(2) MAILservices

POSTFIX (annex DOVECOT, …)

Virtuele gebruikers met achterliggende
(MySQL-)database

22-10-2017

1. Virtuale domeinen/gebruikers (mailboxen)

http://www.postfix.org/VIRTUAL_README.html

"Baas over je eigen e-mail: een Mailserver opzetten met Postfix en Dovecot" F Vervloesem in Linux Magazine jg 16 feb/mrt 2015

Complexer maar veiliger en flexibeler dan lokale gebruikers aan te maken is het werken met virtuele gebruikers met een achterliggende (MySQL)-databank

Installatie van de nodige componenten (indien dit nog niet eerder werd uitgevoerd)

```
apt-get install dovecot-pop3d dovecot-imapd dovecot-lmtpd
dovecot-mysql
```

(we gaan er hier van uit dat postfix & mysql reeds aanwezig zijn op het systeem)

Aanmaak van een systeemgebruiker voor virtual mails (IMAP-service)

Voor het afhandelen van incoming mail maken we een afzonderlijke gebruiker aan die als enige toegang heeft tot de mailboxen

We geven deze gebruiker het groupid 5000 en userid 5000.

```
groupadd vmail -g 5000
```

Dit gebruikersaccount wordt aangemaakt als systeem-account (flag -r), heeft bijgevolg geen login en wordt niet opgeslagen in /etc/shadow.

```
useradd vmail -r -c "virtual mail user" -d /var/vmail -m -
g 5000 -u 5000
```

Systeemaccounts krijgen geen home directory. Die moeten we zelf aanmaken.
We zullen de mails opslaan in `/var/vmail`, bijgevolg is `/var/vmail` de nieuwe home directory. Om die aan te maken voegen we de flag –m toe.

Check even via: `id vmail`

Als alles goed gaat, krijg je username, userid en groupid zoals hoger beschreven.

Tenslotte krijgt de user vmail alle rechten op zijn home directory toegewezen:

```
chown -R vmail:vmail /var/vmail
```

Aanmaak van een (MySQL) database voor de authenticatie van de gebruikers van de virtuele mailbowen.

De databank bevat een eenvoudige tabel met de velden ‚username, domain, password' en ‚quota_limit_bytes'. De databank kan benaderd worden door de gebruiker ‚dovecot'.

```
Mysql -p


CREATE DATABASE dbdovecot


GRANT SELECT ON dbdovecot.* TO 'dovecot'@'localhost'
IDENTIFIED BY 'duivekot';

Use dbdovecot;

CREATE TABLE tblusers (username VARCHAR(128), domain
VARCHAR(128) not null, quota_limit_bytes BIGINT(20),
password VARCHAR(256) not null);
```

De databank zullen we vullen met de nodige gegevens van de mailgebruikers.

Als voorbeeld maken we de gebruiker 'korneel' aan en we geven hem een geëncrypteerd paswoord (korneel).

Daartoe maken we eerst het paswoord aan met de bij dovecot mee-geïnstalleerde tool `doveadm` – de output leiden we om naar een bestand 'wachtwoord'

```
doveadm pw -s SHA512 > /tmp/wachtwoord
```

Terug op het niveau van MySQL voegen we de informatie in de tabel toe:

```
INSERT INTO tblusers(username, domain, password)
VALUES('korneel','familienaam.lab','
Lnm2D7mmLqbf9/nKZ752gsEG8VnI0alHVi6cubGh0B9o9w90MXesE0FJkJ
nKu7AjuF+JbwVLshj/FmtHHqv6gA==');
```

Configuratie van de dovecot-componenten

Dovecots configuratie tref je voornamelijk aan in `/etc/dovecot/conf.d/.`

In `dovecot.conf` vind je slechts beperkte configuratie, er staan wel verwijzingen (includes) in naar subconfiguratiebestanden.

Best maak je eerst een backup van de bestanden in deze directory alvorens je begint te wijzigen – de configuratiebestanden bevatten immers heel wat documentatie-

We gaan nu de masterconfiguratie aanpassen:

`/etc/dovecot/conf.d/10-master.conf`

configuratie van de services voor IMAP,POP3, authenticatie…

http://wiki2.dovecot.org/Services?highlight=%2810-master.conf%29

```
service imap-login {
  inet_listener imap {
     address = 172.20.0.25
     poort = 143
     SSL = no
  }
  inet_listener imaps {
    poort = 993
    SSL = yes
  }
}
```

```
service pop3-login {
  inet_listener pop3 {
     address = 172.20.0.25
     poort = 110
  }
  inet_listener pop3s {
     address = 172.20.0.25
     poort = 995
```

```
    SSL = yes
  }
}
```

```
service lmtp {
    user = vmail
    unix_listener /var/spool/postfix/private/lmtp-
dovecot{
       mode = 0660
       user = postfix
       group = postfix
  }
}
```

```
service auth {
    unix_listener auth-userdb {
}
    unix_listener /var/spool/postfix/private/auth {
       mode = 0666
       user = postfix
       group = postfix
  }
}
```

```
service auth-worker {
    user = $default_internal_user
}
```

```
service dict {
    unix_listener dict{
       mode = 0600
```

```
        user = vmail
        group = vmail
  }
}
```

