

Knot DNS

krátký pohled do budoucnosti

Ondřej Surý • ondrej.sury@nic.cz • 2014 May 23

Knot DNS 1.4

- DNSSEC automatické podepisování

```
zones {  
    example.com {  
        file ``example.com'';  
        dnssec-enable on;  
        dnssec-keydir ``/etc/knot/keys'';  
    }  
}  
$ knotc signzone
```

- Podpora pro IDN v Knot DNS utilitách (kdig, khost, knusupdate)
- Nižší spotřeba paměti



Knot DNS WIP

- Knot DNS 1.5
 - Dynamické moduly
 - Hodně refaktoringu, který není moc vidět
 - Ještě nižší spotřeba paměti
 - Rychlost zpracování odpovědi
- Knot DNS 1.6
 - Vylepšená podpora pro DNSSEC



Dynamické moduly

- „Háčky” ve zpracování query-response
- Dává nám to různé možnosti
 - Split-horizon (GeoIP, ...)
 - Poor man's HA
 - syntéza reverzních a forward záznamů



Syntetizované RR

- IPv6 adresní prostor je obrovský
 1. Není možné mít všechny reverzní záznamy v zóně, ale...
 2. zákazníci chtějí odesílat emaily,
 3. MTA kontrolují existenci PTR záznamů,
 4. a zákazníci si stěžují...
- Konfigurace (detailněji v manuálu)

```
synth_record "(forward|reverse) <prefix> <ttl> \  
<address>/<nn>";
```
- Zatím bez DNSSEC (plán pro 1.6)



Příklad konfigurac

```
example.org. {  
    query_module {  
        synth_record "forward gen- 400 2620:0:b61::/52";  
        synth_record "forward gen- 400 192.168.1.0/25";  
    }  
}  
1.168.192.in-addr.arpa {  
    query_module { synth_record "reverse gen- example.org.  
400 192.168.1.0/25"; }  
}  
1.6.b.0.0.0.0.0.2.6.2.ip6.arpa {  
    query_module { synth_record "reverse gen- example.org.  
400 2620:0:b61::/52"; }  
}
```

