1 Release Notes for BIND Version 9.17.1

1.1 Introduction

BIND 9.17 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 9.18 release, this document will be updated with additional features added and bugs fixed.

Please see the file `CHANGES` for a more detailed list of changes and bug fixes.

1.2 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.

1.3 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.

1.4 Notes for BIND 9.17.1

1.4.1 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]

1.4.2 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]

1.4.3 New Features

- A new option, **nsdname-wait-recurse**, has been added to the **response-policy** clause in the configuration file. When set to **no**, RPZ NSDNAME rules are only applied if the authoritative nameservers for the query name have been looked up and are present in the cache. If this information is not present, the RPZ NSDNAME rules are ignored, but the information is looked up in the background and applied to subsequent queries. The default is **yes**, meaning that RPZ NSDNAME rules should always be applied, even if the information needs to be looked up first. [GL #1138]

1.4.4 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]

1.4.5 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]

1.5 Notes for BIND 9.17.0

1.5.1 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.

1.5.2 New Features

- When a secondary server receives a large incremental zone transfer (IXFR), it can have a negative impact on query performance while the incremental changes are applied to the zone. To address this, **named** can now limit the size of IXFR responses it sends in response to zone transfer requests. If an IXFR response would be larger than an AXFR of the entire zone, it will send an AXFR response instead.

  This behavior is controlled by the **max-ixfr-ratio** option - a percentage value representing the ratio of IXFR size to the size of a full zone transfer. The default is `100%`. [GL #1515]
- A new RPZ option **nsdname-wait-recurse** controls whether RPZ-NSDNAME rules should always be applied even if the names of authoritative name servers for the query name need to be looked up recurively first. The default is **`yes`**. Setting it to **`no`** speeds up initial responses by skipping RPZ-NSDNAME rules when name server domain names are not yet in the cache. The names will be looked up in the background and the rule will be applied for subsequent queries. [GL #1138]

1.5.3 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]
- The **rndc nta -dump** and **rndc secroots** commands now both include **validate-except** entries when listing negative trust anchors. These are indicated by the keyword `permanent` in place of the expiry date. [GL #1532]

1.5.4 Bug Fixes

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

1.6 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/.

1.7 End of Life

BIND 9.17 is an unstable development branch. When its development is complete, it will be renamed to BIND 9.18, which will be a stable branch.

The end of life date for BIND 9.18 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.

1.8 Thank You

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