Vervolgens passen we de mailconfiguratie aan:

`/etc/dovecot/conf.d/10-mail.conf`

configuratie waar de mail bewaard moet worden …, nl. in
`/var/vmail/<domeinnaam>/<gebruikersnaam>/mail`

```
mail_home = /var/vmail/%d/%n
mail_location = sdbox:%h/mail
namespace inbox {
inbox = yes
}
```

%d – variabele domein
%n – variabele naam(gebruiker)
%h– variabele homedirectory

sdbox: http://wiki2.dovecot.org/MailboxFormat

Daarna stellen we de authenticatie in:

`/etc/dovecot/conf.d/10-auth.conf`

Instellingen voor gebruikersauthenticatie – Best schakel je plaintext uit maar daartoe moet je eerst TLS-encryptie inschakelen. Voorlopig laten we dit dus op 'no' staan.

```
disable_plaintext_auth = no
auth_mechanisms = plain login
!include auth-sql.conf.ext
```

Tenslotte stellen we extra logging in wat handig is bij troubleshooting:

`/etc/dovecot/conf.d/10-logging.conf`

```
login_log_format_elements = user=<%u> method=%m rip=%r
lip=%l mpid=%e %c %k
```

Alle gegevens om met de database te verbinden en de juiste queries uit te voeren stellen we in in het bestand `dovecot-sql.conf.ext` onder `/etc/dovecot`

```
driver = mysql

connect = host=localhost dbname=dbdovecot user=dovecot
password=duivekot

default_pass_scheme = SHA512

password_query = SELECT username,domain,password, 'vmail' AS
userdb_uid, 'vmail' AS userdb_gid, concat('*:bytes=',
quota_limit_bytes) AS userdb_quota_rule FROM tblusers WHERE
username = '%n' AND domain = '%d'

user_query = SELECT 'vmail' AS uid, 'vmail' AS gid,
concat('*:bytes=', quota_limit_bytes) AS quota_rule FROM
tblusers WHERE username = '%n' AND domain = '%d'

iterate_query = SELECT CONCAT(username,'@'domain) AS user FROM
tblusers
```

Test en troubleshooten van de opstelling

Vooraleer je de configuratie test stop je best eerst alle mailservices en maak je alle logs leeg alvorens de services te herstarten.

```
root@mail:/var/log# service dovecot stop
[ ok ] Stopping IMAP/POP3 mail server: dovecot.
root@mail:/var/log# service postfix stop
[ ok ] Stopping Postfix Mail Transport Agent: postfix.
```

systeemlogbestand `/var/log/syslog`

maillogbestanden
`/var/log/mail.log`
`/var/log/mail.err`
`/var/log/mail.inf`
`/var/log/mail.warn`

Start eerst postfix: in mail.log en syslog kan je nagaan of de deamon gestart is.
Test via een telnetsessie op de lokale machine of de MTA functioneert.

```
root@mail:/var/log# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 mail ESMTP Postfix (Debian/GNU)
helo mail
250 mail
```

Start vervolgens Dovecot, in de logbestanden kan je dit opnieuw nagaan. IMAP en POP3 werden gestart?

```
root@mail:/var/log# service dovecot start
[ ok ] Starting IMAP/POP3 mail server: dovecot.
root@mail:/var/log# _
```

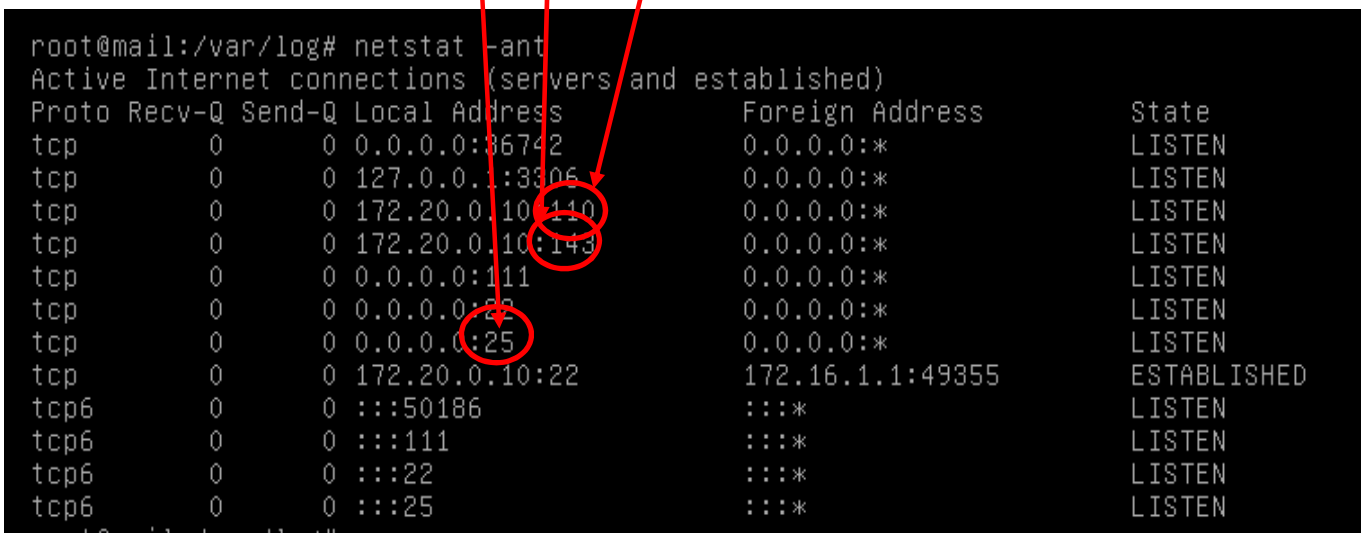
Test via een telnetsessie op de lokale machine of de POP3/IMAP-server functioneert.

```
root@mail:/var/log# telnet localhost 110
Trying ::1...
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

Allicht wordt een verbinding naar “localhost” niet toegelaten, probeer daarna op IP-adres.