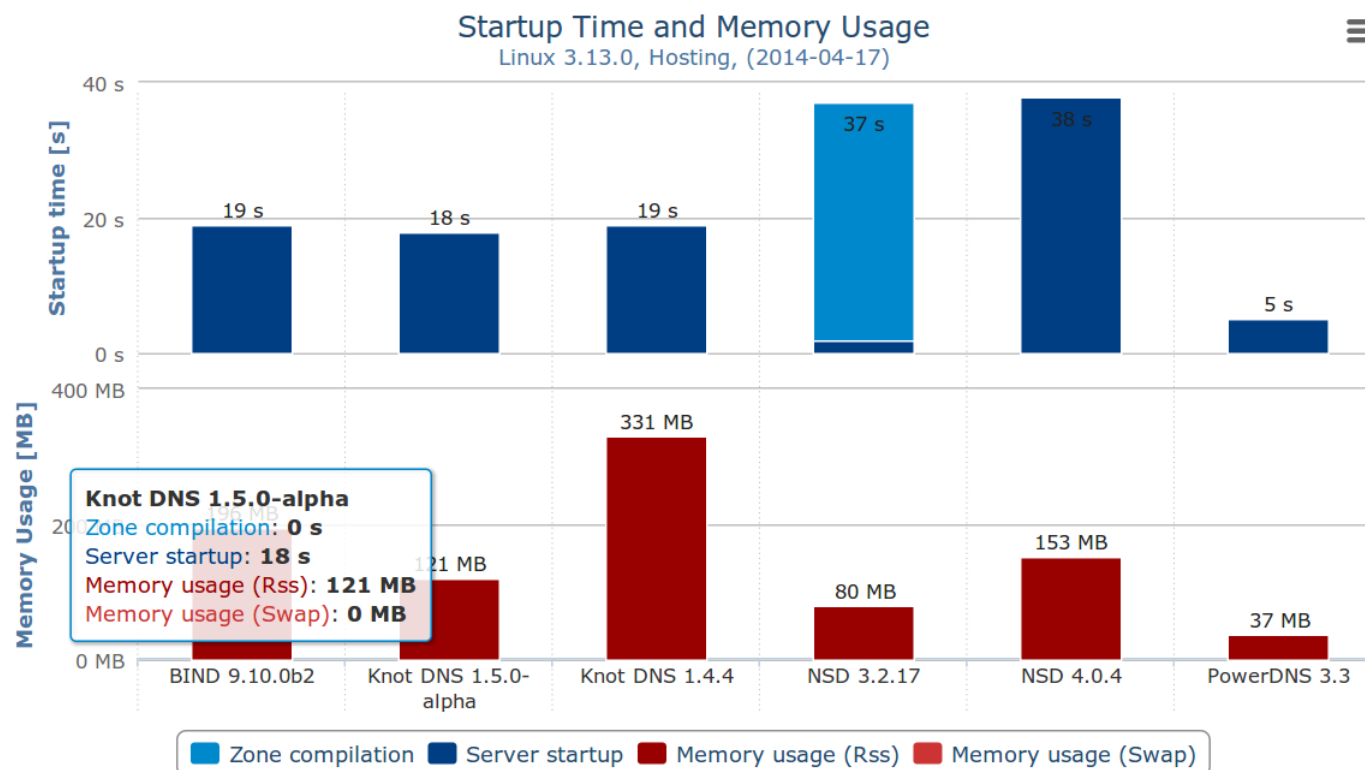


Příklad výstupu

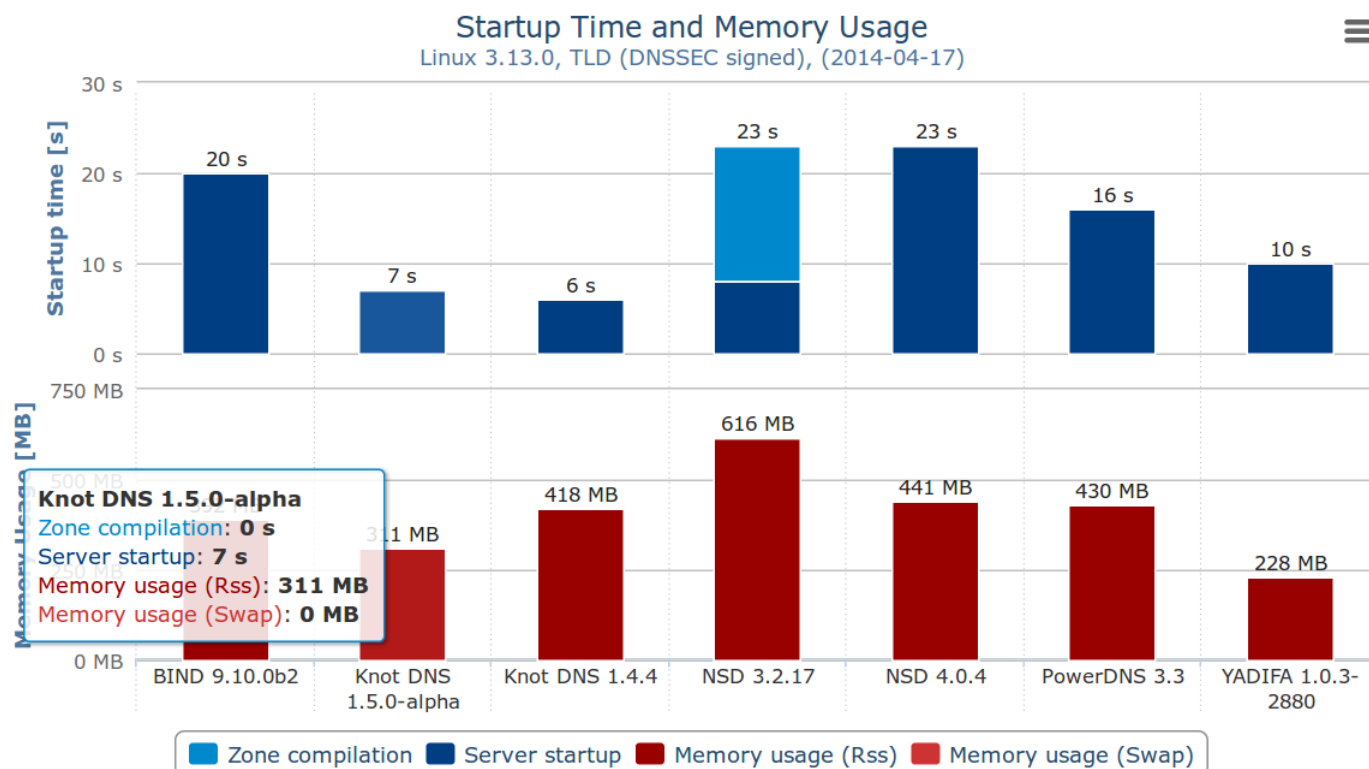
```
$ kdig AAAA gen-2620-0000-0b61-0100-0000-0000-0000-0000-0000.example.org.  
[...]  
;; QUESTION SECTION:  
;; gen-2620-0000-0b61-0100-0000-0000-0000-0000-0000.example.org.  
0 IN AAAA  
;; ANSWER SECTION:  
gen-2620-0000-0b61-0100[...] 400 IN AAAA 2620:0:b61:100::  
  
$ kdig PTR 1.0.0...1.6.b.0.0.0.0.0.0.2.6.2.ip6.arpa.  
[...]  
;; QUESTION SECTION:  
;; 1.0.0...1.6.b.0.0.0.0.0.0.2.6.2.ip6.arpa. 0 IN PTR  
;; ANSWER SECTION:  
[...] 400 IN PTR gen-2620-0000-0b61-0000-0000-0000-0000-0000-0001.example.org.
```



