



Lab Exercise 7 - Troubleshooting

Objectives:

Be able to configure name server's logging facility channel and categorize what type of information are going to be logged.

Familiarization with dig command and Bind's debugging output.

Steps:

A. Using the default log facility

1. Observe what information are being logged in the default channel (syslog) of bind.

Use the `tail -f /var/log/messages` to observe the default logging. If your name server is running using "`named -g -c named.conf`" Press Ctrl-C to exit and run it without -g option so that logs will go to `/var/log/messages`.

2. Open another terminal window and do some query to your name server and see if it's being logged. Perform a zone transfer using dig and observe if it's being logged.

B. Modifying Bind's logging behavior

1. Modify your name server configuration file to include logging of queries, zone transfers and security related activities.

```
logging {
    channel my_dns_log { file "dns_log.txt"; severity info; };
    category queries { my_dns_log; };
    category security { my_dns_log; };
    category xfer-in { my_dns_log; };
    category xfer-out { my_dns_log; };
};
```

2. Restart your name server to activate the new configuration. You might have to do it manually by looking at the process id and kill it.

Get bind process id:

```
ps -ef |grep named
```

Stop bind

```
kill [pid]
```

Start bind:

```
named -c named.conf
```

3. Perform some testing again like queries, zone transfer and check the new log file from another terminal window.

```
tail -f dns_log.txt
```

Note: -The channel name could be any name you want to assign as channel name.

-file statement follows the filename you want to assign to log file.

-channel allow you to filter by message severity, so severity could from more severe to least:

```
critical
error
warning
notice
info
debug [level]
dynamic
```

-category follows the type of information you want to be logged:

```
queries
dnssec
notify
security
update
xfer-in
xfer-out
```

C. Use dig to test your name servers.

1. Getting the soa record of a particular zone from primary and secondary name server. See if they have the same serial number.

```
dig @server1 pcx.net soa
dig @server2 pcx.net soa
```

2. Query for A records of primary & secondary from your primary and secondary name server.

```
dig @server1&2 nsx.pcx.net
```

3. Get the list of name servers for your zone.

```
dig @server1&2 pcx.net NS
```

4. Get the MX record for your zone.

```
dig @server1&2 pcx.net MX
```

5. Use dig to initiate zone transfer.

```
dig @server1 myzone.net AXFR
```

D. Turning on Debugging

1. Bind's debugging can be started from either command line when starting bind or thru control messages. *Control messages will be discussed in RNDC.

Turning on debugging thru command line:

```
%named -g -d [level] -c named.conf
```

*Debugging Levels [1-99] - Lower the debugging level means you get less information.
Level 1 – Zone loading, SOA queries, zone transfers, zone expiration and cache cleaning.
Notify messages, queries received.
Level 2 – Logs multicast requests.