Knot DNS Update

What does the future hold?

Ondřej Surý • ondrej.sury@nic.cz • 2014 May 14

Knot DNS 1.4

- DNSSEC automatic signing

```
zones {
  example.com {
    file ``example.com'';
    dnssec-enable on;
    dnssec-keydir ``/etc/knot/keys'';
  }
}
$ knotc signzone
```

- IDN support in Knot DNS utilities (kdig, khost, knusupdate)
- Lower memory consumption

Knot DNS WIP

- Knot DNS 1.5
  - Dynamic modules
  - Lots of refactoring under the hood
    - Lower memory consumption
    - Processing speed
- Knot DNS 1.6
  - Improved DNSSEC support

Dynamic modules

- Hooks in query-response processing
- Different possibilities
  - Split-horizon (GeoIP, ...)
  - Poor man’s HA
  - reverse and forward resource record synthesis

Synthetized Resource Records

- IPv6 address space is vast
  1. It's not possible to have all PTR records in the DNS server manually
  2. Customers want to send mail from DSL lines
  3. MTAs are checking for reverse records and rejecting emails
  4. Customers are complaining
- Configuration (more in manual)

```
synth_record "(forward|reverse) <prefix> <ttl> \
 <address>/<nn>";
```

- No DNSSEC signing (yet!)

Example Configuration

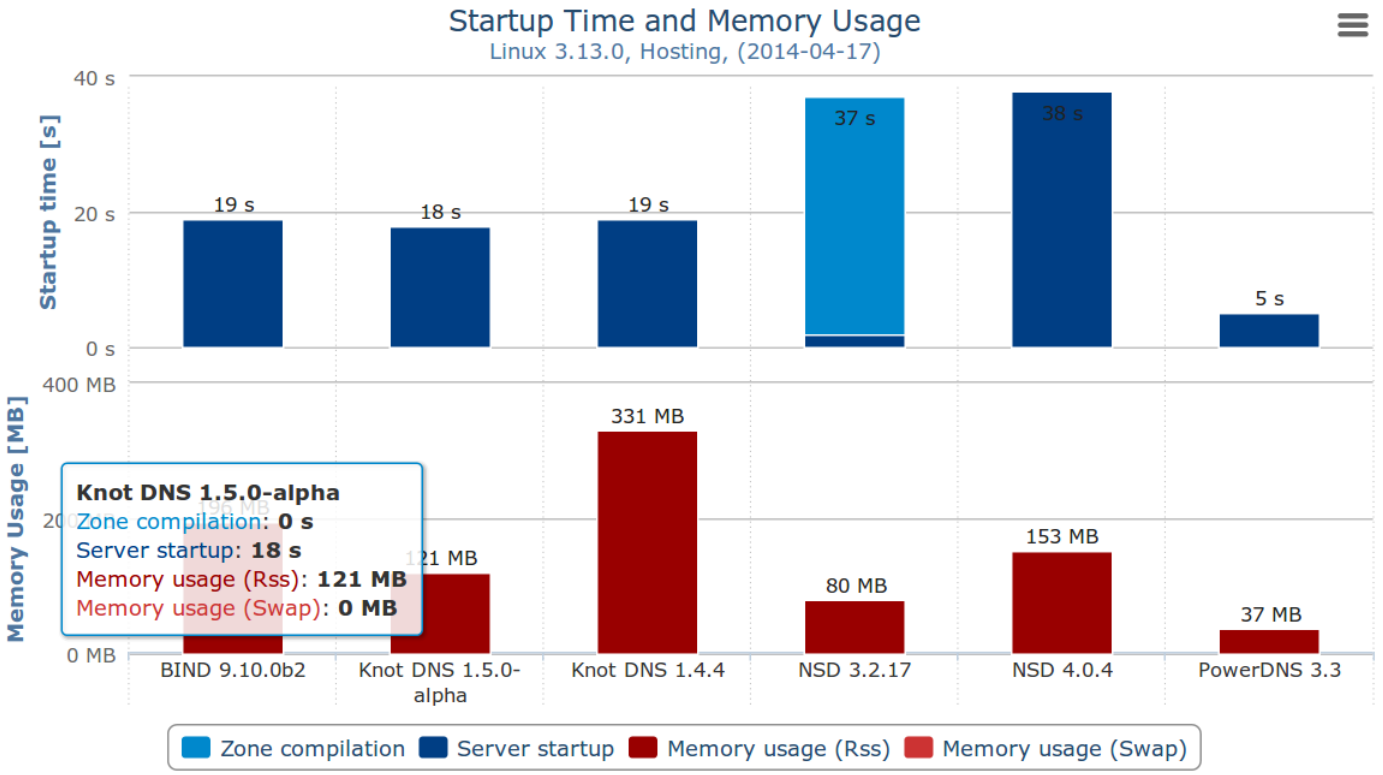
```
example.org. {
  query_module {
    synth_record "forward gen- 400 2620:0:b61::/52";
    synth_record "forward gen- 400 192.168.1.0/25";
  }
}
1.168.192.in-addr.arpa {
  query_module { synth_record "reverse gen- example.org.
400 192.168.1.0/25"; }
}
1.6.b.0.0.0.0.0.0.0.2.6.2.ip6.arpa {
  query_module { synth_record "reverse gen- example.org.
400 2620:0:b61::/52"; }
}
```

