1 Release Notes for BIND Version 9.14.8

1.1 Introduction

BIND 9.14 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 9.14 contains new features added during the BIND 9.13 development process. Henceforth, the 9.14 branch will be limited to bug fixes and new feature development will proceed in the unstable 9.15 branch, and so forth.

1.3 Supported Platforms

Since 9.12, BIND has undergone substantial code refactoring and cleanup, and some very old code has been removed that supported obsolete operating systems and operating systems for which ISC is no longer able to perform quality assurance testing. Specifically, workarounds for UnixWare, BSD/OS, AIX, Tru64, SunOS, TruCluster and IRIX have been removed.

On UNIX-like systems, BIND now 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.

More information can be found in the `PLATFORM.md` file that is included in the source distribution of BIND 9. If your platform 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.

As of BIND 9.14, the BIND development team has also made cryptography (i.e., TSIG and DNSSEC) an integral part of the DNS server. The OpenSSL cryptography library must be available for the target platform. A PKCS#11 provider can be used instead 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.

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 9.14.8

1.5.1 Security Fixes

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

1.5.2 New Features

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

1.5.3 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]

1.6 Notes for BIND 9.14.7

1.6.1 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]

1.7 Notes for BIND 9.14.6

1.7.1 Bug Fixes

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

1.8 Notes for BIND 9.14.5

1.8.1 New Features

- A SipHash 2-4 based DNS Cookie (RFC 7873) algorithm has been added. [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.
- 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]

1.8.2 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** could crash during configuration if configured to use "geoip continent" ACLs with legacy GeoIP. [GL #1163]
- **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]

1.9 Notes for BIND 9.14.4

1.9.1 New Features

- The new GeoIP2 API from MaxMind is now supported when BIND is compiled using **configure --with-geoip2**. The legacy GeoIP API can be used by compiling with **configure --with-geoip** instead. (Note that the databases for the legacy API are no longer maintained by MaxMind.)

  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 the databases support both IPv4 and IPv6 lookups. [GL #182]

- 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]

1.9.2 Bug Fixes

- Glue address records were not being returned in responses to root priming queries; this has been corrected. [GL #1092]

1.10 Notes for BIND 9.14.3

1.10.1 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]

1.10.2 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]

1.11 Notes for BIND 9.14.2

1.11.1 Feature Changes

- When **trusted-keys** and **managed-keys** are both configured for the same name, or when **trusted-keys** is used to configure a trust anchor for the root zone and **dnssec-validation** is set to the default value of `auto`, automatic RFC 5011 key rollovers will fail.

  This combination of settings was never intended to work, but there was no check for it in the parser. This has been corrected; a warning is now logged. (In BIND 9.15 and higher this error will be fatal.) [GL #868]

1.12 Notes for BIND 9.14.1

1.12.1 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. (CVE-2018-5743) [GL #615]

1.12.2 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]

1.12.3 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]

1.13 Notes for BIND 9.14.0

1.13.1 New Features

- Task manager and socket code have been substantially modified. The manager uses per-cpu queues for tasks and network stack runs multiple event loops in CPU-affinitive threads. This greatly improves performance on large systems, especially when using multi-queue NICs.
- Support for QNAME minimization was added and enabled by default in **relaxed** mode, in which BIND will fall back to normal resolution if the remote server returns something unexpected during the query minimization process. This default setting might change to **strict** in the future.
- A new **plugin** mechanism has been added to allow extension of query processing functionality through the use of external libraries. The new `filter-aaaa.so` plugin replaces the **filter-aaaa** feature that was formerly implemented as a native part of BIND.

  The plugin API is a work in progress and is likely to evolve as further plugins are implemented. [GL #15]
- A new secondary zone option, **mirror**, enables **named** to serve a transferred copy of a zone's contents without acting as an authority for the zone. A zone must be fully validated against an active trust anchor before it can be used as a mirror zone. DNS responses from mirror zones do not set the AA bit ("authoritative answer"), but do set the AD bit ("authenticated data"). This feature is meant to facilitate deployment of a local copy of the root zone, as described in RFC 7706. [GL #33]
- BIND now can be compiled against the **libidn2** library to add IDNA2008 support. Previously, BIND supported IDNA2003 using the (now obsolete and unsupported) **idnkit-1** library.
- **named** now supports the "root key sentinel" mechanism. This enables validating resolvers to indicate which trust anchors are configured for the root, so that information about root key rollover status can be gathered. To disable this feature, add **root-key-sentinel no;** to `named.conf`. [GL #37]
- The **dnskey-sig-validity** option allows the **sig-validity-interval** to be overriden for signatures covering DNSKEY RRsets. [GL #145]
- When built on Linux, BIND now requires the **libcap** library to set process privileges. The adds a new compile-time dependency, which can be met on most Linux platforms by installing the **libcap-dev** or **libcap-devel** package. BIND can also be built without capability support by using **configure --disable-linux-caps**, at the cost of some loss of security.

