Novinky v Knot Resolveru

Vladimír Čunát • vladimir.cunat@nic.cz • 10. 11. 2021

CZ.NIC | SPRÁVCE DOMÉNY CZ

Přehled

Poslední rok: verze 5.2.0 – 5.4.2

- Asserty / stabilita
- Logování
- DNS Shotgun
- Stabilizace DoH implementace
- Výběr name-serverů
- Konfigurace v budoucnu

Asserty / stabilita

- Testujeme, ale nejde být 100% bez chyb (nepředvídatelnost internetu, konfigurace, …)
- Dilema – co s interní nekonzistencí (assert):
  - Spadnout: coredump pomáhá opravit chyby
  - Zotavit se: minimalizace narušení DNS služby
- Oboje!
  Fork procesu: potomek spadne, původní proces se zotaví

Logování – metadata

- Dříve čistý text – stdout+stderr, teď syslog+systemd API
- Úroveň
  - = závažnost každé zprávy
  - crit, err, warning, notice, info, debug
  - Například: `journalctl -p err`
- Systemd: navíc přesná pozice ve zdrojových souborech

Logování – skupiny

- Nejde generovat maximum logů *vždy*
- Předchozí rok: `debug` logy pouze pro některé dotazy
- Letos: skupiny
  - Každá zpráva v logu má skupinu
    například `[cache ]` – také každý modul má svou
  - Zapínání `debug` úrovně pro každou skupinu zvlášť
  - Odkaz: dokumentace logování

DNS Shotgun (1/2)

- Vedlejší projekt:

  Generování *realistického* provozu pro DNS resolvery
- Letos:

  V dobře použitelném a zdokumentovaném stavu
- Test co se stane s mými DNS resolvery když:
  - Vzroste počet klientů
  - Část přejde na DNS-over-TLS nebo DNS-over-HTTPS

DNS Shotgun (2/2)

- Vstup:

  Zachycený DNS provoz

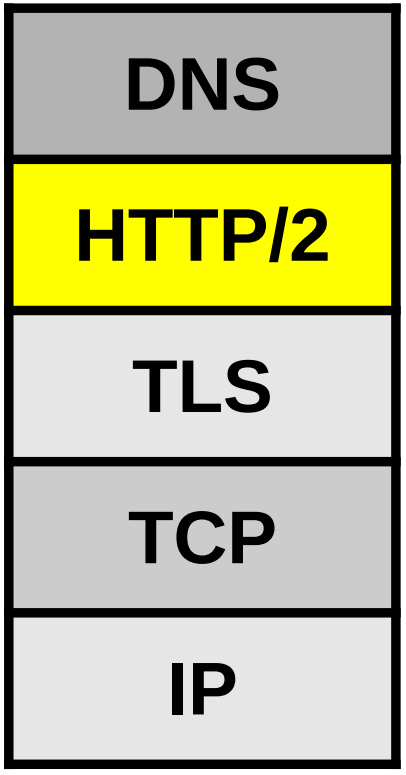
- Cíl:

  Simulace stejně se chovajících klientů

- Lze konfigurovat:
  - Výběr podílu DNS protokolů: UDP, TCP, TLS, HTTP/2
  - Jak rychle klienti zavírají svá otevřená spojení, ...
  - Více klientů / zrychlení (realisticky vůči chování cache)

