Knot DNS

A high-performance authoritative DNS server

Ondřej Surý • ondrej.sury@nic.cz • 2014 October 13

What is Knot DNS?

- https://www.knot-dns.cz/
- high-performance and scalable authoritative DNS server
- free, open-source, written from scratch
- under active development
- standards compliant and fast tracking
- non-stop operation (runtime reconfiguration)
- usable for root, TLD and DNS hosting
- DNSSEC automatic signing
- dynamic modules

Knot DNS History & Roadmap

- Knot DNS 0.8 – 1.4.6 [stable release]
    - First public release in 2011 (0.8)
    - Active development [fast-forward]
    - DNSSEC automatic signing (1.4)
- Knot DNS 1.5
    - Lots of refactoring under the hood
    - Dynamic modules
    - Memory usage reduction
- Knot DNS 1.6
    - Long Term Support release
    - Persistent timers

Dynamic modules

- Hooks in query-response processing
- Implemented modules
  - Synthetized Resource Records (PTR/A/AAAA)
  - dnstap query/response logging – structured binary log (dnstap.info)
- Different possibilities
  - Split-horizon (GeoIP, ...)
  - Poor man’s HA
  - Reverse and forward resource record synthesis

Persistent timers (1.6)

- Requested by RIPE NCC
- Timers will survive the server restart
  - EXPIRE
  - REFRESH
  - FLUSH

Roadmap - Knot DNS 2.0

- Knot DNS 2.0
  - Improved DNSSEC
    - Switch from OpenSSL to GnuTLS (nope, not heartbleed related)
    - Support for hardware security modules (PKCS#11)
    - Key and Signing Policy and tools
    - On-line signing (Minimal NSEC3 encloser, Dynamic modules)
  - New configuration format (machine readable)

Roadmap – 2015

- Knot DNS 2.1+
  - Different storage backends
    - File based
    - Memory based
    - key-value databases
    - SQL databases
  - Different configuration backends
    - File based
    - Database based (for 1M+ zones)
  - Provisioning API (DNS remote API)

Roadmap – Knot DNS Resolver

- Knot DNS Resolver
  - In Development Now
  - Technology Preview by the end of the year
  - Dynamic modules
  - Persistent cache
  - Privacy (QNAME minimization)

Licensing

- GNU GPLv3 license
- Open Development Process
  - Mailing list (knot-dns-users@lists.nic.cz)
  - Git Repository (https://gitlab.labs.nic.cz/labs/knot)

Support & Security

- Support
  - Best effort on mailing List
  - Contractual support (email, phone, ...)
- Security Vulnerability Disclosure
  - “If we know you, we’ll let you know”

Performance or Functionality?

- Both are important
- You don't have to sacrifice one for the other
- Performance
  - Sustain a high load under attack
- Functionality
  - DNS standards support is a MUST
  - Interoperability (RRTYPE support)
  - Ease of deployment (new & existing)
  - Robustness principle (Postel's law)

Performance testing

- Benchmarking should be as open as possible
  - Open code
  - Hardware specification
  - Operating System tuning
  - Software tuning
- It really should be a collaborative work

New features process

- Internal user requests
- External user requests
- DNS Community
- IETF process
- non-IETF ideas (RRL, NSEC5)

Existing TLD users

- CZ.NIC – $\frac{1}{3}$ of .cz servers
- Hostmaster DK (.dk)
- $\frac{1}{3}$ of RIPE NCC DNS Servers – 77 TLDs, in-addr.arpa, ip6.arpa, ...

Questions?