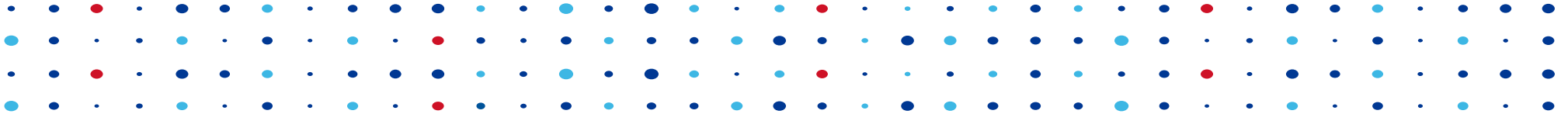


Knot DNS

High-performance authoritative DNS server

Ondřej Surý & Alix Guillard • 12.12.2013
<knot-dns@labs.nic.cz>

What is Knot DNS?

- Authoritative(-only) DNS server
- Open source – GPLv3
- Current stable branch: v1.3.x

Project history

- Fall 2011 – Public beta release
- Spring 2012 – Knot DNS 1.0
- Fall 2012 – Knot DNS 1.1
  - Massive transfer (IXFR) speedups
  - Reference manual!
- Spring 2013 – Knot DNS 1.2
  - Dynamic updates, Response Rate Limiting
- Summer 2013 – Knot DNS 1.3
  - Parser rewrite (Flex/Bison → Ragel)
- Winter 2013 – Knot DNS 1.4
  - DNSSEC signing!

Design goals

- Open-source authoritative-only DNS server
  - Developed in an open way (we do not hide our mistakes)
- Usable for everybody (root zone, TLDs, massive DNS hosting)
- Fast(est), feature-rich
  - Very close to the theoretical limits of the platform (trafgen)
  - 550+kpps on 10GbE
  - https://www.knot-dns.cz/pages/benchmark.html
- On-the-fly reconfiguration
- Portable, modular
  - Linux, *BSD, MacOSX
  - Portability mainly depends on userspace-rcu library

Standards compliant

- AXFR/IXFR (both master and slave)
- All known RR Type support
  - Including TYPEnnnn \# (RFC 3597)
  - Even some obsolete types
- DNSSEC with NSEC3
- TSIG supported
- Root zone support
- NSID support (RFC5001)
- Fast track new standards

Configuration

- Curly braces and semicolons (C-like)
  - Interfaces (IPv4 or IPv6)
  - Remotes (masters or slaves)
  - Zones
  - Keys (TSIG)
- Logging (syslog or file-based)