Stabilizace DoH implementace

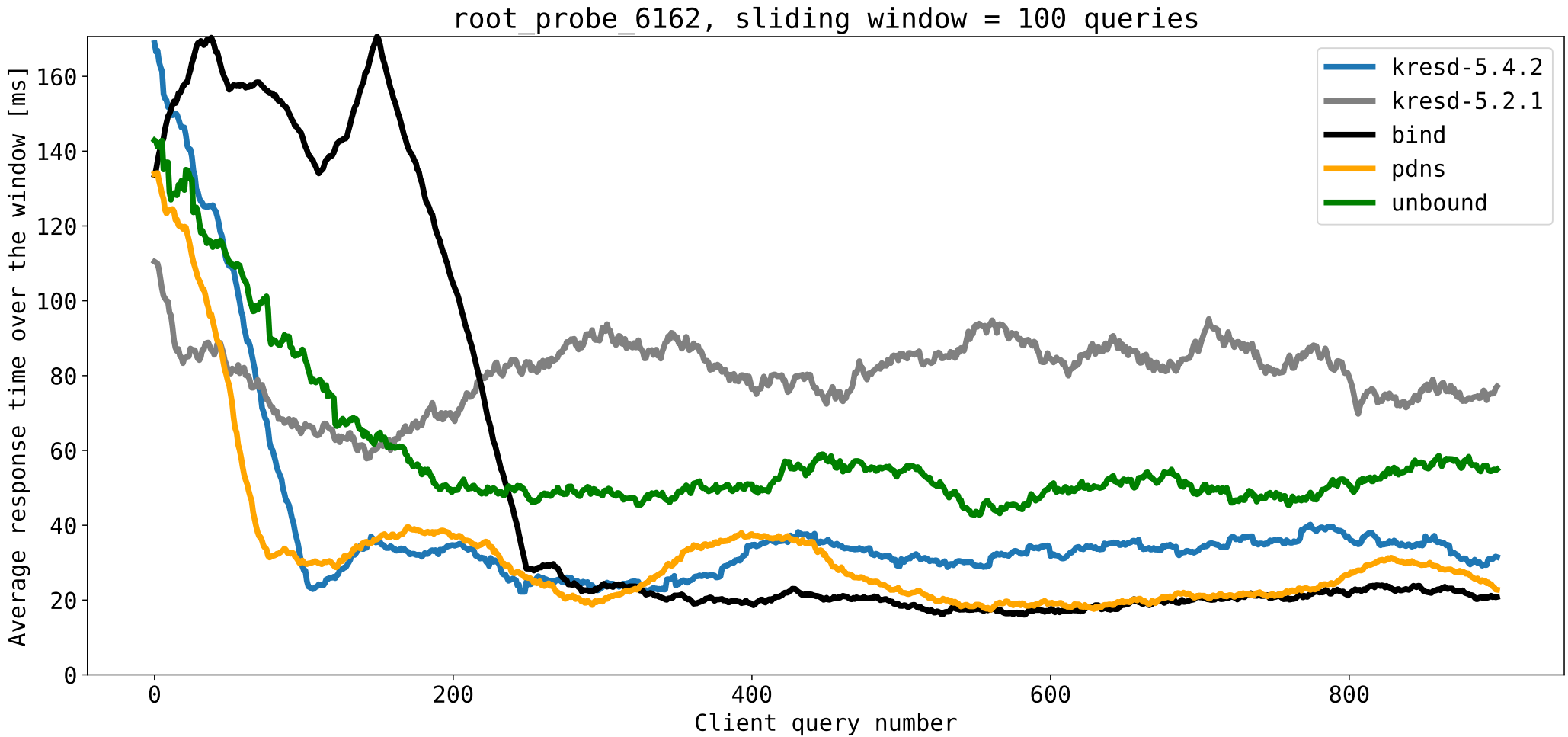
- Loni: nová implementace DNS-over-HTTPS
  - v C (libnghttp2), místo prototypu v Lua
- Letos: doladění, na reálném provozu
  - Otevřené resolvery cz.nic (ODVR)
  - HTTP/2 je složité, variabilita v chování klientů
- Migrujte!
  - Stará implementace DoH není vhodná do produkce
- Stále raději DoT než DoH, pokud si můžete vybrat