Example Output

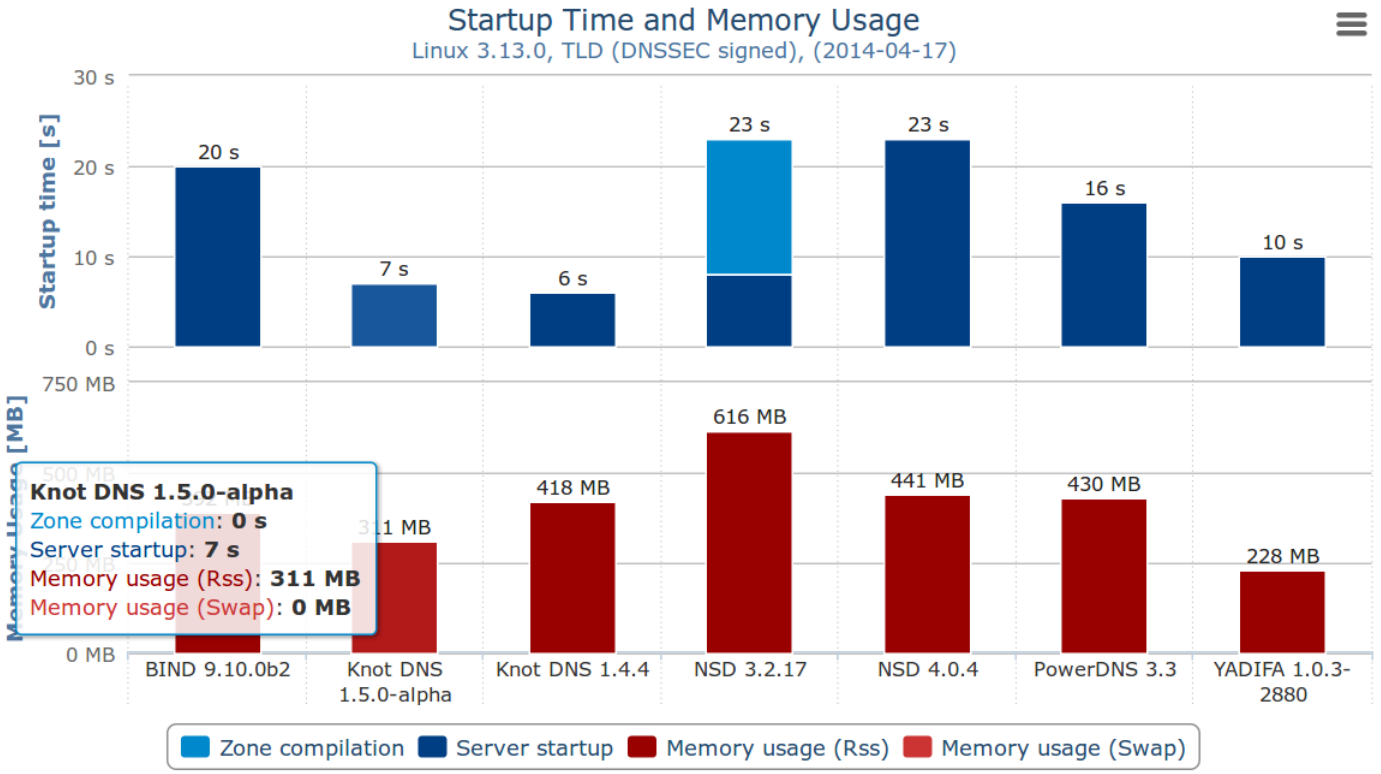
```
$ kdig AAAA gen-2620-0000-0b61-0100-0000-0000-0000-
0000.example.org.
[...]
;; QUESTION SECTION:
;; gen-2620-0000-0b61-0100-0000-0000-0000-0000.example.org.
0 IN AAAA
;; ANSWER SECTION:
gen-2620-0000-0b61-0100[...] 400 IN AAAA 2620:0:b61:100::

$ kdig PTR 1.0.0...1.6.b.0.0.0.0.0.0.2.6.2.ip6.arpa.
[...]
;; QUESTION SECTION:
;; 1.0.0...1.6.b.0.0.0.0.0.0.2.6.2.ip6.arpa. 0 IN PTR
;; ANSWER SECTION:
[...] 400 IN PTR gen-2620-0000-0b61-0000-0000-0000-
0000-0001.example.org.
```

