Set up a mail server with PostfixAdmin and MariaDB on CentOS 7

1. Add software repos, Update the system and install necessary packages

Add software repositories; elrepo, epel, remi and rpmfusion

#yum update

2. Create system user

For security reasons, we will create a new system user who will be the owner of all mailboxes.

useradd -r -u 150 -g mail -d /var/vmail -s /sbin/nologin -c "Virtual Mail User" vmail
mkdir -p /var/vmail
chmod -R 770 /var/vmail
chown -R vmail:mail /var/vmail

3. Install MariaDB

MariaDB 5.5 is shipped in the default CentOS 7 repository, to install it just run:

#yum install mariadb-server

To start the MariaDB service and enable it to start on boot, execute the following commands:

#systemctl start mariadb.service
#systemctl enable mariadb.service

Run the following command to secure your MariaDB installation:

#mysql_secure_installation

Next, we need to create a database for our postfixadminHQ instance.

#mysql -uroot -p
MariaDB [(none)]> CREATE DATABASE postfixadmin;
MariaDB [(none)]> GRANT ALL PRIVILEGES ON postfixadmin.* TO 'postfixadmin'@'localhost' IDENTIFIED BY 'strong_password';
MariaDB [(none)]> FLUSH PRIVILEGES;
MariaDB [(none)]> \q

4. Install PHP and all necessary PHP modules

#yum-config-manager --enable remi-php71.repo
#yum-config-manager --disable remi-php54.repo
#yum install php php-mysql php-imap php-mbstring php-common

If you don’t have Apache installed, install it with:

#yum install httpd

5. Install PostfixAdmin

Download the PostfixAdmin archive from SourceForge and extract it in the /var/www/html/ directory:

wget -q -O - "https://downloads.sourceforge.net/project/postfixadmin/postfixadmin/postfixadmin-3.0.2/postfixadmin-3.0.2.tar.gz" | tar -xzf - -C /var/www/html

Open the mail configuration file and edit the following values:

#vim /var/www/html/postfixadmin-3.0.2/config.inc.php

```
$CONF['configured'] = true;
$CONF['database_type'] = 'mysqli';
$CONF['database_host'] = 'localhost';
$CONF['database_user'] = 'postfixadmin';
$CONF['database_password'] = 'strong_password';
$CONF['database_name'] = 'postfixadmin';

$CONF['domain_path'] = 'NO';
$CONF['domain_in_mailbox'] = 'YES';
```

#chown -R apache: /var/www/html/postfixadmin-3.0.2

To populate the database go to https://Your_IP_Address/postfixadmin-3.0.2/setup.php

Create a new admin user:

#bash /var/www/html/postfixadmin-3.0.2/scripts/postfixadmin-cli admin add admin@your_domain_name.com --password strong_password22 --password2 strong_password22 --superadmin 1 --active 1

6. Install and configure postfix

To install postfix run the command bellow:

#yum install postfix

Once the installation is completed, we need to create configuration files:

#mkdir -p /etc/postfix/sql/

#vim /etc/postfix/sql/mysql_virtual_alias_domain_catchall_maps.cf

```
user = postfixadmin
password = strong_password
hosts = localhost
dbname = postfixadmin
query  = SELECT goto FROM alias,alias_domain WHERE alias_domain.alias_domain = '%d' and alias.address = CONCAT('@', alias_domain.target_domain) AND alias.active = 1 AND alias_domain.active='1'
```

#vim /etc/postfix/sql/mysql_virtual_alias_domain_mailbox_maps.cf

```
user = postfixadmin
password = strong_password
hosts = localhost
dbname = postfixadmin
query = SELECT maildir FROM mailbox,alias_domain WHERE alias_domain.alias_domain = '%d' and mailbox.username = CONCAT('%u', '@', alias_domain.target_domain) AND mailbox.active = 1 AND alias_domain.active='1'
```

#vim /etc/postfix/sql/mysql_virtual_alias_domain_maps.cf

```
user = postfixadmin
password = strong_password
hosts = localhost
dbname = postfixadmin
query = SELECT goto FROM alias,alias_domain WHERE alias_domain.alias_domain = '%d' and alias.address = CONCAT('%u', '@', alias_domain.target_domain) AND alias.active = 1 AND alias_domain.active='1'
```

