

Results from project DNS

IETF 109
November 9-13, 2020
Online

* Town Square - Community OARC Mattermost

DNS-OARC

Community @willem

Town Square

231

Welcome to the OARC chat server.

willem 09:50

@here FYI, I've created a public [~IETF109 Hackthon](#) channel for coming up with ideas for the Hackathon at the IETF109 next week that you can all join. It can be used for communication on projects during the hackathon too.
(edited)

Write to Town Square

Help

14 signed up – but most(all) also still working as usual...

Hacks – DNS Error Reporting

- [draft-arends-dns-error-reporting](#)
- Like Extended DNS Errors [[RFC8914](#)],
but reporting to authoritative instead of querier

* IETF109 Hackthon - Community OARC Mattermost

DNS-OARC

Community @willem

PUBLIC CHANNELS

- catalog-zones
- IETF109 Hackthon
- OARC Software
- Off-Topic
- Town Square
- Workshops
- XDP & eBPF
- More...

PRIVATE CHANNELS

- open-source-dns

DIRECT MESSAGES

- anshu1910
- axel
- banburybill, jan, s...

Switch Channels - CTRL+K

IETF109 Hackthon

Enter your projects here: <https://trac.ietf.org/trac/ietf/me...>

royarends 12:12

Hi folks!

I'm setting up some zones and infra for dns-error-reporting. I'm looking for existing, portable, purposely broken zones 😊

habbie 12:14

servfail.nl, dnssec-failed.org, the sidnlabs workbench, the root canary domain set

royarends 12:14

brilliant habbie, I'll have a look

habbie 12:15

`1400.v4.big.7bits.nl` (assuming your resolver's bufsize is smaller than 1467)

(also 'v6' and 'vx')

(you can adjust the number as needed)

royarends 12:17

I'd need to have some of this data on a server that would return the edns0 option with an agent domain.

habbie 12:17

oh, right!

royarends 12:19

I'll have a look at <https://workbench.sidnlabs.nl/zones/>

Write to IETF109 Hackthon

Help

Reporting

ng

014],

ad of querier

```
willem@makaak: ~
willem@makaak:~$ dig @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednsopt=58160

; <<>> DiG 9.16.6-Ubuntu <<>> @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednsopt=58160
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 51281
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1232
; OPT=58160: 06 72 65 70 6f 72 74 09 6e 6c 6e 65 74 6c 61 62 73 02 6e 6c 00 (".report.nlnetlabs.nl.")
;; QUESTION SECTION:
;broken.nlnetlabs.nl.          IN      TXT

;; AUTHORITY SECTION:
nlnetlabs.nl.                240     IN      SOA     ns.nlnetlabs.nl. hostmaster.nlnetlabs.nl. 2020110905 2
8800 7200 604800 240

;; Query time: 0 msec
;; SERVER: 2a04:b900::8:0:0:60#53(2a04:b900::8:0:0:60)
;; WHEN: do nov 12 15:56:50 CET 2020
;; MSG SIZE rcvd: 123

willem@makaak:~$
```

```
willem@makaak: ~  
willem@makaak:~$ dig @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednsopt=58160  
; <<>> DiG 9.16.6-Ubuntu <<>> @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednsopt=58160  
report.nlnetlabs.nl/dnstap.log.20201109 - Chromium  
report.nlnetlabs.nl/dnstap x +  
Niet beveiligd | report.nlnetlabs.nl/dnstap.log.20201109  
20:30:23.908827 AQ 2a10:3781:85e:0:61d3:eff2:5c0c:e088 UDP 57b "7.1.broken.test._er.report.nlnetlabs.nl." IN TXT  
20:30:32.634195 AQ 2a10:3781:85e:0:61d3:eff2:5c0c:e088 UDP 57b "7.1.broken.test._er.report.nlnetlabs.nl." IN NULL  
20:35:41.150998 AQ 52.73.169.169 UDP 47b "www.cybergreen.net." IN A  
21:09:17.960700 AQ 66.185.123.248 UDP 52b "_eR.rEpORT.nLnetlabs.NL." IN A  
21:09:17.961505 AQ 66.185.123.248 UDP 52b "_er.report.nlnetlabs.nl." IN NS  
21:15:06.572294 AQ 192.241.208.169 UDP 30b "VERSION.BIND." CH TXT  
22:11:57.139319 AQ 2620:0:2830:211::35 UDP 79b "well.done.willem.I.love.it._er.report.nlnetlabs.nl." IN A  
;; SERVER: 2a04:b900::8:0:0:60#53(2a04:b900::8:0:0:60)  
;; WHEN: do nov 12 15:56:50 CET 2020  
;; MSG SIZE rcvd: 123  
willem@makaak:~$
```

