

Infrastructure mail haute disponibilité

Postfix • Dovecot • HAProxy • Roundcube • LMTP • dsync

Conception, mise en œuvre, dépannage et validation de la tolérance aux pannes

Architecture mail redondante - vue logique

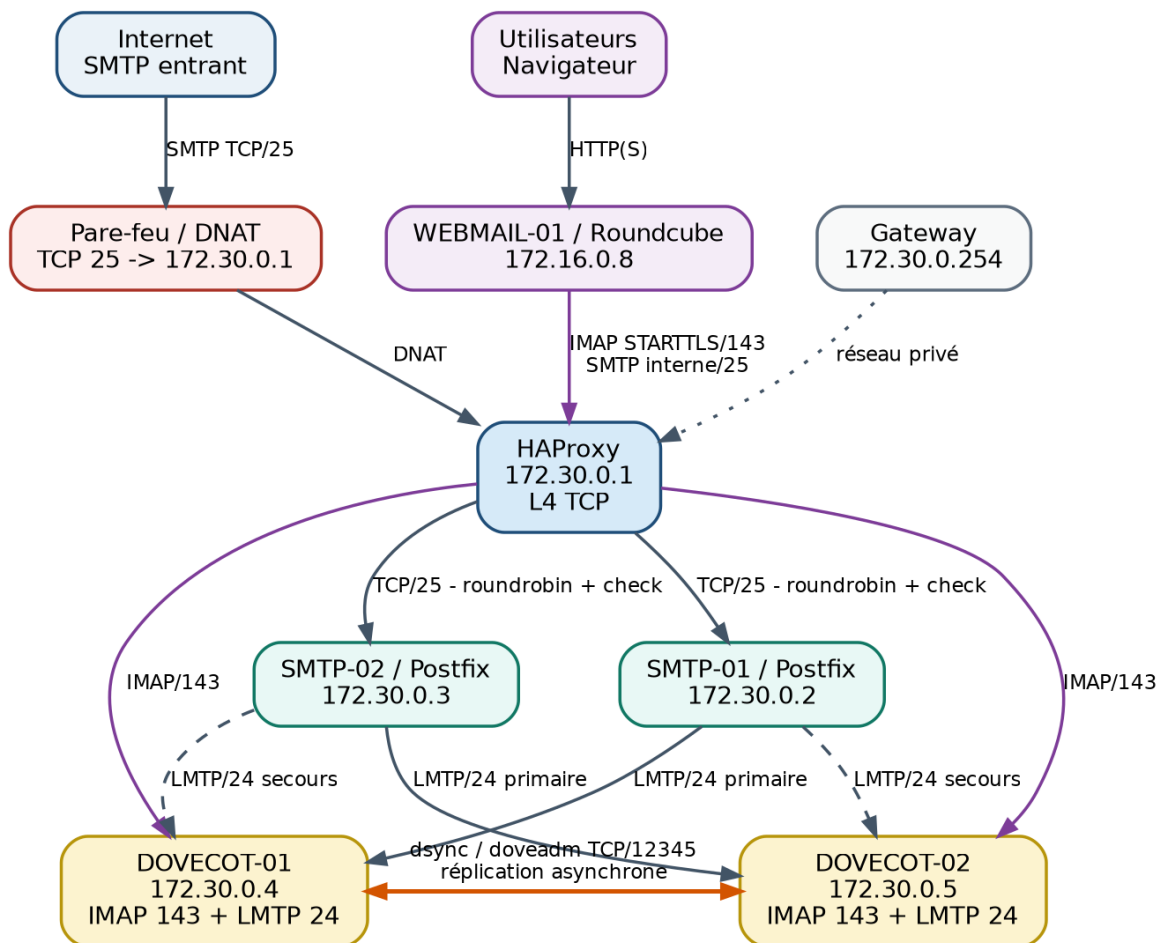


Schéma 1 — Architecture logique finale du laboratoire de messagerie.

Auteur	Adel Sadek
Date	14 août 2026
Environnement	Proxmox / conteneurs LXC Debian 12
Statut	Projet laboratoire — documentation portfolio
Périmètre	SMTP entrant, routage L4, LMTP, IMAP STARTTLS,

Résumé du projet

Je pars d'un objectif simple : séparer le transport SMTP du stockage et de l'accès aux boîtes mail, puis rendre chaque fonction redondante. Je déploie deux Postfix pour le transport, deux Dovecot pour les boîtes et l'IMAP, un HAProxy en frontal et un serveur Roundcube pour l'accès Web. Je valide ensuite chaque maillon par des tests réels : connexion TCP, réception depuis l'extérieur, livraison LMTP, authentification IMAP chiffrée, lecture via le webmail, panne d'un Dovecot et rattrapage automatique après son retour.

La difficulté du projet ne vient pas seulement de l'installation des services. Le vrai travail est dans l'assemblage : classes de domaines Postfix, protocole LMTP, utilisateurs système Dovecot, passage de mbox à Maildir, permissions des sockets UNIX, réplication dsync, comportement du replicator, STARTTLS sur IMAP 143, certificat de laboratoire, filtrage des comptes système et validation de la convergence après panne.

Résultat final — Le test final montre 14 messages dans INBOX sur DOVECOT-01 et 14 messages sur DOVECOT-02 après avoir coupé DOVECOT-01, reçu de nouveaux messages sur DOVECOT-02, puis remis DOVECOT-01 en ligne. La réplication rattrape donc les changements intervenus pendant la panne.

Compétences mobilisées

- Administration Linux Debian et services systemd.
- Virtualisation légère avec Proxmox LXC.
- Postfix : SMTP, domaines virtuels, files d'attente et transport LMTP.
- Dovecot : IMAP, LMTP, authentification, Maildir, dsync et replicator.
- HAProxy en couche 4 TCP avec round-robin et health checks.
- Roundcube comme client IMAP/SMTP centralisé.
- Réseau : DNAT, routage inter-réseaux, ports 25/24/143/12345 et TLS STARTTLS.
- Diagnostic par logs, telnet, nc, openssl s_client, swaks, doveadm, doveconf et postconf.
- Tests de panne et validation de la continuité de service.

Sommaire

- 1. Architecture et plan d'adressage
- 2. Rôle de chaque protocole et de chaque service
- 3. Publication SMTP : DNAT et HAProxy
- 4. Configuration Postfix et domaines hébergés
- 5. Dovecot et livraison LMTP
- 6. Validation du flux SMTP → LMTP → INBOX
- 7. Roundcube et accès IMAP chiffré
- 8. Réplication Dovecot avec dsync
- 9. Journal de dépannage : erreurs, causes et corrections
- 10. Tests de tolérance aux pannes
- 11. Configurations finales de référence
- 12. Limites actuelles et durcissement recommandé
- 13. Conclusion et bilan technique
- Annexe — Captures du projet et preuves de fonctionnement

1. Architecture et plan d'adressage

Je construis l'infrastructure sur un réseau privé 172.30.0.0. Les services sont séparés dans plusieurs conteneurs LXC afin qu'une panne applicative ou un redémarrage d'un service n'oblige pas à arrêter l'ensemble de la chaîne mail.

Composant	Adresse	Rôle principal
HAProxy	172.30.0.1	Point d'entrée TCP pour SMTP et IMAP
SMTP-01 / Postfix	172.30.0.2	MTA SMTP n°1
SMTP-02 / Postfix	172.30.0.3	MTA SMTP n°2
DOVECOT-01	172.30.0.4	IMAP + LMTP + stockage Maildir + réplication
DOVECOT-02	172.30.0.5	IMAP + LMTP + stockage Maildir + réplication
Gateway	172.30.0.254	Passerelle du réseau mail
WEBMAIL-01 / Roundcube	172.16.0.8	Interface Web, client IMAP/SMTP

1.1 Pourquoi séparer Postfix et Dovecot

Postfix et Dovecot n'ont pas le même rôle. Postfix reçoit, met en file d'attente, route et envoie les messages SMTP. Dovecot gère l'accès aux boîtes par IMAP et reçoit la livraison finale par LMTP. En séparant les deux fonctions, je peux redémarrer ou perdre un SMTP sans perdre l'accès aux boîtes, et je peux perdre un Dovecot tout en continuant à présenter l'autre aux utilisateurs.

Cette séparation évite aussi de créer un serveur monolithique qui concentre transport, stockage, authentification et interface Web sur la même machine. Les flux deviennent lisibles et chaque panne peut être isolée.

1.2 Schéma des flux

Architecture mail redondante - vue logique

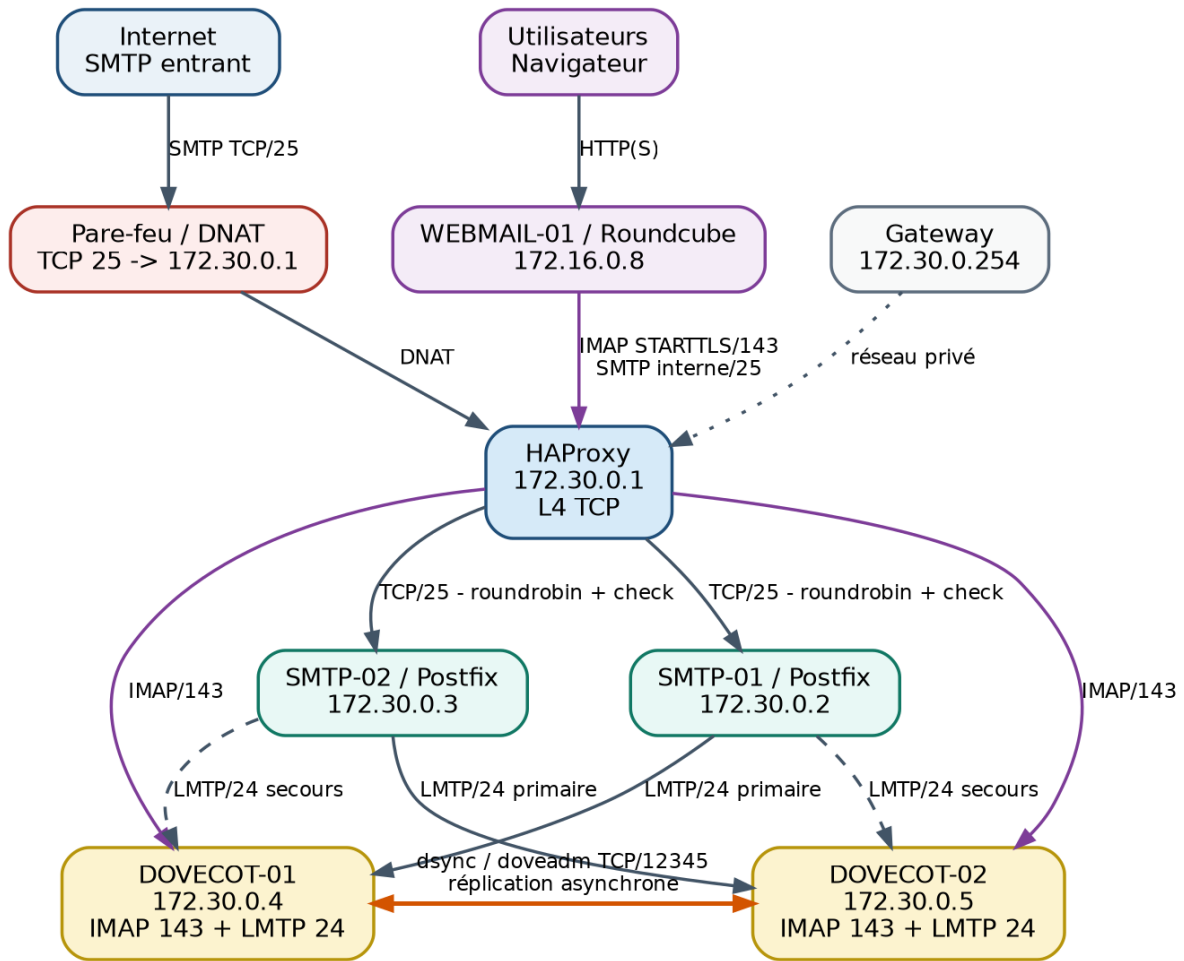


Schéma 2 — Flux SMTP entrant, LMTP, IMAP STARTTLS et réplique dsync.

Limite connue — HAProxy est encore unique dans cette version du laboratoire. Les SMTP et Dovecot sont redondants, mais 172.30.0.1 reste un point unique de panne. Je le traite dans la section de durcissement.

```
virtual_mailbox_domains =
sadek.ovh,
sadek-it.fr
mielamour.ovh
```

Figure 1 — Déclaration initiale des domaines virtuels Postfix dans le brouillon.

2. Rôle de chaque protocole et de chaque service

2.1 SMTP

SMTP transporte le message jusqu'à mon infrastructure. Le port TCP 25 est utilisé pour les échanges entre serveurs. HAProxy reçoit la connexion publique et la distribue vers SMTP-01 ou SMTP-02.

2.2 LMTP

LMTP est utilisé pour la remise finale entre Postfix et Dovecot. Le message a déjà été accepté par Postfix ; LMTP permet ensuite à Dovecot de répondre précisément pour le destinataire local. Dans ce laboratoire, le listener LMTP Dovecot écoute sur TCP 24.

2.3 IMAP et STARTTLS

IMAP permet à Roundcube de lister et lire la boîte. J'utilise le port 143 avec STARTTLS : la connexion commence sur 143 puis passe en TLS avant l'authentification. HAProxy reste en couche 4 et transmet le flux ; c'est Dovecot qui gère le protocole IMAP et le chiffrement.

2.4 dsync / doveadm

dsync est le mécanisme natif Dovecot utilisé pour synchroniser les boîtes. Le service doveadm écoute sur TCP 12345 entre les deux Dovecot. Les plugins notify et replication signalent les changements au replicator qui déclenche la synchronisation asynchrone.

2.5 Roundcube

Roundcube n'est pas le serveur mail. C'est un client Web : il se connecte en IMAP aux Dovecot via HAProxy pour lire les messages et en SMTP via HAProxy pour les envoyer. Les mails restent dans les Maildir Dovecot.

3. Publication SMTP : DNAT et HAProxy

Je publie le port 25 depuis l'extérieur vers le firewall. Une règle de DNAT renvoie ensuite ce port vers HAProxy 172.30.0.1. HAProxy travaille en mode TCP et distribue les nouvelles connexions vers les deux Postfix.

