INSTALLAZIONE SERVER DI POSTA ELETTRONICA - POSTFIX

Contents

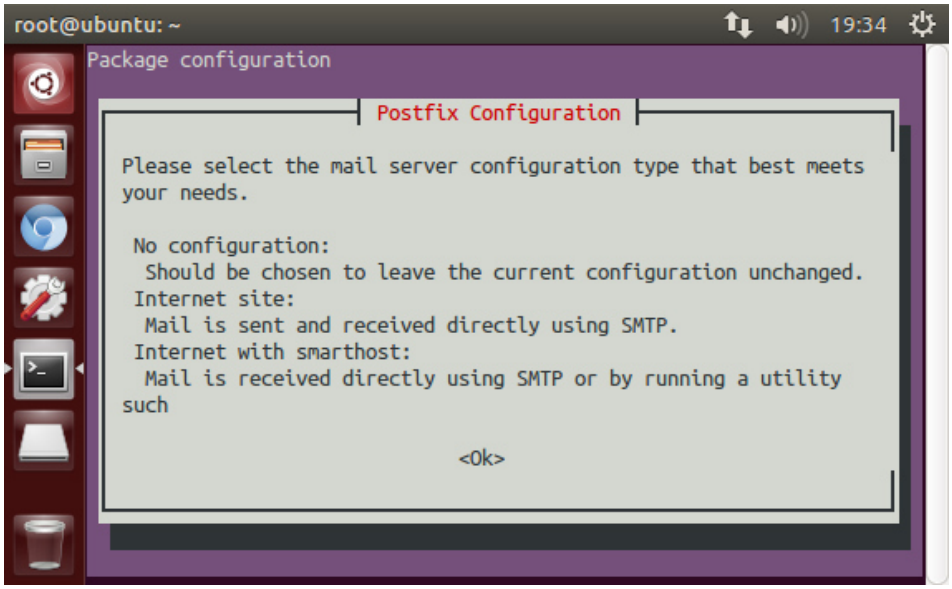
1.0 Installazione Postfix 3
1.1 Configure Postfix 4
1.2 TLS 5
2.0 POSTFIX and MySQL 5
2.1 Configurazione per MailaaS di PRISMA 5
3.0 Virtual user Postfix 7
4.0 AUTHENTICAZIONE – Architettura 9
3.1 Saslauthd 9
5.0 DNS, MX record. 12

1.0 Installazione Postfix

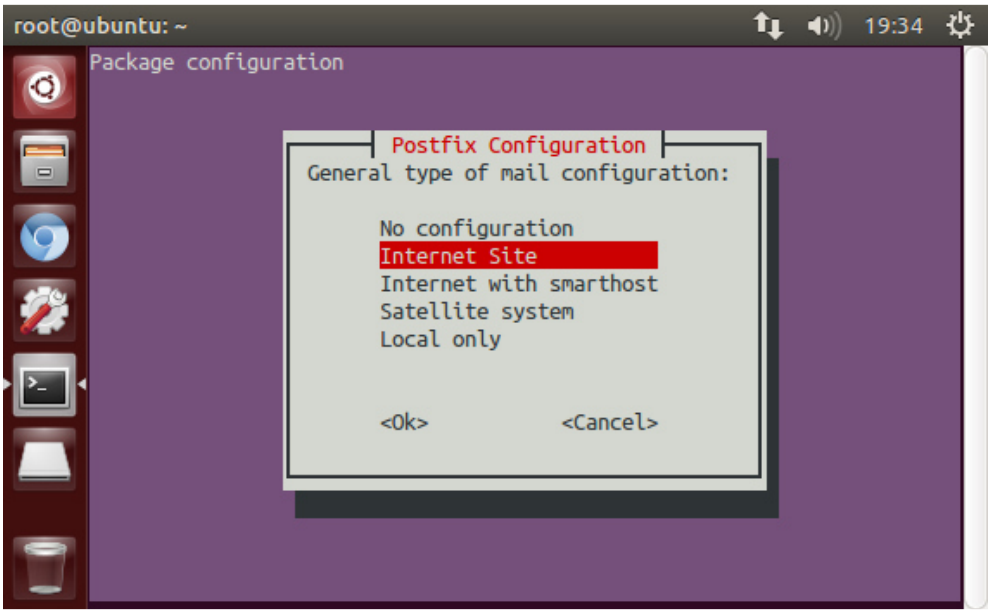
Per le configurazioni di un server di posta elettronica configurare FQDN, DNS, MX record SPF....

