GLOBAL LOCAL ROOT

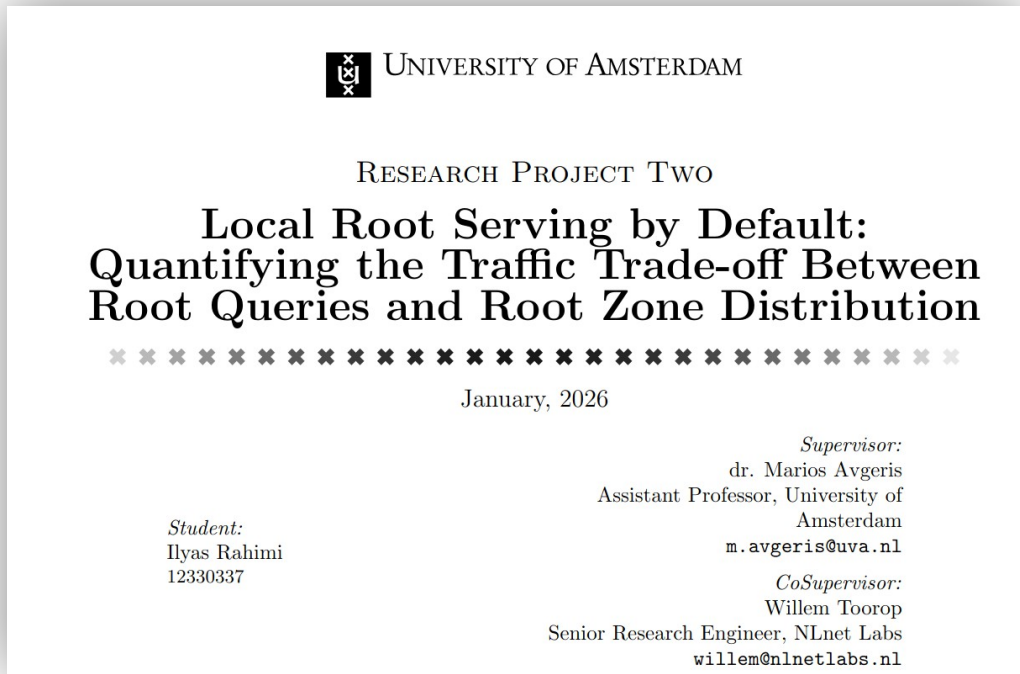
Willem Toorop - NLnet Labs

IEPG @ IETF 125 @ Shenzhen

Sunday 15th of March 2026

Motivation

- draft-wkumari-dnsop-localroot-bcp
- Have the root zone local to the resolver
- How much extra traffic when applied at scale?



University of Amsterdam

Research Project Two

Local Root Serving by Default: Quantifying the Traffic Trade-off Between Root Queries and Root Zone Distribution

January, 2026

Supervisor:
dr. Marios Avgeris
Assistant Professor, University of Amsterdam
m.avgeris@uva.nl

CoSupervisor:
Willem Toorop
Senior Research Engineer, NLnet Labs
willem@nlnetlabs.nl

Student:
Ilyas Rahimi
12330337

Method

- Traffic = bytes transferred per resolver per day
- Setup resolvers à la Appendix A of version -01:
  - BIND transferring the root zone over DNS XFR
  - Unbound transferring the root zone over DNS XFR
  - Unbound transferring the root zone from url[1]
  - Knot Resolver pre-filling cache from url[1]
- Measure traffic between resolver, root and url[1]

1. https://www.internic.net/domain/root.zone

Method – baseline

- Traffic = bytes transferred per resolver per day
- RSSAC002: RSSAC Advisory on Measurements of the Root Server System
- Root Server Operators report metrics, measured at the Root Server Identifier instances
  - The number of sources seen
    - IPv4 and aggregated IPv6
  - The query and response size distribution

Method – baseline

- The query and response size distribution
  - Buckets of size ranges
    - 0-15, 16-31, 32-47, 48-63, 64-79, ..., 4064-4079, 4080-4095, 4096 or greater
  - Number of requests & responses per bucket
  - TCP and UDP

$$\frac{\sum_{bucket} \max(\text{bucket range}) * \text{transactions}}{\text{the number of unique sources seen}}$$

