LDAP, Postfix, TLS, Procmail, SpamAssassin & Courier IMAP

Simon Dassow janus@errornet.de

04-06-2003

Inhaltsverzeichnis

1 Einleitung **3**

2 Installation **4**
2.1 LDAP 4
2.2 Postfix 4
2.3 Procmail 5
2.4 SpamAssassin 6
2.5 Courier IMAP 6

3 Konfiguration **7**
3.1 LDAP 7
3.2 Postfix 9
3.3 Cyrus SASL 11
3.4 Courier IMAP 12

1 Einleitung

Postfix - Ein (inzwischen) recht verbreiteter Ersatz für Sendmail. Das Postfix-Entwicklerteam beschreibt Postfix in etwa so: “Postfix versucht Schnelligkeit, einfache Administration und Sicherheit zu verbinden und trotzdem so kompatibel zu Sendmail zu bleiben um vorhandene Benutzer nicht zu verärgern. Trotz des Sendmail-artigem Äußeren ist es intern sehr unterschiedlich.” Diese nette Beschreibung läßt auf einiges hoffen...

LDAP - Leightweight Directory Access Protocol, ein Verzeichnis (-dienst) der als eine Weiterentwicklung von X.500 bezeichnet werden kann. Da LDAP von der Administration her unproblematisch ist und es viele geeignete Frontends gibt, setzen wir LDAP als Datenbank für unsere ganzen Email-Accounts ein.

TLS - Transport Layer Security. TLS Version 1 ist auch unter der Bezeichnung “SSL - Secure Socket Layer” bekannt. Hierbei handelt es sich - wie der Name schon sagt - um Verschlüsselung der Kommunikation. Es arbeitet mit X.509 Zertifikaten, was einiges an Möglichkeiten bietet.

Procmail - ein so genannter Mail Delivery Agent (kurt: MDA), der Mails sortieren, filtern, verschieben und mehr kann. Auch für Mailinglisten geeignet. Warum wir Procmail einsetzen bedarf wohl keiner weiteren Erklärung.

SpamAssassin - ein Mailfilter der Spam identifiziert. Er hat eine große Basis an Regeln und Tests für Mailheader und -body um Spam (auch als “unerwünschte kommerzielle Emails” bekannt) zu erkennen.

Courier IMAP - damit wir die Mails auch Remote Usern zugänglich machen können benutzen wir Courier IMAP. Das Paket bringt einen IMAPd mit sich sowie einen POP3d und beide sind in der Lage TLS zu machen, als auch LDAP.

Damit ist schon einmal die Erklärung der einzelnen Komponenten vorhanden. Nachdem ich bereits mit Sendmail, Exim und Qmail gearbeitet habe, war Postfix der letzte MTA den ich nicht getestet hatte. Als letztes hatte ich Exim im Einsatz, welcher aber Design-Fehler hat, die mich stören. Qmail hat ein ganz besonderes Problem: den Stolz des Entwicklers und einige halbherzige Patches. Sendmail hat ein ähnliches Problem wie Exim, wobei mich die - oft zitierte - komplexe Konfiguration weniger stört. Den einzigen Nachteil den ich in Postfix noch sehe, ist Cyrus SASL. Ein weiteres (an sich überflüssiges) Layer zwischen Mailer und Datenbank, welches nur für SMTP-AUTH gebraucht wird. Sonst ist Postfix sehr angenehm. Die Konfiguration lässt sich im Nachhinein auch noch von nicht so bewanderten Admins lesen (und ggf. ändern) und der modulare Aufbau sorgt - ähnlich wie bei Qmail - für eine gewisse Sicherheit.

Ich habe die Installation sowohl auf OpenBSD gemacht, als auch auf einem Gentoo Linux, ich dokumentiere hier aber nur für OpenBSD, da dies mein absolut favorisiertes Betriebssystem ist und da sich die Konfiguration nur in wenigen Punkten unterscheidet.

Über Feedback bin ich jederzeit dankbar.

2 Installation

Installieren wir zunächst alle benötigten Komponenten und gehen danach an deren Konfiguration.

Grundlegen dazu sagen muss ich noch:

Der Benutzer der die Maildirs verwaltet ist “vmail”:

```
# groupadd -g 2000 vmail
# useradd -g vmail -u 2000 -d /pool/mail -s /usr/bin/true vmail
```

und alle Maildirs liegen unterhalb von “/pool/mail”:

```
# mkdir -p /pool/mail
```

Das kann natürlich variieren, muss dann aber in den Konfiurationen entsprechend angepasst werden.

