Misguided Warnings of DNS Checker Tools

Peter Thomassen <peter@desec.io>

ICANN81 – SSAC Lightning Talk
November 12, 2024

DNS Replication 101

– – –

- Default mode
  - Secondaries check SOA serial every REFRESH seconds
  - When check fails, try again after RETRY seconds
  - Drop zone if you haven't heard anything for EXPIRE seconds
- deSEC: 15 PoPs, ~50k zones, ~1s reaction time
  → SOA queries at 750 kqps – tough!
- Improve by using NOTIFY to each PoP, and set REFRESH to 60
  - 12,500 SOA qps when primary is unreachable
  - Does not cater for zone removal!
  - Blows up Thursdays 12:00am UTC (when PowerDNS bumps serial and serves new signatures)

deSEC Replication 101

nslord (signer) → nsmaster (hidden master) → secondaries
HTTPS server → API server ↗

- Orange components in VPN (UDP, and ensure that tunneled traffic is TCP)
- Use IP multicast to NOTIFY secondaries
- Every minute, secondaries fetch https://desec.io/api/v1/serials/ (VPN-only)
  - Returns JSON array, mapping zone names and serials (in memcache for 60s)
  - Allows catching missed NOTIFYs, and zone addition/deletion
- Set REFRESH to 86400 → smear out resigning (only affects nslord↔nsmaster!)
- Set RETRY to 3600 → catch up on resigning when signer was unavailable
- Set EXPIRE = 4w > RRSIG expiration window – never else drop a zone!

Facing Reality (deSEC forum post, 10/2022)

– – –

DENIC Predelegation Check (spec, Section 2.1.4)

- RETRY: “The value SHOULD be in range of [900,28800] seconds AND SHOULD be a fractional part between 1/8 and 1/3 of Refresh.”
- Our REFRESH is 86400 → DENIC likes RETRY in range [10800, 28800]

RIPE Recommendation: RETRY = 7200, and indeed REFRESH = 86400 ⚡

- Trying to combine: RETRY = 7200, REFRESH in [21600, 57600] (6–16h)
- But we wanted to smear resigning across the whole day!

(RFC 1912 also has guidance, according to which all our values are fine.)

More SOA Fun

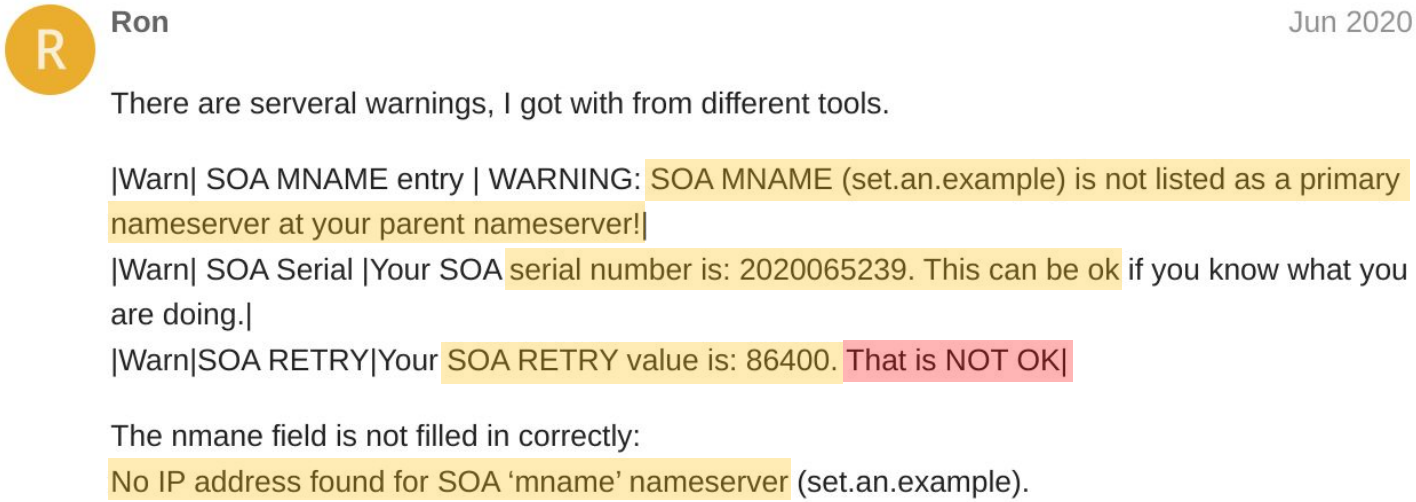
- What are good things to put in MNAME?
  - “the name server that was the original or primary source of data for this zone” (RFC 1035)
  - Might or might not be reachable (hidden, see RFC 2136 Section 4.3)
- And RNAME?
  - zonemaster email
- deSEC: `IN SOA set.an.example. get.desec.io. 0 86400 …`
- Perfectly valid!
  - You can actually send email to get@desec.io
  - Also, when entering get.desec.io in a browser, redirects to main page

