



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.



www.malekal.com

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 trafic 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
```

```

root@www:~# apt -y install clamav-daemon clamsmtp clamav
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés:
 clamav-base clamav-freshclam clamdscan libclamav9 libmspack0 libtftml
Paquets suggérés:
 clamav-docs daemon libclamunrar9
Les NOUVEAUX paquets suivants seront installés:
 clamav clamav-base clamav-daemon clamav-freshclam clamdscan clamsmtp libclamav9 libmspack0 libtftml
0 mis à jour, 9 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 1805 ko dans les archives.
Après cette opération, 5165 ko d'espace disque supplémentaires seront utilisés.
Réception de:1 http://debian.mirrors.ovh.net/debian buster/main amd64 clamav-base all 0.101.2+dfsg-1 [113 kB]
Réception de:2 http://debian.mirrors.ovh.net/debian buster/main amd64 libmspack0 amd64 0.10.1-1 [49,9 kB]
Réception de:3 http://debian.mirrors.ovh.net/debian buster/main amd64 libtftml amd64 0.13-4 [60,5 kB]
Réception de:4 http://debian.mirrors.ovh.net/debian buster/main amd64 libclamav9 amd64 0.101.2+dfsg-1 [770 kB]
Réception de:5 http://debian.mirrors.ovh.net/debian buster/main amd64 clamav-freshclam amd64 0.101.2+dfsg-1 [209 kB]
Réception de:6 http://debian.mirrors.ovh.net/debian buster/main amd64 clamav amd64 0.101.2+dfsg-1 [169 kB]
Réception de:7 http://debian.mirrors.ovh.net/debian buster/main amd64 clamav-daemon amd64 0.101.2+dfsg-1 [251 kB]
Réception de:8 http://debian.mirrors.ovh.net/debian buster/main amd64 clamdscan amd64 0.101.2+dfsg-1 [129 kB]
Réception de:9 http://debian.mirrors.ovh.net/debian buster/main amd64 clamsmtp amd64 1.10-17 [53,8 kB]
1805 ko réceptionnés en 0s (6450 ko/s)
Préconfiguration des paquets...
Sélection du paquet clamav-base précédemment désélectionné.
(Lecture de la base de données... 72880 fichiers et répertoires déjà installés.)
Préparation du paquetage de ../0-clamav-base_0.101.2+dfsg-1_all.deb ...
Dépaquetage de clamav-base (0.101.2+dfsg-1) ...
Sélection du paquet libmspack0:amd64 précédemment désélectionné.
Préparation du paquetage de ../1-libmspack0_0.10.1-1_amd64.deb ...
Dépaquetage de libmspack0:amd64 (0.10.1-1) ...
Sélection du paquet libtftml:amd64 précédemment désélectionné.
Préparation du paquetage de ../2-libtftml_0.13-4_amd64.deb ...
Dépaquetage de libtftml:amd64 (0.13-4) ...
Sélection du paquet libclamav9:amd64 précédemment désélectionné.
Préparation du paquetage de ../3-libclamav9_0.101.2+dfsg-1_amd64.deb ...
Dépaquetage de libclamav9:amd64 (0.101.2+dfsg-1) ...
Sélection du paquet clamav-freshclam précédemment désélectionné.
Préparation du paquetage de ../4-clamav-freshclam_0.101.2+dfsg-1_amd64.deb ...
Dépaquetage de clamav-freshclam (0.101.2+dfsg-1) ...
Sélection du paquet clamav précédemment désélectionné.
Préparation du paquetage de ../5-clamav_0.101.2+dfsg-1_amd64.deb ...
Dépaquetage de clamav (0.101.2+dfsg-1) ...
Sélection du paquet clamav-daemon précédemment désélectionné.
Préparation du paquetage de ../6-clamav-daemon_0.101.2+dfsg-1_amd64.deb ...
Dépaquetage de clamav-daemon (0.101.2+dfsg-1) ...
Sélection du paquet clamdscan précédemment désélectionné.
Préparation du paquetage de ../7-clamdscan_0.101.2+dfsg-1_amd64.deb ...
Dépaquetage de clamdscan (0.101.2+dfsg-1) ...
Sélection du paquet clamsmtp précédemment désélectionné.
Préparation du paquetage de ../8-clamsmtp_1.10-17_amd64.deb ...
Dépaquetage de clamsmtp (1.10-17) ...
Paramétrage de libmspack0:amd64 (0.10.1-1) ...
Paramétrage de libtftml:amd64 (0.13-4) ...
Paramétrage de libclamav9:amd64 (0.101.2+dfsg-1) ...
Paramétrage de clamav-base (0.101.2+dfsg-1) ...
id: clamav: utilisateur inexistant
Paramétrage de clamav-freshclam (0.101.2+dfsg-1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service -> /lib/systemd/system/clamav-freshclam.service.
inserv: script noderige: service noderig already provided!
Paramétrage de clamdscan (0.101.2+dfsg-1) ...

```

Ensuite on édite le fichier /etc/clamsmtpd.conf

Décommentez la ligne Header et changer l'utilisateur pour clamav.

