RFC 6303 : Locally-served DNS Zones

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 juillet 2011

Date de publication du RFC : Juillet 2011

http://www.bortzmeyer.org/6303.html

Autrefois, les serveurs DNS **récursifs**, ceux qui, installés sur un réseau local ou chez un FAI pour ses abonnés, répondent aux requêtes DNS des clients finaux, ne servaient par défaut aucune zone. Tout était demandé aux serveurs DNS faisant autorité, sauf des zones locales configurées à la main. Le problème est que certaines zones privées très répandues étaient oubliées, et que le récurseur allait alors embêter les serveurs faisant autorité avec ces requêtes qui auraient dû rester locales. Ce nouveau RFC demande donc que, par défaut, sans aucune configuration explicite, les récurseurs fassent autorité pour certaines zones locales.

Un exemple typique est celui d'un réseau local numéroté avec les adresses IP privées du RFC 1918 [1], mettons `172.27.0.0/16`. Les machines dudit réseau reçoivent en DHCP l'adresse d'un serveur DNS récursif local. Celui-ci, avant la sortie de notre RFC 6303, ne connaissait pas `27.172.in-adr.arpa`, le domaine utilisé pour les résolutions d'adresses IP en noms. Il va donc transmettre ces requêtes aux serveurs publics, en l'occurrence ceux de l'AS112 (RFC 7534), les faisant travailler pour rien. La bonne pratique, depuis toujours, est que l'administrateur système local ajoute la zone `27.172.in-adr.arpa` à son récurseur. Mais incompétence, manque de temps et négligence (quelqu'un d'autre paie...) se conjuguent pour faire que c'est rarement déployé. L'idée de notre RFC 6303 est donc de déplacer le travail depuis les nombreux administrateurs réseaux vers les nettement moins nombreux auteurs de logiciels serveurs.

La section 3 du RFC décrit le changement chez les résolveurs. Ceux-ci devront répondre avec autorité `NXDOMAIN` (code de réponse 3), indiquant que le nom demandé n'existe pas. Une façon triviale d'implémenter ce comportement est de servir des zones vides, plus exactement, ne contenant que des SOA et des NS (exactement ce que fait l'AS112, cf. RFC 7534). La valeur recommandée pour le SOA et pour les NS est le nom de la zone et, pour l'adresse de contact, `nobody@invalid`. Le SOA est nécessaire pour le cache des réponses négatives (et pour les machines qui tiennent à tenter des mises à jour dynamiques du DNS, qui ont également besoin des NS). Sous forme d'un fichier de zone standard, cela donne (avec un TTL de trois heures) :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc1918.txt`

```
@ 10800 IN SOA @ nobody.invalid. 1 3600 1200 604800 10800
@ 10800 IN NS @
```

Ce comportement **doit** être débrayable, de préférence zone par zone, pour le cas des sites qui utilisent les adresses privées et ont configuré leurs serveurs DNS pour résoudre ces adresses en noms.

La liste initiale des zones à servir figure en section 4. Elle sert de point de départ au registre IANA, <https://www.iana.org/assignments/locally-served-dns-zones/locally-served-dns-zones.xml>, qui est la source faisant autorité (les auteurs de logiciels devraient donc le consulter avant des nouvelles publications de leur logiciel). Le registre est mis à jour (cf. section 6) par le processus « *"IETF review"* » décrit dans le RFC 5226, avec un appel au conservatisme : une fois ajoutée au registre, une zone ne pourra jamais être retirée, puisqu'il faudrait mettre à jour tous les logiciels. Il faut donc réfléchir longtemps avant d'ajouter une zone.

Aujourd'hui, ce registre inclut notamment les zones `in-addr.arpa` correspondant au RFC 1918 et celles correspondant aux réseaux du registre documenté dans le RFC 6890 , qui ne sont pas censés apparaître publiquement (comme les réseaux réservés pour la documentation). Il y a aussi des zones `ip6.arpa` (domaine utilisé pour la résolution d'adresses IPv6 en noms), comme celles des ULA du RFC 4193 (premier RFC à avoir normalisé cette pratique pour les résolveurs DNS, pour le domaine `d.f.ip6.arpa`), celles des adresses locales au lien (RFC 4291, section 2.5.6, un exemple étant `8.e.f.ip6.arpa`), et celle du réseau réservé pour la documentation (RFC 3849).