- Very simple DNSSEC setup and configuration
  - Create the keys

    # mkdir /etc/knot/keys

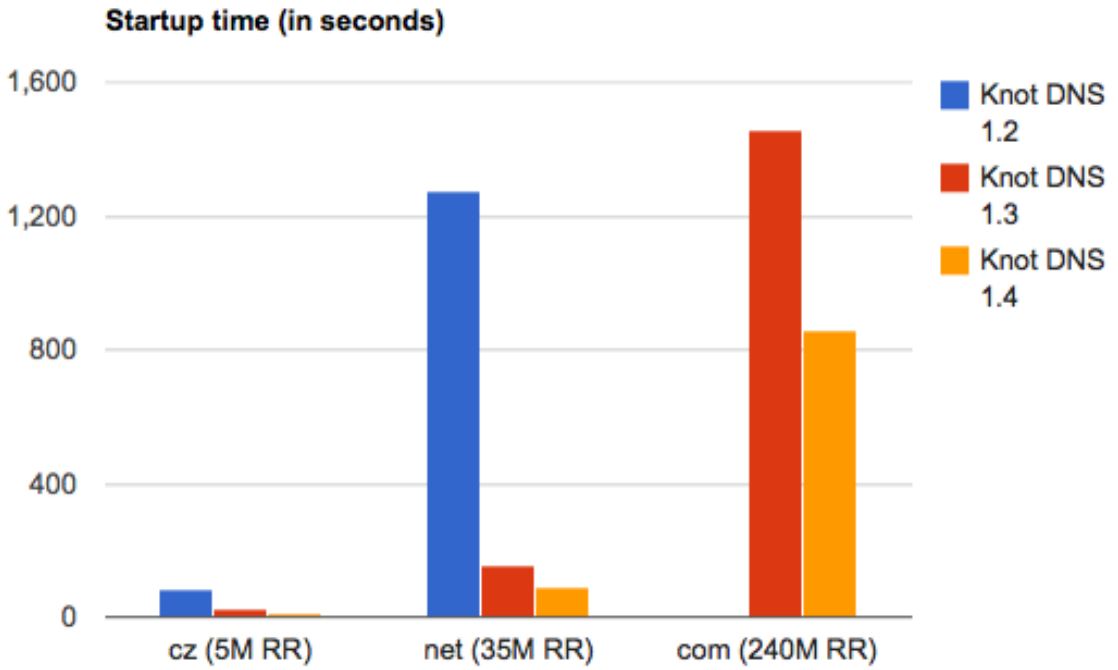
    # cd /etc/knot/keys

    # dnssec-keygen -a RSASHA256 -3 jsres.org

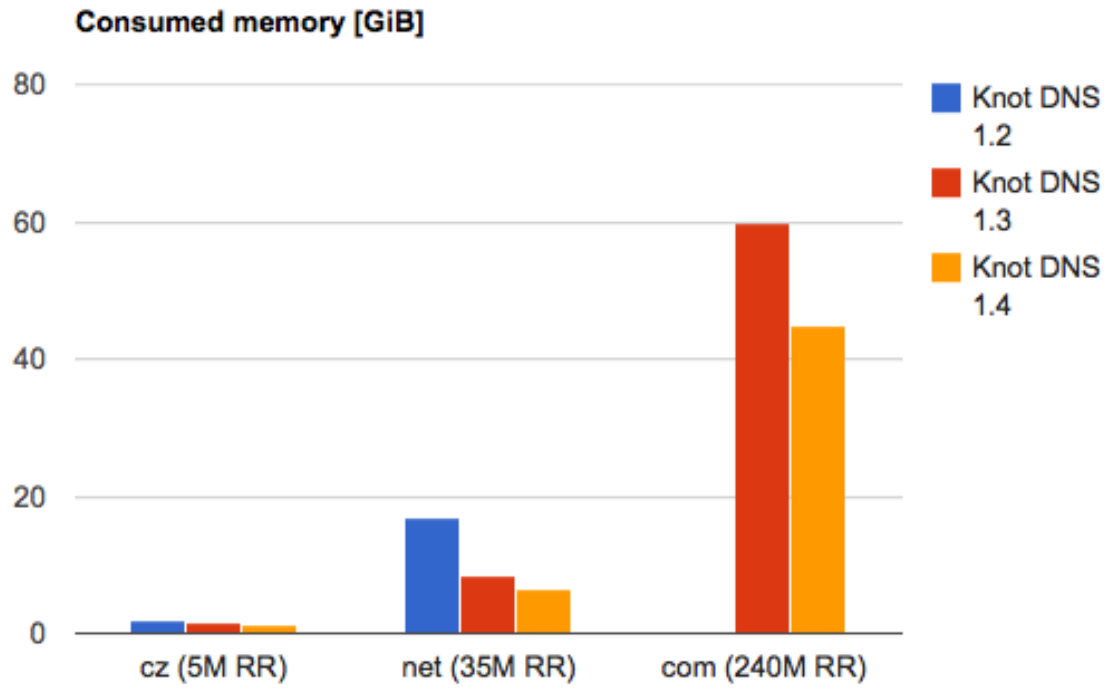
    # dnssec-keygen -a RSASHA256 -fk -3 jres.org
- Configure the zone

```
zones {
  dnssec-keydir “/etc/knot/keys”;
  zone “jres.org” {
    dnssec-enable on;
    file “/etc/knot/zones/jres.org”;
  }
}
```

Startup time [s]



Memory consumption [GiB]



Known deployments

- .CZ (+ several small zones) – anycast cloud
- .DK – slave server
- NIX.CZ – AS112
- hosting90.cz, igloonet.cz (50-100k domains)

Planned deployments

- L-ROOT (ICANN)
  - Huge anycast farm for l.root-servers.net.
  - http://goo.gl/1aLfMT
- RIPE NCC – TLD slave
  - http://goo.gl/WW31k
- .RU
- Other gTLDs: .UA, .SE, .UK
- More Czech registrars

Pre-packaged Knot DNS

- Debian
  - Unstable/Testing(Jessie)
  - Backports (Wheezy)
- Ubuntu PPA
  - ppa:cz.nic-labs/knot-dns (all supported releases)
- FreeBSD
  - http://www.freebsd.org/cgi/cvsweb.cgi/ports/dns/knot/
- Fedora
  - Knot DNS is part of Fedora Project
  - https://admin.fedoraproject.org/pkgdb/acls/name/knot
- OpenSUSE
  - Official packages
  - OpenSUSE Build Service / OpenSUSE Factory
  - http://software.opensuse.org/package/knot

Resources

- Home page: http://www.knot-dns.cz/
- Google+ page with news: http://goo.gl/f7IWF
- Issue tracking and source code
  - Contributions welcome!
  - We are Open Source (not just Source Available)
  - https://gitlab.labs.nic.cz/labs/knot
- Mailing list

  knot-dns-users@lists.nic.cz

Thank You

Ondřej Surý & Alix Guillard • knot-dns@labs.nic.cz

jres Montpellier 2013

CZ DOMAIN REGISTRY