Knot DNS

Independent high-performance DNS server

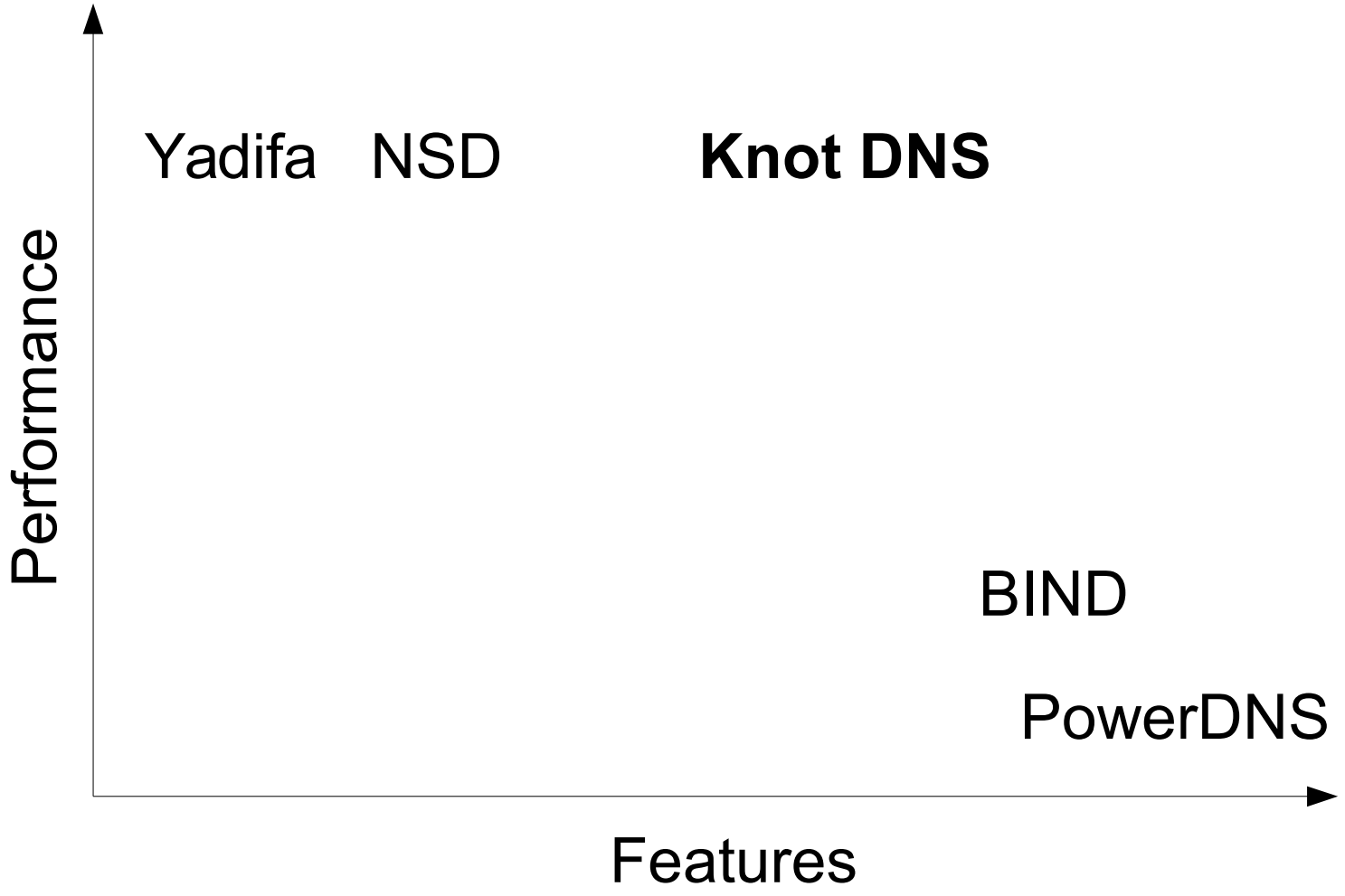
Jan Včelák • jan.vcelak@nic.cz • 31.01.2015

CZ DOMAIN REGISTRY

What is Knot DNS?

- https://www.knot-dns.cz
- Authoritative-only DNS server
- High-performance and scalable
- Designed for universal use
  - Master and slave features
  - Root servers, TLDs, webhosters, single domains

Knot DNS and The Others



Knot DNS history and near future

- 0.8 2011 first stable release
- 1.6 2014 **LTS version**

- 1.99.0 2014/12 new DNSSEC
- 1.99.1 2015/02 DNSSEC with KASP
- 2.0-rc1 2015/02 new configuration

Knot DNS outstanding features

- Non-stop operation (RCU, Read-Copy-Update)
- AXFR/IXFR zone transfers
- DDNS dynamic updates
- DNSSEC, including automatic signing
- RRL (Response Rate Limitting)
- Pluggable modules

PTR/A/AAAA synthesis module

- IPv6 address space is vast
- some services require matching reverse record

```
example.org. {
  query_module {
    synth_record "forward gen- 400 2620:0:b61::/52";
  }
}

1.6.b.0.0.0.0.0.0.0.2.6.2.ip6.arpa {
  query_module {
    synth_record "reverse gen- example.org. 400
                  2620:0:b61::/52";
  }
}
```

