1 Release Notes for BIND Version 9.11.0a1

1.1 Introduction

BIND 9.11.0 is a new feature release of BIND, still under development. This document summarizes new features and functional changes that have been introduced on this branch. With each development release leading up to the final BIND 9.11.0 release, this document will be updated with additional features added and bugs fixed.

1.2 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.

1.3 Security Fixes

- Duplicate EDNS COOKIE options in a response could trigger an assertion failure. This flaw is disclosed in CVE-2016-2088. [RT #41809]
- Insufficient testing when parsing a message allowed records with an incorrect class to be be accepted, triggering a REQUIRE failure when those records were subsequently cached. This flaw is disclosed in CVE-2015-8000. [RT #40987]
- Incorrect reference counting could result in an INSIST failure if a socket error occurred while performing a lookup. This flaw is disclosed in CVE-2015-8461. [RT#40945]
- An incorrect boundary check in the OPENPGPKEY rdatatype could trigger an assertion failure. This flaw is disclosed in CVE-2015-5986. [RT #40286]
- A buffer accounting error could trigger an assertion failure when parsing certain malformed DNSSEC keys.

  This flaw was discovered by Hanno Böck of the Fuzzing Project, and is disclosed in CVE-2015-5722. [RT #40212]
- A specially crafted query could trigger an assertion failure in message.c.

  This flaw was discovered by Jonathan Foote, and is disclosed in CVE-2015-5477. [RT #40046]
- On servers configured to perform DNSSEC validation, an assertion failure could be triggered on answers from a specially configured server.

  This flaw was discovered by Breno Silveira Soares, and is disclosed in CVE-2015-4620. [RT #39795]
- On servers configured to perform DNSSEC validation using managed trust anchors (i.e., keys configured explicitly via **managed-keys**, or implicitly via **dnssec-validation auto;** or **dnssec-lookaside auto;**), revoking a trust anchor and sending a new untrusted replacement could cause **named** to crash with an assertion failure. This could occur in the event of a botched key rollover, or potentially as a result of a deliberate attack if the attacker was in position to monitor the victim's DNS traffic.

  This flaw was discovered by Jan-Piet Mens, and is disclosed in CVE-2015-1349. [RT #38344]
- A flaw in delegation handling could be exploited to put **named** into an infinite loop, in which each lookup of a name server triggered additional lookups of more name servers. This has been addressed by placing limits on the number of levels of recursion **named** will allow (default 7), and on the number of queries that it will send before terminating a recursive query (default 50).

  The recursion depth limit is configured via the `max-recursion-depth` option, and the query limit via the `max-recursion-queries` option.

  The flaw was discovered by Florian Maury of ANSSI, and is disclosed in CVE-2014-8500. [RT #37580]

- Two separate problems were identified in BIND's GeoIP code that could lead to an assertion failure. One was triggered by use of both IPv4 and IPv6 address families, the other by referencing a GeoIP database in `named.conf` which was not installed. Both are covered by CVE-2014-8680. [RT #37672] [RT #37679]

  A less serious security flaw was also found in GeoIP: changes to the **geoip-directory** option in `named.conf` were ignored when running **rndc reconfig**. In theory, this could allow **named** to allow access to unintended clients.

- Specific APL data could trigger an INSIST. This flaw is disclosed in CVE-2015-8704. [RT #41396]

- Certain errors that could be encountered when printing out or logging an OPT record containing a CLIENT-SUBNET option could be mishandled, resulting in an assertion failure. This flaw is disclosed in CVE-2015-8705. [RT #41397]

- Malformed control messages can trigger assertions in named and rndc. This flaw is disclosed in CVE-2016-1285. [RT #41666]

- The resolver could abort with an assertion failure due to improper DNAME handling when parsing fetch reply messages. This flaw is disclosed in CVE-2016-1286. [RT #41753]

1.4 New Features

- Added support for DynDB, a new interface for loading zone data from an external database, developed by Red Hat for the FreeIPA project. (Thanks in particular to Adam Tkac and Petr Spacek of Red Hat for the contribution.)

