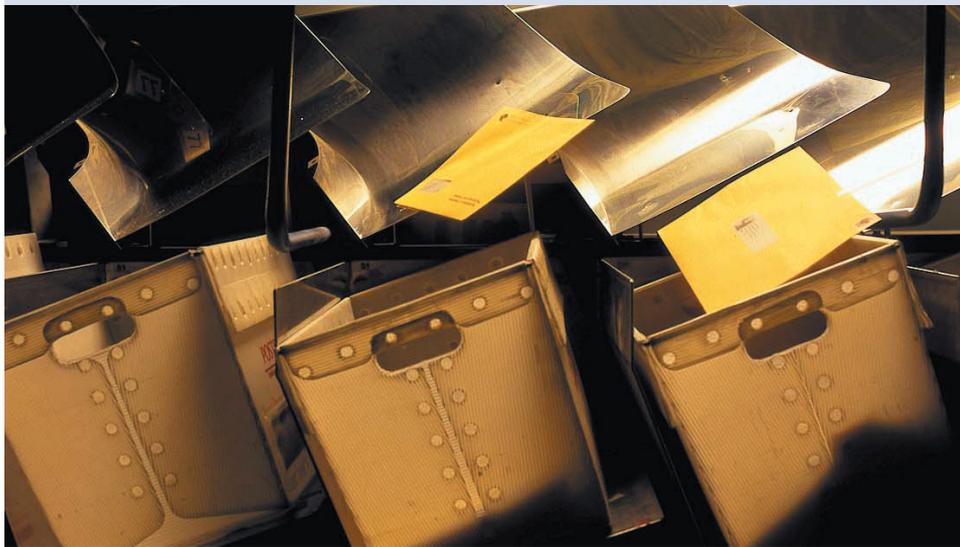


Postmoderne Mail

Ein Mailservers ist heute eine Synthese aus MTA, IMAP- und POP-Server, Authentifizierungssystem und Account-Verwaltung. Der Workshop zeigt, wie mit Postfix, Cyrus-IMAP, MySQL und dem Webfrontend Web-cyradm ein solches System entsteht. Heiner Lamprecht



Wer einen Mailservers für mehrere Domains und für eine große Nutzerschar betreiben will, stößt schnell an die Grenzen des klassischen Mail-Setups unter Linux. Für alle E-Mail-User eigene Shellaccounts anlegen bläht die Anzahl der Benutzer im System unnötig auf, inklusive der Sicherheitsrisiken, die man sich dabei einhandelt.

Ein Mailservers mit eigener, vom System getrennter Benutzer- und Adressverwaltung sollte es also schon sein, am besten gleich mit einem komfortablen Webfrontend. Unter Linux stehen viele Varianten zur Wahl, ein solches System aufzusetzen, dieser Artikel stellt eine besonders leistungsfähige vor.

Das Team

Diese Serverkonfiguration enthält als zentralen Baustein eine MySQL-Datenbank, die alle wichtigen Informationen über die Nutzer, die E-Mail-Adressen und die Domains auf dem Mailservers speichert. Alle anderen Programme ho-

len sich die benötigten Informationen aus der Datenbank.

Für das Senden und Empfangen von Mails bietet sich Postfix [1] an, ein einfach zu administrierender SMTP-Server, der mit hoher Performance und Stabilität glänzt. Anders als zum Beispiel QMail enthält Postfix eine native Unterstützung von MySQL. Zwar lässt sich auch QMail an MySQL anbinden [2], aber die offiziellen Quellen enthalten diese Funktionen bislang nicht. Im produktiven Einsatz können daraus Problemen entstehen, wenn das Einspielen von Sicherheitsupdates an den selbst gepatchten Quellen scheitert.

Die Verteilung der Post über POP und IMAP übernimmt Cyrus-IMAP [3] von der Carnegie Mellon University. Anders als viele andere IMAP-Server benutzt Cyrus-IMAP nicht die Standard-Postfächer, sondern verwaltet die Mails in einem eigenen Verzeichnisbaum. Dort liegt jede Mail als eigene Datei, was die Sicherheit zum Beispiel im Falle eines Dateisystemfehlers erhöht. Auch der Zu-

griff auf einzelne Mails ist dadurch schneller, zumal Cyrus-IMAP eine eigene Datenbank mit Statusinformationen zu den einzelnen Mails pflegt. Tatsächlich gilt Cyrus-IMAP als der zur Zeit schnellste IMAP-Server auf dem Markt, besonders bei hoher Last.

