Version : **2022.01**

Updated: 2022/11/23 09:03

Topic 211: E-Mail Services

Contenu du Module

- **Topic 211: E-Mail Services**
  - Contenu du Module
  - Présentation
  - Configuration de votre Machine Virtuelle
    - Modification du Fichier /etc/hosts
    - Modification du FQDN
    - Modification de SELinux
    - Démarrage du Service ntpd
    - Configurer firewalld
  - LAB #1 - Installation de postfix, de Dovecot et de Cyrus-Imapd
  - LAB #2 - Configuration de Base de Postfix
    - Le fichier /etc/postfix/main.cf
    - La Commande postconf
    - La Commande sendmail de Postfix
    - Tester la Configuration de Postfix
    - Terminer la Configuration
  - LAB #3 - Tester le Serveur SMTP Sortant
  - LAB #4 - Définition des Aliases
  - LAB #5 - Sécurisation de Postfix
    - Cyrus SASL
      - Présentation
      - Configuration de Postfix
        - smtpd_recipient_restrictions

        - smtpd_client_restrictions
        - smtpd_sasl_security_options
    - TLS
- LAB #6 - Configuration de l'Antispam et de l'Antivirus
    - SpamAssassin
        - Installation
        - Configuration
    - ClamAV
        - Installation
- LAB #7 - Configuration du Mandataire MailScanner
    - Préparation à l'Installation
    - Installation
    - Configuration du couple MailScanner/Postfix
- LAB #8 - Installation du Serveur IMAP Dovecot/Cyrus-Imapd
    - Cas #1 - Dovecot
    - Cas #2 - Cyrus-Imap
- LAB #9 - Gestion des Domaines Virtuels avec MariaDB, Postfix et Dovecot
    - Configuration de votre Machine Virtuelle
        - Modification du Fichier /etc/hosts
        - Modification du FQDN
        - Création, Activation et Configuration d'un Profil Réseau d'IP Fixe
        - Modification de SELinux
        - Démarrage du Service ntpd
        - Configurer firewalld
    - Créer un Certificat
    - Installer mariadb et dovecot-mysql
    - Créer les Tables de la Base mailserver
        - virtual_domaines
        - virtual_users
        - virtual_aliases
    - Configurer postfix
        - main.cf
        - mysql-virtual-mailbox-domains.cf
        - mysql-virtual-mailbox-maps.cf

        - mysql-virtual-alias-maps.cf
        - mysql-virtual-email2email.cf
        - Tester la Configuration de Postfix
            - La Commande postmap
        - master.cf
        - Modifier les Permissions
    - Configurer Dovecot
        - dovecot.conf
        - /etc/dovecot/conf.d/10-mail.conf
        - /etc/dovecot/conf.d/10-auth.conf
        - /etc/dovecot/conf.d/auth-sql.conf.ext
        - /etc/dovecot/dovecot-sql.conf.ext
        - /etc/dovecot/conf.d/10-master.conf
        - Dernières Configurations
    - Tester la Configuration
        - trainee@i2tch.com
        - mickey.mouse@i2tch.com
        - trainee@mail.i2tch.com
    - LAB #10 - Configuration de Postfix en Environnement chroot

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.

La commande mail est souvent un lien symbolique ver la commande **mailx** :

```
[root@centos7 ~]# ls -l /bin/mail
lrwxrwxrwx. 1 root root 5 Jan 14 08:17 /bin/mail -> mailx
```

Les options de la commande mailx sont :

```
[root@centos7 ~]# mailx --help
mailx: illegal option -- -
Usage: mailx -eiIUdEFntBDNHRVv~ -T FILE -u USER -h hops -r address -s SUBJECT -a FILE -q FILE -f FILE -A ACCOUNT
-b USERS -c USERS -S OPTION users
```

La syntaxe de la commande mailx dans le cas d'un envoie est :

```
mailx [-s  objet ] [-c  ccadresse ] [-b  bccadresse ] adresse_destinataire
```

Lors de la lecture du spool de mail local, la syntaxe est la suivante :

```
mailx [-f [ spool de mail local ] | -u  nom_utilisateur ]
```

Par exemple :

```
[root@centos7 ~]# mail -s "test  message" -c trainee root
This is a test message
[^D]
EOT
```

```
[root@centos7 ~]# su - trainee
Last login: Mon Jan 14 10:28:37 CET 2019 from 10.0.2.2 on pts/0
[trainee@centos7 ~]$ mail
Heirloom Mail version 12.5 7/5/10.  Type ? for help.
"/var/spool/mail/trainee": 1 message 1 new
>N  1 root                  Mon Jan 14 10:30  19/667   "test  message"
& 1
Message  1:
From root@centos7.fenestros.loc  Mon Jan 14 10:30:47 2019
Return-Path: <root@centos7.fenestros.loc>
X-Original-To: trainee
Delivered-To: trainee@centos7.fenestros.loc
Date: Mon, 14 Jan 2019 10:30:46 +0100
To: root@centos7.fenestros.loc
Subject: test  message
Cc: trainee@centos7.fenestros.loc
User-Agent: Heirloom mailx 12.5 7/5/10
Content-Type: text/plain; charset=us-ascii
From: root@centos7.fenestros.loc (root)
Status: R

This a test massage

& q
Held 1 message in /var/spool/mail/trainee
```

Il est aussi possible d'injecter le contenu d'un fichier sur l'entrée standard de la commande mailx afin de l'utiliser comme le contenu du message :

```
[trainee@centos7 ~]$ echo fenestros > mail.txt
You have mail in /var/spool/mail/trainee
[trainee@centos7 ~]$ mail -s "test message back" < mail.txt root
[trainee@centos7 ~]$ su -
Password:
Last login: Mon Jan 14 10:28:46 CET 2019 on pts/0
```

```
[root@centos7 ~]# mail
Heirloom Mail version 12.5 7/5/10.  Type ? for help.
"/var/spool/mail/root": 4 messages 4 new
>N  1 trainee@centos7.fene  Sat Apr 30 12:38  16/688   "*** SECURITY information for centos7.fenestros.loc ***"
 N  2 trainee@centos7.fene  Mon Apr 23 12:04  16/688   "*** SECURITY information for centos7.fenestros.loc ***"
 N  3 root                  Mon Jan 14 10:30  19/661   "test  message"
 N  4 trainee               Mon Jan 14 10:33  18/636   "test message back"
& q
Held 4 messages in /var/spool/mail/root
```

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@centos7 ~]# vi /etc/hosts
[root@centos7 ~]# cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain6 localhost6
10.0.2.51   i2tch.com
10.0.2.51   mail.i2tch.com  mail
```

Modification du FQDN

Modifiez le FQDN de votre VM :

```
[root@centos7 ~]# nmcli g hostname mail.i2tch.com
[root@centos7 ~]# hostname
mail.i2tch.com
```

Modification de SELinux

```
[root@mail ~]# setenforce permissive
[root@mail ~]# vi /etc/selinux/config
[root@mail ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Démarrage du Service ntpd

Activez et démarrez le serveur **ntpd** :

```
[root@mail ~]# systemctl status ntpd
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@mail ~]# systemctl enable ntpd
Created symlink from /etc/systemd/system/multi-user.target.wants/ntpd.service to
/usr/lib/systemd/system/ntpd.service.
[root@mail ~]# systemctl start ntpd
```

Configurer 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 ~]# yum install postfix procmail dovecot 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
```

A l'installation de postfix, le fichier principal de configuration **main.cf** comporte les directives actives suivantes :

main.cf

```
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
data_directory = /var/lib/postfix
mail_owner = postfix
inet_interfaces = localhost
inet_protocols = all
mydestination = $myhostname, localhost.$mydomain, localhost
unknown_local_recipient_reject_code = 550
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases


debug_peer_level = 2
debugger_command =
     PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
     ddd $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
html_directory = no
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.10.1/samples
readme_directory = /usr/share/doc/postfix-2.10.1/README_FILES
```

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 $mail_name ($mail_version)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############  RELAY HOST  ##############
# relayhost = smtp.bbox.fr
#############  USER/GROUP  ##############
mail_owner = postfix
setgid_group = postdrop
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
############   DEBUGGING   ##############
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5
############   COMMANDES   ##############
```

```
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
############  REPERTOIRES  ##############
mail_spool_directory = /var/spool/mail
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
```

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.
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.
relayhost	La machine par défaut où livrer le courrier extérieur.
mail_owner	Le compte du système qui possède la file d'attente et la plupart des processus démons de Postfix.
setgid_group	Le groupe propriétaire des commandes set-gid de Postfix et des répertoires en écriture pour le groupe.
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.

Directive	Description
debugger_command	La commande externe à exécuter lorsqu'un programme démon de Postfix est invoké avec l'option -D.
mailbox_command	Commande externe optionnelle que l'agent de livraison local doit utiliser pour la livraison des messages.
sendmail_path	Indique l'emplacement de la commande sendmail de Postfix.
newaliases_path	Indique l'emplacement de la commande newaliases.
mailq_path	Indique où est installée la commande Postfix mailq. Cette commande peut être utilisée pour afficher la file d'attente.
mail_spool_directory	Le répertoire où les boîtes-aux-lettres locales sont stockées.
manpage_directory	Emplacement des pages de manuel de Postfix.
sample_directory	Emplacement des exemples de fichiers de configuration de Postfix.
readme_directory	Emplacement des fichiers README de Postfix.
queue_directory	Emplacement du répertoire racine de la file d'attente de Postfix.
command_directory	Emplacement des commandes administratives de Postfix.
daemon_directory	Emplacement des démons Postfix.

Important - La directive **relayhost = smtp.bbox.fr** n'est necéssaire que pour contourner le blocage du port 25 du FAI utilisé pour éloborer ce cours. Elle n'est pas neceéssaire dans un environnement de production.

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_poll_count = ${stress?1}${stress: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_defau
lt_transport_maps
address_verify_sender_dependent_relayhost_maps = $sender_dependent_relayhost_map
--More--
```

```
[root@mail ~]# postconf -n | more
alias_database = hash:/etc/aliases
alias_maps = hash:/etc/aliases
broken_sasl_auth_clients = yes
command_directory = /usr/sbin
config_directory = /etc/postfix
daemon_directory = /usr/libexec/postfix
debugger_command = PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin xxgdb $daemo
n_directory/$process_name $process_id & sleep 5
delay_warning_time = 4h
inet_interfaces = all
```

```
mail_owner = postfix
mail_spool_directory = /var/spool/mail
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN
mailq_path = /usr/bin/mailq.postfix
manpage_directory = /usr/share/man
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
--More--
```

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
[root@mail ~]#
```

A Faire : Consultez le manuel de la commande postfix pour connaître ses options et ses arguments.

