Dernière mise-à-jour : 2020/02/21 07:38

SED801 - Gestion du Serveur de Mail Postfix sous Debian 9

Avant-propos

Dans ce cours vous allez apprendre par la pratique :

- LAB #1 - Installation de postfix, de Dovecot et de Cyrus-Imapd,
- LAB #2 - Configuration de Base de Postfix,
- LAB #3 - Définition des Aliases,
- LAB #4 - Sécurisation de Postfix,
- LAB #5 - Configuration de l'Antispam et de l'Antivirus,
- LAB #6 - Configuration du Mandataire MailScanner,
- LAB #7 - Installation du Serveur IMAP Dovecot/Cyrus-Imapd,
- LAB #8 - Gestion des Domaines Virtuels avec MariaDB, Postfix et Dovecot,
- LAB #9 - Configuration de Postfix en Environnement chroot.

> **A Faire** - Configurez la RAM de votre VM **Debian 9** à 2 048 MB. Démarrez la VM. Connectez-vous via putty en utilisant localhost:2022 et le compte **trainee**/**trainee**. Saisissez la commande **su -** et devenez l'utilisateur **root** grâce au mot de passe **fenestros**.

Présentation

La messagerie utilise les protocols suivants :

- **SMTP** (Simple Message Transfer Protocol),
- **POP** (Post Office Protocol),
- **IMAP** (Internet Message Access Protocol).

Lors de l'utilisation du protocol **SMTP**, c'est l'expéditeur qui initie le transfert tandis qu'avec les protocols POP et IMAP c'est le destinataire qui initie la collecte.

Un serveur SMTP est appelé un **MTA** (Mail Transfer Agent) tandis que les serveurs POP et IMAP sont appelés des **MDA** (Mail Delivery Agent). Enfin les clients de messagerie sont des **MUA** (Mail User Agent).

Dans un système Linux, le mail est stocké pour chaque utilisateur soit dans le répertoire **/var/spool/mail**, soit dans un répertoire dans le répertoire personnel de chaque utilisateur.

Les quatre MTA les plus utilisés sous Linux sont :

- **Sendmail**,
- **Postfix**,
- **Exim**,
- **Qmail**.

> **Important** - Postfix est considéré d'être un des MTA le plus facilement configuré (par 250 directives !!). Ses fichiers sont facilement lisibles par l'être humain ce qui n'est pas le cas de sendmail.

Les MDA les plus utilisés sous Linux sont :

- **Cyrus IMAP**,
- **Dovecot**,
- **Fetchmail**.

> **Important** - Fetchmail remplit un rôle spécifique et n'est utilisé que quand le serveur n'est

pas connecté en permanance à Internet.

Les quatre MUA les plus utilisés sous Linux sont :

- **Evolution**,
- **KMail**,
- **Thunderbird**,
- **mutt**.

Deux utilitaires simples permettent la lecture des spools de mail locaux en ligne de commande aussi bien que l'envoie des messages :

- **mail**,
- **nail**.

La commande **nail** diffère de la commande **mail** par le fait qu'elle peut gérer des fichiers attachés.

Commencez par installer le paquet **mailutils** :

```
root@debian9:~# apt-get install mailutils
```

Les options de la commande mail sont :

```
root@debian9:~# mail --help
Usage : mail [OPTION...] [adresse...]
  ou :  mail [OPTION...] [OPTION...] [fichier]
  ou :  mail [OPTION...] --file [OPTION...] [fichier]
  ou :  mail [OPTION...] --file=fichier [OPTION...]
GNU mail — traite les courriers électroniques.
Si -f ou --file est précisé, mail agit sur la boite spécifiée par le
premier argument, ou sur la boite mbox de l'utilisateur, si aucun argument
n'est précisé.

  -A, --attach=FICHIER       attacher le FICHIER
```

```
 -a, --append=EN-TÊTE: VALEUR
                            ajoute l'en-tête donné au message à expédier
     --content-type=TYPE    sélectionne le type de contenu pour les options
                            --attach suivantes
 -E, --exec=COMMANDE        exécute la COMMANDE
 -e, --exist                retourne « vrai » (true) si du courrier existe

     --encoding=NOM         sélectionne l'encodage pour les options --attach
                            suivantes
 -F, --byname               sauvegarde les messages selon l'expéditeur
 -H, --headers              écrit un résumé de l'en-tête et quitte
 -i, --ignore               ignore les interruptions
 -N, --nosum                ne pas afficher le résumé initial des en-têtes
 -n, --norc                 ne pas lire le fichier système mailrc
 -p, --print, --read        affiche tous les courriels sur la sortie standard
 -q, --quit                 provoque l'arrêt du programme en cas
                            d'interruption
 -r, --return-address=ADRESSE
                            utiliser l'adresse comme adresse de retour lors de
                            l'envoi du courriel
 -s, --subject=OBJ          envoie un message ayant pour Objet OBJ
 -t, --to                   lit les destinataires dans l'en-tête du message
 -u, --user=UTIL.           opère sur la boîte aux lettres de l'UTILISATEUR

Options globales de débogage
     --debug-level=NIVEAU   fixe le niveau de débogage de Mailutils
     --debug-line-info      affiche l'information sur la source avec les
                            messages de débogage

Gestion de la configuration
     --config-file=FICHIER  lire ce fichier de configuration; implique
                            --no-config
     --config-lint          vérifie la syntaxe du fichier de configuration et
                            quitte
```

```
      --config-verbose       journalisation détaillée de l'analyse des
                             fichiers de configuration
      --no-config            ne pas lire les fichiers de configuration du site
                             et de l'utilisateur
      --no-site-config       ne pas lire le fichier de configuration du site
      --no-user-config       ne pas lire le fichier de configuration
                             utilisateur
      --set=PARAM=VALEUR     Assigne le paramètre de configuration

 Options d'information
      --config-help          affiche le résumé du fichier de configuration
      --show-config-options  affiche les options de compilation

  -?, --help                 donne cette liste d'aide
      --usage                affiche un bref message d'utilisation
  -V, --version              affiche la version du programme

Les arguments obligatoires ou optionnels pour les formes longues des options
sont aussi obligatoires ou optionnels pour les formes courtes associées.

Rapportez les anomalies à <bug-mailutils@gnu.org>.
Rapportez les erreurs de traduction à <traduc@traduc.org>
page d'accueil de GNU Mailutils: <http://mailutils.org>
Aide générale sur l'utilisation de logiciels GNU:
<http://www.gnu.org/software/gethelp.fr.html>
```

Par exemple :

```
root@debian9:~# mail -s "test  message" trainee
Cc: root
This is a test message
[^D]
```

```
root@debian9:~# su - trainee
```

```
trainee@debian9:~$ mail
"/var/mail/trainee": 1 message 1 nouveau
>N   1 root@debian9.i2tch mar. janv. 22 15  16/571   test  message
? 1
Return-path: <root@debian9.i2tch.loc>
Envelope-to: trainee@debian9.i2tch.loc,
 root@debian9.i2tch.loc
Delivery-date: Tue, 22 Jan 2019 15:09:24 +0100
Received: from root by debian9.i2tch.loc with local (Exim 4.89)
    (envelope-from <root@debian9.i2tch.loc>)
    id 1glwjz-0000VZ-Rv; Tue, 22 Jan 2019 15:09:23 +0100
Subject: test  message
To: <trainee@debian9.i2tch.loc>
Cc: <root@debian9.i2tch.loc>
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <E1glwjz-0000VZ-Rv@debian9.i2tch.loc>
From: root@debian9.i2tch.loc
Date: Tue, 22 Jan 2019 15:09:23 +0100

This is a test message
? q
1 message sauvegardé dans /home/trainee/mbox
0 message conservé dans /var/mail/trainee
```

Configuration de votre Machine Virtuelle

Modification du Fichier /etc/hosts

Comme vous allez utiliser le nom de domaine **mail.i2tch.com** pour votre serveur postfix, modifiez votre fichier **/etc/hosts** ainsi :

```
root@debian9:~# vi /etc/hosts
```

```
root@debian9:~# cat /etc/hosts
127.0.0.1   localhost
127.0.1.1   debian9.i2tch.loc    debian9
10.0.2.15   i2tch.com
10.0.2.15   mail.i2tch.com  mail

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Modification du FQDN

Modifiez le FQDN de votre VM :

```
root@debian9:~# nmcli g hostname mail.i2tch.com
root@debian9:~# hostname
mail.i2tch.com
```

Création, Activation et Configuration d'un Profil Réseau d'IP Fixe

Créez et activez un profil d'adresse IP fixe dénommé **ip_fixe** :

```
root@debian9:~# nmcli c show
NOM                 UUID                                  TYPE            PÉRIPHÉRIQUE
Wired connection 1  935fbc1c-a7f5-4bc9-a389-591e88989162  802-3-ethernet  enp0s3
root@debian9:~# nmcli connection add con-name ip_fixe ifname enp0s3 type ethernet ip4 10.0.2.15/24 gw4 10.0.2.2
Connexion « ip_fixe » (66f5d126-c0cc-4bc5-9ec1-41c8b0372af2) ajoutée avec succès.
root@debian9:~# nmcli connection up ip_fixe
Connexion activée (chemin D-Bus actif : /org/freedesktop/NetworkManager/ActiveConnection/2)
root@debian9:~# nmcli c show
```

```
NOM                 UUID                                  TYPE            PÉRIPHÉRIQUE
ip_fixe             66f5d126-c0cc-4bc5-9ec1-41c8b0372af2  802-3-ethernet  enp0s3
Wired connection 1  935fbc1c-a7f5-4bc9-a389-591e88989162  802-3-ethernet  --
```

Définissez un DNS pour le profil, redémarrez le service NetworkManager et testez la résolution des noms :

```
root@debian9:~# nmcli connection mod ip_fixe ipv4.dns 8.8.8.8
root@debian9:~# systemctl restart NetworkManager
root@debian9:~# apt-get install dnsutils
root@debian9:~# dig www.i2tch.com

; <<>> DiG 9.10.3-P4-Debian <<>> www.i2tch.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3377
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.i2tch.com.         IN    A

;; ANSWER SECTION:
www.i2tch.com.      21599    IN    CNAME    i2tch.com.
i2tch.com.      59    IN    A    77.153.192.218

;; Query time: 96 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Jan 22 15:20:03 CET 2019
;; MSG SIZE  rcvd: 72
```

Important - Déconnectez-vous et re-connectez-vous.

Démarrage du Service ntpd

Installez le service **ntp** :

```
root@mail:~# apt-get install ntp
root@mail:~# systemctl status ntp
● ntp.service - LSB: Start NTP daemon
   Loaded: loaded (/etc/init.d/ntp; generated; vendor preset: enabled)
   Active: active (running) since Tue 2019-01-22 15:23:28 CET; 12s ago
     Docs: man:systemd-sysv-generator(8)
   CGroup: /system.slice/ntp.service
           └─2760 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 117:122

janv. 22 15:23:32 mail.i2tch.com ntpd[2760]: Soliciting pool server 91.121.154.62
janv. 22 15:23:32 mail.i2tch.com ntpd[2760]: Soliciting pool server 5.196.160.139
janv. 22 15:23:33 mail.i2tch.com ntpd[2760]: Soliciting pool server 151.80.32.142
janv. 22 15:23:33 mail.i2tch.com ntpd[2760]: Soliciting pool server 108.61.177.141
janv. 22 15:23:33 mail.i2tch.com ntpd[2760]: Soliciting pool server 188.165.236.162
janv. 22 15:23:33 mail.i2tch.com ntpd[2760]: Soliciting pool server 195.154.41.195
janv. 22 15:23:34 mail.i2tch.com ntpd[2760]: Soliciting pool server 5.135.3.88
janv. 22 15:23:34 mail.i2tch.com ntpd[2760]: Soliciting pool server 2001:bc8:271b:100::1
janv. 22 15:23:34 mail.i2tch.com ntpd[2760]: Soliciting pool server 37.187.18.4
janv. 22 15:23:34 mail.i2tch.com ntpd[2760]: Soliciting pool server 91.121.91.167
```

Configurer firewalld

Installez le paquet **firewalld** :

```
root@mail:~# apt-get install firewalld
```

Pour ouvrir les ports en relation avec nos serveurs de méssagerie, utilisez les commandes suivantes :

```
[root@mail ~]# firewall-cmd --permanent --add-port=25/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=465/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=587/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=995/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=993/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=143/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=110/tcp
[root@mail ~]# firewall-cmd --reload
```

LAB #1 - Installation de postfix, de Dovecot et de Cyrus-Imapd

Installez le MTA **postfix**, le MDA **Dovecot** et le MDA **Cyrus-Imapd** :

```
root@mail:~# apt-get install postfix procmail dovecot-core dovecot-pop3d cyrus-imapd
```

Lors de l'installation :

- choisissez l'option “Site Internet”,
- spécifiez le nom de domaine mail.i2tch.com,
- répondez **oui** à la question concernant cyrus-imapd.

LAB #2 - Configuration de Base de Postfix

Le fichier /etc/postfix/main.cf

Utilisez les commandes suivantes pour voir les directives actives dans le fichiers **/etc/postfix/main.cf** :

```
root@mail:~# cd /tmp ; grep -E -v '^(#|$)'  /etc/postfix/main.cf > main.cf
root@mail:/tmp# cat main.cf
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
```

```
biff = no
append_dot_mydomain = no
readme_directory = no
compatibility_level = 2
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.i2tch.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, mail.i2tch.com, localhost.i2tch.com, , localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

Ce fichier comporte des directives au formats suivants :

- paramètre = valeur
- autre_paramètre = $paramètre

Sauvegardez votre fichier main.cf en main.old

```
[root@mail tmp]# cd ~
[root@mail ~]# cp /etc/postfix/main.cf /etc/postfix/main.old
```

Modifiez main.cf ainsi :

```
root@mail:~# vi /etc/postfix/main.cf
root@mail:~# cat /etc/postfix/main.cf
#############CONFIG DE BASE##############
myhostname = mail.i2tch.com
mydomain= i2tch.com
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
############   COMMANDES   ##############
mailbox_command = procmail -a "$EXTENSION"
############  REPERTOIRES  ##############
readme_directory = no
```

Les directives dans l'exemple ci-dessus sont :

Directive	**Description**
myhostname	Le nom de machine Internet de ce système de messagerie.
mydomain	Le nom de domaine Internet du système de messagerie.
myorigin	Le domaine par défaut utilisé pour les messages postés localement.
mynetworks	La liste des clients SMTP “internes” qui ont plus de privilèges que les “étrangers”.
mydestination	Liste des domaines livrés par le transporteur de messages.
smtpd_banner	Texte qui suit le code de statut 220 dans la bannière d'accueil.
delay_warning_time	Temps au delà duquel l'expéditeur reçoit les en-têtes d'un message toujours en file d'attente.
recipient_delimiter	Le délimiteur système de l'extension de adresse de destination.

Directive	Description
owner_request_special	Applique un traitement particulier aux parties locales des adresses de listes de propriétaires ou de requêtes.
inet_interfaces	Les adresses réseau par lesquelles le système de messagerie reçoit les messages.
unknown_local_recipient_reject_code	Code numérique de réponse du serveur SMTP de Postfix lorsque le destinataire n'est pas trouvé.
alias_maps	La base de données des alias utilisée pour la livraison locale.
alias_database	La base de données des alias pour la livraison locale.
mailbox_command	Commande externe optionnelle que l'agent de livraison local doit utiliser pour la livraison des messages.
readme_directory	Emplacement des fichiers README de Postfix.

A Faire : Pour plus d'informations concernant les directives, consultez **cette page**.

La Commande postconf

La commande **postconf** peut vous être très utile. Grâce à l'option **-d** vous pouvez visualiser les valeurs par défaut des directives de configuration de postfix au lieu des valeurs utilisées. Grâce à l'option **-n** vous pouvez visualiser les valeurs des directives de configuration de postfix qui sont différentes de valeurs par défaut :

```
root@mail:~# postconf -d | more
2bounce_notice_recipient = postmaster
access_map_defer_code = 450
access_map_reject_code = 554
address_verify_cache_cleanup_interval = 12h
address_verify_default_transport = $default_transport
address_verify_local_transport = $local_transport
address_verify_map = btree:$data_directory/verify_cache
address_verify_negative_cache = yes
address_verify_negative_expire_time = 3d
address_verify_negative_refresh_time = 3h
address_verify_pending_request_limit = 5000
address_verify_poll_count = ${stress?{1}:{3}}
```

```
address_verify_poll_delay = 3s
address_verify_positive_expire_time = 31d
address_verify_positive_refresh_time = 7d
address_verify_relay_transport = $relay_transport
address_verify_relayhost = $relayhost
address_verify_sender = $double_bounce_sender
address_verify_sender_dependent_default_transport_maps = $sender_dependent_default_transport_maps
address_verify_sender_dependent_relayhost_maps = $sender_dependent_relayhost_maps
address_verify_sender_ttl = 0s
address_verify_service_name = verify
address_verify_transport_maps = $transport_maps
address_verify_virtual_transport = $virtual_transport
alias_database = hash:/etc/aliases
alias_maps = hash:/etc/aliases, nis:mail.aliases
allow_mail_to_commands = alias, forward
allow_mail_to_files = alias, forward
allow_min_user = no
allow_percent_hack = yes
allow_untrusted_routing = no
alternate_config_directories =
always_add_missing_headers = no
always_bcc =
anvil_rate_time_unit = 60s
anvil_status_update_time = 600s
append_at_myorigin = yes
append_dot_mydomain = ${{$compatibility_level} < {1} ? {yes} : {no}}
application_event_drain_time = 100s
--Plus--
```

```
root@mail:~# postconf -n
alias_database = hash:/etc/aliases
alias_maps = hash:/etc/aliases
delay_warning_time = 4h
inet_interfaces = all
```

```
mailbox_command = procmail -a "$EXTENSION"
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
mydomain = i2tch.com
myhostname = mail.i2tch.com
mynetworks = 10.0.2.0/24, 127.0.0.0/8
myorigin = $mydomain
owner_request_special = no
readme_directory = no
recipient_delimiter = +
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
unknown_local_recipient_reject_code = 450
```

Le Commande sendmail de Postfix

Les options les plus importantes de la commande sendmail de postfix sont :

```
       -Am (ignored)

       -Ac (ignored)
              Postfix sendmail uses the same configuration file regardless  of
              whether or not a message is an initial submission.

       -B body_type
              The message body MIME type: 7BIT or 8BITMIME.

       -bd    Go  into  daemon  mode. This mode of operation is implemented by
              executing the "postfix start" command.

       -bh (ignored)

       -bH (ignored)
              Postfix has no persistent host status database.
```

```
       -bi    Initialize alias database. See the newaliases command above.

       -bm    Read mail from standard input and arrange for delivery.  This is
              the default mode of operation.

       -bp    List the mail queue. See the mailq command above.

       -bs    Stand-alone  SMTP  server mode. Read SMTP commands from standard
              input, and write responses to standard output.   In  stand-alone
              SMTP  server  mode,  mail relaying and other access controls are
              disabled by default. To enable them,  run  the  process  as  the
              mail_owner user.

              This  mode  of  operation is implemented by running the smtpd(8)
              daemon.

       -bv    Do not collect or deliver a  message.  Instead,  send  an  email
              report  after  verifying each recipient address.  This is useful
              for testing address rewriting and routing configurations.

              This feature is available in Postfix version 2.1 and later.
```

Tester la Configuration de Postfix

Testez votre fichier de configuration avec la commande **postfix** :

```
root@mail:~# postfix check
postfix: Postfix is running with backwards-compatible default settings
postfix: See http://www.postfix.org/COMPATIBILITY_README.html for details
postfix: To disable backwards compatibility use "postconf compatibility_level=2" and "postfix reload"
```

Terminer la Configuration

Modifiez maintenant les droits sur le répertoire **/var/spool/mail**:

```
root@mail:~# chmod 1777 /var/spool/mail
```

Re-démarrez le serveur postfix :

```
root@mail:~# systemctl restart postfix
root@mail:~# systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
   Active: active (exited) since Tue 2019-01-22 15:47:50 CET; 7s ago
  Process: 9361 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 9361 (code=exited, status=0/SUCCESS)

janv. 22 15:47:50 mail.i2tch.com systemd[1]: Starting Postfix Mail Transport Agent...
janv. 22 15:47:50 mail.i2tch.com systemd[1]: Started Postfix Mail Transport Agent.
```

Testez maintenant le serveur smtp de postfix en envoyant un message de root à trainee :

```
root@mail:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (Debian/GNU)
HELO me
250 mail.i2tch.com
MAIL from: root@i2tch.com
250 2.1.0 Ok
RCPT to: trainee@i2tch.com
250 2.1.5 Ok
DATA
```

```
354 End data with <CR><LF>.<CR><LF>
Subject: Test email
Ceci est un test
.
250 2.0.0 Ok: queued as E4BC860584
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Notez :

- le code **220** qui indique sue le serveur attend des instructions,
- le déroulement de la conversation :
  - **HELO me** sert à vous identifier,
  - **MAIL from: root@i2tch.com** indique l'expéditeur,
  - **RCPT to: trainee@i2tch.com** indique le destinataire,
  - **DATA** indique que ce qui suit est le message,
- le code **250** qui indique que la commande s'est bien déroulée.
- le point sur une ligne vide indique la fin de la section DATA.

Consultez maintenant le fichier **/var/log/maillog**. Vous devez constater que votre message a été livré à trainee :

```
root@mail:/var/log# tail /var/log/mail.log
Jan 22 15:47:50 mail postfix[9255]: To disable backwards compatibility use "postconf compatibility_level=2" and
"postfix reload"
Jan 22 15:47:50 mail postfix/postfix-script[9358]: starting the Postfix mail system
Jan 22 15:47:50 mail postfix/master[9360]: daemon started -- version 3.1.8, configuration /etc/postfix
Jan 22 15:48:51 mail postfix/smtpd[9391]: connect from localhost[::1]
Jan 22 15:49:38 mail postfix/smtpd[9391]: E4BC860584: client=localhost[::1]
Jan 22 15:50:08 mail postfix/cleanup[9432]: E4BC860584: message-id=<20190122144938.E4BC860584@mail.i2tch.com>
Jan 22 15:50:08 mail postfix/qmgr[9363]: E4BC860584: from=<root@i2tch.com>, size=325, nrcpt=1 (queue active)
Jan 22 15:50:08 mail postfix/local[9433]: E4BC860584: to=<trainee@i2tch.com>, relay=local, delay=47,
delays=47/0.01/0/0, dsn=2.0.0, status=sent (delivered to command: procmail -a "$EXTENSION")
Jan 22 15:50:08 mail postfix/qmgr[9363]: E4BC860584: removed
```

```
Jan 22 15:50:16 mail postfix/smtpd[9391]: disconnect from localhost[::1] helo=1 mail=1 rcpt=1 data=1 quit=1
commands=5
```

LAB #3 - Définition des Aliases

Les deux lignes suivantes, issues du fichier **/etc/postfix/main.cf** indiquent l'emplacement des fichiers relatifs aux **aliases** :

```
...
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
...
```

Voici le contenu du fichier **/etc/aliases** :

```
root@mail:~# cat /etc/aliases
# /etc/aliases
mailer-daemon: postmaster
postmaster: root
nobody: root
hostmaster: root
usenet: root
news: root
webmaster: root
www: root
ftp: root
abuse: root
noc: root
security: root
root: trainee
```

Il est important de spécifier un utilisateur existant qui recevra le mail de root et ceci pour des raisons légales liées à la boîte de mail **postmaster**, l'administrateur du serveur vu de l'extérieur.

Il est aussi possible de créer des aliases pour harmoniser les adresses email de l'organisation. Si, par exemple, l'adresse email doit être au format **prénom.nom** mais que les noms de comptes du système linux sont au format **prénom**, il convient de rajouter au fichier une ligne pour chaque personne au format suivant :

```
...
prénom.nom:     prénom
...
```

Modifiez donc la fin de ce fichier ainsi :

```
root@mail:~# vi /etc/aliases
root@mail:~# cat /etc/aliases
# /etc/aliases
mailer-daemon: postmaster
postmaster: root
nobody: root
hostmaster: root
usenet: root
news: root
webmaster: root
www: root
ftp: root
abuse: root
noc: root
security: root
root: trainee
mickey.mouse:   trainee
```

Afin de prendre en compte la nouvelle liste d'alias, il faut utiliser la commande **newaliases** :

```
root@mail:~# newaliases
```

et demander à postfix de relire ses fichiers de configuration :

```
root@mail:~# systemctl reload postfix
```

En utilisant telnet, envoyez un message de **trainee** à **mickey.mouse**. Ce message arrivera dans la bôite de réception de trainee grâce à l'alias créé ci dessus :

```
root@mail:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (Debian/GNU)
HELO me
250 mail.i2tch.com
MAIL from: root@i2tch.com
250 2.1.0 Ok
RCPT to: mickey.mouse@i2tch.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject : test
Message de test
.
250 2.0.0 Ok: queued as 36D9A60584
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Consultez maintenant le journal **/var/log/mail.log**. Vous apercevrez des lignes similaires à :

```
root@mail:~# tail /var/log/mail.log
Jan 22 16:11:20 mail postfix/anvil[9788]: statistics: max connection rate 1/60s for (smtp:::1) at Jan 22 16:07:06
Jan 22 16:11:20 mail postfix/anvil[9788]: statistics: max connection count 1 for (smtp:::1) at Jan 22 16:07:06
Jan 22 16:11:20 mail postfix/anvil[9788]: statistics: max cache size 1 at Jan 22 16:07:06
Jan 22 16:11:44 mail postfix/smtpd[9836]: connect from localhost[::1]
Jan 22 16:12:14 mail postfix/smtpd[9836]: 36D9A60584: client=localhost[::1]
```

```
Jan 22 16:12:28 mail postfix/cleanup[9840]: 36D9A60584: message-id=<20190122151214.36D9A60584@mail.i2tch.com>
Jan 22 16:12:28 mail postfix/qmgr[9826]: 36D9A60584: from=<root@i2tch.com>, size=323, nrcpt=1 (queue active)
Jan 22 16:12:28 mail postfix/local[9841]: 36D9A60584: to=<trainee@i2tch.com>, orig_to=<mickey.mouse@i2tch.com>,
relay=local, delay=29, delays=29/0.01/0/0.01, dsn=2.0.0, status=sent (delivered to command: procmail -a
"$EXTENSION")
Jan 22 16:12:28 mail postfix/qmgr[9826]: 36D9A60584: removed
Jan 22 16:12:31 mail postfix/smtpd[9836]: disconnect from localhost[::1] helo=1 mail=1 rcpt=1 data=1 quit=1
commands=5
```

Notez la présence de la ligne suivante :

```
Jan 22 16:12:28 mail postfix/local[9841]: 36D9A60584: to=<trainee@i2tch.com>, orig_to=<mickey.mouse@i2tch.com>,
relay=local, delay=29, delays=29/0.01/0/0.01, dsn=2.0.0, status=sent (delivered to command: procmail -a
"$EXTENSION")
```

Cette ligne démontre que l'alias fonctionne.

