Knot DNS
Knot Resolver

Co přinesl rok 2016?

Ondřej Surý • ondrej.sury@nic.cz • 29. 11. 2016

Knot DNS

Novinky v Knot DNS

- Knot DNS 2.1 (leden 2016)
  - **SO_REUSEPORT**
  - **Dynamická konfigurační databáze**
  - **Podpora PKCS#11 rozhraní (HSM)**
  - Experimentální podpora in-band DNSSEC podpisů
- Knot DNS 2.2 (duben 2016)
  - **Nové knotc API pro konfiguraci serveru**
  - **Podpora pro další PKCS#11 HSM zařízení**
- Knot DNS 2.3 (srpen 2016)
  - **Konfigurace DNSSEC politik přímo v konfiguraci serveru (knot.conf)**
  - Podpora pro DNS privacy
  - Lepší podpora pro velké DNS hostingy
    - Výrazné zrychlení konfiguračních operací při mnoho zónách
    - Konfigurovatelná cesta k zónovým žurnálům
- Knot DNS 2.4 (přelom 2016/2017)
  - Výrazná úspora paměti pro DNS hostingy (qp-trie)
  - **Nové statistiky**

Podpora pro SO_REUSEPORT

- Nastavení soketu SO_REUSEPORT
  - Dříve: Jednotlivá vlákna/procesy “soupeří” o příchozí datagramy
  - Nyní: datagramy rozděluje přímo kernel
- Výsledek:
  - Masivní nárůst výkonu
  - Výkon přes **1.000.000** DNS odpovědí za sekundu

Aktuální výkon Knot DNS

Dynamická konfigurační databáze a nové konfigurační rozhraní

- Interně je konfigurace importována z knot.conf do LMDB databáze
- Všechny změny v konfiguraci se projeví hned po změně
- Knot DNS může běžet jen nad konfigurační databází (bez knot.conf)
- Změny se provádí přes knotc
- Spuštění serveru:
  - knotd -C /var/lib/knot/conf/
- Ideální pro automatizované nasazení
- Změna konfigurace:
  - knotc conf-begin # zahájíme transakci
  - knotc conf-set <item> <data> # nastavíme položku
  - knotc conf-diff # kontrola změn
  - knotc conf-commit # uložení změn

Podpora PKCS#11 HSM

- PKCS#11 – protokol pro přístup ke kryptografickým zařízením (HSM)
- Jeden standard, mnoho implementací :(
  - Feitian ePass 2003
  - SafeNet Network HSM
  - SoftHSM 2.0 (softwareové HSM)
  - Trustway Proteccio NetHSM
  - CrypTech (open hardware, open software) – https://cryptech.is/
- https://www.knot-dns.cz/docs/2.x/html/appendices.html#compatible-pkcs-11-devices

Nová konfigurace DNSSEC politik

- Konfigurace přímo v knot.conf (dříve přes keymgr)

```
policy:
    - id: ecdsa
      algorithm: ecdsap256sha256
      nsec3: on

template:
    - id: default
      dnssec-signing: on
      dnssec-policy: ecdsa

zone:
    - domain: dns.rocks
    - domain: knot-dns.cz
```

Knot DNS 2.4.0 – statistický modul (CLI)

```
$ knotc stats
server.zone-count = 10000
mod-stats.request-protocol[udp4] = 3780695
mod-stats.server-operation[query] = 3780696
mod-stats.request-bytes[query] = 183094816
mod-stats.response-bytes[reply] = 294565975
mod-stats.response-code[NOERROR] = 2268383
mod-stats.response-code[NXDOMAIN] = 739568
mod-stats.response-code[REFUSED] = 772747
mod-stats.query-type[A] = 1870719
mod-stats.query-type[NS] = 641165
mod-stats.query-type[SOA] = 635136
mod-stats.query-type[MX] = 633679
[...]
```

Knot DNS 2.4.0 – statistický modul (YAML/JSON)

- Mini https server v pythonu umí exportovat statistiky pro další použití:

```
---
time: 2016-12-02T19:01:40+0100
identity: knot-benchmark-server.labs.office.nic.cz
server:
 zone-count: 10000
mod-stats:
 request-protocol:
  udp4: 7442384
 server-operation:
  query: 7442384
 request-bytes:
  query: 360424911
 response-bytes:
  reply: 579858100
```