  Unlike the existing DLZ and SDB interfaces, which provide a limited subset of database functionality within BIND --- translating DNS queries into real-time database lookups with relatively poor performance and with no ability to handle DNSSEC-signed data --- DynDB is able to fully implement and extend the database API used natively by BIND.

  A DynDB module could pre-load data from an external data source, then serve it with the same performance and functionality as conventional BIND zones, and with the ability to take advantage of database features not available in BIND, such as multi-master replication.

- New quotas have been added to limit the queries that are sent by recursive resolvers to authoritative servers experiencing denial-of-service attacks. When configured, these options can both reduce the harm done to authoritative servers and also avoid the resource exhaustion that can be experienced by recursives when they are being used as a vehicle for such an attack.

  - `fetches-per-server` limits the number of simultaneous queries that can be sent to any single authoritative server. The configured value is a starting point; it is automatically adjusted downward if the server is partially or completely non-responsive. The algorithm used to adjust the quota can be configured via the `fetch-quota-params` option.
  - `fetches-per-zone` limits the number of simultaneous queries that can be sent for names within a single domain. (Note: Unlike "fetches-per-server", this value is not self-tuning.)

  Statistics counters have also been added to track the number of queries affected by these quotas.

- Added support for **dnstap**, a fast, flexible method for capturing and logging DNS traffic, developed by Robert Edmonds at Farsight Security, Inc., whose assistance is gratefully acknowledged.

  To enable **dnstap** at compile time, the **fstrm** and **protobuf-c** libraries must be available, and BIND must be configured with `--enable-dnstap`.

  A new utility **dnstap-read** has been added to allow **dnstap** data to be presented in a human-readable format.

  For more information on **dnstap**, see http://dnstap.info.

- New statistics counters have been added to track traffic sizes, as specified in RSSAC002. Query and response message sizes are broken up into ranges of histogram buckets: TCP and UDP queries of size 0-15, 16-31, ..., 272-288, and 288+, and TCP and UDP responses of size 0-15, 16-31, ..., 4080-4095, and 4096+. These values can be accessed via the XML and JSON statistics channels at, for example, http://localhost:8888/xml/v3/traffic or http://localhost:8888/json/v1/traffic.

- The serial number of a dynamically updatable zone can now be set using **rndc signing -serial *number zonename***. This is particularly useful with `inline-signing` zones that have been reset. Setting the serial number to a value larger than that on the slaves will trigger an AXFR-style transfer.
- When answering recursive queries, SERVFAIL responses can now be cached by the server for a limited time; subsequent queries for the same query name and type will return another SERVFAIL until the cache times out. This reduces the frequency of retries when a query is persistently failing, which can be a burden on recursive serviers. The SERVFAIL cache timeout is controlled by `servfail-ttl`, which defaults to 1 second and has an upper limit of 30.
- The new **rndc nta** command can now be used to set a "negative trust anchor" (NTA), disabling DNSSEC validation for a specific domain; this can be used when responses from a domain are known to be failing validation due to administrative error rather than because of a spoofing attack. NTAs are strictly temporary; by default they expire after one hour, but can be configured to last up to one week. The default NTA lifetime can be changed by setting the `nta-lifetime` in `named.conf`. When added, NTAs are stored in a file (*`viewname`*`.nta`) in order to persist across restarts of the **named** server.
- The EDNS Client Subnet (ECS) option is now supported for authoritative servers; if a query contains an ECS option then ACLs containing `geoip` or `ecs` elements can match against the the address encoded in the option. This can be used to select a view for a query, so that different answers can be provided depending on the client network.
- The EDNS EXPIRE option has been implemented on the client side, allowing a slave server to set the expiration timer correctly when transferring zone data from another slave server.
- A new `masterfile-style` zone option controls the formatting of text zone files: When set to `full`, the zone file will dumped in single-line-per-record format.
- **dig +ednsopt** can now be used to set arbitrary EDNS options in DNS requests.
- **dig +ednsflags** can now be used to set yet-to-be-defined EDNS flags in DNS requests.
- **dig +[no]ednsnegotiation** can now be used enable / disable EDNS version negotiation.
- **dig +header-only** can now be used to send queries without a question section.
- **dig +ttlunits** causes **dig** to print TTL values with time-unit suffixes: w, d, h, m, s for weeks, days, hours, minutes, and seconds.
- **dig +zflag** can be used to set the last unassigned DNS header flag bit. This bit in normally zero.
- **dig +dscp=*value*** can now be used to set the DSCP code point in outgoing query packets.
- **dig +mapped** can now be used to determine if mapped IPv4 addresses can be used.
- `serial-update-method` can now be set to `date`. On update, the serial number will be set to the current date in YYYYMMDDNN format.
- **dnssec-signzone -N date** also sets the serial number to YYYYMMDDNN.
- **named -L *filename*** causes **named** to send log messages to the specified file by default instead of to the system log.
- The rate limiter configured by the `serial-query-rate` option no longer covers NOTIFY messages; those are now separately controlled by `notify-rate` and `startup-notify-rate` (the latter of which controls the rate of NOTIFY messages sent when the server is first started up or reconfigured).
- The default number of tasks and client objects available for serving lightweight resolver queries have been increased, and are now configurable via the new `lwres-tasks` and `lwres-clients` options in `named.conf`. [RT #35857]
- Log output to files can now be buffered by specifying **buffered yes;** when creating a channel.

