Novinky v  KNOT RESOLVER

Petr Špaček • petr.spacek@nic.cz • 12. 11. 2020

CZ.NIC | SPRÁVCE DOMÉNY CZ

Ve stručnosti

- Balíčky
- Dokumentace
- Verze 4.2.2 ⇒ 5.2.0
- Bezpečnost
- Nové politiky
- Výkon

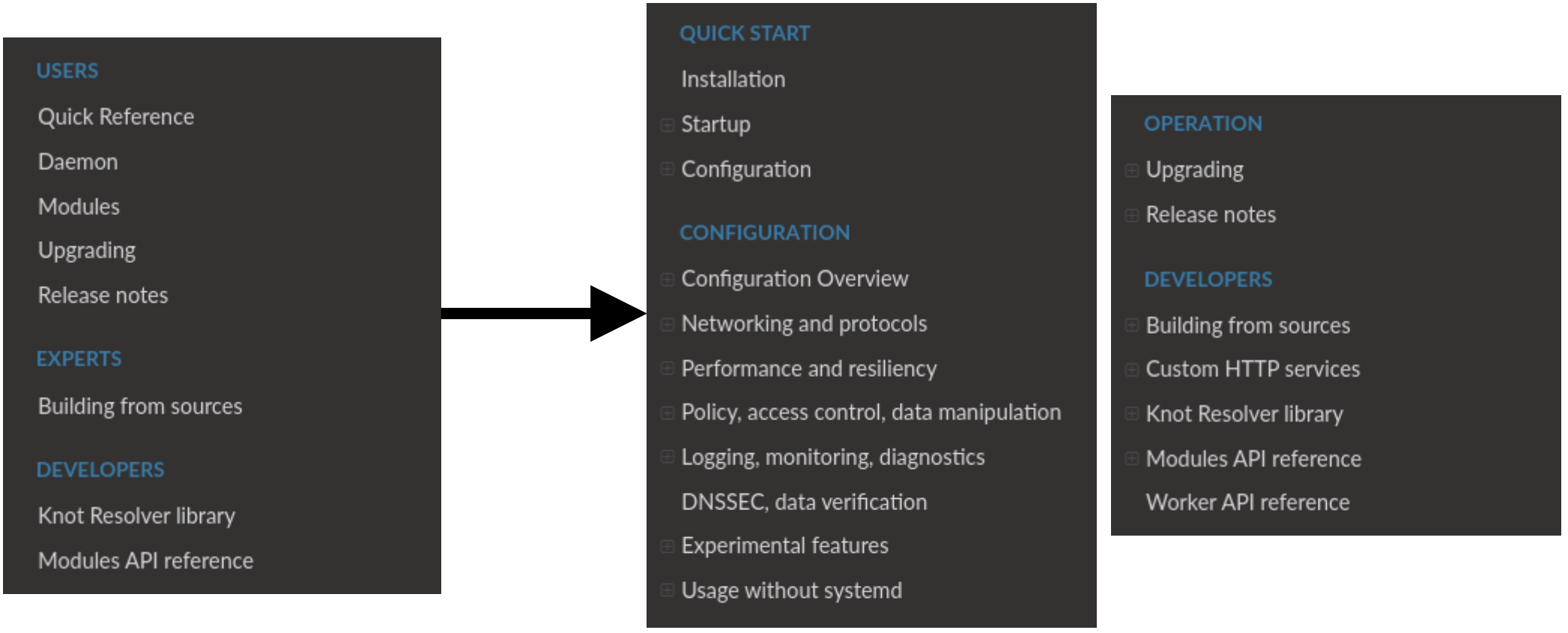
Balíčky od CZ.NIC

- **https://www.knot-resolver.cz/download/**
- 18 kombinací distribuce a verze
- Arch
- CentOS (EPEL) 7, 8
- Debian oldstable, stable, unstable
- Fedora 31, 32, 33, Rawhide
- OpenSUSE 15.1, 15.2, Tumbleweed
- Ubuntu 20.10, 16.04, 18.04, 19.10, 20.04

Balíčky v distribucích

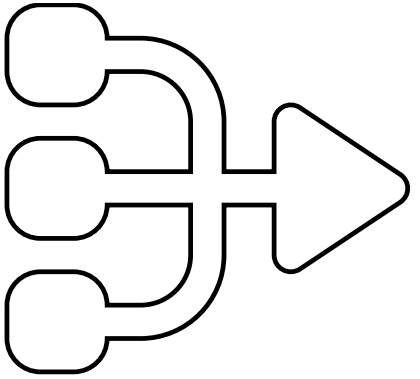
- 14 kombinací distribuce a verze
- CentOS (EPEL) 7, 8
- Fedora 31, 32, 33, Rawhide
- Debianu a Ubuntu
  - Aktualizace v Debian testing a Ubuntu 20.10
  - Pořád je lepší vyhnout se "stable" distribučním balíčkům …
- Nově jeden "balíčkovač" na plný úvazek
  - Světlé zítřky

