
Servidor de correu

Índex

1. Introducció	1
2. Arquitectura del sistema	2
3. Funcionament general	2
4. Seguretat i ports	3
4.1. Taula resum	3
5. Configuracions prèvies	3
6. Postfix	4
6.1. Configuració de Postfix	4
6.2. Autenticació SMTP	5
6.3. Configuració de l'autenticació SMTP	5
6.4. Configuració TLS	6
7. SASL (Simple Authentication and Security Layer)	6
8. SMTPS (SMTP sobre SSL/TLS implícit)	8
9. STARTTLS	8
10. Dovecot	9
10.1. Configuració SSL de Dovecot	9
11. Creació d'un compte de correu	10
12. Instal·lació del webmail Rainloop	10
12.1. Configuració de Rainloop	11
12.2. Configuració HTTP (redirecció a HTTPS)	11
12.3. Protecció del directori data	12
12.4. Habilita mòduls i llocs d'Apache	12
12.5. Dominis (Rainloop)	13
13. Contactes de correu (MariaDB + Rainloop)	14

Aquest document és una guia tècnica detallada per implementar un servidor de correu segur en un entorn GNU/Linux. El manual descriu la configuració de Postfix com a agent de transport, Dovecot per a la gestió de bústies i Rainloop com a interfície de correu web. Es posa un èmfasi especial en la seguretat, detallant l'ús de certificats TLS/SSL i l'autenticació SASL. A més, s'inclouen instruccions per integrar una base de dades MariaDB destinada a la gestió de contactes. Tot el procés està orientat a crear una infraestructura completa que permeti l'enviament i la recepció de missatges sota protocols estàndards i xifrats.

1. Introducció

En aquest document es descriu el procés d'instal·lació i configuració d'un servidor de correu electrònic segur en un entorn GNU/Linux Ubuntu Server 24.04 utilitzant Postfix, Dovecot i Rainloop.

L'objectiu és implementar una infraestructura completa de correu que permeti:

- Enviar i rebre missatges mitjançant el protocol SMTP
- Accedir al correu a través d'IMAP/IMAPS
- Garantir comunicacions xifrades amb TLS
- Habilitar autenticació segura mitjançant SASL
- Proporcionar una interfície web d'accés al correu (webmail)

2. Arquitectura del sistema

El sistema es basa en la separació funcional dels diferents components:

- **Postfix (MTA -- Mail Transfer Agent):** gestiona el transport del correu electrònic.
- **Dovecot (MDA / IMAP Server):** accés a bústies per IMAP/POP3 i autenticació.
- **Rainloop (Webmail):** interfície web per llegir i enviar correu.
- **MariaDB (Base de dades):** emmagatzema informació addicional (ex. contactes del webmail).

