RFC 9606 : DNS Resolver Information

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 18 août 2024

Date de publication du RFC : Juin 2024

https://www.bortzmeyer.org/9606.html

Traditionnellement, tous les résolveurs DNS <https://www.bortzmeyer.org/resolveur-dns.html> fournissaient un service équivalent. Le client avait un résolveur configuré, soit statiquement, soit via DHCP, et ne se souciait pas vraiment du résolveur ainsi désigné, tous étaient pareils. Aujourd'hui, ce n'est plus vraiment le cas : les résolveurs fournissent des services très différents, par exemple en matière de chiffrement, ou de blocage de certains noms. Il est donc utile que le client puisse se renseigner sur son résolveur, ce que permet cette nouvelle technique, le type de données RESINFO, que le client va récupérer dans le DNS.

Voici une liste (non-limitative !) des caractéristiques d'un résolveur <https://www.bortzmeyer.org/resolveur-dns.html> et qui peuvent être présentes ou pas :

- Chiffrement des requêtes, avec DoT, DoH ou DoQ.
- Blocage de certains noms, par exemple la publicité, ou le porno, ou bien les noms qui gênent le gouvernement <https://next.ink/137451/blocage-de-tiktok-en-nouvelle-caledonie-quels-so>, ou encore les noms des services qui osent enfreindre la propriété intellectuelle sacrée.
- Protection de la vie privée via la minimisation des requêtes (RFC 9156 [1]) et/ou l'absence de stockage de l'historique des requêtes.

Avant la solution de ce RFC, la seule manière pour le client DNS de savoir ce que son résolveur proposait était manuelle, en lisant des documentations (cf. par exemple celle de mon résolveur <https://doh.bortzmeyer.fr/policy>). Ce n'est pas pratique quand la configuration du résolveur est automatique ou semi-automatique, via DHCP, ou avec les solutions des RFC 9462 et RFC 9463.

Ce nouveau RFC propose donc un mécanisme qui permet au client de découvrir les caractéristiques d'un résolveur et de les analyser, avant de décider quel résolveur choisir. (Un point important est que ce RFC se veut neutre : il ne dit pas quelles sont les bonnes caractéristiques d'un résolveur, le client reçoit une information, il est libre de l'utiliser comme il veut.)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9156.txt

Place à la technique (section 3 du RFC) : un nouveau type de données DNS est défini, RESINFO (code 261 <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-4>). Son contenu est l'information recherchée, sous forme de couples clé=valeur. Le nom de domaine auquel il est rattaché est le nom du résolveur, récupéré par les méthodes des RFC 9462 et RFC 9463, ou manuellement configuré. Ce nom est désigné par le sigle ADN, pour "*Authentication Domain Name*" (RFC 9463, section 3.1.1). Si on a utilisé le nom spécial `resolver.arpa` (RFC 9462, section 4), on peut lui demander son RESINFO.

Le format du RESINFO (section 4 du RFC) est copié sur celui des enregistrements TXT. Chaque chaine de caractères suit le modèle clé=valeur du RFC 6763, section 6.3. Les clés inconnues doivent être ignorées, ce qui permettra dans le futur d'ajouter de nouvelles clés au registre des clés <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-resolver-information-keys>. Un exemple d'enregistrement RESINFO :

```
resolver IN RESINFO "qnamemin" "exterr=15,17" "infourl=https://resolver.example.com/guide"
```

Il indique (section 5, sur la signification des clés) que ce résolveur fait de la minimisation des requêtes (RFC 9156), et notez que cette clé n'a pas de valeur, c'est juste un booléen dont la présence indique la "*QNAME minimisation*". L'enregistrement continue en donnant les codes EDE ("*Extended DNS Errors*", RFC 8914) que peut renvoyer le résolveur. C'est surtout utile pour indiquer ce qu'il bloque (15 = bloqué par décision de l'administrateurice du résolveur, 17 = bloqué par demande de l'utilisateurice). Et enfin il donne un URL où on peut aller chercher davantage d'information en langue naturelle.

La section 7 du RFC donne quelques conseils de sécurité : avoir un lien sécurisé avec le résolveur qu'on interroge (par exemple avec DoT), pour éviter qu'un méchant ne modifie le RESINFO, et valider la réponse avec DNSSEC (sauf pour `resolver.arpa`, qui est un cas spécial).

La section 8 précise le registre des clés <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-resolver-information-keys> disponibles. Pour ajouter des clés (on note qu'à l'heure actuelle, il n'y en a pas pour indiquer la disponibilité de DoT ou DoH, ou pour la politique de conservation des requêtes), la procédure est « spécification nécessaire » (RFC 8126). Si on veut des clés non normalisées, on doit les préfixer par `temp-`.

RESINFO est récent et donc pas forcément mis en œuvre dans tous les logiciels DNS que vous utilisez. Un dig récent fonctionne :

```
% dig dot.bortzmeyer.fr RESINFO
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34836
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
...
;; ANSWER SECTION:
dot.bortzmeyer.fr. 86369 IN CNAME radia.bortzmeyer.org.
radia.bortzmeyer.org. 86369 IN RESINFO "qnamemin" "infourl=https://doh.bortzmeyer.fr/policy"

;; Query time: 0 msec
;; SERVER: 192.168.2.254#53(192.168.2.254) (UDP)
;; WHEN: Sun Aug 18 08:15:55 UTC 2024
;; MSG SIZE  rcvd: 142
```

Si vous avez un dig plus ancien, il faudra demander TYPE261 et pas RESINFO. Notez que, physiquement, un RESINFO est juste un TXT, ce qui facilite sa mise en œuvre (dans le futur dnspython <https://www.dnspython.org/>, la classe RESINFO hérite simplement de TXT).

Trouve-t-on beaucoup de RESINFO dans la nature ? La plupart des grands résolveurs DNS publics ne semblent pas en avoir. Une exception est DNS4ALL <https://www.bortzmeyer.org/resolveur-dns-sidn.html> :

```
% dig +short dot.dns4all.eu RESINFO
"qnamemin exterr=0-1,3,5-12,18,20 infourl=https://dns4all.eu"
```

Et, comme vous le voyez plus haut, j'en ai mis un dans mon résolveur <https://doh.bortzmeyer.fr/policy>. Le logiciel du serveur primaire ne connaissant pas encore ce type, j'ai utilisé la technique des types inconnus du RFC 3597 :

```
; Pour le résolveur public :
; Type RESINFO (RFC 9606), enregistré à l'IANA mais pas encore connu des logiciels
radia IN TYPE261 \# 50 08716e616d656d696e 28696e666f75726c3d68747470733a2f2f646f682e626f72747a6d657965722e66722f
```

Cette série de chiffres hexadécimaux ayant été produite à partir de la version texte et du programme . On note que, comme ce résolveur public n'est pas menteur, je n'indique pas d'EDE ("*Extended DNS Errors*", RFC 8914).