



Association Lyonnaise
pour le Développement
de l'Informatique Libre



Héberger ses mails

Sébastien Dufromental, Clément Février
ALDIL, Conférence « jeudi du libre »

4 avril 2013



Intervenants

Clément Février

- Doctorant en physique
- Président d'Ubuntu-Lyon et membre de l'ALDIL
- Serveur : tour, sous Ubuntu (desktop).

Sébastien « Elzen » Dufromental

- Doctorant en informatique ; ancien prof d'école
- Fondateur du collectif « Internet : Réseau Libre Non-Centré »
- Serveur : portable, sous Debian.

Pourquoi l'auto-hébergement ?

- Usagers d'*Internet*
- Militants du Logiciel Libre
- Plus pratique, tout simplement

Référence : Benjamin Bayart, « Internet Libre ou Minitel 2.0 »
(→ <http://www.fdn.fr/>)

Voir aussi sur <http://fadrienn.irlnc.org>



Pourquoi héberger ses mails ?

- Tout le monde utilise les mails
- Que feriez-vous avec votre courrier papier ?



Plan

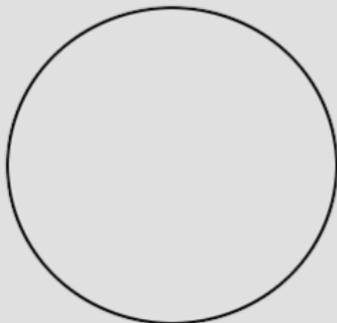
- 1 Introduction
- 2 Principes généraux
- 3 Mise en place
- 4 Administration
- 5 Conclusion

Principes généraux

Légende pour les schémas suivants

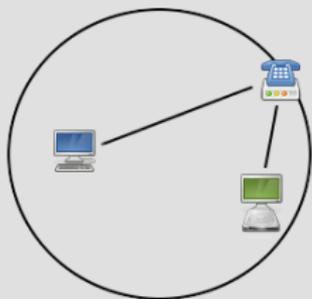


vosre ordinateur, vosre serveur, vosre routeur, vos destinataires, un spammeur



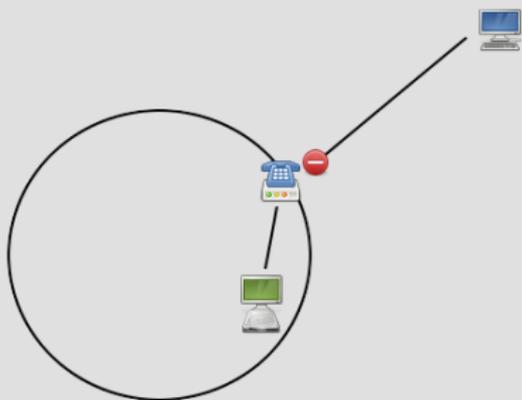
vosre réseau local

Récupération des mails (IMAP)



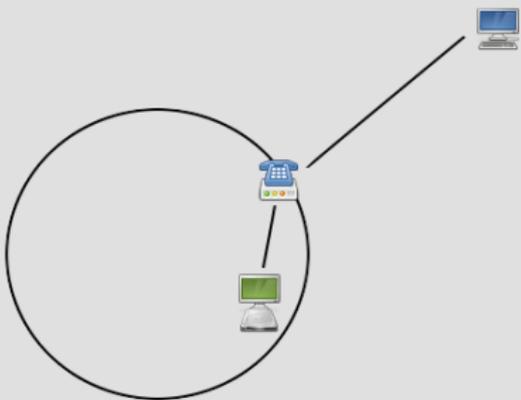
- Échange IMAP interne
- Authentification [OK]

Récupération des mails (IMAP)



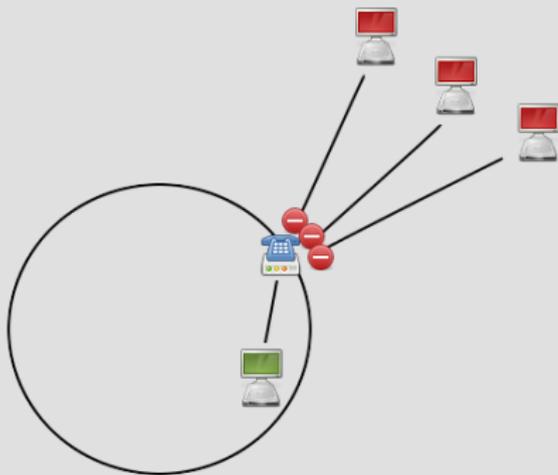
- Échange IMAP externe
- Pas de redirection [KO]

Récupération des mails (IMAP)