☐	LAN OpenVPN VLANERIC1000 WAN	TCP	*	*	This Firewall	25 (SMTP)	172.30.0.1	25 (SMTP)	SMTP-VLAN-SMTP			
	Enabled rule	!	No redirect				↔	Linked rule				
	Disabled rule	!	Disabled no redirect				↔	Disabled linked rule				
	Alias (click to view/edit)											

Figure 2 — Règle de DNAT utilisée pour amener le SMTP public vers HAProxy.

Pour valider le comportement du load balancer, je réalise plusieurs connexions successives depuis une machine externe vers moiselles.sadek.ovh sur le port 25. Les logs montrent que les connexions sont alternativement envoyées vers les deux backends SMTP.

```

root@HA-PROXY-01:~# tail -f /var/log/haproxy.log
2026-08-13T01:20:19.410586+00:00 HA-PROXY-01 haproxy[382]: 51.222.9.215:60472
[13/Aug/2026:01:20:03.735] SMTP-LOADBALANCER-01 CLUSTER-01/num1 1/481/15529
145 -- 1/1/0/0/0 0/0

root@smtp:~# telnet moiselles.sadek.ovh 25
Trying 189.190.94.232...
Connected to moiselles.sadek.ovh.
Escape character is '^'.
220 SMTP-02.localdomain ESMTP Postfix (Debian/GNU)
  
```

Figure 3 — Première connexion externe : HAProxy sélectionne un premier backend SMTP.

```

2026-08-13T01:23:27.981369+00:00 SMTP-01 postfix/smtpd[1371]: connect from unknown[172.30.0.1]
2026-08-13T01:24:17.982902+00:00 SMTP-01 postfix/smtpd[1371]: lost connection after CONNECT from unknown[172.30.0.1]
2026-08-13T01:24:17.983064+00:00 SMTP-01 postfix/smtpd[1371]: disconnect from unknown[172.30.0.1] commands=0/0

[ ] Exclude "SMTP-01" from MultiExec mode

root@HA-PROXY-01:~# tail -f /var/log/haproxy.log
2026-08-13T01:20:19.410586+00:00 HA-PROXY-01 haproxy[382]: 51.222.9.215:60472 [13/Aug/2026:01:20:03.735] SMTP-LOADBALANCER-01 CLUSTER-01/num1 1/481/15529 145 -- 1/1/0/0/0 0/0
2026-08-13T01:23:26.117734+00:00 HA-PROXY-01 haproxy[382]: 51.222.9.215:56510 [13/Aug/2026:01:23:08.733] SMTP-LOADBALANCER-01 CLUSTER-01/num2 1/0/17384 67 -- 1/1/0/0/0 0/0

[ ] Exclude "SMTP-02" from MultiExec mode

root@smtp:~# telnet moiselles.sadek.ovh 25
Trying 109.190.94.232...
Connected to moiselles.sadek.ovh.
Escape character is '^'.
220 SMTP-02.localdomain ESMTP Postfix (Debian/GNU)
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
root@smtp:~# telnet moiselles.sadek.ovh 25
Trying 109.190.94.232...
Connected to moiselles.sadek.ovh.
Escape character is '^'.
220 SMTP-01.localdomain ESMTP Postfix (Debian/GNU)
Connection closed by foreign host.
root@smtp:~#

[ ] Exclude "haproxy-01" from MultiExec mode
[ ] Exclude "smtp.agrepe.com (root)" from MultiExec mode

smtp.agrepe.com 0% 0,63 GB / 1,89 GB 0,01 Mb/s 0,00 Mb/s 34 days root (x2) /: 51% /boot/efi: 10%

```

Figure 4 — Connexion suivante : le backend SMTP change, ce qui valide l'alternance round-robin.

3.1 Configuration HAProxy de principe

```

frontend SMTP-LOADBALANCER-01
  bind 172.30.0.1:25
  mode tcp
  option tcplog
  default_backend CLUSTER-01

backend CLUSTER-01
  mode tcp
  balance roundrobin
  server num1 172.30.0.2:25 check
  server num2 172.30.0.3:25 check

```

Extrait de référence — équilibrage SMTP L4.

Le mot-clé `check` est important : un serveur qui ne répond plus au health check TCP est retiré de la rotation. Le round-robin agit au niveau des connexions, pas au niveau d'un message déjà accepté.

4. Configuration Postfix et domaines hébergés

4.1 Ne pas mélanger mydestination et virtual_mailbox_domains

Au début, mes domaines étaient placés dans mydestination. Ce paramètre correspond aux domaines locaux gérés par la livraison locale Postfix. Or mon objectif est de remettre les messages à Dovecot. Je garde donc uniquement le hostname et localhost dans mydestination, puis je déclare les domaines hébergés dans virtual_mailbox_domains.

```
mydestination =
    $myhostname,
    localhost.$mydomain,
    localhost

virtual_mailbox_domains =
    sadek.ovh,
    sadek-it.fr,
    mieldamour.ovh
```

Point de syntaxe — Une ligne de continuation Postfix doit commencer par un espace ou une tabulation. Sans indentation, une ligne comme « sadek.ovh, » est interprétée comme le nom d'un nouveau paramètre et Postfix renvoie une erreur de syntaxe « missing = after attribute name ».

4.2 Transport LMTP et stratégie primaire/secours

Chaque SMTP privilégie un Dovecot différent. Cela répartit naturellement les livraisons lorsque tout fonctionne, tout en donnant à chaque Postfix un serveur LMTP de secours.

```
# SMTP-01
virtual_transport = lmtp:[172.30.0.4]:24
lmtp_fallback_relay = [172.30.0.5]:24

# SMTP-02
virtual_transport = lmtp:[172.30.0.5]:24
lmtp_fallback_relay = [172.30.0.4]:24
```

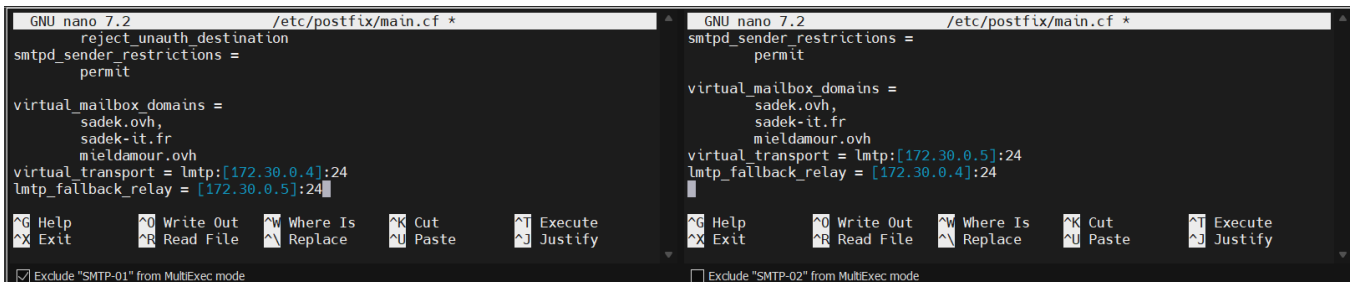


Figure 5 — Configurations Postfix des deux nœuds, avec transport LMTP et fallback inversés.

5. Dovecot et livraison LMTP

5.1 Activation de LMTP

J'installe Dovecot avec le service LMTP puis j'active les protocoles imap et lmtp. Chaque nœud écoute sur sa propre adresse privée, port 24.

```
service lmtp {
  unix_listener lmtp {
    #mode = 0666
  }
  inet_listener lmtp {
    address = 172.30.0.4
    port = 24
  }
}
```

Figure 6 — DOVECOT-01 : listener LMTP sur 172.30.0.4:24.

```
service lmtp {
  unix_listener lmtp {
    #mode = 0666
  }
  inet_listener lmtp {
    address = 172.30.0.5
    port = 24
  }
}
# Create inet listener only if you can't use the above UNIX socket
```

Figure 7 — DOVECOT-02 : listener LMTP sur 172.30.0.5:24.

```
root@DOVECOT-01:~# nano /etc/dovecot/conf.d/10-master.conf
root@DOVECOT-01:~# doveconf protocols
protocols = imap lmtp
root@DOVECOT-01:~#
```

Figure 8 — Vérification des protocoles Dovecot : IMAP et LMTP sont actifs.

```
tivated successfully.
2026-08-13T01:40:06.564019+00:00 DOVECOT-01 systemd[1]: Stopped dovecot.servi
ce - Dovecot IMAP/POP3 email server.
2026-08-13T01:40:06.707293+00:00 DOVECOT-01 systemd[1]: Starting dovecot.servi
ce - Dovecot IMAP/POP3 email server...
2026-08-13T01:40:06.926814+00:00 DOVECOT-01 dovecot: master: Dovecot v2.3.19.
1 (9b53102964) starting up for imap, lmtp (core dumps disabled)
2026-08-13T01:40:06.938067+00:00 DOVECOT-01 systemd[1]: Started dovecot.servi
ce - Dovecot IMAP/POP3 email server.
^C
root@DOVECOT-01:~# ss -lntp | grep ':24'
LISTEN 0      100        172.30.0.4:24      0.0.0.0:*      users:((("dovecot",p
id=3977,fd=26))
root@DOVECOT-01:~#
```

☒ Exclude "dovecot-01" from MultiExec mode

Figure 9 — Dovecot démarre pour imap,lmtp et écoute bien sur 172.30.0.4:24.

5.2 Test de connectivité LMTP

Avant de tester une vraie livraison, je vérifie simplement la couche réseau. Depuis un SMTP, un telnet vers chaque Dovecot sur le port 24 doit retourner la bannière Dovecot.

```
root@SMTP-01:~# telnet 172.30.0.4 24
Trying 172.30.0.4...
Connected to 172.30.0.4.
Escape character is '^]'.
220 DOVECOT-01.1.1.1.1 Dovecot (Debian) ready.
QUIT
221 2.0.0 Bye
```

Figure 10 — Test telnet SMTP-01 → DOVECOT-01 sur TCP 24.

```
root@SMTP-01:~# telnet 172.30.0.5 24
Trying 172.30.0.5...
Connected to 172.30.0.5.
Escape character is '^]'.
220 DOVECOT-02.1.1.1.1 Dovecot (Debian) ready.
```

Figure 11 — Test telnet SMTP-01 → DOVECOT-02 sur TCP 24.

5.3 Correspondance entre adresse mail et utilisateur Linux

Pour le laboratoire, je crée des utilisateurs Linux réels comme asadek et contact sur les deux Dovecot. Comme l'utilisateur se connecte avec une adresse complète, par exemple asadek@sadek.ovh, j'utilise `auth_username_format = %n` afin que Dovecot retire la partie @domaine pour la recherche du compte système.

```
protocol lmtp {
  # Space separated list of plugins to load (default is global mail_plugins).
  #mail_plugins = $mail_plugins
  postmaster_address = postmaster@sadek.ovh
  auth_username_format = %n
```

```
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

Figure 12 — Configuration LMTP avec `postmaster_address` et conversion du nom utilisateur via `%n`.

```
root@DOVECOT-01:~# service dovecot restart
root@DOVECOT-01:~# dovecadm user asadek
field  value
uid    1000
gid    1000
home    /home/asadek
mail    mbox:~/mail:INBOX=/var/mail/asadek
system_groups_user  asadek
root@DOVECOT-01:~#
```

☐ Exclude "dovecot-01" from MultiExec mode

```
root@DOVECOT-02:~# service dovecot restart
root@DOVECOT-02:~# dovecadm user asadek
field  value
uid    1000
gid    1000
home    /home/asadek
mail    mbox:~/mail:INBOX=/var/mail/asadek
system_groups_user  asadek
root@DOVECOT-02:~#
```

☐ Exclude "dovecot-02" from MultiExec mode

Figure 13 — `doveadm user` sur les deux Dovecot : mêmes UID/GID et même home pour asadek.

6. Validation du flux SMTP → LMTP → INBOX

Je teste ensuite un vrai message. swaks me permet d'ouvrir une session SMTP contrôlée, de définir le destinataire et de suivre la réponse du serveur.

```
-> From: root@SMTP-02.1.1.1.1
-> Subject: test Thu, 13 Aug 2026 01:48:39 +0000
-> Message-Id: <20260813014839.001605@SMTP-02.1.1.1.1>
-> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
->
-> This is a test mailing
->
->
-> .
<- 250 2.0.0 Ok: queued as C8B285392
-> QUIT
<- 221 2.0.0 Bye
=== Connection closed with remote host.
root@SMTP-02:~#
```

Figure 14 — Message injecté avec swaks depuis SMTP-02.

Le premier test arrive bien dans le client LMTP Postfix, mais Dovecot répond que l'utilisateur n'existe pas. Cette erreur est utile : elle prouve que le réseau, Postfix et LMTP fonctionnent déjà ; le problème se situe uniquement dans la résolution du destinataire côté Dovecot.

```
nt=unknown[172.30.0.3]
2026-08-13T01:48:39.823100+00:00 SMTP-01 postfix/cleanup[1726]: C8B285392: message-id=<20260813014839.001605@SMTP-02.1.1.1.1>
2026-08-13T01:48:39.826840+00:00 SMTP-01 postfix/smtpd[1722]: disconnect from unknown[172.30.0.3] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
2026-08-13T01:48:39.827421+00:00 SMTP-01 postfix/qmgr[1713]: C8B285392: from=<root@SMTP-02.1.1.1.1>, size=451, nrcpt=1 (queue active)
2026-08-13T01:48:40.002736+00:00 SMTP-01 postfix/lmtp[1731]: C8B285392: to=<adel@sadek.ovh>, relay=172.30.0.4[172.30.0.4]:24, delay=0.18, delays=0.01/0.01/0.01/0.16, dsn=5.1.1, status=bounced (host 172.30.0.4[172.30.0.4] said: 550 5.1.1 <adel@sadek.ovh> User doesn't exist: adel@sadek.ovh (in reply to RCPT TO command))
2026-08-13T01:48:40.004088+00:00 SMTP-01 postfix/cleanup[1726]: 00D50560D: message-id=<20260813014840.00D50560D@SMTP-01.localdomain>
```

Figure 15 — Postfix utilise bien postfix/lmtp vers 172.30.0.4:24 ; Dovecot refuse seulement le destinataire inexistant.