Nasazení Knot DNS

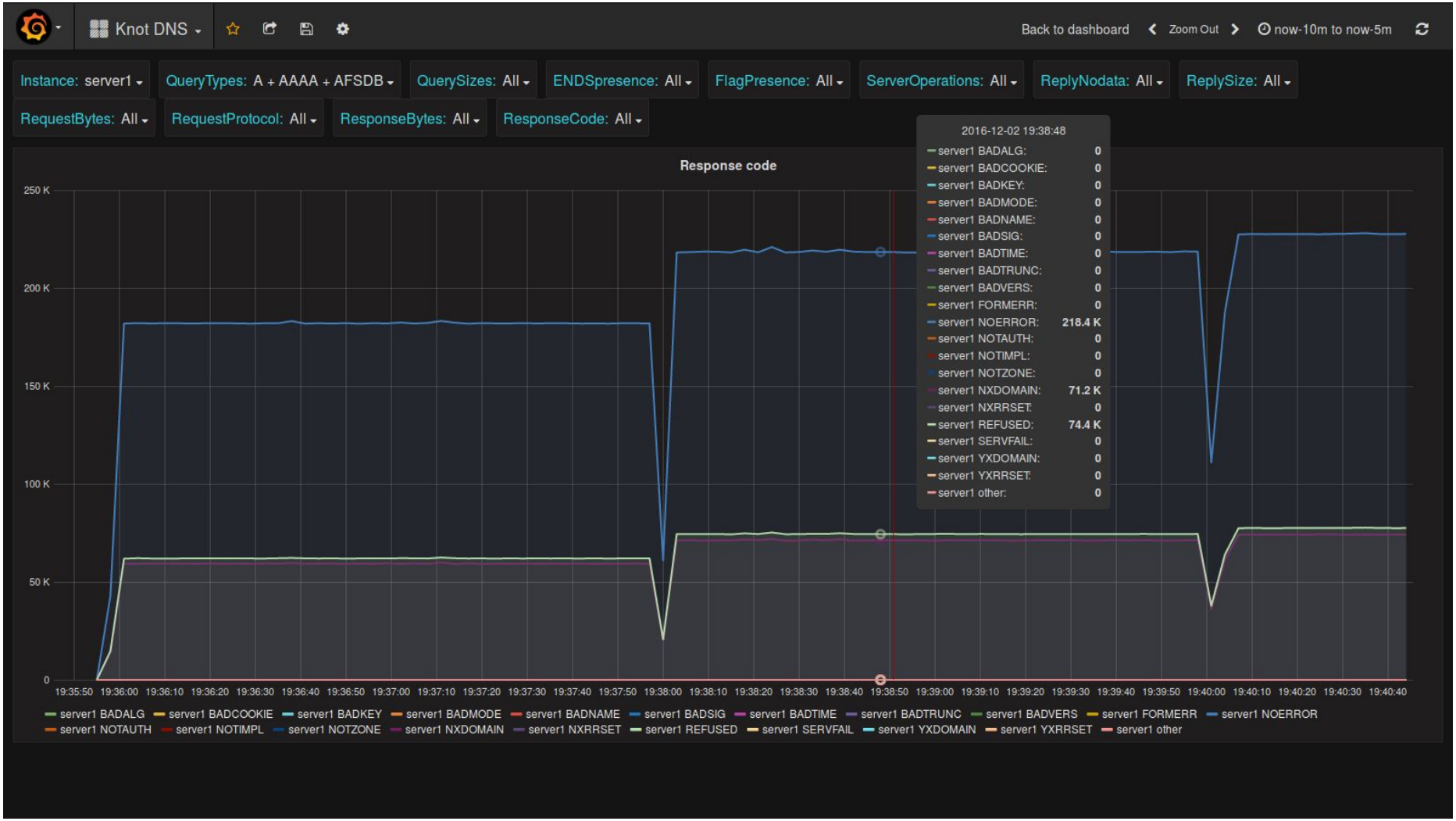
- ICANN
  - L-Root
- RIPE NCC
  - K-Root (https://www.ripe.net/analyse/dns/k-root)
  - 49 TLD
  - Mnoho zón pro reverzní delegace
- Fastly (CDN)
- TLD
  - CZ
  - DK
  - NL
  - CL

Support Contract:

- ICANN
- hostmaster.dk
- RIPE NCC
- NL
- Fastly

Knot DNS 2.4.0 – Grafana (Protokol)

Knot DNS 2.4.0 – Grafana (RCODE)



Knot Resolver

Novinky v Knot Resolver

- Knot Resolver 1.1.0 (srpen 2016)
  - **EDNS Cookies [RFC7873]**
  - **DNS over TLS [RFC7858]**
  - **HTTP/2 web interface**
    - **RESTful API**
    - **Prometheus metrics**
  - **DNS firewall module**
  - Podpora pro socket-activation
- Knot Resolver 1.1.1 (srpen 2016)
  - Drobné opravy
  - **Nasazení na Turris Omnia**
- Knot Resolver 1.2.0 (přelom 2016/2017)
  - EDNS0 Padding
  - “Jepičí” certifikáty pro DNS over TLS
  - Podpora pro +CD flag
  - Spousta vylepšení pod kapotou