Ich habe bei mir alle wichtigen Sachen unterhalb von “/pool” liegen, z.B. sind alle Web-Accounts unter “/pool/www/domain/subdomain”. Die gleiche Struktur benutze ich auch für Mail-Accounts.

2.1 LDAP

Ich setze auf meinen Systemen OpenLDAP ein, andere LDAP-Backends sollten jedoch auch funktionieren.

Die Installation erfolgt - wie bei OpenBSD üblich - aus der Ports Collection:

```
# cd /usr/ports/databases/openldap
# make install clean
```

Jetzt kopieren wir noch die Beispiel-Konfiguration:

```
# mkdir /etc/openldap
# cd /usr/local/share/examples/openldap/
# cp -R {{ldap,slapd}.conf,schema} /etc/openldap
# chmod 600 /etc/openldap/{ldap,slapd}.conf
```

2.2 Postfix

Die Installation geschieht - wie sollte es anders sein - auch aus den Ports:

```
# cd/usr/ports/mail/postfix/stable
# env FLAVOR="pcre sasl2 ldap tls" make install clean
```

Jetzt ist das System erst einmal eine Weile damit beschäftigt die Abhängigkeiten aufzulösen, was natürlich beschleunigt werden kann, indem man folgende Packete schon vorher installiert: openldap, cyrus-sasl2 und pcre.

Wenn Postfix fertig installiert ist, ersetzen wir Sendmail durch Postfix als System-Mailer:

```
  # /usr/local/sbin/postfix-enable
```

In /etc/rc.conf müssen wir aber noch die Flags für Sendmail und syslogd anpassen.

```
sendmail_flags="-bd -q30m"
```

und

```
syslogd_flags="-a /var/spool/postfix/dev/log"
```

Am besten auch direkt den syslogd neu starten:

```
  # ps ax|grep syslog
29963 ??  Is      0:30.69 syslogd -a /var/empty/dev/log
  # kill 29963
  # syslogd -a /var/empty/dev/log -a /var/spool/postfix/dev/log
```

Da Sendmail auch einen Cronjob hat, deaktivieren wir diesen

```
  # crontab -e
```

Und die Zeile

```
*/30 * * * * /usr/sbin/sendmail -L sm-msp-queue -Ac -q
```

auskommentieren.

Jetzt verschieben wir noch die Standard-Konfigurationen und kopieren uns die wichtigen Sachen zurück:

```
  # cd /etc/postfix
  # mkdir default
  # mv * default
  # cp default/master.cf .
  # cp default/post* .
```

2.3 Procmail

Aus den Ports wieder:

```
# cd /usr/ports/mail/procmail
# make install clean
```

Zusätzlich müssen wir für unser Setup noch ein kleines Shell-Script erstellen, welches uns die Emailadresse in Local Part und Domain zerlegt und gleichzeitig die Existenz des Maildirs des Benutzers sicher stellt.

Einfach folgendes in /usr/local/bin/getmailinfo:

```
#!/bin/sh
USER=‘echo $1|awk -F@ ’{print $1}’‘
DOMAIN=‘echo $1|awk -F@ ’{print $2}’‘
MAILDIR=/pool/mail/$DOMAIN/$USER/Maildir/
if [[ ! -d $MAILDIR ]]; then
        mkdir -p $MAILDIR
fi
echo $DOMAIN
```

und ausführbar machen.

2.4 SpamAssassin

Wie immer über die Ports:

```
# cd /usr/ports/mail/p5-Mail-SpamAssassin
# make install clean
```

Hier werden noch ein paar Abhängigkeiten (Perl-Module) mit installiert.

2.5 Courier IMAP

Einfach wie immer:

```
# cd /usr/port/mail/courier-imap
# FLAVOR="no_mysql no_pgsql" make install clean
# pkg_add /usr/ports/packages/i386/All/courier-ldap-*.tgz
# pkg_add /usr/ports/packages/i386/All/courier-pop3-*.tgz
```

Komisch bei diesem Port ist, dass er trotz “no_mysql” und “no_pgsql” bei der Installation MySQL und PostgreSQL installiert. Ich habe das unterbunden indem ich in der Makefile was geändert habe, aber da gibt es bestimmt noch einen besseren Weg.