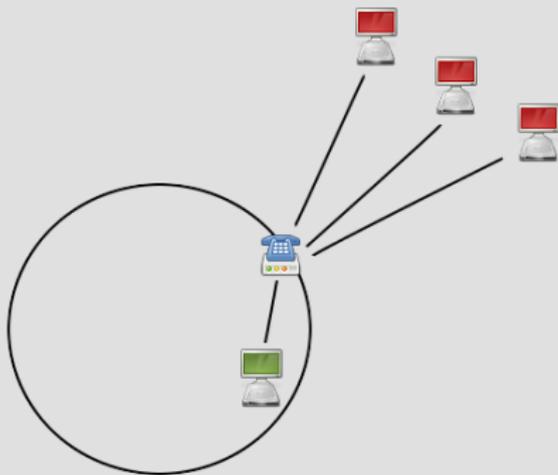
- Échange IMAP externe
- Redirection [OK]
 - port 143 (en clair)
 - port 993 (chiffré)
- Authentification [OK]

Communication entre serveurs (SMTP)



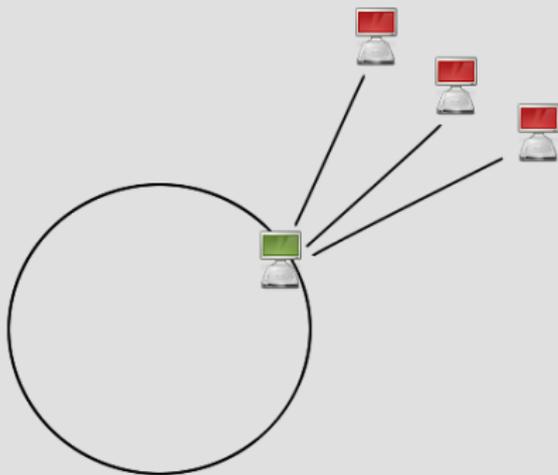
- Échange SMTP externe
- Pas de redirection [KO]

Communication entre serveurs (SMTP)



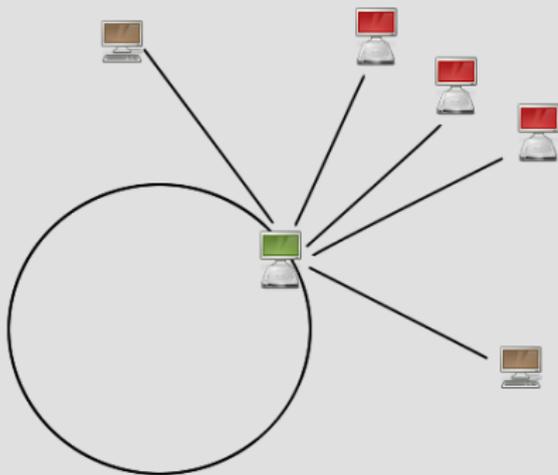
- Échange SMTP externe
- Redirection [OK]
 - port 25 (en clair)
 - port 465 (chiffré)

Communication entre serveurs (SMTP)



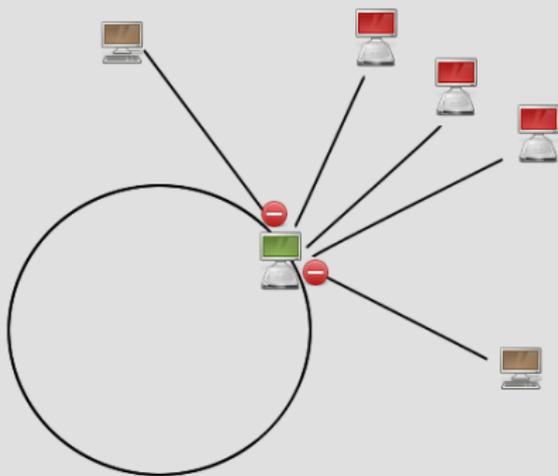
- Échange SMTP externe
- Redirection [OK]
 - port 25 (en clair)
 - port 465 (chiffré)

Envoi de mails (SMTP)



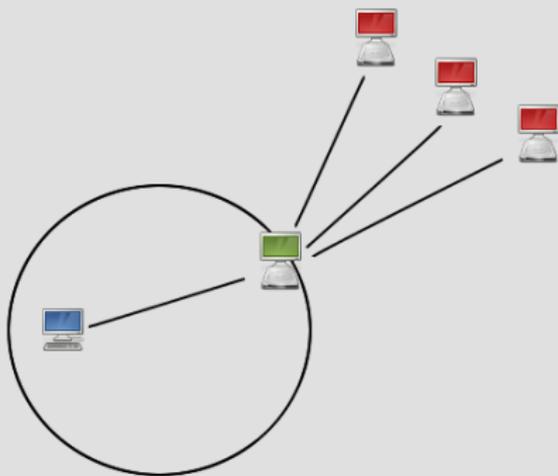
- Échange SMTP externe
- Accès ouvert [KO]

