



Verifying Zonemaster using Internet in a box

2024-11-11 ICANN Tech Day

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.

Usually, a registered domain name under a TLD is running as its own DNS zone. To get full benefit of the domain name it has to work correctly.

The test object for Zonemaster is the DNS zone, and indirectly the domain name.

There are other DNS zones not matching registered domain names that Zonemaster also can test, e.g. TLDs, reverse zones and sub-zones to register domain names. Zonemaster can test any DNS zone.

Why a test tool? – 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. We need a test tool.

Who is behind Zonemaster?

Since 2013 Internetstiftelsen in Sweden (.se and .nu) and Afnic in France (.fr, .re and others) together develop and maintain Zonemaster as a modern tool.

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

Challenges of Zonemaster

There is more than one correct configuration of a zone.

There are many erroneous ways. All of them should be detected.
Even odd errors should be detected.

- Zonemaster should capture all zones with errors, and hopefully give a meaningful message.
- Zonemaster should not report false errors.

Challenges of Zonemaster

	The zone has an error	The zone has no error
Zonemaster reports an error	Correct	Bug in Zonemaster
Zonemaster reports no error	Bug in Zonemaster	Correct

Architecture of Zonemaster

Zonemaster consists of around 75 test cases.

A test case is an aspect of testing a zone, e.g.

- DNSKEY algorithm
- Delegation NS matching NS in child

Every test case is defined by a written specification in prose.

Architecture of Zonemaster

The Zonemaster test suite consists of implementation of these test cases, each test case being a separate unit in the code.

A test tool is a program.

Programs have bugs. Some bugs are known, others are unknown.

How to test the test tool?

It is possible to inspect the Zonemaster test cases by reviewing the specifications.

- Has Zonemaster considered all correct cases?
- Has Zonemaster considered all erroneous cases?
- Does the Zonemaster test cases have a correct (or reasonable) interpretation of the standards?

How to test the test tool?

To verify the implementation of Zonemaster we need DNS zones to test on.

Each test case needs many DNS zones to capture different aspects and contexts.

There is more than one correct context, but there are many more contexts with errors.

It is not enough with a few zones for every test case. We need several.

How to test the test tool?

Test case implementation:	Identifies correct behavior	Captures erroneous behavior
Test zones are available	Can be verified	Can be verified
Test zones are not available	Cannot be verified	Cannot be verified

Use existing zones

First approach is to use different real domain names (zones), both correctly configured ones and ones with error.

- Zones changes. Zonemaster can record (save) the current state, but it might fail when re-recording is needed.
- Impossible to get full coverage
- Impossible to find TLDs with different possible characteristics
- Only one root zone
- The zones are usually not under the control of the Zonemaster project.

Create test zones on public Internet

Second approach is to create public test zones on public Internet.

- Requires multiple servers for a test case. Some errors are hard to create.
- Zones in hierarchical relation cannot coexist on the same server in many scenarios, which requires even more servers.
- Only for second and lower levels, not TLD and root

Create test zones on public Internet

- Risk of exposing open resolvers or vulnerabilities
- Hard to maintain
- Only the Zonemaster project can control the test zones.
- Only one instance at a time.

Make root configurable in Zonemaster

For testing the tool, root does not have to be the real Internet DNS root. Zonemaster supports customized root zone for testing.

- Adds support for different test root zones
- Adds support for test TLDs
- Test zones can be "private"

Why run the test zones on public Internet?

- Why run multiple servers?
- Can all test zones be published on one server? Internally?

Move Internet into one box

Third approach, move into one box with the entire Internet.

One computer

- Can serve multiple IP addresses on loopback
- Can run multiple name servers
- Can serve the entire DNS tree – or at least the parts that we need
- Can serve multiple DNS trees with separate root zones

Move Internet into one box

Zonemaster's support of customizable root zone makes this possible.

Nothing can be seen from the outside, run Zonemaster in the box.

- No limitation of root zones
- No need for multiple servers, only one virtual server is needed
- Control of hosting of parent/child
- Not exposing anything

IP addresses for one box

- Use 127.0.0.0/8 (except 127.0.0.0/16) for IPv4 on loopback
- Use fda1:b2:c3:0:127::/80 for IPv6 (ULA) on loopback

IPv4 will never collide with anything on the outside.

It is unlikely that IPv6 will collide with anything on the outside, if so select another range.

Domain names for one box

- Use TLDs xa, xb etc when possible (private use CC codes)
- Use arpa when needed
- Use different root zones when needed
- Can host private versions of public domain names when needed, not seen from the outside.

Build test zones

Create unique test zones per test case. No risk of collision between test cases. No risk that adjustments for one test case has side effects for another test cases,

Here we define a ***scenario*** to be the specific behavior of a test case that we want to capture.

To give reasonable coverage, we need 10-40 *scenarios* per test case. Usually one dedicated zone per *scenario*, but up to 3 zones per *scenario*.

In total around 2000-4000 test zones will be needed to cover all test cases.

Software for the box

The box is built on Ubuntu. CoreDNS has been selected as the main application:

- It is a flexible DNS server (<https://coredns.io/>)
- Supports plug-ins that can change the behavior of the server.
- Configuration is compact.
- Most importantly, *it permits creating erroneous and strange DNS zone behavior.*

Software for the box

Bind 9 (<https://www.isc.org/bind/>) is used for creating some DNSSEC data.

- CoreDNS has no NSEC3 support at all, but can serve canned responses.

So far CoreDNS is used for all implemented zones, but other tools could be used. IBDNS (<https://gitlab.rd.nic.fr/dns-testing-tools/ibdns>) is a candidate for the future.

- Must be able to create zones with bad behavior, which a "normal" DNS server does not permit

Multiple instances

The box can be repeated in many instances.

Test zones can be updated without interfering with production.

- The test scenario and test zone definitions are open source. Anyone can create an instance. And modify its instance.
- It is possible to test one version of the test zones in one place, at the same time as a different version is used in another place.

Not only test cases

There are other aspects of Zonemaster implementation that are not bound to a test case, e.g. handling of a broken DNS packets.

- The test scenario model in a box can be used in general for Zonemaster.

Status on using the box

The framework has been created for Zonemaster.

Some test cases already use the new framework in the latest version of Zonemaster.

Other test cases are on their way.

Everything is available on Github, and anyone can run a box.

<https://github.com/zonemaster/zonemaster/tree/master/docs/public/specifications/test-zones>

<https://github.com/zonemaster/zonemaster/tree/master/test-zone-data>

Availability of Zonemaster

- 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 use
- Reference installation on <https://zonemaster.net/>
- You can contribute by reporting issues or suggestions for improvement



Thank you!

Questions?

mats.dufberg@internetstiftelsen.se