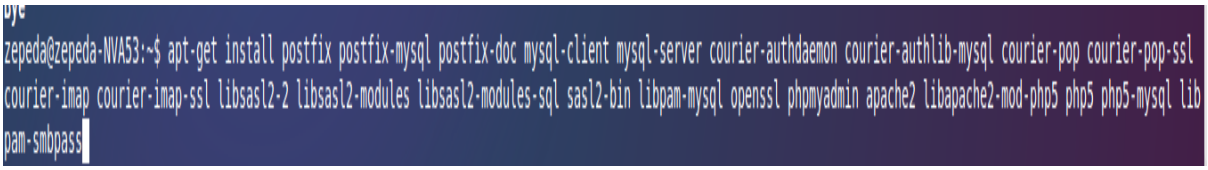
Servidor Postfix, IMAP, POP
* Instalación:
apt-get install postfix postfix-mysql postfix-doc mysql-client mysql-server courier-authdaemon courier-authlib-mysql courier-pop courier-pop-ssl courier-imap courier-imap-ssl libsasl2-2 libsasl2-modules libsasl2-modules-sql sasl2-bin libpam-mysql openssl phpmyadmin apache2 libapache2-mod-php5 php5 php5-mysql libpam-smbpass



Es necesario poner en la configuracion de correo no para directorio , sitio de internet , dominio de correo y ok para SSL

* Parchamos postfix para aceptar limite o cuota de correo
apt-get build-dep postfix

cd /usr/src
apt-get source postfix
wget http://vda.sourceforge.net/VDA/postfix-vda-v13-2.10.0.patch
cd postfix-2.11.0
patch -p1 < ../postfix-vda-v13-2.10.0.patch
(este depende de cual version tengamos instalada) editamos las reglas y ponemos lo siguiente vi debian/rules --> export DEB_BUILD_HARDENING=0
compilamos bien postfix dpkg-buildpackage
nos regresamos a la carpeta anterior y ejecutamos lo siguiente(depende de la version)
dpkg -i postfix_2.11.0-1_amd64.deb postfix-mysql_2.11.0-1_amd64.deb

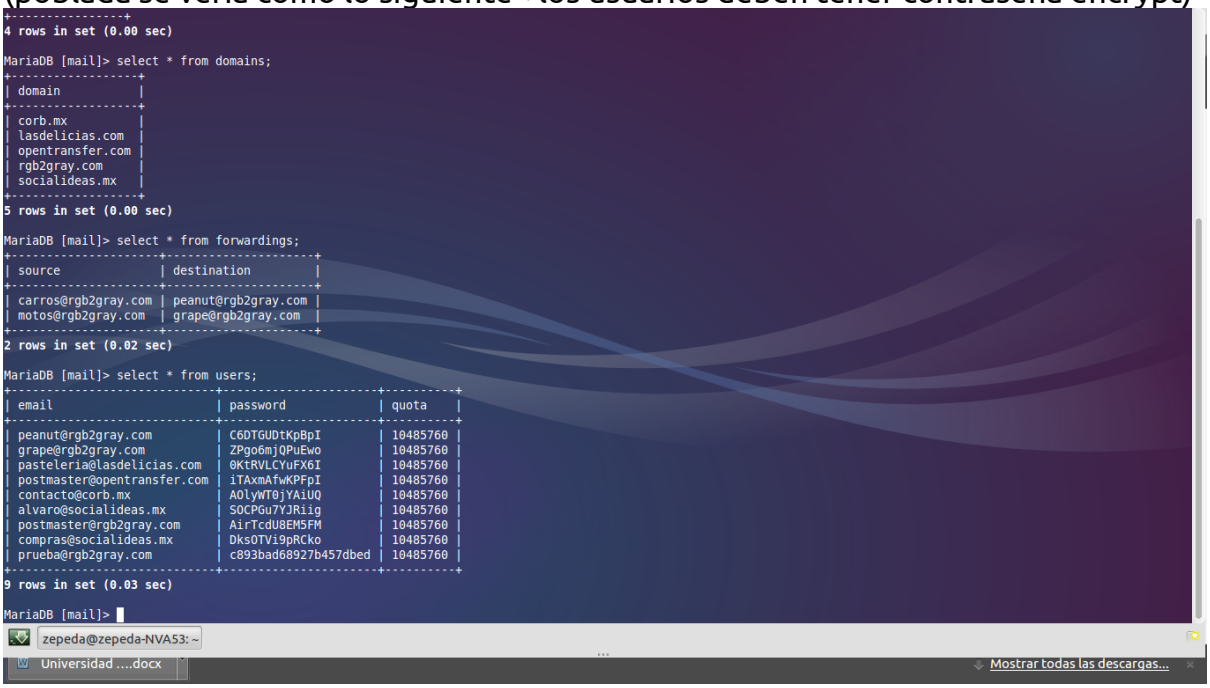
Ahora se configura la base de datos
mysqladmin -u root -p create mail
ingresamos a la base de datos y creamos usuario con privilegios:
GRANT SELECT, INSERT, UPDATE, DELETE ON mail.* TO 'mail_admin'@'localhost' IDENTIFIED BY 'mail_admin_password';
GRANT SELECT, INSERT, UPDATE, DELETE ON mail.* TO 'mail_admin'@'localhost.localdomain' IDENTIFIED BY 'mail_admin_password';
FLUSH PRIVILEGES;