> **Important** : Un utilisateur peut transférer son email vers un autre utilisateur du système ou bien vers une adresse email valide en inscrivant le nom ou l'adresse dans le fichier **~.forward**.

LAB #4 - Sécurisation de Postfix

Cyrus SASL

Présentation

Cyrus SASL (**S**imple **A**uthentification and **S**ecurity **L**ayer) est l'implentation **SASL** de l'**Université de Carnegie Mellon**. SASL est un **Framework**

d'authentification décrit dans la **RFC 2222**.

SASL est organisé en trois couches - **l'interface d'authentification**, **le mécanisme** et **la méthode** :

- l'**interface d'authentification** concerne la phase de communication entre le client et le serveur,
  - le client se connecte au serveur,
  - les serveur annonce ses fonctionnalités,
  - le client détecte l'option d'authentification et la liste des mécanismes possibles,
  - le client choisit un **mécanisme** et génère une chaine de caractères en fonction du mécanisme choisi :
    - **anonyme** - accès anonymes,
    - **texte en clair** - de type **PLAIN** ou **LOGIN**, il fonctionne en encodant le nom d'utilisateur et le mot de passe en **base64**. La version LOGIN est utilisée pour des clients de messagerie non conformes à la RFC tels Outlook™ et Outlook Express™. Le codage **base64** n'est pas chiffré et necéssite l'utilisation de **TLS** (**T**ransport **L**ayer **S**ecurity).,
    - **secret partagé** - il fonctionne selon le principe de secret partagé en utilisant **CRAM-MD5** ou **DIGEST-MD5**,
  - le client envoie la chaîne au serveur en tant que reqûete d'authentification,
  - le serveur transmet la reqûete à SASL,
  - SASL utilise une **méthode** pour contacter la base d'authentification en fonction du **mécanisme** en utilisant :
    - **rimap** - SASL se connecte à un serveur IMAP en utilisant les coordonnées de l'utilisateur. Si la connexion aboutit SASL valide l'authentification,
    - **ldap** - SASL se connecte à un serveur LDAP en utilisant les coordonnées de l'utilisateur. Si la connexion aboutit SASL valide l'authentification,
    - **kerberos** - vérifie le ticket kerberos du client pour vérifier l'authentification,
    - **getpwent/shadow** - accède à /etc/passwd pour vérifier l'authentification,
    - **pam** - utilise un module PAM pour vérifier l'authentification,
    - **sasldb** - consulte la base de données **saslbd2** pour vérifier l'authentification,
    - **sql** - utilise une reqûete SQL auprès de MySQL, SQLite ou PostgreSQL pour vérifier l'authentification,
  - si l'authentification est correcte SASL informe le serveur qui permet la demande du client,.
  - si l'authentification est incorrecte SASL informe le serveur qui informe le client et refuse la demande du client.

SASL propose trois services pour effectuer les procédures décrites ci-dessus :

- **saslauthd** - un service autonome exécuté sous l'identité de root qui peut utiliser le mécanisme texte en clair (PLAIN et LOGIN),
- **auxprop** - un service faisant partie de l'architecture de Cyrus capable d'utiliser les mécanismes texte en clair (PLAIN et LOGIN) et secret partagé (CRAM-MD5 et DIGEST-MD5),
- **authdaemond** - un service écrit pour utiliser le daemon authdaemond du serveur **Courier** qui peut utiliser le mécanisme texte en clair (PLAIN et

LOGIN).

A part le nom du service de vérification du mot de passe et les mécanismes à utiliser, il est aussi possible de trouver la directive **log_level**. Cette directive prend comme valeur un chiffre :

Chiffre	Description
0	Aucune journalisation
1	Journalisation des erreurs inhabituelles
2	Journalisation des échecs d'authentification
3	Journalisation des avertissements inhabituelles
4	Niveau 3 en vv
5	Niveau 3 en vvv
6	Journalisation des événements concernant des protocoles internes de SASL
7	Journalisation des événements concernant des protocoles internes de SASL et mots de passe

Important - La valeur par défaut de la directive **log_level** est de **1**.

Le binaire **saslauthd** est fourni par le paquet **sasl2-bin**. Installez donc le paquet **sasl2-bin** :

```
root@mail:~# apt-get install sasl2-bin
root@mail:~# which saslauthd
/usr/sbin/saslauthd
```

Sachez que plusieurs paquets supplémentaires sont disponibles en fonction de la **méthode** :

```
root@mail:~# apt-cache search cyrus | grep sasl
cyrus-sasl2-doc - cyrus SASL - documentation
libapache2-mod-authn-sasl - fournisseur de dorsal d'authentification SASL pour Apache
libauthen-sasl-cyrus-perl - extension Perl de la bibliothèque SASL de Cyrus
libauthen-sasl-perl - Authen::SASL - structure d'authentification SASL
libsasl2-2 - Cyrus SASL : bibliothèque d'abstraction d'authentification
```

```
libsasl2-modules - Cyrus SASL - modules d'authentification enfichables
libsasl2-modules-db - Cyrus SASL - modules d'authentification DB
libsasl2-dev - Cyrus SASL - development files for authentication abstraction library
libsasl2-modules-gssapi-heimdal - Pluggable Authentication Modules for SASL (GSSAPI)
libsasl2-modules-gssapi-mit - Cyrus SASL - pluggable authentication modules (GSSAPI)
libsasl2-modules-ldap - Cyrus SASL - pluggable authentication modules (LDAP)
libsasl2-modules-otp - Cyrus SASL - pluggable authentication modules (OTP)
libsasl2-modules-sql - Cyrus SASL - pluggable authentication modules (SQL)
sasl2-bin - Cyrus SASL - administration programs for SASL users database
lua-cyrussasl - Cyrus SASL library for the Lua language
lua-cyrussasl-dev - Cyrus SASL development files for the Lua language
libqca2-plugin-cyrus-sasl - transitional package for libqca2-plugins
```

Vérifiez lesquels ont été installés dans Debian 9 :

```
root@mail:~# dpkg --get-selections | grep sasl
libauthen-sasl-perl             install
libgsasl7                   install
libsasl2-2:amd64                install
libsasl2-modules:amd64              install
libsasl2-modules-db:amd64           install
sasl2-bin                   install
```

La configuration de saslauthd se trouve dans le fichier **/etc/default/saslauthd** :

```
root@mail:~# cat /etc/default/saslauthd
#
# Settings for saslauthd daemon
# Please read /usr/share/doc/sasl2-bin/README.Debian for details.
#

# Should saslauthd run automatically on startup? (default: no)
START=no
```

```
# Description of this saslauthd instance. Recommended.
# (suggestion: SASL Authentication Daemon)
DESC="SASL Authentication Daemon"

# Short name of this saslauthd instance. Strongly recommended.
# (suggestion: saslauthd)
NAME="saslauthd"

# Which authentication mechanisms should saslauthd use? (default: pam)
#
# Available options in this Debian package:
# getpwent  -- use the getpwent() library function
# kerberos5 -- use Kerberos 5
# pam       -- use PAM
# rimap     -- use a remote IMAP server
# shadow    -- use the local shadow password file
# sasldb    -- use the local sasldb database file
# ldap      -- use LDAP (configuration is in /etc/saslauthd.conf)
#
# Only one option may be used at a time. See the saslauthd man page
# for more information.
#
# Example: MECHANISMS="pam"
MECHANISMS="pam"

# Additional options for this mechanism. (default: none)
# See the saslauthd man page for information about mech-specific options.
MECH_OPTIONS=""

# How many saslauthd processes should we run? (default: 5)
# A value of 0 will fork a new process for each connection.
THREADS=5

# Other options (default: -c -m /var/run/saslauthd)
```

```
# Note: You MUST specify the -m option or saslauthd won't run!
#
# WARNING: DO NOT SPECIFY THE -d OPTION.
# The -d option will cause saslauthd to run in the foreground instead of as
# a daemon. This will PREVENT YOUR SYSTEM FROM BOOTING PROPERLY. If you wish
# to run saslauthd in debug mode, please run it by hand to be safe.
#
# See /usr/share/doc/sasl2-bin/README.Debian for Debian-specific information.
# See the saslauthd man page and the output of 'saslauthd -h' for general
# information about these options.
#
# Example for chroot Postfix users: "-c -m /var/spool/postfix/var/run/saslauthd"
# Example for non-chroot Postfix users: "-c -m /var/run/saslauthd"
#
# To know if your Postfix is running chroot, check /etc/postfix/master.cf.
# If it has the line "smtp inet n - y - - smtpd" or "smtp inet n - - - - smtpd"
# then your Postfix is running in a chroot.
# If it has the line "smtp inet n - n - - smtpd" then your Postfix is NOT
# running in a chroot.
OPTIONS="-c -m /var/run/saslauthd"
```

Modifiez la directive **START** afin que saslauthd démarre au démarrage du système :

```
root@mail:~# vi /etc/default/saslauthd
root@mail:~# head /etc/default/saslauthd
#
# Settings for saslauthd daemon
# Please read /usr/share/doc/sasl2-bin/README.Debian for details.
#

# Should saslauthd run automatically on startup? (default: no)
START=yes

# Description of this saslauthd instance. Recommended.
```

```
# (suggestion: SASL Authentication Daemon)
```

Les méchanisms de vérification des mots de passe supportés par saslauthd peuvent être visualisés en utilisant l'option **-v** de la commande **saslauthd** :

```
root@mail:~# saslauthd -v
saslauthd 2.1.27
authentication mechanisms: sasldb getpwent kerberos5 pam rimap shadow ldap
```

Configuration de Postfix

Dans le cas de Postfix, le serveur qui prend en charge les reqûetes d'authentification est **smtpd** avec la fonction **SMTP AUTH**. Vérifiez que postfix a été installé avec le support pour **SMTP AUTH** :

```
root@mail:~# apt-get install locate
root@mail:~# updatedb
root@mail:~# locate smtpd
/usr/lib/postfix/sbin/smtpd
/usr/lib/python2.7/smtpd.py
/usr/lib/python2.7/smtpd.pyc
/usr/lib/python3.5/__pycache__/smtpd.cpython-35.pyc
/usr/lib/python3.5/smtpd.py
/usr/share/man/man8/smtpd.8postfix.gz
root@mail:~# ldd /usr/lib/postfix/sbin/smtpd | grep libsasl
    libsasl2.so.2 => /usr/lib/x86_64-linux-gnu/libsasl2.so.2 (0x00007f4bbe78a000)
```

> **Important** - La présence de la bibliothèque **libsasl2** indique que postfix a été installé avec le support pour SASL.

Ajoutez ensuite les lignes suivantes au fichier **/etc/postfix/main.cf** :

```
...
############      SASL     ##############
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
                                  reject_non_fqdn_sender,
                                  reject_non_fqdn_recipient,
                                  reject_unknown_sender_domain,
                                  reject_unknown_recipient_domain,
                                  reject_unauth_pipelining,
                                  reject_rbl_client zen.spamhaus.org,
                                  reject_rbl_client bl.spamcop.net,
                                  reject_rbl_client dnsbl.njabl.org,
                                  reject_rbl_client dnsbl.sorbs.net,
                                  permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtp_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = i2tch.com
smtpd_helo_required = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = cyrus
cyrus_sasl_config_path = /etc/postfix/sasl
```

Vous obtiendrez le résultat suivant :

```
root@mail:~# vi /etc/postfix/main.cf
root@mail:~# cat /etc/postfix/main.cf
```

```
#############CONFIG DE BASE##############
myhostname = mail.i2tch.com
mydomain= i2tch.com
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
relayhost =
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
############   COMMANDES   ##############
mailbox_command = procmail -a "$EXTENSION"
############  REPERTOIRES  ##############
readme_directory = no
############      SASL     ##############
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
                                  reject_non_fqdn_sender,
                                  reject_non_fqdn_recipient,
                                  reject_unknown_sender_domain,
                                  reject_unknown_recipient_domain,
                                  reject_unauth_pipelining,
                                  reject_rbl_client zen.spamhaus.org,
                                  reject_rbl_client bl.spamcop.net,
```

```
                                reject_rbl_client dnsbl.njabl.org,
                                reject_rbl_client dnsbl.sorbs.net,
                                permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = i2tch.com
smtpd_helo_required = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = cyrus
cyrus_sasl_config_path = /etc/postfix/sasl
```

Les directives ajoutées dans l'exemple ci-dessus sont :

Directive	**Description**
smtpd_recipient_restrictions	Restrictions d'accès que le serveur SMTP de Postfix applique dans le contexte d'une commande RCPT TO.
smtpd_client_restrictions	Restrictions d'accès optionelles du serveur SMTP pour les requêtes de connexion au service SMTP.
smtp_sasl_mechanism_filter	La version spécifique LMTP du paramètre smtp_sasl_mechanism_filter.
smtpd_sasl_auth_enable	Active l'authentification SASL dans le serveur SMTP de Postfix.
smtpd_sasl_security_options	Options de sécurité SASL.
broken_sasl_auth_clients	Active l'interoperabilité avec les clients SMTP qui implémentent une version obsolete de la commande AUTH.
smtpd_sasl_local_domain	Nom de royaume d'authentification SASL local.
smtpd_helo_required	Impose au client SMTP de démarrer la session SMTP par une commande HELO ou EHLO.

smtpd_recipient_restrictions

Restriction	**Description**
permit_sasl_authenticated	Autorise la requête lorsque le client est authentifié avec succès via le protocole AUTH.
permit_mynetworks	Autorise la requête si l'adresse IP du client correspond à l'une des adresses ou l'un des réseaux listé dans $mynetworks.
reject_invalid_hostname	Rejette les requêtes lorsque la syntaxe du nom de machine passé avec HELO ou EHLO est invalide.

Restriction	Description
reject_non_fqdn_hostname	Rejette la requête lorsque le nom de domaine n'est pas sous la forme pleinement qualifiée requise par la RFC.
reject_non_fqdn_sender	Rejette la requête lorsque l'adresse MAIL FROM n'est pas sous la forme pleinement qualifiée requise par la RFC.
reject_non_fqdn_recipient	Rejette la requête lorsque l'adresse RCPT TO n'est pas de forme pleinement qualifiée.
reject_unknown_sender_domain	Rejette la requête lorsque Postfix n'est pas la destination finale de l'adresse d'expédition et que l'adresse MAIL FROM n'a pas d'enregistrement DNS A ou MX correspondant, ou lorsque cet enregistrement MX est malformé comme un nom MX de longueur nulle.
reject_unknown_recipient_domain	Rejette la requête lorsque l'adresse RCPT TO ne correspond à aucun enregistrement DNS de type A ou MX et Postfix n'est pas la destination finale de l'adresse de destination.
reject_unauth_pipelining	Rejette la requête lorsque le client envoie des commandes SMTP en dehors des moments où il y est autorisé ou lorsque le client envoie des commandes SMTP avant de savoir que Postfix supporte la canalisation des commandes SMTP (pipelining).
reject_rbl_client	Rejette la requête lorsque la résolution inverse de l'adresse réseau du client correspond à un enregistrement de type A du domaine zen.spamhaus.org, bl.spamcop.net, dnsbl.njabl.org ou dnsbl.sorbs.net.
permit	Autorise la requête. C'est la politique par défaut.

smtpd_client_restrictions

Restriction	Description
permit_sasl_authenticated	Autorise la requête lorsque le client est authentifié avec succès via le protocole AUTH.
permit_mynetworks	Autorise la requête si l'adresse IP du client correspond à l'une des adresses ou l'un des réseaux listé dans $mynetworks.
reject_unauth_destination	Rejette la requête sauf si Postfix transfert le message ou Postfix est la destination finale.

smtpd_sasl_security_options

Option	Description
noplaintext	Interdit les méthodes utilisant les mots de passe en clair.
noactive	Interdit les méthodes sujettes à une attaque active (sans dictionnaire).
nodictionary	Interdit les méthodes sujettes à une attaque passive (par dictionnaire).
noanonymous	Interdit les méthodes qui autorisent l'authentification anonyme.
mutual_auth	N'autorise que les méthodes fournissant une authentification mutuelle.

Editez maintenant le fichier **/etc/postfix/master.cf** en modifiant la valeur de **chroot** dans la ligne **smtp** :

```
root@mail:~# vi /etc/postfix/master.cf
root@mail:~# head -n 15 /etc/postfix/master.cf
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
```

Rechargez la configuration de postfix :

```
root@mail:~# systemctl reload postfix
```

Créez maintenant le fichier **/etc/postfix/sasl/smtpd.conf** :

```
root@mail:~# vi /etc/postfix/sasl/smtpd.conf
root@mail:~# cat /etc/postfix/sasl/smtpd.conf
pwcheck_method: saslauthd
mech_list: PLAIN LOGIN
```

Pour tester l'authentification, vous devez envoyer un nom d'utilisateur et un mot de passe encodés en **base64**. Créez donc une chaîne de caractères encodés en base64 grâce à Perl en utilisant le format **utilisateur\0utilisateur\0motdepasse** :

```
root@mail:~# perl -MMIME::Base64 -e 'print encode_base64("trainee\0trainee\0trainee");'
```

```
dHJhaW5lZQB0cmFpbmVlAHRyYWluZWU=
```

> **Important** - Notez que les caractères **\0** séparent les champs et que le nom d'utilisateur est repété deux fois.

Re-démarrez le service **saslauthd** :

```
root@mail:~# systemctl restart saslauthd
root@mail:~# systemctl status saslauthd
● saslauthd.service - LSB: saslauthd startup script
   Loaded: loaded (/etc/init.d/saslauthd; generated; vendor preset: enabled)
   Active: active (running) since Wed 2019-01-23 10:09:54 CET; 7s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 11846 ExecStop=/etc/init.d/saslauthd stop (code=exited, status=0/SUCCESS)
  Process: 11862 ExecStart=/etc/init.d/saslauthd start (code=exited, status=0/SUCCESS)
    Tasks: 5 (limit: 4915)
   CGroup: /system.slice/saslauthd.service
           ├─11884 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5
           ├─11885 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5
           ├─11886 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5
           ├─11887 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5
           └─11888 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5

janv. 23 10:09:54 mail.i2tch.com systemd[1]: Stopped LSB: saslauthd startup script.
janv. 23 10:09:54 mail.i2tch.com systemd[1]: Starting LSB: saslauthd startup script...
janv. 23 10:09:54 mail.i2tch.com saslauthd[11862]: Starting SASL Authentication Daemon: saslauthd.
janv. 23 10:09:54 mail.i2tch.com systemd[1]: Started LSB: saslauthd startup script.
janv. 23 10:09:54 mail.i2tch.com saslauthd[11884]:                : master pid is: 11884
janv. 23 10:09:54 mail.i2tch.com saslauthd[11884]:                : listening on socket: /var/run/saslauthd/mux
```

Mettez l'utilisateur postfix dans ls groupe **sasl** :

```
root@mail:~# usermod -a -G sasl postfix
```

Testez saslauthd en utilisant la commande **testsaslauthd** :

```
root@mail:~# testsaslauthd -u trainee -p trainee
0: OK "Success."
```

Connectez-vous maintenant au serveur postfix sur le port 25 :

```
root@mail:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (Debian/GNU)
EHLO me
250-mail.i2tch.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH PLAIN dHJhaW5lZQB0cmFpbmVlAHRyYWluZWU=
235 2.7.0 Authentication successful
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Notez l'utilisation de la commande **EHLO**. EHLO est la version *Enhanced* (ESMTP) de **HELO**. Le serveur répond ensuite avec les extensions ESMTP supportées.

Dans le cas de l'exemple ci-dessus, on peut noter la présence des deux lignes **250-AUTH LOGIN PLAIN** et **250-AUTH=LOGIN PLAIN** qui indique que le serveur supporte le mécanisme AUTH.

Notez aussi l'utilisation de la commande AUTH PLAIN qui informe le serveur que les coordonnées de connexion vont être transmises sous forme d'un couple nom d'utilisateur/mot de passe encodés en **base64**.

Les autres extensions supportées dans l'exemple ci-dessus sont :

Extension	**Description**
250-PIPELINING	Service qui permet au client d'envoyer une nouvelle requête sans attendre la réponse à la requête précédente.
250-SIZE 10240000	La taille maximale en octets d'un message
250-VRFY	Service qui permet d'interroger directement le serveur SMTP pour savoir si une adresse existe.
250-ETRN	Service qui permet au serveur mail de demander au serveur mail du FAI de livrer ses messages.
250-ENHANCEDSTATUSCODES	Compatible **Enhanced Status Codes Registry**
250-8BITMIME	Service 8bit-MIMEtransport.
250 DSN	Service Delivery Status Notification (Accusés de réception).

Tester le Serveur SMTP Sortant

Envoyez un message en utilisant telnet à votre adresse d'email avec comme **Subject:** votre prénom :

```
root@mail:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (Debian/GNU)
EHLO me
250-mail.i2tch.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH PLAIN LOGIN
```

```
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH PLAIN dHJhaW5lZQB0cmFpbmVlAHRyYWluZWU=
235 2.7.0 Authentication successful
MAIL from: trainee@i2tch.com
250 2.1.0 Ok
RCPT to: hugh.norris@i2tch.eu
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Hugh
This is a test email
.
250 2.0.0 Ok: queued as A62F06057E
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Consultez maintenant la fin du fichier **/var/log/maillog**. Vous devez constater que votre message est parti. Par exemple :

```
root@mail:~# tail /var/log/mail.log
Jan 23 10:40:03 mail postfix/qmgr[12552]: A62F06057E: from=<trainee@i2tch.com>, size=337, nrcpt=1 (queue active)
Jan 23 10:40:03 mail postfix/smtp[12583]: connect to aspmx.l.google.com[2a00:1450:400c:c06::1a]:25: Network is
unreachable
Jan 23 10:40:04 mail postfix/smtp[12583]: A62F06057E: to=<hugh.norris@i2tch.eu>,
relay=aspmx.l.google.com[173.194.76.27]:25, delay=61, delays=60/0.01/0.65/0.45, dsn=5.7.1, status=bounced (host
aspmx.l.google.com[173.194.76.27] said: 550-5.7.1 [77.136.80.128] The IP you're using to send mail is not
authorized to 550-5.7.1 send email directly to our servers. Please use the SMTP relay at your 550-5.7.1 service
provider instead. Learn more at 550 5.7.1  https://support.google.com/mail/?p=NotAuthorizedError
t207si27379187wmt.144 - gsmtp (in reply to end of DATA command))
Jan 23 10:40:04 mail postfix/cleanup[12581]: 48A60605B1: message-id=<20190123094004.48A60605B1@mail.i2tch.com>
Jan 23 10:40:04 mail postfix/qmgr[12552]: 48A60605B1: from=<>, size=2800, nrcpt=1 (queue active)
```

```
Jan 23 10:40:04 mail postfix/bounce[12584]: A62F06057E: sender non-delivery notification: 48A60605B1
Jan 23 10:40:04 mail postfix/qmgr[12552]: A62F06057E: removed
Jan 23 10:40:04 mail postfix/local[12586]: 48A60605B1: to=<trainee@i2tch.com>, relay=local, delay=0.02,
delays=0/0.01/0/0, dsn=2.0.0, status=sent (delivered to command: procmail -a "$EXTENSION")
Jan 23 10:40:04 mail postfix/qmgr[12552]: 48A60605B1: removed
Jan 23 10:40:05 mail postfix/smtpd[12577]: disconnect from localhost[::1] ehlo=1 auth=1 mail=1 rcpt=1 data=1
quit=1 commands=6
```

Important : Notez que **aspmx.l.google.com** refuse le message à cause de l'adresse IP d'envoi.

