Email Server - Postfix

Contents

Postfix telepítése

Postfix beállítások

Hozzunk létre egy postfix nev? felhasználót, és adjunk olvasási jogot a postfix adatbázisra.

- user: postfix
- pass: liteon
- hozzáférés: localhost
- jogok: csak olvasási, a postfix adatbázisra.

Fontos, hogy a postfix-ben legyen mysql támogatás. A CentOS 6.6-os repóban volt. Így ellenörízhetjük:

```
# ldd /usr/libexec/postfix/smtpd | grep libmysql
        libmysqlclient.so.16 => /usr/lib64/mysql/libmysqlclient.so.16 (0x00007f4439270000)
```

Ha van, akkor meg kell jelenjen a második sor. Ha nincs, akkor baj van, újra kell fordítani mysql támogatással.

Az alapértelmezett konfigurációban csak pár paramétert kell átírni. A myhostname és mydomain paraméterekhez nagyjából mindegy mit írunk, csak ne legyen olyan domain név, ami a virtuális domainek között is szerepelni fog, mert akkor nem fogja virutális domain-ként kezelni a postfix.

```
myhostname = mail.berki2.org
....
mydomain = system.berki2.org


...
#################################
# Bejöv? levelekre megszorítások
#################################
smtpd_error_sleep_time = 1s
smtpd_soft_error_limit = 5
smtpd_hard_error_limit = 10
smtpd_helo_required = yes
```

Virtuális emial boxok

A virtuális email kezeléshez a mail csoporto fogjuk használni. A mail csoportban benne van a postfix user is. A postfix a postfix user nevében fut. Ezért ami a mail tulajdonában van, azt a postifix is tudja olvasni. Listázzuk ki a mail user gid-ját. Ez a 12. Ezt kell majd a dovecot-ban is megadni.

```
# cat /etc/group | grep mail
mail:x:12:mail,postfix
```

A mail csoportba hozzunk létre egy vmail nev? felhasználót, akinek a home könyvtára a leend? virtuális levelezés mappája lesz. Fontos, hogy a uid-ja 150 legyen, mert ezzel fogunk ár hivatkozni a dovecot-ban.

```
# useradd -r -u 150 -g mail -d /var/spool/postfix/virtual -s /sbin/nologin -c "Virtual maildir handler" vmail
```

Hozzuk létre a virtuális levelezés mappáját. Adjuk az új vmail felhasználó és mail csoport tulajdonába. Adjunk rá 770 jogot, tehát a csoport és a tulajdonos is tudja olvasni és írni. Így a postfix és a vamil is hozzáfér majd.

```
# mkdir /var/spool/postfix/virtual
# chown vmail:mail /var/spool/postfix/virtual
# chmod 770 /var/spool/postfix/virtual
```

Hozzuk létre az mysql lekérdezéseket tartalmazó mappát. A domaineket, az email címeket, és az aliasokat a postfix a postfixadmin által létrehozott táblákból fogja kiolvasni. Fontos, hogy a postfix csoport és a root user tulajdonában legyen, és hogy 640 jog legyen rá.

```
# mkdir /etc/postfix/mysql_queries/
# chmod 640 /etc/postfix/mysql_queries/*
# chgrp postfix /etc/postfix/mysql_queries/*
```

mysql_virtual_alias_maps.cf

```
user = postfix
password = liteon
hosts = localhost
dbname = postfix
table = alias
select_field = goto
where_field = address
```

mysql_virtual_domains_maps.cf

```
user = postfix
password = liteon
hosts = localhost
dbname = postfix
table = domain
select_field = domain
where_field = domain
additional_conditions = and active = '1'
```

mysql_virtual_mailbox_maps.cf

```
user = postfix
password = liteon
hosts = localhost
dbname = postfix
table = mailbox
select_field = maildir
where_field = username
#additional_conditions = and active = '1'
```

Nézzük meg milyen beállításokkal lett elindítva.

```
# postconf -n
```

A main.cf végére tegyük az alábbit. Fontos, hogy a uid_maps legyen a vmail user 150-es uid-val, és a gid_maps legyen a mail user a 12-es gid-val.

```
############################
# Virtualis mailboxok
############################

virtual_transport = virtual
virtual_maps = mysql:/etc/postfix/mysql_queries/mysql_virtual_alias_maps.cf

virtual_minimum_uid = 150
virtual_uid_maps = static:150
virtual_gid_maps = static:12

virtual_mailbox_base = /var/spool/postfix/virtual
virtual_mailbox_domains = mysql:/etc/postfix/mysql_queries/mysql_virtual_domains_maps.cf
virtual_mailbox_maps = mysql:/etc/postfix/mysql_queries/mysql_virtual_mailbox_maps.cf

# service postfix start
# chkconfig postfix on
```

SASL (Simple Authentication and Security Laye)

SASL egy alkalmazásrétegbeli autentikációs keretrendszer. Segítségével többek között egy alkalmazás felhasználónév és jelszó páros használatával autentikálni tudja magát egy másik alkalmazásnál. Két dologra fogjuk használni.

