RFC 9432 : DNS Catalog Zones

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 mars 2024

Date de publication du RFC : Juillet 2023

https://www.bortzmeyer.org/9432.html

L'idée de base de ces « zones catalogue » est d'automatiser la configuration d'une nouvelle zone DNS sur les serveurs secondaires <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>, en publiant dans le DNS les caractéristiques des zones qu'ils devront servir. Cela concerne donc surtout les gros hébergeurs qui ont beaucoup de zones.

Petit rappel : une zone, dans le DNS, est une partie contigüe de l'arbre des noms de domaine, gérée comme un tout (mêmes serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autori
html>). Ainsi, si vous venez de louer le nom machin.example, un hébergeur DNS va configurer ses serveurs pour faire autorité pour ce nom. Par exemple, avec le logiciel NSD, sur le primaire (serveur maitre) :

```
zone:
        name: "machin.example"
        zonefile: "primary/machin.example"
        # Les serveurs secondaires :
        notify: 2001:db8:1::53
        provide-xfr: 2001:db8:1::53
        ...
```

Et, sur un serveur secondaire (serveur esclave), qui transférera la zone depuis le primaire (RFC 5936 [1]) :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5936.txt

```
zone:
   name: "machin.example"
   # Le primaire :
   allow-notify: 2001:db8:cafe::1 NOKEY
   request-xfr: AXFR 2001:db8:cafe::1 NOKEY
```

Si on gère beaucoup de zones, avec des ajouts et des retraits tout le temps, l'avitaillement manuel est long et risqué (et si on oublie un serveur ?). Éditer ces fichiers sur tous les serveurs secondaires devient vite pénible. Et si les logiciels sur les secondaires sont différents les uns des autres (ce qui est recommandé, pour la robustesse), il faut se souvenir des différentes syntaxes. Pourquoi faire manuellement ce qu'on peut automatiser ? C'est le principe des zones catalogue.

Le principe est simple : une zone catalogue est une zone comme une autre, produite par les mêmes mécanismes (par exemple emacs) et qui sera servie par un serveur primaire à tous les secondaires, qui changeront alors automatiquement leur configuration en fonction du contenu de la zone catalogue. Chaque zone à configurer est un enregistrement de type PTR, dont la partie gauche est une étiquette interne et la partie droite indique le nom de la zone. Ici, on configure la zone `rutaba.ga`, l'étiquette (qui doit être unique) `label1` est à usage interne (section 4.1 du RFC) :

```
label1.zones.catalog.example. IN PTR rutaba.ga.
```

Le reste est listé sous forme de propriétés (section 4.2). Une propriété évidente est l'adresse IP du primaire. Pour l'instant, elle doit être indiquée via le composant `ext` qui désigne les propriétés pas encore normalisées :

```
primaries.ext.catalog.example.    IN AAAA 2001:db8:bad:dcaf::42
```

La liste des propriétés figure dans un registre IANA <https://www.iana.org/assignments/dns-parameters/dns-parameters.xml#dns-catalog-zones>.

À l'heure actuelle, de nombreux logiciels gèrent ces zones catalogues. Le site Web du projet <https://zones.cat/> (pas mis à jour depuis très longtemps) en liste plusieurs <https://zones.cat/implementations.html>.

Voici un exemple complet de zone catalogue :

```
; -*- zone -*-
catalog.example.    IN SOA ns4.bortzmeyer.org. stephane.bortzmeyer.org. 2023120902 900 600 86400 1
catalog.example.    IN NS invalid.   ; Le NS est inutile mais
                         ; obligatoire et "invalid" est la valeur
                         ; recommandée (section 4).
version.catalog.example.    IN TXT "2"  ; Obligatoire, section 4.2.1

label1.zones.catalog.example. IN PTR rutaba.ga.
primaries.ext.catalog.example.    IN AAAA 2001:db8:bad:dcaf::42
```

La configuration de BIND pour l'utiliser :

```
# La zone catalogue se charge comme n'importe quelle zone. Ceci dit,
# vu le caractère critique de la zone catalogue, la section 7 du RFC
# insiste sur l'importance de sécuriser ce transfert, par exemple avec
# TSIG (RFC 8945) :
zone "catalog.example" {
        type slave;
        file "catalog.example";
        masters {
              2001:db8:666::;
        };

};

# Et, ici, on la désigne comme spéciale :
options {
   ...
   catalog-zones {
     zone "catalog.example"
              in-memory no;
   };
};
```

Naturellement, comme toujours lorsque on automatise, on risque le syndrome de l'apprenti sorcier. Attention donc en générant la zone catalogue. Comme le note le RFC (section 6) : « *"Great power comes with great responsibility. Catalog zones simplify zone provisioning by orchestrating zones on secondary name servers from a single data source : the catalog. Hence, the catalog producer has great power and changes must be treated carefully. For example, if the catalog is generated by some script and this script generates an empty catalog, millions of member zones may get deleted from their secondaries within seconds, and all the affected domains may be offline in a blink of an eye."* »