```
root@mail:/var/log# telnet 172.20.0.10 110
Trying 172.20.0.10...
Connected to 172.20.0.10.
Escape character is '^]'.
+OK Dovecot ready.
```

4 services zijn aan het draaien SMTP, IMAP, POP3 en LMTP (afgeleide van ESMTP, niet over poort 25, voor LAN)
(https://tools.ietf.org/html/rfc2033
https://en.wikipedia.org/wiki/Local_Mail_Transfer_Protocol).




```
netstat -an |more |grep lmtp
```

http://wiki2.dovecot.org/LMTP

Probeer vervolgens effectief een mail te sturen via een telnetsessie op de localhost. Bemerk dat mappen werden aangemaakt onder `/var/vmail/…` volgens het dovecot dbox mailboxformaat

http://wiki2.dovecot.org/MailboxFormat

Vervolgens probeer je via een telnetsessie (poort 110) op de localhost de mail op te halen :

```
root@mail:/# telnet 172.20.0.10 110
Trying 172.20.0.10...
Connected to 172.20.0.10.
Escape character is '^]'.
+OK Dovecot ready.
user korneel@depaepe.lab
+OK
pass korneel
-ERR [SYS/TEMP] Temporary authentication failure. [mail.depaepe.lab:2015-10-03 0
8:03:33]
quit
+OK Logging out
Connection closed by foreign host.
```

Mogelijks loopt dit niet zo gesmeerd. In bovenstaand voorbeeld is er blijkbaar een probleem met het paswoord waardoor authenticatie faalt.
Een blik in `/var/log/mail.log` geeft aan dat er een syntax-foutje is geslopen bij het uitvoeren van de password query op de database.

```
  GNU nano 2.2.6      File: /etc/dovecot/dovecot-sql.conf.ext

# Note that these can be used only as input to SQL query. If the query outputs
# any of these substitutions, they're not touched. Otherwise it would be
# difficult to have eg. usernames containing '%' characters.
#
# Example:
#   password_query = SELECT userid AS user, pw AS password \
#     FROM users WHERE userid = '%u' AND active = 'Y'
#
password_query = \
  SELECT username, domain, password \
  'vmail' as userdb_uid, 'vmail' as userdb_gid, \
```

Na password moet een komma staan. Na de correctie slaan we de configuratie op en proberen opnieuw, met meer succes deze keer.

Na elke actie maken we de logs leeg zodat we duidelijk kunnen zien waar het eventueel foutloopt en vooral wat er op de achtergrond gebeurt.

Op dezelfde manier gaan we te werk om een connectie maken via IMAP.

http://www.anta.net/misc/telnet-troubleshooting/imap.shtml

Aanmaak van mailboxen automatiseren (Enkele mogelijkheden)

addmail.cs :

small tool written in C# and compiles on Mono to add users to Postfix and Dovecot when following the configuration guide found at http://help.ubuntu.com/community/PostfixVirtualMailBoxClamSmtpHowto

Requirements

mkpasswd : maakt deel uit van de package 'whois', evt. moet je dit eerst installeren:

```
sudo apt-get install whois
```

mono + compiler

```
sudo apt-get install mono-runtime mono-gmcs
```

Compilation

download `addmail.cs` van http://code.google.com/p/addmail/downloads/list

compileer de code (na evt. aanpassingen)

```
gmcs addmail.cs
```

kopieer naar `/usr/bin` (of `/usr/sbin`) – de extensie .exe mag je gerust weglaten
cp addmail.exe /usr/bin

Usage