Facing Reality (deSEC forum post, 2020)

– – –

- “The mname points normally to the primary name server [...]”
  - Yes? It’s a great easter egg!
  - If anything, such things should be warnings, not errors
- ”According to RFC 2606 is “.example” a reserved top-level domain.”
  - Perfect! It can’t interfere with anything!
  - Also, which “better” value should we put? Some random host?
- “for […] Zonemaster, this is not fully compliant.”
- “many of those checkertools [...] are not exactly happy with “set.an.example” and seem to lack the sense of humor required these days”

Reality Continued (other forum post, 2020)



Ron — Jun 2020

There are serveral warnings, I got with from different tools.

|Warn| SOA MNAME entry | WARNING: SOA MNAME (set.an.example) is not listed as a primary nameserver at your parent nameserver!|
|Warn| SOA Serial |Your SOA serial number is: 2020065239. This can be ok if you know what you are doing.|
|Warn|SOA RETRY|Your SOA RETRY value is: 86400. That is NOT OK|

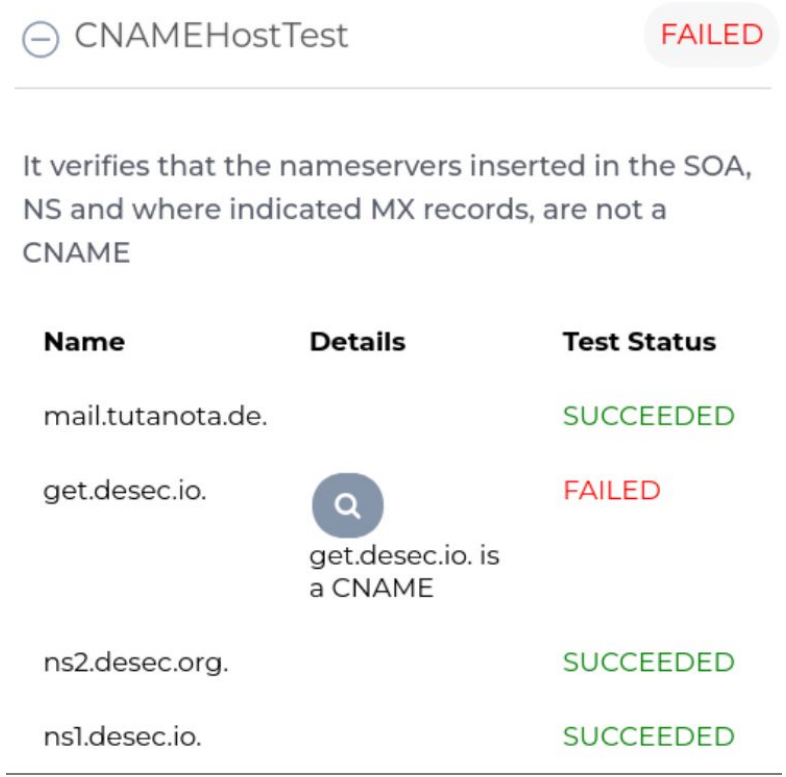
The nmane field is not filled in correctly:
No IP address found for SOA ‘mname’ nameserver (set.an.example).

- ”I wonder, though, how in fact this is supposed to be called an “easter egg” as it sticks out like a sore thumb from any checker-tool report”
  - OK, giving up. It is now: `IN SOA get.desec.io. get.desec.io. 0 86400 …`

SOA Fun the Italian Way

– – –

- NIC.it: CNAMEHostTest FAILED (June 2022)
  - get.desec.io. is a CNAME
  - Parent rejects delegation
- There's no CNAME prohibition for MNAME in RFC 1035
  - MNAME used only by NOTIFY and DNS UPDATE, both don't care
- Anyway, we flattened it …



Serially, MXToolbox? (forum, 10/2024)

Type	Domain Name	IP Address	TTL
NS	ns1.desec.io	45.54.76.1 NetActuate, Inc (AS63911)	60 min
NS	ns2.desec.org	157.53.224.1 NetActuate, Inc (AS36217)	60 min

	Result
✖	Primary Name Server Not Listed At Parent `get.desec.io`
!	SOA Serial Number Format is Invalid `ns1.desec.io reported Serial 2024095870 : Serial day was 58 which is invalid.`
!	SOA Refresh Value is outside of the recommended range `ns1.desec.io reported Refresh 86400 : Refresh is recommended to be between 1200 and 43200.`

Thank you!

… also to our supporter

SSE

Questions?