Cyrus-IMAP ist dafür konzipiert, eine eigene Nutzerdatenbank zu pflegen. Dadurch lassen sich die Mail-Nutzer von denen mit Shellzugriff auf dem Server leicht trennen. Selbst bei Nutzern mit Shellaccount kann das Shell-Passwort vom Mail-Passwort getrennt werden. Angesichts der Tatsache, dass POP und IMAP die Passwörter per se unverschlüsselt durchs Netz schicken, ein wichtiger Sicherheitsaspekt.

Sicherheit mit SASL

Die Authentifizierung der Nutzer erledigt Cyrus-SASL [4] (Simple Authentication and Security Layer). SASL beantwortet Authentifizierungsanfragen von beliebigen Clients. Im hier vorgestellten Setup überprüft es die Passwörter mit Hilfe des PAM-MySQL-Moduls [5]. Prinzipiell können Postfix und Cyrus-IMAP die Nutzer- und Domaininformationen auch von einem LDAP-Server beziehen, was jedoch etwas aufwändiger ist.

Abbildung 1 illustriert, wie die verschiedenen Programme für den Empfang und das Verschicken von Mail zusammenspielen. Empfängt Postfix eine E-Mail, prüft es zuerst in der Datenbank, ob es für die Domain zuständig ist und ob die Empfängeradresse existiert. Erst dann nimmt es die Mail an und übergibt sie, sofern der Administrator keine externe Weiterleitung festgelegt hat, lokal an Cyrus-IMAP. Dieser sortiert sie in das ent-

sprechende Postfach ein. Der Empfänger holt seine Post über POP3 oder IMAP ab, auf Wunsch auch SSL-verschlüsselt. Cyrus-SASL, das über PAM auf die Datenbank zugreift, kümmert sich um die Authentifizierung.

Um Mails zu versenden, muss sich der Nutzer gegenüber Postfix authentifizieren. Auch hier prüft Postfix anhand der Datenbank, ob er das überhaupt darf, und verhindert so unerlaubtes Relaying über den Server. Bei ausgehenden Mails liest Postfix die Informationen der »virtual«- und »alias«-Tabellen aus der Datenbank, um eventuell die Absenderadressen zu verändern.

Installation

Als Basissystem dient für diesen Artikel eine Standardinstallation von Suse 9.0, die Schritte bis zum vollständigen Server sind aber leicht auf andere Versionen und Distributionen übertragbar. Suse Linux enthält die meisten Pakete bereits. Nur Postfix ist neu zu übersetzen, da die von Suse gelieferte Version keine MySQL-Datenbank unterstützt.

Im ersten Schritt installiert man die Datenbank. Zusätzlich sind auch die normalerweise nicht mitinstallierten Devel-Pakete nötig. Da die Datenbank unter anderem Nutzernamen und verschlüsselte Passwörter enthält, darf sie nur von »localhost« erreichbar sein. Hierzu dient der Parameter »--bind-address = 127.0.0.1« im Startskript »/etc/init.d/mysql« – nach dieser Änderung ist natürlich ein Neustart von MySQL fällig.

Auch OpenSSL [6] ist in normalen Distributionen enthalten. Cyrus-IMAP und Cyrus-SASL brauchen die Berkeley DB [7], und zwar mindestens Version 4.0. Diese schlichte Embedded-Datenbank, die viele Systemtools intern nutzen, gehört unter Linux zur Grundausstattung. Suse 9.0 liefert passende Versionen der drei Programme mit. Debian-Systeme

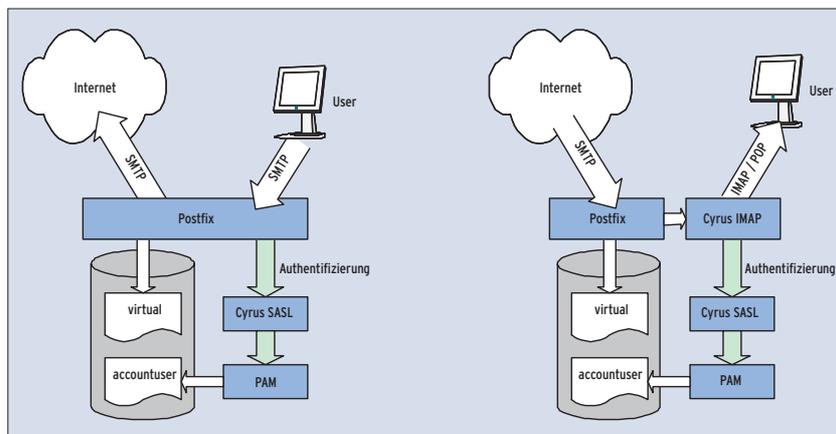


Abbildung 1: Für das Verschicken von E-Mail (links) muss sich der User authentifizieren. Das erledigt Cyrus-SASL über PAM, das die Daten aus einer MySQL-Datenbank bezieht. Ebenfalls über die Datenbank prüft Postfix bei eingelieferten Mails, ob der Server für die Domain zuständig ist, und übergibt die Mail an Cyrus-IMAP (rechts). Wieder läuft die Authentifizierung über Cyrus-SASL, PAM und MySQL.

enthalten oft noch eine ältere Berkeley DB – dann ist ein Update fällig. Cyrus-IMAP und Cyrus-SASL sind dann auch neu zu übersetzen, da sie genau jene Version der Berkeley DB erwarten, mit der sie kompiliert wurden.

