Servidor de correu

Índex

Cicle formatiu: CFGM Sistemes Microinformàtics i Xarxes (SMX) / CFGS Administració de sistemes informàtics en xarxa (ASIX)

Mòdul: 0227 - Serveis de xarxa / 0375 - Serveis de xarxa i Internet

Sistema operatiu: Ubuntu Server 26.04 LTS

Aquest document explica com implementar un servidor de correu segur en un entorn GNU/Linux. 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 (SnappyMail és una alternativa). 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 26.04 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).

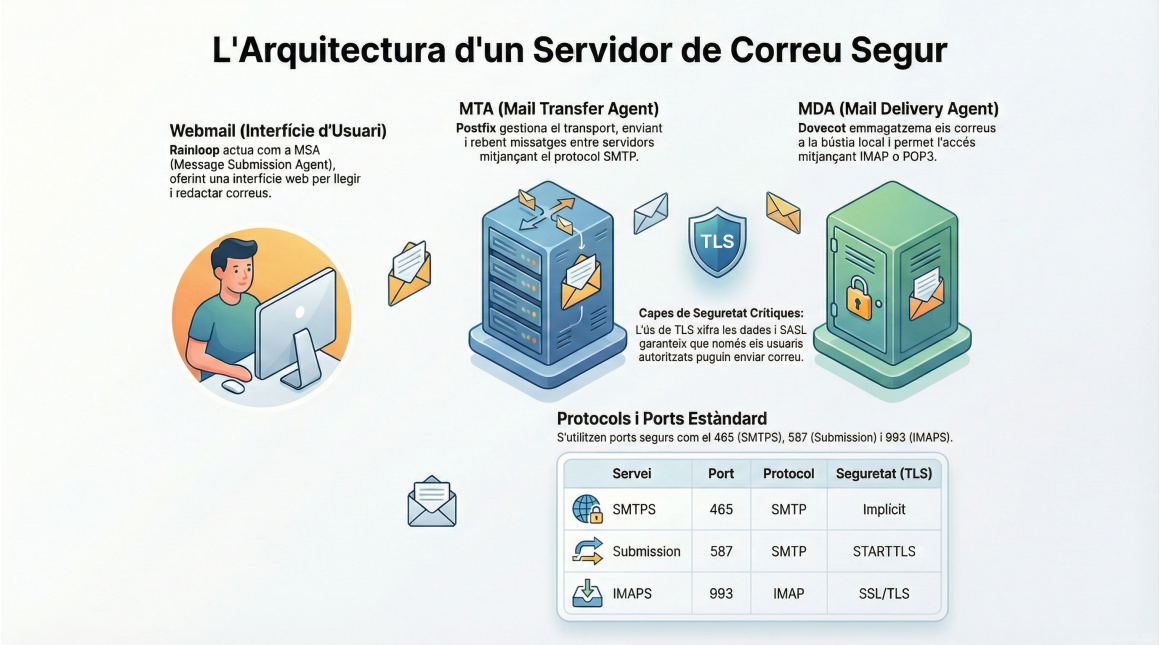

Figura 1: Arquitectura d'un servidor de correu segur

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 autenticat -> 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 correu
```

Configura la interfície de xarxa:

```
sudo nano /etc/netplan/00-installer-config.yaml
```

```
network:
  ethernets:
    enp0s3:
      addresses:
      - 10.0.2.10/24
      match:
        macaddress: 08:00:27:40:ef:70
      nameservers:
        addresses:
        - 8.8.8.8
        - 8.8.4.4
        search: []
      routes:
      - to: default
```

```
        via: 10.0.2.1
      set-name: enp0s3
  version: 2
```

Edita el fitxer de hosts:

```
sudo nano /etc/hosts
```

```
127.0.0.1 localhost
10.0.2.10 correu.thos.local correu
```

Actualitza la llista de paquets:

```
sudo apt update
```

Actualita els paquets:

```
sudo apt upgrade
```

6. Postfix

Instal·la Postfix:

```
sudo apt install postfix
```

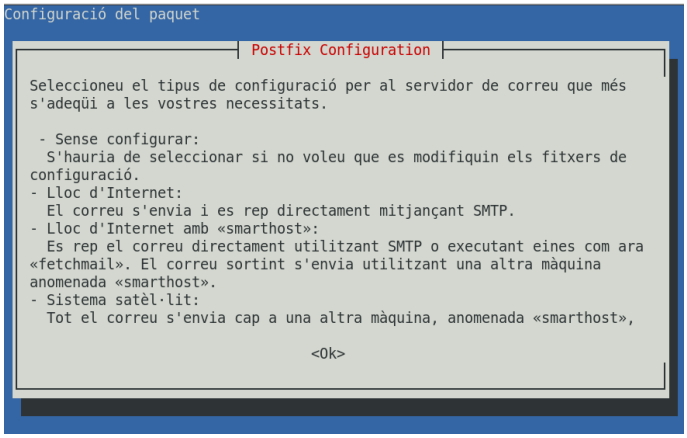

Figura 2: Configuració de Postfix 1/3

Tria **Lloc d'Internet**

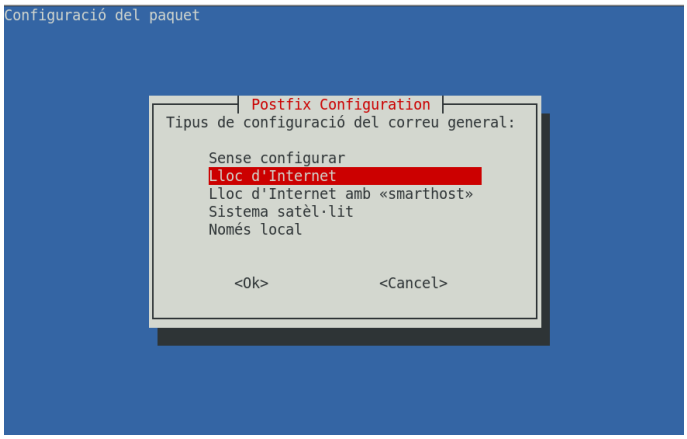

Figura 3: Configuració de Postfix 2/3

Escriu el nom del teu domini:

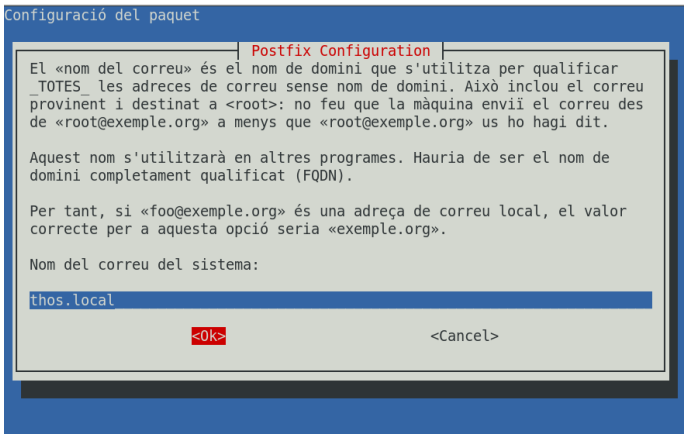

Figura 4: Configuració de Postfix 3/3

6.1. Configura la bústia

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. Configura l'autenticació SMTP

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

Delega l'autenticació a Dovecot:

