GONEMASTER

A Go reimplementation of the Zonemaster DNS testing engine

Patrik Wallström, DNS-OARC, 2026-05-17

Testing DNS delegations? Why?

There are a many reasons of why the quality of a DNS delegation matters:

- Having a fully functional DNS delegation means your internet services are more likely to work as expected
- There will be less noisy traffic on the internet
- Mistakes happen easily – inform the user on how to avoid mistakes
- Mistakes are even more likely to happen with DNSSEC

And it is also caring about the DNS ecosystem.

The requirements on a tool to test DNS

So how do you measure a DNS delegation?

Simple answer: Send a huge amount of DNS queries to all involved servers!

… or by collecting a huge number of requirements for a fully functional DNS delegation, and then;

Convert the requirements into test case specifications, and then;

Implement these test case specifications into code, and then;

Run the code to see if a domain name follows the test case specifications.

What is Gonemaster?

Gonemaster is a full Go reimplementation of the **Zonemaster** DNS delegation testing engine and CLI written in Perl.

Zonemaster was the standard for DNS zone quality checking — created by AFNIC & the Swedish Internet Foundation. Gonemaster brings the same rigor to the Go ecosystem.

DNSCheck was the first tool written by Patrik Fältström, later funded by IIS and rewritten by Jakob Schlyter.

Language

100% Go

Test cases

Zonemaster compatible

License

Open Source (BSD 2-Clause)

First release

January 2026

The Test Case Specifications

Borrowed in large part from Zonemaster, and a few more specs added!

1. **Basic** - can we even resolve this
2. **Address** - nameserver IPs aren't private/reserved/bogon, reverse DNS resolves
3. **Connectivity** - reachability, transport, AS diversity
4. **Consistency** - nameservers give different answers
5. **Delegation** - parent and child disagree
6. **DNSSEC** - signatures, chains, algorithms
7. **Nameserver** - server behavior and conformance
8. **Syntax** - names and records well-formed
9. **Zone** - SOA, MX, SPF, apex hygiene

Additional Test Cases

DNSSEC19	Check DNSKEY records for known cryptographic weaknesses	Detects weak or compromised DNSKEYs, including ROCA, bad RSA parameters, small factors, and badkeys blocklist hits.
DNSSEC20	NSEC/NSEC3 type bitmap at zone apex matches actual RR types	Checks that apex NSEC/NSEC3 bitmaps include RR types that actually exist.
DNSSEC21	Parent zone's DS RRset is signed by a valid DNSKEY	Verifies the parent’s DS RRset RRSIG against parent DNSKEYs.
Nameserver16	EDNS NSID option support	Queries authoritative nameservers with EDNS NSID and reports returned NSID values.
Zone12	CSYNC RR at zone apex	Checks CSYNC presence, consistency, multiplicity, and serial validity.
Zone13	SPF DNS lookup limit compliance	Checks SPF recursive DNS lookup count, loops, recursive errors, and deprecated ptr.
Zone14	ZONEMD record at zone apex	Checks ZONEMD presence, cross-server consistency, serial match, duplicate scheme/hash pairs, and supported hashes.

Why rewrite in Go?

The reason I chose **Go** was that it gives you the following nice properties:

- Single static binary
- Native concurrency
- A well-defined Go library that is easy to embed in other Go software
- miekg/dns gives you a DNS library that covers all modern DNS RFCs
- A minimal amount of external dependencies

The core functionality of Gonemaster

The functionality of Gonemaster as a command line tool:

INPUT a domain name
RUN a test of the DNS delegation of that domain name
OUTPUT a machine- och human-readable test result

The modular test cases are run in parallel Go routines, and the internal resolver is tunable with timeouts, retries, and cache.

```
$ gonemaster --domain example.com
$ gonemaster --json --domain example.com | jq
$ gonemaster --domain example.com --ns ns1.example.com/192.0.2.10
```