despues se usa la base mail y se crean las tablas :
CREATE TABLE domains (
domain varchar(50) NOT NULL,
PRIMARY KEY (domain))
ENGINE=MyISAM;

CREATE TABLE forwardings (
source varchar(80) NOT NULL,
destination TEXT NOT NULL,
PRIMARY KEY (source))
ENGINE=MyISAM;

CREATE TABLE users (
email varchar(80) NOT NULL,
password varchar(20) NOT NULL,
quota INT(10) DEFAULT '10485760',
PRIMARY KEY (email)
) ENGINE=MyISAM;

(poblada se veria como lo siguiente< los usuarios deben tener contrasena encrypt)



Ahora se crean los archivos que permitiran la conexion a la base de datos:
vi /etc/postfix/mysql-virtual_domains.cf
user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT domain AS virtual FROM domains WHERE domain='%s'
hosts = 127.0.0.1
vi /etc/postfix/mysql-virtual_forwardings.cf
user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT destination FROM forwardings WHERE source='%s'
hosts = 127.0.0.1
vi /etc/postfix/mysql-virtual_mailboxes.cf
user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT CONCAT(SUBSTRING_INDEX(email,'@',-1),'/',SUBSTRING_INDEX
(email,'@',1),'/') FROM users WHERE email='%s'
hosts = 127.0.0.1
vi /etc/postfix/mysql-virtual_email2email.cf

user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT email FROM users WHERE email='%s'
hosts = 127.0.0.1
vi /etc/postfix/mysql-virtual_mailbox_limit_maps.cf
user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT quota FROM users WHERE email='%s'
hosts = 127.0.0.1

```
zepeda@zepeda-NVA53:/etc/postfix$ ls
dynamicmaps.cf  mysql-virtual_domains.cf      mysql-virtual_mailboxes.cf          postfix-files   sasl
main.cf         mysql-virtual_email2email.cf  mysql-virtual_mailbox_limit_maps.cf postfix-script  smtpd.cert
master.cf       mysql-virtual_forwardings.cf  mysql-virtual_transports.cf         post-install    smtpd.key
zepeda@zepeda-NVA53:/etc/postfix$
```

cambiamos los permisos de los archivos para que los pueda abrir postfix

```
chmod o= /etc/postfix/mysql-virtual_*.cf
chgrp postfix /etc/postfix/mysql-virtual_*.cf
```

y se crea el usuario para que ingrese a la carpeta de buzones

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

Ahora se agrega la configuracion al archivo de postfix main.cf

```
postconf -e 'myhostname = server1.example.com'
postconf -e 'mydestination = server1.example.com, localhost,
localhost.localdomain'
postconf -e 'mynetworks = 127.0.0.0/8'
postconf -e 'virtual_alias_domains ='
postconf -e 'virtual_alias_maps = proxy:mysql:/etc/postfix/
mysql-virtual_forwardings.cf, mysql:/etc/postfix/mysql-
virtual_email2email.cf'
postconf -e 'virtual_mailbox_domains = proxy:mysql:/etc/
postfix/mysql-virtual_domains.cf'
postconf -e 'virtual_mailbox_maps = proxy:mysql:/etc/postfix/
mysql-virtual_mailboxes.cf'
postconf -e 'virtual_mailbox_base = /home/vmail'
postconf -e 'virtual_uid_maps = static:5000'
postconf -e 'virtual_gid_maps = static:5000'
postconf -e 'smtpd_sasl_auth_enable = yes'
postconf -e 'broken_sasl_auth_clients = yes'
postconf -e 'smtpd_sasl_authenticated_header = yes'
postconf -e 'smtpd_recipient_restrictions = permit_mynetworks,
permit_sasl_authenticated, reject_unauth_destination'
postconf -e 'smtpd_use_tls = yes'
postconf -e 'smtpd_tls_cert_file = /etc/postfix/smtpd.cert'
postconf -e 'smtpd_tls_key_file = /etc/postfix/smtpd.key'

postconf -e 'virtual_maildir_extended = yes'
```

