NSEC3 TO NSEC Transition of .nu

Ulrich Wisser

ulrich.wisser@internetstiftelsen.se

The Swedish Internet Foundation

INTERNETSTIFTELSEN

Ulrich Wisser

Senior DNS Expert

DNSlabs

Swedish Internet Foundation

- **Software Developer / System Architect for .SE registry system**
- **Co-Chair of Centr-Tech WG**
- **Member of DNS-OARC program committee**

INTERNETSTIFTELSEN

RFC 5155

10.5. Transitioning a Signed Zone from NSEC3 to NSEC

To safely transition back to a DNSSEC [RFC4035] signed zone, simply reverse the procedure above:

1. Add NSEC RRs incrementally or all at once.

2. 2. Remove the NSEC3PARAM RRSet. This will signal the server to use the NSEC RRs for negative and wildcard responses.

3. 3. Remove the NSEC3 RRs either incrementally or all at once.

4. Transition all of the DNSKEYs to DNSSEC algorithm identifiers. After this transition is complete, all NSEC3-unaware clients will treat the zone as secure.

What could possibly go wrong?

PTS

NIS

CEO

CISO

DO

SOME

TESTING

NO ANSWER

VS.

Answer: NO ANSWER

NSEC/NSEC3 Testbed

No Data – No Wildcard

No Data – Wildcard

Name Error – No Wildcard

Empty Non Terminal

No NSEC No NSEC3

NSEC/NSEC3 doesn’t cover label

NSEC does cover label - NSEC3 doesn’t

NSEC3 does cover label – NSEC doesn’t

Data with NSEC/NSEC3

https://public-dns.info

RESULTS

	NODATA	NXDOMAIN	SERVFAIL
No Nsec No Nsec3	32	0	39
Nsec Does Not Cover Label	0	32	39
Nsec3 Does Not Cover Label	0	32	39
Nsec And Nsec3 Do Not Cover Label	0	71	0
Nsec Does Cover Label Nsec3 Does Not	0	55	16
Nsec Does Not Cover Label Nsec3 Does	0	65	6

Looks good to go!