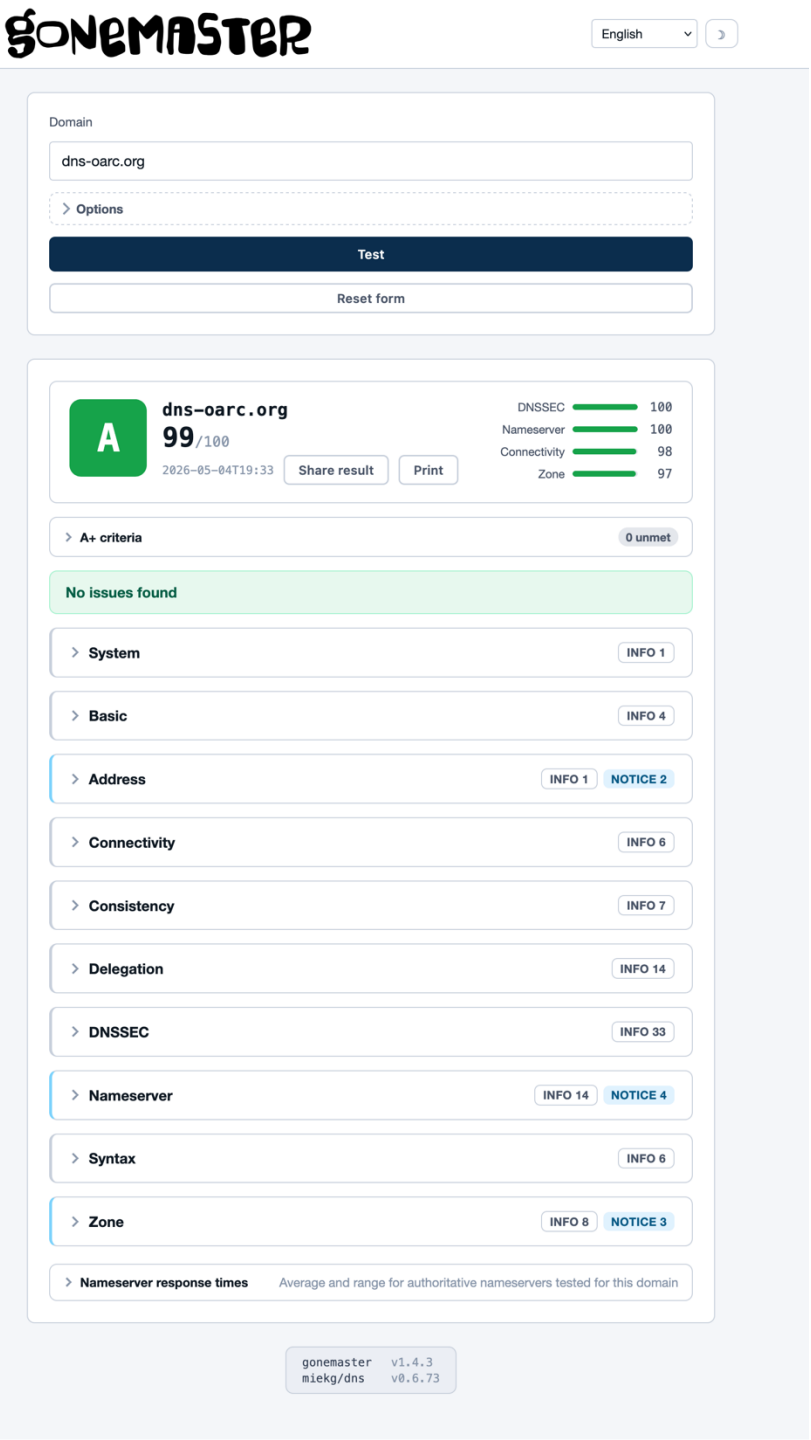
Human-readable output

```
$ gonemaster sunet.se
Seconds Level    Message
======= ======== =======
   6.16 NOTICE   Nameserver ns1.sunet.se has an IP address (2001:6b0:5a:4020::384) without PTR configured.
   6.59 NOTICE   The following name server(s) are announced in the same IPv6 prefix (2001:6b0::/32):
"b.ns.kth.se/2001:6b0:1::250;ns1.sunet.se/2001:6b0:5a:4020::384;sunic.sunet.se/2001:6b0:7::2"
   7.10 WARNING  The following servers respond with the NSEC3 iteration value 5. The recommended practice is to set
this value to 0. Fetched from name servers
"b.ns.kth.se/130.237.72.250;b.ns.kth.se/2001:6b0:1::250;ns1.sunet.se/2001:6b0:5a:4020::384;ns1.sunet.se/89.47.185.240
;server.nordu.net/193.10.252.19;server.nordu.net/2001:948:4:2::19;sunic.sunet.se/192.36.125.2;sunic.sunet.se/2001:6b0
:7::2".
   7.10 WARNING  The following servers respond with a non-empty salt in NSEC3 (16 octets). The recommended practice
is to use an empty salt. Fetched from name servers
"b.ns.kth.se/130.237.72.250;b.ns.kth.se/2001:6b0:1::250;ns1.sunet.se/2001:6b0:5a:4020::384;ns1.sunet.se/89.47.185.240
;server.nordu.net/193.10.252.19;server.nordu.net/2001:948:4:2::19;sunic.sunet.se/192.36.125.2;sunic.sunet.se/2001:6b0
:7::2".
   7.14 WARNING  DNSKEY with tag 7636 and using algorithm 8 (RSA/SHA-256) has a size (1024) smaller than the
recommended one (2048).
   7.30 NOTICE   The following name server(s) respond to software version query "version.bind" with string "9.18.44".
Returned from name servers: "server.nordu.net/193.10.252.19;server.nordu.net/2001:948:4:2::19"
   7.30 NOTICE   The following name server(s) respond to software version query "version.bind" with string
"bind@KTH". Returned from name servers: "b.ns.kth.se/130.237.72.250;b.ns.kth.se/2001:6b0:1::250"
   7.30 NOTICE   The following name server(s) respond to software version query "version.bind" with string "ns1
node1". Returned from name servers: "ns1.sunet.se/2001:6b0:5a:4020::384;ns1.sunet.se/89.47.185.240"
;sunic.sunet.se/2001:6b0:7::2"
```

