February 20, 2011

Contents

1 Introduction **1**

2 Download **1**

3 Support **2**

4 New Features **2**
4.1 9.8.0 2

5 Feature Changes **3**
5.1 9.8.0 3

6 Security Fixes **4**
6.1 9.8.0 4

7 Bug Fixes **4**
7.1 9.8.0 4

8 Known issues in this release **6**

9 Thank You **6**

1 Introduction

BIND 9.8.0 is the first production release of BIND 9.8.

This document summarizes changes from BIND 9.7 to BIND 9.8. Please see the CHANGES file in the source code release for a complete list of all changes.

2 Download

The latest development versions of BIND 9 software can always be found on our web site at http://www.isc.org/downloads/development. There you will find additional information about each release, source code, and some pre-compiled versions for certain operating systems.

3 Support

Product support information is available on http://www.isc.org/services/support for paid support options. Free support is provided by our user community via a mailing list. Information on all public email lists is available at https://lists.isc.org/mailman/listinfo.

4 New Features

4.1 9.8.0

- The ADB hash table stores informations about which authoritative servers to query about particular domains. Previous versions of BIND had the hash table size as a fixed value. On a busy recursive server, this could lead to hash table collisions in the ADB cache, resulting in degraded response time to queries. Bind 9.8 now has a dynamically scalable ADB hash table, which helps a busy server to avoid hash table collisions and maintain a consistent query response time. [RT #21186]

- BIND now supports a new zone type, static-stub. This allows the administrator of a recursive nameserver to force queries for a particular zone to go to IP addresses of the administrator's choosing, on a per zone basis, both globally or per view. I.e. if the administrator wishes to have their recursive server query 192.0.2.1 and 192.0.2.2 for zone example.com rather than the servers listed by the .com gTLDs, they would configure example.com as a static-stub zone in their recursive server. [RT #21474]

- BIND now supports Response Policy Zones, a way of expressing "reputation" in real time via specially constructed DNS zones. See the draft specification here: http://ftp.isc.org/isc/dnsrpz/isc-tn-2010-1.txt [RT #21726]

- BIND 9.8.0 now has DNS64 support. named synthesizes AAAA records from specified A records if no AAAA record exists. IP6.ARPA CNAME records will be synthesized from corresponding IN-ADDR.ARPA. [RT #21991/22769]

- Dynamically Loadable Zones (DLZ) now support dynamic updates. Contributed by Andrew Tridgell of the Samba Project. [RT #22629]

- Added a "dlopen" DLZ driver, allowing the creation of external DLZ drivers that can be loaded as shared objects at runtime rather than having to be linked with named at compile time. Currently this is switched on via a compile-time option, "configure --with-dlz-dlopen". Note: the syntax for configuring DLZ zones is likely to be refined in future releases. Contributed by Andrew Tridgell of the Samba Project. [RT #22629]

- named now retains GSS-TSIG keys across restarts. This is for compatibility with Microsoft DHCP servers doing dynamic DNS updates for clients, which don't know to renegotiate the GSS-TSIG session key when named restarts. [RT #22639]

- There is a new update-policy match type "external". This allows named to decide whether to allow a dynamic update by checking with an external daemon. Contributed by Andrew Tridgell of the Samba Project. [RT #22758]

- There have been a number of bug fixes and ease of use enhancements for configuring BIND to support GSS-TSIG [RT #22629/22795]. These include:

  - Added a "tkey-gssapi-keytab" option. If set, dynamic updates will be allowed for any key matching a Kerberos principal in the specified keytab file. "tkey-gssapi-credential" is no longer required and is expected to be deprecated. Contributed by Andrew Tridgell of the Samba Project. [RT #22629]
  - It is no longer necessary to have a valid /etc/krb5.conf file. Using the syntax DNS/hostname@REALM in nsupdate is sufficient for to correctly set the default realm. [RT #22795]
  - Documentation updated new gssapi configuration options (new option tkey-gssapi-keytab and changes in tkey-gssapi-credential and tkey-domain behavior). [RT 22795]
  - DLZ correctly deals with NULL zone in a query. [RT 22795]
  - TSIG correctly deals with a NULL tkey->creator. [RT 22795]

- A new test has been added to check the apex NSEC3 records after DNSKEY records have been added via dynamic update. [RT #23229]

- RTT banding (randomized server selection on queries) was introduced in BIND releases in 2008, due to the Kaminsky cache poisoning bug. Instead of always picking the authoritative server with the lowest RTT to the caching resolver, all the authoritative servers within an RTT range were randomly used by the recursive server.

  While this did add an extra bit of randomness that an attacker had to overcome to poison a recursive server's cache, it also impacts the resolver's speed in answering end customer queries, since it's no longer the fastest auth server that gets asked. This means that performance optimizations, such using topologically close authoritative servers, are rendered ineffective.