- **delv +tcp** will exclusively use TCP when sending queries.
- **named** will now check to see whether other name server processes are running before starting up. This is implemented in two ways: 1) by refusing to start if the configured network interfaces all return "address in use", and 2) by attempting to acquire a lock on a file specified by the `lock-file` option or the **-X** command line option. The default lock file is `/var/run/named/named.lock`. Specifying `none` will disable the lock file check.
- **rndc delzone** can now be applied to zones which were configured in `named.conf`; it is no longer restricted to zones which were added by **rndc addzone**. (Note, however, that this does not edit `named.conf`; the zone must be removed from the configuration or it will return when **named** is restarted or reloaded.)
- **rndc modzone** can be used to reconfigure a zone, using similar syntax to **rndc addzone**.
- **rndc showzone** displays the current configuration for a specified zone.
- Added server-side support for pipelined TCP queries. Clients may continue sending queries via TCP while previous queries are processed in parallel. Responses are sent when they are ready, not necessarily in the order in which the queries were received.

  To revert to the former behavior for a particular client address or range of addresses, specify the address prefix in the "keep-response-order" option. To revert to the former behavior for all clients, use "keep-response-order { any; };".
- The new **mdig** command is a version of **dig** that sends multiple pipelined queries and then waits for responses, instead of sending one query and waiting the response before sending the next. [RT #38261]
- To enable better monitoring and troubleshooting of RFC 5011 trust anchor management, the new **rndc managed-keys** can be used to check status of trust anchors or to force keys to be refreshed. Also, the managed-keys data file now has easier-to-read comments. [RT #38458]
- An **--enable-querytrace** configure switch is now available to enable very verbose query tracelogging. This option can only be set at compile time. This option has a negative performance impact and should be used only for debugging. [RT #37520]
- A new **tcp-only** option can be specified in **server** statements to force **named** to connect to the specified server via TCP. [RT #37800]
- The **nxdomain-redirect** option specifies a DNS namespace to use for NXDOMAIN redirection. When a recursive lookup returns NXDOMAIN, a second lookup is initiated with the specified name appended to the query name. This allows NXDOMAIN redirection data to be supplied by multiple zones configured on the server or by recursive queries to other servers. (The older method, using a single **type redirect** zone, has better average performance but is less flexible.) [RT #37989]
- The following types have been implemented: CSYNC, NINFO, RKEY, SINK, TA, TALINK.
- A new **message-compression** option can be used to specify whether or not to use name compression when answering queries. Setting this to **no** results in larger responses, but reduces CPU consumption and may improve throughput. The default is **yes**.
- A "read-only" clause is now available for non-destructive control channel access. In such cases, a restricted set of rndc commands are allowed for querying information from named. By default, control channel access is read-write.
- When loading managed signed zones detect if the RRSIG's inception time is in the future and regenerate the RRSIG immediately. This helps when the system's clock needs to be reset backwards.

