

Des résolveurs DNSSEC validant publiquement accessibles ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 27 juillet 2010

<https://www.bortzmeyer.org/resolveurs-dnssec.html>

La récente signature de la racine du DNS, complétée le 15 juillet, a ravivé l'intérêt pour la **validation** des signatures DNSSEC, le service qui vérifie que la signature d'un nom de domaine est correcte, et qui met le bit AD ("*Authentic Data*" à 1 dans la réponse DNS. Installer un tel résolveur validant n'est pas trop difficile (voir par exemple mes articles « Unbound, un autre résolveur DNS <<https://www.bortzmeyer.org/unbound.html>> » ou « Valider la racine du DNS <<https://www.bortzmeyer.org/valider-racine.html>> »). Mais il est encore plus simple d'utiliser un résolveur existant et publiquement accessible.

En voici une liste partielle, ne comportant que des résolveurs que j'ai testé. Lisez bien la documentation de chacun notamment pour voir les clés de confiance ("*trust anchor*") qu'il utilise.

- L'ODVR de l'OARC <<https://www.dns-oarc.net/oarc/services/odvr>>, accessible en IPv4 et IPv6,
- Les résolveurs de Hauke Lampe, 85.10.240.249 (unbound.resolvers.openchaos.org) et 85.10.240.250 (bind.resolvers.openchaos.org) qui utilisent le banc de test de .de en plus de la racine et de DLV.

Autrement, il n'existe que des résolveurs réservés aux clients d'un FAI comme celui de Comcast <<http://www.dnssec.comcast.net/>> ou bien spécifiques à un domaine comme celui de DENIC <<http://www.denic.de/en/domains/dnssec/status/resolver-configuration.html>> pour .de (dans ce dernier cas, on peut toujours configurer son résolveur, par exemple avec la directive `forward` de BIND ou Unbound, pour utiliser ces serveurs DNSSEC au lieu des serveurs normaux).

Il existe de bonnes raisons à ce manque de serveurs publics, exposés dans le RFC 5358¹. Pour éviter les problèmes décrits dans le RFC, le service de l'OARC est limité en débit.

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc5358.txt>