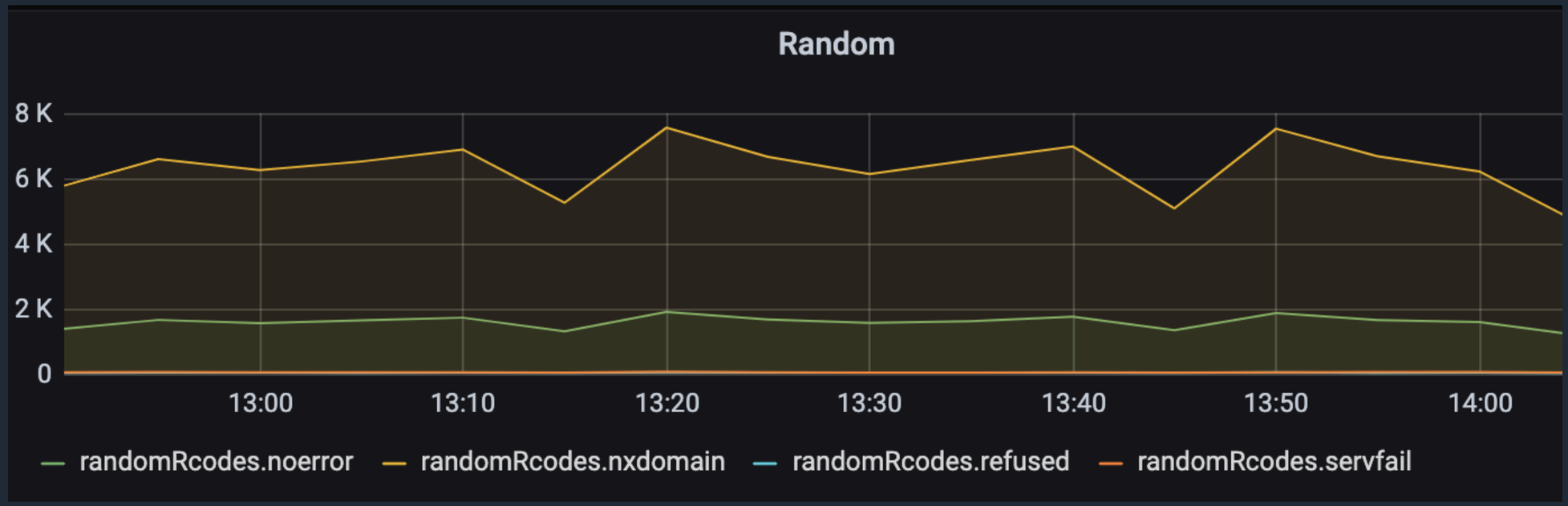
Test Run

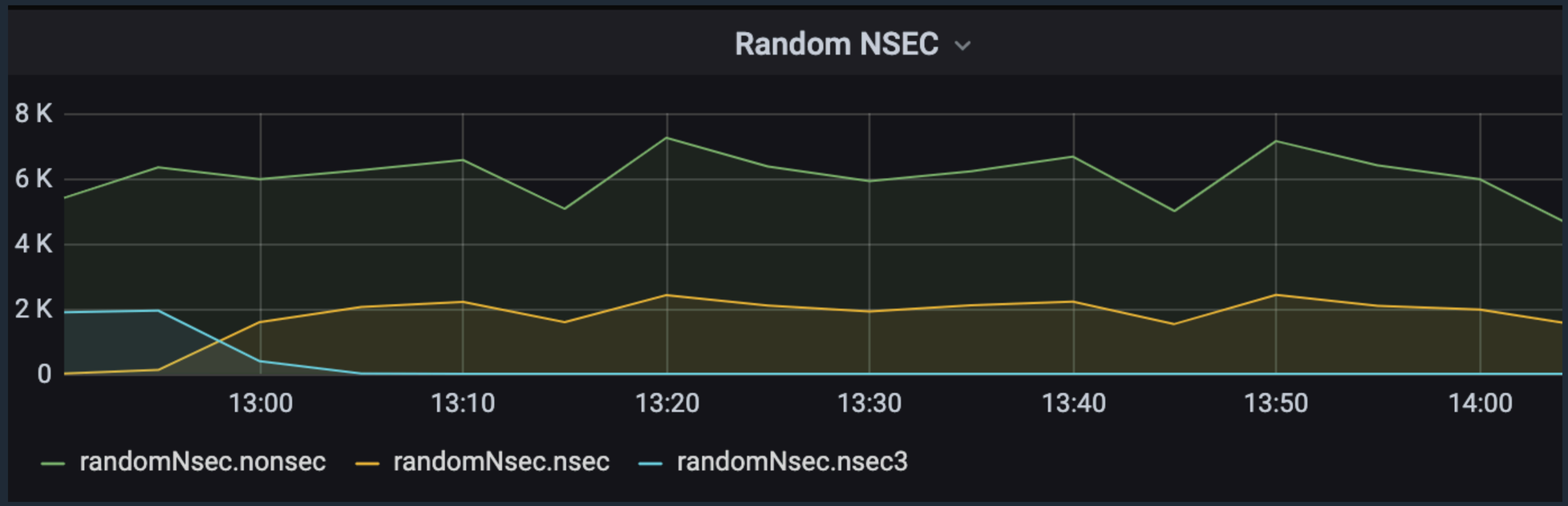
*.NU -> *.NUTEST.NU

OpenDNSSEC

One Anycast DNS Provider

Ripe Atlas Measurement with 500 probes





INTERNETSTIFTELSEN

Looks good!