Alcune di queste configurazioni sono scritte all'interno del paragrafo § 5.0 .

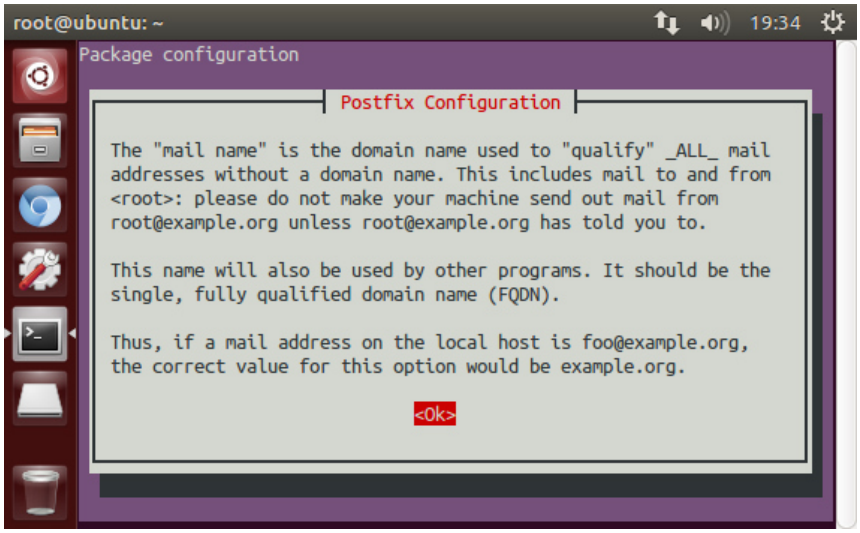
```
sudo apt-get update
sudo apt-get install postfix
```



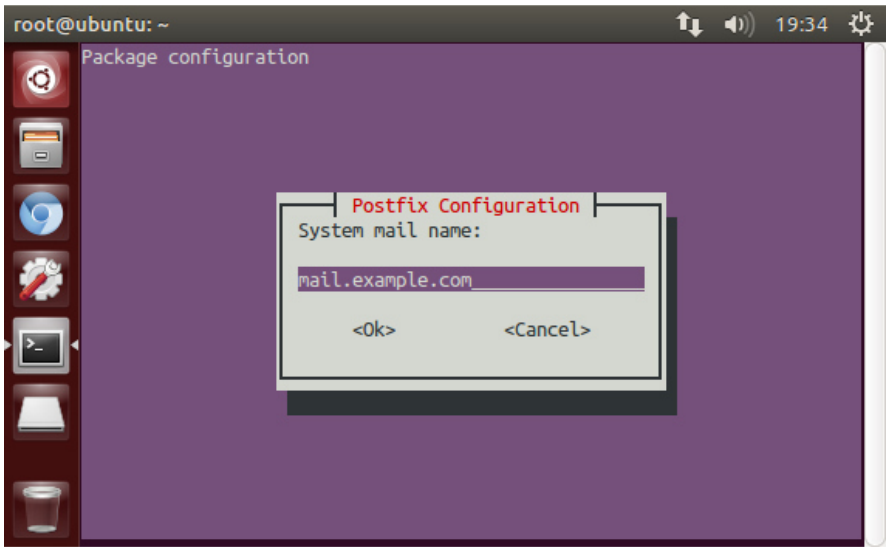
Choose Ok.



Choose Internet Site and press Ok.



Choose Ok.



Insert FQDN valid.

