Travaux Pratiques n°3

Configuration d'un serveur Postfix – Pop – Imap

But du TP

Dans cette manipulation vous allez devoir configurer un serveur de mail (`postfix`) et des serveurs de distribution de mail (`pop` et `imap`).

Mise en place

Cette manipulation peut être effectuée sur chacun des postes des salles 410, 405 voire 102 sans notion de poste client et poste serveur. Tous les PC peuvent être à la fois clients et serveurs. Comme vous devez être administrateur sur le système, vous devrez travailler sur une machine virtuelle. Ce TP suppose l'utilisation de la distribution Debian/v11.02 telle qu'elle est installée sur le disque virtuel `Debian1102-20220323-pm….vdi`. Il faut donc créer une machine virtuelle comme indiqué en adaptant le nom de votre vm.

```
createvm
la commande sans paramètre vous donne la syntaxe à utiliser.
createvm Debian1102-20220323-pm….vdi  ma_vm
```

Ne pas changer l'adresse MAC, cela empêcherait la VM d'obtenir une adresse IP prévisible. On suppose aussi qu'un câble droit relie directement l'interface `en1` de votre PC au switch de la salle (SW102, SW410 ou SW405).

Faites démarrer votre VM, logez-vous en `root` ou en `rt`.

Dans tout le TP il va être question d'adresses IP et de noms de machines. Les exemples utilisent soient la salle 405 soit la 410, soit la 102 : il convient de tout ramener à la salle dans laquelle vous effectuez la manipulation.

I. Présentation des services de messagerie

La transmission de mails (figure n°1 page 2) met en jeu plusieurs logiciels et protocoles. La transmission de mails se fait la plupart du temps au moyen d'un logiciel de transfert de mail (MTA : ***M**ail **T**ransfer **A**gent*) qui travaille sur le port 25 attribué au protocole SMTP (***S**imple **M**ail **T**ransfer **P**rotocol)*. Les plus utilisés sont `postfix`, `exim`, `sendmail`… Le plus fréquemment ces transferts sont non-cryptés.

La récupération de mail à partir de sa boîte aux lettres se fait grâce à un « client lourd » (Thunderbird, Outlook…) qui effectue un transfert, la plupart du temps crypté avec les protocoles POP(S) et IMAP(S).

L'envoi du mail et sa réception sur une machine locale, un portable par exemple, se fait au moyen d'un logiciel que l'on appelle MUA (***M**ail **U**ser **A**gent*).

Un des problèmes du protocole SMTP c'est qu'il intervient à plusieurs niveaux : lors de l'envoi de mails par le MUA, lors des transferts de mail par les MTA entre eux, mais aussi lors de la réception du mail sur la boîte aux lettres du destinataire (le MDA : ***M**ail **D**elivery **A**gent*). C'est principalement la première étape qui pose problème, car elle permet le SPAM (pourriel). Une tentative pour limiter le SPAM est d'authentifier l'envoyeur avec un protocole crypté, on utilise alors les ports 465 ou 587.

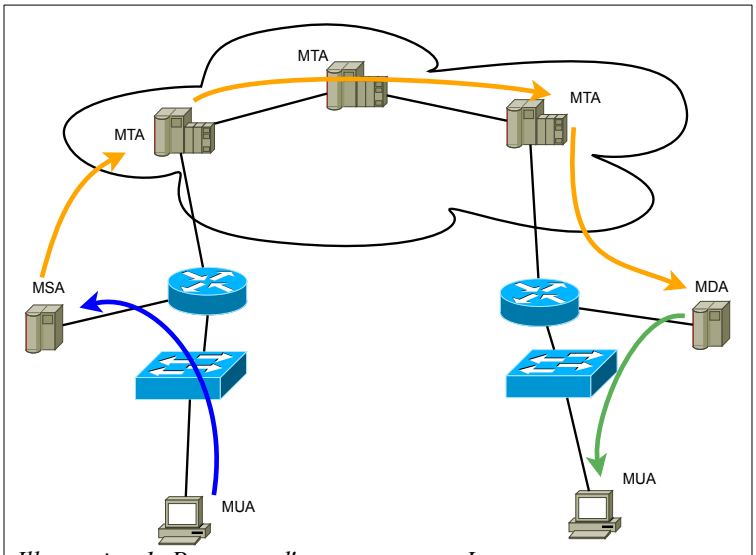

Illustration 1: Parcours d'un message sur Internet

Le port 465 est pour le protocole SMTPS c'est-à-dire avec encryption SSL, alors que le port 587 est pour la transmission du message par le MUA vers le réseau de messagerie dont la porte d'entrée est le MSA (***M**ail **S**ubmission **A**gent*). Le MSA écoute sur le port 587 il utilise normalement le protocole ESMTP (légèrement différent de SMTP) et démarre l'encryption TLS à la demande sur le même port.