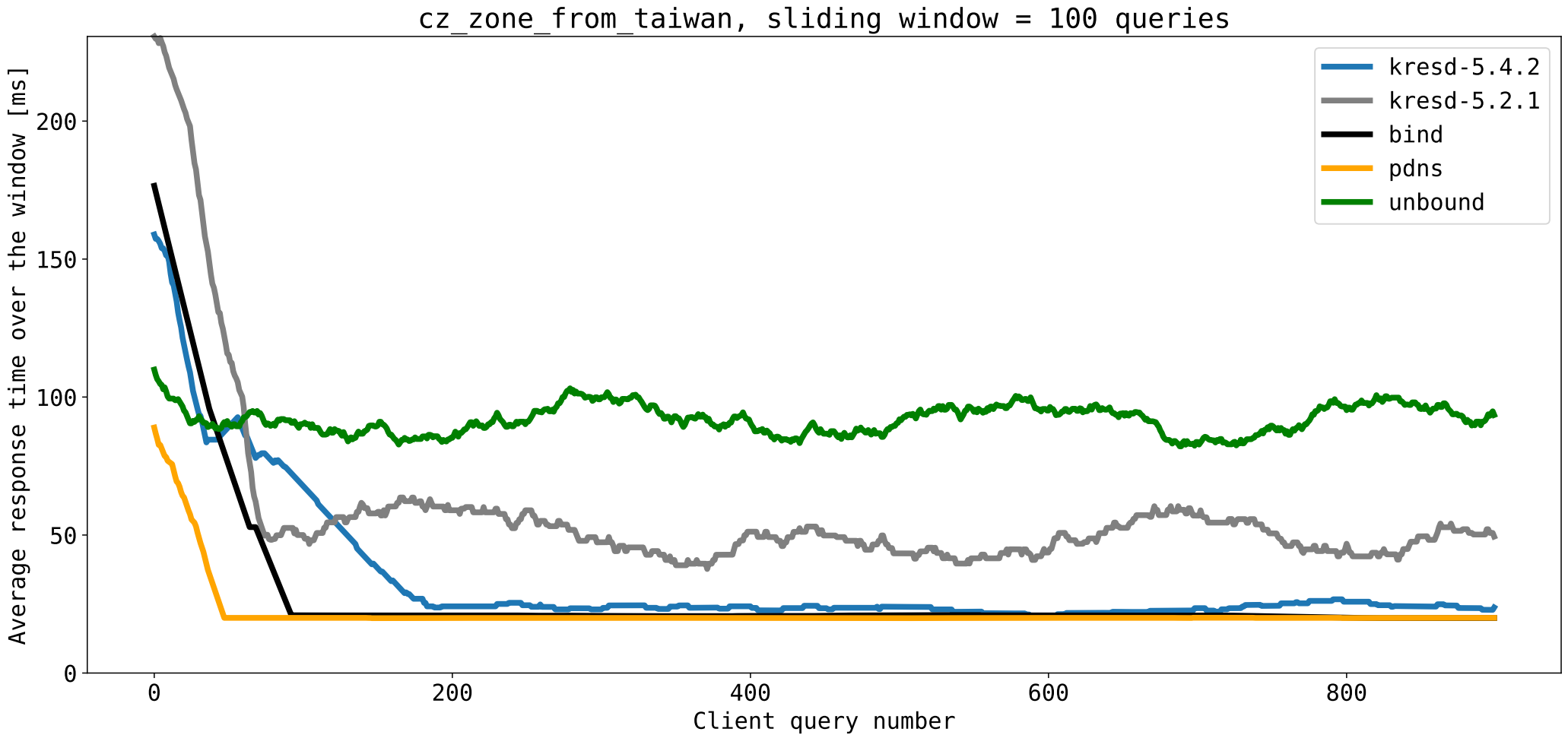
Výběr name-serverů

- O co jde:
  - Více možností při dotazování autoritativních serverů
  - Které IP adresy se dotázat
  - Nebo zjišťovat další IP adresy?
- Proč to bylo špatné?
  - Magický kód – obtížné porozumění, změny, …
  - Nevhodné chování v méně obvyklých situacích
- Přepsání implementace, praktické důsledky:
  - Lepší latence kresd, při cache miss
  - Méně plýtvání packety

