Knot DNS 2.0: Status Update

RIPE 70, Amsterdam

Jan Včelák • jan.vcelak@nic.cz • 2015 May 13

Knot DNS Timeline

- Knot DNS 0.8
  - first release (3 November 2011)
- Knot DNS 1.6
  - **Long-Term Support**
  - 1.6.0 (23 October 2014)
  - 1.6.3 (8 April 2015)
- Knot DNS 2.0
  - 1.99.1 – **KASP based DNSSEC** (11 February 2015)
  - 2.0.0-beta – **new configuration format** (23 April 2015)

Knot DNS 2.0 – Configuration

- Moving towards fast on-the-fly reconfiguration
- Completely revised configuration scheme
  - Reorganization of remotes and ACLs
  - Support for zone templates
- New configuration format
  - Custom format replaced by simplified YAML
  - Internally uses a binary LMDB database

Knot DNS 2.0 – Configuration in YAML

```
server:
    listen: ::@53
remote:
  - id: hidden
    address: 2001:1488::1:1
acl:
  - id: notify_from_hidden
    address: 2001:1488::1:1
    action: notify
  - id: transfer_to_slaves
    address: 2001:1488::1:0/120
    action: transfer
zone:
  - domain: knot-dns.cz
    master: hidden
    acl: [ notify_from_hidden, transfer_to_slaves ]
```

Knot DNS 2.0 – Zone Templates

```
template:
  - id: default
    storage: /var/lib/knot/zones
  - id: slave
    storage: /var/lib/knot/zones/slaved
    master: [ my-master ]
zone:
  - domain: knot-dns.cz
  - domain: dnssec.cz
  - domain: nic.cz
    template: slave
  - domain: unsigned.cz
    template: slave
```

Knot DNS 2.0 – DNSSEC

- Switch from OpenSSL to GnuTLS
- KASP (Key And Signature Policy)
- DNSSEC management:
  - New all-in-one management utility – `keymgr`
  - KASP database instead of key files
  - No longer depends on BIND (or ldns) utilities
- Automatic management features:
  - Generating initial signing keys
  - ZSK rotation (key pre-publish)

Knot DNS 2.0 – DNSSEC with KASP

- Configure zone policy:

```
$ keymgr init
$ keymgr policy add lab algorithm RSASHA256
$ keymgr zone add test.zone policy lab
```

- Start the server and check the logs:

```
zone will be loaded, serial 0
executing event 'generate initial keys'
loaded key, tag 57335, algorithm 8, KSK, public, active
loaded key, tag  8139, algorithm 8, ZSK, public, active
signing started
successfully signed
next signing on 2015-05-19T11:06:18
loaded, serial 0 -> 1131
```

Knot DNS 2.0 – DNSSEC without KASP

- Disable KASP policy:

```
$ keymgr zone set test.zone policy none
```

- Import key in legacy format:

```
$ keymgr zone key import test.zone Ktest.zone.+013+52930
```

- Generate new key:

```
$ keymgr zone key generate test.zone algo 13 size 256
```

- Set key timing parameters:

```
$ keymgr zone key set test.zone 4bc39559 \
  retire +7d remove +14d
```

Knot DNS 2.0 – DNSSEC Online Signing

- Experimental, not in the 2.0.0-beta
- Single-Type Signing Scheme, no caching
- Stacks well with modules (e.g., PTR records synthesis)

```
$ kdig +dnssec -x 2001:678:f::42
...
;; ANSWER SECTION:
2.4.0.0...ip6.arpa. 1200 IN PTR
    ptr-2001-0678-000f-0000-0000-0000-0000-0042.test
2.4.0.0...ip6.arpa. 1200 IN RRSIG
    PTR 13 34 1200 20150513104011 20150512094011 58499
    f.0.0.0.8.7.6.0.1.0.0.2.ip6.arpa. sPDfCc1nkhNg4...
...
```

Significant Users (Who Told Us)

- RIPE NCC (K-root, various TLDs)
- TLD operators (.cz, .dk, .cl)
- Microsoft
- Telefónica O2 Czech Republic
- Netriplex
- ICANN (test environment for L-root)
- various webhosters
- . . .

Thank you!

Jan Včelák • jan.vcelak@nic.cz • www.knot-dns.cz