Envoi de mails (SMTP)



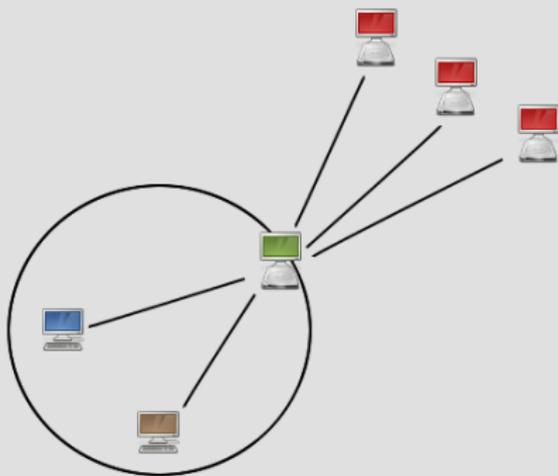
- Échange SMTP externe
- Accès restreint [OK]

Envoi de mails (SMTP)



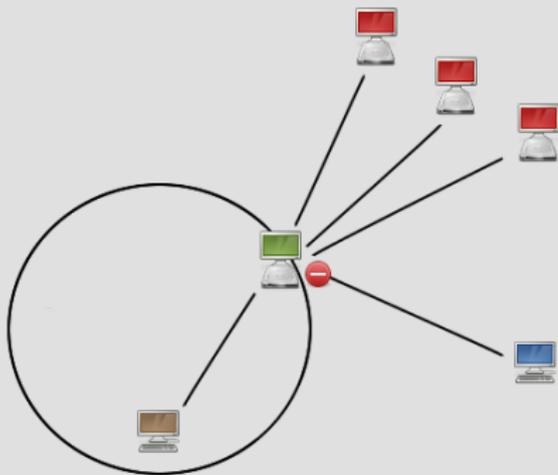
- Échange SMTP interne
- Accès ouvert [OK]

Envoi de mails (SMTP)



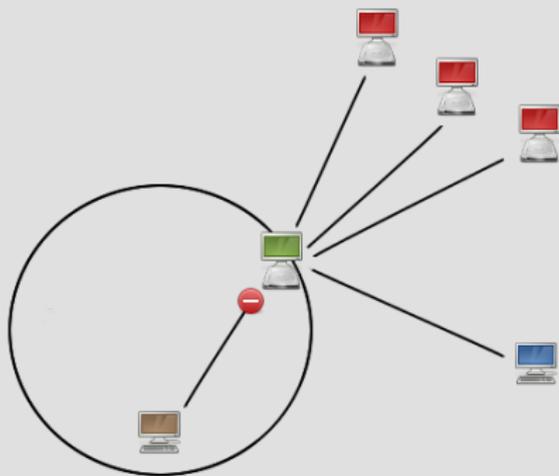
- Échange SMTP interne
- Accès ouvert **[KO]**

Envoi de mails (SMTP)



- Échange SMTP externe
- Accès restreint [KO]

Envoi de mails (SMTP)



- Échange SMTP externe
- Authentification [OK]

Chiffrement des messages réseau



Note : les enveloppes représentent les messages réseaux qui *contiennent* le mail.

- Échanges chiffrés avec le serveur (TLS)...
- ... mais échanges en clair entre serveurs !

⇒ pensez à chiffrer les mails confidentiels !

Chiffrement des mails eux-mêmes



- Système à clef publique/clef privée (RSA)
- Ce qui est chiffré par une clef ne peut être déchiffré que par l'autre
- Utilisé pour le chiffrement, mais aussi pour l'authentification
- Voir sur <http://www.yionel.fr/?p=680>
- Ne dépend pas du serveur ! Configurez votre client.

Mise en place

Matériel requis

- Assez peu de capacités requises
- Ordinateur de récupération, portable, mini-ordinateur. . .
- Un minimum d'espace disque (au moins quelques Gio. . .)
- Possibilité de tourner toute la journée



Conditions d'accès au réseau

- [REQUIS] Connexion permanente
- [REQUIS] Port 25 ouvert
- [CONSEILLÉ] IP fixe
- [CONSEILLÉ] Reverse DNS

⇒ Vérifiez votre FAI !

Conditions d'accès au réseau

- [REQUIS] Connexion permanente
- [REQUIS] Port 25 ouvert
- [CONSEILLÉ] IP fixe
- [CONSEILLÉ] Reverse DNS

⇒ Vérifiez votre FAI !



