1 Release Notes for BIND Version 9.15.8

1.1 Introduction

BIND 9.15 is an unstable development release of BIND. This document summarizes new features and functional changes that have been introduced on this branch. With each development release leading up to the stable BIND 9.16 release, this document will be updated with additional features added and bugs fixed.

1.2 Note on Version Numbering

Until BIND 9.12, new feature development releases were tagged as "alpha" and "beta", leading up to the first stable release for a given development branch, which always ended in ".0". More recently, BIND adopted the "odd-unstable/even-stable" release numbering convention. There will be no "alpha" or "beta" releases in the 9.15 branch, only increasing version numbers. So, for example, what would previously have been called 9.15.0a1, 9.15.0a2, 9.15.0b1, and so on, will instead be called 9.15.0, 9.15.1, 9.15.2, etc.

The first stable release from this development branch will be renamed as 9.16.0. Thereafter, maintenance releases will continue on the 9.16 branch, while unstable feature development proceeds in 9.17.

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 9.15.8

1.5.1 Feature Changes

- The **trust-anchors** statement no longer rejects a mix of both key-style and DS-style trust anchor entries for the same name. [GL #1237]

1.5.2 Bug Fixes

- Fixed an intermittent crash in the validator that could occur when validating negative answers from the cache. [GL #1561]
- Fixed a bug that could cause **named** to crash on machines with more than 40 CPUs. [GL #1493]
- Socket-related statistics counters were not being updated by network manager sockets, but are now fully functional. [GL #1311]

1.6 Notes for BIND 9.15.7

1.6.1 Feature Changes

- The **dnssec-keys** configuration statement, which was introduced in 9.15.1 and revised in 9.15.6, has now been renamed to the more descriptive **trust-anchors**. [GL !2702]

  (See release notes for BIND 9.15.1 and BIND 9.15.6 for prior discussion of this feature.)

- Added support for multithreaded listening for TCP connections in the network manager. [GL !2659]

1.6.2 Bug Fixes

- Fixed a bug that caused **named** to leak memory on reconfiguration when any GeoIP2 database was in use. [GL #1445]
- Fixed several possible race conditions discovered by ThreadSanitizer.

1.7 Notes for BIND 9.15.6

1.7.1 Security Fixes

- Set a limit on the number of concurrently served pipelined TCP queries. This flaw is disclosed in CVE-2019-6477. [GL #1264]

1.7.2 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 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]
- Two new keywords have been added to the **dnssec-keys** 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.

  (Note: Currently, DNSKEY-format and DS-format trust anchors cannot both be used for the same domain name.) [GL #6] [GL #622]

- Added a new statistics variable **tcp-highwater** that reports the maximum number of simultaneous TCP clients BIND has handled while running. [GL #1206]

1.7.3 Feature Changes

- NSEC Aggressive Cache (synth-from-dnssec) has been disabled by default because it was found to have a significant performance impact on the recursive service. The NSEC Aggressive Cache will be enable by default in the future releases. [GL #1265]
- The DNSSEC validation code has been refactored for clarity and to reduce code duplication. [GL #622]

1.8 Notes for BIND 9.15.5

1.8.1 Security Fixes

- **named** could crash with an assertion failure if a forwarder returned a referral, rather than resolving the query, when QNAME minimization was enabled. This flaw is disclosed in CVE-2019-6476. [GL #1051]
- A flaw in DNSSEC verification when transferring mirror zones could allow data to be incorrectly marked valid. This flaw is disclosed in CVE-2019-6475. [GL #1252]

1.9 Notes for BIND 9.15.4

1.9.1 New Features

- Added a new command line option to **dig**: **+[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.
- **dig**, **mdig** and **delv** can all now take a **+yaml** option to print output in a a detailed YAML format. [RT #1145]

1.9.2 Bug Fixes

- When a **response-policy** zone expires, ensure that its policies are removed from the RPZ summary database. [GL #1146]

1.10 Notes for BIND 9.15.3

1.10.1 New Features

- Statistics channel groups are now toggleable. [GL #1030]

1.10.2 Removed Features

- 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]

1.10.3 Feature Changes

- 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 doesn't have any operational impact in most common scenarios. [GL #605]

  If you are running multiple DNS Servers (different versions of BIND 9 or DNS server from multiple vendors) responding from the same IP address (anycast or load-balancing scenarios), you'll have to 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 **-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.