```

# -----
#                               SAMPLE CLAMSMTPD CONFIG FILE
# -----
#
# - Comments are a line that starts with a #
# - All the options are found below with their defaults commented out

# The address to send scanned mail to.
# This option is required unless TransparentProxy is enabled
OutAddress: 10025

# The maximum number of connection allowed at once.
# Be sure that clamd can also handle this many connections
#MaxConnections: 64

# Amount of time (in seconds) to wait on network IO
#TimeOut: 180

# Address to listen on (defaults to all local addresses on port 10025)
Listen: 127.0.0.1:10026

# The address clamd is listening on
ClamAddress: /var/run/clamav/clamdctl

# A header to add to all scanned email
Header: X-AV-Checked: ClamAV using ClamSMTP

# Directory for temporary files
TempDirectory: /var/spool/clamsmtp

# PidFile: location of PID file
PidFile: /var/run/clamsmtp/clamsmtpd.pid

# Whether or not to bounce email (default is to silently drop)
#Bounce: off

# Whether or not to keep virus files
#Quarantine: off

# Enable transparent proxy support
#TransparentProxy: off

# User to run as
User: clamav

# Virus actions: There's an option to run a script every time a
# virus is found. Read the man page for clamsmtpd.conf for details.
~
~
~

```

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 -ltn|grep clam
```

```
root@www:~# netstat -ltn|grep clam
tcp        0      0 127.0.0.1:10026      0.0.0.0:*           LISTEN      21237/clamsmtpd
unix 2      [ ACC ]     STREAM  LISTENING   763376221 21248/clamd      /var/run/clamav/clamdctl
```

Le socket avec clamdctl 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, clamsmtpd 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)

```

```

Aug  7 10:13:29 www opendkim[32025]: D85D110136F: DKIM verification successful
Aug  7 10:13:29 www opendkim[32025]: D85D110136F: s=20161025_d@gmail.com SSL
Aug  7 10:13:30 www postfix/qmgr[23963]: D85D110136F: from=malekalmorte75@gmail.com, size=3620, nrcpt=1 (queue active)
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)
Aug  7 10:13:30 www postfix/qmgr[23963]: BAA591013C5: removed
Aug  7 10:13:30 www postfix/smtpd[24191]: disconnect from localhost.localdomain[127.0.0.1] ehlo=1 xforward=1 mail=1 rcpt=1 data=1 quit=1 commands=6
Aug  7 10:13:30 www postfix/local[24196]: D85D110136F: to=malekalmorte@malekal.com, orig_to=mailling@malekal.com, relay=local, delay=0.16, delays=0.12/0.03/0/0.02, dsn=2.0.0, status=sent (delivered to command: /usr/bin/procmail -Y -a $DOMAIN)

```

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