Il est possible a tout moment de visualiser le contenu du spool de mail en utilisant la commande **mailq** qui est équivalente à la commande **sendmail bp** :

```
root@mail:~# mailq
Mail queue is empty
```

Important : Il est également possible de visualiser le contenu d'un message en utilisant la commande **postcat -vq [message-id]**.

TLS

Le codage **base64** n'est pas chiffré et necéssite l'utilisation de **TLS** (**T**ransport **L**ayer **S**ecurity).

Commencez par exécuter le script CA qui se trouve dans **/usr/lib/ssl/misc** :

```
root@mail:/usr/lib/ssl/misc# ./CA.pl -newca
```

```
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req  -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
.............+++++
.....................................+++++
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:fenestros
Verifying - Enter PEM pass phrase:fenestros
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:SURREY
Locality Name (eg, city) []:ADDLESTONE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:I2TCH LTD
Organizational Unit Name (eg, section) []:TRAINING
Common Name (e.g. server FQDN or YOUR name) []:i2tch.com
Email Address []:infos@i2tch.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:secret
An optional company name []:
==> 0
====
====
```

```
openssl ca  -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -
selfsign -extensions v3_ca -infiles ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:fenestros
Can't open ./demoCA/index.txt.attr for reading, No such file or directory
139740109301120:error:02001002:system library:fopen:No such file or
directory:../crypto/bio/bss_file.c:74:fopen('./demoCA/index.txt.attr','r')
139740109301120:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            c5:b1:b7:bd:b7:1a:f9:7b
        Validity
            Not Before: Jan 23 10:39:05 2019 GMT
            Not After : Jan 22 10:39:05 2022 GMT
        Subject:
            countryName               = GB
            stateOrProvinceName       = SURREY
            organizationName          = I2TCH LTD
            organizationalUnitName    = TRAINING
            commonName                = i2tch.com
            emailAddress              = infos@i2tch.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                24:F4:51:39:C5:64:D3:E6:D8:E8:D4:DB:D1:54:AF:2A:F7:25:8C:90
            X509v3 Authority Key Identifier:
                keyid:24:F4:51:39:C5:64:D3:E6:D8:E8:D4:DB:D1:54:AF:2A:F7:25:8C:90

            X509v3 Basic Constraints: critical
                CA:TRUE
Certificate is to be certified until Jan 22 10:39:05 2022 GMT (1095 days)

Write out database with 1 new entries
```

```
Data Base Updated
==> 0
====
CA certificate is in ./demoCA/cacert.pem
```

Vous obtiendrez deux fichiers - **cacert.pem** et **cakey.pem** :

```
root@mail:/usr/lib/ssl/misc# updatedb
root@mail:/usr/lib/ssl/misc# locate cacert.pem
/usr/lib/ssl/misc/demoCA/cacert.pem
root@mail:/usr/lib/ssl/misc# locate cakey.pem
/usr/lib/ssl/misc/demoCA/private/cakey.pem
```

Vous devez générer maintenant une clef privée ainsi qu'un **Certificate Signing Request** pour le serveur mail. Le **CSR (Certificate Signing Request)** doit alors être envoyé à une des sociétés faisant autorité en la matière afin que celle-ci puisse vous retourner votre certificat définitif. Ce service est payant. C'est ce certificat définitif qui est utilisé pour des connexions sécurisées.

```
root@mail:/usr/lib/ssl/misc# openssl req -new -nodes -keyout lel_clef.pem -out lel_req.pem
Generating a RSA private key
.................+++++
....+++++
writing new private key to 'lel_clef.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:SURREY
Locality Name (eg, city) []:ADDLESTONE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:I2TCH LTD
```

```
Organizational Unit Name (eg, section) []:TRAINING
Common Name (e.g. server FQDN or YOUR name) []:mail.i2tch.com
Email Address []:infos@i2tch.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Vous obtiendrez deux fichiers - **lel_clef.pem** et **lel_req.pem** :

```
root@mail:/usr/lib/ssl/misc# ls
CA.pl  demoCA  lel_clef.pem  lel_req.pem  tsget
```

Vous pouvez maintenant envoyé votre **CSR (Certificate Signing Request)**, **lel_req.pem**, à la société que vous avez choisie. Quand votre certificat **.crt** vous est retourné, copiez-le, ainsi que votre clé privée dans le répertoire **/etc/postfix/ssl**.

Sans passer par un prestataire externe, vous pouvez signer votre **CSR (Certificate Signing Request)** avec votre propre clef afin de générer votre certificat :

```
root@mail:/usr/lib/ssl/misc# openssl ca -out lel_cert.pem -infiles lel_req.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:fenestros
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            c5:b1:b7:bd:b7:1a:f9:7c
        Validity
            Not Before: Jan 23 12:09:31 2019 GMT
            Not After : Jan 23 12:09:31 2020 GMT
        Subject:
            countryName               = GB
            stateOrProvinceName       = SURREY
```

```
            organizationName          = I2TCH LTD
            organizationalUnitName    = TRAINING
            commonName                = mail.i2tch.com
            emailAddress              = infos@i2tch.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                F3:F9:04:23:4F:CB:03:42:A4:4B:B1:0C:77:2B:67:3D:6F:9B:C8:BB
            X509v3 Authority Key Identifier:
                keyid:24:F4:51:39:C5:64:D3:E6:D8:E8:D4:DB:D1:54:AF:2A:F7:25:8C:90

Certificate is to be certified until Jan 23 12:09:31 2020 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Important - Notez que le **commonName** est différent (i2tch.com <> mail.i2tch.com) ! Dans le cas contraire la base de données ne sera pas mise à jour et une erreur sera jetée.

Il convient ensuite de copier les fichiers lel_cert.pem, lel_clef.pem et cacert.pem dans le répertoire **/etc/postfix** puis de modifier les permissions :

```
root@mail:/usr/lib/ssl/misc# cp lel_cert.pem lel_clef.pem /etc/postfix
root@mail:/usr/lib/ssl/misc# cp /usr/lib/ssl/misc/demoCA/cacert.pem /etc/postfix
root@mail:/usr/lib/ssl/misc# chmod 644 /etc/postfix/lel_cert.pem /etc/postfix/cacert.pem
root@mail:/usr/lib/ssl/misc# chmod 400 /etc/postfix/lel_clef.pem
```

Pour activer **TLS** vous allez modifier votre fichier **/etc/postfix/main.cf** en y ajoutant les lignes suivantes :

```
...
############      TLS      ##############
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_sesson_cache
smtp_tls_security_level = may
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_sesson_cache
smtpd_tls_cert_file = /etc/postfix/lel_cert.pem
smtpd_tls_key_file = /etc/postfix/lel_clef.pem
smtpd_tls_received_header = yes
tls_random_source = dev:/dev/urandom
smtpd_tls_security_level = may
smtpd_tls_loglevel = 2
smtpd_tls_ask_ccert = no
```

Vous obtiendrez un résultat similaire à celui-ci :

```
root@mail:/usr/lib/ssl/misc# vi /etc/postfix/main.cf
root@mail:/usr/lib/ssl/misc# cat /etc/postfix/main.cf
#############CONFIG DE BASE##############
myhostname = mail.i2tch.com
mydomain= i2tch.com
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
relayhost =
```

```
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
#############   COMMANDES   ##############
mailbox_command = procmail -a "$EXTENSION"
############  REPERTOIRES  ##############
readme_directory = no
############      SASL     ##############
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
                                  reject_non_fqdn_sender,
                                  reject_non_fqdn_recipient,
                                  reject_unknown_sender_domain,
                                  reject_unknown_recipient_domain,
                                  reject_unauth_pipelining,
                                  reject_rbl_client zen.spamhaus.org,
                                  reject_rbl_client bl.spamcop.net,
                                  reject_rbl_client dnsbl.njabl.org,
                                  reject_rbl_client dnsbl.sorbs.net,
                                  permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = i2tch.com
smtpd_helo_required = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = cyrus
cyrus_sasl_config_path = /etc/postfix/sasl
```

```
############      TLS      ##############
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_sesson_cache
smtp_tls_security_level = may
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_sesson_cache
smtpd_tls_cert_file = /etc/postfix/lel_cert.pem
smtpd_tls_key_file = /etc/postfix/lel_clef.pem
smtpd_tls_received_header = yes
tls_random_source = dev:/dev/urandom
smtpd_tls_security_level = may
smtpd_tls_loglevel = 2
smtpd_tls_ask_ccert = no
```

Les directives ajoutées dans l'exemple ci-dessus sont :

Directive	**Description**
smtpd_tls_CAfile	Fichier contenant le certificat de l'autorité de certification de laquelle est issu le certificat du serveur SMTP de Postfix.
smtpd_tls_session_cache_database	Nom du fichier contenant le cache optionnel des sessions TLS du serveur SMTP de Postfix.
smtpd_tls_cert_file	Fichier contenant le certificat RSA du serveur SMTP de Postfix au format PEM.
smtpd_tls_key_file	Fichier contenat la clef privée RSA du serveur SMTP de Postfix au format PEM.
smtpd_tls_received_header	Requiert que le serveur SMTP de Postfix produise des en-têtes de message Received: qui incluent les informations à propos du protocole et du chiffrement utilisé ainsi que les champs CommonName des certificats client et de l'autorité dont il est issu.
tls_random_source	Source externe d'entropie pour le gestionnaire tlsmgr(8) du pool de générateurs en mémoire de nombres peudo-aléatoires (pseudo random number generator PRNG).
smtpd_tls_loglevel	Active l'enregistrement additionnel de l'activité TLS du serveur SMTP de Postfix. La valeur de deux enregistre les informations concernant la négociation et les certificats ainsi que les niveaux durant la négociation TLS.
smtpd_tls_ask_ccert	Demande au client SMTP distant un certificat client.

Important - Pour plus d'informations concernant les directives **smtp_tls_security_level** et **smtpd_tls_security_level**, consultez **cette page**.

Rechargez la configuration de postfix :

```
[root@mail misc]# systemctl reload postfix
```

Testez maintenant le serveur postfix afin de savoir si celui-ci a pris en compte **TLS** :

```
root@mail:/usr/lib/ssl/misc# cd ~
root@mail:~# openssl s_client -starttls smtp -connect mail.i2tch.com:25
CONNECTED(00000003)
depth=1 C = GB, ST = SURREY, O = I2TCH LTD, OU = TRAINING, CN = i2tch.com, emailAddress = infos@i2tch.com
verify error:num=19:self signed certificate in certificate chain
---
Certificate chain
 0 s:/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=mail.i2tch.com/emailAddress=infos@i2tch.com
   i:/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=i2tch.com/emailAddress=infos@i2tch.com
 1 s:/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=i2tch.com/emailAddress=infos@i2tch.com
   i:/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=i2tch.com/emailAddress=infos@i2tch.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIID9TCCAt2gAwIBAgIJAMWxt723Gvl8MA0GCSqGSIb3DQEBCwUAMHkxCzAJBgNV
BAYTAkdCMQ8wDQYDVQQIDAZTVVJSRVkxEjAQBgNVBAoMCUkyVENIIExURDERMA8G
A1UECwwIVFJBSU5JTkcxEjAQBgNVBAMMCWkydGNoLmNvbTEeMBwGCSqGSIb3DQEJ
ARYPaW5mb3NAaTJ0Y2guY29tMB4XDTE5MDEyMzEyMDkzMVoXDTIwMDEyMzEyMDkz
MVowfjELMAkGA1UEBhMCR0IxDzANBgNVBAgMBlNVUlJFWTESMBAGA1UECgwJSTJU
Q0ggTFREMREwDwYDVQQLDAhUUkFJTklORzEXMBUGA1UEAwwObWFpbC5pMnRjaC5j
b20xHjAcBgkqhkiG9w0BCQEWD2luZm9zQGkydGNoLmNvbTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAMUjVXTva9MmYwJPGxL3gV6Y6LhUS8+o80mHPRlr
xzuY9hezpNg3bL+25+XIGe3pEwDLMRSgYaP6HzxF4cxbDVaRxdhwXiznZzI6Ljcy
k6Bi/KDkVGuUMux/KicfhX2JofHM+07UZyITvqeaqU6by/WbpmD4EbwvT2/VhxHH
J03p9sauX8f3xVSa5faUvhC2ucpTGaaMMLqUag67s7qRQU90ve7OiQwswDFEdwdZ
6JaVcJ0wteVri+4ihsHGdwFBbaNkobIflXxLx7Xo30r/CCu5HjkMlv6XWZSQL5oc
zuwLQd/oUGOZhCsWWZ6ypngiUerlaDx6GYYFCMr2pryjFhcCAwEAAaN7MHkwCQYD
VR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlm
```

```
aWNhdGUwHQYDVR0OBBYEFPP5BCNPywNCpEuxDHcrZz1vm8i7MB8GA1UdIwQYMBaA
FCT0UTnFZNPm2OjU29FUryr3JYyQMA0GCSqGSIb3DQEBCwUAA4IBAQCWUS1mcgP2
zie/3h/g9gnZvBOnjixJzCS901zk21xss8lAAD4T5329xKxtFBKyYwHAFIoiiZ1I
lJx6IakZv4LjZvIY7TSYilD+5Bku+scJYS6Iyefjj1yGOIjMYFxN94TomXVgaYC8
PwtHCqPhF1VSzhUS3R5NvsyYrGBYPsFpcdLMXVTZRgfDyisHd/hF3CjMXY7TOYPr
/wQ2/0nmzhfvBZVeq9uNUns98C7T8KefsDZH7+YNOisvA61frz/8IOX/90Nuwdem
Z1uysTrMNQeO5vEe5eQxoYykNlwqC4Ecp/BUpALQn4iezN9J5McoO16gsQ/7qP4n
yjGpUW3uXYMl
-----END CERTIFICATE-----
subject=/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=mail.i2tch.com/emailAddress=infos@i2tch.com
issuer=/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=i2tch.com/emailAddress=infos@i2tch.com
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 2924 bytes and written 335 bytes
Verification error: self signed certificate in certificate chain
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 1FCA00669F61AFD1CEE2119D4F920CBAE69AC47A958A87A7A4D27F96322771D2
    Session-ID-ctx:
    Master-Key: 46D5E6962D0BF9BE84E03A6694F8B94B61BA28DEBC4AD5B41D91836FD1AFB55E6025F0EE3DEBEFE1CD0A72F759613400
    PSK identity: None
    PSK identity hint: None
    SRP username: None
```

```
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - a5 42 da 72 f2 87 ea a9-11 04 3c 7b c9 07 da 7a   .B.r......<{...z
    0010 - ba 2a 7c d8 26 78 e5 65-b1 04 59 c4 95 aa 48 3b   .*|.&x.e..Y...H;
    0020 - b0 ce cd aa 5f 78 5f ec-c9 69 c0 08 d2 3d 1a db   ...._x_..i...=..
    0030 - a8 9b 79 08 d6 b6 51 ab-0d 09 76 79 6e b7 b6 e2   ..y...Q...vyn...
    0040 - 69 69 8c b3 25 5a 20 97-23 b8 bb 50 9d 80 3c 8e   ii..%Z .#..P..<.
    0050 - 3d 92 e3 df d1 02 eb 22-1b 57 f0 2c 8a 07 97 a5   =......".W.,....
    0060 - 44 1a 08 c9 42 db 62 15-c4 df 48 ee 49 b9 6e 39   D...B.b...H.I.n9
    0070 - 7f 44 59 81 19 52 5b ed-91 2d e4 64 b2 2a 44 aa   .DY..R[..-.d.*D.
    0080 - ff 81 9f 19 4a a9 06 6c-d6 7e 3a 42 f7 2d 66 b9   ....J..l.~:B.-f.
    0090 - 16 89 16 c7 3a 18 2d b2-45 96 d7 1d f8 43 cc 49   ....:.-.E....C.I
    00a0 - 50 d8 6b 67 1b 40 40 fe-8b 42 a4 a2 81 1a 79 37   P.kg.@@..B....y7

    Start Time: 1548245777
    Timeout   : 7200 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
    Extended master secret: yes
---
250 DSN

QUIT
DONE
```

Important - Notez la présence de l'erreur 19 (self signed certificate in certificate chain).

Afin de configurer Postfix pour écouter sur les ports **tcp/465** et **tcp/587**, il convient d'ajouter les deux ligne suivantes au fichier **/etc/postfix/master.cf** :

```
...
# Port 465 pour SSL
```

```
465     inet    n       -       n       -       -       smtpd
# Port 587 pour TLS
587     inet    n       -       n       -       -       smtpd
...
```

Vous obtiendrez donc le résultat suivant :

```
root@mail:~# vi /etc/postfix/master.cf
root@mail:~# head -n 20 /etc/postfix/master.cf
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
# Port 465 pour SSL
465     inet    n       -       n       -       -       smtpd
# Port 587 pour TLS
587     inet    n       -       n       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
#tlsproxy  unix  -       -       y       -       0       tlsproxy
```

Rechargez les fichiers de configuration de Postfix :

```
[root@mail ~]# systemctl reload postfix
```

Utilisez la commande **netstat** pour vérifier que les ports soient à l'écoute :

```
root@mail:~# apt-get install net-tools
root@mail:~# netstat -lnp | grep 587
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN      12549/master
tcp6       0      0 :::587                  :::*                    LISTEN      12549/master
root@mail:~# netstat -lnp | grep 465
tcp        0      0 0.0.0.0:465             0.0.0.0:*               LISTEN      12549/master
tcp6       0      0 :::465                  :::*                    LISTEN      12549/master
```

LAB #5 - Configuration de l'Antispam SpamAssassin

SpamAssassin est une **extension** pour postfix permettant de vérifier chaque message entrant afin d'identifier les messages **SPAM** en passant tous les messages par des tests. En fonction du résultat de ces tests, il attribue un score au message, chaque test rajoutant des points au score.

Installation

Installez SpamAssassin en utilisant apt :

```
root@mail:~# apt-get install spamassassin
```

Configuration

Ouvrez le fichier de configuration de SpamAssassin, **/etc/mail/spamassassin/local.cf** en édition :

- Insérez la ligne **trusted_networks 10.0.2.** pour que celle-ci reflète l'adressage de votre propre réseau.
- Insérez la ligne **ok_languages all**. Cette ligne indique les langues que vous acceptez de recevoir. Vous pouvez également mettre ici **fr** et/ou **en** pour ne recevoir que des messages en français et/ou en anglais.
- Insérez la ligne **required_score 3.0**. Cette ligne définit le score au delà duquel les mails sont considérés comme du spam,

- Insérez la ligne **rewrite_header Subject [SPAM]**. Cette ligne place la chaîne **[SPAM]** au début de l'objet d'un message considéré comme du SPAM,
- Insérez la ligne **report_safe 0**.

Vous obtiendrez un résutat similaire à celui-ci :

```
root@mail:~# vi /etc/mail/spamassassin/local.cf
root@mail:~# cat /etc/mail/spamassassin/local.cf
# This is the right place to customize your installation of SpamAssassin.
#
# See 'perldoc Mail::SpamAssassin::Conf' for details of what can be
# tweaked.
#
# Only a small subset of options are listed below
#
###########################################################################

#   Add *****SPAM***** to the Subject header of spam e-mails
#
# rewrite_header Subject *****SPAM*****
rewrite_header Subject [SPAM]


#   Save spam messages as a message/rfc822 MIME attachment instead of
#   modifying the original message (0: off, 2: use text/plain instead)
#
# report_safe 1
report_safe 0


#   Set which networks or hosts are considered 'trusted' by your mail
#   server (i.e. not spammers)
#
# trusted_networks 212.17.35.
```

```
trusted_networks 10.0.2.


#   Set file-locking method (flock is not safe over NFS, but is faster)
#
# lock_method flock


#   Set the threshold at which a message is considered spam (default: 5.0)
#
# required_score 5.0
required_score 3.0


#   Use Bayesian classifier (default: 1)
#
# use_bayes 1


#   Bayesian classifier auto-learning (default: 1)
#
# bayes_auto_learn 1


#   Set headers which may provide inappropriate cues to the Bayesian
#   classifier
#
# bayes_ignore_header X-Bogosity
# bayes_ignore_header X-Spam-Flag
# bayes_ignore_header X-Spam-Status


#   Whether to decode non- UTF-8 and non-ASCII textual parts and recode
#   them to UTF-8 before the text is given over to rules processing.
```

```
#
# normalize_charset 1

#   Some shortcircuiting, if the plugin is enabled
#
ifplugin Mail::SpamAssassin::Plugin::Shortcircuit
#
#   default: strongly-whitelisted mails are *really* whitelisted now, if the
#   shortcircuiting plugin is active, causing early exit to save CPU load.
#   Uncomment to turn this on
#
# shortcircuit USER_IN_WHITELIST       on
# shortcircuit USER_IN_DEF_WHITELIST   on
# shortcircuit USER_IN_ALL_SPAM_TO     on
# shortcircuit SUBJECT_IN_WHITELIST    on

#   the opposite; blacklisted mails can also save CPU
#
# shortcircuit USER_IN_BLACKLIST       on
# shortcircuit USER_IN_BLACKLIST_TO    on
# shortcircuit SUBJECT_IN_BLACKLIST    on

#   if you have taken the time to correctly specify your "trusted_networks",
#   this is another good way to save CPU
#
# shortcircuit ALL_TRUSTED             on

#   and a well-trained bayes DB can save running rules, too
#
# shortcircuit BAYES_99                spam
# shortcircuit BAYES_00                ham

endif # Mail::SpamAssassin::Plugin::Shortcircuit
ok_languages all
```

A faire - Consultez le manuel de spamassassin pour connaître la signification de la directive **report_safe**.

Activez et démarrez le service spamassissin :

```
root@mail:~# systemctl status spamassassin
● spamassassin.service - Perl-based spam filter using text analysis
   Loaded: loaded (/lib/systemd/system/spamassassin.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
root@mail:~# systemctl enable spamassassin
Synchronizing state of spamassassin.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable spamassassin
root@mail:~# systemctl start spamassassin
root@mail:~# systemctl status spamassassin
● spamassassin.service - Perl-based spam filter using text analysis
   Loaded: loaded (/lib/systemd/system/spamassassin.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2019-01-23 13:38:59 CET; 3s ago
  Process: 19328 ExecStart=/usr/sbin/spamd -d --pidfile=/var/run/spamd.pid $OPTIONS (code=exited,
status=0/SUCCESS)
 Main PID: 19330 (spamd)
    Tasks: 3 (limit: 4915)
   CGroup: /system.slice/spamassassin.service
           ├─19330 /usr/bin/perl -T -w /usr/sbin/spamd -d --pidfile=/var/run/spamd.pid --create-prefs --max-
children 5 --helper-home-dir
           ├─19331 spamd child
           └─19332 spamd child

janv. 23 13:38:58 mail.i2tch.com spamd[19328]: logger: removing stderr method
janv. 23 13:38:58 mail.i2tch.com spamd[19330]: config: failed to parse, now a plugin, skipping, in
"/etc/spamassassin/local.cf": ok_languages all
janv. 23 13:38:59 mail.i2tch.com spamd[19330]: zoom: able to use 346/346 'body_0' compiled rules (100%)
```

```
janv. 23 13:38:59 mail.i2tch.com spamd[19330]: spamd: server started on IO::Socket::IP [::1]:783, IO::Socket::IP
[127.0.0.1]:783 (running version 3.4.2)
janv. 23 13:38:59 mail.i2tch.com spamd[19330]: spamd: server pid: 19330
janv. 23 13:38:59 mail.i2tch.com systemd[1]: Started Perl-based spam filter using text analysis.
janv. 23 13:38:59 mail.i2tch.com spamd[19330]: spamd: server successfully spawned child process, pid 19331
janv. 23 13:38:59 mail.i2tch.com spamd[19330]: spamd: server successfully spawned child process, pid 19332
janv. 23 13:38:59 mail.i2tch.com spamd[19330]: prefork: child states: IS
janv. 23 13:38:59 mail.i2tch.com spamd[19330]: prefork: child states: II
```

LAB #6 - Configuration du Mandataire MailScanner

MailScanner est un mandataire qui est muni d'un système anti-spam et qui est capable d'utiliser la plupart des logiciels anti-virus.

