

Envoyer et recevoir du courrier pour un réseau multi-utilisateurs « masqueradisé »

Olivier Hoarau (olivier.hoarau@funix.org)

V3.3 du 26 décembre 2009

1	Historique du document.....	3
2	Préambule.....	4
3	Recevoir du courrier et configurer un serveur pop.....	4
3.1	Présentation de la configuration.....	4
3.2	Configuration de fetchmail.....	4
3.2.1	Méthode automatique.....	4
3.2.2	Méthode manuelle.....	5
3.3	Limiter la taille des mails récupérés et supprimer les mails sur le serveur.....	6
3.4	Configuration de procmail.....	6
3.5	Configuration du serveur pop.....	8
3.5.1	Pour une Mandriva.....	8
3.5.2	Pour une ubuntu.....	8
4	Sendmail.....	8
4.1	Présentation.....	8
4.2	Installation.....	9
4.2.1	Sous Mandriva.....	9
4.2.2	Sous ubuntu.....	9
4.3	Configuration.....	9
4.4	On relance tout.....	13
4.5	Principe de fonctionnement.....	13
4.6	Masquage de domaine.....	14
4.7	Si vous avez un autre email que celui attribué par le Fai utilisé.....	17
4.8	Attribution d'adresse dynamique.....	19
4.9	Si vous êtes inscrits à plusieurs FAI.....	22
4.10	Sendmail et timeout DNS.....	26
4.11	Sendmail et la lutte anti-spam.....	27
4.12	Sendmail et fichiers de log.....	27
4.13	Sécuriser Sendmail.....	27
4.13.1	Les commandes vrfy et expn.....	27
4.13.2	Modifier l'invite de sendmail.....	28
5	Lutte anti spam et anti virus.....	28
5.1	Présentation de la configuration.....	28
5.2	Filtrage basique.....	29
5.2.1	Filtrer avec procmail.....	29
5.2.2	Filtrer avec mailfilter.....	29
5.3	Filtrer les spams avec spamassassin.....	31
5.3.1	Présentation.....	31

5.3.2	Définitions.....	31
5.3.3	Installation de razor.....	32
5.3.4	Installation de SpamAssassin.....	33
5.3.5	Installation de DCC.....	33
5.3.6	Installation de pyzor.....	35
5.3.7	Configuration de spamassassin.....	35
5.3.8	Interfaçage avec sendmail.....	38
5.3.9	Lancement automatique.....	39
5.3.10	Fonctionnement.....	42
5.4	Mettre en place un anti virus.....	50
5.4.1	Présentation et installation.....	50
5.4.2	Configuration.....	51
5.4.3	Premiers tests.....	56
5.4.4	Lancement automatique.....	57
5.4.5	Interfaçage avec sendmail.....	61

1 Historique du document

- V3.3 26.12.09 passage à SpamAssassin 3.2.5 passage à DCC 1.3.116 et clamav 0.95.3
- V3.2 24.08.07 passage à SpamAssassin 3.2.3, razor 2.84, DCC 1.3.58 et ClamAV 0.91.1
- V3.1 08.03.07 passage à passage à mailfilter 0.8, SpamAssassin 3.1.8, dcc 1.3.53 et ClamAV 0.90.1
- V3.0 25.07.06 passage à SpamAssassin 3.1.8, razor 2.82, DCC 1.3.39, spamass milter 0.3.1 et clamav 0.88.3, adaptation pour installation sous (k)ubuntu, installation d'un serveur POP3 avec dovecot sous (k)ubuntu
- V2.9 29.01.06 passage à spamassassin 3.1.0, razor-agent-2.77 et ClamAntiVirus 0.88
- V2.81 10.08.05 correction d'une erreur pour le script d'apprentissage des spams pour sa-learn
- V2.8 06.08.05 sendmail, un mot sur l'installation avec les packages de la LE2005. passage à spamassassin 3.0.4, razor 2.75, DCC 1.3.12 et clamav 0.86.2
- V2.7 06.05.05 passage à SpamAssassin 3.0.3, DCC 1.34, SpamAssassin Milter 0.3.0 et Clam Anti Virus 0.84
- V2.6 07.01.05 passage à spamassassin 3.0.2, razor 2.67 et DCC 1.2.66, rajout de la configuration du fichier freshclam.conf pour clamav
- V2.5 06.11.04 passage à DCC 1.2.58, SpamAssassin 3.0.1 et Clamav 0.80, modification dans la configuration de clamav et dans l'appel de sa-learn.
- V2.4 02.10.04 passage à mailfilter 0.6.2, SpamAssassin 3.0.0, razor 2.61, DCC 1.2.54 et clamav 0.75.1, modifications dans la configuration de spamassassin (fichier de lancement, droits à fixer)
- V2.3 31.05.04 Passage à DCC 1.2.49 et clamav 0.71, un mot pour indiquer à spamassassin de classer ou non des mails comme spam
- V2.2 18.04.04 Passage à Razor 2.40, DCC 1.2.39 et clamav 0.70
- V2.1 27.03.04 Rajout d'un paragraphe sur la lutte anti virus et anti spam, changement de version des différents softs
- V2.0 04.05.03 Passage à Mandrake 9.1, légères modifications
- V1.9 24.12.02 Passage à Mandrake, changement de version de sendmail
- V1.8 07.07.02 Passage à mailfilter 0.4.0
- V1.7 09.06.02 Passage à Mandrake 8.2, modifs
- version de sendmail et package
- rajout de confCF_VERSION dans le fichier de config pour rajouter un commentaire dans l'entête de mail
- mise à jour de copier/coller d'entêtes de mail
- V1.6 16.12.01 - Passage à Mandrake 8.1, modifs version de sendmail et package
- Rajout de la partie réception du courrier
- V1.5 17.06.01 - Rajout de quelques notes et avertissements dans le chapitre [configuration de sendmail](#)
- Rajout d'un paragraphe sur la sécurisation de sendmail (commandes vfry et expn, modifier l'invite de sendmail).
- Passage à Mandrake 8.0, changement de numéro de version et du chemin du fichier de conf

V1.4 18.03.01 Rajout d'une remarque pour que les mails envoyés sur le réseau local ne partent pas d'abord chez le FAI.

V1.3 03.12.00 Passage à Mandrake 7.2, modifs :

- version sendmail
- fichiers logs sendmail (rajout d'un paragraphe)
- sendmail-cf sur le CD 2
- genericstable.db qui se trouve maintenant sous /etc/mail
- Modification du script ip-up qui reconfigure sendmail suivant leFAI utilisé pour prendre en compte le changement d'emplacement de genericstable.

2 Préambule

Ce document a pour but de présenter une configuration de **sendmail** sur un poste Linux connecté de façon intermittente ou permanente à internet et qui cache un réseau privé « masqueradisé ». Il a pour but de présenter également la manière de récupérer les mails et de filtrer les spams et les virus.

La dernière version de ce document est téléchargeable à l'URL <http://www.funix.org>.

Ce document est sous licence Creative Commons Attribution-ShareAlike 3.0 Unported, le détail de la licence se trouve sur le site <http://creativecommons.org/licenses/by-sa/3.0/legalcode>. Pour résumer, vous êtes libres

- de reproduire, distribuer et communiquer cette création au public
- de modifier cette création

suivant les conditions suivantes:

- **Paternité** — Vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'oeuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l'oeuvre).
- **Partage des Conditions Initiales à l'Identique** — Si vous transformez ou modifiez cette oeuvre pour en créer une nouvelle, vous devez la distribuer selon les termes du même contrat ou avec une licence similaire ou compatible.

Par ailleurs ce document ne peut pas être utilisé dans un but commercial sans le consentement de son auteur. Ce document vous est fourni "dans l'état" sans aucune garantie de toute sorte, l'auteur ne saurait être tenu responsable des quelconques misères qui pourraient vous arriver lors des manipulations décrites dans ce document.

3 Recevoir du courrier et configurer un serveur pop

3.1 Présentation de la configuration

Cette paragraphe a pour objet de vous présenter comment récupérer les mails des utilisateurs de votre réseau et les mettre à leur disposition. Le rôle des différents outils présentés dans cette page est le suivant:

- **fetchmail** permet de récupérer les mails des utilisateurs de votre réseau sur plusieurs serveurs **POP**
- **procmail** permet de faire le tri des mails et de dispatcher suivant le destinataire
- le serveur **POP** permet de rendre accessible aux lecteurs de mails de votre réseau les mails qui sont arrivés, que vos clients soient sous windows ou sous unix.

3.2 Configuration de fetchmail

3.2.1 Méthode automatique

Vous avez la possibilité de lui indiquer d'aller récupérer toutes les 10 minutes le courrier pendant une connexion. Pour cela on va le lancer à l'établissement de la connexion. Vous allez créer un script sous **/etc/ppp** avec pour nom **ip-up.local** qui contiendra les lignes suivantes:

```
#!/bin/bash
/usr/bin/fetchmail
```

Les droits doivent être à 755, faites un **chmod 755 ip-up.local** . Pour info, ce script est appelé à chaque début de connexion PPP.

NOTE Eventuellement rajouter l'appel à **fetchmail** à la fin de **ip-up** (voir page config PPP à la main sur le site www.funix.org).

ATTENTION les commandes lancés dans ce fichier doivent être indiquées avec leur chemin complet.

Maintenant root doit créer un fichier **.fetchmailrc** qui doit se trouver dans sa home directory avec les droits 600 (**chmod 600 ~/.fetchmailrc**). Ce fichier contient les lignes suivantes:

```
set daemon 600
set logfile /var/log/fetchmail.log
poll pop.fai.fr protocol pop3
user login-fai there with password password-fai is olivier here

poll pop.fnac.net protocol pop3
user login-fnac there with password password-fnac is olivier here

poll pop.free.fr protocol pop3
user login-free there with password password-free is olivier here

poll pop.ifrance.com protocol pop3
user login-ifrance there with password password-ifrance is olivier here

poll pop.fnac.net protocol pop3
user login2-fnac there with password password2-fnac is veronique here

poll pop.ifrance.com protocol pop3
user login2-ifrance there with password password2-ifrance is veronique here

poll pop.libertysurf.fr protocol pop3
user login-liberty there with password password-liberty is olivier here
```

Le paramètre 600 fixe la période de relevé de la boîte aux lettres, l'unité étant la seconde. Le fichier **fetchmail** sous **/var/log** est le fichier de log, **pop.fai.fr** est le nom du serveur pop de votre provider. **login-fai** est le nom de votre login chez votre provider, **password-fai** est le mot de passe chez le provider, olivier est le login de l'utilisateur local correspondant. Vous rajoutez autant de ligne poll et user que vous avez de compte pop à d'autre et à gauche, vous noterez qu'on peut en profiter pour relever les emails d'autres utilisateurs de votre réseau (dans l'exemple utilisateur du réseau privé veronique).

ATTENTION: les mots de passe sont marqués en clair (d'où les droits du fichier...).

Pour récupérer le courrier il suffira de lancer une connexion.

3.2.2 Méthode manuelle

Vous avez aussi la possibilité en tant que simple utilisateur de créer votre propre fichier **.fetchmailrc** (syntaxe idem plus haut) que vous placerez dans votre homedirectory et de lancer **fetchmail** d'un shell. Vous pouvez très bien aussi récupérer les mails des autres utilisateurs de votre réseau.

3.3 Limiter la taille des mails récupérés et supprimer les mails sur le serveur

NOTE Si vous voulez limiter la taille des fichiers récupérés à 100Ko par exemple, vous avez l'option:

```
fetchmail -l 100000
```

Ca va laisser tous les fichiers dont la taille est supérieure à 100Ko sur le serveur **pop** du fai, pour visualiser l'header et les supprimer.

```
telnet pop.fai.fr 110
Trying 195.154.205.225...
Connected to pop.fai.fr
Escape character is '^]'.
+OK POP3 mailhub.fai.fr v7.64 server ready
user login-pop
+OK User name accepted, password please
pass password-pop
+OK Mailbox open, 4 messages
list
+OK Mailbox scan listing follows
1 2199201
2 132664
3 388987
4 310757
```

Vous pouvez voir que vous avez 4 messages ainsi que leur taille. Pour visualiser l'header du message 1:

```
top 1 0
```

Vous pouvez visualiser le corps du message mais je ne le vous conseille pas, si c'est une image de 1Mo, ça va bloquer votre shell un certain temps. Je vous donne quand même la commande pour le message 1:

```
retr 1
```

Pour supprimer le message 1:

```
dele 1
```

Et enfin pour quitter:

```
quit
```

3.4 Configuration de procmail

Dans le cas où vous avez un compte pop unique avec plusieurs emails rattachés, **fetchmail** va tout mettre dans la boîte aux lettres de celui qui va lancer la commande **fetchmail**, pour effectuer un tri à la réception, vous devez penser à **procmail**.

Procmail permet de trier le courrier reçu par **fetchmail**. pour cela tout utilisateur avec son **.fetchmailrc** doit avoir un **.procmailrc** également dans sa home directory. Si je prends mon exemple, je disposais d'un compte pop unique chez mon provider fnac.net, mon adresse email était olivier.hoarau@fnac.net, mon compte local est olivier, celle de ma tendre et chère veronique.hoarau@fnac.net et compte local veronique. Si je veux expédier à Véronique tous les courriers dont les champs Destinataire (To) ou Copie (Cc) contiennent le champ veronique ou Véronique ou encore Veronique, voici la tête de mon **.procmailrc**

```
#olivier
:0 c
*^(To|Cc|Bcc):*(veronique|Veronique)
!veronique
```

Celui de ma femme aura cette tête là:

```
#veronique
:0 c
*^(To|Cc|Bcc):*(olivier|Olivier|funboard|Funboard)
!olivier
```

Je suis abonné à une liste funboard, c'est le nom de la liste qui apparaît dans la liste du destinataire ou du destinataire en copie, et non pas mon nom, d'où le critère de tri.

Le ! réexpédie localement le courrier vers le bon destinataire. Vous pouvez très bien aussi faire un fichier unique pour chaque utilisateur qui aura cette tête là:

```
#redirection vers veronique
:0 c
*^(To|Cc|Bcc):*(veronique|Veronique)
!veronique
```

```
#redirection vers olivier
:0 c
*^(To|Cc|Bcc):*(olivier|Olivier|funboard|Funboard)
!olivier
```

```
# les autres mails au destinataire non identifié vont vers olivier, vous pouvez très bien mettre /dev/null
(poubelle) à la place de !olivier
:0
*.*
!olivier
```

A noter que le petit c permet de pouvoir gérer les copies, en son absence si un mail arrive avec pour destinataire (To) Véronique et Olivier en copie (Cc), ce n'est que le premier dans la liste qui recevra le mail (en l'occurrence Véronique dans mon exemple de fichier), c permet qu'olivier reçoive aussi le courrier.

Le courrier échoue sous `/var/spool/mail` dans un fichier qui a pour nom le login de l'utilisateur.

Si vous disposez d'un email unique avec un seul email rattaché et que vous comptez vous en servir pour plusieurs personnes. Vous pouvez demander à vos interlocuteurs de préciser dans le sujet du mail le destinataire et faire un tri similaire à celui vu précédemment en filtrant sur le champ Subject du mail (`*^(Subject):*(veronique|Veronique)`).

Voilà un filtre intéressant trouvé à l'adresse suivante <http://www.linuxfocus.org/Francais/January2003/article279.shtml>. Il permet d'avertir automatiquement l'expéditeur qui vous a envoyé un fichier word.

```
# Promail script to
# reject word documents. Reject the mail, but do not reply to
# error messages "From MAILER-DAEMON"
# If you use ":0 Bc" instead of ":0 B" then you will still get the mail
:0 H
* !^From.*DAEMON
{
# The mime messages with word documents look like this in the body
# of the message:
#-----=_NextPart_000_000C_01C291BE.83569AE0
#Content-Type: application/msword;
# name="some file.doc"
#Content-Transfer-Encoding: base64
#Content-Disposition: attachment;
# filename="real file.doc"
:0 B
* ^Content-Type:.msword
| (formail -r ; cat /home/olivier/reject-text-msword ) | $SENDMAIL -t
}
```

```
# par défaut les autres mails sont envoyés à olivier
:0:
```

!olivier

Le fichier `/home/olivier/reject-text-mword` contient un texte décrivant les raisons pour lesquelles vous ne voulez pas recevoir de fichier word et préférez d'autres formats. A noter que ce script est adaptable pour des réponses automatiques en fonction de certains critères.

3.5 Configuration du serveur pop

3.5.1 Pour une Mandriva

Vous devez installer le package **dovecot**, il contient le serveur **imap** et **pop3**. Le fichier `/etc/dovecot.conf` doit contenir au minimum

```
protocols = pop3
disable_plaintext_auth = no
protocol pop3 {
    pop3_uidl_format = %08Xu%08Xv
}
```

Du coté poste client, configurer votre logiciel de mail favori pour que votre serveur Linux soit le serveur **POP** (il suffit de rajouter le nom du poste en question dans le champ qui va bien), et puis c'est tout, les courriers seront récupérés dans `/var/spool/mail` du serveur.

3.5.2 Pour une ubuntu

On va utiliser **dovecot**, pour l'installer il suffit de taper

```
sudo apt-get install dovecot-common dovecot-pop3d
```

on édite maintenant le fichier de configuration `/etc/dovecot/dovecot.conf` voilà les lignes à modifier

```
protocols = pop3
pop3_uidl_format = %08Xu%08Xv
default_mail_env = mbox:/var/spool/mail/%u
disable_plaintext_auth = no
```

Du coté poste client, configurer votre logiciel de mail favori pour que votre serveur Linux soit le serveur **POP** (il suffit de rajouter le nom du poste en question dans le champ qui va bien), et puis c'est tout, les courriers seront récupérés dans `/var/spool/mail` du serveur.

4 Sendmail

4.1 Présentation

Des outils comme **Netscape** disposent de leur propre mécanisme qui permette d'envoyer du courrier, pour faire plus "pro" on peut utiliser **sendmail** qui est l'outil de référence pour gérer l'expédition de courrier.

Pourquoi s'embêter à configurer **sendmail**, pour la gloire ? Certains disent que tant qu'on a pas cherché à configurer **sendmail**, on n'est pas un vrai administrateur système. Certain gestionnaire de courrier comme **Kmail**, en standard dans la bannière de KDE, fonctionne avec **sendmail**, or la configuration par défaut de ce dernier n'est pas correcte, si vous avez défini un nom de domaine farfelu pour votre machine, tous les courriers sortants vont partir avec au lieu d'utiliser le nom de domaine de votre fournisseur, vos emails seront, à coup sur, rejeter par la plupart des gestionnaires de courrier sur le net, et le peu de personne qui recevra vos emails, ne pourront y répondre car votre nom de domaine est totalement inconnu sur le net.

Une autre raison d'utiliser **sendmail** est dans le cas d'un petit réseau privé, avec plusieurs postes Windows (ou autres) et un serveur Linux, pour pouvoir partager une connexion internet, **sendmail** va faire office de serveur SMTP.

Pour configurer **sendmail** je ne peux que vous conseiller la lecture du [document d'Eric Jacoboni](http://www.linux-france.org/article/mail/sendmail/sendmail.html) que vous trouverez à l'URL <http://www.linux-france.org/article/mail/sendmail/sendmail.html> "lire et envoyer du courrier off-line sur sa machine". Il est vraiment très clair, et il y a vraiment pas grand chose à rajouter. Je m'en suis grandement inspiré pour configurer mon poste Linux avec cependant quelques différences de taille que je mentionnerai, je présente dans cette page uniquement les manips que j'ai faite pour configurer **sendmail**, pour des explications se reporter au document précédemment cité.

Pour résumer les différences avec la documentation de Jacoboni sont :

- le nom de domaine privé n'apparaît aucunement dans les mails sortants, ce qui n'est pas le cas avec la documentation d'Eric où apparaît le nom de domaine privé dans les champs **Received** et **Message-Id**,
- avec ma configuration le serveur linux peut relayer le courrier des postes du domaine privé,
- on peut mailer en local sans que le courrier ait à passer par le FAI, par contre si un utilisateur local répond à un mail d'un autre utilisateur local (fonction **Reply**), le mail ne passe pas d'abord chez le FAI pour revenir sur le réseau, il est acheminé en local. Avec la configuration d'Eric le mail va d'abord chez le FAI.

On suppose que **machine** est le nom de votre machine tel que vous l'aurez défini avec **netcfg** ou **linuxconf**, **domaine.fr** est le nom de votre domaine qui se limite à votre machine ou éventuellement à votre réseau local, **mail.fai.fr** est le serveur de mail de votre provider. **toto** et **tata** sont les deux noms d'utilisateur que vous avez déclarés sur la machine. Vous ne disposez que d'un seul compte chez votre provider, mais par contre vous avez plusieurs emails, du style **toto.nom@fai.fr** et **tata.nom@fai.fr**.

La configuration présentée ici fonctionne pour les versions 8.9.X et 8.12.X de **sendmail**.

4.2 Installation

4.2.1 Sous Mandriva

Tout d'abord pour installer **sendmail**

urpmi sendmail

Si **postfix** cause des problèmes de conflit, forcer sa désinstallation ainsi

rpm -e --nodeps postfix-2.1.5-6mdk

(exemple donné pour LE 2005) Puis retentez l'installation de **sendmail**. Vous aurez encore besoin des packages suivants

sendmail-cf
m4

Et éventuellement le package de documentation **sendmail-doc**. Sachez que vous pourrez toujours trouver la doc de référence sur le site de [sendmail](http://www.sendmail.org).

4.2.2 Sous ubuntu

Il faudra installer le package **sendmail**, le package **m4** doit également être installé si ce n'est pas déjà fait.

4.3 Configuration

Pour une Mandriva j'ai créé ensuite un fichier **/usr/share/sendmail-cf/cf/config.mc** qui a cette tête là:

```
include(`../m4/cf.m4')dnl
OSTYPE(`linux')dnl
FEATURE(redirect)dnl
FEATURE(nocanonify)dnl
```

```

FEATURE(always_add_domain)dnl
FEATURE(local_procmail)dnl
GENERIC_DOMAIN(machine.domaine.fr machine localhost)
FEATURE(genericstable)
FEATURE(masquerade_envelope)dnl
FEATURE(relay_entire_domain)dnl
FEATURE(accept_unresolvable_domains)dnl
define(`confDOMAIN_NAME',`ppp.fai.fr')dnl
define(`SMTP_MAILER_FLAGS',`e9')dnl
define(`confCON_EXPENSIVE',`True')dnl
define(`confME_TOO',`True')dnl
define(`confCF_VERSION',`Commentaire quelconque')dnl
define(`confCOPY_ERRORS_TO',`Postmaster')dnl
define(`confDEF_CHAR_SET',`ISO-8859-1')dnl
define(`confMIME_FORMAT_ERRORS',`True')dnl
define(`SMART_HOST',`smtp8:[mail.fai.fr]')dnl
define(`confRECEIVED_HEADER',`from fai.fr
    by fai.fr ($v/$Z)$?r with $r$. id $i$?u
    for $u; $);
    $.Sb')
define(`confTO_QUEUEWARN',`24h')dnl
MAILER(local)
MAILER(smtp)
Kpirateo hash -o /etc/mail/pirateo
LOCAL_RULE_0
R$+ < @ $+ > $*           $: < $(pirateo $1 @ $2 $: $) > $1 < @ $2 > $3
R< $+ > $+ < @ $+ > $*     @$ $>97 $1
R<> $+ < @ $+ > $*        $: $1 < @ $2 > $3

```

^^^^^^ tabulation unique à cet endroit, ailleurs un simple espace

Sous (k)ubuntu le même fichier doit se trouver sous /etc/mail avec la ligne

```
include(/usr/share/sendmail/cf/m4/cf.m4)dnl
```

au lieu de

```
include(../m4/cf.m4)dnl
```

J'ai une différence notable par rapport à la doc de Jacoboni, j'ai rajouté **FEATURE(relay_entire_domain)** ce qui permet à sendmail d'accepter les mails venants des postes de votre réseau privé appartenant à votre domaine privé, sans ce parametre à l'envoi d'email, vous auriez sur les PC sous windows un message d'erreur du style "Relaying denied".

J'ai rajouté aussi **FEATURE(accept_unresolvable_domains)** car sans quoi si le PC sous linux est off-line pas moyen d'envoyer un mail d'un PC sous Windows vers le PC sous Linux, par contre dès qu'on passe on-line ce paramètre devient parfaitement inutile. Je ne comprends pas trop pourquoi mais je soupçonne une histoire de DNS la dessous.

