DNS Logging

WACREN, DNS/DNSSEC Regional Workshop

Ouagadougou, 10-14 October 2016

Logging and DNS

- DNS logs are useful for troubleshooting
- Understand what is happening with the DNS service
- Statistics collector

Logging Categories

- client, config, database, default, delegation-only, dispatch, dnssec, general, lame-servers, network, notify, queries, resolver, security, unmatch, update, update-security, xfer-in, xfer-out

Logging Categories cont.

Commonly used:

- *dnssec*
- *general*
- *lame-servers*
- *notify*
- *queries*
- resolver
- *security*
- *xfer-in and xfer-out*

Logging Samples

```
10-Feb-2011 17:31:42.748 dispatch: dispatch
0x2bb3c3e0: shutting down due to TCP receive error:
12.34.56.78#53: unexpected end of input
10-Feb-2011 19:07:43.647 client: client
12.34.56.78#58216: error sending response: not
enough free resources
10-Feb-2011 17:21:28.703 general: the working
directory is not writable
14-Feb-2011 13:02:05.623 queries: info: client
120.50.62.74#37899: query: 139.134.110.10.in-
addr.arpa IN PTR + (10.20.0.56)
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
```

Logging Management: part 1

```
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;
        };
```

Logging Management: part 2

Assign categories to logging **channels**:
- i.e. to what log file to write category-specific messages

```
// 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 };

}; // end of logging section
```

Logging with syslog-ng/rsyslog

- Syslog-ng or rsyslog for remote logging
- Aggregate to central logging server
- Analyze log data (swatch, tenshi, many other tools)

Questions ?