1 Release Notes for BIND Version 9.12.0b1

1.1 Introduction

BIND 9.12.0 is a new feature release of BIND, still under development. This document summarizes new features and functional changes that have been introduced on this branch. With each development release leading up to the final BIND 9.12.0 release, this document will be updated with additional features added and bugs fixed.

1.2 Download

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

1.3 License Change

With the release of BIND 9.11.0, ISC changed to the open source license for BIND from the ISC license to the Mozilla Public License (MPL 2.0).

The MPL-2.0 license requires that if you make changes to licensed software (e.g. BIND) and distribute them outside your organization, that you publish those changes under that same license. It does not require that you publish or disclose anything other than the changes you made to our software.

This requirement will not affect anyone who is using BIND without redistributing it, nor anyone redistributing it without changes, therefore this change will be without consequence for most individuals and organizations who are using BIND.

Those unsure whether or not the license change affects their use of BIND, or who wish to discuss how to comply with the license may contact ISC at https://www.isc.org/mission/contact/.

1.4 Windows XP No Longer Supported

As of BIND 9.11.2, Windows XP is no longer a supported platform for BIND, and Windows XP binaries are no longer available for download from ISC.

1.5 Security Fixes

- None.

1.6 New Features

- Many aspects of **named** have been modified to improve query performance, and in particular, performance for delegation-heavy zones:
  - The additional cache ("acache") was found not to significantly improve performance and has been removed; the **acache-enable** and **acache-cleaning-interval** options are now deprecated.
  - In place of the acache, **named** can now use a glue cache to speed up retrieval of glue records when sending delegation responses. Unlike acache, this feature is on by default; use **glue-cache no;** to disable it.
  - The **additional-from-cache** and **additional-from-auth** options have been deprecated.
  - **minimal-responses** is now set to `yes` by default.
  - Several functions have been refactored to improve performance, including name compression, owner name case restoration, hashing, and buffers.
  - When built with default **configure** options, **named** no longer fills memory with tag values when allocating or freeing it. This improves performance, but makes it more difficult to debug certain memory-related errors. The default is reversed if building with developer options. **named -M fill** or **named -M nofill** will set the behavior accordingly regardless of build options.

- Several areas of code have been refactored for improved readability, maintainability, and testability:
  - The **named** query logic implemented in **query_find()** has been split into smaller functions with a context structure to maintain state between them, and extensive comments have been added. [RT #43929]
  - Similarly the iterative query logic implemented in **resquery_response()** function has been split into smaller functions and comments added. [RT #45362]
- Code implementing name server query processing has been moved from **named** to an external library, **libns**. This will make it easier to write unit tests for the code, or to link it into new tools. [RT #45186]
- **named** can now synthesize negative responses (NXDOMAIN, NODATA, or wildcard answers) from cached DNSSEC-verified records that were returned in negative or wildcard responses from authoritative servers.

  This will reduce query loads on authoritative servers for signed domains: when existing cached records can be used by the resolver to determine that a name does not exist in the authorittive domain, no query needs to be sent. Reducing the number of iterative queries should also improve resolver performance.

  This behavior is controlled by the new `named.conf` option **synth-from-dnssec**. It is enabled by default.

  Note: this currently only works for zones signed using NSEC. Support for zones signed using NSEC3 (without opt-out) is planned for the future.

  Thanks to APNIC for sponsoring this work.
- When acting as a recursive resolver, **named** can now continue returning answers whose TTLs have expired when the authoritative server is under attack and unable to respond. This is controlled by the **stale-answer-enable**, **stale-answer-ttl** and **max-stale-ttl** options. [RT #44790]
- The DNS Response Policy Service (DNSRPS) API, a mechanism to allow **named** to use an external response policy provider, is now supported. (One example of such a provider is "FastRPZ" from Farsight Security, Inc.) This allows the same types of policy filtering as standard RPZ, but can reduce the workload for **named**, particularly when using large and frequently-updated policy zones. It also enables **named** to share response policy providers with other DNS implementations such as Unbound.

  This feature is avaiable if BIND is built with **configure --enable-dnsrps**, if a DNSRPS provider is installed, and if **dnsrps-enable** is set to "yes" in `named.conf`. Standard built-in RPZ is used otherwise.

