

Mailserver

Der Mailserver ist nur für die lokalen Konten zu nutzen - virtuelle Nutzer wurden nicht berücksichtigt. Die Vorlage für die Konfiguration unter Debian war diese hier:

<http://www.debianadmin.com/debian-mail-server-setup-with-postfix-dovecot-sasl-squirrel-mail.html>

Da wir nach Außen mit einer IP von KabelBW zu sehen sind, werden normale Mailserver (web.de, t-online etc) unsere Mails nicht annehmen! Zur Lösung siehe: Satelittensystem!

Ubuntu

Das Aufsetzen eines Mailservers unter Ubuntu ist wesentlich einfacher als unter Debian. Wichtige Hinweise zu den Konfigurationsdateien sind aber weiterhin besser unter Debian anzusehen!

MDA und MTA: Dovecot und Postfix unter Ubuntu

Ein

```
sudo apt-get install dovecot-postfix
```

zieht postfix und dovecot an Bord und konfiguriert diese sehr ordentlich für den Serverbetrieb.

StartSSL Zertifikat einbinden

Der etwas ungewöhnliche Ort unter /etc/apache2/ssl für die Zertifikate ergibt sich bei unserem System aus der Apache Konfiguration!

Zuerst wird das Intermediate Certificate von StartSSL mit unserem eigenen Key zusammen geschoben:

```
cat kvfginfo.cert sub.class1.server.ca.pem > kvfginfo.pem
```

In der frischen Datei kvfginfo.pem kontrollieren, ob die Zertifikate hübsch untereinander liegen. Evtl. einen Zeilenumbruch einfügen oder eine Leerzeile zu viel entfernen.

Alte Version der dovecot.conf

Danach wird die /etc/dovecot/dovecot.conf angepasst:

```
ssl = yes
ssl_cert_file = /etc/apache2/ssl/kvfginfo.pem
ssl_key_file = /etc/apache2/ssl/kvfginfo.key
ssl_ca_file = /etc/apache2/ssl/ca.pem
```

Entsprechende Einträge in `/etc/dovecot/conf.d/*` müssen dann auskommentiert werden, dass diese nicht der conf Datei oben in die Quere kommen! Dann den Dovecot neu starten:

```
service dovecot restart
```

und die Logs im Auge behalten. Sollten beim Starten von Dovecot Fehlermeldungen auftauchen, die auf eine neuere Version hinweisen und verlangen, man möge die alten Conf Dateien mit Hilfe von

```
dovecot -n > dovecot-new.conf
```

konvertieren, dann lohnt sich dieser Schritt.

Neue Version der dovecot.conf

In neueren Dovecots müssen die oben angegebenen Zeilen verändert werden zu:

```
ssl_ca=</etc/apache2/ssl/ca.pem  
ssl_cert=</etc/apache2/ssl/kvfginfo.pem  
ssl_key=</etc/apache2/ssl/kvfginfo.key
```

Verbindung zu Dovecot testen

Bei Verbindungstests aus Thunderbird heraus ist zu beachten, dass dieser einige Einstellungen erst nach einem Neustart richtig verdaut. Außerdem kann es sinnvoll sein, im Thunderbird unter *Bearbeiten - Einstellungen - Erweitert - Zertifikate - Zertifikate* evtl. vorhandenen Zertifikate für den Mailserver zu löschen.

Die Verbindung von einem anderen Rechner kann leichter, eindeutiger und aussagekräftiger ohne Intervention von Mailclients wie Thunderbird für die offenen Ports getestet werden - z.B. direkt mit openssl

```
openssl s_client -connect kvfg.info:993 # für SSL/TLS  
openssl s_client -connect kvfg.info:143 # für STARTTLS
```

Hier dann auftretende Fehlermeldungen lassen sich mit eindeutigeren Ergebnissen googlen als Thunderbirdprobleme.