Hacks – DNS Error Reporting

- [draft-arends-dns-error-reporting](#)
- Like Extended DNS Errors [[RFC8914](#)], but reporting to authoritative instead of querier
- Testing environment & 1 auth implementation ready
<https://github.com/NLnetLabs/nsd/tree/features/draft-arends-dns-error-reporting>
- Resolver implementations coming soon...
Knot, PowerDNS, Unbound all have EDE branches

Hacks -

- [draft-arends-](#)
- Like Extended but reporting to
- Testing environ
<https://github.com/NLne>
- Resolver imple
Knot, PowerDNS

* IETF109 Hackthon - Community OARC Mattermost

DNS-OARC

IETF109 Hackthon

habbie
i do worry about the operational impact of starting to send an EDNS option to the world

willem 12:31
Good point

habbie 12:31
which I wish was something I did not have to worry about in 2020, but here we are 😊

willem 12:31
Something that could be measured maybe

habbie 12:32
ednscmp already knows a lot; but 'how many auths are broken' does not tell us 'how many users will cry'

willem 12:32
true... though that could maybe be measured too

willem
by comparing broken auths to the DITL logs for example...

Write to IETF109 Hackthon

Hacks – Message Digest for DNS Zones

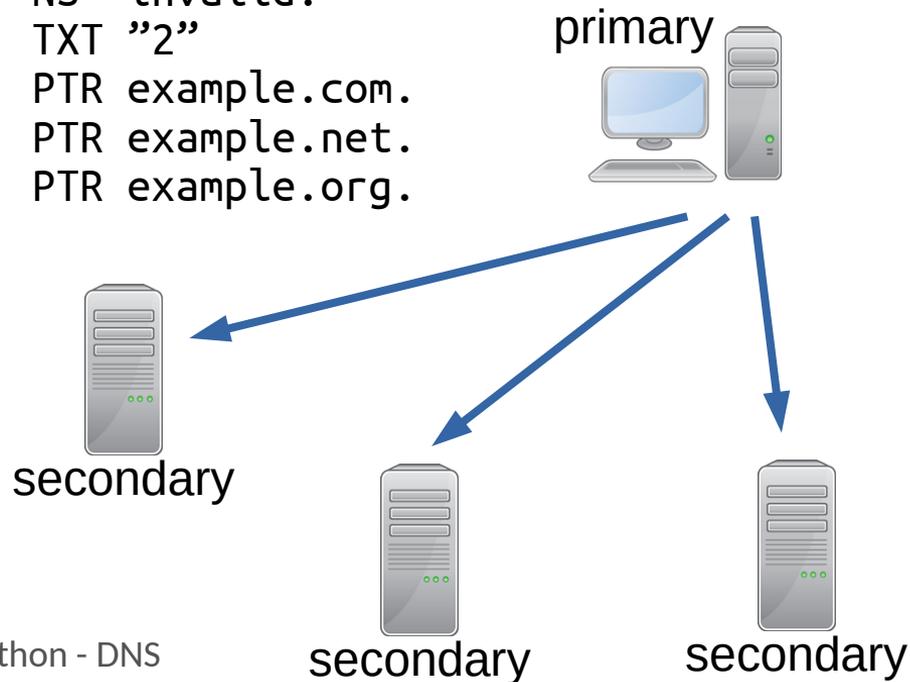
- [draft-ietf-dnsop-dns-zone-digest](#)
- DNSSEC : Integrity and Authenticity for RRsets
- ZONEMD: Integrity and Authenticity for complete zones
- PoC `ldns` tool existed, but was a bit cumbersome to sign:
 - add ZONEMD RR with tool
 - `ldns-signzone`
 - run tool again to equip and sign the ZONEMD RR
- Now, do all this at once with new `-z` option to `ldns-signzone`
- <https://github.com/NLnetLabs/ldns/tree/features/draft-ietf-dnsop-dns-zone-digest>