```
# addmail *user@host* _password_
```

For example: addmail newuser@example.com newpass123

It will confirm everything looks right before actually adding the user.

wget http://addmail.googlecode.com/files/addmail-1.1.cs

```
root@mail:/addmail# mv addmail-1.1.cs addmai
root@mail:/addmail# mv addmail addmail.cs
root@mail:/addmail# gmcs addmail.cs
root@mail:/addmail# ls
addmail.cs  addmail.exe
root@mail:/addmail# mv addmail.exe addmail
```

We moeten diverse zaken aanpassen, op te zoeken zoals connectie met database. Hier worden alle gegevens naar files geschreven.
http://www.codeproject.com/Articles/43438/Connect-C-to-MySQL

http://www.codeproject.com/Articles/43438/Connect-C-to-MySQL

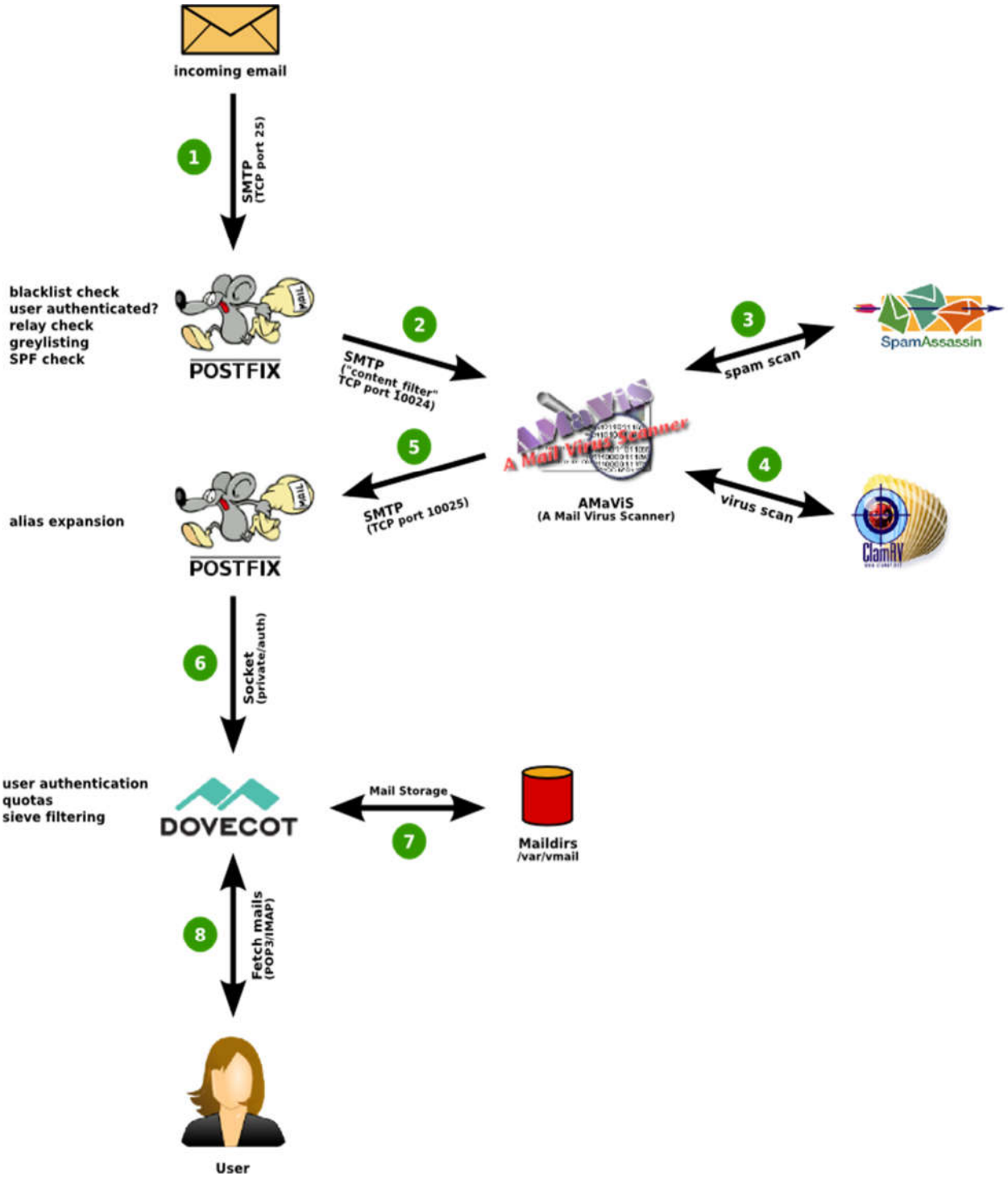
ViMbAdmin :

Het ViMbAdmin project (vim-be-admin) biedt een web based virtual mailbox beheersysteem waarmee mail administrators domeinen, mailboxen & aliases kunnen beheren.

https://github.com/opensolutions/ViMbAdmin/wiki/Installation