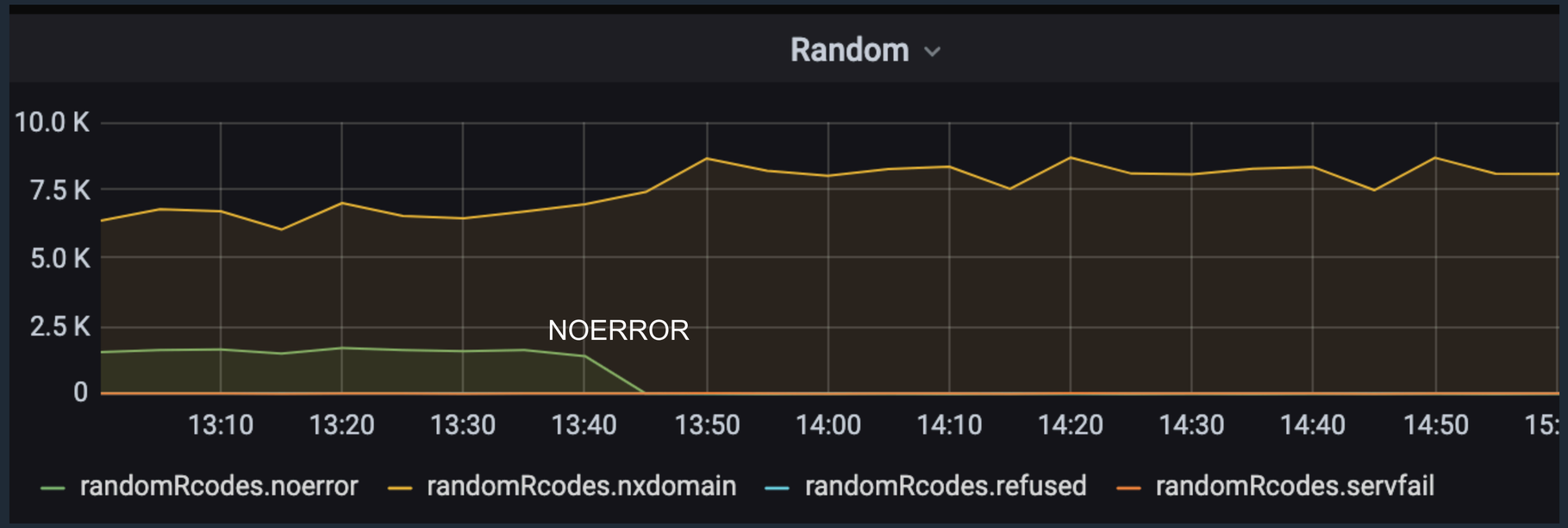
Good to go!

.NU

OpenDNSSEC

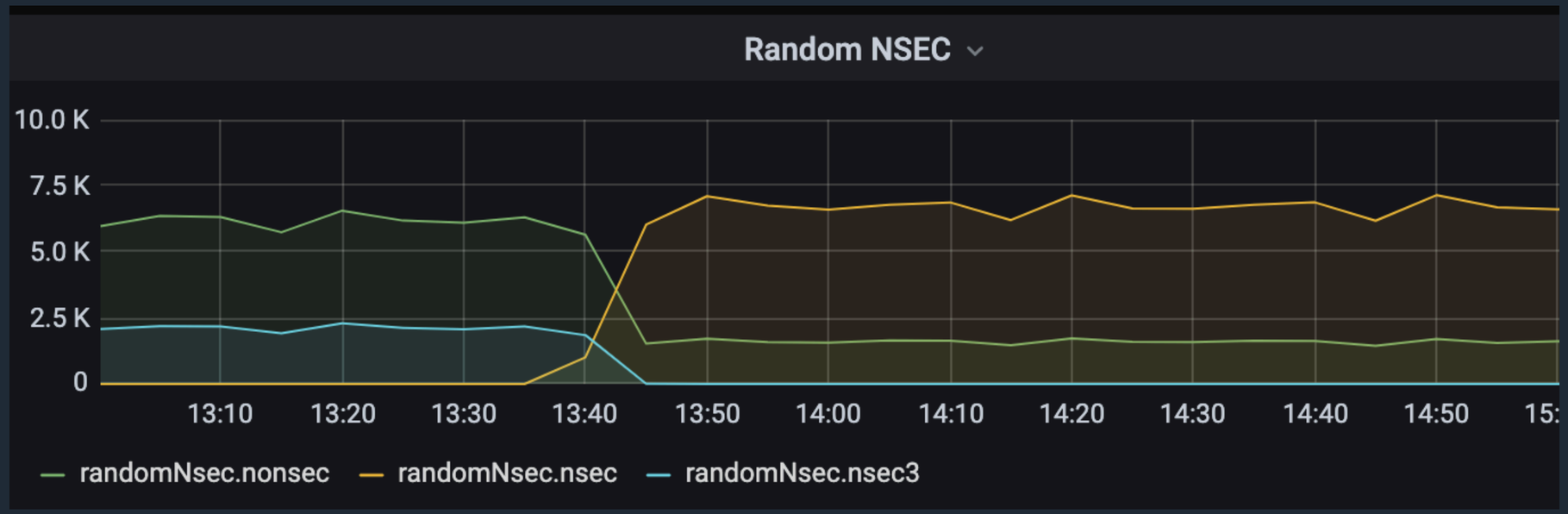
Three Anycast DNS Providers

Ripe Atlas Measurement with 5000 probes



NXDOMAIN

SERVFAIL



NSEC

NO NSEC

NSEC3

SUCCESS