```
nt=unknown[172.30.0.3]
2026-08-13T01:48:39.823100+00:00 SMTP-01 postfix/cleanup[1726]: C8B285392: message-id=<20260813014839.001605@SMTP-02.1.1.1.1>
2026-08-13T01:48:39.826840+00:00 SMTP-01 postfix/smtpd[1722]: disconnect from unknown[172.30.0.3] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
2026-08-13T01:48:39.827421+00:00 SMTP-01 postfix/qmgr[1713]: C8B285392: from=<root@SMTP-02.1.1.1.1>, size=451, nrcpt=1 (queue active)
2026-08-13T01:48:40.002736+00:00 SMTP-01 postfix/lmtp[1731]: C8B285392: to=<adel@sadek.ovh>, relay=172.30.0.4[172.30.0.4]:24, delay=0.18, delays=0.01/0.01/0.01/0.16, dsn=5.1.1, status=bounced (host 172.30.0.4[172.30.0.4] said: 550 5.1.1 <adel@sadek.ovh> User doesn't exist: adel@sadek.ovh (in reply to RCPT TO command))
2026-08-13T01:48:40.004088+00:00 SMTP-01 postfix/cleanup[1726]: 00D50560D: message-id=<20260813014840.00D50560D@SMTP-01.localdomain>
```

Figure 16 — Même trace remise en contexte dans le brouillon : le maillon LMTP est validé malgré le 550 utilisateur inconnu.

6.1 Test depuis l'extérieur

```
root@smtp:~# swaks -t asadek@sadek.ovh -s moiselles.sadek.ovh
=== Trying moiselles.sadek.ovh:25...
=== Connected to moiselles.sadek.ovh.
<- 220 SMTP-02.localdomain ESMTP Postfix (Debian/GNU)
-> EHLO smtp.agrepe.com
<- 250-SMTP-02.localdomain
<- 250-PIPELINING
<- 250-SIZE 10240000
<- 250-VRFY
<- 250-ETRN
<- 250-ENHANCEDSTATUSCODES
<- 250-8BITMIME
<- 250-DSN
<- 250-SMTPUTF8
```

Figure 17 — Envoi externe vers moiselles.sadek.ovh avec swaks.

```
2026-08-13T02:00:59.357101+00:00 HA-PROXY-01 haproxy[382]: 51.222.9.215:59718
[13/Aug/2026:02:00:58.700] SMTP-LOADBALANCER-01 CLUSTER-01/num1 1/0/657 323
-- 1/1/0/0/0 0/0
2026-08-13T02:02:14.903297+00:00 HA-PROXY-01 haproxy[382]: 51.222.9.215:47610
[13/Aug/2026:02:02:14.056] SMTP-LOADBALANCER-01 CLUSTER-01/num2 1/0/846 323
-- 1/1/0/0/0 0/0
```

Figure 18 — Les logs HAProxy montrent les connexions SMTP reçues et distribuées.

```
nt=unknown[172.30.0.1]
2026-08-13T02:02:14.721836+00:00 SMTP-02 postfix/cleanup[1615]: 84C3D56BB: me
ssage-id=<20260813020213.1829988@smtp.agrepe.com>
2026-08-13T02:02:14.726020+00:00 SMTP-02 postfix/qmgr[1593]: 84C3D56BB: from=
<root@smtp.agrepe.com>, size=456, nrcpt=1 (queue active)
2026-08-13T02:02:14.814087+00:00 SMTP-02 postfix/lmtp[1616]: 84C3D56BB: to=<a
sadek@sadek.ovh>, relay=172.30.0.5[172.30.0.5]:24, delay=0.36, delays=0.28/0.
01/0.04/0.03, dsn=2.0.0, status=sent (250 2.0.0 <asadek@sadek.ovh> f05dLqYlfW
r6DwAAaW+5GA Saved)
2026-08-13T02:02:14.814584+00:00 SMTP-02 postfix/qmgr[1593]: 84C3D56BB: remov
ed
2026-08-13T02:02:14.814664+00:00 SMTP-02 postfix/smtpd[1611]: disconnect from
unknown[172.30.0.1] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
```

Figure 19 — Côté Postfix, le message est remis par LMTP au Dovecot sélectionné avec status=sent.

```

2026-08-13T01:58:47.776904+00:00 DOVECOT-02 dovecot: master: Warning: Killed
with signal 15 (by pid=4064 uid=0 code=kill)
2026-08-13T01:58:49.019072+00:00 DOVECOT-02 dovecot: master: Dovecot v2.3.19.
1 (9b53102964) starting up for imap, lmtmp (core dumps disabled)

2026-08-13T02:02:14.778344+00:00 DOVECOT-02 dovecot: lmtmp(4090): Connect from
172.30.0.3
2026-08-13T02:02:14.813507+00:00 DOVECOT-02 dovecot: lmtmp(asadek)<4090><f05dL
qYlfWr6DwAAw+5GA>: msgid=<20260813020213.1829988@smtp.agrepe.com>: saved mai
l to INBOX
2026-08-13T02:02:14.813957+00:00 DOVECOT-02 dovecot: lmtmp(4090): Disconnect f
rom 172.30.0.3: Logged out (state=READY)

☒ Exclude "dovecot-02" from MultiExec mode

```

Figure 20 — Côté Dovecot, LMTP enregistre le message dans INBOX.

Validation — À ce stade, la chaîne Internet → DNAT → HAProxy → Postfix → LMTP → Dovecot → INBOX fonctionne de bout en bout.

6.2 Premier test de panne applicative

Je coupe volontairement SMTP-02 et DOVECOT-02. Les connexions continuent via les nœuds restants. Ce test vérifie que la redondance n'est pas seulement théorique.

```

nt=unknown[172.30.0.1]
2026-08-13T02:06:41.509167+00:00 SMTP-01 postfix/cleanup[1748]: 50C8C5392: me
ssage-id=<20260813020640.1831536@smtp.agrepe.com>
2026-08-13T02:06:41.513124+00:00 SMTP-01 postfix/qmgr[1713]: 50C8C5392: from=
<root@smtp.agrepe.com>, size=456, nrcpt=1 (queue active)
2026-08-13T02:06:41.578377+00:00 SMTP-01 postfix/lmtmp[1749]: 50C8C5392: to=<a
sadek@asadek.ovh>, relay=172.30.0.4[172.30.0.4]:24, delay=0.34, delays=0.28/0.
01/0.01/0.05, dsn=2.0.0, status=sent (250 2.0.0 <asadek@asadek.ovh> kB6dH7EmfW
oFEAA4Jfatg Saved)
2026-08-13T02:06:41.578491+00:00 SMTP-01 postfix/qmgr[1713]: 50C8C5392: remov
ed
2026-08-13T02:06:41.601562+00:00 SMTP-01 postfix/smtpd[1744]: disconnect from
unknown[172.30.0.1] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5

☒ Exclude "SMTP-01" from MultiExec mode

2026-08-13T02:06:27.185749+00:00 HA-PROXY-01 haproxy[382]: [WARNING] (382) :
Server CLUSTER-01/num2 is DOWN, reason: Layer4 timeout, check duration: 2001
ms. 1 active and 0 backup servers left. 0 sessions active, 0 requested, 0 rema
ining in queue.
2026-08-13T02:06:27.185388+00:00 HA-PROXY-01 haproxy[382]: Server CLUSTER-01/
num2 is DOWN, reason: Layer4 timeout, check duration: 2001ms. 1 active and 0
backup servers left. 0 sessions active, 0 requested, 0 remaining in queue.
2026-08-13T02:06:27.185396+00:00 HA-PROXY-01 haproxy[382]: Server CLUSTER-01/
num2 is DOWN, reason: Layer4 timeout, check duration: 2001ms. 1 active and 0
backup servers left. 0 sessions active, 0 requested, 0 remaining in queue.
2026-08-13T02:06:41.690686+00:00 HA-PROXY-01 haproxy[382]: 51.222.9.215:42898
[13/Aug/2026:02:06:41.032] SMTP-LOADBALANCER-01 CLUSTER-01/num1 1/0/658 323
-- 1/1/0/0/0 0/0

☒ Exclude "haproxy-01" from MultiExec mode

2026-08-13T01:58:47.775992+00:00 DOVECOT-01 dovecot: master: Warning: Killed
with signal 15 (by pid=4074 uid=0 code=kill)
2026-08-13T01:58:48.917398+00:00 DOVECOT-01 dovecot: master: Dovecot v2.3.19.
1 (9b53102964) starting up for imap, lmtmp (core dumps disabled)

2026-08-13T02:06:41.530877+00:00 DOVECOT-01 dovecot: lmtmp(4101): Connect from
172.30.0.2
2026-08-13T02:06:41.577307+00:00 DOVECOT-01 dovecot: lmtmp(asadek)<4101><kB6dH
7EmfWoFEAA4Jfatg>: msgid=<20260813020640.1831536@smtp.agrepe.com>: saved mai
l to INBOX
2026-08-13T02:06:41.577917+00:00 DOVECOT-01 dovecot: lmtmp(4101): Disconnect f
rom 172.30.0.2: Logged out (state=READY)

☒ Exclude "dovecot-01" from MultiExec mode

ssage-id=<20260813020213.1829988@smtp.agrepe.com>
2026-08-13T02:02:14.726020+00:00 SMTP-02 postfix/qmgr[1593]: 84C3D56BB: from=
<root@smtp.agrepe.com>, size=456, nrcpt=1 (queue active)
2026-08-13T02:02:14.814087+00:00 SMTP-02 postfix/lmtmp[1616]: 84C3D56BB: to=<a
sadek@asadek.ovh>, relay=172.30.0.5[172.30.0.5]:24, delay=0.36, delays=0.28/0.
01/0.04/0.03, dsn=2.0.0, status=sent (250 2.0.0 <asadek@asadek.ovh> f05dLqYlfW
r6DwAAw+5GA Saved)
2026-08-13T02:02:14.814584+00:00 SMTP-02 postfix/qmgr[1593]: 84C3D56BB: remov
ed
2026-08-13T02:02:14.814664+00:00 SMTP-02 postfix/smtpd[1611]: disconnect from
unknown[172.30.0.1] ehlo=1 mail=1 rcpt=1 data=1 quit=1 commands=5
Connection to 172.30.0.3 closed by remote host.
Connection to 172.30.0.3 closed.
root@0PNsense:~ #

☒ Exclude "SMTP-02" from MultiExec mode

-> From: root@smtp.agrepe.com
-> Subject: test Thu, 13 Aug 2026 02:06:40 +0000
-> Message-Id: <20260813020640.1831536@smtp.agrepe.com>
-> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
->
-> This is a test mailing
->
->
-> .
<- 250 2.0.0 Ok: queued as 50C8C5392
-> QUIT
<- 221 2.0.0 Bye
=== Connection closed with remote host.
root@smtp:~#

☐ Exclude "smtp.agrepe.com (root)" from MultiExec mode

2026-08-13T01:58:49.019072+00:00 DOVECOT-02 dovecot: master: Dovecot v2.3.19.
1 (9b53102964) starting up for imap, lmtmp (core dumps disabled)

2026-08-13T02:02:14.778344+00:00 DOVECOT-02 dovecot: lmtmp(4090): Connect from
172.30.0.3
2026-08-13T02:02:14.813507+00:00 DOVECOT-02 dovecot: lmtmp(asadek)<4090><f05dL
qYlfWr6DwAAw+5GA>: msgid=<20260813020213.1829988@smtp.agrepe.com>: saved mai
l to INBOX
2026-08-13T02:02:14.813957+00:00 DOVECOT-02 dovecot: lmtmp(4090): Disconnect f
rom 172.30.0.3: Logged out (state=READY)
Connection to 172.30.0.5 closed by remote host.
Connection to 172.30.0.5 closed.
root@0PNsense:~ #

☒ Exclude "dovecot-02" from MultiExec mode

```

Figure 21 — Test multi-terminal pendant l'arrêt d'un SMTP et d'un Dovecot : le service continue.

Figure 22 — Vue du pare-feu/règles pendant le test de continuité.

7. Roundcube et accès IMAP chiffré

7.1 Architecture du webmail

Je déploie Roundcube dans un LXC séparé. Roundcube pointe uniquement vers HAProxy : IMAP sur 172.30.0.1:143 et SMTP sur 172.30.0.1:25 pour les tests internes. Ainsi, Roundcube n'a pas besoin de connaître le Dovecot ou le Postfix réellement utilisé derrière le load balancer.

```

inetutils-telnet
The following NEW packages will be installed:
telnet
The following packages will be upgraded:
inetutils-telnet
1 upgraded, 1 newly installed, 0 to remove and 54 not upgraded.
Need to get 163 kB of archives.
After this operation, 56.3 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 inetutils-telnet amd64 2:2.4-2+deb12u3 [121 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 telnet all 0.17+2.4-2+deb12u3 [41.9 kB]
Fetched 163 kB in 0s (1331 kB/s)
apt-listchanges: Reading changelogs...
(Reading database ... 26075 files and directories currently installed.)
Preparing to unpack .../inetutils-telnet_2%3a2.4-2+deb12u3_amd64.deb ...
Unpacking inetutils-telnet (2:2.4-2+deb12u3) over (2:2.4-2+deb12u1) ...
Selecting previously unselected package telnet.
Preparing to unpack .../telnet_0.17+2.4-2+deb12u3_all.deb ...
Unpacking telnet (0.17+2.4-2+deb12u3) ...
Setting up inetutils-telnet (2:2.4-2+deb12u3) ...
Setting up telnet (0.17+2.4-2+deb12u3) ...
Processing triggers for man-db (2.11.2-2) ...
root@WEBMAIL-01:~# telnet 172.30.0.4 143
Trying 172.30.0.4...
Connected to 172.30.0.4.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS LOGINDISABLED] Dovecot (Debian) read
y.

```

Figure 23 — Depuis WEBMAIL-01, telnet vers 172.30.0.4:143 confirme que le service IMAP Dovecot répond et annonce STARTTLS.

```

frontend IMAP-LOADBALANCER-01
    bind 172.30.0.1:143
    default_backend CLUSTER-02
backend CLUSTER-02
    balance roundrobin
    server num1 172.30.0.4:143 check
    server num2 172.30.0.5:143 check

```

Figure 24 — Configuration HAProxy du frontend IMAP 143 et du backend Dovecot en round-robin.

```

GNU nano 7.2 /etc/roundcube/config.inc.php *

$config = [];

// Do not set db_dsnw here, use dpkg-reconfigure roundcube-core to configure database!
include("/etc/roundcube/debian-db-roundcube.php");

// IMAP host chosen to perform the log-in.
// See defaults.inc.php for the option description.
$config['imap_host'] = ["172.30.0.1:143"];

// SMTP server host (for sending mails).
// See defaults.inc.php for the option description.
$config['smtp_host'] = '172.30.0.1:25';

// SMTP username (if required) if you use %u as the username Roundcube
// will use the current username for login
$config['smtp_user'] = '';

// SMTP password (if required) if you use %p as the password Roundcube
// will use the current user's password for login
$config['smtp_pass'] = '';

// provide an URL where a user can get support for this Roundcube installation
// PLEASE DO NOT LINK TO THE ROUND CUBE .NET WEBSITE HERE!