```
sudo postconf -e 'smtpd_sasl_type = dovecot'
```

Indica la ruta:

```
sudo postconf -e 'smtpd_sasl_path = private/auth'
```

Deixa el domini local buit explícitament:

```
sudo postconf -e 'smtpd_sasl_local_domain ='
```

Prohibeix els mecanismes SASL que permeten autenticació anònima:

```
sudo postconf -e 'smtpd_sasl_security_options = noanonymous'
```

Activa compatibilitat amb clients de correu antics:

```
sudo postconf -e 'broken_sasl_auth_clients = yes'
```

Activa el mecanisme d'autenticació SMTP:

```
sudo postconf -e 'smtpd_sasl_auth_enable = yes'
```

Defineix la política de qui pot enviar correu cap a on. Si el client s'ha autenticat amb usuari/contrasenya (via SASL/Dovecot), es permet immediatament, sigui quina sigui la destinació. Si no s'ha autenticat, però la petició ve d'una xarxa de confiança definida a mynetworks (per exemple la teva pròpia xarxa interna thos.local), també es permet:

```
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, normalment `/var/spool/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. Configura 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/correu.key \
  -out /etc/ssl/certs/correu.crt \
  -subj "/C=ES/ST=Catalunya/L=Mataro/O=IES Thos i
   ↪  Codina/OU=ASIX/CN=correu.thos.local"
```

Configura el xifratge TLS de Postfix, tant per al correu que envia cap a fora (client SMTP) com per al que rep dels teus usuaris/clients (servidor SMTP).

Intenta sempre fer STARTTLS si el servidor remot ho ofereix, però si el remot no ho suporta, continua sense xifrar en lloc de fallar l'entrega. És el nivell més compatible, pensat perquè el correu surti igualment encara que el destinatari no tingui TLS.:

```
sudo postconf -e 'smtp_tls_security_level = may'
```

Exigeix STARTTLS abans d'acceptar el missatge:

```
sudo postconf -e 'smtpd_tls_security_level = encrypt'
```

Afegeix un avís als logs (`Warning: ... TLS is available but was not used`). És purament informatiu, per detectar servidors remots mal configurats:

```
sudo postconf -e 'smtp_tls_note_starttls_offer = yes'
```

Nivell de detall dels registres relacionats amb TLS al costat servidor. 1 és un nivell bàsic:

```
sudo postconf -e 'smtpd_tls_loglevel = 1'
```

Fa que Postfix afegeixi informació sobre el xifratge TLS usat dins la capçalera de cada missatge que rep:

```
sudo postconf -e 'smtpd_tls_received_header = yes'
```

Nom canònic del servidor de correu:

```
sudo postconf -e 'myhostname = correu.thos.local'
```

Ruta al certificat públic que Postfix presentarà als clients quan aquests facin STARTTLS:

```
sudo postconf -e 'smtpd_tls_cert_file=/etc/ssl/certs/correu.crt'
```

Ruta a la clau privada corresponent a aquest certificat:

```
sudo postconf -e 'smtpd_tls_key_file=/etc/ssl/private/correu.key'
```

Canvia el propietari del fitxer `/var/spool/postfix/etc/resolv.conf`:

```
sudo chown root:root /var/spool/postfix/etc/resolv.conf
```

Modifica els permisos:

```
sudo chmod 644 /var/spool/postfix/etc/resolv.conf
```

La configuració inicial de Postfix ja s'ha completat. Reinicia el dimoni:

```
sudo systemctl restart postfix
```

Comprova l'estat:

```
sudo systemctl status postfix
```

Resposta esperada:

```
● postfix.service - Postfix Mail Transport Agent (main/default
↪  instance)
     Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled;
↪  preset: enabled)
     Active: active (running) since Mon 2026-07-13 08:07:46 UTC; 1s ago
 Invocation: 2210c014fc5d460ead92496604ed3c71
       Docs: man:postfix(1)
    Process: 3053 ExecStartPre=postfix check (code=exited,
↪  status=0/SUCCESS)
    Process: 3151 ExecStart=postfix debian-systemd-start (code=exited,
↪  status=0/SUCCESS)
   Main PID: 3160 (master)
      Tasks: 3 (limit: 1718)
     Memory: 3M (peak: 4.1M)
        CPU: 229ms
     CGroup: /system.slice/postfix.service
             ├─3160 /usr/lib/postfix/sbin/master -w
             ├─3161 pickup -l -t unix -u
             └─3162 qmgr -l -t unix -u
```

```
de jul. 13 08:07:46 correu systemd[1]: Starting postfix.service -
 ↪  Postfix Mail Transport Agent (main/default instance)...
de jul. 13 08:07:46 correu postfix/master[3160]: daemon started --
 ↪  version 3.10.6, configuration /etc/postfix
de jul. 13 08:07:46 correu systemd[1]: Started postfix.service -
 ↪  Postfix Mail Transport Agent (main/default instance).
```

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.

Instal·la Dovecot:

```
sudo apt install dovecot-core
```

Configura el socket d'autenticació per Postfix:

```
sudo nano -l /etc/dovecot/conf.d/10-master.conf
```

Fes les modificacions (línies 110-114):

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

Activa mecanismes d'autenticació:

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

Descomenta la línia 93:

```
auth_mechanisms = plain login
```

Un cop hagis configurat Dovecot, reinicia-lo i comprova l'estat.

Reinicia:

```
sudo systemctl restart dovecot
```

Comprova l'estat:

```
sudo systemctl status dovecot
```

Resposta esperada:

