DNSSEC for .nz: post-incident recovery and improvement

Or, how to see the train coming down the tunnel. Next time, for sure.

internetnz

Topics in this talk

- A summary of our DNSSEC incident in May 2023
- Our road to recovery
- Increasing our awareness: new monitoring features

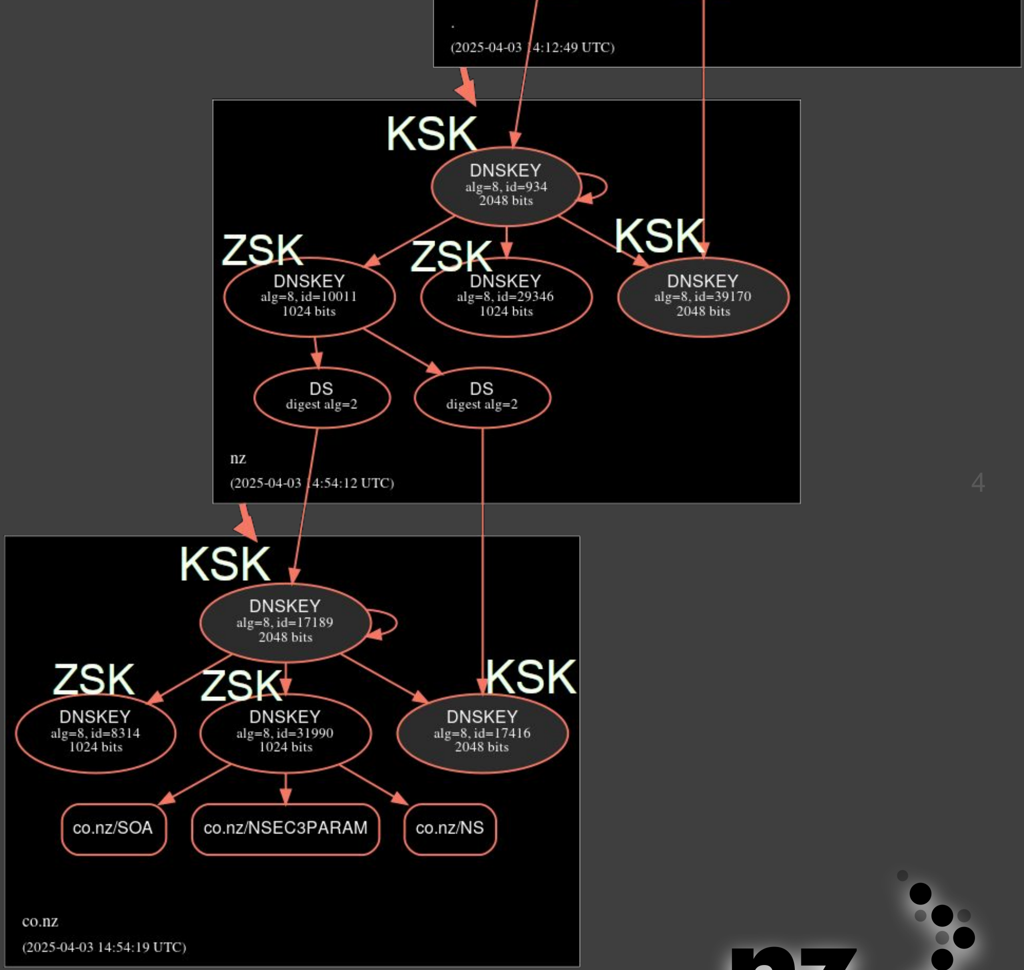
A question

Who actually knows *exactly* what their DNS servers are doing?

Not only right now, but in the past too!

Terminology

- KSK: key-signing key pair
- ZSK: zone-signing key pair
- DNSKEY: the public key half of either a KSK pair or a ZSK pair
- DS: a one-way hash of a DNSKEY
- RRSIG: a cryptographic signature
- Authoritative DNS
- Recursive DNS