Results - baseline

Table 1: Conventional root traffic per resolver (RSSAC002), MB/day

Day	b	c	d	f	h	i	j	k	l	m
1	0.69	0.71	1.04	11.40	0.88	1.30	1.11	1.06	1.35	0.70
2	0.69	0.72	1.08	11.26	0.90	1.27	1.08	1.04	1.35	0.68
3	0.66	0.70	1.03	10.92	0.86	1.25	1.07	1.02	1.32	0.62
4	0.66	0.70	1.04	10.91	0.85	1.30	1.05	1.07	1.34	0.69
5	0.66	0.70	1.06	11.13	0.88	1.25	1.01	1.07	1.31	0.63
6	0.68	0.71	1.06	11.35	0.89	1.22	0.97	1.06	1.33	0.67
7	0.68	0.72	1.06	11.28	0.90	1.25	0.99	1.10	1.36	0.70
Average	**0.67**	**0.71**	**1.05**	**11.18**	**0.88**	**1.26**	**1.04**	**1.06**	**1.34**	**0.67**

Results

Table 2: BIND local root traffic

Date (2026)	Updates	MB per update	Total MB/day
Jan 20	2	1.45	2.90
Jan 21	3	1.45	4.35
Jan 22	4	1.45	5.80
Jan 23	3	1.45	4.35
Average	–	–	**4.35**

Table 3: Unbound (DNS-based) local root traffic

Date (2026)	Updates	MB per update	Total MB/day
Jan 20	2	1.31	2.62
Jan 21	3	1.31	3.93
Jan 22	4	1.31	5.24
Jan 23	3	1.31	3.93
Average	–	–	**3.93**

Table 4: Unbound (HTTPS-based) local root traffic

Date (2026)	Updates/day	MB per update	Total MB/day
Jan 20	48	2.19	105.12
Jan 21	48	2.19	105.12
Jan 22	48	2.19	105.12
Jan 23	48	2.19	105.12
Average	–	–	**105.12**

Table 5: Knot Resolver local root traffic

Date (2026)	Time (CET)	Data transferred (MB)
Jan 20	12:06	2.69
Jan 21	12:06	2.61
Jan 22	12:06	2.67
Jan 23	12:06	2.65
Average	–	**2.65**

Results

Table 2: BIND local root traffic

Date (2026)	Updates	MB per update	Total MB/day
Jan 20	2	1.45	2.90
Jan 21	3	1.45	4.35
Jan 22	4	1.45	5.80
Jan 23	3	1.45	4.35
Average	–	–	**4.35**

Table 3: Unbound (DNS-based) local root traffic

Date (2026)	Updates	MB per update	Total MB/day
Jan 20	2	1.31	2.62
Jan 21	3	1.31	3.93
Jan 22	4	1.31	5.24
Jan 23	3	1.31	3.93
Average	–	–	**3.93**

Table 4: Unbound (HTTPS-based) local root traffic

Date (2026)	Updates/day	MB per update	Total MB/day
Jan 20	48	2.19	105.12
Jan 21	48	2.19	105.12
Jan 22	48	2.19	105.12
Jan 23	48	2.19	105.12
Average	–	–	**105.12**

Table 5: Knot Resolver local root traffic

Date (2026)	Time (CET)	Data transferred (MB)
Jan 20	12:06	2.69
Jan 21	12:06	2.61
Jan 22	12:06	2.67
Jan 23	12:06	2.65
Average	–	**2.65**

Unbound HTTPS XFR Issue

```
.           86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. (
                2026031200 ; serial
                1800       ; refresh (30 minutes)
                900        ; retry (15 minutes)
                604800     ; expire (1 week)
                86400      ; minimum (1 day)
                )
```

2 × 24 × 2.19 MB = 105.12 MB

- Unbound does not (yet) support
  - `ETag` response header
  - `If-None-Match` request header
- But, https://github.com/NLnetLabs/unbound/pull/1422

Knot resolver updates once a day

- Lowest TTL within the root is 1 day anyway
- SOA is for secondaries, TTL for resolvers
- Lowest TTL in the root zone is 86400 (1 day)
  - 86400 for SOA and DS RRsets
  - 172800 for DNSKEY and non-authoritative NS sets and associated glue
  - 518400 for root NS RRset and associated glue
- So, the root is fine with resolvers having maximally 1 day old data anyway… Right?