Listings 1 und 2 zeigen die notwendigen Schritte. Wer die Programme selbst übersetzt, muss auch das System passend konfigurieren. Hierzu gehört, einen eigen-

nen Benutzer »cyrus« anzulegen. Normalerweise haben Daemons eine UID unter 100, Suse-Systeme verwenden für »cyrus« standardmäßig die 96. Der User muss zur Gruppe »mail« gehören. Außerdem muss der Administrator noch ein entsprechendes Start- und Stopp-Skript in »/etc/init.d/« anlegen. PAM (Pluggable Authentication Modules) [8] gehören heutzutage zum Stan-

Listing 1: Kompilieren von Cyrus-SASL

```

01 tar -xvzf cyrus-sasl-2.1.18.tar.gz --with-openssl=/usr/local/ssl
02 cd cyrus-sasl-2.1.18 --with-plugindir=/usr/local/lib/sasl2
03 ./configure --enable-anon --enable-plain 04 su ; make && make install
--enable-login --disable-krb4 --disable-otp 05 mkdir -p /var/run/saslauthd
--disable-cram --disable-digest 06 cd saslauthd
--with-saslauthd=/var/run/saslauthd 07 make testsaslauthd
--with-pam=/lib/security --with-dblib=berkeley 08 cp testsaslauthd /usr/local/bin
--with-bdb-libdir=/usr/local/db/lib 09 echo /usr/local/lib/sasl2 >> /etc/ld.so.conf
--with-bdb-incdir=/usr/local/db/include 10 ldconfig
  
```

Listing 2: Kompilieren von Cyrus-IMAP

```

01 tar -xvzf cyrus-imapd-2.2.3.tar.gz --with-bdb-incdir=/usr/local/db/include
02 cd cyrus-imapd-2.2.3 --with-openssl=/usr/local/ssl --without-ucdsnmp
03 ./configure --with-sasl=/usr/local/lib 04 make depend
--with-perl --with-auth-unix 05 su ; make && make install
--with-dbdir=/usr/local/db 06 su - cyrus
--with-bdb-libdir=/usr/local/db/lib 07 /usr/local/cyrus-imapd-2.2.3/tools/mkimap
  
```

dardumfang jeder Linux-Distribution. Es genügt, das MySQL-Modul [5] nachzuinstallieren oder zu kompilieren. Wer sein MySQL selbst übersetzt, muss unter Umständen im Makefile die Pfade anpassen. Pam_mysql kommt ohne Configure-Skript daher, sodass ein Aufruf von »make« genügt. Das fertige Modul kopiert der Administrator anschließend nach »/lib/security«. Eventuell muss er noch mit »ln -s /tmp/mysql.sock/ var/lib/mysql/mysql.sock« einen Symlink für den MySQL-Socket anlegen.

Postfix ist mittlerweile in vielen Distributionen Standard-MTA, die notwendige MySQL-Anbindung fehlt jedoch in der Regel. Ob sie enthalten ist, zeigt der Befehl »postconf -m«. Fehlt die Angabe »mysql«, ist Postfix neu zu übersetzen. Da die meisten Paketverwaltungen zwingend einen MTA verlangen, sorgt man dafür, dass irgendein Postfix im System ist. Die neu kompilierte Version lässt sich bedenkenlos über die Paketversion installieren. Der Aufruf

```
make makefiles 'CCARGS=-DHAS_MYSQL -I/usr/2
include/mysql -DUSE_SASL_AUTH -I/usr/2
include/sasl' 'AUXLIBS=-L/usr/lib/mysql2
-lmysqlclient -lz -lm -lsasl2'
```

erzeugt die passenden Makefiles, ein »make«-Aufruf startet den Kompilierungsvorgang. »make install« stellt diverse Fragen. In der Regel ist der Defaultwert eine gute Wahl.