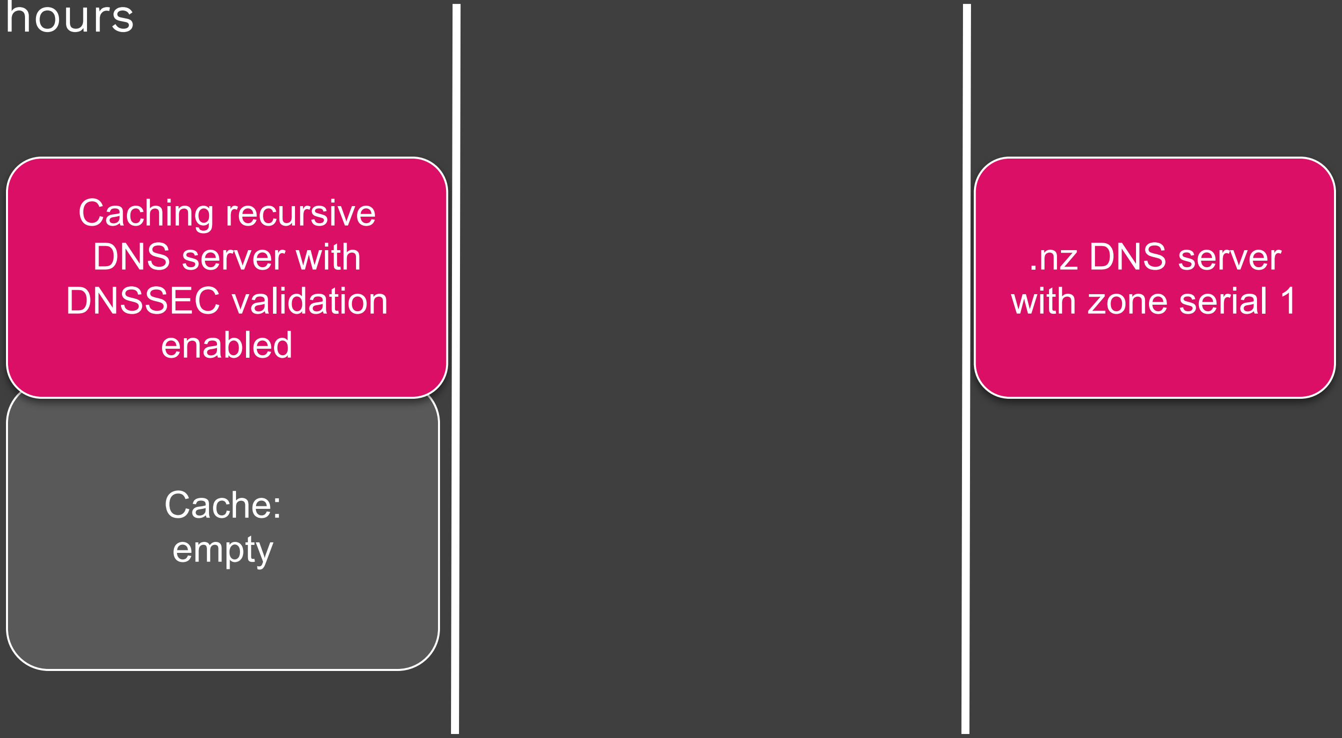


Our .nz DNSSEC incident

- ...has been covered in detail before: a report is available
- In May 2023, many caching recursive servers were unable to validate .nz DNS records, most of those for several hours, but possibly up to two days

The core of the problem, part 1

- T -2 hours



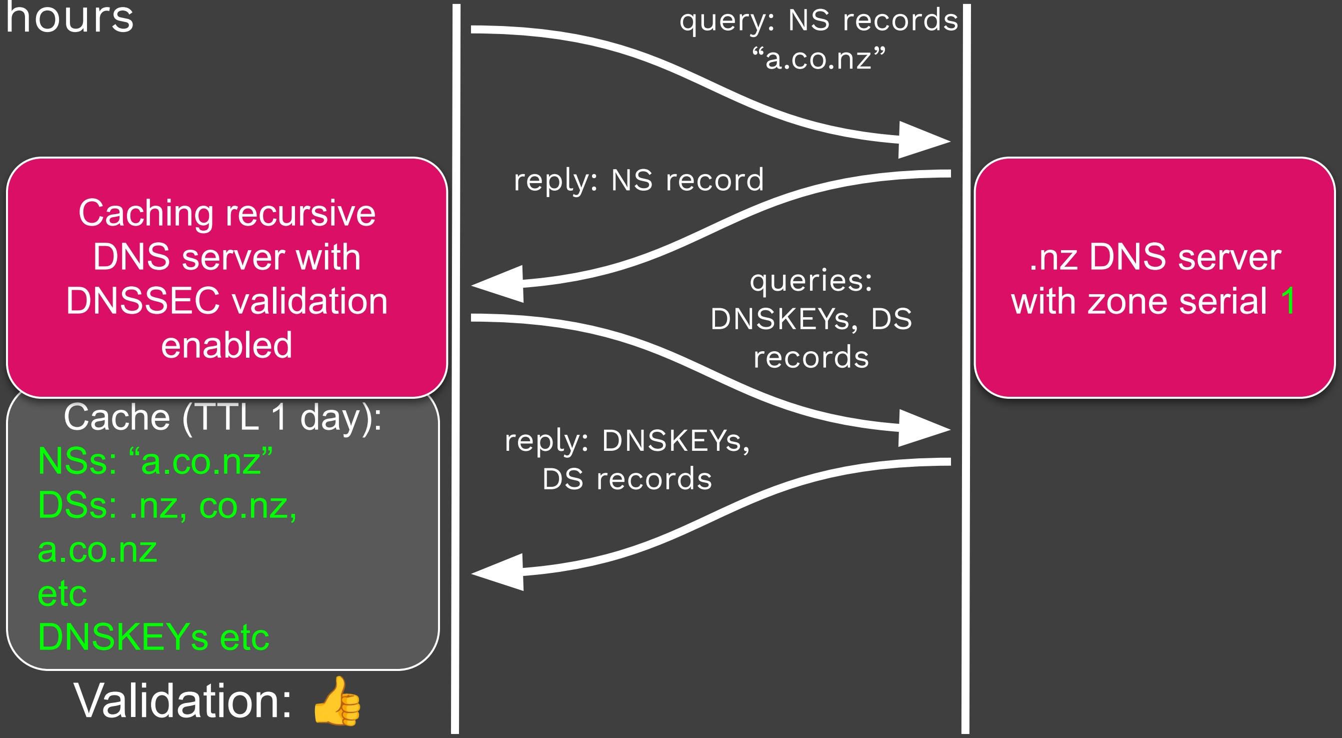
Caching recursive DNS server with DNSSEC validation enabled

