

# Les mail

## Trois logiciels

- Dovecot
- opensmtpd
- dkimsign

Les mails sont dans `/var/mailbox`

Pour ajouter un nouvel identifiant, les fichiers sont dans `/etc/mailbox/`

Pour générer le hash du mot de passe: `doveadm pw -s SHA512-CRYPT`

## Opensmtpd

`/usr/local/etc/mail/smtpd.conf`

```
pki mail.ppsfleet.navy cert "/usr/local/etc/mail/certs/mail.ppsfleet.navy.crt"
pki mail.ppsfleet.navy key "/usr/local/etc/mail/certs/mail.ppsfleet.navy.key"

# --- Filtre rdns --- # Reject if no reverse dns

filter check_rdns phase connect match !rdns \
    disconnect "550 no rDNS"

# --- Filtre fcrdns --- # Reject if no "Forward-confirmed_reverse_DNS" dns(reverse(domain)) =
domain

filter check_fcrdns phase connect match !fcrdns \
    disconnect "550 no FCrDNS"

filter dkimsign proc-exec "/usr/local/libexec/opensmtpd/filter-dkimsign -d ppsfleet.navy -s
mail -k /usr/local/etc/mail/dkim/ppsfleet.navy.key" user _smtpd group _smtpd

table aliases file:/etc/mailbox/aliases.txt
table domains file:/etc/mailbox/domains.txt
table password file:/etc/mailbox/passwd.txt
```

```
# --- mail entrant --- #
listen on vtnet0 port 25 tls pki mail.ppsfleet.navy filter { check_rdns, check_fcrdns}

# --- mail sortant --- #
listen on vtnet0 port submission tls-require pki mail.ppsfleet.navy auth <password> filter {
dkimsign }

action "reception" lmtpl "/var/run/dovecot/lmtpl" rcpt-to virtual <aliases>

action "envoi" relay helo almizan.ppsfleet.navy

# -- entrant --
match from any for domain <domains> action "reception"

# -- sortant --
# Demande authentication si "any auth"
match from any auth for any action "envoi"
match from local for any action "envoi"
```

# Dovecot

/usr/local/etc/mail/dovecot/dovecot.conf

```
ssl_cert = </var/db/caddy/data/caddy/certificates/acme-v02.api.letsencrypt.org-
directory/mail.ppsfleet.navy/mail.ppsfleet.navy.crt
ssl_key = </var/db/caddy/data/caddy/certificates/acme-v02.api.letsencrypt.org-
directory/mail.ppsfleet.navy/mail.ppsfleet.navy.key

ssl_min_protocol = TLSv1.2
ssl_prefer_server_ciphers = yes
ssl = required
disable_plaintext_auth = yes

protocols = lmtpl imap
# sieve

service lmtpl {
```

```
unix_listener lmtpl {
    user = vmail
    group = vmail
}

}

protocol lmtpl {
    mail_plugins = $mail_plugins sieve
}

service managesieve-login {
    inet_listener sieve {
        port = 4190
    }

    #inet_listener sieve_deprecated {
    # port = 2000
    #}

    # Number of connections to handle before starting a new process. Typically
    # the only useful values are 0 (unlimited) or 1. 1 is more secure, but 0
    # is faster. <doc/wiki/LoginProcess.txt>
    service_count = 1

    # Number of processes to always keep waiting for more connections.
    process_min_avail = 0

    # If you set service_count=0, you probably need to grow this.
    vsz_limit = 64M
}

service imap-login {
    inet_listener imap {
        port = 143
    }
    inet_listener imaps {
        port = 993
    }
}

}
```

```
#service auth {
# SASL
# unix_listener auth-client {
#   mode = 0660
#   user = mail
#   group = mail
# }
#}

passdb {
    driver = passwd-file
    args = scheme=SHA512-CRYPT /etc/mailbox/passwd.txt
}

userdb {
    args = uid=vmail gid=vmail home=/var/mailbox/%d/%n
    driver = static
}

namespace inbox {
    # Namespace type: private, shared or public
    type = private

    # Hierarchy separator to use. You should use the same separator for all
    # namespaces or some clients get confused. '/' is usually a good one.
    # The default however depends on the underlying mail storage format.
    separator = '/'

    inbox = yes
}

mail_location = maildir:/var/mailbox/%d/%n
```

---

Révision #1

Créé 2026-05-07 21:09:15 UTC par tjiho

Mis à jour 2026-05-10 11:07:36 UTC par tjiho