1.1 Configure Postfix

Spostiamoci nella directory /etc/postfix ed eseguiamo una copia di backup del file come misura precauzionale:

```
# cd /etc/postfix/
# cp main.cf  main.cf.orig
```

Begin by opening this file with root privileges in your text editor (nano, vi..):

```
sudo nano /etc/postfix/main.cf
```

First, we need to find the `myhostname` parameter. During the configuration, the FQDN we selected was added to the `mydestination` parameter, but `myhostname` remained set to `localhost`. We want to point this to our FQDN too:

```
myhostname = example.com
```

As we said above, the `mydestination` parameter has been modified with the FQDN you entered during installation. This parameter holds any domains that this installation of Postfix is going to be responsible for. It is configured for the FQDN and the localhost.

One important parameter to mention is the `mynetworks` parameter. This defines the computers that are able to use this mail server. It should be set to local only (`127.0.0.0/8` and the other representations). Modifying this to allow other hosts to use this is a huge vulnerability that can lead to extreme cases of spam.

To be clear, the line should be set like this. This should be set automatically, but double check the value in your file:

```
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
```

1.2 TLS

Configurare il TLS come da guida allegata nella stessa folder. Consiglio di configurarlo alla fine della installazione e quando la vm di ejbca è già installata in modo da generare il certificato tramite quella vm.

2.0 POSTFIX and MySQL

Per installare Postfix con relativo supporto agli utenti virtuali su MySQL eseguire i seguenti comandi.

I pacchetti necessari sono:

- **postfix-mysql**: il server di posta Postfix con il supporto per il database MySql;
- **mysql-server**: il server MySql;

```
sudo apt-get install postfix-mysql
sudo apt-get install mysql-server
```

Mettere la pwd desiderata per poi connettersi a MySQL.

2.1 Configurazione per MailaaS di PRISMA

Postfix nella configurazione usuale gira dentro una « jail », cioé in un sottosistema dal quale non è possibile raggiungere direttamente le risorse del sistema principale.

Non potrà quindi accedere al socket di MySQL, quindi se non avete configurato quest'ultimo per le connessioni TCP, dovete modificare il file /etc/mysql/my.cnf inserendo/decommentando la direttiva

```
bind-address = 127.0.0.1
```

Messo 0.0.0.0 per abilitare l'accesso esterno a tutti gli IP, o specificare quello che interessa

e quindi procedendo al riavvio del servizio MySQL con

```
/etc/init.d/mysql restart  (oppure service mysql restart)
```

In questo manuale si è preferito evitare di installare applicazioni web che amministrano database MySQL per questioni di sicurezza. (es. utilizzo di phpMyAdmin). Quindi le configurazioni saranno effettuate direttamente da comandi mysql sul server.

Accedere a mysql shell, e creare un utente di nome postfix con esempio pwd 'plutoPWD e db di nome mydatabasename:

```
USE mysql;
INSERT INTO user (Host, User, Password) VALUES ('localhost','postfix',password('plutoPWD'));
INSERT INTO db (Host, Db, User, Select_priv) VALUES ('localhost','mydatabasename','postfix','Y');
FLUSH PRIVILEGES;
GRANT USAGE ON mydatabasename.* TO postfix@localhost;
GRANT SELECT, INSERT, DELETE, UPDATE ON mydatabasename.* TO postfix@localhost;
CREATE DATABASE mydatabasename;
```

Ricordarsi di abilitare gli IP di mysql:
con il grant...
loggarsi come root e dare i privilegi all'utente postfix.

Valutare come configurare l'accesso al db, da ip specifici o meno. (es. abilitare modifiche al db ed accesso ai business layer, con % sono tutti gli IP.