The Gonemaster Components

In addition to the CLI there are more components included:

- The gonemaster-server
  - A server API together with an administration UI (optional)
  - Also includes a public UI - https://gonemaster.evilbit.de/
  - But more, it includes an Analysis UI
- The gonemaster-client
  - For using to the server API
  - Start and control batch jobs
  - Fetching results
- The gonemaster-nagios
  - For integration in monitoring tools such as Nagios, Icinga, etc.



Public UI & Scoring

Severity	Penalty
NOTICE	1
WARNING	5
ERROR	20
CRITICAL	Auto-F

Category	Weight	Modules
DNSSEC	1.5	DNSSEC
Nameserver health	1.2	Basic, Delegation, Nameserver
Connectivity	1.0	Connectivity, Address
Zone consistency	0.8	Zone, Consistency, Syntax

Entry → Category sub-score → Weighted aggregate → Grade

A+	A	B	C	D	F
100 + bonus	90	75	60	40	0

A+ criteria — 0 unmet

- ✓ Nameserver AS diversity
- ✓ CDS / CDNSKEY published
- ✓ DNSSEC enabled
- ✓ IPv6 on all nameservers
- ✓ NSEC3 without opt-out
- ✓ Strong algorithm (ECDSA / Ed25519)

The Admin UI

- Single Job
- Recent Tests
- **Domains**
- Tags
- Cohorts
- Batch Jobs
- Metrics
- Settings

Domains

Search by name...

All tags

All levels

DOMAIN	TAGS	LATEST LEVEL	SCORE	LAST RUN ▼	RUNS
dns-oarc.org		NOTICE	A 99	2026-05-04	3
kp	TLDs	ERROR	C 69	2026-05-04	3
nk		CRITICAL	F 0	2026-05-04	1
theconference.se		NOTICE	A 100	2026-05-04	1
ica.se		WARNING	B 89	2026-05-04	1
ampeau.fr		WARNING	A 94	2026-05-03	1
pl	TLDs	WARNING	A 97	2026-05-02	3
kirei.se		NOTICE	A 99	2026-05-02	4
fei.se		WARNING	B 80	2026-05-01	1

System Settings

- Single Job
- Recent Tests
- Domains
- Tags
- Cohorts
- Batch Jobs
- Metrics
- **Settings**

System | **Profiles** | Scoring

Profiles

Browse the server default and stored profiles, see where they are used, and edit drafts safely.

Profile Library

Search, filter, and edit stored profiles.

