



ZONEMASTER

INTERNET
STIFTELSEN



Using Zonemaster for quality checks of all .se domain names

2023-06-12

Mats Dufberg

mats.dufberg@internetstiftelsen.se

Zonemaster tests domain names

Zonemaster is a DNS and domain name test tool.

The test object is the domain name, as the term is used in the domain name industry, i.e. Zonemaster can test those.

Registrants register a domain name under a TLD, e.g. .se, and wants to determine if it is correctly operated.

The DNS operator, e.g. web hotel, also wants to determine if there are any issues with the operation of the domain names, especially if issues are reported.

Zonemaster tests DNS zones

Technically, Zonemaster is a DNS and DNS zone test tool.

A registered domain name under .se is delegated to a DNS zone, if active.

The test object for Zonemaster is really the DNS zone.

There are other DNS zones not matching registered domain names that can also be tested by Zonemaster, e.g.:

- TLDs
- Reverse zones
- Zones below the registered domain name

Testing single domain names or large scale

Zonemaster has been designed to be used for single tests, valuable for registrants and troubleshooting issues with single domains names – or DNS zones.

I will presents some findings from a large scale test of all domain names under .se.

First I will give some background to Zonemaster and present it closer.

Keep DNS healthy

- DNS is crucial for all services on Internet
- "Network issue" could be a DNS issue
- DNS is complex to troubleshoot
- DNSSEC makes it even harder

We need a way to check. For that we need a test tool.

Zonemaster is a DNS tool to check DNS zone health

- Zonemaster checks the delegation
- Zonemaster verifies that all name servers give consistent responses
- Zonemaster verifies that all name servers respond to queries
- Zonemaster verifies DNSSEC

Zonemaster is available for anyone

Zonemaster is available for anyone to install – in fact, we know that there are multiple installations around the world. Zonemaster is available as open source program.

Zonemaster is available for anyone to run, e.g.

- <https://zonemaster.net/>
- <https://zonemaster.se/>

There is also a command line tool that can be installed directly or via Docker.

https://zonemaster.net/



[Run test](#) [FAQ](#)



English



Run domain test

icann.org



Run



Options

[About Zonemaster](#)

After a minute or a couple of minutes...

icann.org
2023-06-11 15:13 GMT+02:00

History Export Share

All 54 Info 48 Notice 2 Warning 4 Error 0 Critical 0 Filter text

- ▶ SYSTEM ✓1
- ▶ BASIC ✓3
- ▶ ADDRESS !1 ✓2
- ▶ CONNECTIVITY ✓1
- ▶ CONSISTENCY ✓6
- ▶ DELEGATION ✓7
- ▶ DNSSEC ▲3 ✓3
- ▶ NAMESERVER ✓9
- ▶ SYNTAX ✓8
- ▶ ZONE ▲1 !1 ✓8

Green color means that all is good. Other colors mean that there is something to inspect.

Zonemaster can meet several needs

- Troubleshooting
- Monitoring
- Statistics and measurements
- Check your domain
- Verify that a new domain is ready to be used
- Check all domains under your TLD

Who is behind Zonemaster?

Since 2013 The Swedish Interent foundation (Internetstiftelsen), registry of .se and .nu, and Afnic in France, registry of .fr, .re and others, together develop and maintain Zonemaster as a modern DNS tool.

It is an open-source tool available on Github, and others contribute to the development of Zonemaster.

You can contribute by reporting issues or suggestions for improvements.

Features of Zonemaster

- All tests are based on standards and best practices
- All tests are defined as written specifications available at Github
- Modular built to be possible to integrate parts in other tools for different needs
- Actively maintained with releases twice a year – latest release 2022-12-19 – next release next week
- Available in several languages, besides English

Translations by ccTLD volunteers

Translations are done by volunteers from ccTLDs of that language:

- Danish (.dk ccTLD)
- Norwegian (.no ccTLD)
- Finnish (.fi ccTLD)
- Spanish (.cl ccTLD)
- French (Zonemaster project)
- Swedish (Zonemaster project)

Other languages are welcome! You can contribute by providing a translation.

