

Credns

formally known
as dnssexy

credence ^['krēdns]

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.*

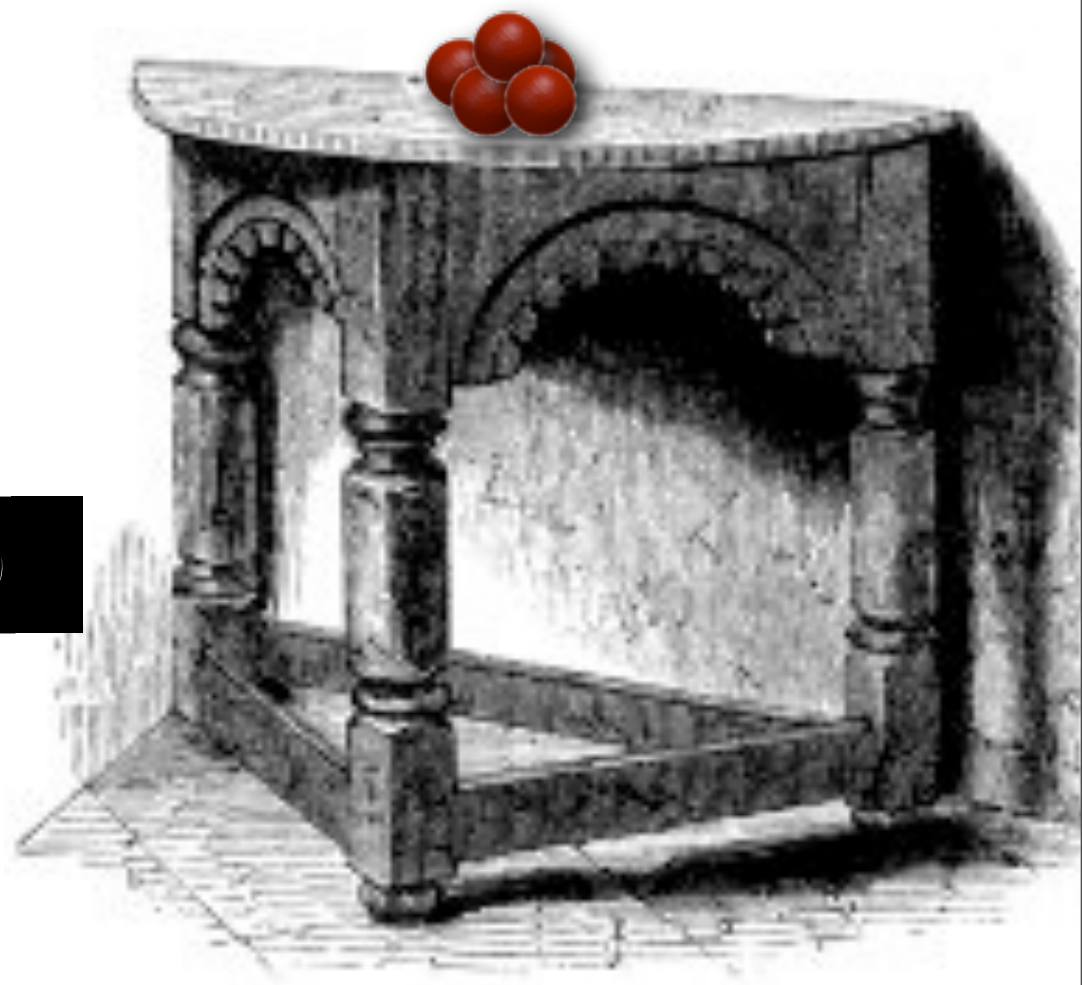
htt
©20

Simple
Architectural
element

Within the
DNS

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

PREVENT BOGUS ZONES
GETTING OUT IN THE WORLD



Not the only tool
around

OpenDNSSEC
Auditor

jdnssec-tools

navgal

validns

.SE
dnssec-monitor

SurfNET
DNSSEC
Checker

Vantages D-
Sync

AFNIC ZoneCheck

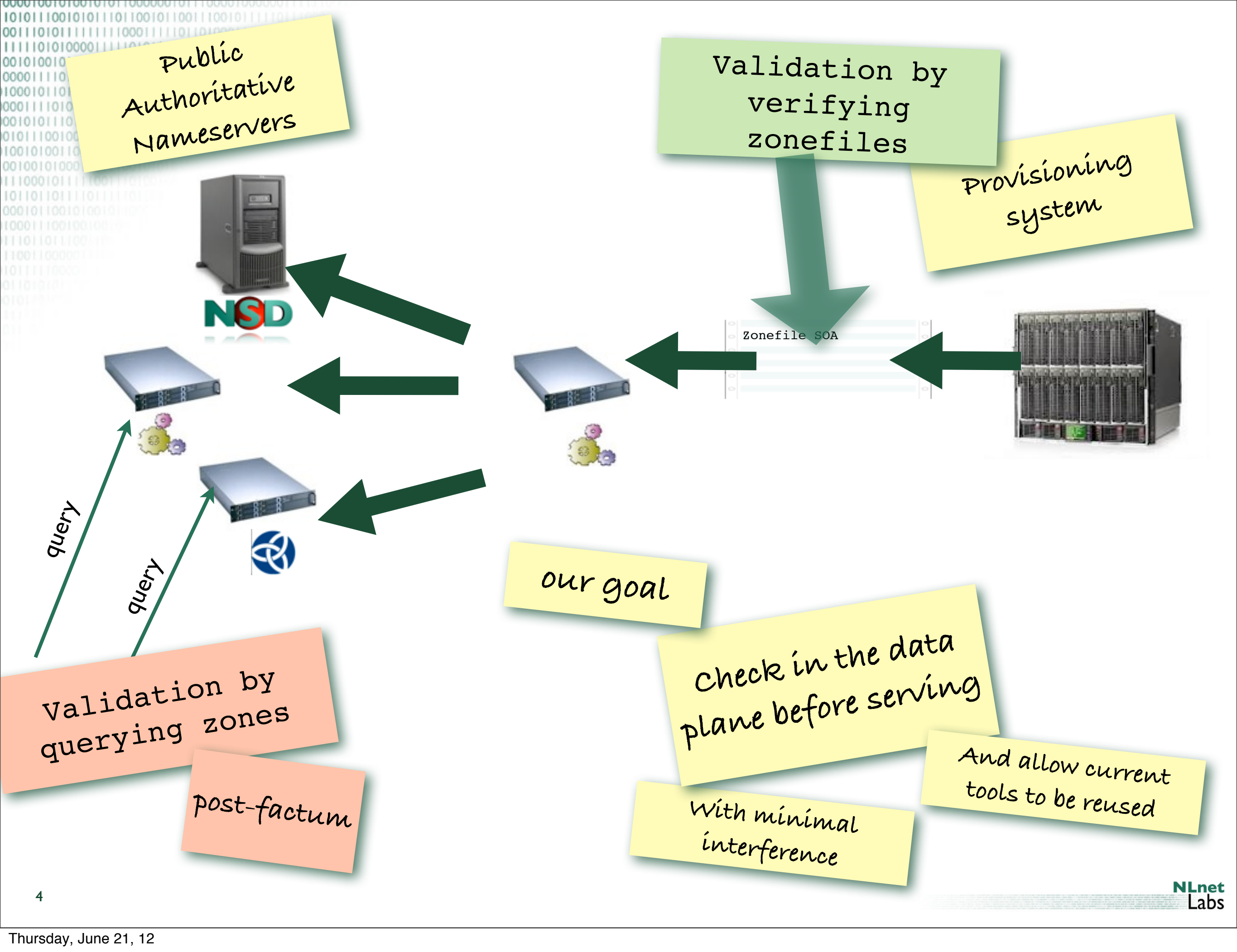
Keychecker

YAZVS

ldns-verify-zone

Validation by
querying zones

Validation by
verifying
zonefiles



Public
Authoritative
Nameservers

Hidden Master

