# Debian 5.0 Lenny Webmail

Aktuelle Version Online: http://www.linuxwiki.de/debian-webmail

# Inhalt

# Vorwort

Angenommen ist ein Debian Lenny System als Standard installiert. Dies ist ein Weg wie man möglichst schnell an ein Webmail kommt auf einem Server.Ein Email Server kann man eigentlich nur auf einer statischen IP aufsetzen, und die Domain offizielle registriert ist. (Schickt doch mal eine Email an hotmail von einer DHCP Adresse aus. Da wird man gleich in eine Spam Liste eingetragen.)

Falls dieses Doku auf einem Bestehend System angewendet wird, müsst ihr zuerst alle aufgeführten aptitude install Pakete* gegen ein aptitude purge Pakete* ersetzen, weg mit dem alten. Dann müsst ihr deluser für sshd , mysql , postfix , clamav , postgrey , amavix machen. Dann müsst Ihr delgroup mysql , ssl-cert , postfix , postdrop , clamav , postgrey , amavis machen. Damit ihr halbwegs auf ein jungfräuliches System kommt. Sonst gibt es ärger beim installen dieser Anleitung. (Ich würde es aber einfach nur auf einem neuen System gleich nur so installen)

# Grundlegend

Arbeite ich mit vim, dieser muss noch etwas nachgeladen werden. Nano und MC wird noch installiert, für weniger gewohnte vi user.

Openssh-server wird installiert, ein ftp server wird nicht mehr benötigt, wir machen nur noch SFTP ab jetzt.

```
aptitude install vim-nox openssh-server ssh nano mc
```

Ab jetzt funktioniert: winscp, ssh, putty, gftp (auf SSH2). Es wird kein ftpd benötigt!! Ich habe mir ein Lesezeichen in Gnome/Nautilus (Explorer) von meinem Server angelegt.

# sources.list

Der Virenscanner ClamAV sollte immer auf dem neusten Stand sein. Darum diese SoftwareQuelle einbauen.

```
echo 'deb http://volatile.debian.org/debian-volatile lenny/volatile main contrib
non-free' >> /etc/apt/sources.list
```

..oder http://debgen.simplylinux.ch/

# hostname und hosts

Die sollten wirklich stimmen. Weil dann stimmen die Domain auch in den installierten Configs automatisch.

Die Dateien /etc/hosts und /etc/hostname muss man anpassen richtige Domain! Das ist sehr wichtig, das hier richtige Domains eingegeben werden. Und 127.0.0.1 ist nur localhost!

/etc/hosts

```
127.0.0.1       localhost
000.000.000.000 my.example.org   (000... wäre deine statische IP)
...
```

/etc/hostname

```
my.example.org
```

⚠ Kontrolle über hostname und hostname -f , ergeben das gleiche.

Bsp. my.example.org

# Updates & Locales

```
aptitude update
aptitude upgrade

dpkg-reconfigure locales
```

⚠ de_DE.ISO-8859-1 muss angewählt werden, andere darf man, und Standard darf auch was anderes sein. Für Squirrelmail deutsch

# Die Skel füllen / Ordner erstellen

Mail Ordner wird aus Kompatibilitätsgründen zu mutt erstellt, wir erstellen später ein mutt-imap Befehl für die Konsole, damit man an die gleichen Mail kommt wie im Webmail.

Dem vim grundsätzlich Highlighting beibringen

```
echo ':syntax on' > .vimrc
cp .vimrc /etc/skel
```

root, für root sich selber

```
mkdir -p /root/Maildir/{cur,new,tmp}
mkdir -p /root/Mail
mkdir -p /root/virusmails
```

root, für neue User

```
mkdir -p /etc/skel/Maildir/{cur,new,tmp}
mkdir -p /etc/skel/Mail
mkdir -p /etc/skel/virusmails
mkdir -p /etc/skel/public_html
mkdir -p /etc/skel/htpasswd
```

root für bestehende User:

```
for homedir in /home/* ; do user=$(basename $homedir) ; maildir=$homedir/Maildir
; mkdir -p $maildir ; for sub in cur new tmp ; do mkdir $maildir/$sub ; done ;
chown -R $user:$user $maildir ; done

for homedir in /home/* ; do user=$(basename $homedir) ; maildir=$homedir/Mail ;
mkdir -p $maildir ; chown -R $user:$user $maildir ; done

for homedir in /home/* ; do user=$(basename $homedir) ;
public_html=$homedir/public_html ; mkdir -p $public_html ; chown -R $user:$user
$public_html ; done

for homedir in /home/* ; do user=$(basename $homedir) ;
virusmails=$homedir/virusmails ; mkdir -p $virusmails;  chown $user:$user
$virusmails ; done
```

Damit User auch in der Konsole auf die richtigen Ordner kommen von ihrem Email.

