Is a single DNS vendor enough?

How can we make multi-vendor setups manageable?

Petr Špaček • petr.spacek@nic.cz • 2019-02-03
Outline

- A single vendor
  - Selection
  - Why not ...
- Multiple vendors
- Recommendations
- Discussion – common config interface
Selecting a vendor

- Features
- Performance
- SLA
- Price
- ...
## Selecting a vendor: Features

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
<th>Pages</th>
<th>Current Status</th>
<th>Obsoleted</th>
<th>Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC6147</td>
<td>DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers</td>
<td>32</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6604</td>
<td>xNAME RCODE and Status Bits Clarification</td>
<td>5</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6605</td>
<td>Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC</td>
<td>8</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6672</td>
<td>DNAME Redirection in the DNS</td>
<td>22</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6725</td>
<td>DNS Security (DNSSEC) DNSKEY Algorithm IANA Registry Updates</td>
<td>5</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6731</td>
<td>Improved Recursive DNS Server Selection for Multi-Interfaced Nodes</td>
<td>29</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6761</td>
<td>Special-Use Domain Names</td>
<td>13</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6840</td>
<td>Clarifications and Implementation Notes for DNS Security (DNSSEC)</td>
<td>21</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6891</td>
<td>Extension Mechanisms for DNS (EDNS(0))</td>
<td>16</td>
<td>INTERNET STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6944</td>
<td>Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status</td>
<td>7</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
<tr>
<td>RFC6975</td>
<td>Signaling Cryptographic Algorithm Understanding in DNS Security Extensions (DNSSEC)</td>
<td>9</td>
<td>PROPOSED STANDARD</td>
<td>0</td>
<td>core</td>
</tr>
</tbody>
</table>
Selecting a vendor: Performance

TLD (1M)

- Zones: 1
- DNSSEC: no
- RR count: 1M
- Content: delegations (2 NS) + glue records (A, AAAA)
- Queries: random QNAME

Other sites:
- Labs
- FRED
- BIRD
- Turris Omnia
- CSIRT
- Turris
- Web scanner powered by

APIs:

- BIND 9.12.2
- Knot DNS 2.7.0
- Knot DNS 2.6.8
- NSD 4.1.22
- PowerDNS 4.1.3

Graph:

- Response Rate
- Linux 4.15.0, TLD (1M), (2018-08-01)
- Queries per second
- Answers per second
- Response Rate
- BIND 9.12.2
- Knot DNS 2.7.0
- Knot DNS 2.6.8
- NSD 4.1.22
- PowerDNS 4.1.3
## Selecting a vendor: SLA, price, ...

<table>
<thead>
<tr>
<th>Feature</th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
<th>Platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Response time</strong></td>
<td>NBD</td>
<td>12 hours</td>
<td>6 hours</td>
<td>3 hours</td>
</tr>
<tr>
<td><strong>Resolution time (hours)</strong></td>
<td>96</td>
<td>72</td>
<td>24/48/72</td>
<td>24/48/72</td>
</tr>
<tr>
<td><strong>Early notifications</strong></td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Prioritized development</strong></td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Phone support</strong></td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Chat support</strong></td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><strong>E-mail support</strong></td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Consultancy (hours)</strong></td>
<td>–</td>
<td>8</td>
<td>24</td>
<td>72</td>
</tr>
<tr>
<td><strong>On-site support</strong></td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td><strong>Yearly fee (EUR)</strong></td>
<td>5 000</td>
<td>10 000</td>
<td>20 000</td>
<td>50 000</td>
</tr>
</tbody>
</table>
Still, you can't avoid ...

Segmentation fault (core dumped)
# CVE Number | Short Description
--- | ---
96 | [2018-5738](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5738) | Some versions of BIND can improperly permit recursive query service to unauthorized clients ([https://kb.isc.org/docs/aa-01616](https://kb.isc.org/docs/aa-01616))
95 | [2018-5737](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5737) | BIND 9.12’s serve-stale implementation can cause an assertion failure in rbtdb.c or other undesirable behavior, even if serve-stale is not enabled ([https://kb.isc.org/docs/aa-01606](https://kb.isc.org/docs/aa-01606))
94 | [2018-5736](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5736) | Multiple transfers of a zone in quick succession can cause an assertion failure in rbtdb.c ([https://kb.isc.org/docs/aa-01602](https://kb.isc.org/docs/aa-01602))
92 | [2017-3145](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3145) | Improper fetch cleanup sequencing in the resolver can cause named to crash ([https://kb.isc.org/docs/aa-01542](https://kb.isc.org/docs/aa-01542))
91 | [2017-3143](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3143) | An error in TSIG handling can permit unauthorized dynamic updates ([https://kb.isc.org/docs/aa-01503](https://kb.isc.org/docs/aa-01503))
90 | [2017-3142](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3142) | An error in TSIG handling can permit unauthorized zone transfers ([https://kb.isc.org/docs/aa-01504](https://kb.isc.org/docs/aa-01504))
89 | [2017-3141](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3141) | Windows service and uninstall paths are not quoted when BIND is installed ([https://kb.isc.org/docs/aa-01496](https://kb.isc.org/docs/aa-01496))
You cannot win with ... Knot

Knot DNS 1.4.0 (2014-01-06)
=================================

Bugfixes:
---------
- AXFR crash with specific packet
You cannot win with ... Microsoft

Microsoft Windows DNS Server Denial of Service Vulnerability

Alert ID: 53604
First Published: 2017 May 9 18:33 GMT
Version: 1
CVE-2017-0171
CWE-399
CVSS Score: Base 5.3, Temporal 4.8
You cannot win with … PowerDNS

All security advisories for the PowerDNS Authoritative Server are listed here.