Les dernières lignes (à partir de **Kpirateo**) permet que le courrier ne part chez le FAI en cas de réponse à un utilisateur du réseau local. Je m'explique, si un utilisateur local **toto** envoie un mail à un autre utilisateur local **tata**, l'email de l'expéditeur va être réécrite (fonction **genericstable**) **toto.nom@fai.fr**, si **tata** répond au mail, la réponse partira vers **toto.nom@fai.fr** et non pas simplement **toto**, en d'autres termes le courrier va d'abord partir chez le fai avant de revenir en local ! Ces lignes permettent que le courrier soit acheminé en local. Cette astuce m'a été communiquée par [Denis Braussen](#) d'après l'idée de [Pablo Saratxaga](#). Vous trouverez plus de détail sur la page de configuration UUCP écrite par Denis au [chapitre 7](#).

ATTENTION: à la tabulation unique dans les trois dernières lignes.

NOTE Attention pour qu'un mail parte en local vers le compte **toto** vous devez taper comme email de destination **toto** (sans le domaine), **toto@machine** ou bien encore **toto@machine.domaine.fr** avec **machine** le nom de votre serveur **sendmail** et **domaine.fr** celui de votre domaine, si vous mettez **toto@domaine.fr**, le mail partira vers le FAI avant de revenir sur le réseau local, même si **domaine.fr** est défini dans la variable **GENERICSTABLE**.

J'ai rajouté aussi `define(`confDOMAIN_NAME',...)` et `define(`confRECEIVED_HEADER',...)` se reporter au paragraphe masquage des domaines.

Ensuite on crée un fichier `/etc/mail/genericstable`, qui contient ces lignes:

```
toto: toto.nom@fai.fr
tata: tata.nom@fai.fr
```

Ce fichier fait la correspondance entre les adresses locales et les adresses "officielles".

Attention il faut mettre une tabulation entre le `:` et l'adresse.

La ligne `define(`confCF_VERSION', `Commentaire quelconque')` permet de rajouter un commentaire quelconque dans l'entête des mails (voir plus bas).

Pour faire prendre en compte la modif de ce fichier, il faut taper ensuite:

```
sendmail -bi -oA/etc/mail/genericstable
```

ATTENTION Attention pour les versions 8.9.X de `sendmail.generistable` se trouve directement sous `/etc` il faudra prendre en compte cette différence dans la suite des opérations si vous disposez de cette version.

On crée ensuite un fichier `/etc/mail/pirateo`, dans lequel vous mettez :

```
toto.nom@fai.fr toto
tata.nom@fai.fr tata
```

Ensuite pour générer le fichier au format qui va bien on tape :

```
makemap hash /etc/mail/pirateo < /etc/mail/pirateo
```

Ce fichier aura le rôle inverse de `/etc/mail/generistable`, il transforme l'adresse du destinataire `toto.nom@fai.fr` en `toto` si celui est un utilisateur local, pour éviter que le mail parte chez le fai.

Ensuite vous modifiez votre fichier `/etc/nsswitch.conf` pour qu'il ressemble à ça:

```
# bla bla
# un tas de commentaires
#
passwd: files
shadow: files
group: files

hosts: files dns

services: files
networks: files
protocols: files
rpc: files
ethers: files
netmasks: files
bootparams: files

netgroup: files

publickey: files

automount: files
aliases: files
```

La doc de Jacoboni demande de modifier `/etc/hosts` pour qu'elle contienne au moins la ligne

```
127.0.0.1 machine.domaine.fr localhost machine
```

Et bien je n'en ai rien fait, j'ai laissé:

127.0.0.1 localhost localhost.localdomain

Pourquoi donc? Parce que si on suit les conseils de Jacoboni, **Samba** ne marche plus, au lieu de travailler sur l'adresse IP de classe C de votre réseau privé que vous avez défini (192.168.13.X par exemple), **Samba** va travailler sur l'adresse de classe A 127.X.X.X, autant dire que rien ne fonctionnera.

Ne vous préoccupez pas des remarques alarmistes de Jacoboni, qu'on suive ces conseils sur **/etc/hosts** ou pas, j'ai constaté un fonctionnement identique de **sendmail**. Par contre n'oubliez pas de rajouter vos postes de votre réseau privé avec le FQDN (Fully qualified domain name, nom complet), ça nous donne donc ça:

```
127.0.0.1 localhost localhost.localdomain
192.168.13.10 machine.domaine.fr machine
192.168.13.11 windows.domaine.fr windows
192.168.13.12 mac.domaine.fr mac
```

windows et mac étant deux machines de votre réseau privé, les adresses IP sont données à titre indicatif.

ATTENTION: si **sendmail** bloque le boot de la machine, ça peut venir justement du fait qu'on n'a pas modifié la première ligne de **/etc/hosts**, **sendmail** n'arrive pas à trouver le nom de la machine et part dans une recherche qui par défaut dure 3 minutes, ceux-ci peut expliquer les remarque d'Eric Jacoboni. Par ailleurs ça peut engendrer des problèmes de résolution de nom sur la machine linux en mode off-line, pour résoudre ces problèmes tout en maintenant la ligne en question inchangée, reportez vous au document installation d'un serveur DNS disponible sur le site funix.org.

Pour rebatir le fichier de configuration de **sendmail**, on tape la commande:

sous Mandriva

```
cd /usr/share/sendmail-cf/cf/
```

sous (k)ubuntu

```
cd /etc/mail ubuntu
```

Pour les deux distribs

```
m4 config.mc > /etc/mail/sendmail.cf
```

Bizarrement même avec sudo j'avais une erreur de droit sous (k)ubuntu j'ai du décomposer la commande ainsi

```
sudo m4 config.mc > /tmp/sendmail.cf
sudo cp /tmp/sendmail.cf /etc/mail
```

Changer (éventuellement) les droits de ce fichier:

```
chmod 600 /etc/mail/sendmail.cf
```

Ca y est c'est fini sous Mandriva, sous (k)ubuntu il y a cependant des petites manip supplémentaires à effectuer sur le fichier **/etc/mail/sendmail.cf**, voilà ce que vous devez modifier

```
# temporary file mode
O TempFileMode=0644
```

```
# queue file mode (qf files)
O QueueFileMode=0640
```

```
# default UID (can be username or userid:groupid)
O DefaultUser=mail:mail
```

```
# chrooted environment for writing to files
O SafeFileEnvironment
```

```
# Trusted user for file ownership and starting the daemon
O TrustedUser=smmta
```

```
# Control socket for daemon management
```

O ControlSocketName=/var/run/sendmail/mta/smcontrol

location of pid file

O PidFile=/var/run/sendmail/mta/sendmail.pid

4.4 On relance tout

Pour relancer tout, il faut d'abord préalablement tuer **sendmail** s'il tourne, pour cela faire:

```
/etc/rc.d/init.d/sendmail stop
```

sous (k)ubuntu

```
/etc/init.d/sendmail stop
```

Puis pour relire le fichier de configuration

sendmail -bd -os

Vous pouvez éventuellement rajouter **-X /var/log/sendmail.log** pour avoir le fichier de log, si vous voulez avoir le fichier de log en permanence (y compris au reboot de la machine), modifiez le fichier de lancement de **sendmail /etc/rc.d/init.d/sendmail** à la ligne:

```
daemon /usr/sbin/sendmail ${[ "$DAEMON" = yes ] && echo -bd} \
```

Rajoutez:

```
daemon /usr/sbin/sendmail -X /var/log/sendmail.log ${[ "$DAEMON" = yes ] && echo -bd} \
```

Pour une ubuntu ça se passe dans le fichier **/etc/init.d/sendmail** au lieu de

```
START_MTA_CMD="start-stop-daemon \  
--pidfile $MTA_PIDFILE \  
--exec $MTA_DAEMON \  
--startas $MTA_COMMAND \  
--start";
```

on écrit

```
START_MTA_CMD="start-stop-daemon \  
--pidfile $MTA_PIDFILE \  
--exec $MTA_DAEMON \  
-- $OPTIONS-sendmail \  
--startas $MTA_COMMAND \  
--start";
```

en définissant plus haut dans le fichier

OPTIONS-sendmail='-X /var/log/sendmail.log'

NOTE: Sous mandrake 6.1, j'avais parfois l'erreur suivante après avoir tapé **sendmail -bd -os**:

```
[root@tavel cf]# sendmail -bd -os  
554 /etc/sendmail.cf: line 51: unknown configuration line "  
"
```

```
[root@tavel cf]#
```

En fait il suffit d'éditer **/etc/mail/sendmail.cf** et de supprimer quelques lignes vides au niveau de la ligne 51, pour que tout rentre dans l'ordre, tapez à nouveau la commande **sendmail -bd -os**.

4.5 Principe de fonctionnement

Pour info tous les courriers partants se retrouvent en attente dans le répertoire **/var/spool/mqueue**, ceux en arrivée se trouvent dans **/var/spool/mail** avec pour nom le nom du destinataire sur la machine.

sous **/var/spool** sous ubuntu voilà ce que j'ai en tapant **ll** dans un shell

```
lrwxrwxrwx 1 root root 7 2006-07-23 17:00 mail -> ../mail
```

drwxr-s--- 2 smmta smmsp 4096 2006-07-25 18:18 mqueue
drwxrws--- 2 smmsp smmsp 4096 2006-07-25 18:18 mqueue-client

et voilà le répertoire `/var/mail`

drwxrwsr-t 5 root mail 4096 2006-07-25 18:28 mail

Pour envoyer le courrier, une fois connecté vous devez taper:

`/usr/sbin/sendmail -q -v`

L'option `-v` étant l'option "verbeuse". Pour visualiser les messages dans la file d'attente, vous pouvez taper:

mailq

Quand vous envoyez un courrier en local (de **toto** vers **tata**), le courrier ne va pas transiter par **mqueue**, de même qu'il est inutile de taper "**sendmail -q**", il va se retrouver directement dans la boîte aux lettres du destinataire local, avec dans le champ **From toto@domaine.fr** (c'est le but du paramètre **FEATURE(always_add_domain)** qui va rajouter automatiquement le nom de domain privé).

En cas d'envoi vers un destinataire extérieur à votre domaine, le courrier va se retrouver dans le répertoire **mqueue**.

4.6 Masquage de domaine

Si on se contente d'appliquer la doc de Jacoboni brut de forme, on est confronté à un gros problème qui se voit à l'envoi du courrier vers des adresses échos comme **echo@cnam.fr**, qui se contente de vous renvoyer votre email avec l'entête complète du mail d'origine, on peut y voir des informations indiscretes que vous ne voudriez pas forcément voir figurer.

Voici le mail qui part du serveur Linux, avec pour contenu :

Subject: test
première ligne

Contenu de l'email de réponse du serveur écho du CNAM:

----- **Le serveur echo du domaine cnam.fr**
----- **a reçu votre message le mar 10 août 22:25:28 MET DST 1999**

----- **Ci-dessous les en-tetes et le corps de votre message**

> **From toto.nom@fai.fr Tue Aug 10 22:25:27 1999**
> **Received: from obelix.fai.fr (obelix.fai.fr [210.205.98.21])**
> **by fermi.cnam.fr (8.8.8/jpm-301097) with ESMTP id WAA11452**
> **for <echo@cnam.fr>; Tue, 10 Aug 1999 22:25:27 +0200 (MET DST)**
> **From: toto.nom@fai.fr**
> **Return-Path: <toto.nom@fai.fr>**
> **Received: from machine.domaine.fr (IDENT:root@ppptc22.fai.fr [210.205.98.22])**
> **by obelix.fai.fr (8.9.1/8.9.1/R&D&B-990119) with ESMTP id WAA26056**
> **for <echo@cnam.fr>; Tue, 10 Aug 1999 22:24:55 +0200**
> **Received: (from toto@localhost)**
> **by machine.domaine.fr (8.9.3/8.9.3/Commentaire quelconque) id WAA00754**
> **for echo@cnam.fr; Tue, 10 Aug 1999 22:25:34 +0200**
> **Date: Tue, 10 Aug 1999 22:25:34 +0200**
> **Message-Id: <199908102025.WAA00754@machine.domaine.fr>**
> **To: echo@cnam.fr**
> **Subject: test**

>
> première ligne
>

----- Fin de votre message

Quelques commentaires:

toto.nom@fai.fr est votre adresse email chez votre fournisseur d'accès, **obelix.fai.fr (IP= 210.205.98.21)** est le nom de la machine chez votre fai qui a "routé" votre email, **ppptc22.fai.fr (IP=210.205.98.22)** c'est votre identité officielle sur le net au moment de votre connexion.

Vous voyez que le nom de votre domaine apparaît dans les champs **Received**, et même le commentaire que vous aurez défini dans le fichier de config de **sendmail**. Certains gestionnaires d'email pourraient rejeter vos emails sous prétexte de contenir un nom de domaine inconnu.

Voyons maintenant un email arrivant d'un de vos postes sous Windows et partant vers le net.

----- Le serveur echo du domaine cnam.fr
----- a reçu votre message le mar 10 août 19:47:08 MET DST 1999

----- Ci-dessous les en-tetes et le corps de votre message

> From toto.nom@fai.fr Tue Aug 10 19:47:07 1999
> Received: from obelix.fai.fr (obelix.fai.fr [210.205.98.21])
> by fermi.cnam.fr (8.8.8/jpm-301097) with ESMTP id TAA05598
> for <echo@cnam.fr>; Tue, 10 Aug 1999 19:47:06 +0200 (MET DST)
> Return-Path: <toto.nom@fai.fr>
> Received: from machine.domaine.fr (IDENT:root@ppptc32.fai.fr [210.205.98.23])
> by obelix.fai.fr (8.9.1/8.9.1/R&D&B-990119) with ESMTP id TAA23230
> for <echo@cnam.fr>; Tue, 10 Aug 1999 19:46:35 +0200
> Received: from windows (windows.domaine.fr [192.168.13.11])
> by machine.domaine.fr (8.9.3/8.9.3/Commentaire quelconque) with ESMTP id TAA00863
> for <echo@cnam.fr>; Tue, 10 Aug 1999 19:38:54 +0200
> Message-Id: <199908101738.TAA00863@machine.domaine.fr>
> From: "Toto Nom" <toto.nom@fai.fr>
> To: <echo@cnam.fr>
> Subject: test de windows
> Date: Tue, 10 Aug 1999 19:37:08 +0200
> X-MSMail-Priority: Normal
> X-Priority: 3
> X-Mailer: Microsoft Internet Mail 4.70.1155
> MIME-Version: 1.0
> Content-Type: text/plain; charset=ISO-8859-1
> Content-Transfer-Encoding: 7bit

>
> première ligne
>

----- Fin de votre message

Dans **Received**, on voit en fait le cheminement que suit le mail envoyé du poste **windows**, va sur **machine** puis par chez votre fai (sur **obelix**), on voit donc le nom de votre domaine, les noms du poste Linux et du poste de votre réseau privé d'où a été envoyé l'email, et même l'adresse IP que vous lui avez attribué !

Le problème est qu'on ne peut dans les paramètres de config de **sendmail**, virer les champs **Received**, **FEATURE(masquerade_enveloppe)** ne fait que masquer les adresses emails.

Pour corriger ça, on va d'abord rajouter **define(`confDOMAIN_NAME', `ppp.fai.fr')** qui permet de redéfinir la manière dont notre serveur Linux va se présenter au serveur SMTP du provider, en clair il va changer toutes les occurrences de **machine.domaine.fr** par **ppp.fai.fr** dans les champs **Received**. Pourquoi mettre **ppp.fai.fr** et ne pas mettre tout simplement **fai.fr**, parce que dans ce cas on ne pourra pas envoyer de mail à des utilisateurs du domaine **fai.fr**, **sendmail** croit que ce sont des utilisateurs locaux ! Avec **ppp.fai.fr** pas de problème, en toute rigueur on pourrait mettre ici le nom attribué lors d'une connexion (du style **ppp18-brest.fai.fr** qu'on peut voir en tapant **ifconfig**) pour cela reporter vous au paragraphe [attribution d'adresse dynamique](#).

Reste le problème des emails partant de postes sous Windows, où apparaît le nom et l'adresse IP, on va carrément redéfinir le champs **Received**:

```
define(`confRECEIVED_HEADER', `from fai.fr
  by fai.fr ($v/$Z)$?r with $r$. id $i$?u
  for $u; $;
  $. $b')
```

Ce qui nous donne pour un mail envoyé d'un PC sous windows:

```
----- Le serveur echo du domaine cnam.fr
----- a reçu votre message le sam jun 1 19:08:31 CEST 2002
----- Ci-dessous les en-tetes et le corps de votre message
> From toto.nom@fai.fr Sat Jun 01 17:08:31 2002
> Return-Path: <toto.nom@fai.fr>
> Delivered-To: echo@cnam.fr
> Received: (qmail 20719 invoked from network); 1 Jun 2002 17:08:31 -0000
> Received: from bougainville.cnam.fr (163.173.128.13)
> by 0 with SMTP; 1 Jun 2002 17:08:31 -0000
> Received: from localhost (localhost [127.0.0.1])
> by bougainville.cnam.fr (Postfix) with ESMTP id 132F82EFB4
> for <echo@cnam.fr>; Sat, 1 Jun 2002 19:08:31 +0200 (CEST)
> Received: from smtp.fai.fr (mail.fai.fr [202.3.225.22])
> by bougainville.cnam.fr (Postfix) with ESMTP id D31492EFAE
> for <echo@cnam.fr>; Sat, 1 Jun 2002 19:08:27 +0200 (CEST)
> Received: from ppp.fai.fr (tc5-bis-014.dialup.fai.fr [202.3.239.14])
> by smtp.fai.fr (Mirapoint Messaging Server MOS 3.1.0.36-EA)
> with ESMTP id ADS19083
> for <echo@cnam.fr>;
> Sat, 1 Jun 2002 07:08:20 -1000 (TAHT)
> Received: from fai.fr
> by fai.fr (8.12.1/8.12.1/Commentaire quelconque) with ESMTP id g51H7FAj002161
> for <echo@cnam.fr>; Sat, 1 Jun 2002 07:07:15 -1000
> Message-ID: <3CF90D0A.5FF74480@fai.fr>
> Date: Sat, 01 Jun 2002 07:06:02 -1100
> From: Toto Nom <toto.nom@fai.fr>
> X-Mailer: Mozilla 4.7 [fr] (WinNT; I)
> X-Accept-Language: fr
> MIME-Version: 1.0
> To: echo@cnam.fr
> Subject: essai
> Content-Type: text/plain; charset=us-ascii
> Content-Transfer-Encoding: 7bit
> X-Virus-Scanned: by AMaViS perl-11
-----

>
> première ligne
>
```

----- Fin de votre message

Voici l'email qui part de notre serveur Linux.

----- Le serveur echo du domaine cnam.fr
----- a reçu votre message le sam jun 1 07:51:15 CEST 2002
----- Ci-dessous les en-tetes et le corps de votre message
> From toto.nom@fai.fr Sat Jun 01 05:51:15 2002
> Return-Path: <toto.nom@fai.fr>
> Delivered-To: echo@cnam.fr
> Received: (qmail 3855 invoked from network); 1 Jun 2002 05:51:14 -0000
> Received: from bougainville.cnam.fr (163.173.128.13)
> by 0 with SMTP; 1 Jun 2002 05:51:14 -0000
> Received: from localhost (localhost [127.0.0.1])
> by bougainville.cnam.fr (Postfix) with ESMTP id CB0A52EFAF
> for <echo@cnam.fr>; Sat, 1 Jun 2002 07:51:14 +0200 (CEST)
> Received: from smtp.fai.fr (mail.fai.fr [202.3.225.22])
> by bougainville.cnam.fr (Postfix) with ESMTP id 8EE6D2EFAE
> for <echo@cnam.fr>; Sat, 1 Jun 2002 07:51:11 +0200 (CEST)
> Received: from ppp.fai.fr (tc5-bis-198.dialup.fai.fr [202.3.239.198])
> by smtp.fai.fr (Mirapoint Messaging Server MOS 3.1.0.36-EA)
> with ESMTP id ADS03894
> for <echo@cnam.fr>;
> Fri, 31 May 2002 19:50:40 -1000 (TAHT)
> Received: from fai.fr
> by fai.fr (8.12.1/8.12.1/Commentaire quelconque) with ESMTP id g515nwFE002664
> for <echo@cnam.fr>; Fri, 31 May 2002 19:49:58 -1000
> Sender: toto.nom@fai.fr
> Message-ID: <3CF86086.351F9560@fai.fr>
> Date: Fri, 31 May 2002 19:49:58 -1000
> From: Toto Nom <toto.nom@fai.fr>
> Organization: Tahiti Connection
> X-Mailer: Mozilla 4.78 [fr] (X11; U; Linux 2.4.18-6mdk i686)
> X-Accept-Language: en
> MIME-Version: 1.0
> To: echo@cnam.fr
> Subject: test
> Content-Type: text/plain; charset=us-ascii
> Content-Transfer-Encoding: 7bit
> X-Virus-Scanned: by AMaViS perl-11

>
> première ligne
>

----- Fin de votre message

4.7 Si vous avez un autre email que celui attribué par le Fai utilisé

Vous pouvez très bien utiliser un FAI du style **fai.fr** et ne pas utiliser une adresse email en **@fai.fr**. Ainsi je me connecte avec **free** et mon adresse email est **olivier.hoarau@fnac.net**, dans ce cas le **Message-Id** et le **Sender** n'ont pas une bonne tête.

Exemple avec cette entête renvoyée par **echo@cnam.fr**

> From olivier.hoarau@fnac.net Sat Jul 15 08:19:16 2000
> Received: from postfix3.free.fr (postfix@postfix3.free.fr [212.27.32.22])
> by fermi.cnam.fr (8.8.8/jpm-301097) with ESMTP id IAA05796
> for <echo@cnam.fr>; Sat, 15 Jul 2000 08:19:16 +0200 (MET DST)
> Return-Path: <olivier.hoarau@fnac.net>
> Received: from ppp.free.fr (massy-4-14-209.dial.proxad.net [213.228.14.209])
> by postfix3.free.fr (Postfix) with ESMTP id 62B6286B67
> for <echo@cnam.fr>; Sat, 15 Jul 2000 08:19:15 +0200 (CEST)

```

> Received: from free.fr
>   by free.fr (8.10.1/8.10.1/Olivier Hoarau-992911) with ESMTP id e6F68IJ01419
>   for <echo@cnam.fr>; Sat, 15 Jul 2000 08:08:18 +0200
> Sender: olivier@free.fr
> Message-ID: <396FFFD2.447D80E1@fnac.net>
> Date: Sat, 15 Jul 2000 08:08:18 +0200
> From: Olivier Hoarau <olivier.hoarau@fnac.net>
> Organization: Breizh Connection
> X-Mailer: Mozilla 4.73 [fr] (X11; I; Linux 2.2.15-4mdk i686)
> X-Accept-Language: en
> MIME-Version: 1.0
> To: echo@cnam.fr
> Subject: asterix
> Content-Type: text/plain; charset=us-ascii
> Content-Transfer-Encoding: 7bit

```

Vous voyez que le **Message-Id** a l'extension **fnac.net** alors qu'il devrait être en **free.fr** puisque j'utilise **free**, de même le **Sender** est **olivier@free.fr** qui ne correspond à rien, vu que mon email chez **free** est ohoarau@free.fr

Pour régler le problème du **Message-Id** et du **Sender**, j'ai écrit ce petit script :

```

#!/bin/bash
cd /var/spool/mqueue
for nom_mail in $(ls qf*)
do
    awk 'BEGIN { FS=":" }
        $1!="H??Message-ID" && $1!="H??Sender" { print $0 }
        $1=="H??Sender" { sub("olivier","ohoarau",$2);print $1,"",$2 }
        $1=="H??Message-ID" { sub("fnac.net","free.fr",$2); print $1,"",$2 }
    ' $nom_mail > /tmp/mail.tmp
    cp /tmp/mail.tmp $nom_mail
done

```

Vous pourrez très facilement adapter ce script à votre situation, quelques commentaires sont peut être utiles:

```

- sub("olivier","ohoarau",$2) ici c'est pour avoir Sender: ohoarau@free.fr au lieu de Sender: olivier@free.fr
- sub("fnac.net","free.fr",$2) ici c'est pour avoir Message-ID: <396FFFD2.447D80E1@free.fr au lieu de Message-ID: <396FFFD2.447D80E1@fnac.net

```

Remplacez les chaînes de caractères adéquates pour que ça marche chez vous. Le proprio du script doit être root, avec des droits en 755, on l'appellera avant **sendmail -q** et qui permettra de changer le **Message-Id** et le **Sender**.