  ISC has evaluated the amount of security added versus the performance hit to end users and has decided that RTT banding is causing more harm than good. Therefore, with this release, BIND is going back to the server selection used prior to adding RTT banding. [RT #23310]

5 Feature Changes

5.1 9.8.0

- There is a new option in dig, +onesoa, that allows the final SOA record in an AXFR response to be suppressed. [RT #20929

- There is additional information displayed in the recursing log (qtype, qclass, qid and whether we are following the original name). [RT #22043]
- Added option 'resolver-query-timeout' in named.conf (max query timeout in seconds) to set a different value than the default (30 seconds). A value of 0 means 'use the compiled in default'; anything longer than 30 will be silently set to 30. [RT #22852]
- For Mac OS X, you can now have the test interfaces used during "make test" stay beyond reboot. See bin/tests/system/README for details.

6 Security Fixes

6.1 9.8.0

None.

7 Bug Fixes

7.1 9.8.0

- BIND now builds with threads disabled in versions of NetBSD earlier than 5.0 and with pthreads enabled by default in NetBSD versions 5.0 and higher. Also removes support for unproven-pthreads, mit-pthreads and ptl2. [RT #19203]
- If BIND has openssl compiled in (the default) and has any permission problems opening the openssl.cnf file, BIND utilities fail. Currently ISC is including a patch to openssl in bin/pkcs11/openssl-0.9.8l-patch but ISC is working on a better solution until openssl fixes this. [RT #20668]
- nsupdate will now preserve the entered case of domain names in update requests it sends. [RT #20928]
- Added a regression test for fix 2896/RT #21045 ("rndc sign" failed to properly update the zone when adding a DNSKEY for publication only). [RT #21324]
- "nsupdate -l" now gives error message if "session.key" file is not found. [RT #21670]
- HPUX now correctly defaults to using /dev/poll, which should increase performance. [RT #21919]
- If named is running as a threaded application, after an "rndc stop" command has been issued, other inbound TCP requests can cause named to hang and never complete shutdown. [RT #22108]
- After an "rndc reconfig", the refresh timer for managed-keys is ignored, resulting in managed-keys not being refreshed until named is restarted. [RT #22296]

- An NSEC3PARAM record placed inside a zone which is not properly signed with NSEC3 could cause named to crash, if changed via dynamic update. [RT #22363]
- "rndc -h" now includes "loadkeys" option. [RT #22493]
- When performing a GSS-TSIG signed dynamic zone update, memory could be leaked. This causes an unclean shutdown and may affect long-running servers. [RT #22573]
- A bug in NetBSD and FreeBSD kernels with SO_ACCEPTFILTER enabled allows for a TCP DoS attack. Until there is a kernel fix, ISC is disabling SO_ACCEPTFILTER support in BIND. [RT #22589]
- When signing records, named didn't filter out any TTL changes to DNSKEY records. This resulted in an incomplete key set. TTL changes are now dealt with before signing. [RT #22590]
- Corrected a defect where a combination of dynamic updates and zone transfers incorrectly locked the in-memory zone database, causing named to freeze. [RT #22614]
- Don't run MX checks (check-mx) when the MX record points to ".". [RT #22645]
- DST key reference counts can now be incremented via dst_key_attach. [RT #22672]
- The IN6_IS_ADDR_LINKLOCAL and IN6_IS_ADDR_SITELOCAL macros in win32 were updated/corrected per current Windows OS. [RT #22724]
- "dnssec-settime -S" no longer tests prepublication interval validity when the interval is set to 0. [RT #22761]
- isc_mutex_init_errcheck() in phtreads/mutex.c failed to destroy attr. [RT #22766]
- The Kerberos realm was being truncated when being pulled from the the host prinicipal, make krb5-self updates fail. [RT #22770]
- Fixed GSS TSIG test problems for Solaris/MacOSX. [RT #22853]
- Prior to this fix, when named was was writing a zone to disk (as slave, when resigning, etc.), it might not correctly preserve the case of domain name labels within RDATA, if the RDATA was not compressible. The result is that when reloading the zone from disk would, named could serve data that did not match the RRSIG for that data, due to case mismatch. named now correctly preserves case. After upgrading to fixed code, the operator should either resign the data (on the master) or delete the disk file on the slave and reload the zone. [RT #22863]
- The man page for dnssec-keyfromlabel incorrectly had "-U" rather than the correct option "-I". [RT #22887]

- The "rndc" command usage statement was missing the "-b" option. [RT #22937]
- Fixed a possible deadlock due to zone re-signing. [RT #22964]
- The TTL for DNS64 synthesized answers was not always set correctly. [RT #23034]
- The secure zone update feature in named is based on the zone being signed and configured for dynamic updates. A bug in the ACL processing for "allow-update { none; };" resulted in a zone that is supposed to be static being treated as a dynamic zone. Thus, name would try to sign/re-sign that zone erroneously. [RT #23120]
- When using auto-dnssec and updating DNSKEY records, named did correctly update the zone. [RT #23232]
- After a failed zone transfer of an RPZ (response policy zone), named would respond with SERVFAIL for subsequent queries in the RPZ zone. [RT #23246]
- If a slave initiates a TSIG signed AXFR from the master and the master fails to correctly TSIG sign the final message, the slave would be left with the zone in an unclean state. named detected this error too late and named would crash with an INSIST. The order dependancy has been fixed. [RT #23254]

8 Known issues in this release

- None.

9 Thank You

Thank you to everyone who assisted us in making this release possible. If you would like to contribute to ISC to assist us in continuing to make quality open source software, please visit our donations page at http://www.isc.org/supportisc.