```
● dovecot.service - Dovecot IMAP/POP3 email server
     Loaded: loaded (/usr/lib/systemd/system/dovecot.service; enabled;
 ↪  preset: enabled)
     Active: active (running) since Mon 2026-07-13 08:24:42 UTC; 5s ago
 Invocation: 8124fb1e97564a6989fe35ba87c0990e
       Docs: man:dovecot(1)
             https://doc.dovecot.org/
   Main PID: 5936 (dovecot)
     Status: "v2.4.2 (0962ed2104) running"
      Tasks: 4 (limit: 1718)
     Memory: 7.2M (peak: 9.3M)
        CPU: 54ms
     CGroup: /system.slice/dovecot.service
             ├─5936 /usr/sbin/dovecot -F
             ├─5938 dovecot/anvil
             ├─5939 dovecot/log
             └─5940 dovecot/config

de jul. 13 08:24:42 correu systemd[1]: Starting dovecot.service -
 ↪  Dovecot IMAP/POP3 email server...
de jul. 13 08:24:42 correu dovecot[5936]: master: Dovecot v2.4.2
 ↪  (0962ed2104) starting up without any protocols (core dumps
 ↪  disabled)
de jul. 13 08:24:42 correu systemd[1]: Started dovecot.service -
 ↪  Dovecot IMAP/POP3 email server.
```

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, obre una connexió directa i en text pla al port 25 de `correu.thos.local`, que és el port estàndard on Postfix escolta connexions SMTP (correu entre servidors) amb Telnet:

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

```
Trying 10.0.2.10...
Connected to correu.thos.local.
Escape character is '^]'.
220 correu.thos.local ESMTP Postfix (Ubuntu)
```

Mostra les extensions que Postfix suporta al port 25 per comprovar que la configuració TLS/SASL que has fet s'ha aplicat correctament:

```
ehlo correu.thos.local
```

Resposta esperada:

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

Observa que apareix la línia `250-STARTTLS`, que confirma que la configuració TLS que has aplicat funciona i el servidor l'anuncia correctament.

Per sortir prem la drecera `^]` (**Ctrl** + **AltGr** + **+**), i al prompt de telnet: `close`.

```
^]
telnet> close
Connection closed.
```

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 -l /etc/postfix/master.cf
```

Comenta la línia 12 i enganxa aquestes línies a continuació:

```
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_m
 ↪  ynetworks,reject_unauth_destination
```

Comprova la sintaxi de la configuració:

```
sudo postfix check
```

Reinicia el dimoni de Postfix:

```
sudo systemctl restart postfix
```

Verifica l'estat:

```
sudo systemctl status postfix
```

Resposta esperada:

```
● postfix.service - Postfix Mail Transport Agent (main/default
 ↪  instance)
     Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled;
 ↪  preset: enabled)
     Active: active (running) since Mon 2026-07-13 09:04:10 UTC; 3s ago
 Invocation: faa06cbcf74841288a2a5a2e77d05e73
       Docs: man:postfix(1)
    Process: 6335 ExecStartPre=postfix check (code=exited,
 ↪  status=0/SUCCESS)
    Process: 6440 ExecStart=postfix debian-systemd-start (code=exited,
 ↪  status=0/SUCCESS)
   Main PID: 6448 (master)
      Tasks: 3 (limit: 1718)
     Memory: 2.8M (peak: 4.4M)
        CPU: 244ms
     CGroup: /system.slice/postfix.service
             ├─6448 /usr/lib/postfix/sbin/master -w
             ├─6449 pickup -l -t unix -u
             └─6450 qmgr -l -t unix -u

de jul. 13 09:04:10 correu systemd[1]: Starting postfix.service -
 ↪  Postfix Mail Transport Agent (main/default instance)...
de jul. 13 09:04:10 correu postfix/master[6448]: daemon started --
 ↪  version 3.10.6, configuration /etc/postfix
de jul. 13 09:04:10 correu systemd[1]: Started postfix.service -
 ↪  Postfix Mail Transport Agent (main/default instance).
```

Prova que el 465 dona certificat:

```
sudo openssl s_client -connect correu.thos.local:465 -crlf
 ↪  -servername correu.thos.local
```