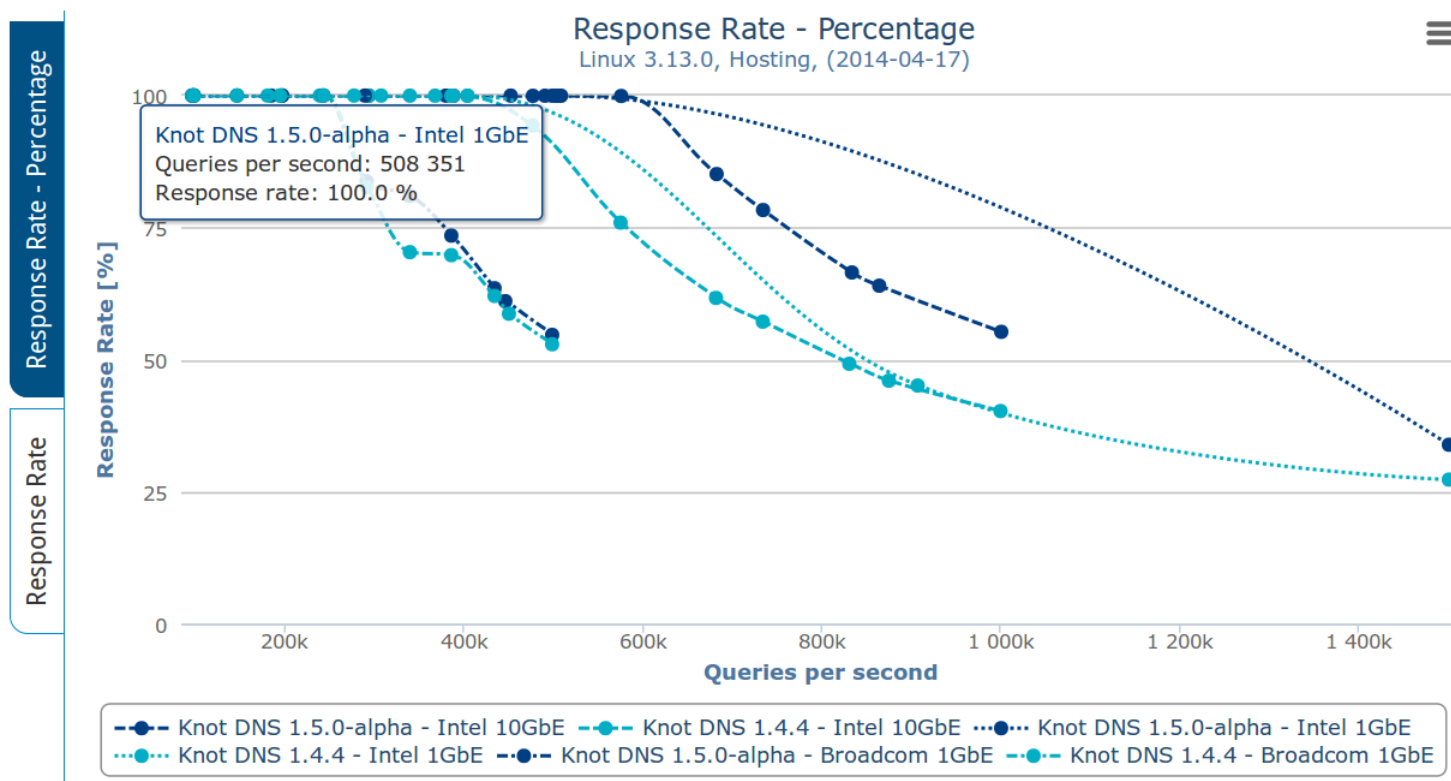
Paměť (10k malých zón)