Befehl bauen für die Console Email Zugriff:

mutt-imap

```
echo 'mutt -f imap://localhost/' > /usr/local/bin/mutt-imap; chmod +x
/usr/local/bin/mutt-imap; chown root.users /usr/local/bin/mutt-imap
```

# Postfix, Courier, Saslauthd, MySQL, rkhunter, binutils,mutt

rkhunter ist ein RootKit Sucher, vielleicht lässt Ihr diesen besser weg, weil er euch täglich eine Meldung an root schickt. Die Datenbank von rkhunter passt nicht so gut, darum meldet er immer Fehler. Die erste Email von rkhunter für Vergleiche später speichern ist das Beste.

```
aptitude install postfix postfix-mysql postfix-doc mysql-client mysql-server
courier-authdaemon courier-authlib-mysql courier-pop courier-pop-ssl courier-
imap courier-imap-ssl libsasl2-2 libsasl2-modules libsasl2-modules-sql sasl2-bin
libpam-mysql openssl courier-maildrop getmail4 binutils mutt rkhunter
```

**folgende Fragen so beantworten**

MySQL Passwort angeben [zweimal eingeben Enter]

WWW NEIN

Internet-Sites

Domain angeben (z.b. my.example.org)

**dann...**

 Edit /etc/default/saslauthd

```
START=yes
```

Neustart Saslauthd

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

Und dann noch, postfix mal auf das richtige Maildir schicken...

```
postconf -e 'home_mailbox = Maildir/'
postconf -e 'mailbox_command ='
/etc/init.d/postfix restart
```

# Unsolicited Commercial Email

Auch bekannt als Spam

Damit Postfix nicht einfach alles annimmt, aus unbekannten Quellen. Hier muss sollte sich jeder selber einlesen in Postfix. Es wird einfach einmal ein Minimum eingestellt. Thema: UCE (Unsolicited Commercial Email), ist eigentlich ein Spam Filter, bei der SMTP Authentifizierung. Solche Emails werden gar nicht entgegengenommen. Sodass Amavis oder Spamassassin diese nicht bearbeiten müssen (ContentFilter). Was etwas die Resourcen unseres Servers schont.

Copy&Paste Sie einfach alles in eine root Console von hier.

```
echo '

#Unsolicited Commercial Email
smtpd_helo_required = yes
smtpd_helo_restrictions =
smtpd_sender_restrictions =
smtpd_recipient_restrictions =
            reject_invalid_hostname,
            reject_non_fqdn_hostname,
            reject_non_fqdn_sender,
            reject_non_fqdn_recipient,
            reject_unknown_sender_domain,
            reject_unknown_recipient_domain,
            permit_mynetworks,
            reject_unauth_destination,
            #check_recipient_access pcre:/etc/postfix/recipient_checks.pcre,
            #check_helo_access dbm:/etc/postfix/helo_checks,
            #check_sender_access dbm:/etc/postfix/sender_checks,
            #check_client_access dbm:/etc/postfix/client_checks,
            #check_client_access pcre:/etc/postfix/client_checks.pcre,
            #reject_rbl_client cbl.abuseat.org,
            #reject_rbl_client sbl.spamhaus.org,
            #reject_rbl_client pbl.spamhaus.org
            permit

        smtpd_data_restrictions =
            reject_unauth_pipelining,
            permit
' >> /etc/postfix/main.cf
/etc/init.d/postfix restart
```

# Amavisd-new, SpamAssassin, Clamav, Postgrey

Anmerkung: Postgrey lehnt zuerst die Emails immer zweimal ab, erst beim dritten Versuch, wird es die Email annehmen. Das ist ein *mechanischer* Spam Schutz, führt aber etwas zu Verzögerungen. Wer das nicht will, installiert es einfach nicht.

```
aptitude install amavisd-new spamassassin clamav clamav-daemon zoo ripole unzip bzip2 arj nomarch lzop cabextract apt-listchanges libnet-ldap-perl libauthen-sasl-perl clamav-docs daemon libio-string-perl libio-socket-ssl-perl libnet-ident-perl zip libnet-dns-perl pyzor razor postgrey
```

