PowerDNS

DNS Flag Day : Votre serveur est-il prêt ?

Rémi Gacogne – Senior PowerDNS Engineer

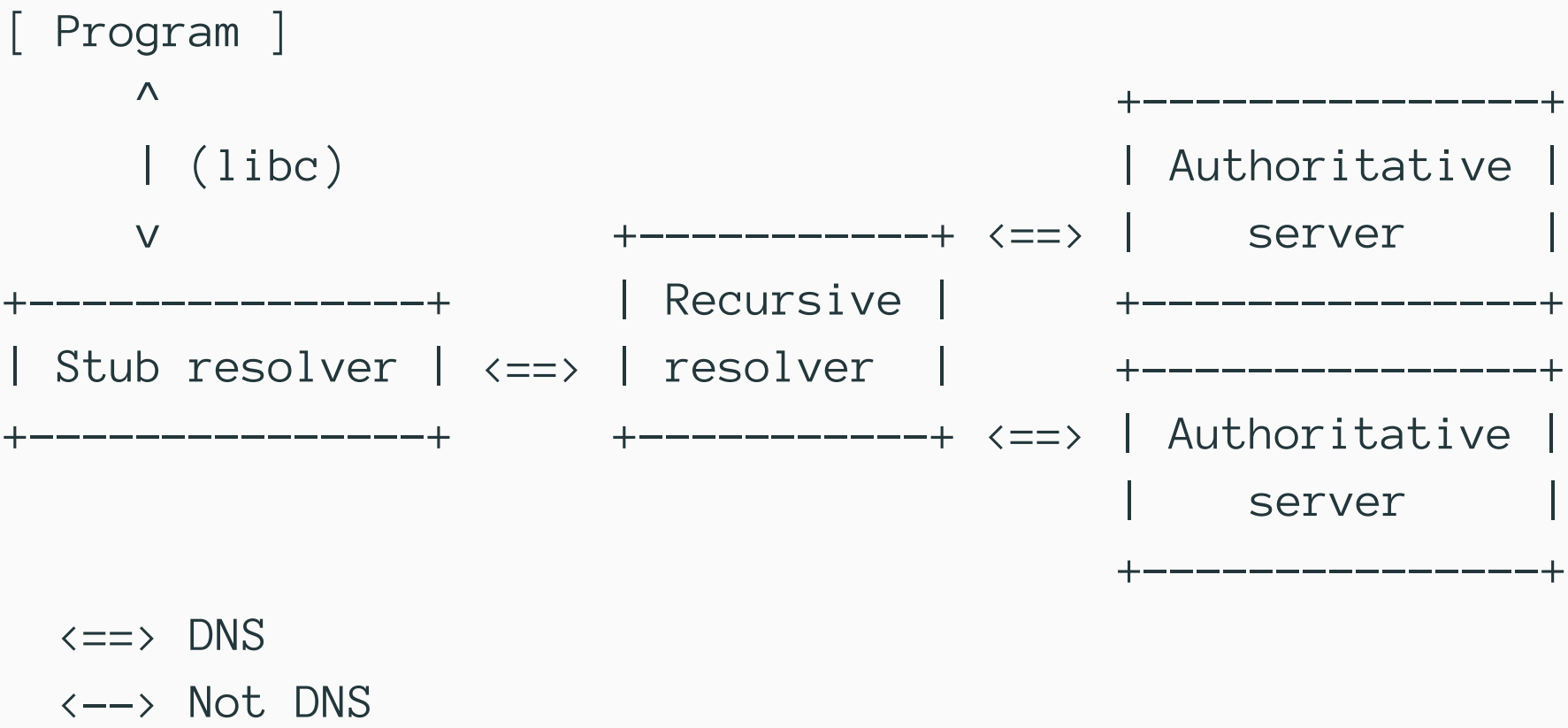
FRnOG 31, 5 octobre 2018

Qu'est-ce ?

La suppression, dans les serveurs DNS récursifs, du code pour gérer les serveurs faisant autorité ne répondant pas **correctement** aux requêtes avec *EDNS*[1]

[1] RFC 2671, datant de 1999, mise à jour par la RFC 6891

Les serveurs quoi ?



EDNS ?

- Un meta-enregistrement *OPT* est ajouté à la requête
- Si le récepteur ne supporte pas *EDNS*, il doit répondre avec *FORMERR*
- Sinon la réponse doit également contenir un meta-enregistrement *OPT*

EDNS ?

- Permet au client d'annoncer la taille maximum d'une réponse transportée par UDP (*UDP Payload Size*)
- Nécessaire pour DNSSEC, qui assure l'intégrité des réponses
- Extensions (Cookies, Client Subnet, ...)

Qu'est ce qu'un serveur ne gérant pas correctement EDNS ?

- Pas de réponse (timeout) sur une requête *EDNS*, impossible à distinguer d'un paquet perdu
- Réponse avec un code d'erreur autre que *FORMERR* lorsque *EDNS* n'est pas implémenté (*SERVFAIL*, *NOTIMP*, *NXDOMAIN*, réponse vide..)
- Pas d'*EDNS* dans la réponse, mais pas d'erreur non plus
- Le contenu de l'enregistrement *OPT* de la requête copié à l'identique dans la réponse

Pourquoi changer ce qui fonctionne ?