Resposta esperada:

```
Connecting to 10.0.2.10
CONNECTED(00000003)
depth=0 C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
verify error:num=18:self-signed certificate
verify return:1
depth=0 C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
verify return:1
---
Certificate chain
```

```
 0 s:C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
   i:C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Jul 13 08:03:45 2026 GMT; NotAfter: Jul 13 08:03:45
 ↪  2027 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIID0zCCArugAwIBAgIULYnVYKPvEpVpQi2SVPRaIlUV8EMwDQYJKoZIhvcNAQEL
BQAweTELMAkGA1UEBhMCRVMxEjAQBgNVBAgMCUNhdGFsdW55YTEPMA0GA1UEBwwG
TWF0YXJvMRowGAYDVQQKDBFJRVMgVGhvcyBpIENvZGluYTENMAsGA1UECwwEQVNJ
WDEaMBgGA1UEAwwRY29ycmV1LnRob3MubG9jYWwwHhcNMjYwNzEzMDgwMzQ1WhcN
MjcwNzEzMDgwMzQ1WjB5MQswCQYDVQQGEwJFUzESMBAGA1UECAwJQ2F0YWx1bnlh
MQ8wDQYDVQQHDAZNYXRhcm8xGjAYBgNVBAoMEUlFUyBUaG9zIGkgQ29kaW5hMQ0w
CwYDVQQLDARBU0lYMRowGAYDVQQDDBFjb3JyZXUudGhvcy5sb2NhbDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKXEDfqAmq1lRYfJB9njURkpWvD6NVbB
2ZD4bRQuQj1IAXo5K0/d/R+r14DcaU0bmIzAkK15TlBGdrni0tzCqbqLHJvxlEBt
E7y8U9M1Cm1gK4Q23oYs3HuTK5+OD8I1Mr0tbgFJ/6MlQOSnkd/9kDQaC8XPdiYL
gzjh5xbUmTFGHcIUXvJM7pTrY5marMBieh6s2masIYI6tMmYLt//E8lJ673crVvw
f4klCqSoa+erlgT3Kn+W0bNP2F7EGqc4PWdI7vxoHqI4y86OUmVkmPnxFdOx1axR
W0pN1wY5hkeCcFXrIHH3BgZl45uhRcFynSdA06LRxjFQ+6owP4sua58CAwEAAaNT
MFEwHQYDVR0OBBYEFGYkJxlnrUrQsiHCyhWDiuGM+47lMB8GA1UdIwQYMBaAFGYk
JxlnrUrQsiHCyhWDiuGM+47lMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEL
BQADggEBABDGVNSSL42nb1/pxWroLw4LDKbN5uhWINBWLx4ggt6oaQy2qnGCw5N4
kgPRvhmVtO1/mEVch5SOmlLPdMv6Y77kJRfj/+8EUIxIMAOynIwr7I0X4CUi2AYh
ClfEXM320a4Woynk9QAZo3lbZ3ZpP6wVI25jfW4Z/qWnD3vof9ZNAjfwuAMKN4T1
EstxTaGUh2kKg19b7b+GKDpT3yvDjyFVQM6s8DV6WwHSXkPBgg8yVdQoXhRZPs6J
dAvRwachG+zLqj/MlhFO7aAzoayS/jKHnaW7aPUPiPklNyln0XgHG6UbasTV1Bt/
dUCnowbO7qmVcg3AQDmWvtvVh/DZkhQ=
-----END CERTIFICATE-----
subject=C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
issuer=C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: rsa_pss_rsae_sha256
Peer Temp Key: X25519, 253 bits
---
SSL handshake has read 1539 bytes and written 1639 bytes
Verification error: self-signed certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Protocol: TLSv1.3
Server public key is 2048 bit
This TLS version forbids renegotiation.
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
```

```
Verify return code: 18 (self-signed certificate)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID:
 ↪  BC0840D33C9715C8FA6B57B300C5D78FEBA9B118F178BF35849A59AD3E8FE86B
    Session-ID-ctx:
    Resumption PSK: 4A1267973CC2EF46683300B74F4C1E9CCC346386F347716F1
 ↪  49089CE5613246A3CB73C79055E7F3F71E6C96DB2004E0A
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - db 85 a4 9e e5 0f d2 29-17 f5 8e 99 44 41 c9 0f
 ↪  .......)....DA..
    0010 - 7a 5e 5d bf ad e6 4d 6e-66 34 ea 66 95 c6 05 35
 ↪  z^]...Mnf4.f...5
    0020 - 36 85 7b 57 2b 57 e4 eb-b4 d9 02 37 98 98 a1 e1
 ↪  6.{W+W.....7....
    0030 - 2a ee c2 fa f6 ea 37 90-0b b5 65 74 7e 91 c1 79
 ↪  *.....7...et~..y
    0040 - 59 14 95 96 c7 88 67 a9-c5 e2 53 3d 05 35 37 d5
 ↪  Y.....g...S=.57.
    0050 - 28 b6 7b bc 52 09 6f af-99 19 f5 78 e4 70 d0 1b
 ↪  (.{.R.o....x.p..
    0060 - aa 84 3f a3 44 b1 17 91-71 f2 ef 82 39 57 71 a5
 ↪  ..?.D...q...9Wq.
    0070 - 89 e5 06 34 e4 c7 3d 89-90 ac 5f 97 0f 2c 21 d6
 ↪  ...4..=..._..,!.
    0080 - 5d 09 46 c5 a2 c2 ee 1a-4d 99 48 fd 6a 16 71 88
 ↪  ].F.....M.H.j.q.
    0090 - f3 1f 78 71 63 07 ea 92-c4 c1 a2 cf ef 4b a7 f7
 ↪  ..xqc........K..
    00a0 - 21 71 9a e8 07 e3 fb ac-6d 99 f7 a7 26 3a 5d 9f
 ↪  !q......m...&:].
    00b0 - 94 52 be 51 eb e2 42 76-7c 06 4e f5 86 96 6b 34
 ↪  .R.Q..Bv|.N...k4
    00c0 - 23 80 e9 03 b4 4b 94 5a-7e c4 68 63 0a 5e 72 1e
 ↪  #....K.Z~.hc.^r.

    Start Time: 1783933977
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
220 correu.thos.local ESMTP Postfix (Ubuntu)
```

Per sortir escriu `quit`:

```
221 2.0.0 Bye
closed
```

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
```

Afegeix aquestes línies al final:

```
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
```

Resposta esperada:

```
LISTEN 0      100          0.0.0.0:587       0.0.0.0:*
 ↪  users:(("master",pid=7142,fd=18))
LISTEN 0      100             [::]:587          [::]:*
 ↪  users:(("master",pid=7142,fd=19))
```

Prova STARTTLS manualment:

```
sudo openssl s_client -starttls smtp -connect correu.thos.local:587
```

Resposta esperada:

```
Connecting to 10.0.2.10
CONNECTED(00000003)
depth=0 C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
verify error:num=18:self-signed certificate
verify return:1
depth=0 C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
verify return:1
---
Certificate chain
 0 s:C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
   i:C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
   a:PKEY: RSA, 2048 (bit); sigalg: sha256WithRSAEncryption
   v:NotBefore: Jul 13 08:03:45 2026 GMT; NotAfter: Jul 13 08:03:45
 ↪  2027 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIID0zCCArugAwIBAgIULYnVYKPvEpVpQi2SVPRaIlUV8EMwDQYJKoZIhvcNAQEL
BQAweTELMAkGA1UEBhMCRVMxEjAQBgNVBAgMCUNhdGFsdW55YTEPMA0GA1UEBwwG
TWF0YXJvMRowGAYDVQQKDBFJRVMgVGhvcyBpIENvZGluYTENMAsGA1UECwwEQVNJ
WDEaMBgGA1UEAwwRY29ycmV1LnRob3MubG9jYWwwHhcNMjYwNzEzMDgwMzQ1WhcN
MjcwNzEzMDgwMzQ1WjB5MQswCQYDVQQGEwJFUzESMBAGA1UECAwJQ2F0YWx1bnlh
MQ8wDQYDVQQHDAZNYXRhcm8xGjAYBgNVBAoMEUlFUyBUaG9zIGkgQ29kaW5hMQ0w
CwYDVQQLDARBU0lYMRowGAYDVQQDDBFjb3JyZXUudGhvcy5sb2NhbDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKXEDfqAmq1lRYfJB9njURkpWvD6NVbB
2ZD4bRQuQj1IAXo5K0/d/R+r14DcaU0bmIzAkK15TlBGdrni0tzCqbqLHJvxlEBt
E7y8U9M1Cm1gK4Q23oYs3HuTK5+OD8I1Mr0tbgFJ/6MlQOSnkd/9kDQaC8XPdiYL
gzjh5xbUmTFGHcIUXvJM7pTrY5marMBieh6s2masIYI6tMmYLt//E8lJ673crVvw
f4klCqSoa+erlgT3Kn+W0bNP2F7EGqc4PWdI7vxoHqI4y86OUmVkmPnxFdOx1axR
W0pN1wY5hkeCcFXrIHH3BgZl45uhRcFynSdA06LRxjFQ+6owP4sua58CAwEAAaNT
MFEwHQYDVR0OBBYEFGYkJxlnrUrQsiHCyhWDiuGM+47lMB8GA1UdIwQYMBaAFGYk
JxlnrUrQsiHCyhWDiuGM+47lMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEL
BQADggEBABDGVNSSL42nb1/pxWroLw4LDKbN5uhWINBWLx4ggt6oaQy2qnGCw5N4
kgPRvhmVtO1/mEVch5SOmlLPdMv6Y77kJRfj/+8EUIxIMAOynIwr7I0X4CUi2AYh
ClfEXM320a4Woynk9QAZo3lbZ3ZpP6wVI25jfW4Z/qWnD3vof9ZNAjfwuAMKN4T1
EstxTaGUh2kKg19b7b+GKDpT3yvDjyFVQM6s8DV6WwHSXkPBgg8yVdQoXhRZPs6J
dAvRwachG+zLqj/MlhFO7aAzoayS/jKHnaW7aPUPiPklNyln0XgHG6UbasTV1Bt/
dUCnowbO7qmVcg3AQDmWvtvVh/DZkhQ=
-----END CERTIFICATE-----
subject=C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
issuer=C=ES, ST=Catalunya, L=Mataro, O=IES Thos i Codina, OU=ASIX,
 ↪  CN=correu.thos.local
---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: rsa_pss_rsae_sha256
Peer Temp Key: X25519, 253 bits
---
```

