



FRED integrates Zonemaster

ICANN82 – TechDay – Seattle

Technical checks

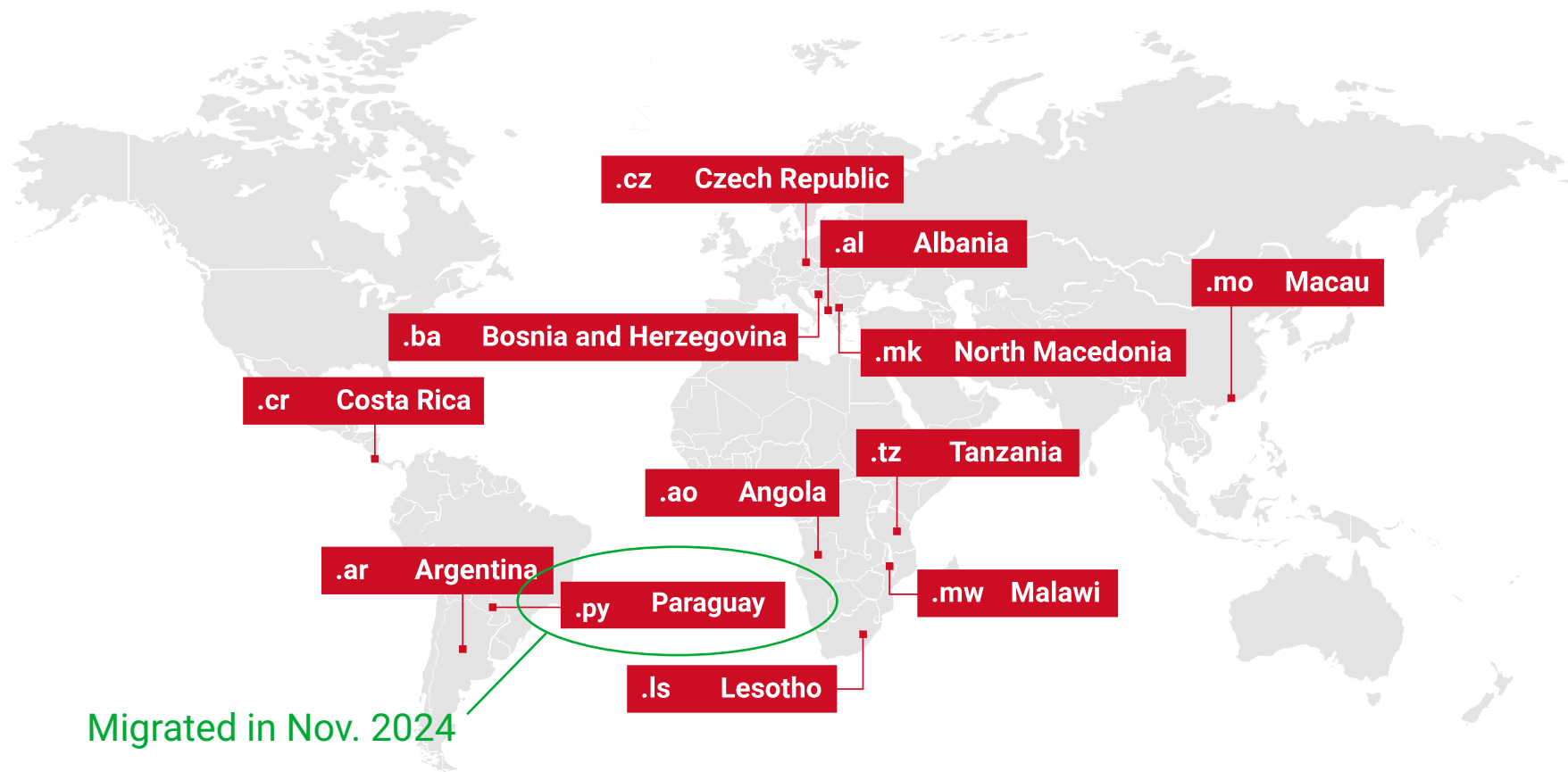
- Many domain registries are checking correctness of delegations for registered domains
- Two main approaches:
 - Pre-delegation / Strict
 - Badly configured nameservers prevent delegation of domain
 - PTI/IANA for TLD delegations in the root zone
 - Post-delegation / Liberal
 - Domain is delegated even with broken configurations
 - Technical check results are mainly service for domain operators to inform them about status
 - Fixing unintended errors helps to have healthy infrastructure
 - In CZ.NIC we used this approach in our registry solution FRED