1. Egyrészt a mi postfix szerverünk SASL autentikáció használatával fogja továbbítani a leveleket az ISP MTA-jának egy felhasználónév/jelszó páros használatával,
2. másrészt a mi felhasználóink SASL használatával fogják magukat autentikálni a mi postfix szerverünk felé, mikor át akarnak adni neki a levelet, hogy küldje azt el a címzettnek.

Fel kell telepítsük a cyrus-sasl csomagot:

```
# yum install cyrus-sasl
```

Levelek befogadása idegen hálózatból (SASL)

A postifx magától csak olyan levelet hajlandó befogadni, és elküldeni az abban szerepl? címzettnek, ami a saját hálózatából érkezik. (Ez nem összekeverend? azzal, mikor a feladó MTA-ja küld levelet a postfix-nek, egy lokális felhasználónak) A szerver saját hálózatát a mynetwork paraméter határozza meg. Ha külön nem definiáljuk, akkor a localhost, és a szerver interfészeinek alhálózatai lesznek benne. Ha a levél feladójának IP címe nem szerepel a mynetwork-el megadott hálózatok között, akkor a postfix el fogja utasítani a levél befogadását és elküldését.

```
Relay access denied;
from=<adam@berki2.org> to=<lali_lali96@gmail.com> proto=ESMTP helo=<[192.168.43.197]>
```

Felhasználóink nem csak a saját hálózatból akarnak levelet küldeni, hanem küls? hálózatokból is, pl okos telefonról, vagy otthonról a laptopjukról.

Lehet?ség van rá, hogy a felhasználók leveleit ne csak az IP cím alapján fogadjuk be továbbküldésre, hanem autentikáció alapján is. Erre szolgál a SASL autentikáció. Ha a SASL autentikáció be van kapcsolva, akkor a SASL-el autentikált felhasználók leveleit is befogadja és elküldi a postfix a levélben szerepl? címzettnek. Mivel a dovecot (IMAP szerver) már amúgy is képes autentikálni a felhasználókat, ezért nem építünk még egy új autentikációs konfigurációt, hanem megmondjuk a postfix-nek, hogy próbálja meg a felhasználókat a dovecot-on keresztül autentikálni.

Note
Az itt leírtaknak semmi köze a titkosításhoz. A lényeg, hogy tetsz?leges hálózatból elfogadjuk az autentikált felhasználók leveleit, amit a postfix majd elküld a címzettnek. Ehhez az kell, hogy a felhasználók egy felhasználónév/jelszó párossal azonosítsák magukat, amit a posftix a dovecot-on keresztül fog majd megtenni.

A main.cf -ba

```
mydestination = localhost

....
....

############################
# SASL
```

```
############################
# A SASL autentikációt egyrészr?l az ISP MTA-ja felé fogjuk azonosításra haszálni,
# másrészt a mi felhasználóink SASL-el fogják magukat azonosítani a postfix szerver
# felé, hogy az befogadja a leveleiket idegen hálózatból is:

# Közös SASL konfig #
#####################
smtpd_sasl_auth_enable = yes

# Kliensek autentikációja #
###########################
#SASL-el authentikáltnak és saját hálózatból elfogadjuk a levelet
smtpd_relay_restrictions =
    permit_mynetworks
    permit_sasl_authenticated
    defer_unauth_destination

smtpd_recipient_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_unauth_destination


broken_sasl_auth_clients = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_security_options = noanonymous
```

A fenti konfigurációval azt mondtuk meg, hogy relay szerverként a postfix a saját hálózatból érkez? leveleket és a sasl-el autentikált felhasználók leveleit fogadja el. Tehát a lokális hálózaton lév? klienseknek nem kell autentikálniuk magukat.