```
SSL handshake has read 1783 bytes and written 1672 bytes
Verification error: self-signed certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Protocol: TLSv1.3
Server public key is 2048 bit
This TLS version forbids renegotiation.
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self-signed certificate)
---
250 CHUNKING
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID:
 ↪  0C3E7D40DCC08B0E49CD7A008D2DA5579267C3AF73E7F3EE9183C91EB22F5276
    Session-ID-ctx:
    Resumption PSK: 91778D9D9378E61F5BD82C736352A68E2B4201E1DBBD150DE
 ↪  CC3983EE030229504564C3DF03F29260F8B656205FC653E
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 99 44 74 b7 79 e8 fc 30-15 e1 03 fd dd a6 5d d2
 ↪  .Dt.y..0......].
    0010 - 2a 12 00 22 9e c6 d1 c0-36 e1 60 36 90 e7 cb 30
 ↪  *.."....6.`6...0
    0020 - cb f5 70 f0 7f 9a 56 f2-2d c4 1f 7a 9c b7 e9 4d
 ↪  ..p...V.-..z...M
    0030 - f3 76 87 18 d3 c4 c1 43-34 27 69 ee 10 b3 52 a9
 ↪  .v.....C4'i...R.
    0040 - 0d 68 f9 77 4d 21 e2 e8-42 4b fa f6 b7 e4 3a 94
 ↪  .h.wM!..BK....:.
    0050 - c4 1e 7f d0 e3 3b be 4f-9c d7 83 f2 d8 d1 c9 ee
 ↪  .....;.O........
    0060 - 76 e3 dc 1d 5a d5 d7 ec-1c cf 66 5b 9f 5b 80 ee
 ↪  v...Z.....f[.[..
    0070 - ec 33 be df e6 19 03 6f-06 e8 3c ea e3 9a dd 99
 ↪  .3.....o..<.....
    0080 - 1d ad 99 a0 52 8e 72 0c-45 8b a4 26 83 e1 75 14
 ↪  ....R.r.E..&..u.
    0090 - 10 e7 87 85 f4 00 d8 c3-46 35 0c 46 95 f5 f6 e2
 ↪  ........F5.F....
    00a0 - b1 8f 4c b5 0e a0 df d0-89 95 0e 4a da 65 44 5d
 ↪  ..L........J.eD]
    00b0 - 70 73 81 61 5b ba 89 d4-54 58 fd c2 8b 02 01 b7
 ↪  ps.a[...TX......
```

```
    00c0 - 01 55 a7 98 32 8c f1 54-8f 80 9c 95 a9 a7 9e bb
↪   .U..2..T........

    Start Time: 1783934282
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
```

Per sortir escriu `quit`:

```
221 2.0.0 Bye
closed
```

10. Dovecot

Dovecot és el servidor IMAP/POP3 que permet accés a les bústies, i també s'utilitza per autenticació (SASL).

Instal·la Dovecot:

```
sudo apt install dovecot-imapd dovecot-pop3d
```

Configura l'emmagatzematge en Maildir i activa SSL per IMAPS:

```
sudo nano -l /etc/dovecot/dovecot.conf
```

Descomenta la línia 30:

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

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

```
auth_allow_cleartext = yes
auth_username_format = %{user | username}
```

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

```
mail_driver = maildir
mail_path = ~/Maildir
# mail_inbox_path = /var/mail/%{user}
mailbox_list_layout = fs
```

Reinicia el dimoni de dovecot

```
sudo systemctl restart dovecot
```

Resposta esperada:

```
● dovecot.service - Dovecot IMAP/POP3 email server
     Loaded: loaded (/usr/lib/systemd/system/dovecot.service; enabled;
 ↪  preset: enabled)
     Active: active (running) since Mon 2026-07-13 09:34:11 UTC; 8s ago
 Invocation: 8b889252e5b6489fb016f41565ebeb90
       Docs: man:dovecot(1)
             https://doc.dovecot.org/
   Main PID: 7626 (dovecot)
     Status: "v2.4.2 (0962ed2104) running"
      Tasks: 4 (limit: 1718)
     Memory: 7.6M (peak: 9.5M)
        CPU: 56ms
     CGroup: /system.slice/dovecot.service
             ├─7626 /usr/sbin/dovecot -F
             ├─7627 dovecot/anvil
             ├─7628 dovecot/log
             └─7629 dovecot/config

de jul. 13 09:34:11 correu systemd[1]: Starting dovecot.service -
 ↪  Dovecot IMAP/POP3 email server...
de jul. 13 09:34:11 correu dovecot[7626]: master: Dovecot v2.4.2
 ↪  (0962ed2104) starting up for imap, pop3 (core dumps disabled)
de jul. 13 09:34:11 correu systemd[1]: Started dovecot.service -
 ↪  Dovecot IMAP/POP3 email server.
```

10.1. Configura 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=Catalunya/L=Mataro/O=IES Thos i
   ↪  Codina/OU=ASIX/CN=correu.thos.local"
```

11. Crea un compte de correu

Crea un compte (usuari local):

```
sudo adduser alumne1
```

12. Instal·la el 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 autoallotjat, 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 5: 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-zip
↪  \
  php-mbstring php-json php-intl libapache2-mod-php php-gd unzip
```

Crea una carpeta per a Rainloop:

```
sudo mkdir /var/www/rainloop
```

Descarrega l'última versió estable:

```
sudo wget -c
↪  https://www.rainloop.net/repository/webmail/rainloop-latest.zip
```

Descomprimeix a la carpeta creada:

```
sudo unzip rainloop-latest.zip -d /var/www/rainloop
```

Esborra el fitxer descarregat:

```
sudo rm rainloop-latest.zip
```

Canvia els permisos de les carpetes:

```
sudo find /var/www/rainloop -type d -exec chmod 755 {} \;
```

Canvia els permisos dels fitxers:

```
sudo find /var/www/rainloop -type f -exec chmod 644 {} \;
```

Canvia el propietari de la carpeta:

```
sudo chown -R www-data:www-data /var/www/rainloop
```

12.1. Configura 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=Catalunya/L=Mataro/O=IES Thos i
   ↪  Codina/OU=ASIX/CN=webmail.thos.local"
```

Crea la configuració de la pàgina de Rainloop amb protocol HTTPS:

```
sudo nano /etc/apache2/sites-available/rainloop-ssl.conf
```

```
<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        ServerName webmail.thos.local
        DocumentRoot /var/www/rainloop
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile /etc/ssl/certs/rainloop.crt
        SSLCertificateKeyFile /etc/ssl/private/rainloop.key
        <FilesMatch "\.(?:cgi|shtml|phtml|php)$">
                SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
```

```
                SSLOptions +StdEnvVars
        </Directory>
        <Directory /var/www/rainloop/>
                AllowOverride All
        </Directory>
</VirtualHost>
```

12.2. Configura la redirecció a HTTPS

Crea la configuració HTTP perquè redirigeix tot el trànsit HTTP cap a HTTPS:

```
sudo nano /etc/apache2/sites-available/rainloop.conf
```

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

12.3. Protegeix el 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 els VirtualHosts de Rainloop:

```
sudo a2ensite rainloop.conf rainloop-ssl.conf
```

Desactiva el VirtualHost predeterminat:

```
sudo a2dissite 000-default.conf
```

Comprova la sintaxi dels fitxers de configuració d'Apache:

```
sudo apachectl configtest
```

Resposta esperada:

```
Syntax OK
```

Reinicia el servei Apache:

```
sudo systemctl restart apache2
```

Verifica l'estat:

```
sudo systemctl status apache2
```

Resposta esperada:

```
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled;
 ↪  preset: enabled)
     Active: active (running) since Mon 2026-07-13 09:56:08 UTC; 6s ago
 Invocation: 196774e395d44fd88edacebd81896c47
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 17294 (apache2)
     Status: "Processing requests..."
      Tasks: 6 (limit: 3995)
     Memory: 16.6M (peak: 16.6M)
        CPU: 58ms
     CGroup: /system.slice/apache2.service
             ├─17294 /usr/sbin/apache2 -k start -DFOREGROUND
             ├─17298 /usr/sbin/apache2 -k start -DFOREGROUND
             ├─17299 /usr/sbin/apache2 -k start -DFOREGROUND
             ├─17300 /usr/sbin/apache2 -k start -DFOREGROUND
             ├─17301 /usr/sbin/apache2 -k start -DFOREGROUND
             └─17306 /usr/sbin/apache2 -k start -DFOREGROUND

de jul. 13 09:56:08 correu systemd[1]: Starting apache2.service - The
 ↪  Apache HTTP Server...
de jul. 13 09:56:08 correu systemd[1]: Started apache2.service - The
 ↪  Apache HTTP Server.
```