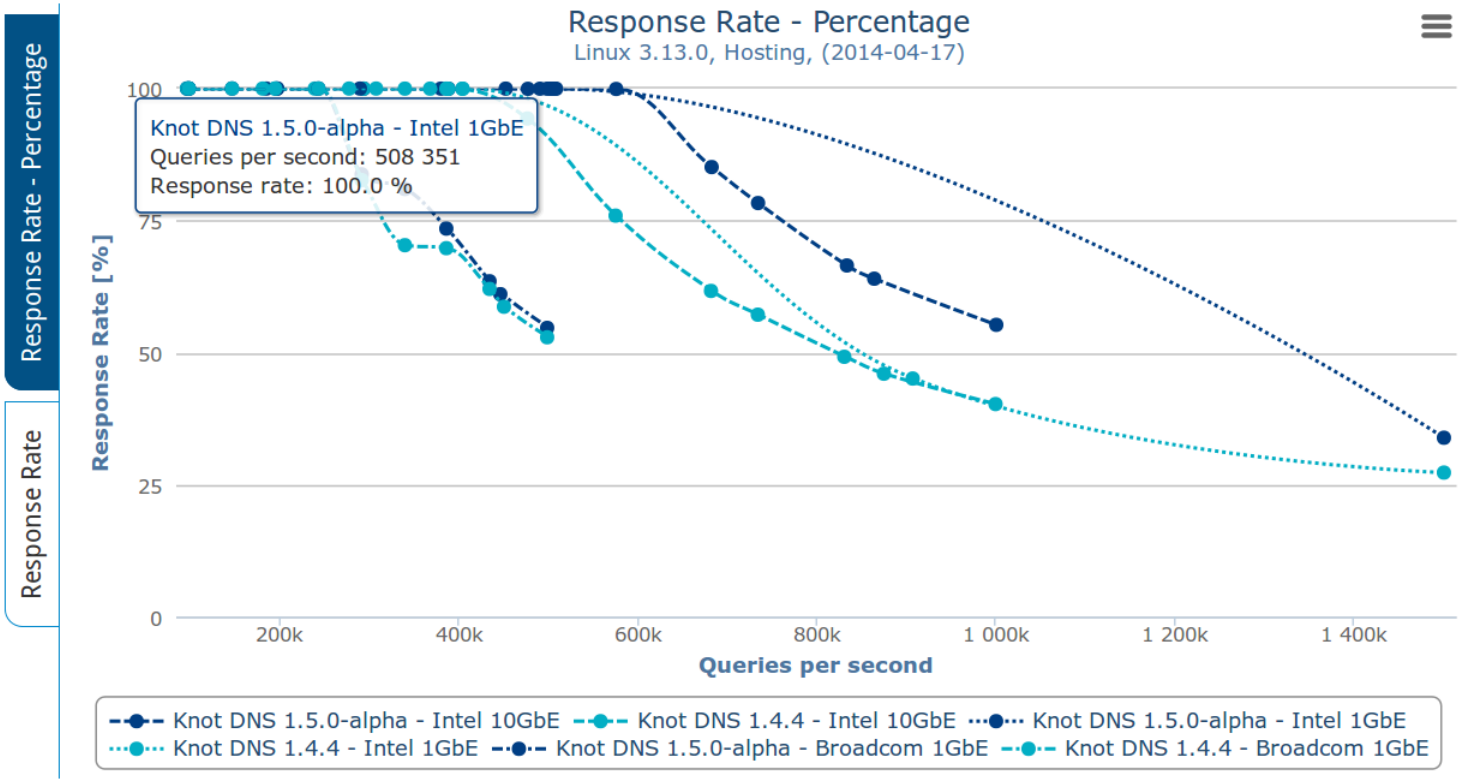
Memory (10k small zones)