Levél küldése Relay hoszton keresztül (SASL)

Mivel dinamikus IP címünk van, a legtöbb MTA nem fogja elfogadni a postfix szerverünk által küldött leveleket. Ezért a leveleket nem közvetlen a címzett MTA-jának fogjuk küldeni, hanem az ISP-nk MTA-jának fogjuk átadni továbbküldésre, mint ha egy email kliens küldte volna a levelet. Ehhez azonban a mi szerverünknek SASL használatával autentikálnia kell magát az ISP MTA-ja felé.

A SASL használatát már korábban bekapcsoltuk a felhasználók leveleinek a befogadására. Itt már csak egy felhasználónév/jelszó map fájlt kell elkészíteni, ami tartalmazza az ISP MTA-jához a felhasználónév/jelszó párosunkat. Hozzunk létre egy jelszó fájlt, amiben egy sort kell csak elhelyezni: <relay hoszt neve> <felhasználónév>:<jelszó>

/etc/postfix/sasl_passwd

```
smtp.upcmail.hu   berki.adam3@upcmail.hu:57446477
```

Adjuk a root tulajdonába, és tegyünk rá 600 jogot. Majd a postmap paranccsal készítsünk bel?le postfix map fájlt.

```
# chown root:root /etc/postfix/sasl_passwd
# chmod 600 /etc/postfix/sasl_passwd
# postmap /etc/postfix/sasl_passwd
```

Ekkor létrejön a sasl_passwd.db fájl.

A /etc/psotfix/main.cf-be állítsuk be, hogy relay hosztot használjon az emaile kiküldésére. A relayhost paraméterrel mondjuk meg a postfix-nek, hogy a kimen? leveleket nem közvetlen kell elküldeni, hanem át kell adni a relay host-nak. A smtp_sasl_password_maps paraméterrel kell megadni az autentikációs map fájl helyét.

```
....

... korábbi SASL konfiguráció ...


# UPC SMTP relay #
##################
relayhost = smtp.upcmail.hu
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
```

Miért tud a localhost üzenetet küldeni root nevében?

Fontos, hogy a mydomain-ba ne adjunk meg olyan domain nevet, ami a virtuális domainek között szerepelni fog. Mikor a rendszer küld egy emailt, pl Raid riasztást, akkor nem ad meg küld? domaint, csak annyit hogy root. Amikor a postfix megkapja a levelet, hozzácsapja a mydomain-t, és így el?áll a root@system.berki2.org feladó. Ezt minden publikus mail szerver el fogja dobni, mert 3 tagból áll a domain név. De mivel a címzett a root@berki2.org, ami szerepel a virtuálist email címek között, és a levelet a localhost küldte, a postfix nem fogja vizsgálni a feladó validságát. Amúgy luxus lenne fenntartani egy valid domain nevet erre a célra.

Titkosított kapcsolatot használata levélküldésre

Az itt leírtaknak semmi köze az IMAP/POP3 szerverrel történ? titkosított kommunikációhoz és ahhoz sem, hogy a felhasználók autentikálják e magukat a postfix felé vagy sem. Itt kizárólag az MTA <-> MTA kommunikáció titkosításáról lesz szó, vagyis hogy TLS felett fogadja és küldje a postfix-ünk a leveleket ha van rá lehet?ség. Sajnos nem minden MTA támogatja a titkosítást, ezért meg kell engedni a titkosítatlan csatorna használatát is az MTA-k között kommunikációban, de a felhasználók felé ki lehet kényszeríteni a titkosítás használatát.

Main.cf

Az smtpd_<..> beállítások a démon beállításai, vagy a levelek fogadására szolgáló paraméterek gy?jteménye, az smtp_<....> pedig a postfix által küldött levelekre vontatkozik.

/etc/postfix/main.cf

```
...
####################################
# SMTP levelek fogadása
####################################
```

```
smtpd_tls_security_level = may
smtpd_tls_key_file = /etc/postfix/ssl/ssl.key/mail.berki2.org-server.key
smtpd_tls_cert_file = /etc/postfix/ssl/ssl.crt/mail.berki2.org-server.crt
smtpd_tls_loglevel = 1

smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_cache
tls_random_source = dev:/dev/urandom
tls_random_exchange_name = /var/lib/postfix/prng_exch
smtpd_tls_auth_only = yes

#####################################
# SMTP levelek kiküldése
#####################################
smtp_tls_security_level = may
smtp_tls_key_file = /etc/postfix/ssl/ssl.key/mail.berki2.org-server.key
smtp_tls_cert_file = /etc/postfix/ssl/ssl.crt/mail.berki2.org-server.crt
smtp_tls_loglevel = 1
...
```

- smtp_tls_security_level = may --> Ha a címzett MTA-ja nem ismeri a TLS-t akkor küldheti TLS nélkül is. Bizonyos MTA-k nem tudnak titkosítani, ezért náluk biztosítani kell a sima küldést is.
- smtpd_tls_auth_only = yes #A SASL autentikáció csak TLS felet mehet. Vagyis, ha egy felhasználó átad egy levelet továbbküldésre, azt nem teheti meg titkosítatlan csatornán.