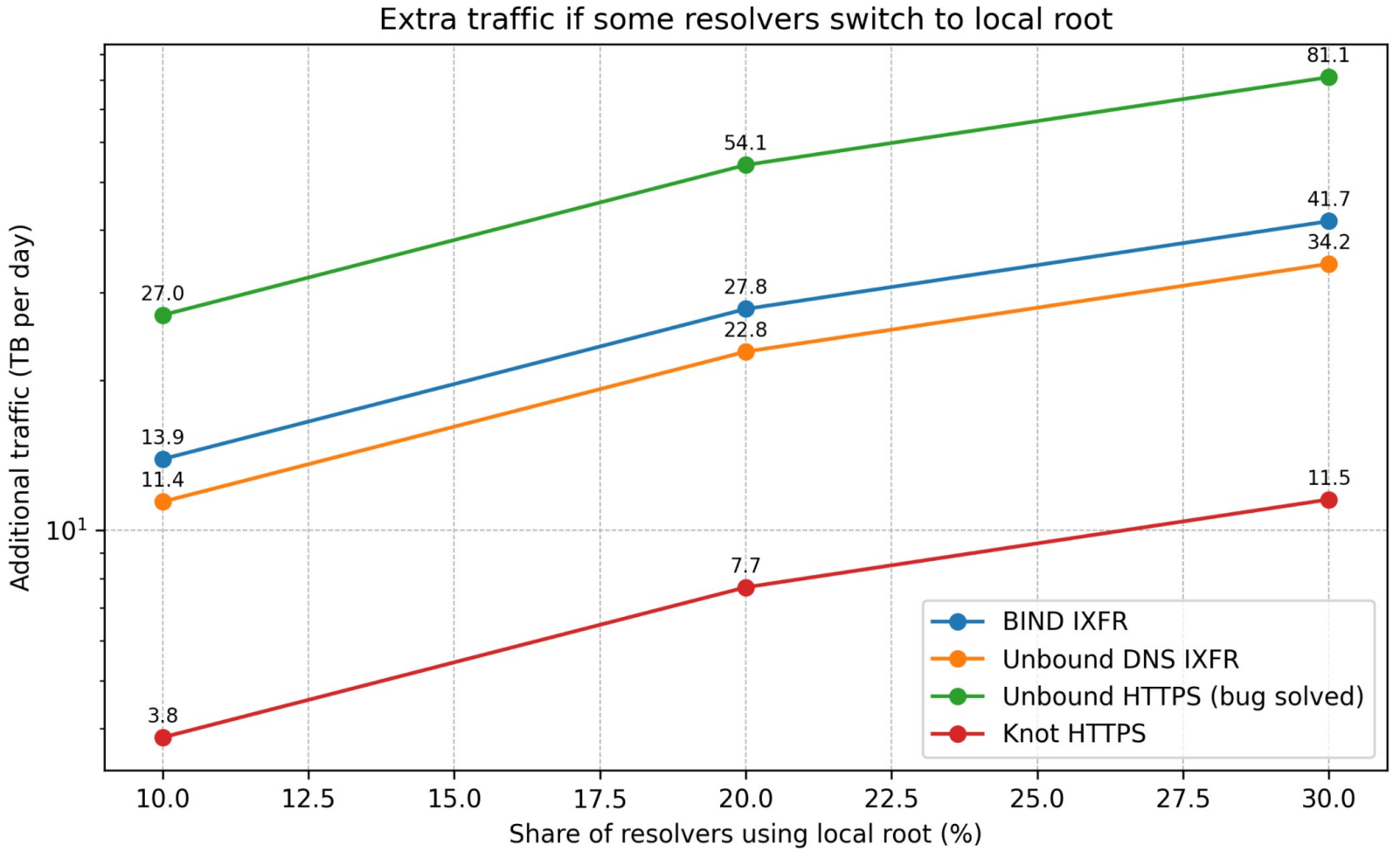


Figure 1: Additional daily traffic under partial deployment of local root resolvers, shown relative to the conventional root query baseline. The values represent total traffic across the entire resolver population in the scenario, rather than per-root-server traffic.