Hacks - Catalog Zones

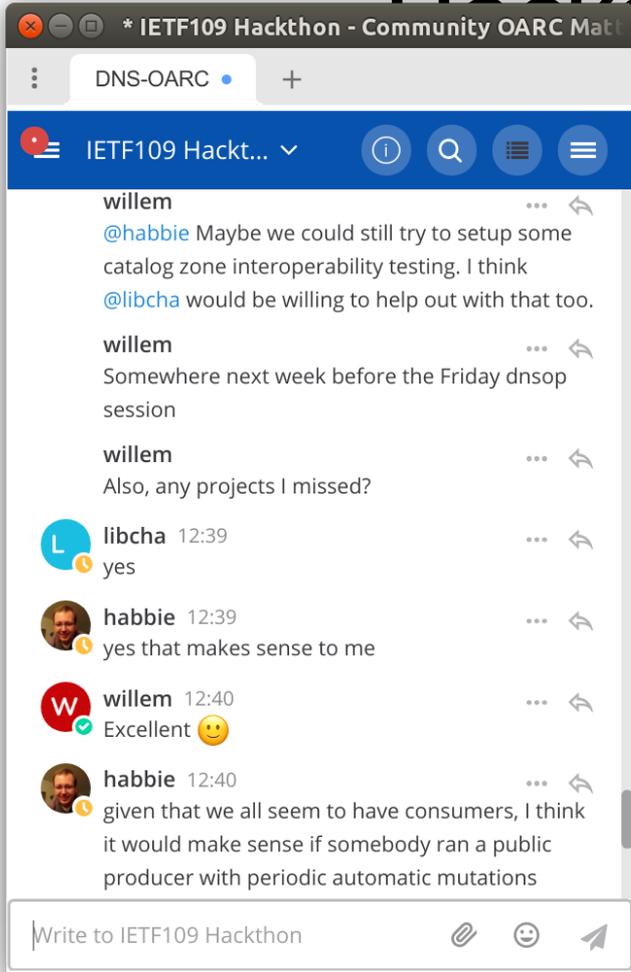
- draft-toorop-dnsop-dns-catalog-zones

```
$ORIGIN catzone.
```

```
@           IN  SOA  . . 1552507036 86400 14400 86400 0  
@           IN  NS   invalid.  
version     IN  TXT  "2"  
<unique-id-1>.zones IN PTR example.com.  
<unique-id-2>.zones IN PTR example.net.  
<unique-id-3>.zones IN PTR example.org.
```



