DNS Exercice 2: Configuration d'un domaine
==

Dans cet exercice, vous allez créer un nouveau domaine,
"nom-de-domaine.cctld.sn.". Vous mettrez en place le
service maître sur votre machine et trouverez quelqu'un
d'autre qui sera votre esclave. Vous demanderez après à
l'administrateur du domaine parent(cctld.sn.) de vous
déléguer votre domaine.

Pour commencer, noter que chaque machine dans la classe a
un nom DNS fonctionnel: pcX.cctld.sn. Vérifier que la
machine est bien configurée avec la commande `hostname`
- e.g. sur le pc1, on doit voir

```
>     # hostname
>     pc1.cctld.sn
```

Sinon, configurez votre machine avec son nom: e.g. pour pc1

```
>     # hostname pc1.cctld.sn
>     # vi /etc/rc.conf
>     ...
>     hostname="pc1.cctld.sn"
>     # vi /etc/hosts
>     ...
>     196.1.97.131     pc1.cctld.sn
```

Vous devriez également voir le nom de votre machine à l'écran
d'ouverture de session:

```
>     FreeBSD/i386 (pc1.cctld.sn) (ttyv0)
>
>     login:
```

Exercice
----

*   Choisissez un nouveau domaine, Ecrivez le ici:
    `_____.cctld.sn`
    (Ne pas choisir un nom de machine comme sous-domaine)

     Nous recommandons votre cctld (e.g. ga,td,ne,dj,sn,bf,rw)

*   Vérifiez que les répertoires dont vous avez besoin existent.
    Sinon créez les:

```
        # mkdir /var/cctld/maître
        # mkdir /var/cctld/esclave
        # chown bind /var/cctld/esclave
```

*   Trouvez quelqu'un qui accepte d'être esclave pour votre
    domaine. Vous devrez choisir quelqu'un sur une table autre
    que la vôtre. (Se rappeler du RFC2182: Les esclaves doivent
    être sur des réseaux distants). Vous pouvez avoir plus d'un
    esclave si vous voulez.

*   Créez votre fichier de zone dans `
    /var/cctld/maître/xxxxxx.cctld.sn`
    (où xxxxxx est le nom choisi)

```
    >     $TTL 10m
    >     @       IN      SOA     pcX.cctld.sn. votre-nom.example.com. (
    >                                     2005091300    ; Serial
    >                                     10m           ; Refresh
    >                                     10m           ; Retry
```

```
>                                       4w            ; Expire
>                                       10m )         ; Negative
>
>                  IN      NS      pcX.cctld.sn.   ; maître
>                  IN      NS      pcY.cctld.sn.   ; esclave
>
>     www     IN      A       196.1.97.X   ; l'adresse IP de votre machine
```

Remplacez `votre-nom.exemple.com.` par votre adresse électronique, en changeant "@" en "." et ajoutant un "." à la fin.

Nous avons choisi exprès de petites valeurs pour TTL, refresh, and retry pour rendre la résolution de problè mes facile dans la classe.Pour un site en production,vous devriez utiliser des valeurs plus élevées e.g. `$TTL 1d`

* Editer `/etc/named.conf` pour configurer que votre machine en tant que maître pour votre domaine (Voir slides sur comment faire ceci)

* Vérifier que votre fichier de configuration et le fichier de zone sont valides et recharger le démon du serveur de nom:

```
# named-checkconf
# named-checkzone xxxxxx.cctld.sn
/var/cctld/maître/xxxxxx.cctld.sn
```

S'il a y a des erreurs,corrigez les

```
# rndc reload
# tail /var/log/messages
```

certaines erreurs de configuration peuvent conduire à l'arrêt total du démon.Dans ce cas démarrer le de nouveau.

démarrer le de nouveau:

```
# named -u bind
```

* Assistez votre esclave à se configurer comme esclave pour votre domaine, et configurez vous en tant que esclave si quelqu'un d'une autre table vous le demande.

Une fois encore, les instructions sur comment faire ces configurations sont dans les slides. Si vous avez changer votre `named.conf` pour être esclave pour quelqu'un d'autre, assurez-vous qu'il n'y a pas des erreurs dans `/var/log/messages` après un `rndc reload`.

* Vérifiez que les esclaves donnent des réponses autoritaires pour votre domaine:

```
# dig +norec @196.1.97.X xxxxxx.cctld.sn. soa
# dig +norec @196.1.97.Y xxxxxx.cctld.sn. soa
```

Vérifiez que vous avez un "AA" (authoritative answer) des deux, et que les numéros de série sont les mêmes.

* Maintenant vous être prêt pour demander la délégation. Apportez le formulaire suivant à l'instructeur jouant le rô le de hostmaître:

```
Nom de domaine:          _____.cctld.sn

Serveur maître:    pc____.cctld.sn

Serveur esclave:     pc____.cctld.sn
```

Serveur esclave: pc____.cctld.sn (optional)

Serveur esclave: pc____.cctld.sn (optional)

* Vous n'aurez pas de délégation jusqu'à ce que le hostmaître s'assure que:

  - Vos serveurs de nom sont tous autoritaires pour votre domaine
  - Ils ont le même numéro de série
  - Les enregistrements NS dans la zone correspondent à la liste de serveurs sur lesquels vous demandez la délégation
  - Les esclaves ne sont pas sur la même table que vous

* Une fois la délégation faite, essayer de résoudre www.xxxxxx.cctld.sn:

  - Avec votre machine dig @196.1.97.x www.xxxxxx.cctld.sn
  - Avec la machine de quelqu'un d'autre(qui n'est pas esclave pour votre domaine)
    dig @196.1.97.z www.xxxxxx.cctld.ucan.sn
  - Avec un serveur récursif sur l'Internet si vous en avez accès
  - essayer de résoudre www.xxxxxx.cctld.sn de la racine vers vos NS

  # dig www.xxxxxx.cctld.sn. A +trace

* Ajoutez un nouvel enregistrement de ressources à votre zone. N'oubliez pas d'augmenter le numéro de série. Vérifiez que les esclaves ont transféré la nouvelle zone. Essayez de résoudre ce nouvel enregistrement de ressource de quelque part d'autre.

* Restreindre les transferts de zone par IP
 - En tant que maître, insérer "allow-transfer { 196.1.97.Y; };" dans la configuration de la zone dans /etc/named.conf
 - En tant qu'esclave, insérer "allow-transfer { none; };" dans la configuration de la zone dans /etc/named.conf
 -Faites un changement dans votre zone (changer le numéro de série et recharger la zone)
 - Vérifiez que les esclaves ont transféré le fichier de zone
 - Essayez de transférer le fichier de zone de quelque part d'autre

  # dig @pcX.cctld.sn xxxxxx.cctld.sn. axfr

* Restreindre les transferts de zone sur clés et IP

A faire pendant jour 4

Préparé par Alain Patrick AINA
Traduit par Alain Patrick AINA
