„Knot, Knot“
„Who’s there?“
„Resolver“
„Resolver who?“

Oto Šťáva • 23.01.2024

Knot Resolver 6

CSNOG 2024

Oto Šťáva • 23.01.2024

CZ.NIC | SPRÁVCE DOMÉNY CZ

Knot Resolver

- Open-source DNS resolver
- Modulární a flexibilní
  - Rychlé tenké jádro
  - Moduly v Lua a C
  - Lua konfigurace
  - Oddělené jednovláknové procesy
- www.knot-resolver.cz

Kde byl problém?

- Programy a procesy
  - Knot Resolver daemon (kresd)
    - Jádro Knot Resolveru – stará se o samotný resolving, přijímá DNS dotazy, poskytuje odpovědi
    - Jednovláknový
      - Pro škálování na více jader oddělené procesy – balancing řeší kernel
      - Obtížná agregace statistik a metrik
      - Systemd pro správu – není dostupné všude (docker, Turris, ...)
  - Cache garbage collector (cache-gc)
    - Oddělený proces, který pročišťuje cache, když se naplní
    - Ve výchozím nastavení spouštěn pomocí systemd

Kde byl problém?

- Modularita
  - Nepovinné pokročilé funkcionality nejsou zátěž
  - Před použitím je nutné moduly explicitně načíst v Lua
  - Neintuitivní pro vestavěné moduly
- Lua konfigurace
  - Mocná: plnohodnotný skriptovací jazyk
  - Pro potřeby většiny uživatelů těžko uchopitelná
  - Skryté chyby projevující se za běhu – chybí validace

Kde byl problém?

- Policy modul
  - Modifikuje odpovědi na základě definovaných pravidel
  - Umožňuje např. blokování škodlivých domén
  - Složitějších pravidel je obtížné dosáhnout bez znalosti vnitřního fungování
    - Aplikují se (a překrývají) v deklarovaném pořadí
    - Chybí „chytřejší“ systém pro určení, které pravidlo se kdy aplikuje

Jak to řeší verze 6?

- Manager
  - Správce procesů kresd a cache-gc
  - Sběrač statistik a metrik
- Deklarativní konfigurace v YAML
  - Komplexní validace
  - Uchopitelnější pro neprogramátory
  - Přehlednější
- Nový přístup ke psaní policy pravidel

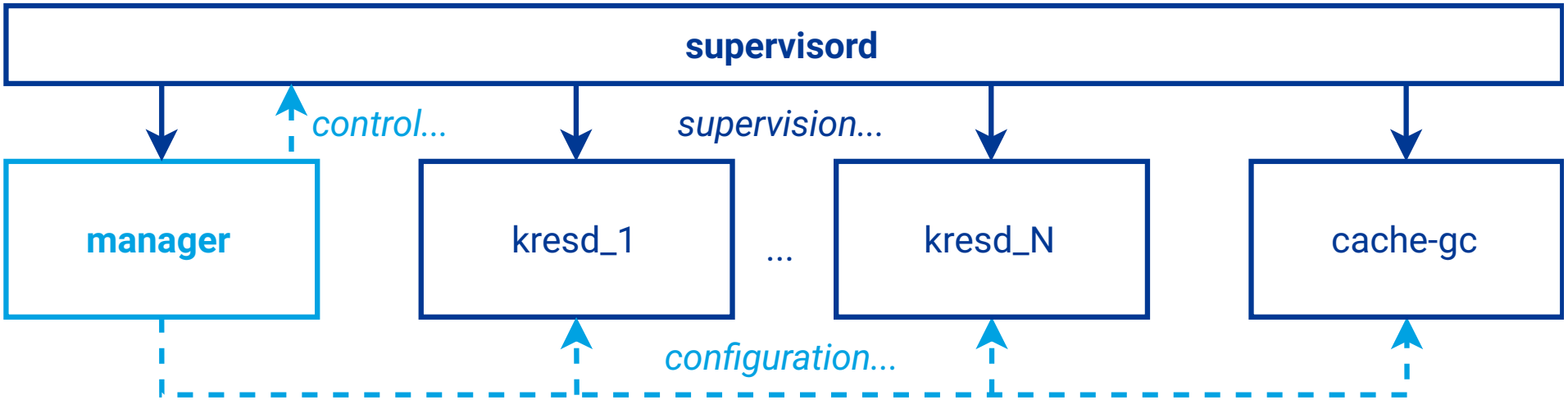
Testování verze 6

knot-resolver.cz/documentation/latest

Manager

- Podle potřeby spravuje procesy
  - Sjednocení přístupu na všech systémech – zejména na těch bez systemd
  - Automatická zero-downtime rekonfigurace procesů
- HTTP API pro on-demand změny konfigurace
- Agregace statistik a metrik

