Catalog zones: progress and difficulties

https://tools.ietf.org/html/draft-toorop-dnsop-dns-catalog-zones

Libor Peltan • **libor.peltan@nic.cz** • **2021-03-11**
Peter van Dijk
Ondřej Surý
Willem Toorop
Leo Vandewoestijne

Catalog zones

- Sync configuration primary -> secondaries
  - Mostly list of zones

- Fake or generated zone + XFR

Draft-Muks (2016)

- Configuration file encoded in DNS zone

- Bind9, PowerDNS (external, partial)

Draft-Toorop (2020)

- Just list of member zones

- No configuration in catz

- Knot DNS 3.0

Draft-Toorop (2020): Member configuration

```
version.$CATZ 0 IN TXT "2"
<unique-1>.zones.$CATZ 0 IN PTR example.com.
<unique-2>.zones.$CATZ 0 IN PTR example.net.
<unique-3>.zones.$CATZ 0 IN PTR example.org.
```

- More config groups => more catalog zones

Draft-Toorop (2020): Member transfer

- Unsynchronized XFR of two catalog zones

- Difficult to implement

- Difficult to operate

- Takes two steps

Draft-Toorop (2020): Additional requirement

- Control over member transfer at origin catz

Outcome: member properties

- Configuration group

- Member SOA serial

- Change-of-ownership (coo)

Outcome: member properties

```
        <unique-1>.zones.$CATZ IN PTR   member.com.
  group.<unique-1>.zones.$CATZ IN TXT   "configgroup"
 serial.<unique-1>.zones.$CATZ IN CSYNC 1614769374 0
    coo.<unique-1>.zones.$CATZ IN PTR   another.catalog.
```

Configuration groups

- Several within one catalog zone

- Atomic switch

- Avoids the need to have multiple catzones (for most use-cases)

```
<unique-1>.zones.$CATZ       0 IN PTR example.org.
group.<unique-1>.zones.$CATZ  0 IN TXT sign-with-nsec3
<unique-2>.zones.$CATZ       0 IN PTR example.net.
group.<unique-2>.zones.$CATZ  0 IN TXT nodnssec
```

Member SOA serial

- More efficient signaling of member zone updates to secondary

- Can avoid lots of SOA queries

- Puts primary in control of synchronisation

```
serial.<unique-1>.zones.$CATZ IN CSYNC 1614769374 0
```

Change of ownership

- If you drop a zone from a catalog, another catalog might pick it up, but which one?

- `coo` property allows admin to decide where a zone goes

- `coo` property points to target catalog zone using `PTR`

```
coo.<unique-1>.zones.$CATZ IN PTR   another.catalog.
```

Open questions

- Should the unique ID for a zone be predictable? This would allow direct lookups into catalog zones. May enable future use cases.

- Serial signaling: `TXT`? `CSYNC`? A new `SERIAL` rrtype?

- Operators, please tell us if the current draft version (messy as it is), seems viable to you.