Installer clamav sur postfix avec une Debian

Cet article vous guide pour installer clamav sur une passerelle SMTP avec Postfix.
La distribution utilisée est une Debian.

On peut donc voir cet article comme un prolongement de : Installation et configuration Postfix avec SPF + DKIM

Comment Installer clamsmtp et clamav sur Postfix sur une Debian afin d'analyser les emails par un antivirus.

Installer Clamav

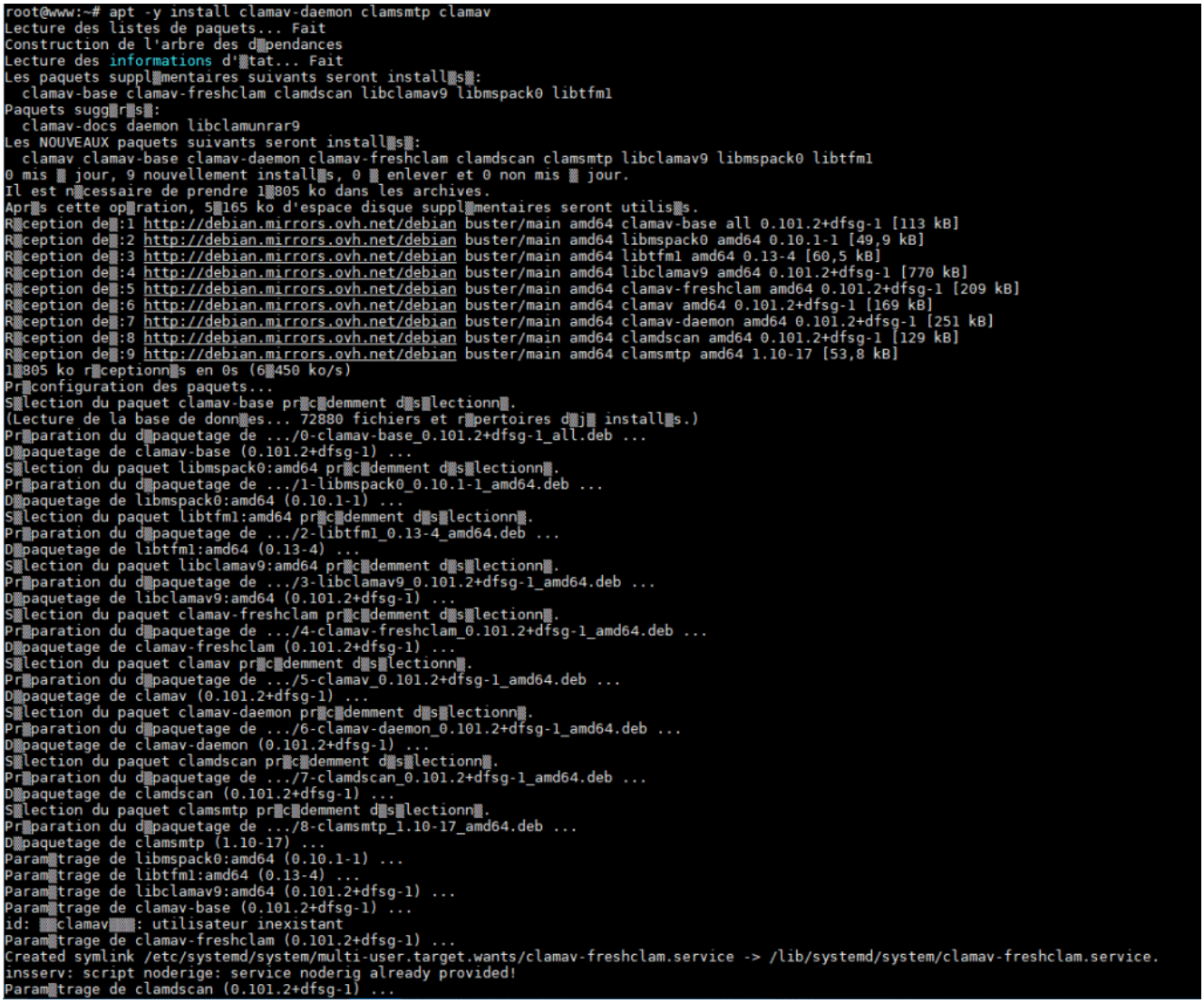
Dans un premier temps il faut installer clamav et ClamSMTP.