FRED



- Open source registry solution
- EPP, WHOIS, RDAP, DNSSEC with automation via CDNSKEY scanning, ...
- Developed (and used) by CZ.NIC since 2006
- Website: <https://fred.nic.cz>
- Documentation: <https://fred.nic.cz/documentation/html/>
- Source code: <https://gitlab.nic.cz/fred>
- It is possible to order support (consultations, help with migration, NBD responses...)

Who uses FRED



FRED approach in the past

- Post-delegation technical checks are in the system from beginning
- Two methods of invocation
 - Regular automated check
 - Once a month
 - Result goes via e-mail to technical contacts
 - Registrar could invoke check via EPP command
 - Possibility to check nameservers for not yet delegated domain
 - Result is passed in poll message
- Attribute on nameserver set for requested report level of checking
 - Integer value from “no checks” up to “all checks”
 - Set via EPP

FRED approach in the past

- System implemented just a few checks
 - Existence – nameservers respond
 - Presence – domain is present on nameservers
 - DNSSEC – DNSSEC is correctly configured
 - Software diversity – different nameserver software
 - Network diversity – different AS
- Set of Python scripts mostly using tool *drill* and others from *ldns-utils*
- Scheduler in Python that selects and invoke tests

Challenges of old approach

- Implemented as part of bigger group of services call “PyFRED” where all other services have already been migrated out
- Old Python 2.7 code and usage of CORBA interfaces to the backend that is being deprecated
- Not very well working re-try mechanism
- Queues with scheduled checks started to be overloaded
- Sometimes system had to be “kicked on” by restarting
- Invocation via EPP was not used at all
- Limited number of checks
- Why to work on this when there are better open source tools?

- Open source tool for checking delegations
- Implemented by registries of .SE and .FR since 2013
- Website <https://zonemaster.net/>
- Source code <https://github.com/zonemaster/>
- Documentation <https://doc.zonemaster.net/latest/>
- Around 75 tests
- Each check perfectly documented <https://doc.zonemaster.net/latest/specifications/tests/index.html#list-of-defined-test-cases>

