BIND 9.9.0b1 Release Notes

AA-00528

BIND 9.9.0b1 is the first beta release for BIND 9.9.

This document summarizes changes from BIND 9.8 to BIND 9.9. Please see the CHANGES file in the source code release for a complete list of all changes.

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.

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.

New Features

9.9.0

* 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]
* Improved 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]
* 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]

* "rndc flushtree <name>" command removes the specified name

and all names under it from the cache. [RT #19970]
* "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]
* 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]

* The "also-notify" option now takes the same syntax as "masters", thus it can use named master lists and TSIG keys. [RT #23508]
* "auto-dnssec" zones can now have NSEC3 parameters set prior to signing. [RT #23684]
* 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]
* "dnssec-signzone -R" forces removal of signatures that are not expired but were created by a key which no longer exists. [RT #22471]
* "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]
* "-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]
* "dnssec-dsfromkey -f -" allows for reading keys from standard input, making it easier to convert DNSKEY records to DS.

[RT #20662]
* 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 #20693]
* Per RFC 6303, RFC 1918 reverse zones are now part of the built-in list of empty zones. [RT #24990]
* Added support for Uniform Resource Identifier (URI) resource records [RT #23386]
* Client requests using TSIG now log the name of the TSIG key used. [RT #23619]

Feature Changes

9.9.0

* dig has been modified to produce more human readable and parsable DNSSEC data output. DNSKEY record comments are more verbose and no longer used in multiline mode only, multiline RRSIG records are now reformatted, multiline output mode for NSEC3PARAM records is now supported. New related options in dig are "+nocomments" to suppress DNSKEY comments, "+split=X" will break hex/base64 records into fields of width X, and "+nosplit" causes RDATA fields to not be split at all. [RT #22820]

Bug Fixes

9.9.0

* Improved 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
  lots of zones will be serving that zone data much sooner. [RT #24406]
* dnssec-signzone -t now records timestamps just before and just after
  signing, improving the accuracy of signing statistics. [RT #16030]
* If allow-new-zones was set to yes and ACLs were given names, issuing
  "rndc reconfig" could cause named to crash. [RT #22739]
* When a validating resolver received a NODATA response for DNSKEY, it was
  not caching the NODATA. Fixed and test added. [RT #22908]
* Using Response Policy Zone (RPZ) with DNAME records and querying the
  subdomain of that label can cause named to crash; named now logs that
  DNAME is not supported. [RT #24766]
* If "ixfr-from-differences" is set to no and a dynamic zone's serial number
  has been changed, "rndc thaw" will now remove the zone's journal file.
  [RT #24687]
* RT #23136 (CHANGES #3114) fixed a problem where named would delete old
  signatures even when the private key wasn't available to re-sign the zone,
  resulting in a zone with missing signatures. However, the initial fix as
  found to be incomplete particularly when multiple algorithms may have been
  used. [RT #24577]
* named would log warnings that empty zones may fail to transfer to slaves due
  to serial number 0. These spurious errors have now been silenced. [RT #25079]
* corrected memory leaks and out of order operations that could cause named
  to crash during a normal shutdown. [RT #25210]

Known issues in this release

* NOEDNS caching is too aggressive in 9.9.0b1 and can cause validation
  to fail by preventing the DNSSEC records from being requested. A fix has
  already been committed for 9.9.0[b2/rc1]. [RT #23392/24964]

Please see the file CHANGES for a detailed list of changes in this release.