BIND SÉCURISATION DU TRANSFERT

Nous allons limiter le transfert de zone de vos zones de sorte que seulement vos serveurs esclave/secondaires sont autorisés à demander des copies des zones.

Remarque: si dans votre classe ce sont les d'instructeurs (par exemple, groupe 0) qui sert d'esclave esclave (secondaire) pour votre domaine, alors le «partenaire» auquel il est fait référence ci-dessous est l'instructeur responsable du groupe 0.

Sécurité à base d'ACL

Pour commencer, nous activons les ACL par IP - sur l'hôte AUTH1:

1. Commencez par éditer le fichier /etc/namedb/named.conf, et dans la section "options", nous allons définir qui est autorisé à transférer votre zone.

   allow-transfer {127.0.0.1; :: 1; VOTRE_PROPRE_IP; myslaves; };

   ... remplacer "VOTRE_PROPRE_IP" avec l'adresse IP de votre machine :)

   Maintenant, nous devons définir l'ACL "myslaves". Pour ce faire, APRÈS la section options (trouver le symbole '};' à la fin de la section), ajouter quelque chose semblable à ceci:

   (Si l'esclave de votre domaine "MYTLD" est auth1.grp25, par exemple)

```
acl myslaves { 10.10.25.1; }; // ACL avec l'IP du master Group25
```

Cela signifie "myslaves est un ACL composé de l'IP 10.10.25.1.

Si vous avec également configuré NSD, vous aurez besoin d'ajouter l'adresse IP de votre secondaire sur votre réseau à l'ACL (cela s'applique uniquement si vous avez configuré comme NSD un serveur secondaire dans votre groupe. Sinon, sautez ignorez ceci!)

```
acl myslaves { 10.10.25.1; 10.10.X.2; }; // ACL avec l'IP du maitre
     // du Groupe 25 et votre secondaire NSD 10.10.25.2.
```

Note: N'oubliez pas de saisir les valeurs correctes! Vous devez écrire l'IP de la machine qui est votre secondaire dans la classe - rappelez-vous!

2. Redémarrez named

```
$ sudo service named restart
```

3. Assurez-vous vous que le transfert de zone fonctionne toujours, en

demandant à votre partenaire esclave d'éxécuter un transert de zone
en interrogeant VOTRE machine.

Depuis leur serveur:

$ dig @auth1.grpX.dns.nsrc.org MYTLD axfr

Assurez-vous que cela fonctionne toujours.

4. Maintenant, essayer de demander à quelqu'un d'autre dans la classe dont
le serveur n'est PAS dans l'ACL d'essayer la même commande axfr comme
ci-dessus.

Q: Est-ce qu'ils réussissent?

Q: Qu'est-ce que vous voyez dans les journaux /etc/namedb/log/general ?
Qu'est-ce que vous voyez dans les journaux /etc/namedb/log/
transfers ?