```
mail.malekal.com/?_task=mail&_ui X +
https://mail.malekal.com/?_ta
Return-Path: <malekalmorte75@gmail.com>
X-Original-To: mailling@malekal.com
Delivered-To: mailling@malekal.com
Received: from www.malekal.com (localhost.localdomain [127.0.0.1])
  by www.malekal.com (Postfix) with ESMTPE id D85D110136F
  for <mailling@malekal.com>; Wed, 7 Aug 2019 10:13:29 +0200 (CEST)
Authentication-Results: www.malekal.com;
  dkim=pass (2048-bit key; unprotected) header.d=gmail.com header.i=@gmail.com header.b="lrWNzdVu";
  dkim-atps=neutral
Received: by www.malekal.com (Postfix, from userid 1004)
  id BAA591013CS; Wed, 7 Aug 2019 10:13:29 +0200 (CEST)
X-Spam-Checker-Version: SpamAssassin 3.4.2 (2018-09-13) on www.malekal.com
X-Spam-Level:
X-Spam-Status: No, score=-2.0 required=5.0 tests=BAYES_00,DKIM_SIGNED,
  DKIM_VALID,DKIM_VALID_AU,FREEMAIL_FROM,HTML_MESSAGE,SPF_HELO_NONE,
  SPF_PASS autolearn=ham autolearn_force=no version=3.4.2
Received-SPF: Pass (mailfrom) identity=mailfrom; client-ip=209.85.210.48; helo=mail-otl-f48.google.com;
  envelope-from=malekalmorte75@gmail.com; receiver=<UNKNOWN>
Authentication-Results: www.malekal.com; dmarc=pass (p=none dis=none) header.from=gmail.com
Received: from mail-otl-f48.google.com (mail-otl-f48.google.com [209.85.210.48])
  by www.malekal.com (Postfix) with ESMTPE id C89AA10136F
  for <mailling@malekal.com>; Wed, 7 Aug 2019 10:13:24 +0200 (CEST)
Received: by mail-otl-f48.google.com with SMTP id l15sol00949047otn.9
  for <mailling@malekal.com>; Wed, 07 Aug 2019 01:13:24 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=gmail.com; s=20161025;
  h=mime-version:from:date:message-id:subject:to;
  bh=qztLeLBELyQjKz386B5HPTS3RYn521c6klyBXzz8T8U=;
  b=lrWNzdVufng460y4Sh/JEHYdgHokCSTWKFj5NgqwZrq+DM+4qhSWiqqE6QnWCq741
  v40gELKAWD+2H4yGv00wPFXAOFYiL1jn6Ke2snEQXvCA/knosxq9/xga6jLgKFcrUi7
  AtrqluKSAIdo5VKWqAkgs5ZnHwpPCzIV9CR5xS0yocQzDQccSc0jx8AjGJ+G9iWzrpuW
  5F9jBnMW3bWPFcjuxA8zGLwZ63UzNnwVHHYtRv+MYP0hbHlvmjrR+gcpyiR2NTUtnupu
  GPNwRe2zL1YcIQtYAYgE61nNhP6UFJ01IY8tFtUI8oA9JEXL+Hfn9C3VrFzFgGq+rGEG
  DZNQ==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=1e100.net; s=20161025;
  h=x-gm-message-state:mime-version:from:date:message-id:subject:to;
  bh=qztLeLBELyQjKz386B5HPTS3RYn521c6klyBXzz8T8U=;
  b=XvIxHkqfEH2a3ctj7831foFAwT+xlx915GdC8kbHKVoIFnMZORZEavm5Et1PG+NRqKw
  mQQKRLB66Lg2WakR3k08pvQIJo4giCE/WVVZWE04SRLQ+ts7NkBR42+QhOOSIneKw2wz
  tteAuJvFUFBUylgCwQ+5QVEId556zcidgDttB8zZpMs/aShbunS4W41mcasS0V4whvcG
  WwC/vk8F5q2mkoUyUBqvwEVU6Qw9OD0yNrk6G8MyBFSz20XuyNvp91Wsxk1YsySUzDES
  VtGX+ojGJ2og50dlRjpm1HOBfwmyD4WJca3jXOMwQs94ajRcealuW5XUnFTIeUHV3WQ
  LlkQ==
X-Gm-Message-State: APjAAAXb75BA/3G8zmfY5f9k814EB15FsQZVGP7INZfuEQdv7MJRsEFk
  icQn+EH1G6kPuIFx5vnOe+GeSYOnKM0iGjBBEUeUxMr
X-Google-Smtp-Source: APXvYqyoyS7G7PtIjp+wsRkGKmr4nkioENPQSyKRTcHkrv3NCI8ocj/TLieGB9
  /vlzj3jhQ78XIjZUZNF+Dhtfp/WcY=
X-Received: by 2002:aca:1107:: with SMTP id 7mr4762096oir.94.1565165603582;
  Wed, 07 Aug 2019 01:13:23 -0700 (PDT)
MIME-Version: 1.0
From: Malekal_morte <malekalmorte75@gmail.com>
Date: Wed, 7 Aug 2019 10:13:16 +0200
Message-ID: <CAE9g8pShAZXDDEud+6CQBPUgcDzU9e9yRVgVy5q0jSDdHJbKrEA@mail.gmail.com>
Subject: test
To: Malekal_morte <mailling@malekal.com>
Content-Type: multipart/alternative; boundary="000000000000d0ff33058f8283f6"
X-AV-Checked: ClamAV using ClamSMTP

--000000000000d0ff33058f8283f6
Content-Type: text/plain; charset="UTF-8"
```

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

```
Aug 6 19:25:34 mail-ovh opendmarc[8788]: ignoring connection from localhost
Aug 6 19:25:34 mail-ovh postfix/smtpd[27821]: B090EDF9FD: client=localhost[127.0.0.1]
Aug 6 19:25:34 mail-ovh postfix/smtp[27807]: 953290FBA0: relay=127.0.0.1[127.0.0.1]:10026, delay=0.14, delays=0.09/0/0.04/0.01, dsn=2.0.0, status=sent (250 Virus Detecte
d; Discarded Email)
Aug 6 19:25:34 mail-ovh clamsmtpd: 100012: status=VIRUS:Eicar-Test-Signature
Aug 6 19:25:34 mail-ovh postfix/qmgr[27792]: 953290FBA0: removed
Aug 6 19:25:34 mail-ovh postfix/smtpd[27821]: disconnect from localhost[127.0.0.1] ehlo=1 xforward=1 mail=1 rcpt=1 rset=1 quit=1 commands=6
```

Liens

- [Installer et configurer spamassassin avec postfix sur Debian](#)