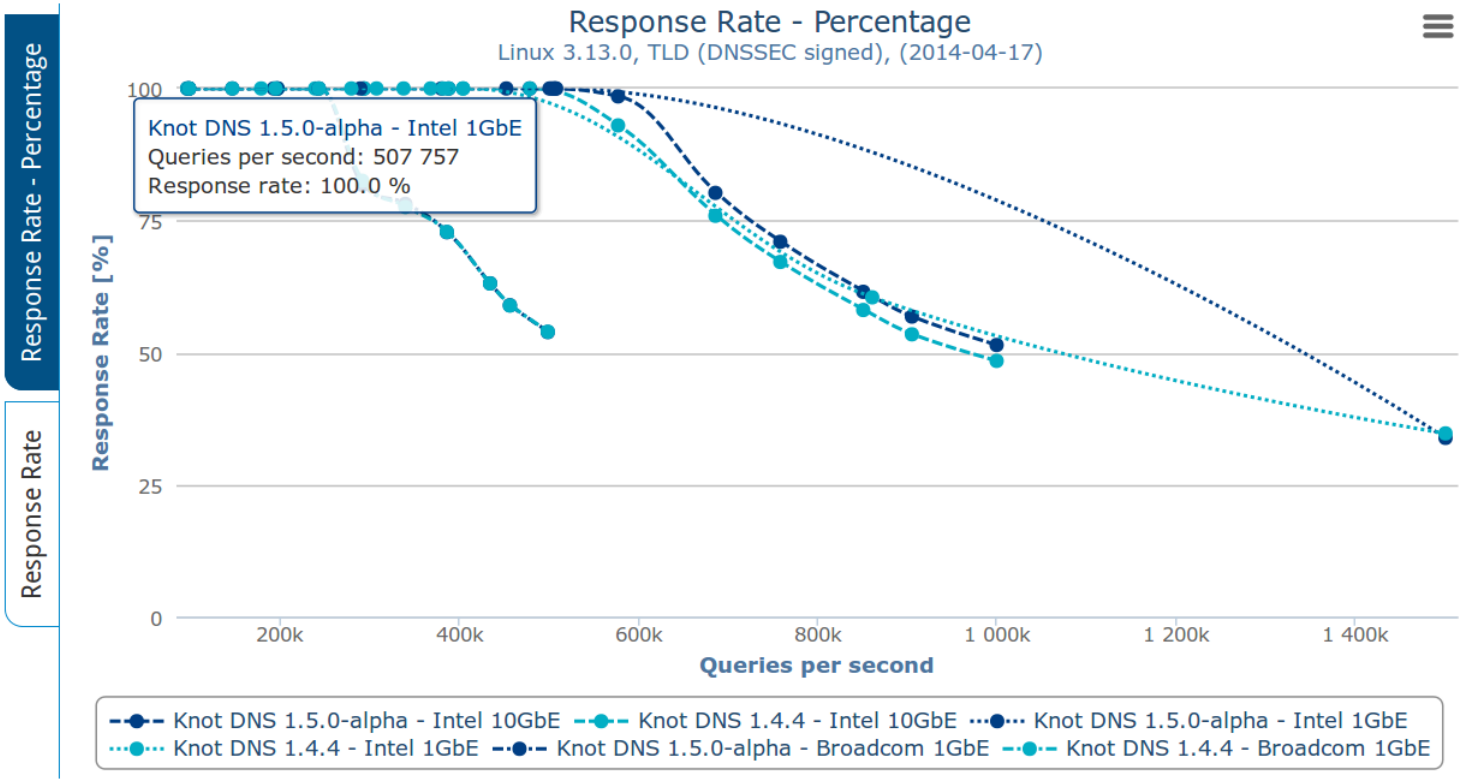
Memory (TLD signed; 250k RRs)



