Remise distante des messages

1. Fonctionnement conjoint des MTA, MDA et des MUA

Le rôle d'un MTA (*Mail Transfer Agent*) en ce qui concerne la réception de messages se cantonne à la récupération et au stockage des mails entrants. Pour que l'utilisateur puisse lire et traiter confortablement son courrier, il utilise un MUA (*Mail User Agent* ou client de messagerie) qui fonctionne avec un protocole de retrait de courrier : POP ou IMAP. Postfix n'étant qu'un MTA et ne gérant pas ces protocoles, il faut lui adjoindre un service MDA (*Mail Delivery Agent*) de retrait de courrier pour les utilisateurs. Nous couvrirons ici la configuration de deux des principaux MDA : les services courrier et Dovecot.

Quand un message arrive au MTA, il a d'un point de vue SMTP terminé son voyage. Le MTA l'enregistre donc dans un espace de stockage local, dans notre cas au format mbox ou maildir. Si un serveur POP ou IMAP est installé, son rôle sera après avoir identifié l'utilisateur de retrouver les messages arrivés dans cet espace de stockage, et de les fournir au client de messagerie.

a. Le protocole POP3

Le protocole POP3 fonctionne sur le port 110 et est transporté par TCP. Il télécharge les messages depuis une boîte utilisateur vers un client de messagerie. Les messages sont ensuite normalement effacés de la boîte et libèrent l'espace disque du serveur. Toutefois, il est de plus en plus fréquent de configurer POP depuis le client afin qu'il laisse une copie des messages sur le serveur.

b. Le protocole IMAP4

Le protocole IMAP4 fonctionne sur le port 143 et est transporté par TCP. Il télécharge les en-têtes de messages depuis le serveur, et le client décide ensuite de l'action à mener sur ces messages : consulter, effacer, déplacer, etc. Les messages sont conservés sur le serveur, mais il est possible de configurer les clients IMAP afin qu'ils synchronisent les messages téléchargés pour une consultation hors-ligne.

2. Serveurs Courier-IMAP et Courier-POP

Les serveurs Courier-pop et Courier-imap appartiennent à une suite applicative appelée « Courier Mail Server ». Cette suite logicielle a été conçue pour fournir l'ensemble des services courants de gestion de courrier électronique, mais étant de nature modulaire, ses composants sont souvent utilisés seuls pour fournir un service précis.

a. Format de messages pour les services courrier

Les services Courier-pop et Courier-imap vont trouver les mails arrivés exclusivement dans un répertoire au format maildir. Tout fonctionnement avec le format mbox est impossible. Il faudra donc configurer postfix pour qu'il utilise le format maildir.

b. Configuration des services

C'est la bonne nouvelle, il n'y a en principe rien d'autre à faire que d'installer le service et de le démarrer. Les paramètres par défaut sont satisfaisants pour les fonctionnements standards. Les fichiers de configuration se trouvent généralement dans le répertoire **/etc/courier**, et s'appellent **pop3d** pour le service POP, et **imapd** pour le service IMAP.

Si le répertoire de stockage des courriers au format maildir ne devait pas utiliser le nom par défaut (Maildir), il faudrait préciser dans ces fichiers de configuration le nom utilisé.

Nom de répertoire maildir dans le fichier de configuration pop3d ou imapd

```
MAILDIRPATH=nomrepmaildir
```

Où *nomrepmaildir* représente le répertoire employé pour le stockage des messages reçus au format maildir.

Si le serveur dispose de plusieurs interfaces physiques, on peut limiter les interfaces d'écoute du démon imap.

Restrictions de l'interface active dans le fichier de configuration pop3d ou imapd

```
address = adresse_interface
```

Où *adresse_interface* représente l'adresse IP de l'interface apte à recevoir les connexions clientes.

c. Validation de l'authentification

Lors de l'utilisation de Courier-POP ou de Courier-IMAP, un client de messagerie présente l'identifiant et le mot de passe de l'utilisateur dont il veut relever le courrier. Ces éléments d'identification sont alors validés par la bibliothèque d'authentification « courier » commune aux deux services. Il peut être utile de vérifier en lignes de commandes que le compte utilisé est bien exploitable pour l'authentification par cette bibliothèque. L'utilitaire **authtest** est là pour ça.

