KNOT RESOLVER

A flexible DNSSEC-validating Resolver

Ondřej Surý • ondrej.sury@nic.cz • 31.1.2016

CZ DOMAIN REGISTRY

Who are those CZ.NIC people?

https://www.knot-dns.cz/

http://bird.network.cz/

https://omnia.turris.cz/

What is Knot DNS Resolver?

- **Platform for building recursive DNS service**
- Open-source DNS Resolver (GPLv3+)
- Full DNSSEC support:
  - RFC 6650 – ECDSA support
  - RFC 5011 – Automated Trust Anchor Management
  - RFC 7646 – Negative Trust Anchors

What is Knot DNS Resolver?

- Written in C and LuaJIT
- Scriptable daemon with dynamic configuration in Lua
- Simple **core** extensible with modules in C, Lua & Go
- “Happy Eyeballs” IPv6 (20ms headstart)
- No internal threading, scales by self-replication

Who is it for? Everybody!

- Large recursive DNS farms
- Small recursors in private networks
- Personal resolvers
- Geeks, tinkerers, and your granma :)

Large recursive DNS farms

- Scales, the really fast scriptable engine allows you to change resolution
- Flexible cache backends (lmdb, memcached, redis)
- Great statistics, metrics, and plotting with Graphite backend
- RF7646 Negative Trust Anchors
- Cluster-aware – etcd module for self-configuration
- Views and ACL support
- Prefetching

