Reducing default DS TTLs for Faster Failure Recovery

Viktor Dukhovni, Puneet Sood
Google Public DNS

OARC 40 Lightning Talk

Shorter DS TTLs: shorter ***Mean Time to Recovery***

- Ability to rollback changes promptly is a requirement for important network services
- DNSSEC for popular domains would need to meet this requirement
- Bad DS RRsets require ability to do prompt fixes/rollbacks
    - Desirable to avoid 24-hour or more downtime after emergency DS updates
- Shorter DS TTLs will expire bad RRsets faster
    - Some increase in DS query volume
    - We're studying expected effect on parent (eTLD)
- **Note**: Cached validated child RRsets keep their existing TTLs!
    - No expected impact on child zone query volume
- Similar idea in Operational Experience with DNSSEC Signed Zones yesterday

Shorter DS TTLs: Child Zone Considerations

- Resolvers may cache zone as “signed” per TTL of cached DNSKEY RRset
- 2LD DS from parent zone may not be queried again until cached 2LD DNSKEYs expires
- Both DS from parent zone and DNSKEY TTLs from child zone need to be short for fast rollback to unsigned
- Child zone operator can adjust DNSKEY TTLs (before changes?) to meet mean-time-to-repair needs
- ***Profit!***… provided the parent DS TTL is not too long.

Google Public DNS

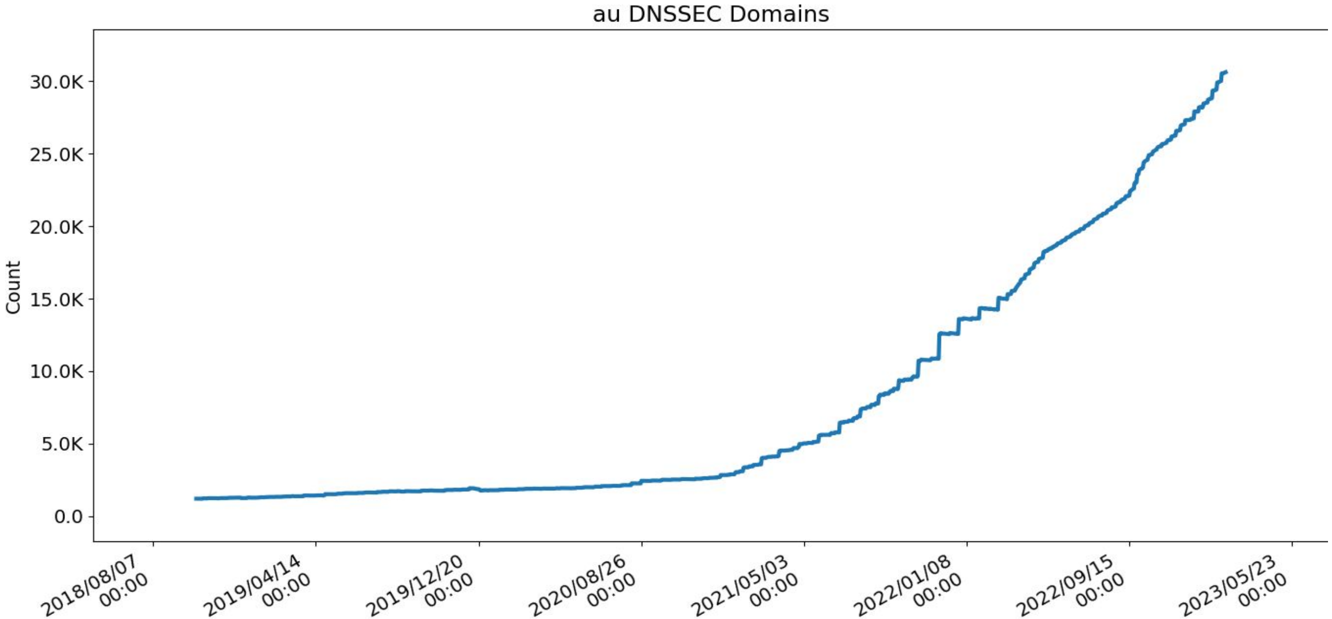
TLD DS TTLs: Top 50 TLDs by signed-delegation count

- Most of top 50 DNSSEC TLDs use 1 hour DS TTLs:
  - **48:00**: 2 TLDs (fr ovh)
  - **24:00**: 12 TLDs (com eu net be pl de hu ca es in me mx)
  - 08:00: 1 TLD (hk)
  - 06:00: 1 TLD (fi)
  - 03:00: 2 TLDs (at it)
  - 02:00: 3 TLDs (dk no biz)
  - **01:00**: 30 TLDs (nl ch br se cz org uk sk nu info dev app …)
  - **00:15**: 1 TLD (au)
- 24 hours+ TTLs extend outage windows and deter adoption
  - Resolvers may cache with a lower TTL, but domain owner can’t rely on this

Public DNS

TLD DS TTLs: Can we (gradually) get to ~10 minutes?

- .AU uses 15 min DS TTLs are only 4x smaller than common 1H TTL
- Many child DNSKEY TTLs will be longer, reducing refresh load on parent
- Can TLDs publish lower DS TTLs 1H (or lower) instead of 24 hours?



Google Public DNS