Esempio di privilegi a postfix sul database mydatabasename per tutti gli ip:

```
GRANT ALL ON mydatabasename.* TO 'postfix'@'%'identified by 'plutoPWD';
```

Ricordarsi anche di configurare opportunamente il file /etc/mysql/my.cnf alla seguente riga del file:

```
bind-address        = 127.0.0.1
```

Creazione delle tabelle per MailaaS

Creare le tabelle nel database:

```
USE mydatabasename;

CREATE TABLE `virtual_domains` (
  `id` int(11) NOT NULL auto_increment,
  `name` varchar(50) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;


CREATE TABLE `virtual_users` (
  `id` int(11) NOT NULL auto_increment,
  `virtual_domain_id` int(11) NOT NULL,
  `user_prisma_id` bigint(20) NOT NULL,
  `user` varchar(100) NOT NULL,
  `password` varchar(128) NOT NULL,
  `email` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `email` (`email`),
  FOREIGN KEY (domain_id) REFERENCES virtual_domains(id) ON DELETE CASCADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Esempio di inserimento dati nella tabella.

```
USE mydatabasename;
INSERT INTO virtual_domains (name) VALUES ('mydomain.it');
```

Se si vuole aggiungere degli utenti iniziali lo si può fare tramite l'INSERT INTO direttamente da shell mysql. Poi comunque gli utenti del sistema verrano inseriti da sistema, accedendo all'interfaccia grafica della WEBUI del portale.

Di seguito il comando di esempio per poter inserire un utente:

```
INSERT INTO virtual_users (user,email,password,virtual_domain_id, user_prisma_id) VALUES ('
miouserprova1', ' miouserprova1@mydomain.it, MD5(' miouserprovapwd'),'1','123');
```

Ricordarsi di dare i privilege a mysql su quel db da parte degli IP che comunicheranno con esso, ad esempio del business layer.

3.0 Virtual user Postfix

User will be called vmail and will have a group with ID 5000 on the system.

Now we create a user and group called vmail with the home directory /home/vmail. This is where all mail boxes will be stored. That he belongs to group 5000 and that it's home folder is `/home/vmail`.

groupadd -g 5000 vmail
useradd -g vmail -u 5000 vmail -d /home/vmail –m

==========

Altra opzione:

In alcuni casi viene fatto invece una opzione in più:

```
useradd -s /usr/sbin/nologin -g vmail -u 5000 vmail -d /home/vmail -m
```

dove s /usr/sbin/nologin è fatto in modo che this user will not be able to log on to the system (unix)).

postconf -e 'virtual_mailbox_base = /home/vmail'
postconf -e 'virtual_uid_maps = static:5000'
postconf -e 'virtual_gid_maps = static:5000'

==========

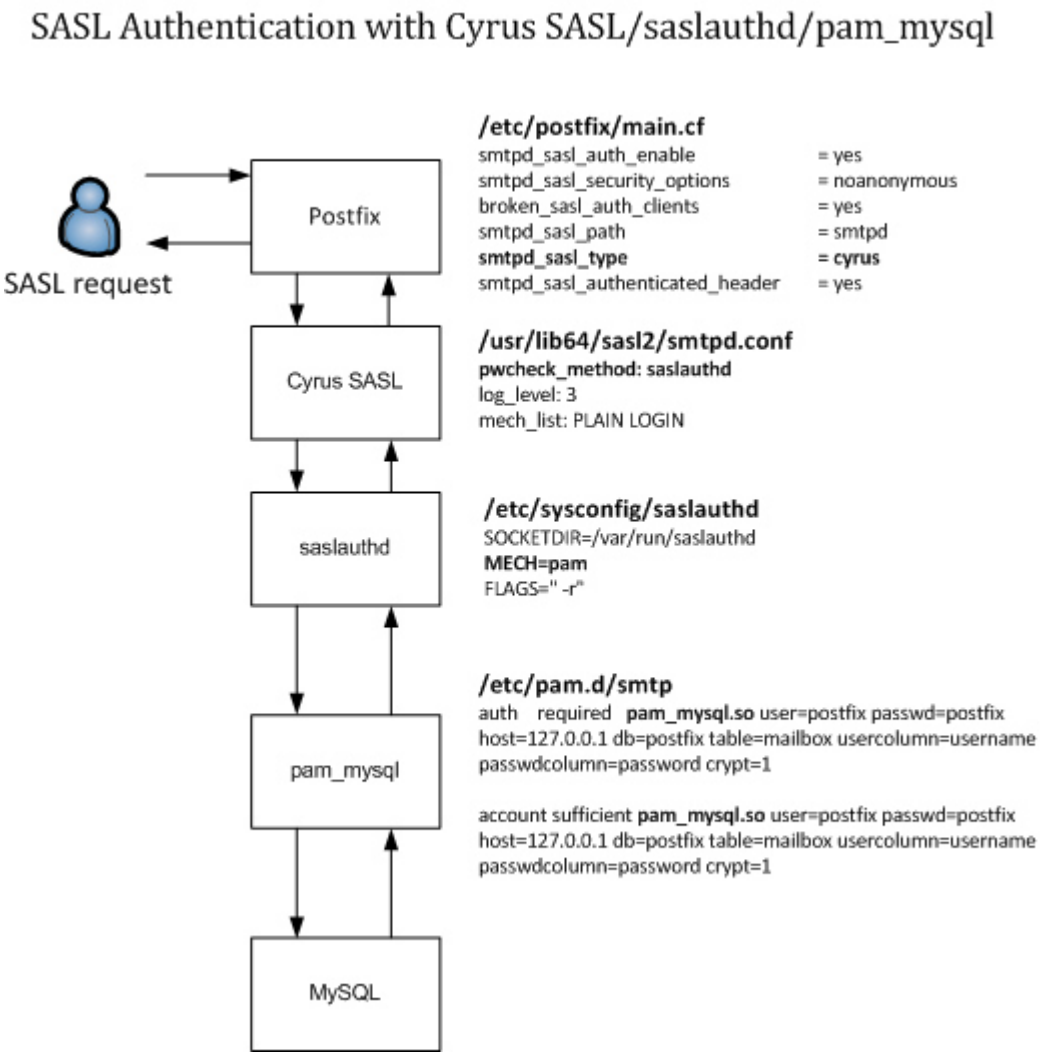
Dopo aver aggiunto vmail, andare a configurare il file /etc/postfixmain.cf:

#virtual user configuration

# vengono assegnate all'utente che gestirà le mailbox un uid e gid statici
# così da evitare di dover creare un utente reale per ogni utente virtuale
virtual_gid_maps = static:5000
virtual_uid_maps = static:5000
# questa direttiva indica dove verranno collocate le mailbox virtuali
virtual_mailbox_base = /home/vmail
# indica in quale file di configurazione sono presenti i parametri per ottenere la
# lista delle mailbox presenti nel sistema
virtual_minimum_uid = 5000
virtual_transport = virtual

4.0 AUTHENTICAZIONE – Architettura

Soluzione adottata per l'autenticazione in postfix.



3.1 Saslauthd

Since we want to allow users to log in to our mail server so they can send emails, we need to configure some kind of protection. First we need to make sure users can log in using the same username and password as the one they will be using for checking email.

For this, we are going to use Saslauthd. Saslauthd will also use the same database we already created to verify user credentials.

```
apt-get install libsasl2-2 libsasl2-modules libsasl2-modules-sql sasl2-bin
libpam-mysql
```

Open `/etc/default/saslauthd` with nano and change `START=no` to `START=yes`. At the end of the file we need to change `OPTIONS="-c -m /var/run/saslauthd"` to

```
OPTIONS="-c -r -m /var/spool/postfix/var/run/saslauthd"
```

This change needs to be made because Postfix on Debian is run under chroot so it needs access to saslauthd socket and adding of `-r` parameter is needed because otherwise username is not passed correctly from Postfix to saslauthd.

We also need to create this directory

```
mkdir -p /var/spool/postfix/var/run/saslauthd
```

and one symbolic link (because Postfix on Debian is running from a chrooted environment and other applications you maybe using on your server (including testsaslauthd for testing if saslauthd is working correctly) are not aware of us changing the saslauthd directory).