Plotting in Grafana

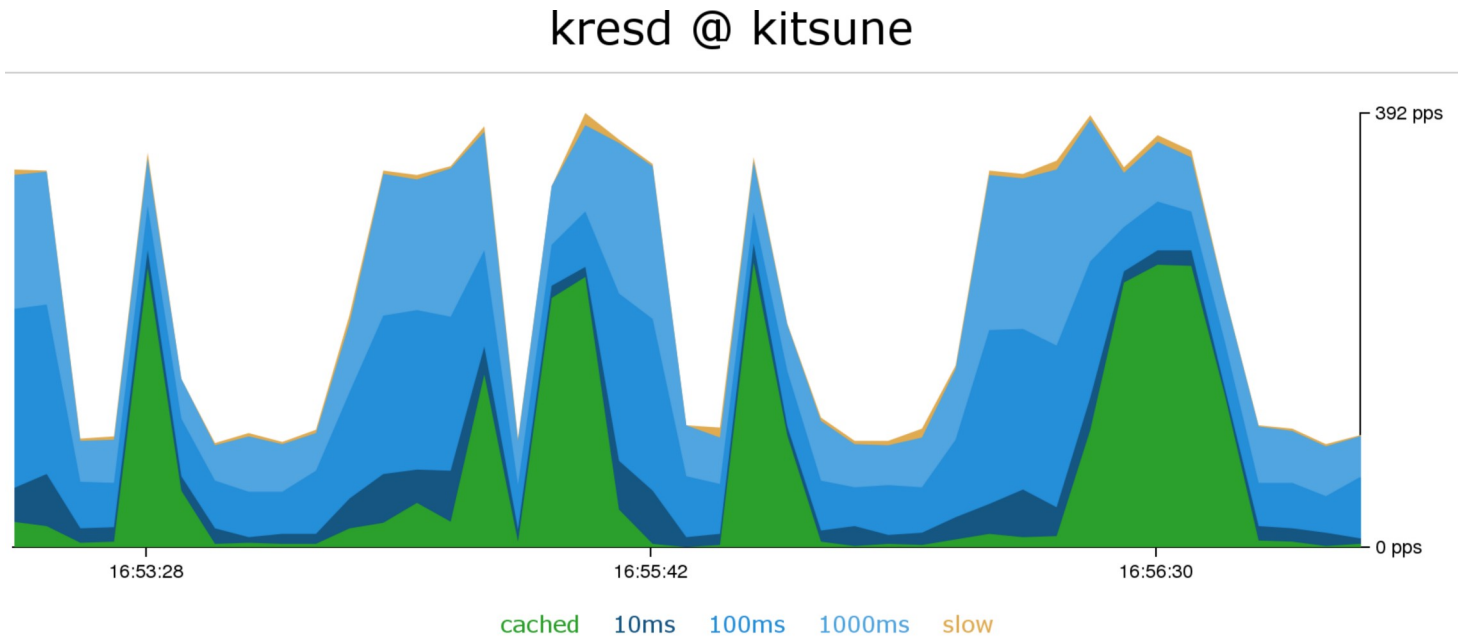
Small recursors in private networks

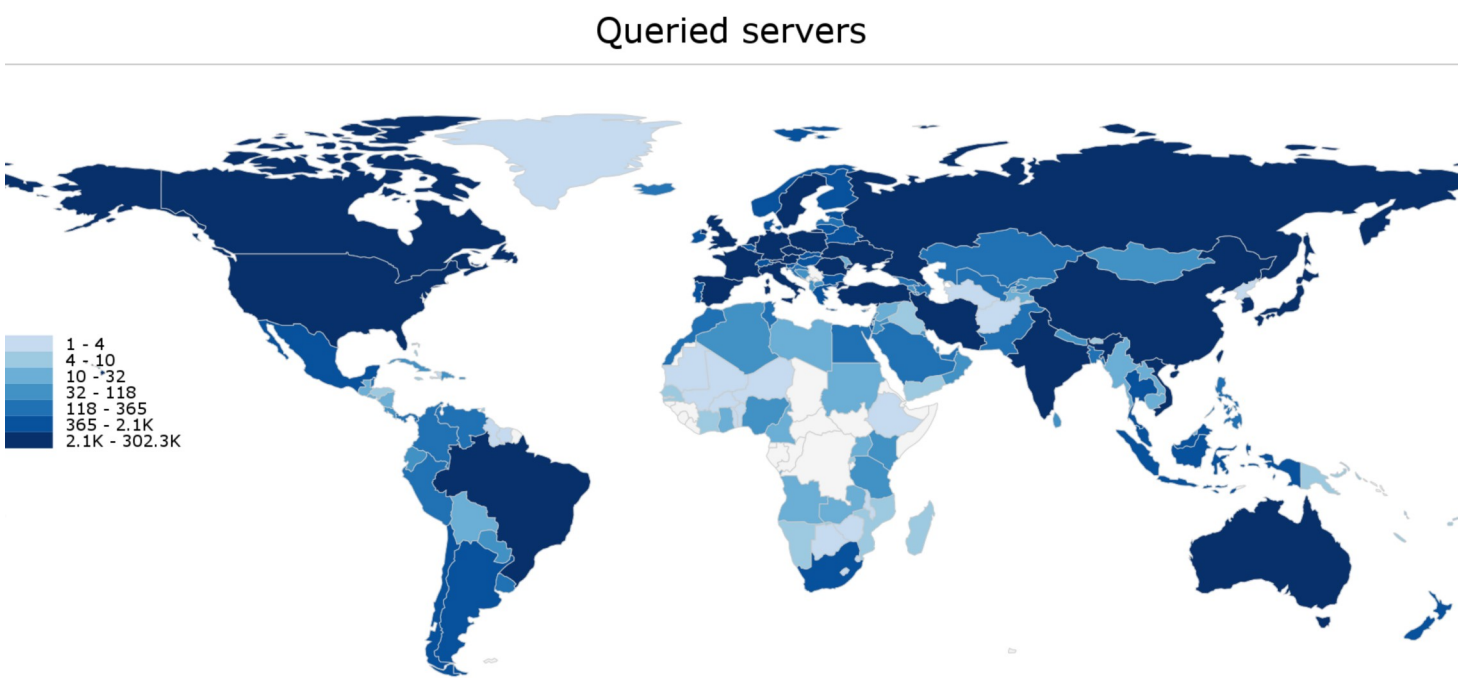
- QNAME minimisation for DNS privacy
- DNSSEC and RFC5011 key management
- Low memory consumption (cache can be paged out)
- Query policy based resolution
  - Match: pattern, suffix, RPZ
  - Action: PASS, DENY, DROP, FORWARD, TC
- DNS64 support to complement NAT64

Personal resolvers

- Simple config-less operation
  - Just give it a writeable file for DNSSEC root trust anchor and you are good to go
- Persistent caching (survives reloads/reboots)
- Tinyweb module for monitoring your queries
  - Live Demo: https://kitsune.labs.nic.cz/
- Future:
  - DNS over HTTP and dealing with “hotel wifis”
  - DNS over TLS (as the standards mature)

Tinyweb output





Geek, Tinkers, …

- kresd is scriptable without binding go port 53
- scripts/kresd-host.lua
  - dig/host like utility

```
$ ./scripts/kresd-host.lua -c IN -t AAAA www.fosdem.org
www.fosdem.org has IPv6 address 2001:67c:1808::5
```

- scripts/kresd-query.lua
  - Prints DNS response QNAME

```
kresd-query.lua -t SOA cz "print(pkt:qname())"
cz
```

  - Prints RCODE from the DNS response

```
kresd-query.lua -t SOA nan. "print(pkt:rcode())"
3 # ← NXDOMAIN
```

  - API specification in the documentation

Current status

- A beta phase of the project
- Comes with extensive documentation
  - http://knot-resolver.rtfd.org
- Give it a try!
  - Shiny new website: https://www.knot-resolver.cz/
  - Debian and Ubuntu packages (see the website)
  - Sources: https://gitlab.labs.nic.cz/knot/resolver
  - Docker # docker run cznic/knot-resolver
- Throw a normal and a weird DNS stuff on it
- Report back any oddities or success stories

Thank You

Ondřej Surý • ondrej.sury@nic.cz