New profile

Search profiles

Search name

Filter

All profiles

default Default

Server base profile

default

Default

Server base profile

NAME
default

DESCRIPTION
Server base profile

SOURCE
Server base profile

New from default

Config JSON

Batched Jobs

- Single Job
- Recent Tests
- Domains
- Tags
- Cohorts
- **Batch Jobs**
- Metrics
- Settings

Batch Jobs

Domain list | From tag

Domains (one per line)

example.com
example.org

Tags

tld, ccTLD

Comma-separated tag names (must already exist).

Stored profile

Use tag default / server default

Optional stored profile. Leave blank to inherit tag or server defaults.

Run Batch

Active Batches

Pause queue

No active batches.

Batch Inspector

Recent batches

batch_1777492479206646547_1 - 2026-04-29

Latest 20 unique batch IDs, newest first.

Batch ID

batch_1777492479206646547_1

Refresh | Auto refresh: off

Delete batch

Sort

Start time (newest)

Page size

20

Status

all

Domain contains

example

QUEUE & WORKERS

QUEUE DEPTH	IN-FLIGHT JOBS	JOBS/MIN
0	0	0

DNS

DNS LOOKUPS	CACHE HITS	CACHE MISSES	CACHE HIT RATE	EXTERNAL IPV4	EXTERNAL IPV6
44,8K	15,7K	29,1K	35.0%	12K	11,1K

JOB OUTCOMES

TOTAL JOBS FINISHED	FAILED JOBS	SUCCESS RATE	FAILURE RATE
10	0	100.0%	0.0%

PERFORMANCE

AVG JOB DURATION	API P90
17,434 ms	250 ms

SEVERITY

NOTICE	WARNING	ERROR	CRITICAL
61	16	2	1

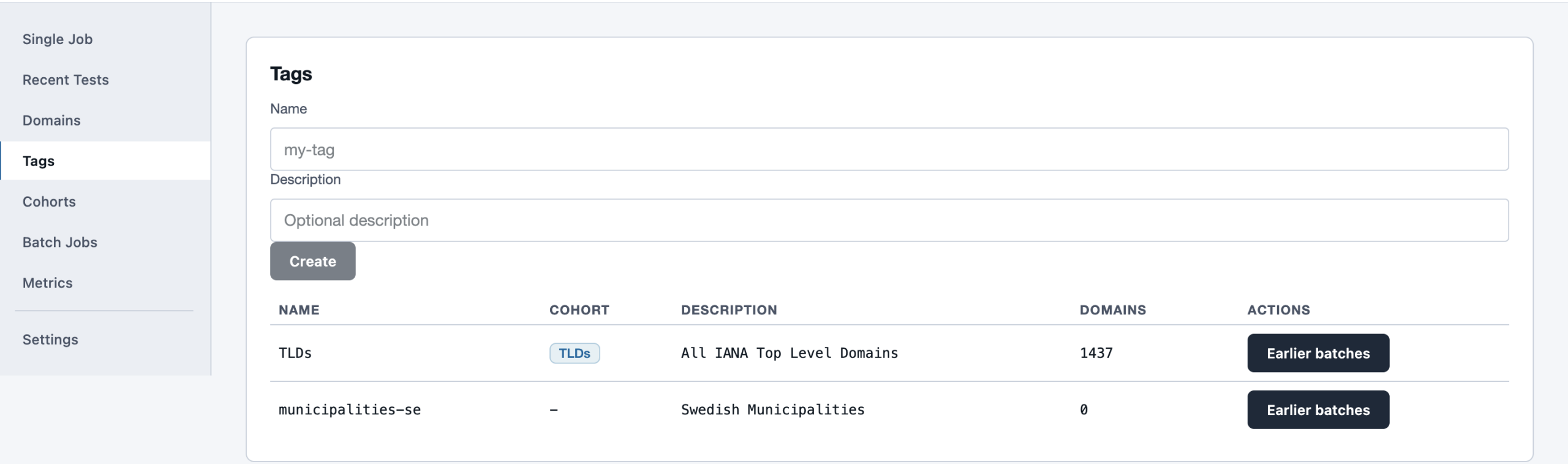
Throughput 0/bucket

Failures 0/bucket

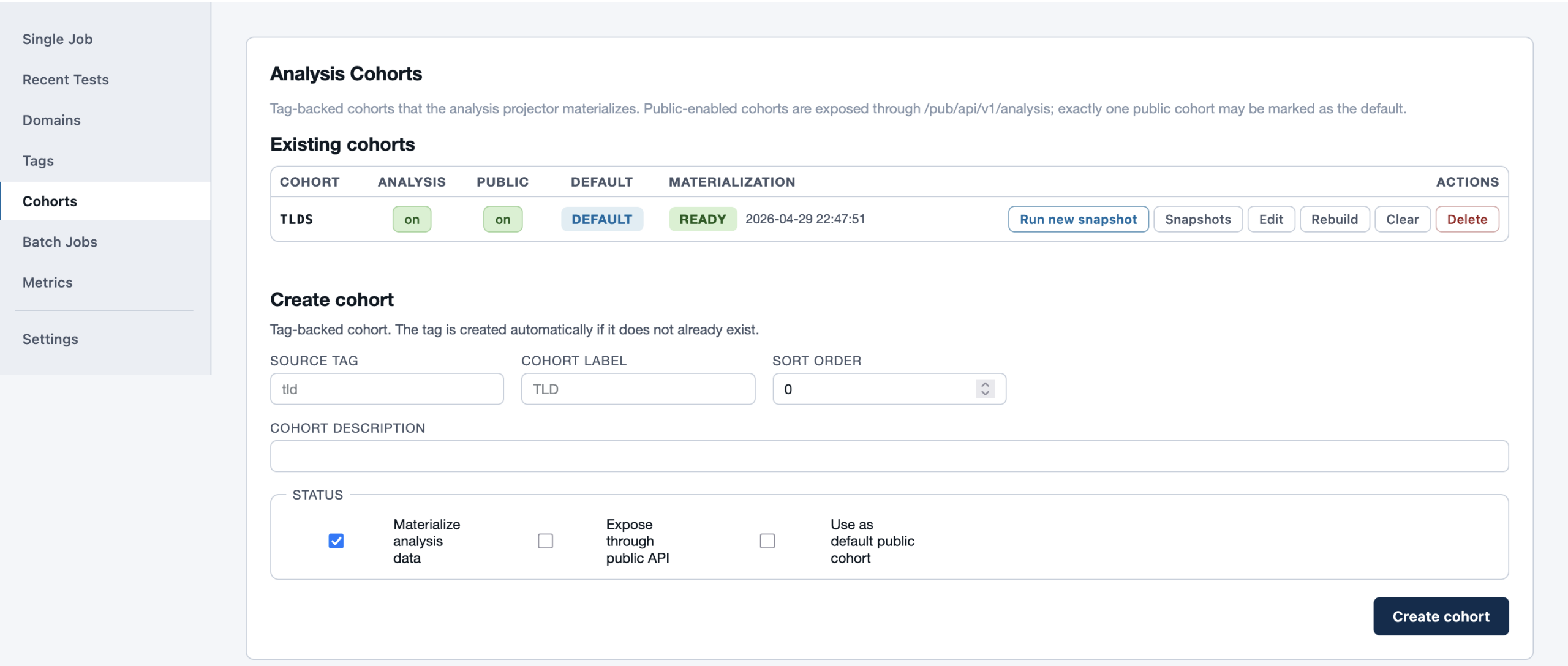
DNS queries/s 0/s

Cache hit rate 0.0%

Tags – Tagged batches



Cohorts – An analysis of a Tagged batch



Snapshot: **2026-04-29** | Built 2026-04-29 22:48:20

TLDs

All IANA Top Level Domains

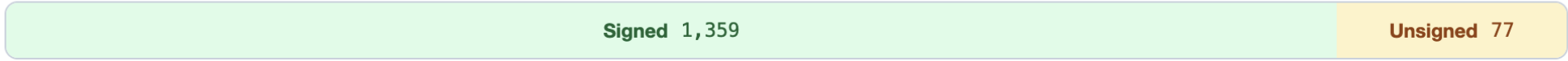
Last analyzed: 2026-04-29 22:47:51

Domain health

Each domain counted by the worst severity in its latest run.

DNSSEC posture

Signed vs unsigned domains in the cohort.



Grade distribution

Letter grade assigned by the scoring engine at run time.

