DNS SESSION 2 EXERCICE !

Analyse et correction des informations (debugging) des serveurs de noms en utilisant dig +norec

Vous n'avez pas besoin d'être root pour faire cet exercice.
NOTE : c'est toujours pratique de mettre le '.' a la fin du nom – ceci empêche le nom de domaine par défaut du fichier /etc/resolv.conf d'être rajouté

Exemple : tester www.tiscali.co.uk

1. Faire une requête en commençant avec un serveur root

dig +norec @a.root-servers.net. www.tiscali.co.uk. a

```
; <<>> DiG 8.3 <<>> +norec @a.root-servers.net. www.tiscali.co.uk. a
; (1 server found)
;; res options: init defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29971
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 6
;; QUERY SECTION:
;;      www.tiscali.co.uk, type = A, class = IN

;; AUTHORITY SECTION:
uk.                     2D IN NS        NS1.NIC.uk.
uk.                     2D IN NS        NS0.JA.NET.
uk.                     2D IN NS        NS.UU.NET.
uk.                     2D IN NS        SEC-NOM.DNS.UK.PSI.NET.
uk.                     2D IN NS        NS2.NIC.uk.

;; ADDITIONAL SECTION:
NS1.NIC.uk.             2D IN A         195.66.240.130
NS0.JA.NET.             2D IN A         128.86.1.20
NS0.JA.NET.             2D IN A         193.63.94.20
NS.UU.NET.              2D IN A         137.39.1.3
SEC-NOM.DNS.UK.PSI.NET. 2D IN A          154.32.105.90
NS2.NIC.uk.             2D IN A         217.79.164.131

;; Total query time: 662 msec
;; FROM: vaio.linnet.org to SERVER: a.root-servers.net.  198.41.0.4
;; WHEN: Mon Jun  9 09:31:00 2003
;; MSG SIZE  sent: 35  rcvd: 248
```

Note : Nous avons seulement récupéré des enregistrements NS (plus d'autres informations relatives - les enregistrements A qui correspondent à ces serveurs de noms). C'est une RÉFÉRENCE.
Dans la théorie nous devrions répéter cette requête pour b.root-servers.net, c.root-servers.net etc.. et contrôler que nous obtenons les mêmes réponses. De temps en temps les serveurs de racine ont des problèmes.

2. Noter les cinq serveurs de noms que nous avons eu dans la réponse

(se rappeler que les noms utilisés dans le DNS ne sont pas sensibles au type des caracteres; majuscule ou minuscule)
ns1.nic.uk.
ns0.ja.net.
ns.uu.net.
sec-nom.dns.uk.psi.net.
ns2.nic.uk.

3. Répéter la requête pour tous les enregistrements NS tour à tour

```
$ dig +norec @ns1.nic.uk. www.tiscali.co.uk. a
; <<>> DiG 8.3 <<>> +norec @ns1.nic.uk. www.tiscali.co.uk. a
; (1 server found)
;; res options: init defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15102
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1
;; QUERY SECTION:
;;      www.tiscali.co.uk, type = A, class = IN

;; AUTHORITY SECTION:
tiscali.co.uk.          2D IN NS        ns0.tiscali.co.uk.
tiscali.co.uk.          2D IN NS        ns0.as9105.com.

;; ADDITIONAL SECTION:
ns0.tiscali.co.uk.      2D IN A         212.74.114.132    <-- "Glue record"

;; Total query time: 757 msec
;; FROM: vaio.linnet.org to SERVER: ns1.nic.uk.  195.66.240.130
;; WHEN: Mon Jun  9 09:31:25 2003
;; MSG SIZE  sent: 35  rcvd: 97

$ dig +norec @ns0.ja.net. www.tiscali.co.uk. a
... resultats
$ dig +norec @ns.uu.net. www.tiscali.co.uk. a
... resultats
$ dig +norec @sec-nom.dns.uk.psi.net. www.tiscali.co.uk. a
... resultats
$ dig +norec @ns2.nic.uk. www.tiscali.co.uk. a
... resultats
```

Vérifier si les résultats sont identiques! (Note: si un serveur est autoritaire pour un domaine et un sous-domain, il renverra immédiatement le résultat pour le sous-domain. C'est CORRECT)

4. Continuer de répéter la requête pour tous les enregistrements NS trouvés

```
$ dig +norec @ns0.tiscali.co.uk. www.tiscali.co.uk. a
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57638
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUERY SECTION:
;;      www.tiscali.co.uk, type = A, class = IN

;; ANSWER SECTION:
www.tiscali.co.uk.      1H IN A         212.74.101.10

;; AUTHORITY SECTION:
tiscali.co.uk.          6H IN NS        ns0.as9105.com.
tiscali.co.uk.          6H IN NS        ns0.tiscali.co.uk.

;; ADDITIONAL SECTION:
ns0.as9105.com.         1D IN A         212.139.129.130
ns0.tiscali.co.uk.      6H IN A         212.74.114.132

$ dig +norec @ns0.as9105.com. www.tiscali.co.uk. a
...
;; ANSWER SECTION:
```

www.tiscali.co.uk. 1H IN A 212.74.101.10

Vérifier que les informations sont identiques

Nous avons maintenant trouvé la réponse. Vérifier également que la section ' AUTHORITY SECTION ' dans la réponse a la **même** liste de serveurs de noms que nous avions utilisé pour exécuter la requête. (ce sont les enregistrements NS contenus dans le serveur autoritaire lui-même)

5. Liste de contrôle

- Tous les serveurs de noms étaient-ils accessibles?
- Y avait-il au moins deux serveurs de noms sur deux sous-réseaux différents?
- Tous ont-ils donné une référence ou un AA (réponse autoritaire)?
- Toutes les réponses étaient-elles les mêmes?
- Les valeurs TTL étaient-elles raisonnables?
- La liste finale de serveurs de noms dans la
- section ' AUTHORITY SECTION ' correspond-t-elle à la liste de serveurs de noms dans la référence?