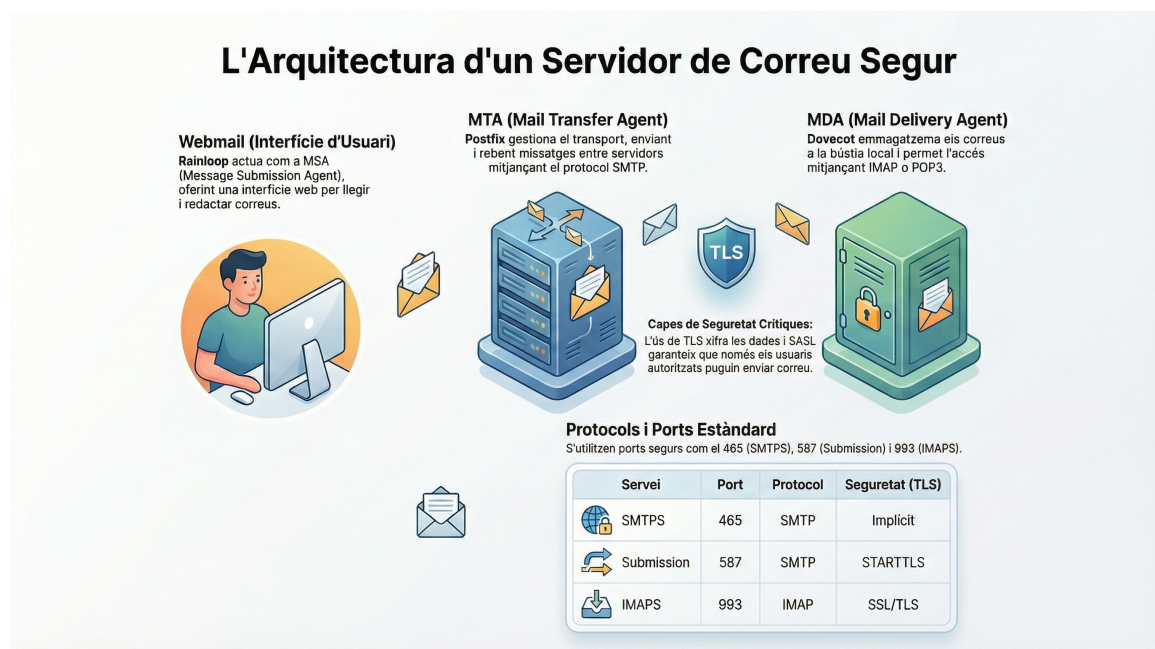


Figura 1: Arquitectura d'un servidor de correu segur

3. Funcionament general

El flux de correu dins del sistema és el següent:

- **Recepció de correu:** Un servidor extern envia un missatge al nostre servidor -> Postfix el rep -> el lliura a la bústia corresponent -> Dovecot el posa a disposició de l'usuari.
- **Enviament de correu:** L'usuari accedeix a Rainloop -> Rainloop envia el missatge a Postfix mitjançant SMTP autènticat -> Postfix el lliura al servidor destinatari.

4. Seguretat i ports

La configuració inclou:

- Xifrat de les comunicacions mitjançant TLS
- Autenticació SMTP amb SASL
- Ús de ports segurs com IMAPS (993), SMTPS (465) i Submission (587)

Aquesta implementació permet construir un servidor de correu funcional i segur, adequat per a entorns de pràctica o laboratoris formatius, i estableix les bases per a una possible adaptació a entorns de producció.

4.1. Taula resum

Servei	Port	Protocol	TLS
SMTP	25	SMTP	Opcional
SMTPS	465	SMTP	Implícit
Submission	587	SMTP	STARTTLS
IMAPS	993	IMAP	SSL

5. Configuracions prèvies

Abans de començar, fes les configuracions bàsiques del servidor (hostname, IP, hosts, ports i actualització).

```
# Canvia el nom de la màquina
sudo hostnamectl set-hostname servidor

# Configura la interfície de xarxa
sudo nano /etc/netplan/50-cloud-init.yaml
```

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses:
        - "10.0.3.70/24"
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
      search: []
      routes:
        - to: "default"
          via: "10.0.3.1"
```

```
# Edita el fitxer de hosts
sudo nano /etc/hosts
```

```
127.0.0.1 localhost
127.0.1.1 servidor
10.0.3.70 servidor.thos.local thos.local servidor
```

```
# Actualitza paquets
sudo apt update
sudo apt upgrade
```

6. Postfix

Inicialment, pots acceptar els valors per defecte prement Enter per a cada pregunta. Algunes de les opcions de configuració s'investigaran amb més detall a la fase de configuració.