Discussion

- Currently the root is *fully* signed ~2,5 times a day
  - At 4am and 4pm UTC and when changes happen

	XFR size	Daily traffic
Baseline (without F)		0.96 MB
DNS XFR	1.31 MB	3.28 MB
HTTPS XFR	2.19 MB	105.12 MB
HTTPS XFR (bug fixed)	2.19 MB	5.48 MB
HTTPS cache pre-fill	2.19 MB	2.19 MB

Discussion

- Currently the root is *fully* signed ~2,5 times a day
  - At 4am and 4pm UTC and when changes happen
- Fully signed means full transfer always, because 2 * sizeoff(all RRsigs) > sizeoff(whole zone)
- What if it would have been incrementally signed
  - Portion of (oldest) RRsigs is renewed twice a day
  - Only the changes resigned when changes happen

Incrementally signed root

- RRSIG lifetime must be longer then SOA expire

  [Section 4.3.4 of RFC 6781]

- All (except 1) RRSIGs have 13 days and 1 hour
  - Exception is the KSK DNSKEY RRSIG which lives for 21 days
-
```
86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. (
    2026031200 ; serial
    1800       ; refresh (30 minutes)
    900        ; retry (15 minutes)
    604800     ; expire (1 week)
    86400      ; minimum (1 day)
    )
```

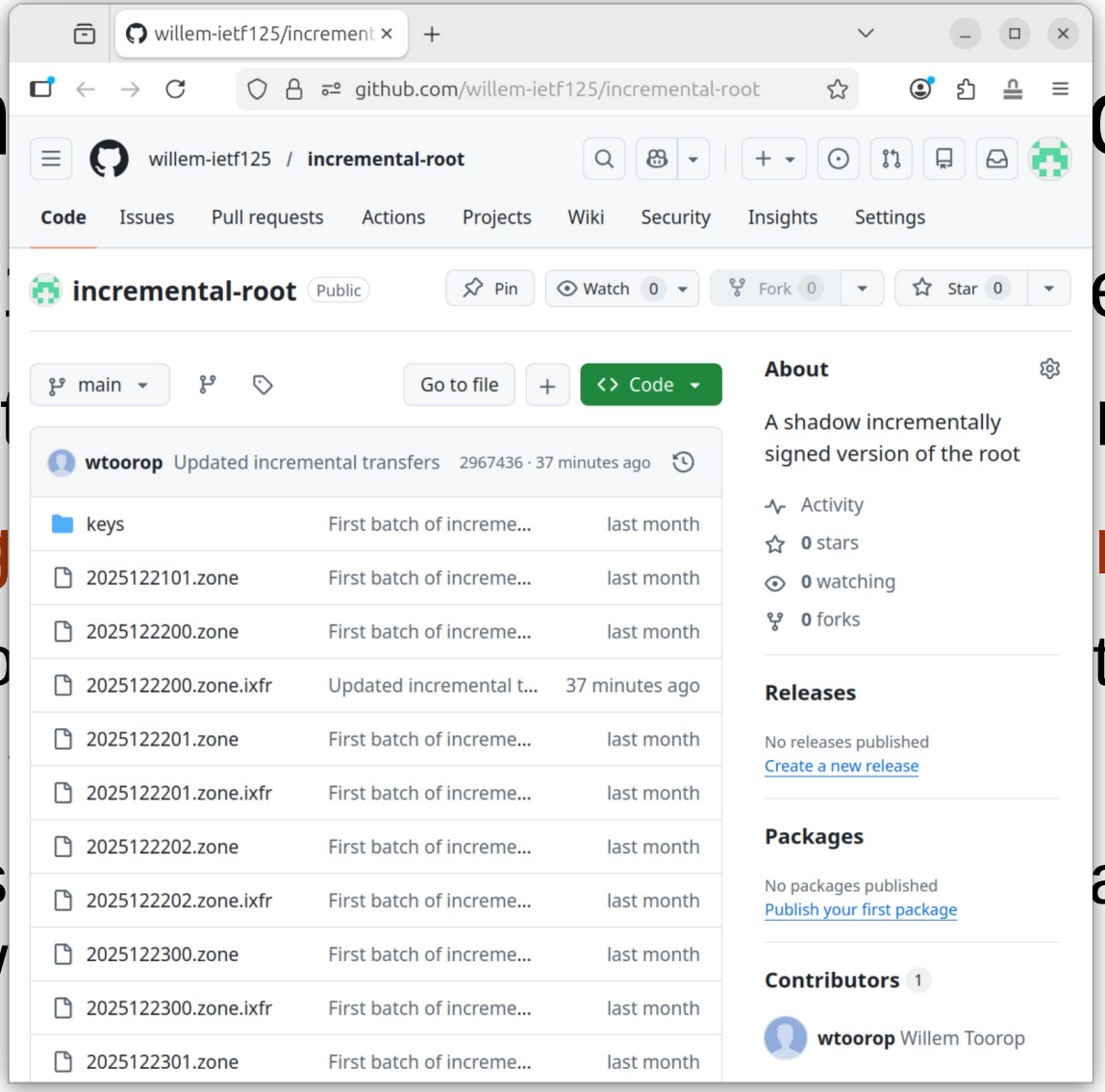
- Fresh RRSIG at least every 13 – 7 = 6 days