Listing 3: »/etc/pam.d/imap«

```
01 auth sufficient pam_mysql.so user=mailadmin passwd=geheim
host=localhost db=mail table=accountuser
usercolumn=username passwdcolumn=password crypt=1
logtable=log logmsgcolumn=msg logusercolumn=user
loghostcolumn=host logpidcolumn=pid logtimecolumn=time
02 account required pam_mysql.so user=mailadmin
passwd=geheim host=localhost db=mail table=accountuser
usercolumn=username passwdcolumn=password crypt=1
logtable=log logmsgcolumn=msg logusercolumn=user
loghostcolumn=host logpidcolumn=pid logtimecolumn=time
```

Listing 4: »/etc/postfix/main.cf«

```
01 smtpd_sasl_auth_enable = yes
02 smtpd_sasl_security_options = noanonymous
03 broken_sasl_auth_clients = yes
04 smtpd_recipient_restrictions = permit_sasl_authenticated,
permit_mynetworks, reject_unauth_destination
05 mailbox_transport = cyrus
06 mydestination = mysql:/etc/postfix/mysql-mydestination.cf
07 virtual_alias_maps = mysql:/etc/postfix/mysql-virtual.cf
08 sender_canonical_maps = mysql:/etc/postfix/
mysql-canonical.cf
```

Wer möchte, konfiguriert Cyrus-IMAP komplett per Kommandozeile. Komfortabler geht es jedoch mit dem Webfrontend Web-cyradm [9]. Zum Installieren reicht es, das Paket auszupacken und an eine beliebige Stelle unterhalb des Document-Verzeichnisses des Webservers zu kopieren. Zusätzlich ist mit »touch /var/log/web-cyradm.log« eine Logdatei anzulegen und dem passenden User, zum Beispiel »nobody«, zuzuweisen.

Konfiguration

Sobald alle benötigten Programme installiert sind, beginnt die eigentliche Konfiguration. Im ersten Schritt legt der Admin die Datenbank an. Web-cyradm bringt dazu zwei SQL-Skripte mit. Das Skript »insertuser_mysql.sql« erzeugt die benötigten Nutzer für die Datenbank sowie die leere Datenbank. Vor dem Aufruf sind auf jeden Fall noch die Passwörter im Skript zu ändern. Dann folgt:

```
/usr/bin/mysql -u root -p < /srv/www/2
htdocs/web-cyradm/scripts/insertuser2
_mysql.sql
```

Das Skript »create_mysql.sql« erzeugt alle Tabellen innerhalb der Datenbank:

```
/usr/bin/mysql mail -u mailadmin -p < 2
/srv/www/htdocs/web-cyradm/scripts/2
create_mysql.sql
```

Als Nächstes sind die Konfigurationseinstellungen für PAM in der Datei »/etc/pam.d/imap« an der Reihe (siehe Listing 3). Wer die Authentifizierungsfunktion auch für die anderen Services nutzen will, kopiert die Datei anschließend dreimal:

```
cp /etc/pam.d/imap /etc/pam.d/pop
cp /etc/pam.d/imap /etc/pam.d/sieve
cp /etc/pam.d/imap /etc/pam.d/smt
```

Postfix

Postfix wird über »/etc/postfix/main.cf« konfiguriert. Diese Datei legt unter anderem fest, welche Datenquellen der MTA für die einzelnen so genannten Lookup Tables verwendet. In diesen Tabellen stehen die Einstellungen für Postfächer, Weiterleitungen, Umleitungen, Zugriffskontrollen und Ähnliches. Postfix kennt verschiedene Typen von Quellen für die einzelnen Tabellen, die es beliebig kombinieren kann. Wer mehr über die Bedeutung der rund 300 verschiedenen Parameter erfahren möchte, sollte einen Blick in das Postfix-Buch von Peer Heinlein [10] werfen.

Listing 4 zeigt einen Ausschnitt der »main.cf« mit den für dieses Beispiel wichtigen Parametern. Die Zeilen 1 bis 3 steuern die SMTP-Authentifizierung. Damit sie funktioniert, muss der Adminis-