- The **validate-except** option specifies a list of domains beneath which DNSSEC validation should not be performed, regardless of whether a trust anchor has been configured above them. [GL #237]
- Two new update policy rule types have been added **krb5-selfsub** and **ms-selfsub** which allow machines with Kerberos principals to update the name space at or below the machine names identified in the respective principals.
- The new configure option **--enable-fips-mode** can be used to make BIND enable and enforce FIPS mode in the OpenSSL library. When compiled with such option the BIND will refuse to run if FIPS mode can't be enabled, thus this option must be only enabled for the systems where FIPS mode is available.
- Two new configuration options **min-cache-ttl** and **min-ncache-ttl** has been added to allow the BIND 9 administrator to override the minimum TTL in the received DNS records (positive caching) and for storing the information about non-existent records (negative caching). The configured minimum TTL for both configuration options cannot exceed 90 seconds.
- **rndc status** output now includes a **reconfig/reload in progress** status line if named configuration is being reloaded.
- The new **answer-cookie** option, if set to `no`, prevents **named** from returning a DNS COOKIE option to a client, even if such an option was present in the request. This is only intended as a temporary measure, for use when **named** shares an IP address with other servers that do not yet support DNS COOKIE. A mismatch between servers on the same address is not expected to cause operational problems, but the option to disable COOKIE responses so that all servers have the same behavior is provided out of an abundance of caution. DNS COOKIE is an important security mechanism, and this option should not be used to disable it unless absolutely necessary.

1.13.2 Removed Features

- Workarounds for servers that misbehave when queried with EDNS have been removed, because these broken servers and the workarounds for their noncompliance cause unnecessary delays, increase code complexity, and prevent deployment of new DNS features. See https://dnsflagday.net for further details.

  In particular, resolution will no longer fall back to plain DNS when there was no response from an authoritative server. This will cause some domains to become non-resolvable without manual intervention. In these cases, resolution can be restored by adding **server** clauses for the offending servers, specifying **edns no** or **send-cookie no**, depending on the specific noncompliance.

  To determine which **server** clause to use, run the following commands to send queries to the authoritative servers for the broken domain:

  ```
  dig soa <zone> @<server> +dnssec
  dig soa <zone> @<server> +dnssec +nocookie
  dig soa <zone> @<server> +noedns
  ```

  If the first command fails but the second succeeds, the server most likely needs **send-cookie no**. If the first two fail but the third succeeds, then the server needs EDNS to be fully disabled with **edns no**.

  Please contact the administrators of noncompliant domains and encourage them to upgrade their broken DNS servers. [GL #150]
- Previously, it was possible to build BIND without thread support for old architectures and systems without threads support. BIND now requires threading support (either POSIX or Windows) from the operating system, and it cannot be built without threads.
- The **filter-aaaa**, **filter-aaaa-on-v4**, and **filter-aaaa-on-v6** options have been removed from **named**, and can no longer be configured using native `named.conf` syntax. However, loading the new `filter-aaaa.so` plugin and setting its parameters provides identical functionality.

- **named** can no longer use the EDNS CLIENT-SUBNET option for view selection. In its existing form, the authoritative ECS feature was not fully RFC-compliant, and could not realistically have been deployed in production for an authoritative server; its only practical use was for testing and experimentation. In the interest of code simplification, this feature has now been removed.

  The ECS option is still supported in **dig** and **mdig** via the +subnet argument, and can be parsed and logged when received by **named**, but it is no longer used for ACL processing. The **geoip-use-ecs** option is now obsolete; a warning will be logged if it is used in `named.conf`. **ecs** tags in an ACL definition are also obsolete, and will cause the configuration to fail to load if they are used. [GL #32]

- **dnssec-keygen** can no longer generate HMAC keys for TSIG authentication. Use **tsig-keygen** to generate these keys. [RT #46404]

- Support for OpenSSL 0.9.x has been removed. OpenSSL version 1.0.0 or greater, or LibreSSL is now required.

- The **configure --enable-seccomp** option, which formerly turned on system-call filtering on Linux, has been removed. [GL #93]

- IPv4 addresses in forms other than dotted-quad are no longer accepted in master files. [GL #13] [GL #56]

- IDNA2003 support via (bundled) idnkit-1.0 has been removed.