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 (/usr/lib/systemd/system/postfix.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2019-01-14 11:46:44 CET; 6s ago
  Process: 7755 ExecStop=/usr/sbin/postfix stop (code=exited, status=0/SUCCESS)
  Process: 7768 ExecStart=/usr/sbin/postfix start (code=exited, status=0/SUCCESS)
  Process: 7766 ExecStartPre=/usr/libexec/postfix/chroot-update (code=exited, status=0/SUCCESS)
  Process: 7764 ExecStartPre=/usr/libexec/postfix/aliasesdb (code=exited, status=0/SUCCESS)
 Main PID: 7840 (master)
   CGroup: /system.slice/postfix.service
           ├─7840 /usr/libexec/postfix/master -w
           ├─7841 pickup -l -t unix -u
           └─7842 qmgr -l -t unix -u

Jan 14 11:46:43 mail.i2tch.com systemd[1]: Stopped Postfix Mail Transport Agent.
Jan 14 11:46:43 mail.i2tch.com systemd[1]: Starting Postfix Mail Transport Agent...
Jan 14 11:46:44 mail.i2tch.com postfix/master[7840]: daemon started -- version 2.10.1, configuration /etc/postfix
Jan 14 11:46:44 mail.i2tch.com systemd[1]: Started Postfix Mail Transport Agent.
```

Installez maintenant telnet :

```
[root@mail ~]# yum install telnet
```

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

```
[root@mail ~]# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (2.10.1)
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 E68953344BC3
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 ~]# tail /var/log/maillog
Jan 14 11:46:43 centos7 postfix/master[2903]: terminating on signal 15
Jan 14 11:46:44 centos7 postfix/postfix-script[7838]: starting the Postfix mail system
Jan 14 11:46:44 centos7 postfix/master[7840]: daemon started -- version 2.10.1, configuration /etc/postfix
Jan 14 11:48:46 centos7 postfix/smtpd[8731]: connect from localhost.localdomain[127.0.0.1]
Jan 14 11:49:13 centos7 postfix/smtpd[8731]: E68953344BC3: client=localhost.localdomain[127.0.0.1]
Jan 14 11:49:42 centos7 postfix/cleanup[8948]: E68953344BC3: message-
id=<20190114104913.E68953344BC3@mail.i2tch.com>
Jan 14 11:49:42 centos7 postfix/qmgr[7842]: E68953344BC3: from=<root@i2tch.com>, size=342, nrcpt=1 (queue active)
Jan 14 11:49:42 centos7 postfix/local[9161]: E68953344BC3: to=<trainee@i2tch.com>, relay=local, delay=38,
delays=38/0.05/0/0.08, dsn=2.0.0, status=sent (delivered to command: /usr/bin/procmail -Y -a $DOMAIN)
Jan 14 11:49:42 centos7 postfix/qmgr[7842]: E68953344BC3: removed
Jan 14 11:49:51 centos7 postfix/smtpd[8731]: disconnect from localhost.localdomain[127.0.0.1]
```

LAB #3 - Tester le Serveur SMTP Sortant

Envoyez un message en utilisant telnet à hugh.norris@hugh-norris.info avec comme **Subject:** votre prénom :

```
[root@mail ~]# telnet localhost 25
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (2.6.6)
HELO me
250 mail.i2tch.com
MAIL from: root@i2tch.com
250 2.1.0 Ok
RCPT to: hugh.norris@hugh-norris.info
250 2.1.5 Ok
DATA
```

```
354 End data with <CR><LF>.<CR><LF>
Subject : root
Message de Test
.
250 2.0.0 Ok: queued as AF03C70A3
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 :

```
...
May  1 10:54:17 mail postfix/smtpd[5899]: connect from localhost[127.0.0.1]
May  1 10:54:50 mail postfix/smtpd[5899]: AF03C70A3: client=localhost[127.0.0.1]
May  1 10:55:04 mail postfix/cleanup[5903]: AF03C70A3: message-id=<20140501085450.AF03C70A3@mail.i2tch.com>
May  1 10:55:04 mail postfix/qmgr[5061]: AF03C70A3: from=<root@i2tch.com>, size=390, nrcpt=1 (queue active)
May  1 10:55:04 mail postfix/smtp[5904]: AF03C70A3: to=<hugh.norris@hugh-norris.info>,
relay=smtp.bbox.fr[194.158.122.55]:25, delay=31, delays=31/0.01/0.16/0.05, dsn=2.0.0, status=sent (250 2.0.0 Ok:
queued as 4EF645A)
May  1 10:55:04 mail postfix/qmgr[5061]: AF03C70A3: removed
May  1 10:55:08 mail postfix/smtpd[5899]: disconnect from localhost[127.0.0.1]
```

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]**.

LAB #4 - 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
#
#  Aliases in this file will NOT be expanded in the header from
#  Mail, but WILL be visible over networks or from /bin/mail.
#
#   >>>>>>>>>>    The program "newaliases" must be run after
#   >> NOTE >>    this file is updated for any changes to
#   >>>>>>>>>>    show through to sendmail.
#

# Basic system aliases -- these MUST be present.
mailer-daemon:  postmaster
postmaster: root

# General redirections for pseudo accounts.
bin:        root
daemon:     root
adm:        root
lp:     root
sync:       root
shutdown:   root
halt:       root
```

```
mail:       root
news:       root
uucp:       root
operator:   root
games:      root
gopher:     root
ftp:        root
nobody:     root
radiusd:    root
nut:        root
dbus:       root
vcsa:       root
canna:      root
wnn:        root
rpm:        root
nscd:       root
pcap:       root
apache:     root
webalizer:  root
dovecot:    root
fax:        root
quagga:     root
radvd:      root
pvm:        root
amandabackup:       root
privoxy:    root
ident:      root
named:      root
xfs:        root
gdm:        root
mailnull:   root
postgres:   root
sshd:       root
smmsp:      root
```

```
postfix:    root
netdump:    root
ldap:       root
squid:      root
ntp:        root
mysql:      root
desktop:    root
rpcuser:    root
rpc:        root
nfsnobody:  root

ingres:     root
system:     root
toor:       root
manager:    root
dumper:     root
abuse:      root

newsadm:    news
newsadmin:  news
usenet:     news
ftpadm:     ftp
ftpadmin:   ftp
ftp-adm:    ftp
ftp-admin:  ftp
www:        webmaster
webmaster:  root
noc:        root
security:   root
hostmaster: root
info:       postmaster
marketing:  postmaster
sales:      postmaster
support:    postmaster
```

```
# trap decode to catch security attacks
decode:     root

# Person who should get root's mail
#root:      marc
```

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 ~]# tail /etc/aliases


# trap decode to catch security attacks
decode:     root

# Person who should get root's mail
root:       trainee

# Employee Accounts
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 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (2.10.1)
HELO me
250 mail.i2tch.com
MAIL from: trainee@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 B46C23344BC3
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

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

```
[root@mail ~]# tail /var/log/maillog
```

```
Jan 14 11:49:51 centos7 postfix/smtpd[8731]: disconnect from localhost.localdomain[127.0.0.1]
Jan 14 12:42:34 centos7 postfix/postfix-script[373]: refreshing the Postfix mail system
Jan 14 12:42:34 centos7 postfix/master[7840]: reload -- version 2.10.1, configuration /etc/postfix
Jan 14 12:43:08 centos7 postfix/smtpd[654]: connect from localhost.localdomain[127.0.0.1]
Jan 14 12:43:41 centos7 postfix/smtpd[654]: B46C23344BC3: client=localhost.localdomain[127.0.0.1]
Jan 14 12:44:09 centos7 postfix/cleanup[908]: B46C23344BC3: message-
id=<20190114114341.B46C23344BC3@mail.i2tch.com>
Jan 14 12:44:09 centos7 postfix/qmgr[377]: B46C23344BC3: from=<trainee@i2tch.com>, size=343, nrcpt=1 (queue
active)
Jan 14 12:44:09 centos7 postfix/local[1100]: B46C23344BC3: to=<trainee@i2tch.com>,
orig_to=<mickey.mouse@i2tch.com>, relay=local, delay=36, delays=36/0.02/0/0.03, dsn=2.0.0, status=sent (delivered
to command: /usr/bin/procmail -Y -a $DOMAIN)
Jan 14 12:44:09 centos7 postfix/qmgr[377]: B46C23344BC3: removed
Jan 14 12:44:12 centos7 postfix/smtpd[654]: disconnect from localhost.localdomain[127.0.0.1]
```

Notez la présence de la ligne suivante :

```
Jan 14 12:44:09 centos7 postfix/local[1100]: B46C23344BC3: to=<trainee@i2tch.com>,
orig_to=<mickey.mouse@i2tch.com>, relay=local, delay=36, delays=36/0.02/0/0.03, dsn=2.0.0, status=sent (delivered
to command: /usr/bin/procmail -Y -a $DOMAIN)
```

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 #5 - 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).

La configuration de SASL se trouve dans le fichier **/etc/sasl2/smtpd.conf** :

```
[root@mail ~]# cat /etc/sasl2/smtpd.conf
pwcheck_method: saslauthd
mech_list: plain 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 **cyrus-sasl** :

```
[root@mail ~]# yum provides saslauthd
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * updates: mirror.in2p3.fr
cyrus-sasl-2.1.26-23.el7.i686 : The Cyrus SASL library
Repo        : base
Matched from:
Filename    : /usr/sbin/saslauthd



cyrus-sasl-2.1.26-23.el7.x86_64 : The Cyrus SASL library
Repo        : base
Matched from:
Filename    : /usr/sbin/saslauthd



cyrus-sasl-2.1.26-23.el7.x86_64 : The Cyrus SASL library
Repo        : @base
Matched from:
Filename    : /sbin/saslauthd



cyrus-sasl-2.1.26-23.el7.x86_64 : The Cyrus SASL library
Repo        : @base
Matched from:
Filename    : /usr/sbin/saslauthd
```

Installez donc le paquet **Cyrus-sasl** :

```
[root@mail ~]# yum install -y cyrus-sasl
```

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

```
[root@mail ~]# yum search cyrus-sasl
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * updates: mirror.in2p3.fr
============================================================================ N/S matched: cyrus-sasl
============================================================================
cyrus-sasl.i686 : The Cyrus SASL library
cyrus-sasl.x86_64 : The Cyrus SASL library
cyrus-sasl-devel.i686 : Files needed for developing applications with Cyrus SASL
cyrus-sasl-devel.x86_64 : Files needed for developing applications with Cyrus SASL
cyrus-sasl-gs2.i686 : GS2 support for Cyrus SASL
cyrus-sasl-gs2.x86_64 : GS2 support for Cyrus SASL
cyrus-sasl-gssapi.i686 : GSSAPI authentication support for Cyrus SASL
cyrus-sasl-gssapi.x86_64 : GSSAPI authentication support for Cyrus SASL
cyrus-sasl-ldap.i686 : LDAP auxprop support for Cyrus SASL
cyrus-sasl-ldap.x86_64 : LDAP auxprop support for Cyrus SASL
cyrus-sasl-lib.i686 : Shared libraries needed by applications which use Cyrus SASL
cyrus-sasl-lib.x86_64 : Shared libraries needed by applications which use Cyrus SASL
cyrus-sasl-md5.i686 : CRAM-MD5 and DIGEST-MD5 authentication support for Cyrus SASL
cyrus-sasl-md5.x86_64 : CRAM-MD5 and DIGEST-MD5 authentication support for Cyrus SASL
cyrus-sasl-ntlm.i686 : NTLM authentication support for Cyrus SASL
cyrus-sasl-ntlm.x86_64 : NTLM authentication support for Cyrus SASL
cyrus-sasl-plain.i686 : PLAIN and LOGIN authentication support for Cyrus SASL
cyrus-sasl-plain.x86_64 : PLAIN and LOGIN authentication support for Cyrus SASL
cyrus-sasl-scram.i686 : SCRAM auxprop support for Cyrus SASL
cyrus-sasl-scram.x86_64 : SCRAM auxprop support for Cyrus SASL
```

```
cyrus-sasl-sql.i686 : SQL auxprop support for Cyrus SASL
cyrus-sasl-sql.x86_64 : SQL auxprop support for Cyrus SASL

  Name and summary matches only, use "search all" for everything.
```

Vérifiez lesquels ont été installés dans CentOS 7 :

```
[root@mail ~]# rpm -qa | grep sasl
cyrus-sasl-plain-2.1.26-23.el7.x86_64
cyrus-sasl-lib-2.1.26-23.el7.x86_64
cyrus-sasl-scram-2.1.26-23.el7.x86_64
cyrus-sasl-md5-2.1.26-23.el7.x86_64
cyrus-sasl-gssapi-2.1.26-23.el7.x86_64
cyrus-sasl-2.1.26-23.el7.x86_64
```

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

```
[root@mail ~]# cat /etc/sysconfig/saslauthd
# Directory in which to place saslauthd's listening socket, pid file, and so
# on.  This directory must already exist.
SOCKETDIR=/run/saslauthd

# Mechanism to use when checking passwords.  Run "saslauthd -v" to get a list
# of which mechanism your installation was compiled with the ablity to use.
MECH=pam

# Additional flags to pass to saslauthd on the command line.  See saslauthd(8)
# for the list of accepted flags.
FLAGS=
```

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 2.1.26
```

```
authentication mechanisms: getpwent kerberos5 pam rimap shadow ldap httpform
```

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 ~]# ldd /usr/libexec/postfix/smtpd | grep libsasl
    libsasl2.so.3 => /lib64/libsasl2.so.3 (0x00007f68eceda000)
```

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
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = i2tch.com
smtpd_helo_required = yes
```

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 $mail_name ($mail_version)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############  RELAY HOST  ##############
# relayhost = smtp.bbox.fr
#############  USER/GROUP  ##############
mail_owner = postfix
setgid_group = postdrop
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
```

```
alias_database = hash:/etc/aliases
############   DEBUGGING   ##############
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5
############   COMMANDES   ##############
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
############  REPERTOIRES  ##############
mail_spool_directory = /var/spool/mail
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
############      SASL     ##############
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
```

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.
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.