  Thanks to Vernon Schryver and Farsight Security for the contribution. [RT #43376]
- Setting **max-journal-size** to `default` limits journal sizes to twice the size of the zone contents. This can be overridden by setting **max-journal-size** to `unlimited` or to an explicit value up to 2G. Thanks to Tony Finch for the contribution. [RT #38324]
- **dnstap** logfiles can now be configured to automatically roll when they reach a specified size. If **dnstap-output** is configured with mode `file`, then it can take optional **size** and **versions** key-value arguments to set the logfile rolling parameters. (These have the same semantics as the corresponding options in a **logging** channel statement.) [RT #44502]
- Logging channels and **dnstap-output** files can now be configured with a **suffix** option, set to either `increment` or `timestamp`, indicating whether log files should be given incrementing suffixes when they roll over (e.g., `logfile.0`, `.1`, `.2`, etc) or suffixes indicating the time of the roll. The default is `increment`. [RT #42838]
- The **print-time** option in the **logging** configuration can now take arguments **`local`**, **`iso8601`** or **`iso8601-utc`** to indicate the format in which the date and time should be logged. For backward compatibility, **`yes`** is a synonym for **`local`**. [RT #42585]

- The new **dnssec-cds** command generates a new DS set to place in a parent zone, based on the contents of a child zone's validated CDS or CDNSKEY records. It can produce a `dsset` file suitable for input to **dnssec-signzone**, or a series of **nsupdate** to update the parent zone via dynamic DNS. Thanks to Tony Finch for the contribution. [RT #46090]
- **nsupdate** and **rndc** now accepts command line options **-4** and **-6** which force using only IPv4 or only IPv6, respectively. [RT #45632]
- **nsec3hash -r** ("rdata order") takes arguments in the same order as they appear in NSEC3 or NSEC3PARAM records. This makes it easier to generate an NSEC3 hash using values cut and pasted from an existing record. Thanks to Tony Finch for the contribution. [RT #45183]
- The **new-zones-directory** option allows **named** to store configuration parameters for zones added via **rndc addzone** in a location other than the working directory. Thanks to Petr Menšík of Red Hat for the contribution. [RT #44853]
- The **dnstap-read -x** option prints a hex dump of the wire format DNS message encapsulated in each **dnstap** log entry. [RT #44816]
- The **host -A** option returns most records for a name, but omits types RRSIG, NSEC and NSEC3.
- **dig +ednsopt** now accepts the names for EDNS options in addition to numeric values. For example, an EDNS Client-Subnet option could be sent using **dig +ednsopt=ecs:...**. Thanks to John Worley of Secure64 for the contribution. [RT #44461]
- Added support for the EDNS TCP Keepalive option (RFC 7828); this allows negotiation of longer-lived TCP sessions to reduce the overhead of setting up TCP for individual queries. [RT #42126]
- Added support for the EDNS Padding option (RFC 7830), which obfuscates packet size analysis when DNS queries are sent over an encrypted channel. [RT #42094]
- **rndc** commands which refer to zone names can now reference a zone of type **redirect** by using the special zone name "-redirect". (Previously this was not possible because **redirect** zones always have the name ".", which can be ambiguous.)

  In the event you need to manipulate a zone actually called "-redirect", use a trailing dot: "-redirect."

  Note: This change does not appply to the **rndc addzone** or **rndc modzone** commands.
- **named-checkconf -l** lists the zones found in `named.conf`. [RT #43154]
- Query logging now includes the ECS option, if one was present in the query, in the format "[ECS *`address/source/scope`*]".
- By default, BIND now uses the random number generation functions in the cryptographic library (i.e., OpenSSL or a PKCS#11 provider) as a source of high-quality randomness rather than `/dev/random`. This is suitable for virtual machine environments, which may have limited entropy pools and lack hardware random number generators.

  This can be overridden by specifying another entropy source via the **random-device** option in `named.conf`, or via the **-r** command line option. However, for functions requiring full cryptographic strength, such as DNSSEC key generation, this *cannot* be overridden. In particular, the **-r** command line option no longer has any effect on **dnssec-keygen**.

  This can be disabled by building with **configure --disable-crypto-rand**, in which case `/dev/random` will be the default entropy source. [RT #31459] [RT #46047]
- **rndc managed-keys destroy** shuts down all RFC 5011 DNSSEC trust anchor maintenance, and deletes any existing managed keys database. If immediately followed by **rndc reconfig**, this will reinitialize key maintenance just as if the server was being started for the first time.

  This is intended for testing purposes, but can be used -- with extreme caution -- as a brute-force repair for unrecoverable problems with a managed keys database, to jumpstart the key acquisition process if `bind.keys` is updated, etc. [RT #32456]
- **dnssec-signzone -S** can now add or remove synchronization records (CDS and CDNSKEY) based on key metadata set by the **-Psync** and **-Dsync** options to **dnssec-keygen**, **dnssec-settime**, etc. [RT #46149]

1.7 Protocol Changes

- BIND can now use the Ed25519 and Ed448 Edwards Curve DNSSEC signing algorithms described in RFC 8080. Note, however, that these algorithms must be supported in OpenSSL; currently they are only available in the development branch of OpenSSL at https://github.com/openssl/openssl. [RT #44696]

- EDNS KEY TAG options are verified and printed.

