1 Release Notes for BIND Version 9.13.1

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 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.

1.4 Security Fixes

- 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]

1.5 New Features

- 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]

1.6 Removed Features

- **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.

1.7   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 provder (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]

- **dig +noidnin** can be used to disable IDN processing on the input domain name, when BIND is compiled with IDN support.

- 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.

1.8 Bug Fixes

- None.

1.9 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/.

1.10 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.

1.11 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/.