Restriction	Description
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.

Rechargez la configuration de postfix :

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

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.

Activez et démarrez le service **saslauthd** :

```
[root@mail ~]# systemctl status saslauthd
● saslauthd.service - SASL authentication daemon.
   Loaded: loaded (/usr/lib/systemd/system/saslauthd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@mail ~]# systemctl enable saslauthd
Created symlink from /etc/systemd/system/multi-user.target.wants/saslauthd.service to
/usr/lib/systemd/system/saslauthd.service.
[root@mail ~]# systemctl start saslauthd
[root@mail ~]# systemctl status saslauthd
● saslauthd.service - SASL authentication daemon.
   Loaded: loaded (/usr/lib/systemd/system/saslauthd.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2019-01-14 13:05:23 CET; 3s ago
  Process: 10849 ExecStart=/usr/sbin/saslauthd -m $SOCKETDIR -a $MECH $FLAGS (code=exited, status=0/SUCCESS)
 Main PID: 10850 (saslauthd)
   CGroup: /system.slice/saslauthd.service
           ├─10850 /usr/sbin/saslauthd -m /run/saslauthd -a pam
           ├─10851 /usr/sbin/saslauthd -m /run/saslauthd -a pam
           ├─10852 /usr/sbin/saslauthd -m /run/saslauthd -a pam
           ├─10853 /usr/sbin/saslauthd -m /run/saslauthd -a pam
           └─10854 /usr/sbin/saslauthd -m /run/saslauthd -a pam

Jan 14 13:05:23 mail.i2tch.com systemd[1]: Starting SASL authentication daemon....
Jan 14 13:05:23 mail.i2tch.com saslauthd[10850]: detach_tty      : master pid is: 10850
```

```
Jan 14 13:05:23 mail.i2tch.com saslauthd[10850]: ipc_init        : listening on socket: /run/saslauthd/mux
Jan 14 13:05:23 mail.i2tch.com systemd[1]: Started SASL authentication daemon..
```

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

```
[root@mail ~]# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (2.10.1)
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).

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 **/etc/pki/tls/misc** :

```
[root@mail ~]# cd /etc/pki/tls/misc
[root@mail misc]# ls -l
total 24
-rwxr-xr-x. 1 root root 5178 Oct 30 23:42 CA
-rwxr-xr-x. 1 root root  119 Oct 30 23:42 c_hash
-rwxr-xr-x. 1 root root  152 Oct 30 23:42 c_info
-rwxr-xr-x. 1 root root  112 Oct 30 23:42 c_issuer
-rwxr-xr-x. 1 root root  110 Oct 30 23:42 c_name

[root@mail misc]# ./CA -newca
CA certificate filename (or enter to create)

Making CA certificate ...
Generating a 2048 bit RSA private key
```

```
..+++
.....................................................................................+++
writing new private key to '/etc/pki/CA/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) [XX]:GB
State or Province Name (full name) []:SURREY
Locality Name (eg, city) [Default City]:ADDLESTONE
Organization Name (eg, company) [Default Company Ltd]:I2TCH LTD
Organizational Unit Name (eg, section) []:TRAINING
Common Name (eg, your name or your server's hostname) []: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 []:
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            d9:6a:23:bb:78:9c:f8:80
        Validity
            Not Before: Jan 14 13:08:21 2019 GMT
```

```
            Not After : Jan 13 13:08:21 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:
                2D:14:39:2D:F5:C2:FE:75:31:9A:CB:95:A2:C0:19:18:9D:8C:7D:EE
            X509v3 Authority Key Identifier:
                keyid:2D:14:39:2D:F5:C2:FE:75:31:9A:CB:95:A2:C0:19:18:9D:8C:7D:EE

            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until Jan 13 13:08:21 2022 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
```

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

```
[root@mail misc]# ls /etc/pki/CA
cacert.pem  careq.pem  certs  crl  index.txt  index.txt.attr  index.txt.old  newcerts  private  serial
[root@mail misc]# ls /etc/pki/CA/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 misc]# openssl req -new -nodes -keyout lel_clef.pem -out lel_req.pem
Generating a 2048 bit 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) [XX]:GB
State or Province Name (full name) []:SURREY
Locality Name (eg, city) [Default City]:ADDLESTONE
Organization Name (eg, company) [Default Company Ltd]:I2TCH LTD
Organizational Unit Name (eg, section) []:TRAINING
Common Name (eg, your name or your server's hostname) []: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 misc]# ls
CA  c_hash  c_info  c_issuer  c_name  lel_clef.pem  lel_req.pem
```

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 misc]# openssl ca -out lel_cert.pem -infiles lel_req.pem
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:fenestros
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            d9:6a:23:bb:78:9c:f8:81
        Validity
            Not Before: Jan 14 13:14:14 2019 GMT
            Not After : Jan 14 13:14:14 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:
                B8:63:90:BF:FD:A6:8F:4F:7B:2E:67:76:C5:FB:6E:78:9B:E1:59:02
            X509v3 Authority Key Identifier:
                keyid:2D:14:39:2D:F5:C2:FE:75:31:9A:CB:95:A2:C0:19:18:9D:8C:7D:EE

Certificate is to be certified until Jan 14 13:14:14 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 misc]# cp lel_cert.pem lel_clef.pem /etc/postfix
[root@mail misc]# cp /etc/pki/CA/cacert.pem /etc/postfix
[root@mail misc]# chmod 644 /etc/postfix/lel_cert.pem /etc/postfix/cacert.pem
[root@mail 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 :

```
...
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 misc]# vi /etc/postfix/main.cf
```

```
[root@mail 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 $mail_name ($mail_version)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############  RELAY HOST  ##############
# relayhost = smtp.bbox.fr
#############  USER/GROUP  ##############
mail_owner = postfix
setgid_group = postdrop
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
#############   DEBUGGING   ##############
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5
#############   COMMANDES   ##############
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
#############  REPERTOIRES  ##############
mail_spool_directory = /var/spool/mail
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
```

```
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
############      SASL     ##############
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
############      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 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-----
MIID9TCCAt2gAwIBAgIJANlqI7t4nPiBMA0GCSqGSIb3DQEBCwUAMHkxCzAJBgNV
BAYTAkdCMQ8wDQYDVQQIDAZTVVJSRVkxEjAQBgNVBAoMCUkyVENIIExURDERMA8G
A1UECwwIVFJBSU5JTkcxEjAQBgNVBAMMCWkydGNoLmNvbTEeMBwGCSqGSIb3DQEJ
ARYPaW5mb3NAaTJ0Y2guY29tMB4XDTE5MDExNDEzMTQxNFoXDTIwMDExNDEzMTQx
NFowfjELMAkGA1UEBhMCR0IxDzANBgNVBAgMBlNVUlJFWTESMBAGA1UECgwJSTJU
Q0ggTFREMREwDwYDVQQLDAhUUkFJTklORzEXMBUGA1UEAwwObWFpbC5pMnRjaC5j
b20xHjAcBgkqhkiG9w0BCQEWD2luZm9zQGkydGNoLmNvbTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAKfKIWo0A9OWHMy15nOfanFb6igLA3Wi7EbfhhTS
BrhqoROyZYI2MezAxp3/t1Ur3z+UYufJdMeaR0Ea4drKYqIusBPvOjgCuEGF7mDx
kg93RtVTvt2vsGqc9/tzIZeZifWhURShE2+Tsq0ATZkVTcQvohZwHGuRvmOzW0Hd
dhsIMEoCimVl69lvuuMYv4RIHz+Ssv+WCSQn+YiROU5MulIKaiLEr6n1VSU44xLg
QmZ1vQVe2rr+wgZRPStnvMfZahzb8SYMnkr7cYfV3umUQDz0Pqwbv5RBbD54q23a
to9AQ6gLKwoGjD1puDv0QmVzuEEZ5n4E+/82rrTv1ibufjsCAwEAAaN7MHkwCQYD
VR0TBAIwADAsBglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlm
aWNhdGUwHQYDVR0OBBYEFLhjkL/9po9Pey5ndsX7bnib4VkCMB8GA1UdIwQYMBaA
FC0UOS31wv51MZrLlaLAGRidjH3uMA0GCSqGSIb3DQEBCwUAA4IBAQBbmvEz4pLu
1VibJpHe+2HA/olm43lwvB+fee2ppF/X9aVS13l/zMB2XjuUbweNuHHvtbHOh4Il
ViOr1gZdnyQWSptwc89v8DDx0lB1TMTgTg5F0XZ9ZsL5JZkYzjPN5PDEl7yiVMTU
BlRw0m9CpKFiRU7CszM3+KvlnV2l8ORaN/iFmGki+imkuNlU2FFEr/rqOXxEi6ns
4nrIc0QKKwlZGa3ny9WYD8uCIcZ3m0QcyoD69URWiyjvXZOT9fXp6DPjs3VLCFb9
```

```
vmHYqSbDmrYMw7qFDOFgxXNEK6Fr2tKxCDKOQ5eGN+DnLglTQNLPrUlzIBXNGa8l
CHYTQ3ojMs6N
-----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 2902 bytes and written 450 bytes
---
New, TLSv1/SSLv3, 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: 9DCAE8A1C3815FDD4A9C7A7F49BFD3FE1937ACC0E15FA95040C37AB2AC128121
    Session-ID-ctx:
    Master-Key: DE9DF946F81A7ECBFDCAB886D13C663C0B97D3ECE0CEB24BAF4D6CA7BE962411274057F88D1E2CE9C70C05D5D5AEFF73
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    TLS session ticket lifetime hint: 3600 (seconds)
    TLS session ticket:
    0000 - a7 68 78 12 4d a2 52 ff-b2 98 d1 d9 b8 93 d1 20   .hx.M.R........
    0010 - c6 93 98 a9 f6 26 2d 5d-99 31 ef 60 1b 98 f9 b0   .....&-].1.`....
    0020 - 0d 79 aa 4f f0 2a fe d1-1f b9 fb 35 e4 99 92 f2   .y.O.*.....5....
    0030 - 5a 65 91 1e 3b 9e c5 08-67 0c d5 96 71 88 7a a0   Ze..;...g...q.z.
```

```
    0040 - 48 e7 3b d3 bc a9 dd 35-ba 5d 04 2c 0d 5b ec a2   H.;....5.].,.[..
    0050 - 64 d3 69 9b fc ca 23 5a-a8 60 ca 8f 98 08 fa d4   d.i...#Z.`......
    0060 - 05 78 42 90 f6 f7 cd ec-5b 3c 13 f8 58 ab bb 72   .xB.....[<..X..r
    0070 - 6e 86 61 7b 66 dc 1b f3-55 5f 83 aa bf 25 de cf   n.a{f...U_...%..
    0080 - 7f f1 70 49 dc 31 c5 1c-79 77 0f 71 af 03 a5 68   ..pI.1..yw.q...h
    0090 - 80 14 c1 5d da 73 34 0c-96 de e9 00 1e 4d 90 e9   ...].s4......M..