Kulcsok elhelyezése

Ugyan azt a kulcsot fogjuk használni, amit az Apache-ban is használunk (ezek mail.berki2.org domain kucsa és cert-je), mivel ugyan az a domain. De muszáj hogy a postfix alá másoljuk, különben megsérti a SELinux rendszabást. Másoljuk a kulcsokat (ssl.key és ssl.crt) /etc/postfix/ssl/ mappába. Fontos, hogy másoljuk, hogy a Selinux kontextusa rendbe legyen a fájloknak:

```
# /etc/postfix/ssl/ ll -Z
drwxr-----. root postfix unconfined_u:object_r:postfix_etc_t:s0 ssl.crt
drwxr-----. root postfix unconfined_u:object_r:postfix_etc_t:s0 ssl.key
```

Adjuk a postfix csoport tulajdonába, és csak a tulaj és a csoport tudja olvasni.

```
# cd /etc/postfix/ssl/
# cp ... kulcsok másolás ...
# chown -R  :postfix *
# chmod -R 740 *
```

587-es port engedélyezése titkosított bejöv? csatornának

Ahhoz, hogy ne csak a 25-ös porton fogadjon el a postfix STARTTLS kapcsolatot, hanem a szabványos 587 porton is, a master.cf-ben ki kell venni a kommentet a submission sor el?l:

```
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
submission inet n       -       n       -       -       smtpd
```

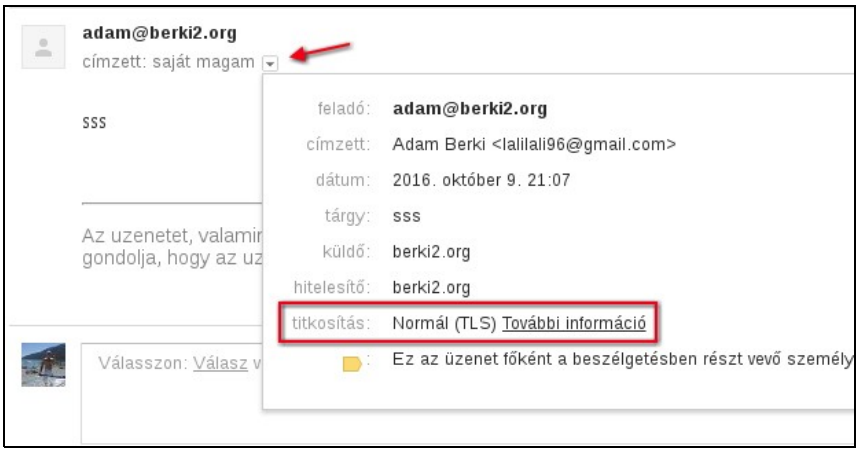
A maillog-ban láthatjuk a TLS-en befogadott levelet: connect from 254C26B6.nat.pool.telekom.hu[37.76.38.182] setting up TLS connection from 254C26B6.nat.pool.telekom.hu[37.76.38.182] Anonymous TLS connection established from 254C26B6.nat.pool.telekom.hu[37.76.38.182]: TLSv1 with cipher DHE-RSA-CAMELLIA256-SHA (256/256 bits)

Tesztelés

Küldjünk egy levelet a gmail-es címünkre. A log-ban látunk kell, hogy a TLS kapcsolat felépült:

```
...
postfix/smtp[8359]: setting up TLS connection to gmail-smtp-in.l.google.com[74.125.71.26]:25
...
```

A gmail-ben kattintsunk a küld? melletti kis nyílra. A felugró ablakban látnunk kell, hogy az üzenet TLS-el lett titkosítva:



file:///home/adam/Downloads/tls_yes.png

Amennyiben a TLS nincs bekapcsolva a kimen? email-ekre, úgy a gmail-ben az üzenet mellett megjelenik egy kis piros lakat, és a felugró ablakban is látható hogy nem volt titkosítás használva:

file:///home/adam/Downloads/tls_no.png

Email statisztikák

Pflogsumm

https://www.linode.com/docs/email/postfix/pflogsumm-for-postfix-monitoring-on-centos-6