- Réduire la complexité du code
- Diminuer la latence pour les utilisateurs
- Permettre au DNS d'évoluer

Qui ?

Plusieurs éditeurs de serveurs DNS Open Source :

- Internet Systems Consortium (BIND)
- CZ.NIC (Knot Resolver)
- NLNetLabs (Unbound)
- PowerDNS (PowerDNS Recursor)

Quel impact ?

- Pour la majorité des domaines, aucun
- Pour ceux servis par des serveurs ne gérant pas correctement *EDNS*, ou placés derrière un pare-feu mal configuré : résolution lente voire impossible

Comment tester ?

https://ednscomp.isc.org/ednscomp/

Comment tester ? – loadays.org

EDNS Compliance Tester

Checking: 'loadays.org' as at 2018-04-17T21:06:10Z

loadays.org @149.202.166.43 (ns01.multihost.be.): edns=ok edns1=ok edns@512=ok ednsopt=ok edns1opt=ok do=ok ednsflags=ok docookie=ok edns@512tcp=ok optlist=ok

loadays.org @37.187.243.140 (ns03.multihost.be.): edns=ok edns1=ok edns@512=ok ednsopt=ok edns1opt=ok do=ok ednsflags=ok docookie=ok edns@512tcp=ok optlist=ok

All Ok

Codes

- *ok* - test passed.

Comment tester – google.com

EDNS Compliance Tester

Checking: 'google.com' as at 2018-04-17T21:23:04Z

google.com @216.239.32.10 (ns1.google.com.): edns=noopt edns1=status,noopt,soa edns@512=noopt ednsopt=noopt edns1opt=status,noopt,soa do=noopt ednsflags=noopt docookie=noopt edns@512tcp=noopt optlist=subnet
google.com @2001:4860:4802:32::a (ns1.google.com.): edns=noopt,ipv6 edns1=status,noopt,soa edns@512=noopt ednsopt=noopt edns1opt=status,noopt,soa do=noopt ednsflags=noopt docookie=noopt edns@512tcp=noopt optlist=subnet

google.com @216.239.34.10 (ns2.google.com.): edns=noopt edns1=status,noopt,soa edns@512=noopt ednsopt=noopt edns1opt=status,noopt,soa do=noopt ednsflags=noopt docookie=noopt edns@512tcp=noopt optlist=subnet
google.com @2001:4860:4802:34::a (ns2.google.com.): edns=noopt,ipv6 edns1=status,noopt,soa edns@512=noopt ednsopt=noopt edns1opt=status,noopt,soa do=noopt ednsflags=noopt docookie=noopt edns@512tcp=noopt optlist=subnet

google.com @216.239.36.10 (ns3.google.com.): edns=noopt edns1=status,noopt,soa edns@512=noopt ednsopt=noopt edns1opt=status,noopt,soa do=noopt ednsflags=noopt docookie=noopt edns@512tcp=noopt optlist=subnet
google.com @2001:4860:4802:36::a (ns3.google.com.): edns=noopt,ipv6 edns1=status,noopt,soa edns@512=noopt ednsopt=noopt edns1opt=status,noopt,soa do=noopt ednsflags=noopt docookie=noopt edns@512tcp=noopt optlist=subnet

google.com @216.239.38.10 (ns4.google.com.): edns=noopt edns1=status,noopt,soa edns@512=noopt ednsopt=noopt edns1opt=status,noopt,soa do=noopt ednsflags=noopt docookie=noopt edns@512tcp=noopt optlist=subnet
google.com @2001:4860:4802:38::a (ns4.google.com.): edns=noopt,ipv6 edns1=status,noopt,soa edns@512=noopt ednsopt=noopt edns1opt=status,noopt,soa do=noopt ednsflags=noopt

Comment tester – mateksys.com

Checking: 'mateksys.com' as at 2018-04-09T19:47:11Z

mateksys.com @106.11.211.53 (dns7.hichina.com.): edns=ok **edns1=timeout** edns@512=ok **ednsopt=timeout** **edns1opt=timeout** do=ok ednsflags=ok **docoo**
edns@512tcp=timeout **optlist=timeout**
mateksys.com @106.11.141.123 (dns7.hichina.com.): edns=ok **edns1=timeout** edns@512=ok **ednsopt=timeout** **edns1opt=timeout** do=ok ednsflags=ok **doco**
edns@512tcp=timeout **optlist=timeout**
mateksys.com @106.11.141.113 (dns7.hichina.com.): edns=ok **edns1=timeout** edns@512=ok **ednsopt=timeout** **edns1opt=timeout** do=ok ednsflags=ok **doco**
edns@512tcp=timeout **optlist=timeout**
mateksys.com @140.205.81.13 (dns7.hichina.com.): edns=ok **edns1=timeout** edns@512=ok **ednsopt=timeout** **edns1opt=timeout** do=ok ednsflags=ok **docoo**
edns@512tcp=timeout **optlist=timeout**

Que faire ?

- Mettre à jour !
  - Bind 9.12+
  - Knot (toutes versions)
  - NSD 1.0.0+
  - PowerDNS Authoritative Server 4.0+
- Vérifier la configuration des pare-feux et autre boites

Quand ?

Le 1 février 2019

Testez vos domaines

Mettez vos serveurs à jour, et gardez-les à jour !

Questions ?

Merci !