1.5 Feature Changes

- The timers returned by the statistics channel (indicating current time, server boot time, and most recent reconfiguration time) are now reported with millisecond accuracy. [RT #40082]
- Updated the compiled in addresses for H.ROOT-SERVERS.NET.
- ACLs containing **geoip asnum** elements were not correctly matched unless the full organization name was specified in the ACL (as in **geoip asnum "AS1234 Example, Inc.";**). They can now match against the AS number alone (as in **geoip asnum "AS1234";**).
- When using native PKCS#11 cryptography (i.e., **configure --enable-native-pkcs11**) HSM PINs of up to 256 characters can now be used.
- NXDOMAIN responses to queries of type DS are now cached separately from those for other types. This helps when using "grafted" zones of type forward, for which the parent zone does not contain a delegation, such as local top-level domains. Previously a query of type DS for such a zone could cause the zone apex to be cached as NXDOMAIN, blocking all subsequent queries. (Note: This change is only helpful when DNSSEC validation is not enabled. "Grafted" zones without a delegation in the parent are not a recommended configuration.)
- Update forwarding performance has been improved by allowing a single TCP connection to be shared between multiple updates.
- By default, **nsupdate** will now check the correctness of hostnames when adding records of type A, AAAA, MX, SOA, NS, SRV or PTR. This behavior can be disabled with **check-names no**.
- Added support for OPENPGPKEY type.
- The names of the files used to store managed keys and added zones for each view are no longer based on the SHA256 hash of the view name, except when this is necessary because the view name contains characters that would be incompatible with use as a file name. For views whose names do not contain forward slashes ('/'), backslashes ('\'), or capital letters - which could potentially cause namespace collision problems on case-insensitive filesystems - files will now be named after the view (for example, `internal.mkeys` or `external.nzf`). However, to ensure consistent behavior when upgrading, if a file using the old name format is found to exist, it will continue to be used.
- "rndc" can now return text output of arbitrary size to the caller. (Prior to this, certain commands such as "rndc tsig-list" and "rndc zonestatus" could return truncated output.)
- Errors reported when running **rndc addzone** (e.g., when a zone file cannot be loaded) have been clarified to make it easier to diagnose problems.
- When encountering an authoritative name server whose name is an alias pointing to another name, the resolver treats this as an error and skips to the next server. Previously this happened silently; now the error will be logged to the newly-created "cname" log category.
- If **named** is not configured to validate answers, then allow fallback to plain DNS on timeout even when we know the server supports EDNS. This will allow the server to potentially resolve signed queries when TCP is being blocked.
- Large inline-signing changes should be less disruptive. Signature generation is now done incrementally; the number of signatures to be generated in each quantum is controlled by "sig-signing-signatures *number*;". [RT #37927]
- The experimental SIT option (code point 65001) of BIND 9.10.0 through BIND 9.10.2 has been replaced with the COOKIE option (code point 10). It is no longer experimental, and is sent by default, by both **named** and **dig**.

  The SIT-related named.conf options have been marked as obsolete, and are otherwise ignored.
- When **dig** receives a truncated (TC=1) response or a BADCOOKIE response code from a server, it will automatically retry the query using the server COOKIE that was returned by the server in its initial response. [RT #39047]

- A alternative NXDOMAIN redirect method (nxdomain-redirect) which allows the redirect information to be looked up from a namespace on the Internet rather than requiring a zone to be configured on the server is now available.
- Retrieving the local port range from net.ipv4.ip_local_port_range on Linux is now supported.
- Within the `response-policy` option, it is now possible to configure RPZ rewrite logging on a per-zone basis using the `log` clause.
- The default preferred glue is now the address type of the transport the query was received over.
- On machines with 2 or more processors (CPU), the default value for the number of UDP listeners has been changed to the number of detected processors minus one.
- Zone transfers now use smaller message sizes to improve message compression. This results in reduced network usage.
- Added support for the type AVC.

1.6 Porting Changes

- None.

1.7 Bug Fixes

- None.

1.8 End of Life

The end of life for BIND 9.11 is yet to be determined but will not be before BIND 9.13.0 has been released for 6 months. https://www.isc.org/downloads/software-support-policy/

1.9 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/.