Postfix anpassen und testen

Jetzt `/etc/postfix/main.cf` anpassen:

```
smtpd_tls_cert_file = /etc/apache2/ssl/kvfginfo.pem  
smtpd_tls_key_file = /etc/apache2/ssl/kvfginfo.key  
smtpd_tls_CAfile = /etc/apache2/ssl/ca.pem
```

und den Postfix neu starten.

```
/etc/init.d/postfix restart
```

Die Verbindung von einem anderen Rechner aus für die offenen Ports testen - z.B. mit

```
openssl s_client -connect kvfg.info:25 -starttls smtp
```

Gute Hinweise waren hier zu finden:

<http://sandboxblog.de/startssl-zertifikat-fur-dovecot-und-postfix-verwenden/>

MUAs

mutt

Mutt ist für das Lesen der Mails auf der Konsole so oder so mit dabei. Eine Anleitung ist hier zu finden:

<http://www.mutt.org/doc/manual/>

Default ist nano - wer nen vi will, muss sich dies selbst einrichten. Hierzu im eigenen Homeverzeichnis eine Datei .muttrc anlegen und die folgende Zeile reinschreiben:

```
set editor="vim -c \"set spell spelllang=de,en\""
```

Weitere Tricks hier: <http://wiki.mutt.org/?ConfigTricks>



Wer schon einen mutt am Laufen hatte, bevor der IMAP Server installiert wurde, hat nun das Problem, dass mutt in /var/mail/user nach Mails sucht, während diese jedoch inzwischen von dovecot verwaltet werden!

Also legen wir uns eine .muttrc im eigenen Home an mit dem folgenden Eintrag:

```
set spoolfile=imap://benutzer@kvfg.info/INBOX
set folder=imap://benutzer@kvfg.info
```

Weitere Hinweise hier: <http://wiki.dovecot.org/mutt>

Squirrelmail

Wer will, kann sich jetzt noch eine Webmail Oberfläche hinzu installieren - und weil er zwar hässlich, jedoch einfach zu installieren ist, wählten wir das Eichhörnchen:

```
apt-get install squirrelmail
```

Unter Ubuntu wurde noch ein Paket installiert, das die Benutzer dazu zwingt, sich über SSL anzumelden:

```
apt-get install squirrelmail-secure-login
```

Die Basiskonfiguration von Squirrelmail kann wie folgt aufgerufen werden:

```
/usr/sbin/squirrelmail-configure
```

Damit die Weboberfläche erreichbar ist, muss der Apache davon wissen:

```
vi /etc/apache2/apache2.conf
```

und hier am Ende (oder auch am Anfang) hinzufügen:

```
Include /etc/squirrelmail/apache.conf
```

In dieser Datei kann auch der Alias so geändert werden, dass Squirrelmail auch über andere Verzeichnisaufrufe zu erreichen ist als über domain.tld/squirrelmail - in unserem Fall also über /mail

Jetzt den Apachen neu starten:

```
/etc/init.d/apache2 restart
```

Der Mailer ist nun zu erreichen und für lokale Benutzer auch zu nutzen.