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Und
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_/ Go To Line M-F Red

```

Figure 25 — Configuration Roundcube : IMAP et SMTP pointent vers l'adresse HAProxy 172.30.0.1.

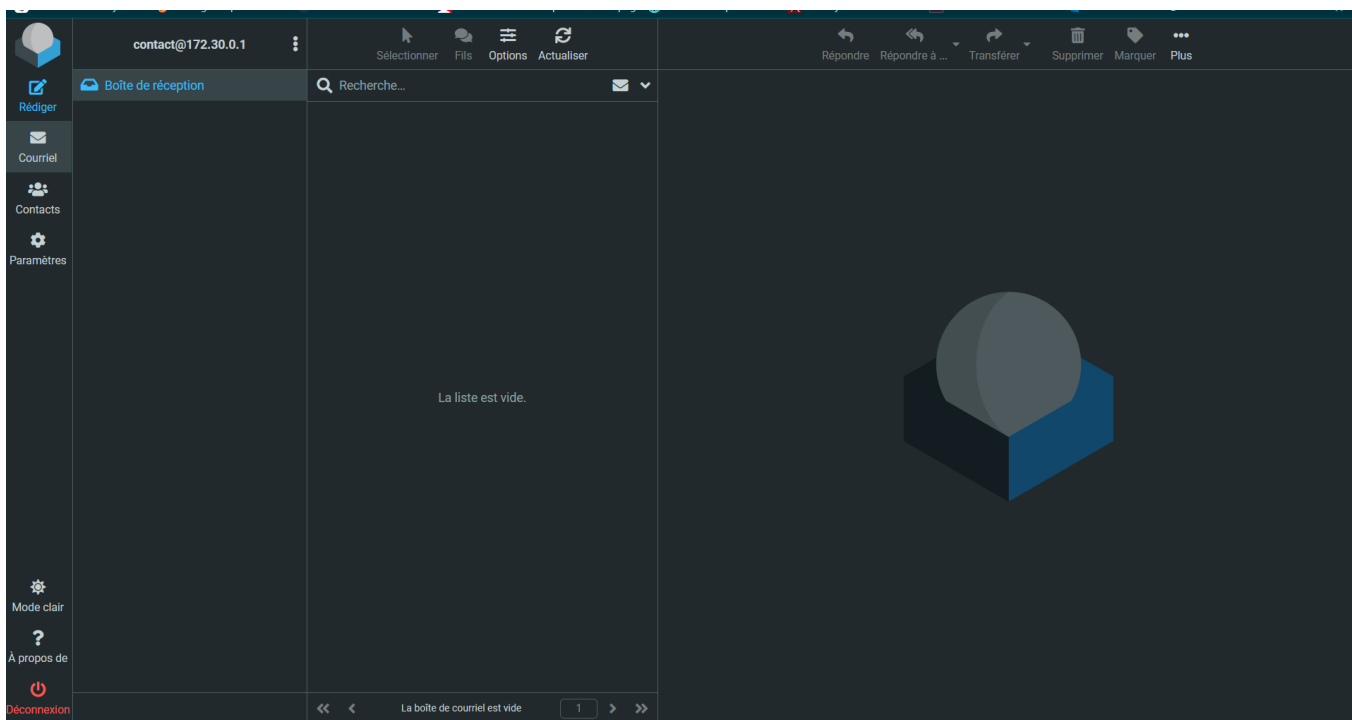


Figure 26 — Première ouverture du webmail Roundcube après raccordement à l'infrastructure.

7.2 STARTTLS sur 143

Dovecot refuse l'authentification LOGIN/PLAIN sur une connexion non chiffrée. Je garde cette protection et je fais utiliser STARTTLS à Roundcube sur le port 143. La configuration Roundcube devient `tls://172.30.0.1:143`.

```

$config['imap_host'] = 'tls://172.30.0.1:143';
$config['smtp_host'] = '172.30.0.1:25';

```

Dans les logs, le passage de « unsupported auth mechanism » à « disallowed plaintext auth » m'a permis de distinguer deux problèmes : d'abord le mécanisme LOGIN absent, ensuite l'absence de TLS. J'active donc `auth_mechanisms = plain login` et je conserve `disable_plaintext_auth = yes`.

7.3 Certificat de laboratoire

Le certificat Dovecot par défaut avait un CN=localhost. Roundcube se connectant à 172.30.0.1, PHP refuse la négociation TLS à cause du nom de certificat. Pour le laboratoire, je désactive temporairement la validation du peer côté Roundcube afin de valider la chaîne fonctionnelle.

```
$config['imap_conn_options'] = [  
  'ssl' => [  
    'verify_peer' => false,  
    'verify_peer_name' => false,  
    'allow_self_signed' => true,  
  ],  
];
```

Important — Ce contournement ne doit pas rester en production. La version durcie doit utiliser un certificat valide pour un nom DNS stable (ex. mail.sadek.ovh), puis réactiver `verify_peer` et `verify_peer_name`.

8. Réplication Dovecot avec dsync

Le webmail fonctionne, mais avec deux Dovecot en stockage local, un nouveau problème apparaît : une connexion IMAP peut tomber sur un serveur qui ne possède pas encore le même état de boîte. Il faut donc synchroniser les deux Maildir.

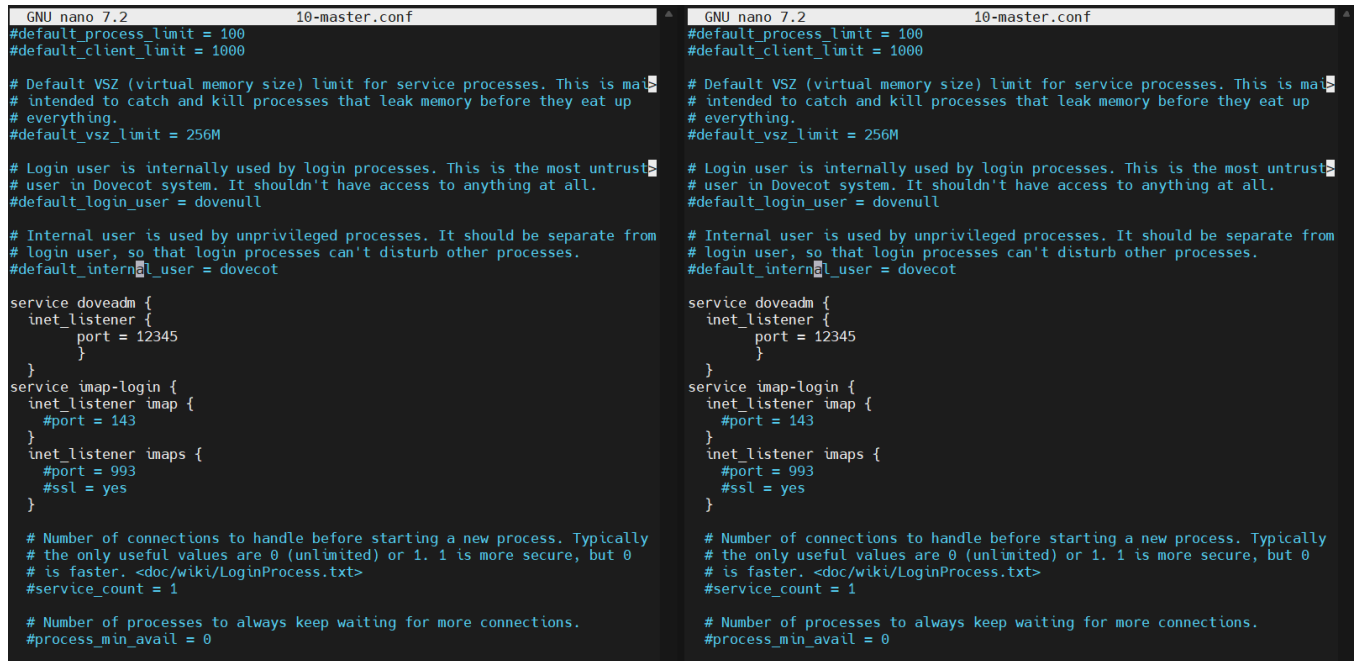


Figure 27 — Roundcube fonctionne, mais la réplication des deux Dovecot reste à mettre en place.

8.1 Pourquoi dsync et pas rsync

Je n'utilise pas rsync directement sur les fichiers de boîtes actives. Dovecot maintient des UID, des flags, des index et des fichiers de contrôle. dsync connaît ces métadonnées et sait fusionner les changements des deux côtés. C'est donc l'outil adapté à une réplication Dovecot.

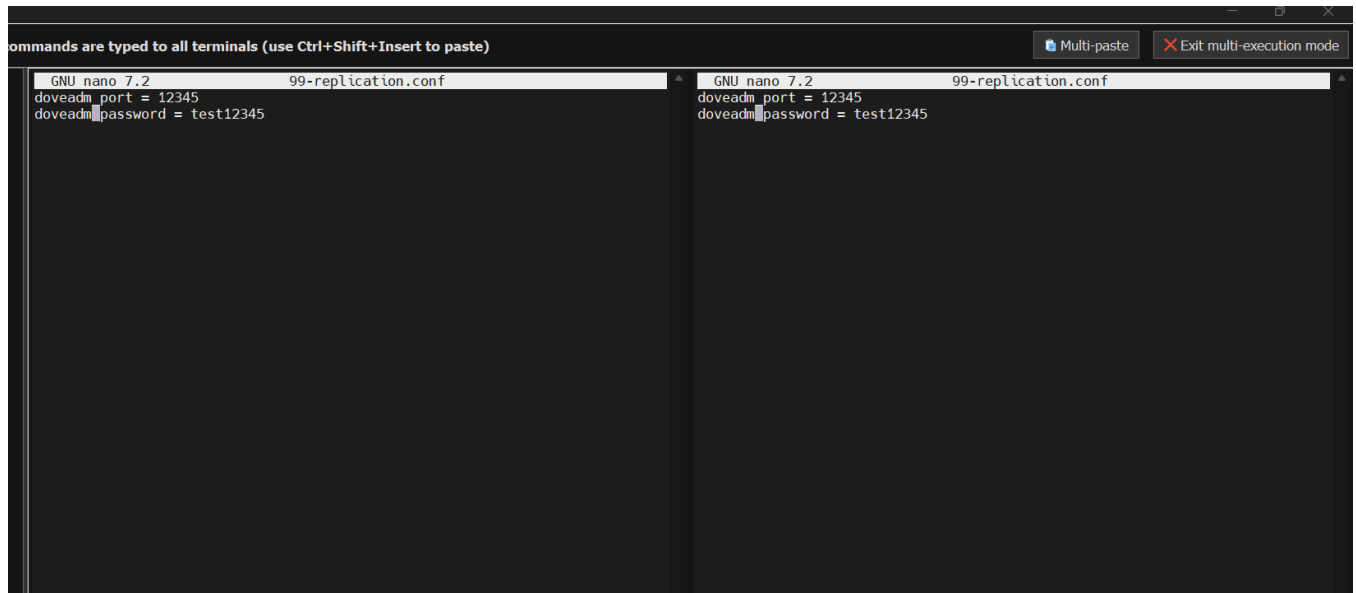


Figure 28 — Ajout initial du listener dovecadm TCP 12345 dans 10-master.conf pendant la phase de test.

```

: commands are typed to all terminals (use Ctrl+Shift+Insert to paste)
Multi-paste Exit multi-execution mode

root@DOVECOT-01:/etc/dovecot/conf.d# nano 99-replication.conf
root@DOVECOT-01:/etc/dovecot/conf.d# service dovecot restart
root@DOVECOT-01:/etc/dovecot/conf.d# telnet 172.30.0.5 12345
Trying 172.30.0.5...
Connected to 172.30.0.5.
Escape character is '^J'.

root@DOVECOT-02:/etc/dovecot/conf.d# nano 99-replication.conf
root@DOVECOT-02:/etc/dovecot/conf.d# service dovecot restart
root@DOVECOT-02:/etc/dovecot/conf.d# telnet 172.30.0.4 12345
Trying 172.30.0.4...
Connected to 172.30.0.4.
Escape character is '^J'.

```

Figure 29 — Premiers paramètres de réplication et secret partagé dans 99-replication.conf.

```

: commands are typed to all terminals (use Ctrl+Shift+Insert to paste)
Multi-paste Exit multi-execution mode

root@DOVECOT-01:/etc/dovecot/conf.d# id asadek
uid=1000(asadek) gid=1000(asadek) groups=1000(asadek),100(users)
root@DOVECOT-01:/etc/dovecot/conf.d#

root@DOVECOT-02:/etc/dovecot/conf.d# id asadek
uid=1000(asadek) gid=1000(asadek) groups=1000(asadek),100(users)
root@DOVECOT-02:/etc/dovecot/conf.d#

```

Figure 30 — Vérification de la connectivité TCP/12345 entre les deux Dovecot.

8.2 Secret de réplication

Identifiant temporaire — Secret utilisé pendant le laboratoire : test12345. Il est documenté ici volontairement, mais doit être remplacé immédiatement après export de cette documentation.

```
doveadm_password = test12345
```

8.3 Passage obligatoire à Maildir

La première commande dsync déclenche un panic dans mbox-lock.c. À ce moment, Dovecot utilise encore le stockage mbox issu des comptes Linux. Je force donc le stockage en Maildir sur les deux nœuds : mail_location = maildir:~/Maildir.