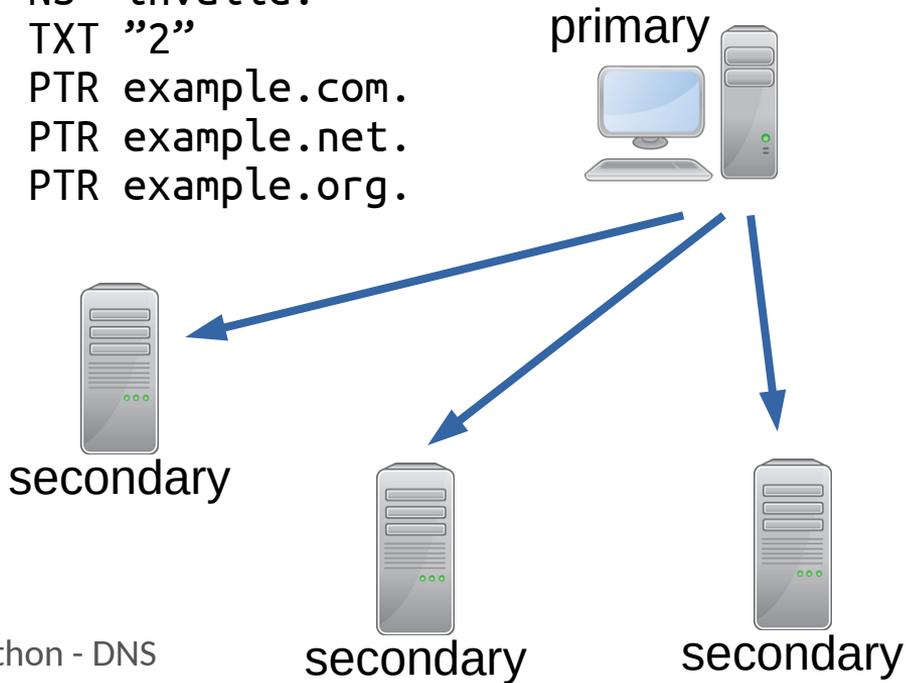
Hacks - Catalog Zones



top-dns-catalog-zones

one.

```
IN SOA . . 1552507036 86400 14400 86400 0
IN NS invalid.
IN TXT "2"
>.zones IN PTR example.com.
>.zones IN PTR example.net.
>.zones IN PTR example.org.
```



Hacks – Catalog Zones

- draft - toorop - dnsop - dns - catalog - zones
- Interoperability testing



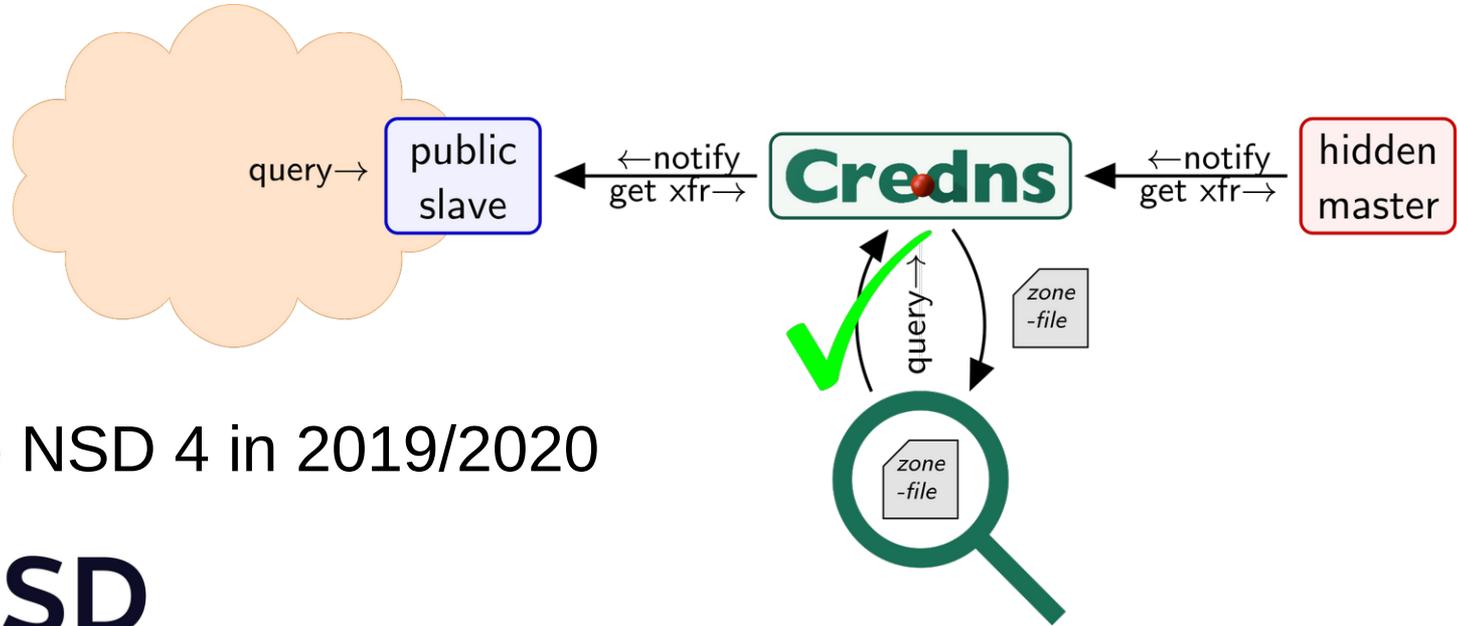
- Consumes version 2 Catalog Zones since version 3.0.0
(September 2020)
- Producer in the make