Large scale test

In the design of Zonemaster the single test has been in focus. In March 2023 we ran a complete test of all domain names in .se, around 1.5 million domain names, as a pilot.

Running one test is fast. Running 1.5 million tests took five days to complete.

All results were collected to a database.

My colleague Mats Strålberg who set up and ran the tests should have all credit for collecting the data.

The tests run are grouped into 9 modules

Basic	Tests for availability of the zone to be tested
Address	IP address tests
Connectivity	Tests of name server connectivity
Consistency	Tests of consistency between name servers
DNSSEC	Tests of DNSSEC
Delegation	Tests of the delegation of the domain name (DNS zone)
Nameserver	Tests of the behavior of the name servers
Syntax	Tests of the domain name as name
Zone	Tests of different data in the zone

Several tests in each group – 72 tests are run for each domain name

Test Plan/Test Case	Test Case Description	DNSSEC-TP	
Address-TP		DNSSEC01	Legal values for the DS hash digest algorithm
ADDRESS01	Name server address must be globally routable	DNSSEC02	DS must match a valid DNSKEY in the child zone
ADDRESS02	Reverse DNS entry exists for name server IP address	DNSSEC03	Check for too many NSEC3 iterations
ADDRESS03	Reverse DNS entry matches name server name	DNSSEC04	Check for too short or too long RRSIG lifetimes
Basic-TP		DNSSEC05	Check for invalid DNSKEY algorithms
BASIC01	The domain must have a parent domain	DNSSEC06	Verify DNSSEC additional processing
BASIC02	The domain must have at least one working name server	DNSSEC07	If DNSKEY at child, parent should have DS
BASIC03	The <i>Broken but functional</i> test	DNSSEC08	Valid RRSIG for DNSKEY
Connectivity-TP		DNSSEC09	RRSIG(SOA) must be valid and created by a valid DNSKEY
CONNECTIVITY01	UDP connectivity to name servers	DNSSEC10	Zone contains NSEC or NSEC3 records
CONNECTIVITY02	TCP connectivity to name servers	DNSSEC11	DS in delegation requires signed zone
CONNECTIVITY03	AS Diversity	DNSSEC12	Test for DNSSEC Algorithm Completeness
Consistency-TP		DNSSEC13	All DNSKEY algorithms used to sign the zone
CONSISTENCY01	SOA serial number consistency	DNSSEC14	Check for valid RSA DNSKEY key size
CONSISTENCY02	SOA RNAME consistency	DNSSEC15	Existence of CDS and CDNSKEY
CONSISTENCY03	SOA timers consistency	DNSSEC16	Validate CDS
CONSISTENCY04	Name server NS consistency	DNSSEC17	Validate CDNSKEY
CONSISTENCY05	Consistency between glue and authoritative data	DNSSEC18	Validate trust from DS to CDS and CDNSKEY
CONSISTENCY06	SOA MNAME consistency		

Several tests... -- Continued

Delegation-TP		Syntax-TP	
DELEGATION01	Minimum number of name servers	SYNTAX01	No illegal characters in the domain name
DELEGATION02	Name servers must have distinct IP addresses	SYNTAX02	No hyphen ('-') at the start or end of the domain name
DELEGATION03	No truncation of referrals	SYNTAX03	There must be no double hyphen ('--') in position 3 and 4 of the domain name
DELEGATION04	Name server is authoritative	SYNTAX04	The NS name must have a valid domain/hostname
DELEGATION05	Name server must not point at CNAME alias	SYNTAX05	Misuse of '@' character in the SOA RNAME field
DELEGATION06	Existence of SOA	SYNTAX06	No illegal characters in the SOA RNAME field
DELEGATION07	Parent glue name records present in child	SYNTAX07	No illegal characters in the SOA MNAME field
Nameserver-TP		Zone-TP	
NAMESERVER01	A name server should not be a recursor	ZONE01	Fully qualified master nameserver in SOA
NAMESERVER02	Test of EDNS0 support	ZONE02	SOA 'refresh' minimum value
NAMESERVER03	Test availability of zone transfer (AXFR)	ZONE03	SOA 'retry' lower than 'refresh'
NAMESERVER04	Same source address	ZONE04	SOA 'retry' at least 1 hour
NAMESERVER05	Behaviour against AAAA query	ZONE05	SOA 'expire' minimum value
NAMESERVER06	NS can be resolved	ZONE06	SOA 'minimum' maximum value
NAMESERVER07	To check whether authoritative name servers return an upward referral	ZONE07	SOA master is not an alias
NAMESERVER08	Testing QNAME case insensitivity	ZONE08	MX is not an alias
NAMESERVER09	Testing QNAME case sensitivity	ZONE09	MX record present
NAMESERVER10	Test for undefined EDNS version	ZONE10	No multiple SOA records
NAMESERVER11	Test for unknown EDNS OPTION-CODE		
NAMESERVER12	Test for unknown EDNS flags		
NAMESERVER13	Test for truncated response on EDNS query		
NAMESERVER14	Test for unknown version with unknown OPTION-CODE		