Si ce script s'appelle **chg-message** et se trouve dans **/usr/sbin**, vous pouvez le mettre dans le fichier **/etc/ppp/ip-up** lancé à chaque connexion, comme ceci

```

/usr/sbin/chg-message
/usr/sbin/sendmail -q

```

Voilà en final la tête mon mail envoyé de mon poste linux tel que l'a renvoyé le serveur écho du cnam:

```

----- Le serveur echo du domaine cnam.fr
----- a reçu votre message le sam 15 jul 09:23:10 MET DST 2000

----- Ci-dessous les en-tetes et le corps de votre message

```

```

> From olivier.hoarau@fnac.net Sat Jul 15 09:23:09 2000
> Received: from postfix1.free.fr (postfix@postfix1.free.fr [212.27.32.21])
>   by fermi.cnam.fr (8.8/jpm-301097) with ESMTP id JAA10064

```

> for <echo@cnam.fr>; Sat, 15 Jul 2000 09:23:09 +0200 (MET DST)
 > Return-Path: <olivier.hoarau@fnac.net>
 > Received: from ppp.free.fr (massy-2-11-231.dial.proxad.net [213.228.11.231])
 > by postfix1.free.fr (Postfix) with ESMTP id DA7D228043
 > for <echo@cnam.fr>; Sat, 15 Jul 2000 09:23:03 +0200 (MEST)
 > Received: from free.fr
 > by free.fr (8.10.1/8.10.1/Olivier Hoarau-992911) with ESMTP id e6F72bP02146
 > for <echo@cnam.fr>; Sat, 15 Jul 2000 09:02:37 +0200
 > Sender: ohoarau@free.fr
 > Message-ID: <39700C8D.3443567C@free.fr>
 > Date: Sat, 15 Jul 2000 09:02:37 +0200
 > From: Olivier Hoarau <olivier.hoarau@fnac.net>
 > Organization: Breizh Connection
 > X-Mailer: Mozilla 4.73 [fr] (X11; I; Linux 2.2.15-4mdk i686)
 > X-Accept-Language: en
 > MIME-Version: 1.0
 > To: echo@cnam.fr
 > Subject: essai
 > Content-Type: text/plain; charset=us-ascii
 > Content-Transfer-Encoding: 7bit

Le **Message-Id** et le **Sender** ont maintenant une bonne tête.

Voilà le message renvoyé d'un mail partant d'un poste client windows du réseau:

----- Le serveur echo du domaine cnam.fr
 ----- a reçu votre message le sam 15 jul 09:46:21 MET DST 2000

----- Ci-dessous les en-tetes et le corps de votre message

> From olivier.hoarau@fnac.net Sat Jul 15 09:46:21 2000
 > Received: from postfix2.free.fr (postfix@postfix2.free.fr [212.27.32.74])
 > by fermi.cnam.fr (8.8.8/jpm-301097) with ESMTP id JAA11374
 > for <echo@cnam.fr>; Sat, 15 Jul 2000 09:46:21 +0200 (MET DST)
 > Return-Path: <olivier.hoarau@fnac.net>
 > Received: from ppp.free.fr (massy-2-10-239.dial.proxad.net [213.228.10.239])
 > by postfix2.free.fr (Postfix) with ESMTP id 7FB1D740DB
 > for <echo@cnam.fr>; Sat, 15 Jul 2000 09:46:20 +0200 (MEST)
 > Received: from free.fr
 > by free.fr (8.10.1/8.10.1/Olivier Hoarau-992911) with ESMTP id e6F7iTG02453
 > for <echo@cnam.fr>; Sat, 15 Jul 2000 09:44:30 +0200
 > Message-ID: <39701660.10A22F73@free.fr>
 > Date: Sat, 15 Jul 2000 09:44:32 +0200
 > From: Olivier Hoarau <olivier.hoarau@fnac.net>
 > X-Mailer: Mozilla 4.6 [fr] (Win98; I)
 > X-Accept-Language: fr
 > MIME-Version: 1.0
 > To: echo@cnam.fr
 > Subject: tavel
 > Content-Type: text/plain; charset=us-ascii
 > Content-Transfer-Encoding: 7bit

Vous pouvez constater qu'il n'y a pas de champ **Sender**.

4.8 Attribution d'adresse dynamique

Vous pouvez redéfinir le nom de votre machine, tel qu'il apparaîtra dans les headers, pour qu'il corresponde exactement avec le nom que vous a attribué le fai, pendant une connexion et ceci même si ce nom change à

chaque connexion. Je me sers d'un truc trouvé dans le [guide du rootard](http://www.linux-France/article/grl) à l'URL www.linux-France/article/grl que j'ai très légèrement adapté (au chapitre 13.10 pour être précis). Le truc c'est qu'à chaque connexion on lance un petit programme **gethost** qui détermine le nom attribué dynamiquement, on modifie dans la foulée le **config.mc** en conséquence, on régénère **sendmail.cf**, on kill sendmail et on le relance dans la foulée. Pour cela j'ai créé un programme **gethost.c** dont voici le contenu:

```
#include <stdio.h>
#include <netdb.h>
#include <arpa/inet.h>
#include <string.h>

int main(argc,argv)
char argc;
char *argv[];
{
    struct hostent *host;
    struct in_addr ia;

    if (argc < 2) {
        fprintf(stderr,"Usage: %s adresse_IP_locale\n",argv[0]);
        exit(1);
    }
    if (!inet_aton (argv[1],&ia)) {
        fprintf(stderr,"Erreur: adresse invalide\n");
        exit(1);
    }

    host=gethostbyaddr((char*)&ia,sizeof(ia),AF_INET);

    if (!host) {
        fprintf(stderr,"Erreur: adresse non trouvée ou pas de DNS\n");
        exit(1);
    }
    printf("%s\n",host->h_name);
    exit(0);
}
```

On le compile tout simplement en tapant:

```
gcc gethost.c -o gethost
```

En tant que root, copiez l'exécutable **gethost** sous **/usr/local/sbin** (ou **/usr/bin** c'est vous qui voyez...). Maintenant on va modifier **/etc/ppp/ip-up** qui est lancé à chaque début de connexion pour reconstruire le fichier de config de **sendmail** en fonction du nom déterminé par **gethost** et relancer **sendmail**.

```
#!/bin/bash
# $4 correspond à l'adresse IP attribuée lors d'une connexion
ADRESSE=$4

# détermination du nom connaissant l'adresse IP
HOST=`/usr/local/sbin/gethost $ADRESSE`

# on modifie le fichier de config pour avoir le nom qui va bien (à noter que config.mc n'est jamais touché)
if [ -n "$HOST" ] ; then
    sed s/ppp.fai.fr/$HOST/ /usr/share/sendmail-cf/cf/config.mc > /usr/share/sendmail-
cf/cf/config.current.mc
    # on régénère sendmail.cf
    cd /usr/share/sendmail-cf/cf
    m4 config.current.mc > /etc/sendmail.cf
```

```

# on tue sendmail
kill -1 `head -1 /var/run/sendmail.pid`

# Si nécessaire on appelle le script chg-message
# pour que le Message-Id et le Sender soit correct
# /usr/sbin/chg-message

# on relance sendmail
/usr/sbin/sendmail -bd -os
fi
exit 0

```

Autre solution beaucoup plus simple, si vous voulez pas vous embêter avec un programme C, remplacer la ligne **HOST** par:

```
HOST=`(nslookup $ADRESSE|grep Name:|sed 's/Name:*/')`
```

A la prochaine connexion, vous aurez donc un **sendmail** avec une config tip-top. Voilà un mail envoyé de mon poste linux:

```

----- Le serveur echo du domaine cnam.fr
----- a reçu votre message le mer 1 déc 18:08:00 MET 1999

```

```

----- Ci-dessous les en-tetes et le corps de votre message

```

```

> From olivier.hoarau@fnac.net Wed Dec 1 18:07:59 1999
> Received: from mailhub1.isdnet.net (mailhub1.isdnet.net [195.154.209.21])
>   by fermi.cnam.fr (8.8.8/jpm-301097) with ESMTP id SAA27323
>   for <echo@cnam.fr>; Wed, 1 Dec 1999 18:07:59 +0100 (MET)
> Return-Path: <olivier.hoarau@fnac.net>
> Received: from ppp7-brest.isdnet.net (ppp7-brest.isdnet.net [194.149.178.134])
>   by mailhub1.isdnet.net (8.9.3/8.9.3) with ESMTP id SAA18750
>   for <echo@cnam.fr>; Wed, 1 Dec 1999 18:07:57 +0100 (CET)
> Received: from fnac.net
>   by fnac.net (8.9.3/8.9.3/Olivier Hoarau-992911) with ESMTP id SAA00908
>   for <echo@cnam.fr>; Wed, 1 Dec 1999 18:08:06 +0100
> Sender: olivier.hoarau@fnac.net
> Message-ID: <384555EA.84111C99@fnac.net>
> Date: Wed, 01 Dec 1999 17:07:57 +0000
> From: Olivier Hoarau <olivier.hoarau@fnac.net>
> Organization: FNAC.net
> X-Mailer: Mozilla 4.61 [en] (X11; I; Linux 2.2.13-7mdk i586)
> X-Accept-Language: fr, en
> MIME-Version: 1.0
> To: echo@cnam.fr
> Subject: de tavel netscape
> Content-Type: multipart/alternative;
> boundary="-----510B10AEB1791042330882C7"

```

mon texte

```

----- Fin de votre message

```

Envoyé d'un poste client sous Windows:

```

----- Le serveur echo du domaine cnam.fr
----- a reçu votre message le mer 1 déc 18:08:00 MET 1999

```

----- Ci-dessous les en-tetes et le corps de votre message

```
> From olivier.hoarau@fnac.net Wed Dec 1 18:07:58 1999
> Received: from mailhub1.isdnet.net (mailhub1.isdnet.net [195.154.209.21])
>   by fermi.cnam.fr (8.8.8/jpm-301097) with ESMTP id SAA27306
>   for <echo@cnam.fr>; Wed, 1 Dec 1999 18:07:58 +0100 (MET)
> Return-Path: <olivier.hoarau@fnac.net>
> Received: from ppp7-brest.isdnet.net (ppp7-brest.isdnet.net [194.149.178.134])
>   by mailhub1.isdnet.net (8.9.3/8.9.3) with ESMTP id SAA18743
>   for <echo@cnam.fr>; Wed, 1 Dec 1999 18:07:56 +0100 (CET)
> Received: from fnac.net
>   by fnac.net (8.9.3/8.9.3/Olivier Hoarau-992911) with ESMTP id SAA00910
>   for <echo@cnam.fr>; Wed, 1 Dec 1999 18:08:31 +0100
> Message-ID: <3845554F.7814F4EB@fnac.net>
> Date: Wed, 01 Dec 1999 18:05:20 +0100
> From: Olivier Hoarau <olivier.hoarau@fnac.net>
> Organization: FNAC net
> X-Mailer: Mozilla 4.61 [en] (Win95; I)
> X-Accept-Language: fr-FR,en
> MIME-Version: 1.0
> To: echo@cnam.fr
> Subject: shuttle
> Content-Type: text/plain; chars
et=us-ascii
> Content-Transfer-Encoding: 7bit
```

texte

----- Fin de votre message

NOTE: A noter que de temps à autre, il n'est pas possible de déterminer le nom d'hôte dynamique de la machine attribué lors de la connexion, et cela quelque soit la manière utilisée pour le faire (avec **gethost** ou **nslookup**). C'est pour ça que dans le script **ip-up** vous trouvez un test sur la valeur de **HOST** (vide ou non vide).

4.9 Si vous êtes inscrits à plusieurs FAI

Si vous êtes inscrits à plusieurs FAI comme moi, le problème avec qu'avec la configuration que je viens de présenter, vous ne pouvez envoyer du courrier qu'avec un FAI. Voici donc mon script qui permet de pouvoir reconfigurer **sendmail** à chaque connexion conformément au FAI utilisé.

Tout se passe dans le fichier **/etc/ppp/ip-up** voici le mien

```
#!/bin/bash
```

```
# This file should not be modified -- make local changes to
# /etc/ppp/ip-up.local instead
# l'argument 4 correspond à l'adresse IP attribuée par le FAI
# l'argument 6 correspond est passé en argument de la commande pppd juste
# après ipparam, voir /etc/ppp/ppp-on dans la page connexion à plusieurs FAI
ADRESSE=$4
CONNEXION=$6
```

```
# écriture des paramètres de connexion dans un fichier de log
echo " " >> /var/log/connex
echo "Connecté à $CONNEXION adresse $4 le " >> /var/log/connex
date >> /var/log/connex
```

```
# suivant le FAI, on définit le nom du serveur SMTP, de l'identité à apparaître
# dans les champs RECEIVED et les emails chez le FAI
```

```

case $CONNEXION in
    fnac)
        SERVEUR=smtp.fnac.net
        REC=fnac.net
        MAIL_O=olivier.hoarau@fnac.net
        MAIL_V=veronique.hoarau@fnac.net
        ;;
    liberty)
        SERVEUR=mail.libertysurf.fr
        REC=libertysurf.fr
        MAIL_O=olivier.hoarau2@libertysurf.fr
        MAIL_V=veronique.hoarau@libertysurf.fr
        ;;
    free)
        SERVEUR=smtp.free.fr
        REC=free.fr
        MAIL_O=ohoarau@free.fr
        MAIL_V=veronique.hoarau@free.fr
        ;;
    waika9)
        SERVEUR=smtp.waika9.com
        REC=waika9.com
        MAIL_O=olivier.hoarau@waika9.com
        MAIL_V=veronique.hoarau@waika9.com
        ;;
    *)
        echo "Nom de connexion inconnu $CONNEXION ??"
        exit 0
        ;;
esac

# on met à jour le serveur SMTP
sed s/smtp.fnac.net/$SERVEUR/ /usr/share/sendmail-cf/cf/config.mc >/tmp/config.mc

# maintenant on met à jour la variable confDOMAIN_NAME
HOST=`/usr/local/sbin/gethost $ADRESSE`
#ou si vous préférez
#HOST=`(nslookup $ADRESSE|grep Name:|sed 's/Name:*/')`

echo "Nom de l'hote $HOST" >> /var/log/connex
if [ -n "$HOST" ] ; then
    sed s/ppp.fnac.net/$HOST/ /tmp/config.mc >/tmp/config2.mc
else
    cat /tmp/config.mc > /tmp/config2.mc
fi

# on met à jour l'identité dans les champs RECEIVED
sed s/fnac.net/$REC/g /tmp/config2.mc >/usr/share/sendmail-cf/cf/config.current.mc

# on régénère sendmail.cf
cd /usr/share/sendmail-cf/cf
m4 config.current.mc > /etc/sendmail.cf

# on réécrit /etc/mail/genericstable
# ATTENTION tabulation après le :
cat <<END_OF-DATA > /etc/mail/genericstable
olivier:    $MAIL_O
veronique:  $MAIL_V
END_OF-DATA
# et on régénère genericstable.db
/usr/sbin/sendmail -bi -oA/etc/mail/genericstable

```

```

# on réécrit pirateo
cat <<END_OF-DATA > /etc/mail/pirateo
$MAIL_O olivier
$MAIL_V veronique
END_OF-DATA
# on régénère au format qui va bien
makemap hash /etc/mail/pirateo < /etc/mail/pirateo

# on relance sendmail
kill -1 `head -1 /var/run/sendmail.pid`
/usr/sbin/sendmail -bd -os -X /var/log/sendmail.log

echo "Expédition du courrier en attente" >> /var/log/connex
/usr/sbin/sendmail -q -v >> /var/log/connex

exit 0

```

ATTENTION au chemin de **sendmail-cf** et **genericstable** qui n'est pas forcément le même sur votre système.

Voilà donc la tête du message renvoyé par le service écho du CNAM et expédié de mon poste linux alors que j'étais connecté avec Free :

```

----- Le serveur echo du domaine cnam.fr
----- a reçu votre message le sam 11 déc 14:25:23 MET 1999

```

```

----- Ci-dessous les en-tetes et le corps de votre message

```

```

> From ohoarau@free.fr Sat Dec 11 14:25:22 1999
> Received: from postfix1.free.fr (postfix@postfix1.free.fr [212.27.32.21])
>   by fermi.cnam.fr (8.8.8/jpm-301097) with ESMTP id OAA30761
>   for <echo@cnam.fr>; Sat, 11 Dec 1999 14:25:22 +0100 (MET)
> From: ohoarau@free.fr
> Return-Path: <ohoarau@free.fr>
> Received: from velizy-27-60.dial.proxad.net (velizy-27-60.dial.proxad.net [213.228.27.60])
>   by postfix1.free.fr (Postfix) with ESMTP id 8AAA3281B1
>   for <echo@cnam.fr>; Sat, 11 Dec 1999 14:23:21 +0100 (MET)
> Received: from free.fr
>   by free.fr (8.9.3/8.9.3/Olivier Hoarau-991112) id OAA01011
>   for echo@cnam.fr; Sat, 11 Dec 1999 14:26:15 +0100
> Date: Sat, 11 Dec 1999 14:26:15 +0100
> Message-Id: <199912111326.OAA01011@velizy-27-60.dial.proxad.net>
> To: echo@cnam.fr

```

```

-----

```

```

>
> texte
>

```

```

----- Fin de votre message

```

Ze problème maintenant vient de Netscape Messenger, en effet avec ce dernier quand vous êtes logués sous un compte, vous définissez une adresse email unique, pas moyen d'avoir plusieurs configurations comme sous Windows. Chez moi dans Netscape, j'ai défini **olivier.hoarau@fnac.net** pourtant quand je me connecte chez Free, les mails sont parfaitement relayés, il n'y a aucune vérification du nom de domaine, c'est limite inquiétant pour les histoires de spam. Vous n'avez cependant pas intérêt à mettre un email du genre **mickey.mouse@disneyworld.com**, car personne ne pourra vous répondre.

Voici le contenu du mail envoyé d'un de mes postes clients

----- Le serveur echo du domaine cnam.fr
----- a reçu votre message le sam 11 déc 14:56:43 MET 1999

----- Ci-dessous les en-tetes et le corps de votre message

> From olivier.hoarau@fnac.net Sat Dec 11 14:56:42 1999
> Received: from postfix1.free.fr (postfix@postfix1.free.fr [212.27.32.21])
> by fermi.cnam.fr (8.8.8/jpm-301097) with ESMTP id OAA32210
> for <echo@cnam.fr>; Sat, 11 Dec 1999 14:56:42 +0100 (MET)
> Return-Path: <olivier.hoarau@fnac.net>
> Received: from velizy-27-60.dial.proxad.net (unknown [213.228.40.12])
> by postfix1.free.fr (Postfix) with ESMTP id 5A2AA28318
> for <echo@cnam.fr>; Sat, 11 Dec 1999 14:54:40 +0100 (MET)
> Received: from free.fr
> by free.fr (8.9.3/8.9.3/Olivier Hoarau-991112) with ESMTP id OAA01077
> for <echo@cnam.fr>; Sat, 11 Dec 1999 14:52:42 +0100
> Message-ID: <38525657.C711C933@fnac.net>
> Date: Sat, 11 Dec 1999 14:49:12 +0100
> From: Olivier Hoarau <olivier.hoarau@fnac.net>
> Organization: FNAC net
> X-Mailer: Mozilla 4.61 [en] (Win95; I)
> X-Accept-Language: fr-FR,en
> MIME-Version: 1.0
> To: echo@cnam.fr
> Subject: shuttle
> Content-Type: text/plain; charset=us-ascii
> Content-Transfer-Encoding: 7bit

>
> texte
>

----- Fin de votre message

Pour en avoir le cœur net je me suis envoyé d'un poste client un mail avec en destinataire mon compte chez libertysurf avec pour email déclaré dans Netscape **mickey.mouse@disneyworld.com** voici le corps du mail reçu:

Return-Path: <mickey.mouse@disneyworld.com>
Received: from free.fr
by free.fr (8.9.3/8.9.3/Olivier Hoarau-991112) with ESMTP id PAA01225
for <olivier@localhost>; Sat, 11 Dec 1999 15:11:42 +0100
Received: from pop.libertysurf.fr
by localhost with POP3 (fetchmail-5.0.3)
for olivier@localhost (single-drop); Sat, 11 Dec 1999 15:11:42 +0100 (CET)
Received: by mailhub5.libertysurf.fr (mbox login-pop-chez-libertysurf)
(with Cubic Circle's cucipop (v1.31 1998/05/13) Sat Dec 11 15:13:54 1999)
X-From_: mickey.mouse@disneyworld.com Sat Dec 11 15:13:07 1999
Received: from postfix1.free.fr (postfix1.free.fr [212.27.32.21])
by mailhub5.libertysurf.fr (8.9.3/8.9.3) with ESMTP id PAA74338
for <olivier.hoarau2@libertysurf.fr>; Sat, 11 Dec 1999 15:13:07 +0100 (CET)
Received: from velizy-27-60.dial.proxad.net (unknown [213.228.40.67])
by postfix1.free.fr (Postfix) with ESMTP id C3E7C282BC
for <olivier.hoarau2@libertysurf.fr>; Sat, 11 Dec 1999 15:07:51 +0100 (MET)
Received: from free.fr
by free.fr (8.9.3/8.9.3/Olivier Hoarau-991112) with ESMTP id PAA01172

for <olivier.hoarau2@libertysurf.fr>; Sat, 11 Dec 1999 15:07:16 +0100
Message-ID: <385259C3.5860B95@disneyworld.com>
Date: Sat, 11 Dec 1999 15:03:47 +0100
From: Mickey Mouse <mickey.mouse@disneyworld.com>
Organization: Disney World
X-Mailer: Mozilla 4.61 [en] (Win95; I)
X-Accept-Language: fr-FR,en
MIME-Version: 1.0
To: olivier.hoarau2@libertysurf.fr
Subject: de shuttle
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
X-Mozilla-Status: 8001
X-Mozilla-Status2: 00000000

essai

Groupes !! ça marche... Bon heureusement c'est pas du vrai spam, on voit l'origine **velizy-27-60.dial.proxad.net** avec adresse IP **213.228.40.67**, mais ça permet de faire quelques bonnes blagues. A noter que c'est exactement pareil avec libertysurf.

ATTENTION: Y a un problème dans mon script dans un certain cas de figure, illustration :

- je me connecte avec free, sendmail est donc configuré pour free
- je me déconnecte, sendmail est toujours configuré pour free
- j'envoie un mail dans la liste d'attente, configuré donc pour free
- je me connecte avec libertysurf, le mail part bien mais est mal formaté (avec du free.fr de partout)

Il y a donc un problème au moment du switch entre deux FAI s'il y a du mail dans la file d'attente, je suis en train de rédiger un script pour corriger cela, à suivre.

4.10 Sendmail et timeout DNS

Si avec Microsoft Internet Mail, il est impossible d'envoyer des mails d'un poste Windows vers le serveur Linux quand celui-ci est offline, avec l'erreur suivante dans les fichiers de log:

```
00762 >>> 220 machine.domaine.fr ESMTP Sendmail 8.9.3/8.9.3/Commentaire quelconque qui apparaitre
dans l'entete - 15/08/99; Sat, 21 Aug 1999 09:32:54 +0200
00762 <<< EHLO windows
00762 >>> 250-machine.domaine.fr Hello windows.domaine.fr [192.168.13.11], pleased to meet you
00762 >>> 250-EXPN
00762 >>> 250-VERB
00762 >>> 250-8BITMIME
00762 >>> 250-SIZE
00762 >>> 250-DSN
00762 >>> 250-ONEX
00762 >>> 250-ETRN
00762 >>> 250-XUSR
00762 >>> 250 HELP
00762 <<< RSET
00762 >>> 250 Reset state
00762 <<< MAIL FROM:<toto.nom@fai.fr>
00763 >>> 250 <toto.nom@fai.fr>... Sender ok
00763 <<< RCPT TO:<echo@cnam.fr>
00763 >>> 250 <echo@cnam.fr>... Recipient ok
00763 <<< [EOF]
00763 >>> 421 machine.domaine.fr Lost input channel from windows.domaine.fr [192.168.13.11]
```

Et que par contre il n'y a aucun problème quand le serveur est on-line. C'est que vous avez un problème de DNS. A noter que le problème est similaire avec Outlook Express et d'une manière générale avec les outils de mail de Microsoft .

Si avec Netscape l'envoi de mail en mode off-line vers la file d'attente (répertoire **mqueue**) prend au moins 80s autant dire un éternité, que ce soit d'un poste client ou du poste serveur. C'est que vous avez aussi un problème de DNS.

Pour résoudre ça, il faut installer un serveur DNS sur la machine.

4.11 Sendmail et la lutte anti-spam

Vous pouvez faire appel à des serveurs qui listent les serveurs de mails indéliçats (Open Relay), bien souvent les spams viennent de ces domaines. **sendmail** ira d'abord vérifier si le mail ne vient pas de ces domaines avant de le délivrer localement. Voilà les lignes à rajouter dans votre fichier `/usr/share/sendmail-cf/cf/config.mc`

```
FEATURE(dnsbl, `blackholes.mail-abuse.org', `Rejected - see http://www.mail-abuse.org/rbl/')dnl
FEATURE(dnsbl, `dialups.mail-abuse.org', `Dialup - see http://www.mail-abuse.org/dul/')dnl
FEATURE(dnsbl, `relays.mail-abuse.org', `Open spam relay - see http://www.mail-abuse.org/rss/')dnl
FEATURE(`dnsbl', `list.dsbl.org')dnl
FEATURE(`dnsbl', `bl.spamcop.net')dnl
FEATURE(`dnsbl', `sbl.spamhaus.org')dnl
```

Vous devez ensuite reconstruire `/etc/mail/sendmail.cf` avec **m4** et relancer **sendmail**.