Vérification de la validité d'un compte avec authtest

```
authtest utilisateur motdepasse
```

Où *utilisateur* et *motdepasse* sont les éléments d'authentification que le client de messagerie présentera pour se connecter en imap ou pop au serveur.

Exemple d'utilisation de authtest

Jusque-là tout va bien...

```
alpha:/etc/courier# authtest tic password
Authentication succeeded.

     Authenticated: tic  (system username: tic)
    Home Directory: /home/tic
           Maildir: (none)
             Quota: (none)
Encrypted Password: $1$YSIbmjnM$makfir51Gla3ZpfRq5dmu.
Cleartext Password: password
           Options: (none)
alpha:/etc/courier#
```

3. Serveur Dovecot

Dovecot est un autre serveur de retrait de courrier développé dans le but d'assurer un maximum de performances et de sécurité. Sa mise en œuvre est relativement simple, mais du fait de sa richesse fonctionnelle, les possibilités de configuration sont nombreuses et souvent décourageantes.

Dovecot supporte nativement les formats de boîtes aux lettres mbox et maildir.

a. Configuration de Dovecot

Le serveur Dovecot trouve sa configuration dans un fichier **dovecont.conf**, généralement situé dans le répertoire **/etc/dovecot**. Si le service doit être utilisé dans une infrastructure simple et courante, il faudra simplement modifier sa configuration afin qu'il accepte les authentifications par mots de passe en texte clair. Il peut paraître surprenant de ne pas sécuriser les mots de passe sur un serveur de messagerie, mais dans une utilisation traditionnelle, le message lorsqu'il circule sur Internet n'est absolument pas protégé et est visible de tous. Sécuriser alors la seule étape client-serveur revient alors à assurer une sécurité un peu illusoire sur le contenu du message. Le mot de passe du client de messagerie ne circule plus en clair, mais le message n'est protégé que de ses voisins immédiats. Il est toutefois possible de configurer son client de messagerie pour utiliser les protocoles POP ou IMAP sur SSL, la confidentialité est alors apportée sur le tronçon client-serveur mais il faut bien garder en tête que le message a sans doute transité en clair sans aucune protection avant d'arriver sur le serveur. La véritable sécurité sur le contenu des messages ne peut être apportée que par un protocole agissant de bout en bout comme SMIME.

Autorisation des authentifications en texte clair dans le fichier dovecot.conf

```
disable_plaintext_auth = no
```

Cette ligne peut être ajoutée à tout endroit du fichier de configuration mais existe généralement sous forme commentée dans les fichiers pré-configurés livrés avec les logiciels.

b. Visualisation de la configuration

Le nombre de paramètres possible dans le fichier **dovecot.conf** peut impressionner et rendre son interprétation difficile. De plus, il peut être utile de vérifier un paramètre de configuration sans avoir à parcourir les dizaines ou centaines de lignes du fichier. La commande **dovecot** appelée avec l'option **-a** permet de voir les paramètres effectifs sur le serveur.

Exemple d'utilisation de la commande dovecot pour visualiser la configuration

Le résultat ci-dessous est tronqué.

```
alpha:/etc/dovecot# dovecot -a | wc -l
139
alpha:/etc/dovecot# dovecot -a | head -20
# 1.0.15: /etc/dovecot/dovecot.conf
base_dir: /var/run/dovecot
log_path:
info_log_path:
log_timestamp: %Y-%m-%d %H:%M:%S
syslog_facility: mail
protocols: imap imaps pop3 pop3s
listen: *
ssl_listen:
ssl_disable: no
ssl_ca_file:
ssl_cert_file: /etc/ssl/certs/dovecot.pem
ssl_key_file: /etc/ssl/private/dovecot.pem
ssl_key_password:
ssl_parameters_regenerate: 168
ssl_cipher_list:
ssl_verify_client_cert: no
disable_plaintext_auth: no
verbose_ssl: no
shutdown_clients: yes
alpha:/etc/dovecot#
```