    Start Time: 1547472649
    Timeout   : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
---
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").
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (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       -       n       -       1       postscreen
#smtpd     pass  -       -       n       -       -       smtpd
#dnsblog   unix  -       -       n       -       0       dnsblog
#tlsproxy  unix  -       -       n       -       0       tlsproxy
#submission inet n       -       n       -       -       smtpd
```

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 ~]# netstat -ln | grep 587
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN
tcp6       0      0 :::587                  :::*                    LISTEN
[root@mail ~]# netstat -ln | grep 465
tcp        0      0 0.0.0.0:465             0.0.0.0:*               LISTEN
tcp6       0      0 :::465                  :::*                    LISTEN
```

```
unix  2      [ ACC ]     STREAM     LISTENING     619465   public/cleanup
```

LAB #6 - Configuration de l'Antispam et de l'Antivirus

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 yum :

```
[root@mail ~]# yum 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.
- Modifiez la ligne **required_hits 5** à **required_hits 3**. Cette ligne définit le score au delà duquel les mails sont considérés comme du spam.

Vous obtiendrez un résutat similaire à celui-ci :

```
[root@mail ~]# vi /etc/mail/spamassassin/local.cf
[root@mail ~]# cat /etc/mail/spamassassin/local.cf
# These values can be overridden by editing ~/.spamassassin/user_prefs.cf
```

```
# (see spamassassin(1) for details)

# These should be safe assumptions and allow for simple visual sifting
# without risking lost emails.

required_hits 3
report_safe 0
rewrite_header Subject [SPAM]
trusted_networks 10.0.2.
ok_languages all
```

Important - Notez que les messages suspects seront marqués avec la chaine **[SPAM]** au début de l'objet du message. Consultez le manuel de spamassassin pour connaître la signification de la directive **report_safe**.

Activez et démarrez le service spamassisin :

```
[root@mail ~]# systemctl status spamassassin
● spamassassin.service - Spamassassin daemon
   Loaded: loaded (/usr/lib/systemd/system/spamassassin.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@mail ~]# systemctl enable spamassassin
Created symlink from /etc/systemd/system/multi-user.target.wants/spamassassin.service to
/usr/lib/systemd/system/spamassassin.service.
[root@mail ~]# systemctl start spamassassin
[root@mail ~]# systemctl status spamassassin
● spamassassin.service - Spamassassin daemon
   Loaded: loaded (/usr/lib/systemd/system/spamassassin.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2019-01-14 16:44:55 CET; 9s ago
  Process: 12343 ExecStart=/usr/bin/spamd --pidfile /var/run/spamd.pid $SPAMDOPTIONS (code=exited,
status=0/SUCCESS)
```

```
  Process: 12342 ExecStartPre=/sbin/portrelease spamd (code=exited, status=0/SUCCESS)
 Main PID: 12368 (/usr/bin/spamd )
   CGroup: /system.slice/spamassassin.service
           ├─12368 /usr/bin/spamd --pidfile /var/run/spamd.pid -d -c -m5 -H
           ├─12383 spamd child
           └─12384 spamd child

Jan 14 16:44:50 mail.i2tch.com systemd[1]: Starting Spamassassin daemon...
Jan 14 16:44:52 mail.i2tch.com spamd[12343]: logger: removing stderr method
Jan 14 16:44:53 mail.i2tch.com spamd[12368]: config: failed to parse, now a ...l
Jan 14 16:44:55 mail.i2tch.com spamd[12368]: spamd: server started on IO::So...)
Jan 14 16:44:55 mail.i2tch.com spamd[12368]: spamd: server pid: 12368
Jan 14 16:44:55 mail.i2tch.com spamd[12368]: spamd: server successfully spaw...3
Jan 14 16:44:55 mail.i2tch.com spamd[12368]: spamd: server successfully spaw...4
Jan 14 16:44:55 mail.i2tch.com systemd[1]: Started Spamassassin daemon.
Jan 14 16:44:55 mail.i2tch.com spamd[12368]: prefork: child states: IS
Jan 14 16:44:55 mail.i2tch.com spamd[12368]: prefork: child states: II
Hint: Some lines were ellipsized, use -l to show in full.
```

ClamAV

ClamAV est un antivirus pour Linux.

Installation

Installez clamav à partir du dépôt **EPEL** :

```
[root@mail ~]# yum install epel-release -y
[root@mail ~]# yum install clamav clamd
```

Ouvrez le fichier **/etc/freshclam.conf** et éditez-le selon l'exemple ci-dessous :

```
[root@mail ~]# vi /etc/freshclam.conf
[root@mail ~]# cat /etc/freshclam.conf
UpdateLogFile /var/log/freshclam.log
LogFileMaxSize 2M
LogTime yes
LogRotate yes
DatabaseMirror db.fr.clamav.net
DatabaseMirror db.local.clamav.net
MaxAttempts 5
```

Creéz ensuite le fichier de journalisation de freshclam :

```
[root@mail ~]# touch /var/log/freshclam.log
[root@mail ~]# chown clamupdate:clamupdate /var/log/freshclam.log
```

Mettez à jour les définitions des virus :

```
[root@mail ~]# freshclam
Mon Jan 14 17:02:26 2019 -> ClamAV update process started at Mon Jan 14 17:02:26 2019
Mon Jan 14 17:02:26 2019 -> ^Your ClamAV installation is OUTDATED!
Mon Jan 14 17:02:26 2019 -> ^Local version: 0.101.0 Recommended version: 0.101.1
Mon Jan 14 17:02:26 2019 -> DON'T PANIC! Read https://www.clamav.net/documents/upgrading-clamav
Mon Jan 14 17:02:46 2019 -> Downloading main.cvd [100%]
Mon Jan 14 17:03:29 2019 -> main.cvd updated (version: 58, sigs: 4566249, f-level: 60, builder: sigmgr)
Mon Jan 14 17:03:38 2019 -> Downloading daily.cvd [100%]
Mon Jan 14 17:03:46 2019 -> daily.cvd updated (version: 25299, sigs: 2209178, f-level: 63, builder: raynman)
Mon Jan 14 17:03:46 2019 -> Downloading bytecode.cvd [100%]
Mon Jan 14 17:03:46 2019 -> bytecode.cvd updated (version: 328, sigs: 94, f-level: 63, builder: neo)
Mon Jan 14 17:03:54 2019 -> Database updated (6775521 signatures) from db.fr.clamav.net (IP: 104.16.185.138)
```

LAB #7 - 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.

Préparation à l'Installation

Installez les dépendances de MailScanner :

```
[root@mail ~]# yum install rpm-build perl-Filesys-Df perl-DBD-SQLite
```

Installation

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

```
[root@mail ~]# wget https://github.com/MailScanner/v5/archive/refs/tags/5.1.2-2.tar.gz
```

et désarchivez-le :

```
[root@mail ~]# tar xvf v5-5.1.2-2.tar.gz
v5-5.1.2-2/
v5-5.1.2-2/Build.debian
v5-5.1.2-2/Build.nix
v5-5.1.2-2/Build.rhel
v5-5.1.2-2/Build.suse
```

```
v5-5.1.2-2/LICENSE
v5-5.1.2-2/README
v5-5.1.2-2/builds/
v5-5.1.2-2/builds/MailScanner-5.1.2-2.deb.tar.gz
v5-5.1.2-2/builds/MailScanner-5.1.2-2.nix.tar.gz
v5-5.1.2-2/builds/MailScanner-5.1.2-2.rhel.tar.gz
v5-5.1.2-2/builds/MailScanner-5.1.2-2.suse.tar.gz
...
```

Placez-vous dans le répertoire **v5-5.1.2-2/rhel/** et exécutez le script **install.sh**. Ce script a pour but de construire les RPMs nécessaires pour l'installation puis de les installer :

```
[root@centos6 ~]# cd v5-5.1.2-2/rhel/
[root@centos6 rhel]# ./install.sh
MailScanner Installation for RPM Based Systems


This will INSTALL or UPGRADE the required software for MailScanner on RPM based systems
via the Yum package manager. Supported distributions are RHEL 5,6,7 and associated
variants such as CentOS and Scientific Linux. 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 if you opt to use CPAN. You may also ignore 'No package available' notices
during the yum installation of 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 Yum 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 EPEL? (Extra Packages for Enterprise Linux)

Installing EPEL will make more yum packages available, such as extra perl modules
and ClamAV, which is recommended. This will also reduce the number of Perl modules
installed via CPAN. Note that EPEL is considered a third party repository.

Recommended: Y (yes)

Install EPEL? [n/Y] : N
[Entrée]



Do you want to install tnef via RPM if missing?

I will attempt to install tnef via the Yum Package Manager, but if not found I can
install this from an RPM provided by the MailScanner Community Project. Tnef allows
MailScanner to handle Microsoft specific winmail.dat files.
```

```
Recommended: Y (yes)

Install missing tnef via RPM? [n/Y] : Y
[Entrée]



Do you want to install unrar via RPM if missing?

I will attempt to install unrar via the Yum Package Manager, but if not found I can
install this from an RPM provided by MailScanner Community Project. unrar allows
MailScanner to handle archives compressed with rar.

Recommended: Y (yes)

Install missing unrar via RPM? [n/Y] :
[Entrée]



Do you want to install missing perl modules via CPAN?

I will attempt to install Perl modules via yum, 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] :
[Entrée]



Do you want to install perl-Filesys-Df and perl-Sys-Hostname-Long via RPM if missing?

perl-Filesys-Df and perl-Sys-Hostname-Long and known to be missing from the Yum base and the
EPEL repo for RHEL7 at the release of this installer. I will try to install them from the
official Yum base and EPEL repo first. (If you elected the EPEL option.) If they are still
```

```
missing I can attempt to install these two missing RPMs with 3rd party RPM packages. If they
are still missing and you selected the CPAN remediation I will try to install them from CPAN.

Recommended: Y (yes)

Install these missing items via RPM? [n/Y] : Y
[Entrée]



Set PERMISSIVE mode for SELinux?

SELinux will cause problems for virus scanners accessing the working directory
used when processing email. Enabling permissive mode will allow the virus scanner
to access the files that need to be scanned until you can create a policy to
allow working directory file access while in ENFORCING mode. If you have already
disabled SELinux selecting 'yes' will not change that. Note that a reboot is
required after the installation for this to take effect.

