Building zone file (exercise)
Debug and troubleshooting

cctld-workshop
amsterdam, 19-22 june 2004

aalain@trstech.net
Building Master zone file(1)

Choose your domain name
  cctld.ws.isc.org

Write down the name and the IP of your pc
  ns1.cctld.ws.isc.org (for the lab)
  193.0.2.x

As user bind, create sub-directories in
  /etc/namedb for zone files

  “Master” for master zones
  “Slave” for slave zones
Building Master zone file(2)

Create the zone file for your domain name

/etc/namedb/Master/cctld.ws.isc.org

$TTL 30m

@ IN SOA ns1.cctld.ws.isc.org. hostmaster.cctld.ws.isc.org. ( 2004061900 ;serial
1h ;refresh 15m ;retry 4w ;expire 5m ;nttl
)

IN NS ns1.cctld.ws.isc.org.

ns1 IN A 193.0.2.x
Loading the zone(1)

Edit named config file /etc/namedb/named.conf to make your server “master” for the zone

zone “cctld.ws.isc.org” {
    type master;
    file “Master/cctld.ws.isc.org”;
};

Start your name server
    named -c /etc/namedb/named.conf -u bind

Check for errors
    tail /var/log/messages
Loading the zone (2)

Check your server for “authoritative answers”

Dig @localhost cctld.ws.isc.org. soa +nored
Dig @localhost cctld.ws.isc.org. ns +nored
Conclude !!!
Configuring Slave (1)

Slave transfers zone file from master

To set up slave for your friend zone f-cctld.ws.isc.org

- Your friend must add your server as NS in his zone file and reload the zone

-On your server(slave), edit /etc/namedb/named.conf zone “f-cctld.ws.isc.org” {
  type slave;
  file “Slave/f-cctld.ws.isc.org”;
  masters { ip_of_friend server; };
};
Configuring slave(2)

Load the zone
   Killall -HUP named

Check for the zone file (f-cctld.ws.isc.org) in /etc/namedb/Slave

Check your server for “authoritative answers”
   Dig @localhost f-cctld.ws.isc.org. soa +norec
   Dig @localhost f-cctld.ws.isc.org. ns +norec
Conclude !!!
Getting delegation from parent(1)

When the slave is serving your zone, you can request delegation from your parent

dig @slave_ip cctld.ws.isoc.org ns +norec
dig @slave_ip cctld.ws.isc.org soa +norec

Fill the delegation form for your domain

Follow the procedures to get delegation

-We will talk later about the requirements
Getting delegation from parent(2)

When Parent acknowledges the delegation

- Check parent servers for your delegation
  
  -dig @parent_NS cctld.ws.isc.org ns +norec
  
- Make sure the authority section shows what you submitted
  
  -Check the path to your zone from root servers with
  
  - dig @server cctld.ws.isoc.org ns +trace
Why Troubleshoot?

- What Can Go Wrong?
  - Misconfigured zone
  - Misconfigured server
  - Misconfigured host
  - Misconfigured network
Tools

- BIND Logging Facility
- named's built-in options
- ping and traceroute
- tcpdump and ethereal
- dig and nslookup
The Best Way To Handle Mistakes

- Assume You Will Make Them
- Prepare The Name Server via Logging
BIND Logging

- Telling named which messages to send
  - category specification
- Telling named where to send messages
  - channel specification
BIND Categories

- BIND has many categories
- Short descriptions of each can be found in the Administrator's Reference Manual (ARM)
  - Section 6.2.10.2, page 49
  - Example:
    ```
    category dnssec {
      dnssec_log;
    };
    ```
BIND channels

- BIND can use syslog
- BIND can direct output to other files

**Example:**

```plaintext
channel dnssec_log {
  file "seclog" versions 3 size 10m;
  print-time yes;
  print-category yes;
  print-severity yes;
  severity debug 3;
};
```
So You've Set Up A Server

- What testing should be done?
- From Basic liveness
  - Is the (right) server running?
  - Is the machine set up correctly?
- To data being served
  - Has the zone loaded?
  - Have zone transfers happened?
Checking the Configuration

- To see named start, use the -g flag
  - Keeps named process in the foreground
  - Prints some diagnostics
  - But does not execute logging
- When satisfied with named's start, kill the process and start without the flag
- Other option
  - named-checkconf
  - checks syntax only
Is the Server Running?

- Once the name server is thought to be running, make sure it is
  - `dig @127.0.0.1 version.bind chaos txt`
- This makes the name server do the simplest lookup it can - its version string
- This also confirms which version you started
  - Common upgrade error: running the old version, forgetting to 'make install'
Is the Server Data Correct?

- Now that the server is the right one (executable)
  - `dig @127.0.0.1 <zone> soa`
- Check the serial number to make sure the zone has loaded
- Also test changed data in case you forgot to update the serial number
- When we get to secondary servers, this check is made to see if the zone transferred
Is the Server Reachable?

- If the dig tests fail, it's time to test the environment (machine, network)
  - ping <server machine ip address>
- This tests basic network flow, common errors
  - Network interface not UP
  - Routing to machine not correct
- Pinging 'locally' is useful, believe it or not
  - Confirms that the IP address is correctly configured
Is the Server Listening?

- If the server does not respond, but machine responds to ping
  - look at system log files
  - telnet server 53
- Server will run even if it can't open the network port
  - logs will show this
  - telnet opens a TCP connection, tests whether port was opened at all
Is the Server Logging the Right Stuff?

- Provoking and examining the logs
  - Log files only appear when needed
  - For example, dnssec logs will start only if 'trusted-keys' are configured and are used
  - Each category is triggered differently
    - Triggers may not be obvious
Using the Tools

- named itself
- dig/nslookup
- host diagnostics
- packet sniffers
Built in to named

- named -g to retain command line
  - named -g -c <conf file>
  - keeps named in foreground
- named -d <level>
  - sets the debug output volume
  - <level>'s aren't strictly defined
  - -d 3 is popular, -d 99 gives a lot of detail
dig

- domain internet groper
  - already used in examples
  - best tool for testing
  - shows query and response syntax
  - documentation
    - `man dig`
    - `dig -help`
- Included in named distribution
Non-BIND Tools

- Tools to make sure environment is right
  - Tools to look at server machine
  - Tools to test network
  - Tools to see what messages are on the network
ifconfig

- InterFace CONFIGuration
  - ifconfig -a
  - shows the status of interfaces
  - operating system utility
- Warning, during boot up, ifconfig may configure interfaces after named is started
  - named can't open delayed addresses
- Documentation
  - man ifconfig
ping

- Checks routing, machine health
  - Most useful if run from another host
  - Could be reason "no servers are reached"
  - Can be useful on local machine - to see if the interface is properly configured
traceroute

- If ping fails, traceroute can help pinpoint where trouble lies
  - the problem may be routing
  - if so - it's not named that needs fixing!
  - but is it important to know...
Once confident in the environment, problems with DNS set ups may exist

To see what is happening in the protocol, use traffic sniffers

These tools can help debug "forwarding" of queries

etereal can be retrieved from

http://www.ethereal.com/