RFC 8552 : Scoped Interpretation of DNS Resource Records through "Underscored" Naming of Attribute Leaves

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 avril 2019

Date de publication du RFC : Mars 2019

https://www.bortzmeyer.org/8552.html

Une convention répandue pour les noms de domaine est de préfixer les services par un tiret bas, par exemple _xmpp-client._tcp.jabber.ietf.org. Cette pratique n'avait jamais été documentée mais c'est désormais fait. Et il existe désormais un registre IANA des noms ainsi préfixés <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#underscored-globally-scoped-dns

Bien sûr, on peut mettre des ressources sous n'importe quel nom. Le DNS n'impose aucune restriction pour cela, et vous pouvez décider que le service X sera sous le nom $X%.example.com (si vous ne me croyez pas, relisez le RFC 1035[1] et RFC 2181). Mais les humains aiment les conventions, par exemple pour les machines, comme www comme préfixe d'un serveur Web (préfixe d'ailleurs contesté <http://no-www.org/>, souvent pour de mauvaises raisons <https://www.yes-www.org/>) ou mail pour un serveur de messagerie. Ce ne sont que des conventions, le DNS s'en moque, et on peut mettre un serveur Web en mail.example.com si on veut, cela ne perturbera que les humains. D'autant plus qu'on peut utiliser n'importe quel type de données avec n'importe quel nom (par exemple un enregistrement MX pour www.example.org).

La convention du tiret bas initial est répandue, notamment parce qu'elle évite toute confusion avec les noms de machines <https://www.bortzmeyer.org/host-vs-domain.html>, qui ne peuvent pas comporter ce caractère (RFC 952). Elle est donc très commune en pratique. Cette convention permet de restreindre explicitement une partie de l'arbre des noms de domaine pour certains usages. Comme ce RFC ne fait que documenter une convention, il ne nécessite aucun changement dans les logiciels.

Une alternative au tiret bas serait d'utiliser un type de données spécifique. Quant aux types « généralistes » comme TXT, ils ont l'inconvénient qu'on récupère, lors de la résolution DNS, des informations inutiles, par exemple les TXT des autres services. Bref, vous créez un nouveau service, mettons X, vous avez le choix, pour le cas du domaine parent example.org, entre :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1035.txt

— Un nouveau type d'enregistrements DNS, nommons-le par exemple `TYPEX` (en pratique, c'est long et compliqué, et sans déploiement garanti, cf. RFC 5507),
— Un type d'enregistrement générique comme TXT cité plus haut ou bien le URI du RFC 7553, menant à des ensembles d'enregistrements (RRset) potentiellement assez gros, problème détaillé en section 1.2,
— Une convention de nommage comme `x.example.org`,
— Une convention de nommage avec un tiret bas (`_x.example.org`), l'objet de ce RFC 8552.

Un exemple d'un service réel utilisant la convention avec le tiret bas est DKIM (RFC 6376), avec le préfixe `_domainkey` :

```
% dig +short TXT mail._domainkey.gendarmerie.interieur.gouv.fr
"v=DKIM1; k=rsa; t=y; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDIgwhYZeeZgM94IofX9uaGAwQ+tynFX7rYs/igs+d1afqr
```

Comme beaucoup de choses, la convention « tiret bas » s'entend mal avec les jokers du DNS. D'abord, on ne peut pas utiliser les jokers entre le préfixe et le reste du nom (`_x.*.example.net` ne marche pas), ensuite, un joker couvre également les noms avec tiret bas donc `*.example.net` va répondre positivement pour `_x.example.net` même si on ne le voulait pas.

La section 1.5 de notre RFC détaille l'histoire de la convention « tiret bas au début ». Beaucoup de services utilisaient cette convention mais sans coordination, et sans qu'il existe une liste complète. Du fait de l'existence de plusieurs choix possibles (énumérés plus haut), ce RFC n'a pas obtenu de consensus immédiatement et les débats ont été longs et compliqués.

La section 2 du RFC explique comment remplir le nouveau registre des noms à tiret bas. On ne met dans ce registre que le nom le plus proche de la racine du DNS. Si un service mène à des noms comme `_foo._bar.example.org`, seul le `_bar` sera mis dans le registre. C'est particulièrement important pour le cas des enregistrements SRV qui ont souvent deux niveaux de noms préfixés (par exemple `_sip._tcp.cisco.com`). Seul le nom le plus proche de la racine, ici `_tcp`, est enregistré (ici, `_sip` est quand même enregistré car il peut en théorie être utilisé sans le `_tcp` mais il me semble que c'est rare en pratique).

Les règles pour les noms plus spécifiques sous le `_bar` (ou `_tcp`) sont spécifiées lors de la description du service en question. Par exemple, pour DKIM, le RFC 6376 précise que que sous le nom `_domainkey`, on trouve un sélecteur dont l'identificateur apparait dans le courrier signé. Donc, pour un message envoyé avec `s=mail` et `d=gendarmerie.interieur.gouv.fr`, on cherche les informations DKIM en `mail._domainkey.gendarmerie.interieur.gouv.fr`.

Le formulaire pour demander l'enregistrement d'un nouveau nom préfixé par un tiret bas figure en section 3 du RFC. Il faut indiquer le type de données DNS (un enregistrement n'est valable que pour un certain type, donc la clé du registre est un couple {type, nom}), le nom et la référence du document décrivant le service en question. Le registre est décrit en section 4 du RFC. L'ajout dans ce registre se fait selon la politique « examen par un expert » (RFC 8126, section 4.5). La section 5 de notre RFC donne quelques indications à l'IANA sur cet examen.

Un ensemble d'entrées à ajouter pour initialiser ce nouveau registre est indiqué. On y trouve par exemple {TXT, `_domainkey`} pour DKIM, {TLSA, `_tcp`} pour DANE (RFC 6698), {TXT, `_acme-challenge`} pour ACME (RFC 8555), etc. Deux cas particuliers : le nom `_example` est réservé pour tous les types d'enregistrement, lorsqu'on a besoin de donner un exemple, sans spécifier un cas réel, et le nom `_ta`, qui sert au mécanisme de signalement des clés DNSSEC du RFC 8145, désigne en fait tous les noms commençant par `_ta`.