MAXPERIP` wie die Voreinstellung 4 stehen schnell zu wenig Verbindungen zur Verfügung. Das kann z.B. dazu führen, daß der IMAP-Client einen leeren Ordner anzeigt. Sicherlich ist das als Bug des Clients zu werten, führt beim Anwender doch zu erheblicher Verwirrung.

Die automatische Konfiguration des Namespace gemäß RFC 2342 funktioniert bei einigen IMAP-Clients nicht. Für den Anwender erscheint es dann so, als ob er nur Unterordner von `INBOX` anlegen kann.

8.3 Konfiguration

Ausgewählte Konfigurationsvariablen aus `/etc/courier/imapd`:

Tabelle 3: IMAP-Konfiguration

Variable	Beschreibung
<code>MAXDAEMONS</code>	maximale Anzahl der IMAP-Server
<code>MAXPERIP</code>	maximale Anzahl der von einer IP-Adresse ausgehenden Verbindungen (u.U. mehrere pro IMAP-Server)
<code>IMAP_KEYWORDS</code>	IMAP-Schlagworte
<code>IMAP_ULIMITD</code>	maximale Größe des Datensegments des Serverprozesses (Schutzmaßnahme gegen Speicherlecks)

9 Maildrop

Maildrop wird zur Filterung und lokalen Auslieferung von Emails verwendet.

Folgendes einfache Beispiel illustriert die Filterung mit einem externen Programm:

```
import VDIR
```

```

# Send everything smaller than 256 KB to Spamassassin
if ($SIZE < 262144)
{
    xfilter "/usr/bin/spamc -U /var/run/spamd.sock"

    if (/^X-Spam-Status: Yes/:h)
    {
        exception {
            to "$VDIR/.SPAM/."
        }
    }
}

to "$VDIR/."

```

10 SqWebMail

Die Webmailvariante aus dem Courierpaket nennt sich SqWebMail und besteht aus einem minimalen CGI-Programm und einem Dämon für die Auslieferung der eigentlichen HTML-Seiten.

Im Gegensatz zu vielen anderen Webmailern arbeitet SqWebMail auf der Dateisystemebene und verbindet sich nicht mit einem vorhandenen POP- bzw. IMAP-Server. Häufig wird SqWebMail aber durch eine solche Lösung ersetzt.

10.1 Kalender

Die Kalenderfunktionen werden in der Konfigurationsdatei `calendarmode` festgelegt. Diese sind aktiviert, wenn die Datei die Werte `local` (lokaler Modus) oder `net` (Groupware-Modus) enthält.

11 courierlm

Auf den Mailinglistenserver aus dem Courierpaket möchte ich an dieser Stelle nicht weiter eingehen, da er eher geringe Verbreitung erfahren hat. Statt `courierlm` können Alternativen wie `Sympa` oder `Mailman` eingesetzt werden.

12 SSL/TLS

Alle relevanten Komponenten des Courier-Mailservers erlauben die Abwicklung über mit SSL/TLS geschützten Verbindungen. Dies geschieht entweder direkt über einen speziellen Port (465 für SMTP, 993 für IMAP und 995 für POP3) oder über die STARTTLS-Erweiterung der jeweiligen Protokolle.

Durch Einsatz eines speziellen SSL/TLS-Wrappers (`couriertls`) werden keine gesonderten Programme benötigt, sondern es können dieselben wie für ungeschützte Verbindungen verwendet werden.

13 Installation

Die Installation von Courier kann direkt aus den Quellen erfolgen oder es können Debian- bzw. RPM-Pakete verwendet werden.

Die Installation aus den Quellen wird umfangreich im `INSTALL`-Dokument beschrieben, daß im Quellarchiv vorhanden ist bzw. online verfügbar ist.

Zusätzlich zu den typischen Befehlen zur Kompilierung und Installation eines Open-Source-Pakets werden im letzten Schritt die Konfigurationsdateien installiert bzw. aktualisiert:

```
./configure
make
make install
make install-configure
```

14 Weitere Informationen

<<http://www.courier-mta.org/>> Courier Homepage

<<http://www.courier-mta.org/FAQ.html>> Courier FAQ

courier-announce <<http://lists.sourceforge.net/mailman/listinfo/courier-announce>> Ankündigung
zum Courier-Mailserver

courier-users <<http://lists.sourceforge.net/mailman/listinfo/courier-users>> Mailingliste
für Courier-Mailserver

courier-imap <<http://lists.sourceforge.net/mailman/listinfo/courier-imap>> Mailingliste für
Courier-IMAP

maildrop <<http://lists.sourceforge.net/mailman/listinfo/courier-maildrop>> Mailingliste
für Maildrop

14.1 RFCs

Tabelle 4: RFCs

2095	Authentication	CRAM-MD5
2342	IMAP	NAMESPACE
2595	SSL/TLS	STARTTLS
