# Récupérer une zone DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 décembre 2006. Dernière mise à jour le 16 décembre 2008

https://www.bortzmeyer.org/recuperer-zone-dns.html

---

Il est fréquent que l'on souhaite étudier le contenu d'une zone DNS. Il existe un mécanisme standard pour les transférer (cf. RFC 5936 [1]) mais la plupart des serveurs de noms refusent désormais ce transfert. Il est donc préférable d'automatiser les essais.

Le contenu d'une zone DNS permet de savoir le nombre d'enregistrements dans la zone (par exemple, on voit que le domaine de l'ex-Yougoslavie, `.yu`, que l'IANA, voudrait supprimer <https://www.icann.org/announcements/announcement-2-05dec06.htm> contient encore des dizaines de milliers de domaines), permet de les étudier en détail, peut permettre de détecter des bogues. Par exemple, il y a peu, <http://louvre.museum/> était inaccessible une fois sur deux car la vraie adresse IP du serveur Web avait été mise dans le fichier de zone de `.museum` en même temps que l'adresse IP « attrape-tout » de `.museum`, celle qui sert à récupérer les fautes de frappe. En récupérant le fichier de la zone `.museum`, le diagnostic a été bien plus facile à faire.

Mais cela peut être jugé très indiscret : on comprend que de nombreux gestionnaires de zone refusent tout accès à cette zone (c'est le cas de presque tous les registres européens). Ou qu'ils le fassent payer (c'est le cas des gros TLD commerciaux). Pour cette raison et aussi pour des raisons plus pratiques (un transfert de zone peut prendre pas mal de ressources, notamment si la zone est grosse), le transfert de zone est en général désactivé sur la plupart des serveurs de noms.

Lorsqu'on cherche à obtenir une zone, il est donc pénible d'essayer les serveurs un par un. Pour la racine du DNS, par exemple, seuls deux serveurs sur les treize acceptent aujourd'hui le transfert. D'où l'idée d'une simple automatisation, avec ce petit script shell qui s'utilise ainsi :

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

```
% try-get-zone fr
No willing nameservers from which to transfer fr

% try-get-zone museum
Got museum from ns1.getty.edu.
```

Ici, je n'ai pu obtenir `.fr`, protégé, mais `.museum` est accessible.

Voici le script : (en ligne sur `https://www.bortzmeyer.org/files/try-get-zone.sh`)

Attention en interprétant les résultats : certains TLD comme `.uk` ou `.jp` n'enregistrent qu'au troisième niveau (`co.uk` ou `or.uk` pour les britanniques). Même si on réussit à transférer le fichier de zone du TLD, le nombre d'enregistrements n'est donc pas forcément le bon (merci à Elisabeth Porteneuve pour avoir noté ce problème dans un test précédent).

Une autre question est à garder en mémoire : s'il ne fait aucun doute que certaines zones sont transférables délibérement, dans d'autres cas, c'est simplement le responsable technique qui a fait une erreur, rendant la zone accessible sans s'en rendre compte. Il est normal dans ce cas de le prévenir...

Une autre solution, mais qui est assez « limite » est, pour les zones signées avec DNSSEC, d'utiliser le parcours de zone ("*zone walking*"). Cette technique utilise le fait que DNSSEC permet, lorsqu'un nom de domaine n'existe pas dans la zone, de récupérer le nom du domaine suivant qui existe. De proche en proche, on peut ainsi dérouler toute la zone. Cette technique peut être mise en œuvre par un script comme celui de Kim-Minh Kaplan :

```
#!/bin/sh
# $Id: dnssec-walk.sh,v 1.6 2008/12/16 17:20:02 kaplan Exp $
if test $# -lt 1 -o $# -gt 2
then
    echo "usage: $0 <zone> [<resolver>]" >&2
    exit 1
fi
zone=${1%.}.
resolver=
if test $# -eq 2
then
    resolver=@${2#@}
fi

pred=$zone
step=$pred
set -- `dig +short +dnssec $resolver $step NSEC`
while test "$1" != "$zone"
do
    if test -z "$1"             # Walk next if NSEC not served
    then
        label=${step%.$zone}
        step=$label-.$zone
        set -- `dig +dnssec $resolver $step NSEC | grep ^$pred.*NSEC`
        if test "$1" == "$pred"
        then
            shift
            shift
            shift
            shift
        else
            echo $1 !!!
        fi
```

```
    else
        pred=$1
        step=$1
        echo $pred
        set -- `dig +short +dnssec $resolver $pred NSEC`
    fi
done
```

Elle est également implémentée dans le logiciel DNSSEC walker <http://josefsson.org/walker/> et aussi comme exemple ldns <http://www.nlnetlabs.nl/svn/ldns/trunk/examples/ldns-walk.c>.

Attention, cette façon de récupérer la zone n'est probablement pas conforme aux conditions d'accès du registre. En outre, certains registres mettent en œuvre des restrictions qui empêchent le "*walker*" de fonctionner.

Un bon article sur les risques de sécurité associés au transfert de zone, avec une jolie zone ouverte pour la démonstration, est « "*ZoneTransfer.me*" <http://www.digininja.org/projects/zonetransferme.php> ».