```
root@DOVECOT-01:/etc/dovecot/conf.d# id asadek
uid=1000(asadek) gid=1000(asadek) groups=1000(asadek),100(users)
root@DOVECOT-01:/etc/dovecot/conf.d# doveadm sync -f -u asadek tcp:172.30.0.5:12345
doveadm(asadek): Error: /run/dovecot/auth-userdb: Configured passdbs don't support credentials lookups (to see if user is proxied, because doveadm_port is set)
root@DOVECOT-01:/etc/dovecot/conf.d#
```

Figure 31 — Première tentative de synchronisation et première erreur liée au backend d'authentification/port doveadm.

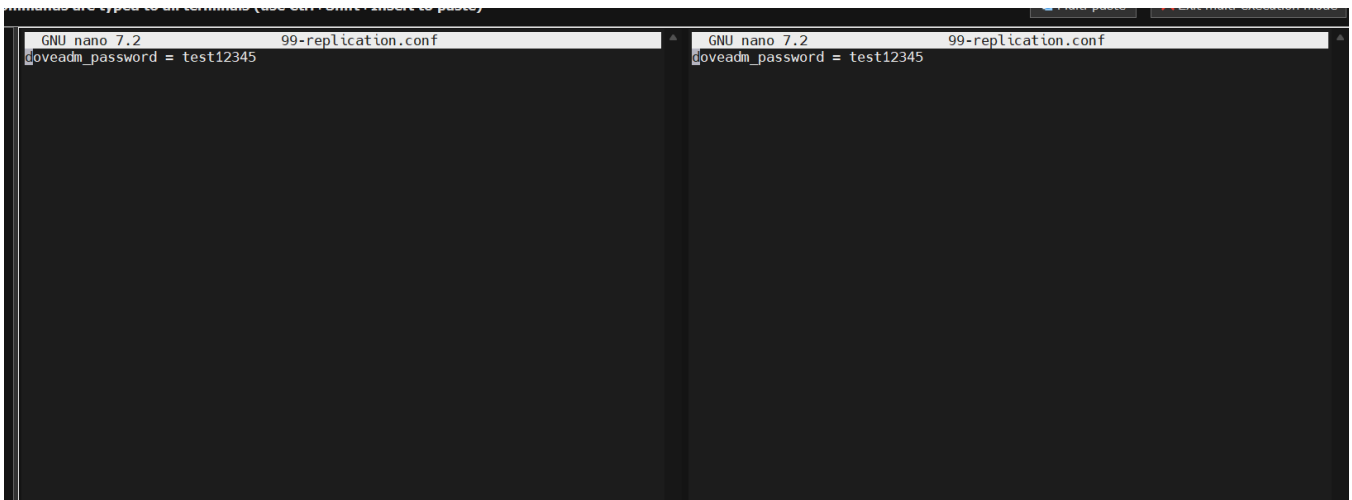


Figure 32 — Correction intermédiaire de la configuration de réplication.

```

root@DOVECOT-01:/etc/dovecot/conf.d# nano 99-replication.conf
root@DOVECOT-01:/etc/dovecot/conf.d# servie dovecot restart
-bash: servie: command not found
root@DOVECOT-01:/etc/dovecot/conf.d# service dovecot restart
root@DOVECOT-01:/etc/dovecot/conf.d# dovecadm sync -f -u asadek tcp:172.30.0.5
:12345
doveadm(asadek)<4463><Y075AuLLfWpvEQAA4Jfatg>: Panic: file mbox-lock.c: line
796 (mbox_lock): assertion failed: (lock_type == F_RDLCK || mbox->mbox_lock_t
ype != F_RDLCK)
doveadm(asadek)<4463><Y075AuLLfWpvEQAA4Jfatg>: Error: Raw backtrace: #0 t_ask
pass[0x71d88c6aac10] -> #1 backtrace_append[0x71d88c6aae80] -> #2 backtrace_g
et[0x71d88c6ab010] -> #3 execvp_const[0x71d88c6b6200] -> #4 default_fatal_han
dler[0x71d88c6b62d0] -> #5 i_panic[0x71d88c60c0d4] -> #6 [unw_get_proc_name()
failed: -10] -> #7 mbox_save_begin[0x71d88c820570] -> #8 mailbox_save_begin[
0x71d88c7ecb30] -> #9 mail_storage_copy[0x71d88c7e09d0] -> #10 mailbox_save_b
egin[0x71d88c7ecc70] -> #11 mailbox_move[0x71d88c7ecf20] -> #12 dsync_mailbox
_node_name_cmp[0x58c477257fe0] -> #13 dsync_mailbox_export_next_mail[0x58c477
2615b0] -> #14 dsync_mailbox_import_changes_finish[0x58c477261bb0] -> #15 dsy
nc_brain_sync_mails[0x58c477255780] -> #16 dsync_brain_sync_mails[0x58c477256
110] -> #17 dsync_brain_run[0x58c477256960] -> #18 compression_get_default_le
vel_zstd[0x58c4772633a0] -> #19 io_loop_call_io[0x71d88c6cdee0] -> #20 io_loo
p_handler_run_internal[0x71d88c6cfbe0] -> #21 io_loop_handler_run[0x71d88c6cf
d70] -> #22 io_loop_run[0x71d88c6cff40] -> #23 who_lookup[0x58c47723bbe0] ->
#24 who_lookup[0x58c47723cb20] -> #25 dovecadm_cmd_ver2_to_mail_cmd_wrapper[0x
58c47723dcc0] -> #26 dovecadm_cmd_run_ver2[0x58c477248120] -> #27 dovecadm_cmd_
try_run_ver2[0x58c477248660] -> #28 main[0x58c477229f20] -> #29 __libc_init_f
irst[0x71d88c2c31d0] -> #30 __libc_start_main[0x71d88c2c3280] -> #31 _start[0
x58c47722a390]
Aborted
root@DOVECOT-01:/etc/dovecot/conf.d#

```

Figure 33 — Panic mbox-lock.c pendant dsync : le stockage mbox n'est pas adapté à la réplication mise en place.

<pre> # # %u - username # %n - user part in user@domain, same as %u if there's no domain # %d - domain part in user@domain, empty if there's no domain # %h - home directory # # See doc/wiki/Variables.txt for full list. Some examples: # # mail_location = maildir:~/Maildir # mail_location = mbox:~/mail:INBOX=/var/mail/%u # mail_location = mbox:/var/mail/%d/%n/INDEX=/var/indexes/%d/%n/%n # # <doc/wiki/MailLocation.txt> # #mail_location = mbox:~/mail:INBOX=/var/mail/%u mail_location = maildir:~/Maildir # # If you need to set multiple mailbox locations or want to change default # namespace settings, you can do it by defining namespace sections. # # You can have private, shared and public namespaces. Private namespaces # are for user's personal mails. Shared namespaces are for accessing other # users' mailboxes that have been shared. Public namespaces are for shared # mailboxes that are managed by sysadmin. If you create any shared or public # namespaces you'll typically want to enable ACL plugin also, otherwise all # users can access all the shared mailboxes, assuming they have permissions # on filesystem level to do so. namespace inbox { # Namespace type: private, shared or public </pre>	<pre> # # %u - username # %n - user part in user@domain, same as %u if there's no domain # %d - domain part in user@domain, empty if there's no domain # %h - home directory # # See doc/wiki/Variables.txt for full list. Some examples: # # mail_location = maildir:~/Maildir # mail_location = mbox:~/mail:INBOX=/var/mail/%u # mail_location = mbox:/var/mail/%d/%n/INDEX=/var/indexes/%d/%n/%n # # <doc/wiki/MailLocation.txt> # #mail_location = mbox:~/mail:INBOX=/var/mail/%u mail_location = maildir:~/Maildir # # If you need to set multiple mailbox locations or want to change default # namespace settings, you can do it by defining namespace sections. # # You can have private, shared and public namespaces. Private namespaces # are for user's personal mails. Shared namespaces are for accessing other # users' mailboxes that have been shared. Public namespaces are for shared # mailboxes that are managed by sysadmin. If you create any shared or public # namespaces you'll typically want to enable ACL plugin also, otherwise all # users can access all the shared mailboxes, assuming they have permissions # on filesystem level to do so. namespace inbox { # Namespace type: private, shared or public </pre>
--	--

Figure 34 — Configuration des deux Dovecot avec mail_location = maildir:~/Maildir.

```

root@DOVECOT-01:/etc/dovecot/conf.d# nano 10-mail.conf
root@DOVECOT-01:/etc/dovecot/conf.d# service dovecot restart
root@DOVECOT-01:/etc/dovecot/conf.d# doveconf -n | grep mail_location
doveadm user asadek
ls -lh /var/mail/asadek
mail_location = maildir:~/Maildir
field      value
uid        1000
gid        1000
home       /home/asadek
mail       maildir:~/Maildir
system_groups_user      asadek
-rw----- 1 asadek mail 1.8K Aug 13 02:24 /var/mail/asadek
root@DOVECOT-01:/etc/dovecot/conf.d#

```

Figure 35 — Vérification : doveadm user asadek retourne désormais maildir:~/Maildir.

```

root@DOVECOT-01:/etc/dovecot/conf.d# doveadm sync -f -u asadek tcp:172.30.0.5:12345
root@DOVECOT-01:/etc/dovecot/conf.d#

```

Figure 36 — Première commande dsync après passage en Maildir.

8.4 Configuration automatique notify + replication

Une commande doveadm sync manuelle ne suffit pas. Je veux que chaque modification de boîte déclenche automatiquement une réplication. J'active donc les plugins notify et replication, le service replicator, les sockets de notification et mail_replica.

```

INBOX messages=0
root@DOVECOT-01:/etc/dovecot/conf.d# doveadm sync -f -u asadek tcp:172.30.0.5:12345
doveadm(asadek)<4508><LfRdJ6/NfWqcEQAA4Jfatg>: Warning: Mailbox changes cause d a desync. You may want to run dsync again: Remote lost mailbox GUID 90559a2ca1cd7d6a7a020000696fb918 (maybe it was just deleted?)
root@DOVECOT-01:/etc/dovecot/conf.d#
root@DOVECOT-01:/etc/dovecot/conf.d# doveadm sync -f -u asadek tcp:172.30.0.5:12345
root@DOVECOT-01:/etc/dovecot/conf.d# doveadm sync -f -u asadek tcp:172.30.0.5:12345
root@DOVECOT-01:/etc/dovecot/conf.d#
root@DOVECOT-01:/etc/dovecot/conf.d#

INBOX messages=0
root@DOVECOT-02:/etc/dovecot/conf.d#
root@DOVECOT-02:/etc/dovecot/conf.d# systemctl stop dovecot
rm -rf /home/asadek/Maildir
systemctl start dovecot
root@DOVECOT-02:/etc/dovecot/conf.d# systemctl start dovecot
root@DOVECOT-02:/etc/dovecot/conf.d# systemctl start dovecot
root@DOVECOT-02:/etc/dovecot/conf.d# ls -la /home/asadek/Maildir
total 36
drwx----- 5 asadek asadek 4096 Aug 13 14:00 .
drwx----- 4 asadek asadek 4096 Aug 13 14:00 ..
drwx----- 2 asadek asadek 4096 Aug 13 14:00 cur
-rw----- 1 asadek asadek 51 Aug 13 14:00 dovecot-uidlist
-rw----- 1 asadek asadek 8 Aug 13 14:00 dovecot-uidvalidity
-r--r--r-- 1 asadek asadek 0 Aug 13 14:00 dovecot-uidvalidity.6a7dcd6b
-rw----- 1 asadek asadek 416 Aug 13 14:00 dovecot.index.log
-rw----- 1 asadek asadek 696 Aug 13 14:00 dovecot.list.index.log
-rw----- 1 asadek asadek 0 Aug 13 14:00 maildirfolder
drwx----- 2 asadek asadek 4096 Aug 13 14:00 new
drwx----- 2 asadek asadek 4096 Aug 13 14:00 tmp
root@DOVECOT-02:/etc/dovecot/conf.d#

```

Figure 37 — Création et initialisation du Maildir sur les deux nœuds.

```

GNU nano 7.2 /etc/dovecot/conf.d/99-replication.conf *
doveadm_password = test12345
mail_plugins = $mail_plugins notify replication
replication_max_conns = 10
plugin {
  mail_replica = tcp:172.30.0.5:12345
  replication_sync_timeout = 2
}
service replicator {
  process_min_avail = 1

  unix_listener replicator-doveadm {
    mode = 0660
  }
}
service aggregator {
  fifo_listener replication-notify-fifo {
    mode = 0666
  }
  unix_listener replication-notify {
}
}
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
☐ Exclude "dovecot-01" from MultiExec mode

```

Figure 38 — 99-replication.conf : plugins notify/replication et service replicator.

```

GNU nano 7.2 /etc/dovecot/conf.d/99-replication.conf *
}
service aggregator {
  fifo_listener replication-notify-fifo {
    mode = 0666
  }
  unix_listener replication-notify {
    mode = 0666
  }
}
service doveadm {
  user = root

  inet_listener {
    address = 172.30.0.4
    port = 12345
  }
}
}
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify
☐ Exclude "dovecot-01" from MultiExec mode

```

Figure 39 — 99-replication.conf : aggregator et listener doveadm sur l'adresse propre à chaque nœud.

```

# Exemple DOVECOT-01
doveadm_password = test12345
mail_plugins = $mail_plugins notify replication
replication_max_conns = 10

plugin {
  mail_replica = tcp:172.30.0.5:12345
}

service replicator {
  process_min_avail = 1
  vsz_limit = 2G
  unix_listener replicator-doveadm {
    mode = 0666
  }
}

service aggregator {
  fifo_listener replication-notify-fifo {
    mode = 0666
  }
  unix_listener replication-notify {
    mode = 0666
  }
}

service doveadm {
  user = root
  inet_listener {
    address = 172.30.0.4
    port = 12345
  }
}

```

Configuration de référence DOVECOT-01. Sur DOVECOT-02, la cible mail_replica devient 172.30.0.4 et le listener local 172.30.0.5.

8.5 Nettoyage des anciennes directives

Je retire le bloc doveadm ajouté précédemment dans 10-master.conf afin de ne pas définir le même service à plusieurs endroits. Je retire aussi doveadm_port = 12345. Le port est déjà explicitement indiqué dans mail_replica = tcp:IP:12345. Cette correction est importante avec mon passdb PAM : doveadm_port global déclenchait une recherche de credentials que PAM ne fournit pas dans ce contexte.

