Update on the DLV Shutdown
Vicky Risk
ISC.org

source: flickr, lic cc 2.0
Marrakech Market by Jacky Jourdren
DLV, the DNS Lookaside Validator

- Created in 2006
- To allow use of DNSSEC before root and TLDs were signed
- Root and 70+% of TLDs are now signed
- DLV has accomplished what it can to assist with early adoption
Shutdown Process Initiated

Announce shutdown plan
- Feb 2015 – June 2015
  - ICANN Singapore
dlv.isc.org
www.isc.org
- Internet mailing lists
- BIND OS packagers
- NANOG 64 San Francisco
- Direct email to every user

Discourage resolver queries
- May 2015 – present
  - Update default configurations to remove DLV (BIND and BIND packages, and Unbound)
  - What else can we do here?

Remove zones
- July 2015 – June 2017
  - June 2015 request to remove broken or unnecessary delegations
  - July 2015 removed broken zones
  - March 2016 limit new zones
  - July 2016 No new zones
  - July 2016 Purge zones that can otherwise validate
  - June 2017 Purge all zones

Continue answering queries indefinitely
Broken Zones

Currently the following zones are configured in the ISC DLV registry, but are non-functional in some way. This could be due to an incomplete delegation, broken or missing keys, or some other failure. Since these are not currently serving any useful purpose, they will be removed at the end of July 2015.

example.com (Key Missing)

Can Validate

We've walked the following zones and found that they properly DNSSEC validate full from the global DNS Root. Hence, they no longer need DLV. Please remove these zones from the ISC DLV Registry at http://dlv.isc.org at your earliest convenience. Any zones that can fully validate to the Root that remain will be automatically removed at the end of 2015.

example.com
Example User Reaction

... DLV is the only way for most holders of static IP addresses to sign their reverse (in-addr.arpa/ip6.arpa) address zones. And that until that's fixed, DLV needs to remain. This problem can not be solved by contacting any registrar/registry. It's an ISP issue, and customers have no leverage.
Example User Reaction

unfortunately, although my top-level domains (elided) are DNSSEC signed, and my domain also is, the registry (elided) claims not to be able to sign second levels. Neither are they able to configure their glue appropriately. Unfortunately, even changing providers won't help, since (elided) is the TLD registry. And if they do not support DS, nobody will 😞

....

unfortunately I have no chance, but to rely on the DLV service. I am well aware, that this is conceptually a bad kludge and completely undermines the idea of how DNSSEC delegates trust.
Status of Zone Reduction

- 2867 working zones a year ago
- 2080 working zones remain today
  - ~800 working zones removed by the owner
  - many more non-working zones purged by ISC
- remaining zones may have no other secure option
<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 2015</td>
<td>Announced sunset plan @ ICANN</td>
</tr>
<tr>
<td>August 2015</td>
<td>Removed broken zones/users</td>
</tr>
<tr>
<td>Jan 2016</td>
<td>Purge zones that could otherwise validate (20% of total)</td>
</tr>
<tr>
<td>March 2016</td>
<td>No registration of new zones that could validate without DLV</td>
</tr>
<tr>
<td>July 2016</td>
<td>No registration of new zones/users</td>
</tr>
<tr>
<td>July 2016</td>
<td>Purge all zones that could validate without DLV (extended by 6 months)</td>
</tr>
<tr>
<td>July 2017</td>
<td>Remove remaining DLV records (2 yr notice)</td>
</tr>
</tbody>
</table>
Queries to DLV

- Querying the DLV puts extra burden on validating resolvers, particularly with so few actual zones in the DLV. Desirable to minimize these queries going forward.
- More than 8k qps to the DLV in 2014
- Less than 4K qps to the DLV today
  - Currently, ISC sees < 2K qps
  - Affilias sees ~2K qps average, spikes of 3K
Serving dlv.isc.org

- Our staged shutdown process will leave DLV empty by August 2017
- There will be queries made to the DLV for some time
- It is best for them to return a quick “no” than to time out
- So we will leave DNS service running on dlv.isc.org until it is no longer in use
Summary

- ISC created DLV to encourage more use of DNSSEC
- DLV has assisted those early adopters
- DLV is not a solution for the systemic problem of non-support by the whole DNS chain
Thank you

for years of providing secondary name service for dlv.isc.org
Admin mode enabled. (list all zones) (list all users) (statistics)

(add a zone for isc-ops) (list isc-ops's zones) (account info for isc-ops)

<table>
<thead>
<tr>
<th>Owner</th>
<th>isc-ops</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>0.6.0.0.0.0.5.0.1.0.0.2.ip6.arpa (delete)</td>
</tr>
<tr>
<td>DLV Status</td>
<td>✅ No problems were detected.</td>
</tr>
<tr>
<td>DNSSEC Status</td>
<td>could be secured</td>
</tr>
<tr>
<td>DNSKEY Records</td>
<td>1 (add)</td>
</tr>
<tr>
<td>Created</td>
<td>2009-11-03 23:51:46 UTC</td>
</tr>
<tr>
<td>Last Update</td>
<td>2015-06-24 16:49:04 UTC</td>
</tr>
</tbody>
</table>

**DNSKEY Records**

(add record)

<table>
<thead>
<tr>
<th>More</th>
<th>Status</th>
<th>Published</th>
<th>Key Tag</th>
<th>Flags</th>
<th>Type</th>
<th>Key (partial)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(details) (show log)</td>
<td>✅ Good</td>
<td>Yes</td>
<td>4798</td>
<td>257 (KSK)</td>
<td>RSASHA1</td>
<td>BEAAA...IzWqH8qeEx6dNSV</td>
</tr>
</tbody>
</table>
**Example: Needs DLV**

<table>
<thead>
<tr>
<th>Owner</th>
<th>Name</th>
<th>DLV Status</th>
<th>DNSSEC Status</th>
<th>DNSKEY Records</th>
<th>Created</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.0.0.0</td>
<td>✔️ No problems were detected.</td>
<td>needs DLV</td>
<td>2 (add)</td>
<td>2012-01-05 10:09:17 UTC</td>
<td>2016-01-19 19:26:47 UTC</td>
</tr>
</tbody>
</table>

**DNSKEY Records**

(Add record)

<table>
<thead>
<tr>
<th>More</th>
<th>Status</th>
<th>Published</th>
<th>Key Tag</th>
<th>Flags</th>
<th>Type</th>
<th>Key (partial)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(details)</td>
<td>Good</td>
<td>Yes</td>
<td>31008</td>
<td>256 (ZSK)</td>
<td>RSASHA1</td>
<td>AwEAA...dKPs59YDo0n24hz</td>
</tr>
<tr>
<td>(show log)</td>
<td>Good</td>
<td>Yes</td>
<td>62458</td>
<td>257 (KSK)</td>
<td>RSASHA1</td>
<td>AwEAA...o7JdBZiSSpH07E=</td>
</tr>
</tbody>
</table>

No DNSKEY records require TXT records to be added to your zone at this time. The TXT records for name `dlv.0.0.0.0.2.0.0.0.0.3.4.0.3.1.f.1.0.7.4.0.1.0.0.2.ip6.arpa` may be removed if desired. If you use DNAME, the TXT records you added are at the zone apex, and they should be removed.
~6K queries to DLV in 2014
Reduced to <2K qps today

~800 qps at our Amsterdam node
Afilias sees about 2K qps
Waning interest in DLV

Google analytics measurement of people visiting DLV portal