> **Important** - MailScanner est utilisé dans plus de 225 pays sur plus de 40 000 sites et a été téléchargé plus de 1.3 millions de fois.

Installation

Téléchargez le fichier **MailScanner-5.1.2-2.deb.tar.gz** :

```
root@mail:~# wget https://s3.amazonaws.com/msv5/release/MailScanner-5.1.2-2.deb.tar.gz
--2019-01-23 13:56:44--  https://s3.amazonaws.com/msv5/release/MailScanner-5.1.2-2.deb.tar.gz
Résolution de s3.amazonaws.com (s3.amazonaws.com)… 52.216.86.197
Connexion à s3.amazonaws.com (s3.amazonaws.com)|52.216.86.197|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 452451 (442K) [application/x-gzip]
Sauvegarde en : « MailScanner-5.1.2-2.deb.tar.gz »
```

```
MailScanner-5.1.2-2.deb.tar.gz
100%[=======================================================================================>] 441,85K   580KB/s
in 0,8s

2019-01-23 13:56:46 (580 KB/s) – « MailScanner-5.1.2-2.deb.tar.gz » sauvegardé [452451/452451]
```

et désarchivez-le :

```
root@mail:~# tar xvf MailScanner-5.1.2-2.deb.tar.gz
MailScanner-5.1.2-2/
MailScanner-5.1.2-2/patch.diff
MailScanner-5.1.2-2/MailScanner-5.1.2-2-noarch.deb
MailScanner-5.1.2-2/changelog
MailScanner-5.1.2-2/LICENSE
MailScanner-5.1.2-2/install.sh
MailScanner-5.1.2-2/README
```

Placez-vous dans le répertoire **cd MailScanner-5.1.2-2** et exécutez le script **install.sh**. Ce script a pour but de construire les DEBs nécessaires pour l'installation puis de les installer :

```
root@mail:~# cd MailScanner-5.1.2-2
root@mail:~/MailScanner-5.1.2-2# ./install.sh

MailScanner Installation for Debian Based Systems


This will INSTALL or UPGRADE the required software for MailScanner on Debian based systems
via the Apt package manager. Supported distributions are Debian and associated variants
such as Ubuntu. Internet connectivity is required for this installation script to execute.

WARNING - Make a backup of any custom configuration files if upgrading - WARNING

You may press CTRL + C at any time to abort the installation. Note that you may see
some errors during the perl module installation. You may safely ignore errors regarding
```

```
failed tests for optional packages.

When you are ready to continue, press return ...
[Entrée]



Do you want to install a Mail Transfer Agent (MTA)?

I can install an MTA via the apt package manager to save you the trouble of having to do
this later. If you plan on using an MTA that is not listed below, you will have install
it manually yourself if you have not already done so.

1 - sendmail
2 - postfix
3 - exim
N - Do not install

Recommended: 1 (sendmail)

Install an MTA? [1] : N
[Entrée]



Do you want to install or update ClamAV during this installation process?

This package is recommended unless you plan on using a different virus scanner.
Note that you may use more than one virus scanner at once with MailScanner.

Even if you already have ClamAV installed you should select this option so I
will know to check the clamav-wrapper and make corrections if required.

Recommended: Y (yes)

Install or update ClamAV? [n/Y] : Y
```

```
[Entrée]


Do you want to install missing perl modules via CPAN?

I will attempt to install Perl modules via apt, but some may not be unavailable during the
installation process. Missing modules will likely cause MailScanner to malfunction.

Recommended: Y (yes)

Install missing Perl modules via CPAN? [n/Y] : Y
[Entrée]


Do you want to ignore MailScanner dependencies?

This will force install the MailScanner .deb package regardless of missing
dependencies. It is highly recommended that you DO NOT do this unless you
are debugging.

Recommended: N (no)

Ignore MailScanner dependencies (nodeps)? [y/N] : N
[Entrée]


Do you want to create a RAMDISK?

This will create a mount in /etc/fstab that attaches the processing
directory /var/spool/MailScanner/incoming to a RAMDISK, which greatly
increases processing speed at the cost of the reservation of some of
the system RAM. The size depends on the number of MailScanner children,
the number of messages per batch, and incoming email volume.
```

```
Specify a size in MB or leave blank for none.

Suggestions:
        None        0
        Small        256
        Medium        512
        Large        1024 or 2048
        Enterprise    4096 or 8192

Example: 1024

Specify a RAMDISK size? [0] : 0
[Entrée]
```

> **Important** - Dans le cas d'un système en production, il est préférable de répondre **512** à la dernière question.

A la question concernant **Sendmail::PMilter**, réppondez **yes**. Dans le cas contraire MailScanner ne fonctionnera **pas** :

```
The Sendmail::PMilter distribution includes a module that supplies a
compatibility interface emulating the standard Sendmail::Milter API,
rather than using the native libmilter (which is not compatible
with modern Perl threads).

Choose "no" below ONLY IF the standard Sendmail::Milter package is
installed or will be installed.  Otherwise, the compatibility
interface MUST be installed, as it is needed for Sendmail::PMilter
to function properly.

Do you wish to install the Sendmail::Milter interface? [yes] yes
```

A l'issu de l'installation, vous obtiendrez un résultat similaire à celui-ci :

```
...
Installing the MailScanner .deb package ...
Sélection du paquet mailscanner précédemment désélectionné.
(Lecture de la base de données... 104828 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../MailScanner-5.1.2-2-noarch.deb ...
Dépaquetage de mailscanner (5.1.2-2) ...
Paramétrage de mailscanner (5.1.2-2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/mailscanner.service →
/lib/systemd/system/mailscanner.service.

------------------------------------------------------------
Installation Complete

See http://www.mailscanner.info for more information and
support via the MailScanner mailing list.


Review: Set your preferences in /etc/MailScanner/MailScanner.conf
and review /etc/MailScanner/defaults
```

Configuration du couple MailScanner/Postfix

Arrêtez le service postfix :

```
root@mail:~/MailScanner-5.1.2-2# systemctl stop postfix
```

Editez ensuite **/etc/postfix/main.cf** et ajoutez les lignes suivantes à la fin du fichier :

```
...
############ HEADER CHECKS ###############
```

```
header_checks = regexp:/etc/postfix/header_checks
```

Vous obtiendrez :

```
root@mail:~/MailScanner-5.1.2-2# vi /etc/postfix/main.cf
root@mail:~/MailScanner-5.1.2-2# cat /etc/postfix/main.cf
#############CONFIG DE BASE##############
myhostname = mail.i2tch.com
mydomain= i2tch.com
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
relayhost =
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
############   COMMANDES   ##############
mailbox_command = procmail -a "$EXTENSION"
############  REPERTOIRES  ##############
readme_directory = no
############      SASL     ##############
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
                                  reject_non_fqdn_sender,
```

```
                                    reject_non_fqdn_recipient,
                                    reject_unknown_sender_domain,
                                    reject_unknown_recipient_domain,
                                    reject_unauth_pipelining,
                                    reject_rbl_client zen.spamhaus.org,
                                    reject_rbl_client bl.spamcop.net,
                                    reject_rbl_client dnsbl.njabl.org,
                                    reject_rbl_client dnsbl.sorbs.net,
                                    permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = i2tch.com
smtpd_helo_required = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = cyrus
cyrus_sasl_config_path = /etc/postfix/sasl
############      TLS      ##############
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_sesson_cache
smtp_tls_security_level = may
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_sesson_cache
smtpd_tls_cert_file = /etc/postfix/lel_cert.pem
smtpd_tls_key_file = /etc/postfix/lel_clef.pem
smtpd_tls_received_header = yes
tls_random_source = dev:/dev/urandom
smtpd_tls_security_level = may
smtpd_tls_loglevel = 2
smtpd_tls_ask_ccert = no
############ HEADER CHECKS ###############
header_checks = regexp:/etc/postfix/header_checks
```

A Faire - Pour plus d'informations concernant les directives, consultez **cette page**.

Créez ensuite **/etc/postfix/header_checks** en ajoutant les lignes suivantes :

```
root@mail:~/MailScanner-5.1.2-2# vi /etc/postfix/header_checks
root@mail:~/MailScanner-5.1.2-2# cat /etc/postfix/header_checks
/^Received:/ HOLD
/^User-Agent:/              IGNORE
```

Le but de la première ligne est de placer tous les messages entrant dans le répertoire **/var/spool/postfix/hold** afin de les traiter par MailScanner.

Le but de la deuxième ligne est de retirer la ligne commençant par **User-Agent:** des en-têtes des messages sortants.

```
root@mail:~/MailScanner-5.1.2-2# ls /var/spool/postfix
active  bounce    corrupt  defer    deferred  dev  etc  flush  hold  incoming  lib    maildrop  pid  private
public    saved  trace  usr
```

Comprendre la fonction des répertoires dans **/var/spool/postfix** nécessite une compréhension des processus principaux de postfix :

Processus	**Description**
master	Processus central de postfix. Il lance les autres processus. Il est lancé par root. Ses paramètres de configuration se trouvent dans le fichier **/etc/postfix/master.cf**
qmgr	Processus qui lit la queue **incoming** et place une partie des messages dans **active**. Ensuite il efface les messages où le traitement s'est bien passé. Dans le cas contraire, il place les messages dans **deferred**.
pickup	Processus qui attend d'être informé par **postdrop** de la présence de nouveaux messages dans le répertoire **maildrop**. Il passe ensuite les messages au processus **cleanup**.
smtpd	Processus qui reçoit les messages de l'extérieur et les passe au processus **cleanup**.
cleanup	Processus qui reçoit les messages de **pickup** ou de **smtpd** et qui les complète en termes de champs manquants (p.e. From: To: etc) tout en éliminant les doublons d'adresses destinataires. Il délègue au processus **trivial-rewrite** la tâche de transformer les adresses de l'enveloppe et des en-têtes d'adresses de type nom@fqdn.extension. Il place les messages traités dans le répertoire **incoming** et informe le processus **qmgr** qu'il faut examiner ce dernier.

Processus	Description
bounce	Processus qui délivre des messages de notification en cas d'échec définitif, de remise différée, de remise avec succès ou de vérifications d'adresses. IL maintient dans le répertoire **bounce** des informations sur les raisons des rejets des messages.
defer	Un alias du processus bounce qui maintient dans le répertoire **defer** les informations d'explications des raisons des messages différés.
trace	Un alias du processus bounce qui maintient dans le répertoire **trace** les informations de suivi de la remise des messages si ces informations ont été demandées en utilisant la commande **sendmail -bv** ou **sendmail -v**.
flush	Processus qui constitue une liste de messages, corréspondants à la directive du fichier **/etc/postfix/main.cf fast_flush_domain**, qui vont être traités plus prioritairement.
trivial-rewrite	Voir les processus **cleanup** et **qmgr**.
verify	Processus qui maintient une base d'addresses connues valides ou invalides.
scache	Processus qui maintient un cache des serveurs extérieurs où le processus smtpd a pu se connecter. Ces informations sont gardés pendant le temps spécifié par la directive **max_idle**.
anvil	Processus qui est chargé de la collecte des statistiques du nombre de connexions et de requêtes éffectuées par chaque client.
showcase	Processus qui rapporte l'état des files d'attente.

Après avoir vu les processus de postfix, nous pouvons se concentrer sur les répertoires présents dans **/var/spool/postfix** :

Répertoire	Contenu
active	Répertoire de file d'attente. Contient les messages en cours de traitement. En réalité ce répertoire est vide car les messages concernés sont tous en mémoire.
bounce	Répertoire contenant les raisons des rejets des messages.
corrupt	Répertoire contenant des messages corrompus.
defer	Répertoire de stockage temporaire. Contient les informations sur la raison des échecs des messages qui se trouvent dans le répertoire **deferred**.
deferred	Répertoire de file d'attente. Contient des sous-répertoires qui contiennent les messages qui n'ont pas pu être remis. Chaque sous-répertoire est nommé après le premier caractère de la **Queue ID** du message.
flush	Répertoire utilisé par le processus **flush**.
hold	Répertoire de stockage temporaire. Voir ci-dessus.
incoming	Répertoire de file d'attente. Contient les messages placés par le processus **cleanup**.
maildrop	Répertoire de stockage temporaire. Contient des messages crées localement.
pid	Répertoire de stockage temporaire. Contient les PID des processus postfix lancés.
private	Répertoire contenant une liste de sockets disponibles pour des utilisateurs priviligiés.

Répertoire	Contenu
public	Répertoire contenant une liste de sockets disponibles pour tout le monde.
trace	Répertoire utilisé par le processus **trace**.

Ouvrez maintenant le fichier **/etc/MailScanner/MailScanner.conf**.

Ce fichier doit être modifié pour fonctionner avec **postfix** et **clamav**. Recherchez les directives suivantes et modifiez-les comme indiqué :

1. Run As User = postfix
2. Run As Group = postfix
3. Incoming Queue Dir = /var/spool/postfix/hold
4. Outgoing Queue Dir = /var/spool/postfix/incoming
5. MTA = postfix
6. SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin
7. Virus Scanners = clamav
8. Notify Senders Of Viruses = yes
9. Spam Subject Text = [SPAM]
10. High Scoring Spam Subject Text = [SPAM]
11. Required SpamAssassin Score = 3

Ces directives indiquent que :

- Lignes 1 et 2 octroient à MailScanner les mêmes droits que postfix,
- Ligne 3 indique à MailScanner où il va trouver les messages à traiter,
- Ligne 4 indique où MailScanner doit mettre les messages à la fin de son traitement de ces derniers,
- Ligne 5 indique à MailScanner de travailler avec postfix,
- Ligne 6 - indique à MailScanner qu'il doit utiliser clamav pour examiner les messages,
- Ligne 7 - indique que le destinataire d'un message contenant un virus doit être informé de l'adresse de l'expéditeur,
- Lignes 8, 9 et 10 - assurent la compatibilité avec la configuration de et Spamassassin.

Créez le répertoire **/var/spool/MailScanner/spamassassin** et donnez les droits à postfix :

```
root@mail:~/MailScanner-5.1.2-2# mkdir /var/spool/MailScanner/spamassassin
root@mail:~/MailScanner-5.1.2-2# chown postfix:postfix /var/spool/MailScanner/spamassassin
```

Ouvrez maintenant le fichier **/etc/MailScanner/virus.scanners.conf** :

```
root@mail:~/MailScanner-5.1.2-2# cat /etc/MailScanner/virus.scanners.conf
# This is a list of the names of the virus scanning engines, along with the
# filename of the command or script to run to invoke each one.
# Three fields:
#  1.  Name of virus scanner as known by MailScanner. Do not change this.
#  2.  Location of -wrapper script. You should not need to change this.
#  3.  Installation directory of virus scanner. This does not usually include
#      any "bin" directory in the path to the scanner program itself.
# You can test a -wrapper script with a command like this:
#
#      /usr/lib/MailScanner/wrapper/clamav-wrapper /usr /tmp
#
# That command will attempt to scan /tmp using clamscan. If it works you
# should see some sensible output. If it fails, you will probably just see
# an error message such as "Command not found" or similar.
#
# updated 21 October 2018 - Shawn Iverson
#

avg             /usr/lib/MailScanner/wrapper/avg-wrapper            /usr/local4
avast           /usr/lib/MailScanner/wrapper/avast-wrapper            /bin
bitdefender     /usr/lib/MailScanner/wrapper/bitdefender-wrapper     /opt/BitDefender
clamav          /usr/lib/MailScanner/wrapper/clamav-wrapper             /usr
clamd           /bin/false                                            /usr
clamavmodule    /bin/false                                            /usr/share/perl5/ClamAV
esets           /usr/lib/MailScanner/wrapper/esets-wrapper            /opt/eset/esets/sbin
f-secure        /usr/lib/MailScanner/wrapper/f-secure-wrapper        /opt/f-secure/fsav
generic         /usr/lib/MailScanner/wrapper/generic-wrapper        /dev/null
sophos          /usr/lib/MailScanner/wrapper/sophos-wrapper             /opt/sophos-av
sophossavi      /bin/false                                            /tmp
none            /bin/false                                            /dev/null
drweb           /usr/lib/MailScanner/wrapper/drweb-wrapper            /usr/bin
```

```
kaspersky       /usr/lib/MailScanner/wrapper/kaspersky-wrapper        /opt/kaspersky/klms
```

> **Important** - Dans la troisième colonne sont indiqués des chemins. C'est dans le chemin indiqué, ou bien dans le sous-répertoire /bin du chemin indiqué que MailScanner cherche l'exécutable de l'anti-virus concerné.

Vérifiez maintenant le **wrapper** utilisé pour appeler l'anti-virus clamav par MailScanner en testant le répertoire **/tmp** :

```
root@mail:~/MailScanner-5.1.2-2# /usr/lib/MailScanner/wrapper/clamav-wrapper /usr /tmp
/tmp/.X0-lock: OK
/tmp/main.cf: OK

----------- SCAN SUMMARY -----------
Known viruses: 6779278
Engine version: 0.100.2
Scanned directories: 1
Scanned files: 2
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 15.586 sec (0 m 15 s)
```

Finalement, **postfix** a besoin d'avoir accès aux répertoires suivants :

- /var/spool/MailScanner/incoming
- /var/spool/MailScanner/quarantine

Modifiez donc le propriétaire ainsi que le groupe :

```
[root@mail MailScanner-5.1.2-2]# chown -R postfix.postfix /var/spool/MailScanner/incoming
[root@mail MailScanner-5.1.2-2]# chown -R postfix.postfix /var/spool/MailScanner/quarantine
```

Créez le fichier **/var/spool/postfix/.pyzor** suivant necéssaire pour les tests **pyzor** ;

```
[root@mail MailScanner-5.1.2-2]# cd ~
root@mail:~# vi /var/spool/postfix/.pyzor
root@mail:~# cat /var/spool/postfix/.pyzor
public.pyzor.org:24441
```

Modifiez le droits sur ce fichier afin que postfix puisse y avoir accès :

```
root@mail:~# chown -R postfix /var/spool/postfix/.pyzor
```

Afin de pouvoir démarrer MailScanner, il est necéssaire d'éditer le fichier **/etc/MailScanner/defaults** en modificant la valeur de la variable **run_mailscanner** à **1** :

```
root@mail:~# vi /etc/MailScanner/defaults
root@mail:~# head /etc/MailScanner/defaults
# MailScanner Run Options
#
# This file controls the system level behavior of MailScanner.
#
# Enable MailScanner Daemon
#
# Change this to 1 to allow the MailScanner daemon to run.
# 0 = off, 1 = on
#
run_mailscanner=1
```

Démarrez le service MailScanner :

```
root@mail:~# systemctl status mailscanner
● mailscanner.service - LSB: MailScanner daemon
   Loaded: loaded (/usr/lib/MailScanner/init/ms-init; enabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:systemd-sysv-generator(8)
```

```
root@mail:~# systemctl enable mailscanner
root@mail:~# systemctl start mailscanner
root@mail:~# systemctl status mailscanner
● mailscanner.service - LSB: MailScanner daemon
   Loaded: loaded (/usr/lib/MailScanner/init/ms-init; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2019-01-23 14:48:04 CET; 2s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 1963 ExecStart=/usr/lib/MailScanner/init/ms-init start (code=exited, status=0/SUCCESS)
 Main PID: 2501 (MailScanner: st)
    Tasks: 2 (limit: 4915)
   CGroup: /system.slice/mailscanner.service
           ├─2501 MailScanner: starting children
           └─2502 MailScanner: starting children

janv. 23 14:48:04 mail.i2tch.com root[2504]: MailScanner started
janv. 23 14:48:04 mail.i2tch.com MailScanner[2502]: Reading configuration file /etc/MailScanner/MailScanner.conf
janv. 23 14:48:04 mail.i2tch.com ms-init[1963]: MailScanner started with process id 2501
janv. 23 14:48:04 mail.i2tch.com systemd[1]: Started LSB: MailScanner daemon.
janv. 23 14:48:04 mail.i2tch.com MailScanner[2502]: Reading configuration file /etc/MailScanner/conf.d/README
janv. 23 14:48:04 mail.i2tch.com MailScanner[2502]: Read 1500 hostnames from the phishing whitelist
janv. 23 14:48:04 mail.i2tch.com MailScanner[2502]: Read 16624 hostnames from the phishing blacklists
janv. 23 14:48:05 mail.i2tch.com MailScanner[2502]: Using SpamAssassin results cache
janv. 23 14:48:05 mail.i2tch.com MailScanner[2502]: Connected to SpamAssassin cache database
janv. 23 14:48:05 mail.i2tch.com MailScanner[2502]: Enabling SpamAssassin auto-whitelist functionality...
```

Démarrez le service postfix :

```
root@mail:~# systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Wed 2019-01-23 14:26:54 CET; 22min ago
 Main PID: 12550 (code=exited, status=0/SUCCESS)

janv. 23 10:24:19 mail.i2tch.com systemd[1]: Starting Postfix Mail Transport Agent...
```

```
janv. 23 10:24:19 mail.i2tch.com systemd[1]: Started Postfix Mail Transport Agent.
janv. 23 13:15:57 mail.i2tch.com systemd[1]: Reloading Postfix Mail Transport Agent.
janv. 23 13:15:57 mail.i2tch.com systemd[1]: Reloaded Postfix Mail Transport Agent.
janv. 23 13:21:07 mail.i2tch.com systemd[1]: Reloading Postfix Mail Transport Agent.
janv. 23 13:21:07 mail.i2tch.com systemd[1]: Reloaded Postfix Mail Transport Agent.
janv. 23 14:26:54 mail.i2tch.com systemd[1]: Stopped Postfix Mail Transport Agent.
root@mail:~# systemctl start postfix
root@mail:~# systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
   Active: active (exited) since Wed 2019-01-23 14:49:14 CET; 1s ago
  Process: 2697 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 2697 (code=exited, status=0/SUCCESS)

janv. 23 14:49:14 mail.i2tch.com systemd[1]: Starting Postfix Mail Transport Agent...
janv. 23 14:49:14 mail.i2tch.com systemd[1]: Started Postfix Mail Transport Agent.
```

Procédez ensuite à une envoi de test à votre serveur postfix :

```
root@mail:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (Debian/GNU)
EHLO me
250-mail.i2tch.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
```

```
250-8BITMIME
250 DSN
AUTH PLAIN dHJhaW5lZQB0cmFpbmVlAHRyYWluZWU=
235 2.7.0 Authentication successful
MAIL from: root@i2tch.com
250 2.1.0 Ok
RCPT to: mickey.mouse@i2tch.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: MailScanner test
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
.
250 2.0.0 Ok: queued as AEC6661B63
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Important - La chaîne de caractères **XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X** est une chaîne de test qui indique à MailScanner et SpamAssassin que le massage est du spam.

Consultez la fin du fichier **/var/log/mail.log** :

```
root@mail:~# tail /var/log/mail.log
Jan 23 14:49:52 mail postfix/tlsmgr[2707]: tlsmgr_cache_run_event: start TLS smtpd session cache cleanup
Jan 23 14:49:53 mail postfix/smtpd[2705]: connect from localhost[::1]
Jan 23 14:50:26 mail postfix/smtpd[2705]: AEC6661B63: client=localhost[::1], sasl_method=PLAIN,
sasl_username=trainee@i2tch.com
Jan 23 14:50:44 mail postfix/cleanup[2710]: AEC6661B63: hold: header Received: from me (localhost [IPv6:::1])??by
mail.i2tch.com (Postfix) with ESMTPA id AEC6661B63??for <mickey.mouse@i2tch.com>; Wed, 23 Jan 2019 14:50:17 +0100
```