Recommended: Y (yes)

Set permissive mode for SELinux? [n/Y] :
[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 l'issu de l'installation, vous obtiendrez un résultat similaire à celui-ci :

```
...
Summary
-------
Read 372 settings from old /etc/MailScanner/MailScanner.conf.original
Used 370 settings from old /etc/MailScanner/MailScanner.conf.original
Used 4 default settings from new /etc/MailScanner/MailScanner.conf.dist



To configure MailScanner, edit the following files:

/etc/MailScanner/defaults
/etc/MailScanner/MailScanner.conf
```

```
To activate MailScanner run the following commands:

--SysV Init--
chkconfig mailscanner on
service mailscanner start

--Systemd--
systemctl enable mailscanner.service
systemctl start mailscanner.service

To activate Sendmail for Mailscanner (if in use) run the following commands:

--SysV Init--
chkconfig sendmail off
chkconfig sm-client off
chkconfig ms-sendmail on
service ms-sendmail start

--Systemd--
systemctl disable sendmail.service
systemctl disable sm-client.service
systemctl enable ms-sendmail.service
systemctl start ms-sendmail.service

To activate MSMilter for Mailscanner (if in use) run the following commands:

--SysV Init--
chkconfig msmilter on
service msmilter start

--Systemd--
systemctl enable msmilter.service
systemctl start msmilter.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 $mail_name ($mail_version)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############  RELAY HOST  ##############
# relayhost = smtp.bbox.fr
#############  USER/GROUP  ##############
mail_owner = postfix
setgid_group = postdrop
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
############   DEBUGGING   ##############
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5
############   COMMANDES   ##############
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
############  REPERTOIRES  ##############
mail_spool_directory = /var/spool/mail
html_directory = no
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
############      SASL     ##############
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
############      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**.

Editez ensuite **/etc/postfix/header_checks** en ajoutant les lignes suivantes à la fin du fichier :

```
...
/^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  flush  hold  incoming  maildrop  pid  private  public  saved  trace
```

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**.

Processus	Description
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.
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**.

Répertoire	**Contenu**
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.
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
```

```
[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

----------- SCAN SUMMARY -----------
Known viruses: 6768273
Engine version: 0.101.0
Scanned directories: 1
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 16.674 sec (0 m 16 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 anti-spam **pyzor** ;

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

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

```
[root@mail MailScanner-5.1.2-2]# 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 MailScanner-5.1.2-2]# vi /etc/MailScanner/defaults
[root@mail MailScanner-5.1.2-2]# 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 MailScanner-5.1.2-2]# systemctl status mailscanner
● mailscanner.service - LSB: MailScanner daemon
```

```
   Loaded: loaded (/usr/lib/MailScanner/init/ms-init; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:systemd-sysv-generator(8)
[root@mail MailScanner-5.1.2-2]# systemctl enable mailscanner
Created symlink from /etc/systemd/system/multi-user.target.wants/mailscanner.service to
/usr/lib/systemd/system/mailscanner.service.
[root@mail MailScanner-5.1.2-2]# systemctl start mailscanner
[root@mail MailScanner-5.1.2-2]# 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 13:05:35 CET; 7s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 8339 ExecStart=/usr/lib/MailScanner/init/ms-init start (code=exited, status=0/SUCCESS)
 Main PID: 8902 (MailScanner: st)
   CGroup: /system.slice/mailscanner.service
           ├─8902 MailScanner: starting children
           ├─8904 MailScanner: starting children
           ├─9004 /usr/bin/python -Wignore::DeprecationWarning /bin/pyzor check
           └─9010 MailScanner: starting children

Jan 15 13:05:36 mail.i2tch.com MailScanner[8904]: Enabling SpamAssassin auto-whitelist functionality...
Jan 15 13:05:40 mail.i2tch.com MailScanner[9010]: MailScanner Email Processor version 5.1.2 starting...
Jan 15 13:05:40 mail.i2tch.com python[9004]: detected unhandled Python exception in '/bin/pyzor'
Jan 15 13:05:40 mail.i2tch.com MailScanner[9010]: Reading configuration file /etc/MailScanner/MailScanner.conf
Jan 15 13:05:40 mail.i2tch.com MailScanner[9010]: Reading configuration file /etc/MailScanner/conf.d/README
Jan 15 13:05:40 mail.i2tch.com MailScanner[9010]: Read 1500 hostnames from the phishing whitelist
Jan 15 13:05:40 mail.i2tch.com MailScanner[9010]: Read 16624 hostnames from the phishing blacklists
Jan 15 13:05:40 mail.i2tch.com MailScanner[9010]: Using SpamAssassin results cache
Jan 15 13:05:40 mail.i2tch.com MailScanner[9010]: Connected to SpamAssassin cache database
Jan 15 13:05:40 mail.i2tch.com MailScanner[9010]: Enabling SpamAssassin auto-whitelist functionality...
```

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

```
[root@mail MailScanner-5.1.2-2]# telnet localhost 25
```

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.i2tch.com ESMTP Postfix (2.10.1)
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 8F8753344BC3
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/maillog** :

```
[root@mail MailScanner-5.1.2-2]# tail /var/log/maillog
Jan 15 13:30:25 mail postfix/smtpd[21411]: connect from localhost.localdomain[127.0.0.1]
Jan 15 13:31:05 mail postfix/smtpd[21411]: C2F683344BC3: client=localhost.localdomain[127.0.0.1],
sasl_method=PLAIN, sasl_username=trainee@i2tch.com
Jan 15 13:31:25 mail postfix/cleanup[21727]: C2F683344BC3: hold: header Received: from me (localhost.localdomain
[127.0.0.1])??by mail.i2tch.com (Postfix) with ESMTPA id C2F683344BC3??for <mickey.mouse@i2tch.com>; Tue, 15 Jan
2019 13:30:56 +0100 (CET) from localhost.localdomain[127.0.0.1]; from=<root@i2tch.com>
to=<mickey.mouse@i2tch.com> proto=ESMTP helo=<me>
Jan 15 13:31:25 mail postfix/cleanup[21727]: C2F683344BC3: message-
id=<20190115123105.C2F683344BC3@mail.i2tch.com>
Jan 15 13:31:25 mail MailScanner[9269]: New Batch: Scanning 1 messages, 1201 bytes
Jan 15 13:31:25 mail MailScanner[9269]: Virus and Content Scanning: Starting
Jan 15 13:31:26 mail MailScanner[9269]: SpamAssassin cache hit for message C2F683344BC3.A958A
Jan 15 13:31:26 mail MailScanner[9269]: Spam Checks: Found 1 spam messages
Jan 15 13:31:26 mail MailScanner[9269]: Deleted 1 messages from processing-database
Jan 15 13:31:29 mail postfix/smtpd[21411]: disconnect from localhost.localdomain[127.0.0.1]
```

Important - Notez la présence de la ligne suivante : **Jan 15 13:31:26 mail MailScanner[9269]: Spam Checks: Found 1 spam messages**.

LAB #8 - 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 :

```
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 MailScanner-5.1.2-2]# cd ~
[root@mail ~]# vi /etc/dovecot/dovecot.conf
[root@mail ~]# cat /etc/dovecot/dovecot.conf
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-mail.conf    15-lda.conf        20-lmtp.conf  90-plugin.conf              auth-
deny.conf.ext  auth-master.conf.ext      auth-static.conf.ext
10-director.conf  10-master.conf  15-mailboxes.conf  20-pop3.conf  90-quota.conf               auth-
```

```
dict.conf.ext  auth-passwdfile.conf.ext  auth-system.conf.ext
10-logging.conf   10-ssl.conf     20-imap.conf       90-acl.conf   auth-checkpassword.conf.ext  auth-
ldap.conf.ext  auth-sql.conf.ext         auth-vpopmail.conf.ext
```

Afin de dire à Dovecot où regarder pour retrouver les mails, éditez le fichier **/etc/dovecot/conf.d/10-mail.conf** en décommentant la directive **mail_location** suivante :

```
...
#
#   mail_location = maildir:~/Maildir
mail_location = mbox:~/mail:INBOX=/var/mail/%u
#   mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
...
```

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
# 2.2.36 (1f10bfa63): /etc/dovecot/dovecot.conf
# OS: Linux 3.10.0-957.1.3.el7.x86_64 x86_64 CentOS Linux release 7.6.1810 (Core)
# Hostname: mail.i2tch.com
first_valid_uid = 1000
mail_location = mbox:~/mail:INBOX=/var/mail/%u
mail_privileged_group = mail
mbox_write_locks = fcntl
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
}
ssl = required
ssl_cert = </etc/pki/dovecot/certs/dovecot.pem
ssl_key =  # hidden, use -P to show it
userdb {
  driver = passwd
}
```

Activez et démarrez le service dovecot :

```
[root@mail ~]# systemctl status dovecot
● dovecot.service - Dovecot IMAP/POP3 email server
   Loaded: loaded (/usr/lib/systemd/system/dovecot.service; disabled; vendor preset: disabled)
```

```
   Active: inactive (dead)
     Docs: man:dovecot(1)
           http://wiki2.dovecot.org/
[root@mail ~]# systemctl enable dovecot
Created symlink from /etc/systemd/system/multi-user.target.wants/dovecot.service to
/usr/lib/systemd/system/dovecot.service.
[root@mail ~]# systemctl start dovecot
[root@mail ~]# systemctl status dovecot
● dovecot.service - Dovecot IMAP/POP3 email server
   Loaded: loaded (/usr/lib/systemd/system/dovecot.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-01-15 14:01:20 CET; 2s ago
     Docs: man:dovecot(1)
           http://wiki2.dovecot.org/
  Process: 10242 ExecStart=/usr/sbin/dovecot (code=exited, status=0/SUCCESS)
  Process: 10235 ExecStartPre=/usr/libexec/dovecot/prestartscript (code=exited, status=0/SUCCESS)
 Main PID: 10244 (dovecot)
   CGroup: /system.slice/dovecot.service
           ├─10244 /usr/sbin/dovecot
           ├─10245 dovecot/anvil
           ├─10246 dovecot/log
           └─10248 dovecot/config

Jan 15 14:01:20 mail.i2tch.com systemd[1]: Starting Dovecot IMAP/POP3 email server...
Jan 15 14:01:20 mail.i2tch.com systemd[1]: PID file /var/run/dovecot/master.pid not readable (yet?) after start.
Jan 15 14:01:20 mail.i2tch.com dovecot[10244]: master: Dovecot v2.2.36 (1f10bfa63) starting up for imap, pop3,
lmtp (core dumps disabled)
Jan 15 14:01:20 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 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK Dovecot ready.
USER trainee
+OK
PASS trainee
+OK Logged in.
LIST
+OK 1 messages:
1 440
.
RETR 1
+OK 440 octets
Return-Path: <root@i2tch.com>
X-Original-To: trainee@i2tch.com
Delivered-To: trainee@i2tch.com
Received: from me (localhost.localdomain [127.0.0.1])
    by mail.i2tch.com (Postfix) with SMTP id E68953344BC3
    for <trainee@i2tch.com>; Mon, 14 Jan 2019 11:49:03 +0100 (CET)
Subject: Test email
Message-Id: <20190114104913.E68953344BC3@mail.i2tch.com>
Date: Mon, 14 Jan 2019 11:49:03 +0100 (CET)
From: root@i2tch.com
```

```
Ceci est un test
.
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
Removed symlink /etc/systemd/system/multi-user.target.wants/dovecot.service.
[root@mail ~]# systemctl status dovecot
● dovecot.service - Dovecot IMAP/POP3 email server
   Loaded: loaded (/usr/lib/systemd/system/dovecot.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:dovecot(1)
           http://wiki2.dovecot.org/

Jan 15 14:01:20 mail.i2tch.com systemd[1]: Started Dovecot IMAP/POP3 email server.
Jan 15 14:03:51 mail.i2tch.com dovecot[10246]: pop3-login: Login: user=<trainee>, method=PLAIN, rip=127.0.0.1,
lip=127.0.0.1, mpid=11390, secured, session=<.../+KV/AAAB>
Jan 15 14:04:35 mail.i2tch.com dovecot[10246]: pop3(trainee): Disconnected: Logged out top=0/0, retr=1/641,
del=0/6, size=14166
Jan 15 14:05:51 mail.i2tch.com dovecot[10246]: pop3-login: Login: user=<trainee>, method=PLAIN, rip=127.0.0.1,
lip=127.0.0.1, mpid=12286, secured, session=<.../YqZ/AAAB>
Jan 15 14:06:14 mail.i2tch.com dovecot[10246]: pop3(trainee): Disconnected: Logged out top=0/0, retr=1/456,
```

```
del=0/6, size=14166
Jan 15 14:08:47 mail.i2tch.com dovecot[10246]: pop3-login: Login: user=<trainee>, method=PLAIN, rip=127.0.0.1,
lip=127.0.0.1, mpid=13684, secured, session=<.../BKd/AAAB>
Jan 15 14:09:00 mail.i2tch.com dovecot[10246]: pop3(trainee): Disconnected: Logged out top=0/0, retr=1/456,
del=0/1, size=440
Jan 15 14:30:35 mail.i2tch.com systemd[1]: Stopping Dovecot IMAP/POP3 email server...
Jan 15 14:30:35 mail.i2tch.com dovecot[10244]: master: Warning: Killed with signal 15 (by pid=23481 uid=0
code=kill)
Jan 15 14:30:36 mail.i2tch.com systemd[1]: Stopped Dovecot IMAP/POP3 email server.
Hint: Some lines were ellipsized, use -l to show in full.
```

Cas #2 - Cyrus-Imap

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

```
[root@mail ~]# vi /etc/imapd.conf
[root@mail ~]# cat /etc/imapd.conf
defaultdomain:              i2tch.com
servername:                 mail.i2tch.com
configdirectory:        /var/lib/imap
partition-default:      /var/spool/imap
admins:             root
sievedir:           /var/lib/imap/sieve
sendmail:           /usr/sbin/sendmail
hashimapspool:          true
sasl_pwcheck_method:        saslauthd
sasl_mech_list:         PLAIN LOGIN
allowanonymouslogin:        no
allowplaintext:         yes
tls_cert_file:          /etc/pki/cyrus-imapd/lel_cert.pem
tls_key_file:           /etc/pki/cyrus-imapd/lel_clef.pem
tls_ca_file:            /etc/pki/tls/certs/cacert.pem
```

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**.