```

commands are typed to all terminals (use Ctrl+Shift+Insert to paste)
Multi-paste Exit multi-execution mode

root@DOVECOT-02:~# nano /etc/dovecot/conf.d/99-replication.conf
root@DOVECOT-02:~# nano /etc/dovecot/conf.d/10-
10-auth.conf      10-mail.conf      10-tcpwrapper.conf
10-director.conf  10-master.conf
10-logging.conf   10-ssl.conf
root@DOVECOT-02:~# nano /etc/dovecot/conf.d/10-master.conf
root@DOVECOT-02:~# doveconf -n >/dev/null && echo "CONFIG OK"
CONFIG OK
root@DOVECOT-02:~#

root@DOVECOT-01:~# nano /etc/dovecot/conf.d/99-replication.conf
root@DOVECOT-01:~# nano /etc/dovecot/conf.d/10-
10-auth.conf      10-mail.conf      10-tcpwrapper.conf
10-director.conf  10-master.conf
10-logging.conf   10-ssl.conf
root@DOVECOT-01:~# nano /etc/dovecot/conf.d/10-master.conf
root@DOVECOT-01:~# doveconf -n >/dev/null && echo "CONFIG OK"
CONFIG OK
root@DOVECOT-01:~#

☐ Exclude "dovecot-01" from MultiExec mode
☐ Exclude "dovecot-02" from MultiExec mode

```

Figure 40 — Vérification/centralisation de la configuration avant redémarrage des deux Dovecot.

9. Journal de dépannage : erreurs, causes et corrections

Cette partie est volontairement détaillée. Elle montre le raisonnement suivi pendant le montage et les causes réelles des erreurs. Dans un projet HA, les erreurs les plus intéressantes sont souvent celles qui apparaissent uniquement quand plusieurs services commencent à interagir.

Symptôme	Cause identifiée	Correction
Postfix: missing = after attribute name	Ligne mal formée / continuation sans indentation	Retaper la directive et indenter les lignes suivantes
DNS Host not found: adek.ovh	Faute de frappe dans le destinataire	Tester avec asadek@sadek.ovh
LMTP 550 User doesn't exist	Dovecot ne trouve pas le compte local	Créer le compte et utiliser %n pour retirer le domaine
Unsupported authentication mechanism	Roundcube tente LOGIN non annoncé	auth_mechanisms = plain login
Plaintext authentication disabled	LOGIN tenté avant chiffrement	Utiliser STARTTLS sur IMAP 143
CN localhost != 172.30.0.1	Certificat de lab non conforme au nom utilisé	Bypass temporaire puis certificat valide en production
Configured passdbs don't support credentials lookups	doveadm_port global avec passdb PAM	Supprimer doveadm_port et mettre :12345 dans mail_replica
Panic mbox-lock.c	Stockage mbox pendant dsync	Passer les deux nœuds en Maildir
Section not allowed here	Accolade manquante dans plugin {}	Fermer le bloc avant service replicator
bind(...): Cannot assign requested address	Un nœud écoute sur l'IP de l'autre	Listener = IP locale, mail_replica = IP distante
Réplication de nobody/systemd-*	userdb énumère les comptes système	Définir first_valid_uid/gid et redémarrer Dovecot
replicator crash / timeout	replication_sync_timeout instable dans cette config	Retirer replication_sync_timeout et garder l'asynchrone
Permission denied replicator-doveadm	Socket 0600 incompatible avec plusieurs UID utilisateurs	Passer à 0666 pour le lab
Connection refused pendant panne du pair	Le serveur distant est réellement arrêté	Comportement attendu : stocker localement puis rattraper au retour

9.1 Erreurs de configuration Dovecot et adresses de listener

```

2026-08-13T23:02:36.473578+00:00 DOVECOT-01 dovecot: master: Dovecot v2.3.19.
1 (9b53102964) starting up for imap, lmtp (core dumps disabled)
2026-08-13T23:02:36.659108+00:00 DOVECOT-01 dovecot: doveadm(nobody)<4788><0x
efJQxNfmq0EgAA4Jfatg>: Error: mkdir(/nonexistent/Maildir) failed: Permission
denied (euid=65534(nobody) egid=65534(nogroup))
2026-08-13T23:02:36.659193+00:00 DOVECOT-01 dovecot: doveadm(nobody)<4788><0x
efJQxNfmq0EgAA4Jfatg>: Error: mkdir(/nonexistent/Maildir) failed: Permission
denied (euid=65534(nobody) egid=65534(nogroup))
2026-08-13T23:02:36.702630+00:00 DOVECOT-01 dovecot: doveadm(systemd-timesync
)<4791><vcU7KAXNfmq3EgAA4Jfatg>: Error: mkdir(/Maildir) failed: Permission d
enied (euid=997(systemd-timesync) egid=997(systemd-timesync) missing +w perm:
/, dir owned by 0:0 mode=0755)
2026-08-13T23:02:36.702958+00:00 DOVECOT-01 dovecot: doveadm(systemd-timesync
)<4791><vcU7KAXNfmq3EgAA4Jfatg>: Error: Couldn't lock //.dovecot-sync.lock: s
afe_mkstemp(/.dovecot-sync.lock) failed: Permission denied
2026-08-13T23:02:36.712808+00:00 DOVECOT-01 dovecot: doveadm(systemd-network)
<4792><3srPKAXNfmq4EgAA4Jfatg>: Error: mkdir(/Maildir) failed: Permission de
nied (euid=998(systemd-network) egid=998(systemd-network) missing +w perm: /,
dir owned by 0:0 mode=0755)
2026-08-13T23:02:36.713074+00:00 DOVECOT-01 dovecot: doveadm(systemd-network)
<4792><3srPKAXNfmq4EgAA4Jfatg>: Error: Couldn't lock //.dovecot-sync.lock: sa
fe_mkstemp(/.dovecot-sync.lock) failed: Permission denied
root@DOVECOT-01:~#

connect(172.30.0.4:12345) failed: Connection refused
2026-08-13T23:02:21.822701+00:00 DOVECOT-02 dovecot: doveadm(systemd-timesync
): Fatal: connect(172.30.0.4:12345) failed: Connection refused
2026-08-13T23:02:21.830258+00:00 DOVECOT-02 dovecot: doveadm(systemd-network)
: Fatal: connect(172.30.0.4:12345) failed: Connection refused
2026-08-13T23:02:36.655177+00:00 DOVECOT-02 dovecot: doveadm(nobody)<990><jNr
BJgxNfmreAwAAwH5GA>: Error: mkdir(/nonexistent/Maildir) failed: Permission d
enied (euid=65534(nobody) egid=65534(nogroup))
2026-08-13T23:02:36.703008+00:00 DOVECOT-02 dovecot: doveadm(systemd-timesync
)<993><vhC5K0xNfmrhAwAAwH5GA>: Error: mkdir(/Maildir) failed: Permission de
nied (euid=997(systemd-timesync) egid=997(systemd-timesync) missing +w perm:
/, dir owned by 0:0 mode=0755)
2026-08-13T23:02:36.713197+00:00 DOVECOT-02 dovecot: doveadm(systemd-network)
<994><VpXKqpxNfmriAwAAwH5GA>: Error: mkdir(/Maildir) failed: Permission den
ied (euid=998(systemd-network) egid=998(systemd-network) missing +w perm: /,
dir owned by 0:0 mode=0755)
2026-08-13T23:02:36.740627+00:00 DOVECOT-02 dovecot: doveadm(contact)<991><17
CVJwXNfmrfAwAAwH5GA>: Error: net_connect_unix(/run/dovecot/replicator-doveadm
m) failed: Permission denied
2026-08-13T23:02:36.768102+00:00 DOVECOT-02 dovecot: doveadm(asadek)<992><0k2
VKAXNfmrgAwAAwH5GA>: Error: net_connect_unix(/run/dovecot/replicator-doveadm
) failed: Permission denied
root@DOVECOT-02:~#

```

Figure 41 — Erreur de configuration/bind lors de la mise en place du listener de réplication.

Un listener doit être attaché à une adresse réellement présente sur le serveur. DOVECOT-01 écoute sur 172.30.0.4:12345 et réplique vers 172.30.0.5:12345 ; DOVECOT-02 fait exactement l'inverse.

9.2 Filtrer les comptes système

```

GNU nano 7.2 /etc/dovecot/conf.d/10-mail.conf *
# Directory where mails can be temporarily stored. Usually it's used only for
# mails larger than >= 128 kB. It's used by various parts of Dovecot, for
# example LDA/LMTP while delivering large mails or zlib plugin for keeping
# uncompressed mails.
#mail_temp_dir = /tmp

# Valid UID range for users, defaults to 500 and above. This is mostly
# to make sure that users can't log in as daemons or other system users.
# Note that denying root logins is hardcoded to dovecot binary and can't
# be done even if first_valid_uid is set to 0.
#first_valid_uid = 500
#last_valid_uid = 0
first_valid_uid = 1000
last_valid_uid = 60000

first_valid_gid = 1000
last_valid_gid = 60000
# Valid GID range for users, defaults to non-root/wheel. Users having
# non-valid GID as primary group ID aren't allowed to log in. If user

GNU nano 7.2 /etc/dovecot/conf.d/10-mail.conf *
# Directory where mails can be temporarily stored. Usually it's used only for
# mails larger than >= 128 kB. It's used by various parts of Dovecot, for
# example LDA/LMTP while delivering large mails or zlib plugin for keeping
# uncompressed mails.
#mail_temp_dir = /tmp

# Valid UID range for users, defaults to 500 and above. This is mostly
# to make sure that users can't log in as daemons or other system users.
# Note that denying root logins is hardcoded to dovecot binary and can't
# be done even if first_valid_uid is set to 0.
#first_valid_uid = 500
#last_valid_uid = 0
first_valid_uid = 1000
last_valid_uid = 60000

first_valid_gid = 1000
last_valid_gid = 60000
# Valid GID range for users, defaults to non-root/wheel. Users having
# non-valid GID as primary group ID aren't allowed to log in. If user

```

Figure 42 — Les comptes système apparaissent dans les tentatives de réplication et génèrent des erreurs de permissions/UID.

```

root@DOVECOT-01:~# service dovecot restart
root@DOVECOT-01:~# doveadm user '*'
asadek
contact
root@DOVECOT-01:~#

```

Figure 43 — Première vérification de la liste doveadm user après correction.

```

root@DOVECOT-01:~# doveadm user '*'
asadek
contact
root@DOVECOT-01:~# [200~doveadm replicator status~^C
root@DOVECOT-01:~# doveadm replicator status
Queued 'sync' requests 0
Queued 'high' requests 0
Queued 'low' requests 0
Queued 'failed' requests 0
Queued 'full resync' requests 0
Waiting 'failed' requests 3
Total number of known users 5
root@DOVECOT-01:~# doveadm replicator status '*'
username priority fast sync full sync success sync failed
nobody none 00:01:51 00:06:51 - y
systemd-timesync none 00:01:51 00:06:51 - y
contact none 00:06:51 00:06:51 00:06:51 -
systemd-network none 00:01:51 00:06:51 - y
asadek none 00:06:51 00:06:51 00:06:51 -
root@DOVECOT-01:~# doveadm replicator remove nobody
doveadm replicator remove systemd-network
doveadm replicator remove systemd-timesync
root@DOVECOT-01:~#

2026-08-13T23:02:36.768102+00:00 DOVECOT-02 dovecot: doveadm(asadek)<992><0k2
VKAXNfmrgAwAAwH5GA>: Error: net_connect_unix(/run/dovecot/replicator-doveadm
) failed: Permission denied
root@DOVECOT-02:~# /etc/dovecot/conf.d/10-mail.conf
-bash: /etc/dovecot/conf.d/10-mail.conf: Permission denied
root@DOVECOT-02:~# nano /etc/dovecot/conf.d/10-mail.conf
root@DOVECOT-02:~#
root@DOVECOT-02:~# service dovecot restart
root@DOVECOT-02:~# nano /etc/dovecot/conf.d/10-mail.conf
root@DOVECOT-02:~# doveadm replicator status^C
root@DOVECOT-02:~# doveadm replicator status
Queued 'sync' requests 0
Queued 'high' requests 0
Queued 'low' requests 0
Queued 'failed' requests 0
Queued 'full resync' requests 0
Waiting 'failed' requests 3
Total number of known users 5
root@DOVECOT-02:~#
root@DOVECOT-02:~# doveadm replicator remove nobody
doveadm replicator remove systemd-network
doveadm replicator remove systemd-timesync
root@DOVECOT-02:~#

```

Figure 44 — État du replicator avant nettoyage des anciens comptes mémorisés.

Figure 45 — Ajout explicite des comptes mail asadek et contact dans le replicator.

Figure 46 — Le replicator ne conserve plus que les deux comptes mail et leurs synchronisations réussissent.

Le point important est le redémarrage après modification de `first_valid_uid` / `first_valid_gid`. Sans restart, `doveadm user '*'` continuait à afficher les comptes système. Après restart, seuls `asadek` et `contact` restent éligibles.

9.3 Crash replicator et timeout synchrone

Figure 47 — Traces d'échec de réplication : comptes système, socket et crash du replicator.

```

GNU nano 7.2 /etc/dovecot/conf.d/99-replication.conf
doveadm_password = test12345
mail_plugins = $mail_plugins notify replication
replication_max_conns = 10
plugin {
  mail_replica = tcp:172.30.0.5:12345
  replication_sync_timeout = 2
}
service replicator {
  process_min_avail = 1
  vsz_limit = 2G
  unix_listener replicator-doveadm {
    mode = 0600
  }
}

GNU nano 7.2 /etc/dovecot/conf.d/99-replication.conf
doveadm_password = test12345
mail_plugins = $mail_plugins notify replication
replication_max_conns = 10
plugin {
  mail_replica = tcp:172.30.0.4:12345
  replication_sync_timeout = 2
}
service replicator {
  process_min_avail = 1
  unix_listener replicator-doveadm {
    mode = 0600
  }
}
vsz_limit = 2G
service aggregator {
  fifo_listener replication-notify-fifo {
    mode = 0666
  }
  unix_listener replication-notify {
    mode = 0666
  }
}
  
```

Figure 48 — Configuration recommandée : vsz_limit du replicator augmenté et timeout encore visible pendant le diagnostic.

Je supprime ensuite replication_sync_timeout = 2. La réplication reste automatique, mais elle redevient pleinement asynchrone : LMTP n'attend plus deux secondes le résultat de la réplication distante avant de rendre la main.

```

2026-08-13T23:17:37.059846+00:00 DOVECOT-01 dovecot: doveadm(asadek)<4920><3q+pApFQfmo4EwAA4Jfatg>: Error: net_connect_unix(/run/dovecot/replicator-doveadm) failed: Connection reset by peer
  
```

Figure 49 — Connection reset by peer sur le socket replicator-doveadm pendant la phase de crash.

