Novinky v Knot Resolver 6.x

LinuxDays 2023 / IT23

Aleš Mrázek • 07.10.2023

CZ.NIC | SPRÁVCE DOMÉNY CZ

O projektu

- Open-source DNS resolver
- Modularita a flexibilita
  - Jednovláknové procesy
  - Moduly (Lua, C)
  - Lua konfigurace
- www.knot-resolver.cz

Kde je problém?

- Management jednotlivých procesů
  - Využití vícejádrových procesorů
  - Statistiky a metriky
- Jednotlivé moduly je před použitím potřeba nejdříve explicitně načíst
- Lua konfigurace
  - Je jednoduché udělat chybu a může být obtížné chybu najít

Vylepšení ve verzi 6.x

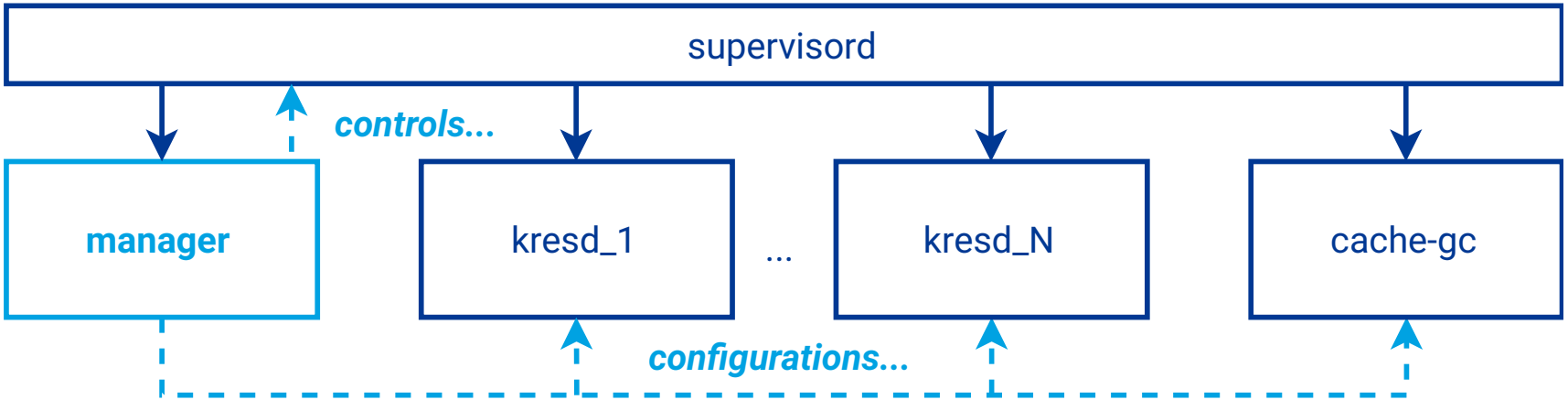
- knot-resolver-manager
  - Nový nástroj, který spravuje procesy resolveru (kresd, cache-gc)
- Deklarativní formát konfigurace
  - Validace
  - Čitelnost
- Nový přístup k psaní policy pravidel

Testování verze 6.x

https://knot.pages.nic.cz/knot-resolver/

knot-resolver-manager

- Spravuje jednotlivé procesy podle potřeby
  - supervisord (docker, Turris OS, ...)
  - Spouštění a vypínání procesů
  - Konfigurace a rekonfigurace procesů
- Management HTTP API
- Agregace statistik/metrik


supervisord
controls...
manager
kresd_1
...
kresd_N
cache-gc
configurations...

Deklarativní konfigurace

- YAML, JSON, JSON schema
- Komplexní validace před použitím
- Čitelnější a intuitivnější než Lua
- Konverze na Lua konfiguraci (Jinja2 templaty)

```
Configuration validation errors detected:
  [/network/listen[0]/port] value 65536 is higher than the maximum 65535
  [/logging/level] 'degugg' does not match any of the expected values ('crit', ..., 'debug')
```

