1 Release Notes for BIND Version 9.16.0

1.1 Introduction

BIND 9.16 is a stable branch of BIND. This document summarizes significant changes since the last production release on that branch.

Please see the file `CHANGES` for a more detailed list of changes and bug fixes.

1.2 Note on Version Numbering

As of BIND 9.13/9.14, BIND has adopted the "odd-unstable/even-stable" release numbering convention. BIND 9.16 contains new features added during the BIND 9.15 development process. Henceforth, the 9.16 branch will be limited to bug fixes and new feature development will proceed in the unstable 9.17 branch.

1.3 Supported Platforms

To build on UNIX-like systems, BIND requires support for POSIX.1c threads (IEEE Std 1003.1c-1995), the Advanced Sockets API for IPv6 (RFC 3542), and standard atomic operations provided by the C compiler.

The `libuv` asynchronous I/O library and the OpenSSL cryptography library must be available for the target platform. A PKCS#11 provider can be used instead of OpenSSL for Public Key cryptography (i.e., DNSSEC signing and validation), but OpenSSL is still required for general cryptography operations such as hashing and random number generation.

More information can be found in the `PLATFORMS.md` file that is included in the source distribution of BIND 9. If your compiler and system libraries provide the above features, BIND 9 should compile and run. If that isn't the case, the BIND development team will generally accept patches that add support for systems that are still supported by their respective vendors.

1.4 Download

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

1.5 Notes for BIND 9.16.0

Note: this section only lists changes from BIND 9.14 (the previous stable branch of BIND).

1.5.1 New Features

- A new asynchronous network communications system based on **libuv** is now used by **named** for listening for incoming requests and responding to them. This change will make it easier to improve performance and implement new protocol layers (for example, DNS over TLS) in the future. [GL #29]
- The new **dnssec-policy** option allows the configuration of a key and signing policy (KASP) for zones. This option enables **named** to generate new keys as needed and automatically roll both ZSK and KSK keys. (Note that the syntax for this statement differs from the DNSSEC policy used by **dnssec-keymgr**.) [GL #1134]

- In order to clarify the configuration of DNSSEC keys, the **trusted-keys** and **managed-keys** statements have been deprecated, and the new **trust-anchors** statement should now be used for both types of key.

  When used with the keyword **initial-key**, **trust-anchors** has the same behavior as **managed-keys**, i.e., it configures a trust anchor that is to be maintained via RFC 5011.

  When used with the new keyword **static-key**, **trust-anchors** has the same behavior as **trusted-keys**, i.e., it configures a permanent trust anchor that will not automatically be updated. (This usage is not recommended for the root key.) [GL #6]

- Two new keywords have been added to the **trust-anchors** statement: **initial-ds** and **static-ds**. These allow the use of trust anchors in DS format instead of DNSKEY format. DS format allows trust anchors to be configured for keys that have not yet been published; this is the format used by IANA when announcing future root keys.

  As with the **initial-key** and **static-key** keywords, **initial-ds** configures a dynamic trust anchor to be maintained via RFC 5011, and **static-ds** configures a permanent trust anchor. [GL #6] [GL #622]

- **dig**, **mdig** and **delv** can all now take a **+yaml** option to print output in a detailed YAML format. [GL #1145]

- **dig** now has a new command line option: **+[no]unexpected**. By default, **dig** won't accept a reply from a source other than the one to which it sent the query. Add the **+unexpected** argument to enable it to process replies from unexpected sources. [RT #44978]

- **dig** now accepts a new command line option, **+[no]expandaaaa**, which causes the IPv6 addresses in AAAA records to be printed in full 128-bit notation rather than the default RFC 5952 format. [GL #765]

- Statistics channel groups can now be toggled. [GL #1030]

1.5.2 Feature Changes

- When static and managed DNSSEC keys were both configured for the same name, or when a static key was used to configure a trust anchor for the root zone and **dnssec-validation** was set to the default value of `auto`, automatic RFC 5011 key rollovers would be disabled. This combination of settings was never intended to work, but there was no check for it in the parser. This has been corrected, and it is now a fatal configuration error. [GL #868]

