Bien maitriser ses chaines de dépendance DNS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 septembre 2024

https://www.bortzmeyer.org/chaine-dns.html

Le DNS repose sur un système de délégation, avec des **dépendances** qui ne sont pas toujours maitrisées. (Si vous êtes responsables d'un nom de domaine, veillez à connaitre ces dépendances et à les examiner !) Un exemple concret aujourd'hui avec `telehouse.fr`.

Ce nom de domaine est utilisé par le gérant de centres de données pour certains services à destination des clients (un portail clients, par exemple). Ce matin, il ne répond pas (dans l'après-midi, tout remarchait) :

```
% dig telehouse.fr
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 44602
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
...
;; Query time: 4000 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Sep 24 11:13:46 CEST 2024
;; MSG SIZE  rcvd: 41
```

SERVFAIL signifie "*SERVer FAILure*" et, comme ce nom l'indique, c'est mauvais. Si on demande à un autre résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> qui met en œuvre les rapports d'erreur détaillés (RFC 8914 [1]), on a :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8914.txt

```
% dig @1.1.1.1 telehouse.fr
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 20599
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; EDE: 22 (No Reachable Authority): (at delegation telehouse.fr.)
...
;; Query time: 4256 msec
;; SERVER: 1.1.1.1#53(1.1.1.1) (UDP)
;; WHEN: Tue Sep 24 11:14:37 CEST 2024
;; MSG SIZE  rcvd: 74
```

L'EDE ("*Extended DNS Error*") nous dit que le résolveur n'a pu joindre aucun des serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>. On va donc devoir creuser. D'abord, quels sont ces serveurs faisant autorité pour `telehouse.fr` ? Demandons à un des serveurs du domaine parent `.fr` :

```
% dig @d.nic.fr telehouse.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21940
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 1
;; WARNING: recursion requested but not available
...
;; AUTHORITY SECTION:
telehouse.fr.  3600 IN NS ns1.fr.kddi.com.
telehouse.fr.  3600 IN NS ns2.fr.kddi.com.
```

Bien, nous avons les noms de ces serveurs, interrogeons-les :

```
% dig ns1.fr.kddi.com.
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 20153
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
...
;; Query time: 12 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Sep 24 11:15:12 CEST 2024
;; MSG SIZE  rcvd: 44
```

Ah, raté, on ne peut pas résoudre le nom du serveur de noms. Le serveur est toujours là et, si on connait son adresse IP (par exemple parce qu'elle est encore dans la mémoire du résolveur), on peut l'interroger :

```
%  dig @85.90.48.10 telehouse.fr
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15119
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
...
;; ANSWER SECTION:
telehouse.fr.  900 IN A 85.90.40.15
```

Bon, et si on n'a pas cette adresse IP ? Demandons au domaine parent :

```
% dig kddi.com NS
...
;; ANSWER SECTION:
kddi.com.  85645 IN NS dnsa01.kddi.ne.jp.
kddi.com.  85645 IN NS dnsa02.kddi.ne.jp.
kddi.com.  85645 IN NS dns103.kddi.ne.jp.
kddi.com.  85645 IN NS dns104.kddi.ne.jp.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Sep 24 11:15:33 CEST 2024
;; MSG SIZE  rcvd: 131
```

Et interrogeons-les :

```
% dig @dnsa01.kddi.ne.jp. fr.kddi.com  NS
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43194
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available
...
;; AUTHORITY SECTION:
fr.kddi.com.  86400 IN NS ns1.kddi-telehouse.eu.
fr.kddi.com.  86400 IN NS ns2.kddi-telehouse.eu.

;; Query time: 216 msec
;; SERVER: 54.64.39.199#53(dnsa01.kddi.ne.jp.) (UDP)
;; WHEN: Tue Sep 24 11:15:57 CEST 2024
;; MSG SIZE  rcvd: 121
```

Et suivons cette délégation :

```
% dig ns1.kddi-telehouse.eu.
...
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 48644
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
...
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Tue Sep 24 11:16:11 CEST 2024
;; MSG SIZE  rcvd: 50
```

Bon, même problème, le nom du serveur de noms ne peut pas être résolu. Poursuivons notre quête auprès des serveurs de `.eu` :