En revanche, certaines zones ne sont **pas** incluses (section 5) comme les anciennes adresses locales au site d'IPv6 (RFC 4291, sections 2.4 et 2.5.7) ou comme des zones plus controversées comme les TLD numériques (pour traiter le cas des logiciels qui feraient des résolutions pour ces adresses, en les prenant pour des noms).

Suivre les recommandations de ce RFC peut-il avoir des effets négatifs ? La section 2 examine le cas. Comme les serveurs sont incités à ne servir les zones privées que si elles n'ont pas été configurées explicitement, les sites qui utilisent le RFC 1918 et ont peuplé les zones en `in-addr.arpa` ne devraient pas avoir de problème. La section 2 conclut que le problème ne se posera que dans un seul cas, les sites qui utilisent une délégation (typiquement depuis une racine locale, non connectée à l'Internet), sans que les résolveurs ne le voient. Ceux-ci devront explicitement reconfigurer leurs résolveurs pour ne pas servir les zones vides désormais installées par défaut.

Aujourd'hui, plusieurs récurseurs mettent déjà en œuvre ce RFC. C'est le cas par exemple d'Unbound (testé avec la 1.4.9). Un commentaire dans le fichier de configuration livré avec ce serveur dit :

```
# defaults are localhost address, reverse for 127.0.0.1 and ::1
# and nxdomain for AS112 zones. If you configure one of these zones
# the default content is omitted, or you can omit it with 'nodefault'.
```

Le commentaire ne semble pas tout à fait correct, Unbound sert aussi par défaut des zones qui ne sont pas gérées par l'AS112 (comme les adresses réservées à la documentation). Voici sa réponse par défaut, lors d'une tentative de trouver le nom correspondant à l'adresse IP `172.27.1.1` :

```
% dig -x 172.27.1.1
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 8856
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; AUTHORITY SECTION:
27.172.in-addr.arpa. 10800 IN SOA localhost. nobody.invalid. 1 3600 1200 604800 10800

;; Query time: 67 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Jul  8 17:47:21 2011
;; MSG SIZE  rcvd: 111
```

À noter que `localhost` est mis comme nom de serveur maître, pas `27.172.in-addr.arpa` comme le demande le RFC (et je n'ai pas trouvé de moyen de le configurer). Pour le cas cité dans la section 2, où on veut interroger les serveurs faisant normalement autorité, on peut simplement mettre dans la configuration :

```
        local-zone: "27.172.in-addr.arpa" nodefault
```

et la zone `27.172.in-addr.arpa` ne sera plus traitée comme spéciale, elle ne suivra plus ce RFC.

BIND (testé en version 9.8.0-P2) reconnait un certain nombre de zones automatiquement remplies et prévient au démarrage :

```
08-Jul-2011 19:43:59.410 automatic empty zone: 2.0.192.IN-ADDR.ARPA
08-Jul-2011 19:43:59.410 automatic empty zone: 100.51.198.IN-ADDR.ARPA
08-Jul-2011 19:43:59.410 automatic empty zone: 113.0.203.IN-ADDR.ARPA
...
```

Mais cette liste ne comprend pas encore les zones du RFC 1918. Voici le résultat en interrogeant les zones spéciales pour BIND :

```
% dig -x 192.0.2.1
...
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 22522
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
...
;; AUTHORITY SECTION:
2.0.192.in-addr.arpa. 86400 IN SOA 2.0.192.in-addr.arpa. . 0 28800 7200 604800 86400

;; Query time: 1 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Jul  8 19:45:03 2011
;; MSG SIZE  rcvd: 86
```

On note que BIND ne respecte pas encore le RFC (l'adresse de contact n'est pas `nobody@invalid`) et que sa liste de zones spéciales n'est pas encore celle du registre IANA. Toutefois, tout cela est modifiable. Regardez la section « *"Built-in Empty Zones"* » de l'ARM (*"Administrator Reference Manual"*). Par exemple, vous pouvez changer l'adresse de contact avec `empty-contact nobody@invalid` dans la section `options`. Vous pouvez désactiver le comportement spécial pour une zone avec `disable-empty-zone 2.0.192.in-addr.arpa` dans la même section (l'équivalent du `nodefault` d'Unbound). Et bien d'autres possibilités.