Important - Les scripts Sieve ou **filtres** Sieve sont utilisés par Cyrus-Imap et par Dovecot et sont appliqués lorsque l'e-mail est remis à une boîte aux lettres. Pour plus d'informations, consultez **cette page**

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

```
[root@mail ~]# cp /etc/pki/CA/cacert.pem /etc/pki/tls/certs
[root@mail ~]# cp /etc/pki/tls/misc/lel_cert.pem /etc/pki/cyrus-imapd/
[root@mail ~]# cp /etc/pki/tls/misc/lel_clef.pem /etc/pki/cyrus-imapd/
[root@mail ~]# chmod 644 /etc/pki/tls/certs/cacert.pem
[root@mail ~]# chmod 640 /etc/pki/cyrus-imapd/lel_clef.pem /etc/pki/cyrus-imapd/lel_cert.pem
[root@mail ~]# chown root:mail /etc/pki/cyrus-imapd/lel_clef.pem /etc/pki/cyrus-imapd/lel_cert.pem
```

Activez le service **cyrus-imapd** :

```
[root@mail ~]# systemctl status cyrus-imapd
● cyrus-imapd.service - Cyrus-imapd IMAP/POP3 email server
   Loaded: loaded (/usr/lib/systemd/system/cyrus-imapd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@mail ~]# systemctl enable cyrus-imapd
Created symlink from /etc/systemd/system/multi-user.target.wants/cyrus-imapd.service to
/usr/lib/systemd/system/cyrus-imapd.service.
```

Configurez postfix pour utiliser Cyrus-Imapd en décommentant la ligne suivante 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 $mail_name ($mail_version)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############  RELAY HOST  ##############
# relayhost = smtp.bbox.fr
#############  USER/GROUP  ##############
mail_owner = postfix
```

```
setgid_group = postdrop
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
############   DEBUGGING   ##############
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5
############   COMMANDES   ##############
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
############  REPERTOIRES  ##############
mail_spool_directory = /var/spool/mail
html_directory = no
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
############      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
############      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
```

Démarrez le service **cyrus-imapd** :

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

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

```
[root@mail ~]# cyradm localhost
```

```
Password:
localhost.localdomain> cm user.trainee
localhost.localdomain> setquota user.trainee 20000
quota:20000
localhost.localdomain> 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
```

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

```
[root@mail ~]# 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 v2.4.17-Fedora-RPM-2.4.17-13.el7 server ready
C: S01 STARTTLS
S: S01 OK Begin TLS negotiation now
verify error:num=19:self signed certificate in certificate chain
TLS connection established: TLSv1.2 with cipher DHE-RSA-AES256-GCM-SHA384 (256/256 bits)
C: C01 CAPABILITY
S: * CAPABILITY IMAP4rev1 LITERAL+ ID ENABLE ACL RIGHTS=kxte QUOTA MAILBOX-REFERRALS NAMESPACE UIDPLUS
NO_ATOMIC_RENAME UNSELECT CHILDREN MULTIAPPEND BINARY CATENATE CONDSTORE ESEARCH SORT SORT=MODSEQ SORT=DISPLAY
THREAD=ORDEREDSUBJECT THREAD=REFERENCES ANNOTATEMORE LIST-EXTENDED WITHIN QRESYNC SCAN XLIST URLAUTH
URLAUTH=BINARY X-NETSCAPE AUTH=PLAIN AUTH=LOGIN SASL-IR COMPRESS=DEFLATE IDLE
S: C01 OK Completed
Please enter your password: trainee
C: A01 AUTHENTICATE PLAIN AHJvb3QAZmVuZXN0cm9z
```

```
S: A01 OK [CAPABILITY IMAP4rev1 LITERAL+ ID ENABLE ACL RIGHTS=kxte QUOTA MAILBOX-REFERRALS NAMESPACE UIDPLUS
NO_ATOMIC_RENAME UNSELECT CHILDREN MULTIAPPEND BINARY CATENATE CONDSTORE ESEARCH SORT SORT=MODSEQ SORT=DISPLAY
THREAD=ORDEREDSUBJECT THREAD=REFERENCES ANNOTATEMORE LIST-EXTENDED WITHIN QRESYNC SCAN XLIST URLAUTH
URLAUTH=BINARY X-NETSCAPE LOGINDISABLED COMPRESS=DEFLATE IDLE] Success (tls protection)
SESSIONID=<mail.i2tch.com-2975-1547560305-1>
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 ~]# imtest --help
imtest: invalid option -- '-'
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 #9 - Gestion des Domaines Virtuels avec MariaDB, Postfix et Dovecot

A Faire - Demandez à votre formateur de restaurer le snapshot d'origine de votre VM.

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@centos7 ~]# vi /etc/hosts
You have mail in /var/spool/mail/root
[root@centos7 ~]# cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain6 localhost6
10.0.2.51   i2tch.com
10.0.2.51   mail.i2tch.com  mail
```

Modification du FQDN

Modifiez le FQDN de votre VM :

```
[root@centos7 ~]# nmcli g hostname mail.i2tch.com
[root@centos7 ~]# hostname
mail.i2tch.com
```

Modification de SELinux

```
[root@mail ~]# setenforce permissive
[root@mail ~]# vi /etc/selinux/config
[root@mail ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Démarrage du Service ntpd

Activez et démarrez le serveur **ntpd** :

```
[root@mail ~]# systemctl status ntpd
● ntpd.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@mail ~]# systemctl enable ntpd
Created symlink from /etc/systemd/system/multi-user.target.wants/ntpd.service to
/usr/lib/systemd/system/ntpd.service.
[root@mail ~]# systemctl start ntpd
```

Configurer 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
```

Créer un Certificat

Commencez par exécuter le script CA qui se trouve dans **/etc/pki/tls/misc** :

```
[root@mail ~]# cd /etc/pki/tls/misc
[root@mail misc]# ls -l
total 24
-rwxr-xr-x. 1 root root 5178 Oct 30 23:42 CA
-rwxr-xr-x. 1 root root  119 Oct 30 23:42 c_hash
```

```
-rwxr-xr-x. 1 root root  152 Oct 30 23:42 c_info
-rwxr-xr-x. 1 root root  112 Oct 30 23:42 c_issuer
-rwxr-xr-x. 1 root root  110 Oct 30 23:42 c_name

[root@mail misc]# ./CA -newca
CA certificate filename (or enter to create)

Making CA certificate ...
Generating a 2048 bit RSA private key
..+++
.....................................................................................+++
writing new private key to '/etc/pki/CA/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) [XX]:GB
State or Province Name (full name) []:SURREY
Locality Name (eg, city) [Default City]:ADDLESTONE
Organization Name (eg, company) [Default Company Ltd]:I2TCH LTD
Organizational Unit Name (eg, section) []:TRAINING
Common Name (eg, your name or your server's hostname) []: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 []:
```

```
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            d9:6a:23:bb:78:9c:f8:80
        Validity
            Not Before: Jan 14 13:08:21 2019 GMT
            Not After : Jan 13 13:08:21 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:
                2D:14:39:2D:F5:C2:FE:75:31:9A:CB:95:A2:C0:19:18:9D:8C:7D:EE
            X509v3 Authority Key Identifier:
                keyid:2D:14:39:2D:F5:C2:FE:75:31:9A:CB:95:A2:C0:19:18:9D:8C:7D:EE

            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until Jan 13 13:08:21 2022 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
```

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

```
[root@mail misc]# ls /etc/pki/CA
cacert.pem  careq.pem  certs  crl  index.txt  index.txt.attr  index.txt.old  newcerts  private  serial
```

```
[root@mail misc]# ls /etc/pki/CA/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 misc]# openssl req -new -nodes -keyout lel_clef.pem -out lel_req.pem
Generating a 2048 bit 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) [XX]:GB
State or Province Name (full name) []:SURREY
Locality Name (eg, city) [Default City]:ADDLESTONE
Organization Name (eg, company) [Default Company Ltd]:I2TCH LTD
Organizational Unit Name (eg, section) []:TRAINING
Common Name (eg, your name or your server's hostname) []: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 misc]# ls
CA  c_hash  c_info  c_issuer  c_name  lel_clef.pem  lel_req.pem
```

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 misc]# openssl ca -out lel_cert.pem -infiles lel_req.pem
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:fenestros
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            d9:6a:23:bb:78:9c:f8:81
        Validity
            Not Before: Jan 14 13:14:14 2019 GMT
            Not After : Jan 14 13:14:14 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:
                B8:63:90:BF:FD:A6:8F:4F:7B:2E:67:76:C5:FB:6E:78:9B:E1:59:02
```

```
            X509v3 Authority Key Identifier:
                keyid:2D:14:39:2D:F5:C2:FE:75:31:9A:CB:95:A2:C0:19:18:9D:8C:7D:EE

Certificate is to be certified until Jan 14 13:14:14 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 misc]# cp lel_cert.pem lel_clef.pem /etc/postfix
[root@mail misc]# cp /etc/pki/CA/cacert.pem /etc/postfix
[root@mail misc]# chmod 644 /etc/postfix/lel_cert.pem /etc/postfix/cacert.pem
[root@mail misc]# chmod 400 /etc/postfix/lel_clef.pem
```

Installer mariadb et dovecot-mysql

Installez le deux paquets suivants à l'aide de **yum** :

```
[root@mail ~]# yum install postfix dovecot mariadb-server dovecot-mysql
```

Votre VM devrait contenir les versions suivantes ou supérieures des paquets **postfix**, **dovecot** et **mariadb** :

```
[root@mail ~]# rpm -qa | grep postfix
```

```
postfix-2.10.1-7.el7.x86_64
[root@mail ~]# rpm -qa | grep dovecot
dovecot-mysql-2.2.36-3.el7.x86_64
dovecot-2.2.36-3.el7.x86_64
[root@mail ~]# rpm -qa | grep maria
mariadb-libs-5.5.60-1.el7_5.x86_64
mariadb-server-5.5.60-1.el7_5.x86_64
mariadb-5.5.60-1.el7_5.x86_64
```