- The "rbtdb64" database implementation (a parallel implementation of "rbt") has been removed. [GL #217]

- The **-r randomdev** option to explicitly select random device has been removed from the **ddns-confgen**, **rndc-confgen**, **nsupdate**, **dnssec-confgen**, and **dnssec-signzone** commands.

  The **-p** option to use pseudo-random data has been removed from the **dnssec-signzone** command.

- Support for the RSAMD5 algorithm has been removed freom BIND as the usage of the RSAMD5 algorithm for DNSSEC has been deprecated in RFC6725, the security of the MD5 algorithm has been compromised, and its usage is considered harmful.

- Support for the ECC-GOST (GOST R 34.11-94) algorithm has been removed from BIND, as the algorithm has been superseded by GOST R 34.11-2012 in RFC6986 and it must not be used in new deployments. BIND will neither create new DNSSEC keys, signatures and digests, nor it will validate them.

- Support for DSA and DSA-NSEC3-SHA1 algorithms has been removed from BIND as the DSA key length is limited to 1024 bits and this is not considered secure enough.

- **named** will no longer ignore "no-change" deltas when processing an IXFR stream. This had previously been permitted for compatibility with BIND 8, but now "no-change" deltas will trigger a fallback to AXFR as the recovery mechanism.

- BIND 9 will no longer build on platforms that don't have proper IPv6 support. BIND 9 now also requires POSIX-compatible pthread support. Most of the platforms that lack these featuers are long past their end-of-lifew dates, and they are neither developed nor supported by their respective vendors.

- The incomplete support for internationalization message catalogs has been removed from BIND. Since the internationalization was never completed, and no localized message catalogs were ever made available for the portions of BIND in which they could have been used, this change will have no effect except to simplify the source code. BIND's log messages and other output were already only available in English.

1.13.3 Feature Changes

- BIND will now always use the best CSPRNG (cryptographically-secure pseudo-random number generator) available on the platform where it is compiled. It will use the **arc4random()** family of functions on BSD operating systems, **getrandom()** on Linux and Solaris, **CryptGenRandom** on Windows, and the selected cryptography provider library (OpenSSL or PKCS#11) as the last resort. [GL #221]
- The default setting for **dnssec-validation** is now **`auto`**, which activates DNSSEC validation using the IANA root key. (The default can be changed back to **`yes`**, which activates DNSSEC validation only when keys are explicitly configured in `named.conf`, by building BIND with **configure --disable-auto-validation**.) [GL #30]
- BIND can no longer be built without DNSSEC support. A cryptography provider (i.e., OpenSSL or a hardware service module with PKCS#11 support) must be available. [GL #244]
- Zone types **primary** and **secondary** are now available as synonyms for **master** and **slave**, respectively, in `named.conf`.
- **named** will now log a warning if the old root DNSSEC key is explicitly configured and has not been updated. [RT #43670]
- **dig +nssearch** will now list name servers that have timed out, in addition to those that respond. [GL #64]
- Up to 64 **response-policy** zones are now supported by default; previously the limit was 32. [GL #123]
- Several configuration options for time periods can now use TTL value suffixes (for example, `2h` or `1d`) in addition to an integer number of seconds. These include **fstrm-set-reopen-interval**, **interface-interval**, **max-cache-ttl**, **max-ncache-ttl**, **max-policy-ttl**, and **min-update-interval**. [GL #203]
- NSID logging (enabled by the **request-nsid** option) now has its own **nsid** category, instead of using the **resolver** category.
- The **rndc nta** command could not differentiate between views of the same name but different class; this has been corrected with the addition of a **-class** option. [GL #105]
- **allow-recursion-on** and **allow-query-cache-on** each now default to the other if only one of them is set, in order to be consistent with the way **allow-recursion** and **allow-query-cache** work. [GL #319]
- When compiled with IDN support, the **dig** and **nslookup** commands now disable IDN processing when the standard output is not a TTY (i.e., when the output is not being read by a human). When running from a shell script, the command line options **+idnin** and **+idnout** may be used to enable IDN processing of input and output domain names, respectively. When running on a TTY, the **+noidnin** and **+noidnout** options may be used to disable IDN processing of input and output domain names.
- The configuration option **max-ncache-ttl** cannot exceed seven days. Previously, larger values than this were silently lowered; now, they trigger a configuration error.
- The new **dig -r** command line option disables reading of the file `$HOME/.digrc`.
- Zone signing and key maintenance events are now logged to the **dnssec** category rather than **zone**.

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

The end of life date for BIND 9.14 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. 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 https://www.isc.org/donate/.