postconf -e 'virtual_mailbox_limit_maps = proxy:mysql:/etc/postfix/mysql-virtual_mailbox_limit_maps.cf'
postconf -e 'virtual_mailbox_limit_override = yes'
postconf -e 'virtual_maildir_limit_message = "The user you are trying to reach is over quota."'
postconf -e 'virtual_overquota_bounce = yes'
postconf -e 'proxy_read_maps = $local_recipient_maps $mydestination $virtual_alias_maps $virtual_alias_domains $virtual_mailbox_maps $virtual_mailbox_domains $relay_recipient_maps $relay_domains $canonical_maps $sender_canonical_maps $recipient_canonical_maps $relocated_maps $transport_maps $mynetworks $virtual_mailbox_limit_maps'

cd /etc/postfix
openssl req -new -outform PEM -out smtpd.cert -newkey rsa:2048 -nodes -keyout smtpd.key -keyform PEM -days 365 -x509
Con este comando se genera un certificado para el servidor y ahora se cambian los permisos del certificado chmod o= /etc/postfix/smtpd.key
creamos la siguiente carpeta mkdir -p /var/spool/postfix/var/run/saslauthd y modificamos el archivo /etc/default/saslauthd al cual le agregaremos en start yes y en options lo siguiente OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd -r", ahora se edita el siguiente archivo /etc/pam.d/smtp y agregamos las lineas auth required pam_mysql.so user=mail_admin passwd=mail_admin_password host=127.0.0.1 db=mail table=users usercolumn=email passwdcolumn=password crypt=1
account sufficient pam_mysql.so user=mail_admin passwd=mail_admin_password

host=127.0.0.1 db=mail table=users usercolumn=email passwdcolumn=password crypt=1

```
auth    required   pam_mysql.so user=mail_admin passwd=mail_admin_password host=127.0.0.1 db=mail table=users usercolumn=email passwdcolumn=password crypt=1
account sufficient pam_mysql.so user=mail_admin passwd=mail_admin_password host=127.0.0.1 db=mail table=users usercolumn=email passwdcolumn=password crypt=1
```

ahora se crea el siguiente archivo
/etc/postfix/sasl/smtpd.conf

pwcheck_method: saslauthd
mech_list: plain login
allow_plaintext: true
auxprop_plugin: sql
sql_engine: mysql
sql_hostnames: 127.0.0.1
sql_user: mail_admin
sql_passwd: mail_admin_password
sql_database: mail
sql_select: select password from users where email = '%u@%r'

el cual contiene instrucciones sobre la base de datos.
después de ello agregamos el usuario postfix al grupo sasl
adduser postfix sasl y reiniciamos servicio service postfix restart service saslauthd restart,
ahora configuraremos el servicio courier al cual después de abrirlo se agregara la linea
/etc/courier/authdaemonrc
authmodulelist="authmysql"
eliminamos la información de este archivo y lo modificamos agregando lo siguiente

cat /dev/null > /etc/courier/authmysqlrc

```
MYSQL_SERVER localhost
MYSQL_USERNAME mail_admin
MYSQL_PASSWORD mail_admin_password
MYSQL_PORT 0
MYSQL_DATABASE mail
MYSQL_USER_TABLE users
MYSQL_CRYPT_PWFIELD password
#MYSQL_CLEAR_PWFIELD password
MYSQL_UID_FIELD 5000
MYSQL_GID_FIELD 5000
MYSQL_LOGIN_FIELD email
MYSQL_HOME_FIELD "/home/vmail"
MYSQL_MAILDIR_FIELD CONCAT(SUBSTRING_INDEX(email,'@',-1),'/',SUBSTRING_INDEX(email,'@',1),'/')
#MYSQL_NAME_FIELD
MYSQL_QUOTA_FIELD quota
```

ahora vamos a courier y eliminamos certificados de imap y pop
cd /etc/courier
rm -f /etc/courier/imapd.pem
rm -f /etc/courier/pop3d.pem
despues abrimos el archivo de pop [pop3d.cnf] e imap [imapd.cnf] y ponemos en CN= nuestro dominio real , recreamos los certificados mkimapdcert
mkpop3dcert

por ultimo reiniciamos los servicio
service courier-authdaemon restart
service courier-imap restart

service courier-imap-ssl restart
service courier-pop restart
service courier-pop-ssl restart

y el servidor esta listo para ser usado