Cache: empty

.nz DNS server with zone serial 1

The core of the problem, part 2

- T -2 hours



Caching recursive DNS server with DNSSEC validation enabled

Cache (TTL 1 day):
NSs: “a.co.nz”
DSs: .nz, co.nz, a.co.nz
etc
DNSKEYs etc

Validation: 👍

query: NS records “a.co.nz”

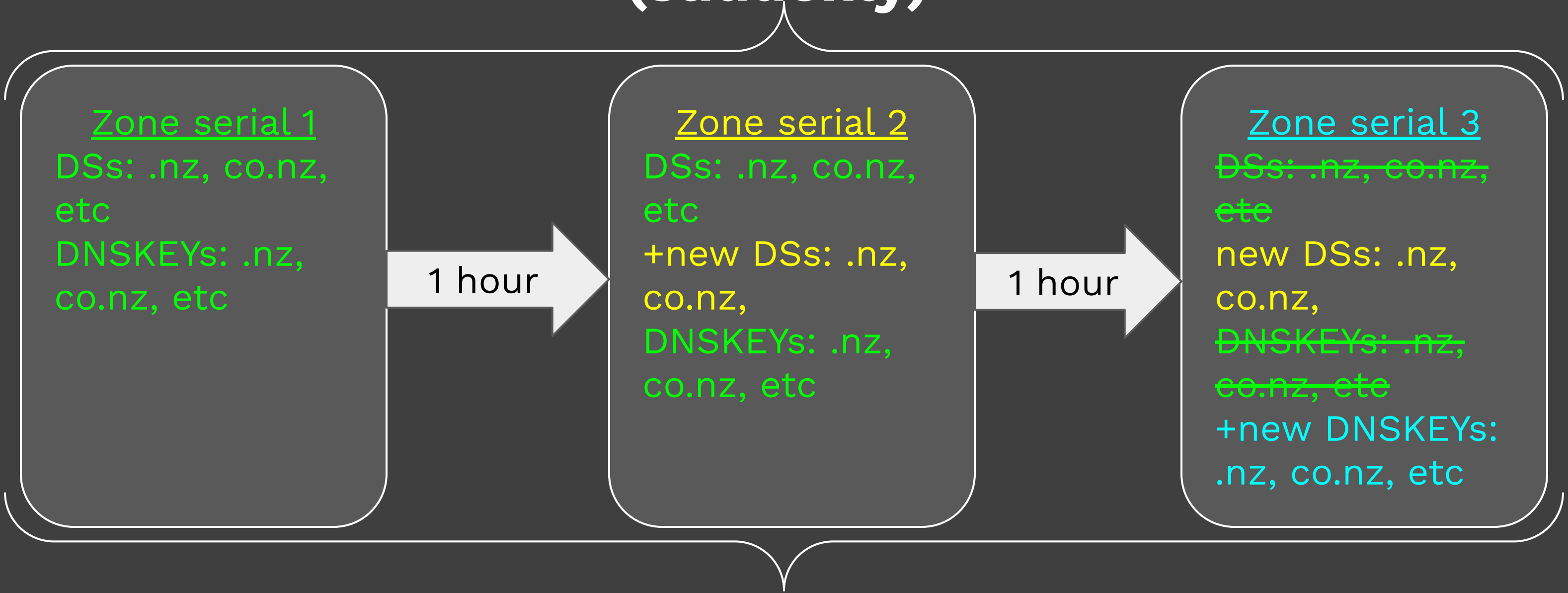
reply: NS record

queries: DNSKEYs, DS records

reply: DNSKEYs, DS records

.nz DNS server with zone serial 1

But then...
(suddenly)



