Divers astuces sur Postfix

Vider la file de messages deferred

```
postsuper -d ALL deferred
```

Très utile de vider cette file quand certains messages n'arrivent pas a être délivrés... Ca évite qu'ils tournent en boucle en réessai pour finir par vous blacklister dans les référentiels de spam.

Ne pas se faire refuser les mails envoyé sur internet depuis son dédié

Quand vous avez un serveur ou vous gérez vous même l'intégralité de la configuration, incluant postfix, vous pourrez rapidement vous heurter la des serveurs mails distants tatillons qui vous refusent vos mails alors que vous n'êtes pourtant pas spammeur et encore moins blacklisté (même si cela peut arriver).

Vérifier que votre domaine / ip n'est pas blacklisté

Ca m'est arrivé d'être blacklisté. Je ne sais pas pourquoi puisque mon serveur est sain. J'imagine que j'ai hérité à l'achat d'une IP déjà blacklistée ou alors que j'ai été dénoncé par un serveur mail qui fait trop de zèle en voyant que ma config n'était pas au top.

Bref, pour cela vous pouvez vous rentre en ligne que quelques outils pour avoir un état des lieux :

- http://www.dnsbl.info/dnsbl-database-check.php
- http://cbl.abuseat.org/lookup.cgi

Et ce ne sont pas les seuls.

Ensuite, une vois que vous avez identifié un système qui vous a blacklisté, il faut aller chez lui pour faire une demande de suppression de la blacklist (assez facile) et être patient. Par contre assurez vous avant d'avoir bien vérifié toute votre config car si vous vous refaites blacklisté derrière, vous finirez par être bloqués...

Envoyer ses mails avec un expéditeur correct et accessible

Vous pouvez peut être être victime de quelque chose comme ceci :

```
Postfix : host mail.domain.tld[aaa.bbb.ccc.ddd] refused to talk to me: 501
```

```
Syntax error in parameters or arguments
```

Ceci se passe quand vous envoyez un mail avec une configuration de hostname mauvaise das votre configuration postfix. En gros le serveur distant va recevoir un mail d'un serveur mail avec un hostname comme host.domain.tld. La première chose qu'il va faire et de vérifier que host.domain.tld existe sur le net. Si ce n'est pas le cas, il va tout bonnement refuser la connexion...

De même s'il trouve le domaine sur le net (dans les DNS donc), il va aussi vérifier que l'IP du serveur qui lui a envoyé le mail (le votre donc) correspond bien à celle du domaine. Encore un fois si ce n'est pas le cas, risque de refus.

Pour ma part je n'avais pas fait attention surtout que ça marchait bien avec pas mal de fournisseur de mails. Je recevais bien les mails de mon serveur. Mais beaucoup d'autres sont plus tatillons.

Merci donc à ce site, qui m'a apporté la solution ci dessous que je reprends brutalement :

Si vous avez le message suivant sur postfix (ou autre MTA), c'est peut-être une erreur DNS. Le nom présenté par le serveur mail n'est pas connu.

Par défaut c'est le nom de host de la machine. Vous avez peut-être mis un nom interne : mail.domain.int.

Pour forcer le nom sur postfix, ouvrez le fichier :

```
/etc/postfix/main.cf
```

et ajoutez ou modifiez :

```
myhostname = host.domain.tld
```

ou host.domain.tld correspond à un nom dns connu qui renvoie sur l'adresse IP public de votre serveur de mail.

Pensez à redémarrer votre postfix.

Attention : Ne faites pas la même erreur que moi, le *dkpkg-reconfigure postfix* fait une autre modification (elle règle le mydomain) mais pas le hostname... Donc les deux opérations sont complémentaires je dirais.

Note 1 : La vérification du hostname par le serveur distant se fait au moment de la commande HELO. Et c'est bien myhostname que postfix pose dans le HELO.

Note 2 : Attention, si votre serveur mail est en NAT derrière un autre serveur, il faut spécifier les information de ce dernier dans votre configuration (puisque c'est le front qui semble envoyer les mails). Ok, il y a peut être une architecture mieux à faire mais bon en l'état c'est comme ça.

Utiliser SPF

Une autre façon de diminuer encore la possibilité de se faire jeter est de mettre en place SPF sur votre DNS. En résumé, il s'agit d'ajouter une entrée TXT sur votre dns pour le domaine que vous

souhaitez utiliser pour votre mail. Dedans, entre autres choses, vous y mettrez l'IP du serveur autorisé a envoyer des mails. Cela est une autre manière de s'assurer qu'il a bien correspondance entre domaine et serveur.

Merci à ce site pour l'information, que je reprends ici :

Il vous faut simplement éditer vos zones DNS chez votre registrar, pour y ajouter une entrée de type TXT. L'instruction pour la cas décrit précédemment est :

```
v=spf1 a mx ip4:<IP> -all
```

Paramètres :

- Liste à pucespf1 : la version de SPF
- a : s'applique au A-record courant
- mx : s'applique à l'entre MX courante
- ip4<IP> : n'accepte que l'IP spécifiée (IP du serveur)
- -all : refuse tous les autres

Avoir un reverse DNS qui match bien le domaine utilisé et l'ip du serveur

Si j'en crois certains fournisseurs de mails (celui la me refuse tout quoi que je fasse).

Il faut aussi que le domaine utilisé corresponde bien à l'ip du serveur via le reverse DSN. Sinon il peut y avoir rejet.

Pour configurer c'est généralement sur votre serveur ou dans l'IHM d'admin de votre serveur dédié.

Pour tester :

```
nslookup votre_ip
```

et voir qu'elle renvoie bien le domaine que vous utilisez.

Déboguer quand ça ne fonctionne toujours pas

Pour cela le site officiel postfix donne des informations intéressantes sur la partie debug.

Pour ma part, la méthode brut de traçage des flux avec tcpdump à bien fonctionné :

```
tcpdump -w monfichierdump -s 0 port 25
```

Sans oublier que le fichier dump ne peut être lu comme ça (fichier binaire).

Lire le dump en ligne de commande :

```
tcpdump -qns 0 -X -r monfichierdump
```

Vu sur ce ticket.

Wireshark :

Récupérer le fichier sur votre PC (transfert en mode binaire) et le lire avec Wireshark.