1 Release Notes for BIND Version 9.13.5

1.1 Introduction

BIND 9.13 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 9.14 release, this document will be updated with additional features added and bugs fixed.

1.2 Note on Version Numbering

Prior to BIND 9.13, 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".

Now, however, BIND has adopted the "odd-unstable/even-stable" release numbering convention. There will be no "alpha" or "beta" releases in the 9.13 branch, only increasing version numbers. So, for example, what would previously have been called 9.13.0a1, 9.13.0a2, 9.13.0b1, and so on, will instead be called 9.13.0, 9.13.1, 9.13.2, etc.

The first stable release from this development branch will be renamed as 9.14.0. Thereafter, maintenance releases will continue on the 9.14 branch, while unstable feature development proceeds in 9.15.

1.3 Supported Platforms

BIND 9.13 has undergone substantial code refactoring and cleanup, and some very old code has been removed that was needed to support legacy platforms which are no longer supported by their vendors and for which ISC is no longer able to perform quality assurance testing. Specifically, workarounds for old versions of 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 9.13, 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 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.

1.5 Security Fixes

- There was a long-existing flaw in the documentation for **ms-self**, **krb5-self**, **ms-subdomain**, and **krb5-subdomain** rules in **update-policy** statements. Though the policies worked as intended, operators who configured their servers according to the misleading documentation may have thought zone updates were more restricted than they were; users of these rule types are advised to review the documentation and correct their configurations if necessary. New rule types matching the previously documented behavior will be introduced in a future maintenance release. [GL !708]

- When recursion is enabled but the **allow-recursion** and **allow-query-cache** ACLs are not specified, they should be limited to local networks, but they were inadvertently set to match the default **allow-query**, thus allowing remote queries. This flaw is disclosed in CVE-2018-5738. [GL #309]

- **named** could crash during recursive processing of DNAME records when **deny-answer-aliases** was in use. This flaw is disclosed in CVE-2018-5740. [GL #387]

- Code change #4964, intended to prevent double signatures when deleting an inactive zone DNSKEY in some situations, introduced a new problem during zone processing in which some delegation glue RRsets are incorrectly identified as needing RRSIGs, which are then created for them using the current active ZSK for the zone. In some, but not all cases, the newly-signed RRsets are added to the zone's NSEC/NSEC3 chain, but incompletely -- this can result in a broken chain, affecting validation of proof of nonexistence for records in the zone. [GL #771]

1.6 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.

- 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]

- 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]

- 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]

- 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.

- 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.

1.7 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 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 digest, nor it will validate them.

- Add the ability to not return a DNS COOKIE option when one is present in the request. To prevent a cookie being returned add 'answer-cookie no;' to named.conf. [GL #173]

  answer-cookie 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 should not be disabled unless absolutely necessary.

  Remove support for silently ignoring 'no-change' deltas from BIND 8 when processing an IXFR stream. 'no-change' deltas will now trigger a fallback to AXFR as the recovery mechanism.

  BIND 9 will no longer build on platforms that doesn't have proper IPv6 support. BIND 9 now also requires non-broken POSIX-compatible pthread support. Such platforms are usually long after their end-of-life date and they are neither developed nor supported by their respective vendors.

  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.

1.8 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 **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`.

1.9 Bug Fixes

- Running **rndc reconfig** could cause **inline-signing** zones to stop signing. [GL #439]
- Reloading all zones caused zone maintenance to stop for **inline-signing** zones. [GL #435]
- Signatures loaded from the journal for the signed version of an **inline-signing** zone were not scheduled for refresh. [GL #482]
- A referral response with a non-empty ANSWER section was incorrectly treated as an error; this caused certain domains to be non-resolvable. [GL #390]
- When a negative trust anchor was added to multiple views using **rndc nta**, the text returned via **rndc** was incorrectly truncated after the first line, making it appear that only one NTA had been added. This has been fixed. [GL #105]
- The view name is now included in the output of **rndc nta -dump**, for consistency with other options. [GL !816]
- **named** now rejects excessively large incremental (IXFR) zone transfers in order to prevent possible corruption of journal files which could cause **named** to abort when loading zones. [GL #339]

1.10 License

BIND is open source software licenced 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/.

1.11 End of Life

BIND 9.13 is an unstable development branch. When its development is complete, it will be renamed to BIND 9.14, which will be a stable branch.

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://www.isc.org/downloads/software-support-policy/ for details of ISC's software support policy.

1.12 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/.