Nová dokumentace



Bezpečnost

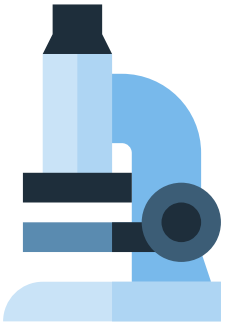
- NXNSAttack
  - DDoS skrz resolvery, CVE-2020-12667
  - Umělý limit na počet NS jmen v delegacích
  - Hlavně domény bez DNSSECu
  - [odkaz na popis]
- DNS flag day 2020
  - Omezení fragmentace na IP vrstvě
  - Zmenšení max. velikosti UDP odpovědi na 1232 bytů
  - [odkaz na další informace]



Nové politiky

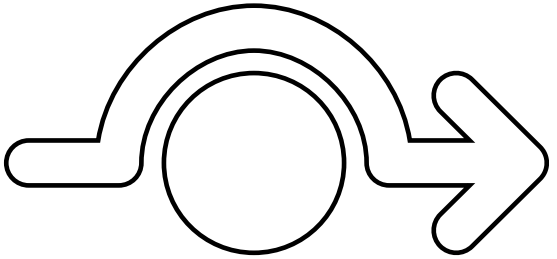
- Rozšíření podpory Response Policy Zone [dokumentace]
- Nová `policy.ANSWER`
  - Možnost generovat odpovědi na resolveru [dokumentace]
- Zacílené ladící výpisy [dokumentace]

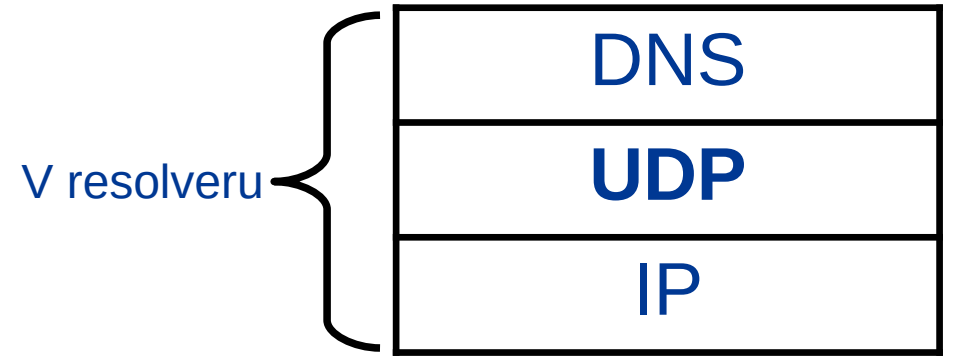
```
policy.add(policy.suffix(
    policy.DEBUG_CACHE_MISS,
    policy.todnames({'example.com.'})))
```



Výkon: UDP

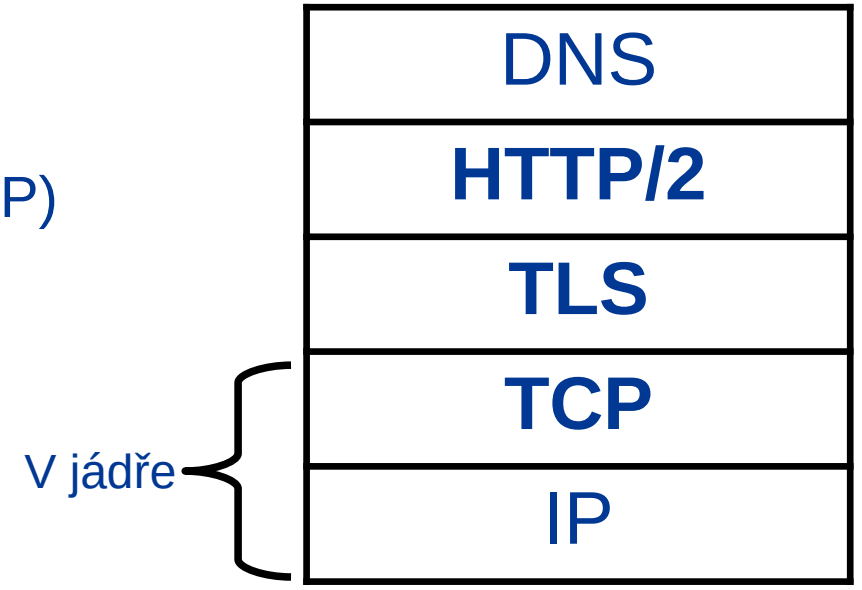
- Využití eXpress Data Path v Linuxu 4.18+
- Obchází síťový stack pro UDP provoz
  - Žádný firewall, žádný tcpdump, jen symetrické směrování
- Úspora CPU -50 až +50 % :-)
  - Dle ovladače síťové karty a jádra
    - i40e, ice, ixgbe, mlx5, mvneta, solarflare
  - Dle charakteru provozu
- Experimentální
  - Linux 5.9.2 na loopbacku zpanikaří (pozor při testech)





Výkon: DNS-over-HTTPS

- Reimplementace od základů
- Podpora pouze HTTP/2 přes TLS
  - Knihovny libnghttp2 + GnuTLS
- Zhruba 3,4 x "dražší" než UDP (bez XDP)
  - ECC certifikáty, "slušní" klienti
- Nové neznámé
  - "Neslušní" klienti?
  - Útoky proti TLS a HTTP?



Děkuji za pozornost

Petr Špaček • petr.spacek@nic.cz