Activez et démarrez MariaDB :

```
[root@mail ~]# systemctl enable mariadb
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to
/usr/lib/systemd/system/mariadb.service.
[root@mail ~]# systemctl start mariadb
[root@mail ~]# systemctl status mariadb
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-01-15 17:34:16 CET; 50min ago
 Main PID: 13180 (mysqld_safe)
   CGroup: /system.slice/mariadb.service
           ├─13180 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
           └─13342 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-
dir=/usr/lib64/mysql/plugin --log-error=/var/log/mariadb/mariadb.log --pid-fil...

Jan 15 17:34:14 mail.i2tch.com mariadb-prepare-db-dir[13090]: MySQL manual for more instructions.
Jan 15 17:34:14 mail.i2tch.com mariadb-prepare-db-dir[13090]: Please report any problems at
http://mariadb.org/jira
Jan 15 17:34:14 mail.i2tch.com mariadb-prepare-db-dir[13090]: The latest information about MariaDB is available
at http://mariadb.org/.
Jan 15 17:34:14 mail.i2tch.com mariadb-prepare-db-dir[13090]: You can find additional information about the MySQL
part at:
Jan 15 17:34:14 mail.i2tch.com mariadb-prepare-db-dir[13090]: http://dev.mysql.com
Jan 15 17:34:14 mail.i2tch.com mariadb-prepare-db-dir[13090]: Consider joining MariaDB's strong and vibrant
```

```
community:
Jan 15 17:34:14 mail.i2tch.com mariadb-prepare-db-dir[13090]: https://mariadb.org/get-involved/
Jan 15 17:34:14 mail.i2tch.com mysqld_safe[13180]: 190115 17:34:14 mysqld_safe Logging to
'/var/log/mariadb/mariadb.log'.
Jan 15 17:34:15 mail.i2tch.com mysqld_safe[13180]: 190115 17:34:15 mysqld_safe Starting mysqld daemon with
databases from /var/lib/mysql
Jan 15 17:34:16 mail.i2tch.com systemd[1]: Started MariaDB database server.
```

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): [Entrée]
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:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 11
Server version: 5.5.60-MariaDB MariaDB Server

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)]>
```

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

Créer les Tables de la Base 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 [(none)]> USE mailserver;
Database changed
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]>
```

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
smtpd_banner = $myhostname ESMTP $mail_name (CentOS)
biff = no

append_dot_mydomain = no

readme_directory = no

smtpd_tls_cert_file=/etc/postfix/lel_cert.pem
smtpd_tls_key_file=/etc/postfix/lel_clef.pem
smtpd_use_tls=yes
smtpd_tls_auth_only = yes
smtp_tls_security_level = may
smtpd_tls_security_level = may
smtpd_sasl_security_options = noanonymous, noplaintext
smtpd_sasl_tls_security_options = noanonymous

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = i2tch.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```

```
mydomain = i2tch.com
myorigin = $mydomain
mydestination = localhost, localhost.$mydomain
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all

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
● 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 20:25:51 CET; 10s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 26951 ExecStop=/usr/lib/MailScanner/init/ms-init stop (code=exited, status=0/SUCCESS)
  Process: 27020 ExecStart=/usr/lib/MailScanner/init/ms-init start (code=exited, status=0/SUCCESS)
 Main PID: 27591 (MailScanner: st)
   CGroup: /system.slice/mailscanner.service
           ├─27591 MailScanner: starting children
           ├─27593 MailScanner: waiting for messages
           ├─27682 MailScanner: starting children
           └─27802 MailScanner: starting children

Jan 15 20:25:57 mail.i2tch.com MailScanner[27682]: Connected to SpamAssassin cache database
Jan 15 20:25:57 mail.i2tch.com MailScanner[27682]: Enabling SpamAssassin auto-whitelist functionality...
Jan 15 20:25:57 mail.i2tch.com python[27683]: detected unhandled Python exception in '/bin/pyzor'
Jan 15 20:26:00 mail.i2tch.com MailScanner[27593]: Connected to Processing Attempts Database
Jan 15 20:26:00 mail.i2tch.com MailScanner[27593]: Found 0 messages in the Processing Attempts Database
Jan 15 20:26:00 mail.i2tch.com MailScanner[27593]: Using locktype = flock
Jan 15 20:26:01 mail.i2tch.com MailScanner[27802]: MailScanner Email Processor version 5.1.2 starting...
Jan 15 20:26:01 mail.i2tch.com MailScanner[27802]: Reading configuration file /etc/MailScanner/MailScanner.conf
Jan 15 20:26:01 mail.i2tch.com MailScanner[27802]: Reading configuration file /etc/MailScanner/conf.d/README
Jan 15 20:26:01 mail.i2tch.com MailScanner[27802]: Read 1500 hostnames from the phishing whitelist
```

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)   (yes)    (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
#smtp      inet  n       -       -       -       1       postscreen
#smtpd     pass  -       -       -       -       -       smtpd
#dnsblog   unix  -       -       -       -       0       dnsblog
#tlsproxy  unix  -       -       -       -       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=dovecot
  -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=dovecot
  -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 (/usr/lib/systemd/system/postfix.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2019-01-17 16:25:31 CET; 6s ago
  Process: 7276 ExecStop=/usr/sbin/postfix stop (code=exited, status=0/SUCCESS)
  Process: 7290 ExecStart=/usr/sbin/postfix start (code=exited, status=0/SUCCESS)
  Process: 7288 ExecStartPre=/usr/libexec/postfix/chroot-update (code=exited, status=0/SUCCESS)
  Process: 7286 ExecStartPre=/usr/libexec/postfix/aliasesdb (code=exited, status=0/SUCCESS)
 Main PID: 7362 (master)
   CGroup: /system.slice/postfix.service
           ├─7362 /usr/libexec/postfix/master -w
           ├─7363 pickup -l -t unix -u
           └─7364 qmgr -l -t unix -u

Jan 17 16:25:30 mail.i2tch.com systemd[1]: Stopped Postfix Mail Transport Agent.
Jan 17 16:25:30 mail.i2tch.com systemd[1]: Starting Postfix Mail Transport Agent...
Jan 17 16:25:31 mail.i2tch.com postfix/master[7362]: daemon started -- version 2.10.1, configuration /etc/postfix
Jan 17 16:25:31 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
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
```

Important - **Local Mail Transfer Protocol** (LMTP, protocole local de transfert de courrier) est une variante de ESMTP. LMTP est défini dans la RFC 20331.

/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
}
first_valid_uid = 1000
protocol !indexer-worker {
}
mbox_write_locks = fcntl
```

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/
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
```

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 (/usr/lib/systemd/system/dovecot.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2019-01-15 22:54:38 CET; 7s ago
     Docs: man:dovecot(1)
           http://wiki2.dovecot.org/
  Process: 31442 ExecStop=/usr/bin/doveadm stop (code=exited, status=0/SUCCESS)
  Process: 31457 ExecStart=/usr/sbin/dovecot (code=exited, status=0/SUCCESS)
  Process: 31446 ExecStartPre=/usr/libexec/dovecot/prestartscript (code=exited, status=0/SUCCESS)
 Main PID: 31459 (dovecot)
   CGroup: /system.slice/dovecot.service
           ├─31459 /usr/sbin/dovecot
           ├─31462 dovecot/anvil
           ├─31463 dovecot/log
           └─31465 dovecot/config

Jan 15 22:54:38 mail.i2tch.com systemd[1]: Stopped Dovecot IMAP/POP3 email server.
Jan 15 22:54:38 mail.i2tch.com systemd[1]: Starting Dovecot IMAP/POP3 email server...
Jan 15 22:54:38 mail.i2tch.com systemd[1]: PID file /var/run/dovecot/master.pid not readable (yet?) after start.
Jan 15 22:54:38 mail.i2tch.com dovecot[31459]: master: Dovecot v2.2.36 (1f10bfa63) starting up for imap, pop3,
lmtp (core dumps disabled)
Jan 15 22:54:38 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
Subject: Test
This is a test using MariaDB
[^D]
EOT
```

Consultez la fin du fichier **/var/log/maillog** :

```
[root@mail ~]# tail /var/log/maillog
Jan 17 16:25:31 mail postfix/master[7362]: daemon started -- version 2.10.1, configuration /etc/postfix
Jan 17 16:30:48 mail dovecot: master: Dovecot v2.2.36 (1f10bfa63) starting up for imap, pop3, lmtp (core dumps
disabled)
Jan 17 16:31:34 mail postfix/pickup[7363]: 9C2D83344BC4: uid=0 from=<root>
Jan 17 16:31:34 mail postfix/cleanup[10141]: 9C2D83344BC4: message-id=<20190117153134.9C2D83344BC4@i2tch.com>
Jan 17 16:31:34 mail postfix/qmgr[7364]: 9C2D83344BC4: from=<root@i2tch.com>, size=440, nrcpt=1 (queue active)
Jan 17 16:31:34 mail dovecot: lmtp(10155): Connect from local
Jan 17 16:31:34 mail dovecot: lmtp(trainee@i2tch.com): msgid=<20190117153134.9C2D83344BC4@i2tch.com>: saved mail
to INBOX
Jan 17 16:31:34 mail dovecot: lmtp(10155): Disconnect from local: Successful quit
Jan 17 16:31:34 mail postfix/lmtp[10150]: 9C2D83344BC4: to=<trainee@i2tch.com>, relay=i2tch.com[private/dovecot-
lmtp], delay=0.29, delays=0.16/0.06/0.02/0.05, dsn=2.0.0, status=sent (250 2.0.0 <trainee@i2tch.com>
yMMqMNafQFyrJwAAUpw4tw Saved)
Jan 17 16:31:34 mail postfix/qmgr[7364]: 9C2D83344BC4: 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 trainee]# yum install mutt
[root@mail trainee]# mutt -f .
```

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

```
t  d:Del  u:Undel  s:Save  m:Mail  r:Reply  g:Group  ?:Help
   1     Jan 17 root            (0.1K) Test MariaDB
```

En sélectionnant ce message, vous constaterez son contenu :

```
i:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.  d:Del  r:Reply  j:Next ?:Help
Date: Thu, 17 Jan 2019 16:31:34 +0100
From: root <root@i2tch.com>
To: trainee@i2tch.com
Subject: Test MariaDB
User-Agent: Heirloom mailx 12.5 7/5/10

This is a test with MariaDB
```

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

```
[root@mail trainee]# find
.
./cur
./cur/1547739094.M848526P10155.mail.i2tch.com,S=627,W=645
./new
./tmp
./dovecot.index.log
./dovecot-uidvalidity.5c409fd6
./dovecot-uidvalidity
./dovecot-uidlist
```

```
./dovecot.index.cache
[root@mail trainee]# cd cur
[root@mail cur]# ls
1547739094.M848526P10155.mail.i2tch.com,S=627,W=645:2,S
[root@mail cur]# cat 1547739094.M848526P10155.mail.i2tch.com\,S\=627\,W\=645\:2\,S
Return-Path: <root@i2tch.com>
Delivered-To: trainee@i2tch.com
Received: from i2tch.com
    by mail.i2tch.com with LMTP id yMMqMNafQFyrJwAAUpw4tw
    for <trainee@i2tch.com>; Thu, 17 Jan 2019 16:31:34 +0100
Received: by i2tch.com (Postfix, from userid 0)
    id 9C2D83344BC4; Thu, 17 Jan 2019 16:31:34 +0100 (CET)
Date: Thu, 17 Jan 2019 16:31:34 +0100
To: trainee@i2tch.com
Subject: Test MariaDB
User-Agent: Heirloom mailx 12.5 7/5/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20190117153134.9C2D83344BC4@i2tch.com>
From: root@i2tch.com (root)

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

Consultez la fin du fichier **/var/log/maillog** :

