ZONEMASTER

INTERNET
STIFTELSEN

afnic

Zonemaster Test for CDS and CDNSKEY

2021-10-27

Mats Dufberg

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.

Zonemaster is a DNS tool to check DNS 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 does not check resolvers

Zonemaster can meet several needs

- Troubleshooting
- Monitoring
- Statistics and measurements
- Verify that a new domain is ready to be used

Latest release 2021-06-01

Latest release includes:

- **Added CDS/CDSNKEY testing**
- Added translation into Finnish
- Completed translation into Norwegian
- Many other improvements

Next release will in November 2021.

CDS/CDNSKEY tests

- DNSSEC15: Existence of CDS and CDNSKEY – Does the domain have CDS or CDNSSEC records?
- DNSSEC16: Validate CDS – Are the CDS records protocol valid?
- DNSSEC17: Validate CDNSKEY – Same here.
- DNSSEC18: Validate trust from DS to CDS and CDNSKEY (next release) – Can CDS/CDNSSEC be validated by existing DS?

All tests are defined with written specification on Github.

DNSSEC15: Existence of CDS and CDNSKEY

The test case

- **Notifies** if the zone has CDS but not CDNSKEY, or vice versa
- Emits an **error** if not all name servers have the same set of CDS or CDNSKEY
- Emits an **error** if the zone has both CDS and CDNSKEY, but they do not match

The test case also emits an **information message** if the zone has no CDS/CDNSKEY or if it has both.

DNSSEC16: Validate CDS (1)

The test case emits an **error** if

- The CDS RRset is unsigned
- There is CDS without DNSKEY
- There is invalid RRSIG for the CDS RRset
- The CDS RRset is signed by an unknown DNSKEY
- The CDS RRset is a mixture of "delete" CDS and normal CDS records

DNSSEC16: Validate CDS (2)

The test case emits a **warning** if

- A CDS record does not match any DNSKEY
- The DNSKEY RRset is not signed by all DNSKEY records that the CDS records points at.

The test case emits an **informational message** if the CDS RRset consists of a single "delete" record.

DNSSEC17: Validate CDNSKEY

This test case does the same thing as DNSSEC16, but for CDNSKEY

DNSSEC18: Validate trust from DS

The test case emits an **error** if

- There is no correct chain of trust from existing DS to the CDS or DNSKEY RRset

This test case will be added in the release in November 2021. The written specification can be found at Github as a pull request.

Who is behind Zonemaster?

Since 2013 Internetstiftelsen and Afnic together develop and maintain Zonemaster as a modern tool.

https://internetstiftelsen.se/en/

https://www.afnic.fr/en/

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/
- Internetstiftelsen has a customized GUI using the standard Zonemaster backend and engine on https://zonemaster.iis.se/
- There are more installations around the world, both public and private.

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 2021-06-01
- Translated into several languages (Danish, English, Finnish, French, Norwegian and Swedish)

Thank you!

Any questions on Zonemaster:
mats.dufberg@internetstiftelsen.se