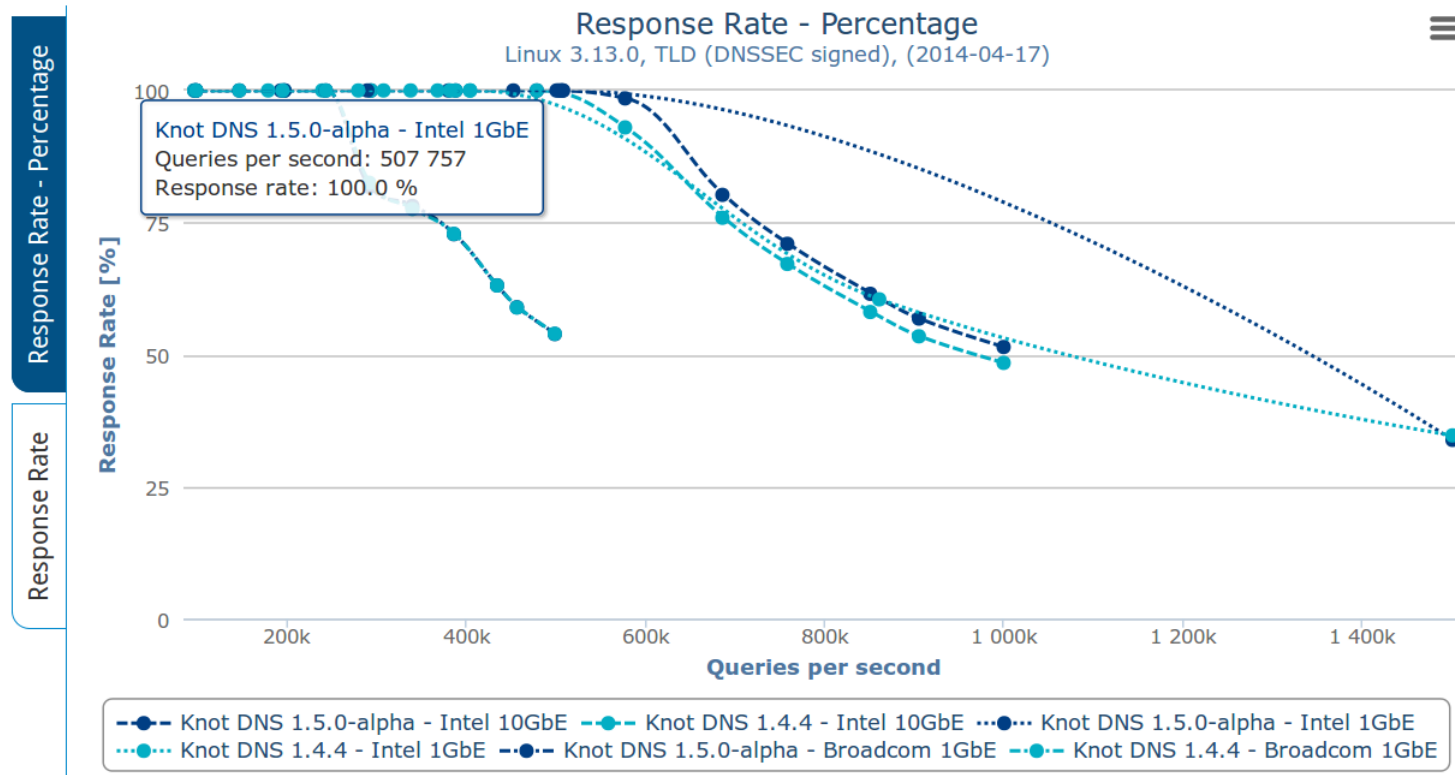
Paměť (podepsaná TLD; 250k RRs)