https://www.dev-metal.com/setup-latest-version-php-5-5-debian-wheezy-7-07-1-fix-gpg-key-error/
http://www.bravo-kernel.com/2014/08/how-to-install-composer-on-debian/

https://github.com/opensolutions/ViMbAdmin/wiki
http://www.vimbadmin.net/
http://pietervogelaar.nl/ubuntu-12-04-install-postfix-dovecot-and-vimbadmin

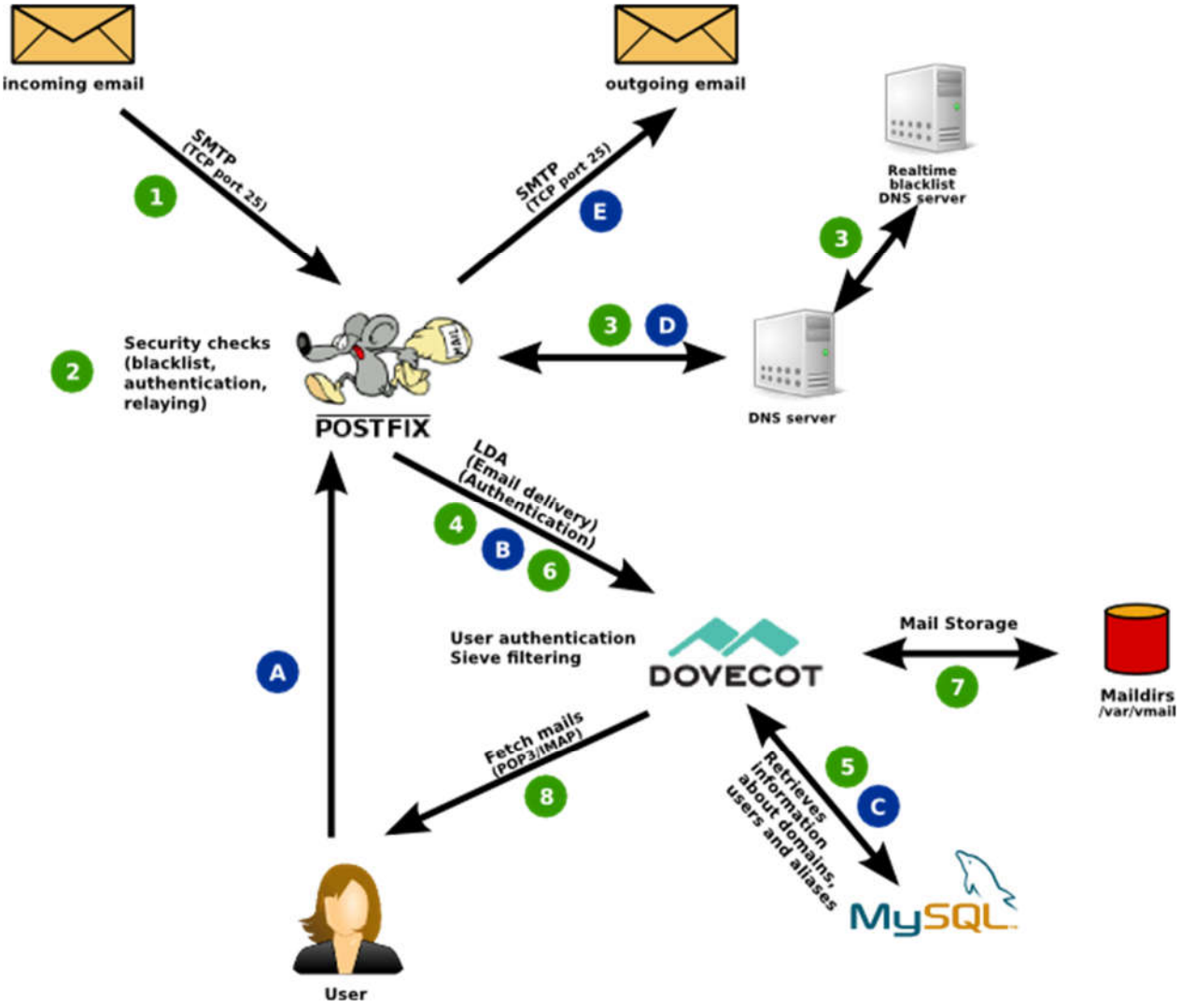
De wondere wegen van email (the big picture)

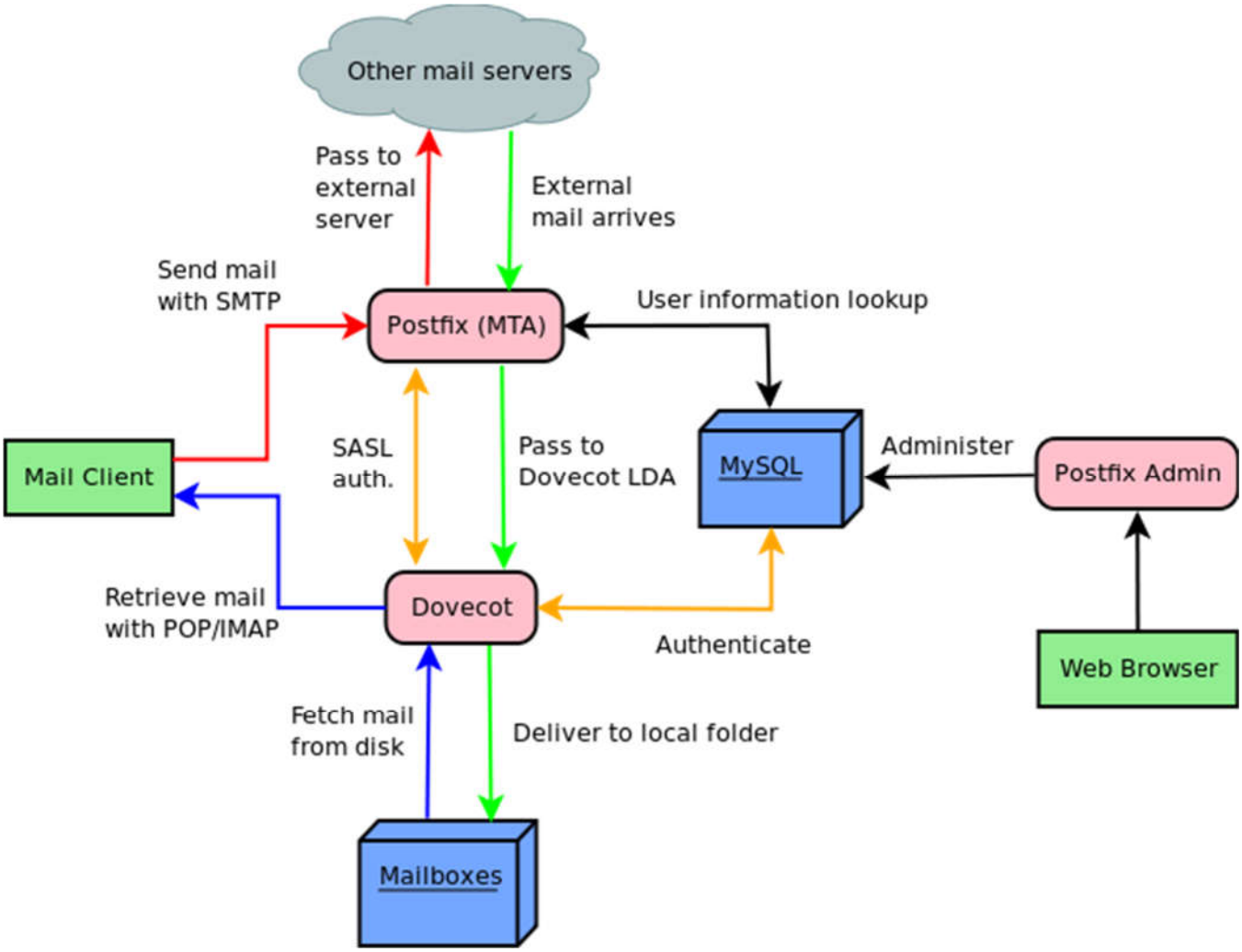


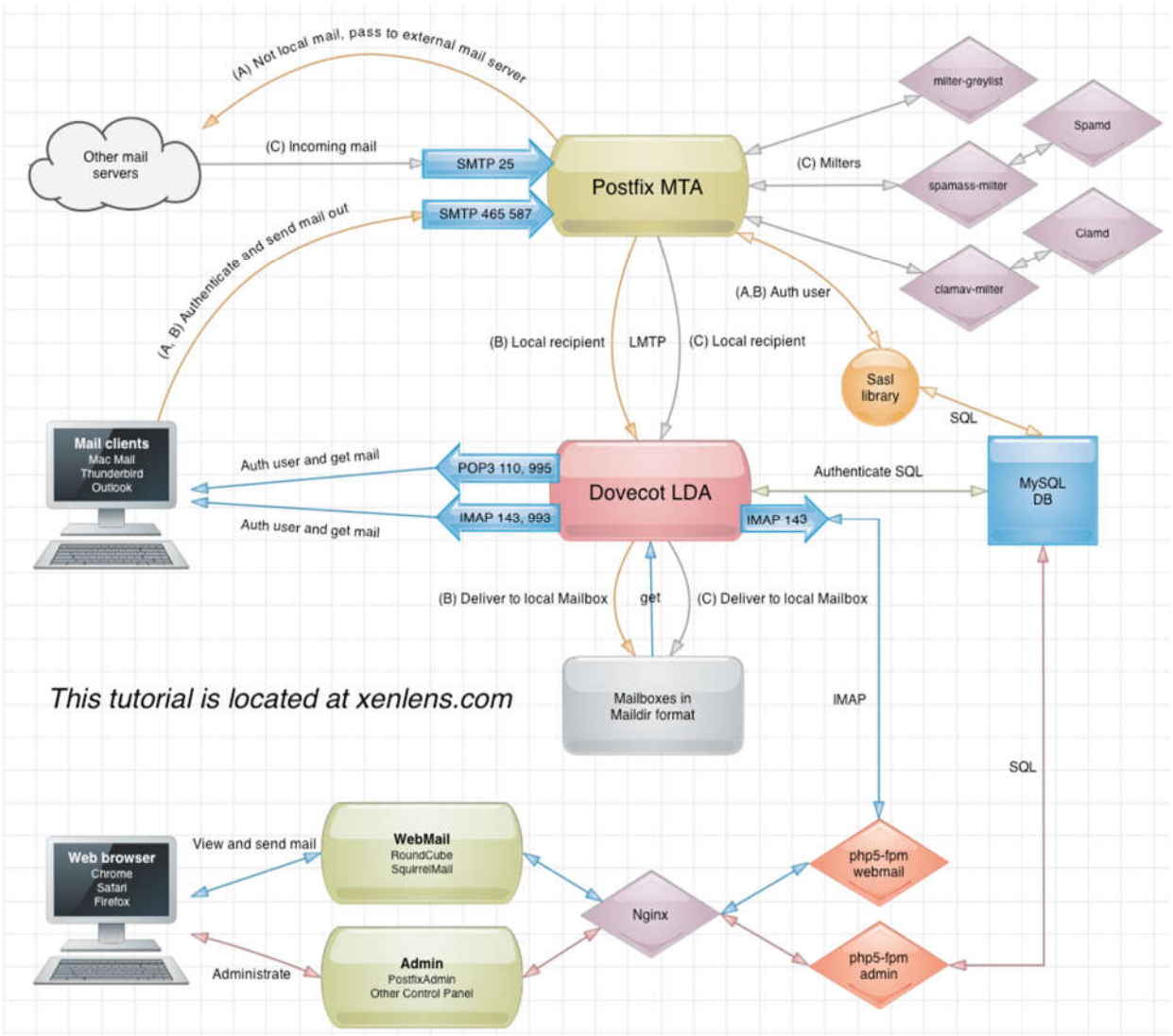
1. An email is sent to your server via the SMTP protocol on TCP port 25. Postfix accepts the connection, reads the email and does some basic checks. Is the sender blacklisted on a realtime blacklist? Is the email from an authenticated user so we

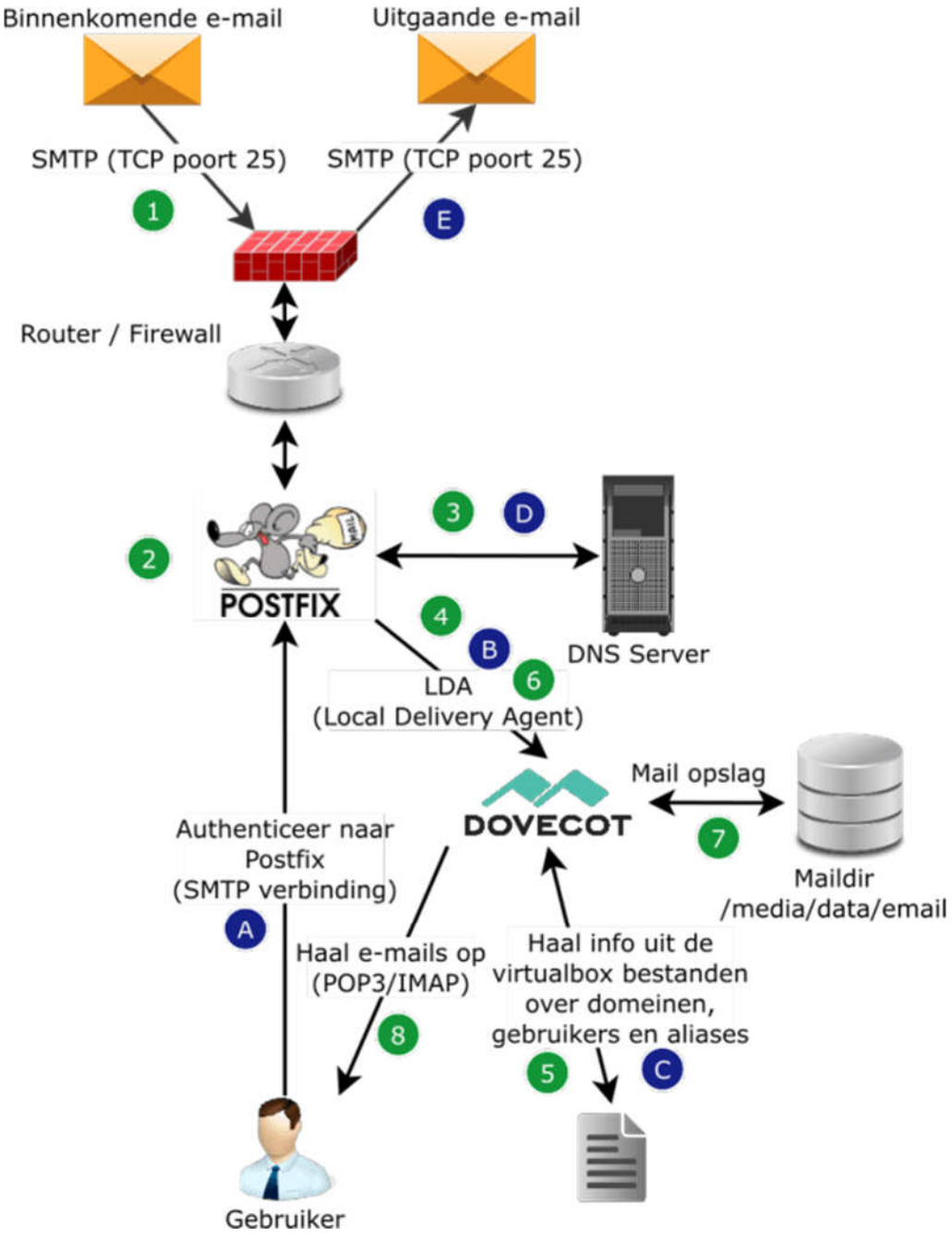
bypass relay checks? Or is the recipient of the email a valid user on our system? If we don't trust the remote system yet we apply greylisting. At this stage Postfix can reject the email or accept it.