Avec le schéma décrit ci-dessus, les fournisseurs d'accès peuvent interdire l'usage du port 25, réservé aux MTA et n'autoriser que le 587 (ou 465) pour l'envoi de message. Cela garantit au FAI que très peu de SPAM seront issus de son réseau, car il authentifie tous les mails. Les SPAM viennent pour la plupart de zones d'Internet mal ou pas gérées.

II. Configuration de `Postfix`

La configuration d'un serveur de mail est une opération très délicate. En effet le serveur doit gérer des flux entrants, sortants et en relai. C'est, comme d'habitude, difficile de savoir quoi autoriser sans qu'il y ait d'abus.

1. Configuration élémentaire

Faute de temps et d'espace réseau (des pare-feu empêchent toute communication externe) nous nous contenterons d'un serveur local et ne pourrons pas tester les configurations de relai.

> Avant de configurer `postfix` nous allons vérifier qu'une anomalie qui gêne le fonctionnement de `postfix` a été rectifiée. Si vous avez utilisé le vdi Debian1102... vous ne devriez pas avoir de problème.
>
> Dans le fichier `/etc/hosts` vérifiez que vous n'avez pas de référence à `debian` ni `debian.unice.fr` qui soit traduit par 127.0.0.1. remplacez ces noms par le **nom de vôtre machine** du genre `rt410p101` et `rt410p101.gtr.tp`.
>
> Dans le fichier `/etc/hostname` vérifiez que vous avez le nom de votre machine sans la partie domaine. Si ce n'est pas le cas, le modifier.

> Normalement `postfix` est pré-installé[1]. Il nous faut seulement reprendre la configuration.

Il y a environ 1000 paramètres possibles, mais très peu sont nécessaires pour avoir un fonctionnement de base.

- `myhostname` : le nom fqdn de votre serveur (ex. `rt405p103.gtr.tp`)
- `mydomain` : le nom de votre domaine (ex. : `gtr.tp`)
- `myorigin` : ce qui complète votre adresse quand vous envoyez un mail
  - deux cas usuels (il faut en choisir un)
    - = `$myshostname` : on obtient des adresses en `user@rt405p103.gtr.tp`
    - = `$mydomain` : pour des adresses en `user@gtr.tp`
  - en Debian par défaut c'est le nom de la machine qui est aussi dans le fichier `/etc/mailname`.
- `mydestination` : les adresses de destination qui sont acceptées par le serveur de **mail local**.
  - exemple : `mydestination = $myhostname localhost.$mydomain localhost $mydomain`
  - toutes les autres destinations sont refusées ou relayées
- `mynetworks` : les réseaux privilégiés (**origine** du mail), dont on fait suivre le courrier. Par défaut uniquement `localhost`. Le serveur délivra par défaut tous les mails qui arrivent de `mynetworks`, mais aussi ceux qui vont vers `relay_domains` et vers l'hôte local.

1 Si `postfix` ou `dovecot` ne sont pas installés utilisez les commandes :
`# apt-get update ; apt-get install postfix dovecot-core dovecot-pop3d dovecot-imapd`

- `relay_domains` : les domaines de **destination** vers lesquels le serveur relaie le courrier.
  Ici pas de relai.
- `relayhost` : vers quelle machine le serveur fait suivre le courrier ou l'envoie directement.

Plutôt que de modifier le fichier de configuration à la main, nous utilisons le gestionnaire de paquets :

```
# dpkg-reconfigure postfix
```

Répondre aux questions en indiquant que :

- il s'agit d'un serveur Internet
  (le serveur envoie aux autres serveurs en SMTP)
- « Nom de courrier » indiquez le nom fqdn de votre serveur (`myorigin`)
  - pour les destinataires sans domaine (ex. : rt) il faut ajouter le nom complet de votre machine (le fqdn ex. : `rt410p102.gtr.tp`), ce qui donnera l'adresse mail complète rt@rt410p101.gtr.tp.
- laissez le champ vide pour les messages à root : c'est un cas particulier qu'il faut traiter dans la vraie vie mais que nous laissons de côté durant le TP.
- votre serveur accepte ce qui pour `localhost` et pour votre machine (fqdn).(paramètre `mydestination`)
- ne pas relayer le courrier en dehors de la machine locale (paramètre `mynetworks`)
- vous n'utilisez que IPv4

La configuration est alors présente dans le fichier `/etc/postfix/main.cf` que l'on peut comparer au fichier général `/usr/share/postfix/main.cf.dist`

Il est clair que l'on n'a pas configuré toutes les possibilités.

