Labo DNS : dig, partie 1

Dans les laboratoires qui suivent, nous allons utiliser "auth1" comme machine de travail. En réalité, ce n'est pas très important, car nous allons seulement utiliser la commande 'dig'.

DIG
---

1. émettre des requêtes DNS à l'aide de 'dig':

Remarque: assurez-vous que vous spécifiez explicitement le serveur de noms à
interroger à l'aide de la syntaxe "@" de dig:

    $ dig @ip_serveur ...

Si vous ne spécifiez pas l'ip du serveur avec @, dig utilisera alors le serveur
de noms(s) listés dans /etc/resolv.conf

1a. Exécutez chaque commande, cherchez la section réponse et notez le résultat.
    Notez le TTL ainsi.

Répétez la commande. Est-ce que la durée de vie est la même ? Les réponses sont
-elles autoritaires?

                                                        Résultat 1
        Résultat 2

    $ dig @10.10.0.254 votre-domaine-prefere a
    $ dig @10.10.0.254 www.google.com. a
    $ dig @10.10.0.254 afnog.org. mx
    $ dig @10.10.0.254 NonExistentDomain.sometld any
    $ dig @10.10.0.254 tiscali.co.uk. txt
    $ dig @10.10.0.254 www.afrinic.net aaaa
    $ dig @10.10.0.254 ipv6.google.com aaaa

1b. Maintenant, envoyer des requêtes vers un autre serveur de cache.

    (Lancer chacune des commandes suivantes deux fois, et noter le temps en ms
        pour chaque tentative)

Résultat 1

Résultat 2

---

dig @8.8.8.8 $ news.bbc.co.uk. a
dig @208.67.222.222 $ yahoo.com. a
$ dig @<a serveur de votre choix> <domain de votre choix> a

Combien de temps a-t-il fallu avant que chaque réponse soit reçue?
(Sur la première, et sur la seconde recherche)

2. Les recherches DNS inverses

Maintenant, essayez quelques recherches DNS inversées - notons ici que nous
ne spécifions pas explicitement les serveurs de noms que dig doit
interroger. Quelle serveur de noms sera utilisé?

$ dig -x 10.10.X.1
$ dig -x 10.10.X.2
$ dig -x 10.10.X.3

... où X est une adresse IP dans la plage 1-25

Répétez l'opération pour une adresse IP de votre choix, sur l'Internet.
Rappelez-vous, vous aurez à utiliser 10.10.0.254 pour être en mesure
d'effectuer des requêtes DNS sur Internet ...

Maintenant, essayez de rechercher:

$ dig 1.X.%REVERSE%.in-addr.arpa. PTR

... où X est dans la gamme de 1 à 25.

Que remarquez-vous?

Essayons maintenant IPv6:

$ dig -x 2001:42d0::200:2:1

Quelles sont les différences que vous pouvez observer dans les résultats,
entre les inverses DNS pour IPv6 et les adresses IPv4?

Remarque: Vous n'obtiendres peut-être pas de réponse pour l'adresse v6 -
mais comparer la section question de la requête pour les adresses IPv4
et IPv6 inverses.

3. DNSSEC et EDNS0

Essayez quelques-unes des questions ci-dessus, mais cette fois ajouter
l'option "+edns=0".

Par exemple:

$ dig @10.10.0.254 www.icann.org +edns=0

(Vous pouvez utiliser "more" pour limiter la sortie de la commande à un écran à la fois)

$ dig @10.10.0.254 www.icann.org +edns=0 | more

Remarquez le PSEUDOSECTION de l'OPT, en début de la réponse ?

Que remarquez-vous dans la section flags: dans la section OPT?

Nous allons activer explicitement l'option BUFSIZE, mais pas EDNS0:

$ dig @10.10.0.254 www.icann.org +bufsize=1024 | more

Notez que EDNS est activé automatiquement, et vous verrez la taille de
la section udp: dans le pseudosection OPT (en haut)

Maintenant, nous allons essayer de récupérer des enregistrements DNSSEC:

$ dig @10.10.0.254 isoc.org DNSKEY | more
$ dig @10.10.0.254 www.isoc.org RRSIG | more

Et enfin, nous allons dire à notre serveur DNS que nous supportons DNSSEC:

$ dig @10.10.0.254 www.isoc.org A +dnssec
$ dig @10.10.0.254 isoc.org NS +dnssec

Avez-vous remarqué un nouveau champ dans les "flags:" de la réponse?

```
$ dig @10.10.0.254 www.isoc.org A
$ dig @10.10.0.254 isoc.org NS
```

Comparer avec dig faire sans l'option +dnssec:

Si votre machine locale fait déjà tourner un serveur de noms, qu'advient-il
si vous lui envoyez des requêtes +dnssec:

```
$ dig @127.0.0.1 noc.dns.nsrc.org A +dnssec
$ dig @127.0.0.1 dns.nsrc.org NS +dnssec
```