BIND JOURNALISATION

Par défaut, les journaux à partir de named sont envoyés dans /var/log/messages via syslog.

Faisons journaliser BIND de façon plus détaillée.

Sur AUTH1 (auth1.grpX - et si vous utilisez BIND sur votre résolveur, sur resolv.grpX aussi):

1. Créez le répertoire du journal:

```
$ sudo mkdir -p /etc/namedb/log
$ sudo chown bind /etc/namedb/log
```

2. Modifier le fichier /etc/rc.conf, et activer named (BIND), au cas où vous ne l'avez pas déjà fait:

```
$ sudo ee /etc/rc.conf

named_chrootdir=""
named_enable="YES"
```

Enregistrez le fichier et quittez.

3. Editer /etc/namedb/named.conf

Si elle est toujours là, trouver et *ENLEVER* la ligne "listen-on" (dans la section "options"):

```
options {
    ...
    listen-on { 127.0.0.1; };       // <- supprimez cette ligne!
    ...
};
```

Passons maintenant à la fin du fichier, et créons la section «logging» (journalisation):

```
// - - - - - - - - - - - - Copier ci-desssous - - - - - - - - - - - - - -

logging {
        // Channels

        channel transfers {
            file "/etc/namedb/log/transfers" versions 3 size 10M;
            print-time yes;
                        severity info;
        };
```

```
        channel notify {
            file "/etc/namedb/log/notify" versions 3 size 10M;
            print-time yes;
                        severity info;
        };
        channel dnssec {
            file "/etc/namedb/log/dnssec" versions 3 size 10M;
            print-time yes;
                        severity info;
        };
        channel query {
            file "/etc/namedb/log/query" versions 5 size 10M;
            print-time yes;
                        severity info;
        };
        channel general {
            file "/etc/namedb/log/general" versions 3 size 10M;
            print-time yes;
                        severity info;
        };

        // Categories

        category xfer-out { transfers; };
        category xfer-in { transfers; };
        category notify { notify; };

        category lame-servers { general; };
        category config { general; };
        category default { general; };
        category security { general; };
        category dnssec { dnssec; };

        // category queries { query; };

};

// - - - - - - - - - - - - - - Fin de copie - - - - - - - - - - - - - - - -
```

Sauvegardez et quittez le fichier, et tester que cela fonctionne:

```
    $ sudo named-checkconf /etc/namedb/named.conf
```

A noter que la catégorie des «requêtes» est commentée. C'est volontaire: ce fichier de journalisation devenir très volumineux rapidement sur des serveurs très solicitiés.

4. Maintenant reconfig ou redémarrer bind:

```
   $ sudo rndc reconfig
```

- Regardez dans /etc/namedb/log/, et de voir si les fichiers sont créés.

Si cela ne fonctionne pas, essayez de:

- Vérifier les permissions pour le répertoir /etc/named/log
- Redémarrer named (service named restart)

5. Faire un transfert de votre propre domaine:

```
    $ dig @auth1.grpX.dns.nsrc.org AXFR MYTLD
    ...
```

    - Vérifiez que le transfert apparait dans /etc/named/log/transfers

```
17-Feb-2011 11:18:15.331 client 127.0.0.1#61235: transfer of 'MYTLD/IN':
AXFR started
17-Feb-2011 11:18:15.331 client 127.0.0.1#61235: transfer of 'MYTLD/IN':
AXFR ended
```

6. Mettre à jour le numéro de série de votre fichier de zone maître:

```
    $ sudo vi /etc/namedb/master/MYTLD
```

Incrémenter le numéro de série par 1 puis enregistrez le fichier de zone.

```
         # rndc reload MYTLD
```

Dans le fichier de journalisation "notify", il devrait y avoir une ligne similaire à celle-ci:

```
         $ cat /etc/namedb/log/notify
```

```
22-Feb-2012 23:43:48.647 zone MYTLD/IN: sending notifies (serial
2012022306)
```