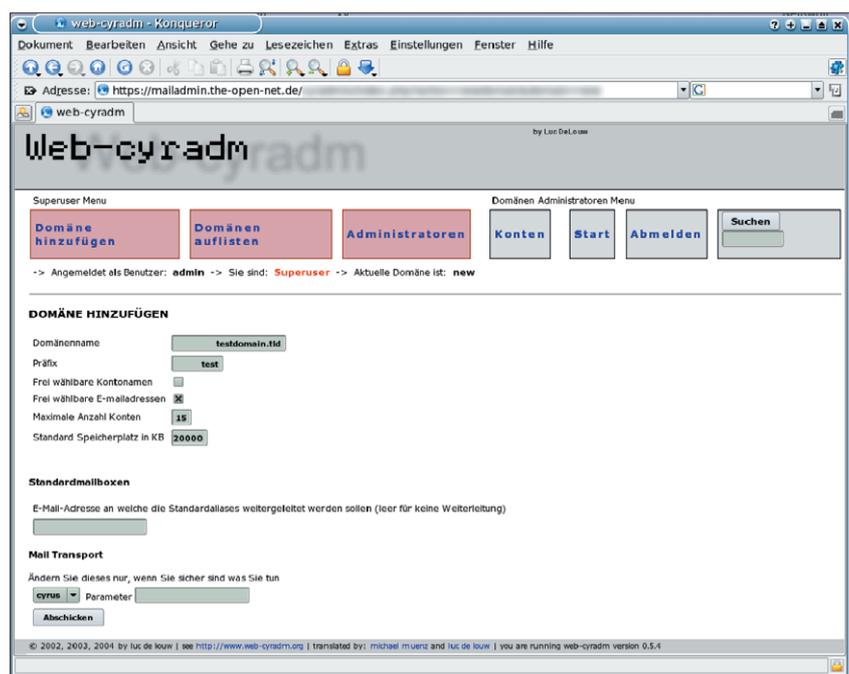


Abbildung 2: Der Dialog für die Einrichtung einer neuen Domain. Das Frontend Web-cyradm macht es möglich, Domains komfortabel zu verwalten.

trator außerdem die Datei »/usr/lib/sasl2/smtpd.conf« anlegen. Sie enthält nur zwei Zeilen:

```
pwcheck_method: saslauthd
mech_list: plain login
```

Der Parameter »permit_sasl_authenticated« in Zeile 4 in [Listing 4](#) sorgt dafür, dass nur per SASL authentifizierte Benutzer über den Server Mails versenden dürfen. Ein unautorisiertes Versenden unterbindet der Parameter »reject_unauth_destination«. Damit ist sichergestellt, dass der Server kein offenes Relay ist, das Spammer missbrauchen könnten. Zeile 5 weist Postfix an, E-Mails lokal über Cyrus-IMAP zu verteilen.

Datenbank-Zugriff

Die restlichen Zeilen legen fest, welche Konfigurationsdateien Postfix für den Zugriff auf die Datenbank verwenden soll. Der Aufbau dieser Dateien ist immer derselbe, lediglich die Angaben über die Tabellen und Spalten ändern sich. [Listing 5a](#) zeigt eine vollständige Datei »mysql-canonical.cf«, [Listings 5b](#) und

[5c](#) enthalten nur die davon abweichenden Zeilen der übrigen Dateien.

Cyrus-IMAP

Zur Konfiguration von Cyrus-IMAP dient die Datei »/etc/imapd.conf« (siehe [Listing 6](#)). Die Zeile 4 ist auskommentiert, um zu verhindern, dass Admins sich von außen einloggen. Um lokalen Admin-Zugriff zu erlauben, legt man eine gleichlautende Datei »/etc/imapd-local.conf« zusätzlich an und entfernt darin das Kommentarzeichen in Zeile 4. In Zeile 8 muss der vollständige Hostname des Servers stehen.

Zeile 21 legt fest, auf welche Art Cyrus die Benutzernamen bilden soll. Ist die Zeile auskommentiert oder der Wert auf »no« gesetzt, nummeriert es die User einfach durch. Alternativ lassen sich die Namen aber auch nach dem Schema »user.domain.tld« zusammensetzen. Soll später ein Webmail-Frontend wie Squirrelmail [\[11\]](#) zum Einsatz kommen, darf der Wert nicht auf »yes« stehen. Andernfalls kann Squirrelmail verschiedene Mailordner nicht anlegen. ▶

Listing 5a: »/etc/postfix/mysql-canonical.cf«

```
01 # user name and password to log into the mysql server
02 hosts = localhost
03 user = mailadmin
04 password = geheim
05 # database name on the servers
06 dbname = mail
07 # table name and columns
08 table = virtual
09 select_field = alias
10 where_field = username
11 # return the first match only
12 additional_conditions = and status = '1' limit 1
```

Listing 5b: »mysql-virtual.cf«

```
01 # table name and columns
02 table = virtual
03 select_field = dest
04 where_field = alias
05 additional_conditions = and status = '1'
```

Listing 5c: »mysql-mydestination.conf«

```
01 # table name and columns
02 table = domain
03 select_field = domain_name
04 where_field = domain_name
```

Listing 6: »/etc/imapd.conf«

```
01 postmaster: postmaster
02 configdirectory: /var/lib/imap
03 partition-default: /var/spool/imap
04 # admins: cyrus # no admins!
05 allowanonymouslogin: no
06 allowplaintext: yes
07 sasl_mech_list: PLAIN
08 servername: test-server.tld
09 autocretequota: 10000
10 reject8bit: no
11 quotawarn: 90
12 timeout: 30
13 poptimeout: 10
14 dracinterval: 0
15 drachost: localhost
16 sasl_pwcheck_method: saslauthd
17 sieve_dir: /usr/sieve
18 sendmail: /usr/sbin/sendmail
19 sieve_maxscriptsize: 32
20 sieve_maxscripts: 5
21 # unixhierarchyp: yes
```

