

Generalized DNS Notifications

John Levine | ICANN 80 Kigali



We've been here before

- Secondary name servers AXFR zones from primary
- Query SOA, has something changed?
- Frequent polling is inefficient
- Infrequent polling means stale data
- NOTIFY(SOA) provokes a poll
- Parent name servers use CDS or CSYNC records from child
- Query CDS/CSYNC, has something changed?
- Frequent polling is inefficient
- Infrequent polling means stale data
- Gosh, what can we do?

Generalized notify

- RFC 1996 defined NOTIFY message in a general way
- RRTYPE in message says what kind of notification, currently only SOA
- Now add CDS and CSYNC to say child has new CDS or CSYNC

Where to send the notification?

- SOA notifies originally went from primary to secondaries
- But hidden servers mean they often go other places
- Configuration is generally manual
- Can we do better for CDS or CSYNC?

Where to send the notification?

- General case: parent?
- TLDs
 - Parent name server?
 - Registrar?
 - Registry?
- Maybe they want different kind of notifications, e.g. API

DSYNC record

- DSYNC in parent says where to notify
- Notification type (CDS or CSYNC)
- Scheme (1 for NOTIFY, 2 for ...)
- Port (5301 or 5302 here)
- Target DNS name

```
_dsync.parent. IN SOA ...  
IN DSYNC CDS 1 5301 nfy.parent.  
IN DSYNC CSYNC 1 5302 nfy.parent.
```

Many DSYNC records

- In RRR model, how to notify registrar?
- DSYNC record per child?
 - That's a lot of new records
 - Will registrars want to do that?
- Wildcard for default
 - Wildcards in TLDs? Stunt DNS servers?
- Hybrid: specific name, else parent name
 - Two queries, but not very often

```
_dsync.parent. IN SOA ...  
IN DSYNC CDS 1 5301 nfy.parent.
```

```
child._dsync.parent  
IN DSYNC CDS 1 5301 nfy.registrar.
```

```
*._dsync.parent  
IN DSYNC CDS 1 5301 nfy.registry.
```

How will this work with RRR?

- DSYNC port number: notifications sent to a service, not just name server
- Registrar notified, uses EPP to update registry?
- Registry notified, uses EPP to tell registrar to check?
- Something else?
- Changes to contracts, EPP, zone content rules, may be hard
- Authors are not all totally happy with this

Security model

- NOTIFY is just a hint to parent to query
- Responses to CDS and CSYNC queries are DNSSEC signed
- Parent could scan anyway, no changes to security model
- Junk NOTIFY could be DoS
 - Rate limit to ignore them, but then they could prevent the update ...

Status of proposal

- Active draft in IETF DNSOP working group
 - draft-ietf-dnsop-generalized-notify-01
- Close to last call, could be published later this year
- Working code
 - <https://github.com/johanix/tdns>
 - <https://github.com/johanix/gen-notify-test>

Loose ends

- Put the whole update in the NOTIFY packet? Or use UPDATE?
 - Could include signed records+DNSKEY
- Related draft in DNSOP could use NOTIFY(DS)
 - Automatic DNSSEC Bootstrapping using Authenticated Signals from the Zone's Operator
 - `draft-ietf-dnsop-dnssec-bootstrapping-10`
- Who can send NOTIFY?
 - NOTIFY(SOA) often only allowed from primary or hand managed list
- Multiple signers
 - Use DSYNC per NS so they can coordinate?

Generalized DNS Notifications

John Levine | ICANN 80 Kigali

