Does parent delegation NS TTL matter?

Oh, DNS, thee nasty beast, thee at each moment has't ways to hoyday me.

Ondřej Surý • ondrej.sury@nic.cz • 14. 5. 2017

CZ.NIC | SPRÁVCE DOMÉNY CZ

The test subjects

- Knot Resolver 1.3.0-unreleased (lua_peek_rr branch for cache snooping)
- Unbound 1.6.2
- BIND 9.11.1
- PowerDNS Recursor 4.0.4

The test setup

- udp53.cz “TLD” zone
- Matrix of:
  - TTL values <no/low/high/max>
  - Answer minimization <nomin/min>
  - DNSSEC <nodnssec/dnssec>
  - NS Types <in-domain/in-bailiwick/external>
- Zones pattern: parent-ttl-$ttl-$amin-$dnssec-$nstype.udp53.cz.
- Examples:
  - parent-ttl-no-ttl-nomin-nodnssec-in-bailiwick.udp53.cz
  - Parent-ttl-max-ttl-min-dnssec-external.udp53.cz
- Total of 64 zones

The test “script”

- Series of digs and look into the cache:

```
kdig +noall +rec -t A parent-ttl-high-min-nodnssec-external.udp53.cz. -p 53001 @::1
kdig +noall +rec -t AAAA parent-ttl-high-min-nodnssec-external.udp53.cz. -p 53001 @::1
kdig +noall +rec -t MX parent-ttl-high-min-nodnssec-external.udp53.cz. -p 53001 @::1
kdig +noall +rec -t A www.parent-ttl-high-min-nodnssec-external.udp53.cz. -p 53001 @::1
kdig +noall +rec -t AAAA www.parent-ttl-high-min-nodnssec-external.udp53.cz. -p 53001 @::1

kdig +noall +authority +norec -t NS parent-ttl-high-min-nodnssec-external.udp53.cz. -p 53001 @::1
```

- Issue single NS query and look into the cache:

```
kdig +noall +rec -t MX parent-ttl-high-min-nodnssec-external.udp53.cz. -p 53001 @::1

kdig +noall +authority +norec -t NS parent-ttl-high-min-nodnssec-external.udp53.cz. -p 53001 @::1
```

Quirks

- Knot Resolver doesn’t have cache snooping (yet)
  - Check the results via **socat - UNIX-CONNECT:tty/$PID** using this syntax:

```
cache.peek_rr("parent-ttl-max-min-dnssec-external.udp53.cz.", kres.type.NS):tolist()
[1] => {
    [owner] => "parent-ttl-max-min-dnssec-external\5udp53\2cz\0
    [ttl] => 18000
}
[2] => {
    [owner] => "parent-ttl-max-min-dnssec-external\5udp53\2cz\0
    [ttl] => 18000
}
```

What has effect on DNS server behaviour?

	Child TTL	DNSSEC	Answer Minimization	Type of delegation	Direct NS query
Knot Resolver	No	No	**Yes**	No	Yes
Unbound	No	No	**Yes**	No	Yes
BIND	**Yes, ignores child NS TTL > parent TTL**	**Yes, ignores unsigned child NS**	**Yes**	No	Yes
PowerDNS	No	No	**Yes**	No	**No**

Answer minimization effects on DNS caching

- When used in the parent zone
  - No effect on caches
  - **Effect on response size (+++)**
- When used in the child zone
  - **NS RRSet TTL might never be updated (---)**

Does parent delegation NS TTL matter?

Maybe?

Conclusions (for most DNS resolvers)

- Minimum effect on existing domain names
  - Child NS TTL overrides parent NS TTL
  - But answer minimization removes that effect
- Parent TTL has a big impact on:
  - Non-existing domain names (negative caching)
  - When error is made (positive caching)

Recommendations

- DNS Resolvers
    - Update TTL from child even if longer
        - But have a default maximum TTL to prevent GHOST domains (day or week)
    - **Update NS from child after serving the client**
        - Ummm, “post-prefetching”?
- Child zones DNS Operators
    - Enable answer minimization if you care about traffic (DDoS vectors)
    - Disable answer minimization if you care about caches and your NS TTL
- Parent zones DNS Operators (TLDs)
    - Parent NS TTL should be as low as reasonable (~= zone generation interval);
    - Or parent NS TTL should be configurable and kept in sync with child NS TTL
    - Implement RFC7477 – Child-to-Parent Synchronization in DNS

https://github.com/oerdnj/parent-ttl

Questions?

Comments?

Pull Requests?

Ondřej Surý • ondrej.sury@nic.cz • 14. 5. 2017