Overview | **Domains** | Nameservers | Addresses | ASNs | Tags | Trends | Diff

SEARCH

substring match

Domains

PAGE SIZE 50 | CSV | JSON

DOMAIN ↕	SCORE ↕	GRADE	WORST ↕	OPERATOR	NAMESERVERS ↕	ENDPOINTS ↕	ASNS ↕	PREFIXES ↕	LAST ANALYZEI
AAA	96	A	WARNING	VERCARA - Vercara, LLC, US AS12008	6	12	1	12	2026-04-29 21:54:54
AARP	96	A	WARNING	*Multiple (2)*	6	12	2	12	2026-04-29 21:54:57
ABB	92	A	WARNING	*Multiple (2)*	4	8	2	8	2026-04-29 21:55:10
ABBOTT	94	A	WARNING	*Multiple (2)*	4	8	2	8	2026-04-29 21:55:08
ABBVIE	96	A	NOTICE	*Multiple (2)*	8	16	2	16	2026-04-29 21:54:59
ABC	91	A	WARNING	*Multiple (2)*	6	12	2	12	2026-04-29 21:55:16
ABLE	96	A	WARNING	VERCARA - Vercara, LLC, US AS12008	6	12	1	12	2026-04-29 21:54:53
ABOGADO	96	A	WARNING	*Multiple (2)*	6	12	2	12	2026-04-29

SEARCH

substring match

Nameservers

PAGE SIZE 50 | CSV | JSON

NAMESERVER ↕	OPERATOR	DOMAINS ↓	ENDPOINTS ↕	IPV4	IPV6
NS01.TRS-DNS.COM	AS393818 TUCOWS-TRS-DNS1 - Tucows.com Co., CA	75	2	1	1
NS01.TRS-DNS.NET	AS63363 TUCOWS-TRS-DNS2 - Tucows.com Co., CA	75	2	1	1
NS10.TRS-DNS.INFO	AS42 WOODYNET-1 - WoodyNet, Inc., US	71	2	1	1
NS10.TRS-DNS.ORG	AS42 WOODYNET-1 - WoodyNet, Inc., US	71	2	1	1
A.GMOREGISTRY.NET	AS12008 VERCARA - Vercara, LLC, US	46	2	1	1
B.GMOREGISTRY.NET	AS12008 VERCARA - Vercara, LLC, US	46	2	1	1
K.GMOREGISTRY.NET	AS12008 VERCARA - Vercara, LLC, US	46	1	1	0
L.GMOREGISTRY.NET	AS12008 VERCARA - Vercara, LLC, US	46	2	1	1
NS-TLD1.CHARLESTONROADREGISTRY.COM	AS15169 GOOGLE - Google LLC, US	46	2	1	1
NS-TLD2.CHARLESTONROADREGISTRY.COM	AS15169 GOOGLE - Google LLC, US	46	2	1	1
NS-TLD3.CHARLESTONROADREGISTRY.COM	AS15169 GOOGLE - Google LLC, US	46	2	1	1

← ASNs

AS393818

TUCOWS-TRS-DNS1 - Tucows.com Co., CA

DOMAINS	ADDRESSES	NAMESERVERS	PREFIXES
75	2	2	2

Domains

bar blockbuster click cloud coop country creditunion data dish diy dm dot dtv dvr feedback
food forum fun gift hiphop hiv host in iq kfh ky latino lifestyle link living locker
love mobile music my observer ollo online ott phone pid press property pw realty rest sexy
site sling space store tech to trust uno vana website xn--2scrj9c xn--3hcrj9c xn--45br5cyl
xn--45brj9c xn--fpcrj9c3d xn--gecrj9c xn--h2breg3eve xn--h2brj9c xn--h2brj9c8c xn--mgbbh1a xn--mgbbh1a71e
xn--mgbgu82a xn--mgbtx2b xn--ngbe9e0a xn--rvc1e0am3e xn--s9brj9c xn--xkc2dl3a5ee0h yandex