ClamSMTP est un daemon mandataire SMTP qui vérifie la présence de virus en utilisant le logiciel anti-virus ClamAV. Il peut agir comme un mandataire SMTP classique avec des ports accessibles publiquement, ou bien comme un mandataire transparent, vers lequel le traffic SMTP est redirigé par votre routeur.

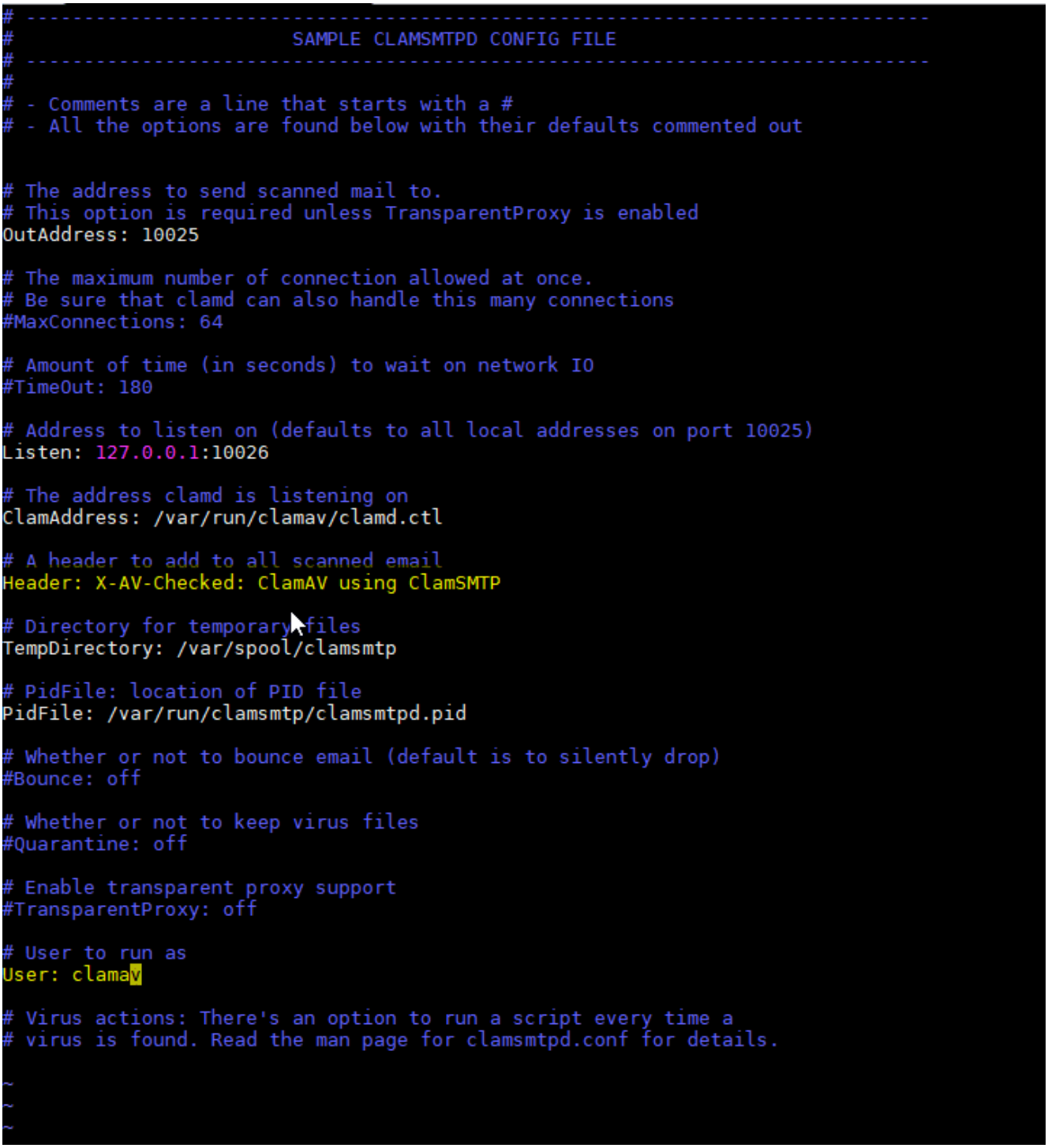
ClamSMTP se veut léger, fiable et simple plutôt que d'avoir une myriade d'options. Il est écrit en C sans dépendances majeures. ClamSMTP ne fait pas de filtrage de pourriel, il vérifie seulement la présence possible de virus.