Noch die Beispiel-Konfigurationen kopieren:

```
# cp -R /usr/local/share/examples/courier-imap /etc
```

3 Konfiguration

Nun folgt die Konfiguration der einzelnen Komponenten unseres Mailsystems. Bei LDAP kann man den ersten Teil ignorieren, für den Fall dass man schon einen LDAP-Server laufen hat.

3.1 LDAP

Zunächst kopieren wir das Schema für Postfix zu den anderen:

```
  # cp mailserver.schema /etc/openldap/schema/
```

Da das Schema von diversen anderen abhängt tragen wir direkt in /etc/openldap/slapd.conf ein, dadurch ergibt sich bei mir eine Liste folgender Schemata:

```
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/mailserver.schema
```

Am Ende der Datei müssen wir noch die Basisdaten angeben, die bei mri so aussehen:

```
database        ldbm
suffix          "o=myOrg"
rootdn          "cn=Manager,o=myOrg"
rootpw          {SSHA}x+DYhErMFkh5RjcqojjTszP1mTUtZ+9q
directory       /usr/local/var/openldap-ldbm
```

Das Verzeichnis in dem die Daten liegen werden (/usr/local/var/openldap-ldbm bei mir) muss ggf. erst noch erstellt werden:

```
  # mkdir -p /usr/local/var/openldap-ldbm
```

Was bei rootpw steht ist ein SSHA-verschlüsseltes Passwort. Man kann es sich mit "slappasswd" generieren:

```
  # slappasswd
New password:
Re-enter new password:
{SSHA}x+DYhErMFkh5RjcqojjTszP1mTUtZ+9q
```

Jetzt können wir den LDAP-Server starten und ihn anschließend mit Daten "füttern":

```
# /usr/local/libexec/slapd
```

Ein LDIF mit den entsprechenden Einträgen ist wäre[1]:

```
# myOrg
dn: o=myOrg
objectClass: top
objectClass: organization
o: myOrg

# email, myOrg
dn: ou=email, o=myOrg
objectClass: top
objectClass: organizationalunit
ou: email

# test.lan, email, myOrg
dn: dc=test.lan, ou=email, o=myOrg
accountActive: TRUE
editPostmasters: TRUE
editAccounts: TRUE
objectClass: top
objectClass: mailDomain
dc: test.lan
delete: FALSE
lastChange: 111
postfixTransport: procmail:

# foo, test.lan, email, myOrg
dn: uid=foo, dc=test.lan, ou=email, o=myOrg
accountActive: TRUE
lastChange: 111
mail: foo@test.lan
objectClass: top
objectClass: mailAccount
uid: foo
delete: FALSE
homeDirectory: /pool/mail
mailbox: test.lan/foo/Maildir/

# bar, test.lan, email, myOrg
dn: name=foo, dc=test.lan, ou=email, o=myOrg
accountActive: TRUE
mail: bar@test.lan
name: bar
objectClass: top
objectClass: mailAlias
maildrop: foo@test.lan
lastChange: 1111
```

[1] ist Anhang zusammen mit den anderen Konfigurationsdateien noch einmal aufgeführt

Damit haben wir eine MailDomain (test.lan), ein MailAccount (foo@test.lan) und einen MailAlias (bar@test.lan -¿ foo@test.lan).

3.2 Postfix

Die Konfiguration von Postfix im einzelnen werde ich hier nicht erklären, sondern einfach meine Abbilden. Die meisten Sachen sind sowieso selbsterklärend. Vorher muss allerdings noch etwas in der "/etc/postfix/master.cf" geändert werden, damit TLS auch auf Port 465 funktioniert und wir müssen noch einen Transport für Procmail anlegen.

Zunächst die Zeile mit "smtps" am Anfang auskommentierten:

```
smtps     inet  n       -       -       -       -       smtpd \
-o smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
```

Dann den Transport für Procmail eintragen (einfach an das Ende der Datei):

```
procmail  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail:vmail argv=/usr/local/bin/procmail -a $recipient -a $sender -a $user
```