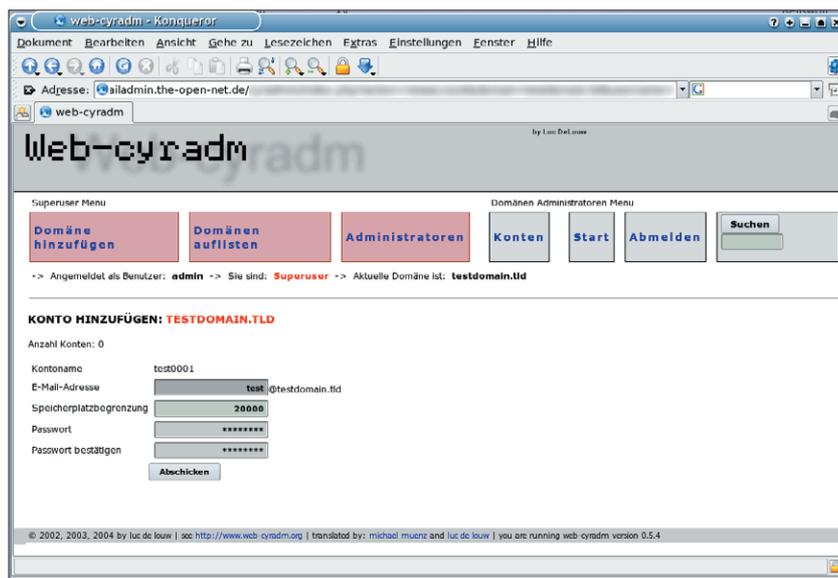


Abbildung 3: Per Browser lassen sich in Web-cyradm bequem neue Mailaccounts einrichten.

Für die TLS/SSL-Verschlüsselung legt der Admin als Nächstes ein Zertifikat an (Listing 7). Das ist allerdings von keiner anerkannten Zertifizierungsstelle unterzeichnet. Manche Mailclients zeigen daher eine Warnung an, die man jedoch ignorieren kann. Das Zertifikat dient ja nicht zur Identifizierung des Servers, sondern zur Verschlüsselung. Wer möchte, kann aber auch den Fingerprint des Zertifikats auf seiner Website veröffentlichen, damit die Benutzer es überprüfen können.

Die Datei »/etc/cyrus.conf« steuert den Master-Prozess von Cyrus. Sie legt fest, in welchen Situationen der IMAP-Daemon welche Konfigurationsdatei verwenden soll. Hier erfolgt auch die erwähnte Unterscheidung zwischen lokalem Zugriff, der auch dem Admin-User »cyrus« erlaubt ist, und dem Zugriff von außen. In Listing 8 muss die IP-Adresse 192.168.0.1 durch die externe IP-Adresse des Servers ersetzt werden. Außerdem

Listing 7: Anlegen eines OpenSSL-Zertifikats

```
01 openssl req -new -nodes -out req.pem -keyout key.pem
02 openssl rsa -in key.pem -out new.key.pem
03 openssl x509 -in req.pem -out ca-cert -req -signkey
   new.key.pem -days 999
04 mkdir /var/lib/imap
05 mv new.key.pem /var/lib/imap/server.pem
06 cat ca-cert >> /var/lib/imap/server.pem
07 chown cyrus:mail /var/lib/imap/server.pem
08 chmod 600 /var/lib/imap/server.pem
09 echo tls_ca_file: /var/lib/imap/server.pem >>
   /etc/imapd.conf
10 echo tls_cert_file: /var/lib/imap/server.pem >>
   /etc/imapd.conf
11 echo tls_key_file: /var/lib/imap/server.pem >>
   /etc/imapd.conf
```

Listing 8: »/etc/cyrus.conf«

```
01 START {
02   # do not delete this entry!
03   recover      cmd="ctl_cyrusdb -r"
04 }
05 # UNIX sockets start with a slash and are put into /var/lib/imap/socket
06 SERVICES {
07   # add or remove based on preferences
08   imap         cmd="imapd" listen="192.168.0.1:imap" prefork=0
09   imaplocal    cmd="imapd -C /etc/imapd-local.conf" listen="127.0.0.1:imap"
10   prefork=0
11   imaps        cmd="imapd -s" listen="192.168.0.1:imaps" prefork=0
12   imapslocal   cmd="imapd -C /etc/imapd-local.conf" listen="127.0.0.1:imaps"
13   prefork=0
14   pop3         cmd="pop3d" listen="pop3" prefork=0
15   pop3s        cmd="pop3d -s" listen="pop3s" prefork=0
16   sieve        cmd="timsieved" listen="192.168.0.1:sieve" prefork=0
17   sievelocal   cmd="timsieved -C /etc/imapd-local.conf
18               listen="127.0.0.1:sieve"
19   prefork=0
19   # at least one LMTP is required for delivery
20   lmtpunix     cmd="lmtpd" listen="/var/lib/imap/socket/lmtp" prefork=0
21 }
22 EVENTS {
23   # this is required
24   checkpoint   cmd="ctl_cyrusdb -c" period=30
25   # this is only necessary if using duplicate delivery suppression
26   delprune     cmd="ctl_deliver -E 3" period=1440
27   # this is only necessary if caching TLS sessions
28   tlsprune     cmd="tls_prune" period=1440
29 }
```