```
(CET) from localhost[::1]; from=<root@i2tch.com> to=<mickey.mouse@i2tch.com> proto=ESMTP helo=<me>
Jan 23 14:50:44 mail postfix/cleanup[2710]: AEC6661B63: message-id=<20190123135026.AEC6661B63@mail.i2tch.com>
Jan 23 14:50:46 mail MailScanner[2519]: New Batch: Scanning 1 messages, 1068 bytes
Jan 23 14:50:46 mail MailScanner[2519]: Virus and Content Scanning: Starting
Jan 23 14:50:48 mail postfix/smtpd[2705]: disconnect from localhost[::1] ehlo=1 auth=1 mail=1 rcpt=1 data=1
quit=1 commands=6
Jan 23 14:50:50 mail MailScanner[2519]: Spam Checks: Found 1 spam messages
Jan 23 14:50:50 mail MailScanner[2519]: Deleted 1 messages from processing-database
```

Important - Notez la présence de la ligne suivante : **Jan 23 14:50:50 mail MailScanner[2519]: Spam Checks: Found 1 spam messages**.

LAB #7 - Installation du Serveur IMAP Dovecot/Cyrus-Imapd

Cas #1 - Dovecot

Nous souhaitons que le serveur mail fournisse un accès en **POP3** et en **IMAP** aux clients sur le réseau. Le serveur postfix n'est pas un serveur POP3 ou IMAP. Le serveur POP3/IMAP est inclut dans le paquet **dovecot**.

Le fichier principal de configuration de Dovecot 2 est **/etc/dovecot/dovecot.conf**. Les directives actives de ce fichier sont :

```
!include_try /usr/share/dovecot/protocols.d/*.protocol
dict {
  #quota = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
  #expire = sqlite:/etc/dovecot/dovecot-dict-sql.conf.ext
}
!include conf.d/*.conf
!include_try local.conf
```

Editez le fichier **/etc/dovecot/dovecot.conf** en y ajoutant la directive **mail_privileged_group** :

```
root@mail:~# vi /etc/dovecot/dovecot.conf
root@mail:~# cat /etc/dovecot/dovecot.conf
!include_try /usr/share/dovecot/protocols.d/*.protocol
dict {
  #quota = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
  #expire = sqlite:/etc/dovecot/dovecot-dict-sql.conf.ext
}
mail_privileged_group = mail
!include conf.d/*.conf
!include_try local.conf
```

La directive **!include conf.d/*.conf** fait appel aux fichiers de configuration se trouvant dans le répertoire **/etc/dovecot/conf.d** :

```
root@mail:~# ls /etc/dovecot/conf.d
10-auth.conf      10-master.conf      15-mailboxes.conf  90-quota.conf              auth-master.conf.ext    auth-
system.conf.ext
10-director.conf  10-ssl.conf         20-pop3.conf     auth-checkpassword.conf.ext  auth-passwdfile.conf.ext
auth-vpopmail.conf.ext
10-logging.conf   10-tcpwrapper.conf  90-acl.conf    auth-deny.conf.ext          auth-sql.conf.ext
10-mail.conf      15-lda.conf          90-plugin.conf     auth-dict.conf.ext          auth-static.conf.ext
```

Vérifiez que le fichier **/etc/dovecot/conf.d/10-mail.conf** contient la ligne suivante :

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

> **Important** - Dovecot va regarder dans le répertoire **/var/mail/%u**, où %u représente le nom de l'utilisateur, pour trouver des messages non-lus. Quand un message a été lu, il est transféré dans le répertoire **~/mail** de l'utilisateur concerné. Notez que /var/mail/ est un

lien symbolique vers /var/spool/mail.

Les directives actives dans tous les fichiers peuvent être visualisées grâce à la commande **dovecot** en utilisant l'option **-n** de la commande :

```
[root@mail ~]# dovecot -n
root@mail:~# dovecot -n
# 2.2.27 (c0f36b0): /etc/dovecot/dovecot.conf
# Pigeonhole version 0.4.16 (fed8554)
# OS: Linux 4.9.0-8-amd64 x86_64 Debian 9.6
mail_location = mbox:~/mail:INBOX=/var/mail/%u
mail_privileged_group = mail
namespace inbox {
  inbox = yes
  location =
  mailbox Drafts {
    special_use = \Drafts
  }
  mailbox Junk {
    special_use = \Junk
  }
  mailbox Sent {
    special_use = \Sent
  }
  mailbox "Sent Messages" {
    special_use = \Sent
  }
  mailbox Trash {
    special_use = \Trash
  }
  prefix =
}
passdb {
  driver = pam
```

```
}
protocols = " pop3"
ssl = no
userdb {
  driver = passwd
}
```

Re-démarrez le service dovecot :

```
root@mail:~# systemctl restart dovecot
root@mail:~# systemctl status dovecot
● dovecot.service - Dovecot IMAP/POP3 email server
   Loaded: loaded (/lib/systemd/system/dovecot.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2019-01-23 15:32:55 CET; 2s ago
     Docs: man:dovecot(1)
           http://wiki2.dovecot.org/
  Process: 2775 ExecStop=/usr/bin/doveadm stop (code=exited, status=0/SUCCESS)
  Process: 2780 ExecStart=/usr/sbin/dovecot (code=exited, status=0/SUCCESS)
 Main PID: 2781 (dovecot)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/dovecot.service
           ├─2781 /usr/sbin/dovecot
           ├─2782 dovecot/anvil
           ├─2783 dovecot/log
           └─2785 dovecot/config

janv. 23 15:32:55 mail.i2tch.com systemd[1]: Starting Dovecot IMAP/POP3 email server...
janv. 23 15:32:55 mail.i2tch.com dovecot[2781]: master: Dovecot v2.2.27 (c0f36b0) starting up for pop3 (core
dumps disabled)
janv. 23 15:32:55 mail.i2tch.com systemd[1]: dovecot.service: PID file /var/run/dovecot/master.pid not readable
(yet?) after start: No such file or directory
janv. 23 15:32:55 mail.i2tch.com systemd[1]: Started Dovecot IMAP/POP3 email server.
```

Créez maintenant le répertoire **/home/trainee/mail** :

```
root@mail:~# mkdir /home/trainee/mail
```

Modifiez l'utilisateur, le groupe et les permissions du répertoire **/home/trainee/mail** :

```
root@mail:~# chmod 700 /home/trainee/mail
root@mail:~# chown trainee:mail /home/trainee/mail
```

Modifiez les permissions du fichier **/var/spool/mail** :

```
root@mail:~# chmod 700 /var/spool/mail/trainee
```

Pour tester le serveur POP3, vous devez vous connecter au serveur en utilisant le protocol **TELNET**:

```
root@mail:~# telnet localhost 110
Trying ::1...
Connected to localhost.
Escape character is '^]'.
+OK Dovecot ready.
USER trainee
+OK
PASS trainee
+OK Logged in.
LIST
+OK 5 messages:
1 567
2 423
3 405
4 431
5 2884
.
RETR 1
+OK 567 octets
Return-path: <trainee@debian9.i2tch.loc>
```

```
Envelope-to: root@debian9.i2tch.loc
Delivery-date: Tue, 22 Jan 2019 15:11:14 +0100
Received: from trainee by debian9.i2tch.loc with local (Exim 4.89)
    (envelope-from <trainee@debian9.i2tch.loc>)
    id 1glwlm-0000Vo-T1
    for root@debian9.i2tch.loc; Tue, 22 Jan 2019 15:11:14 +0100
Subject: test message back
To: <root@debian9.i2tch.loc>
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <E1glwlm-0000Vo-T1@debian9.i2tch.loc>
From: trainee <trainee@debian9.i2tch.loc>
Date: Tue, 22 Jan 2019 15:11:14 +0100

fenestros
.
QUIT
+OK Logging out.
Connection closed by foreign host.
```

Notez l'utilisation de :

- **USER** est un compte sur votre système,
- **PASS** le mot de passe dudit compte,
- **LIST** obtient une liste des messages,
- **RETR n** permet de lire le message n,
- **QUIT** permet de quitter convenablement.

Arrêtez et désactivez le service dovecot :

```
root@mail:~# systemctl stop dovecot
root@mail:~# systemctl disable dovecot
Synchronizing state of dovecot.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable dovecot
root@mail:~# systemctl status dovecot
```

```
● dovecot.service - Dovecot IMAP/POP3 email server
   Loaded: loaded (/lib/systemd/system/dovecot.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:dovecot(1)
           http://wiki2.dovecot.org/

janv. 23 15:32:55 mail.i2tch.com systemd[1]: Stopped Dovecot IMAP/POP3 email server.
janv. 23 15:32:55 mail.i2tch.com systemd[1]: Starting Dovecot IMAP/POP3 email server...
janv. 23 15:32:55 mail.i2tch.com dovecot[2781]: master: Dovecot v2.2.27 (c0f36b0) starting up for pop3 (core
dumps disabled)
janv. 23 15:32:55 mail.i2tch.com systemd[1]: dovecot.service: PID file /var/run/dovecot/master.pid not readable
(yet?) after start: No such file or directory
janv. 23 15:32:55 mail.i2tch.com systemd[1]: Started Dovecot IMAP/POP3 email server.
janv. 23 15:34:45 mail.i2tch.com dovecot[2783]: pop3-login: Login: user=<trainee>, method=PLAIN, rip=::1,
lip=::1, mpid=2796, secured, session=<dGHH/iCAKukAAAAAAAAAAAAAA
janv. 23 15:35:28 mail.i2tch.com dovecot[2783]: pop3(trainee): Disconnected: Logged out top=0/0, retr=1/583,
del=0/5, size=4710
janv. 23 15:36:02 mail.i2tch.com systemd[1]: Stopping Dovecot IMAP/POP3 email server...
janv. 23 15:36:02 mail.i2tch.com dovecot[2781]: master: Warning: Killed with signal 15 (by pid=2800 uid=0
code=kill)
janv. 23 15:36:02 mail.i2tch.com systemd[1]: Stopped Dovecot IMAP/POP3 email server.
```

Cas #2 - Cyrus-Imap

Le fichier de configuration de **Cyrus-Imap** est **/etc/imapd.conf**. Les directives actives de ce fichier sont :Modifiez ce fichier ainsi :

```
root@mail:/tmp# cat imapd.conf
configdirectory: /var/lib/cyrus
proc_path: /run/cyrus/proc
mboxname_lockpath: /run/cyrus/lock
defaultpartition: default
partition-default: /var/spool/cyrus/mail
partition-news: /var/spool/cyrus/news
```

```
newsspool: /var/spool/news
altnamespace: no
unixhierarchysep: no
lmtp_downcase_rcpt: yes
allowanonymouslogin: no
popminpoll: 1
autocreate_quota: 0
umask: 077
sieveusehomedir: false
sievedir: /var/spool/sieve
httpmodules: caldav carddav
hashimapspool: true
allowplaintext: yes
sasl_pwcheck_method: auxprop
sasl_auto_transition: no
tls_client_ca_dir: /etc/ssl/certs
tls_session_timeout: 1440
lmtpsocket: /run/cyrus/socket/lmtp
idlesocket: /run/cyrus/socket/idle
notifysocket: /run/cyrus/socket/notify
syslog_prefix: cyrus
```

Editez ce fichier en remplacant la ligne **sasl_pwcheck_method: auxprop** avec les lignes suivantes :

```
defaultdomain:              i2tch.com
servername:                 mail.i2tch.com
admins:             root
sendmail:           /usr/sbin/sendmail
sasl_pwcheck_method:        saslauthd
sasl_mech_list:         PLAIN LOGIN
tls_server_cert:                        /etc/pki/cyrus-imapd/lel_cert.pem
tls_server_key:                         /etc/pki/cyrus-imapd/lel_clef.pem
tls_client_ca_file:                     /etc/pki/tls/certs/cacert.pem
```

Vous obtiendrez :

```
root@mail:~# vi /etc/imapd.conf
root@mail:~# cat /etc/imapd.conf
configdirectory: /var/lib/cyrus
proc_path: /run/cyrus/proc
mboxname_lockpath: /run/cyrus/lock
defaultpartition: default
partition-default: /var/spool/cyrus/mail
partition-news: /var/spool/cyrus/news
newsspool: /var/spool/news
altnamespace: no
unixhierarchysep: no
lmtp_downcase_rcpt: yes
allowanonymouslogin: no
popminpoll: 1
autocreate_quota: 0
umask: 077
sieveusehomedir: false
sievedir: /var/spool/sieve
httpmodules: caldav carddav
hashimapspool: true
allowplaintext: yes
defaultdomain:              i2tch.com
servername:                 mail.i2tch.com
admins:             root
sendmail:           /usr/sbin/sendmail
sasl_pwcheck_method:        saslauthd
sasl_mech_list:         PLAIN LOGIN
tls_server_cert:                        /etc/pki/cyrus-imapd/lel_cert.pem
tls_server_key:                         /etc/pki/cyrus-imapd/lel_clef.pem
tls_client_ca_file:                     /etc/pki/tls/certs/cacert.pem
sasl_auto_transition: no
tls_client_ca_dir: /etc/ssl/certs
```

```
tls_session_timeout: 1440
lmtpsocket: /run/cyrus/socket/lmtp
idlesocket: /run/cyrus/socket/idle
notifysocket: /run/cyrus/socket/notify
syslog_prefix: cyrus
```

Les directives les plus importantes dans le fichier ci-dessus sont :

Directive	**Description**
defaultdomain	Le domaine par défaut.
servername	Le nom visible dans les messages d'accueil POP, IMAP et LMTP.
configdirectory	Le nom du chemin du répertoire de configuration d'IMAP.
sievedir	Le répertoire où sont recherchés des **Sieve scripts**.
sasl_pwcheck_method	Le mechanism utilisé par le serveur pour vérifier des mots de passe **plaintext**.

Copiez les fichiers générés précedement pour la mise en place de TLS sous Postfix :

```
root@mail:~# mkdir /usr/lib/ssl/cyrus-imapd
root@mail:~# cp /etc/postfix/cacert.pem /usr/lib/ssl/certs
root@mail:~# cp /etc/postfix/lel_cert.pem /usr/lib/ssl/cyrus-imapd
root@mail:~# cp /etc/postfix/lel_clef.pem /usr/lib/ssl/cyrus-imapd
root@mail:~# chmod 644 /usr/lib/ssl/certs/cacert.pem
root@mail:~# chmod 640 /usr/lib/ssl/cyrus-imapd/lel_clef.pem /usr/lib/ssl/cyrus-imapd/lel_cert.pem
root@mail:~# chown root:mail /usr/lib/ssl/cyrus-imapd/lel_clef.pem /usr/lib/ssl/cyrus-imapd/lel_cert.pem
```

Editez le fichier **/etc/cyrus.conf**. Commentez les lignes des services autre que imap :

```
root@mail:~# cat /etc/cyrus.conf
# Debian defaults for Cyrus IMAP server/cluster implementation
# see cyrus.conf(5) for more information
#
# All the tcp services are tcpd-wrapped. see hosts_access(5)
```

```
START {
    # do not delete this entry!
    recover        cmd="/usr/sbin/cyrus ctl_cyrusdb -r"
    # this is only necessary if idlemethod is set to "idled" in imapd.conf
    #idled        cmd="idled"

    # this is useful on backend nodes of a Murder cluster
    # it causes the backend to syncronize its mailbox list with
    # the mupdate master upon startup
    #mupdatepush   cmd="/usr/sbin/cyrus ctl_mboxlist -m"

    # this is recommended if using duplicate delivery suppression
    delprune    cmd="/usr/sbin/cyrus expire -E 3"
    # this is recommended if caching TLS sessions
    tlsprune    cmd="/usr/sbin/cyrus tls_prune"
}

# UNIX sockets start with a slash and are absolute paths
# you can use a maxchild=# to limit the maximum number of forks of a service
# you can use babysit=true and maxforkrate=# to keep tight tabs on the service
# most services also accept -U (limit number of reuses) and -T (timeout)
SERVICES {
    # --- Normal cyrus spool, or Murder backends ---
    # add or remove based on preferences
    imap        cmd="imapd -U 30" listen="imap" prefork=0 maxchild=100
    #imaps        cmd="imapd -s -U 30" listen="imaps" prefork=0 maxchild=100
    # pop3        cmd="pop3d -U 30" listen="pop3" prefork=0 maxchild=50
    #pop3s        cmd="pop3d -s -U 30" listen="pop3s" prefork=0 maxchild=50
    # nntp        cmd="nntpd -U 30" listen="nntp" prefork=0 maxchild=100
    #nntps        cmd="nntpd -s -U 30" listen="nntps" prefork=0 maxchild=100
    #http        cmd="httpd -U 30" listen="8008" prefork=0 maxchild=100
    #https        cmd="httpd -s -U 30" listen="8443" prefork=0 maxchild=100
```

```
    # At least one form of LMTP is required for delivery
    # (you must keep the Unix socket name in sync with imap.conf)
    #lmtp        cmd="lmtpd" listen="localhost:lmtp" prefork=0 maxchild=20
    lmtpunix    cmd="lmtpd" listen="/run/cyrus/socket/lmtp" prefork=0 maxchild=20
    # ----------------------------------------------

    # useful if you need to give users remote access to sieve
    # by default, we limit this to localhost in Debian
    sieve        cmd="timsieved" listen="localhost:sieve" prefork=0 maxchild=100

    # this one is needed for the notification services
    notify        cmd="notifyd" listen="/run/cyrus/socket/notify" proto="udp" prefork=1

    # --- Murder frontends -------------------------
    # enable these and disable the matching services above,
    # except for sieve (which deals automatically with Murder)

    # mupdate database service - must prefork at least 1
    # (mupdate slaves)
    #mupdate       cmd="mupdate" listen=3905 prefork=1
    # (mupdate master, only one in the entire cluster)
    #mupdate       cmd="mupdate -m" listen=3905 prefork=1

    # proxies that will connect to the backends
    #imap        cmd="proxyd" listen="imap" prefork=0 maxchild=100
    #imaps        cmd="proxyd -s" listen="imaps" prefork=0 maxchild=100
    #pop3        cmd="pop3proxyd" listen="pop3" prefork=0 maxchild=50
    #pop3s        cmd="pop3proxyd -s" listen="pop3s" prefork=0 maxchild=50
    #lmtp        cmd="lmtpproxyd" listen="lmtp" prefork=1 maxchild=20
    # ----------------------------------------------
}

EVENTS {
    # this is required
```

```
    checkpoint    cmd="/usr/sbin/cyrus ctl_cyrusdb -c" period=30

    # this is only necessary if using duplicate delivery suppression
    delprune    cmd="/usr/sbin/cyrus expire -E 3" at=0401

    # this is only necessary if caching TLS sessions
    tlsprune    cmd="/usr/sbin/cyrus tls_prune" at=0401

    # Expire data older than 28 days.
    deleteprune    cmd="/usr/sbin/cyrus expire -E 4 -D 28" at=0430
    expungeprune    cmd="/usr/sbin/cyrus expire -E 4 -X 28" at=0445
    # indexing of mailboxes for server side fulltext searches

    # reindex changed mailboxes (fulltext) approximately every other hour
    #squatter_1    cmd="/usr/bin/nice -n 19 /usr/sbin/cyrus squatter -s" period=120

    # reindex all mailboxes (fulltext) daily
    #squatter_a    cmd="/usr/sbin/cyrus squatter" at=0517
}
```

Créez le fichier **/var/lib/cyrus/tls_sessions.db** avec les permissions adéquates :

```
root@mail:~# touch /var/lib/cyrus/tls_sessions.db
root@mail:~# chown cyrus:mail /var/lib/cyrus/tls_sessions.db
```

Démarrez le service **cyrus-imapd** :

```
[root@mail ~]# systemctl start cyrus-imapd
```

Configurez postfix pour utiliser Cyrus-Imapd en décommentant les lignes suivantes au fichier **/etc/postfix/master.cf** :

```
...
cyrus     unix  -       n       n       -       -       pipe
  user=cyrus argv=/usr/lib/cyrus-imapd/deliver -e -r ${sender} -m ${extension} ${user}
```

```
...
```

Ajoutez les trois lignes suivantes à la fin de votre fichier **/etc/postfix/main.cf** :

```
...
############ CYRUS-IMAPD ###############
cyrus_destination_recipient_limit=1
local_transport = cyrus
```

Vous obtiendrez le résultat suivant :

```
root@mail:~# vi /etc/postfix/main.cf
root@mail:~# cat /etc/postfix/main.cf
#############CONFIG DE BASE##############
myhostname = mail.i2tch.com
mydomain= i2tch.com
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
relayhost =
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
############   COMMANDES   ##############
mailbox_command = procmail -a "$EXTENSION"
############  REPERTOIRES  ##############
readme_directory = no
############      SASL     ##############
```

```
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
                                  reject_non_fqdn_sender,
                                  reject_non_fqdn_recipient,
                                  reject_unknown_sender_domain,
                                  reject_unknown_recipient_domain,
                                  reject_unauth_pipelining,
                                  reject_rbl_client zen.spamhaus.org,
                                  reject_rbl_client bl.spamcop.net,
                                  reject_rbl_client dnsbl.njabl.org,
                                  reject_rbl_client dnsbl.sorbs.net,
                                  permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = i2tch.com
smtpd_helo_required = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = cyrus
cyrus_sasl_config_path = /etc/postfix/sasl
#############      TLS      ###############
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_sesson_cache
smtp_tls_security_level = may
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_sesson_cache
smtpd_tls_cert_file = /etc/postfix/lel_cert.pem
smtpd_tls_key_file = /etc/postfix/lel_clef.pem
```

```
smtpd_tls_received_header = yes
tls_random_source = dev:/dev/urandom
smtpd_tls_security_level = may
smtpd_tls_loglevel = 2
smtpd_tls_ask_ccert = no
############ HEADER CHECKS ###############
header_checks = regexp:/etc/postfix/header_checks
############ CYRUS-IMAPD ###############
cyrus_destination_recipient_limit=1
local_transport = cyrus
```

A Faire - Pour plus d'informations concernant les directives, consultez **cette page**.

Re-démarrez maintenant le service MailScanner :

```
[root@mail ~]# systemctl restart mailscanner
[root@mail ~]# systemctl status mailscanner
● mailscanner.service - LSB: MailScanner daemon
   Loaded: loaded (/usr/lib/MailScanner/init/ms-init; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-01-15 14:45:11 CET; 7s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 30624 ExecStop=/usr/lib/MailScanner/init/ms-init stop (code=exited, status=0/SUCCESS)
  Process: 30693 ExecStart=/usr/lib/MailScanner/init/ms-init start (code=exited, status=0/SUCCESS)
 Main PID: 31259 (MailScanner: st)
   CGroup: /system.slice/mailscanner.service
           ├─31259 MailScanner: starting children
           ├─31260 MailScanner: waiting for messages
           └─31366 MailScanner: starting children

Jan 15 14:45:16 mail.i2tch.com MailScanner[31366]: Reading configuration file /etc/MailScanner/MailScanner.conf
Jan 15 14:45:16 mail.i2tch.com MailScanner[31366]: Reading configuration file /etc/MailScanner/conf.d/README
```

```
Jan 15 14:45:16 mail.i2tch.com MailScanner[31366]: Read 1500 hostnames from the phishing whitelist
Jan 15 14:45:16 mail.i2tch.com MailScanner[31366]: Read 16624 hostnames from the phishing blacklists
Jan 15 14:45:16 mail.i2tch.com MailScanner[31366]: Using SpamAssassin results cache
Jan 15 14:45:16 mail.i2tch.com MailScanner[31366]: Connected to SpamAssassin cache database
Jan 15 14:45:16 mail.i2tch.com MailScanner[31366]: Enabling SpamAssassin auto-whitelist functionality...
Jan 15 14:45:17 mail.i2tch.com MailScanner[31260]: Connected to Processing Attempts Database
Jan 15 14:45:17 mail.i2tch.com MailScanner[31260]: Found 0 messages in the Processing Attempts Database
Jan 15 14:45:17 mail.i2tch.com MailScanner[31260]: Using locktype = flock
```

Créez la BAL de l'utilisateur **trainee** et y mettre un quota de 20 000 Ko :

```
root@mail:~# apt-get install cyrus-admin
root@mail:~# cyradm localhost
Password: fenestros
localhost> cm user.trainee
localhost> setquota user.trainee 20000
quota:20000
localhost> exit
```

Déclarez le mot de passe de trainee dans la base de données de Cyrus SASL :

```
root@mail:~# saslpasswd2 trainee
Password: trainee
Again (for verification): trainee
```

Modifiez les permissions sur la base de données de Cyrus **/etc/sasldb2** :

```
root@mail:~# chmod 640 /etc/sasldb2
root@mail:~# chown root:mail /etc/sasldb2
```

Re-démarrez le service **cyrus-imapd** :

```
[root@mail ~]# systemctl restart cyrus-imapd
```

Testez votre configuration avec la commande **imtest** :