Installation du serveur



POSTFIX

« postfix, sasl2-bin »



« dovecot-imapd »

Sources du tutoriel :

<http://blog.rom1v.com/2009/08/hebergez-vos-mails-sur-ubuntu-server-et-liberez-vous/>

<http://blog.rom1v.com/2010/01/ajouter-lauthentification-smtp-sur-un-serveur-mail/>

(<http://fadrienn.irlnc.org/serveur/installation/mails/>)

Configuration de postfix

```
elzen@amateria: ~$ sudo dpkg-reconfigure postfix
```

Configuration de postfix

Outil de configuration des paquets

Postfix Configuration

Veillez choisir la configuration type de votre serveur de messagerie la plus adaptée à vos besoins.

Pas de configuration :

Devrait être choisi pour laisser la configuration actuelle inchangée.

Site Internet :

L'envoi et la réception s'effectuent directement en SMTP.

Site Internet avec un smarthost :

Les messages sont reçus directement en SMTP ou grâce à un utilitaire comme fetchmail. Les messages sortants sont envoyés en utilisant un smarthost.

Système satellite :

Tous les messages sont envoyés vers une autre machine, nommée un smarthost.

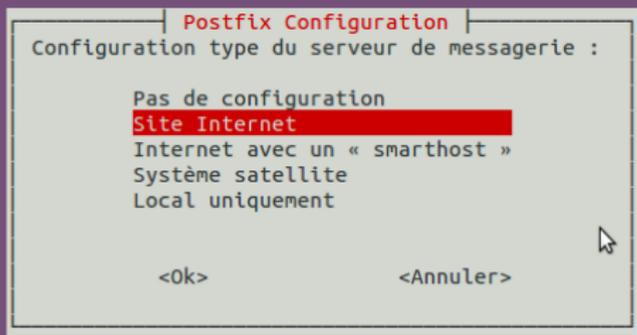
Local uniquement :

Le seul courrier géré est le courrier pour les utilisateurs locaux. Il n'y a pas de mise en réseau.

<Ok>

Configuration de postfix

Outil de configuration des paquets



Configuration de postfix

Outil de configuration des paquets

Postfix Configuration

Le « nom de courrier » est le nom employé pour qualifier toutes les adresses n'ayant pas de nom de domaine. Cela inclut les courriels de et vers l'adresse du superutilisateur (root). Il est donc conseillé de veiller à éviter d'envoyer des courriels en tant que « root@example.org ».

D'autres programmes se servent de ce nom ; il doit correspondre au domaine unique et complètement qualifié (FQDN) d'où le courrier semblera provenir.

Ainsi, si une adresse provenant de l'hôte local est foo@example.org, la valeur correcte pour cette option serait example.org.

Nom de courrier :

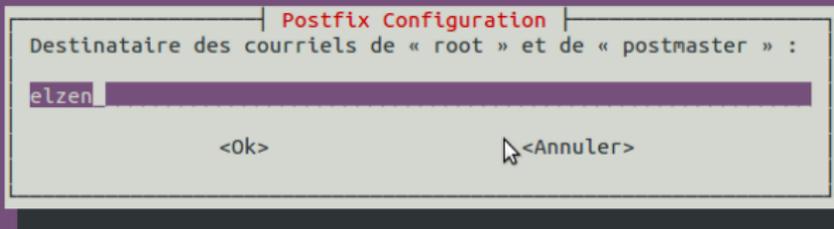
amateria.irln.org

<Ok>

<Annuler>

Configuration de postfix

Outil de configuration des paquets



Configuration de postfix

Outil de configuration des paquets

Postfix Configuration

Veillez indiquer une liste des domaines, séparés par des virgules, que cette machine reconnaîtra comme lui appartenant. Si la machine est un serveur de courriels, il est conseillé d'inclure le domaine de plus haut niveau.

Autres destinations pour lesquelles le courrier sera accepté (champ vide autorisé) :

amateria, localhost.localdomain, , localhost

<Ok>

<Annuler>

Configuration de postfix

Outil de configuration des paquets

Postfix Configuration

Lorsque les mises à jour synchronisées sont imposées, l'envoi des courriels se fait plus lentement. Dans le cas contraire, des courriels risquent d'être perdus si le système s'arrête inopinément et si vous n'utilisez pas un système de fichiers journalisé, comme ext3.

Faut-il forcer des mises à jour synchronisées de la file d'attente des courriels ?

<Oui>

<Non>

Configuration de postfix

Outil de configuration des paquets

Postfix Configuration

Veillez indiquer les réseaux pour lesquels cette machine relaie le courrier. Par défaut, seuls les courriels de l'hôte local sont acceptés, ce qui est demandé par certains lecteurs de courrier. Ce choix par défaut concerne à la fois l'IPv4 et l'IPv6. Si vous êtes connecté par une seule version du protocole IP, la valeur inutilisée peut être supprimée.

Si ce serveur est un « smarthost » pour un ensemble de machines, vous devez indiquer l'ensemble des réseaux, sinon le courrier sera rejeté plutôt qu'expédié.

Pour utiliser les valeurs par défaut de postfix (basées sur les sous-réseaux connectés), veuillez entrer une valeur vide.