ist wichtig, dass die Zeile »lmtpunix« den richtigen Pfad enthält.

Nun kann der Admin den SASL- und IMAP-Daemon starten. Mit dem Befehl

```
saslpasswd2 -c cyrus
```

legt er den ersten IMAP-Nutzer an, den Web-cyradm später beim Zugriff auf Cyrus-IMAP verwendet. Bei der Passwortanfrage »saslpasswd2« sollte er das gleiche Passwort angeben, das er vorher in der letzten Zeile von »create_mysql.sql« eingetragen hat. Mit dem Aufruf von »cyradm« lässt sich das Passwort auch gleich ausprobieren. »cyradm« authentifiziert gegen den SASL- und IMAP-Daemon, die also beide laufen müssen:

```
cyradm --user cyrus --server localhost
--auth plain
IMAP Password:
localhost>
```

Im letzten Konfigurationsschritt richtet der Administrator Web-cyradm ein. In dem Unterverzeichnis »config« von Web-cyradm liegt bereits eine allgemeine Konfigurationsdatei »conf.php.dist«, die er in »conf.php« umbenennt. In ihr legt er jetzt die Angaben für das Einloggen beim Cyrus-IMAP-Server fest. Zurzeit kann Web-cyradm nicht über eine verschlüsselte Verbindung auf den IMAP-Server zugreifen. Wenn beide Systeme aber auf demselben Server laufen, ist dies kein Problem mehr. Anschließend wird die Datenbankverbindung in der Datei angegeben.

Web-cyradm bietet über die Variable »\$CRYPT« mehrere Möglichkeiten der Passwortverschlüsselung. Der sinnvollste Wert hierfür ist »crypt«. Dann verwen-

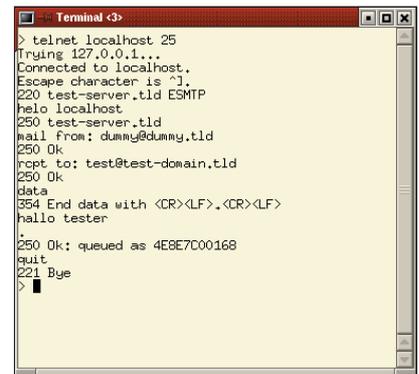


Abbildung 4: Testen des Mailserver mit Telnet.

det Web-cyradm die gleiche Verschlüsselung wie das Shadow-Passwortsystem. Als Letztes bestimmt der Administrator, wie Web-cyradm die Nutzernamen vergeben soll. Wer bei der Einrichtung der »/etc/imapd.conf« den Wert »unixhierarchie« auf »yes« gesetzt hat, sollte nun die Variable »DOMAIN_AS_PREFIX« auf »1« setzen.

Los geht's

Die Konfiguration ist abgeschlossen, nun lassen sich MySQL, Apache, Postfix, Cyrus-IMAP und der SASL-Daemon über die Skripte in »/etc/init.d« starten. Der Befehl »netstat -an | grep LISTEN« prüft, ob sie korrekt laufen. Die Ports, 25, 80, 110, 143, 993 und 995 sollten von außen erreichbar sein, Port 3306 dagegen möglichst nur vom Server selbst, also über 127.0.0.1. Sieht alles gut aus, startet der Admin als Nächstes einen Browser und ruft die Web-cyradm-Einstiegsseite auf. Dort loggt er sich als »admin« mit dem zuvor in »create_mysql.sql« gesetzten Passwort ein.



Abbildung 5a: Zum Testen des neu eingerichteten Mailservers dient KMail, hier der Reiter mit den Account-Einstellungen für ein IMAP-Postfach. »Benutzer«, »Passwort« und »Server« sollten die passenden Daten enthalten.