```
rm -rf /var/run/saslauthd

ln -s /var/spool/postfix/var/run/saslauthd /var/run/saslauthd
```

Warning

If you do not delete `/var/run/saslauthd` before creating a symbolic link the link will we created in `/var/run/saslauthd/saslauthd`and testing SASL with testsaslauthd will result in an error: "`connect() : No such file or directory 0`".

We also need to create two more files:

```
vi /etc/pam.d/smtp
```

```
auth    required   pam_mysql.so user=mailadmin passwd=newpassword host=127.0.0.1
db=mail table=mailbox usercolumn=username passwdcolumn=password crypt=0

account sufficient pam_mysql.so user=mailadmin passwd=newpassword host=127.0.0.1
db=mail table=mailbox usercolumn=username passwdcolumn=password crypt=0
```

Modificare opportunamente con i propri dati del database mysql di autenticazione, database, tabella ed algoritmo di crypting della pwd degli utenti di posta.

Esempio:

auth required pam_mysql.so user=postfix passwd=mypwdused host=127.0.0.1 db=myDBused table=virtual_users usercolumn=email passwdcolumn=password crypt=0

account sufficient pam_mysql.so user=postfix passwd=mypwdused host=127.0.0.1 db=myDBused table=virtual_users usercolumn=email passwdcolumn=password crypt=0

```
vi /etc/postfix/sasl/smtpd.conf
```

```
pwcheck_method: saslauthd
mech_list: plain login
allow_plaintext: true

io messo:
pwcheck_method: saslauthd
mech_list: plain login
allow_plaintext: true
log_level:3
```

We need to add Postfix to the sasl group so it can access the saslauthd process we just created:

```
adduser postfix sasl
```

Restart Postfix and sasl

```
/etc/init.d/postfix restart   (service postfix restart)
/etc/init.d/saslauthd restart
```

Now, we can check is saslauthd is working correctly.

```
testsaslauthd -s smtp -u root@example.com -p newpassword
```

Ofcourse use your own credentials here. Authentification should work.

```
atlantis:~# testsaslauthd -s smtp -u root@example.com -p newpassword
0: OK "Success."
```

If you do not get “Success.” as a response, check that you have a symbolic link in `/var/run/` named `saslauthd` and that it points to`/var/spool/postfix/var/run/saslauthd`.

We have to change permissions to these two files as well:

```
chgrp sasl /etc/pam.d/smtp
chmod 640 /etc/pam.d/smtp
chgrp postfix /etc/postfix/sasl/smtpd.conf
chmod 640 /etc/postfix/sasl/smtpd.conf
```

We also need to tell Postfix to allow authenticated users to send mail. Edit `/etc/postfix/main.cf` and add :

```
# SASL SUPPORT FOR CLIENTS
# The following options set parameters needed by Postfix to enable
# Cyrus-SASL support for authentication of mail clients.
#
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions = permit_sasl_authenticated, reject_unauth_destination, permit_mynetworks
check_relay_domain
```

Restart Postfix and sasl.

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

Esempio

```
root@nameServerMail:/# service postfix start
 * Starting Postfix Mail Transport Agent postfix
[ OK ]
root@nameServerMail:/# /etc/init.d/saslauthd start
 * Starting SASL Authentication Daemon saslauthd
```

5.0 DNS, MX record.

Creare FQDN, record MX sul dns. Aprire le porte per smtp porta 25, smtps..

Il *server* SMTP sulla *porta* 465 (con SSL) e sulla *porta 587* (con TLS).

Per evitare spam dal server Gmail è opportuno configurare il record SPF. Di seguito un esempio di spf configurato funzionante. Ovviamente cambiare i dati specifici con i propri:

This is the TXT DNS I had to add.
EXAMPLE

Code example:

```
v=spf1 a mx ip4:212.199.167.172 ~all
```

Ricordarsi sempre di aggiornare il dns sia ad esempio per

pr01mail01._____

mail._____ creare il record mx

ed aggiornare spf come da esempio sopra. Ricordarsi che da interfaccia web per configurare i DNS gli aggiormenti sono operativi solo se si preme sul tasto Apply!!

Aggiungere per evitare che le email vengano rejected questa riga nel file

/etc/postfix/main.cf:

always_add_missing_headers = yes

Si possono verificare i vari main.cf degli altri mail server configurati.