```
root@mail:~# apt-get install cyrus-clients
root@mail:~# /usr/lib/cyrus/bin/imtest -t "" mail.i2tch.com -a trainee
S: * OK [CAPABILITY IMAP4rev1 LITERAL+ ID ENABLE STARTTLS AUTH=PLAIN AUTH=LOGIN SASL-IR] mail.i2tch.com Cyrus
IMAP 2.5.10-Debian-2.5.10-3 server ready
C: S01 STARTTLS
S: S01 NO Error initializing TLS
Please enter your password: trainee
C: A01 AUTHENTICATE PLAIN AHRyYWluZWUAdHJhaW5lZQ==
S: A01 OK [CAPABILITY IMAP4rev1 LITERAL+ ID ENABLE ACL RIGHTS=kxten QUOTA MAILBOX-REFERRALS NAMESPACE UIDPLUS
NO_ATOMIC_RENAME UNSELECT CHILDREN MULTIAPPEND BINARY CATENATE CONDSTORE ESEARCH SORT SORT=MODSEQ SORT=DISPLAY
SORT=UID THREAD=ORDEREDSUBJECT THREAD=REFERENCES ANNOTATEMORE ANNOTATE-EXPERIMENT-1 METADATA LIST-EXTENDED LIST-
STATUS LIST-MYRIGHTS WITHIN QRESYNC SCAN XLIST XMOVE MOVE SPECIAL-USE CREATE-SPECIAL-USE URLAUTH URLAUTH=BINARY
LOGINDISABLED COMPRESS=DEFLATE X-QUOTA=STORAGE X-QUOTA=MESSAGE X-QUOTA=X-ANNOTATION-STORAGE X-QUOTA=X-NUM-FOLDERS
IDLE] Success (no protection) SESSIONID=<mail.i2tch.com-4359-1548258532-1-13341529482450476217>
Authenticated.
Security strength factor: 256
. logout
* BYE LOGOUT received
. OK Completed
Connection closed.
```

Consultez l'aide de la commande **imtest** pour comprendre l'utilisation de l'option **-t** :

```
root@mail:~# /usr/lib/cyrus/bin/imtest --help
/usr/lib/cyrus/bin/imtest: invalid option -- '-'
/usr/lib/cyrus/bin/imtest: invalid option -- 'e'
Usage: imtest [options] hostname
  -p port  : port to use (default=standard port for protocol)
  -z       : timing test
  -k #     : minimum protection layer required
  -l #     : max protection layer (0=none; 1=integrity; etc)
  -u user  : authorization name to use
```

```
  -a user  : authentication name to use
  -w pass  : password to use (if not supplied, we will prompt)
  -v       : verbose
  -m mech  : SASL mechanism to use
             ("login" for IMAP LOGIN)
  -f file  : pipe file into connection after authentication
  -r realm : realm
  -s       : Enable imap over SSL (imaps)
  -t file  : Enable TLS. file has the TLS public and private keys
             (specify "" to not use TLS for authentication)
  -q       : Enable imap COMPRESSion (before last authentication attempt)
  -c       : enable challenge prompt callbacks
             (enter one-time password instead of secret pass-phrase)
  -n       : number of auth attempts (default=1)
  -I file  : output my PID to (file) (useful with -X)
  -x file  : open the named socket for the interactive portion
  -X file  : same as -X, except close all file descriptors & dameonize
```

LAB #8 - Gestion des Domaines Virtuels avec MariaDB, Postfix et Dovecot

A Faire - Détruisez votre VM CentOS 7. Importez une nouvelle VM CentOS 7. Configurez la RAM de votre VM **CentOS 7** à 2 048 MB. Démarrez la VM. Connectez-vous via putty en utilisant localhost:3022 et le compte **trainee**/**trainee**. Saisissez la commande **su -** et devenez l'utilisateur **root** grâce au mot de passe **fenestros**.

Configuration de votre Machine Virtuelle

Modification du Fichier /etc/hosts

Comme vous allez utiliser le nom de domaine **mail.i2tch.com** pour votre serveur postfix, modifiez votre fichier **/etc/hosts** ainsi :

```
root@debian9:~# vi /etc/hosts
root@debian9:~# cat /etc/hosts
127.0.0.1   localhost
127.0.1.1   debian9.i2tch.loc    debian9
10.0.2.15   i2tch.com
10.0.2.15   mail.i2tch.com  mail

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Modification du FQDN

Modifiez le FQDN de votre VM :

```
root@debian9:~# nmcli g hostname mail.i2tch.com
root@debian9:~# hostname
mail.i2tch.com
```

Création, Activation et Configuration d'un Profil Réseau d'IP Fixe

Créez et activez un profil d'adresse IP fixe dénommé **ip_fixe** :

```
root@debian9:~# nmcli c show
NOM                 UUID                                  TYPE            PÉRIPHÉRIQUE
```

```
Wired connection 1  935fbc1c-a7f5-4bc9-a389-591e88989162  802-3-ethernet  enp0s3
root@debian9:~# nmcli connection add con-name ip_fixe ifname enp0s3 type ethernet ip4 10.0.2.15/24 gw4 10.0.2.2
Connexion « ip_fixe » (66f5d126-c0cc-4bc5-9ec1-41c8b0372af2) ajoutée avec succès.
root@debian9:~# nmcli connection up ip_fixe
Connexion activée (chemin D-Bus actif : /org/freedesktop/NetworkManager/ActiveConnection/2)
root@debian9:~# nmcli c show
NOM                 UUID                                  TYPE            PÉRIPHÉRIQUE
ip_fixe             66f5d126-c0cc-4bc5-9ec1-41c8b0372af2  802-3-ethernet  enp0s3
Wired connection 1  935fbc1c-a7f5-4bc9-a389-591e88989162  802-3-ethernet  --
```

Définissez un DNS pour le profil, redémarrez le service NetworkManager et testez la résolution des noms :

```
root@debian9:~# nmcli connection mod ip_fixe ipv4.dns 8.8.8.8
root@debian9:~# systemctl restart NetworkManager
root@debian9:~# apt-get install dnsutils
root@debian9:~# dig www.i2tch.com

; <<>> DiG 9.10.3-P4-Debian <<>> www.i2tch.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3377
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.i2tch.com.         IN    A

;; ANSWER SECTION:
www.i2tch.com.      21599    IN    CNAME    i2tch.com.
i2tch.com.      59    IN    A    77.153.192.218

;; Query time: 96 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
```

```
;; WHEN: Tue Jan 22 15:20:03 CET 2019
;; MSG SIZE  rcvd: 72
```

Important - Déconnectez-vous et re-connectez-vous.

Démarrage du Service ntpd

Installez le service **ntp** :

```
root@mail:~# apt-get install ntp
root@mail:~# systemctl status ntp
● ntp.service - LSB: Start NTP daemon
   Loaded: loaded (/etc/init.d/ntp; generated; vendor preset: enabled)
   Active: active (running) since Tue 2019-01-22 15:23:28 CET; 12s ago
     Docs: man:systemd-sysv-generator(8)
   CGroup: /system.slice/ntp.service
           └─2760 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 117:122

janv. 22 15:23:32 mail.i2tch.com ntpd[2760]: Soliciting pool server 91.121.154.62
janv. 22 15:23:32 mail.i2tch.com ntpd[2760]: Soliciting pool server 5.196.160.139
janv. 22 15:23:33 mail.i2tch.com ntpd[2760]: Soliciting pool server 151.80.32.142
janv. 22 15:23:33 mail.i2tch.com ntpd[2760]: Soliciting pool server 108.61.177.141
janv. 22 15:23:33 mail.i2tch.com ntpd[2760]: Soliciting pool server 188.165.236.162
janv. 22 15:23:33 mail.i2tch.com ntpd[2760]: Soliciting pool server 195.154.41.195
janv. 22 15:23:34 mail.i2tch.com ntpd[2760]: Soliciting pool server 5.135.3.88
janv. 22 15:23:34 mail.i2tch.com ntpd[2760]: Soliciting pool server 2001:bc8:271b:100::1
janv. 22 15:23:34 mail.i2tch.com ntpd[2760]: Soliciting pool server 37.187.18.4
janv. 22 15:23:34 mail.i2tch.com ntpd[2760]: Soliciting pool server 91.121.91.167
```

Configurer firewalld

Installez le paquet **firewalld** :

```
root@mail:~# apt-get install firewalld
```

Pour ouvrir les ports en relation avec nos serveurs de méssagerie, utilisez les commandes suivantes :

```
[root@mail ~]# firewall-cmd --permanent --add-port=25/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=465/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=587/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=995/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=993/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=143/tcp
[root@mail ~]# firewall-cmd --permanent --add-port=110/tcp
[root@mail ~]# firewall-cmd --reload
```

Installer mariadb et dovecot-mysql

Installez le paquets suivants à l'aide de **apt-get** :

```
[root@mail ~]# apt-get install postfix postfix-mysql procmail dovecot-core dovecot-pop3d dovecot-mysql dovecot-
lmtpd dovecot-imapd mailutils mysql-server
```

Lors de l'installation :

- choisissez l'option “Site Internet”,
- spécifiez le nom de domaine mail.i2tch.com.

Utilisez la script **mysql_secure_installation** pour sécuriser l'installation de MariaDB :

```
root@mail:~# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user.  If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.

Set root password? [Y/n] y
New password: fenestros
Re-enter new password: fenestros
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] Y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.
```

```
Disallow root login remotely? [Y/n] Y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] Y
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MariaDB
installation should now be secure.

Thanks for using MariaDB!
```

Important - Notez que le mot de passe ne sera **pas** visible.

Créez une base de données pour utiliser avec postfix :

```
root@mail:~# mysqladmin -u root -p create mailserver
```

```
Enter password:fenestros
```

Important - Notez que le mot de passe ne sera **pas** visible.

Connectez-vous à MariaDB et créez un utilisateur ayant tous les privilèges sur la base de données **mailserver** :

```
root@mail:~# mysql -u root -p
Enter password: fenestros
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 11
Server version: 10.1.37-MariaDB-0+deb9u1 Debian 9.6

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> GRANT SELECT ON mailserver.* TO 'mailuser'@'127.0.0.1' IDENTIFIED BY 'fenestros';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> exit
Bye
```

Important - Notez que le mot de passe ne sera **pas** visible.

Créer un Certificat

Commencez par exécuter le script CA qui se trouve dans **/usr/lib/ssl/misc** :

```
root@mail:~# cd /usr/lib/ssl/misc/
root@mail:/usr/lib/ssl/misc# ./CA.pl -newca
CA certificate filename (or enter to create)

Making CA certificate ...
====
openssl req  -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
.............+++++
.....................................+++++
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:fenestros
Verifying - Enter PEM pass phrase:fenestros
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:SURREY
Locality Name (eg, city) []:ADDLESTONE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:I2TCH LTD
Organizational Unit Name (eg, section) []:TRAINING
Common Name (e.g. server FQDN or YOUR name) []:i2tch.com
Email Address []:infos@i2tch.com
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:secret
An optional company name []:
==> 0
====
====
openssl ca  -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -
selfsign -extensions v3_ca -infiles ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:fenestros
Can't open ./demoCA/index.txt.attr for reading, No such file or directory
139740109301120:error:02001002:system library:fopen:No such file or
directory:../crypto/bio/bss_file.c:74:fopen('./demoCA/index.txt.attr','r')
139740109301120:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            c5:b1:b7:bd:b7:1a:f9:7b
        Validity
            Not Before: Jan 23 10:39:05 2019 GMT
            Not After : Jan 22 10:39:05 2022 GMT
        Subject:
            countryName               = GB
            stateOrProvinceName       = SURREY
            organizationName          = I2TCH LTD
            organizationalUnitName    = TRAINING
            commonName                = i2tch.com
            emailAddress              = infos@i2tch.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                24:F4:51:39:C5:64:D3:E6:D8:E8:D4:DB:D1:54:AF:2A:F7:25:8C:90
            X509v3 Authority Key Identifier:
```

```
               keyid:24:F4:51:39:C5:64:D3:E6:D8:E8:D4:DB:D1:54:AF:2A:F7:25:8C:90

            X509v3 Basic Constraints: critical
                CA:TRUE
Certificate is to be certified until Jan 22 10:39:05 2022 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
==> 0
====
CA certificate is in ./demoCA/cacert.pem
```

Vous obtiendrez deux fichiers - **cacert.pem** et **cakey.pem** :

```
root@mail:/usr/lib/ssl/misc# apt-get install locate
root@mail:/usr/lib/ssl/misc# updatedb
root@mail:/usr/lib/ssl/misc# locate cacert.pem
/usr/lib/ssl/misc/demoCA/cacert.pem
root@mail:/usr/lib/ssl/misc# locate cakey.pem
/usr/lib/ssl/misc/demoCA/private/cakey.pem
```

Vous devez générer maintenant une clef privée ainsi qu'un **Certificate Signing Request** pour le serveur mail. Le **CSR (Certificate Signing Request)** doit alors être envoyé à une des sociétés faisant autorité en la matière afin que celle-ci puisse vous retourner votre certificat définitif. Ce service est payant. C'est ce certificat définitif qui est utilisé pour des connexions sécurisées.

```
root@mail:/usr/lib/ssl/misc# openssl req -new -nodes -keyout lel_clef.pem -out lel_req.pem
Generating a RSA private key
.................+++++
....+++++
writing new private key to 'lel_clef.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GB
State or Province Name (full name) [Some-State]:SURREY
Locality Name (eg, city) []:ADDLESTONE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:I2TCH LTD
Organizational Unit Name (eg, section) []:TRAINING
Common Name (e.g. server FQDN or YOUR name) []:mail.i2tch.com
Email Address []:infos@i2tch.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Vous obtiendrez deux fichiers - **lel_clef.pem** et **lel_req.pem** :

```
root@mail:/usr/lib/ssl/misc# ls
CA.pl  demoCA  lel_clef.pem  lel_req.pem  tsget
```

Vous pouvez maintenant envoyé votre **CSR (Certificate Signing Request)**, **lel_req.pem**, à la société que vous avez choisie. Quand votre certificat **.crt** vous est retourné, copiez-le, ainsi que votre clé privée dans le répertoire **/etc/postfix/ssl**.

Sans passer par un prestataire externe, vous pouvez signer votre **CSR (Certificate Signing Request)** avec votre propre clef afin de générer votre certificat :

```
root@mail:/usr/lib/ssl/misc# openssl ca -out lel_cert.pem -infiles lel_req.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:fenestros
Check that the request matches the signature
Signature ok
Certificate Details:
```

```
        Serial Number:
            c5:b1:b7:bd:b7:1a:f9:7c
        Validity
            Not Before: Jan 23 12:09:31 2019 GMT
            Not After : Jan 23 12:09:31 2020 GMT
        Subject:
            countryName               = GB
            stateOrProvinceName       = SURREY
            organizationName          = I2TCH LTD
            organizationalUnitName    = TRAINING
            commonName                = mail.i2tch.com
            emailAddress              = infos@i2tch.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                F3:F9:04:23:4F:CB:03:42:A4:4B:B1:0C:77:2B:67:3D:6F:9B:C8:BB
            X509v3 Authority Key Identifier:
                keyid:24:F4:51:39:C5:64:D3:E6:D8:E8:D4:DB:D1:54:AF:2A:F7:25:8C:90

Certificate is to be certified until Jan 23 12:09:31 2020 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Important - Notez que le **commonName** est différent (i2tch.com <> mail.i2tch.com) ! Dans le cas contraire la base de données ne sera pas mise à jour et une erreur sera jetée.

Il convient ensuite de copier les fichiers lel_cert.pem, lel_clef.pem et cacert.pem dans le répertoire **/etc/postfix** puis de modifier les permissions :

```
root@mail:/usr/lib/ssl/misc# cp lel_cert.pem lel_clef.pem /etc/postfix
root@mail:/usr/lib/ssl/misc# cp /usr/lib/ssl/misc/demoCA/cacert.pem /etc/postfix
root@mail:/usr/lib/ssl/misc# chmod 644 /etc/postfix/lel_cert.pem /etc/postfix/cacert.pem
root@mail:/usr/lib/ssl/misc# chmod 400 /etc/postfix/lel_clef.pem
```

Créer les Tables de la Base mailserver

Connectez-vous à MariaDB :

```
root@mail:/usr/lib/ssl/misc# cd ~
root@mail:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 12
Server version: 10.1.37-MariaDB-0+deb9u1 Debian 9.6

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> USE mailserver;
Database changed
MariaDB [mailserver]>
```

virtual_domaines

Créez une table dénommée **virtual_domains** pour contenir la liste des domaines pour lesquels postfix recevra des messages en utilisant la requête SQL suivante :

```
CREATE TABLE `virtual_domains` (
  `id` int(11) NOT NULL auto_increment,
  `name` varchar(50) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Vous obtiendrez :

```
MariaDB [mailserver]> CREATE TABLE `virtual_domains` (
    ->   `id` int(11) NOT NULL auto_increment,
    ->   `name` varchar(50) NOT NULL,
    ->   PRIMARY KEY (`id`)
    -> ) ENGINE=InnoDB DEFAULT CHARSET=utf8;
Query OK, 0 rows affected (0.06 sec)

MariaDB [mailserver]>
```

Insérez des données dans la table en utilisant la requête SQL suivante :

```
INSERT INTO `mailserver`.`virtual_domains`
  (`id` ,`name`)
VALUES
  ('1', 'i2tch.com'),
  ('2', 'mail.i2tch.com'),
  ('3', 'mail'),
  ('4', 'localhost.i2tch.com');
```

Vous obtiendrez :

```
MariaDB [mailserver]> INSERT INTO `mailserver`.`virtual_domains`
    ->   (`id` ,`name`)
    -> VALUES
    ->   ('1', 'i2tch.com'),
```

```
    ->   ('2', 'mail.i2tch.com'),
    ->   ('3', 'mail'),
    ->   ('4', 'localhost.i2tch.com');
Query OK, 4 rows affected (0.04 sec)
Records: 4  Duplicates: 0  Warnings: 0

MariaDB [mailserver]>
```

Important - Notez les numéros de domaines dans le champs **id**. Ces numéros seront utiliser lors de l'insertion des données dans la table **virtual_users**.

Contrôlez le contenu de la table :

```
MariaDB [mailserver]> SELECT * FROM mailserver.virtual_domains;
+----+---------------------+
| id | name                |
+----+---------------------+
|  1 | i2tch.com           |
|  2 | mail.i2tch.com      |
|  3 | mail                |
|  4 | localhost.i2tch.com |
+----+---------------------+
4 rows in set (0.00 sec)

MariaDB [mailserver]>
```

virtual_users

Créez une table dénommée **virtual_users** pour contenir les adresses email et les mots de passe en utilisant la requête SQL suivante :

```
CREATE TABLE `virtual_users` (
  `id` int(11) NOT NULL auto_increment,
  `domain_id` int(11) NOT NULL,
  `password` varchar(106) NOT NULL,
  `email` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  UNIQUE KEY `email` (`email`),
  FOREIGN KEY (domain_id) REFERENCES virtual_domains(id) ON DELETE CASCADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Vous obtiendrez :

```
MariaDB [mailserver]> CREATE TABLE `virtual_users` (
    ->   `id` int(11) NOT NULL auto_increment,
    ->   `domain_id` int(11) NOT NULL,
    ->   `password` varchar(106) NOT NULL,
    ->   `email` varchar(100) NOT NULL,
    ->   PRIMARY KEY (`id`),
    ->   UNIQUE KEY `email` (`email`),
    ->   FOREIGN KEY (domain_id) REFERENCES virtual_domains(id) ON DELETE CASCADE
    -> ) ENGINE=InnoDB DEFAULT CHARSET=utf8;
Query OK, 0 rows affected (0.05 sec)

MariaDB [mailserver]>
```

Insérez des données dans la table en utilisant la requête SQL suivante :

```
INSERT INTO `mailserver`.`virtual_users`
  (`id`, `domain_id`, `password` , `email`)
VALUES
  ('1', '1', ENCRYPT('fenestros', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'root@i2tch.com'),
  ('2', '1', ENCRYPT('trainee', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'trainee@i2tch.com'),
  ('3', '2', ENCRYPT('fenestros', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'root@mail.i2tch.com'),
```

```
  ('4', '2', ENCRYPT('trainee', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'trainee@mail.i2tch.com');
```

> **Important** - Notez que les valeurs du champs **domain_id** sont celles du champs **id** de la table **virtual_domains**.

Vous obtiendrez :

```
MariaDB [mailserver]> INSERT INTO `mailserver`.`virtual_users`
    ->   (`id`, `domain_id`, `password` , `email`)
    -> VALUES
    ->   ('1', '1', ENCRYPT('fenestros', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'root@i2tch.com'),
    ->   ('2', '1', ENCRYPT('trainee', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'trainee@i2tch.com'),
    ->   ('3', '2', ENCRYPT('fenestros', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'root@mail.i2tch.com'),
    ->   ('4', '2', ENCRYPT('trainee', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'trainee@mail.i2tch.com');
Query OK, 4 rows affected (0.04 sec)
Records: 4  Duplicates: 0  Warnings: 0

MariaDB [mailserver]>
```

Contrôlez le contenu de la table :

```
MariaDB [mailserver]> SELECT * FROM mailserver.virtual_users;
+----+-----------+-------------------------------------------------------------------------------------------
-------------+-----------------------+
| id | domain_id | password
| email                   |
+----+-----------+-------------------------------------------------------------------------------------------
-------------+-----------------------+
|  1 |         1 |
$6$be5627f90975f9b1$UJ7S/CEgg/7hb3et6p2dPgYXhmqoAH5fC0R3sactGttioKVV8zzxd6cTyLp0hdVSm.fzsAXuzPtjQ4OhtrfFi1 |
root@i2tch.com         |
```

```
|  2 |         1 |
$6$9bd6d74a6ff8e016$Il56Yshyn7HAv3R6u/HfvoKuqwUuXkSvZeXhK.BHpgHn/nYo3/lSSyIUjpdnpo6VzpUllLC6Y3xKaY5ROdmYM. |
trainee@i2tch.com      |
|  3 |         2 |
$6$fd93e32a7a1a1ef3$WerO8ZCiPtMgBFUG0IllYKOI3uIXdRIAjmsg44nRYwWGKj.vS5wy4MD3N.1Qo/CYBM4GqzvhSC3S4mLsEfwqz/ |
root@mail.i2tch.com    |
|  4 |         2 |
$6$6a4ed3695d5771f4$BPkkmlbZhipVo.OlpE5I1SVOAsB0Y7azSOr7cz8QrzbnMZnS2U/2Il5OXUwc3dCgge/BtDf/5EcjS/WDCXR3H1 |
trainee@mail.i2tch.com |
+----+-----------+-----------------------------------------------------------------------------------------
-------------+-----------------------+
4 rows in set (0.01 sec)

MariaDB [mailserver]>
```

virtual_aliases

Créez une table dénommée **virtual_aliases** pour contenir les aliases en utilisant la requête SQL suivante :

```
CREATE TABLE `virtual_aliases` (
  `id` int(11) NOT NULL auto_increment,
  `domain_id` int(11) NOT NULL,
  `source` varchar(100) NOT NULL,
  `destination` varchar(100) NOT NULL,
  PRIMARY KEY (`id`),
  FOREIGN KEY (domain_id) REFERENCES virtual_domains(id) ON DELETE CASCADE
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Vous obtiendrez :

```
MariaDB [mailserver]> CREATE TABLE `virtual_aliases` (
    ->   `id` int(11) NOT NULL auto_increment,
```

```
    ->   `domain_id` int(11) NOT NULL,
    ->   `source` varchar(100) NOT NULL,
    ->   `destination` varchar(100) NOT NULL,
    ->   PRIMARY KEY (`id`),
    ->   FOREIGN KEY (domain_id) REFERENCES virtual_domains(id) ON DELETE CASCADE
    -> ) ENGINE=InnoDB DEFAULT CHARSET=utf8;
Query OK, 0 rows affected (0.04 sec)

MariaDB [mailserver]>
```

Insérez des données dans la table en utilisant la requête SQL suivante :

```
INSERT INTO `mailserver`.`virtual_aliases`
  (`id`, `domain_id`, `source`, `destination`)
VALUES
  ('1', '1', 'mickey.mouse@i2tch.com', 'trainee@i2tch.com');
```

Important - Notez que la valeur du champs **domain_id** est celle du champs **id** de la table **virtual_domains**.

Vous obtiendrez :

```
MariaDB [mailserver]> INSERT INTO `mailserver`.`virtual_aliases`
    ->   (`id`, `domain_id`, `source`, `destination`)
    -> VALUES
    ->   ('1', '1', 'mickey.mouse@i2tch.com', 'trainee@i2tch.com');
Query OK, 1 row affected (0.04 sec)

MariaDB [mailserver]>
```

Contrôlez le contenu de la table :