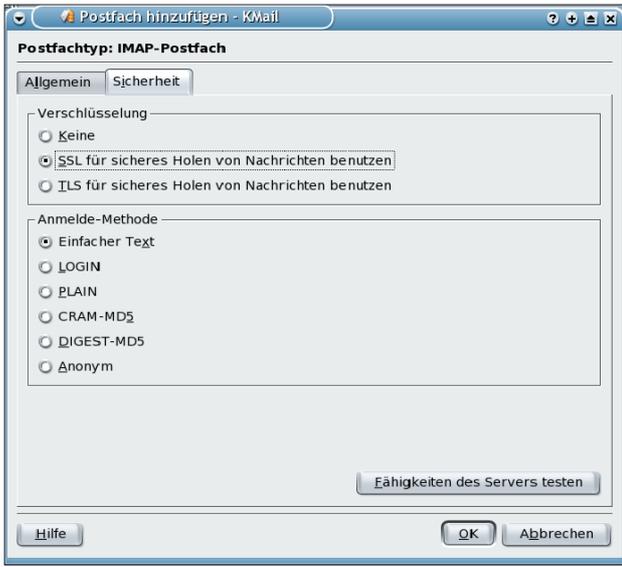


Abbildung 5b: Der Reiter »Sicherheit« führt zu den Einstellungen für SSL und die verwendete Login-Methode. Über »Fähigkeiten des Servers testen« prüft KMail selbstständig, welche Methoden der Mailserver unterstützt.

Anschließend lassen sich hier nach beliebigen Domains und zugehörigen E-Mail-Adressen konfigurieren (Abbildung 2 und 3). Auch für die Weiterleitungen ist Web-cyradm zuständig. Beim Anlegen der Domains ist darauf zu achten, dass diese auch tatsächlich zu dem jeweiligen Server gehören. Wer nur testen will, trägt die Domains kurzfristig in »/etc/hosts« ein, damit eventuelle Testmails nichts nach draußen gelangen. Wer den Wartungsaufwand für den Admin so gering wie möglich halten möchte, richtet weitere so genannte Domain-Administratoren ein: Diese dürfen eine oder mehrere Domains komplett verwalten, aber keine neuen Domains und User einrichten.

Testlauf

Nachdem der Administrator die ersten Testdomains und -Adressen angelegt hat, sollte er über einen Mailclient oder einfacher noch mit Telnet prüfen, ob Postfix auch Mails für die Adressen an-

nimmt. **Abbildung 4** zeigt eine solche Verbindung. Der Server selbst heißt dabei »test-server.tld«, die virtuelle Domain ist »test-domain.tld«.

Wenn statt der Rückmeldung in Zeile 11 etwas anderes erscheint, zum Beispiel

```
451 <test@test-domain.tld>: 2
Temporary lookup failure
```

dann kann Postfix nicht auf die Datenbank zugreifen. Entweder ist MySQL gar nicht gestartet oder die Zugriffsrechte sind falsch gesetzt oder in einer der MySQL-Konfigurationsdateien in »/etc/postfix« stehen falsche Angaben. Bei allen Problemen mit Postfix lohnt sich ein Blick in die Logdatei »/var/log/mail«. Hier stehen meist genauere Angaben darüber, was falsch gelaufen ist. Zum Abrufen der soeben erfolgreich gesendeten Mail lässt sich jeder beliebige Mailclient nutzen, wahlweise über POP3 oder IMAP. Die **Abbildungen 5a und 5b** zeigen die passenden Einstellungen für KMail. Läuft beim Test alles gut, ist der Mailserver einsatzbereit. (eba) ■

Infos

- [1] Postfix: [<http://www.postfix.org>]
- Peer Heinlein, „Selbstverteidigungskurs“: Linux-Magazin 12/02, S. 52
- [2] QMail/MySQL: [<http://iain.cx/qmail/mysql/>]
- [3] Cyrus-IMAP: [<http://asg.web.cmu.edu/cyrus/imapd/>]
- [4] SASL: [<http://asg.web.cmu.edu/sasl/>]
- [5] PAM-MySQL: [<http://pam-mysql.sf.net>]
- [6] OpenSSL: [<http://www.openssl.org>]
- [7] DBM: [<http://www.sleepycat.com>]
- [8] Linux-PAM: [<http://www.kernel.org/pub/linux/libs/pam/>] und Dirk. v. Suchodoletz, M. Walter, „Alles über PAM“: Linux-Magazin 05/04, S. 38
- [9] Webfrontend für Cyrus: [<http://www.web-cyradm.org>]
- [10] Postfix-Buch: [<http://www.postfixbuch.de>]
- [11] Squirrelmail: [<http://www.squirrelmail.org>]

Der Autor

Heiner Lamprecht arbeitet als Produktmanager bei der Barco Orthogon AG. Mit der Firma Theopen-net bietet er Internet-basierte Dienstleistungen für Firmen und Organisationen an.