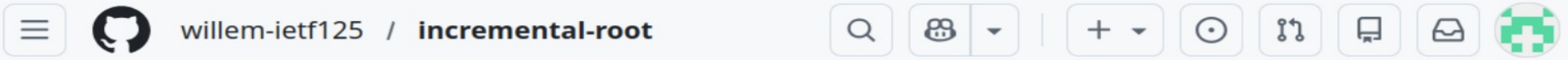
Incrementally signed root

- Resign 1/12th of the oldest RRSIGs twice a day
- Resign the changes when they happen
- https://github.com/willem-ietf125/incremental-root
  - Shadow incrementally signed version of the root zone
  - All versions since 22nd of December 2025
  - IXFRs from version to version in presentation format with wire format size in comment

In ot

- Resign e a day
- Resign n
- https://g mental-root
  - Shado the root zone
  - Since
  - IXFRs ation format with w





willem-ietf125 / **incremental-root**

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

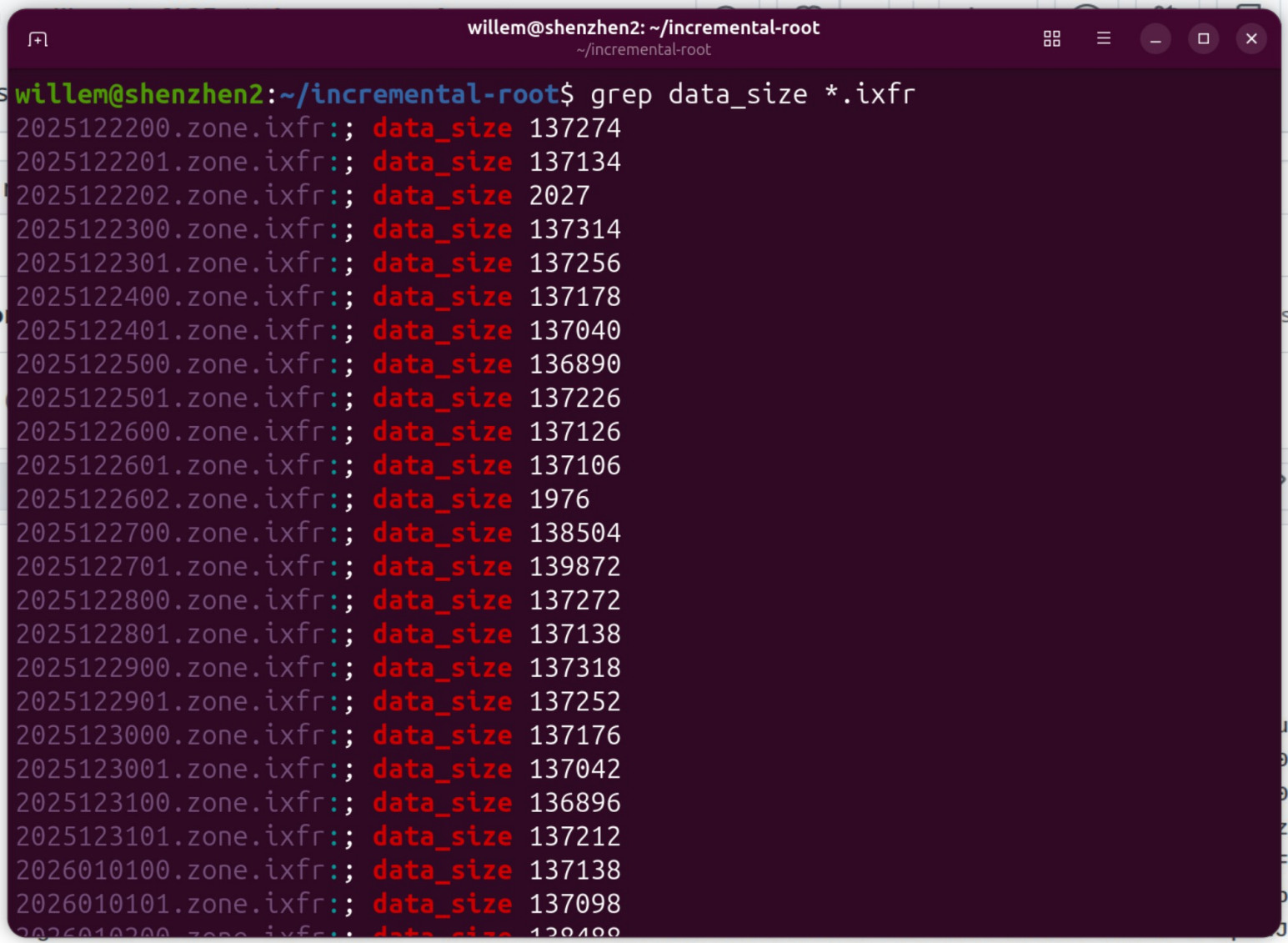
main **incremental-root** / **2026031200.zone.ixfr** Go to file t