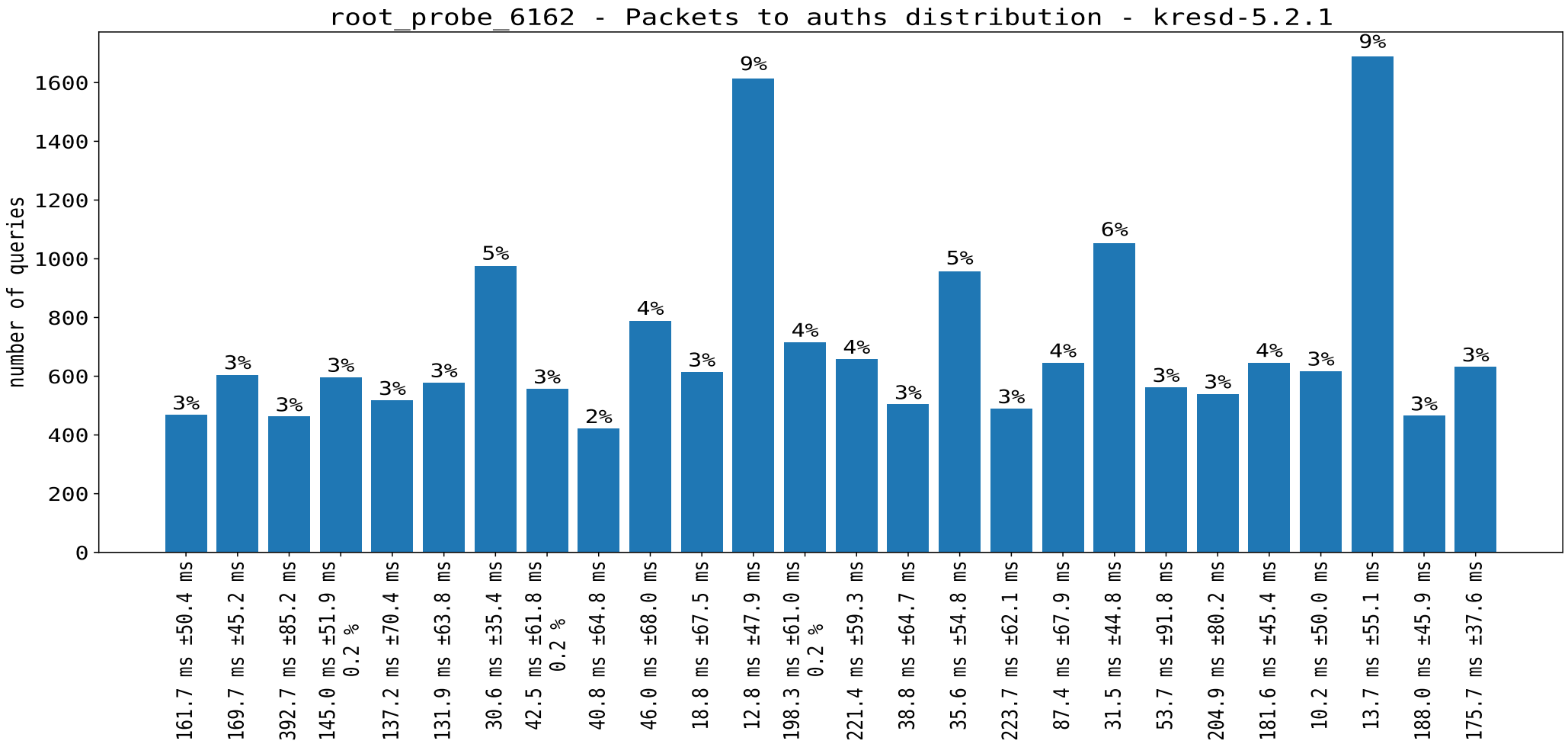
Výběr NS: root servery, Nová Kaledonie



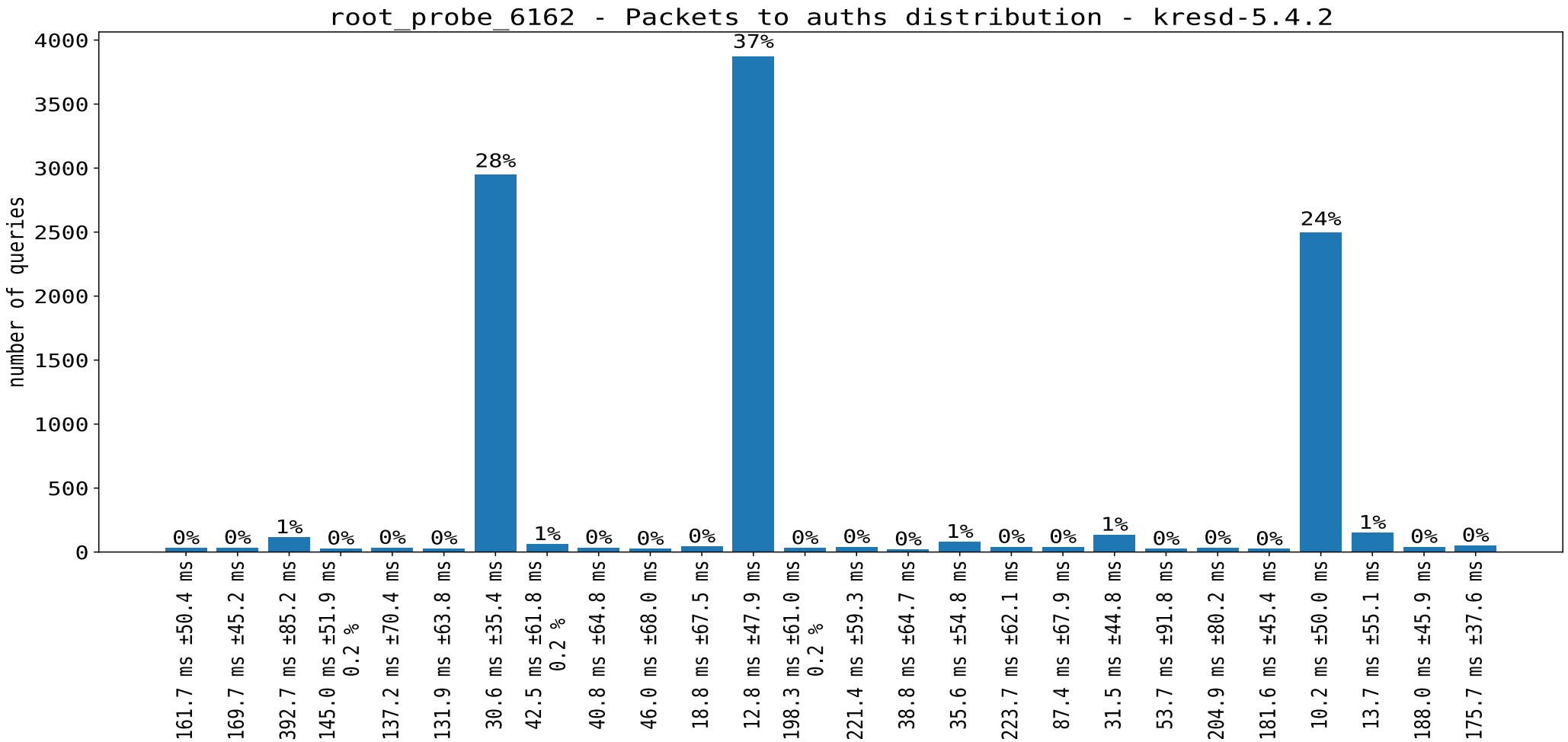
Výběr NS: .cz servery, Taiwan



Výběr NS: root, Nová Kaledonie, starý kresd



Výběr NS: root, Nová Kaledonie, nový kresd



Konfigurace v budoucnu

- Teď: lua skript
  - Vysoká míra flexibility
  - Mnoho příležitostí se spálit: slabá syntaxe, …
  - Obtížné zpracování nástroji
- Plán: 99% konfigurace v YAML / JSON
  - Silná kontrola dle schématu – místo *spuštění* lua skriptu
- Před rokem průzkum: Jak nastavujete DNS resolvery?

