Novinky z vývoje Knot DNS

Daniel Salzman • 22. 11. 2022

CZ.NIC | SPRÁVCE DOMÉNY CZ

O projektu

- Autoritativní DNS server
- Důraz na výkon
  - Odpovídání DNS dotazů
  - Zpracování zón (DNSSEC)
- Pokročilé funkce
- www.knot-dns.cz

Dokončení DNS-over-TCP v režimu XDP

- Z minula (Knot DNS 3.1)
  - Využití XDP a AF_XDP socketů k urychlení zpracování síťového provozu (Linux 4.18+)
  - Vlastní zjednodušená implementace TCP stacku (libknot)
  - Vyšší výkon (10^6 qps) a lepší odolnost proti útokům vyčerpání zdrojů a Slowloris
- Dokončení implementace (Knot DNS 3.2)
  - Vylepšení odolnosti proti některým dalším útokům (SYN flood)
  - Možnost použití pro zónové transfery (optimalizováno pro malé zóny)
  - DDNS není a nebude podporováno (z pohledu výkonu ani nedává smysl)
- kxdpgun nabízí několik testovacích režimů (***--tcp=<režim>***)

DNS-over-QUIC

- QUIC
  - Síťový šifrovaný transportní protokol využívající UDP (efektivnější než TCP+TLS)
- DNS-over-QUIC (DoQ)
  - RFC 9250 (květen 2022)
  - Autentizace serverů zatím není řešena (neexistuje standard)
- Prvotní implementace v Knot DNS (3.2)
  - Zatím jen odpovídání na dotazy v režimu XDP
  - Využití knihovny ngtcp2
    - Rozhraní není ještě stabilní
    - Z praktických důvodů začleněna do projektu
  - Kryptografické operace vyžadují GnuTLS 3.7.2+
  - Vyšší spotřeba CPU (10^5 qps) a paměti

Ukázky DoQ s kdig a kxdpgun

```
$ kdig @dns.adguard.com knot-dns.cz +quic
;; QUIC session (QUICv1)-(TLS1.3)-(ECDHE-X25519)-(ECDSA-SECP256R1-SHA256)-(AES-128-GCM)
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 0
;; Flags: qr rd ra ad; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 1

;; EDNS PSEUDOSECTION:
;; Version: 0; flags: ; UDP size: 4096 B; ext-rcode: NOERROR
;; PADDING: 84 B

;; QUESTION SECTION:
;; knot-dns.cz.                    IN     A

;; ANSWER SECTION:
knot-dns.cz.         175    IN     A      217.31.192.130

;; Received 144 B
;; Time 2022-11-15 14:18:43 CET
;; From 2a10:50c0::ad1:ff@853(UDP) in 49.8 ms
```

```
$ sudo kxdpgun -i querydb -Q 10000 -U 192.168.21.1
using interface enp196s0f0, XDP threads 8, QUIC, native mode
thread#03: sent 6251, received 6251
thread#02: sent 6250, received 6250
thread#05: sent 6251, received 6251
thread#04: sent 6251, received 6251
thread#01: sent 6251, received 6251
thread#00: sent 6251, received 6251
thread#07: sent 6251, received 6251
thread#06: sent 6251, received 6251
total initials:    50007 (10001 pps)
total handshakes:  4250 (850 pps) (8%)
total replies:     50007 (10001 pps) (100%)
average DNS reply size: 111 B
average Ethernet reply rate: 134706014 bps (134.71 Mbps)
responded NOERROR:   50007
duration: 5 s
```

Inkrementální správa klíčů pro DNSSEC

- Možnost dodatečného vkládání (DNSKEY, CDS, CDNSKEY) záznamů do zóny, která je podepisována s automatickou správou klíčů
- Vkládání přes zónový soubor, DDNS, XFR nebo ctl
- Užitečné při migraci podepsané zóny mezi operátory nebo při provozu více DNSSEC signerů
- Konfigurační vobla ***dnskey-management*** v sekci ***policy***

Zjednodušení konfigurace serveru

- Automatické ACL
  - Možnost implicitní autorizace požadavků na základě kontextu
  - **Odchozí transfer** je povolen pro klienty, kteří jsou uvedeni v ***notify***
  - **Příchozí notify** je povoleno pro klienty, kteří jsou uvedeni v ***master***
- Definice skupin serverů
  - Nová sekce ***remotes*** v konfiguraci
  - Nahrazení opakujících se výčtů serverů jedním identifikátorem
  - Lze použít místo identifikátoru pro ***remote*** (např. *acl.remote*, *zone.notify*)

Testování Knot DNS na 100GbE

- Cílem je plně využít výkon fyzického serveru
  - Při testech na 40GbE narážíme na kapacitu linky
- Intel E810-CQDA2
  - Ovladač **ice** – problémy se stabilitou v režimu XDP :-(
  - Zatím horší výsledky než Intel XL710 (40GbE) :-(
- Úvahy o testování karty od Mellanox/NVIDIA
- Někdo se zkušenostmi či zájmem o problematiku? :-)

Komunikace se vzdáleným serverem

- Možnost recyklace odchozího spojení (XFR, NOTIFY,...)
  - ***remote-pool-limit*** a ***remote-pool-timeout*** v sekci ***server***
- Dočasné odstavení komunikace s nedostupným serverem
  - ***remote-retry-delay*** v sekci ***server***
- Dočasné zablokování odchozích transferů
  - ***knotc zone-xfr-freeze*** / ***zone-xfr-thaw***
- Přeplánování odchozího NOTIFY při chybě
- Implementace EDNS volby EXPIRE (RFC 7314)

Některá další vylepšení

- Snížení paměťové náročnosti
  - Příchozí IXFR, podepisování DNSSEC, DDNS, aktualizace zónového katalogu
- Podpora VLAN v režimu XDP
  - ***knotd –*** zohlednění nastavení *xdp.route-check*
  - ***kxdpgun --vlan <id>***
- Zrychlení sémantických kontrol
  - Využití funkce DNSSEC validace zóny
- Podpora výstupu ve formátu JSON
  - ***kdig +json*** (RFC 8427)
  - ***keymgr --json***

Děkuji vám za pozornost!

Dotazy?

Daniel Salzman • 22. 11. 2022

CZ.NIC | SPRÁVCE DOMÉNY CZ