Réseaux internes :

127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128

<ok>

<Annuler>

Configuration de postfix

Outil de configuration des paquets

Postfix Configuration

Veillez choisir la limite que Postfix mettra à la taille des boîtes aux lettres pour empêcher les erreurs de logiciels incontrôlables. Une valeur nulle signifie aucune limite. Les créateurs du logiciel utilisent une valeur par défaut de 51200000.

Taille maximale des boîtes aux lettres (en octets) :

<Ok> <Annuler>

Configuration de postfix

Outil de configuration des paquets

Postfix Configuration

Veillez choisir le caractère définissant une extension d'adresse locale.

Pour ne pas utiliser d'extension pour les adresses locales, laissez le champ vide.

Caractère d'extension des adresses locales :

Configuration de postfix

Outil de configuration des paquets

```
Postfix Configuration
Par défaut, Postfix utilise tous les protocoles internet actifs sur le
système. Vous pouvez annuler ce comportement avec les valeurs suivantes :

tous : utilisation des adresses IPv4 et IPv6 ;
ipv6 : écoute uniquement les adresses IPv6 ;
ipv4 : écoute uniquement les adresses IPv4.

Protocoles internet à utiliser :

tous
ipv6
ipv4

<Ok>                                <Annuler>
```

Configuration de postfix

```
elzen@amateria: ~$ sudo dpkg-reconfigure postfix
* Stopping Postfix Mail Transport Agent postfix [ OK ]
setting synchronous mail queue updates: false
setting myorigin
setting destinations: amateria, localhost.localdomain, , localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix is now set up with the changes above.  If you need to make changes, edit
/etc/postfix/main.cf (and others) as needed.  To view Postfix configuration
values, see postconf(1).

After modifying main.cf, be sure to run '/etc/init.d/postfix reload'.

Running newaliases
* Stopping Postfix Mail Transport Agent postfix [ OK ]
* Starting Postfix Mail Transport Agent postfix [ OK ]
elzen@amateria: ~$ sudo vim /etc/postfix/main.cf
```

Configuration de postfix

```
19
20 # TLS parameters
21 smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
22 smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
23 smtpd_use_tls=yes
24 smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
25 smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
26
27 # See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
28 # information on enabling SSL in the smtp client.
29
30 myhostname = amateria
31 alias_maps = hash:/etc/aliases
32 alias_database = hash:/etc/aliases
33 mydestination = amateria, localhost.localdomain, , localhost
34 relayhost =
35 mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
36 mailbox_size_limit = 0
37 recipient_delimiter = +
38 inet_interfaces = all
39 myorigin = /etc/mailname
40 inet_protocols = all
41
42 home_mailbox = Maildir/
-- INSERTION --
```

42,24

Bas

Configuration de postfix

```
elzen@amateria: ~$ sudo service postfix reload
* Reloading Postfix configuration... [ OK ]
elzen@amateria: ~$ █
```

Configuration de dovecot

```
elzen@amateria: ~$ sudo vim /etc/dovecot/dovecot.conf
```

A terminal window with a black background and white text. The prompt is 'elzen@amateria: ~\$' followed by the command 'sudo vim /etc/dovecot/dovecot.conf'. A white cursor is positioned at the end of the command. A mouse cursor is visible on the right side of the terminal area.

Configuration de dovecot

```
77
78 dict {
79   #quota = mysql:/etc/dovecot/dovecot-dict-sql.conf.ext
80   #expire = sqlite:/etc/dovecot/dovecot-dict-sql.conf.ext
81 }
82
83 # Most of the actual configuration gets included below. The filenames are
84 # first sorted by their ASCII value and parsed in that order. The 00-prefixes
85 # in filenames are intended to make it easier to understand the ordering.
86 !include conf.d/*.conf
87
88 # A config file can also tried to be included without giving an error if
89 # it's not found:
90 !include_try local.conf
91
92 # Ajouts à partir d'ici ↓
93 protocols = imap
94 mail_location = maildir:~/Maildir
~
~
~
~
~
-- INSERTION --
```

94,34

Bas

Configuration de dovecot

```
elzen@amateria: ~$ sudo vim /etc/dovecot/dovecot.conf
elzen@amateria: ~$ sudo service dovecot restart
dovecot stop/waiting
dovecot start/running, process 2289
elzen@amateria: ~$ █
```

Configuration de SASL

```
elzen@amateria: ~$ # sudo apt-get install sasl2-bin
elzen@amateria: ~$ sudo adduser postfix sasl
Ajout de l'utilisateur « postfix » au groupe « sasl »...
Ajout de l'utilisateur postfix au groupe sasl
Fait.
elzen@amateria: ~$ sudo vim /etc/default/saslauthd █
```



