BIND LOGGING

By default, logs from named are sent to /var/log/messages via syslog.

Let's make BIND log in a more detailed fashion.

On AUTH1 (auth1.grpX - and if running BIND on your resolver, on resolv.grpX as well):

1. Create the log directory:

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

2. Edit /etc/rc.conf, and enable named (BIND), in case you haven't already done so:

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

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

Save the file and exit.

3. Edit /etc/namedb/named.conf

If it is still there, find and *REMOVE* the "listen-on" line (in the "options" section):

```
options {
    ...
    listen-on       { 127.0.0.1; };      // <- remove this line!
    ...
};
```

Now move to the bottom (end) of the file, and create the "logging section":

```
// - - - - - - - - - - - - - - - cut below - - - - - - - - - - - - - - -

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; };

};

// - - - - - - - - - - - - - - - - cut above - - - - - - - - - - - - - - - -
```

Save and exit the file, and TEST that it works:

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

Note that the "queries" category is commented out. This is on purpose as this log file on many servers could become very large quickly.

4. Now reconfig or restart bind:

```
   $ sudo rndc reconfig
```

      - Look into /etc/namedb/log/, and see if the files get created.

      If it doesn't work, try:

      - check permissions for /etc/namedb/log
      - restarting named (service named restart)

    Note: it is required for query logging for BIND to be restarted.

5. Do a zone transfer of you own domain:

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

      - Verify that the transfer shows up in /etc/namedb/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. Update the serial number on your master zone file:

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

Increment Serial by 1 then save the zone file.

```
# rndc reload MYTLD
```

In the notify log file there should be a line that looks something like this:

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

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