Redémarrez `postfix`.

```
# service postfix restart
```

Cependant les paramètres sont quand même positionnés :

```
# postconf
```

montre l'ensemble des paramètres de configuration.

L'autre fichier à configurer dans `postfix` est `master.cf`. Il gère les utilitaires intégrés à `postfix`. Nous n'y touchons pas pour l'instant.

Vérifier que port 25 est ouvert puis vous y connecter par telnet.

2. Envoi d'un message par `telnet`

Vous savez que le protocole smtp, celui du transfert de mail est en texte et qu'il est très permissif. Nous allons envoyer un message complètement forgé pour en comprendre le principe. C'est une des techniques du SPAM.

Vous inspirer du Listing 1 page 5 en adaptant à votre cas sur votre machine, il faut bien-sûr envoyer votre message à un compte existant. Les éléments tapés sont en gras. Si le motif <CR><LF>.<CR><LF> ne suffit pas, finissez la saisie du message par un ^D (CtrlD).

```
root@Debian:~# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 debian.unice.fr ESMTP Postfix (Debian/GNU)
mail from: totolebeau@zorro.ca
250 2.1.0 Ok
rcpt to:rt
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
From: moi@trifouille.com
To: toi@lepirate.com
Voici mon message
Ton ami toto
.
250 2.0.0 Ok: queued as 5D5AE1A1F67
quit
221 2.0.0 Bye
Connection closed by foreign host.
root@Debian:~#
```

Listing 1 Exemple de connexion au serveur de mail

On peut lire les mails qui sont arrivés sur une boîte mail, directement en ligne de commande : aidez-vous de l'exemple sur le listing 2 page 6.

Nous avons vu dans la manipulation précédente, que le contenu d'un message et le nom de l'envoyeur sont complètement quelconques et ne sont en aucun cas authentifiés. Seul le destinataire doit être correct, sinon le message n'arrivera pas !

Dans le listing n°2 page 6 le message 1 a été envoyé sans les lignes From : et To : dans le contenu du message et l'on voit que le message est attribué à totolebeau. Par contre avec ces deux lignes, le message est attribué à moi@trifouille.com.

Il est donc possible de tromper le client mail qui affiche comme destinataire un autre nom que le nom de celui qui a reçu le mail. Il n'y a donc aucune confiance d'aucune sorte à accorder à un message reçu par mail. Seul le champ « `Received :` » semble être correct, mais il faut regarder les entêtes.

```
rt@rt410p102:~$ mail
"/var/mail/rt": 2 messages 1 nouveau 1 non lu
 U   1 totolebeau@rt410p1 jeu. mai 12 14:0  17/502
>N   2 moi@trifouille.com jeu. mai 12 14:2  13/421
? 2
Return-Path: <totolebeau@zorro.ca>
X-Original-To: rt
Delivered-To: rt@rt410p102.gtr.tp
Received: from localhost (localhost [127.0.0.1])
       by rt410p102.gtr.tp (Postfix) with SMTP id
79A3FBFC01
       for <rt>; Thu, 12 May 2022 14:20:14 +0200 (CEST)
From: moi@trifouille.com
To: toi@lepirate.com
Message-Id: <20220512122022.79A3FBFC01@rt410p102.gtr.tp>
Date: Thu, 12 May 2022 14:20:14 +0200 (CEST)

Voici mon message
Ton ami toto
? q
1 message sauvegardé dans /home/rt/mbox
1 message conservé dans /var/mail/rt
Vous avez du courrier dans /var/mail/rt
rt@rt410p102:~$
```

Listing 2 : Exemple de lecture du message en ligne de commande

Nous allons, dans la suite, utiliser des techniques plus pratiques.

3. Envoi d'un message en texte

La commande « mail » sert à lire les messages en local, mais aussi à les envoyer.

a) Utilisateur local

Si votre configuration est correcte, la suite devrait être assez simple.

