RFC 6186 : Use of SRV Records for Locating Email Submission/Access services

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 31 mars 2011

Date de publication du RFC : Mars 2011

https://www.bortzmeyer.org/6186.html

Les enregistrements DNS de type SRV ont été normalisés dans le RFC 2782 [1] il y a dix ans, pour permettre de trouver la ou les machines rendant un service (par exemple de messagerie instantanée avec XMPP), en ne connaissant que le nom de domaine délégué, par exemple `example.org` ou `apple.example`. Ils ont été adoptés par la plupart des protocoles Internet, avec deux exceptions importantes : le Web ne les utilise toujours pas, ce qui mène à des bricolages contestables comme de mettre une adresse IP sur un nom de domaine délégué. Et le courrier électronique n'utilise pas non plus SRV car, pour trouver le serveur d'un domaine, il compte sur une technique plus ancienne, proche du SRV mais spécifique au courrier, le MX (les MX ne présentent aucun avantage spécifique et, si tout était à refaire de zéro, on utiliserait certainement les SRV aussi pour cela). Les enregistrements MX ne concernent toutefois que la transmission de courrier de MTA à MTA. Pour les autres logiciels de courrier, comment font-ils ?

Depuis ce RFC 6186, ils utilisent SRV à leur tour. Ainsi, un MUA qui cherche à quel serveur transmettre le courrier n'aura plus besoin d'être configuré explicitement (options "*Mail submission server*", "*Mail retrieval server*", ou quelque chose de ce genre). Il suffira d'indiquer l'adresse électronique de l'utilisateur (mettons `jeanne@example.org`) et le MUA pourra extraire le domaine (`example.org`) et chercher des enregistrements SRV qui lui indiqueront où trouver ces serveurs. (Une autre méthode ancienne était d'utiliser des **conventions** comme de mettre le serveur IMAP en `imap.example.org` mais elle est moins souple, les SRV permettent en effet d'indiquer plusieurs serveurs, de préciser leurs priorités, etc.)

Bien, commençons par l'introduction. Une liste (sans doute non limitative) des services de courrier est donnée par la section 1 :

— Service SMTP (RFC 5321) et son profil spécifique à la soumission initiale de messages (RFC 6409),

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc2782.txt`

— Services de récupération du courrier, IMAP (RFC 3501) et POP (RFC 1939).

Le premier cité de ces RFC, le RFC 5321 (section 5) normalise l'utilisation des enregistrements MX pour trouver le serveur de courrier suivant. Mais il ne dit rien des autres services. Par exemple, un MUA ne peut pas trouver dans les MX le serveur de soumission. Résultat, les MUA dépendent d'une configuration manuelle des serveurs à utiliser, parfois augmentée d'une série d'heuristiques (du genre, essayer l'IMAP sur le serveur de soumission, au cas où ce serait le même...). Ce système est complexe pour les utilisateurs (≪ Indiquez le numéro de port de votre serveur IMAP ; si vous ne le connaissez pas, écrivez à `jenerepondsjamaisintelligemment@support.votre-fai.net` ≫...)

Les différents noms SRV utilisés sont normalisés en section 3 :

— `submission` (section 3.1) sert pour la soumission initiale de message, telle que décrite dans le RFC 6409. Ainsi, pour le domaine `example.org`, on pourrait voir un enregistrement `_submission._tcp.example.org. SRV 0 1 9587 mail.example.NET.` indiquant que les messages doivent être soumis à `mail.example.NET`, sur le port non-standard 9587. À noter que cet enregistrement couvre les connexions avec ou sans TLS, ce qui est une autre source de confusion lors de la configuration <https://www.bortzmeyer.org/thunderbird-et-crypto.html>.

— `imap` (section 3.2) et `imaps` servent pour trouver le serveur IMAP. Donc, par exemple, avec cette fois le port standard, `_imap._tcp.example.org. SRV 0 1 143 imap.example.NET.`.

— `pop3` et `pop3s` servent à localiser le serveur POP3. Leur absence peut donc indiquer que ce vieux protocole n'est pas disponible pour un domaine.

Les enregistrements SRV indiqués ici utilisent évidemment la sémantique standard du RFC 2782. Ainsi, l'ensemble suivant :

```
$ORIGIN example.org.
 _imap._tcp     SRV 0 1 143 imap.example.net.
                SRV 10 1 143 imap.plan-B.example.
```

signifie, en raison du champ Priorité (mis à zéro pour le premier enregistrement et à 10 pour le second), que le client IMAP **doit** tenter d'abord de se connecter à `imap.example.net` et ne doit essayer `imap.plan-B.example` que si le premier est injoignable. Tout cela est ancien et bien connu. Mais le courrier présente un défi spécifique, l'existence de deux protocoles de récupération, IMAP et POP. Que doit faire le MUA si les deux sont annoncés dans le DNS ? La section 3.4 tranche : le MUA qui gère les deux protocoles devrait récupérer les enregistrements pour POP et IMAP et utiliser ensuite le champ Priorité, non seulement à l'intérieur d'un ensemble (POP ou IMAP) mais même pour choisir entre les deux protocoles. Ainsi, ces données :

```
$ORIGIN example.org.
_imap._tcp     SRV 10 1 143 imap.example.net.

_pop3._tcp      SRV 50 1 143 pop.example.net.
```

indiquent sans ambiguité que l'administrateur système voudrait qu'on utilise de préférence IMAP (champ Priorité plus petit, donc plus prioritaire).