```
MariaDB [mailserver]> SELECT * FROM mailserver.virtual_aliases;
+----+-----------+-----------------------+-------------------+
| id | domain_id | source                | destination       |
+----+-----------+-----------------------+-------------------+
|  1 |         1 | mickey.mouse@i2tch.com | trainee@i2tch.com |
+----+-----------+-----------------------+-------------------+
1 row in set (0.00 sec)

MariaDB [mailserver]> exit
Bye
```

Configurer postfix

main.cf

Sauvegardez le fichier **/etc/postfix/main.cf** :

```
root@mail:~# cp /etc/postfix/main.cf /etc/postfix/main.cf.orig
```

Ouvrez le fichier **/etc/postfix/main.cf** en édition et remplacez son contenu avec le contenu suivant :

```
root@mail:~# vi /etc/postfix/main.cf
root@mail:~# cat /etc/postfix/main.cf
#############CONFIG DE BASE##############
myhostname = mail.i2tch.com
mydomain= i2tch.com
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mydestination = localhost
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
delay_warning_time = 4h
recipient_delimiter = +
```

```
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
############   COMMANDES   ##############
mailbox_command = procmail -a "$EXTENSION"
############  REPERTOIRES  ##############
readme_directory = no
################  SASL  ################
smtpd_sasl_security_options = noanonymous, noplaintext
smtpd_sasl_tls_security_options = noanonymous
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
################  TLS  ################
smtpd_tls_cert_file=/etc/postfix/lel_cert.pem
smtpd_tls_key_file=/etc/postfix/lel_clef.pem
smtpd_use_tls=yes
smtp_tls_security_level = may
smtpd_tls_security_level = may
#########  VIRTUAL TRANSPORT  ###########
virtual_transport = lmtp:unix:private/dovecot-lmtp
virtual_mailbox_domains = mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
virtual_mailbox_maps = mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
virtual_alias_maps = mysql:/etc/postfix/mysql-virtual-alias-maps.cf,
        mysql:/etc/postfix/mysql-virtual-email2email.cf
```

mysql-virtual-mailbox-domains.cf

Créez maintenant le fichier **/etc/postfix/mysql-virtual-mailbox-domains.cf** :

```
root@mail:~# vi /etc/postfix/mysql-virtual-mailbox-domains.cf
root@mail:~# cat /etc/postfix/mysql-virtual-mailbox-domains.cf
```

```
user = mailuser
password = fenestros
hosts = 127.0.0.1
dbname = mailserver
query = SELECT 1 FROM virtual_domains WHERE name='%s'
```

mysql-virtual-mailbox-maps.cf

Créez maintenant le fichier **/etc/postfix/mysql-virtual-mailbox-maps.cf** :

```
root@mail:~# vi /etc/postfix/mysql-virtual-mailbox-maps.cf
root@mail:~# cat /etc/postfix/mysql-virtual-mailbox-maps.cf
user = mailuser
password = fenestros
hosts = 127.0.0.1
dbname = mailserver
query = SELECT 1 FROM virtual_users WHERE email='%s'
```

mysql-virtual-alias-maps.cf

Créez maintenant le fichier **/etc/postfix/mysql-virtual-alias-maps.cf** :

```
root@mail:~# vi /etc/postfix/mysql-virtual-alias-maps.cf
root@mail:~# cat /etc/postfix/mysql-virtual-alias-maps.cf
user = mailuser
password = fenestros
hosts = 127.0.0.1
dbname = mailserver
query = SELECT destination FROM virtual_aliases WHERE source='%s'
```

mysql-virtual-email2email.cf

Créez maintenant le fichier **/etc/postfix/mysql-virtual-email2email.cf** :

```
root@mail:~# vi /etc/postfix/mysql-virtual-email2email.cf
root@mail:~# cat /etc/postfix/mysql-virtual-email2email.cf
user = mailuser
password = fenestros
hosts = 127.0.0.1
dbname = mailserver
query = SELECT email FROM virtual_users WHERE email='%s'
```

Tester la Configuration de Postfix

Re-démarrez le service **postfix** :

```
root@mail:~# systemctl restart postfix
root@mail:~# systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
   Active: active (exited) since Thu 2019-01-24 09:13:28 CET; 29s ago
  Process: 10686 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 10686 (code=exited, status=0/SUCCESS)

janv. 24 09:13:28 mail.i2tch.com systemd[1]: Starting Postfix Mail Transport Agent...
janv. 24 09:13:28 mail.i2tch.com systemd[1]: Started Postfix Mail Transport Agent.
```

La Commande postmap

La commande postmap est utilisée pour créer, mettre à jour ou intérroger les tables de recherche de Postfix.

Exécutez la commande afin de vérifier que postfix peut intérroger la table **virtual_domains**. La commande retourne la valeur **1** en cas de réussite :

```
root@mail:~# postmap -q i2tch.com mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
1
```

Exécutez de nouveau la commande afin de vérifier que postfix peut intérroger la table **virtual_users**. La commande retourne la valeur **1** en cas de réussite :

```
root@mail:~# postmap -q root@i2tch.com mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
1
```

Exécutez maintenant la commande afin de vérifier que postfix peut obtenir l'adresse email de l'alias à partir de la table **virtual_aliases**. La commande retourne l'adresse **trainee@i2tch.com** en cas de réussite :

```
root@mail:~# postmap -q mickey.mouse@i2tch.com mysql:/etc/postfix/mysql-virtual-alias-maps.cf
trainee@i2tch.com
```

master.cf

Sauvegardez le fichier **/etc/postfix/master.cf** :

```
root@mail:~# cp /etc/postfix/master.cf /etc/postfix/master.cf.orig
```

Ouvrez le fichier **/etc/postfix/master.cf** en édition et remplacez le début du fichier avec le contenu suivant :

```
root@mail:~# vi /etc/postfix/master.cf
root@mail:~# cat /etc/postfix/master.cf
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
```

```
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================================
smtp      inet  n       -       y       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
#tlsproxy  unix  -       -       y       -       0       tlsproxy
submission inet n       -       -       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sasl_type=cyrus
  -o smtpd_sasl_path=private/auth
  -o smtpd_reject_unlisted_recipient=no
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
smtps     inet  n       -       -       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sasl_type=cyrus
  -o smtpd_sasl_path=private/auth
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
...
```

Modifier les Permissions

Modifiez les permissions sur le répertoire **/etc/postfix** ainsi :

```
root@mail:~# chmod -R o-rwx /etc/postfix
```

Dernièrement re-démarrez le service postfix :

```
root@mail:~# systemctl restart postfix
root@mail:~# systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor preset: enabled)
   Active: active (exited) since Thu 2019-01-24 09:25:31 CET; 20s ago
  Process: 11141 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 11141 (code=exited, status=0/SUCCESS)

janv. 24 09:25:31 mail.i2tch.com systemd[1]: Starting Postfix Mail Transport Agent...
janv. 24 09:25:31 mail.i2tch.com systemd[1]: Started Postfix Mail Transport Agent.
```

Configurer Dovecot

Sauvegardez tous les fichiers de configuration de Dovecot :

```
root@mail:~# cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.orig
root@mail:~# cp /etc/dovecot/conf.d/10-mail.conf /etc/dovecot/conf.d/10-mail.conf.orig
root@mail:~# cp /etc/dovecot/conf.d/10-auth.conf /etc/dovecot/conf.d/10-auth.conf.orig
root@mail:~# cp /etc/dovecot/conf.d/auth-sql.conf.ext /etc/dovecot/conf.d/auth-sql.conf.ext.orig
root@mail:~# cp /etc/dovecot/conf.d/10-master.conf /etc/dovecot/conf.d/10-master.conf.orig
root@mail:~# cp /etc/dovecot/conf.d/10-ssl.conf /etc/dovecot/conf.d/10-ssl.conf.orig
```

dovecot.conf

Editez le fichier **/etc/dovecot/dovecot.conf** en ajoutant la directive **protocols = imap pop3 lmtp** et **mail_privileged_group = mail** :

```
[root@mail ~]# vi /etc/dovecot/dovecot.conf
[root@mail ~]# cat /etc/dovecot/dovecot.conf
!include_try /usr/share/dovecot/protocols.d/*.protocol
dict {
  #quota = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
  #expire = sqlite:/etc/dovecot/dovecot-dict-sql.conf.ext
}
protocols = imap pop3 lmtp
mail_privileged_group = mail
!include conf.d/*.conf
!include_try local.conf
```

/etc/dovecot/conf.d/10-mail.conf

Editez le fichier **/etc/dovecot/conf.d/10-mail.conf** en ajoutant la directive **mail_privileged_group = mail** et en modifiant la valeur de la directive **mail_location** :

```
root@mail:~# vi /etc/dovecot/conf.d/10-mail.conf
root@mail:~# cat /etc/dovecot/conf.d/10-mail.conf
mail_location = maildir:/var/mail/vhosts/%d/%n
mail_privileged_group = mail
namespace inbox {
  inbox = yes
}
```

Créez le répertoire pour le domain **i2tch.com** :

```
root@mail:~# mkdir -p /var/mail/vhosts/i2tch.com
```

Créez le groupe **vmail** avec le GID de 5 000 ainsi que l'utilisateur **vmail** avec l'UID de 5000 dont le répertoire personnel est **/var/mail** :

```
root@mail:~# groupadd -g 5000 vmail && useradd -g vmail -u 5000 vmail -d /var/mail/
```

Modifiez le propriétaire et le groupe du répertoire **/var/mail** :

```
root@mail:~# chown -R vmail:vmail /var/mail/
```

/etc/dovecot/conf.d/10-auth.conf

Editez le fichier **/etc/dovecot/conf.d/10-auth.conf** ainsi :

```
root@mail:~# vi /etc/dovecot/conf.d/10-auth.conf
root@mail:~# cat /etc/dovecot/conf.d/10-auth.conf
disable_plaintext_auth = yes
auth_mechanisms = plain login
!include auth-system.conf.ext
!include auth-sql.conf.ext
```

/etc/dovecot/conf.d/auth-sql.conf.ext

Editez le fichier **/etc/dovecot/conf.d/auth-sql.conf.ext** ainsi :

```
root@mail:~# vi /etc/dovecot/conf.d/auth-sql.conf.ext
root@mail:~# cat /etc/dovecot/conf.d/auth-sql.conf.ext
passdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}

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

/etc/dovecot/dovecot-sql.conf.ext

Créez le fichier **/etc/dovecot/dovecot-sql.conf.ext** contenant les coordonnées de connexion à la base de données :

```
root@mail:~# vi /etc/dovecot/dovecot-sql.conf.ext
root@mail:~# cat /etc/dovecot/dovecot-sql.conf.ext
driver = mysql
connect = host=127.0.0.1 dbname=mailserver user=mailuser password=fenestros
default_pass_scheme = SHA512-CRYPT
password_query = SELECT email as user, password FROM virtual_users WHERE email='%u';
```

/etc/dovecot/conf.d/10-master.conf

Editez le fichier **/etc/dovecot/conf.d/10-master.conf** ainsi :

```
root@mail:~# vi /etc/dovecot/conf.d/10-master.conf
root@mail:~# cat /etc/dovecot/conf.d/10-master.conf
service imap-login {
  inet_listener imap {
    port = 0
  }
  inet_listener imaps {
    port = 993
    ssl = yes
  }

}
service pop3-login {
  inet_listener pop3 {
    port = 0
  }
  inet_listener pop3s {
```

```
    port = 995
    ssl = yes
  }
}
service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    mode = 0600
    user = postfix
    group = postfix
  }
}
service imap {

}
service pop3 {

}
service auth {
  unix_listener auth-userdb {
    mode = 0600
    user = vmail
  }

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

  user = dovecot
}
service auth-worker {
  user = vmail
}
```

```
service dict {

  unix_listener dict {

  }
}
```

Dernières Configurations

Modifiez le propriétaire et les permissions du répertoire **/etc/dovecot** :

```
root@mail:~# chown -R vmail:dovecot /etc/dovecot
root@mail:~# chmod -R o-rwx /etc/dovecot
```

Re-démarrez le service dovecot :

```
root@mail:~# systemctl restart dovecot
root@mail:~# systemctl status dovecot
● dovecot.service - Dovecot IMAP/POP3 email server
   Loaded: loaded (/lib/systemd/system/dovecot.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2019-01-24 10:12:16 CET; 5s ago
     Docs: man:dovecot(1)
           http://wiki2.dovecot.org/
  Process: 11919 ExecStop=/usr/bin/doveadm stop (code=exited, status=0/SUCCESS)
  Process: 11924 ExecStart=/usr/sbin/dovecot (code=exited, status=0/SUCCESS)
 Main PID: 11925 (dovecot)
    Tasks: 4 (limit: 4915)
   CGroup: /system.slice/dovecot.service
           ├─11925 /usr/sbin/dovecot
           ├─11926 dovecot/anvil
           ├─11927 dovecot/log
           └─11929 dovecot/config
```

```
janv. 24 10:12:16 mail.i2tch.com systemd[1]: Starting Dovecot IMAP/POP3 email server...
janv. 24 10:12:16 mail.i2tch.com systemd[1]: dovecot.service: PID file /var/run/dovecot/master.pid not readable
(yet?) after start: No such file or directory
janv. 24 10:12:16 mail.i2tch.com dovecot[11925]: master: Dovecot v2.2.27 (c0f36b0) starting up for imap, pop3,
lmtp (core dumps disabled)
janv. 24 10:12:16 mail.i2tch.com systemd[1]: Started Dovecot IMAP/POP3 email server.
```

Tester la Configuration

trainee@i2tch.com

Envoyez un message à **trainee@i2tch.com** :

```
root@mail:~# mail trainee@i2tch.com
Cc:
Subject: Test
This is a test using MariaDB
[^D]
```

Consultez la fin du fichier **/var/log/mail.log** :

```
root@mail:~# tail /var/log/mail.log
Jan 24 10:17:05 mail postfix/master[12137]: /etc/postfix/master.cf: line 26: using backwards-compatible default
setting chroot=y
Jan 24 10:17:05 mail postfix/master[12137]: daemon started -- version 3.1.8, configuration /etc/postfix
Jan 24 10:17:30 mail postfix/pickup[12139]: 395AE606EA: uid=0 from=<root@mail.i2tch.com>
Jan 24 10:17:30 mail postfix/cleanup[12145]: 395AE606EA: message-id=<20190124091730.395AE606EA@mail.i2tch.com>
Jan 24 10:17:30 mail postfix/qmgr[12140]: 395AE606EA: from=<root@mail.i2tch.com>, size=354, nrcpt=1 (queue
active)
Jan 24 10:17:30 mail dovecot: lmtp(12148): Connect from local
Jan 24 10:17:30 mail dovecot: lmtp(trainee@i2tch.com): D9w+D6qCSVx0LwAAUpw4tw:
msgid=<20190124091730.395AE606EA@mail.i2tch.com>: saved mail to INBOX
```

```
Jan 24 10:17:30 mail postfix/lmtp[12147]: 395AE606EA: to=<trainee@i2tch.com>,
relay=mail.i2tch.com[private/dovecot-lmtp], delay=0.1, delays=0.06/0.01/0/0.03, dsn=2.0.0, status=sent (250 2.0.0
<trainee@i2tch.com> D9w+D6qCSVx0LwAAUpw4tw Saved)
Jan 24 10:17:30 mail dovecot: lmtp(12148): Disconnect from local: Successful quit
Jan 24 10:17:30 mail postfix/qmgr[12140]: 395AE606EA: removed
```

Important - Notez que le message à trainee@i2tch.com a bien été livré.

Installez le client mail **mutt** et lancez-le :

```
root@mail:~# cd /var/mail/vhosts/i2tch.com/trainee
root@mail:/var/mail/vhosts/i2tch.com/trainee# apt-get install mutt
[root@mail trainee]# mutt -f .
```

Constatez la présence du message **Test MariaDB** :

```
q:Quitter  d:Effacer  u:Récup  s:Sauver  m:Message  r:Répondre  g:Groupe  ?:Aide
   1 N F janv. 24 To trainee@i2tc (0,1K) Test
```

En sélectionnant ce message, vous constaterez son contenu :

```
i:Quitter  -:PgPréc  <Space>:PgSuiv v:Voir attach.  d:Effacer  r:Répondre  j:Suivant ?:Aide
Date: Thu, 24 Jan 2019 10:17:30 +0100 (CET)
From: root <root@mail.i2tch.com>
To: trainee@i2tch.com
Subject: Test
X-Mailer: mail (GNU Mailutils 3.1.1)

This is a test using MariaDB
```

Consultez le contenu du répertoire **/var/mail/vhosts/i2tch.com/trainee/** :

```
root@mail:/var/mail/vhosts/i2tch.com/trainee# find
.
./dovecot-uidlist
./cur
./cur/1548321450.M272340P12148.mail.i2tch.com,S=564,W=579:2,S
./dovecot.index.cache
./dovecot-uidvalidity.5c4982aa
./new
./dovecot-uidvalidity
./tmp
./dovecot.index.log
root@mail:/var/mail/vhosts/i2tch.com/trainee# cd cur
root@mail:/var/mail/vhosts/i2tch.com/trainee/cur# ls
1548321450.M272340P12148.mail.i2tch.com,S=564,W=579:2,S
root@mail:/var/mail/vhosts/i2tch.com/trainee/cur# cat
1548321450.M272340P12148.mail.i2tch.com\,S\=564\,W\=579\:2\,S
Return-Path: <root@mail.i2tch.com>
Delivered-To: trainee@i2tch.com
Received: from mail.i2tch.com
    by mail.i2tch.com (Dovecot) with LMTP id D9w+D6qCSVx0LwAAUpw4tw
    for <trainee@i2tch.com>; Thu, 24 Jan 2019 10:17:30 +0100
Received: by mail.i2tch.com (Postfix, from userid 0)
    id 395AE606EA; Thu, 24 Jan 2019 10:17:30 +0100 (CET)
To: <trainee@i2tch.com>
Subject: Test
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <20190124091730.395AE606EA@mail.i2tch.com>
Date: Thu, 24 Jan 2019 10:17:30 +0100 (CET)
From: root@mail.i2tch.com (root)

This is a test using MariaDB
```

Important - Notez que le message à trainee@i2tch.com se trouve dans le sous-répertoire **cur**.

mickey.mouse@i2tch.com

Envoyez un message maintenant à **mickey.mouse@i2tch.com** :

```
root@mail:~# mail mickey.mouse@i2tch.com
Cc:
Subject: Test Mickey Mouse
This is a test to Mickey Mouse
[^D]
```

Consultez la fin du fichier **/var/log/mail.log** :

```
root@mail:~# tail /var/log/mail.log
Jan 24 10:17:30 mail dovecot: lmtp(12148): Disconnect from local: Successful quit
Jan 24 10:17:30 mail postfix/qmgr[12140]: 395AE606EA: removed
Jan 24 10:31:38 mail postfix/pickup[12139]: 2C095606D4: uid=0 from=<root@mail.i2tch.com>
Jan 24 10:31:38 mail postfix/cleanup[12467]: 2C095606D4: message-id=<20190124093138.2C095606D4@mail.i2tch.com>
Jan 24 10:31:38 mail postfix/qmgr[12140]: 2C095606D4: from=<root@mail.i2tch.com>, size=374, nrcpt=1 (queue
active)
Jan 24 10:31:38 mail dovecot: lmtp(12470): Connect from local
Jan 24 10:31:38 mail dovecot: lmtp(trainee@i2tch.com): 3JxyDPqFSVy2MAAAUpw4tw:
msgid=<20190124093138.2C095606D4@mail.i2tch.com>: saved mail to INBOX
Jan 24 10:31:38 mail postfix/lmtp[12469]: 2C095606D4: to=<trainee@i2tch.com>, orig_to=<mickey.mouse@i2tch.com>,
relay=mail.i2tch.com[private/dovecot-lmtp], delay=0.13, delays=0.09/0.01/0.01/0.02, dsn=2.0.0, status=sent (250
2.0.0 <trainee@i2tch.com> 3JxyDPqFSVy2MAAAUpw4tw Saved)
Jan 24 10:31:38 mail dovecot: lmtp(12470): Disconnect from local: Successful quit
Jan 24 10:31:38 mail postfix/qmgr[12140]: 2C095606D4: removed
```

Important - Notez que le message à mickey.mouse@i2tch.com a bien été livré à trainee@i2tch.com.

Consultez le contenu du répertoire **/var/mail/vhosts/i2tch.com/trainee/** :

```
root@mail:/var/mail/vhosts/i2tch.com/trainee/cur# cd ..
root@mail:/var/mail/vhosts/i2tch.com/trainee# find
.
./dovecot-uidlist
./cur
./cur/1548321450.M272340P12148.mail.i2tch.com,S=564,W=579:2,S
./dovecot.index.cache
./dovecot-uidvalidity.5c4982aa
./new
./new/1548322298.M224264P12470.mail.i2tch.com,S=584,W=599
./dovecot-uidvalidity
./tmp
./dovecot.index.log
root@mail:/var/mail/vhosts/i2tch.com/trainee# cd new
root@mail:/var/mail/vhosts/i2tch.com/trainee/new# ls
1548322298.M224264P12470.mail.i2tch.com,S=584,W=599
root@mail:/var/mail/vhosts/i2tch.com/trainee/new# cat 1548322298.M224264P12470.mail.i2tch.com\,S\=584\,W\=599
Return-Path: <root@mail.i2tch.com>
Delivered-To: trainee@i2tch.com
Received: from mail.i2tch.com
    by mail.i2tch.com (Dovecot) with LMTP id 3JxyDPqFSVy2MAAAUpw4tw
    for <trainee@i2tch.com>; Thu, 24 Jan 2019 10:31:38 +0100
Received: by mail.i2tch.com (Postfix, from userid 0)
    id 2C095606D4; Thu, 24 Jan 2019 10:31:38 +0100 (CET)
To: <mickey.mouse@i2tch.com>
Subject: Test Mickey Mouse
```

```
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <20190124093138.2C095606D4@mail.i2tch.com>
Date: Thu, 24 Jan 2019 10:31:38 +0100 (CET)
From: root@mail.i2tch.com (root)

This is a test to Mickey Mouse
```

Important - Notez que le message à mickey.mouse@i2tch.com se trouve dans le sous-répertoire **new**.

trainee@mail.i2tch.com

Envoyez un message à trainee@mail.i2tch.com et constatez son statut :

```
root@mail:/var/mail/vhosts/i2tch.com/trainee/new# mail trainee@mail.i2tch.com
Cc:
Subject: Test
This is a test to the mail.i2tch.com domain
[^D]
root@mail:/var/mail/vhosts/i2tch.com/trainee/new# tail /var/log/mail.log
Jan 24 11:03:46 mail postfix/local[12496]: 8FC9C6070D: to=<trainee@mail.i2tch.com>, relay=local, delay=0.11,
delays=0.1/0.01/0/0, dsn=2.0.0, status=sent (delivered to command: procmail -a "$EXTENSION")
Jan 24 11:03:46 mail postfix/qmgr[12140]: 8FC9C6070D: removed
Jan 24 11:07:06 mail postfix/pickup[12139]: 2739B6070D: uid=0 from=<root@mail.i2tch.com>
Jan 24 11:07:06 mail postfix/cleanup[12507]: 2739B6070D: message-id=<20190124100706.2739B6070D@mail.i2tch.com>
Jan 24 11:07:06 mail postfix/qmgr[12140]: 2739B6070D: from=<root@mail.i2tch.com>, size=374, nrcpt=1 (queue
active)
Jan 24 11:07:06 mail dovecot: lmtp(12510): Connect from local
Jan 24 11:07:06 mail dovecot: lmtp(trainee@mail.i2tch.com): t/4YC0qOSVzeMAAAUpw4tw:
msgid=<20190124100706.2739B6070D@mail.i2tch.com>: saved mail to INBOX
```

```
Jan 24 11:07:06 mail postfix/lmtp[12509]: 2739B6070D: to=<trainee@mail.i2tch.com>,
relay=mail.i2tch.com[private/dovecot-lmtp], delay=0.06, delays=0.02/0.01/0.01/0.03, dsn=2.0.0, status=sent (250
2.0.0 <trainee@mail.i2tch.com> t/4YC0qOSVzeMAAAUpw4tw Saved)
Jan 24 11:07:06 mail dovecot: lmtp(12510): Disconnect from local: Successful quit
Jan 24 11:07:06 mail postfix/qmgr[12140]: 2739B6070D: removed
```

