Troubleshooting BIND

Joe Abley <jabley@isc.org>

Agenda

- Troubleshooting Tips
- Things that Can Go Wrong
- Common Approaches
- Troubleshooting Toolbox

These Slides

http://www.isc.org/misc/apnic16/troubleshooting.pdf

- You might like to take notes
- These slides will not be a good record of my handwaving, my elaborate whiteboard scribbling or of the useful experience you hear from other people in the room

Troubleshooting Tips

Realism

- Assume you will make mistakes, so check before, during and after you make changes
- Prepare all the components to do plenty of logging
- Get used to checking the logs

Don’t Panic

- Sometimes, faults can go unnoticed for a long time
- By the time they are noticed, people are already yelling and pulling their hair out
  - Don’t Panic
  - Take your time
  - Think logically

Don’t Panic

- Keep the number of people looking at the problem small
  - but at least, keep the people coordinated
  - make it a rule that nobody makes changes without everybody knowing what is happening

Don’t Panic

- Take control
- Breathe
- Smile, confidently
  - (don’t smile too much, or you will be fired)

Things that Can Go Wrong

Misconfigured Zone

- If there is a syntactic error in a zonefile, BIND will refuse to load it
  - an older copy of the zone may be retained
  - the zone may be dropped entirely if the nameserver is restarted
  - slave servers will time out, eventually
- Dropping a zone will result in delegations from that zone being lost

Misconfigured Server

- Syntactic errors in named.conf will prevent BIND from starting
  - all zones dropped from the master server
  - slaves will time out eventually
- More subtle errors can leave the nameserver functioning, but broken

Misconfigured Slaves

- Are zone transfers happening?
- Do all authoritative servers carry a current version of the zone?

Bad Delegation

- Does the parent zone have a correct delegation for the zone?
- Did somebody forget to pay the registry for the domain name?

Misconfigured Host

- Can the host which is reporting problems successfully look up other names?
- Are all the successful queries cached somewhere?
- Is the DHCP or PPP server handing out the right nameserver addresses?
- Is the caching resolver configured to allow recursive queries from the host?

Broken Network

- Can the stub resolver reach the caching resolvers?
- Can the caching resolvers reach the authoritative nameservers?
  - don’t just ping!

Common Approaches

BIND Logging

BIND Logging

- Tell named which log messages you are interested in
  - category specification
- Tell named where to send log messages
  - channel specification

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

```
category dnssec {
  dnssec_log;
};
```

Channels

- BIND can use syslog
- BIND can send logging output directly to other files

```
channel dnssec_log {
  file “seclog” versions 3 size 10m;
  print-type yes;
  print-category yes;
  print-severity yes;
  sevrity debug 3;
};
```

Checking named.conf

Checking named.conf

- If named.conf has syntactic errors, named will not start
  - check logs
  - check named.conf (there are tools)
- Non-syntactic errors may allow named to start, but not operate correctly
  - check logs
  - check revision history

Checking Zone Files

Checking Zone Files

- If zone files have syntactic errors, they will not load
  - named may continue to serve old versions of the zone
  - if restarted, named may drop the zone altogether
    - slaves will eventually time out

Is the Server Running?

Server Running

- One you have started the name server, check that it really is running
- Check that the right version is running
  - many operating systems ship with BIND 8, some may even ship with BIND 4
  - are you sure you are running the right binary?

Is The Server Data Correct?

Correct Server Data

- Check the SOA record on the authoritative servers for the zone
  - every zone must have at least an SOA
  - do the SOA serial numbers agree?
- Are recent changes to the zone showing up consistently on all servers?
  - did you forget to increase the serial?

Correct Server Data

- If you are querying an authoritative server, make sure it is not giving you a non-authoritative response
  - may also be a recursive resolver
  - turn of recursion when you make your test query

Are the Servers Reachable?

Servers Reachable?

- If the DNS lookup fails, we'd better check that the servers are reachable
  - ping <server IP address>
- Common errors:
  - network interface not up
  - default route is incorrect

Servers Reachable

- Routing between testing point at server may be incorrect
  - traceroute to each endpoint from the other end
- Tell the server to ping itself
  - real interface address, not loopback

Are the Servers Listening?

Server Listening

- If the server does not respond, but the server host responds to ping
  - telnet <server address> 53
  - netstat -an | grep \.53
- Server will run even if it can't open the network port
  - is the server configured to listen on the right address?

Are the Servers Logging the Right Things?

Server Logging

- Provoke and examine the logs
  - log files only appear when needed
    - e.g. DNSSEC logs will only start if "trusted-keys" are configured and used
- Each category is triggered differently
  - triggers may not be obvious

Troubleshooting Toolbox

named -g

- To see named start, use the -g flag
  - keeps named process in the foreground
  - prints some diagnostics
  - does not execute logging
- When you are satisfied that named is starting correctly, kill the process and start without -g

named -d

- To increase the debug level for named, use the -d flag
  - named -d <level>
    - <level> sets the debug output volume
    - <level> isn't strictly defined
    - -d 3 is popular, -d 99 gives a lot of detail

named-checkconf

- named-checkconf is a uitility that ships with BIND 9
- Uses the same configuration parser as is used within BIND
  - can be run independently of named
  - will tell you about configuration errors before without having to try them out with the nameserver

named-checkzone

- named-checkzone is a uitility that ships with BIND 9
- Uses the same zone file parser as is used within BIND
  - can be run independently of named
  - will tell you about zone data errors before without having to try them out with the nameserver

dig

- Domain Internet Groper
  - what a horrible name
  - Ships with BIND
  - already used in examples
    - best tool for testing, better than nslookup or host
    - shows query and response syntax

dig

- Documentation
  - man dig
  - dig -help
- dig @server label class type +option
  - +norecurse is useful

ifconfig

- Interface Configuration
  - ifconfig -a
    - shows the status of interfaces
  - operating system utility
- Check that during boot, named is started after interfaces are configured
- man ifconfig

ping

- Checks routing, aliveness of machine
- Most useful if run from another host
  - but can also be useful on the local host
- Beware of ping failures which are really DNS failures
- Beware of over-enthusiastic firewall administrators

traceroute

- If ping fails, traceroute can help pinpoint where the trouble lies
  - the problem may be the network, not the nameserver
  - traceroute in both directions
- mtr

tcpdump, ethereal

- To see what is actually being received and sent by individual hosts, you need to look at the packet level
- Packet traces will also show details of recursive lookups
- Ethereal has lots of protocol debugging capability
  - http://www.ethereal.com/

The End

http://www.isc.org/misc/netsa2003/troubleshooting.pdf

Joe Abley <jabley@isc.org>