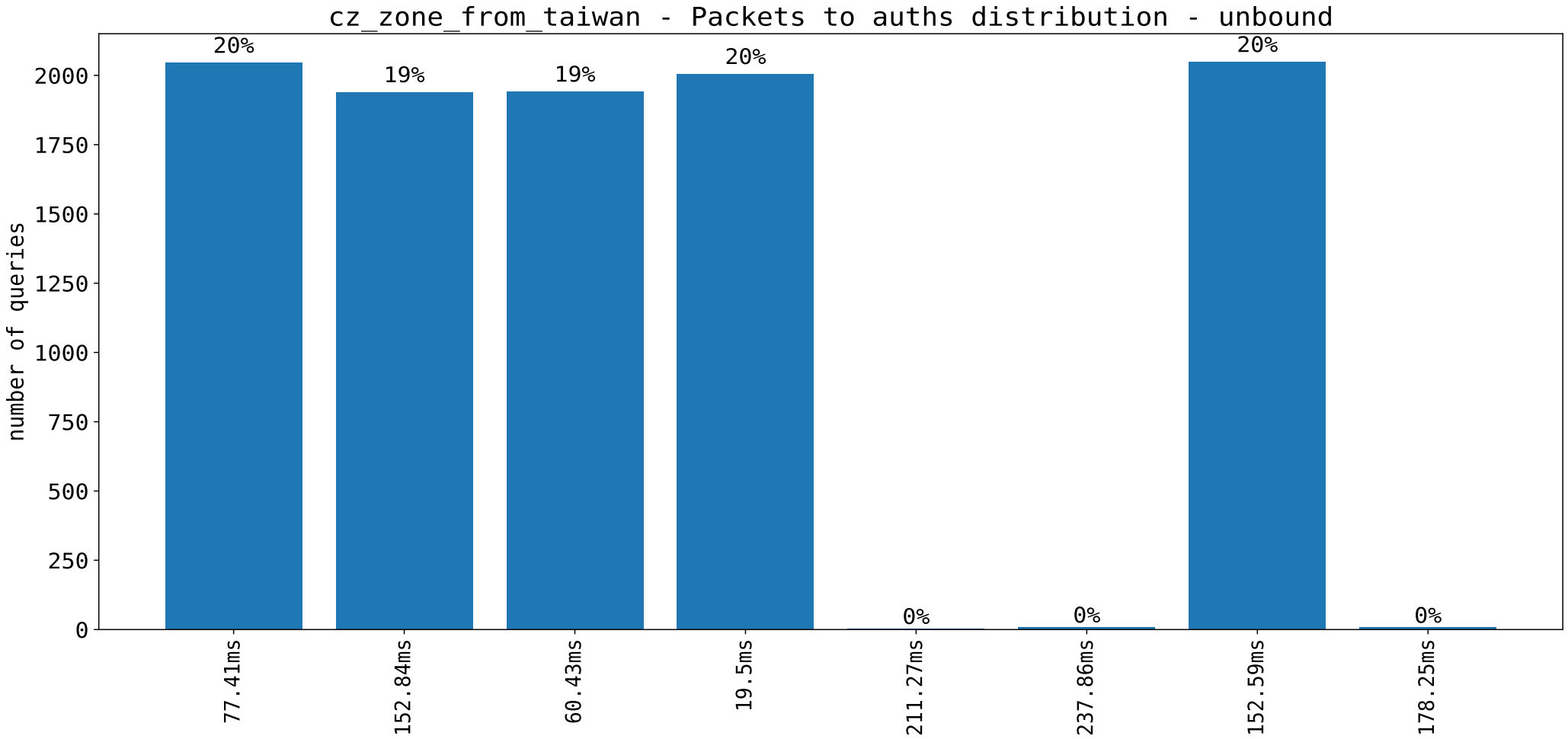
Přehled

Poslední rok: verze 5.2.0 – 5.4.2

- Asserty / stabilita
- Logování
- DNS Shotgun
- Stabilizace DoH implementace
- Výběr name-serverů
- Konfigurace v budoucnu

CZ.NIC | SPRÁVCE DOMÉNY CZ

Výběr NS: .cz servery, Taiwan, unbound 1.13.2



Novinky v Knot Resolveru

Vladimír Čunát • vladimir.cunat@nic.cz • 10. 11. 2021

CZ.NIC | SPRÁVCE DOMÉNY CZ

Přehled

Poslední rok: verze 5.2.0 – 5.4.2

- Asserty / stabilita
- Logování
- DNS Shotgun
- Stabilizace DoH implementace
- Výběr name-serverů
- Konfigurace v budoucnu

KNOT RESOLVER

CZ.NIC | SPRÁVCE DOMÉNY CZ

Asserty / stabilita

- Testujeme, ale nejde být 100% bez chyb (nepředvídatelnost internetu, konfigurace, …)
- Dilema – co s interní nekonzistencí (assert):
  - Spadnout: coredump pomáhá opravit chyby
  - Zotavit se: minimalizace narušení DNS služby
- Oboje!
  Fork procesu: potomek spadne, původní proces se zotaví

Logování – metadata

- Dříve čistý text – stdout+stderr, teď syslog+systemd API
- Úroveň
  - = závažnost každé zprávy
  - crit, err, warning, notice, info, debug
  - Například: `journalctl -p err`
- Systemd: navíc přesná pozice ve zdrojových souborech

Logování – skupiny

- Nejde generovat maximum logů *vždy*
- Předchozí rok: `debug` logy pouze pro některé dotazy
- Letos: skupiny
  - Každá zpráva v logu má skupinu
    například `[cache ]` – také každý modul má svou
  - Zapínání `debug` úrovně pro každou skupinu zvlášť
  - Odkaz: dokumentace logování

DNS Shotgun (1/2)

- Vedlejší projekt:

  Generování *realistického* provozu pro DNS resolvery
- Letos:

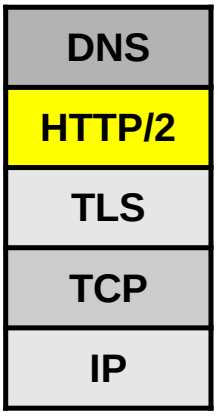
  V dobře použitelném a zdokumentovaném stavu
- Test co se stane s mými DNS resolvery když:
  - Vzroste počet klientů
  - Část přejde na DNS-over-TLS nebo DNS-over-HTTPS

DNS Shotgun (2/2)

- Vstup:
  - Zachycený DNS provoz
- Cíl:
  - Simulace stejně se chovajících klientů
- Lze konfigurovat:
  - Výběr podílu DNS protokolů: UDP, TCP, TLS, HTTP/2
  - Jak rychle klienti zavírají svá otevřená spojení, ...
  - Více klientů / zrychlení (realisticky vůči chování cache)

