Novinky v projektech Knot DNS a Knot Resolver

Daniel Salzman • daniel.salzman@nic.cz • 15. 11. 2018

CZ.NIC | SPRÁVCE DOMÉNY CZ

Knot DNS 2.7

- Úklid knihoven
  - Jednodušší a efektivnější API
  - Odstranění přežitého kódu
- Zohlednění bezpečnostního auditu
  - Použití robustnějších algoritmů a struktur
- Výkonové optimalizace zpracování odpovědí
- Odstranění některých kompatibilit se starými verzemi (RRL, žurnál, ...)
  - Zjednodušení kódu a zpřehlednění chování serveru
- Lepší využití Linux capabilities
  - Server není třeba spouštět pod uživatelem root
- Podpora automatické inkrementace SOA serial

Knot DNS 2.7 – Moduly

- Nový modul Query ACL
  - Omezování dotazů dle zdrojové či cílové IP adresy pro danou zónu
- Nový modul GeoIP
  - Přizpůsobení odpovědi na základě geografické polohy či IP adresy klienta
- Nový modul DNS Cookies
  - Zaručení autentičnosti dotazu vzhledem ke zdrojové IP adrese
  - Deaktivace modulu Response Rate Limiting pro dotazy s platnou DNS Cookie
- Online podepisování DNSSEC
  - Podpora automatické rotace klíčů
  - Opraveno podepisování delegací

Knot DNS 2.7 – Paměťové optimalizace

- Výrazné snížení spotřeby paměti při odchozím IXFR
- Drobné zmenšení struktur zónových dat
- Při náročném nasazení doporučeno nepoužívat malloc z glibc
  - Díky náchylnosti na fragmentaci paměti může dojít až na OOM
  - Porovnání spotřeby fyzické paměti při 1 milionu malých zón
    - glibc: 2834 MiB ~ minimum
    - jemalloc: 2317 MiB
    - TCMalloc: 2280 MiB

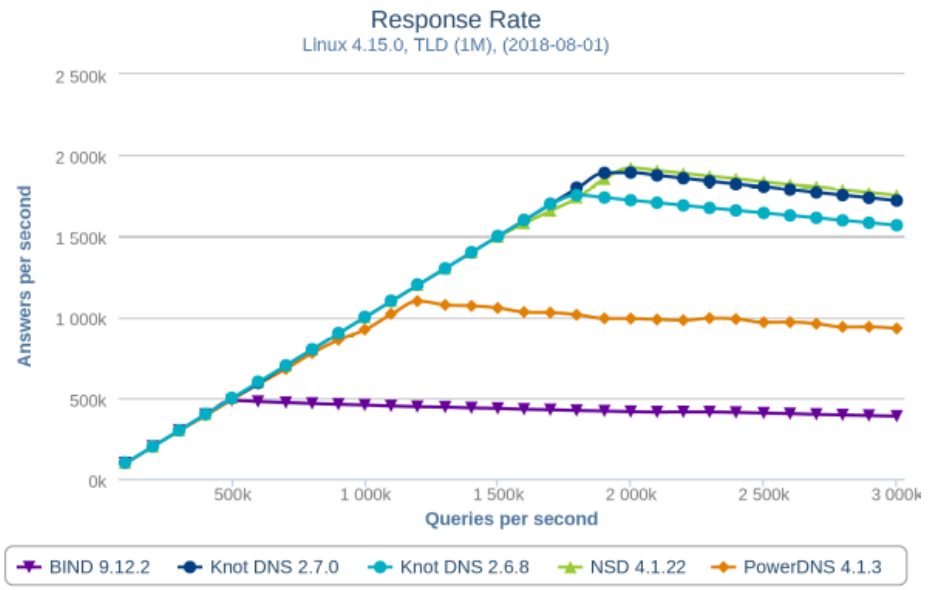
Knot DNS 2.7 – Testování

- Začlenění do projektu OSS-Fuzz (https://github.com/google/oss-fuzz)
- Kontinuální fuzz testování pro OSS
- Používané nástroje
  - AFL – American fuzzy lop (ASAN)
  - libFuzzer (ASAN, UBSAN, MSAN)
- Zvěřejnění reportů
  - Za 30 dnů po ověřené opravě
  - Nejpozději za 90 dnů

Benchmarking

- https://www.knot-dns.cz/benchmark
- Porovnávání výkonu dominantních OSS implementací autoritativních DNS serverů
- Užitečné při optimalizacích či odhalení nežádoucí regrese
- Zjednodušená a přepracovaná měřící infrastruktura
- Zpřesněné a rozšířené testovací datasety (NSEC3, IPv6, ...)

Benchmarking – Ukázky



Knot DNS – Verzování projektu

- Knot DNS X.X.X
  - Verze – určuje velké změny, úpravy API, změny konfigurace
  - Revize – určuje drobná vylepšení a opravy
- Každá verze má svoji větev v repozitáři
  - Průběžná kumulace oprav a vylepšení
  - Zpravidla v řádu měsíců se vydává revize
- Současně dvě udržované verze
  - current stable (2.7)
  - previous stable (2.6)

Knot DNS – Balíčkování

- Repozitáře CZ.NIC
  - Debian (i386, amd64), Ubuntu (Launchpad)
  - current stable, previous stable
- Open Build System
  - Debian, Ubuntu, CentOS, Fedora, OpenSUSE, Arch
  - amd64, arm64, armv7l
  - current stable
- Distribuční repozitáře
  - Dostupnost na většině distribucí Linuxu (včetně OpenWRT), *BSD a macOS
  - Spolupráce nebo přímá účast na balíčkování

KNOT RESOLVER

CZ.NIC | SPRÁVCE DOMÉNY CZ

Knot Resolver 2.2 – 2.4

- Podpora agresivního kešování pro zóny s NSEC3
  - Snížení latence odpovídání
  - Menší vytěžování autoritativních serverů
- Modul pro automatické přednaplnění kořenové zóny do keše
  - Snížení latence odpovídání a redukce komunikace s kořenovými servery
  - Zvýšení odolnosti provozu při nedostupnosti kořenových serverů
- Zlepšení výkonu DNS-over-TLS
- Modul na ochranu proti útokům DNS Rebinding
- Vylepšení odolnosti proti útokům Slowloris

Knot Resolver 3.0 – 3.1

- Přechod na knihovnu libknot 2.7
  - Zjednodušení kódu
  - Využití výkonových optimalizací
  - Implementace rotace záznamů v odpovědi
- Vylepšení výkonu a stability (včetně TLS)
- Rozšířené možnosti čištění keše
- Odstranění modulů DNS Cookies a Version


DNS
FLAG
DAY

DNS flag day

- Iniciativa vývojářů a veřejných provozovatelů rekurzivních DNS serverů
- Cíle projektu
  - Ukončení podpory rozbitých implementací DNS
  - Usnadnění dalšího rozvoje DNS
- Důsledek
  - Některé domény mohou být časem nedostupné
- Technické podrobnosti a testovací nástroje
  - https://dnsflagday.net
- Zahájení 1. února 2019

Děkuji za pozornost

Daniel Salzman • daniel.salzman@nic.cz