DNS session 2 - exercice N°2 : Réaliser un cache DNS

1. Vérifiez que vous avez installé correctement les paquetages

$ named –v

BIND 9.8.1-P1

Pour installer # apt-get install bind9

2. Commencer le cache DNS et vérifier qu'il est démarré

named
ps auxwww | grep named
tail /var/log/syslog
Vérifier que le démarrage a réussi, aucuns messages d'erreur !

3. Modifier votre resolver pour utiliser votre propre cache DNS seulement

Éditer le fichier /etc/resolv.conf comme suit:

search ws.afnog.org
nameserver 127.0.0.1
#nameserver 192.188.58.126
#nameserver 192.188.58.2

Enlever toutes les lignes existantes qui commencent par le mot ' nameserver ', ou commenter les en insérant le caractère # au début de la ligne comme montré ci-dessus.

4. Envoyer quelques requêtes

A l'issue de la requête. Noter si la réponse a le flag (drapeau) ' AA ' placé. Regarder la section de réponse, noter le TTL de la réponse.
Noter combien de temps la requête a pris pour s'exécuter.

Répéter alors la même exacte requête, et noter l'information encore

dig yahoo.com. A-t-il le drapeau ' aa '? _____

Quelle est le TTL de la réponse? _____ seconds

Combien est le temps de requête ? _____ milliseconds

dig yahoo.com. A-t-il le drapeau ' aa '? _____

Quelle est le TTL de la réponse? _____ seconds

Combien est le temps de requête ? _____ milliseconds

Répéter le une troisième fois. Pouvez-vous expliquer les différences?

Essayer d'envoyer quelques requêtes au cache de votre voisin.
(si ceci échoue, c'est peut être un problème avec IP firewalling)

5. Observer le cache en opération

Vous pouvez prendre un instantané du contenu de cache comme ceci:

```
# /usr/sbin/rndc dumpdb
# less /var/cache/bind/named_dump.db
```

(Ne pas faire ceci sur un cache occupé - vous produirez un
fichier énorme de dump!)

```
# tcpdump -n -s1500 -i eth0 udp port 53
```

Tandis que ceci fonctionne, dans la première fenêtre, éclater votre cache (ainsi il oublie toutes les données existantes)

```
# rndc flush
# dig yahoo.com.      -- et regarder le tcpdump.  Que voyez-vous?

# dig yahoo.com.      -- regarder le tcpdump. Maintenant que voyez-vous?
```

6. Serrez la configuration

(Si vous avez du temps)

En suivant les exemples sur la présentation, créer un ACL qui limite à votre machine seulement l'accès à votre cache. Demander à quelqu'un d'autre d'essayer de résoudre des noms en utilisant votre cache. Se rappeler:

rndc reload
pour rendre votre configuration modifiée active

tail /var/log/syslog pour vérifier les erreurs dans votre configuration