RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE NCC DNS Update

Anand Buddhdev | 28 Oct 2020 | RIPE 81

Secondary DNS with Neustar

- The query volume at Neustar kept increasing
  - In April this year, the volume increased substantially, going over our contracted volume
  - The overuse charges were quite high
- The cost of this service was too high, with no visible benefit
  - We withdrew service from Neustar in July
  - We forwent renewal of the contract in September
- ripe.net and our other zones are secondaried by AFRINIC, APNIC, ARIN and LACNIC

K-root

- Since RIPE 79, we have added 11 new instances
- As of RIPE 81, there are 81 active instances
- Average query rate is 120,000 q/s
  - Peaks at just over 200,000 q/s

AuthDNS

- This year we have been working on expansion
  - Even more important after cancelling the Neustar service
- New servers and routers for the core sites
- Deployed two new hosted instances
  - Rome (hosted by NaMeX)
  - Oslo (hosted by JCloud)

Name Server Diversity

- We continue to value name server diversity, by running a mixture of BIND, Knot DNS and NSD
- Recently, bugs in two of the implementations have caused the name server software to crash
  - The other implementations continued to run and provide service
  - Justifies the effort of understanding, packaging, configuring and maintaining three different implementations in parallel

DNSSEC Algorithm Roll-over

- All zones are currently signed with RSASHA256 (algorithm 8)
- RFC 8624 recommends upgrading to ECDSAP256SHA256 (algorithm 13)
  - Many zones, including some ccTLDs and gTLDs are using signed with algorithm 13
- This year we will develop a plan for an algorithm roll-over
  - We intend to upgrade to algorithm 13 in 2021

CDS/CDNSKEY for reverse DNS

- RFC 8078
  - Automatic update of a signed child zone’s DS record in the parent zone
  - Eases DNSSEC deployment
- The work on this has been delayed, due to other priorities
  - We are now aiming to have this implemented by mid January 2021

DNS Flag Day 2020

- Recommendations for authoritative servers
  - Answer queries over TCP - we already do this
  - Set the EDNS buffer size to 1232
    - Knot DNS has been doing this for a while
    - BIND >= 9.16.8 and NSD >= 4.3.3 also default to 1232
  - We intend to keep the defaults
    - As we upgrade our K-root and AuthDNS servers to newer versions, they will use this lower EDNS buffer size
    - We do not anticipate any problems because we do not observe any UDP responses larger than 800 bytes

Questions

anandb@ripe.net