Knot DNS 2.0

Seznámení s novými vlastnostmi

Jan Včelák • jan.vcelak@nic.cz • 13. 11. 2015

CZ.NIC | SPRÁVCE DOMÉNY CZ

Obsah prezentace

- Konfigurace serveru
- DNSSEC podepisování
- Testování výkonu
- Připravované vlastnosti

Konfigurace

- Konfigurační formát
  - Zjednodušený YAML namísto vlastního formátu
  - Interní binární reprezentace v LMDB
- Cílem je možnost úplné rekonfigurace serveru za běhu
- Konceptuální změny oproti Knot DNS 1.6
  - Definice vzdálených serverů, oprávnění
  - Zónové šablony

Konfigurace – textový formát

```
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 ]
```

Konfigurace – šablony pro zóny

```
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
```

Konfigurace – rozhraní příkazové řádky

- Přidání zóny do serveru:

```
$ knotc conf-set zone[labs.nic.cz]
```

- Zapnutí DNSSEC podepisování pro jednu zónu:

```
$ knotc conf-set zone[unsigned.cz].dnssec-signing true
```

- Odstranění slave serveru z notifikací:

```
$ knotc conf-unset template[default].notify slave007
```

- Získání seznamu nakonfigurovaných zón:

```
$ knotc conf-read zone.domain
```

DNSSEC

- Přechod z OpenSSL na GnuTLS
- KASP (Key And Signature Policy)
- Správa pomocí utility **keymgr**
- Automatické operace:
  - Generování počátečních klíčů
  - Rotace ZSK klíče (metodou „key pre-publish“)

DNSSEC – KASP

- Konfigurace politiky:

```
$ keymgr init
$ keymgr policy add lab algorithm ECDSAP256SHA256
$ keymgr zone add unsigned.cz policy lab
```

- Logy po spuštění serveru:

```
... zone will be loaded, serial 0
... executing event 'generate initial keys'
... loaded key, tag 62872, algorithm 13, KSK, public, active
... loaded key, tag 18932, algorithm 13, ZSK, public, active
... signing started
... successfully signed
... next signing on 2015-11-22T17:21:09
... loaded, serial 0 -> 2
```

DNSSEC – manuální podepisování

- Odebrání politiky:

```
$ keymgr zone set dnssec.cz policy none
```

- Vygenerování klíče:

```
$ keymgr zone key generate dnssec.cz algorithm 13 size 256
```

- Nastavení časových parametrů:

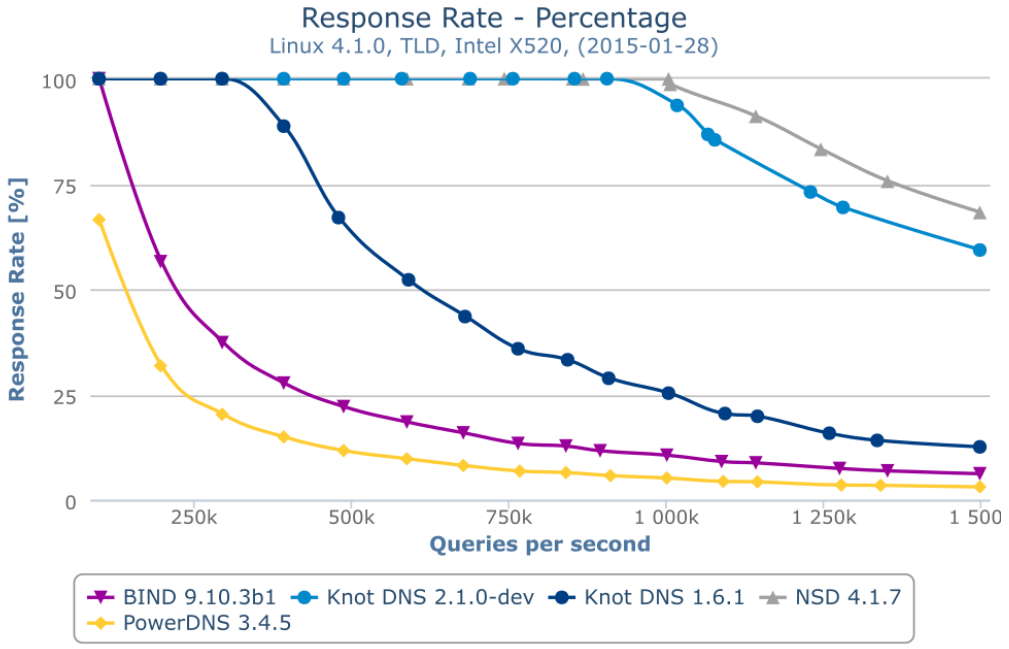
```
$ keymgr zone key set dnssec.cz 4bc39de7 retire +2d remove +4d
```

DNSSEC – online podepisování

- Experimentální modul
- Lze kombinovat s dalšími moduly, například syntézou PTR:

```
$ kdig +dnssec -x 2001:678:f::42
...
;; ANSWER SECTION:
2.4.0.0...ip6.arpa. 1200 IN PTR
    ip-2001-0678-000f-0000-0000-0000-0000-0042.example.net.
2.4.0.0...ip6.arpa. 1200 IN RRSIG
    PTR 13 34 1200 20151113192636 20151112182636 58499
    f.0.0.0.8.7.6.0.1.0.0.2.ip6.arpa. s4E3ywzD4aGcL...
...
```

Testování výkonu



- Různé scénáře testování
- Vše je open source
- UDP
- SO_REUSEPORT na Linuxu

Připravované vlastnosti

- DNSSEC: HSM moduly přes PKCS #11
- Modul pro geografický split-horizon
- Modul pro statistiky (kompatibilní s BIND)
- Obecné zlepšení výkonu na TCP

Naši uživatelé

- Microsoft
- RIPE NCC (K-root, .arpa, generické TLD)
- ICANN (L-root)
- Národní TLD operátoři (.cz, .dk, .cl)
- ...

Děkuji za pozornost

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