4.12 Sendmail et fichiers de log

Sous une Mandrake 8 les fichiers de logs sont sous `/var/log/mail` et sont décomposés en :

errors contenant les erreurs

info contenant les informations diverses (récupération et expédition de mails)

warnings comme son nom l'indique

Sur les versions antérieurs le fichier de log étaient `/var/log/maillog` ou encore `/var/log/mail.log`, ce fichier rassemblait les erreurs, informations et warnings.

4.13 Sécuriser Sendmail

4.13.1 Les commandes vrfy et expn

Par défaut on peut effectuer un **telnet** sur le port utilisé par **sendmail** et l'interroger avec des commandes, cela permet notamment de connaître les emails déclarés sur le serveur et même les emails d'une liste ou d'un alias. Démonstration, pour la connexion

```
olivier@zoulou olivier]$ telnet zoulou 25
Trying 192.168.13.11...
Connected to zoulou.kervao.fr.
Escape character is '^]'.
220 rennes-1-a7-7-251.dial.proxad.net ESMTP Sendmail 8.11.3/8.11.3/Olivier Hoarau-992911;
Sat, 16 Jun 2001 09:40:20 -0400
```

Vous disposer de **verfy** (verify) pour vérifier l'existence d'une adresse sur le serveur

```
vrfy olivier
250 2.1.5 olivier@rennes-1-a7-7-251.dial.proxad.net
```

Quand l'utilisateur est inconnu

```
vrfy toto
550 5.1.1 toto... User unknown
```

Vous disposez de la commande **expn** (expand) qui est identique à **verfy** mais qui permet aussi de lister les personnes d'une liste et autres alias.

```
expn olivier
```

250 2.1.5 olivier@rennes-1-a7-7-251.dial.proxad.net

Pour désactiver les commandes **vrfy** et **exn** vous devez rajouter au fichier de config **config.mc** la ligne suivante:

```
define(^ confPRIVACY_FLAGS', `novrfy noexn')dnl
```

Voilà le résultat:

```
vrfy olivier
252 2.5.2 Cannot VRFY user; try RCPT to attempt delivery (or try finger)
```

Pour info la commande **finger** est désactivé sur **sendmail** de la Mandrake 8.X

NOTE Pour sortir du **telnet** je n'ai pas trouvé mieux que de faire un **kill** du process

4.13.2 Modifier l'invite de sendmail

En faisant un **telnet** on peut obtenir des renseignements sur le serveur **sendmail**, pour éviter cela, on peut rajouter la ligne suivante dans le fichier de config **config.mc**:

```
define(^ confSMTP_LOGIN_MSG', `Serveur de mail; $b')dnl
```

Voilà ce que ça donne:

```
telnet zoulou 25
Trying 192.168.13.11...
Connected to zoulou.kervao.fr.
Escape character is '^]'.
220 Serveur ESMTP de mail; Sun, 17 Jun 2001 09:19:37 -0400
```

5 Lutte anti spam et anti virus

5.1 Présentation de la configuration

Depuis quelque temps, plus d'un email sur deux que je reçois est un spam ou contient un virus, la lutte anti spam et anti virus est donc devenue une nécessité car il devient vraiment pénible d'avoir sa boîte aux lettres polluée de "pourriels" en tout genre. La lutte est d'autant plus nécessaire si vous avez des utilisateurs sous windows qui sont des cibles privilégiées pour les virus.

Dans cette page sont présentées les outils des plus simples (et moins efficaces) aux plus sophistiquées (et plus efficaces mais moins faciles à mettre en place). On commencera par les outils les plus simples:

- **procmail** permet de filtrer avec des règles statiques des emails qui ont été déjà délivrés par le serveur de mail local (MTA)

- **mailfilter** permet de filtrer avec des règles statiques des emails qui n'ont pas encore été délivrés par le serveur de mail local, c'est à dire qu'ils se trouvent encore sur le serveur pop de votre fournisseur d'accès (en fait seul l'entête est téléchargé pour traitement).

Les outils les plus sophistiqués sont

- **spamassassin** pour la lutte anti spam qui utilisent pour une meilleure efficacité trois autres outils du même genre à savoir **Razor**, **Pyzor** et **DCC**

- **clam anti virus** pour la lutte anti virus.

Ces deux derniers outils complètement interfaçables à **sendmail** ce qui permet un filtrage à la source des emails sur votre réseau local sans que l'utilisateur final n'ait à configurer quoi que ce soit.

En mettant en place tous ces outils je peux vous garantir que vous aurez un excellent taux de rejet de "pourriels".

Dans ce paragraphe par défaut sans mention du contraire toutes les manip marchent aussi bien pour une Mandriva que pour une ubuntu.

5.2 Filtrage basique

5.2.1 Filtrer avec procmail

procmail est une commande simple qui permet de faire beaucoup de choses. Il est très simple de définir des filtres. L'exemple ci-dessous permet de supprimer les mails contenant dans le sujet I Love You

```
:0
* ^Subject:.*ILOVEYOU
/dev/null
```

Il suffit d'adapter cette règle en fonction du sujet (ou du from). Cette autre règle très utile permet de sauvegarder dans un fichier **virus** tous les mails arrivant avec les extensions qui y sont citées.

```
:0 H
*^Content-type: (multipart/mixed)
{
:0 B
*^Content-Disposition: (attachment|inline)
*filename=".*\.(ocx|vbs|wsf|shs|exe|com|bat|chm|pif|vbe|hta|scr)"
{
:0
virus
}
}
```

Le fichier virus pourra être ouvert en tant que boîte aux lettres avec un logiciel comme kmail. Le filtre suivant

```
:0
^Subject:.*[^\ ~][^\ ~][^\ ~][^\ ~]
/dev/null
```

supprime tous les mails dont le sujet commence par 4 caractères consécutifs non ASCII (cas particulier des mails écrits en asiatiques). **Procmail** est quand même assez limité puisqu'il ne permet que de filtrer sur des règles précises (mot clef).

5.2.2 Filtrer avec mailfilter

Il est particulièrement pénible quand on n'a pas une liaison permanente d'avoir à télécharger tous les spams et autres virus, mailfilter permet de pouvoir filtrer les emails directement sur le serveur pop du fournisseur d'accès sans avoir à télécharger le mail dans son intégralité (seul l'entête est téléchargé pour analyse). Mailfilter repose sur le principe de filtre par règles statiques à définir, en utilisant les expressions régulières.

Le site officiel est mailfilter.sourceforge.net vous y récupérerez l'archive de la dernière version stable que vous décompresserez en tapant:

```
tar xvzf mailfilter-0.8.1.tar.gz
```

Cela va donner un répertoire **mailfilter-0.8.1** Avant de passer à la compilation installez éventuellement les packages **byacc** et **bison**, on peut taper maintenant dans le répertoire de **mailfilter**

```
./configure
```

Puis

```
make
```

Et en tant que root

```
make install
```

maintenant on va créer un **.mailfilterrc** qui va se trouver dans la homedirectory. Voilà le contenu de ce fichier:

```
#chemin pour le fichier de log
```

```
LOGFILE=/home/olivier/tmp/.mailfilter.log
```

```
# niveau de bavardage au niveau du log, le niveau 6 (max), n'apporte pas grand chose en plus
VERBOSE=4
```

```

# définition des différents comptes pop de vos utilisateurs
SERVER=pop.fnac.net
USER=login1-fnac
PASS=mot-passe1
PROTOCOL=pop3
PORT=110

SERVER=pop.proxad.net
USER=login1-online
PASS=mot-passe2
PROTOCOL=pop3
PORT=110

SERVER=pop.proxad.net
USER=login2-online
PASS=mot-passe3
PROTOCOL=pop3
PORT=110

# Est-ce qu'on prend en compte la différence majuscule-minuscule dans les expressions régulières
REG_CASE=no

# type d'expression régulière, vous avez le choix entre basic (basic) et étendu (extended)
REG_TYPE=extended

# taille max des fichiers
# attention si la taille est supérieure, le mail est supprimé
# sauf pour ceux qui satisfont aux directives ALLOW
MAXSIZE_DENY=500000

# nombre max de caractères dans une ligne de l'header du mail
# mettre à 0 pour désactiver
MAXLENGTH=998

# on supprime les mails dont les champ To ou Cc ne contiennent ni
# la chaine hoarau, ni funix et ni funboard (liste de diffusion)
DENY<>(^To|^Cc):(*hoarau.*|*funix.*|*funboard.*)
# on supprime les mails qui contiennent le champ sex dans le sujet
DENY=^Subject:.*sex.*
# on supprime les mails dont le champ From contient thecounter
DENY=^From:.*thecounter.*

# -----
# "Normalisation" du message avant passage du filtre, c'est à dire que
# ',L,E-G,A,L; ,C.A-B`L`E, +.B-O`X` ;D`E`S,C;R,A.MB;L,E.R-]'
# devient 'LEGAL CABLE BOX DESCRAMBLER' qui peut être filtré.
NORMAL=yes

# taille max des mails satisfaisants aux directives ALLOW
# Pour désactiver mettre 0
MAXSIZE_ALLOW=1000000

# celui là a le droit de m'envoyer un fichier supérieur à 500Ko (mais inférieur à 1Mo)
ALLOW=^From:.*toto@wanadoo\.fr

Pour aller plus loin, vous pouvez bloquer tout un domaine, sauf quelques personnes de ce domaine, ainsi
DENY=^(From|Received):.*hotmail.com.*
ALLOW=^From:.*copain@hotmail.com.*

Dans un premier temps, si vous avez peur de supprimer des mails sur le serveur, rajoutez en début de fichier
TEST=yes

Pour plus d'info sur la syntaxe de ce fichier, n'oubliez pas
man mailfilterrc
et
man mailfilterex

```

Maintenant pour commencer une analyse, il suffit de taper **mailfilter** , voici le résultat (verbose=4)

```
mailfilter -v 4
```

```
mailfilter: 0.8.1 recherche de login1_fnac@pop.fnac.net sur Wed Dec 12 16:40:25 2001
```

```
mailfilter: Analyse de 0 message(s).
```

```
mailfilter: 0.8.1 recherche de login1_online@pop.proxad.net sur Wed Dec 12 16:40:30 2001
```

```
mailfilter: Analyse de 1 message(s).
```

```
mailfilter: 0.8.1 recherche de login2_online@pop.proxad.net sur Wed Dec 12 16:40:37 2001
```

```
mailfilter: Analyse de 2 message(s).
```

```
mailfilter: Deleted Olivier Hoarau <olivier.hoarau@funix.org>: sex, Sat, 15 Dec 2001 09:36:55 -1000.  
[Applied filter: '^Subject:.*sex.*']
```

```
mailfilter: Deleted Olivier Hoarau <fromabove1@yahoo.fr>: ztreahqzrj, Sat, 15 Dec 2001 09:38:09 -1000.  
[Applied filter: '<>(^To|^Cc):(*hoarau.*.*funix.*.*funboard.*)']
```

Vous constaterez que les messages non supprimés ne sont pas téléchargés, **mailfilter** se contente de filtrer. Pour récupérer il faudra toujours faire appel à **fetchmail**. On va utiliser **fetchmail** en conjonction avec **mailfilter**.

Pour faire appel à votre fichier **.mailfilterrc** par **fetchmail** il suffit de modifier votre fichier **.fetchmailrc** comme ceci

```
poll pop.fai.fr protocol pop3
```

```
user login-fai with password password-fai is olivier here
```

```
preconnect "/usr/local/bin/mailfilter"
```

Dans le cas d'un fichier **.mailfilterrc** commun à tous les utilisateurs, créer un fichier **mailfilterrc** général que vous placerez sous **/etc**.

Dans votre **.fetchmailrc** vous allez rajouter

```
set daemon 600
```

```
set logfile /var/log/fetchmail.log
```

```
poll pop.fai.fr protocol pop3
```

```
user login-fai there with password password-fai is olivier here
```

```
preconnect "mailfilter --mailfilterrc=/etc/mailfilterrc"
```

```
poll pop.fnac.net protocol pop3
```

```
user login-fnac there with password password-fnac is olivier here
```

```
(...)
```

En lançant **fetchmail**, il y aura un appel de **mailfilter** qui fera préalablement le ménage sur les différents serveurs POP appelés par **fetchmail**.

5.3 Filtrer les spams avec spamassassin

5.3.1 Présentation

Spamassassin est un logiciel anti spam, il repose entre autres sur l'analyse heuristique et bayésienne des emails et utilise d'autres outils anti spam comme pyzor, razor et DCC qui sont vus également dans cette page. D'abord quelques définitions.

5.3.2 Définitions

Le filtrage heuristique

C'est une technique qui permet d'identifier du spam en fonction de certaines caractéristiques communes (ponctuation, html, lien vers une image,)

Le filtrage bayésien

le filtrage bayésien repose sur le principe qu'un évènement peut se produire en fonction des mêmes évènements survenus précédemment. En clair pour le mail, si on rencontre certains mots ou phrases plus souvent dans du mail classé spam que dans du mail classé normal on peut penser que la prochaine fois qu'on rencontrera ces mêmes mots et phrases il y a de bonnes chances que ce soit dans un mail de spam.

Pour cela une base de données de mots et phrases est créée et enrichie au fur et à mesure de la réception et de l'envoi de mails qui soient valides ou considérés comme spam. Chaque mot ou sentence reçoit une valeur calculée en fonction de la probabilité qu'il soit relié à du spam, elle dépend du nombre de fois que le terme

apparaît dans du spam par rapport au nombre de fois que le même terme est rencontré dans du courrier valide. Par conséquent certains mots pourront avoir une forte probabilité d'être rattaché à du spam pour certains utilisateurs et pour d'autres pas, exemple concret une entreprise travaillant dans le domaine médical le terme "drug" aura une faible probabilité d'être rattaché à du spam car il est très souvent employé dans les mails valides, pour d'autres personnes ce terme sera systématiquement rattaché à du spams. Par conséquent le filtre bayésien a la particularité et l'avantage de s'adapter à l'utilisateur, il réduit le risque des faux positifs (courrier valide considéré comme spam). Par ailleurs le filtre n'est pas statique, la base de donnée est en constante évolution et donc le filtre sera de plus en plus performant de jour en jour et s'adaptera en fonction des utilisateurs de votre réseau et des techniques nouvelles utilisées par les spammeurs.

Exemple concret du dernier point, jusqu'à présent les spammeurs envoyaient des mails avec des mots du style "sex, free, viagra, ...", il était assez simple de mettre en place un filtre basé sur des mots clef pour supprimer les mails en question, les spammeurs ont donc modifié légèrement la sémantique de mots "s-e-x, f r e e" ou bien encore "v\$!\$a\$g\$r\$a", avec un simple filtrage par mots clé, il est quasi impossible d'établir une règle efficace pour filtrer ces mails. Le filtre bayésien aura aucun problème pour lui attribuer une valeur de probabilité de spam élevée.

Autre avantage du filtre bayésien et non des moindres, il s'adapte à toutes les langues. En clair pour qu'un spammeur puisse tromper un filtre bayésien il doit connaître l'utilisateur qu'il veut toucher et éviter d'utiliser les mots que l'utilisateur en question utilise le moins...

5.3.3 Installation de razor

Razor repose sur le principe d'un serveur central qui identifie les spams en leur attribuant une signature digitale. Chaque utilisateur de razor attribue une signature digitale à chaque email reçu et la compare avec celles du serveur central, permettant ainsi le classement de l'email. Pour identifier les spammeurs, le serveur central diffuse largement des emails valides pour recevoir un max de spams (uniquement du spam, pas de mails valides pour éviter les faux positifs), plus il en reçoit meilleur est razor !

Maintenant on va récupérer **razor** qui va compléter **spamassassin** dans la recherche de spam sur cet URL razor.sourceforge.net/. On décompresse l'archive en tapant

```
tar xvzf razor-agents-2.84.tar.gz
```

Cela donne le répertoire **razor-agents-2.84**, avant d'aller plus loin il faudra installer en tant que root les modules de **perl** suivants

```
perl -MCPAN -e shell
```

Puis au prompt

```
install Digest::SHA1
install Digest::HMAC_MD5
```

Dans le répertoire **razor-agents-2.84** on tape maintenant

```
perl Makefile.PL
```

Puis

```
make
```

Puis en tant que root

```
make install
```

Voilà la trace de **razor2** dans le fichier **/var/log/mail/info** (**/var/log/mail.info** sous ubuntu):

```
Jul 24 16:14:36 mana spamd[6540]: plugin: loading Mail::SpamAssassin::Plugin::Razor2 from @INC
Jul 24 16:14:36 mana spamd[6540]: razor2: razor2 is available, version 2.84
Jul 24 16:14:36 mana spamd[6540]: plugin: did not register Mail::SpamAssassin::Plugin::Razor2=HASH(0x91d5e64), already registered
```

J'en déduis que **razor2** marche correctement.

5.3.4 Installation de SpamAssassin

On récupérera **spamassassin** sur le site www.spamassassin.org/. On décompresse l'archive en tapant

```
tar xvfz Mail-SpamAssassin-3.2.5.tar.gz
```

Cela donne le répertoire **Mail-SpamAssassin-3.2.5**. Avant d'aller plus loin j'ai du installer les packages

```
perl-devel
perl-Net-DNS
perl-Mail-SPF
perl-Mail-SPF-Query
perl-ip-country
perl-net-ident
perl-io-socket-inet6
perl-io-socket-ssl
perl-compress-zlib
perl-mail-domainkeys
perl-mail-dkim
perl-archive-tar
perl-encode-detect
```

Maintenant revenons dans le répertoire **Mail-SpamAssassin-3.2.5** où l'on tape

```
perl Makefile.PL PREFIX=/usr/local
```

Voilé le résultat

```
What email address or URL should be used in the suspected-spam report
text for users who want more information on your filter installation?
(In particular, ISPs should change this to a local Postmaster contact)
default text: [the administrator of that system] olivier
```

```
NOTE: settings for "make test" are now controlled using "t/config.dist".
See that file if you wish to customise what tests are run, and how.
```

```
checking module dependencies and their versions...
Writing Makefile for Mail::SpamAssassin
Makefile written by ExtUtils::MakeMaker 6.42
```

On tape alors

```
make
```

Puis en tant que root

```
make install
```

attention curieusement mes binaires se sont retrouvés sous **/usr/local/local/bin** il faut les replacer sous **/usr/local/bin**

5.3.5 Installation de DCC

DCC repose également sur un serveur central, chaque mail reçu reçoit une signature digitale, le serveur comptabilise toutes les signatures, plus le nombre d'une signature est élevé sur le serveur plus le risque que ce soit un spam est élevé.

Concrètement, à la réception d'un mail le client **DCC** lui attribue une signature digitale (checksum), récupère sur le serveur le nombre de fois que cette signature apparaît dans le serveur central, si ce nombre dépasse une certaine valeur configurable (threshold) et que l'expéditeur du mail en question n'est pas dans la whitelist (configurable elle aussi), le mail est considéré comme spam et traité comme tel.

On va étoffer encore **SpamAssassin** avec **DCC** qu'on récupérera ici <http://www.rhyolite.com/anti-spam/dcc/>. On décompresse l'archive en tapant

```
tar xvfz dcc.tar.Z
```

Cela donne le répertoire **dcc-1.3.116**. Pensez maintenant à installer le package **sendmail-devel** (package **libmilter-dev** sous ubuntu), on revient dans le répertoire de **DCC** dans lequel on tape successivement

```
./configure  
make
```

Puis en tant que root

```
make install
```

Maintenant si on tape (il faut se connecter)

```
cdcc 'info'
```

On obtient

```
# 07/25/06 18:56:53 CEST /var/dcc/map  
# Re-resolve names after 20:56:48 Check RTTs after 19:11:53  
# 1317.41 ms threshold, 1255.48 ms average 12 total, 9 working servers  
IPv6 off  
  
dcc1.dcc-servers.net,- RTT+1000 ms anon  
# 142.27.70.214,- CollegeOfNewCaledonia ID 1189  
# 100% of 1 requests ok 421.40+1000 ms RTT 116 ms queue wait  
# *194.109.153.82,- NIET ID 1080  
# 100% of 1 requests ok 155.48+1000 ms RTT 50 ms queue wait  
# 208.201.249.233,- sonic.net ID 1117  
# 100% of 1 requests ok 311.64+1000 ms RTT 102 ms queue wait  
  
dcc2.dcc-servers.net,- RTT+1000 ms anon  
# 192.84.137.21,- INFN-TO ID 1233  
# 100% of 1 requests ok 217.41+1000 ms RTT 100 ms queue wait  
# 198.137.254.147,- Misty ID 1170  
# 100% of 1 requests ok 365.83+1000 ms RTT 176 ms queue wait  
  
dcc3.dcc-servers.net,- RTT+1000 ms anon  
# 137.208.8.26,-  
# not answering  
# 208.201.249.232,- sonic.net ID 1156  
# 100% of 1 requests ok 403.05+1000 ms RTT 101 ms queue wait  
  
dcc4.dcc-servers.net,- RTT+1000 ms anon  
# 137.118.60.88,-  
# not answering  
# 203.147.165.193,- MessageCare ID 1108  
# protocol version 4  
# 100% of 2 requests ok 585.42+1000+2000 ms RTT 116 ms queue wait  
  
dcc5.dcc-servers.net,- RTT+1000 ms anon  
# 80.69.8.186,- MC ID 1128  
# protocol version 4  
# 100% of 1 requests ok 289.34+1000+2000 ms RTT 100 ms queue wait  
# 212.203.14.116,- EATSERVER ID 1166  
# 100% of 1 requests ok 385.48+1000 ms RTT 200 ms queue wait  
  
127.0.0.1,- RTT-1000 ms 32768 2669901009x248  
# 127.0.0.1,-  
# not answering
```

```
#####  
# 07/25/06 18:56:53 CEST GreyList /var/dcc/map  
# Re-resolve names after 20:56:53  
# 1 total, 0 working servers  
# skipping asking Greylist server 256 seconds more
```

```
127.0.0.1,-          Greylist 32768 2669901009x248  
# 127.0.0.1,6276  
#   not answering
```

Le répertoire par défaut se trouve sous **/var/dcc**. les serveurs par défaut se trouvent dans le fichier **/var/dcc/map**, il est automatiquement créé à l'installation à partir du fichier **dcc-1.3.58/homedir/map.txt**. Dans ce dernier répertoire on trouve également le fichier **whitelist**, pour avoir la syntaxe il faut jeter un coup d'oeil dans le fichier **whitecommon**.

En upgradant d'une version précédente j'ai eu droit à l'erreur suivante

```
open(/var/dcc/map): Too many open files  
open(/tmp/map1MdB2): Too many open files  
?
```

Je n'ai eu d'autres choix que de supprimer **/var/run/dcc** et de refaire un **make install**.