1.8 Feature Changes

- The ISC DNSSEC Lookaside Validation (DLV) service has been shut down; all DLV records in the dlv.isc.org zone have been removed. References to the service have been removed from BIND documentation. Lookaside validation is no longer used by default by **delv**. The DLV key has been removed from `bind.keys`. Setting **dnssec-lookaside** set to **auto** or to use dlv.isc.org as a trust anchor is now a fatal configuration error. [RT #46155]

- **named** will no longer start or accept reconfiguration if the working directory (specified by the **directory** option) or the managed-keys directory (specified by **managed-keys-directory** are not writable by the effective user ID. [RT #46077]

- Initializing keys specified in a **managed-keys** statement or by **dnssec-validation auto;** are no longer treated as valid for any use other than validation of RFC 5011 initialization queries. The effect of this is that DNSSEC validation will fail if RFC 5011 key maintenance cannot be initialized: initialization problems will not be masked, but will be immediately visible. [RT #46077]

- Previously, **update-policy local;** accepted updates from any source so long as they were signed by the locally-generated session key. This has been further restricted; updates are now only accepted from locally configured addresses. [RT #45492]

- The lightweight resolver daemon and library (**lwresd** and **liblwres**) have been removed. [RT #45186]

- **dnssec-keygen** no longer has default algorithm settings. It is necessary to explicitly specify the algorithm on the command line with the **-a** option when generating keys. This may cause errors with existing signing scripts if they rely on current defaults. The intent is to reduce the long-term cost of transitioning to newer algorithms in the event of RSASHA1 being deprecated. [RT #44755]

- **dig +sigchase** and related options **+trusted-keys** and **+topdown** have been removed. **delv** is now the recommended command for looking up records with DNSSEC validation. [RT #42793]

- The Response Policy Zone (RPZ) implementation has been substantially refactored: updates to the RPZ summary database are no longer directly performed by the zone database but by a separate function that is called when a policy zone is updated. This improves both performance and reliability when policy zones receive frequent updates. Summary database updates can be rate-limited by using the **min-update-interval** option in a **response-policy** statement. [RT #43449]

- **dnstap** now stores both the local and remote addresses for all messages, instead of only the remote address. The default output format for **dnstap-read** has been updated to include these addresses, with the initiating address first and the responding address second, separated by "->" or "<-" to indicate in which direction the message was sent. [RT #43595]

- Expanded and improved the YAML output from **dnstap-read -y**: it now includes packet size and a detailed breakdown of message contents. [RT #43622] [RT #43642]

- Threads in **named** are now set to human-readable names to assist debugging on operating systems that support that. Threads will have names such as "isc-timer", "isc-sockmgr", "isc-worker0001", and so on. This will affect the reporting of subsidiary thread names in **ps** and **top**, but not the main thread. [RT #43234]

- If an ACL is specified with an address prefix in which the prefix length is longer than the address portion (for example, 192.0.2.1/8), it will now be treated as a fatal error during configuration. [RT #43367]

- **dig** now warns about .local queries which are reserved for Multicast DNS. [RT #44783]
- The view associated with the query is now logged unless it it is "_default/IN" or "_dnsclient/IN" when logging DNSSEC validator messages.
- When **named** was reconfigured, failure of some zones to load correctly could leave the system in an inconsistent state; while generally harmless, this could lead to a crash later when using **rndc addzone**. Reconfiguration changes are now fully rolled back in the event of failure. [RT #45841]
- Fixed a bug that was introduced in an earlier development release which caused multi-packet AXFR and IXFR messages to fail validation if not all packets contained TSIG records; this caused interoperability problems with some other DNS implementations. [RT #45509]
- Multiple **cookie-secret** clauses are now supported. The first **cookie-secret** in `named.conf` is used to generate new server cookies. Any others are used to accept old server cookies or those generated by other servers using the matching **cookie-secret**.
- A new statistics counter has been added to track prefetch queries. [RT #45847]
- The **dnssec-signzone -x** flag and the **dnssec-dnskey-kskonly** option in **named.conf**, which suppress the use of the ZSK when signing DNSKEY records, now also apply to CDNSKEY and CDS records. Thanks to Tony Finch for the contribution. [RT #45689]

1.9 Bug Fixes

- The introduction of **libns** caused a bug in which TCP client objects were not recycled after use, leading to unconstrained memory growth. [RT #46029]

1.10 End of Life

The end of life for BIND 9.12 is yet to be determined but will not be before BIND 9.14.0 has been released for 6 months. https://www.isc.org/downloads/software-support-policy/

1.11 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/donate/.