Provisioning
system

Credns

NSD

Hidden Master

Credns is just
another nameserver

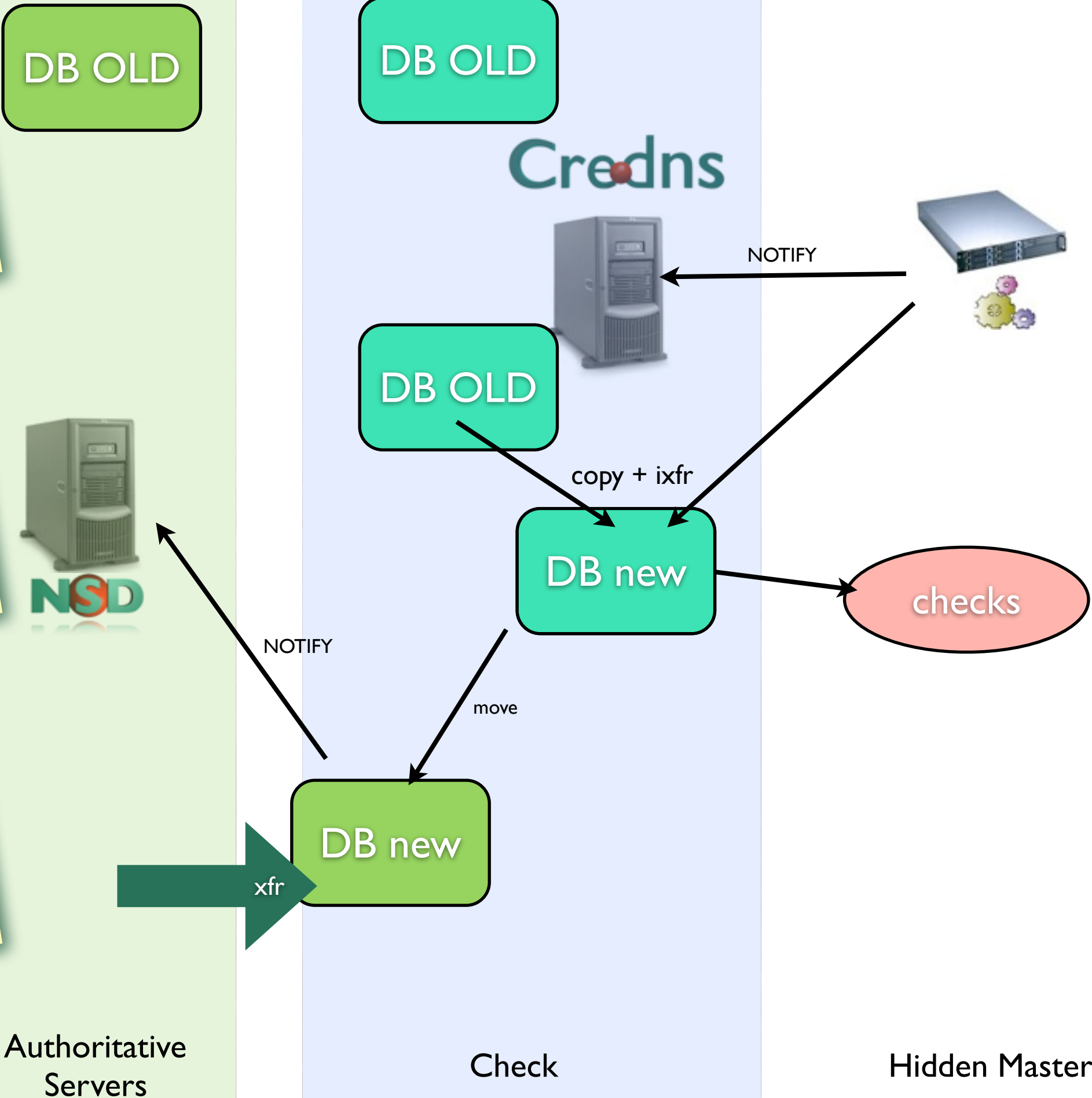
In fact it is an
NSD3.2 fork

Proven code

NSD 3.2 properties

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?

```
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
querying zones

All controlled by
one process and
pre-publication

```
zone:  
    name: example.com  
    [...]  
    verifier: ldns-verify-zone -V2  
    # alternative  
    # verifier: validns -
```

Validation by
verifying
zonefiles

credns
as NSD fork

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

PULL ON SIGNAL

Provisioning system

Hidden Master

notify

notify

Prevent pulling zone after failure by tweaking SOA

Credns performs checks without becoming part of the datapath

Credns

For the future

Wishlist

Framework
Improvements

Checks on IXFR
fragments (specialize
on only diffs)

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

User contributed plugin
directory

For now

We want you to share
your needs and
experiences





That's it folks

*Questions to:
labs@nlnetlabs.nl*

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

If you use our software then consider to support
NLnet Labs' mission Financially:

<http://www.nlnetlabs.nl/labs/contributors/>

**NLnet
Labs**

© 2006-2010 NLnet Labs