Configuration de SASL

```
46 # WARNING: DO NOT SPECIFY THE -d OPTION.
47 # The -d option will cause saslauthd to run in the foreground instead of as
48 # a daemon. This will PREVENT YOUR SYSTEM FROM BOOTING PROPERLY. If you wish
49 # to run saslauthd in debug mode, please run it by hand to be safe.
50 #
51 # See /usr/share/doc/sasl2-bin/README.Debian for Debian-specific information.
52 # See the saslauthd man page and the output of 'saslauthd -h' for general
53 # information about these options.
54 #
55 # Example for chroot Postfix users: "-c -m /var/spool/postfix/var/run/saslauthd"
56 # Example for non-chroot Postfix users: "-c -m /var/run/saslauthd"
57 #
58 # To know if your Postfix is running chroot, check /etc/postfix/master.cf.
59 # If it has the line "smtp inet n - y - - smtpd" or "smtp inet n - - - smtpd"
60 # then your Postfix is running in a chroot.
61 # If it has the line "smtp inet n - n - - smtpd" then your Postfix is NOT
62 # running in a chroot.
63 # OPTIONS="-c -m /var/run/saslauthd"
64 OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"
```

-- INSERTION --

64,53

Bas

Configuration de SASL

```
1 #
2 # Settings for saslauthd daemon
3 # Please read /usr/share/doc/sasl2-bin/README.Debian for details.
4 #
5
6 # Should saslauthd run automatically on startup? (default: no)
7 # START=no
8 START=yes
9
10 # Description of this saslauthd instance. Recommended.
11 # (suggestion: SASL Authentication Daemon)
12 DESC="SASL Authentication Daemon"
13
14 # Short name of this saslauthd instance. Strongly recommended.
15 # (suggestion: saslauthd)
16 NAME="saslauthd"
17
18 # Which authentication mechanisms should saslauthd use? (default: pam)
19 #
20 # Available options in this Debian package:
21 # getpwent -- use the getpwent() library function
22 # kerberos5 -- use Kerberos 5
23 # pam      -- use PAM
24 # rimap    -- use a remote IMAP server
"/etc/default/saslauthd" 63L, 2326C écrit(s)      8,9      Haut
```

Configuration de SASL

```
elzen@amateria: ~$ sudo service saslauthd start
* Starting SASL Authentication Daemon saslauthd [ OK ]
elzen@amateria: ~$ sudo vim /etc/postfix/main.cf
```


Configuration de SASL

```
elzen@amateria: ~$ sudo service saslauthd start
* Starting SASL Authentication Daemon saslauthd [ OK ]
elzen@amateria: ~$ sudo vim /etc/postfix/main.cf
elzen@amateria: ~$ sudo vim /etc/postfix/sasl/smtpd.conf
```


Configuration de SASL

```
elzen@amateria: ~$ sudo service saslauthd start
* Starting SASL Authentication Daemon saslauthd [ OK ]
elzen@amateria: ~$ sudo vim /etc/postfix/main.cf
elzen@amateria: ~$ sudo vim /etc/postfix/sasl/smtpd.conf
elzen@amateria: ~$ sudo service postfix reload
* Reloading Postfix configuration... [ OK ]
elzen@amateria: ~$ █
```

Administration

Gestion des redirections

- Fichier `/etc/aliases`

```
1 # /etc/aliases
2 mailer-daemon: postmaster
3 postmaster: root
4 nobody: root
5 hostmaster: root
6 usenet: root
7 news: root
8 webmaster: root
9 www: root
10 ftp: root
11 abuse: root
12 noc: root
13 security: root
14 lighttpd: root
15 www-data: root
16 jabber: root
17 xmpp: root
18 root: elzen
19 quest: elzen
```

- Fichier `$HOME/.forward`

Lire les logs

Répertoire de base pour les logs : `/var/log`

```
elzen@fadienn: ~$ ls -lh /var/log/mail.log
-rw-r----- 1 root adm 400K avril  4 00:30 /var/log/mail.log
elzen@fadienn: ~$
```

- lisible par le root
- modifié en temps réel
- fichiers d'archives (`mail.log.1`, `mail.log.2.gz`, ...)

Lire les logs

Répertoire de base pour les logs : /var/log

```
elzen@fadienn: ~$ ls -lh /var/log/mail.log
-rw-r----- 1 root adm 400K avril  4 00:30 /var/log/mail.log
elzen@fadienn: ~$
```

Affichage du contenu :

```
elzen@fadienn: ~$ sudo tail -f /var/log/mail.log
Apr  4 00:27:24 fadienn postfix/smtpd[31672]: 4F61C320076: client=lns-5-49-61-3.dsl.
dyn.abo.bbox.fr[5.49.61.3]
Apr  4 00:27:24 fadienn postfix/cleanup[31677]: 4F61C320076: message-id=<515CACA9.70
00201@forumanalogue.fr>
```

Lire les logs

```
Apr  4 00:30:46 fadrienn postfix/anvil[31674]: statistics: max connection rate 1/60s  
for (smtp:5.49.61.3) at Apr  4 00:27:18  
Apr  4 00:30:46 fadrienn postfix/anvil[31674]: statistics: max connection count 1 for  
(smtp:5.49.61.3) at Apr  4 00:27:18  
Apr  4 00:30:46 fadrienn postfix/anvil[31674]: statistics: max cache size 1 at Apr  4  
00:27:18
```

- Statistiques **[OK]**
- Rien de particulier à dire...