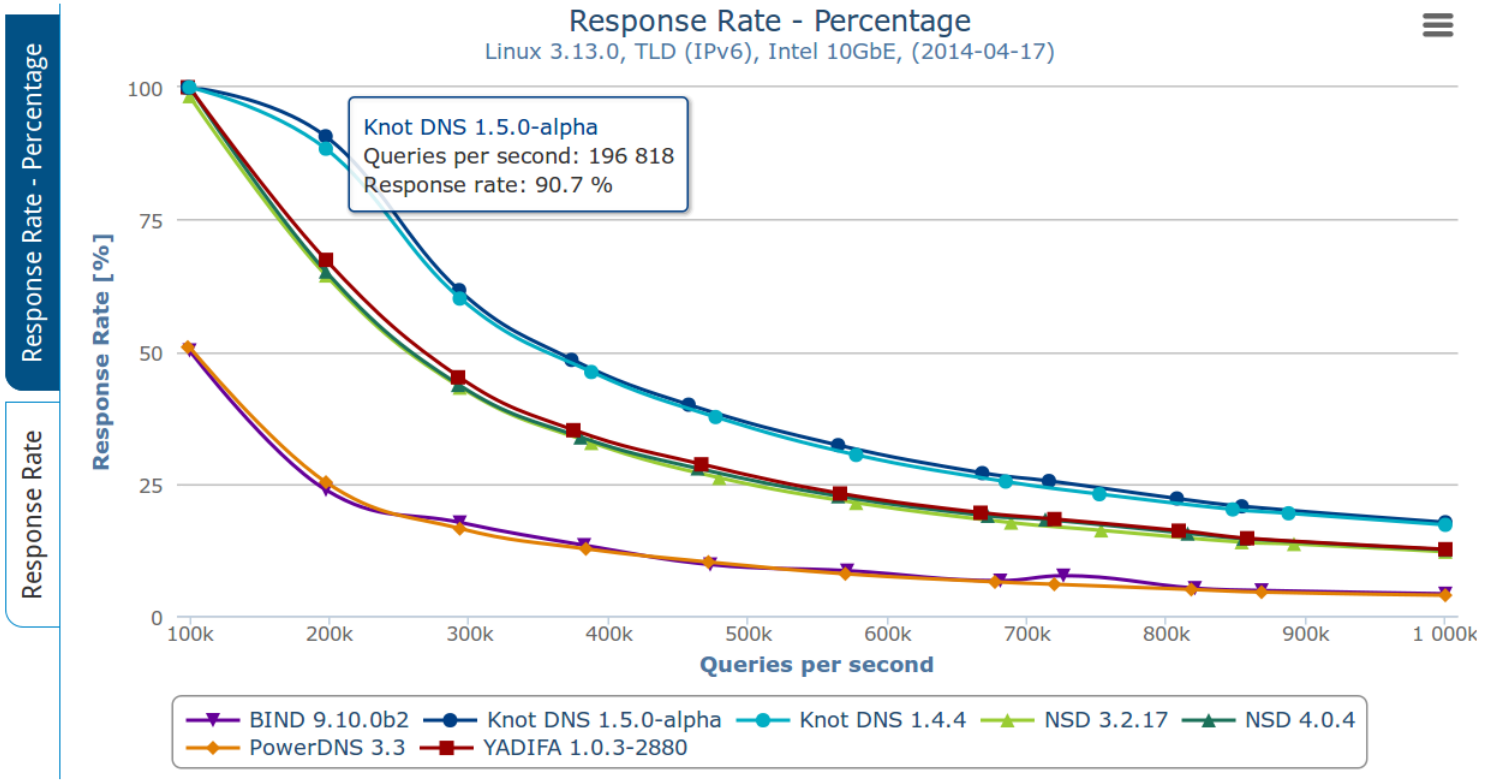
Response Rate (10k small zones)



Response Rate (TLD signed; 250k RRs)



Response Rate (TLD; IPv6)



Improved DNSSEC support

- lib(knot)dnssec separation
  - Switch from OpenSSL to GnuTLS (nope, not heartbleed related)
  - Support for hardware security modules (PKCS#11)
  - Key and Signing Policy
- On-line signing
  - Minimal NSEC3 encloser responses
  - Dynamic modules

Questions?