Stabilizace DoH implementace

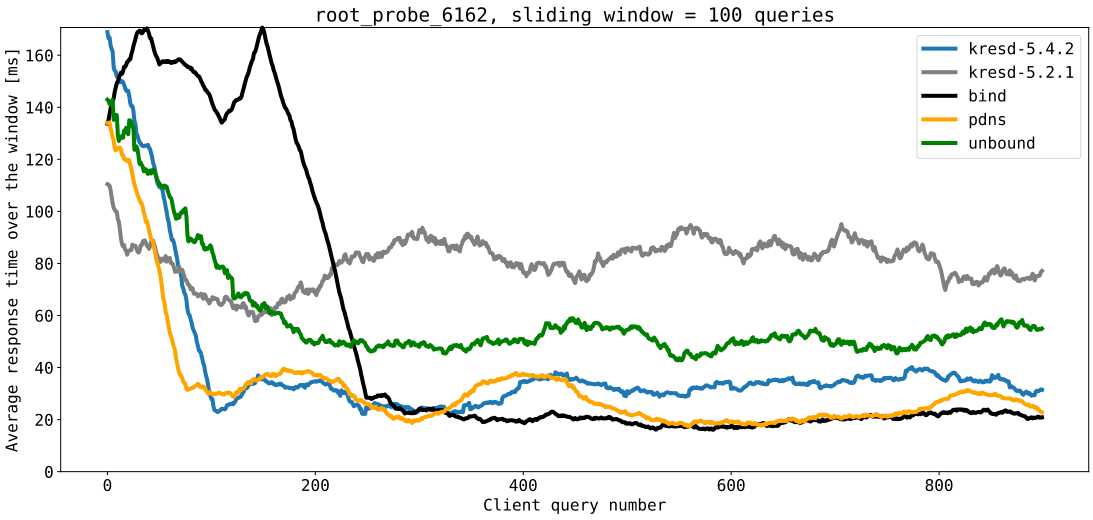
- Loni: nová implementace DNS-over-HTTPS
  - v C (libnghttp2), místo prototypu v Lua
- Letos: doladění, na reálném provozu
  - Otevřené resolvery cz.nic (ODVR)
  - HTTP/2 je složité, variabilita v chování klientů
- Migrujte!
  - Stará implementace DoH není vhodná do produkce
- Stále raději DoT než DoH, pokud si můžete vybrat



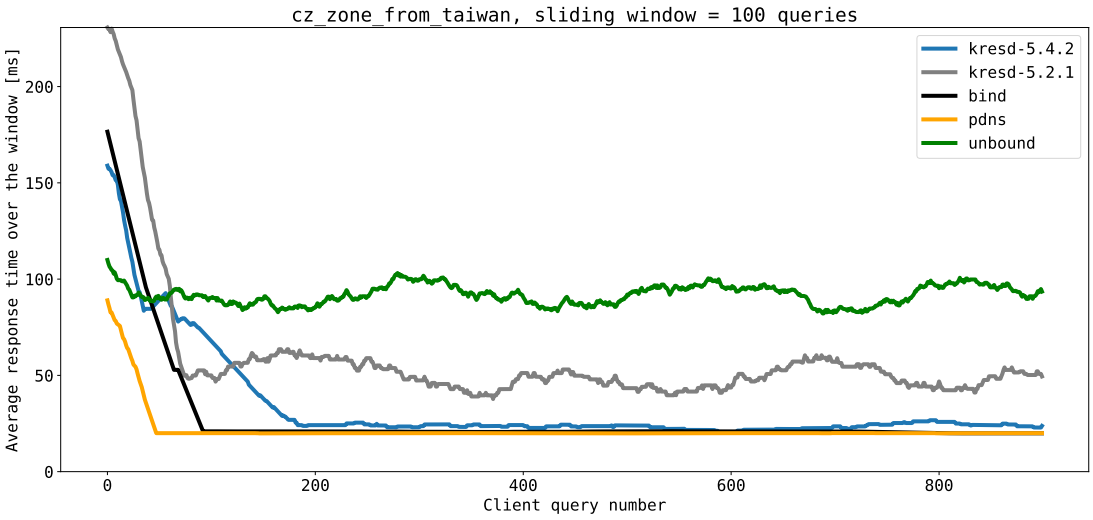
Výběr name-serverů

- O co jde:
  - Více možností při dotazování autoritativních serverů
  - Které IP adresy se dotázat
  - Nebo zjišťovat další IP adresy?
- Proč to bylo špatné?
  - Magický kód – obtížné porozumění, změny, …
  - Nevhodné chování v méně obvyklých situacích
- Přepsání implementace, praktické důsledky:
  - Lepší latence kresd, při cache miss
  - Méně plýtvání packety