What tests are run?

Complete list is available on Github

<https://github.com/zonemaster/zonemaster>

CRITICAL – tests cannot be run

7% of all domain names had issues that made it impossible to run a test.

- NXDOMAIN – the domain does not exist in DNS anymore – delegation removed, deactivated or registration removed.
- Severe errors in the delegation made it impossible to get in touch with the DNS zone.

This version of Zonemaster does not report the difference. Will be solved in the next version.

ERROR – Domain name may be unreliable

16% of the domains names had ERROR in at least one test.

The most common causes of ERROR:

- 5% had one or several name servers that are not configured with the DNS zone (domain name) – decreased redundancy
- 5% uses SHA-1 as DS algorithm – it works but it is not considered to be safe

WARNING – Domain name works but the stability can be threatened

74% of the domain names had WARNING in at least one test.

The most common causes of WARNING:

- 65% had all name servers IP addresses in the same AS, for IPv4 or IPv6 or both.
- 8% had no working reverse lookup on one or several nameserver IP address
- 7% had one or more name servers with incorrect handling of protocol parameters for EDNS
- 5% had inconsistent or unexpected response on MX (mail server) query
- 2% were signed zone, but no DS in parent – signed, but DNSSEC is not used

ERROR or WARNING

82% of the domain names had ERROR or WARNING on at least one test, but maybe several.

Improvements can be done

We can see that most domain names under .se can improve its quality.

In most cases, the registrar is also the DNS operator.

The registrars can improve many domains names at the same time.

Zonemaster is available for installation

You can repeat our test of the .se domains names.

- .se is available
- Zonemaster is available
 - Published as open source with full documentation and full installation instructions on Github <https://github.com/zonemaster/zonemaster>
 - Permissive license to be installed as-is or for other uses

GUI, CLI or integration in a system

The Zonemaster web GUI is not the only way to use Zonemaster. Zonemaster is available as a CLI tool too. The CLI is of course more light weight and easier to install.

Zonemaster is also used as an integrated tool. There are several ways to integrate Zonemaster depending on needs.

- Directly integrating Zonemaster-Engine Perl libraries.
- Wrapper around the Zonemaster-CLI tool.
- RPC-API calls to Zonemaster-Backend (as the GUI does), which also includes database storage of completed tests.

Zonemaster on Docker

Zonemaster CLI is now available on Docker Hub to be by any system with support for Docker. If you have Docker installed on your laptop, just run the following to test “icann.org”:

```
❏ docker run -t --rm zonemaster/cli --no-ipv6 icann.org
```

(Docker has no support for IPv6 unless you run it on Linux laptop. Limitation of Docker, not of Zonemaster.)

<https://github.com/zonemaster/zonemaster-cli/blob/master/USING.md>

Results are stored in a database

Tests run from the GUI or directly to Zonemaster-Backend are stored in a database. The results can be retrieved later.

A special link to the GUI can reach the test run.



Thank you!

Questions?

mats.dufberg@internetstiftelsen.se