5.3.6 Installation de pyzor

pyzor repose sur le même principe que **razor**, c'est normal puisque le premier est issu du second et réécrit en python. Cela ne signifie pas qu'il marche exactement de la même manière en utilisant les mêmes serveurs, il a évolué différemment et les deux se complètent très bien.

pyzor s'interface également avec **spamassassin**, on le trouvera ici pyzor.sourceforge.net, on décompresse l'archive en tapant

```
tar xvfj pyzor-0.5.0.tar.bz2
```

Cela donne le répertoire **pyzor-0.5.0** dans lequel on tape

```
python setup.py build
```

On passe root, on installe d'abord le package **libpython-devel** puis on tape

```
python setup.py install
```

et

```
chmod -R a+rX /usr/share/doc/pyzor  
chmod -R a+rX /usr/lib/python2.X/site-packages/pyzor
```

A ce niveau mettez le numéro de version de **python** qui va bien

```
chmod -R a+rX /usr/bin/pyzor /usr/bin/pyzord  
ln -s /usr/bin/python /usr/bin/python2
```

5.3.7 Configuration de spamassassin

Revenons à **SpamAssassin**, on peut générer un fichier de config interactivement à la page www.yrex.com/spam/spamconfig.php. Voilà mon fichier de configuration **v310.pre** qu'on trouvera sous **/etc/mail/spamassassin**

```
# This is the right place to customize your installation of SpamAssassin.  
#
```

```
# See 'perldoc Mail::SpamAssassin::Conf' for details of what can be
# tweaked.
#
# This file was installed during the installation of SpamAssassin 3.1.0,
# and contains plugin loading commands for the new plugins added in that
# release. It will not be overwritten during future SpamAssassin installs,
# so you can modify it to enable some disabled-by-default plugins below,
# if you so wish.
#
#####

# DCC - perform DCC message checks.
#
# DCC is disabled here because it is not open source. See the DCC
# license for more details.
#
loadplugin Mail::SpamAssassin::Plugin::DCC

# Pyzor - perform Pyzor message checks.
#
loadplugin Mail::SpamAssassin::Plugin::Pyzor

# Razor2 - perform Razor2 message checks.
#
# Razor2 is disabled here because it is not available for unlimited free
# use. It is currently free for personal use, subject to capacity
# constraints. See the Cloudmark SpamNet Service Policy for more details.
#
loadplugin Mail::SpamAssassin::Plugin::Razor2

# SpamCop - perform SpamCop message reporting
#
loadplugin Mail::SpamAssassin::Plugin::SpamCop

# AntiVirus - some simple anti-virus checks, this is not a replacement
# for an anti-virus filter like Clam AntiVirus
#
loadplugin Mail::SpamAssassin::Plugin::AntiVirus

# AWL - do auto-whitelist checks
#
loadplugin Mail::SpamAssassin::Plugin::AWL

# AutoLearnThreshold - threshold-based discriminator for Bayes auto-learning
#
loadplugin Mail::SpamAssassin::Plugin::AutoLearnThreshold

# TextCat - language guesser
#
loadplugin Mail::SpamAssassin::Plugin::TextCat

# AccessDB - lookup from-addresses in access database
#
loadplugin Mail::SpamAssassin::Plugin::AccessDB

# WhitelistSubject - Whitelist/Blacklist certain subject regular expressions
#
loadplugin Mail::SpamAssassin::Plugin::WhiteListSubject

#####
# experimental plugins

# DomainKeys - perform DomainKeys verification
```

```
#
# External modules required for use, see INSTALL for more information.
#
#loadplugin Mail::SpamAssassin::Plugin::DomainKeys

# MIMEHeader - apply regexp rules against MIME headers in the message
#
loadplugin Mail::SpamAssassin::Plugin::MIMEHeader

# ReplaceTags
#
loadplugin Mail::SpamAssassin::Plugin::ReplaceTags
```

et voilà mon fichier **local.cf**

```
required_score 4.0
```

```
bayes_path /var/spool/mail/.spamassassin/bayes
```

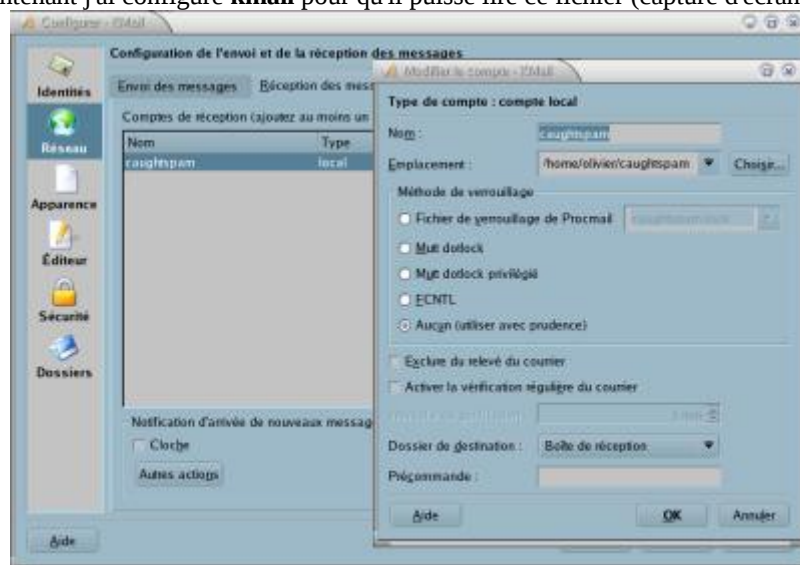
A noter le chemin **bayes_path** on doit mettre ici le chemin où sera stockée la base de données du filtrage bayésien, comme c'est l'utilisateur **mail** qui est propriétaire du process et que sa homedirectory est fixée à **/var/spool/mail**, j'ai fixé la variable pour pointer vers cet endroit. Si vous voulez placer ces fichiers ailleurs, n'oubliez pas que l'utilisateur **mail** (ou celui propriétaire du process) doit avoir les droits en accès et écriture sur le répertoire en question.

Maintenant j'ai créé un fichier **.procmailrc** sous ma homedirectory qui contient

```
:0fw: spamassassin.lock
* < 256000
| spamassassin
```

```
:0:
* ^X-Spam-Status: Yes
caughtspam
```

Tous les fichiers ayant une taille inférieure à 256000 octets passent à la moulinette **SpamAssassin**, car la plupart des spams ne dépassent pas cette taille, ceux qui sont considérés comme spams sont sauvegardés dans le fichier **caughtspam**. Maintenant j'ai configuré **kmail** pour qu'il puisse lire ce fichier (capture d'écran ci-dessous)



Maintenant si un mail venant d'un expéditeur particulier (les sites de vente par internet par exemple avec leur email bourré de HTML) est considéré comme spam alors qu'il ne devrait pas l'être. Rajoutez dans le fichier **/home/root/.spamassassin/user_prefs** la ligne

whitelist_from *@ldlc.fr *@rueducommerce.com *@fnac.com

Il faudra préalablement que vous ayez déjà utilisé **spamassassin** pour que le répertoire **/home/root/.spamassassin** existe avec tous les fichiers qu'il contient. Plus d'info sur le fichier de configuration de **SpamAssassin** à cet endroit http://spamassassin.org/doc/Mail_SpamAssassin_Conf.html
Pourquoi l'utilisateur root ? Parce que **spamassassin** cherche par défaut **user_prefs** de root et non pas le **user_prefs** de celui qui a lancé **fetchmail**. Voir plus [lien](#) pour un moyen plus élégant pour indiquer à **spamassassin** des faux spams.

ATTENTION: avec la version 3 de SpamAssassin le format de la base bayésienne a légèrement évolué, la mise à jour est faite automatiquement, mais vous pouvez la forcer manuellement en tapant en tant que root

sa-learn --sync

voilà ce que peut donner le résultat

bayes: synced databases from journal in 0 seconds: 1244 unique entries (2102 total entries)

A noter que j'ai du dans le répertoire **/var/spool/mail/.spamassassin** remettre l'utilisateur **mail** propriétaire de tous les fichiers, sinon dans le fichier **/var/log/mail/info** j'avais l'erreur suivante

**Oct 2 08:56:32 tosh spamd[25524]: debug: bayes: 25524 tie-ing to DB file R/O
/var/spool/mail/.spamassassin/bayes_toks**

**Oct 2 08:56:32 tosh spamd[25524]: Cannot open bayes databases /var/spool/mail/.spamassassin/bayes_*
R/O: tie failed: Permission denied**

Attention sous ubuntu le répertoire **/var/spool/mail/.spamassassin** doit avoir comme proprio **mail** (groupe **mail**)

5.3.8 Interfaçage avec sendmail

Spamassassin s'interface facilement avec **sendmail**, le filtrage s'opère aussi bien à la réception qu'à l'envoi d'email de manière totalement transparente ou presque, car il faut savoir que **spamassassin** est assez gourmand en ressource et que ça ralentit beaucoup la réception et l'envoi de mails.

On va récupérer ensuite une "rustine" pour que **spamassassin** puisse s'interfacer avec **sendmail** sur le site <http://savannah.nongnu.org/projects/spamass-milt>. Avant d'aller plus loin, il faudra installer le package **sendmail-devel** (package **libmilter-dev** sous ubuntu) si ce n'est pas déjà fait. On décompresse l'archive en tapant

tar xvfz spamass-milter-0.3.1.tar.gz

Cela donne le répertoire **spamass-milter-0.3.1** dans le quel on tape successivement

**./configure
make**

Puis en tant que root

make install

/usr/local/local/bin/spamd

Tout d'abord on doit lancer le daemon **spamassassin** en tant que root

spamd -d -D -u mail -H /var/spool/mail

-d mode daemon
-D mode debug (optionnel, utile au tout début)
-u mail l'utilisateur mail sera propriétaire du process.
-H le répertoire où se trouve la base de données bayésienne

Toujours en tant que root on lance **spamass-milter** en tapant

spamass-milter -u mail -p /var/run/spamass.sock -f

On modifie à présent le fichier de configuration de **sendmail**, en supposant qu'il soit sous **/usr/share/sendmail-cf/cf** (sous **/etc/mail** sous ubuntu) et qu'il s'appelle **config.mc**

```
cd /usr/share/sendmail-cf/cf
```

On rajoute à la fin les lignes suivantes

```
INPUT_MAIL_FILTER(`spamassassin', `S=local:/var/run/spamass.sock, F=,
T=C:15m;S:4m;R:4m;E:10m')dnl
define(`confINPUT_MAIL_FILTERS', `spamassassin')
```

On relance **sendmail**

sous Mandriva

```
/etc/rc.d/init.d/sendmail stop
m4 /usr/share/sendmail-cf/cf/config.mc > /etc/mail/sendmail.cf
sendmail -bd -os
```

sous ubuntu

```
sudo /etc/init.d/sendmail stop
sudo m4 /etc/mail/config.mc > /etc/mail/sendmail.cf
sendmail -bd -os
```

5.3.9 Lancement automatique

Pour une Mandriva

Pour un lancement automatique de **spamd** et **spamass-milter** on créera le fichier **/etc/rc.d/init.d/spamd**

```
#!/bin/bash
#
# crond Start/Stop spamd daemon.
#
# chkconfig: 2345 90 60
# description: lancement auto de spamd et spamass-milter
# processname: spamd et spamass-milter
# config: /etc/mail/spamassassin/local.cf
# pidfile: /var/lock/subsys/spamd et spamass-milter

# Source function library.
. /etc/init.d/functions

RETVAL=0

# See how we were called.

prog="spamd"
milter="spamass-milter"

progdir="/usr/local/bin"
progdir2="/usr/local/sbin"

start() {
    echo -n $"Starting $prog: "
    daemon $progdir/$prog -d -u mail -H /var/spool/mail
    RETVAL1=$?
    echo
    [ $RETVAL1 -eq 0 ] && touch /var/lock/subsys/spamd
    echo -n $"Starting $milter: "
```

```

daemon $progr2/$milter -u mail -p /var/run/spamass.sock -f
RETVAL=$?
echo
[ $RETVAL -eq 0 ] && touch /var/lock/subsys/spamass-milter
return $RETVAL1
}

stop() {
echo -n "$Stopping $prog: "
killproc $prog
RETVAL1=$?
echo
[ $RETVAL1 -eq 0 ] && rm -f /var/lock/subsys/spamd && rm -f /var/run/spamass.sock
echo -n "$Stopping $milter: "
killproc $milter
RETVAL=$?
echo
[ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/spamass-milter
return $RETVAL
}

restart() {
stop
start
}

case "$1" in
start)
start
;;
stop)
stop
;;
restart)
restart
;;
*)
echo "$Usage: $0 {start|stop|restart}"
exit 1
esac

exit $?

```

On lui donne des droits d'exécution

```
chmod 755 /etc/rc.d/init.d/spamd
```

Pour un lancement automatique à l'état de marche 3, 4 et 5

```
chkconfig --level 345 spamd on
```

Et un arrêt aux autres états de marche on tapera

```
chkconfig --level 0126 spamd off
```

Pour une ubuntu

Pour un lancement automatique de **spamd** et **spamass-milter** on créera le fichier **/etc/init.d/spamd**

```

#!/bin/bash
#
# crond Start/Stop spamd daemon.
#

```

```

# description: lancement auto de spamd et spamass-milter
# processname: spamd et spamass-milter
# config: /etc/mail/spamassassin/local.cf
# pid /var/lock/spamd et spamass-milter

# Source function library.
. /lib/lsb/init-functions

RETVAL=0

# See how we were called.

prog="/usr/local/bin/spamd"
milter="/usr/local/sbin/spamass-milter"

OPTIONS1='-d -u mail -H /var/spool/mail'
OPTIONS2='-u mail -p /var/run/spamass.sock -f'

start() {
    echo -n "$Starting $prog: "
    start-stop-daemon --start --quiet --pidfile /var/run/spamd.pid --oknodo --exec $prog -- $OPTIONS1
    RETVAL1=$?
    echo
    [ $RETVAL1 -eq 0 ] && touch /var/lock/spamd
    echo -n "$Starting $milter: "
    start-stop-daemon --start --quiet --pidfile /var/run/spamass-milter.pid --oknodo --exec $milter --
    $OPTIONS2
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/spamass-milter
    return $RETVAL1
}

stop() {
    echo -n "$Stopping $prog: "
    start-stop-daemon --stop --quiet --oknodo --pidfile /var/run/spamd.pid
    RETVAL1=$?
    echo
    rm -f /var/lock/spamd && rm -f /var/run/spamass.sock
    echo -n "$Stopping $milter: "
    start-stop-daemon --stop --quiet --oknodo --pidfile /var/run/spamass-milter.pid
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/spamass-milter
    return $RETVAL
}

restart() {
    stop
    start
}

case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart)
        restart
        ;;
    *)

```

```

    echo $"Usage: $0 {start|stop|restart}"
    exit 1
esac

exit $?

```

Pour que le lancement soit effectif au démarrage à l'état de marche 2, 3, 4 et 5 on tapera

```
sudo update-rc.d spamd start 20 2 3 4 5 . stop 20 0 1 6 .
```

5.3.10 Fonctionnement

Voilà c'est fait, plus besoin de modifier le fichier **.procmailrc** (il peut être vide) **sendmail** va s'en charger pour vous en amont.

J'ai eu un soucis quand je récupérais les mails de mes utilisateurs, l'utilisateur mail ne pouvant créer de fichier dans leur homedirectory

```

Oct 2 09:58:53 tosh spamd[1676]: debug: open of AWL file failed: lock: 1676 cannot create tmp
lockfile                /home/olivier/.spamassassin/auto-whitelist.lock.tosh.kervao.fr.1676      for
/home/olivier/.spamassassin/auto-whitelist.lock: Permission denied

```

Pour résoudre cela, le répertoire **.spamassassin** de tous mes utilisateurs (à créer éventuellement) appartient à l'utilisateur mail. Pour info AWL (autowhitelist) permet de mettre un score aux adresses email que vous utilisez le plus pour mieux démarquer vos interlocuteurs habituels et les autres. L'AWL est activé par défaut, pour le désactiver dans le fichier **/etc/mail/spamassassin/local.cf** il suffit de rajouter la ligne

```
use_auto_whitelist 0
```

Voilà ce que donne le fichier **/var/log/mail/info** avec un lancement en mode debug du daemon **spamd**

```

ul 13 21:20:31 mana spamd[30535]: spamd: server started on port 783/tcp (running version 3.2.5)
Jul 13 21:20:32 mana spamd[30535]: spamd: server pid: 30535
Jul 13 21:20:32 mana spamd[30535]: spamd: server successfully spawned child process, pid 30557
Jul 13 21:20:32 mana spamd[30535]: spamd: server successfully spawned child process, pid 30558
Jul 13 21:20:32 mana spamd[30535]: prefork: child states: II
Jul 13 21:21:02 mana dovecot: pop3-login: Login: user=<olivier>, method=PLAIN, rip=192.168.2.10, lip=192.168.2.11
Jul 13 21:21:02 mana dovecot: POP3(olivier): Disconnected: Logged out top=0/0, retr=0/0, del=0/9, size=877451
Jul 13 21:22:06 mana spamass-milter[30545]: SpamAssassin: mi_stop=1
Jul 13 21:22:08 mana spamd[30703]: logger: successfully added syslog method
Jul 13 21:22:08 mana spamd[30703]: spamd: will perform setuids? 0
Jul 13 21:22:08 mana spamd[30703]: spamd: creating INET socket:
Jul 13 21:22:09 mana spamd[30703]: spamd: Listen: 128
Jul 13 21:22:09 mana spamd[30703]: spamd: LocalAddr: 127.0.0.1
Jul 13 21:22:09 mana spamd[30703]: spamd: LocalPort: 783
Jul 13 21:22:09 mana spamd[30703]: spamd: Proto: 6
Jul 13 21:22:10 mana spamd[30703]: spamd: ReuseAddr: 1
Jul 13 21:22:10 mana spamd[30703]: spamd: Type: 1
Jul 13 21:22:10 mana spamd[30703]: logger: adding facilities: all
Jul 13 21:22:11 mana spamd[30703]: logger: logging level is DBG
Jul 13 21:22:11 mana spamd[30703]: generic: SpamAssassin version 3.2.5
Jul 13 21:22:11 mana spamd[30703]: config: score set 0 chosen.
Jul 13 21:22:11 mana spamd[30703]: dns: is Net::DNS::Resolver available? yes
Jul 13 21:22:12 mana spamd[30703]: dns: Net::DNS version: 0.65
Jul 13 21:22:12 mana spamd[30703]: logger: removing stderr method
Jul 13 21:22:12 mana spamd[30709]: spamd: successfully daemonized
Jul 13 21:22:12 mana spamd[30709]: spamd: Preloading modules with HOME=/tmp/spamd-30709-init
Jul 13 21:22:13 mana spamd[30709]: ignore: test message to precompile patterns and load modules
Jul 13 21:22:13 mana spamd[30709]: config: using "/etc/mail/spamassassin" for site rules pre files
Jul 13 21:22:13 mana spamd[30709]: config: read file /etc/mail/spamassassin/init.pre
Jul 13 21:22:13 mana spamd[30709]: config: read file /etc/mail/spamassassin/v310.pre
Jul 13 21:22:14 mana spamd[30709]: config: read file /etc/mail/spamassassin/v312.pre
Jul 13 21:22:14 mana spamd[30709]: config: read file /etc/mail/spamassassin/v320.pre
Jul 13 21:22:14 mana spamd[30709]: config: using "/usr/local/share/spamassassin" for sys rules pre files
Jul 13 21:22:14 mana spamd[30709]: config: using "/usr/local/share/spamassassin" for default rules dir
Jul 13 21:22:15 mana spamd[30709]: config: read file /usr/local/share/spamassassin/10_default_prefs.cf
Jul 13 21:22:15 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_advance_fee.cf
Jul 13 21:22:15 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_body_tests.cf
Jul 13 21:22:15 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_compensate.cf
Jul 13 21:22:16 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_dnsbl_tests.cf
Jul 13 21:22:16 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_drugs.cf
Jul 13 21:22:16 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_dynrdns.cf
Jul 13 21:22:16 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_fake_helo_tests.cf
Jul 13 21:22:17 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_head_tests.cf
Jul 13 21:22:17 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_html_tests.cf
Jul 13 21:22:17 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_imageinfo.cf

```

Jul 13 21:22:17 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_meta_tests.cf
 Jul 13 21:22:18 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_net_tests.cf
 Jul 13 21:22:18 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_phrases.cf
 Jul 13 21:22:18 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_porn.cf
 Jul 13 21:22:18 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_ratware.cf
 Jul 13 21:22:19 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_uri_tests.cf
 Jul 13 21:22:19 mana spamd[30709]: config: read file /usr/local/share/spamassassin/20_vbounce.cf
 Jul 13 21:22:19 mana spamd[30709]: config: read file /usr/local/share/spamassassin/23_bayes.cf
 Jul 13 21:22:19 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_accessdb.cf
 Jul 13 21:22:20 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_antivirus.cf
 Jul 13 21:22:20 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_asn.cf
 Jul 13 21:22:20 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_dcc.cf
 Jul 13 21:22:20 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_dkim.cf
 Jul 13 21:22:21 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_domainkeys.cf
 Jul 13 21:22:21 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_hashcash.cf
 Jul 13 21:22:21 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_pyzor.cf
 Jul 13 21:22:21 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_razor2.cf
 Jul 13 21:22:22 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_replace.cf
 Jul 13 21:22:22 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_spf.cf
 Jul 13 21:22:22 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_textcat.cf
 Jul 13 21:22:22 mana spamd[30709]: config: read file /usr/local/share/spamassassin/25_uribl.cf
 Jul 13 21:22:23 mana spamd[30709]: config: read file /usr/local/share/spamassassin/30_text_de.cf
 Jul 13 21:22:23 mana spamd[30709]: config: read file /usr/local/share/spamassassin/30_text_fr.cf
 Jul 13 21:22:23 mana spamd[30709]: config: read file /usr/local/share/spamassassin/30_text_it.cf
 Jul 13 21:22:23 mana spamd[30709]: config: read file /usr/local/share/spamassassin/30_text_nl.cf
 Jul 13 21:22:24 mana spamd[30709]: config: read file /usr/local/share/spamassassin/30_text_pl.cf
 Jul 13 21:22:24 mana spamd[30709]: config: read file /usr/local/share/spamassassin/30_text_pt_br.cf
 Jul 13 21:22:24 mana spamd[30709]: config: read file /usr/local/share/spamassassin/50_scores.cf
 Jul 13 21:22:24 mana spamd[30709]: config: read file /usr/local/share/spamassassin/60_awl.cf
 Jul 13 21:22:25 mana spamd[30709]: config: read file /usr/local/share/spamassassin/60_shortcircuit.cf
 Jul 13 21:22:25 mana spamd[30709]: config: read file /usr/local/share/spamassassin/60_whitelist.cf
 Jul 13 21:22:25 mana spamd[30709]: config: read file /usr/local/share/spamassassin/60_whitelist_dk.cf
 Jul 13 21:22:25 mana spamd[30709]: config: read file /usr/local/share/spamassassin/60_whitelist_dkim.cf
 Jul 13 21:22:26 mana spamd[30709]: config: read file /usr/local/share/spamassassin/60_whitelist_spf.cf
 Jul 13 21:22:26 mana spamd[30709]: config: read file /usr/local/share/spamassassin/60_whitelist_subject.cf
 Jul 13 21:22:26 mana spamd[30709]: config: read file /usr/local/share/spamassassin/72_active.cf
 Jul 13 21:22:26 mana spamd[30709]: config: read file /usr/local/share/spamassassin/72_removed.cf
 Jul 13 21:22:27 mana spamd[30709]: config: using "/etc/mail/spamassassin" for site rules dir
 Jul 13 21:22:27 mana spamd[30709]: config: read file /etc/mail/spamassassin/local.cf
 Jul 13 21:22:27 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::URIDNSBL from @INC
 Jul 13 21:22:27 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::Hashcash from @INC
 Jul 13 21:22:28 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::SPF from @INC
 Jul 13 21:22:28 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::DCC from @INC
 Jul 13 21:22:28 mana spamd[30709]: dcc: network tests on, registering DCC
 Jul 13 21:22:28 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::Pyzor from @INC
 Jul 13 21:22:29 mana spamd[30709]: pyzor: network tests on, attempting Pyzor
 Jul 13 21:22:29 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::Razor2 from @INC
 Jul 13 21:22:29 mana spamd[30709]: razor2: razor2 is available, version 2.84
 Jul 13 21:22:30 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::SpamCop from @INC
 Jul 13 21:22:30 mana spamd[30709]: reporter: network tests on, attempting SpamCop
 Jul 13 21:22:30 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::AntiVirus from @INC
 Jul 13 21:22:30 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::AWL from @INC
 Jul 13 21:22:31 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::AutoLearnThreshold from @INC
 Jul 13 21:22:31 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::WhiteListSubject from @INC
 Jul 13 21:22:31 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::MIMEHeader from @INC
 Jul 13 21:22:31 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::ReplaceTags from @INC
 Jul 13 21:22:32 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::Check from @INC
 Jul 13 21:22:32 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::HTTPSMismatch from @INC
 Jul 13 21:22:32 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::URIDetail from @INC
 Jul 13 21:22:32 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::Bayes from @INC
 Jul 13 21:22:33 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::BodyEval from @INC
 Jul 13 21:22:33 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::DNSEval from @INC
 Jul 13 21:22:33 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::HTMLEval from @INC
 Jul 13 21:22:33 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::HeaderEval from @INC
 Jul 13 21:22:34 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::MIMEEval from @INC
 Jul 13 21:22:34 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::RelayEval from @INC
 Jul 13 21:22:34 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::URIEval from @INC
 Jul 13 21:22:34 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::WLBLEval from @INC
 Jul 13 21:22:35 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::VBounce from @INC
 Jul 13 21:22:35 mana spamd[30709]: plugin: loading Mail::SpamAssassin::Plugin::ImageInfo from @INC
 Jul 13 21:22:36 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::DCC, already registered
 Jul 13 21:22:36 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::Pyzor, already registered
 Jul 13 21:22:36 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::Razor2, already registered
 Jul 13 21:22:37 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::SpamCop, already registered
 Jul 13 21:22:37 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::AntiVirus, already registered
 Jul 13 21:22:37 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::AWL, already registered
 Jul 13 21:22:37 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::AutoLearnThreshold, already registered
 Jul 13 21:22:38 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::WhiteListSubject, already registered
 Jul 13 21:22:38 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::MIMEHeader, already registered
 Jul 13 21:22:38 mana spamd[30709]: plugin: did not register Mail::SpamAssassin::Plugin::ReplaceTags, already registered
 Jul 13 21:22:39 mana spamd[30709]: rules: __MO_OL_9B90B merged duplicates: __MO_OL_C65FA
 Jul 13 21:22:39 mana spamd[30709]: rules: __XM_OL_22B61 merged duplicates: __XM_OL_A842E
 Jul 13 21:22:39 mana spamd[30709]: rules: __MO_OL_07794 merged duplicates: __MO_OL_8627E __MO_OL_F3B05
 Jul 13 21:22:39 mana spamd[30709]: rules: __XM_OL_07794 merged duplicates: __XM_OL_25340 __XM_OL_3857F __XM_OL_4F240
 __XM_OL_58CB5 __XM_OL_6554A __XM_OL_812FF __XM_OL_C65FA __XM_OL_CF0C0 __XM_OL_F475E
 __XM_OL_F6D01
 Jul 13 21:22:40 mana spamd[30709]: rules: FH_MSGID_01C67 merged duplicates: __MSGID_VGA
 Jul 13 21:22:40 mana spamd[30709]: rules: FS_NEW_SOFT_UPLOAD merged duplicates: HS_SUBJ_NEW_SOFTWARE

