Results from project DNS

IETF 109
November 9-13, 2020
Online
IETF Hackathon - DNS

Hackathon Plan

• What problem were you working on?
• What drafts/RFC's were involved?
• Specific problems to solve
• How you planned to solve it?

2

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

IETF Hackathon - DNS
Hacks – DNS Error Reporting

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

Hacks – DNS Error Reporting

- draft-arends-dns-error-reporting
- Like Extended DNS Errors (RFC8914), but reporting to authoritative instead of querier.
willemmakaak:$ dig @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednseopt=58160

; <<>> DiG 9.16.6-Ubuntu <<>> @ns.nlnetlabs.nl broken.nlnetlabs.nl TXT +ednseopt=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 6f 66 65 74 6c 61 62 73 02 6e 6f 66 65 20 (".report.nlnetlabs.nl")
; QUESTION SECTION:
;broken.nlnetlabs.nl. IN TXT

; AUTHORITY SECTION:
;ns.nlnetlabs.nl. 240 IN SOA ns.nlnetlabs.nl. hostmaster.nlnetlabs.nl. 2020119052 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 rcd: 123
IETF Hackathon - DNS

DNS - Hacks

- draft-arends-dns-error-reporting
  - Like Extended DNS Errors [RFC8914]
    - but reporting to authoritative instead of querier
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 – 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

IETF Hackathon - Community OARC Mattermost

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
ednscomp 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...
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](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

draft-toorop-dnsop-dns-catalog-zones

A zone.

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.

secondary

primary

secondary

secondary
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

IETF Hackathon - DNS
Hacks – Catalog Zones

• Interoperability testing

• Ported to NSD 4 in 2019/2020
Hacks – Catalog Zones

• Interoperability testing
• Ported to NSD 4 in 2019/2020
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)

<table>
<thead>
<tr>
<th>Server</th>
<th>Software</th>
<th>catalog1</th>
<th>catalog2</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns1.zones.cat</td>
<td>NSD</td>
<td>Producer</td>
<td>Consumer</td>
</tr>
<tr>
<td>ns2.zones.cat</td>
<td>NSD</td>
<td>Consumer</td>
<td>Consumer</td>
</tr>
<tr>
<td>ns3.zones.cat</td>
<td>Knot DNS</td>
<td>Consumer</td>
<td>Producer</td>
</tr>
<tr>
<td>ns4.zones.cat</td>
<td>PowerDNS</td>
<td>Consumer</td>
<td>Consumer</td>
</tr>
</tbody>
</table>
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