Repairing DNS at TLD scale

DNS health in .CZ

Petr Černohouz • petr.cernohouz@nic.cz • 04.02.2018

CZ DOMAIN REGISTRY

CZ.NIC introduction

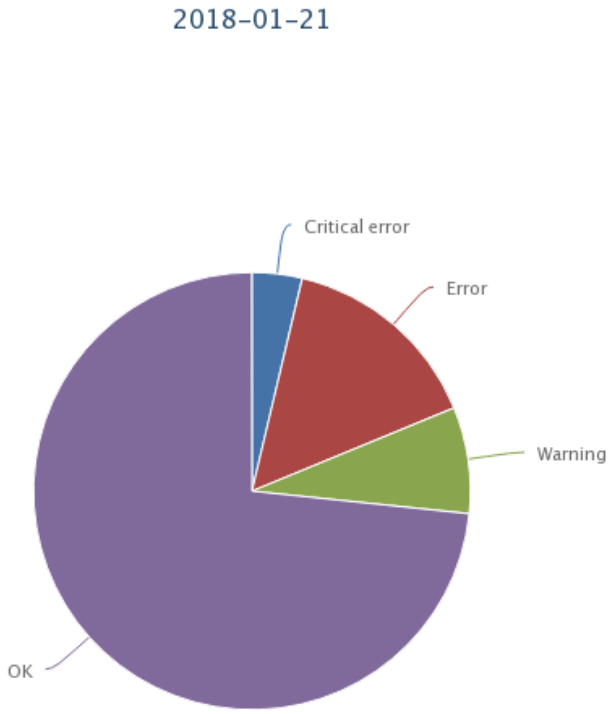
- .CZ TLD registry
- 1 300 000 domains
- R&D department
  - Knot DNS
  - Knot Resolver
  - BIRD
  - Turris Omnia
  - research

DNS server requirements in .CZ

- Two authoritative servers for initial delegation
- …
- Periodical technical checks
- Sends email on contacts
  - Who is the contact?
- Domain holders are responsible(?!)

Getting data

- Inspired by IIS.se
  - Health report
- Past - DNScheck
  - Slow – 10 days
  - Hard to process results
- Zonemaster
  - Very fast – hours
  - Previous presentation



Definition of correct state

- TCP and UDP 53
- IPv4 and IPv6
- Not recursive
- In different AS
- Without public zone transfers
- SOA times in some range
- Correct reverse records

Guideline

- Based on Zonemaster default policy
- Covers only Critical and Error states
- Explained why is every setting important
- Used by National cybersecurity office
  - Required for government name servers
- Available for everybody (only in Czech now)

Some data

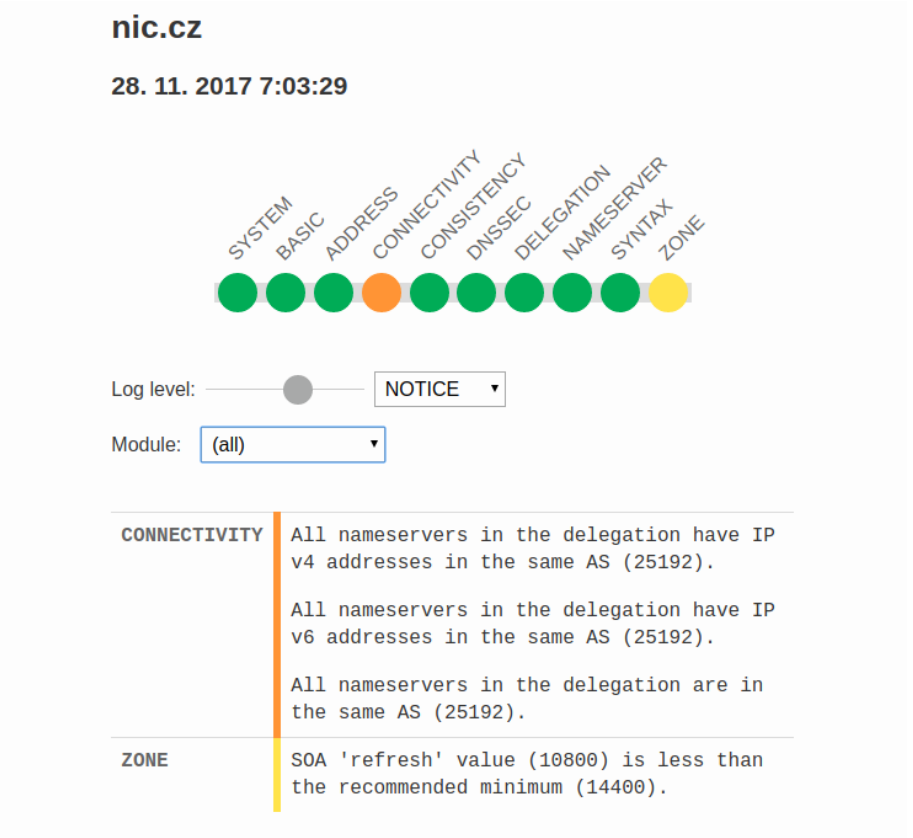
- 3,5% domains with critical error
  - Domains are unavailable
  - No simple solution
- 14% domains with error
  - 5% - delegation mismatch
  - 3,5% - no TCP
  - Recursive servers
  - Private addresses
  - DNSSEC related problems

Some data

- 33% domains with warnings
  - 18% - no reverse records
    - IPv6
  - 5% - bad EDNS0 answer
  - Multiple serial numbers
  - To low expire value
    - Lower than refresh

Next steps

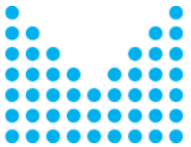
- Join with other data
  - DNS magnitude (nic.at)
- Contact the correct people
- Educate, educate, educate



Thank You

Petr Černohouz • petr.cernohouz@nic.cz

Project DNS health (VH20172018013) is funded by



MINISTRY OF THE INTERIOR
OF THE CZECH REPUBLIC

CZ DOMAIN REGISTRY