BIND 9 & BIND10
João Damas

What is BIND?

- The DNS reference implementation
- Open Source Software

Reference implementation

- Follows and implements protocol standards
- Often used to test new protocol ideas through special releases
  - –crucial in the development of DNSSEC
- Hopefully, all no standard behaviour will be off by default or available separately

Open Source

- Code is available with an ISC license
  - very few restrictions
- Anyone can modify it for their own purposes
  - no need to give back, though welcome
- If ISC goes astray, others can pick it up
  - stability, security

BIND 9

- Available since 1999
- Long evolution
- currently release is 9.9
- examples of recent new features
  - inline signing
  - RPZ
  - increased performance in several areas

1 The new "inline-signing" option, in combination with the "auto-dnssec" option that was introduced in BIND 9.7, allows named to sign zones completely transparently. Previously automatic zone signing only worked on master zones that were configured to be dynamic; now, it works on any master or slave zone. In a master zone with inline signing, the zone is loaded from disk as usual, and a second copy of the zone is created to hold the signed version. The original zone file is not touched; all comments remain intact. When you edit the zone file and reload, named detects the incremental changes that have been made to the raw version of the zone, and applies those changes to the signed version, adding signatures as needed. A slave zone with inline signing works similarly, except that instead of loading the zone from disk and then signing it, the slave transfers the zone from a master server and then signs it. This enables "bump in the wire" signing: a dedicated signing server acting as an intermediary between a hidden master server (which provides the raw zone data) and a set of publicly accessible slave servers (which only serve the signed data). [RT #26224/23657]

2 NXDOMAIN redirection is now possible. This enables a resolver to respond to a client with locally-configured information when a query would otherwise have gotten an answer of "no such domain". This allows a recursive nameserver to provide alternate suggestions for misspelled domain names. Note that names that are in DNSSEC-signed domains are exempted from this when validation is in use. [RT #23146]

3 "rndc flushtree <name>" command removes the specified name and all names under it from the cache. [RT #19970]

4 "rndc sync" command dumps pending changes in a dynamic zone to disk without a freeze/thaw cycle. "rndc sync -clean" removes the journal file after syncing. "rndc freeze" no longer removes journal files. [RT #22473]

5 The new "rndc signing" command provides greater visibility and control of the automatic DNSSEC signing process. Options to this new command include "-list <zone>" which will show the current state of signing operations overall or per specified zone. [RT #23729]

6 "auto-dnssec" zones can now have NSEC3 parameters set prior to signing. [RT #23684]

7 Improves the startup time for an authoritative server with a large number of zones by making the zone task table of variable size rather than fixed size. This means that authoritative servers with many zones will be serving that zone data much sooner. [RT #24406]

8 Improves initial start-up and server reload time by increasing the default size of the hash table the configuration parser uses to keep track of loaded zones and allowing it to grow dynamically to better handle systems with large numbers of zones. [RT #26523]

9 Improves scalability by using multiple threads to listen for and process queries. Previously named only listened for queries on one thread regardless of the number of overall threads used. [RT #22992]

10 Improves startup and reconfiguration time by allowing zones to load in multiple threads. [RT #25333]

11 The "also-notify" option now takes the same syntax as "masters", thus it can use named master lists and TSIG keys. [RT #23508]

12 The "dnssec-signzone -D" option causes dnssec-signzone to write DNSSEC data to a separate output file. This allows you to put "$INCLUDE example.com.signed" into the zonefile for example.com, run "dnssec-signzone -SD example.com", and the result is a fully signed zone which did *not* overwrite your original zone file. Running the same command again will incrementally re-sign the zone, replacing only those signatures that need updating, rather than signing the entire zone from scratch. [RT #22896]

13 "dnssec-signzone -R" forces removal of signatures that are not expired but were created by a key which no longer exists. [RT #22471]

14 "dnssec-signzone -X" option allows signatures on DNSKEY records to have a different expiration date from other signatures. This makes it more convenient to keep your KSK on a separate system, and resign the zone with it less frequently. [RT #22141]

15 "-L" option to dnssec-keygen, dnssec-settime, and dnssec-keyfromlabel sets the default TTL for the key when it is converted into a DNSKEY RR. [RT #23304]

16 "dnssec-dsfromkey -f -" allows for reading keys from standard input, making it easier to convert DNSKEY records to DS. Example usage: "dig +noall +answer dnskey example.com | dnssec-dsfromkey -f - example.com" [RT #20662]

17 The 'serial-update-method' option allows dynamic zones to have their SOA serial number set to the current UNIX time if desired, rather than simply incrementing the serial number with each change to the zone. [RT #23849]

18 Per RFC 6303, RFC 1918 reverse zones are now part of the built-in list of empty zones. [RT #24990]

19 Added support for Uniform Resource Identifier (URI) resource records [RT #23386]

20 Client requests using TSIG now log the name of the TSIG key used. [RT #23619]

21 Add a 'named -U' option to set the number of UDP listener threads per interface. [RT #26485]

22 dnssec-signzone: "-f -" prints to stdout; "-O full" option prints in single-line-per-record format. [RT #20287]

23 Add a configuration switch "dnssec-lookaside 'no'" to set explicitly the current default behavior. [RT #24858]

24 'rndc querylog' can now be given an on/off parameter instead of only being used as a toggle. [RT #18351]

25 When the server logs messages about the state of recursive client processing, it will include the name the client had requested in the log messages, to make it easier to identify problems when they occur. Such log messages will now look similar to this one: 03-Nov-2011 14:14:44.981 client 10.53.0.7#49775 (www.example.com): send

26 Several RPZ feature improvements have been made. Highlights are a new "rpz" logging channel and RPZ CNAME RDATA can now include wildcards. [RT #25172]

27 Enables DLZ modules to retrieve client information so that responses can be changed depending on the source address of the query. For more information see contrib/dlz/example/README. (Note that this change will be of limited interest to most BIND users - it is intended for developers who are working with DLZ) [RT #25768/26215]

BIND 10

- In development
- All new:
  - new architecture
  - new programming languages
  - new development style
- based on experience with BIND9

BIND10

- Open, modular architecture
  - choice of backends
  - choice of functionality
  - Hooks for special processing
- New developer-friendly libraries
- Release schedule
  - beta in September 2012

Questions?

joao@isc.org