6. Vérifier maintenant l'enregistrement NS lui-même !

Noter que chaque enregistrement NS pointe vers un NOM d'hôte, pas vers une adresse IP. (cela est illégal qu'un enregistrement NS pointe vers une adresse IP, il ne fonctionnera pas du tout)

Toutefois pendant chaque ' dig ', nous comptions sur dig (disons-nous) pour convertir ' ns0.as9105.com ' à l'adresse IP correcte.

Elle exécute une consultation récursive pour trouver l'adresse IP de ce serveur, de sorte qu'elle puisse envoyer la requête là-bas.

Par conséquent, vous devez recommencer et vérifier chaque enregistrement NS que vous avez trouvé, exactement de la même manière!

C'est pénible, et généralement les serveurs root sont corrects. Mais il est intéressant de vérifier les enregistrements NS de votre code pays et vos propres enregistrements NS

Exemple: ns0.as9105.com.

```
$ dig +norec @a.root-servers.net. ns0.as9105.com. a
... referral vers [a-m].gtld-servers.net.
$ dig +norec @a.gtld-servers.net. ns0.as9105.com. a
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; ANSWER SECTION:
ns0.as9105.com.          2D IN A          212.139.129.130

;; AUTHORITY SECTION:
as9105.com.              2D IN NS         ns0.as9105.com.
as9105.com.              2D IN NS         ns0.tiscali.co.uk.
```

Mais ce n'est pas une réponse d'un serveur autoritaire! (aussi bien que le ' AA ' manque, noter que la machine que nous avons questionnée n'est pas une des machines listé dans la section 'authority section')

Ce n'est pas une erreur aussi longtemps que la réponse est correcte, mais nous devons continuer au niveau inférieur pour trouver la véritable source autoritaire.

```
$ dig +norec @ns0.as9105.com. as9105.com. a
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; ANSWER SECTION:
ns0.as9105.com.          1D IN A         212.139.129.130

;; AUTHORITY SECTION:
as9105.com.              1D IN NS        ns0.as9105.com.
as9105.com.              1D IN NS        ns0.tiscali.co.uk.

$ dig +norec @ns0.tiscali.co.uk. as9105.com. a
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; ANSWER SECTION:
ns0.as9105.com.          1D IN A         212.139.129.130

;; AUTHORITY SECTION:
as9105.com.              1D IN NS        ns0.tiscali.co.uk.
as9105.com.              1D IN NS        ns0.as9105.com.
```

Maintenant nous vérifions:
Toutes les réponses étaient-elles les mêmes? (Oui: 212.139.129.130
de tous les deux a.gtld-servers.net et des serveurs autoritaires

La délégation correspond t-elle aux enregistrements NS dans les serveurs autoritaires ? (oui: la délégation à ns0.as9105.com et à ns0.tiscali.co.uk, et ces deux enregistrements ont été énumérés dans la zone)

Réponses négatives

La non-existence d'un ER est aussi une information importante. La réponse que vous obtenez devrait ressembler à ceci:

```
$ dig +norec @ns0.tiscali.co.uk. wibble.tiscali.co.uk. a
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 4
;; flags: qr aa; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUERY SECTION:
;;      wibble.tiscali.co.uk, type = A, class = IN

;; AUTHORITY SECTION:
tiscali.co.uk.                  1H  IN  SOA             ns0.tiscali.co.uk.
hostmaster.uk.tiscali.com. (
                                        2003060301      ; serial
                                        3H              ; refresh
                                        1H              ; retry
                                        1W              ; expiry
                                        1H )            ; minimum
```

Le AA est retourné, mais il n'y a rien dans la réponse à l'exception du SOA. Les paramètres dans le SOA sont employés pour établir combien de temps de cache des réponses négatives est permis. (les anciens cache utilisent le TTL du SOA lui-même; les nouveaux caches utilise la valeur minimum du SOA ' minimum '. C'est mieux de mettre tous les deux à la même valeur).

Signification des `flags' drapeaux (de RFC 1034/RFC 1035)

QR Un champ d'un bit qui indique si ce message est une requête (0), ou une réponse (1).

AA Réponse des serveurs autoritaires - ce bit est valide dans les réponses, et indique que le serveur qui répond est autoritaire pour le nom de domaine dans la section requête.

RD Récursivité désirée - ce bit peut être placé dans une requête et est copié dans la réponse. Si le RD est placé, il spécifie au serveur de noms de poursuivre la requête de façon récursive. Le support de la requête récursive est facultatif.

RA La récursivité est disponible - ce bit est placé ou effacé dans une réponse, et dénote si le support des requêtes récursives de question est disponible sur le serveur de noms

Aussi bien que manque le drapeau (flag) de ' AA', une bonne manière de repérer les réponses cachées est de répéter la requête plusieurs fois et d'observer le décomptage du TTL

```
$ dig @noc.ws.afnog.org. psg.com.
;; ANSWER SECTION:
psg.com.                53m44s IN A     147.28.0.62

$ dig @noc.ws.afnog.org. psg.com.
;; ANSWER SECTION:
psg.com.                53m38s IN A     147.28.0.62
```