Zone serial 1

DSs: .nz, co.nz, etc

DNSKEYs: .nz, co.nz, etc

1 hour

Zone serial 2

DSs: .nz, co.nz, etc

+new DSs: .nz, co.nz,

DNSKEYs: .nz, co.nz, etc

1 hour

Zone serial 3

~~DSs: .nz, co.nz, etc~~

new DSs: .nz, co.nz,

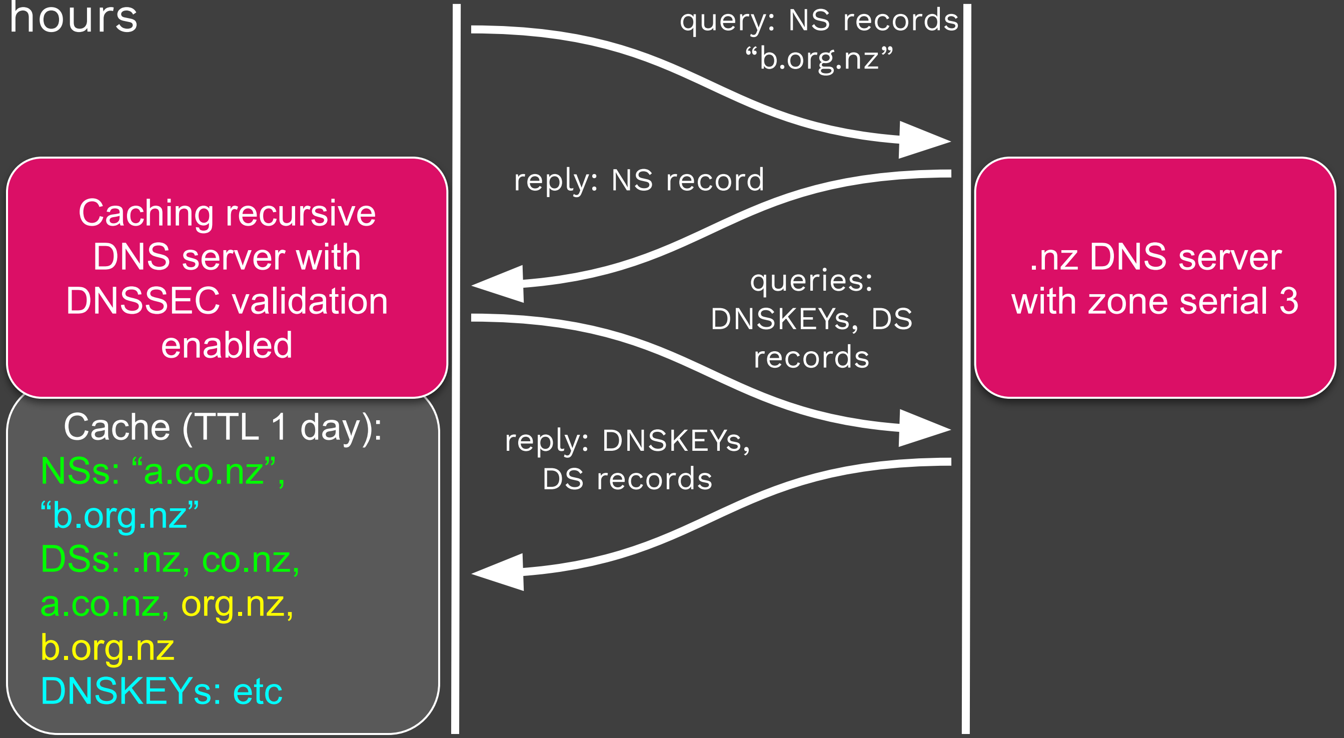
~~DNSKEYs: .nz, co.nz, etc~~

+new DNSKEYs: .nz, co.nz, etc

The keys rolled, and everything changed

The core of the problem, part 3

- T -0 hours



Caching recursive DNS server with DNSSEC validation enabled

Cache (TTL 1 day):
NSs: “a.co.nz”,
“b.org.nz”
DSs: .nz, co.nz,
a.co.nz, org.nz,
b.org.nz
DNSKEYs: etc

query: NS records “b.org.nz”

reply: NS record

queries: DNSKEYs, DS records

reply: DNSKEYs, DS records

.nz DNS server with zone serial 3

Validation: 🥵💩💥

The road to recovery

Two different, connected, and competing, priorities

- “Return to normal operations”
- “The incident must never happen again”

What was the holdup, exactly?