```
# Instal·la postfix
sudo apt install postfix
```

6.1. Configuració de Postfix

Hi ha quatre coses que has de decidir abans de configurar:

- La xarxa i el rang de classes del servidor de correu (10.0.3.0/24)
- El domini de correu electrònic (thos.local)
- El nom d'usuari (ex. ramon)
- El format de la bústia: predeterminat mbox, però es recomana Maildir

```
# Configura postfix
sudo dpkg-reconfigure postfix
```

Es mostrarà la interfície d'usuari. A cada pantalla, selecciona els valors següents (exemple):

```
Lloc d'Internet
thos.local
ramon
thos.local, localhost.localdomain, localhost
No
127.0.0.0/8 10.0.3.0/24
0
+
ipv4
```

Per definir el format de la bústia de correu, pots editar directament el fitxer o utilitzar postconf. En qualsevol cas, els paràmetres s'emmagatzemen a /etc/postfix/main.cf

```
# Configura el format de la bústia (Maildir)
sudo postconf -e 'home_mailbox = Maildir/'
```

Això col·locarà el correu nou a /home/<nom d'usuari>/Maildir, de manera que hauràs de configurar el teu agent de lliurament de correu (MDA) per utilitzar la mateixa ruta.

6.2. Autenticació SMTP

SMTP-AUTH permet a un client identificar-se mitjançant el mecanisme d'autenticació Simple Authentication and Security Layer (SASL), utilitzant Transport Layer Security (TLS) per xifrar el procés d'autenticació. Un cop s'hagi autenticat, el servidor SMTP permetrà al client retransmetre el correu.

6.3. Configuració de l'autenticació SMTP

Per configurar Postfix per a SMTP-AUTH mitjançant SASL (Dovecot SASL), executa aquestes ordres al terminal:

```
sudo postconf -e 'smtpd_sasl_type = dovecot'
sudo postconf -e 'smtpd_sasl_path = private/auth'
sudo postconf -e 'smtpd_sasl_local_domain ='
sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
sudo postconf -e 'broken_sasl_auth_clients = yes'
sudo postconf -e 'smtpd_sasl_auth_enable = yes'
sudo postconf -e 'smtpd_recipient_restrictions =
↳ permit_sasl_authenticated,
↳ permit_mynetworks,reject_unauth_destination'
```

NOTA

El paràmetre de configuració **smtpd_sasl_path** és una ruta relativa al directori de cua de Postfix.

Hi ha diverses propietats del mecanisme SASL que val la pena avaluar per millorar la seguretat del desplegament. L'opció **"noanonymous"** impedeix l'ús de mecanismes que permeten l'autenticació anònima.

6.4. Configuració TLS

La seguretat requereix xifrar la comunicació. S'utilitzen certificats TLS/SSL (autosignats en laboratoris, o CA en producció).

A continuació, genera o obté un certificat digital per a TLS. Els MUA que es connecten al servidor de correu mitjançant TLS hauran de reconèixer el certificat utilitzat per a TLS. Això es pot fer mitjançant un certificat de Let's Encrypt, d'una CA comercial o amb un certificat autosignat que els usuaris instal·len/accepten manualment. Per a MTA-a-MTA, els certificats TLS mai es validen sense l'acord previ de les organitzacions afectades. Per a TLS MTA-a-MTA, no hi ha cap raó per no utilitzar un certificat autosignat tret que la política local ho requereixi.

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
↳ /etc/ssl/private/server.key -out /etc/ssl/certs/server.crt -subj
↳ "/C=ES/ST=Barcelona/L=Mataro/O=IES Thos i
↳ Codina/OU=ASIX/CN=thos.local/emailAddress=ramon@thosicodina.cat"
sudo postconf -e 'smtp_tls_security_level = may'
sudo postconf -e 'smtpd_tls_security_level = encrypt'
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
sudo postconf -e 'smtpd_tls_loglevel = 1'
sudo postconf -e 'smtpd_tls_received_header = yes'
sudo postconf -e 'myhostname = thos.local'
sudo postconf -e 'smtpd_tls_cert_file=/etc/ssl/certs/server.crt'
sudo postconf -e 'smtpd_tls_key_file=/etc/ssl/private/server.key'
```

La configuració inicial de Postfix ja s'ha completat. Reinicia el dimoni de Postfix i comprova l'estat.

```
# Reinicia el dimoni
sudo systemctl restart postfix

# Comprova l'estat
sudo systemctl status postfix
```

7. SASL (Simple Authentication and Security Layer)

Postfix admet el mecanisme d'autenticació SMTP-AUTH tal com es defineix a RFC2554. Està basat en SASL. Tanmateix, encara cal configurar l'autenticació SASL abans de poder utilitzar SMTP-AUTH.

