BIND 9 Update,
OARC 38

Vicky Risk, vicky@isc.org
Fixing tech debt in an enterprise codebase
Expanded QA team

• ~70 CI tests for every version of every MR
  • new CI test for memory leaks

• Daily extended tests, including respdfiff, extra scrutiny for monthly releases

• on-going realistic performance testing, adding TCP
we're comparing what **NAMED** returns for a predefined set of queries against what Knot Resolver (5.5.1), Unbound (1.13.1), and PowerDNS Recursor (4.5.9) return

if the *ratio* of discrepancies exceeds a preset threshold (0.5%), the job fails (we investigate a possible BIND error)

note, however, how this is calculated: a difference only counts if **all** other resolvers return the same response and **NAMED** returns something different
Target disagreements between the tested version and the reference one (Knot Resolver 5.5.1, Unbound 1.13.1, and PowerDNS Recursor 4.5.9) comprise 0.34% of not ignored answers; of these, 38.11% are timeout disagreements, which can be attributed to network issues*.

* Network differences occur even between separate runs with the same software, due to the natural variability of the live Internet.
9.16 vs 9.18 (UDP)

**Response Time (ms)**

- **Higher latency**
  - 20% of 9.16 queries take > 10 msec
  - <4% of 9.18 queries take > 10 msec

- **Lower latency**

Replacing RBTDB

Goals

1. Code simplification

2. reduce blocking on updates

3. not slower

4. not more memory

Plan

• Adapt qp-trie, invented by Tony Finch in 2015

• used by Knot DNS since 2016, experiments using NSD 2020-2021

• more complete multithreading, multi-version concurrency

• test in isolation, replace rbtdb in stages

Photo by Jan Antonin Kolar on Unsplash
qp-trie Status

in early testing before merge into main (dev) branch

double-threaded code solid, multithreaded in progress

<table>
<thead>
<tr>
<th></th>
<th>RBT</th>
<th>qp-trie</th>
</tr>
</thead>
<tbody>
<tr>
<td>time to load 1M domain names</td>
<td>1.0 seconds</td>
<td>0.7 seconds</td>
</tr>
<tr>
<td>memory consumed</td>
<td>113.3 MiB</td>
<td>45.4 MiB</td>
</tr>
</tbody>
</table>

research code, blog articles, and notes:  https://dotat.at/prog/qp/

other WIP

• moar Extended Errors
• catalog zones update to the 06 draft
• sponsoring an OpenSSL 3.0 PKCS #11 provider engine
• refactoring: “stream DNS” for TLS & TCP
• ARM update with Ron Aitchison (ProDNS and BIND author)
Linking, tagging in the ARM

8.3.2. Transfer Tag Statements

<table>
<thead>
<tr>
<th>Statement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-notify</td>
<td>Defines an address_match_list that is allowed to send NOTIFY messages for the zone, in addition to addresses defined in the primaries option for the zone.</td>
</tr>
<tr>
<td>allow-transfer</td>
<td>Defines an address_match_list of hosts that are allowed to transfer the zone information from this server.</td>
</tr>
<tr>
<td>allow-update</td>
<td>Defines an address_match_list of hosts that are allowed to submit dynamic updates for primary zones.</td>
</tr>
<tr>
<td>allow-update-forwarding</td>
<td>Defines an address_match_list of hosts that are allowed to submit dynamic updates to a secondary server for transmission to a primary.</td>
</tr>
<tr>
<td>also-notify</td>
<td>Defines one or more hosts that are sent NOTIFY messages when zone changes occur.</td>
</tr>
<tr>
<td>alt-transfer-source</td>
<td>Defines alternate local IPv4 address(es) to be used by the server for inbound zone transfers, if the address(es) defined by transfer-source fail and use-alt-transfer-source is enabled.</td>
</tr>
<tr>
<td>alt-transfer-source-v6</td>
<td>Defines alternate local IPv6 address(es) to be used by the server for inbound zone transfers.</td>
</tr>
<tr>
<td>ixfr-from-differences</td>
<td>Controls how IXFR transfers are calculated.</td>
</tr>
<tr>
<td>max-journal-size</td>
<td>Controls the size of journal files.</td>
</tr>
</tbody>
</table>
Parent vs Child

We are debating changing BIND from child-centric to parent-centric.

Your comments are welcome at:

https://gitlab.isc.org/isc-projects/bind9/-/issues/3311
Current Stable - 9.18

Now on a 2-year development cycle. 9.18 released Jan 2022.

- Better recursive performance
- Better memory usage, reduced fragmentation with jemalloc
- TLS security - DoH, DoT & XoT, dig +tls
- DNSSEC KASP
- OpenSSL 3.0
- Extended errors
Links

• Tony’s blog (qp-trie): https://dotat.at/prog/qp/

• Parent vs child discussion: https://gitlab.isc.org/isc-projects/bind9/-/issues/3311

• Stream DNS issue: https://gitlab.isc.org/isc-projects/bind9/-/issues/3374

• example res-diff output: https://gitlab.isc.org/isc-projects/bind9/-/jobs/2635397