Thunderbird

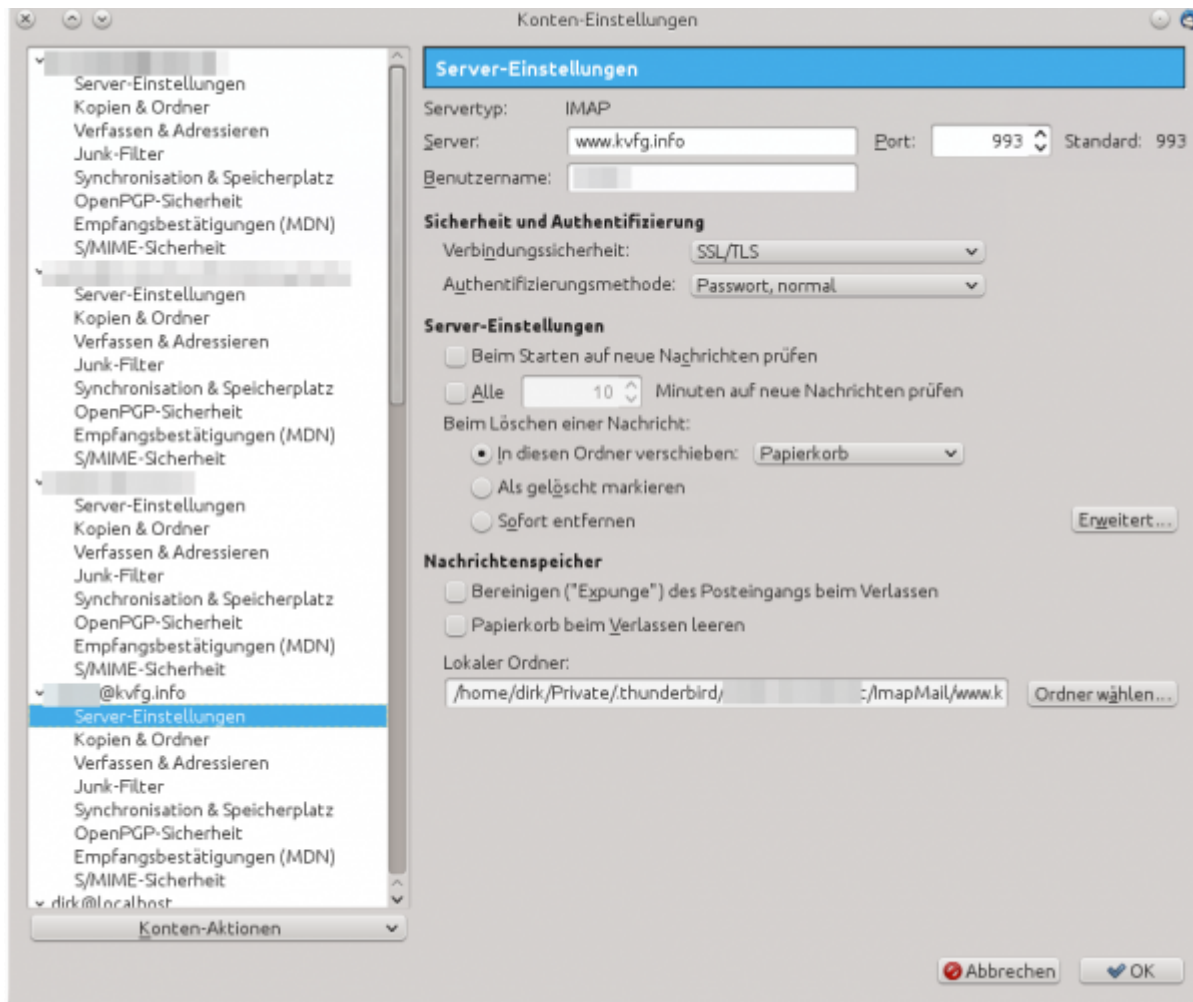
Beim Einrichten des lokalen MUAs Thunderbird ist zu beachten, dass dieser automatisch Servernamen vergibt, die wir hier nicht brauchen können. Die Einträge

```
imap.kvfg.info  
smtp.kvfg.info
```

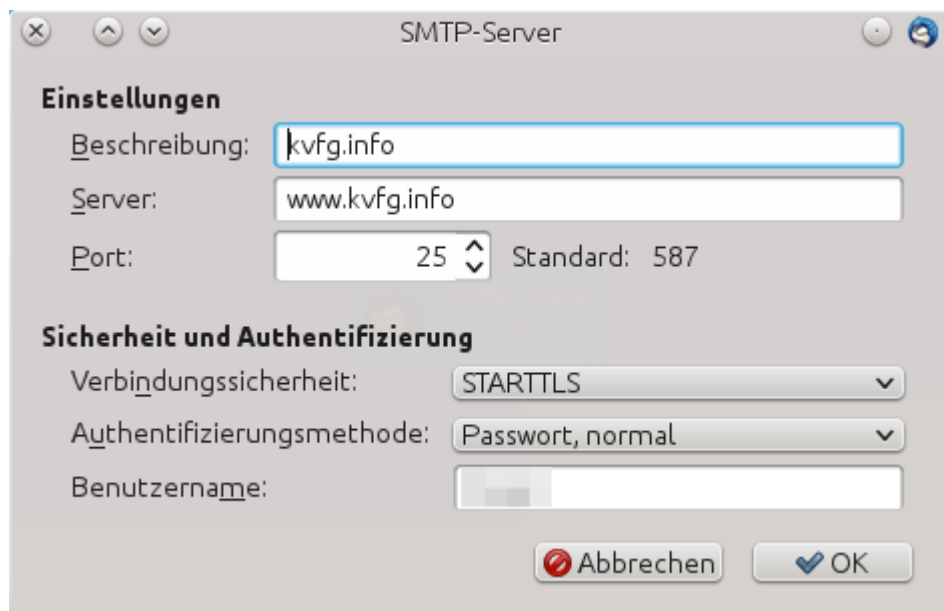
sind bei uns zu ersetzen durch

```
kvfg.info
```