Jul 13 21:22:40 mana spamd[30709]: rules: __FH_HAS_XMSMAIL merged duplicates: __HAS_MSMAIL_PRI
Jul 13 21:22:40 mana spamd[30709]: rules: __MO_OL_015D5 merged duplicates: __MO_OL_6554A
Jul 13 21:22:41 mana spamd[30709]: rules: __XM_OL_015D5 merged duplicates: __XM_OL_4BF4C __XM_OL_4EEDB __XM_OL_5B79A
__XM_OL_9B90B __XM_OL_ADFF7 __XM_OL_B30D1 __XM_OL_B4B40 __XM_OL_BC7E6 __XM_OL_F3B05
__XM_OL_FF5C8
Jul 13 21:22:41 mana spamd[30709]: rules: __MO_OL_91287 merged duplicates: __MO_OL_B30D1 __MO_OL_CF0C0
Jul 13 21:22:41 mana spamd[30709]: rules: KAM_STOCKOTC merged duplicates: KAM_STOCKTIP15 KAM_STOCKTIP20 KAM_STOCKTIP21
KAM_STOCKTIP4 KAM_STOCKTIP6
Jul 13 21:22:41 mana spamd[30709]: rules: __MO_OL_22B61 merged duplicates: __MO_OL_4F240 __MO_OL_ADFF7
Jul 13 21:22:42 mana spamd[30709]: rules: __MO_OL_812FF merged duplicates: __MO_OL_BC7E6
Jul 13 21:22:42 mana spamd[30709]: rules: __MO_OL_25340 merged duplicates: __MO_OL_4EEDB __MO_OL_7533E
Jul 13 21:22:42 mana spamd[30709]: rules: __MO_OL_58CB5 merged duplicates: __MO_OL_B4B40
Jul 13 21:22:42 mana spamd[30709]: rules: __DOS_HAS_ANY_URI merged duplicates: __HAS_ANY_URI
Jul 13 21:22:43 mana spamd[30709]: rules: AXB_RCVD_ZOOBSEND merged duplicates: BROKEN_RATWARE_BOM CTYPE_001C_A
DEAR_HOMEOWNER DIV_CENTER_A_HREF DRUG_RA_PRICE FM_DDDD_TIMES_2 FM_SEX_HOSTDDDD HG_HORMONE
HS_PHARMA_1 HS_UPLOADED_SOFTWARE OEBOUND STOX_RCVD_N_NN_N URIBL_RHS_ABUSE URIBL_RHS_BOGUSMX
URIBL_RHS_DSN URIBL_RHS_POST URIBL_RHS_TLD_WHOIS URIBL_RHS_WHOIS URIBL_XS_SURBL URI_L_PHP
XMAILER_MIMEOLE_OL_5E7ED XMAILER_MIMEOLE_OL_C7C33 XMAILER_MIMEOLE_OL_D03AB X_LIBRARY
YOUR_CRD_RATING
Jul 13 21:22:43 mana spamd[30709]: rules: __MO_OL_72641 merged duplicates: __MO_OL_A842E
Jul 13 21:22:43 mana spamd[30709]: rules: __MO_OL_F475E merged duplicates: __MO_OL_FF5C8
Jul 13 21:22:43 mana spamd[30709]: rules: __MO_OL_4BF4C merged duplicates: __MO_OL_F6D01
Jul 13 21:22:44 mana spamd[30709]: conf: finish parsing
Jul 13 21:22:44 mana spamd[30709]: plugin: Mail::SpamAssassin::Plugin::ReplaceTags=HASH(0x9ad98a8) implements 'finish_parsing_end', priority
0
Jul 13 21:22:44 mana spamd[30709]: replacetags: replacing tags
Jul 13 21:22:44 mana spamd[30709]: replacetags: done replacing tags
Jul 13 21:22:45 mana spamd[30709]: bayes: tie-ing to DB file R/O /var/spool/mail/spamassassin/bayes_toks
Jul 13 21:22:45 mana spamd[30709]: bayes: tie-ing to DB file R/O /var/spool/mail/spamassassin/bayes_seen
Jul 13 21:22:45 mana spamd[30709]: bayes: found bayes db version 3
Jul 13 21:22:45 mana spamd[30709]: bayes: DB journal sync: last sync: 0
Jul 13 21:22:46 mana spamd[30709]: bayes: not available for scanning, only 0 spam(s) in bayes DB < 200
Jul 13 21:22:46 mana spamd[30709]: bayes: untie-ing
Jul 13 21:22:46 mana spamd[30709]: config: score set 1 chosen.
Jul 13 21:22:46 mana spamd[30709]: message: main message type: text/plain
Jul 13 21:22:47 mana spamd[30709]: message: ---- MIME PARSER START ----
Jul 13 21:22:47 mana spamd[30709]: message: parsing normal part
Jul 13 21:22:47 mana spamd[30709]: message: ---- MIME PARSER END ----
Jul 13 21:22:47 mana spamd[30709]: plugin: Mail::SpamAssassin::Plugin::DNSEval=HASH(0x9b71ba0) implements 'check_start', priority
0
Jul 13 21:22:48 mana spamd[30709]: bayes: no dbs present, cannot tie DB R/O: /tmp/spamd-30709-init/.spamassassin/bayes_toks
Jul 13 21:22:48 mana spamd[30709]: plugin: Mail::SpamAssassin::Plugin::Check=HASH(0x9b27ee8) implements 'check_main', priority
0
Jul 13 21:22:48 mana spamd[30709]: conf: trusted_networks are not configured; it is recommended that you configure trusted_networks
manually
Jul 13 21:22:48 mana spamd[30709]: metadata: X-Spam-Relays-Trusted:
Jul 13 21:22:49 mana spamd[30709]: metadata: X-Spam-Relays-Untrusted:
Jul 13 21:22:49 mana spamd[30709]: metadata: X-Spam-Relays-Internal:
Jul 13 21:22:49 mana spamd[30709]: metadata: X-Spam-Relays-External:
Jul 13 21:22:49 mana spamd[30709]: message: no encoding detected
Jul 13 21:22:50 mana spamd[30709]: plugin: Mail::SpamAssassin::Plugin::URIDNSBL=HASH(0x9535c70) implements 'parsed_metadata', priority
0
Jul 13 21:22:50 mana spamd[30709]: dns: is_dns_available() last checked 1247512970.0 seconds ago; re-checking
Jul 13 21:22:50 mana spamd[30709]: dns: is Net::DNS::Resolver available? yes
Jul 13 21:22:50 mana spamd[30709]: dns: Net::DNS version: 0.65
Jul 13 21:22:51 mana spamd[30709]: dns: name server: 80.10.246.1, LocalAddr: 0.0.0.0
Jul 13 21:22:51 mana spamd[30709]: dns: resolver socket rx buffer size is 112640 bytes
Jul 13 21:22:51 mana spamd[30709]: dns: testing resolver nameservers: 80.10.246.1, 80.10.246.132
Jul 13 21:22:51 mana spamd[30709]: dns: trying (3) msn.com...
Jul 13 21:22:52 mana spamd[30709]: dns: looking up NS for 'msn.com'
Jul 13 21:22:52 mana spamd[30709]: dns: NS lookup of msn.com using 80.10.246.1 succeeded => DNS available (set dns_available to
override)
Jul 13 21:22:52 mana spamd[30709]: dns: name server: 80.10.246.132, LocalAddr: 0.0.0.0
Jul 13 21:22:52 mana spamd[30709]: dns: resolver socket rx buffer size is 112640 bytes
Jul 13 21:22:53 mana spamd[30709]: dns: trying (3) mit.edu...
Jul 13 21:22:53 mana spamd[30709]: dns: looking up NS for 'mit.edu'
Jul 13 21:22:53 mana spamd[30709]: dns: NS lookup of mit.edu using 80.10.246.132 succeeded => DNS available (set dns_available to
override)
Jul 13 21:22:54 mana spamd[30709]: dns: name server: 80.10.246.132, LocalAddr: 0.0.0.0
Jul 13 21:22:54 mana spamd[30709]: dns: resolver socket rx buffer size is 112640 bytes
Jul 13 21:22:54 mana spamd[30709]: dns: NS list: 80.10.246.1, 80.10.246.132
Jul 13 21:22:54 mana spamd[30709]: dns: name server: 80.10.246.1, LocalAddr: 0.0.0.0
Jul 13 21:22:55 mana spamd[30709]: dns: resolver socket rx buffer size is 112640 bytes
Jul 13 21:22:55 mana spamd[30709]: dns: is DNS available? 1
Jul 13 21:22:55 mana spamd[30709]: uridnsbl: domains to query:
Jul 13 21:22:55 mana spamd[30709]: dns: checking RBL sa-other.bondedsender.org., set bsp-untrusted
Jul 13 21:22:56 mana spamd[30709]: dns: checking RBL plus.bondedsender.org., set ssc-firsttrusted
Jul 13 21:22:56 mana spamd[30709]: dns: checking RBL combined.njabl.org., set njabl
Jul 13 21:22:56 mana spamd[30709]: dns: checking RBL bl.spamcop.net., set spamcop
Jul 13 21:22:56 mana spamd[30709]: dns: checking RBL zen.spamhaus.org., set zen-lastexternal
Jul 13 21:22:57 mana spamd[30709]: dns: checking RBL dnsbl.sorbs.net., set sorbs-lastexternal
Jul 13 21:22:57 mana spamd[30709]: dns: checking RBL dnsbl.sorbs.net., set sorbs
Jul 13 21:22:57 mana spamd[30709]: dns: checking RBL zen.spamhaus.org., set zen-lastexternal
Jul 13 21:22:57 mana spamd[30709]: dns: checking RBL sa-accredit.habeas.com., set habeas-firsttrusted
Jul 13 21:22:58 mana spamd[30709]: dns: checking RBL list.dnswl.org., set dnswl-firsttrusted
Jul 13 21:22:58 mana spamd[30709]: dns: checking RBL list.dsbl.org., set dsbl-lastexternal
Jul 13 21:22:58 mana spamd[30709]: dns: checking RBL sa-trusted.bondedsender.org., set bsp-firsttrusted
Jul 13 21:22:58 mana spamd[30709]: dns: checking RBL zen.spamhaus.org., set zen
Jul 13 21:22:59 mana spamd[30709]: dns: checking RBL iadb.isipp.com., set iadb-firsttrusted

Jul 13 21:22:59 mana spamd[30709]: check: running tests for priority: -1000
 Jul 13 21:22:59 mana spamd[30709]: rules: running head tests; score so far=0
 Jul 13 21:22:59 mana spamd[30709]: rules: compiled head tests
 Jul 13 21:23:00 mana spamd[30709]: eval: all '*From' addr: ignore@compiling.spamassassin.taint.org
 Jul 13 21:23:00 mana spamd[30709]: eval: all '*To' addr:
 Jul 13 21:23:00 mana spamd[30709]: rules: running body tests; score so far=0
 Jul 13 21:23:00 mana spamd[30709]: rules: compiled body tests
 Jul 13 21:23:01 mana spamd[30709]: rules: running uri tests; score so far=0
 Jul 13 21:23:01 mana spamd[30709]: rules: compiled uri tests
 Jul 13 21:23:01 mana spamd[30709]: rules: running rawbody tests; score so far=0
 Jul 13 21:23:01 mana spamd[30709]: rules: compiled rawbody tests
 Jul 13 21:23:02 mana spamd[30709]: rules: running full tests; score so far=0
 Jul 13 21:23:02 mana spamd[30709]: rules: compiled full tests
 Jul 13 21:23:02 mana spamd[30709]: rules: running meta tests; score so far=0
 Jul 13 21:23:02 mana spamd[30709]: rules: compiled meta tests
 Jul 13 21:23:03 mana spamd[30709]: check: running tests for priority: -950
 Jul 13 21:23:03 mana spamd[30709]: rules: running head tests; score so far=0
 Jul 13 21:23:03 mana spamd[30709]: rules: compiled head tests
 Jul 13 21:23:03 mana spamd[30709]: rules: running body tests; score so far=0
 Jul 13 21:23:04 mana spamd[30709]: rules: compiled body tests
 Jul 13 21:23:04 mana spamd[30709]: rules: running uri tests; score so far=0
 Jul 13 21:23:04 mana spamd[30709]: rules: compiled uri tests
 Jul 13 21:23:04 mana spamd[30709]: rules: running rawbody tests; score so far=0
 Jul 13 21:23:05 mana spamd[30709]: rules: compiled rawbody tests
 Jul 13 21:23:05 mana spamd[30709]: rules: running full tests; score so far=0
 Jul 13 21:23:05 mana spamd[30709]: rules: compiled full tests
 Jul 13 21:23:05 mana spamd[30709]: rules: running meta tests; score so far=0
 Jul 13 21:23:06 mana spamd[30709]: rules: compiled meta tests
 Jul 13 21:23:06 mana spamd[30709]: check: running tests for priority: -900
 Jul 13 21:23:06 mana spamd[30709]: rules: running head tests; score so far=0
 Jul 13 21:23:06 mana spamd[30709]: rules: compiled head tests
 Jul 13 21:23:07 mana spamd[30709]: rules: running body tests; score so far=0
 Jul 13 21:23:07 mana spamd[30709]: rules: compiled body tests
 Jul 13 21:23:07 mana spamd[30709]: rules: running uri tests; score so far=0
 Jul 13 21:23:07 mana spamd[30709]: rules: compiled uri tests
 Jul 13 21:23:08 mana spamd[30709]: rules: running rawbody tests; score so far=0
 Jul 13 21:23:08 mana spamd[30709]: rules: compiled rawbody tests
 Jul 13 21:23:08 mana spamd[30709]: rules: running full tests; score so far=0
 Jul 13 21:23:08 mana spamd[30709]: rules: compiled full tests
 Jul 13 21:23:09 mana spamd[30709]: rules: running meta tests; score so far=0
 Jul 13 21:23:09 mana spamd[30709]: rules: compiled meta tests
 Jul 13 21:23:09 mana spamd[30709]: check: running tests for priority: -400
 Jul 13 21:23:09 mana spamd[30709]: rules: running head tests; score so far=0
 Jul 13 21:23:10 mana spamd[30709]: rules: compiled head tests
 Jul 13 21:23:10 mana spamd[30709]: rules: running body tests; score so far=0
 Jul 13 21:23:10 mana spamd[30709]: rules: compiled body tests
 Jul 13 21:23:10 mana spamd[30709]: rules: running uri tests; score so far=0
 Jul 13 21:23:11 mana spamd[30709]: rules: compiled uri tests
 Jul 13 21:23:11 mana spamd[30709]: rules: running rawbody tests; score so far=0
 Jul 13 21:23:11 mana spamd[30709]: rules: compiled rawbody tests
 Jul 13 21:23:11 mana spamd[30709]: rules: running full tests; score so far=0
 Jul 13 21:23:12 mana spamd[30709]: rules: compiled full tests
 Jul 13 21:23:12 mana spamd[30709]: rules: running meta tests; score so far=0
 Jul 13 21:23:12 mana spamd[30709]: rules: compiled meta tests
 Jul 13 21:23:12 mana spamd[30709]: check: running tests for priority: 0
 Jul 13 21:23:13 mana spamd[30709]: rules: running head tests; score so far=0
 Jul 13 21:23:13 mana spamd[30709]: rules: compiled head tests
 Jul 13 21:23:13 mana spamd[30709]: rules: ran header rule __MISSING_REF =====> got hit: "UNSET"
 Jul 13 21:23:14 mana spamd[30709]: rules: ran header rule __MSGID_OK_HOST =====> got hit: "@spamassassin_spamd_init">
 Jul 13 21:23:14 mana spamd[30709]: rules: ran header rule __MSGID_OK_DIGITS =====> got hit: "1247512932"
 Jul 13 21:23:14 mana spamd[30709]: rules: ran header rule __MSOE_MID_WRONG_CASE =====> got hit: "
 Jul 13 21:23:14 mana spamd[30709]: rules: Message-Id: "
 Jul 13 21:23:15 mana spamd[30709]: rules: ran header rule __HAS_MSGID =====> got hit: "<"
 Jul 13 21:23:15 mana spamd[30709]: rules: ran header rule __SANE_MSGID =====> got hit: "<1247512932.76911@spamassassin_spamd_init">
 Jul 13 21:23:15 mana spamd[30709]: rules: "
 Jul 13 21:23:15 mana spamd[30709]: rules: ran header rule MISSING_DATE =====> got hit: "UNSET"
 Jul 13 21:23:16 mana spamd[30709]: spf: checking to see if the message has a Received-SPF header that we can use
 Jul 13 21:23:16 mana spamd[30709]: spf: using Mail::SPF for SPF checks
 Jul 13 21:23:16 mana spamd[30709]: spf: no suitable relay for spf use found, skipping SPF-helo check
 Jul 13 21:23:16 mana spamd[30709]: spf: already checked for Received-SPF headers, proceeding with DNS based checks
 Jul 13 21:23:17 mana spamd[30709]: spf: no suitable relay for spf use found, skipping SPF check
 Jul 13 21:23:17 mana spamd[30709]: rules: ran eval rule NO_RELAYS =====> got hit (1)
 Jul 13 21:23:17 mana spamd[30709]: rules: ran eval rule __GATED_THROUGH_RCVD_REMOVER =====> got hit (1)
 Jul 13 21:23:17 mana spamd[30709]: spf: def_spf_whitelist_from: already checked spf and didn't get pass, skipping whitelist check
 Jul 13 21:23:18 mana spamd[30709]: rules: ran eval rule MISSING_HEADERS =====> got hit (1)
 Jul 13 21:23:18 mana spamd[30709]: spf: whitelist_from_spf: already checked spf and didn't get pass, skipping whitelist check
 Jul 13 21:23:18 mana spamd[30709]: rules: running body tests; score so far=1.581
 Jul 13 21:23:19 mana spamd[30709]: rules: compiled body tests
 Jul 13 21:23:19 mana spamd[30709]: rules: ran body rule __NONEMPTY_BODY =====> got hit: "I"
 Jul 13 21:23:19 mana spamd[30709]: rules: running uri tests; score so far=1.581
 Jul 13 21:23:19 mana spamd[30709]: rules: compiled uri tests
 Jul 13 21:23:20 mana spamd[30709]: eval: stock info total: 0
 Jul 13 21:23:20 mana spamd[30709]: rules: running rawbody tests; score so far=1.581
 Jul 13 21:23:20 mana spamd[30709]: rules: compiled rawbody tests
 Jul 13 21:23:20 mana spamd[30709]: rules: running full tests; score so far=1.581
 Jul 13 21:23:21 mana spamd[30709]: rules: compiled full tests

```

Jul 13 21:23:21 mana spamd[30709]: info: entering helper-app run mode
Jul 13 21:23:23 mana spamd[30709]: info: leaving helper-app run mode
Jul 13 21:23:24 mana spamd[30709]: razor2: part=0 engine=4 contested=0 confidence=0
Jul 13 21:23:24 mana spamd[30709]: razor2: results: spam? 0
Jul 13 21:23:24 mana spamd[30709]: razor2: results: engine 8, highest cf score: 0
Jul 13 21:23:24 mana spamd[30709]: razor2: results: engine 4, highest cf score: 0
Jul 13 21:23:25 mana spamd[30709]: util: current PATH is: /sbin:/usr/sbin:/bin:/usr/bin
Jul 13 21:23:25 mana spamd[30709]: util: executable for pyzor was found at /usr/bin/pyzor
Jul 13 21:23:25 mana spamd[30709]: pyzor: pyzor is available: /usr/bin/pyzor
Jul 13 21:23:25 mana spamd[30709]: info: entering helper-app run mode
Jul 13 21:23:26 mana spamd[30709]: pyzor: opening pipe: /usr/bin/pyzor check < /tmp/.spamassassin30709RB9gQ1tmp
Jul 13 21:23:26 mana spamd[30807]: util: setuid: ruid=0 euid=0
Jul 13 21:23:26 mana spamd[30709]: pyzor: [30807] finished: exit=0x0100
Jul 13 21:23:27 mana spamd[30709]: pyzor: got response: /usr/lib/python2.6/site-packages/pyzor/_init_.py:11: DeprecationWarning: the sha module is deprecated; use the hashlib module instead\n import sha\nusr/lib/python2.6/site-packages/pyzor/client.py:12: DeprecationWarning: the multifile module has been deprecated since Python 2.5\n import multifile\nusr/lib/python2.6/site-packages/pyzor/_init_.py:429: DeprecationWarning: object.__init__() takes no parameters\n super(ThreadId, self).__init__(i)\npublic.pyzor.org:24441 (200, 'OK') 0 0
Jul 13 21:23:27 mana spamd[30709]: info: leaving helper-app run mode
Jul 13 21:23:27 mana spamd[30709]: pyzor: failure to parse response "/usr/lib/python2.6/site-packages/pyzor/_init_.py:11: DeprecationWarning: the sha module is deprecated; use the hashlib module instead"
Jul 13 21:23:27 mana spamd[30709]: pyzor: failure to parse response " import sha"
Jul 13 21:23:28 mana spamd[30709]: pyzor: failure to parse response "/usr/lib/python2.6/site-packages/pyzor/client.py:12: DeprecationWarning: the multifile module has been deprecated since Python 2.5"
Jul 13 21:23:28 mana spamd[30709]: pyzor: failure to parse response " import multifile"
Jul 13 21:23:28 mana spamd[30709]: pyzor: failure to parse response "/usr/lib/python2.6/site-packages/pyzor/_init_.py:429: DeprecationWarning: object.__init__() takes no parameters"
Jul 13 21:23:28 mana spamd[30709]: pyzor: failure to parse response " super(ThreadId, self).__init__(i)"
Jul 13 21:23:29 mana spamd[30709]: dcc: dccifd is not available: no r/w dccifd socket found
Jul 13 21:23:29 mana spamd[30709]: dcc: dccproc is not available: no dccproc executable found
Jul 13 21:23:29 mana spamd[30709]: dcc: dccifd and dccproc are not available, disabling DCC
Jul 13 21:23:29 mana spamd[30709]: rules: running meta tests; score so far=1.581
Jul 13 21:23:30 mana spamd[30709]: rules: compiled meta tests
Jul 13 21:23:30 mana spamd[30709]: check: running tests for priority: 500
Jul 13 21:23:30 mana spamd[30709]: dns: harvest_dnsbl_queries
Jul 13 21:23:30 mana spamd[30709]: rules: running head tests; score so far=1.581
Jul 13 21:23:31 mana spamd[30709]: rules: compiled head tests
Jul 13 21:23:31 mana spamd[30709]: rules: running body tests; score so far=1.581
Jul 13 21:23:31 mana spamd[30709]: rules: compiled body tests
Jul 13 21:23:31 mana spamd[30709]: rules: running uri tests; score so far=1.581
Jul 13 21:23:32 mana spamd[30709]: rules: compiled uri tests
Jul 13 21:23:32 mana spamd[30709]: rules: running rawbody tests; score so far=1.581
Jul 13 21:23:32 mana spamd[30709]: rules: compiled rawbody tests
Jul 13 21:23:32 mana spamd[30709]: rules: running full tests; score so far=1.581
Jul 13 21:23:33 mana spamd[30709]: rules: compiled full tests
Jul 13 21:23:33 mana spamd[30709]: rules: running meta tests; score so far=1.581
Jul 13 21:23:33 mana spamd[30709]: rules: compiled meta tests
Jul 13 21:23:33 mana spamd[30709]: check: running tests for priority: 1000
Jul 13 21:23:34 mana spamd[30709]: rules: running head tests; score so far=2.865
Jul 13 21:23:34 mana spamd[30709]: rules: compiled head tests
Jul 13 21:23:34 mana spamd[30709]: locker: safe_lock: created /tmp/spamd-30709-init/.spamassassin/auto-whitelist.lock.mana.kervao.fr.30709
Jul 13 21:23:34 mana spamd[30709]: locker: safe_lock: trying to get lock on /tmp/spamd-30709-init/.spamassassin/auto-whitelist with 0 retries
Jul 13 21:23:35 mana spamd[30709]: locker: safe_lock: link to /tmp/spamd-30709-init/.spamassassin/auto-whitelist.lock: link ok
Jul 13 21:23:35 mana spamd[30709]: auto-whitelist: tie-ing to DB file of type DB_File R/W in /tmp/spamd-30709-init/.spamassassin/auto-whitelist
Jul 13 21:23:35 mana spamd[30709]: auto-whitelist: db-based ignore@compiling.spamassassin.taint.org?ip=none scores 0/0
Jul 13 21:23:35 mana spamd[30709]: auto-whitelist: AWL active, pre-score: 2.865, autolearn score: 2.865, mean: undef, IP: undef
Jul 13 21:23:36 mana spamd[30709]: auto-whitelist: DB addr list: untie-ing and unlocking
Jul 13 21:23:36 mana spamd[30709]: auto-whitelist: DB addr list: file locked, breaking lock
Jul 13 21:23:36 mana spamd[30709]: locker: safe_unlock: unlink /tmp/spamd-30709-init/.spamassassin/auto-whitelist.lock
Jul 13 21:23:37 mana spamd[30709]: auto-whitelist: post auto-whitelist score: 2.865
Jul 13 21:23:37 mana spamd[30709]: rules: running body tests; score so far=2.865
Jul 13 21:23:37 mana spamd[30709]: rules: compiled body tests
Jul 13 21:23:37 mana spamd[30709]: rules: running uri tests; score so far=2.865
Jul 13 21:23:38 mana spamd[30709]: rules: compiled uri tests
Jul 13 21:23:38 mana spamd[30709]: rules: running rawbody tests; score so far=2.865
Jul 13 21:23:38 mana spamd[30709]: rules: compiled rawbody tests
Jul 13 21:23:38 mana spamd[30709]: rules: running full tests; score so far=2.865
Jul 13 21:23:39 mana spamd[30709]: rules: compiled full tests
Jul 13 21:23:39 mana spamd[30709]: rules: running meta tests; score so far=2.865
Jul 13 21:23:39 mana spamd[30709]: rules: compiled meta tests
Jul 13 21:23:39 mana spamd[30709]: check: is spam? score=2.865 required=4
Jul 13 21:23:40 mana spamd[30709]: check: tests=MISSING_DATE,MISSING_HEADERS,MISSING_SUBJECT,NO_RECEIVED,NO_RELAYS

Jul 13 21:23:40 mana spamd[30709]: check: subtests=_GATED_THROUGH_RCVD_REMOVER,_HAS_MSGID,_MISSING_REF,_MSGID_OK_DIGITS,_MSGID_OK_HOST,_MSOE_MID_WRONG_CASE,_NONEMPTY_BODY,_SANE_MSGID,_UNUSABLE_MSGID
Jul 13 21:23:40 mana spamd[30709]: learn: initializing learner
Jul 13 21:23:40 mana spamd[30709]: config: copying current conf to backup
Jul 13 21:23:41 mana spamd[30709]: spamd: server started on port 783/tcp (running version 3.2.5)
Jul 13 21:23:41 mana spamd[30709]: spamd: server pid: 30709
Jul 13 21:23:41 mana spamd[30824]: prefork: sysread(8) not ready, wait max 300 secs
Jul 13 21:23:41 mana spamd[30709]: spamd: server successfully spawned child process, pid 30824
Jul 13 21:23:41 mana spamd[30709]: prefork: child 30824: entering state 0
Jul 13 21:23:42 mana spamd[30709]: prefork: new lowest idle kid: none
Jul 13 21:23:42 mana spamd[30825]: prefork: sysread(9) not ready, wait max 300 secs