Bien qu'envoyé, ce message n'apparait pas dans le dossier **/var/mail/vhosts/i2tch.com/trainee/new** :

```
root@mail:/var/mail/vhosts/i2tch.com/trainee/new# ls
1548322298.M224264P12470.mail.i2tch.com,S=584,W=599
root@mail:/var/mail/vhosts/i2tch.com/trainee/new# cd ..
root@mail:/var/mail/vhosts/i2tch.com/trainee# find
.
./dovecot-uidlist
./cur
./cur/1548321450.M272340P12148.mail.i2tch.com,S=564,W=579:2,S
./dovecot.index.cache
./dovecot-uidvalidity.5c4982aa
./new
./new/1548322298.M224264P12470.mail.i2tch.com,S=584,W=599
./dovecot-uidvalidity
./tmp
./dovecot.index.log
```

En effet, le message a été placé dans le répertoire /var/mail/vhosts/**mail.i2tch.com**/trainee/new :

```
root@mail:/var/mail/vhosts/i2tch.com/trainee/new# cd ~
root@mail:~# ls /var/mail/vhosts/
i2tch.com  mail.i2tch.com
root@mail:~# cd /var/mail/vhosts/mail.i2tch.com/
root@mail:/var/mail/vhosts/mail.i2tch.com# find
.
./trainee
./trainee/dovecot-uidlist
```

```
./trainee/cur
./trainee/dovecot.index.cache
./trainee/dovecot-uidvalidity.5c498e4a
./trainee/new
./trainee/new/1548324426.M202144P12510.mail.i2tch.com,S=594,W=609
./trainee/dovecot-uidvalidity
./trainee/tmp
./trainee/dovecot.index.log
root@mail:/var/mail/vhosts/mail.i2tch.com# cat
trainee/new/1548324426.M202144P12510.mail.i2tch.com\,S\=594\,W\=609
Return-Path: <root@mail.i2tch.com>
Delivered-To: trainee@mail.i2tch.com
Received: from mail.i2tch.com
    by mail.i2tch.com (Dovecot) with LMTP id t/4YC0qOSVzeMAAAUpw4tw
    for <trainee@mail.i2tch.com>; Thu, 24 Jan 2019 11:07:06 +0100
Received: by mail.i2tch.com (Postfix, from userid 0)
    id 2739B6070D; Thu, 24 Jan 2019 11:07:06 +0100 (CET)
To: <trainee@mail.i2tch.com>
Subject: test
X-Mailer: mail (GNU Mailutils 3.1.1)
Message-Id: <20190124100706.2739B6070D@mail.i2tch.com>
Date: Thu, 24 Jan 2019 11:07:06 +0100 (CET)
From: root@mail.i2tch.com (root)

This is a test to the mail.i2tch.com domain
```

LAB #9 - Configuration de Postfix en Environnement chroot

Configuration de Postfix

Sous Debian 9, postfix est **chrooté** par défaut :

```
root@mail:~# cd /var/spool/postfix/
root@mail:/var/spool/postfix# ls
active  bounce    corrupt  defer    deferred  dev  etc  flush  hold  incoming  lib    maildrop  pid  private
public    saved  trace  usr
root@mail:/var/spool/postfix# cd etc
root@mail:/var/spool/postfix/etc# ls
host.conf  hosts  localtime  nsswitch.conf  resolv.conf  services  ssl
root@mail:/var/spool/postfix/etc# cd ../dev
root@mail:/var/spool/postfix/dev# ls
log  random  urandom
root@mail:/var/spool/postfix/dev# cd ../lib
root@mail:/var/spool/postfix/lib# ls
x86_64-linux-gnu
root@mail:/var/spool/postfix/lib# cd x86_64-linux-gnu/
root@mail:/var/spool/postfix/lib/x86_64-linux-gnu# ls
libgcc_s.so.1          libnss_dns-2.24.so    libnss_files.so.2        libnss_mdns4_minimal.so.2
libnss_mdns6.so.2     libnss_nis-2.24.so     libnss_nis.so.2
libnss_compat-2.24.so  libnss_dns.so.2       libnss_hesiod-2.24.so  libnss_mdns4.so.2
libnss_mdns_minimal.so.2  libnss_nisplus-2.24.so  libresolv-2.24.so
libnss_compat.so.2     libnss_files-2.24.so  libnss_hesiod.so.2     libnss_mdns6_minimal.so.2  libnss_mdns.so.2
libnss_nisplus.so.2     libresolv.so.2
root@mail:/var/spool/postfix/lib/x86_64-linux-gnu# cd ../../usr
root@mail:/var/spool/postfix/usr# ls
lib
root@mail:/var/spool/postfix/usr# cd lib
root@mail:/var/spool/postfix/usr/lib# ls
sasl2  zoneinfo
```

```
root@mail:~# head -n 15 /etc/postfix/master.cf
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
#
```

```
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================================
smtp      inet  n       -       y       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
```

Configuration de SASL

Dans ce cas, la configuration de sasl doit être modifiée. Commencez par installer le paquet **sasl2-bin** :

```
root@mail:/var/spool/postfix/usr/lib# cd ~
root@mail:~# apt-get install sasl2-bin
```

Modifiez la directive **START** du fichier **/etc/default/saslauthd** afin que saslauthd démarre au démarrage du système. Modifiez la directive **OPTIONS** pour la prise en compte du chroot :

```
root@mail:~# vi /etc/default/saslauthd
root@mail:~# cat /etc/default/saslauthd
#
# Settings for saslauthd daemon
# Please read /usr/share/doc/sasl2-bin/README.Debian for details.
#

# Should saslauthd run automatically on startup? (default: no)
START=yes

# Description of this saslauthd instance. Recommended.
# (suggestion: SASL Authentication Daemon)
```

```
DESC="SASL Authentication Daemon"

# Short name of this saslauthd instance. Strongly recommended.
# (suggestion: saslauthd)
NAME="saslauthd"

# Which authentication mechanisms should saslauthd use? (default: pam)
#
# Available options in this Debian package:
# getpwent  -- use the getpwent() library function
# kerberos5 -- use Kerberos 5
# pam       -- use PAM
# rimap     -- use a remote IMAP server
# shadow    -- use the local shadow password file
# sasldb    -- use the local sasldb database file
# ldap      -- use LDAP (configuration is in /etc/saslauthd.conf)
#
# Only one option may be used at a time. See the saslauthd man page
# for more information.
#
# Example: MECHANISMS="pam"
MECHANISMS="pam"

# Additional options for this mechanism. (default: none)
# See the saslauthd man page for information about mech-specific options.
MECH_OPTIONS=""

# How many saslauthd processes should we run? (default: 5)
# A value of 0 will fork a new process for each connection.
THREADS=5

# Other options (default: -c -m /var/run/saslauthd)
# Note: You MUST specify the -m option or saslauthd won't run!
#
```

```
# WARNING: DO NOT SPECIFY THE -d OPTION.
# The -d option will cause saslauthd to run in the foreground instead of as
# a daemon. This will PREVENT YOUR SYSTEM FROM BOOTING PROPERLY. If you wish
# to run saslauthd in debug mode, please run it by hand to be safe.
#
# See /usr/share/doc/sasl2-bin/README.Debian for Debian-specific information.
# See the saslauthd man page and the output of 'saslauthd -h' for general
# information about these options.
#
# Example for chroot Postfix users: "-c -m /var/spool/postfix/var/run/saslauthd"
# Example for non-chroot Postfix users: "-c -m /var/run/saslauthd"
#
# To know if your Postfix is running chroot, check /etc/postfix/master.cf.
# If it has the line "smtp inet n - y - - smtpd" or "smtp inet n - - - - smtpd"
# then your Postfix is running in a chroot.
# If it has the line "smtp inet n - n - - smtpd" then your Postfix is NOT
# running in a chroot.
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"
```

Les méchanisms de vérification des mots de passe supportés par saslauthd peuvent être visualisés en utilisant l'option **-v** de la commande **saslauthd** :

```
root@mail:~# saslauthd -v
saslauthd 2.1.27
authentication mechanisms: sasldb getpwent kerberos5 pam rimap shadow ldap
```

Dans le cas de Postfix, le serveur qui prend en charge les reqûetes d'authentification est **smtpd** avec la fonction **SMTP AUTH**. Vérifiez que postfix a été installé avec le support pour **SMTP AUTH** :

```
root@mail:~# apt-get install locate
root@mail:~# updatedb
root@mail:~# locate smtpd
/usr/lib/postfix/sbin/smtpd
/usr/lib/python2.7/smtpd.py
/usr/lib/python2.7/smtpd.pyc
```

```
/usr/lib/python3.5/__pycache__/smtpd.cpython-35.pyc
/usr/lib/python3.5/smtpd.py
/usr/share/man/man8/smtpd.8postfix.gz
root@mail:~# ldd /usr/lib/postfix/sbin/smtpd | grep libsasl
    libsasl2.so.2 => /usr/lib/x86_64-linux-gnu/libsasl2.so.2 (0x00007f4bbe78a000)
```

Important - La présence de la bibliothèque **libsasl2** indique que postfix a été installé avec le support pour SASL.

Dans le fichier **/etc/postfix/main.cf** remplacez leslignes de la section SASL avec les lignes suivantes :

```
...
############      SASL     ##############
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
                                  reject_non_fqdn_sender,
                                  reject_non_fqdn_recipient,
                                  reject_unknown_sender_domain,
                                  reject_unknown_recipient_domain,
                                  reject_unauth_pipelining,
                                  reject_rbl_client zen.spamhaus.org,
                                  reject_rbl_client bl.spamcop.net,
                                  reject_rbl_client dnsbl.njabl.org,
                                  reject_rbl_client dnsbl.sorbs.net,
                                  permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
```

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = i2tch.com
smtpd_helo_required = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = cyrus
cyrus_sasl_config_path = /etc/postfix/sasl
```

Vous obtiendrez le résultat suivant :

```
root@mail:~# vi /etc/postfix/main.cf
root@mail:~# cat /etc/postfix/main.cf
#############CONFIG DE BASE##############
myhostname = mail.i2tch.com
mydomain= i2tch.com
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mydestination = localhost
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
#############   COMMANDES   ##############
mailbox_command = procmail -a "$EXTENSION"
############  REPERTOIRES  ##############
readme_directory = no
################  SASL  #################
############      SASL     ##############
```

```
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
                                  reject_non_fqdn_sender,
                                  reject_non_fqdn_recipient,
                                  reject_unknown_sender_domain,
                                  reject_unknown_recipient_domain,
                                  reject_unauth_pipelining,
                                  reject_rbl_client zen.spamhaus.org,
                                  reject_rbl_client bl.spamcop.net,
                                  reject_rbl_client dnsbl.njabl.org,
                                  reject_rbl_client dnsbl.sorbs.net,
                                  permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtp_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = i2tch.com
smtpd_helo_required = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = dovecot
cyrus_sasl_config_path = /etc/postfix/sasl
#################  TLS  #################
smtpd_tls_cert_file=/etc/postfix/lel_cert.pem
smtpd_tls_key_file=/etc/postfix/lel_clef.pem
smtpd_use_tls=yes
smtp_tls_security_level = may
smtpd_tls_security_level = may
#########  VIRTUAL TRANSPORT  ############
```

```
virtual_transport = lmtp:unix:private/dovecot-lmtp
virtual_mailbox_domains = mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
virtual_mailbox_maps = mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
virtual_alias_maps = mysql:/etc/postfix/mysql-virtual-alias-maps.cf,
        mysql:/etc/postfix/mysql-virtual-email2email.cf
```

Rechargez la configuration de postfix :

```
root@mail:~# systemctl reload postfix
```

Créez le répertoire **/var/spool/postfix/etc/postfix/sasl** :

```
root@mail:~# mkdir -p /var/spool/postfix/etc/postfix/sasl
```

Créez maintenant le fichier **/etc/postfix/sasl/smtpd.conf** :

```
root@mail:~# vi /etc/postfix/sasl/smtpd.conf
root@mail:~# cat /etc/postfix/sasl/smtpd.conf
pwcheck_method: saslauthd
mech_list: PLAIN LOGIN
```

Pour tester l'authentification, vous devez envoyer un nom d'utilisateur et un mot de passe encodés en **base64**. Créez donc une chaîne de caractères encodés en base64 grâce à Perl en utilisant le format **utilisateur\0utilisateur\0motdepasse** :

```
root@mail:~# perl -MMIME::Base64 -e 'print encode_base64("trainee\0trainee\0trainee");'
dHJhaW5lZQB0cmFpbmVlAHRyYWluZWU=
```

Re-démarrez le service **saslauthd** :

```
root@mail:~# systemctl restart saslauthd
root@mail:~# systemctl status saslauthd
● saslauthd.service - LSB: saslauthd startup script
   Loaded: loaded (/etc/init.d/saslauthd; generated; vendor preset: enabled)
```

```
   Active: active (running) since Thu 2019-01-24 11:35:27 CET; 7s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 12857 ExecStop=/etc/init.d/saslauthd stop (code=exited, status=0/SUCCESS)
  Process: 12873 ExecStart=/etc/init.d/saslauthd start (code=exited, status=0/SUCCESS)
    Tasks: 5 (limit: 4915)
   CGroup: /system.slice/saslauthd.service
           ├─12895 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5
           ├─12896 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5
           ├─12897 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5
           ├─12898 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5
           └─12899 /usr/sbin/saslauthd -a pam -c -m /var/run/saslauthd -n 5

janv. 24 11:35:26 mail.i2tch.com systemd[1]: Stopped LSB: saslauthd startup script.
janv. 24 11:35:26 mail.i2tch.com systemd[1]: Starting LSB: saslauthd startup script...
janv. 24 11:35:27 mail.i2tch.com saslauthd[12873]: Starting SASL Authentication Daemon: saslauthd.
janv. 24 11:35:27 mail.i2tch.com systemd[1]: Started LSB: saslauthd startup script.
janv. 24 11:35:27 mail.i2tch.com saslauthd[12895]:                : master pid is: 12895
janv. 24 11:35:27 mail.i2tch.com saslauthd[12895]:                : listening on socket: /var/run/saslauthd/mux
```

Mettez l'utilisateur postfix dans ls groupe **sasl** :

```
root@mail:~# usermod -a -G sasl postfix
```

Testez saslauthd en utilisant la commande **testsaslauthd** :

```
root@mail:~# testsaslauthd -u trainee -p trainee
0: OK "Success."
```

Connectez-vous maintenant au serveur postfix sur le port 25 :

```
root@mail:~# telnet localhost 25
Trying ::1...
Connected to localhost.
Escape character is '^]'.
```

```
220 mail.i2tch.com ESMTP Postfix (Debian/GNU)
EHLO me
250-mail.i2tch.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH PLAIN dHJhaW5lZQB0cmFpbmVlAHRyYWluZWU=
235 2.7.0 Authentication successful
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Configuration de TLS

Dans le fichier **/etc/postfix/main.cf** remplacez leslignes de la section TLS avec les lignes suivantes : :

```
...
############      TLS      ##############
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_sesson_cache
smtp_tls_security_level = may
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_sesson_cache
smtpd_tls_cert_file = /etc/postfix/lel_cert.pem
smtpd_tls_key_file = /etc/postfix/lel_clef.pem
smtpd_tls_received_header = yes
```

```
tls_random_source = dev:/dev/urandom
smtpd_tls_security_level = may
smtpd_tls_loglevel = 2
smtpd_tls_ask_ccert = no
```

Vous obtiendrez un résultat similaire à celui-ci :

```
root@mail:~# cat /etc/postfix/main.cf
#############CONFIG DE BASE##############
myhostname = mail.i2tch.com
mydomain= i2tch.com
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mydestination = localhost
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
#############   COMMANDES   ##############
mailbox_command = procmail -a "$EXTENSION"
#############  REPERTOIRES  ##############
readme_directory = no
#############      SASL     ##############
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
```

```
                                    reject_non_fqdn_sender,
                                    reject_non_fqdn_recipient,
                                    reject_unknown_sender_domain,
                                    reject_unknown_recipient_domain,
                                    reject_unauth_pipelining,
                                    reject_rbl_client zen.spamhaus.org,
                                    reject_rbl_client bl.spamcop.net,
                                    reject_rbl_client dnsbl.njabl.org,
                                    reject_rbl_client dnsbl.sorbs.net,
                                    permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = i2tch.com
smtpd_helo_required = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = cyrus
cyrus_sasl_config_path = /etc/postfix/sasl
############      TLS      ##############
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_sesson_cache
smtp_tls_security_level = may
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_sesson_cache
smtpd_tls_cert_file = /etc/postfix/lel_cert.pem
smtpd_tls_key_file = /etc/postfix/lel_clef.pem
smtpd_tls_received_header = yes
tls_random_source = dev:/dev/urandom
smtpd_tls_security_level = may
smtpd_tls_loglevel = 2
smtpd_tls_ask_ccert = no
#########  VIRTUAL TRANSPORT  ############
```

```
virtual_transport = lmtp:unix:private/dovecot-lmtp
virtual_mailbox_domains = mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
virtual_mailbox_maps = mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf
virtual_alias_maps = mysql:/etc/postfix/mysql-virtual-alias-maps.cf,
        mysql:/etc/postfix/mysql-virtual-email2email.cf
```

Rechargez la configuration de postfix :

```
[root@mail misc]# systemctl reload postfix
```

Testez maintenant le serveur postfix afin de savoir si celui-ci a pris en compte **TLS** :

```
root@mail:~# openssl s_client -starttls smtp -connect mail.i2tch.com:25
CONNECTED(00000003)
depth=1 C = GB, ST = SURREY, O = I2TCH LTD, OU = TRAINING, CN = i2tch.com, emailAddress = infos@i2tch.com
verify error:num=19:self signed certificate in certificate chain
---
Certificate chain
 0 s:/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=mail.i2tch.com/emailAddress=infos@i2tch.com
   i:/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=i2tch.com/emailAddress=infos@i2tch.com
 1 s:/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=i2tch.com/emailAddress=infos@i2tch.com
   i:/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=i2tch.com/emailAddress=infos@i2tch.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIID9TCCAt2gAwIBAgIJAPEavi5fdQyUMA0GCSqGSIb3DQEBCwUAMHkxCzAJBgNV
BAYTAkdCMQ8wDQYDVQQIDAZTVVJSRVkxEjAQBgNVBAoMCUkyVENIIExURDERMA8G
A1UECwwIVFJBSU5JTkcxEjAQBgNVBAMMCWkydGNoLmNvbTEeMBwGCSqGSIb3DQEJ
ARYPaW5mb3NAaTJ0Y2guY29tMB4XDTE5MDEyNDA2MzUzMloXDTIwMDEyNDA2MzUz
MlowfjELMAkGA1UEBhMCR0IxDzANBgNVBAgMBlNVUlJFWTESMBAGA1UECgwJSTJU
Q0ggTFREMREwDwYDVQQLDAhUUkFJTklORzEXMBUGA1UEAwwObWFpbC5pMnRjaC5j
b20xHjAcBgkqhkiG9w0BCQEWD2luZm9zQGkydGNoLmNvbTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAP8QFliKvC/ipomSl+RYfYjV9/wyGYgCDNcJcQp2
DZ5ofS5bYcMt3izD6G0GopUfIM+NxyPYWUa6d5tVP0cPtw3aGiPN/je9MgIDvB8C
```

```
E+0g4bJCI+ghaCYFaPQ+41gSYVUlNjQVyKEweKThZJ35yRcns518AQhTZiVFQm1y
en2ZRJs5uqknq/9pN23G18OzXOZX+IdqoptlWYctrqqvR8QrK8nu1RJRhhcnChV0
/MI3kbR+0GIhGeZXT6YLEWuKE+/63V8LWppriUSQR+dMnDfhft2DVMPnuaYv0st4
WpiwSjH9ZJgKS5u0fLM4hrDA7mUwlxmBD8vkEKu4X/Ua8McCAwEAAaN7MHkwCQYD
VR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlm
aWNhdGUwHQYDVR0OBBYEFF5KH1E5/wgFL7LwTMFqDE/ajTxNMB8GA1UdIwQYMBaA
FMjHUBgB9mPEmGMdGmizeYAK2q0LMA0GCSqGSIb3DQEBCwUAA4IBAQC26hXBGpwL
bpbFoFgzJxvjhDXI4+4HY1MDOYXdrzv0ZVABPc5OfdtvzV14wEM6Q9zxnvuZ0CzE
yVyGLPwR4STMxdF2yc6o5dMVw3fAcetmjxHCD7p4eMALToLA/e9Prh3GhPfhGNs/
v8ijz9NH/Lt3NNoxoZr0Nb+dEgp3rhEFdSzP1Q/YMUe48WYRhlrGEPL20xmgXwMi
TyvnbOcHn3tDZuGgLRRvYI9y/M6q0sK5/aW5TIP76xuUpAULFd5RrB8nrEpxqvTQ
FD1EZRfG2i4xnPmD2t72UoKO3/1dJOkGlsQ/ac34VMeUHOkFKZXYd8xQZsVeICgP
GYCzs+5txGR7
-----END CERTIFICATE-----
subject=/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=mail.i2tch.com/emailAddress=infos@i2tch.com
issuer=/C=GB/ST=SURREY/O=I2TCH LTD/OU=TRAINING/CN=i2tch.com/emailAddress=infos@i2tch.com
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 2924 bytes and written 335 bytes
Verification error: self signed certificate in certificate chain
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: B50C7C9A6350615AF4BF3B839F32FAD6B6AE750E27C3F0E2EC6B2FA0F09E5B5A
```

```
    Session-ID-ctx:
    Master-Key: D1405647C8069180F3C8374E7041072F06B2EDBEBE94C75508D16EF233BF06B17F752FA03588710F82A7701A6AFA8C9A
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 75 55 08 90 60 54 8d e6-5a f6 eb 12 41 42 62 88   uU..`T..Z...ABb.
    0010 - 1c e8 2e 03 c2 2e 17 c1-31 e8 26 bb f8 d7 32 91   ........1.&...2.
    0020 - 09 22 0d 8b 15 7f a3 0d-6e 90 ab f2 7d db 26 f3   ."......n...}.&.
    0030 - f8 fb 1f d5 c6 9c ea 3c-ca f6 de 08 3a a3 76 5c   .......<....:.v\
    0040 - a2 70 a8 17 f9 aa 34 f7-fc a3 e5 08 30 6f 10 85   .p....4.....0o..
    0050 - 2e 3b ed 8e d5 ee c0 ad-46 30 aa f4 f5 90 24 73   .;......F0....$s
    0060 - ad 72 1e 2d 7f cc 4e 20-43 01 5b 5b 63 1a 01 95   .r.-..N C.[[c...
    0070 - b8 ef 24 98 61 86 0d fc-c6 c5 4b 29 58 44 4c 68   ..$.a.....K)XDLh
    0080 - b9 78 22 0e 7a ea 36 3a-bb fd 67 d2 61 2f 6e 86   .x".z.6:..g.a/n.
    0090 - 4d af 86 f3 30 a3 79 89-2b b6 20 2e 0a 9a e1 a0   M...0.y.+. .....
    00a0 - 4d f0 2d ef 8c 99 88 af-3d bc ef d5 01 52 83 61   M.-.....=....R.a

    Start Time: 1548332024
    Timeout   : 7200 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
    Extended master secret: yes
---
250 DSN
QUIT
DONE
```

Important - Notez la présence de l'erreur 19 (self signed certificate in certificate chain).

Afin de configurer Postfix pour écouter sur les ports **tcp/465** et **tcp/587**, il convient d'ajouter les deux ligne suivantes au fichier

/etc/postfix/master.cf :

```
...
# Port 465 pour SSL
465     inet    n       -       n       -       -       smtpd
# Port 587 pour TLS
587     inet    n       -       n       -       -       smtpd
...
```

Vous obtiendrez donc le résultat suivant :

```
root@mail:~# vi /etc/postfix/master.cf
root@mail:~# head -n 20 /etc/postfix/master.cf
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master" or
# on-line: http://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
# Port 465 pour SSL
465     inet    n       -       n       -       -       smtpd
# Port 587 pour TLS
587     inet    n       -       n       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
#tlsproxy  unix  -       -       y       -       0       tlsproxy
```

Rechargez les fichiers de configuration de Postfix :

```
[root@mail ~]# systemctl reload postfix
```

Utilisez la commande **netstat** pour vérifier que les ports soient à l'écoute :

```
root@mail:~# apt-get install net-tools
root@mail:~# netstat -lnp | grep 587
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN      12549/master
tcp6       0      0 :::587                  :::*                    LISTEN      12549/master
root@mail:~# netstat -lnp | grep 465
tcp        0      0 0.0.0.0:465             0.0.0.0:*               LISTEN      12549/master
tcp6       0      0 :::465                  :::*                    LISTEN      12549/master
```

Testez donc TLS :

```
root@mail:~# telnet localhost 587
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (Debian/GNU)
EHLO me
250-mail.i2tch.com
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
STARTTLS
220 2.0.0 Ready to start TLS
QUIT
```

```
Connection closed by foreign host.
```

<html>

</html>
