AuthDNS and Zonemaster

• Fourth AuthDNS core site
  - Hardware delivery in July
  - New site will likely be in Asia

• Hosted AuthDNS
  - 11 active instances (handling 23,000 q/s - 16% of total query rate)

• Zonemaster
  - Updated to version 2022.2.2
  - User interface in RIPEstat coming soon
Software updates and data collection

- CentOS 7 is coming to end-of-life in 2024
  - Upgrades to Oracle Linux 9
- DITL - Day in the life
  - 50 hours of pcap data from K-root and AS112 uploaded to DNS OARC
  - Available to researchers who have agreements with DNS OARC
Zone propagation incident

- One of our secondaries was serving older versions of two RIPE NCC reverse DNS zones
- DNSSEC signatures in the zones had expired
  - DNSSEC validation failures
  - Worse than SERVFAIL
Expiry timers

25.in-addr.arpa. SOA pri.authdns.ripe.net. dns.ripe.net. ( 
   1684926122 ; serial
   3600 ; refresh (1 hour)
   600 ; retry (10 minutes)
   864000 ; expire (10 days)
   3600 ; minimum (1 hour)
)

25.in-addr.arpa. RRSIG SOA 13 3 3600 20230607110202 20230524093202 ( 
   3096 25.in-addr.arpa.
   F6PixyE86N...
)

Anand Buddhdev | RIPE 86 | May 2023
Simple DNS infrastructure

• Secondary DNS server responds with SERVFAIL
• DNS resolvers try other servers

Primary DNS server

Zone transfer

Secondary DNS server

Zone expiry after 10 days
Tiered zone transfer infrastructure

Primary DNS server ➔ XFR server ➔ XFR server ➔ Publication server

Expiration after
10 days
20 days
30 days

Zone is served, with expired DNSSEC signatures for 16 days!
The solution

• EDNS EXPIRE option

• RFC 7314
  - EXPIRE option valid in SOA and XFR queries and responses
  - Primary server sets zone’s expiry timer from zone’s SOA record
  - Primary server responds with this expiry value in the EXPIRE field of the response
  - XFR client uses this value for the zone lifetime
  - Intermediate XFR server passes on this value to downstream XFR clients
  - Only works if all servers in the chain support the EXPIRE option
Example using EXPIRE option

dig @manus.authdns.ripe.net ripe.net soa +noall +comments +answer +expire +norec +multi
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48134
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; EXPIRE: 861439 (1 week 2 days 23 hours 17 minutes 19 seconds)
;; ANSWER SECTION:
ripe.net. 3600 IN SOA manus.authdns.ripe.net. dns.ripe.net. (1684949195 ; serial
3600 ; refresh (1 hour)
600 ; retry (10 minutes)
864000 ; expire (1 week 3 days)
3600 ; minimum (1 hour)
)
EXPIRE support in software

- BIND 9 (including dig)
- Knot DNS since version 3.2 (including kdig)
- NSD - not yet
  - https://github.com/NLnetLabs/nsd/issues/274
Lessons learned

• Review zone and signature expiry timer values
• More monitoring of our secondary DNS servers
• Work with secondary DNS providers to encourage use of the EXPIRE option
• Get EXPIRE support into all name servers in the K-root and AuthDNS anycast clusters
Questions

anandb@ripe.net