Bien, maintenant, dans le futur (car, aujourd'hui, il n'y a à ma connaissance aucune mise en œuvre de ce RFC dans un logiciel), comment se comportera un MUA lorsque ce RFC sera déployé ? La section 4 expose le mode d'emploi. Il leur suffira d'interroger l'utilisateur sur son adresse électronique et tout le reste pourra être trouvé dans le DNS, en prenant la partie à droite du @ et en cherchant les SRV pour les différents services. Regardez par exemple le domaine `bortzmeyer.fr` comment c'est fait (enregistrements `_submission._tcp`, `_imap._tcp` et `_imaps._tcp`). Si la recherche des SRV ne donne rien, le MUA pourra alors, comme aujourd'hui, demander à l'utilisateur ces informations.

Notez toutefois que beaucoup d'hébergeurs DNS ne permettent pas, via le panneau de contrôle qu'ils proposent à leurs clients, d'ajouter un enregistrement SRV. Même lorsque cette possibilité existe, elle est souvent boguée comme chez Gandi où le formulaire ne permet pas d'indiquer proprement poids, priorité ou port (astuce : il faut les taper dans le champ Valeur, dans le bon ordre).

La partie de cette section concernant TLS est plus faible (mais a été changée dans le RFC 8314, bien plus détaillé). Si on trouve un serveur IMAP, par exemple, le RFC demande de tenter la commande `STARTTLS` pour voir si elle marche. Les enregistrements SRV de notre RFC ne permettent pas d'indiquer que la gestion de TLS est obligatoire (chose que l'on peut configurer dans beaucoup de MUA) et, si TLS échoue, le MUA doit donc compter sur une configuration manuelle par l'utilisateur (du genre « Toujours utiliser TLS »). La section 6 détaille ce choix.

Notons aussi que l'utilisation des SRV peut compliquer la vérification de l'identité du serveur distant (si le domaine est `mapetiteentreprise.example` et que l'enregistrement SRV indique que le serveur IMAP est `mail.grosfournisseur.example`, l'identité du serveur dans le certificat ne sera **pas** `mapetiteentreprise.example`). La procédure du RFC 6125 doit impérativement être utilisée.

Lors de la connexion au serveur IMAP ou au serveur SMTP de soumission, il faut en général s'authentifier, ce qui implique qu'on puisse indiquer un nom d'utilisateur. Notre section 4 impose au MUA d'utiliser **d'abord** l'adresse électronique entière, puis la partie à gauche du @. Si ces deux tentatives échouent, il reste à demander à l'utilisateur (le nom pour la procédure d'authentification n'est en effet pas forcément dans l'adresse de courrier).

Les informations sur les serveurs peuvent être conservées pour éviter de demander au DNS à chaque fois. Mais, si la connexion a marché à un moment mais échoue par la suite, le MUA doit ré-interroger le DNS pour voir si les serveurs n'ont pas changé.

La section 4 conseillait les auteurs de MUA. La section 5 aide les fournisseurs de courrier. Le principal conseil est de permettre comme nom de connexion l'adresse électronique complète, vu que c'est la première chose que tenteront les MUA.

La section 6 est celle de la sécurité. En l'absence de signatures DNSSEC, la récupération des enregistrements SRV n'est pas sûre. Si un attaquant a réussi à empoisonner le cache du résolveur DNS, il peut rediriger le courrier vers n'importe quel serveur de son choix. Notez bien que c'est un des cas où l'argument des sceptiques sur DNSSEC « Il suffit d'utiliser TLS » ne tient pas. Sans DNSSEC pour sécuriser le SRV (le lien entre un nom de domaine et les noms des serveurs), TLS ne protégerait rien puisque les serveurs d'un attaquant peuvent parfaitement avoir un certificat valide et correspondant à leur nom.

La section 6 conseille, au cas où DNSSEC ne soit pas utilisé (ce qui est aujourd'hui le cas le plus fréquent), de vérifier que les serveurs sont dans le même domaine que le domaine de l'adresse de courrier et, sinon, de demander confirmation à l'utilisateur, procédure lourde qui annulerait une partie de l'intérêt de ce RFC (et qui n'est pas suivie dans l'exemple de `bortzmeyer.fr` donné plus haut).