#vim /etc/postfix/sql/mysql_virtual_alias_maps.cf

```
user = postfixadmin
password = strong_password
hosts = localhost
dbname = postfixadmin
query = SELECT goto FROM alias WHERE address='%s' AND active = '1'
#expansion_limit = 100
```

#vim /etc/postfix/sql/mysql_virtual_domains_maps.cf

```
user = postfixadmin
password = strong_password
hosts = localhost
dbname = postfixadmin
query          = SELECT domain FROM domain WHERE domain='%s' AND active = '1'
#query          = SELECT domain FROM domain WHERE domain='%s'
#optional query to use when relaying for backup MX
#query          = SELECT domain FROM domain WHERE domain='%s' AND backupmx = '0' AND active = '1'
#expansion_limit = 100
```

#vim /etc/postfix/sql/mysql_virtual_mailbox_limit_maps.cf

```
user = postfixadmin
password = strong_password
hosts = localhost
dbname = postfixadmin
query = SELECT quota FROM mailbox WHERE username='%s' AND active = '1'
```

#vim /etc/postfix/sql/mysql_virtual_mailbox_maps.cf

```
user = postfixadmin
password = strong_password
hosts = localhost
dbname = postfixadmin
query          = SELECT maildir FROM mailbox WHERE username='%s' AND active = '1'
#expansion_limit = 100
```

Edit the main.cf file:

```
#postconf -e "myhostname = $(hostname -f)"

#postconf -e "virtual_mailbox_domains =
#proxy:mysql:/etc/postfix/sql/mysql_virtual_domains_maps.cf"
#postconf -e "virtual_alias_maps = proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_maps.cf,
#proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_maps.cf,
#proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_catchall_maps.cf"
#postconf -e "virtual_mailbox_maps =
#proxy:mysql:/etc/postfix/sql/mysql_virtual_mailbox_maps.cf,
#proxy:mysql:/etc/postfix/sql/mysql_virtual_alias_domain_mailbox_maps.cf"

#postconf -e "smtpd_tls_cert_file = /etc/pki/tls/certs/localhost.crt"
#postconf -e "smtpd_tls_key_file = /etc/pki/tls/private/localhost.key"
#postconf -e "smtpd_use_tls = yes"
#postconf -e "smtpd_tls_auth_only = yes"

#postconf -e "smtpd_sasl_type = dovecot"
#postconf -e "smtpd_sasl_path = private/auth"
#postconf -e "smtpd_sasl_auth_enable = yes"
#postconf -e "smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks,
reject_unauth_destination"

#postconf -e "mydestination = localhost"
#postconf -e "mynetworks = 192.168.0.0/24"
#postconf -e "inet_protocols = ipv4"
#postconf -e "inet_interfaces = all"

#postconf -e "virtual_transport = lmtp:unix:private/dovecot-lmtp"
```

Open the master.cf file, find submission inet n and smtps inet n sections and edit as follows:

#vim /etc/postfix/master.cf

```
submission inet n       -       n       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
```

```
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
smtps     inet  n       -       n       -       -       smtpd
  -o syslog_name=postfix/smtps
#  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#  -o smtpd_client_restrictions=$mua_client_restrictions
#  -o smtpd_helo_restrictions=$mua_helo_restrictions
#  -o smtpd_sender_restrictions=$mua_sender_restrictions
#  -o smtpd_recipient_restrictions=
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
```

Enable the postfix service

```
#systemctl enable postfix
#systemctl restart postfix
```

7. Install and Configure Dovecot

Install dovecot with MySQL support using the command bellow:

```
#yum install dovecot dovecot-mysql
```

Open the /etc/dovecot/conf.d/10-mail.conf file and change the following values:

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

mail_location = maildir:/var/vmail/%d/%n
mail_privileged_group = mail
mail_uid = vmail
mail_gid = mail
first_valid_uid = 150
last_valid_uid = 150
```

Open the /etc/dovecot/conf.d/10-auth.conf file and change the following values:

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

auth_mechanisms = plain login
#!include auth-system.conf.ext
!include auth-sql.conf.ext
```

Create a new dovecot-sql.conf.ext file:

```
#vim /etc/dovecot/dovecot-sql.conf.ext

driver = mysql
connect = host=localhost dbname=postfixadmin user=postfixadmin password=strong_password
```

default_pass_scheme = MD5-CRYPT
password_query = SELECT username as user, password, '/var/vmail/%d/%n' as userdb_home, 'maildir:/var/vmail/%d/%n' as userdb_mail, 150 as userdb_uid, 8 as userdb_gid FROM mailbox WHERE username = '%u' AND active = '1'
user_query = SELECT '/var/vmail/%d/%u' as home, 'maildir:/var/vmail/%d/%u' as mail, 150 AS uid, 8 AS gid, concat('dirsize:storage=', quota) AS quota FROM mailbox WHERE username = '%u' AND active = '1'

In the /etc/dovecot/conf.d/10-ssl.conf file enable SSL support:

ssl = yes

Open the /etc/dovecot/conf.d/15-lda.conf file and set the postmaster_address email address.