- Proof of Concept hack: PowerCATZ
(October 2016)

Hacks - Catalog Zones

- Interoperability testing

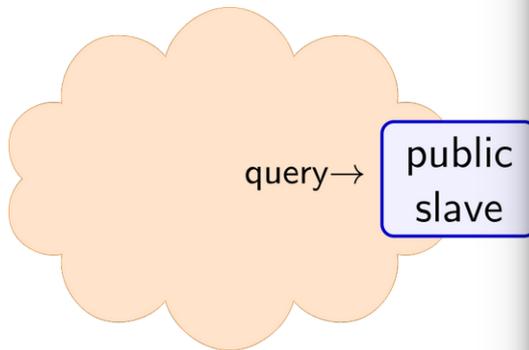


- Ported to NSD 4 in 2019/2020

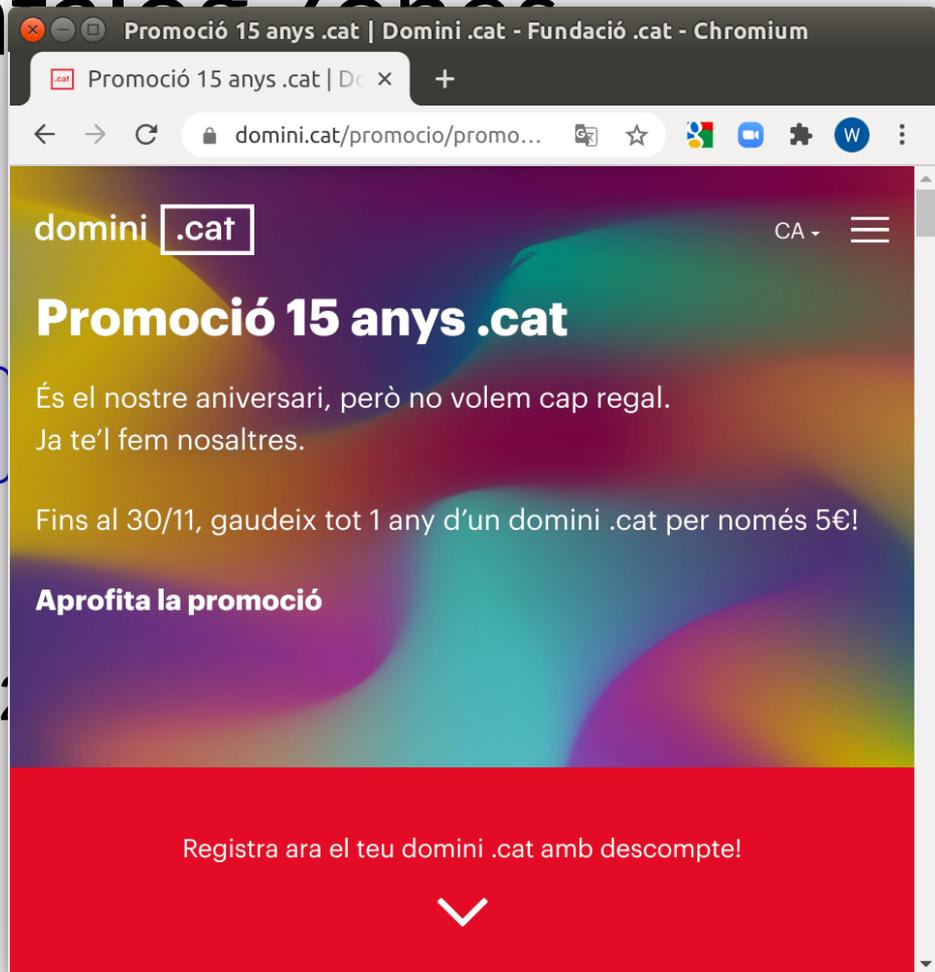


Hacks – Cateles Zones

- Interoperability testing



- Ported to NSD 4 in 2019/2020



Hacks - Catalog Zones

```
root@ns1: /etc/nsd/nsd.conf.d
root@ns1: /etc/nsd/nsd.conf.d 91x13
zone:
  name: "zones.cat"
  include-pattern: "secondary"
  allow-notify: ::0/0 tsig.zones.cat.
  allow-notify: 0.0.0.0/0 tsig.zones.cat.
  request-xfr: 2a04:b900:0:100::53 tsig.zones.cat.
  request-xfr: 185.49.141.53 tsig.zones.cat.
  provide-xfr: ::0/0 NOKEY
  provide-xfr: 0.0.0.0/0 NOKEY
  verify-zone: yes
  verifier: /usr/local/bin/ldns-verify-zone -S -k /var/lib/unbound/root.key -V4

root@ns1:/etc/nsd/nsd.conf.d#
root@ns1: ~ 91x5
Nov 18 16:32:00 ns1 nsd[2323]: verify: started verifier for zone zones.cat (pid 2328)
Nov 18 16:32:00 ns1 nsd[2323]: Zone digest matched the zone content
Nov 18 16:32:00 ns1 nsd[2323]: Zone is verified and complete
Nov 18 16:32:00 ns1 nsd[2323]: verify: verifier for zone zones.cat (pid 2328) exited with 0
:[]
```

- Interoperab

The screenshot shows a Chromium browser window with the title "DNS Catalog Zones - Implementations & Interoperability - Chromium". The address bar shows the URL "zones.cat/implementations...". The page content includes a navigation bar with links for "About", "Implementations & Interoperability", and "draft-ietf-dnsop-dns-catalog-zones". The main heading is "DNS Catalog Zones - Implementations & Interoperability". Below the heading is a