Accedeix a: `https://webmail.thos.local/?admin`

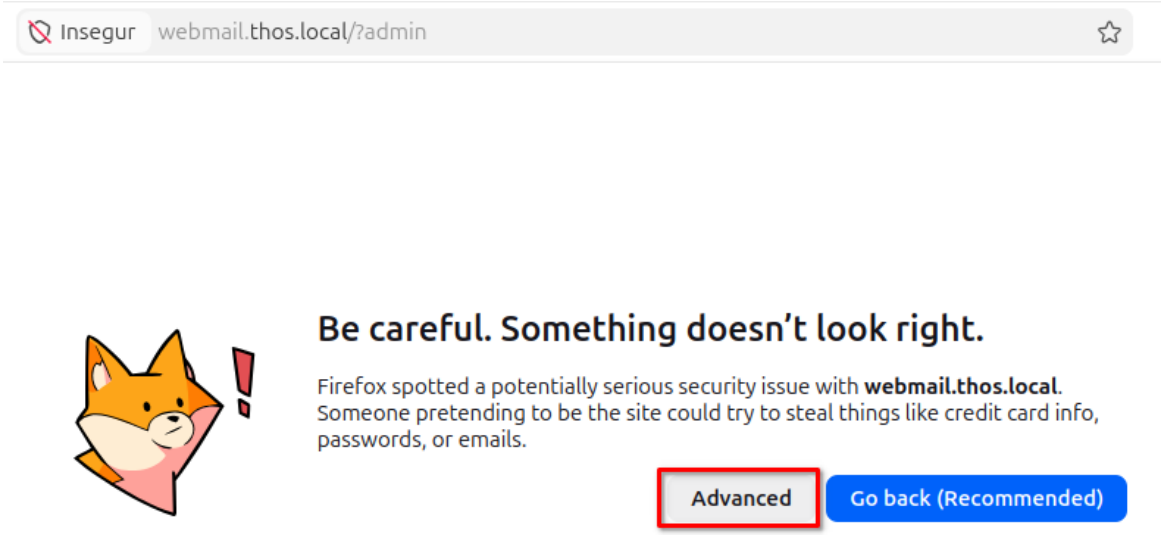

Figura 6: Avís de seguretat

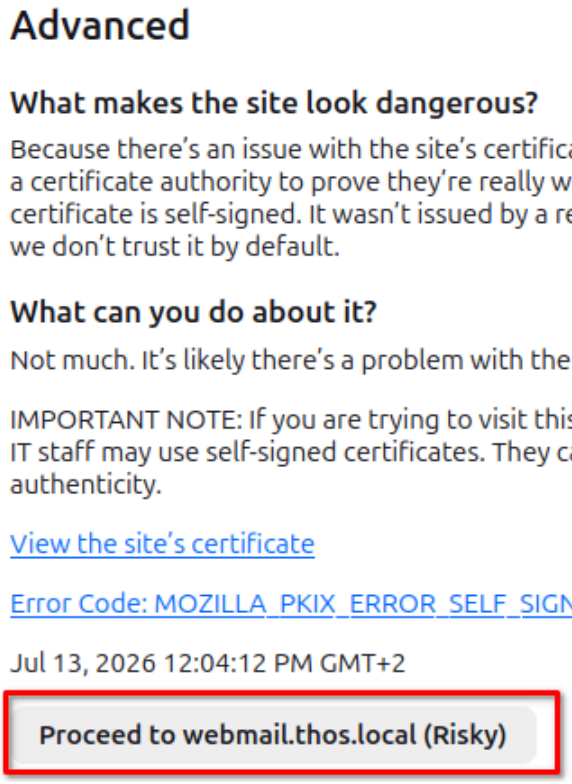

Figura 7: Accepta el risc

Credencials: `admin/12345`

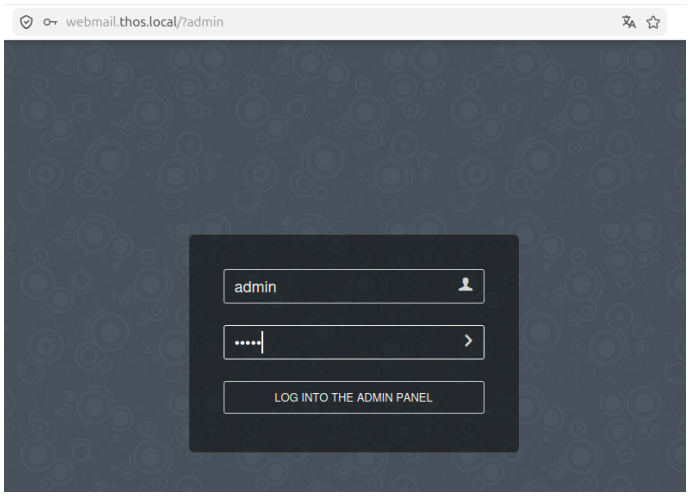

Figura 8: Login d'admin

Modifica:

- General -> Modifica l'idioma de la interfície

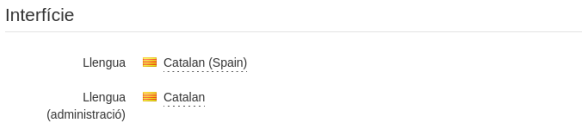

Figura 9: Idioma de la interfície

- Seguretat -> Modifica la contrasenya de l'usuari admin

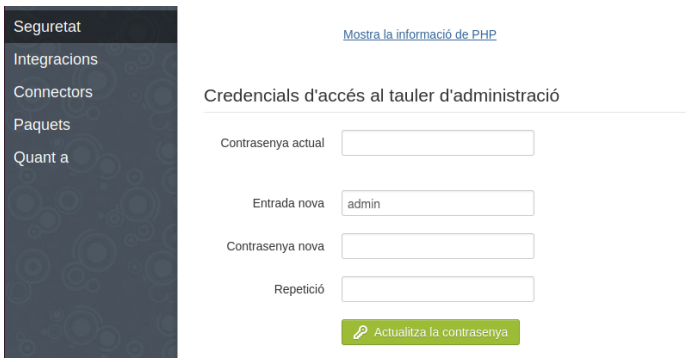

Figura 10: Canvia la contrasenya

- Dominis -> Afegeix el domini thos.local

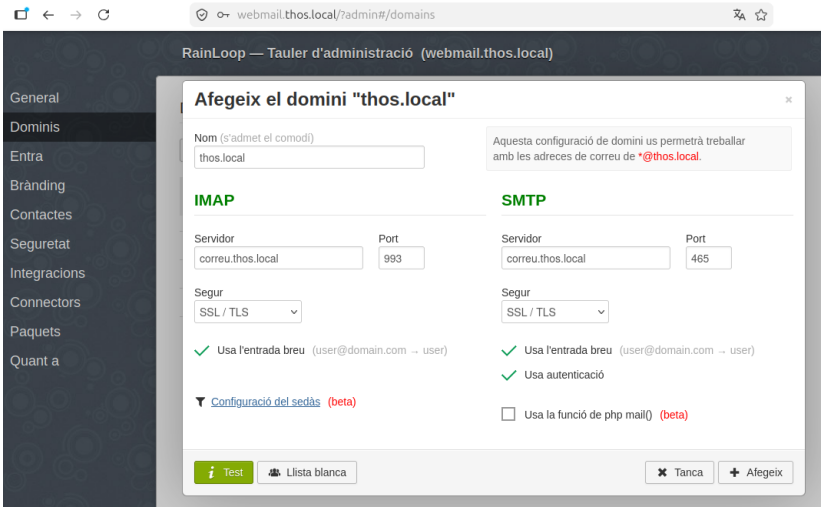

Figura 11: Domini thos.local

Accedeix a **`https://webmail.thos.local`** amb un usuari:

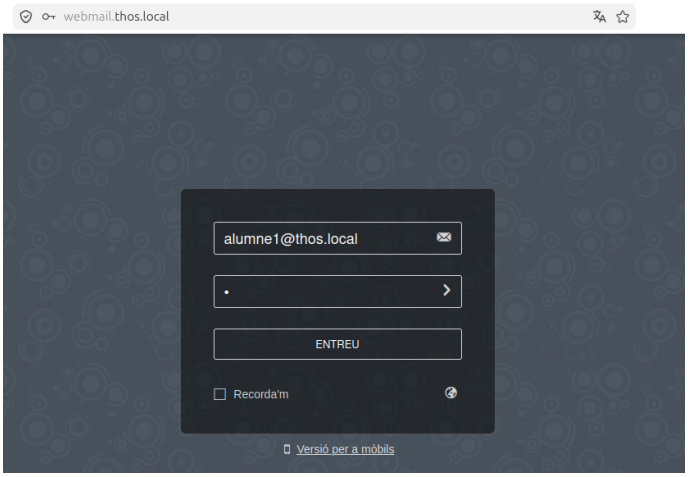

Figura 12: Login d'usuari

Crea un nou missatge:

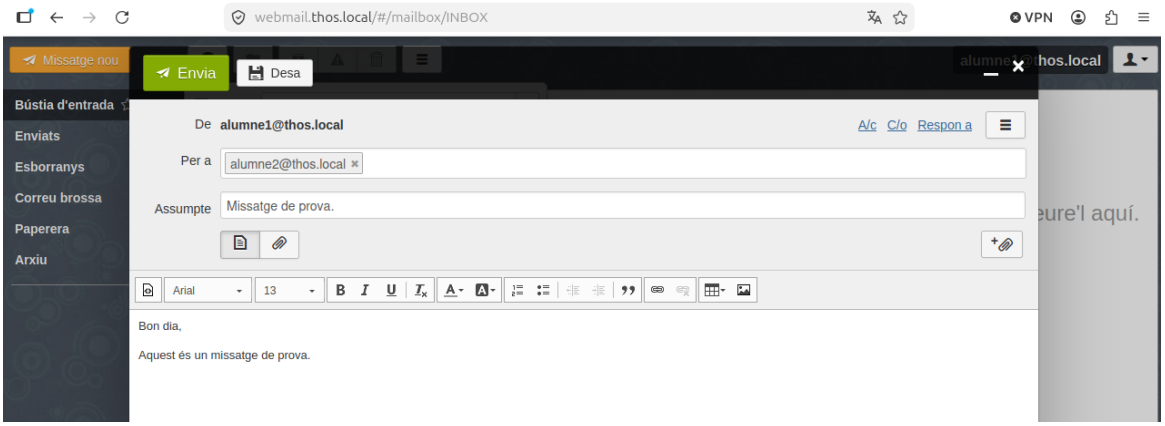

Figura 13: Nou correu

Missatge enviat:

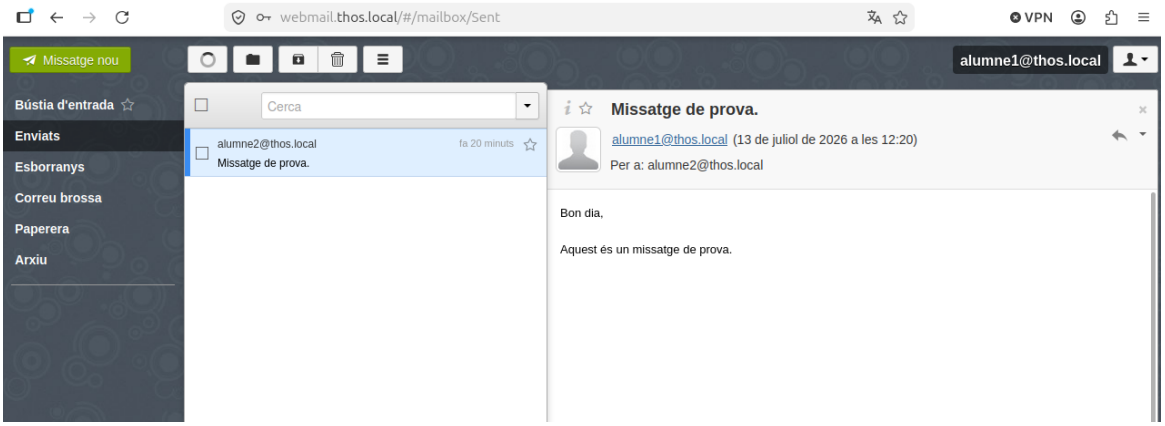

Figura 14: Missatge enviat

Accedeix amb l'usuari destinatari del correu:

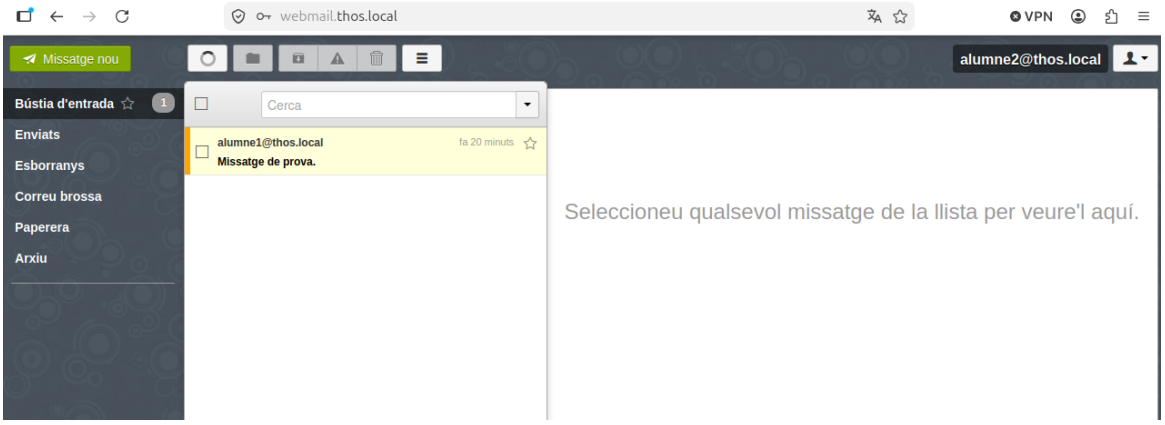

Figura 15: Safata d'entrada

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;
```

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

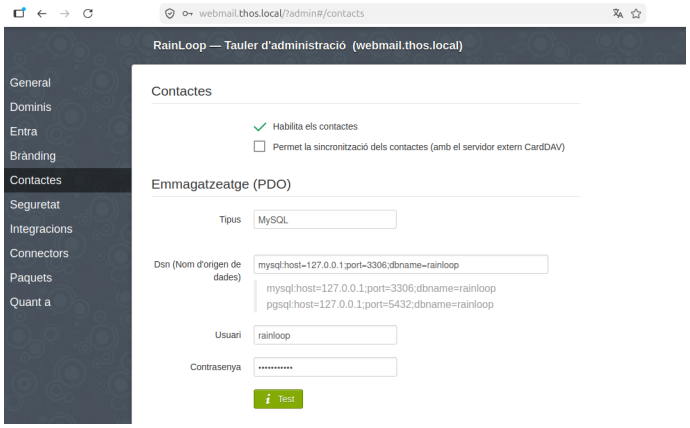

Figura 16: Configuració de contactes

Afegeix un nou contacte:

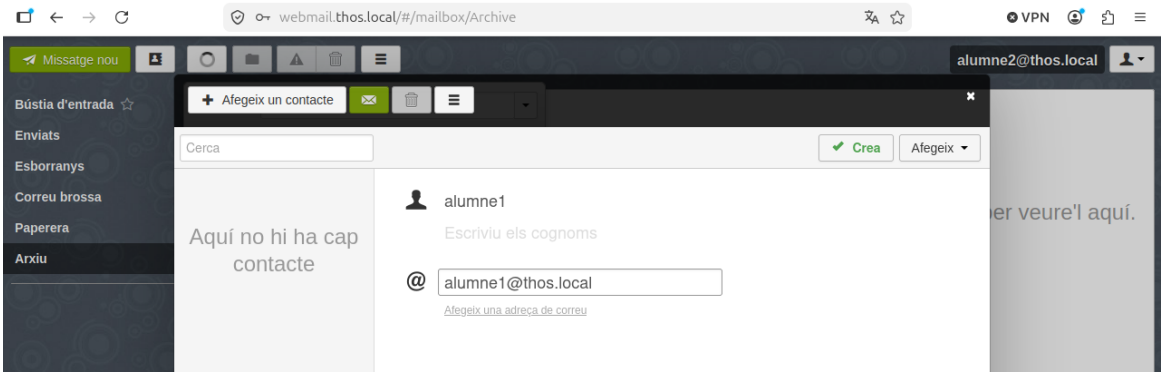

Figura 17: Nou contacte

Índex de figures

Versions d'aquest document

- HTML
- PDF
- ODT
- MD