D'abord en local, vers un utilisateur local à votre machine, sans indiquer l'adresse mail complète :

`mail rt`

Tapez votre message en le finissant par une ligne qui ne comporte qu'un ctrl D (touches ctrl et D).

Sous le compte du récipiendaire (ex.: `rt`) vérifiez l'arrivée du message, et les adresses mails qui ont été utilisées. (commande `mail`)

Les différentes étapes de l'envoi et de la réception sont visibles dans les traces (`/var/log/syslog` ou `/var/log/mail.{log,warn,err}`)

b) Utilisateur distant

Au lieu d'envoyer et de lire les messages sur la même machine, vous pouvez les envoyer à l'autre machine de votre paillasse (ou d'une autre), si vous l'avez configurée. Vous pouvez créer des utilisateurs pour tester plusieurs origines et destination.

Attention pour que cela fonctionne correctement, il faut utiliser le fqdn dans l'adresse mail ! (ex. : `mail rt@rt405p101.gtr.tp`).

Les salles de TP étant isolées du monde par le pare-feu pour des raisons de sécurité, vous ne pourrez pas faire parvenir de mail sur vos comptes personnels.

c) Limitation d'accès

Dans la variable `mynetwork` vous avez
« `127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128` » ce qui ne limite pas les accès puisque ce n'indique que des adresses locales et pas la machine distante.

Pour limiter les accès à `mynetwork` il faut ajouter dans le fichier `/etc/postfix/main.cf` la ligne ci-dessous.

```
smtpd_recipient_restrictions = permit_mynetworks, reject
```

Ajoutez la ligne et redémarrer `postfix`.

Testez l'envoi de mail vers le serveur de mail modifié à partir de votre autre PC. Cela ne devrait plus passer et vous devriez en être informé.

Pour ré-ouvrir l'accès, mais cette fois sous forme contrôlée, ajouter à la définition de `mynetworks` les paramètres suivants : « `10.0.0.0/8 , gtr.tp` », ce qui ouvre l'accès à toutes la partie TP « système et réseau » du bâtiment, mais pas aux autres machines.

Relancez `postfix` et testez.

III. Configuration des serveurs de récupération de mail

Les serveurs de récupération de mail POP (***P**ost **O**ffice **P**rotocol*) et IMAP (***I**nternet **M**ail **A**ccess **P**rotocol*) sont souvent associés. Ici nous utilisons le serveur par défaut de la distribution `Debian/Bullseye`, qui s'appelle `dovecot`. Il est normalement déjà installé[1].

1. Dovecot

Du temps de `uw-{pop,imap}` nous n'aurions rien eu à configurer, tout fonctionnait tout seul (ou ne fonctionnait pas). Quelques points, faciles à remanier, ne permettaient pas de véritablement configurer le logiciel.

Ce nouveau logiciel `dovecot` dispose de nombreuses possibilités de configuration. Il intègre nativement POP3 et IMAP4, et fournit les protocoles en version native, TLS et SSL. Un gros avantage de ce logiciel est la possibilité de gérer des comptes mails indépendants des comptes `unix`. De cette manière, avoir une adresse mail, ne donne aucun accès au système.

Nous mettrons en œuvre à la fois les services non cryptés et cryptés. Le mode chiffré peut fonctionner de deux manières : en SSL et en TLS. L'avantage du TLS est qu'il utilise le même port que le mode en clair (110) alors que pop3s utilise le port 995. Bien que vous n'ayez pas encore vu la notion de cryptographie et de certificat nous allons les utiliser, vous n'avez pas besoin de notions théoriques.

1 Si `dovecot` n'est pas installé, reportez-vous à la note du bas de la page 3.

Vous pouvez parcourir l'arborescence de configuration `/etc/dovecot`.

Vérifiez quels processus existent pour le mail :

```
# lsof -i
```

montre toutes les connexions Internet (`-i`) et donc les ports ouverts. Utilise-t-on imap2 ou imap4 ?

Effectivement `dovecot` est installé mais ne démarre pas tout seul : on doit l'activer. Vérifions qu'il n'est pas démarré et même désactivé.

```
# systemctl --type=service list-unit-files
```

On l'active pour qu'il démarre à l'initialisation du système. :

```
# systemctl enable dovecot
```

Vérifiez que les services `imap` et `pop` ne sont pas activés. On le démarre

```
# systemctl start dovecot
```

Quels sont les ports ouverts en POP et IMAP ?

```
# lsof -i
```

De quelles origines sont acceptées les connexions ?