SASL permet autenticació segura per a SMTP. En aquesta guia s'integra amb Dovecot per oferir SMTP-AUTH.

```
sudo apt install dovecot-core

# Configura el socket d'autenticació per Postfix
sudo nano /etc/dovecot/conf.d/10-master.conf
```

```
# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
  mode = 0660
  user = postfix
  group = postfix
}
```

```
# Activa mecanismes d'autenticació (compatibilitat)
sudo nano /etc/dovecot/conf.d/10-auth.conf
```

```
auth_mechanisms = plain login
```

```
# Un cop hagi configurat Dovecot, reinicia-lo i comprova l'estat.
sudo systemctl restart dovecot
sudo systemctl status dovecot
```

Comprovació STARTTLS (exemple d'output):

La configuració SMTP-AUTH s'ha completat; ara és el moment de provar la configuració. Per veure si SMTP-AUTH i TLS funcionen correctament, executa l'ordre següent:

```
sudo telnet thos.local 25
```

```
ehlo thos.local
```

```
250-thos.local
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
```

8. SMTPS (SMTP sobre SSL/TLS implícit)

SMTPS (port 465) és el protocol SMTP però amb xifratge TLS des del primer moment (TLS implícit). Es configura al fitxer `/etc/postfix/master.cf`

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

```
smtps inet n - y - - smtpd
-o syslog_name=postfix/smtps
-o smtpd_tls_wrappermode=yes
-o smtpd_sasl_auth_enable=yes
-o smtpd_sasl_type=dovecot
-o smtpd_sasl_path=private/auth
-o smtpd_recipient_restrictions=permit_sasl_authenticated,
↪ permit_mynetworks,reject_unauth_destination
```

```
# Reinicia el dimoni de Postfix
sudo systemctl restart postfix

# Prova que el 465 dona certificat
sudo openssl s_client -connect thos.local:465 -crlf -servername
↪ thos.local
```

9. STARTTLS

STARTTLS (port 587) és una ordre que permet convertir una connexió no xifrada en una connexió xifrada, utilitzant TLS (TLS explícit). És a dir, comences parlant en text pla i després “actives” el xifratge dins la mateixa connexió. És l'opció habitual per a “Submission” i clients de correu.

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

```
submission inet n - y - - smtpd
-o syslog_name=postfix/submission
-o smtpd_tls_security_level=encrypt
-o smtpd_sasl_auth_enable=yes
-o smtpd_sasl_type=dovecot
-o smtpd_sasl_path=private/auth
-o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
-o smtpd_tls_auth_only=yes
```

```
# Reinicia el dimoni de Postfix
sudo systemctl restart postfix

# Comprova que el 587 està escoltant
sudo ss -tlnp | grep 587
```

```
# Prova STARTTLS manualment
sudo openssl s_client -starttls smtp -connect thos.local:587
```

10. Dovecot

Dovecot és el servidor IMAP/POP3 que permet accés a les bústies, i també s'utilitza per autenticació (SASL). Configura l'emmagatzematge en Maildir i activa SSL per IMAPS.

```
sudo apt install dovecot-imapd dovecot-pop3d
sudo nano /etc/dovecot/dovecot.conf
```

```
listen = *, ::
```

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

```
disable_plaintext_auth = no
auth_username_format = %n
```

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

```
mail_location = maildir:~/Maildir
```

```
# Reinicia el dimoni de dovecot
sudo systemctl restart dovecot
```

10.1. Configuració SSL de Dovecot

Per defecte, Dovecot està configurat per utilitzar SSL automàticament mitjançant el paquet `ssl-cert` que proporciona un certificat autosignat.