- We needed to establish confidence (which introduces change)
- DNSSEC is… hard

Procedures and processes and tooling

- Previous technical procedures: inadequate
  ⇒ create new procedures that are thoroughly reviewed
- Previous organisational processes: ad-hoc, or nothing at all
  ⇒ create new processes that can be included in our DR plan
- Previous tooling: minimal automation and monitoring
  ⇒ create better automation and a greater monitoring scope

Technical solutions for technical problems

- Procedures and processes are human/social solutions
- But we had a technical problem too, during our incident:
  InternetNZ always produced valid DNS zones
- This was a mismatch of perspective

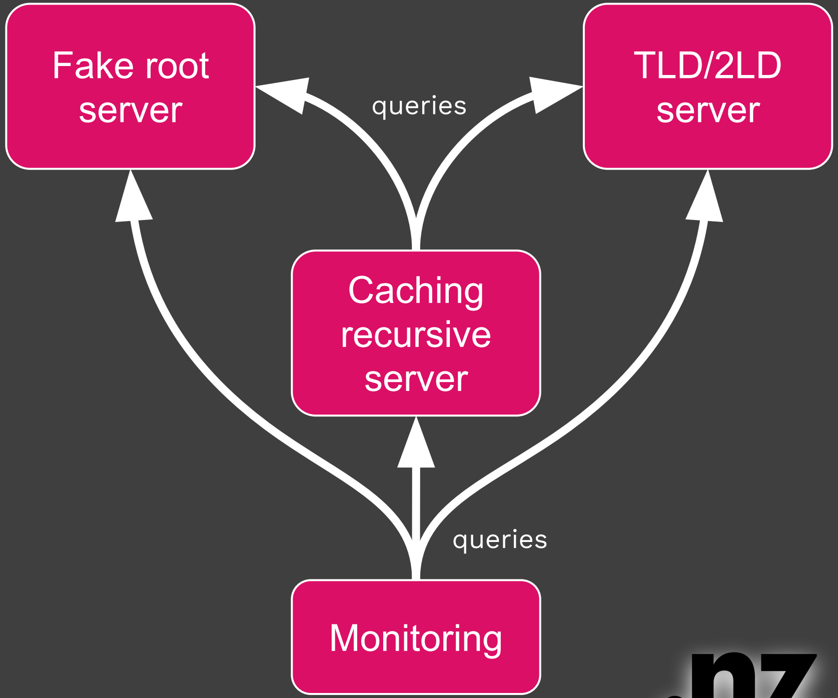
Making progress and increasing awareness

Wait, what about the technical solution?

- “Just run some recursive servers”, we (initially) said
- There is a better way: multiple end-to-end “fake” DNS root instances

Running DNS fake root environments (inspired by SIDN)

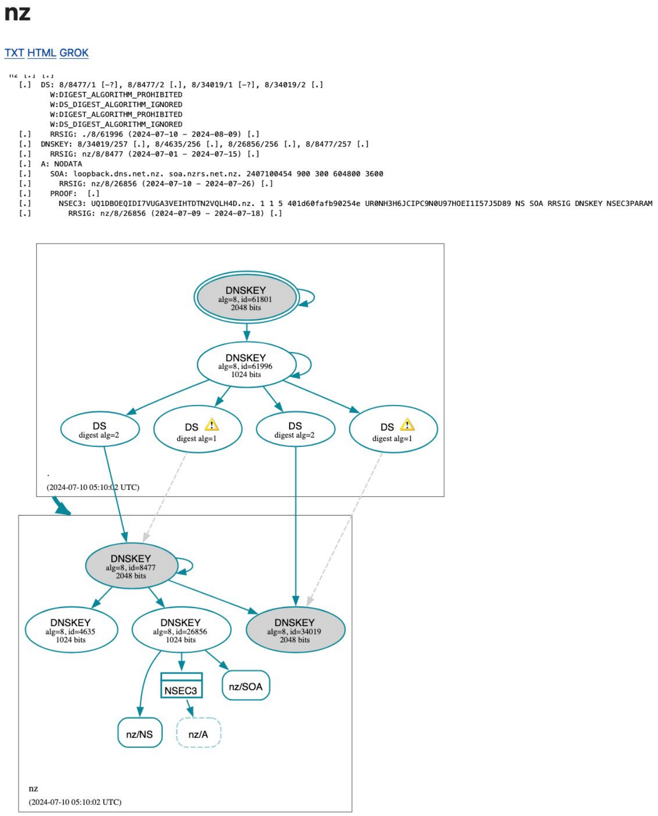
- A VM running containers:
- One DNS fake root (“.”) authoritative server
- One DNS TLD/2LD authoritative server (.nz, etc)
- One DNS caching recursive server



Making use of these DNS fake root environments

- Monitoring and experimenting with:
  - DNSSEC tracing and validation, including internal DNSviz
  - RRSIG expiration and server-reply checks
- A sizeable portion of this is novel work