wtoorop Updated incremental transfers 2967436 · 39 minutes ago

480 lines (480 loc) · 192 KB

Code Blame Raw

```
1   ; IXFR data file
2   ; zone .
3   ; from_serial 2026031102
4   ; to_serial 2026031200
5   ; data_size 137190
6   ; IXFR created by NSD 4.8.0 for . 2026031102 to 2026031200 of 137190 bytes at time Thu Mar 12 05:
7   .   86400   IN  SOA a.root-servers.net. nstld.verisign-grs.com. 2026031200 1800 900 604800 86400
8   .   86400   IN  SOA a.root-servers.net. nstld.verisign-grs.com. 2026031102 1800 900 604800 86400
9   .   86400   IN  RRSIG   SOA 8 0 86400 20260324200000 20260311190000 31128 . cyuo24sQmzMjEhvQfR4B2
10  .   86400   IN  RRSIG   ZONEMD 8 0 86400 20260324200000 20260311190000 31128 . J0T0GWFc4514R+zLbt
11  .   86400   IN  ZONEMD  2026031102 1 1 95e624995e4688d6e03e44bd89839b7f131b32854b0b43b2868d333ac3
12  global. 86400   IN  RRSIG   NSEC 8 1 86400 20260319050000 20260306040000 31128 . hpwuJkmK65l+r5aD
```


willem@shenzhen2: ~/incremental-root
~/incremental-root
willem@shenzhen2:~/incremental-root$ grep data_size *.ixfr
2025122200.zone.ixfr:; data_size 137274
2025122201.zone.ixfr:; data_size 137134
2025122202.zone.ixfr:; data_size 2027
2025122300.zone.ixfr:; data_size 137314
2025122301.zone.ixfr:; data_size 137256
2025122400.zone.ixfr:; data_size 137178
2025122401.zone.ixfr:; data_size 137040
2025122500.zone.ixfr:; data_size 136890
2025122501.zone.ixfr:; data_size 137226
2025122600.zone.ixfr:; data_size 137126
2025122601.zone.ixfr:; data_size 137106
2025122602.zone.ixfr:; data_size 1976
2025122700.zone.ixfr:; data_size 138504
2025122701.zone.ixfr:; data_size 139872
2025122800.zone.ixfr:; data_size 137272
2025122801.zone.ixfr:; data_size 137138
2025122900.zone.ixfr:; data_size 137318
2025122901.zone.ixfr:; data_size 137252
2025123000.zone.ixfr:; data_size 137176
2025123001.zone.ixfr:; data_size 137042
2025123100.zone.ixfr:; data_size 136896
2025123101.zone.ixfr:; data_size 137212
2026010100.zone.ixfr:; data_size 137138
2026010101.zone.ixfr:; data_size 137098
Code
Is
wtoo
s ago
480 lines
Code

Incrementally signed root

	XFR size	Daily traffic
Baseline (without F)		0.96 MB
DNS XFR	1.31 MB	3.28 MB
HTTPS XFR	2.19 MB	105.12 MB
HTTPS XFR (bug fixed)	2.19 MB	5.48 MB
HTTPS cache pre-fill	2.19 MB	2.19 MB
Incremental DNS XFR	0.11 MB	0.27 MB

Global Local Root

- Command line tool to incrementally sign, here: https://github.com/NLnetLabs/dnst/tree/signer-incremental
  - Example script: https://github.com/Philip-NLnetLabs/root-incrementally-signed
- Some discussion points
  - Does traffic size matter at all?
  - W.r.t. timing & refreshing, SOA or TTL secondary semantics or resolver semantics
- WDYT?