```

GNU nano 7.2 /etc/dovecot/conf.d/99-replication.conf *
doveadm_password = test12345
mail_plugins = $mail_plugins notify replication
replication_max_conns = 10
plugin {
  mail_replica = tcp:172.30.0.5:12345
}
service replicator {
  process_min_avail = 1
  vsz_limit = 2G
  unix_listener replicator-doveadm {
    mode = 0600
  }
}
service aggregator {
  fifo_listener replication-notify-fifo {
    mode = 0666
  }
}

GNU nano 7.2 /etc/dovecot/conf.d/99-replication.conf *
doveadm_password = test12345
mail_plugins = $mail_plugins notify replication
replication_max_conns = 10
plugin {
  mail_replica = tcp:172.30.0.4:12345
}
service replicator {
  process_min_avail = 1
  vsz_limit = 2G
  unix_listener replicator-doveadm {
    mode = 0600
  }
}
service aggregator {
  fifo_listener replication-notify-fifo {
    mode = 0666
  }
}
  
```

Figure 50 — Configuration après suppression du timeout ; le service replicator conserve vsz_limit = 2G.

9.4 Permissions du socket replicator-doveadm

```

2026-08-13T23:16:43.480617+00:00 DOVECOT-01 dovecot: doveadm(systemd-timesync
): Fatal: connect(172.30.0.5:12345) failed: Connection refused
2026-08-13T23:16:43.493638+00:00 DOVECOT-01 dovecot: doveadm(nobody): Fatal:
connect(172.30.0.5:12345) failed: Connection refused
2026-08-13T23:16:43.501286+00:00 DOVECOT-01 dovecot: doveadm(systemd-network)
: Fatal: connect(172.30.0.5:12345) failed: Connection refused
2026-08-13T23:17:37.059846+00:00 DOVECOT-01 dovecot: doveadm(asadek)<4920><3q
+ApF0fm04EwAA4Jfatg>: Error: net_connect_unix(/run/dovecot/replicator-doveadm)
Failed: Connection reset by peer
2026-08-13T23:20:00.618945+00:00 DOVECOT-01 dovecot: master: Warning: Killed
with signal 15 (by pid=4933 uid=0 code=kill)
2026-08-13T23:20:01.719329+00:00 DOVECOT-01 dovecot: master: Warning: Dovecot v2.3.19.
1 (9b53102964) starting up for 'imap, lmtmp (core dumps disabled)'

2026-08-13T23:20:17.192750+00:00 DOVECOT-01 dovecot: lmtmp(4947): Connect from
172.30.0.2
2026-08-13T23:20:17.203671+00:00 DOVECOT-01 dovecot: lmtmp(asadek)<4947><eTB1C
zFRfmpTEwAA4Jfatg>: msgid=<20260813232016.2173779@smtp.agrepe.com>; saved mai
l to INBOX
2026-08-13T23:20:17.206196+00:00 DOVECOT-01 dovecot: lmtmp(4947): Disconnect f
rom 172.30.0.2: Logged out (state=READY)

[ ] Exclude "dovecot-01" from MultiExec mode

<- 250 CHUNKING
-> MAIL FROM:<root@smtp.agrepe.com>
<- 250 2.1.0 Ok
-> RCPT TO:<asadek@sadek.ovh>
<- 250 2.1.5 Ok
-> DATA
<- 354 End data with <CR><LF>.<CR><LF>
-> Date: Thu, 13 Aug 2026 23:20:16 +0000
-> To: asadek@sadek.ovh
-> From: root@smtp.agrepe.com
-> Subject: test Thu, 13 Aug 2026 23:20:16 +0000
-> Message-Id: <20260813232016.2173779@smtp.agrepe.com>
-> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
->
-> This is a test mailing
->
->
<- 250 2.0.0 Ok: queued as F1C99560E
-> QUIT
<- 221 2.0.0 Bye
=== Connection closed with remote host.
root@smtp:~#

[ ] Exclude "smtp.agrepe.com (root)" from MultiExec mode

```

```

172.30.0.3
2026-08-13T23:18:01.555572+00:00 DOVECOT-02 dovecot: lmtmp(asadek)<1100><wSwbG
pB0fmpMBAAAaW+5GA>: Warning: replication(asadek): Sync failure: Timeout in 2
secs
2026-08-13T23:18:02.545421+00:00 DOVECOT-02 dovecot: lmtmp(asadek)<1100><wSwbG
pB0fmpMBAAAaW+5GA>: msgid=<20260813231735.2172295@smtp.agrepe.com>; saved mai
l to INBOX
2026-08-13T23:18:02.574043+00:00 DOVECOT-02 dovecot: replicator: Fatal: maste
r: service(replicator): child 1090 killed with signal 9
2026-08-13T23:18:02.574085+00:00 DOVECOT-02 dovecot: lmtmp(1100): Disconnect f
rom 172.30.0.3: Logged out (state=READY)
2026-08-13T23:18:03.112321+00:00 DOVECOT-02 dovecot: master: Warning: Killed
with signal 15 (by pid=1104 uid=0 code=kill)
2026-08-13T23:18:06.149190+00:00 DOVECOT-02 dovecot: log(1092): Warning: Kill
ed with signal 15 (by pid=1 uid=0 code=kill)
2026-08-13T23:20:01.664822+00:00 DOVECOT-02 dovecot: master: Dovecot v2.3.19.
1 (9b53102964) starting up for 'imap, lmtmp (core dumps disabled)'

2026-08-13T23:20:17.440140+00:00 DOVECOT-02 dovecot: doveadm(asadek)<1131><o8
DbEjFRfmpRBAaAaW+5GA>: Error: net_connect_unix(/run/dovecot/replicator-doveadm)
Failed: Permission denied

[ ] Exclude "dovecot-02" from MultiExec mode

```

Figure 51 — Nouvelle erreur : Permission denied sur /run/dovecot/replicator-doveadm.

Mes utilisateurs mail sont de vrais comptes Linux distincts. Un socket en 0600 ne permet pas à ces UID différents de contacter le replicator. Pour le laboratoire, je passe donc le socket à 0666. Cette correction débloquent immédiatement la réplication.

```

GNU nano 7.2 /etc/dovecot/conf.d/99-replication.conf
doveadm_password = test12345

mail_plugins = $mail_plugins notify replication

replication_max_conns = 10

plugin {
  mail_replica = tcp:172.30.0.5:12345
}

service replicator {
  process_min_avail = 1
  vsz_limit = 26
  unix_listener replicator-doveadm {
    mode = 0666
  }
}

service aggregator {
  fifo_listener replication-notify-fifo {
    mode = 0666
  }
  unix_listener replication-notify {
    mode = 0666
  }
}

[ ] Exclude "smtp.agrepe.com (root)" from MultiExec mode

```

```

GNU nano 7.2 /etc/dovecot/conf.d/99-replication.conf
doveadm_password = test12345
mail_plugins = $mail_plugins notify replication
replication_max_conns = 10
plugin {
  mail_replica = tcp:172.30.0.4:12345
}
service replicator {
  process_min_avail = 1
  vsz_limit = 26
  unix_listener replicator-doveadm {
    mode = 0666
  }
}
service aggregator {
  fifo_listener replication-notify-fifo {
    mode = 0666
  }
  unix_listener replication-notify {
    mode = 0666
  }
}

[ ] Exclude "smtp.agrepe.com (root)" from MultiExec mode

```

Figure 52 — Passage du socket replicator-doveadm de mode 0600 à 0666 sur les deux nœuds.

Durcissement futur — 0666 est volontairement permissif. Dans une architecture de production, je préférerais un UID/GID vmail commun et un socket 0660 limité à un groupe dédié.

9.5 Test après correction

```

file, uid from userdb lookup).
2026-08-13T23:21:43.537429+00:00 DOVECOT-01 dovecot: doveadm(systemd-timesync
): Error: Failed to start remote dsync-server command: Remote exit_code=75 TE
MPFAIL
2026-08-13T23:23:03.027764+00:00 DOVECOT-01 dovecot: doveadm(asadek)<4961><KS
d0AddRfmpHwAA4Jfatg>: Error: net_connect_unix(/run/dovecot/replicator-dovead
m) failed: Connection reset by peer
2026-08-13T23:24:10.520724+00:00 DOVECOT-01 dovecot: master: Warning: Killed
with signal 15 (by pid=4968 uid=0 code=kill)
2026-08-13T23:24:11.021275+00:00 DOVECOT-01 dovecot: master: Dovecot v2.3.19.
1 (9b53102964) starting up for imap, lmtmp (core dumps disabled)

2026-08-13T23:25:47.571657+00:00 DOVECOT-01 dovecot: lmtmp(4988): Connect from
172.30.0.2
2026-08-13T23:25:47.582153+00:00 DOVECOT-01 dovecot: lmtmp(asadek)<4988><<L8NI
ntSfmp8fWAA4Jfatg>: msgid=<20260813232546.2176563@smtp.agrepe.com>: saved mai
l to INBOX
2026-08-13T23:25:47.584313+00:00 DOVECOT-01 dovecot: lmtmp(4988): Disconnect f
rom 172.30.0.2: Logged out (state=READY)

[ ] Exclude "dovecot-01" from MultiExec mode
<- 250 CHUNKING
-> MAIL FROM:<root@smtp.agrepe.com>
<- 250 2.1.0 OK
-> RCPT TO:<asadek@sadek.ovh>
<- 250 2.1.5 OK
-> DATA
<- 354 End data with <CR><LF>.<CR><LF>
-> Date: Thu, 13 Aug 2026 23:25:50 +0000
-> To: asadek@sadek.ovh
-> From: root@smtp.agrepe.com
-> Subject: test Thu, 13 Aug 2026 23:25:50 +0000
-> Message-Id: <20260813232550.2176612@smtp.agrepe.com>
-> X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
->
-> This is a test mailing
->
->
<- 250 2.0.0 Ok: queued as BF7075936
-> QUIT
<- 221 2.0.0 Bye
=== Connection closed with remote host.
root@smtp:~#

[ ] Exclude "smtp.agrepe.com (root)" from MultiExec mode

```

```

2026-08-13T23:24:10.528563+00:00 DOVECOT-02 dovecot: master: Warning: Killed
with signal 15 (by pid=1152 uid=0 code=kill)
2026-08-13T23:24:56.093553+00:00 DOVECOT-02 dovecot: master: Dovecot v2.3.19.
1 (9b53102964) starting up for imap, lmtmp (core dumps disabled)

2026-08-13T23:25:40.394864+00:00 DOVECOT-02 dovecot: lmtmp(1180): Connect from
172.30.0.3
2026-08-13T23:25:40.394864+00:00 DOVECOT-02 dovecot: lmtmp(asadek)<1180><<8G7WF
nRSfmp8fWAA4Jfatg>: msgid=<20260813232539.2176515@smtp.agrepe.com>: saved mai
l to INBOX
2026-08-13T23:25:40.396814+00:00 DOVECOT-02 dovecot: lmtmp(1180): Disconnect f
rom 172.30.0.3: Logged out (state=READY)
2026-08-13T23:25:50.967361+00:00 DOVECOT-02 dovecot: lmtmp(1180): Connect from
172.30.0.3
2026-08-13T23:25:50.978014+00:00 DOVECOT-02 dovecot: lmtmp(asadek)<1180><<P+h0
XSSfmp8fWAA4Jfatg>: msgid=<20260813232550.2176612@smtp.agrepe.com>: saved mai
l to INBOX
2026-08-13T23:25:50.982041+00:00 DOVECOT-02 dovecot: lmtmp(1180): Disconnect f
rom 172.30.0.3: Logged out (state=READY)

[ ] Exclude "dovecot-02" from MultiExec mode

```

Figure 53 — Après correction des permissions, les livraisons et répliquions passent sans blocage.

À ce moment, je retourne sur le webmail : les messages sont de nouveau lisibles et les deux Dovecot convergent.

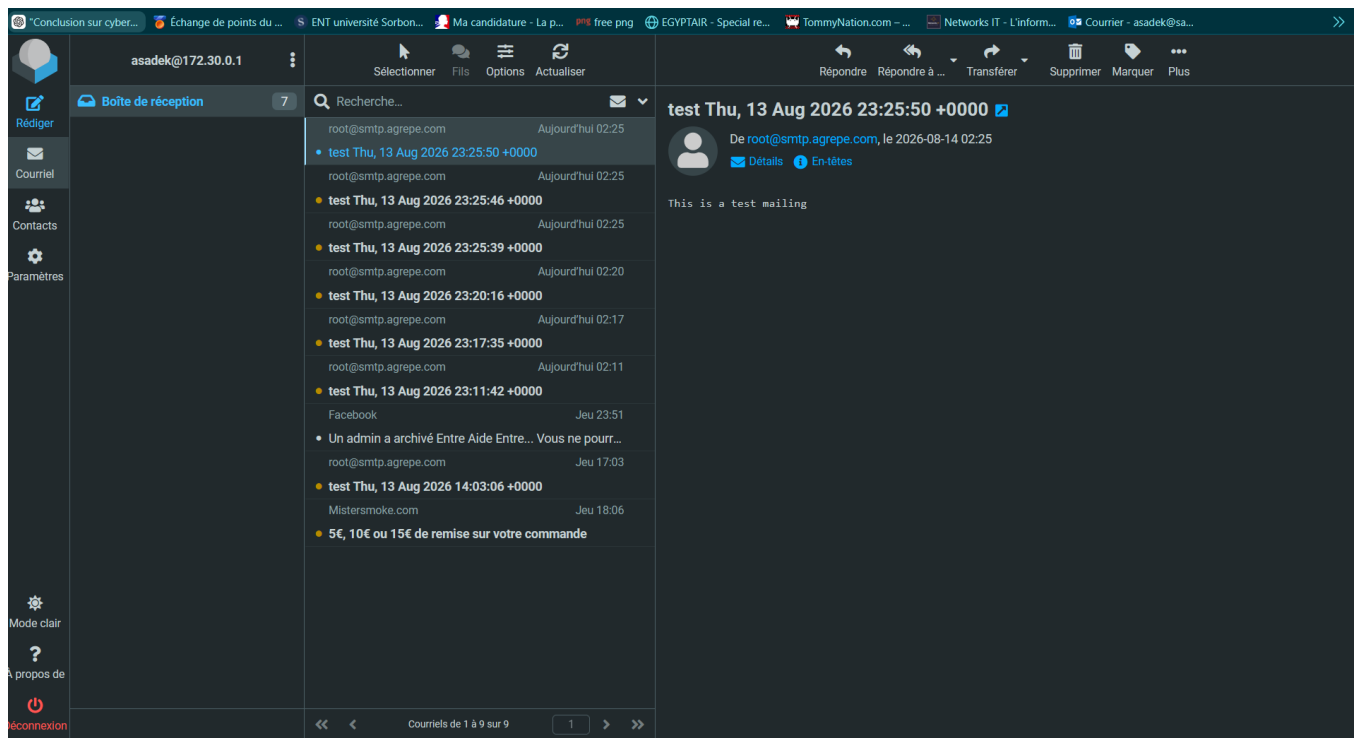


Figure 54 — Roundcube affiche correctement les messages après stabilisation de la répliquion.

Scénario de panne validé

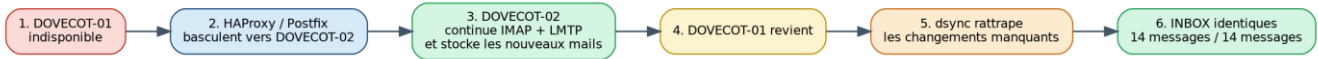


Schéma 3 — Séquence de panne et de rattrapage validée en laboratoire.

Test de résilience validé — Le test démontre trois propriétés : continuité IMAP, continuité de livraison LMTP et convergence des boîtes après le retour du nœud. C'est la preuve la plus importante du projet.

11. Configurations finales de référence

Les extraits ci-dessous synthétisent la configuration qui a permis d'obtenir le fonctionnement observé dans les captures finales. Ils ne remplacent pas les fichiers complets de Debian, mais ils regroupent les paramètres structurants du projet.

11.1 Postfix — SMTP-01