PTR/A/AAAA synthesis module

- Non-live demo:

```
$ kdig +short PTR \
  2.4.0...0.0.0.0.0.0.0.0.1.6.b.0.0.0.0.0.0.2.6.2.ip6.arpa

gen-2620-0000-0b61-0000-0000-0000-0000-0042.example.org.

$ kdig +short AAAA \
  gen-2620-0000-0b61-0000-0000-0000-0000-0042.example.org

2620:0:b61::42
```

DNSSEC in Knot DNS 1.6

- Technology Preview (but rock stable)
- Depends on BIND or ldns utilities
  - dnssec-keygen
  - dnssec-settime
- Some signing parameters are hardcoded
- Not how we think DNSSEC should be done

DNSSEC in Knot DNS 2.0

- Technology Preview
- KASP (Key And Signature Policy) based automatic key management
- New management utility (keymgr)
- libdnssec
  - Build you custom DNSSEC solution
  - GnuTLS replaces OpenSSL as a crypto backend
  - Future support for PKCS #11, offline keys, etc.

DNSSEC in Knot DNS 2.0

- Non-live demo:

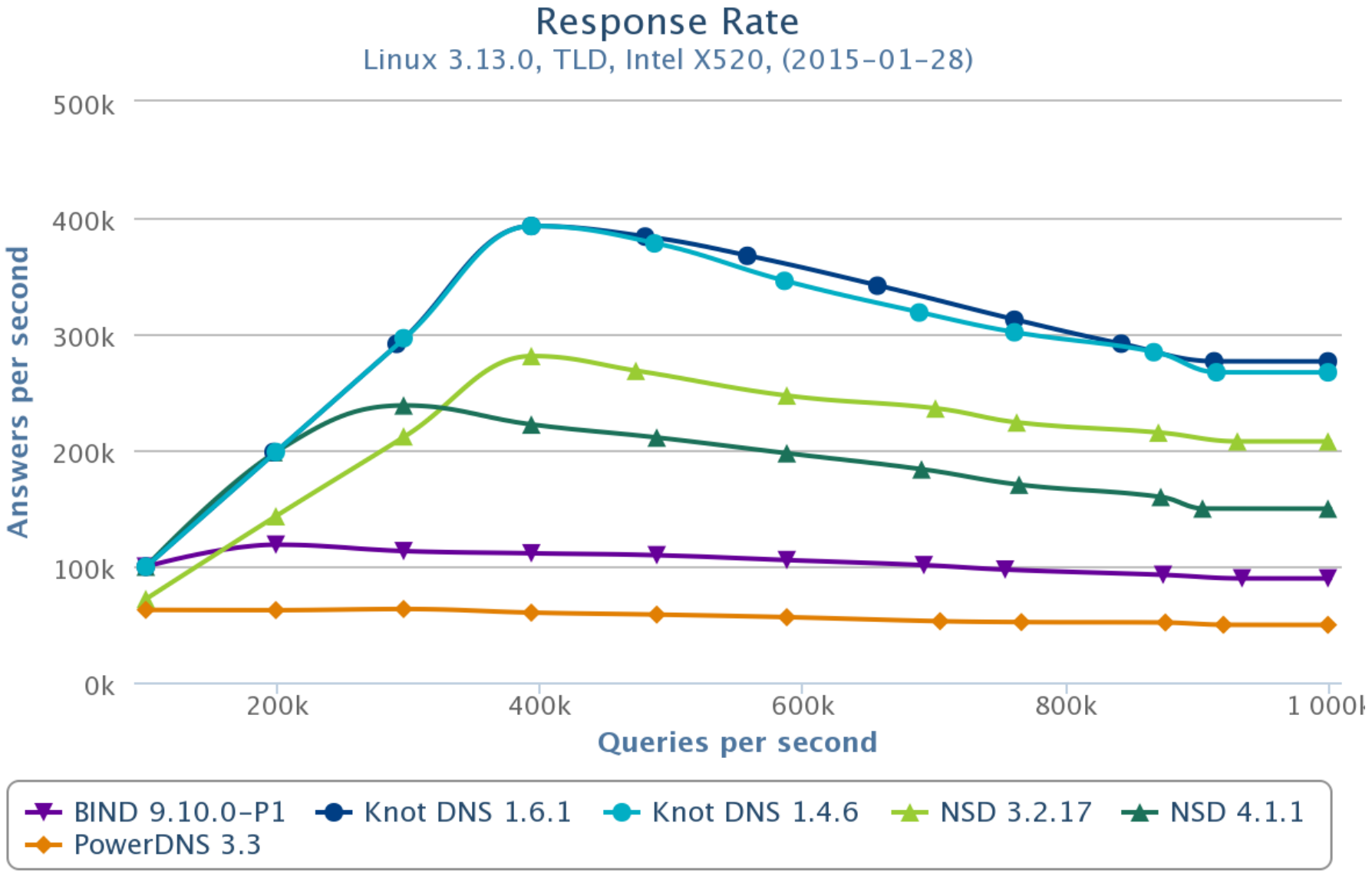
```
$ cd keys
$ keymgr init
$ keymgr zone add example.com
$ knotc reload

reloading configuration
DNSSEC, starting
DNSSEC, executing event 'generate initial keys'
DNSSEC, loaded key 43786, RSA-SHA256, KSK, public, active
DNSSEC, loaded key 57770, RSA-SHA256, ZSK, public, active
DNSSEC, signing started
DNSSEC, successfully signed
DNSSEC, next signing on 2015-01-30T23:56:24
```

