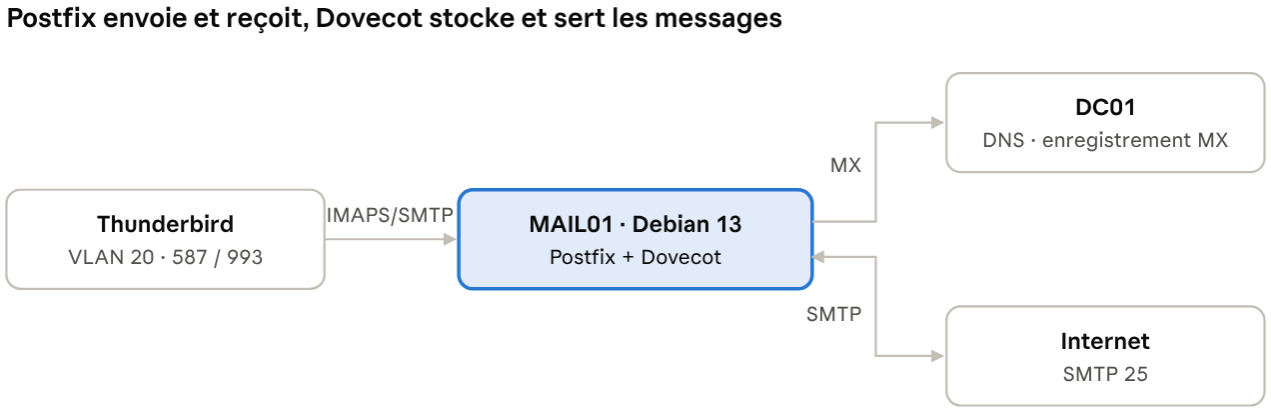
Serveur de messagerie Postfix + Dovecot sous Debian 13

Nov 27, 2026 · @Serge Martins

Objectif

Installer **MAIL01** (Debian 13 « Trixie ») comme serveur de messagerie du domaine **martinscie.lan** : Postfix 3.10 assure l'envoi et la réception SMTP, Dovecot 2.4 stocke les messages (Maildir) et les sert en IMAPS. Les comptes sont des utilisateurs système Linux. Le DNS (enregistrements A et MX) est porté par DC01.

Élément	Valeur
Nom	mail01.martinscie.lan
Adresse IP	192.168.10.25/24 (VLAN 10 Serveurs)
Passerelle	192.168.10.254 (RFW01 pfSense)
DNS	192.168.10.10 (DC01)
Logiciels	Postfix 3.10, Dovecot 2.4 (IMAP + LMTP)
Ports	25 (SMTP), 587 (Submission STARTTLS), 993 (IMAPS)



MAIL01 · flux de messagerie Postfix + Dovecot

Les clients du VLAN 20 envoient par le port 587 et lisent par IMAPS (993) ; Postfix reçoit le courrier entrant sur le port 25 et le remet à Dovecot via LMTP.

Prérequis

- VM Debian 13 minimale (1 vCPU, 2 Go RAM, 20 Go disque), SSH installé.
- IP fixe configurée dans `/etc/network/interfaces` et nom d'hôte `mail01`.
- Accès administrateur à DC01 pour créer les enregistrements DNS.

```
hostnamectl set-hostname mail01
echo "192.168.10.25 mail01.martinscie.lan mail01" >> /etc/hosts
hostname -f   # doit afficher mail01.martinscie.lan
```

Étape 1 – Enregistrements DNS sur DC01

Sur DC01 (PowerShell administrateur) :

```
Add-DnsServerResourceRecordA -ZoneName "martinscie.lan" -Name "mail01" -
IPv4Address 192.168.10.25 -CreatePtr
Add-DnsServerResourceRecordMX -ZoneName "martinscie.lan" -Name "." -
MailExchange "mail01.martinscie.lan" -Preference 10
```

Vérification depuis MAIL01 :

```
apt install -y bind9-dnsutils
dig +short MX martinscie.lan
dig +short mail01.martinscie.lan
```

Étape 2 – Installation des paquets

```
apt update
DEBIAN_FRONTEND=noninteractive apt install -y postfix dovecot-imapd dovecot-
lmtpd mailutils
```

Puis lancer `dpkg-reconfigure postfix` : type **Site Internet**, nom de courrier **martinscie.lan**.