Nameservers

ns01.trs-dns.com ns1.registry.in

Prefixes

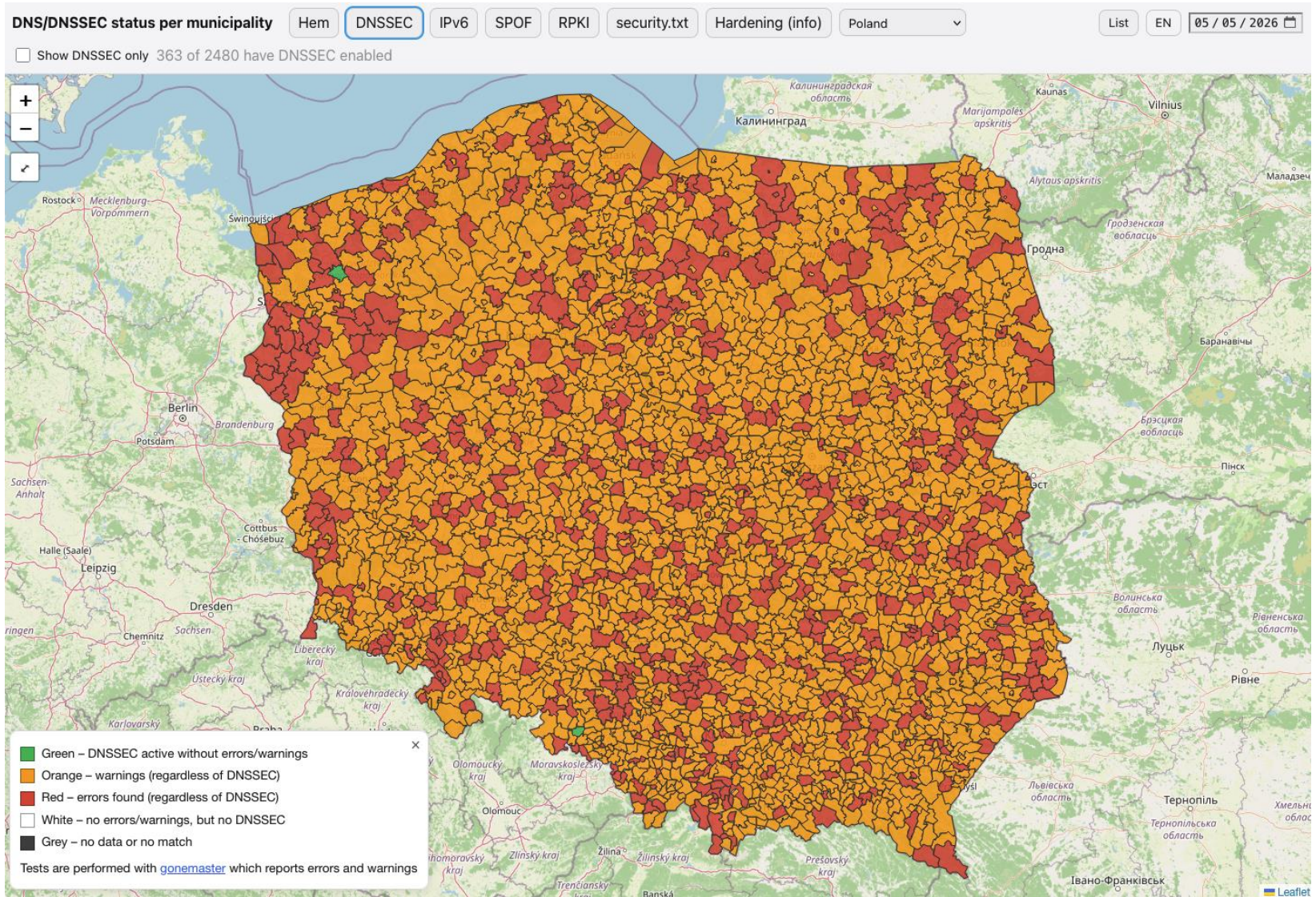
Cross-reference anything

- Tags
- Nameservers
- Addresses
- Prefixes
- ASN
- Domains

Upcoming in Analysis UI:

- Better view of trends over time
- Diffs between specific runs

kommunermeddnssec.se



Links and questions!

Public UI: https://gonemaster.evilbit.de/
Analysis UI: https://gonemaster.evilbit.de/analysis/
Code: https://codeberg.org/pawal/gonemaster/

Tobbe: https://kommunermeddnssec.se/

Mail me: pawal@amplitut.de