RFC 8749 : Moving DNSSEC Lookaside Validation (DLV) to Historic Status

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 mars 2020

Date de publication du RFC : Mars 2020

https://www.bortzmeyer.org/8749.html

DLV ("*DNSSEC Lookaside Validation*") était un mécanisme permettant de contourner le fait que plusieurs zones DNS importantes, dont la racine, n'étaient pas signées. Jamais très utilisé, et aujourd'hui inutile, DLV est ici officiellement abandonné, et les RFC le décrivant sont reclassés « intérêt historique seulement ».

Normalement, DNSSEC (RFC 4033 [1] et suivants) suit le modèle de confiance du DNS. La résolution DNS part de la racine, puis descend vers les domaines de premier niveau, de deuxième niveau, etc. De même, un résolveur validant avec DNSSEC connait la clé publique de la racine, s'en sert pour valider la clé du premier niveau, qui sert ensuite pour valider la clé du deuxième niveau, etc. C'est ainsi que DNSSEC était prévu, et qu'il fonctionne aujourd'hui. Mais il y a eu une période de transition, pendant laquelle la racine, et la plupart des TLD, n'étaient pas signés. Le résolveur validant aurait donc dû gérer autant de clés publiques qu'il y avait de zones signées. Pour éviter cela, DLV ("*DNSSEC Lookaside Validation*") avait été créé. Le principe de DLV était de mettre les clés des zones signées dans une zone spéciale (par exemple `dlv.operator.example`) et que les résolveurs cherchent les clés à cet endroit. Ainsi, le résolveur validant n'avait besoin que de la clé de la zone DLV. DLV a bien rempli son rôle, et a sérieusement aidé au déploiement de DNSSEC. Mais, aujourd'hui, les choses sont différentes, la racine (depuis 2010 <https://www.bortzmeyer.org/la-racine-commence-signature.html>) et tous les TLD importants sont signés (1 389 TLD sur 1 531 sont signés, `.fr` l'a également été en 2010), et DLV n'a donc plus de raison d'être.

Bien sûr, il reste encore des zones de délégation non signées et donc en théorie des gens qui pourraient avoir besoin de DLV. Mais le consensus était clair à l'IETF sur l'abandon de DLV, car (section 3 de notre RFC) :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc4033.txt`

— Le maintien de DLV risque de décourager les zones manquantes de signer (« pas la peine, les gens n'ont qu'à utiliser DLV »),
— Toute occasion de simplifier le code des résolveurs (plus besoin du cas spécial de DLV) est bonne à prendre, et améliore la sécurité,
— D'ailleurs, tous les résolveurs n'ont pas DLV et donc, de toute façon, il ne remplace pas un chemin de validation « normal ».

Il n'y avait en pratique d'une seule zone DLV sérieuse, `dlv.isc.org`, et elle a été arrêtée en 2017, il ne reste donc de toute façon plus d'utilisateurs connus de DLV.

Donc (section 4 de notre RFC), les deux RFC qui décrivaient DLV, le RFC 4431 et le RFC 5074 passent du statut « Pour information » à celui de « Intérêt historique seulement ». (Vous pouvez consulter les détails du processus <`https://datatracker.ietf.org/doc/status-change-dlv-to-historic/`>.) Même chose pour le type d'enregistrement DNS `DLV` (code 32769), qui apparait désormais dans le registre IANA <`https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-parameters-4`> comme "*(OBSOLETE)*".