# Exercice DNS - Délégation

Dans cet exercice, nous allons créer un nouveau TLD dans notre racine.
par exemple: MYTLD

Vous allez créer un service de nom maître sur votre propre machine, et quelqu'un d'autre offrira un service esclave. Ensuite, vous pourrez demander à l'administrateur du domaine au-dessus de vous (la racine) de vous déléguer votre domaine.

Note: ce qui suit devra être fait tant que le super utilisateur «root».

Tout d'abord, notez que votre nom d'hôte (hostname) est configuré correctement sur votre machine. Vérifiez qu'il est correctement configuré en utilisant la commande 'hostname' - par exemple sur auth1.grpXX.dns.nsrc.org, si vous tapez:

```
 # hostname
```

Vous devriez voir:

```
  auth1.grpXX.dns.nsrc.org
```

Si non, alors configurez votre serveur avec son nom: par exemple, pour auth1.grp25.dns.nsrc.org, tapez:

```
# hostname auth1.grp25.dns.nsrc.org
```

N'oubliez pas de remplacer "grpXX" par le numéro du groupe approprié!

Editez le fichier /etc/rc.conf (en utilisant "vi" ou "ee", c'est à dire: ee /etc/rc.conf), et mettre à jour le "hostname":

```
# hostname = "auth1.grpXX.dns.nsrc.org"
```

Dans le fichier /etc/hosts, vous devriez voir une ligne:

```
  10.10.X.1 auth1.grpXX auth1.grpXX.dns.nsrc.org
```

## Exercice

* Choisissez un nouveau nom de domaine, notez-le quelque part

    ex: «MYTLD» ou «mycooldomain» - ce qui vous plaît.

    (NE PAS choisir l'un des noms de PC, par exemple `auth1.grpXX`, comme votre sous-domaine)

    Cela pourrait être par exemple le code de votre TLD existant, le nom de votre pays, le nom de votre entrepris, etc.

    Mais n'oubliez pas que quelqu'un pourrait prendre le même nom!  Premier arrivé, premier servi.

* Trouvez quelqu'un qui accepterait d'être esclave de votre domaine.
  S'il vous plaît, choisir quelqu'un qui n'est pas immédiatement assis à côté de vous: (pas à votre table) (Rappelez-vous RFC 2182: les secondaires doivent

être sur des réseaux distants mais ici nous travaillons sur un réseau plat).
Vous pouvez avoir plus d'un esclave si vous le souhaitez.

* Créez votre fichier de zone dans `/etc/namedb/master/MYTLD`

(Où MYTLD est votre domaine choisi) - vous pouvez très bien «copier-coller» la section ci-dessous - mais n'oubliez pas de mettre à jour XXX avec votre adresse IP:

*** Rappelez-vous, vous aurez besoin pour devenir root pour créer ce fichier,
*** Ainsi, par exemple
***
*** $ cd /etc/namedb/master
*** $ sudo vi MYTLD
***
*** (N'hésitez pas à utiliser un autre éditeur à la place de vi, par exemple, joe, ee)

```
------------- Copier à partir de ci-dessous ------------

$TTL 2m
@                   IN SOA auth1.grpXX.dns.nsrc.org. votre.adresse.email. (
                        2012022301; Serial
                        10m; Refresh
                        5m; Retry
                        4W; Expire
                        2m); Negative

        IN NS auth1.grpXXX.dns.nsrc.org. ; Maitre
        IN NS auth1.grpYYY.dns.nsrc.org. ; Esclave

www       IN A 10.10.XXX.1                       ; votre propre adresse IP

------------- Couper au-dessus ------------
```

Remplacez `votre.adresse.email.` par votre adresse E-mail privée, de sorte que user@domain.name devienne user.domain.name

XXX et YYY sont l'adresse IP de votre groupe et votre esclave, respectivement.

Nous avons choisi exprès des valeurs faibles pour le TTL, le rafraîchissement (refresh), et le réessai (retry), pour rendre plus facile le dépannage en classe. Pour un domaine de production, vous utiliseriez des valeurs plus élevées.