2. Postfix forwards the email via the SMTP protocol on the TCP port 10024 to AMaViS for content checking. Notice that at this stage the email can't be rejected any more. So AMaVis can either accept it or throw it away. Commonly AMaViS is configured to add a certain email header so the user can see that AMaViS thinks it is spam.
3. AMaViS lets SpamAssassin check the email for spam. SpamAssassin will be taught which emails are spam to increase its detection accuracy.
4. AMaViS also runs the email through ClamAV to see if it contains any viruses.
5. After these checks AMaViS returns the email to the Postfix process but on TCP port 10025. Postfix is configured to trust emails sent to this port so further content checks are skipped.
6. Postfix forwards the email to Dovecot. Dovecot can optionally apply per-user filters so that emails can be stored in certain email folders automatically if desired.
7. Dovecot writes the email to the hard disk in maildir format.
8. The user's email client can now fetch the new emails from Dovecot using the POP3 or IMAP protocol


incoming email
outgoing email
SMTP (TCP port 25)
1
SMTP (TCP port 25)
E
Realtime blacklist DNS server
3
2
Security checks (blacklist, authentication, relaying)
POSTFIX
3
D
DNS server
LDA (Email delivery) (Authentication)
4
B
6
User authentication
Sieve filtering
DOVECOT
Mail Storage
7
Maildirs /var/vmail
A
Fetch mails (POP3/IMAP)
8
5
C
Retrieves information about domains, users and aliases
MySQL
User


Other mail servers
Pass to external server
External mail arrives
Send mail with SMTP
Postfix (MTA)
User information lookup
Mail Client
SASL auth.
Pass to Dovecot LDA
MySQL
Administer
Postfix Admin
Retrieve mail with POP/IMAP
Dovecot
Authenticate
Web Browser
Fetch mail from disk
Deliver to local folder
Mailboxes


(A) Not local mail, pass to external mail server
Other mail servers
(C) Incoming mail
SMTP 25
SMTP 465 587
Postfix MTA
(C) Milters
milter-greylist
Spamd
spamass-milter
Clamd