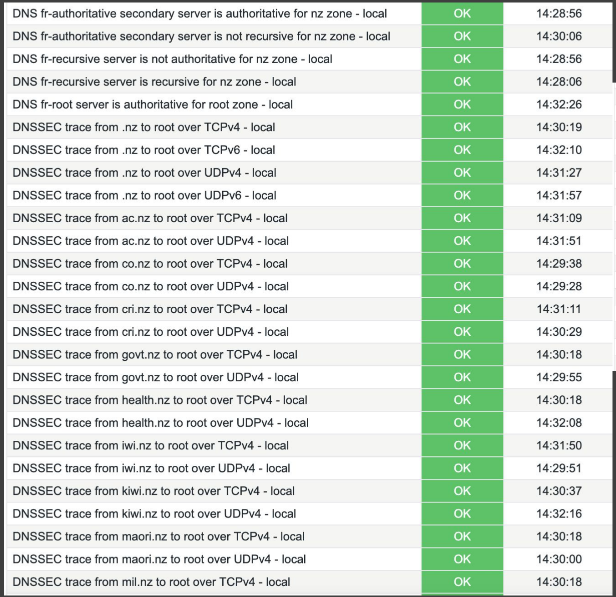
Examples of monitoring in a DNS fake root



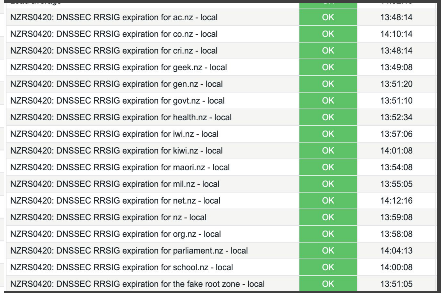
nz

TXT HTML GROK

```
nz [.] [.]
  [.]  DS: 8/8477/1 [-?], 8/8477/2 [.], 8/34019/1 [-?], 8/34019/2 [.]
         W:DIGEST_ALGORITHM_PROHIBITED
         W:DS_DIGEST_ALGORITHM_IGNORED
         W:DIGEST_ALGORITHM_PROHIBITED
         W:DS_DIGEST_ALGORITHM_IGNORED
  [.]    RRSIG: ./8/61996 (2024-07-10 - 2024-08-09) [.]
  [.]  DNSKEY: 8/34019/257 [.], 8/4635/256 [.], 8/26856/256 [.], 8/8477/257 [.]
  [.]    RRSIG: nz/8/8477 (2024-07-01 - 2024-07-15) [.]
  [.]  A: NODATA
  [.]    SOA: loopback.dns.net.nz. soa.nzrs.net.nz. 2407100454 900 300 604800 3600
  [.]      RRSIG: nz/8/26856 (2024-07-10 - 2024-07-26) [.]
  [.]    PROOF:  [.]
  [.]      NSEC3: UQ1DBOEQIDI7VUGA3VEIHTDTN2VQLH4D.nz. 1 1 5 401d60fafb90254e UR0NH3H6JCIPC9N0U97HOEI1I57J5D89 NS SOA RRSIG DNSKEY NSEC3PARAM
  [.]        RRSIG: nz/8/26856 (2024-07-09 - 2024-07-18) [.]
```