En comptes d'això, pots generar el teu propi certificat personalitzat per a Dovecot utilitzant `openssl`, per exemple:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
↳ /etc/dovecot/private/dovecot.key -out
↳ /etc/dovecot/private/dovecot.pem -subj
↳ "/C=ES/ST=Barcelona/L=Mataró/O=IES Thos i
↳ Codina/OU=ASIX/CN=thos.local/emailAddress=ramon@thosicodina.cat"
```

11. Creació d'un compte de correu

```
# Crea un compte (usuari local).
sudo adduser alumne1
```

12. Instal·lació del webmail Rainloop

RainLoop és un client de correu web (webmail) simple, modern i ràpid, basat en web.

Característiques principals:

- És una aplicació de codi obert que gestiona múltiples comptes de correu sense necessitat de base de dades, la qual cosa simplifica molt la instal·lació i el manteniment.
- Suporta els protocols SMTP i IMAP per enviar i rebre correu.
- Ofereix una interfície moderna amb dreceres de teclat, correus multilingües, notificacions del navegador i càrrega de fitxers arrossegant-los (drag-and-drop).
- És autoal·lotjat, cosa que dona als usuaris control total sobre les seves dades de correu, a diferència de solucions al núvol com Gmail.
- La instal·lació és senzilla: es descarrega un ZIP, es descomprimeix al directori web, i es configuren permisos i un vhost de Nginx/Apache amb PHP.



Figura 2: Rainloop logo

Aquesta secció instal·la Apache i PHP, descarrega Rainloop, configura permisos i activa HTTPS amb certificat TLS.

```
# Instal·la Apache i PHP
sudo apt install apache2 php php-fpm php-cli php-curl php-xml
↪ php-mbstring php-zip php-json php-intl libapache2-mod-php php-gd
↪ php-imap php-opcache unzip

# Descarrega i instal·la Rainloop
sudo mkdir /var/www/rainloop
sudo cd /var/www/rainloop
sudo wget
↪ https://www.rainloop.net/repository/webmail/rainloop-latest.zip
sudo unzip rainloop-latest.zip
sudo rm rainloop-latest.zip
sudo find . -type d -exec chmod 755 {} \;
sudo find . -type f -exec chmod 644 {} \;
sudo chown -R www-data:www-data ./
sudo cd
```

12.1. Configuració de Rainloop

Genera un certificat autosignat per a accedir al webmail

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
↳ /etc/ssl/private/rainloop.key -out /etc/ssl/certs/rainloop.crt
↳ -subj "/C=ES/ST=Barcelona/L=Mataró/O=IES Thos i Codina /OU=ASIX/
↳ CN=webmail.thos.local/emailAddress=ramon@thosicodina.cat"

# Copia la configuració de la pàgina predeterminada d'Apache
# amb protocol HTTPS anomenant-la rainloop-ssl.conf
sudo cp /etc/apache2/sites-available/default-ssl.conf
↳ /etc/apache2/sites-available/rainloop-ssl.conf

# Edita la configuració de la pàgina de Rainloop amb protocol HTTPS
sudo nano /etc/apache2/sites-available/rainloop-ssl.conf
```

```
ServerName webmail.thos.local
DocumentRoot /var/www/rainloop
SSLCertificateFile /etc/ssl/certs/rainloop.crt
SSLCertificateKeyFile /etc/ssl/private/rainloop.key
<Directory /var/www/rainloop/>
    AllowOverride All
</Directory>
```

12.2. Configuració HTTP (redirecció a HTTPS)

```
# Copia la configuració de la pàgina predeterminada d'Apache
# amb protocol HTTP anomenant-la rainloop.conf
sudo cp /etc/apache2/sites-available/000-default.conf
↳ /etc/apache2/sites-available/rainloop.conf

# Edita la configuració de la pàgina de Rainloop amb protocol HTTP
sudo nano /etc/apache2/sites-available/rainloop.conf
```

```
<VirtualHost *:80>
    ServerName webmail.thos.local
    Redirect permanent / https://webmail.thos.local
</VirtualHost>
```

