Measurement of CDS/CDNSKEY inconsistencies

IETF 119 DNSOP
March 22, 2024

Peter Thomassen
How inconsistent are CDS/CDNSKEY across auths?

- Asking a single nameserver does not ensure consistency
  - This can go seriously wrong
  - Example failure modes: multi-homing, provider change, lame delegation hijack
  - In multi-provider setups: each party is a single point of failure

→ draft-ietf-dnsop-cds-consistency proposes consistency check before acting

- How about measuring prevalence of this?

- Max Planck researchers F. Steurer and T. Fiebig collected CDS/CDNSKEY
  - ~300M eTLD+1 domains

- Asked each authoritative NS for both RRsets
  - Both parent and child side NS
Basic Insights

● How to classify unreachable NS?
  ○ draft-ietf-dnsop-cds-consistency assumes consistency (after retries)
    → treat similarly for this study

Number of zones (1–5% have timeouts for some NS):
● 8.4M with CDS
● 1.3M with CDNSKEY

Instances of inconsistent RRset content across NS (including empty, ignoring TTL):
● 6886 for CDS = 0.08%
● 853 for CDNSKEY = 0.07%
  → Around 1/1000 of zones have inconsistent CDS/CDNSKEY records
Case Study: $redacted.ch

$ dig +noall +auth @a.nic.ch. $redacted.ch. NS
$redacted.ch. 3600IN NS ns1.$redactedNS1. ; and ns2
$redacted.ch. 3600IN NS ns1.$redactedNS2. ; and ns2

$ dig +short @ns1.$redactedNS1. $redacted.ch. CDS
3714 13 2 6EF464A4FBA7A432CCCF84FE1253BE4144DF438D99AC1D3292434507...
3714 13 4 E3F6D5992515F46BAB55CC362F3137F35F9ED00F18A582DC5CEDD62A...

$ dig +short @ns1.$redactedNS1. $redacted.ch. CDNSKEY
257 3 13 /JFSTlxQo8av9zzv4qmbhj3lQwfXR9zGZ2HVBCjIk+7Z+2rh2cyW1L2A...

$ dig +short @ns1.$redactedNS2. $redacted.ch. CDS
19170 13 2 0467ACE2E19997D180EC0B4CC0747E637FB6CD32F8D36B65EBEBBC2A...
19170 13 4 ED4F2E45477F18FCBDCE9486FBEDB8784078C5B918BC27535E485737...

$ dig +short @ns1.$redactedNS2. $redacted.ch. CDNSKEY
257 3 13 KiTFHfBpLEkRwkNrc6IJKAP5Zoo8vB8Ubm0vCQac77ZN7V+h/Z6mf8fRl...
Case Study: $redacted.ch

- .ch performs CDS processing ([https://www.nic.ch/security/cds/](https://www.nic.ch/security/cds/))
Case Study: $redacted.ch

- .ch performs CDS processing (https://www.nic.ch/security/cds/)

$ dig +short $redacted.ch. DS

3714 13 2 6EF464A4FBA7A432CCCF84FE1253BE4144DF438D99AC1D3292434507...
3714 13 4 E3F6D5992515F46BAB55CC362F3137F35F9ED00F18A582DC5CEDD62A...

![Diagram showing DNSKEY records](image-url)
Case Study: $redacted.com

$ dig +noall +auth @d.gtld-servers.net. $redacted.com NS

$ dig +short @ns-cloud-b2.googledomains.com. $redacted.com CDS 44854 8 2 D8747EE52247BFF70061DCC4941214316935426D186D478A24A2EBBB...
$ dig +short @ns-cloud-b3.googledomains.com. $redacted.com CDS 44854 8 2 D8747EE52247BFF70061DCC4941214316935426D186D478A24A2EBBB...
$ dig +short @ns-cloud-b4.googledomains.com. $redacted.com CDS 44854 8 2 D8747EE52247BFF70061DCC4941214316935426D186D478A24A2EBBB...
$ dig +short @ns-cloud-a1.googledomains.com. $redacted.com CDS 32551 8 2 7F72E32B74402ABB68954FCF5A98E329A0D0D559B864ED1399E92CA8...
More Insights

● 90-95% of cross-NS inconsistencies are because one NS serves empty
● 402 instances of all-nonempty inconsistent CDS remaining
● 248 of those are with Google Domains & WixDNS
  ○ All kinds of anomalies observed (e.g., WixDNS in parent, Google Domains in child)
  ○ Similar observations with other provider combinations
● Usually not true multi-signer setups (no KSK exchange)
● Usually not even securely delegated
Conclusion

- Weird misconfigurations happen at both small and large DNS operators!
- Significant number of domains breaks without proper DS acceptance checks
  - This includes CDS/CDNSKEY consistency checks
- Automated DS provisioning should not tolerate 0.1% failure rate