Lire les logs

```
Apr  4 01:11:53 fadrienn dovecot: imap-login: Login: user=<[REDACTED]>, method=PLAIN, rip=81.220.210.50, lip=192.168.0.7, mpid=32068, TLS, session=<CNHB+nzZawBR3NIy>  
Apr  4 01:11:58 fadrienn dovecot: imap([REDACTED]): Disconnected: Logged out in=261 out=41432
```

- Connexion par un client mail **[OK]**
- Contientra plus de lignes en cas d'action/de message

Lire les logs

```
Mar 31 21:10:47 fadrienn postfix/smtpd[399]: connect from [redacted] [94.23.53.151]
Mar 31 21:10:48 fadrienn postfix/smtpd[399]: 0E7E8320076: client=tdct.org[94.23.53.151]
Mar 31 21:10:48 fadrienn postfix/cleanup[403]: 0E7E8320076: message-id=<51588A2E.20908@tdct.org>
Mar 31 21:10:48 fadrienn postfix/qmgr[30332]: 0E7E8320076: from=<[redacted]>, size=15765, nrcpt=1 (queue active)
Mar 31 21:10:48 fadrienn postfix/smtpd[399]: disconnect from tdct.org[94.23.53.151]
Mar 31 21:10:48 fadrienn postfix/local[404]: 0E7E8320076: to=<[redacted]@fadrienn.irlnc.org>, relay=local, delay=0.26, delays=0.19/0.01/0/0.06, dsn=2.0.0, status=sent (delivered to maildir)
Mar 31 21:10:48 fadrienn postfix/qmgr[30332]: 0E7E8320076: removed
```

- Réception de mail **[OK]**
- Adresse d'expéditeur, de destinataire
- Pris en charge et délivré

Lire les logs

```
Mar 27 21:35:31 fadrienn postfix/smtp[881]: connect to gmail-smtp-in.l.google.com[2a00:1450:400c:c00::1a]:25: Network is unreachable
Mar 27 21:35:32 fadrienn postfix/smtp[881]: DBB74320074: to=<[REDACTED]@gmail.com>, relay=gmail-smtp-in.l.google.com[173.194.67.27]:25, delay=1.5, delays=0.42/0.04/0.49/0.52, dsn=2.0.0, status=sent (250 2.0.0 OK 1364416532 i4si8861054wjb.63 - gsmt)
Mar 27 21:35:32 fadrienn postfix/qmgr[30332]: DBB74320074: removed
Mar 27 21:37:27 fadrienn dovecot: imap(seth): Disconnected: Logged out in=456 out=63486
```

- Envoi de mail [OK]
- Adresse de destinataire, pas d'expéditeur
- Accepté par le serveur distant

Lire les logs

```
Mar 25 20:57:31 fadrienn postfix/error[8767]: C467832108B: to=<[REDACTED]@marinecorps.com>, relay=none, delay=437385, delays=437342/41/0/1.3, dsn=4.4.1, status=deferred (delivery temporarily suspended: connect to marinecorps.com[98.124.198.1]:25: Connection refused)
Mar 25 20:57:31 fadrienn postfix/error[8749]: CF894320FA5: to=<[REDACTED]@aol.com>, relay=none, delay=438772, delays=438730/42/0/0.17, dsn=4.0.0, status=deferred (delivery temporarily suspended: host mailin-01.mx.aol.com[205.188.159.42] refused to talk to me: 554- (RTR:BB) http://postmaster.info.aol.com/errors/554rtrbb.html 554 Connecting IP: 82.233.208.64)
```

- Message temporairement refusé [Oups...]
- Réponse du serveur distant

Lire les logs

```
Mar 26 11:13:09 fadrienn postfix/smtp[14009]: 49D0232019B: host relaysmtp.luiss.it[193.204.157.66] refused to talk to me: 550 5.7.1 Service unavailable; Client host [82.233.208.64] blocked using Trend Micro RBL+. Please see http://www.mail-abuse.com/cgi-bin/lookup?ip\_address=82.233.208.64; Mail from 82.233.208.64 blocked using Trend Micro Email Reputation database. Please see <http://www.mail-abuse.com/cgi-bin/lookup?82.233.208.64>
```

- Message refusé [KO]
- Réponse du serveur distant

Je spamme ! Que faire ?