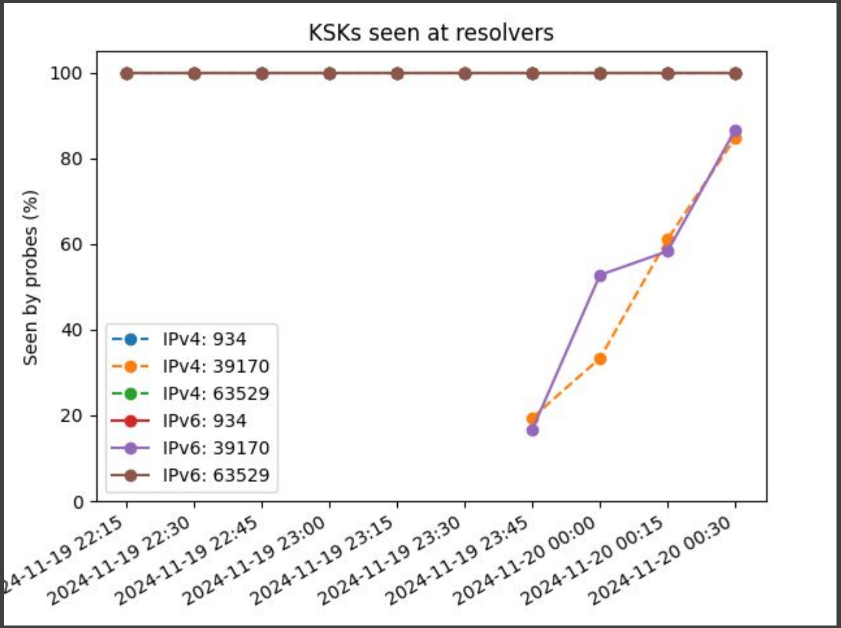


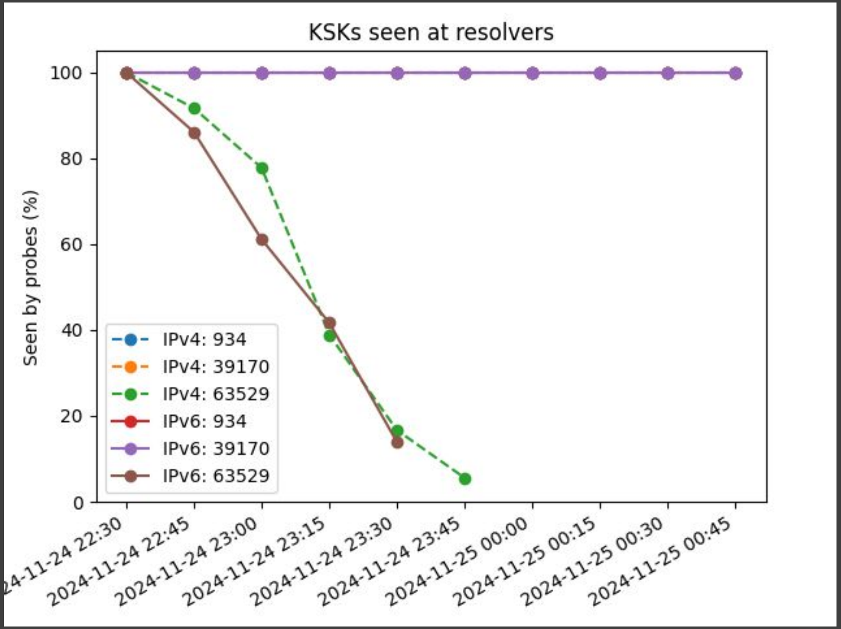
DNS fr-authoritative secondary server is authoritative for nz zone - local	OK	14:28:56
DNS fr-authoritative secondary server is not recursive for nz zone - local	OK	14:30:06
DNS fr-recursive server is not authoritative for nz zone - local	OK	14:28:56
DNS fr-recursive server is recursive for nz zone - local	OK	14:28:06
DNS fr-root server is authoritative for root zone - local	OK	14:32:26
DNSSEC trace from .nz to root over TCPv4 - local	OK	14:30:19
DNSSEC trace from .nz to root over TCPv6 - local	OK	14:32:10
DNSSEC trace from .nz to root over UDPv4 - local	OK	14:31:27
DNSSEC trace from .nz to root over UDPv6 - local	OK	14:31:57
DNSSEC trace from ac.nz to root over TCPv4 - local	OK	14:31:09
DNSSEC trace from ac.nz to root over UDPv4 - local	OK	14:31:51
DNSSEC trace from co.nz to root over TCPv4 - local	OK	14:29:38
DNSSEC trace from co.nz to root over UDPv4 - local	OK	14:29:28
DNSSEC trace from cri.nz to root over TCPv4 - local	OK	14:31:11
DNSSEC trace from cri.nz to root over UDPv4 - local	OK	14:30:29
DNSSEC trace from govt.nz to root over TCPv4 - local	OK	14:30:18
DNSSEC trace from govt.nz to root over UDPv4 - local	OK	14:29:55
DNSSEC trace from health.nz to root over TCPv4 - local	OK	14:30:18
DNSSEC trace from health.nz to root over UDPv4 - local	OK	14:32:08
DNSSEC trace from iwi.nz to root over TCPv4 - local	OK	14:31:50
DNSSEC trace from iwi.nz to root over UDPv4 - local	OK	14:29:51
DNSSEC trace from kiwi.nz to root over TCPv4 - local	OK	14:30:37
DNSSEC trace from kiwi.nz to root over UDPv4 - local	OK	14:32:16
DNSSEC trace from maori.nz to root over TCPv4 - local	OK	14:30:18
DNSSEC trace from maori.nz to root over UDPv4 - local	OK	14:30:00
DNSSEC trace from mil.nz to root over TCPv4 - local	OK	14:30:18