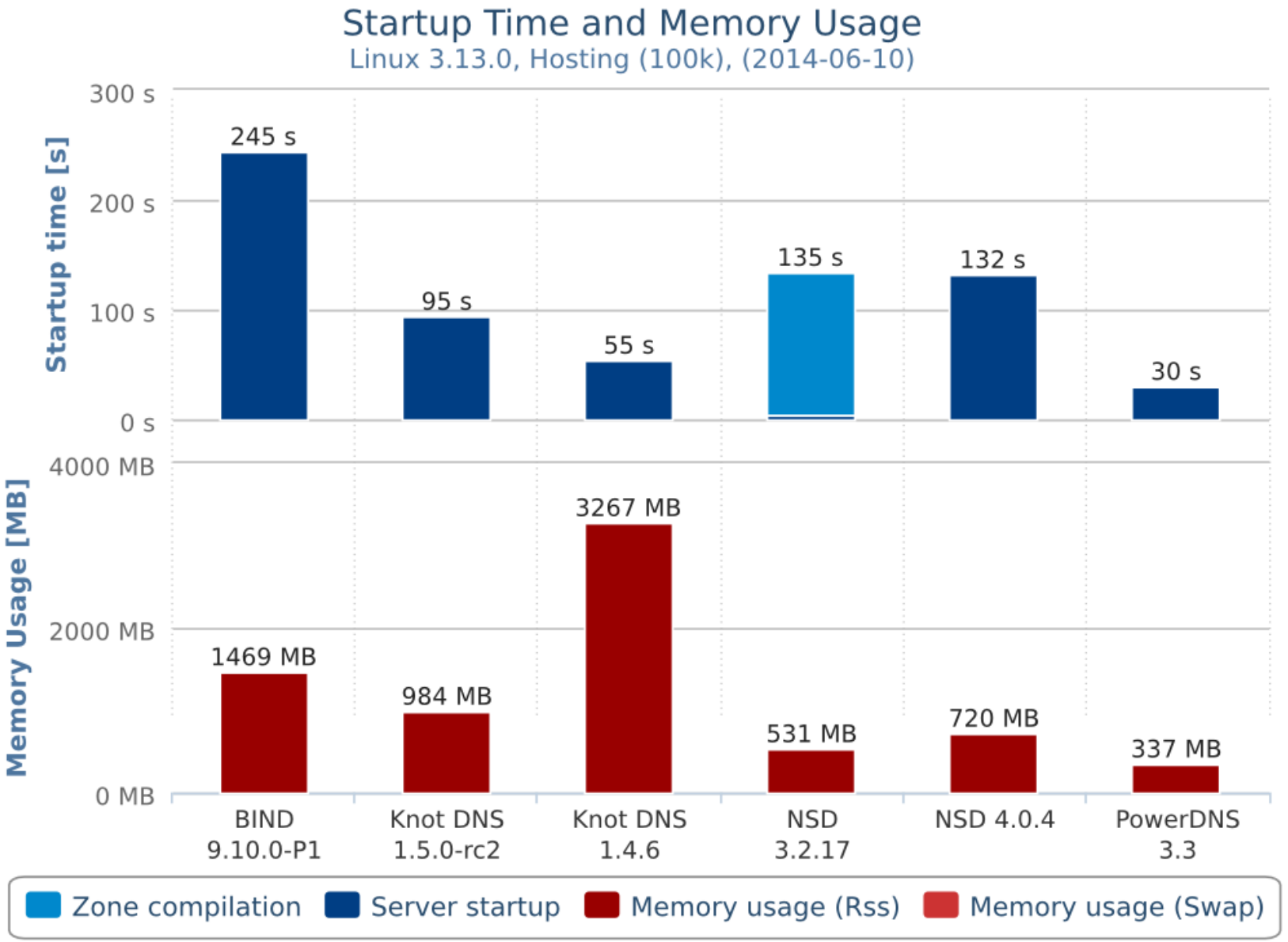
News in Knot DNS 2.x (where x > 0)

- New configuration format (binary storage)
- Remote provisioning
- On-line DNSSEC signing
- Additional modules (GeoIP, statistics, …)
- Just tell us what you need...

Benchmarking



Benchmarking



Significant Users (who told us)

- ICANN (L-root)
- RIPE NCC (K-root, various TLDs)
- TLD operators (.cz, .dk, .cl)
- Netriplex
- Telefonica O2 in Czech Republic
- various webhosters in Czech Republic
- …

Thank You

Jan Včelák • jan.vcelak@nic.cz • www.knot-dns.cz