## Amavis anpassen

Edit /etc/amavis/conf.d/15-content_filter_mode

```
@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);


@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);
```

Copy&Paste Sie einfach alles in eine root Console von hier.

```
echo '


smtp-amavis     unix    -       -       -       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o smtp_send_xforward_command=yes
        -o disable_dns_lookups=yes
        -o max_use=20

127.0.0.1:10025 inet    n       -       -       -       -       smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_delay_reject=no
        -o smtpd_client_restrictions=permit_mynetworks,reject
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o smtpd_data_restrictions=reject_unauth_pipelining
        -o smtpd_end_of_data_restrictions=
        -o mynetworks=127.0.0.0/8
        -o smtpd_error_sleep_time=0
        -o smtpd_soft_error_limit=1001
        -o smtpd_hard_error_limit=1000
        -o smtpd_client_connection_count_limit=0
        -o smtpd_client_connection_rate_limit=0
        -o
receive_override_options=no_header_body_checks,no_unknown_recipient_checks
' >> /etc/postfix/master.cf
```

Clamav zur Gruppe amavis hinzufügen

```
adduser clamav amavis
```

Postfix Email umleiten an amavis

```
postconf -e 'content_filter = smtp-amavis:[127.0.0.1]:10024'
postconf -e 'receive_override_options=no_address_mappings'
```

Neustart der Dienste ist etwas weiter unten dann.

## Spamassassin Spamfilterung

Hier muss nichts eingestellt werden. Amavis ruft es aber auf. Wer doch etwas machen will, muss sich einlesen. Eine Möglichkeit wäre: Edit /etc/spamassassin/local.cf

```
#   Use Bayesian classifier (default: 1)
#
use_bayes 1

#   Bayesian classifier auto-learning (default: 1)
#
bayes_auto_learn 1


#pyzor
use_pyzor 1
pyzor_path /usr/bin/pyzor
pyzor_add_header 1

#razor
use_razor2 1
razor_config /etc/razor/razor-agent.conf
```

## Abschliessen mit Neustart der Dienste

```
/etc/init.d/clamav-daemon restart
/etc/init.d/spamassassin restart
/etc/init.d/amavis restart
/etc/init.d/postfix restart
```

# Apache2, PHP5, FCGI, suExec, Pear, mcrypt

```
aptitude install apache2 apache2.2-common apache2-doc apache2-mpm-prefork
apache2-utils libexpat1 ssl-cert libapache2-mod-php5 php5 php5-common php5-gd
php5-mysql php5-imap  php5-cli php5-cgi libapache2-mod-fcgid apache2-suexec php-
pear php-auth php5-mcrypt mcrypt php5-imagick imagemagick libapache2-mod-suphp
```

Optional: phpmyadmin

```
a2enmod suexec rewrite ssl actions include userdir
a2ensite default-ssl
/etc/init.d/apache2 restart
```

# squirrelmail

```
aptitude install squirrelmail squirrelmail-viewashtml
```

Konfigurieren Squirrelmail:

```
squirrelmail-configure  [Enter]
```

(courier-imap wählen) D [Enter], courier{eintippen}[Enter], continue... [Enter]

(Sprache wählen) 10 [Enter] , 1 [Enter] , de{eintippen}[Enter], S [Enter], continue... [Enter], R [Enter] (ein allenfalls Save? mit y beantworten)

(Plugins wählen) 8 [Enter], fügen Sie calendar ,filters, mail_fetch, message_details, translate, squirrelspell, delete_move_next hinzu, indem Sie die Nummer dazu drücken, dann S [Enter], contiune... [Enter], Q [Enter]

**Verlinken squirrelmail**

```
ln -s /usr/share/squirrelmail/ /var/www/webmail
```

Optional: ln -s /usr/share/phpmyadmin/ /var/www/phpmyadmin

Ab diesem Moment funktioniert http://DeineDomain/webmail

⚠ Ich würde es aber wie in Tipps über https schicken, verschlüsselt die Anmeldung!

# Tipp: squirrelmail

## 'Redirect Webmail to https'

squirrelmail-secure-login Paket funktioniert die Anmeldung nicht, ich überlasse die Umleitung sowieso lieber Apache. Ich würde in die /etc/apache2/sites-available/default folgendes reinschreiben vor dem Directory:

```
     Redirect /webmail  https://dein.server.org/webmail
       <Directory /var/www/>
```

damit es immer über https läuft (verschlüsselt die Anmeldung).