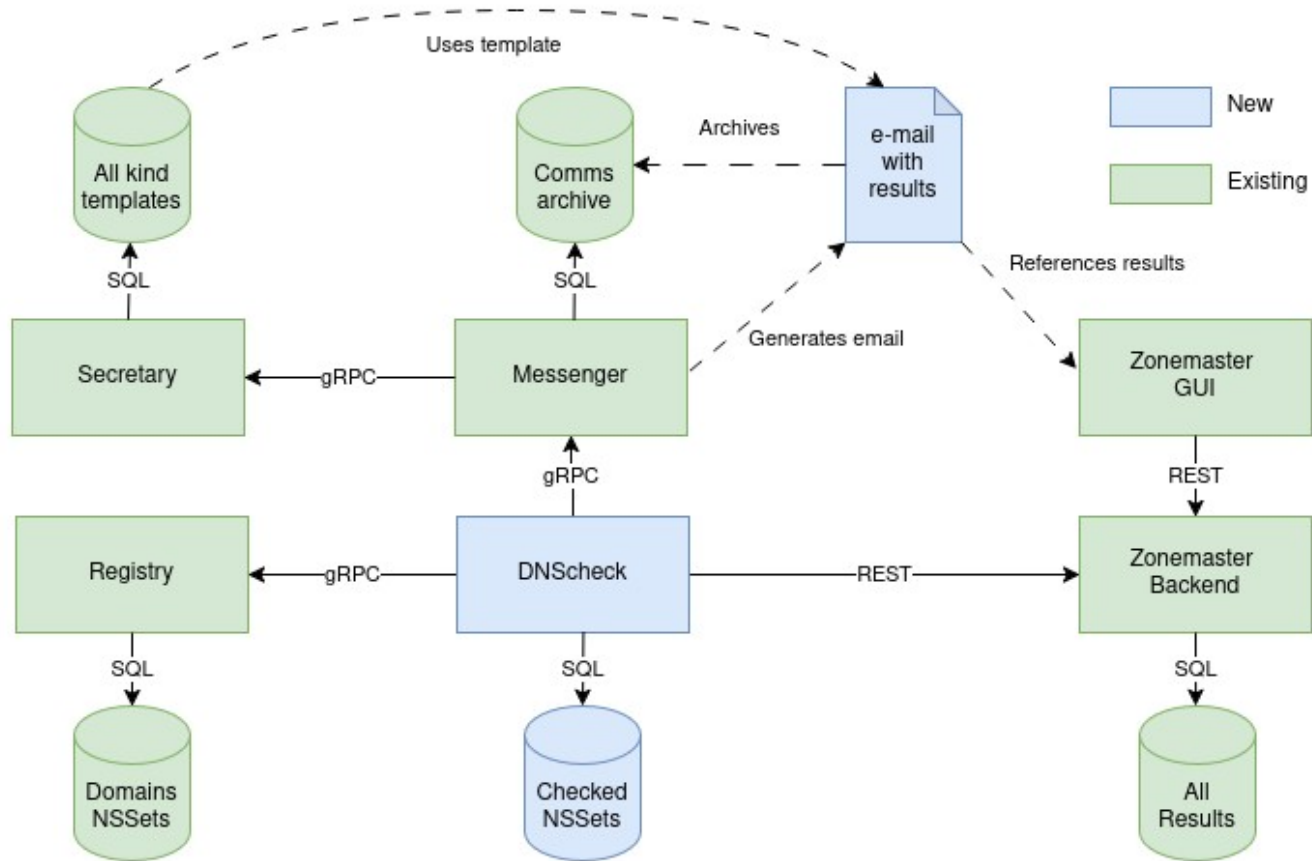
New DNScheck module

- In 2023 we stopped old service
- In 2024 we developed a new module called DNScheck that integrates registry backend with Zonemaster
 - Modern Python
 - SQLAlchemy ORM framework for database administration
 - Using gRPC instead of CORBA RPC
 - Distributed as Docker
- Launched in production in December 2024

DNScheck features

- We kept idea of regular automated checks of all delegated domains with reporting results of these checks via e-mail to technical contacts
 - Scheduler works on the list of active nameserver sets that is synced daily from registry database
 - Nameserver sets are selected based on longest time since last check, but keeping minimal length from last control (24 days)
 - Speed is about 5000 domains per hour (whole registry can be checked in less than 2 weeks)
- We had to re-map report levels on existing nameserver sets
 - New levels are (0 – no check, 1 – only CRITICAL, 2 – also ERRORS, 3 - also WARNINGS, 4 – also NOTICE)
- Invocation via EPP was abandoned since there is a Zonemaster GUI that can take over the same role – <https://zonemaster.nic.cz>

DNScheck architecture



https://gitlab.nic.cz/fred/dnscheck/

README.rst

Fred-DNScheck

Fred-DNScheck is a service for healthchecking DNS records and nameservers.

