KNOT RESOLVER

A flexible DNSSEC-validating Resolver

Jaromír Talíř • jaromir.talir@nic.cz • 7.11.2016

CZ DOMAIN REGISTRY

Agenda

- What is Knot DNS Resolver
- Main features
- New features in 1.1 (released in Aug 2016)
- DNSSEC and root key rollover readiness

What is Knot DNS Resolver?

- Open-source DNS Resolver (GPLv3+) built on top of Knot DNS libraries
  - First version 1.0.0 – May 2016
  - Last version 1.1.1 – Aug 2016
- Check the website https://www.knot-resolver.cz
  - Deb and RPM packages
  - Sources at https://gitlab.labs.nic.cz/knot/resolver
  - Documentation: http://knot-resolver.rtfd.org
- Used in Turris Omnia routers (cca 4200 deployed)

Features

- Flexible shared cache backends (cache survives reloads)
  - Local (lmdb) and remote (memcached, redis)
  - New instances just pick the data from the shared cache
- Performance
  - No internal threading, scales by self-replication
  - Low memory consumption (lmdb cache can be paged out)
  - Performance testing
    - https://gitlab.labs.nic.cz/knot/resolver/wikis/Comparison-different-cache-usage-and-QPS
  - “Happy Eyeballs” IPv6 (20ms headstart)

Features

- Simple core extensible with modules in C, Lua & Go
- QNAME minimisation for DNS privacy
- DNS64 support to complement NAT64
- Views and ACL support
- Query policy based resolution
  - Match: pattern, suffix, RPZ
  - Action: PASS, DENY, DROP, FORWARD, TC

New features in 1.1

- DNS over TLS
- DNS cookies
- HTTP/2 module for monitoring your queries
- Restful API
- DNS Firewall
- https://ripe73.ripe.net/presentations/177-OMG-A-DNS-Firewall.pdf

General DNSSEC support

- RFC 403[3-5] – Full DNSSEC validation
- RFC 6650 – ECDSA support
- RFC 7646 – Negative Trust Anchors
- Implementation of CD (Checking Disabled) is in progress

Root key rollover readiness

- RFC 5011 – Automated Trust Anchor Management
  - Running instances will get new key automatically
  - File with the key must have read/write permissions
- Deb and RPM packages contains existing key
  - They will be updated after publication of new key

Root key rollover readiness

- Installation from source code will bootstrap key from IANA via HTTPS request to https://data.iana.org/root-anchors/root-anchors.xml
  - Functional DNS resolver must be present to resolve IANA address
  - Luasec module doesn’t support PKCS#7 yet
  - CA certificate of DigiCert is in source code
- http://knot-resolver.readthedocs.io/en/latest/daemon.html#enabling-dnssec

Thank You

Jaromir Talir • jaromir.talir@nic.cz

CZ DOMAIN REGISTRY