12.3. Protecció del directori data

```
# Crea un fitxer .htaccess
sudo nano /var/www/rainloop/data/.htaccess
```

```
Require all denied
```

12.4. Habilita mòduls i llocs d'Apache

```
# Habilita els mòduls rewrite, headers, env, dir, mime
# i ssl en Apache
sudo a2enmod rewrite headers env dir mime ssl

# Habilita les pàgines de Rainloop
sudo a2ensite rainloop.conf rainloop-ssl.conf

# Reinicia el servei Apache
sudo systemctl restart apache2
```

Accedeix a: <https://webmail.thos.local/?admin>

Credencials: admin/12345

Modifica:

- General -> Modifica l'idioma de la interfície
- Seguretat -> Modifica la contrasenya de l'usuari admin
- Dominis -> Afegeix el domini thos.local

12.5. Dominis (Rainloop)

The screenshot shows the RainLoop administration interface. On the left is a sidebar with navigation options: General, Dominis, Entra, Brànding, Contactes, Seguretat, Integracions, Connectors, Paquets, and Quant a. The main area displays the 'Dominis' section with a list of domains: gmail.com, outlook.com, qq.com, and yahoo.com. A modal dialog titled 'Afegeix el domini "thos.local"' is open. It contains the following fields and options:

- Nom** (s'admet el comodí): thos.local
- IMAP**: Servidor (thos.local), Port (993), Segur (SSL / TLS), Usa l'entrada breu (user@domain.com → user)
- SMTP**: Servidor (thos.local), Port (465), Segur (SSL / TLS), Usa autenticació, Usa la funció de php mail() (beta)
- Buttons: Test, Llista blanca, Tanca, Afegeix

A note at the top right of the dialog states: 'Aquesta configuració de domini us permetrà treballar amb les adreces de correu de *@thos.local.'

Figura 3: Afegeix el domini thos.local

The screenshot shows the same RainLoop administration interface, but the modal dialog is titled 'Edita el domini "thos.local"'. The 'thos.local' domain is now listed in the background domain list. The dialog contains the following fields and options:

- IMAP**: Servidor (thos.local), Port (143), Segur (STARTTLS), Usa l'entrada breu (user@domain.com → user)
- SMTP**: Servidor (thos.local), Port (587), Segur (STARTTLS), Usa autenticació, Usa la funció de php mail() (beta)
- Buttons: Test, Llista blanca, Tanca, Actualitza