Learn more about the project and our community on the [FRED's home page](#)

Configuration

DNScheck searches for configuration files in following order:

1. Configuration file set by `DNSCHECK_CONFIG` environment variable.
2. `~/fred/dnscheck.conf`
3. `/etc/fred/dnscheck.conf`

The configuration file is in YAML format with following options:

Service connections

db_connection

Database connection string. Default is `sqlite://` which creates in-memory SQLite database. This is only useful for testing purposes, since all data from the in-memory database will be lost when the process terminates.

db_echo

If `True`, DNScheck logs every performed SQL query. Default is `False`.

db_poolclass

Dotted path to database poolclass. E.g. `psycopg_pool.NullConnectionPool`. Default is `None`.

db_schema

Database schema to use for DNScheck database. Default is `None`, meaning no schema is used.

messenger_netloc

Network location, i.e. host and port, of the messenger service. Default is `None`, which disables the email notification.

messenger_ssl_cert

Path to file with SSL root certificate. Default is `None`, i.e. no SSL encryption.

registry_netloc

Network location, i.e. host and port, of the registry service. This setting is required.

registry_ssl_cert

Path to file with SSL root certificate. Default is `None`, i.e. no SSL encryption.

zonemaster_api_url

URL of Zonemaster RPC API (e.g. `https://zonemaster.example.com/api/`). Default is `http://localhost/`.

zonemaster_language

ISO 639-1 language code supported by Zonemaster. Default is `en`.

Limits

check_once_per_month

If true, each nsset will be checked at most once in each calendar month. Default is `True`.

domain_zones

List of allowed domain zones. Domains out of these zones are disregarded. Example value is `["org", "com"]`. If empty, domains from all the zones are processed. Default is `[]`, meaning there is no filter.

max_domain_checks

Maximum concurrent domain checks. This limits the load put on Zonemaster. Default is `30`.

max_notified_domains

Maximum number of bad domains reported in notification email. Default is `10`.

min_check_interval

Required minimum interval between NSSET checks of the same NSSET. See [acceptable formats](#). Value of `check_once_per_month` is still honored in addition to this setting. Default is 24 days.

Sample e-mail

Hello,

we would like to inform you about the results of the technical check for the nameserver set NSSET-ID-1234. For more information about technical checks, please visit: <https://podpora.nic.cz/en/domains/#technical-checks-nameserver-sets>.

We recommend reviewing the status and configuration of your DNS and nameservers. If necessary, please contact your technical administrator of the nameserver set or the person responsible for managing the listed domains.

Check date: 07.03.2025 14:25:21 CET

Number of detected errors on checked domain names:

- Severity Error: 8
- Severity Critical: 2

This nameserver set is authoritative for the domain names listed below. We provide a link to the error report detail for up to 50 domain names with the worst results.

You can modify the settings for receiving information about checks on this nameserver set with your registrar REGISTRAR-ID.

Domain name test results:

example-1.cz: <https://zonemaster.nic.cz/cs/result/59dde79387f7gds3>

example-2.cz: <https://zonemaster.nic.cz/cs/result/d3420bb20basf2rc>

Your sincerely

Support of CZ.NIC, the CZ domain registry

Recipient's feedback

- Over December and January, we have significant increase on our customer support lines
 - People didn't understand what does it mean and what to do
 - People who partially understand wanted to explain why the test is failing and how to fix it
 - Sometimes they were sending questions directly to Zonemaster developers
- Several rounds of changes in text of e-mail
- The wave of questions dropped over time

Feedback to Zonemaster

- Working on full Czech translation
- Suggestion to change error level of some checks
 - Non zero iterations in NSEC3 parameters - ERROR → WARNING
 - <https://github.com/zonemaster/zonemaster/pull/1352>
 - Missing DNSSEC - NOTICE → WARNING
 - <https://github.com/orgs/zonemaster/discussions/1364>

Statistics from February

- Total domains scanned – 1 474 205
- Statistics based on worse result for the domain:
 - Critical: 55 512 (3.8%)
 - Error: 389 264 (26.4%)
 - Warning: 783 071 (53.1%)
 - Notice + Info: 246 359 (16.7%)

Future plans

- Updating FRED installation guide and FRED demo VM to include DNScheck
 - Registries using FRED are encouraged to migrate to the most recent version
- Tracking zone health in time and integrate results into statistics portal
- Integration into registrant portal (just ideas)
 - Setting the report level directly
 - Definition and selection of various checking profiles as provided by Zonemaster
 - Invocation of checks for select group of owned domains
 - Displaying history of checks and trends for owned domains

Thank you for watching!