Pour commencer on installe les paquets avec apt.

```
apt -y install clamav-daemon clamsmtp clamav
```



Ensuite on édite le fichier /etc/clamsmtpd.conf
Décommettez la ligne Header et changer l’utilisateur pour clamav.



Ensuite on mets les droits pour l’utilisateur clamav.

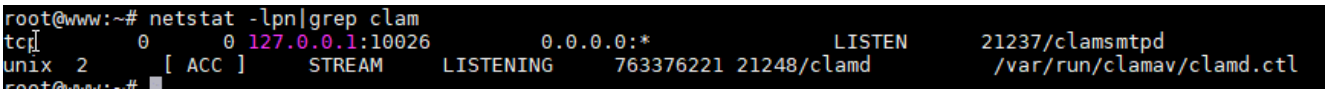
```
chown -R clamav. /var/spool/clamsmtp
chown -R clamav. /var/run/clamsmtp
```

Enfin on redémarre tous les daemons.

systemctl restart clamav-daemon clamsmtp clamav-freshclam

Pour terminer, vérifiez que le socket clamav est bien ouvert afin que la communication vers ce dernier se fasse bien.
Pour cela, on utilise la commande netstat :

netstat -lpn|grep clam



Le socket avec clamd.ctl doit bien être présent.

Configurer Postfix

On peut passer à la configuration de Postfix.
Le but est de faire passer les mails vers le proxy clamsmtp.

Editez le fichier /etc/postfix/main.cf pour ajouter à la fin

content_filter = scan:127.0.0.1:10026

Enfin éditez le fichier /etc/postfix/master.cf pour ajouter ceci à la fin.
Il faut bien laissez un espace devant chaque ligne -o.

