1 Release Notes for BIND Version 9.16.3

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 9.16.3

1.5.1 Security Fixes

- To prevent exhaustion of server resources by a maliciously configured domain, the number of recursive queries that can be triggered by a request before aborting recursion has been further limited. Root and top-level domain servers are no longer exempt from the **max-recursion-queries** limit. Fetches for missing name server address records are limited to 4 for any domain. This issue was disclosed in CVE-2020-8616. [GL #1388]
- Replaying a TSIG BADTIME response as a request could trigger an assertion failure. This was disclosed in CVE-2020-8617. [GL #1703]

1.5.2 Known Issues

- BIND crashes on startup when linked against libuv 1.36. This issue is related to recvmmsg() support in libuv which was first included in libuv 1.35. The problem was addressed in libuv 1.37, but the relevant libuv code change requires a special flag to be set during library initialization in order for recvmmsg() support to be enabled. This BIND release sets that special flag when required, so recvmmsg() support is now enabled when BIND is compiled against either libuv 1.35 or libuv >= 1.37; libuv 1.36 is still not usable with BIND. [GL #1761] [GL #1797]

1.5.3 Feature Changes

- BIND 9 no longer sets receive/send buffer sizes for UDP sockets, relying on system defaults instead. [GL #1713]
- The default rwlock implementation has been changed back to the native BIND 9 rwlock implementation. [GL #1753]
- The native PKCS#11 EdDSA implementation has been updated to PKCS#11 v3.0 and thus made operational again. Contributed by Aaron Thompson. [GL !3326]
- The OpenSSL ECDSA implementation has been updated to support PKCS#11 via OpenSSL engine (see engine_pkcs11 from libp11 project). [GL #1534]
- The OpenSSL EdDSA implementation has been updated to support PKCS#11 via OpenSSL engine. Please note that an EdDSA-capable OpenSSL engine is required and thus this code is only a proof-of-concept for the time being. Contributed by Aaron Thompson. [GL #1763]
- Message IDs in inbound AXFR transfers are now checked for consistency. Log messages are emitted for streams with inconsistent message IDs. [GL #1674]

1.5.4 Bug Fixes

- A bug in dnstap initialization could prevent some dnstap data from being logged, especially on recursive resolvers. [GL #1795]
- When running on a system with support for Linux capabilities, **named** drops root privileges very soon after system startup. This was causing a spurious log message, "unable to set effective uid to 0: Operation not permitted", which has now been silenced. [GL #1042] [GL #1090]
- When **named-checkconf -z** was run, it would sometimes incorrectly set its exit code. It reflected the status of the last view found; if zone-loading errors were found in earlier configured views but not in the last one, the exit code indicated success. Thanks to Graham Clinch. [GL #1807]
- When built without LMDB support, **named** failed to restart after a zone with a double quote (") in its name was added with **rndc addzone**. Thanks to Alberto Fernández. [GL #1695]

1.6 Notes for BIND 9.16.2

1.6.1 Security Fixes

- DNS rebinding protection was ineffective when BIND 9 is configured as a forwarding DNS server. Found and responsibly reported by Tobias Klein. [GL #1574]

1.6.2 Known Issues

- We have received reports that in some circumstances, receipt of an IXFR can cause the processing of queries to slow significantly. Some of these were related to RPZ processing, which has been fixed in this release (see below). Others appear to occur where there are NSEC3-related changes (such as an operator changing the NSEC3 salt used in the hash calculation). These are being investigated. [GL #1685]

1.6.3 Feature Changes

- The previous DNSSEC sign statistics used lots of memory. The number of keys to track is reduced to four per zone, which should be enough for 99% of all signed zones. [GL #1179]

1.6.4 Bug Fixes

- When an RPZ policy zone was updated via zone transfer and a large number of records was deleted, **named** could become nonresponsive for a short period while deleted names were removed from the RPZ summary database. This database cleanup is now done incrementally over a longer period of time, reducing such delays. [GL #1447]
- When trying to migrate an already-signed zone from **auto-dnssec maintain** to one based on **dnssec-policy**, the existing keys were immediately deleted and replaced with new ones. As the key rollover timing constraints were not being followed, it was possible that some clients would not have been able to validate responses until all old DNSSEC information had timed out from caches. BIND now looks at the time metadata of the existing keys and incorporates it into its DNSSEC policy operation. [GL #1706]

1.7 Notes for BIND 9.16.1

1.7.1 Known Issues

- UDP network ports used for listening can no longer simultaneously be used for sending traffic. An example configuration which triggers this issue would be one which uses the same `address:port` pair for **listen-on(-v6)** statements as for **notify-source(-v6)** or **transfer-source(-v6)**. While this issue affects all operating systems, it only triggers log messages (e.g. "unable to create dispatch for reserved port") on some of them. There are currently no plans to make such a combination of settings work again.

1.7.2 Feature Changes

- The system-provided POSIX Threads read-write lock implementation is now used by default instead of the native BIND 9 implementation. Please be aware that glibc versions 2.26 through 2.29 had a bug that could cause BIND 9 to deadlock. A fix was released in glibc 2.30, and most current Linux distributions have patched or updated glibc, with the notable exception of Ubuntu 18.04 (Bionic) which is a work in progress. If you are running on an affected operating system, compile BIND 9 with **--disable-pthread-rwlock** until a fixed version of glibc is available. [GL !3125]

1.7.3 Bug Fixes

- Fixed re-signing issues with inline zones which resulted in records being re-signed late or not at all.

1.8 Notes for BIND 9.16.0

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

1.8.1 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]

1.8.2 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]

1.8.3 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]

1.9 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/.

1.10 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.

1.11 Thank You

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