⇒ Premier réflexe : couper le serveur !

```
elzen@fadienn: ~$ sudo service postfix stop
[ ok ] Stopping Postfix Mail Transport Agent: postfix.
elzen@fadienn: ~$ sudo postsuper -d ALL
elzen@fadienn: ~$
```

- Puis vider la queue (les mails en attente)
- Puis vérifier la configuration
- Ne pas hésiter à demander de l'aide

Lire les logs

```
Mar 27 10:58:26 fadrienn postfix/smtpd[28613]: connect from [REDACTED]  
fr[94.23.233.155]  
Mar 27 10:58:46 fadrienn postfix/smtpd[28613]: NOQUEUE: reject: RCPT from [REDACTED]  
[94.23.233.155]: 554 5.7.1 <[REDACTED]>: Relay access den  
ied; from=<[REDACTED]> to=<[REDACTED]@[REDACTED].fr> proto=SMTP helo=<[REDACTED]>  
>  
Mar 27 10:59:48 fadrienn postfix/smtpd[28613]: disconnect from [REDACTED]  
[94.23.233.155]
```

- Tentative d'envoi non-autorisé
- Pas passé : configuration correcte ?

Lire les logs

```
Mar 27 10:59:59 fadrienn postfix/smtpd[28613]: connect from [5.135.139.61]
Mar 27 10:59:59 fadrienn postfix/smtpd[28613]: E1450320074: client=[5.135.139.61], sasl_method=LOGIN, sasl_username=guest
Mar 27 11:00:01 fadrienn postfix/cleanup[28621]: E1450320074: message-id=<>
Mar 27 11:00:01 fadrienn postfix/qmgr[20646]: E1450320074: from=<>, size=23426, nrcpt=50 (queue active)
Mar 27 11:00:01 fadrienn postfix/smtpd[28613]: disconnect from [5.135.139.61]
```

- Connexion SASL authentifiée...
- Tiens, ne serait-ce pas la faille ?

Lire les logs

```
Mar 27 10:59:59 fadrienn postfix/smtpd[28613]: connect from [5.135.139.61]
Mar 27 10:59:59 fadrienn postfix/smtpd[28613]: E1450320074: client=[5.135.139.61], sasl_method=LOGIN, sasl_username=guest
Mar 27 11:00:01 fadrienn postfix/cleanup[28621]: E1450320074: message-id=<>
Mar 27 11:00:01 fadrienn postfix/qmgr[20646]: E1450320074: from=<>, size=23426, nrcpt=50 (queue active)
Mar 27 11:00:01 fadrienn postfix/smtpd[28613]: disconnect from [5.135.139.61]
```

- Connexion SASL authentifiée...
- Tiens, ne serait-ce pas la faille ?

⇒ Toujours vérifier les comptes accessibles !

Après un blacklistage. . .

Adresses fournies dans les messages d'erreurs envoyés :

SPAMHAUS

 THE SPAMHAUS PROJECT

Home

SBL

XBL

PBL

DBL

DROP

ROKSO

WHITELIST

Blocklist Removal Center
About Spamhaus | FAQs | News Blog

Blocklist Removal Center

IP Address Lookup

This Lookup tool is **only** for IP Addresses - do not enter domains or email addresses.

If you do not know what an IP address is, or what IP to look up, please contact your Internet Service Provider and ask them to help you.

IP Address Lookup Tool. This lookup tool checks to see if the **IP Address** you enter is currently listed in the live Spamhaus IP blocklists: **SBL, XBL and PBL**.

If your IP address is listed on one of our IP blocklists; SBL, XBL or PBL (collectively known as the "Zen" blocklist), this lookup tool will tell you which one and will give you a link to information on what to do.

Domain Lookup

This Lookup tool is **only** for Domains (not IP Addresses). The DBL only lists domains currently involved in spam, therefore it is extremely unlikely that normal domains will be on the DBL.

Domain Lookup Tool. This lookup tool checks to see if the **Domain** you enter is currently listed in the live Spamhaus Domain Blocklist (**DBL**).

If your Domain is listed on the Spamhaus Domain Blocklist (DBL), this Lookup tool will give you a link to information on what to do.

Associated Documents

- ▶ How Blocklists Work
- ▶ What is an "IP Address"?

On me spamme ! Que faire ?

Installer un antispam pour filtrer les messages reçus :

- amavis-news (le choix de clément)
- spamassassin (le choix de rom1v)

Pas encore essayé : je ne reçois pas (encore ?) de spam.

Pour aller plus loin...



Conclusion

- Un peu long, mais pas trop dur à mettre en place
- Besoins de base couverts assez facilement
- Attention à la sécurité (mais pas besoin d'être expert)
- À vous d'essayer !

