

Un MX secondaire est-il vraiment utile ?

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 Mai 2007. Dernière mise à jour le 2 Juin 2007

<http://www.bortzmeyer.org/mx-secondaire.html>

On voit souvent des administrateurs de serveurs de messagerie demander des conseils sur la configuration d'un serveur de secours, un MX secondaire. Est-ce vraiment utile ?

Pour la grande majorité des sites, non, un MX secondaire ne sert pas à grand'chose et présente des risques, notamment en terme de lutte anti-spam.

En effet, le courrier électronique n'est pas le Web. Il est asynchrone et peu pressé. En cas de panne du serveur de messagerie, les autres serveurs qui tentent de lui envoyer du courrier feront comme les MTA ont toujours fait depuis l'aube des temps : ils attendront et réessaieront (la plupart du temps, pendant cinq jours, la durée maximum configurée par défaut dans sendmail et Postfix).

Il n'y a donc aucun risque de perte du courrier si le serveur de messagerie est coupé ou bien injoignable pendant quelques jours.

En revanche, le serveur de secours, le MX secondaire (du nom des enregistrements MX du DNS) présente des pièges, notamment en ce qui concerne les règles anti-spam. Par exemple, les listes noires ne servent à rien si on a un MX secondaire (les spammeurs se connectent souvent au MX de plus **basse** priorité, comptant, en général à juste titre, qu'il est moins protégé). À moins que le MX secondaire soit configuré avec exactement les mêmes règles anti-spam que le serveur principal (ce qui est difficile à faire, surtout s'il est situé dans une autre organisation), il représentera le maillon faible de la résistance aux spams.

Avoir un second serveur viole surtout le **principe de simplicité** : deux serveurs sont plus compliqués à configurer qu'un, augmentant ainsi les probabilités de problème. C'est en général au moment où le primaire tombe en panne qu'on s'aperçoit soudain que le secondaire n'acceptait plus du courrier pour le domaine depuis des mois, sans que personne n'ait détecté ce changement de configuration.

Et si les utilisateurs réclament leur courrier immédiatement, sans délai, même si le serveur primaire est en panne ? Il faut d'abord expliquer à ces utilisateurs que le courrier, service **asynchrone**, n'a jamais

été prévu pour cela, et leur dire que, s'ils veulent du synchrone, il y a le téléphone ou Jabber. (Amavis est, par exemple, un bon moyen de retarder le courrier, souvent de plusieurs heures.) Ensuite, il faut noter qu'il ne suffit pas d'un MX secondaire pour avoir une délivrance rapide même en cas de panne du primaire. Il faut aussi que ce MX secondaire puisse délivrer directement dans les boîtes aux lettres. Cela implique en général qu'il soit sur le même site que le primaire, augmentant ainsi la probabilité qu'il tombe en panne en même temps, victime de la même pelleuse.

D'autres regretteront que, en cas de panne du primaire, les expéditeurs distants peuvent voir qu'on est en panne, avec la commande `mailq` sur leur serveur de messagerie Postfix. Mais peu d'expéditeurs suivent ainsi le cheminement de leur courrier, comme si c'était un colis envoyé par FedEx. En revanche, c'est vrai que les bêtes messages de retard qu'envoient certains serveurs à leurs utilisateurs "*« Your message was not delivered yet, we continue to try, you have nothing to do »*" peuvent perturber leur lecteur, qui ne le comprend pratiquement jamais (et qu'il interprète parfois de façon farfelue). À une époque, c'était le comportement par défaut de `sendmail`.

Un autre cas où il peut-être utile d'avoir plusieurs MX est celui où on tient absolument à garder trace des messages, en les laissant rentrer sur une machine qu'on contrôle, même si on ne les délivre pas tout de suite dans les boîtes aux lettres. C'est dangereux, car, en acceptant les messages, on accepte aussi une responsabilité. Il faut être sûr de pouvoir les traiter un jour.

Mais, diront enfin certains, Gmail ou Yahoo ont plusieurs serveurs, comme on peut le voir avec un `dig MX gmail.com`. Ma réponse est que, si vous êtes responsable du courrier de Gmail, vous n'allez probablement pas chercher des conseils sur ce blog. Mais, pour les nombreux sites qui sont **nettement** plus petits et moins pourvus en ressources humaines que Gmail, ces conseils de simplicité peuvent vous être utiles.

(Merci à Gilles Mocellin, Yves Rutschle, Benoit Lathière, François Tourde, Vincent Bernat et Daniel Caillibaud, pour une intéressante discussion sur la liste des utilisateurs francophones de Debian. Naturellement, les idées exprimées ici sont uniquement les miennes et patati et patata.)

Antoine cite d'autres cas où l'utilisation d'un MX secondaire est utile (à condition qu'on ait les moyens humains de le configurer correctement :

- Le délai de cinq jours, qui est par défaut le temps d'attente maximal de la plupart des MTA peut être trop court si le seul administrateur système du site part en vacances une semaine. Le MX secondaire peut être configuré pour garder le courrier plus longtemps (peu le sont).
- Si (c'est un gros Si) le MX secondaire permet de consulter le courrier mis en attente (ne serait-ce qu'en utilisant `more` sur les fichiers du "*spool*"), alors cela permet, en dépannage, de voir « le courrier du client que l'on attend maintenant tout de suite immédiatement », même quand le serveur de courrier principal est tombé.