```
[root@mail ~]# tail /var/log/maillog
Jan 17 16:31:34 mail postfix/qmgr[7364]: 9C2D83344BC4: removed
Jan 17 16:50:43 mail dovecot: pop3-login: Disconnected (no auth attempts in 7 secs): user=<>, rip=127.0.0.1,
lip=127.0.0.1, TLS handshaking: SSL_accept() failed: error:140760FC:SSL routines:SSL23_GET_CLIENT_HELLO:unknown
protocol, session=<xzRsW6l/zsF/AAAB>
Jan 17 16:59:18 mail postfix/pickup[7363]: 0F1543344BC4: uid=0 from=<root>
Jan 17 16:59:18 mail postfix/cleanup[22808]: 0F1543344BC4: message-id=<20190117155918.0F1543344BC4@i2tch.com>
Jan 17 16:59:18 mail postfix/qmgr[7364]: 0F1543344BC4: from=<root@i2tch.com>, size=453, nrcpt=1 (queue active)
Jan 17 16:59:18 mail dovecot: lmtp(22823): Connect from local
Jan 17 16:59:18 mail dovecot: lmtp(trainee@i2tch.com): msgid=<20190117155918.0F1543344BC4@i2tch.com>: saved mail
to INBOX
Jan 17 16:59:18 mail dovecot: lmtp(22823): Disconnect from local: Successful quit
Jan 17 16:59:18 mail postfix/lmtp[22822]: 0F1543344BC4: to=<trainee@i2tch.com>, orig_to=<mickey.mouse@i2tch.com>,
relay=i2tch.com[private/dovecot-lmtp], delay=0.19, delays=0.09/0.02/0.02/0.06, dsn=2.0.0, status=sent (250 2.0.0
<trainee@i2tch.com> UEr5B1amQFwnWQAAUpw4tw Saved)
Jan 17 16:59:18 mail postfix/qmgr[7364]: 0F1543344BC4: 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 ~]# cd -
/var/mail/vhosts/i2tch.com/trainee/cur
[root@mail cur]# cd ..
[root@mail trainee]# find
.
./cur
./cur/1547739094.M848526P10155.mail.i2tch.com,S=627,W=645:2,S
./new
./new/1547740758.M173817P22823.mail.i2tch.com,S=640,W=658
./tmp
./dovecot.index.log
./dovecot-uidvalidity.5c409fd6
./dovecot-uidvalidity
./dovecot-uidlist
./dovecot.index.cache
[root@mail trainee]# cd new
[root@mail new]# ls
1547740758.M173817P22823.mail.i2tch.com,S=640,W=658
[root@mail new]# cat 1547740758.M173817P22823.mail.i2tch.com\,S\=640\,W\=658
Return-Path: <root@i2tch.com>
Delivered-To: trainee@i2tch.com
Received: from i2tch.com
    by mail.i2tch.com with LMTP id UEr5B1amQFwnWQAAUpw4tw
    for <trainee@i2tch.com>; Thu, 17 Jan 2019 16:59:18 +0100
Received: by i2tch.com (Postfix, from userid 0)
    id 0F1543344BC4; Thu, 17 Jan 2019 16:59:18 +0100 (CET)
Date: Thu, 17 Jan 2019 16:59:17 +0100
To: mickey.mouse@i2tch.com
Subject: Test Mickey Mouse
User-Agent: Heirloom mailx 12.5 7/5/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20190117155918.0F1543344BC4@i2tch.com>
```

```
From: root@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**.

A Faire - Pour plus d'explications concernant le format du nom **1547740758.M173817P22823.mail.i2tch.com,S=640,W=658**, consultez **cette page**.

trainee@mail.i2tch.com

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

```
[root@mail new]# mail trainee@mail.i2tch.com
Subject: Test mail.i2tch.com
This is a test to the mail.i2tch.com domain
EOT
[root@mail new]# tail /var/log/maillog
Jan 17 16:59:18 mail postfix/lmtp[22822]: 0F1543344BC4: to=<trainee@i2tch.com>, orig_to=<mickey.mouse@i2tch.com>,
relay=i2tch.com[private/dovecot-lmtp], delay=0.19, delays=0.09/0.02/0.02/0.06, dsn=2.0.0, status=sent (250 2.0.0
<trainee@i2tch.com> UEr5B1amQFwnWQAAUpw4tw Saved)
Jan 17 16:59:18 mail postfix/qmgr[7364]: 0F1543344BC4: removed
Jan 17 17:04:20 mail postfix/pickup[7363]: E1DDC3344BC4: uid=0 from=<root>
Jan 17 17:04:20 mail postfix/cleanup[25142]: E1DDC3344BC4: message-id=<20190117160420.E1DDC3344BC4@i2tch.com>
Jan 17 17:04:21 mail postfix/qmgr[7364]: E1DDC3344BC4: from=<root@i2tch.com>, size=468, nrcpt=1 (queue active)
```

```
Jan 17 17:04:21 mail dovecot: lmtp(25152): Connect from local
Jan 17 17:04:21 mail dovecot: lmtp(trainee@mail.i2tch.com): msgid=<20190117160420.E1DDC3344BC4@i2tch.com>: saved
mail to INBOX
Jan 17 17:04:21 mail dovecot: lmtp(25152): Disconnect from local: Successful quit
Jan 17 17:04:21 mail postfix/lmtp[25151]: E1DDC3344BC4: to=<trainee@mail.i2tch.com>,
relay=i2tch.com[private/dovecot-lmtp], delay=0.21, delays=0.12/0.02/0.01/0.06, dsn=2.0.0, status=sent (250 2.0.0
<trainee@mail.i2tch.com> +AojAoWnQFxAYgAAUpw4tw Saved)
Jan 17 17:04:21 mail postfix/qmgr[7364]: E1DDC3344BC4: removed
```

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

```
[root@mail new]# ls
1547740758.M173817P22823.mail.i2tch.com,S=640,W=658
[root@mail new]# cd ..
[root@mail trainee]# find
.
./cur
./cur/1547739094.M848526P10155.mail.i2tch.com,S=627,W=645:2,S
./new
./new/1547740758.M173817P22823.mail.i2tch.com,S=640,W=658
./tmp
./dovecot.index.log
./dovecot-uidvalidity.5c409fd6
./dovecot-uidvalidity
./dovecot-uidlist
./dovecot.index.cache
```

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

```
[root@mail vhosts]# cd ~
[root@mail ~]# ls /var/mail/vhosts/
i2tch.com  mail.i2tch.com
[root@mail ~]# cd /var/mail/vhosts/mail.i2tch.com/
[root@mail mail.i2tch.com]# find
```

```
.
./trainee
./trainee/cur
./trainee/new
./trainee/new/1547741061.M81284P25152.mail.i2tch.com,S=665,W=683
./trainee/tmp
./trainee/dovecot.index.log
./trainee/dovecot-uidvalidity.5c40a785
./trainee/dovecot-uidvalidity
./trainee/dovecot-uidlist
./trainee/dovecot.index.cache
[root@mail mail.i2tch.com]# cat trainee/new/1547741061.M81284P25152.mail.i2tch.com\,S\=665\,W\=683
Return-Path: <root@i2tch.com>
Delivered-To: trainee@mail.i2tch.com
Received: from i2tch.com
    by mail.i2tch.com with LMTP id +AojAoWnQFxAYgAAUpw4tw
    for <trainee@mail.i2tch.com>; Thu, 17 Jan 2019 17:04:21 +0100
Received: by i2tch.com (Postfix, from userid 0)
    id E1DDC3344BC4; Thu, 17 Jan 2019 17:04:20 +0100 (CET)
Date: Thu, 17 Jan 2019 17:04:20 +0100
To: trainee@mail.i2tch.com
Subject: Test mail.i2tch.com
User-Agent: Heirloom mailx 12.5 7/5/10
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Message-Id: <20190117160420.E1DDC3344BC4@i2tch.com>
From: root@i2tch.com (root)

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

LAB #10 - Configuration de Postfix en Environnement chroot

Le site de Postfix fournit un script permettant de configurer postfix en chroot :

```
[root@centos7 ~]# cat LINUX2
#! /bin/sh

# LINUX2 - shell script to set up a Postfix chroot jail for Linux
# Tested on SuSE Linux 5.3 (libc5) and 7.0 (glibc2.1)

# Other testers reported as working:
#
# 2001-01-15 Debian sid (unstable)
#            Christian Kurz <shorty@getuid.de>

# Copyright (c) 2000 - 2001 by Matthias Andree
# Redistributable unter the MIT-style license that follows:
# Abstract: "do whatever you want except hold somebody liable or change
# the copyright information".

# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to
# deal in the Software without restriction, including without limitation the
# rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
# sell copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in
# all copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.  IN NO EVENT SHALL THE
```

```
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
# FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
# IN THE SOFTWARE.

# 2000-09-29
# v0.1: initial release

# 2000-12-05
# v0.2: copy libdb.* for libnss_db.so
#       remove /etc/localtime in case it's a broken symlink
#       restrict find to maxdepth 1 (faster)

# Revision 1.4  2001/01/15 09:36:35  emma
# add note it was successfully tested on Debian sid
#
# 20060101 /lib64 support by Keith Owens.
#

CP="cp -p"

cond_copy() {
  # find files as per pattern in $1
  # if any, copy to directory $2
  dir=`dirname "$1"`
  pat=`basename "$1"`
  lr=`find "$dir" -maxdepth 1 -name "$pat"`
  if test ! -d "$2" ; then exit 1 ; fi
  if test "x$lr" != "x" ; then $CP $1 "$2" ; fi
}

set -e
umask 022
```

```
POSTFIX_DIR=${POSTFIX_DIR-/var/spool/postfix}
cd ${POSTFIX_DIR}

mkdir -p etc lib usr/lib/zoneinfo
test -d /lib64 && mkdir -p lib64

# find localtime (SuSE 5.3 does not have /etc/localtime)
lt=/etc/localtime
if test ! -f $lt ; then lt=/usr/lib/zoneinfo/localtime ; fi
if test ! -f $lt ; then lt=/usr/share/zoneinfo/localtime ; fi
if test ! -f $lt ; then echo "cannot find localtime" ; exit 1 ; fi
rm -f etc/localtime

# copy localtime and some other system files into the chroot's etc
$CP -f $lt /etc/services /etc/resolv.conf /etc/nsswitch.conf etc
$CP -f /etc/host.conf /etc/hosts /etc/passwd etc
ln -s -f /etc/localtime usr/lib/zoneinfo

# copy required libraries into the chroot
cond_copy '/lib/libnss_*.so*' lib
cond_copy '/lib/libresolv.so*' lib
cond_copy '/lib/libdb.so*' lib
if test -d /lib64; then
  cond_copy '/lib64/libnss_*.so*' lib64
  cond_copy '/lib64/libresolv.so*' lib64
  cond_copy '/lib64/libdb.so*' lib64
fi

postfix reload
```

Créez ce script et rendez-le exécutable :

```
[root@centos7 ~]# vi LINUX2
```

```
[root@centos7 ~]# chmod u+x LINUX2
```

Exécutez ce script :

```
[root@centos7 ~]# ./LINUX2
postfix/postfix-script: refreshing the Postfix mail system
```

Notez la création des répertoires **etc**, **lib**, **lib64** et **usr** dans le chroot de postfix :

```
[root@centos7 ~]# ls /var/spool/postfix
active  bounce  corrupt  defer  deferred  etc  flush  hold  incoming  lib  lib64  maildrop  pid  private  public
saved  trace  usr
```

Vérifiez le bon fonctionnement de postfix :

```
[root@centos7 ~]# systemctl status postfix
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2019-01-18 12:09:46 CET; 4min 57s ago
  Process: 2645 ExecStart=/usr/sbin/postfix start (code=exited, status=0/SUCCESS)
  Process: 2637 ExecStartPre=/usr/libexec/postfix/chroot-update (code=exited, status=0/SUCCESS)
  Process: 2594 ExecStartPre=/usr/libexec/postfix/aliasesdb (code=exited, status=0/SUCCESS)
 Main PID: 2902 (master)
   CGroup: /system.slice/postfix.service
           ├─2902 /usr/libexec/postfix/master -w
           ├─4943 pickup -l -t unix -u
           └─4944 qmgr -l -t unix -u

Jan 18 12:09:41 centos7.fenestros.loc systemd[1]: Starting Postfix Mail Transport Agent...
Jan 18 12:09:46 centos7.fenestros.loc postfix/postfix-script[2896]: starting the Postfix mail system
Jan 18 12:09:46 centos7.fenestros.loc postfix/master[2902]: daemon started -- version 2.10.1, configuration
/etc/postfix
Jan 18 12:09:46 centos7.fenestros.loc systemd[1]: Started Postfix Mail Transport Agent.
```

```
Jan 18 12:14:10 centos7.fenestros.loc postfix/master[2902]: reload -- version 2.10.1, configuration /etc/postfix
```