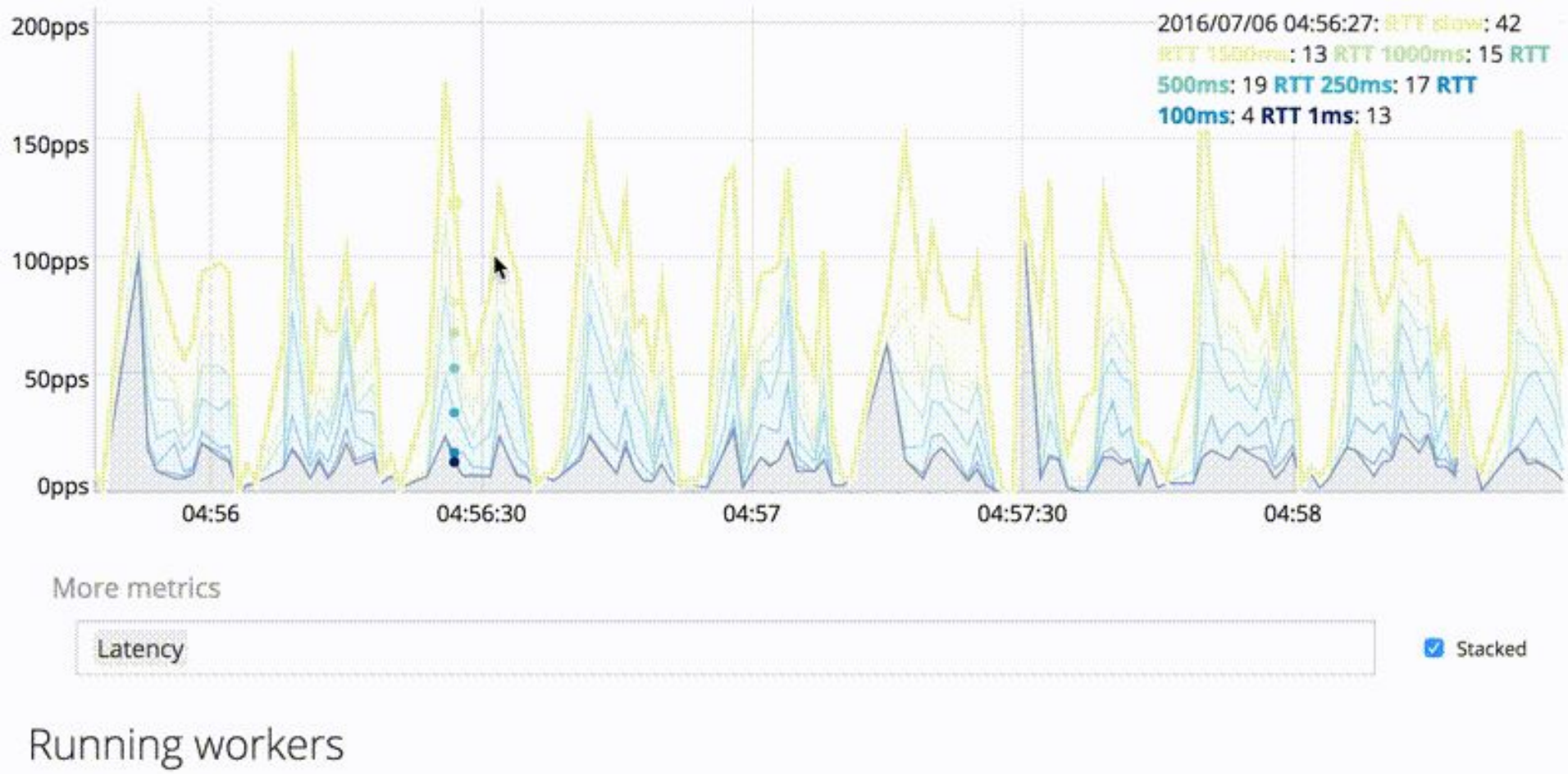
EDNS Cookies TL;DR

- Klient a server se mohou domluvit na sdílené cookie
  - Mimo dobu útoku
  - Přes TCP
- V případě útoku server odpovídá jen klientům s platnou cookie
- Ostatní přesměruje na TCP
- Velmi účinná ochrana proti DDoS útokům přes DNS

HTTP/2 rozhraní

- Interní webové rozhraní
- Napsané jako modul v Lua
- Poskytuje:
  - Jednoduché statistiky
  - Metriky pro Prometheus.io
- Rozšiřitelný dalšími moduly

HTTP/2 rozhraní – statistiky



HTTP/2 rozhraní – Geolokace serverů

DNS Firewall

- Poskytuje mocnější konfiguraci nad Policy modulem
- Pravidla:
  - IP adresy
  - QNAME
  - and/or logika
  - Další pravidla se dají dopsat v Lua
- Akce
  - PASS, DENY, DROP
  - TC
  - FORWARD
  - MIRROR
  - REROUTE
  - REWRITE
- Spolu s HTTP/2 modulem poskytuje RESTful rozhraní na správu pravidel

DNS Firewall – HTTP/2 Module

Otázky?

Ondřej Surý • ondrej.sury@nic.cz • 03. 12. 2016