Manager



Deklarativní konfigurace

- Ve formátu YAML
- Podoba definovaná pomocí JSON Schema

YAML

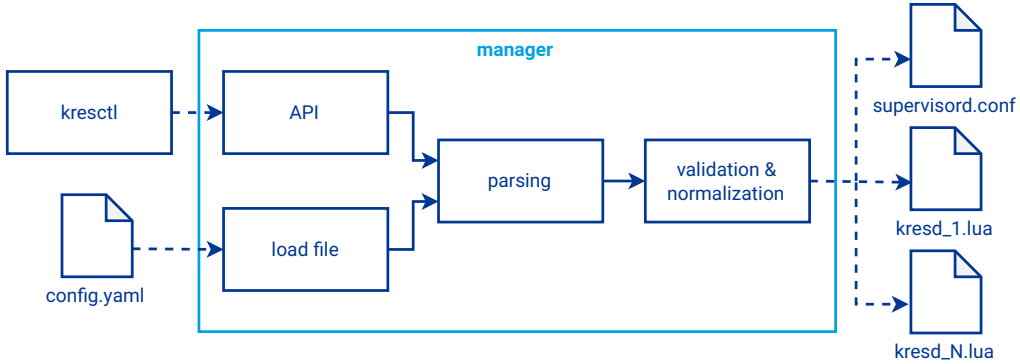
```yaml
network:
  listen:
    # Unencrypted DNS (port 53)
    - interface: &interfaces
        - 127.0.0.1
        - ::1
    # DNS-over-TLS (port 853)
    - interface: *interfaces
      kind: dot
    # DNS-over-HTTPS (port 443)
    - interface: *interfaces
      kind: doh2
```

Lua

```lua
-- Unencrypted DNS (port 53)
net.listen('127.0.0.1',  53, { kind = 'dns' })
net.listen('::1',        53, { kind = 'dns' })
-- DNS-over-TLS (port 853)
net.listen('127.0.0.1', 853, { kind = 'tls' })
net.listen('::1',       853, { kind = 'tls' })
-- DNS-over-HTTPS (port 443)
net.listen('127.0.0.1', 443, { kind = 'doh2' })
net.listen('::1',       443, { kind = 'doh2' })
```

Deklarativní konfigurace

- Spravovaná managerem
- Komplexně validovaná
- Automatické načítání potřebných modulů
- Lua je nyní interní
  - Stále se generuje na pozadí
  - Lze vložit do YAML či importovat ze souboru
  - Pracujeme na rozdělení dokumentace pro lepší přehlednost a vyhledávání na část uživatelskou a vývojářskou



Policies, access control

- Views
  - Rozhodnutí podle původce dotazu
    - Nejblíže odpovídající pravidlo vyhrává (podle podsítě – pořadí pravidel v YAMLu nerozhoduje)
  - Může odmítnout, upravit chování, přiřadit tagy
- Local data
  - Syntéza a úprava záznamů pro dotazované domény
  - Pravidla na základě tagů
  - Podpora RPZ
- Forwarding
  - Přeposlání dotazu na jiný server
  - Nově podporuje i autoritativní servery (funkční CNAME záznamy)

Policies, access control

```
views:
  - subnets: [ 0.0.0.0/0, "::/0" ]
    answer: refused
  - subnets: [ 10.0.10.0/24, 127.0.0.0/24, "::1" ]
    answer: allow
```

```
local-data:
  addresses:
    a1.example.com: 2001:db8::1
  addresses-files:
    - /etc/hosts
```

```
local-data:
  records: |
    www.google.com CNAME forcesafesearch.google.com
  rpz:
    - file: /tmp/malware.rpz
      tags: [ malware ]
```

```
forward:
  subtree: internal.example.com
  servers: [ 10.0.0.53 ]
  options:
    authoritative: true
    dnssec: false
```

Co teď?

- Získávání zpětné vazby z testování
- Doladění chyb, dokumentace a konfiguračního modelu
- Nasazení pro testovací provoz na ODVR (nic.cz/odvr)
- Vydání Knot Resolver 6.1.0 – **Q1 2024**

Shrnutí

- Knot Resolver Manager
- Deklarativní konfigurace namísto Lua
  - Lua stále dostupná pro pokročilé uživatele
  - Pracujeme na oddělené dokumentaci
- Přepracované policies
- Testujeme: knot-resolver.cz/documentation/latest
- Ostré vydání **Q1 2024**

Pár slov na konec

- Detailnější rozbor v článku Aleše Mrázka na Root.cz:
  - tinyurl.com/Kres6Root (root.cz/clanky/novinky-v-knot-resolveru-6-x-spravce-procesu-a-prehlednejsi-konfigurace)
- Dlouhodobě hledáme posily do našeho týmu:
  - nic.cz/kariera/#DNS_prog
- Děkujeme za dosavadní zpětnou vazbu k verzi 6

Knot Resolver tým: Vladimír Čunát, Aleš Mrázek, Lukáš Ondráček, Oto Šťáva

Děkuji Vám za pozornost!

Oto Šťáva • 23.01.2024

CZ.NIC | SPRÁVCE DOMÉNY CZ