Nun die Haupt-Konfiguration für Postfix "/etc/postfix/main.cf":

```
#biff                   = no
debug_peer_level        = 2
#delay_warning_time     = 4

command_directory       = /usr/local/sbin
daemon_directory        = /usr/local/libexec/postfix
mailbox_command         = /usr/local/bin/proctest
queue_directory         = /var/spool/postfix

# ownership
mail_owner = postfix

# version banner
smtpd_banner = $myhostname ESMTP $mail_name


# parallel delivery
local_destination_concurrency_limit = 2
default_destination_concurrency_limit = 10

# domaine
mydomain = test.lan
# origin
myorigin = $mydomain

# network
```

```
mynetworks = 127.0.0.0/8, 192.168.100.0/24

# TLS (server side)
smtpd_tls_key_file = /etc/postfix/smtpd.key
smtpd_tls_cert_file = /etc/postfix/smtpd.crt
smtpd_tls_CAfile = /etc/postfix/ca.crt
smtpd_use_tls = yes

# TLS (client side)
smtp_tls_key_file = /etc/postfix/smtpd.key
smtp_tls_cert_file = /etc/postfix/smtpd.crt
smtp_tls_CAfile = /etc/postfix/ca.crt
smtp_use_tls = yes

smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =
smtpd_recipient_restrictions = permit_sasl_authenticated, check_relay_domains
broken_sasl_auth_clients = yes
smtp_sasl_security_options =

# Transports
transport_server_host = localhost
transport_search_base = ou=Email,o=myOrg
transport_query_filter = (&(dc=%s)(objectClass=mailDomain)(accountActive=TRUE)(delete=FALSE)
transport_result_attribute = postfixTransport
#transport_cache = yes
transport_bind = no
transport_scope = one

# Aliases
aliases_server_host = localhost
aliases_search_base = ou=Email,o=myOrg
aliases_query_filter = (&(objectClass=mailAlias)(mail=\%s)(accountActive=TRUE))
aliases_result_attribute = maildrop
aliases_bind = no
#aliases_cache = yes

# Accounts
accounts_server_host = localhost
accounts_search_base = ou=Email,o=myOrg
accounts_query_filter = (&(objectClass=mailAccount)(mail=\%s)(accountActive=TRUE)(delete=FALS
accounts_result_attribute = mailbox
accounts_bind = no
#accounts_cache = yes

accountsmap_server_host = localhost
accountsmap_search_base = ou=Email,o=myOrg
accountsmap_query_filter = (&(objectClass=mailAccount)(mail=\%s)(accountActive=TRUE)(delete=F
accountsmap_result_attribute = mail
accountsmap_bind = no
#accountsmap_cache = yes

# Transport map
```

```
transport_maps = ldap:transport
mydestination = $myhostname, localhost.$mydomain, $mydomain, mail.$mydomain, $transport_maps

# Virtual maps
virtual_maps = ldap:aliases, ldap:accountsmap

# Virtual accounts
virtual_mailbox_base = /pool/mail
virtual_mailbox_maps = ldap:accounts
virtual_minimum_uid = 2000
virtual_uid_maps = static:2000
virtual_gid_maps = static:2000

# Local accounts
local_alias_maps = hash:/etc/aliases
local_recipient_maps = $local_alias_maps unix:passwd.byname
```

Es müssen ausserdem noch die Zertifikate kopiert werden. Ich habe mein Zertifikat "smtpd.crt" genannt und der Key ist in "smtpd.key". Zusätzlich noch "ca.crt", was die Root-CA ist der "smtpd.crt" signiert hat. Diese einfach nach /etc/postfix/ kopieren.

3.3 Cyrus SASL

...wurde als Abhängigkeit von Postfix installiert, machen wir uns nun an die Konfiguration.

Wir tragen in "/usr/local/lib/sasl2/smtpd.conf" folgendes ein:

```
pwcheck_method: saslauthd
mech_list: plain login
saslauthd_path: /var/sasl2/mux
```

Damit der saslauthd auch beim booten startet tragen wir folgedes in "/etc/rc.local" ein:

```
/usr/local/sbin/saslauthd -a ldap -m /var/spool/postfix/var/sasl2/mux
```

Die sich SASL irgendwie des öfteren über das Fehlen der Datei "/etc/kerberosIV/srvtab" beschwert, hab ich sie kurzer Hand einfach erstellt:

```
  # touch /etc/kerberosIV/srvtab
```

und die Fehler waren weg.

Zusätzlich muss man im Postfix-Chroot noch den Pfad für SASL erstellen:

```
  # mkdir -p /var/spool/postfix/var/sasl2
```

Jetzt sollte man “saslauthd” starten können:

```
# /usr/local/sbin/saslauthd -a ldap -m /var/spool/postfix/var/sasl2/mux
```

3.4 Courier IMAP