```
mydestination = $myhostname, localhost.$mydomain, localhost
virtual_mailbox_domains = sadek.ovh, sadek-it.fr, mielamour.ovh
virtual_transport = lmtp:[172.30.0.4]:24
lmtp_fallback_relay = [172.30.0.5]:24
inet_interfaces = all
inet_protocols = ipv4
```

11.2 Postfix — SMTP-02

```
mydestination = $myhostname, localhost.$mydomain, localhost
virtual_mailbox_domains = sadek.ovh, sadek-it.fr, mielamour.ovh
virtual_transport = lmtp:[172.30.0.5]:24
lmtp_fallback_relay = [172.30.0.4]:24
inet_interfaces = all
inet_protocols = ipv4
```

11.3 Dovecot — LMTP

```
protocols = imap lmtp

service lmtp {
    inet_listener lmtp {
        address = 172.30.0.X
        port = 24
    }
}

protocol lmtp {
    postmaster_address = postmaster@sadek.ovh
}

auth_username_format = %n
auth_mechanisms = plain login
disable_plaintext_auth = yes
```

11.4 Dovecot — stockage et filtre UID

```
mail_location = maildir:~/Maildir
first_valid_uid = 1000
last_valid_uid = 60000
first_valid_gid = 1000
last_valid_gid = 60000
```

11.5 Dovecot — réplication DOVECOT-01

```
doveadm_password = test12345
mail_plugins = $mail_plugins notify replication
replication_max_conns = 10

plugin {
    mail_replica = tcp:172.30.0.5:12345
}

service replicator {
    process_min_avail = 1
    vsz_limit = 2G
    unix_listener replicator-doveadm {
        mode = 0666
    }
}
```

```

}

service aggregator {
    fifo_listener replication-notify-fifo { mode = 0666 }
    unix_listener replication-notify { mode = 0666 }
}

service doveadm {
    user = root
    inet_listener {
        address = 172.30.0.4
        port = 12345
    }
}

```

11.6 Dovecot — réplication DOVECOT-02

```

doveadm_password = test12345
mail_plugins = $mail_plugins notify replication
replication_max_conns = 10

plugin {
    mail_replica = tcp:172.30.0.4:12345
}

service replicator {
    process_min_avail = 1
    vsz_limit = 2G
    unix_listener replicator-doveadm {
        mode = 0666
    }
}

service aggregator {
    fifo_listener replication-notify-fifo { mode = 0666 }
    unix_listener replication-notify { mode = 0666 }
}

service doveadm {
    user = root
    inet_listener {
        address = 172.30.0.5
        port = 12345
    }
}

```

11.7 HAProxy — IMAP

```

frontend IMAP-LOADBALANCER-01
    bind 172.30.0.1:143
    mode tcp
    default_backend CLUSTER-02

backend CLUSTER-02
    mode tcp
    balance roundrobin
    server num1 172.30.0.4:143 check
    server num2 172.30.0.5:143 check

```

11.8 Roundcube

```

$config['imap_host'] = 'tls://172.30.0.1:143';
$config['smtp_host'] = '172.30.0.1:25';
$config['smtp_user'] = '';
$config['smtp_pass'] = '';

$config['imap_conn_options'] = [
    'ssl' => [
        'verify_peer' => false,
        'verify_peer_name' => false,
        'allow_self_signed' => true,
    ],
];

```

```
];
```

11.9 Commandes de contrôle utiles

```
# Postfix
postfix check
postconf -n
tail -f /var/log/mail.log

# Dovecot
doveconf -n
doveadm user '*'
doveadm replicator status '*'
doveadm mailbox status -u asadek messages INBOX

# Réseau
telnet 172.30.0.4 24
nc -vz 172.30.0.5 12345
openssl s_client -connect 172.30.0.1:143 -starttls imap

# HAProxy
haproxy -c -f /etc/haproxy/haproxy.cfg
journalctl -u haproxy -f
```

12. Limites actuelles et durcissement recommandé

Le projet atteint son objectif de laboratoire, mais plusieurs choix ont été faits pour aller jusqu'au bout du fonctionnement et des tests de panne. Pour un service exposé durablement en production, je renforcerais les points suivants.

Point	État du laboratoire	Évolution recommandée
HAProxy	Un seul nœud 172.30.0.1	Ajouter HAProxy-02 + Keepalived/VIP ou deux entrées MX publiques
Certificat IMAP	CN localhost, vérification désactivée dans Roundcube	Certificat valide pour mail.sadek.ovh ou PKI interne
Socket replicator	mode 0666	Compte/groupe vmail commun + mode 0660
Comptes mail	Utilisateurs Linux locaux sur les deux Dovecot	SQL/LDAP/passwd-file centralisé ou automatisation de provisioning
SMTP Roundcube	Port 25 interne sans AUTH	Submission 587 + STARTTLS + SMTP AUTH
Réseaux de confiance Postfix	À restreindre précisément	Éviter les /8 trop larges dans mynetworks
Réplication doveadm	TCP privé 12345	Firewall strict, réseau dédié ; activer TLS doveadm si nécessaire
IP client vue par Postfix	HAProxy peut masquer la source	Étudier PROXY protocol / architecture adaptée à l'antispam
Antispam et réputation	Hors périmètre	Rspamd, SPF, DKIM, DMARC, PTR, rate limiting
Supervision	Logs manuels	Wazuh/Prometheus/Grafana + alertes
Sauvegarde	Réplication ≠ sauvegarde	Backups indépendants des Maildir et configurations

12.1 Réplication et sauvegarde : deux objectifs différents

La réplication protège la disponibilité : si un Dovecot tombe, l'autre possède une copie récente. Elle ne protège pas contre une suppression logique répliquée, une corruption applicative ou une erreur d'administration qui se propage aux deux nœuds. Il faut donc conserver des sauvegardes indépendantes et versionnées.

12.2 Sticky sessions IMAP

La réplication dsync est asynchrone. Dovecot recommande de préférence de garder un même utilisateur sur la même réplique quand c'est possible. Mon round-robin fonctionne grâce à la réplication, mais une stratégie de persistance par source/utilisateur réduirait les bascules inutiles et les fenêtres de divergence.

12.3 Sécurité du SMTP

La réception sur TCP 25 doit accepter les serveurs externes sans transformer l'infrastructure en open relay. Les réseaux déclarés dans mynetworks doivent rester strictement limités. Pour les clients humains, je séparerais la soumission sur 587 avec authentification et TLS.

13. Conclusion et bilan technique

Ce projet m'a permis de construire une chaîne mail réellement modulaire. Je ne me suis pas contenté d'installer Postfix et Dovecot : j'ai séparé les rôles, introduit un load balancer, utilisé LMTP pour la remise finale, ajouté un webmail, activé STARTTLS et surtout mis en place la réplication dsync avec des tests de panne réels.

Le point le plus formateur a été le dépannage. Plusieurs erreurs venaient d'interactions entre composants : Postfix et la syntaxe des domaines virtuels, Roundcube et les mécanismes d'authentification Dovecot, le certificat TLS, PAM et doveadm_port, le format mbox, les UID des comptes système, les permissions du socket replicator-doveadm et le fonctionnement asynchrone du replicator. Chaque erreur a été isolée par les logs puis corrigée sans masquer le symptôme.

Le test final constitue la preuve de réussite : je coupe DOVECOT-01, DOVECOT-02 continue à servir l'IMAP et à recevoir les messages LMTP, puis DOVECOT-01 revient et récupère automatiquement les mails manquants. Les deux nœuds affichent finalement le même nombre de messages dans INBOX.

Bilan — Architecture fonctionnelle, redondance Postfix validée, redondance Dovecot validée, réplication dsync validée, webmail Roundcube fonctionnel, failover et rattrapage après panne validés.

13.1 Ce que je retiens

- Un service redondant n'est réellement HA que si ses dépendances et son stockage le sont aussi.
- Un test de port ouvert ne suffit pas : il faut tester la chaîne fonctionnelle complète et le retour après panne.
- LMTP simplifie la frontière entre MTA et stockage de boîte.
- Les permissions UNIX et les UID sont structurants dès qu'un service de réplication agit au nom de plusieurs utilisateurs.
- La réplication asynchrone doit être observée comme une convergence, pas comme un stockage partagé instantané.
- Les logs de chaque maillon permettent de localiser précisément où s'arrête un message.

Références techniques

Les explications de cette documentation ont été consolidées avec les documentations officielles des composants utilisés. La configuration effectivement testée reste celle visible dans les captures et les logs du projet.

- **Postfix — Virtual Domain Hosting Howto** : https://www.postfix.org/VIRTUAL_README.html
- **Postfix — paramètres postconf** : <https://www.postfix.org/postconf.5.html>
- **Dovecot 2.3 — Replication with dsync** : https://doc.dovecot.org/2.3/configuration_manual/replication/
- **Dovecot 2.3 — Postfix and Dovecot LMTP** : https://doc.dovecot.org/2.3/configuration_manual/howto/postfix_dovecot_lmtp/
- **Dovecot 2.3 — Maildir Configuration** : https://doc.dovecot.org/2.3/configuration_manual/mail_location/Maildir/
- **Dovecot 2.3 — Service configuration** : https://doc.dovecot.org/2.3/configuration_manual/service_configuration/
- **HAProxy — Backends / round-robin / checks** : <https://www.haproxy.com/documentation/haproxy-configuration-tutorials/proxying-essentials/configuration-basics/backends/>
- **HAProxy — Health checks** : <https://www.haproxy.com/documentation/haproxy-configuration-tutorials/reliability/health-checks/>
- **Roundcube — Configuration** : <https://github.com/roundcube/roundcubemail/wiki/Configuration>
- **Roundcube — defaults.inc.php** : <https://github.com/roundcube/roundcubemail/blob/master/config/defaults.inc.php>

Annexe — Index des captures intégrées

Toutes les captures techniques du brouillon ont été reprises dans cette version, y compris la capture répétée du test LMTP qui était présente deux fois dans le document source. L'index ci-dessous facilite la recherche d'une preuve particulière.

N°	Capture	Emplacement
1	Capture source #1	Intégrée dans la section correspondante du déroulé
2	Capture source #2	Intégrée dans la section correspondante du déroulé
3	Capture source #3	Intégrée dans la section correspondante du déroulé
4	Capture source #4	Intégrée dans la section correspondante du déroulé
5	Capture source #5	Intégrée dans la section correspondante du déroulé
6	Capture source #6	Intégrée dans la section correspondante du déroulé
7	Capture source #7	Intégrée dans la section correspondante du déroulé
8	Capture source #8	Intégrée dans la section correspondante du déroulé
9	Capture source #9	Intégrée dans la section correspondante du déroulé
10	Capture source #10	Intégrée dans la section correspondante du déroulé
11	Capture source #11	Intégrée dans la section correspondante du déroulé
12	Capture source #12	Intégrée dans la section correspondante du déroulé
13	Capture source #13	Intégrée dans la section correspondante du déroulé

N°	Capture	Emplacement
14	Capture source #14	Intégrée dans la section correspondante du déroulé
15	Capture source #15	Intégrée dans la section correspondante du déroulé
16	Capture source #16	Intégrée dans la section correspondante du déroulé
17	Capture source #17	Intégrée dans la section correspondante du déroulé
18	Capture source #18	Intégrée dans la section correspondante du déroulé
19	Capture source #19	Intégrée dans la section correspondante du déroulé
20	Capture source #20	Intégrée dans la section correspondante du déroulé
21	Capture source #21	Intégrée dans la section correspondante du déroulé
22	Capture source #22	Intégrée dans la section correspondante du déroulé
23	Capture source #23	Intégrée dans la section correspondante du déroulé
24	Capture source #24	Intégrée dans la section correspondante du déroulé
25	Capture source #25	Intégrée dans la section correspondante du déroulé
26	Capture source #26	Intégrée dans la section correspondante du déroulé
27	Capture source #27	Intégrée dans la section correspondante du déroulé
28	Capture source #28	Intégrée dans la section correspondante du déroulé
29	Capture source #29	Intégrée dans la section correspondante du déroulé
30	Capture source #30	Intégrée dans la section correspondante du déroulé
31	Capture source #31	Intégrée dans la section correspondante du déroulé
32	Capture source #32	Intégrée dans la section correspondante du déroulé
33	Capture source #33	Intégrée dans la section correspondante du déroulé
34	Capture source #34	Intégrée dans la section correspondante du déroulé
35	Capture source #35	Intégrée dans la section correspondante du déroulé
36	Capture source #36	Intégrée dans la section correspondante du déroulé
37	Capture source #37	Intégrée dans la section correspondante du déroulé
38	Capture source #38	Intégrée dans la section correspondante du déroulé
39	Capture source #39	Intégrée dans la section correspondante du déroulé
40	Capture source #40	Intégrée dans la section correspondante du déroulé
41	Capture source #41	Intégrée dans la section correspondante du déroulé

N°	Capture	Emplacement
42	Capture source #42	Intégrée dans la section correspondante du déroulé
43	Capture source #43	Intégrée dans la section correspondante du déroulé
44	Capture source #44	Intégrée dans la section correspondante du déroulé
45	Capture source #45	Intégrée dans la section correspondante du déroulé
46	Capture source #46	Intégrée dans la section correspondante du déroulé
47	Capture source #47	Intégrée dans la section correspondante du déroulé
48	Capture source #48	Intégrée dans la section correspondante du déroulé
49	Capture source #49	Intégrée dans la section correspondante du déroulé
50	Capture source #50	Intégrée dans la section correspondante du déroulé
51	Capture source #51	Intégrée dans la section correspondante du déroulé
52	Capture source #52	Intégrée dans la section correspondante du déroulé
53	Capture source #53	Intégrée dans la section correspondante du déroulé
54	Capture source #54	Intégrée dans la section correspondante du déroulé
55	Capture source #55	Intégrée dans la section correspondante du déroulé
56	Capture source #56	Intégrée dans la section correspondante du déroulé

Adel Sadek

Projet infrastructure mail haute disponibilité — août 2026