* Modifier `/etc/namedb/named.conf` et procédez comme suit:

*** Rappelez-vous, vous aurez besoin pour devenir root pour modifier ce fichier,
*** Ainsi, par exemple
***
*** $ cd /etc/namedb
*** $ sudo vi named.conf
***
*** (N'hésitez pas à utiliser un autre éditeur à la place de vi, par exemple, joe, ee)

- Si elle est toujours là, supprimez la ligne suivante:

```
     listen-on {127.0.0.1;};

... et ajouter une autre ligne dans la section des options:

    allow-query {any;};

... afin que votre serveur de noms réponde maintenant aux requêtes
          provenant du réseau.

- Ajouter une section pour configurer votre machine en tant que maître de
  votre domaine, en ajoutant quelque chose comme ce qui suit à la fin
        (en bas) du fichier:

  zone "MYTLD" {
    type master;
    file "/etc/namedb/master/MYTLD";
  };

Faites attention à la ';' et '}'!

* Vérifiez que votre fichier de configuration et le fichier de zone sont
  valides:

        # named-checkconf
        # named-checkzone MYTLD /etc/namedb/master/MYTLD

    * S'il ya des erreurs, corrigez-les! *

* Si ce n'est pas déjà fait, activez le serveur de noms dans la configuration
  de votre serveur, en éditant le fichier /etc/rc.conf et ajouter, si ce n'est
  pas déjà fait:

     ** Rappelez-vous, encore une fois, vous avez besoin d'être root pour modifier
ce fichier

        named_chrootdir=""
        named_enable="YES"

    - Puis démarrage / redémarrage du serveur de noms par la commande:

        # service named restart

    Vérifiez le résultat avec

        # tail /var/log/messages

    Vérifiez avec dig que MYTLD est maintenant configuré sur votre hôte:

        # dig @ 10.10.XXX.1 MYTLD. NS

    Où "XXX" est le groupe de votre machine.

        Vous pouvez également vérifier l'état de serveur de noms en utilisant rndc:

        # rndc status

    - S'il y a des erreurs, corrigez-les. Certaines erreurs de configuration
            peuvent provoquer l'arrêt complet du serveur de noms, auquel cas vous
            pourriez avoir à le redémarrez, après avoir corrigé les erreurs:
```

```
        # service named restart
```

* Aider vos esclaves à se configurer comme esclave pour votre domaine, et
  configurer votre serveur en tant qu'esclave si une autre table vous demande
  d'être esclave pour eux.

    Voici l'essentiel de ce que vous devez ajouter à la fin du fichier named.conf:

```
      zone "MYTLD" {
         type slave;
         masters { 10.10.xxx.1; };
         file "/etc/namedb/slave/MYTLD";
      };
```

    ... où XXX est le groupe où le maître se trouve.

    Si vous avez changé votre `named.conf` afin de devenir esclave pour
    quelqu'un d'autre, assurez-vous qu'il n'y a pas d'erreurs dans
          `/var/log/messages` après avoir redémarré votre serveur de noms.

    Vous aurez besoin d'un répertoire slave avec les permissions appropriées
          et ou l'utilisateur bind peut écrire le fichier de zone reçu du maître.

* Vérifiez que vous et vos esclaves donnent des réponses faisant autorité pour
  votre nom de domaine:

```
        # dig +norec @10.10.XXX.1 MYTLD. SOA
        # dig +norec @10.10.YYY.1 MYTLD. SOA
```

    Vérifiez que vous obtenez un 'aa' (réponse faisant autorité) pour chaque,
          et que les numéros de série correspondent.

* Maintenant vous êtes prêt à demander la délégation:

    a) si vous utilisez le RZM:

    Aller à https://rzm.dnssek.org/

    Choisissez 'signup'.

    Le nom d'utilisateur est votre nom de domaine ("coco") par exemple.
    Le mot de passe est libre à vous, mais vous devez vous en souvenir!

    Nous ferons une démo de l'interface en classe.

    b) si vous n'utilisez pas le RZM:

    Indiquez à l'instructeur, sur un morceau de papier:

```
        Nom de domaine: ____________________

        serveur de noms maitre:  auth1.grp___.dns.nsrc.org

        serveur de noms esclave: auth1.grp___.dns.nsrc.org
```

* Vous n'obtiendrez pas la délégation tant que l'instructeur aura vérifié:

- Vos serveurs DNS font tous autorité pour votre domaine
- Ils ont tous le même numéro de série SOA
- Les enregistrements NS dans la zone correspondant à la liste des
  serveurs que vous avez indiqué dans votre demande de délegation
- Le(s) esclave(s) ne sont pas à la même table que vous ou à côté
  de vous!

=> C'est ce qu'on appelle la politique d'un registre!

* Une fois que vous avez obtenu la délégation, essayez de résoudre www.MYTLD:

- Sur votre propre machine
- Sur la machine de quelqu'un d'autre (qui n'est pas esclave pour vous):

```
# dig @ 10.10.XXX.1 www.MYTLD    (où MYTLD est votre domaine)
```

* Ajouter un nouvel enregistrement dans votre fichier de zone.
  N'oubliez pas de mettre à jour le le numéro de série. Vérifiez que vos
  esclaves ont mis à jour. Essayez de résoudre ce nouveau nom.