Étape 3 – Certificat TLS auto-signé

```
openssl req -x509 -newkey rsa:4096 -sha256 -days 825 -nodes \
  -keyout /etc/ssl/private/mail01.key -out /etc/ssl/certs/mail01.crt \
  -subj "/CN=mail01.martinscie.lan" \
  -addext "subjectAltName=DNS:mail01.martinscie.lan"
chmod 600 /etc/ssl/private/mail01.key
```

Étape 4 – Configuration de Dovecot 2.4

> Dovecot 2.4 (Debian 13) n'accepte plus la syntaxe 2.3. Le fichier doit commencer par `dovecot_config_version` et `dovecot_storage_version`, et plusieurs paramètres ont été renommés. On remplace donc entièrement la configuration.

```
cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.orig
nano /etc/dovecot/dovecot.conf
```

```
dovecot_config_version = 2.4.0
dovecot_storage_version = 2.4.0

protocols {
  imap = yes
  lmtp = yes
}

mail_driver = maildir
mail_path = ~/Maildir

ssl = required
ssl_server_cert_file = /etc/ssl/certs/mail01.crt
ssl_server_key_file = /etc/ssl/private/mail01.key

auth_allow_cleartext = no
auth_mechanisms = plain login
auth_username_format = %{user | username | lower}

passdb pam {
}
userdb passwd {
}

service auth {
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
  }
}

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

```
    user = postfix
    group = postfix
  }
}

namespace inbox {
  inbox = yes
  mailbox Drafts {
    special_use = \Drafts
    auto = subscribe
  }
  mailbox Sent {
    special_use = \Sent
    auto = subscribe
  }
  mailbox Trash {
    special_use = \Trash
    auto = subscribe
  }
  mailbox Junk {
    special_use = \Junk
    auto = subscribe
  }
}
```

```
doveconf -n          # vérifie la syntaxe
systemctl restart dovecot
```

Étape 5 – Configuration de Postfix

```
postconf -e "myhostname = mail01.martinscie.lan"
postconf -e "mydomain = martinscie.lan"
postconf -e "myorigin = \$mydomain"
postconf -e "mydestination = \$myhostname, \$mydomain, localhost"
postconf -e "mynetworks = 127.0.0.0/8 192.168.10.0/24 192.168.20.0/24"
postconf -e "home_mailbox = Maildir/"
postconf -e "mailbox_transport = lmtp:unix:private/dovecot-lmtp"
postconf -e "smtpd_tls_cert_file = /etc/ssl/certs/mail01.crt"
postconf -e "smtpd_tls_key_file = /etc/ssl/private/mail01.key"
postconf -e "smtpd_tls_security_level = may"
postconf -e "smtpd_sasl_type = dovecot"
postconf -e "smtpd_sasl_path = private/auth"
postconf -e "smtpd_relay_restrictions = permit_mynetworks,
permit_sasl_authenticated, reject_unauth_destination"
```

Activer le port de soumission 587 dans `/etc/postfix/master.cf` (décommenter et compléter) :

```
submission inet n       -       y       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

```
postfix check
systemctl restart postfix
```

Étape 6 – Comptes de messagerie

```
adduser --gecos "Alice Durand" adurand
adduser --gecos "Bruno Petit" bpetit
```

Chaque utilisateur reçoit son courrier dans `~/Maildir`, créé automatiquement à la première livraison.

Étape 7 – Tests

```
ss -tlnp | grep -E ':25|:587|:993'
echo "Test interne" | mail -s "Bienvenue" adurand@martinscie.lan
ls /home/adurand/Maildir/new/
tail -f /var/log/mail.log    # ou : journalctl -u postfix -f
openssl s_client -connect mail01.martinscie.lan:993 -quiet
```

Sur un poste client (VLAN 20), configurer **Thunderbird** :

Paramètre	Valeur
Serveur entrant	IMAP – mail01.martinscie.lan – 993 – SSL/TLS
Serveur sortant	SMTP – mail01.martinscie.lan – 587 – STARTTLS
Identifiant	adurand (mot de passe normal)

Accepter l'exception de sécurité du certificat auto-signé, puis échanger des messages entre adurand et bpetit.

Étape 8 (optionnel) – Webmail Roundcube

```
apt install -y roundcube roundcube-plugins apache2 libapache2-mod-php
```

Dans `/etc/roundcube/config.inc.php` : `imap_host` = `ssl://mail01.martinscie.lan:993` et `smtp_host` = `tls://mail01.martinscie.lan:587`. Le webmail est alors accessible sur `http://mail01.martinscie.lan/roundcube`.

Sécurité et bonnes pratiques

- Ne jamais ouvrir le relais : `mynetworks` limité aux VLAN internes, tous les autres clients doivent s'authentifier.
- Pare-feu local : `nft` ou `ufw` n'autorisant que 22, 25, 587 et 993.
- Fail2ban sur les jails `postfix` et `dovecot` contre la force brute.
- En production : certificat Let's Encrypt, enregistrements SPF, DKIM (OpenDKIM) et DMARC, filtrage antispam (Rspamd).
- Sauvegarder `/etc/postfix`, `/etc/dovecot` et les dossiers `Maildir`.

Dépannage

Symptôme	Piste
Dovecot ne démarre pas	Syntaxe 2.3 résiduelle : `doveconf -n`, convertisseur dovecot.org/upgrader
`Relay access denied`	Client hors `mynetworks` et non authentifié sur le port 587
Message non livré	`/var/log/mail.log`, droits sur `private/dovecot-lmtp`
Thunderbird refuse l'authentification	Vérifier `auth_allow_cleartext = no` + TLS actif côté client