RFC 6729 : Indicating Email Handling States in Trace Fields

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 septembre 2012

Date de publication du RFC : Septembre 2012

https://www.bortzmeyer.org/6729.html

Lorsqu'on débogue un problème de courrier électronique en examinant un message reçu, le technicien regarde souvent en premier les champs `Received:` de l'en-tête. Ceux-ci indiquent les différents MTA qui ont pris en charge le message et sont notamment très utiles en cas de retard inattendu : ils permettent de voir quel MTA a traîné dans la remise du message au MTA suivant. Mais cela ne suffit pas toujours. Aujourd'hui, il est de plus en plus fréquent que les messages soient retardés en raison d'un traitement local à une machine, par exemple le passage par un programme de sécurité qui met très longtemps à vérifier quelque chose. Il n'y avait pas de moyen pratique avec les champs `Received:` pour indiquer ces traitements. C'est désormais fait avec un nouvel indicateur dans `Received:` : `state` qui permet de signaler le passage d'un traitement lent à un autre.

Voici un exemple d'une suite de champs `Received:`. Rappelez-vous qu'elle se lit de bas en haut :

```
Received: from slow3-v.mail.gandi.net (slow3-v.mail.gandi.net [217.70.178.89])
        by mail.bortzmeyer.org (Postfix) with ESMTP id 5EC103AD82
        for <stephane+blog@bortzmeyer.org>; Thu,  6 Sep 2012 18:26:36 +0000 (UTC)
Received: from relay4-d.mail.gandi.net (relay4-d.mail.gandi.net [217.70.183.196])
        by slow3-v.mail.gandi.net (Postfix) with ESMTP id 2268638B64
        for <stephane+blog@bortzmeyer.org>; Thu,  6 Sep 2012 20:21:20 +0200 (CEST)
Received: from mfilter1-d.gandi.net (mfilter1-d.gandi.net [217.70.178.130])
        by relay4-d.mail.gandi.net (Postfix) with ESMTP id 0844C172094
        for <stephane+blog@bortzmeyer.org>; Thu,  6 Sep 2012 20:21:10 +0200 (CEST)
Received: from relay4-d.mail.gandi.net ([217.70.183.196])
        by mfilter1-d.gandi.net (mfilter1-d.gandi.net [10.0.15.180]) (amavisd-new, port
        10024)
        with ESMTP id 9nO2SZ5sO3KB for <stephane+blog@bortzmeyer.org>;
        Thu,  6 Sep 2012 20:21:08 +0200 (CEST)
```

On note que la machine `mfilter1-d.gandi.net` a renvoyé le message à `relay4-d.mail.gandi.net` d'où il venait. Ce n'est pas une erreur, `mfilter1-d.gandi.net` est la machine de filtrage et utilise Amavis pour un certain nombre de tests sur le message (absence de virus, par exemple) avant de le réinjecter. Ici, cet examen a été rapide (deux secondes, si on peut se fier aux horloges des machines) mais, s'il est plus long (et Amavis peut être **très** long), il serait souhaitable de pouvoir le marquer plus clairement.

Il existe bien des tests/vérifications/etc qui peuvent ainsi ralentir un message : mise en quarantaine, modération, tests anti-spam ou anti-virus, etc. Pour les indiquer plus clairement, notre RFC reprend le champ `Received:` (défini à la section 4.4 du RFC 5321[1] et un des outils les plus importants du technicien qui fait fonctionner le courrier électronique). Ce champ comprend plusieurs clauses (dans les exemples ci-dessus, on voit les clauses `from`, `by`, `with` et `for`, définies dans la section 4.4 du RFC 5321). Notre RFC en ajoute une nouvelle, `state` (désormais enregistrée `<https://www.iana.org/assignments/mail-parameters>`, section "*Additional-registered-clauses*"), qui ressemble à ça (exemple du RFC car je n'ai pas encore trouvé de clause `state` dans mes boîtes aux lettres, bien qu'il existe apparemment déjà une mise en œuvre en production) :

```
Received: from newyork.example.com
                (newyork.example.com [192.0.2.250])
            by mail-router.example.net (8.11.6/8.11.6)
                with ESMTP id i7PK0sH7021929
                for <recipient@example.net>;
            Fri, Feb 15 2002 18:33:29 -0800
Received: from internal.example.com
                (internal.example.com [192.168.0.1])
            by newyork.example.com (8.11.6/8.11.6)
                with ESMTP id i9MKZCRd064134
                for <secret-list@example.com>
                state moderation (sender not subscribed);
            Fri, Feb 15 2002 17:19:08 -0800
```

Ici, le MTA de `newyork.example.com` a décidé de ne pas envoyer le message tout de suite mais de le soumettre à un modérateur (avant-dernière ligne du plus ancien `Received:`, clause `state`). Cela suffit à expliquer le délai d'une heure vingt entre les deux `Received:`, sans imaginer une coupure réseau ou une autre panne. On voit que la clause `state` indique l'**entrée** dans un nouvel état (ici, l'état « en attente d'approbation par le modérateur »), la **sortie** étant marquée par le champ `Received:` suivant (qui, ici, n'a pas d'état explicite). Rappelez-vous (promis, c'est la dernière fois que je le dis) que les champs `Received:` se lisent de bas en haut.

La clause `state` dans l'exemple ci-dessus utilisait le mot-clé `moderation`. Une liste limitative de tels mots-clés est enregistrée `<https://www.iana.org/assignments/mail-parameters>` (section "*Registered-states*") et elle comprend notamment :

— `auth` : le message attend une authentification,
— `content` : le contenu du message va être analysé, par exemple pour s'assurer qu'il ne contient pas de spam ou de "*malware*",
— `moderation` : passage par le modérateur,
— `timed` : message délibérement gardé, en attendant l'heure de la remise (voir RFC 4865),
— `normal` : ce mot-clé est enregistré mais, en fait, c'est celui par défaut, lorsqu'aucune clause `state` n'est présente,

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5321.txt`

— `other` : il y a toujours des cas où on ne sait pas :-)

À noter que le mot-clé peut être suivi d'une barre oblique et d'une valeur (non enregistrée, on met ce qu'on veut), on peut donc avoir `moderation/not-subscribed` ou `quarantine/spam`. D'autres états pourront être enregistrés dans le futur, sous la politique « Premier arrivé, premier servi » (cf. RFC 5226). Ce point avait été le principal sujet de discussion avant la publication du RFC, certains auraient préféré la politique plus restrictive « Examen par un expert ».

Les programmeurs de MTA qui veulent ajouter cette clause aux champs `Received:` qu'ils écrivent ont tout intérêt à bien lire les sections 4 et 5, qui discutent de quand utiliser la clause `state`. Elle n'est pas prévue pour des opérations différentes à l'intérieur d'un même agent. Le RFC recommande bien qu'elle ne soit utilisée que lorsqu'on passe à un agent différent, par exemple de Postfix à Amavis. Autrement, on risque de se retrouver avec plein de `Received:` qui rendront l'analyse plus difficile (et risquent d'atteindre la limite des MTA, qui rejettent les messages ayant trop de `Received:`, pensant qu'ils bouclent). L'idée est de déboguer les performances et donc cette clause est là uniquement pour les problèmes temporels, pas pour n'importe quelle action ou changement d'état interne à l'agent.