Results from project DNS

IETF 109
November 9-13, 2020
Online
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
Hacks – DNS Error Reporting

- draft-arends-dns-error-reporting
- Like Extended DNS Errors [RFC 8914], but reporting to authoritative instead of querier
Like Extended DNS Errors [RFC8914], but reporting to authoritative instead of querier.
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

- **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 all have EDE branches

hbbie 12:31
i do worry about the operational impact of starting to send an EDNS option to the world

willem 12:31
Good point

hbbie 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

hbbie 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

@. IN SOA . . 1552507036 86400 14400 86400 0
@. IN NS invalid.
@. 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.

willem
@hbbie Maybe we could still try to setup some catalog zone interoperability testing. I think @libcha would be willing to help out with that too.

willem
Somewhere next week before the Friday dnsop session

willem
Also, any projects I missed?

libcha 12:39
yes

hbbie 12:39
yes that makes sense to me

willem 12:40
Excellent 😊

hbbie 12:40
given that we all seem to have consumers, I think it would make sense if somebody ran a public producer with periodic automatic mutations
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 – 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

```
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
```

```
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
```
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