#postmaster_address = postmaster@llcmail.com

Open the /etc/dovecot/conf.d/10-master.conf file, find the service lmtp section and change it to:

```
service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    mode = 0600
    user = postfix
    group = postfix
  }
}
```

find the service auth section and change it to:

```
service auth {
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }
  unix_listener auth-userdb {
    mode = 0600
    user = vmail
    #group = vmail
  }
  user = dovecot
}
```

Change the service auth-worker section to the following:

```
service auth-worker {
  user = vmail
}
```

Set the permissions:

```
#chown -R vmail:dovecot /etc/dovecot
#chmod -R o-rwx /etc/dovecot
```

Enable and restart the dovecot service

#systemctl enable dovecot
#systemctl restart dovecot

8. Install and configure Spamassassin

Install spamassassin using the command bellow:

#yum install spamassassin

Create a spamassassin system user:

groupadd spamd
useradd -g spamd -s /bin/false -d /var/log/spamassassin spamd
chown spamd:spamd /var/log/spamassassin

9. Configure Postfix to use SpamAssassin

Open the master.cf file and edit as follows:

#vim /etc/postfix/master.cf

change

smtp inet n - n - - smtpd

with

smtp inet n - n - - smtpd -o content_filter=spamassassin

add the following line at the end of the file:

spamassassin unix - n n - - pipe flags=R user=spamd argv=/usr/bin/spamc -e /usr/sbin/sendmail -oi -f ${sender} ${recipient}

Enable and restart the spamassassin service

#systemctl enable spamassassin
#systemctl restart spamassassin

Restart the postfix service

#systemctl restart postfix

If everything is set up correctly now you should be able to log in to your PostfixAdmin backend by going to http://192.168.0.23/postfixadmin-3.0.2.2 and create your first virtual domain and mailbox.

Setting up RoundCube

1. Create a MariaDB username and database for the Roundcube installation. Log into the MariaDB client with the command:
#mysql -u root -p

2. Log in with the root password, then create a Roundcube database:
#create database roundcube_db;

4. Create a user for this database.
#grant all on roundcube_db.* to roundcube_user@localhost identified by 'roundcube_db_password';

Replace:

roundcube_user with the username you want to create for your database.
roundcube_db_password with a strong password for this user.

Then exit MariaDB:

quit;

5. Go to your website's document root. Download the current release from the Roundcube website by using the command:
#sudo wget https://github.com/roundcube/roundcubemail/releases/download/1.2.3/roundcubemail-1.2.3-complete.tar.gz

6. Uncompress this file to your webroot
#tar -xvf roundcubemail-1.2.3-complete.tar.gz -C /var/www/html/

7. Rename the extracted directory roundcube:
#mv roundcubemail-1.2.3 roundcube

8. Set the ownership of the files to the Apache user:
#chown -R apache:apache roundcube

To complete the installation, switch to a browser and go to the URL http://192.168.0.23/roundcube/installer/.
Scroll down to the bottom of the page and click NEXT.
In the next section, you will need to fill out the database information.
Fill out the MariaDB database name, username, and password which you created above. Then scroll down and click CREATE CONFIG.

Note: There are many potential configurations. You can change or set them at any time in the future.

After the config file is created, click CONTINUE to continue.

Click the Initialize database button to set up the database.

Test the mail server configuration by sending a test SMTP email.

Sender: Your new email address on this server. (For example, faith@llcmail.com)
Recipient: An external email address. (For example, alex@llcmail.com)

Then click Send test mail. After a few moments, check the external email account to see if your email was sent.

Test the IMAP configurations by logging in with your username and password.

Note that your username is NOT your full email address. For example, log in with the username faith, not faith@llcmail.com.

Now that the configuration is complete, you can log in at http://192.168.0.23/webmail to check and send email.