```

Jul 13 21:23:42 mana spamd[30709]: spamd: server successfully spawned child process, pid 30825
Jul 13 21:23:42 mana spamd[30709]: prefork: child 30825: entering state 0
Jul 13 21:23:42 mana spamd[30709]: prefork: new lowest idle kid: none
Jul 13 21:23:43 mana spamd[30709]: prefork: child 30824: entering state 1
Jul 13 21:23:43 mana spamd[30709]: prefork: new lowest idle kid: 30824
Jul 13 21:23:43 mana spamd[30709]: prefork: child reports idle
Jul 13 21:23:43 mana spamd[30709]: prefork: child 30825: entering state 1
Jul 13 21:23:44 mana spamd[30709]: prefork: new lowest idle kid: 30824
Jul 13 21:23:44 mana spamd[30709]: prefork: child reports idle
Jul 13 21:23:44 mana spamd[30709]: prefork: child states: II

A noter qu'il faut au moins 200 spams dans la base de données bayésienne pour que le filtre puisse fonctionner. Dans le cas de la mise à jour, vous pouvez très bien récupérer vos fichiers **bayes_seen** et **bayes_toks** et les placer sous **/var/spool/mail/spamassassin** avant lancement du daemon. Voilà ce que ça donne en réception d'un spam (mode debug)

```
ul 13 21:25:04 mana sendmail[30929]: n6DJP4Ik030929: from=<postmaster@voilesnews.fr>, size=104309, class=0, nrpts=1, msgid=
<20090713035446.3846.qmail@ns28408.ovh.net>, bodytype=8BITMIME, proto=ESMTP, daemon=MTA, relay=localhost [127.0.0.1]
Jul 13 21:25:05 mana spamd[30709]: prefork: ordered 30824 to accept
Jul 13 21:25:05 mana spamd[30824]: spamd: connection from localhost [127.0.0.1] at port 38543
Jul 13 21:25:05 mana spamd[30709]: prefork: child 30824: entering state 2
Jul 13 21:25:05 mana spamd[30824]: config: read_scoreonly_config: cannot open "/export/home/olivier/spamassassin/user_prefs"
: Aucun fichier ou dossier de ce type
Jul 13 21:25:05 mana spamd[30709]: prefork: new lowest idle kid: 30825
Jul 13 21:25:05 mana spamd[30824]: info: user has changed
Jul 13 21:25:05 mana spamd[30824]: bayes: tie-ing to DB file R/O /var/spool/mail/spamassassin/bayes_toks
Jul 13 21:25:06 mana spamd[30824]: bayes: tie-ing to DB file R/O /var/spool/mail/spamassassin/bayes_seen
Jul 13 21:25:06 mana spamd[30824]: bayes: found bayes db version 3
Jul 13 21:25:06 mana spamd[30824]: bayes: DB journal sync: last sync: 0
Jul 13 21:25:06 mana spamd[30824]: bayes: not available for scanning, only 0 spam(s) in bayes DB < 200
Jul 13 21:25:07 mana spamd[30824]: bayes: untie-ing
Jul 13 21:25:07 mana spamd[30824]: config: score set 1 chosen.
Jul 13 21:25:07 mana spamd[30824]: spamd: running as uid 8
Jul 13 21:25:07 mana spamd[30824]: dns: name server: 80.10.246.1, LocalAddr: 0.0.0.0
Jul 13 21:25:08 mana spamd[30824]: dns: resolver socket rx buffer size is 112640 bytes
Jul 13 21:25:08 mana spamd[30824]: message: line ending changed to CRLF
Jul 13 21:25:08 mana spamd[30824]: message: main message type: multipart/alternative
Jul 13 21:25:08 mana spamd[30824]: spamd: processing message <20090713035446.3846.qmail@ns28408.ovh.net> for olivier:8
Jul 13 21:25:09 mana spamd[30824]: bayes: tie-ing to DB file R/O /var/spool/mail/spamassassin/bayes_toks
Jul 13 21:25:09 mana spamd[30824]: bayes: tie-ing to DB file R/O /var/spool/mail/spamassassin/bayes_seen
Jul 13 21:25:09 mana spamd[30824]: bayes: found bayes db version 3
Jul 13 21:25:09 mana spamd[30824]: bayes: DB journal sync: last sync: 0
Jul 13 21:25:10 mana spamd[30824]: bayes: not available for scanning, only 0 spam(s) in bayes DB < 200
Jul 13 21:25:10 mana spamd[30824]: bayes: untie-ing
Jul 13 21:25:10 mana spamd[30824]: conf: trusted_networks are not configured; it is recommended that you configure trusted_ne
tworks manually
Jul 13 21:25:10 mana spamd[30824]: received-header: parsed as [ ip=127.0.0.1 rdns=localhost helo=mana.kervao.fr by=ppp.free.f
r!8.13.0/8.13.0 ident= envfrom=postmaster@voilesnews.fr intl=0 id=n6DJP4Ik030929 auth= msa=0 ]
Jul 13 21:25:11 mana spamd[30824]: received-header: 'from' 127.0.0.1 has private IP
Jul 13 21:25:11 mana spamd[30824]: received-header: relay 127.0.0.1 trusted? yes msa? no
Jul 13 21:25:11 mana spamd[30824]: received-header: found fetchmail marker, restarting parse
Jul 13 21:25:11 mana spamd[30824]: received-header: parsed as [ ip=91.121.94.13 rdns=91.121.94.13 helo=ns28408.ovh.net by=qma
il-6.online.net ident= envfrom= intl=0 id= auth= msa=0 ]
Jul 13 21:25:12 mana spamd[30824]: received-header: do not trust any hosts from here on
Jul 13 21:25:12 mana spamd[30824]: received-header: relay 91.121.94.13 trusted? no internal? no msa? no
Jul 13 21:25:12 mana spamd[30824]: metadata: X-Spam-Relays-Trusted:
Jul 13 21:25:12 mana spamd[30824]: metadata: X-Spam-Relays-Untrusted: [ ip=91.121.94.13 rdns=91.121.94.13 helo=ns28408.ovh.ne
t by=qmail-6.online.net ident= envfrom= intl=0 id= auth= msa=0 ]
Jul 13 21:25:13 mana spamd[30824]: metadata: X-Spam-Relays-Internal:
Jul 13 21:25:13 mana spamd[30824]: metadata: X-Spam-Relays-External: [ ip=91.121.94.13 rdns=91.121.94.13 helo=ns28408.ovh.net
by=qmail-6.online.net ident= envfrom= intl=0 id= auth= msa=0 ]
Jul 13 21:25:13 mana spamd[30824]: message: ---- MIME PARSER START ----
Jul 13 21:25:13 mana spamd[30824]: message: parsing multipart, got boundary: =_FIRST_e2225f15f9c70e85162f3e1e90936ce0
Jul 13 21:25:14 mana spamd[30824]: message: found part of type text/plain, boundary: =_FIRST_e2225f15f9c70e85162f3e1e90936ce0
Jul 13 21:25:14 mana spamd[30824]: message: added part, type: text/plain
Jul 13 21:25:14 mana spamd[30824]: message: found part of type text/html, boundary: =_FIRST_e2225f15f9c70e85162f3e1e90936ce0
Jul 13 21:25:14 mana spamd[30824]: message: added part, type: text/html
Jul 13 21:25:15 mana spamd[30824]: message: parsing normal part
Jul 13 21:25:15 mana spamd[30824]: message: parsing normal part
Jul 13 21:25:15 mana spamd[30824]: message: ---- MIME PARSER END ----
Jul 13 21:25:15 mana spamd[30824]: message: decoding base64
Jul 13 21:25:16 mana spamd[30824]: message: decoding base64
Jul 13 21:25:16 mana spamd[30824]: uridnsbl: domains to query: nautisports.com zar-formenti.com world-oceans.com helicesnews.
fr lemoussaillon.fr eyb.fr tvmer.fr voilesnews.fr windward-islands.net sailingregate.fr ruedelamer.com theglobesailor.com ski
ppers.tv streamlike.com geovoile.com plaisance-evolution.com tonysshop.fr
Jul 13 21:25:16 mana spamd[30824]: async: starting: URI-DNSBL, DNSBL:multi.uribl.com.:nautisports.com (timeout 15.0s, min 3.0
s)
Jul 13 21:25:17 mana spamd[30824]: dns: URIBL_RED lookup start
Jul 13 21:25:17 mana spamd[30824]: dns: URIBL_GREY lookup start
Jul 13 21:25:17 mana spamd[30824]: async: starting: URI-DNSBL, DNSBL:bl.open-whois.org.:nautisports.com (timeout 15.0s, min 3
.0s)
Jul 13 21:25:17 mana spamd[30824]: dns: WHOIS_SECUREWHOIS lookup start
Jul 13 21:25:18 mana spamd[30824]: dns: WHOIS_MYPRIVREG lookup start
Jul 13 21:25:18 mana spamd[30824]: dns: WHOIS_NETSOLPR lookup start
Jul 13 21:25:18 mana spamd[30824]: dns: WHOIS_AITPRIV lookup start
```

Jul 13 21:25:18 mana spamd[30824]: async: starting: URI-DNSBL, DNSBL:multi.surbl.org.:nautisports.com (timeout 15.0s, min 3.0s)
Jul 13 21:25:19 mana spamd[30824]: dns: URIBL_SC_SURBL lookup start
Jul 13 21:25:19 mana spamd[30824]: dns: URIBL_AB_SURBL lookup start
Jul 13 21:25:19 mana spamd[30824]: dns: WHOIS_CONTACTPRIV lookup start
Jul 13 21:25:19 mana spamd[30824]: dns: WHOIS_NAMEKING lookup start
Jul 13 21:25:20 mana spamd[30824]: dns: WHOIS_PRIVPROT lookup start
Jul 13 21:25:20 mana spamd[30824]: dns: WHOIS_WHOISGUARD lookup start
Jul 13 21:25:20 mana spamd[30824]: dns: URIBL_PH_SURBL lookup start
Jul 13 21:25:20 mana spamd[30824]: dns: URIBL_BLACK lookup start
Jul 13 21:25:21 mana spamd[30824]: dns: WHOIS_PRIVACYPOST lookup start
Jul 13 21:25:21 mana spamd[30824]: async: starting: URI-DNSBL, DNSBL:dob.sibl.support-intelligence.net:nautisports.com (timeout 15.0s, min 3.0s)
Jul 13 21:25:21 mana spamd[30824]: dns: URIBL_RHS_DOB lookup start
Jul 13 21:25:21 mana spamd[30824]: dns: URIBL_JP_SURBL lookup start
Jul 13 21:25:22 mana spamd[30824]: dns: URIBL_WS_SURBL lookup start

(...)

Jul 13 21:26:11 mana spamd[30824]: dns: URIBL_PH_SURBL lookup start
Jul 13 21:26:11 mana spamd[30824]: dns: URIBL_BLACK lookup start
Jul 13 21:26:12 mana spamd[30824]: dns: WHOIS_PRIVACYPOST lookup start
Jul 13 21:26:12 mana spamd[30824]: async: starting: URI-DNSBL, DNSBL:dob.sibl.support-intelligence.net:voilesnews.fr (timeout 15.0s, min 3.0s)
Jul 13 21:26:12 mana spamd[30824]: dns: URIBL_RHS_DOB lookup start
Jul 13 21:26:12 mana spamd[30824]: dns: URIBL_JP_SURBL lookup start
Jul 13 21:26:13 mana spamd[30824]: dns: URIBL_WS_SURBL lookup start
Jul 13 21:26:13 mana spamd[30824]: dns: URIBL_OB_SURBL lookup start
Jul 13 21:26:13 mana spamd[30824]: dns: WHOIS_DMNBYPROXY lookup start
Jul 13 21:26:13 mana spamd[30824]: dns: WHOIS_REGISTERFLY lookup start
Jul 13 21:26:14 mana spamd[30824]: dns: WHOIS_UNLISTED lookup start
Jul 13 21:26:14 mana spamd[30824]: dns: WHOIS_MONIKER_PRIV lookup start
Jul 13 21:26:14 mana spamd[30824]: async: starting: URI-NS, NS:voilesnews.fr (timeout 15.0s, min 3.0s)
Jul 13 21:26:14 mana spamd[30824]: dns: URIBL_SBL lookup start
Jul 13 21:26:15 mana spamd[30824]: async: starting: URI-DNSBL, DNSBL:multi.uribl.com.:windward-islands.net (timeout 15.0s, min 3.0s)
Jul 13 21:26:15 mana spamd[30824]: dns: URIBL_RED lookup start
Jul 13 21:26:15 mana spamd[30824]: dns: URIBL_GREY lookup start
Jul 13 21:26:15 mana spamd[30824]: async: starting: URI-DNSBL, DNSBL:bl.open-whois.org.:windward-islands.net (timeout 15.0s, min 3.0s)
Jul 13 21:26:16 mana spamd[30824]: dns: WHOIS_SECUREWHOIS lookup start
Jul 13 21:26:16 mana spamd[30824]: dns: WHOIS_MYPRIVREG lookup start
Jul 13 21:26:16 mana spamd[30824]: dns: WHOIS_NETSOLPR lookup start
Jul 13 21:26:16 mana spamd[30824]: dns: WHOIS_AITPRIV lookup start
Jul 13 21:26:17 mana spamd[30824]: async: starting: U

[\[Retour haut de la page\]](#)

Et voilà une partie du corps d'un spam après traitement par SpamAssassin.

Return-Path: <postmaster@voilesnews.fr>
Received: from orange.fr
by orange.fr (8.14.3/8.14.3/Sendmail de FUNIX) with ESMTP id n6E81GO4004749
for <olivier@localhost>; Tue, 14 Jul 2009 10:01:16 +0200
Delivered-To: funix.org-olivier.hoarau@funix.org
Received: from pop.online.net [88.191.253.80]
by mana.kervao.fr with POP3 (fetchmail-6.3.9)
for <olivier@localhost> (single-drop); Tue, 14 Jul 2009 10:01:16 +0200 (CEST)
Received: (qmail 6225 invoked from network); 13 Jul 2009 11:38:10 -0000
Received: from 91.121.94.13 (HELO ns28408.ovh.net) (91.121.94.13)
by qmail-6.online.net with SMTP; 13 Jul 2009 11:38:10 -0000
Received: (qmail 3847 invoked by uid 510); 13 Jul 2009 03:54:46 -0000
Date: 13 Jul 2009 03:54:46 -0000
Message-ID: <20090713035446.3846.qmail@ns28408.ovh.net>
To: "olivier.hoarau@funix.org" <olivier.hoarau@funix.org>
Subject: Voiles News : newsletter n542, Dossier : Bénéteau Océanis 58, JPK 998, Lagoon 620, Nautitech 441 et 442, système hybride Nanni Diesel, News : Grand Pavois, Bordeaux 60, So Much Yachting, Cavaledeux, Bavaria, RM, Briand Design, Sunsail, ...
From: Voiles News <newsletter@voilesnews.fr>
MIME-Version: 1.0
X-Priority: 3
Content-Type: multipart/mixed;
boundary="-----=_4A5C3B54.048479D9"
X-Virus-Scanned: ClamAV using ClamSMTP
X-Spam-Flag: YES
X-Spam-Status: Yes, score=7.5 required=4.0 tests=DATE_IN_PAST_06_12,
HTML_MESSAGE,MIME_BASE64_TEXT,SUBJECT_NEEDS_ENCODING,SUBJ_ILLEGAL_CHARS

autolearn=no version=3.2.5
X-Spam-Level: *****
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on mana.kervao.fr
Status: R
X-Status: N
X-KMail-EncryptionState:
X-KMail-SignatureState:
X-KMail-MDN-Sent:

----- Début de Rapport SpamAssassin -----
Ce message est probablement du SPAM (message non sollicité envoyé en masse, publicité, escroquerie...).

Cette notice a été ajoutée par le système d'analyse "SpamAssassin" sur votre serveur de courrier "mana.kervao.fr", pour vous aider à identifier ce type de messages.

Le système SpamAssassin ajoute un en-tête "X-Spam-Flag: YES" aux messages qu'il considère comme étant probablement du Spam. Vous pouvez si vous le souhaitez utiliser cette caractéristique pour régler un filtre dans votre logiciel de lecture de courrier, afin de détruire ou de classer à part ce type de message.

Si ce robot a classifié incorrectement un message qui vous était destiné, ou pour toute question, veuillez contacter l'administrateur du système par e-mail à olivier .

Voir <http://spamassassin.apache.org/tag/> pour plus de détails (en anglais).

Détails de l'analyse du message: (7.5 points, 4.0 requis)
1.9 DATE_IN_PAST_06_12 Date: est 6 à 12 heures avant la date de l'en-tête
Received:
1.5 SUBJ_ILLEGAL_CHARS Subject: contient trop de caractères bruts
invalides
0.0 HTML_MESSAGE BODY: HTML inclus dans le message
2.8 MIME_BASE64_TEXT RAW: Texte du message camouflé par encodage en
BASE64
1.3 SUBJECT_NEEDS_ENCODING SUBJECT_NEEDS_ENCODING

----- Fin de Rapport SpamAssassin -----

Chaque mail reçoit les informations suivantes en en tête du style

X-Spam-Flag: YES
X-Spam-Status: Yes, score=32.3 required=4.0 tests=BAYES_99,DATE_IN_PAST_06_12,

DIGEST_MULTIPLE,FORGED_MUA_OUTLOOK,HELO_LH_HOME,INVALID_MSGID,PYZOR_CHECK,

RAZOR2_CF_RANGE_51_100,RAZOR2_CF_RANGE_E4_51_100,RAZOR2_CF_RANGE_E8_51_100,
RAZOR2_CHECK,RCVD_IN_BL_SPAMCOP_NET,RCVD_IN_PBL,RCVD_IN_SORBS_DUL,

RCVD_IN_SORBS_WEB,STOX_REPLY_TYPE,URIBL_BLACK,URIBL_JP_SURBL,URIBL_OB_SURBL,

URIBL_SBL,URIBL_SC_SURBL autolearn=spam version=3.2.5

X-Spam-Level: *****
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on mana.kervao.fr

A présent vous devez aider **spamassassin** à identifier les spams en lui indiquant les mails qui auraient du être qualifiés de spam et ceux qui n'auraient pas du être identifiés comme spam. Avec **kmail** qui me sert à lire la boîte aux lettres de spam, j'ai créé un dossier fauxspams où je déplace les mails

qui n'auraient pas du être classés comme spams.

Avec **thunderbird** qui me sert à lire la boîte aux lettres des mails normaux, j'ai créé un dossier **spams** dans lequel je déplace les mails qui auraient du être classés comme spam.

Maintenant la commande à taper en tant que root pour qu'il ne prenne plus en compte les mails comme spams est la suivante

```
sa-learn --ham --dir /home/olivier/.Mail/fauxspam/cur
```

Voilà le résultat

```
Learned from 3 message(s) (3 message(s) examined).
```

La commande à taper en tant que root pour qu'il prenne en compte les mails comme spams est la suivante

```
sa-learn --spam --mbox /home/olivier/.thunderbird/ent0h7vk.default/Mail/asterix/spams
```

Vous adapterez en fonction du chemin du dit fichier. Voilà le résultat

```
Learned from 1 message(s) (1 message(s) examined).
```

Pour automatiser tout cela vous pouvez créer le fichier **/etc/cron.daily/bayes** contenant

```
#!/bin/bash
sa-learn --ham --dir /home/olivier/.Mail/fauxspam/cur
sa-learn --spam --mbox /home/olivier/.thunderbird/ent0h7vk.default/Mail/asterix/spams
```

Et lui donner des droits en exécution

```
chmod 755 /etc/cron.daily/bayes
```

A noter que le traitement de certains messages peut échouer avec l'erreur suivante

```
Parsing of undecoded UTF-8 will give garbage when decoding entities at
/usr/local/lib/perl5/site_perl/5.8.6/Mail/SpamAssassin/HTML.pm line 182.
```

Il semblerait que ce soit un bogue, on espère qu'il soit corrigé vite fait.

