RFC 7793 : Add 100.64.0.0/10 prefixes to IPv4 Locally-Served DNS Zones Registry

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 mai 2016

Date de publication du RFC : Mai 2016

https://www.bortzmeyer.org/7793.html

Il existe un registre <https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xml> des zones DNS qui doivent être gérées localement par le résolveur DNS et pour lesquelles les requêtes ne sont pas transmises aux serveurs de la racine. Ce nouveau RFC ajoute à ce registre les zones correspondant au préfixe IPv4 `100.64.0.0/10`, que le RFC 6598 [1] avait réservé pour la numérotation des machines situées derrière les CGN.

Le but de ce registre est d'éviter de surcharger les serveurs racine avec des requêtes qui sont inutiles puisque les noms dans ces zones n'ont qu'une signification locale, et ne pourraient pas recevoir une réponse sensée de la racine. Le RFC 6303 avait donc créé ce registre des noms pour lesquels, par défaut, le résolveur DNS doit retourner `NXDOMAIN` (code indiquant que le nom n'existe pas) tout de suite. On y trouve par exemple la zone `10.in-addr.arpa`, zone correspondant aux adresses IP du RFC 1918.

Le RFC 6598 avait réservé tout le préfixe `100.64.0.0/10` pour les CGN. Notre nouveau RFC met donc les zones `64.100.in-addr.arpa` à `127.100.in-addr.arpa` dans le registre des zones à servir localement <https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zon xml>. Au fur et à mesure des mises à jour des résolveurs (leur code, ou bien la configuration locale), toute requête `PTR` dans une de ces zones doit être traitée localement par le résolveur.

Ces zones sont déléguées aux serveurs de noms de l'IANA, pour attraper les requêtes qui ne suivent pas ces règles :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6598.txt`

```
% dig +short NS 64.100.in-addr.arpa
a.iana-servers.net.
b.iana-servers.net.
c.iana-servers.net.
```

Sinon, aujourd'hui, par défaut, Unbound « délègue » ces zones à... `localhost` (si on veut un vrai contenu, il faut configurer explicitement ces zones) :

```
% dig +short NS 64.100.in-addr.arpa
localhost.
```

BIND les délègue à un serveur inexistant, portant le nom de la zone :

```
% dig +short  NS 64.100.in-addr.arpa
64.100.IN-ADDR.ARPA.
```