- DS records included in DNS referral messages can now be validated and cached immediately, reducing the number of queries needed for a DNSSEC validation. [GL #964]

1.10.4 Bug Fixes

- Cache database statistics counters could report invalid values when stale answers were enabled, because of a bug in counter maintenance when cache data becomes stale. The statistics counters have been corrected to report the number of RRsets for each RR type that are active, stale but still potentially served, or stale and marked for deletion. [GL #602]
- Interaction between DNS64 and RPZ No Data rule (CNAME *.) could cause unexpected results; this has been fixed. [GL #1106]
- **named-checkconf** now checks DNS64 prefixes to ensure bits 64-71 are zero. [GL #1159]
- **named-checkconf** now correctly reports a missing **dnstap-output** option when **dnstap** is set. [GL #1136]
- Handle ETIMEDOUT error on connect() with a non-blocking socket. [GL #1133]
- **dig** now correctly expands the IPv6 address when run with **+expandaaaa +short**. [GL #1152]

1.11 Notes for BIND 9.15.2

1.11.1 New Features

- The GeoIP2 API from MaxMind is now supported. Geolocation support will be compiled in by default if the **libmaxminddb** library is found at compile time, but can be turned off by using **configure --disable-geoip**.

  The default path to the GeoIP2 databases will be set based on the location of the **libmaxminddb** library; for example, if it is in `/usr/local/lib`, then the default path will be `/usr/local/share/GeoIP`. This value can be overridden in `named.conf` using the **geoip-directory** option.

  Some **geoip** ACL settings that were available with legacy GeoIP, including searches for **netspeed**, **org**, and three-letter ISO country codes, will no longer work when using GeoIP2. Supported GeoIP2 database types are **country**, **city**, **domain**, **isp**, and **as**. All of these databases support both IPv4 and IPv6 lookups. [GL #182] [GL #1112]
- Two new metrics have been added to the **statistics-channel** to report DNSSEC signing operations. For each key in each zone, the **dnssec-sign** counter indicates the total number of signatures **named** has generated using that key since server startup, and the **dnssec-refresh** counter indicates how many of those signatures were refreshed during zone maintenance, as opposed to having been generated as a result of a zone update. [GL #513]

1.11.2 Bug Fixes

- When **qname-minimization** was set to **relaxed**, some improperly configured domains would fail to resolve, but would have succeeded when minimization was disabled. **named** will now fall back to normal resolution in such cases, and also uses type A rather than NS for minimal queries in order to reduce the likelihood of encountering the problem. [GL #1055]
- **./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.
- Glue address records were not being returned in responses to root priming queries; this has been corrected. [GL #1092]

1.12 Notes for BIND 9.15.1

1.12.1 Security Fixes

- A race condition could trigger an assertion failure when a large number of incoming packets were being rejected. This flaw is disclosed in CVE-2019-6471. [GL #942]

1.12.2 New Features

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

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

1.12.3 Removed Features

- The **cleaning-interval** option has been removed. [GL !1731]

1.12.4 Feature Changes

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

1.13 Notes for BIND 9.15.0

1.13.1 Security Fixes

- In certain configurations, **named** could crash with an assertion failure if **nxdomain-redirect** was in use and a redirected query resulted in an NXDOMAIN from the cache. This flaw is disclosed in CVE-2019-6467. [GL #880]
- The TCP client quota set using the **tcp-clients** option could be exceeded in some cases. This could lead to exhaustion of file descriptors. This flaw is disclosed in CVE-2018-5743. [GL #615]

1.13.2 New Features

- The new **add-soa** option specifies whether or not the **response-policy** zone's SOA record should be included in the additional section of RPZ responses. [GL #865]

1.13.3 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]

1.13.4 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**.

1.13.5 Bug Fixes

- The **allow-update** and **allow-update-forwarding** options were inadvertently treated as configuration errors when used at the **options** or **view** level. This has now been corrected. [GL #913]

1.14 License

BIND 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/mission/contact/.

1.15 End of Life

BIND 9.15 is an unstable development branch. When its development is complete, it will be renamed to BIND 9.16, which will be a stable branch.

The end of life date for BIND 9.16 has not yet been determined. For those needing long term support, the current Extended Support Version (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.

1.16 Thank You

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