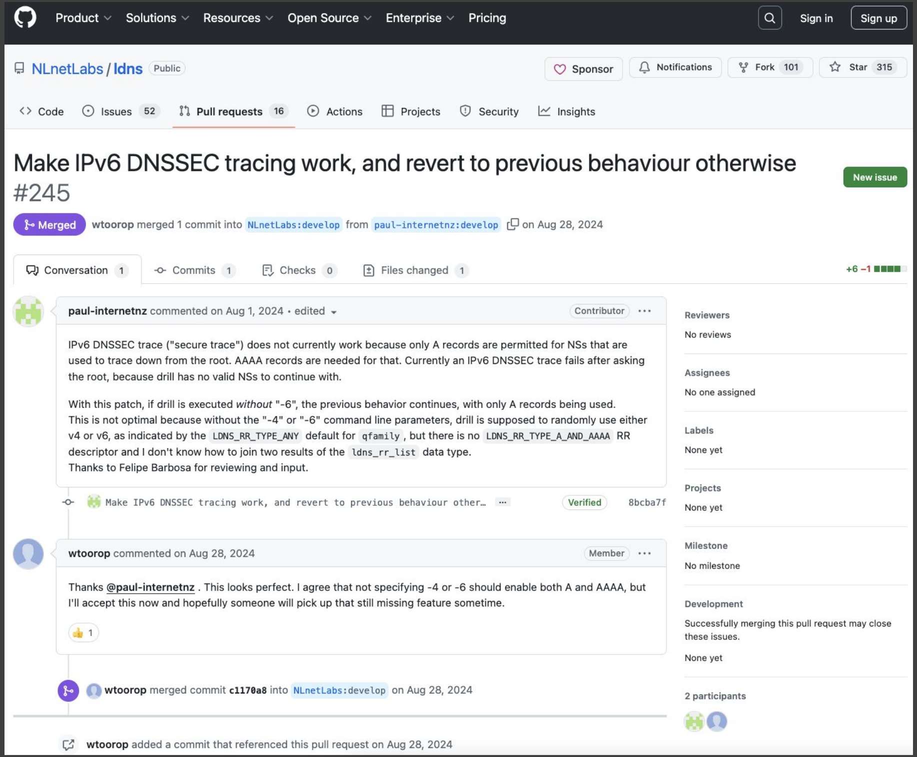
NZRS0420: DNSSEC RRSIG expiration for ac.nz - local	OK	13:48:14
NZRS0420: DNSSEC RRSIG expiration for co.nz - local	OK	14:10:14
NZRS0420: DNSSEC RRSIG expiration for cri.nz - local	OK	13:48:14
NZRS0420: DNSSEC RRSIG expiration for geek.nz - local	OK	13:49:08
NZRS0420: DNSSEC RRSIG expiration for gen.nz - local	OK	13:51:20
NZRS0420: DNSSEC RRSIG expiration for govt.nz - local	OK	13:51:10
NZRS0420: DNSSEC RRSIG expiration for health.nz - local	OK	13:52:34
NZRS0420: DNSSEC RRSIG expiration for iwi.nz - local	OK	13:57:06
NZRS0420: DNSSEC RRSIG expiration for kiwi.nz - local	OK	14:01:08
NZRS0420: DNSSEC RRSIG expiration for maori.nz - local	OK	13:54:08
NZRS0420: DNSSEC RRSIG expiration for mil.nz - local	OK	13:55:05
NZRS0420: DNSSEC RRSIG expiration for net.nz - local	OK	14:12:16
NZRS0420: DNSSEC RRSIG expiration for nz - local	OK	13:59:08
NZRS0420: DNSSEC RRSIG expiration for org.nz - local	OK	13:58:08
NZRS0420: DNSSEC RRSIG expiration for parliament.nz - local	OK	14:04:13
NZRS0420: DNSSEC RRSIG expiration for school.nz - local	OK	14:00:08
NZRS0420: DNSSEC RRSIG expiration for the fake root zone - local	OK	13:51:05

Examples of monitoring the real .nz





Hitting an old, never-reported bug



Make IPv6 DNSSEC tracing work, and revert to previous behaviour otherwise #245

Merged wtoorop merged 1 commit into `NLnetLabs:develop` from `paul-internetnz:develop` on Aug 28, 2024

paul-internetnz commented on Aug 1, 2024 • edited — Contributor

IPv6 DNSSEC trace ("secure trace") does not currently work because only A records are permitted for NSs that are used to trace down from the root. AAAA records are needed for that. Currently an IPv6 DNSSEC trace fails after asking the root, because drill has no valid NSs to continue with.

With this patch, if drill is executed *without* "-6", the previous behavior continues, with only A records being used. This is not optimal because without the "-4" or "-6" command line parameters, drill is supposed to randomly use either v4 or v6, as indicated by the `LDNS_RR_TYPE_ANY` default for `qfamily`, but there is no `LDNS_RR_TYPE_A_AND_AAAA` RR descriptor and I don't know how to join two results of the `ldns_rr_list` data type.
Thanks to Felipe Barbosa for reviewing and input.

`Make IPv6 DNSSEC tracing work, and revert to previous behaviour other…` Verified 8bcba7f

wtoorop commented on Aug 28, 2024 — Member

Thanks **@paul-internetnz** . This looks perfect. I agree that not specifying -4 or -6 should enable both A and AAAA, but I'll accept this now and hopefully someone will pick up that still missing feature sometime.

👍 1

wtoorop merged commit **c1170a8** into `NLnetLabs:develop` on Aug 28, 2024

wtoorop added a commit that referenced this pull request on Aug 28, 2024

Reviewers
No reviews

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
Successfully merging this pull request may close these issues.
None yet

2 participants

- “drill” from the LDNS software project could never do DNSSEC tracing over IPv6

Conclusion

- Pre-incident, we only thought about authoritative DNS
- A large part of our response has been improving our awareness

Questions?