bulleted list of implementation details. At the bottom of the page is a table with four columns: "Server", "Software", "catalog1.", and "catalog2.". The table lists four servers: ns1.zones.cat, ns2.zones.cat, ns3.zones.cat, and ns4.zones.cat, along with their respective software (NSD or Knot DNS or PowerDNS) and their roles as Producer or Consumer.

About | [Implementations & Interoperability](#) | [draft-ietf-dnsop-dns-catalog-zones](#)

DNS Catalog Zones - Implementations & Interoperability

- Knot DNS has DNS Catalog Zones since [Knot DNS Version 3.0.0](#)
 - [Documentation](#)
 - [catalog_generate](#) Branch for generating Catalog Zones
- [PowerCATZ](#) program to handle Catalog Zones with PowerDNS
- [NSDCatZ](#) PoC scripts for producing and consuming Catalog Zones with NSD (version from [zone-verification branch](#))

Server	Software	catalog1.	catalog2.
<code>ns1.zones.cat</code>	NSD	Producer	Consumer
<code>ns2.zones.cat</code>	NSD	Consumer	Consumer
<code>ns3.zones.cat</code>	Knot DNS	Consumer	Producer
<code>ns4.zones.cat</code>	PowerDNS	Consumer	Consumer

What we learned

- I miss the in-person hackathon & meeting!
 - better ad-hoc conversations & social interaction
 - dedicated time-slot
- Online hackathon still worth it, because
 - implementers focus on new ideas and standards
 - still good input for the workgroup

What we learned

- I miss the in-person hackathon & meeting!
 - better ad-hoc conversations & social interaction
 - dedicated time-slot
- Online hackathon still worth it, because
 - implementers focus on new ideas and standards
 - still good input for the workgroup