Neustart Apache

**/etc/init.d/apache2 restart**

## Spam Ordner anlegen

Jeder Benutzer kann im squirrelmail über **Ordner** sich einen Spam Ordner anlegen, und unter **Optionen** einen **Nachrichtenfilter** anlegen.

Nachrichtenfilter -> Neu -> Kopfzeile ->

```
X-Spam-Status: Yes
```

Ordner wählen Spam [Senden]

Aber Spam mit hohem Score werden einfach gelöscht, die erhält man nicht.

# Test Viren Spam

Schauen Sie zu was der Mail Server macht mit **tail -f /var/log/mail.log**

## Spam Test

Schicken Sie sich an den neuen Email Server eine Email mit dem Inhalt:

```
Der Gtube Test:
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Dies erzielt aber ein Score von 1000, diese wird einfach gelöscht.

## Viren Test

Senden Sie sich an den neuen Email Server eine Email mit Attachment von Eicar Virentest , etwas runterscrollen. Diese Email wird einfach gelöscht.

## Ein paar TestEmails mit Sendmail, lokaler Test

Dazu musst Du root sein, ein test Benützer anlegen. Und schon kann der Test losgehen. Es hat ein Liesmich.txt der alles erklärt. Test_Spam_Virus_Mails.zip

# Emails Umleiten

## Emails nach User umleiten

Wir schicken mal alles möglich an den Benützer Karl. (fiktiver Namen, müsste natürlich ein richtiger Benutzer sein)

Edit /etc/aliases

```
root: karl
webmaster: karl
postmaster: karl
info@my.example.org:  karl
sales:  karl@hatnochein_hotmail.com
```

Aktivieren:

```
postalias /etc/aliases
```

## Emails nach Domain umleiten

Edit /etc/postfix/main.cf (zu unterst anfügen)

```
virtual_alias_domains = myother.example.org (hier kann man mehrere Domains mit
leerzeichen einfügen)
virtual_alias_maps = hash:/etc/postfix/virtual
```

Edit /etc/postfix/virtual

```
postmaster@myother.example.org postmaster
info@myother.example.org       joe
sales@myother.example.org      jane
customer@myother.example.org   karl@hatnochein_hotmail.com
# Uncomment entry below to implement a catch-all address
# @myother.example.org         jim    (Alle email von da an jim)
  ...virtual aliases for more domains..
```

Aktivieren:

```
postmap /etc/postfix/virtual
postfix reload
```

# Mögliche Erweiterungen

getmail4, um Emails von irgendwo anders abzuholen auf Server Ebene. (POP3 Abholer ist in Squirelle Optionen bereits vorhanden für jeden Benützer)

Procmail, um gezieltes ausfiltern von emails zu ermöglichen auf Server Ebene.

# Tipps

## htaccess

Die Datei .htaccess wird nur in den $HOME/public_html Verzeichniss verwendet. Falls ein Benützer ein Ordner Privat halten will.

Ich würde in /etc/apache2/mods-available/autoindex.conf

```
IndexOptions FancyIndexing VersionSort HTMLTable NameWidth=* DescriptionWidth=*
Charset=UTF-8
```

umschreiben auf ...

```
IndexOptions FancyIndexing VersionSort HTMLTable NameWidth=* DescriptionWidth=*
Charset=UTF-8 ShowForbidden
```

Dann werden Verzeichnisse doch gelistet, sind aber dennoch geschützt mit Passwort vor Zugriff. Man kann Sie dann doch noch ausschalten die Verzeichnisse dass sie nicht mehr gelistet werden, siehe unten. Aktivieren **/etc/init.d/apache2 restart**

.htaccess Beispiel

```
AuthType Basic
AuthName "Bitte Passwort eingeben"
AuthUserFile /home/"USER"/htpasswd/htpasswdfile
Require valid-user
#Option -Indexes  #Ordner nicht mehr anzeigen.
```

# fail2ban

Sobald ein paar Dienste laufen, wäre es eigentlich gut, wenn unser system, Passwort Angreifer, automatisch ausschliesst mit iptables (Firewall). Fail2ban ist über aptitude fail2ban installierbar.

# Firewall

Folgende Ports müssen offen sein 22(ssh), 25(smtp), 80 (http), 110 (pop3), 443 (https)

# System aktuell halten

So monatlich sollte man das machen:

```
aptitude update
aptitude upgrade
```

Von: (Korrektur lesen)  Juni2010