5.4 Mettre en place un anti virus

5.4.1 Présentation et installation

Clam Anti virus (clamav) comme son nom l'indique est un anti virus qui est totalement libre, le site officiel est <http://www.clamav.net/> on y récupérera l'archive qu'on décompresse en tapant

```
tar xvfz clamav-0.95.3.tar.gz
```

Cela donne **clamav-0.95.3** avant d'aller plus loin vous pouvez récupérer la très bonne documentation disponible à cet endroit <http://wiki.clamav.net/Main/WebHome>. En suivant les instructions on doit d'abord en tant que root créer un utilisateur **clamav**

```
groupadd clamav
useradd -g clamav -s /bin/false -c "Clam Anti Virus" clamav
```

Ensuite en tant que simple utilisateur dans le répertoire **clamav-0.95.3** on doit taper

```
./configure --sysconfdir=/etc --enable-milter
```

L'option **sysconfdir** permet de retrouver le fichier de configuration sous **/etc**, l'option **enable-milter** est nécessaire si vous utilisez **sendmail**, attention dans ce dernier cas, installez le package **sendmail-devel** (package **libmilter-dev** sous ubuntu) omettez cette dernière option si vous n'utilisez pas **sendmail**. Il se peut qu'il se plaint que vous ayez une version trop ancienne de **zlib** (c'est le cas avec une Mdk 10.1), dans ce cas upgradez (conseillé) ou rajoutez comme option **--disable-zlib-vcheck** (non conseillé).

sous mandriva il faudra install **zlib-devel** et sous ubuntu vous devez installer le package suivant **zlib1g-dev**

On tape ensuite sous **clamav-0.95.3**

make

Puis en tant que root

make install

On rajoute si ce n'est déjà fait la ligne **/usr/local/lib** dans le fichier **/etc/ld.so.conf** et on tape

ldconfig

Maintenant on crée le répertoire de log de **clamav**, l'utilisateur **clamav** doit en être propriétaire

```
mkdir /var/log/clamav
chown clamav:clamav /var/log/clamav
```

5.4.2 Configuration

On édite le fichier **/etc/clamd.conf** voici comment je l'ai configuré

```
##
## Example config file for the Clam AV daemon
## Please read the clamd.conf(5) manual before editing this file.
##

# Comment or remove the line below.
#Example

# Uncomment this option to enable logging.
# LogFile must be writable for the user running daemon.
# A full path is required.
# Default: disabled
LogFile /var/log/clamav/clamd.log

# By default the log file is locked for writing - the lock protects against
# running clamd multiple times (if want to run another clamd, please
# copy the configuration file, change the LogFile variable, and run
# the daemon with --config-file option).
# This option disables log file locking.
# Default: disabled
#LogFileUnlock

# Maximal size of the log file.
# Value of 0 disables the limit.
# You may use 'M' or 'm' for megabytes (1M = 1m = 1048576 bytes)
# and 'K' or 'k' for kilobytes (1K = 1k = 1024 bytes). To specify the size
# in bytes just don't use modifiers.
# Default: 1M
LogFileMaxSize 2M

# Log time with each message.
# Default: disabled
LogTime yes

# Also log clean files. Useful in debugging but drastically increases the
# log size.
# Default: disabled
```

LogClean yes

Use system logger (can work together with LogFile).
Default: disabled
#LogSyslog

Specify the type of syslog messages - please refer to 'man syslog'
for facility names.
Default: LOG_LOCAL6
#LogFacility LOG_MAIL

Enable verbose logging.
Default: disabled
LogVerbose yes

This option allows you to save a process identifier of the listening
daemon (main thread).
Default: disabled
PidFile /var/log/clamav/clamd.pid

Optional path to the global temporary directory.
Default: system specific (usually /tmp or /var/tmp).
TemporaryDirectory /tmp

Path to the database directory.
Default: hardcoded (depends on installation options)
DatabaseDirectory /usr/local/share/clamav

The daemon works in a local OR a network mode. Due to security reasons we
recommend the local mode.

Path to a local socket file the daemon will listen on.
Default: disabled
LocalSocket /var/log/clamav/clamd.sock

Remove stale socket after unclean shutdown.
Default: disabled
FixStaleSocket yes

TCP port address.
Default: disabled
#TCPSocket 3310

TCP address.
By default we bind to INADDR_ANY, probably not wise.
Enable the following to provide some degree of protection
from the outside world.
Default: disabled
TCPAddr 127.0.0.1

Maximum length the queue of pending connections may grow to.
Default: 15
#MaxConnectionQueueLength 30

Close the connection if this limit is exceeded.
Default: 10M
#StreamMaxLength 20M

Maximal number of threads running at the same time.
Default: 10
MaxThreads 20

Waiting for data from a client socket will timeout after this time (seconds).

Value of 0 disables the timeout.
Default: 120
ReadTimeout 120

Waiting for a new job will timeout after this time (seconds).
Default: 30
#IdleTimeout 60

Maximal depth directories are scanned at.
Default: 15
#MaxDirectoryRecursion 20

Follow directory symlinks.
Default: disabled
#FollowDirectorySymlinks

Follow regular file symlinks.
Default: disabled
#FollowFileSymlinks

Perform internal sanity check (database integrity and freshness).
Default: 1800 (30 min)
#SelfCheck 600

Execute a command when virus is found. In the command string %v will
be replaced by a virus name.
Default: disabled
#VirusEvent /usr/local/bin/send_sms 123456789 "VIRUS ALERT: %v"

Run as a selected user (clamd must be started by root).
Default: disabled
User clamav

Initialize supplementary group access (clamd must be started by root).
Default: disabled
#AllowSupplementaryGroups

Don't fork into background.
Default: disabled
#Foreground

Enable debug messages in libclamav.
Default: disabled
#Debug

Do not remove temporary files (for debug purposes).
Default: disabled
#LeaveTemporaryFiles

By default clamd uses scan options recommended by libclamav. This option
disables recommended options and allows you to enable selected ones below.
DO NOT TOUCH IT unless you know what you are doing.
Default: disabled
#DisableDefaultScanOptions

##
Executable files
##

PE stands for Portable Executable - it's an executable file format used
in all 32-bit versions of Windows operating systems. This option allows
ClamAV to perform a deeper analysis of executable files and it's also

**# required for decompression of popular executable packers such as UPX, FSG,
and Petite.
Default: enabled
ScanPE yes**

**# With this option clamav will try to detect broken executables and mark
them as Broken.Executable
Default: disabled
DetectBrokenExecutables yes**

**##
Documents
##**

**# This option enables scanning of Microsoft Office document macros.
Default: enabled
ScanOLE2 yes**

ScanPDF yes

**##
Mail files
##**

**# Enable internal e-mail scanner.
Default: enabled
ScanMail yes**

**# If an email contains URLs ClamAV can download and scan them.
WARNING: This option may open your system to a DoS attack.
Never use it on loaded servers.
Default: disabled
#MailFollowURLs**

PhishingSignatures yes

**##
HTML
##**

**# Perform HTML normalisation and decryption of MS Script Encoder code.
Default: enabled
ScanHTML yes**

**##
Archives
##**

**# ClamAV can scan within archives and compressed files.
Default: enabled
ScanArchive yes**

**# Due to license issues libclamav does not support RAR 3.0 archives (only the
old 2.0 format is supported). Because some users report stability problems
with unrarlib it's disabled by default and you must uncomment the directive
below to enable RAR 2.0 support.
Default: disabled
#ScanRAR**

**# The options below protect your system against Denial of Service attacks
using archive bombs.**

```
# Files in archives larger than this limit won't be scanned.
# Value of 0 disables the limit.
# Default: 10M
#ArchiveMaxFileSize 15M

# Nested archives are scanned recursively, e.g. if a Zip archive contains a RAR
# file, all files within it will also be scanned. This options specifies how
# deep the process should be continued.
# Value of 0 disables the limit.
# Default: 5
#ArchiveMaxRecursion 8

# Number of files to be scanned within an archive.
# Value of 0 disables the limit.
# Default: 1000
#ArchiveMaxFiles 1500

# If a file in an archive is compressed more than ArchiveMaxCompressionRatio
# times it will be marked as a virus (Oversized.ArchiveType, e.g. Oversized.Zip)
# Value of 0 disables the limit.
# Default: 250
#ArchiveMaxCompressionRatio 300

# Use slower but memory efficient decompression algorithm.
# only affects the bzip2 decompressor.
# Default: disabled
#ArchiveLimitMemoryUsage

# Mark encrypted archives as viruses (Encrypted.Zip, Encrypted.RAR).
# Default: disabled
#ArchiveBlockEncrypted

# Mark archives as viruses if ArchiveMaxFiles, ArchiveMaxFileSize, or
# ArchiveMaxRecursion limit is reached.
# Default: disabled
#ArchiveBlockMax

##
## Clamuko settings
## WARNING: This is experimental software. It is very likely it will hang
## up your system!!!
##

# Enable Clamuko. Dazuko (/dev/dazuko) must be configured and running.
# Default: disabled
#ClamukoScanOnAccess

# Set access mask for Clamuko.
# Default: disabled
#ClamukoScanOnOpen
#ClamukoScanOnClose
#ClamukoScanOnExec

# Set the include paths (all files in them will be scanned). You can have
# multiple ClamukoIncludePath directives but each directory must be added
# in a seperate line.
# Default: disabled
#ClamukoIncludePath /home
#ClamukoIncludePath /students

# Set the exclude paths. All subdirectories are also excluded.
```

```
# Default: disabled
#ClamukoExcludePath /home/guru
```

```
# Don't scan files larger than ClamukoMaxFileSize
# Value of 0 disables the limit.
# Default: 5M
#ClamukoMaxFileSize 10M
```

A noter qu'il existe une extension nommée **Clamuko** (pour faire un scan en temps réel des fichiers), il est cependant conseillé de ne pas l'utiliser sur un serveur en production, j'ai choisi pour l'instant de ne pas m'en occuper.

Le fichier de configuration de **clamav-milter** s'appelle **/etc/clamav-milter.conf** le voici, voilà les lignes que j'ai modifiées

```
#example
```

```
MilterSocket /var/log/clamav/clmilter.sock
```

```
ClamdSocket unix:/var/log/clamav/clamd.sock
```

```
AddHeader Replace
```

```
LogFile /var/log/clamav/clamav-milter.log
```

pour le reste tout est en commentaire

On configure maintenant le fichier **/etc/freshclam.conf** en mettant en commentaire la ligne suivante

```
#Example
```

Puis en modifiant la ligne suivante conformément à ce qui a été défini dans le fichier **clamd.conf**

```
# définition de la base des données des virus
DatabaseDirectory /usr/local/share/clamav
```

J'ai modifié ensuite les lignes suivantes

```
# définition du fichier de log de freshclam
UpdateLogFile /var/log/clamav/freshclam.log
```

```
# serveur miroir à contacter pour récupérer les mises à jour
DatabaseMirror db.fr.clamav.net
```

```
# database.clamav.net is a round-robin record which points to our most
# reliable mirrors. It's used as a fall back in case db.XY.clamav.net is
# not working. DO NOT TOUCH the following line unless you know what you
# are doing.
DatabaseMirror database.clamav.net
```

5.4.3 Premiers tests

On lance maintenant **clamd** en tant que root

```
clamd
```

On va faire un test maintenant sur le répertoire **clamav-0.95.3** en tant que simple utilisateur

```
clamscan -r -l log.txt clamav-0.95.3
```

L'option **-r** permet d'avoir une recherche récursive (à travers le répertoire et ses sous répertoires), **-l** pour logger dans le fichier **log.txt**. Voilà un extrait du contenu du dit-fichier après l'exécution de la commande

----- SCAN SUMMARY -----

Known viruses: 147235
Engine version: 0.91.1
Scanned directories: 56
Scanned files: 924
Infected files: 6
Data scanned: 47.14 MB
Time: 15.928 sec (0 m 15 s)

Il y a des virus qui ont été volontairement placés dans ce répertoire pour mener des essais. Pour scanner le répertoire de mail `/var/spool/mail` il faudra être root et rajouter l'option `--mbox`.

La commande `freshclam` permet de mettre à jour la base de données à partir d'informations récupérées sur internet, en tant que root tapez `freshclam` voilà le résultat:

```
ClamAV update process started at Thu Mar 8 18:51:39 2007
SECURITY WARNING: NO SUPPORT FOR DIGITAL SIGNATURES
See the FAQ at http://www.clamav.net/support/faq for an explanation.
main.cvd is up to date (version: 42, sigs: 83951, f-level: 10, builder: tkojm)
Downloading daily-2778.cdiff [100%]
Downloading daily-2779.cdiff [100%]
daily.cvd updated (version: 2779, sigs: 13408, f-level: 14, builder: arnaud)
Database updated (97359 signatures) from db.fr.clamav.net (IP: 193.218.105.9)
```

Pour information quand cette commande est lancée c'est l'utilisateur `clamav` qui devient propriétaire du process.

5.4.4 Lancement automatique

On peut configurer un lancement automatique pour les mises à jour de la base de donnée avec `cron`, pour une mise à jour tous les jours on créera dans le fichier `/etc/cron.daily` le fichier `freshclam`

```
#!/bin/bash
/usr/local/bin/freshclam --quiet -l /var/log/clamav/clam-update.log
```

Avec les droits d'exécution

```
chmod 755 freshclam
```

On va créer maintenant un fichier de log pour les mises à jour et rendre l'utilisateur `clamav` propriétaire

```
touch /var/log/clamav/clam-update.log
chmod 600 /var/log/clamav/clam-update.log
chown clamav:clamav /var/log/clamav/clam-update.log
```

Autre solution pour un lancement simple en tant que daemon (lancement six fois par jour) on tape

```
freshclam -d -c 6 -l /var/log/clamav/clam-update.log
```

Maintenant pour un lancement automatique du daemon `clamd`

Pour une mandriva

on copiera le fichier `clamd` suivant sous `/etc/rc.d/init.d` (en tant que root)

```
#!/bin/bash
#
# crond Start/Stop the clam antivirus daemon.
#
# chkconfig: 2345 70 41
# description: clamd is a standard Linux/UNIX program that scans for Viruses.
# processname: clamd
```

```

# config: /usr/local/etc/clamd.conf
# pidfile: /var/lock/subsys/clamd

# Source function library.
./etc/init.d/functions

RETVAL=0

TMPDIR=/tmp
export TMPDIR

# See how we were called.

prog="clamd"
progdir="/usr/local/sbin"

# Source configuration
if [ -f /etc/sysconfig/$prog ] ; then
    ./etc/sysconfig/$prog
fi

start() {
    echo -n "Starting $prog: "
    LANG= daemon $progdir/$prog
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/subsys/clamd

    return $RETVAL
}

stop() {
    echo -n "Stopping $prog: "
    # Would be better to send QUIT first, then killproc if that fails
    killproc $prog
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/clamd

    return $RETVAL
}

rhstatus() {
    status clamd
}

restart() {
    stop
    start
}

reload() {
    echo -n "Reloading clam daemon configuration: "
    killproc clamd -HUP
    retval=$?
    echo
    return $RETVAL
}

case "$1" in
    start)
        start
        ;;

```

```

stop)
    stop
    ;;
restart)
    restart
    ;;
reload)
    reload
    ;;
status)
    rhstatus
    ;;
condrestart)
    [ -f /var/lock/subsys/clamd ] && restart || :
    ;;
*)
    echo $"Usage: $0 {start|stop|status|reload|restart|condrestart}"
    exit 1
esac

exit $?

```

Pour un lancement à l'état de marche 3, 4 et 5 on tapera

```
chkconfig --level 345 clamd on
```

Et pour un arrêt aux autres états de marche

```
chkconfig --level 0126 clamd off
```

Pour une ubuntu

Créer le fichier `/etc/init.d/clamd` qui va contenir

```

#!/bin/bash
#
# crond Start/Stop the clam antivirus daemon.
#
# chkconfig: 2345 70 41
# description: clamd is a standard Linux/UNIX program that scans for Viruses.
# processname: clamd
# config: /usr/local/etc/clamd.conf
# pidfile: /var/lock/subsys/clamd

# Source function library.
#. /etc/init.d/functions
. /lib/lsb/init-functions

RETVAL=0
TMPDIR=/tmp
export TMPDIR

# See how we were called.

prog="/usr/local/sbin/clamd"

start() {
    echo -n $"Starting $prog: "
    start-stop-daemon --start --quiet --oknodo --exec $prog
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/clamd
    return $RETVAL
}

```

```

}

stop() {
    echo -n $"Stopping $prog: "
    # Would be better to send QUIT first, then killproc if that fails
    start-stop-daemon --stop --quiet --oknodo --exec $prog
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/clamd
    return $RETVAL
}

rhstatus() {
    status clamd
}

restart() {
    stop
    start
}

reload() {
    echo -n $"Reloading clam daemon configuration: "
    start-stop-daemon --stop --quiet --oknodo --exec clamd -HUP
    retval=$?
    echo
    return $RETVAL
}

case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart)
        restart
        ;;
    reload)
        reload
        ;;
    status)
        rhstatus
        ;;
    condrestart)
        [ -f /var/lock/clamd ] && restart || :
        ;;
    *)
        echo $"Usage: $0 {start|stop|status|reload|restart|condrestart}"
        exit 1
esac

exit $?

```

Pour que le lancement soit effectif au démarrage à l'état de marche 2, 3, 4 et 5 on tapera

```
sudo update-rc.d spamd start 20 2 3 4 5 . stop 20 0 1 6 .
```

Lancement automatique du scanner

Pour un lancement automatique du scanner vous pouvez utiliser **cron**, créer un fichier **scanvirus** à placer sous

`/etc/cron.daily` (chaque jour) ou `/etc/cron.hourly` (chaque heure) contenant

```
#!/bin/bash
/usr/local/bin/clamscan -r -l /var/log/clamscan/scan.log /home
/usr/local/bin/clamscan -r --mbox /var/spool/mail
```

Il faut le rendre exécutable

```
chmod 755 /etc/cron.daily/scanvirus.
```

Il scannera tous les jours les répertoires `/home` et `/var/spool/mail`. Libre à vous de rajouter des scans dans les partages `samba` ou vos partitions windows.

5.4.5 Interfaçage avec sendmail

L'intérêt maintenant d'un anti virus est un scan automatique à la réception mais également à l'envoi d'emails. Pour cela **Clam Anti Virus** peut très facilement s'interfacier avec **sendmail**. Si la compilation s'est bien passée vous devriez trouver un fichier **clamav-milter** sous `/usr/local/sbin`. Dans le fichier de config de **sendmail** (sous `/etc/mail/` ou `/usr/share/sendmail-cf/cf`) on rajoutera tout à la fin les lignes

```
INPUT_MAIL_FILTER(`clmilter', `S=local:/var/log/clamav/clmilter.sock, F=, T=S:4m;R:4m')dnl
define(`confINPUT_MAIL_FILTERS', `clmilter')
```

Dans l'hypothèse où **spamassassin** est déjà interfacé avec **sendmail**, il faudra modifier les dernières lignes comme cela.

```
INPUT_MAIL_FILTER(`clmilter', `S=local:/var/log/clamav/clmilter.sock, F=, T=S:4m;R:4m')dnl
INPUT_MAIL_FILTER(`spamassassin', `S=local:/var/run/spamass.sock, F=,
T=C:15m;S:4m;R:4m;E:10m')dnl
define(`confINPUT_MAIL_FILTERS', `clmilter,spamassassin')
```

Dans le fichier `/etc/clamd.conf` on modifiera la ligne suivante

```
# Path to the local socket. The daemon doesn't change the mode of the
# created file (portability reasons). You may want to create it in a directory
# which is only accessible for a user running daemon.
# je n'ai pas mis le répertoire par défaut car l'utilisateur clamav
# ne peut écrire sous /var/run
LocalSocket /var/log/clamav/clamd.sock
```

On relance maintenant **clamd**

```
/etc/rc.d/init/clamd restart
```

Et on lance **clamav-milter**

```
clamav-milter -c /etc/clamav-milter.conf
```

Pour information même en le lançant en tant que root, ce sera l'utilisateur **clamav** qui sera le propriétaire du process **clamav-milter**. Maintenant on relance **sendmail** en supposant que votre fichier de conf se trouve sous `/usr/share/sendmail-cf/cf` et se nomme **config.mc**

sous Mandriva

```
/etc/rc.d/init.d/sendmail stop
m4 /usr/share/sendmail-cf/cf/config.mc > /etc/mail/sendmail.cf
sendmail -bd -os
```

sous ubuntu

```
sudo /etc/init.d/sendmail stop
sudo m4 /etc/mail/config.mc > /etc/mail/sendmail.cf
```

sendmail -bd -os

Maintenant pour lancer **clamav-milter** automatiquement on modifiera le fichier **/etc/(rc.d)/init.d/clamd**. Au tout début à la suite de

RETVAL=0

On rajoute

TMPDIR=/tmp
export TMPDIR

Puis après

prog="clamd"

On rajoute

milter="clamav-milter"

Puis rectifiez comme suit sous Mandriva

```
start() {
    echo -n "Starting $prog: "
    daemon $progdir/$prog
    RETVAL1=$?
    echo
    [ $RETVAL1 -eq 0 ] && touch /var/lock/subsys/clamd
    echo -n "Starting $milter: "
    daemon $progdir/$milter -c /etc/clamav-milter.conf
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/subsys/milter
    return $RETVAL1
}

stop() {
    echo -n "Stopping $prog: "
    # Would be better to send QUIT first, then killproc if that fails
    killproc $prog
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/clamd

    echo -n "Stopping $milter: "
    killproc $milter
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/subsys/milter && rm -f /var/log/clamav/clmilter.sock
    rm -f /var/lock/subsys/milter
    rm -f /var/log/clamav/clmilter.sock

    return $RETVAL
}
```

et sous ubuntu

milter="/usr/local/sbin/clamav-milter"
OPTIONS='-c /etc/clamav-milter.conf'

```

start() {
    echo -n "$"Starting $prog: "
    start-stop-daemon --start --quiet --oknodo --exec $prog
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/clamd
    echo -n "$"Starting $milter: "
    start-stop-daemon --start --quiet --oknodo --exec $milter -- $OPTIONS
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && touch /var/lock/milter
    return $RETVAL
}

stop() {
    echo -n "$"Stopping $prog: "
    # Would be better to send QUIT first, then killproc if that fails
    start-stop-daemon --stop --quiet --oknodo --exec $prog
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/clamd
    echo -n "$"Stopping $milter: "
    start-stop-daemon --stop --quiet --oknodo --exec $milter
    RETVAL=$?
    echo
    [ $RETVAL -eq 0 ] && rm -f /var/lock/milter && rm -f /var/log/clamav/clmilter.sock
    rm -f /var/lock/milter
    rm -f /var/log/clamav/clmilter.sock
    return $RETVAL
}

```

Si au lancement du script `/etc/rc.d/init.d/clamd` vous avez l'erreur suivante

```
/usr/local/sbin/clamav-milter: --max-children must be given if --external is not given
```

Vérifiez bien que vous avez décommenté la ligne suivante dans le fichier `/etc/clamd.conf`

```
# Maximal number of threads running at the same time.
# Default: 10
MaxThreads 20
```

Maintenant comment sait-on si un virus a été intercepté ? Avec **fetchmail** quand on récupère le courrier on a un message de ce genre

```
fetchmail: lecture du message olivier.hoarau@funix.org@pop.pro.proxad.net:36 parmi 37 (3143 octets)
fetchmail: éliminé
fetchmail: Le serveur SMTP a refusé de délivrer le courrier
```

Pour que le mail soit purement et simplement supprimé. Dans votre fichier `.fetchmailrc` il faudra rajouter la ligne suivante

```
poll pop.fai.net protocol pop3
user olivier.hoarau@funix.org with password machinchose is olivier here
options antisipam 550 554;
```

Sinon il restera dans `/var/spool/mail`. Plus en détail dans le fichier `/var/log/mail/info` on obtient

```
Aug 23 12:20:08 web sm-mta[5974]: I7NAHEvp005825: to=<olivier@localhost>, delay=00:00:03,
xdelay=00:00:00, mailer=local, pri=32226, dsn=2.0.0, stat=Sent
Aug 23 12:20:08 web sm-mta[5825]: I7NAHEvq005825: from=<ron@bakernet.com>, size=1356, class=0,
nrcpts=1, msgid=<IINISJ-000JQP-FP@216-201-156-242.res.logixcom.net>, proto=ESMTP,
daemon=MTA, relay=localhost [127.0.0.1]
Aug 23 12:20:08 web sm-mta[5825]: I7NAHEvq005825: Milter add: header: X-Virus-Scanned: ClamAV
0.91.1/4016/Tue Aug 21 01:40:52 2007 on web.kervao.fr
Aug 23 12:20:08 web sm-mta[5825]: I7NAHEvq005825: Milter add: header: X-Virus-Status: Infected
with Email.Webaccount-4
```

Aug 23 12:20:08 web sendmail[5976]: I7NAK8cl005976: from=clamav, size=499, class=0, nrcpts=2, msgid=<200708231020.I7NAK8cl005976@web.kervao.fr>, relay=clamav@localhost
Aug 23 12:20:08 web sendmail[5976]: I7NAK8cl005976: to=postmaster, delay=00:00:00, mailer=relay, pri=60499, stat=queued
Aug 23 12:20:08 web sendmail[5976]: I7NAK8cl005976: to=olivier, delay=00:00:00, mailer=relay, pri=60499, stat=queued
Aug 23 12:20:08 web sm-mta[5825]: I7NAHEvq005825: Milter: data, discard
Aug 23 12:20:08 web sm-mta[5825]: I7NAHEvq005825: discarded

Chaque mail se voit rajouter la ligne suivante dans son entête

X-Virus-Scanned: clamav-milter 0.95.2 at mana
X-Virus-Status: Clean