Dann motzt Thunderbird auch nicht mehr wegen den Zertifikaten. Im Detail sieht das dann wie folgt aus:



Die Einstellungen im Bild oben übernehmen, um E-Mails über IMAPs auf dem Server zu lesen und diese dort zu belassen.



Die Einstellungen im Bild oben übernehmen, um E-Mails vom lokalen MUA Thunderbird an den Mailserver auf kvfg.info zu senden (und von dort aus dann weiter zum Empfänger).

Debian

Die Konfiguration unter Debian erweist sich als komplexer als unter Ubuntu. Hier der Stand von 2008.

MTA: Postfix unter Debian

Installiert ist bei Debian Systemen eigentlich exim - aber mit dem kenn ich mich nicht aus. Also zuerst der Exim raus

```
/etc/init.d/exim4 stop  
apt-get remove exim4
```

und dann ein Postfix ins System:

```
apt-get install postfix postfix-tls libsasl2-2 sasl2-bin libsasl2-modules
```

Eingegeben wurde in der Konfiguration:

```
Internet Site  
kvfg.info
```

Dann wurde die

```
/etc/postfix/main.cf
```

kontrolliert und der Postfix neu gestartet:

```
/etc/init.d/postfix restart
```

Damit die Mails kein user@www.kvfg.info tragen, sondern user@kvfg.info muss für Postfix evtl. noch die folgende Datei angepasst werden:

```
/etc/mailname
```

Ein postfix restart liest die Änderungen ein.

MDA: Dovecot unter Debian

Dann kam ein Dovecot hinzu, damit wir über POP3 und IMAP auf den Mailserver kommen:


```
apt-get install dovecot-imapd dovecot-pop3d dovecot-common
```

Die Installation wurde kontrolliert:

```
vi /etc/dovecot/dovecot.conf
```

Angepasst wurden die folgenden Zeilen - der Rest blieb:

```
protocols = imaps pop3s
disable_plaintext_auth = yes
```

Plaintext sollte kein Problem sein, wenn wir verschlüsselt mit dem Mailserver kommunizieren. Aber nur dann 

Der Dovecot wurde neu gestartet:

```
/etc/init.d/dovecot restart
```

 Keine ungesicherten Verbindungen zum Server aufbauen 

Auth unter Debian

Für die Authentifizierung wurden die folgenden Einstellungen getroffen:

```
vi /etc/postfix/main.cf
```

Hier wurde hinzugefügt:

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = kvfg.info
smtpd_recipient_restrictions =
permit_mynetworks,permit_sasl_authenticated,reject_unauth_destination
smtpd_sasl_security_options = noanonymous
```

Nachdem das Verschicken von Mails von meinem lokalen Rechner hiernach nicht funktionierte, wurden die folgenden Zeilen ergänzt:

```
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
```

Wie in der oben verlinkten Anleitung wurde nun der SASL AuthDaemon eingerichtet:

```
rm -r /var/run/saslauthd/
mkdir -p /var/spool/postfix/var/run/saslauthd
ln -s /var/spool/postfix/var/run/saslauthd /var/run
chgrp sasl /var/spool/postfix/var/run/saslauthd
adduser postfix sasl
```

 Ideal ist IMHO der Symlink nicht. Da müssen wir nochmal ran 

Auch der nächste Punkt fehlt der Anleitung, ist aber nötig:

```
vi /etc/default/saslauthd
```

und hier dann:

```
START=yes
```

setzen, damit der nach einem Reboot selbst wieder hoch kommt.

Die obige Anleitung bearbeitet nun die

```
/etc/dovecot/dovecot.conf
```

indem der folgende Codeschnipsel hinzugefügt und der auth default dann umbenannt wird:

```
auth default {
mechanisms = plain login
passdb pam {
}
userdb passwd {
}
socket listen {
client {
path = /var/spool/postfix/private/auth
mode = 0660
user = postfix
group = postfix
}
}
}
```

Ich hab gleich den auth default wie oben angepasst.

Jetzt noch alle Dienste neu starten:

```
/etc/init.d/saslauthd restart
/etc/init.d/postfix restart
/etc/init.d/dovecot restart
```

Mailserver als Satellitensystem

Man kann auch den Mailserver von Lehrerpost dazu nutzen, Mails aus Karl und Karlchen auszuliefern. Dazu wird der Postfix schon bei der Installation als Satelliten-System eingetragen.

Der SMTP-Relay-Server ist dann

```
[mail.lehrerpost.de]:587
```

Jetzt die /etc/postfix/main.cf bei TLS Parameter anpassen:

```
smtp_sasl_auth_enable = yes
smtp_sasl_security_options = noanonymous
smtp_sasl_password_maps = hash:/etc/postfix/sasl_password
```



```
smtp_tls_security_level = may
```

In die folgende Datei

```
/etc/postfix/sasl_password
```

kommen nun Benutzername und Passwort unseres Lehrerpost-Mail-Accounts

```
[mail.lehrerpost.de]:587 benutzer@domain.tld:geheim
```

Die Rechte an dieser Datei ändern:

```
chmod 600 /etc/postfix/sasl_password
```

Nun eine Datenbank für den Postfix erstellen:

```
postmap hash:/etc/postfix/sasl_password
```

und dann den Postfix neu starten:

```
/etc/init.d/postfix restart
```

oder auch mit

```
service postfix restart
```

Jetzt sollte man die Mailfunktion testen - z.B. mit

```
echo "test" | mail -s 'test' benutzer@web.de
```

... oder jedem anderen Mailkonto außerhalb.

Weitere Hinweise und Quellen: [1](#) und [2](#)

Mailserver absichern

Fail2ban kontrollieren und für den Dovecot noch die folgenden Anpassungen hinzufügen.

Eine **Filterdatei** anlegen in `/etc/fail2ban/filter.d/dovecot-pop3imap.conf`

```
[Definition]
failregex = (? : pop3-login|imap-login): .*(?:Authentication failure|Aborted
login \(auth failed|Aborted login \((tried to use disabled|Disconnected
\(auth failed|Aborted login \(\d+ authentication
attempts).*rip=(?P<host>\S*),.*
ignoreregex =
```

Dann das **Jail** anpassen:

```
[dovecot-pop3imap]
enabled = true
filter = dovecot-pop3imap
port = pop3,pop3s,imap,imaps
action = iptables-multiport[name=dovecot-pop3imap,
port="pop3,pop3s,imap,imaps", protocol=tcp]
# optionally mail notification # mail[name=dovecot-pop3imap,
dest=root@domain] # see /etc/fail2ban/action.d/ or Fail2Ban doc
logpath = /var/log/mail.log
maxretry = 10
findtime = 1200
bantime = 1200
```

Quelle: <http://wiki.dovecot.org/HowTo/Fail2Ban>

From:
<https://www.kvfg.net/wiki/> - **KvFG Wiki**

Permanent link:
<https://www.kvfg.net/wiki/doku.php?id=ag:computer:karlchen:mailserver>

Last update: **2014/11/04 17:55**