clamav-milter
(A, B) Authenticate and send mail out
(A,B) Auth user
(B) Local recipient
LMTP
(C) Local recipient
Sasl library
SQL
Mail clients
Mac Mail
Thunderbird
Outlook
Auth user and get mail
POP3 110, 995
IMAP 143, 993
Auth user and get mail
Dovecot LDA
Authenticate SQL
MySQL DB
IMAP 143
(B) Deliver to local Mailbox
get
(C) Deliver to local Mailbox
This tutorial is located at xenlens.com
Mailboxes in Maildir format
IMAP
SQL
Web browser
Chrome
Safari
Firefox
View and send mail
WebMail
RoundCube
SquirrelMail
Nginx
php5-fpm webmail
Administrate
Admin
PostfixAdmin
Other Control Panel
php5-fpm admin


Binnenkomende e-mail
Uitgaande e-mail
SMTP (TCP poort 25)
SMTP (TCP poort 25)
1
E
Router / Firewall
2
POSTFIX
3
D
DNS Server
4
B
6
LDA
(Local Delivery Agent)
Mail opslag
DOVECOT
7
Maildir
/media/data/email
Authenticeer naar
Postfix
(SMTP verbinding)
A
Haal e-mails op
(POP3/IMAP)
8
Haal info uit de
virtualbox bestanden
over domeinen,
gebruikers en aliases
5
C
Gebruiker