credence ˈkrēdns
noun
1 belief in or acceptance of something as true: psychoanalysis
finds little credence among laymen.
• the likelihood of something being true; plausibility: being
called upon by the media as an expert lends credence to one’s
opinions.
2 [usu. as modifier] a small side table, shelf, or niche in a
church for holding the elements of the Eucharist before they
are consecrated: a credence table.
Within the DNS

Put aside the zone and test it, before further distribution.

Simple Architectural element

Prevent Bogus Zones getting out in the world
Not the only tool around

OpenDNSSEC Auditor

dnssec-monitor

jdnssec-tools

SurfNET DNSSEC Checker

Keychecker

vantages D-Sync

Validdns

AFNIC ZoneCheck

ldns-verify-zone

YAZVS

Validation by querying zones

Validation by verifying zonefiles
Validation by verifying zone files

Provisioning system

Public Authoritative Nameservers

Validation by querying zones

Check in the data plane before serving

our goal

Post-factum

With minimal interference

And allow current tools to be reused
In fact it is an NSD3.2 fork

Proven code

Public Authoritative Nameservers

Credns is just another nameserver

Provisioning system

Hidden Master

Hidden Master

In fact it is an NSD3.2 fork

Proven code
Incoming xfr spawns a process with a copy of the new zone.

We use that process to perform checks on, and only when those succeed the new process takes over.
Checks, What Checks?

All controlled by one process and pre-publication

Validation by querying zones

server:
  verifier-ip-address: 127.0.0.1
  verifier-port: 5347

zone:
  name: example.com

  [...]
  verifier: drill -S -k example.com.ds @localhost -p 5347 example.com SOA

Validation by verifying zonefiles
Credns is not NSD
==================
WARNING! Because credns is implemented as a fork of NSD3, it currently functions as a complete authoritative DNS nameserver and will actually answer queries for zones that were deemed correct by a verifier. However, this functionality is not necessary for credns type operation and should disappear in future releases. It is recommended not to rely on credns's ability to answer queries to the public. In future releases credns might well be answering queries to verifiers only. Credns has a different orientation as NSD and might develop into an entirely different direction.
Alternative Configuration

Provisioning system

Pull on signal

Hidden Master

Credns performs checks without becoming part of the datapath

Prevent puling zone after failure by tweaking SOA
For the future

Check on IXFR fragments (specialize on only diffs)

For now

We want you to share your needs and experiences

Wishlist

Framework improvements

More reporting options e.g. Nagios, Mail, flashing lights

User contributed plugin directory

For now
If you use our software then consider to support NLnet Labs’ mission Financially:
http://www.nlnetlabs.nl/labs/contributors/

That’s it folks

Questions to:
labs@nlnetlabs.nl

This work was partly funded through a grant from the RIPE NCC

Thursday, June 21, 12