kresctl utilita

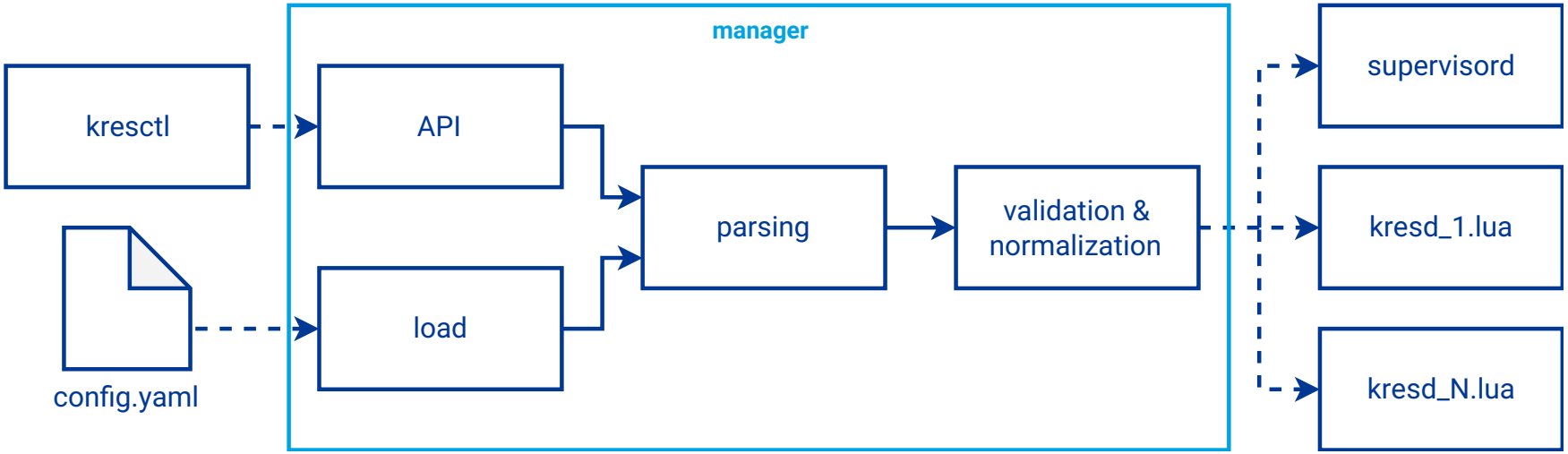
- Práce s konfigurací
  - validate, convert
- Komunikace s HTTP API
  - config: get, set, delete
  - metrics, schema, reload, stop

```
$ kresctl validate /etc/knot-resolver/config.yaml
```

```
$ kresctl convert /etc/knot-resolver/config.yaml
```

```
$ kresctl config get --yaml
$ kresctl config set -p /workers 8
```

```
$ kresctl metrics
```


manager
kresctl
API
parsing
validation &
normalization
supervisord
kresd_1.lua
kresd_N.lua
load
config.yaml

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

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

views: Kdo poslal dotaz?

- Nejlépe odpovídající pravidlo vyhraje (nezávisle na pořadí)
- Rozhodne o odmítnutí, přiřazení tagů, …
- Tagy dále slouží jako filtr pro jiná pravidla ovlivňující záznamy v odpovědích

```
views:
  - subnets: [ 0.0.0.0/0, "::/0" ]
    answer: refused
  - subnets: [ 10.0.10.0/24, 127.0.0.1, "::1" ]
    answer: allow
  - subnets: [ 192.168.1.0/24 ]
    tags: [ malware, localnames ]
```

local-data: Úpravy v DNS záznamech

- Deklarativní přístup: změny v DNS stromu
  - Starý přístup policy: přišel dotaz, jakou na něj dát odpověď?
- Kombinace různých pravidel se častěji chovají tak jak lidé čekají
  - CNAME, pravidla pro vzájemně vnořené podstromy - včetně forwardování, blokování PTR

```
local-data:
  Addresses:
    a1.example.com: 2001:db8::1
    a2.example.org:
      - 192.0.2.2
      - 192.0.2.3
      - 2001:db8::4
  Addresses-files:
    - /etc/hosts
```

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

forward: Koho se ptát dál?

- Deklarativní přístup umožnil pokrytí dalších častých použití
- Přeposlání na více míst i rámci jediného dotazu
- Cílem může nově být i autoritativní server (již nerozbije CNAME)

```
forward:
  - subtree: '.'
    servers:
    - address:
        - 2001:148f:fffe::1
        - 193.17.47.1
    transport: tls
    hostname: odvr.nic.cz
```

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

```yaml
views:
  - subnets: [ 0.0.0.0/0, "::/0" ]
    answer: refused
  - subnets: [ 10.0.10.0/24, 127.0.0.1, "::1" ]
    answer: allow
  - subnets: [ 192.168.1.0/24 ]
    tags: [ malware ]
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
```

```
-- Je potřeba být velmi opatrný s pořadím pravidel,
-- jinak se vzájemně zastíní "nechtěným způsobem".
view:addr('192.168.1.0/24',
    policy.rpz(policy.DENY, '/tmp/malware.rpz'))

view:addr('10.0.10.0/24', policy.all(policy.PASS))
view:addr('127.0.0.1,',   policy.all(policy.PASS))
view:addr('::1',          policy.all(policy.PASS))

view:addr('0.0.0.0/0',    policy.all(policy.REFUSE))
view:addr('::/0',         policy.all(policy.REFUSE))

-- www.google.com: nejde, CNAME nefungují v lua
policy modulu.

-- Knot Resolver předpokládá, že cílem je resolver
-- a tedy třeba CNAME se budou rozbíjet.
policy.add(policy.suffix(
    policy.STUB('10.0.0.53'),
    {todname('internal.example.com')}))
```

Shrnutí novinek

- Knot-resolver-manager
  - Odpadá management jednotlivých procesů (kresd, cache-gc)
- Deklarativní konfigurace
  - Komplexní validace
- Management HTTP API
- kresctl utilita

Co dále?

- Stabilizace a drobná zlepšení modelu konfigurace
- Zpětná vazba od uživatelů
- Nasazení na ODVR
- Knot Resolver 6.1.0

Děkuji Vám za pozornost!

Aleš Mrázek • 07.10.2023

CZ.NIC | SPRÁVCE DOMÉNY CZ