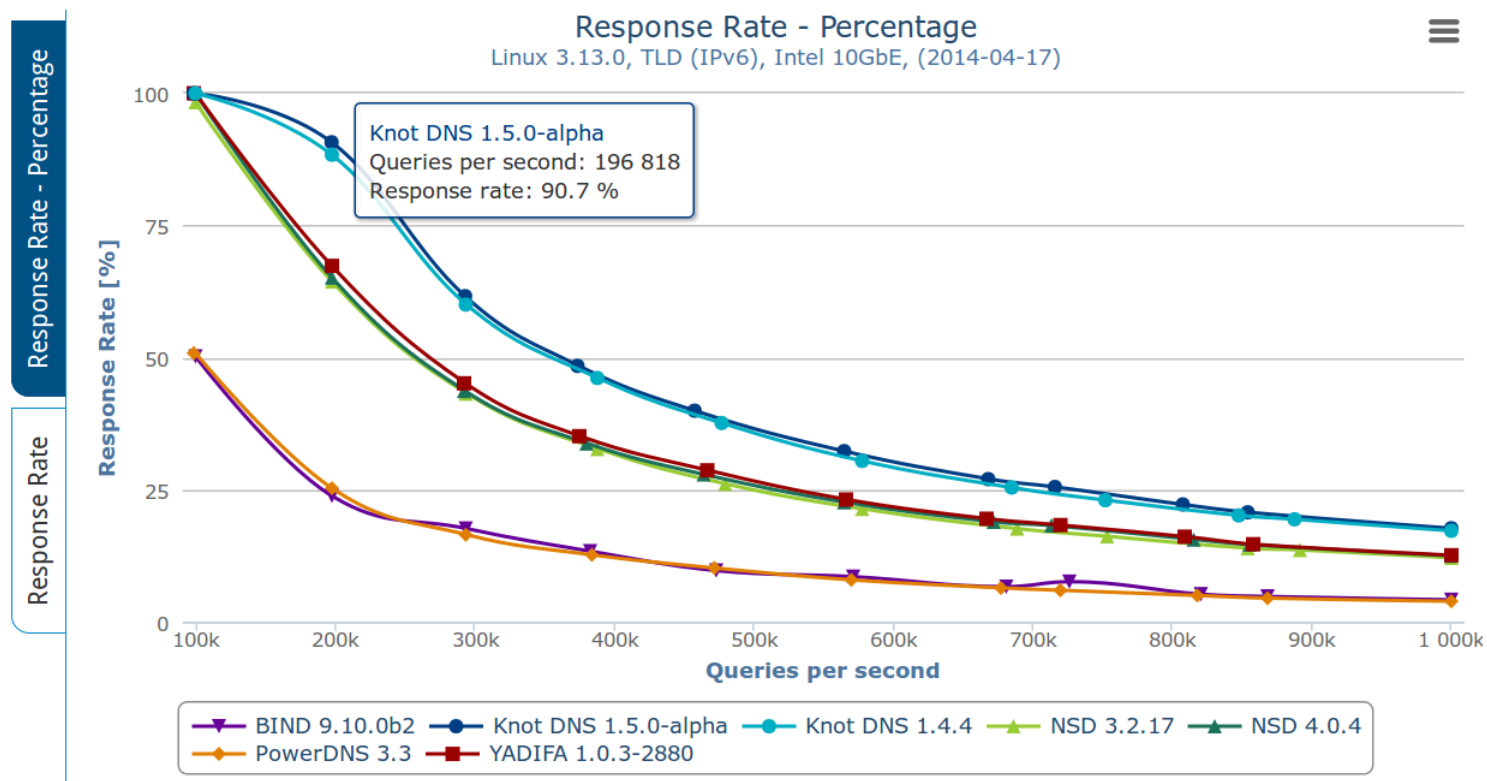
Rychlost (10k malých zón)



Rychlost (TLD signed; 250k RRs)



Rychlost (TLD; IPv6)



Vylepšená podpora DNSSEC

- libdnssec separation
 - Změna z OpenSSL na GnuTLS (ještě před heartbleed)
 - Podpora pro hardware security modules (PKCS#11)
 - Key and Signing Policy (KASP)
- On-line podepisování
 - Minimální odpovědi NSEC3 encloser
 - Podepisování odpovědí z dynamických modulů



Questions?