On va modifier un peu la configuration des deux protocoles : on ne veut pas que la communication non cryptée puisse avoir lieu de n'importe où. Seul `localhost` devra pouvoir se connecter en clair.

Modifier le fichier `/etc/dovecot/conf.d/10-master.conf` en ajoutant la directive
`address = 127.0.0.1`
aux services « `imap-login` » et « `pop3-login` » pour les « `listener` » `imap` et `pop3`.

On veut aussi que le ssl soit activé : dans le fichier `/etc/dovecot/conf.d/10-ssl.conf` modifiez l'option `ssl` du début en 'yes'.

Dé-commentez les deux lignes `ssl_cert` et `ssl_key`.

Il faut générer des certificats qui seront auto-signés :

```
# cd /usr/share/dovecot/
```

Dans le fichier `dovecot-openssl.cnf` il faut modifier les champs

- `organizationName` = unNomdOrganisation
- `organizationalUnitName` = uneOrganisationUnit
- `commonName` = leNomFQDN_deLaMachine
- `emailAddress` = leMailDeLadmin

Commentez la ligne qui débute par RANDFILE vers `/dev/urandom`.

Après ces modifications, modifiez le script `mkcert.sh` pour que les chemins de la clé et du certificat correspondent à ceux du fichier de configuration `10-ssl.conf`, puis faire :

```
# ./mkcert.sh
```

Redémarrer le service pop et imap.

```
# service dovecot reload
```

a) POP3

On peut alors vérifier par `telnet` que le serveur pop écoute sur le port 110. Il est aussi possible de vérifier que les ports 110 et 995 sont ouverts. Attention de bien utiliser la bonne interface sur laquelle le serveur écoute.

Normalement la configuration par défaut suffit. Si dans `/var/log/mail.err` vous notez que `dovecot` n'y arrive pas, il peut être nécessaire de modifier le fichier `10-mail.conf` en ajoutant la ligne (dans les versions récentes cette ligne est déjà présente et dé-commentée). :

```
mail_location = mbox:~/:INBOX=/var/mail/%u
```

On a maintenant tout ce qu'il faut pour lire et envoyer des messages.

Configurer un client mail pour lire les messages sur le site local avec un utilisateur autre que `root`. Attention `root` est traité de manière spéciale. Vous pouvez utiliser « `Evolution` » qui est déjà installé mais pas configuré, ou par exemple « `thunderbird` » que vous pouvez installer.

Il vous est demandé d'envoyer et de lire les messages de votre machine en local ET de l'autre machine de la paillasse.

Envoyez un message en local à `rt` ou autre compte que vous pouvez créer pour l'occasion. Puis allez lire ce message.

Vérifiez que la connexion est cryptée. Utilisez pour cela wireshark soit en tant que root (si vous vous êtes logés en root intialement) ou en tant que rt. Attention dans le cas rt, il faut d'abord ajouter rt au groupe wireshark sinon vous ne voyez pas les interfaces. Il faut, en tant que root, utiliser la commande :

```
usermod -a -G wireshark rt
```

Puis il faut démarrer un nouveau terminal en rt pour que cela fonctionne.

Une fois wireshark activée, il faudra écouter sur l'interface sur laquelle Dovecot a démarré pop3 (la loopback en l'occurence).

b) IMAP

Cette configuration est très proche de celle de POP. Il faut surtout savoir que `IMAP` permet de consulter ses messages plus facilement, car il intègre une meilleure gestion des

fichiers et des répertoires. C'est le système qu'il faudra choisir si les clients consultent leurs messages à partir de plusieurs lieux, le serveur conservant les messages à disposition. Par contre il est à éviter si la place disponible est faible et le serveur peu puissant, ou que l'on est très inquiet sur la sécurité.

Vérifiez que les messages peuvent être récupérés par IMAP et qu'ils sont cryptés. Tous les transferts sont-ils cryptés ? Le vérifier avec `wireshark`.

Il vous est encore demandé d'envoyer et de lire les messages de votre machine en local ET de l'autre machine de la paillasse en créant des comptes POP et IMAP de chaque côté sur votre client lourd.

Fichier *TP-3_postPopImap-2223.odt* imprimé le 3 mai 2024