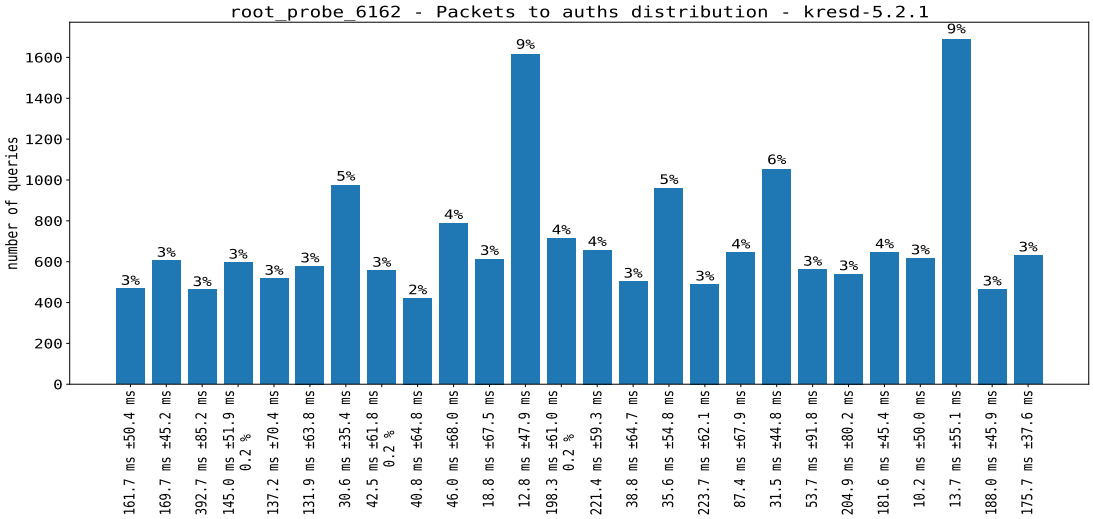
Výběr NS: root servery, Nová Kaledonie



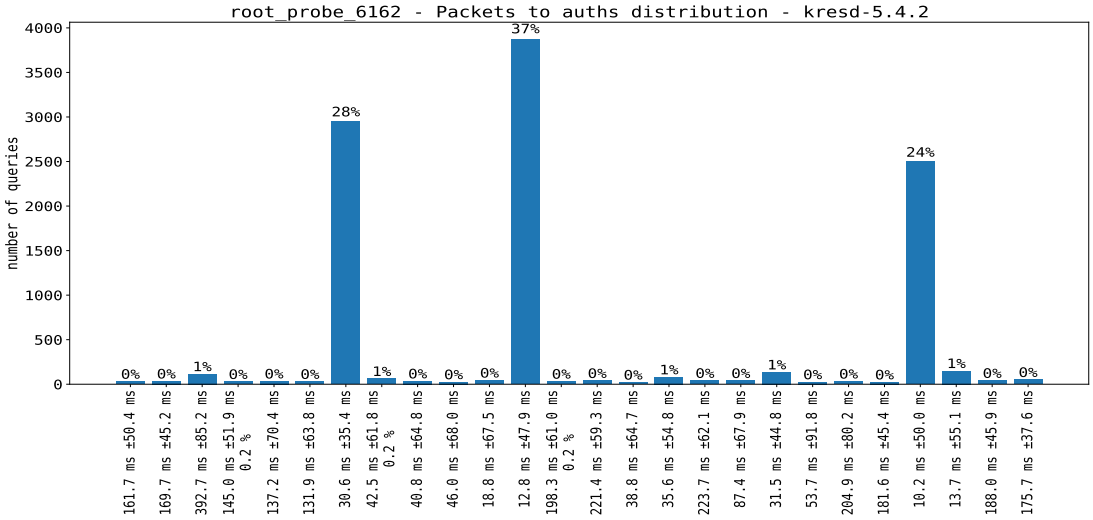
Výběr NS: .cz servery, Taiwan



Výběr NS: root, Nová Kaledonie, starý kresd



Výběr NS: root, Nová Kaledonie, nový kresd



Konfigurace v budoucnu

- Teď: lua skript
  - Vysoká míra flexibility
  - Mnoho příležitostí se spálit: slabá syntaxe, …
  - Obtížné zpracování nástroji
- Plán: 99% konfigurace v YAML / JSON
  - Silná kontrola dle schématu – místo *spuštění* lua skriptu
- Před rokem průzkum: Jak nastavujete DNS resolvery?

Přehled

Poslední rok: verze 5.2.0 – 5.4.2

- Asserty / stabilita
- Logování
- DNS Shotgun
- Stabilizace DoH implementace
- Výběr name-serverů
- Konfigurace v budoucnu

KNOT RESOLVER

CZ.NIC | SPRÁVCE DOMÉNY CZ


cz.nic
SPRÁVCE
DOMÉNY CZ

Výběr NS: .cz servery, Taiwan, unbound 1.13.2