scan unix - - n - 16 smtp

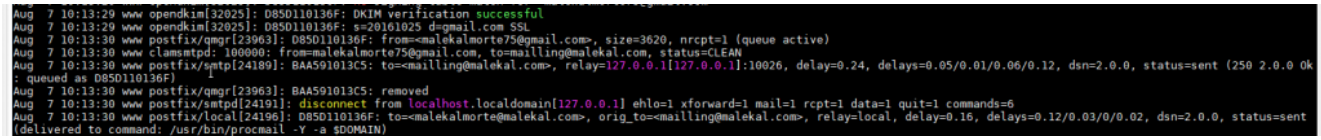
```
   -o smtp_data_done_timeout=1200
   -o smtp_send_xforward_command=yes
   -o disable_dns_lookups=yes
127.0.0.1:10025 inet n       -       n       -       16
smtpd
   -o content_filter=
   -o local_recipient_maps=
   -o relay_recipient_maps=
   -o smtpd_restriction_classes=
   -o smtpd_client_restrictions=
   -o smtpd_helo_restrictions=
   -o smtpd_sender_restrictions=
   -o smtpd_recipient_restrictions=permit_mynetworks,reject
   -o mynetworks_style=host
   -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

Enfin on relance postfix :

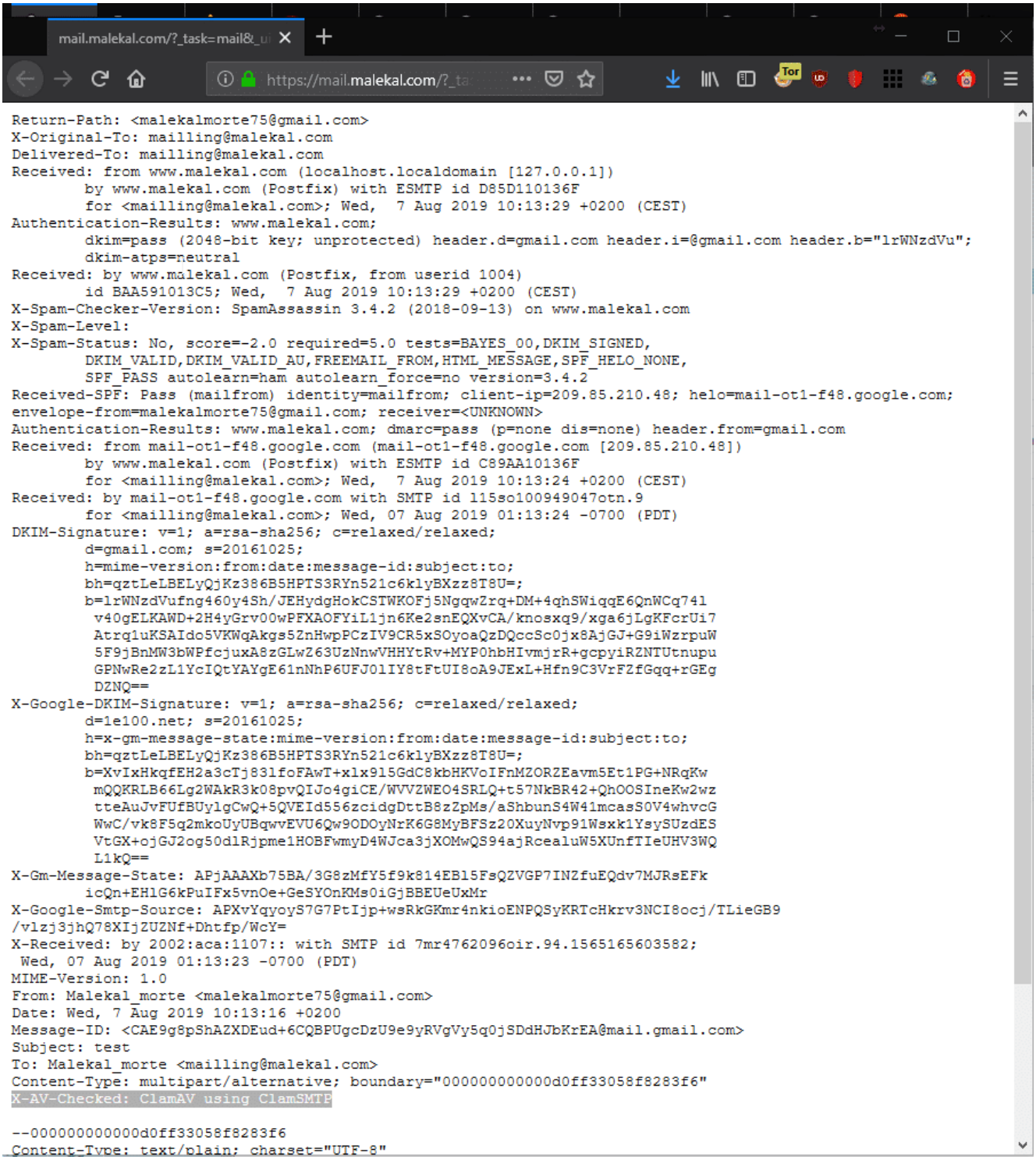
```
systemctl restart  postfix
```

Il ne vous reste plus qu’à tester l’envoi de mail et vérifier les mail.log.
Lorsque le mail est sain, clamstpd retourne un status CLEAN.

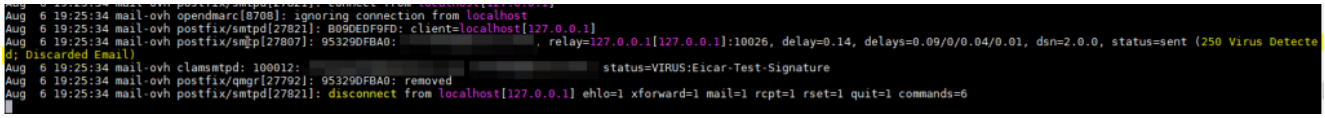
```
Aug       7    10:13:30    www    clamsmtpd:    100000:
from=malekalmorte75@gmail.com,    to=mailling@malekal.com,
status=CLEAN
 Aug   7 10:13:30 www postfix/smtp[24189]: BAA591013C5:
to=mailling@malekal.com,   relay=127.0.0.1[127.0.0.1]:10026,
delay=0.24, delays=0.05/0.01/0.06/0.12, dsn=2.0.0, status=sent
(250 2.0.0 Ok: queued as D85D110136F)
```



De plus, une ligne X-AV-Checked est ajouté dans le header du mail.



Enfin un test eicar montre bien que le mail est rejeté.



Liens

- [Installer et configurer spamassassin avec postfix sur Debian]