Figura 4: Edita el domini thos.local

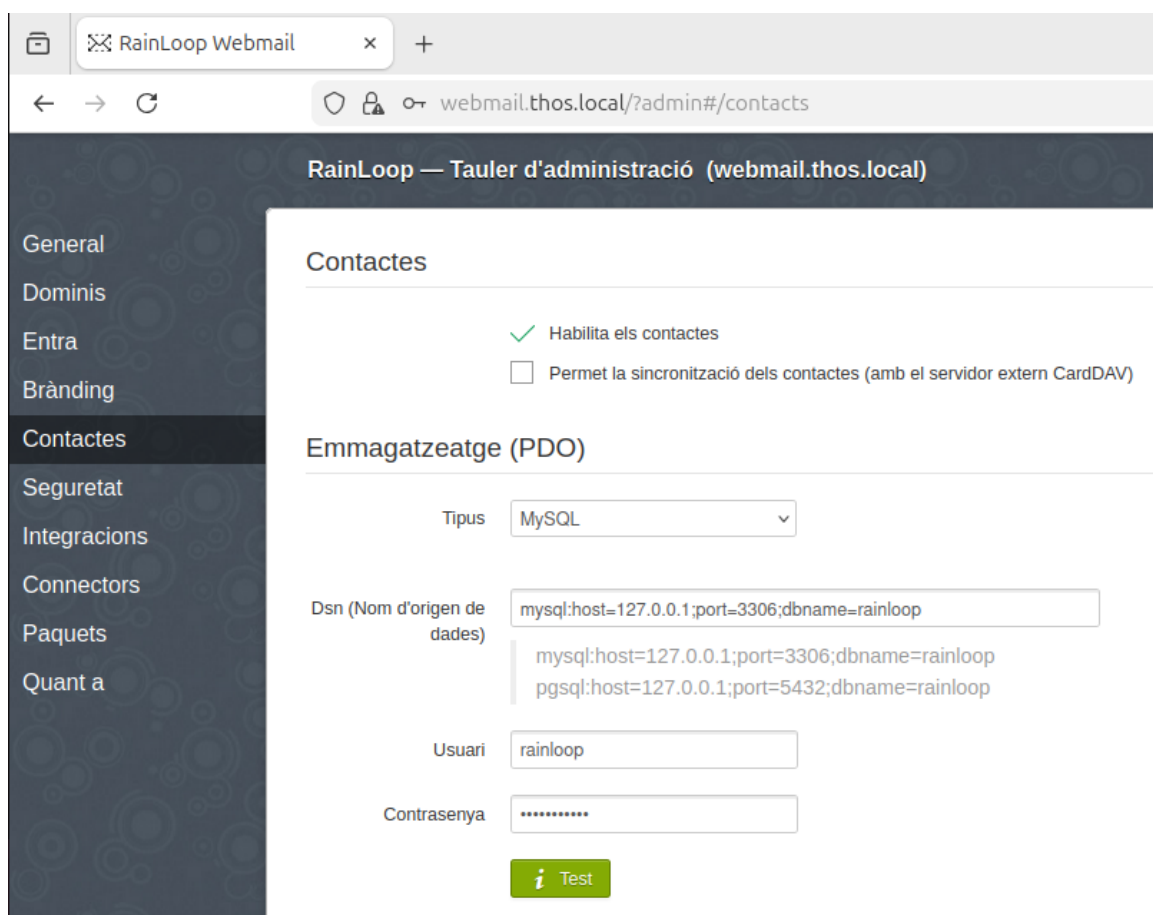
13. Contactes de correu (MariaDB + Rainloop)

Per emmagatzemar contactes al webmail, es crea una base de dades MariaDB, un usuari i permisos, i després es configura a Rainloop (PDO).

```
# Instal·la el servidor de bases de dades MariaDB
sudo apt install mariadb-server php-mysql
```

```
# Accedeix a la consola de MariaDB
sudo mysql -u root -p
```

```
CREATE DATABASE rainloop CHARACTER SET utf8mb4 COLLATE
↳ utf8mb4_general_ci;
CREATE USER rainloop@localhost IDENTIFIED BY 'contrasenya';
GRANT ALL PRIVILEGES ON rainloop.* TO rainloop@localhost;
FLUSH PRIVILEGES;
EXIT;
```



The screenshot shows the RainLoop administration interface in a browser window. The page title is "RainLoop — Tauler d'administració (webmail.thos.local)". The left sidebar contains a menu with options: General, Dominis, Entra, Brànding, Contactes (selected), Seguretat, Integracions, Connectors, Paquets, and Quant a. The main content area is titled "Contactes" and includes the following settings:

- Habilita els contactes
- Permet la sincronització dels contactes (amb el servidor extern CardDAV)
- Emmagatzematge (PDO)**
 - Tipus: MySQL
 - Dsn (Nom d'origen de dades): mysql:host=127.0.0.1;port=3306;dbname=rainloop
 - Usuari: rainloop
 - Contrasenya:
 -

Figura 5: Configuració de contactes (PDO MySQL)

Pantalla de configuració de Contactes (PDO) a Rainloop.

Valors típics (PDO):

- Tipus: MySQL
- DSN: mysql:host=127.0.0.1;port=3306;dbname=rainloop
- Usuari: rainloop
- Contrasenya: contrasenya

Versions d'aquest document

- HTML - [correu.html](#)
- PDF - [correu.pdf](#)
- ODT - [correu.odt](#)
- MD - [correu.md](#)

[Domini Públic \(CC0\)](#)