- DS and CDS records are now generated with SHA-256 digests only, instead of both SHA-1 and SHA-256. This affects the default output of **dnssec-dsfromkey**, the `dsset` files generated by **dnssec-signzone**, the DS records added to a zone by **dnssec-signzone** based on `keyset` files, the CDS records added to a zone by **named** and **dnssec-signzone** based on "sync" timing parameters in key files, and the checks performed by **dnssec-checkds**. [GL #1015]

- **named** will now log a warning if a static key is configured for the root zone. [GL #6]

- A SipHash 2-4 based DNS Cookie (RFC 7873) algorithm has been added and made default. Old non-default HMAC-SHA based DNS Cookie algorithms have been removed, and only the default AES algorithm is being kept for legacy reasons. This change has no operational impact in most common scenarios. [GL #605]

  If you are running multiple DNS servers (different versions of BIND 9 or DNS servers from multiple vendors) responding from the same IP address (anycast or load-balancing scenarios), make sure that all the servers are configured with the same DNS Cookie algorithm and same Server Secret for the best performance.

- The information from the **dnssec-signzone** and **dnssec-verify** commands is now printed to standard output. The standard error output is only used to print warnings and errors, and in case the user requests the signed zone to be printed to standard output with the **-f -** option. A new configuration option **-q** has been added to silence all output on standard output except for the name of the signed zone. [GL #1151]

- The DNSSEC validation code has been refactored for clarity and to reduce code duplication. [GL #622]
- Compile-time settings enabled by the **--with-tuning=large** option for **configure** are now in effect by default. Previously used default compile-time settings can be enabled by passing **--with-tuning=small** to **configure**. [GL !2989]
- JSON-C is now the only supported library for enabling JSON support for BIND statistics. The **configure** option has been renamed from **--with-libjson** to **--with-json-c**. Set the **PKG_CONFIG_PATH** environment variable accordingly to specify a custom path to the **json-c** library, as the new **configure** option does not take the library installation path as an optional argument. [GL #855]
- **./configure** no longer sets **--sysconfdir** to **/etc** or **--localstatedir** to **/var** when **--prefix** is not specified and the aforementioned options are not specified explicitly. Instead, Autoconf's defaults of **$prefix/etc** and **$prefix/var** are respected. [GL #658]

1.5.3 Removed Features

- The **dnssec-enable** option has been obsoleted and no longer has any effect. DNSSEC responses are always enabled if signatures and other DNSSEC data are present. [GL #866]
- DNSSEC Lookaside Validation (DLV) is now obsolete. The **dnssec-lookaside** option has been marked as deprecated; when used in `named.conf`, it will generate a warning but will otherwise be ignored. All code enabling the use of lookaside validation has been removed from the validator, **delv**, and the DNSSEC tools. [GL #7]
- The **cleaning-interval** option has been removed. [GL !1731]

1.6 License

BIND 9 is open source software licensed under the terms of the Mozilla Public License, version 2.0 (see the `LICENSE` file for the full text).

The license requires that if you make changes to BIND and distribute them outside your organization, those changes must be published under the same license. It does not require that you publish or disclose anything other than the changes you have made to our software. This requirement does not affect anyone who is using BIND, with or without modifications, without redistributing it, nor anyone redistributing BIND without changes.

Those wishing to discuss license compliance may contact ISC at https://www.isc.org/contact/.

1.7 End of Life

The end of life date for BIND 9.16 has not yet been determined. At some point in the future BIND 9.16 will be designated as an Extended Support Version (ESV). Until then, the current ESV is BIND 9.11, which will be supported until at least December 2021.

See https://kb.isc.org/docs/aa-00896 for details of ISC's software support policy.

1.8 Thank You

Thank you to everyone who assisted us in making this release possible.