- PowerDNS Security Advisory 2018-03: Crafted zone record can cause a denial of service (powerdns-advisory-2018-03.html)
- PowerDNS Security Advisory 2016-05: Crafted zone record can cause a denial of service (powerdns-advisory-2016-05.html)
- PowerDNS Security Advisory 2016-04: Insufficient validation of TSIG signatures (powerdns-advisory-2016-04.html)
- PowerDNS Security Advisory 2016-03: Denial of service via the web server (powerdns-advisory-2016-03.html)
- PowerDNS Security Advisory 2016-02: Crafted queries can cause abnormal CPU usage (powerdns-advisory-2016-02.html)
- PowerDNS Security Advisory 2016-01: Crafted queries can cause unexpected backend load (powerdns-advisory-2016-01.html)
- PowerDNS Security Advisory 2015-03: Packet parsing bug can lead to crashes (powerdns-advisory-2015-03.html)
- PowerDNS Security Advisory 2015-02: Packet parsing bug can cause thread or process abortion (powerdns-advisory-2015-02.html)
- PowerDNS Security Advisory 2015-01: Label decompression bug can cause crashes or CPU spikes (powerdns-advisory-2015-01.html)
You cannot win with ... Unbound

Incorrect proof processing for NSEC3-signed zone

<table>
<thead>
<tr>
<th>Date</th>
<th>2011-12-20</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE:</td>
<td>CVE-2011-4869</td>
</tr>
<tr>
<td>Affects:</td>
<td>Unbound 1.4.13p2 and earlier versions</td>
</tr>
<tr>
<td>Not affected:</td>
<td>Other versions</td>
</tr>
<tr>
<td>Severity:</td>
<td>Medium</td>
</tr>
<tr>
<td>Impact:</td>
<td>Denial of service (daemon crash)</td>
</tr>
<tr>
<td>Exploit:</td>
<td>DNS servers can send a malformed response that lacks expected NSEC3 records</td>
</tr>
<tr>
<td>Solution:</td>
<td>Upgrade to a newer version of Unbound</td>
</tr>
</tbody>
</table>

validator/val_nsec3.c in Unbound before 1.4.13p2 does not properly perform proof processing for NSEC3-signed zones, which allows remote DNS servers to cause a denial of service (daemon crash) via a malformed response that lacks expected NSEC3 records, a different vulnerability than CVE-2011-4528.
Cloud to the rescue?
You cannot win with ... Cloudflare

APNIC Labs/CloudFlare DNS 1.1.1.1 Outage: Hijack or Mistake?

By Aftab Siddiqui
Technical Engagement Manager for Asia-Pacific

At 29-05-2018 08:09:45 UTC, BGPMon (A very well known BGP monitoring system to detect prefix hijacks, route leaks and instability) detected a possible BGP hijack of 1.1.1.0/24 prefix. Cloudflare Inc has been announcing this prefix from AS 13335 since 1st April 2018 after signing an initial 5-year research agreement with APNIC Research and Development (Labs) to offer DNS services.

Shanghai Anchang Network Security Technology Co., Ltd. (AS58879) started announcing 1.1.0.24 at 08:09:45 UTC, which is normally announced by Cloudflare (AS13335). The possible hijack lasted only for less than 2min. The last announcement of 1.1.0.24 was made at 08:10:27 UTC. The BGPlay screenshot of 1.1.0.24 is given below:
You cannot win with ... Dyn

Post Mortem: Today's Attack To Dyn
Standard DNS Nameservers | Dyn Blog

For customers utilizing the Dyn Standard DNS platform who were impacted by a DDoS attack on our service today, the following is an account of what happened and steps we’re taking to improve. No outages were observed on the DynECT Managed DNS platform (served using an Anycast network) during the course of the event.

11:52 UTC: The Dyn Operations team began to see traffic increase to various data centers across the network. Over the next 15 minutes, the traffic increased to the point that it was clear there was a Distributed Denial of Service (DDoS) attack against all five Dyn Standard DNS name servers and the team immediately began investigating the issue. The attack brought in a tremendous amount of traffic and caused the name servers to become overwhelmed. It
Google DNS Outage: 4.7% drop in global traffic

Google's brief outage caused a noticeable drop in GoSquared Traffic

Simon Tabor on October 13, 2014

Google’s DNS service (8.8.8.8 and 8.8.4.4) went down very briefly today at 11:29am GMT. This took down Google.com at the same time – preventing website domains from being resolved and users from searching for information. Because of this, there was a noticeable drop in the number of pageviews coming into
What can we do?

The DNS was designed for **diversity**, but site admins aren't buying it. Harvard bods warn: if you want to avoid a big outage, use more than one DNS provider.

By Richard Chirgwin 1 Mar 2018 at 05:02

The world's top eight DNS providers now control 59 per cent of name resolution for the biggest Websites - and that puts the Web at risk, according to a group of Harvard University researchers.
- if your mission to another star *depends* on every single piece of complex equipment staying up with zero reboots for 200+ years, you have some serious technology problems.
Trust me, if you are going to another star, you'd better have the capabilities to handle bugs. You'd better have multiple fail-over etc.

A notion of "robustness" cannot and must not hinge on "no bugs". That's unrealistic.
Multiple vendors: advantages

- Avoids SPOF
  - "packet-of-death" unlikely
- Lessens pressure
  - 9:00 Monday vs.
    - 2:15 Saturday (or Christmas day)
- Cheaper support contracts?
Multiple vendors: costs

- Selection process $N$ times
- Higher operational complexity
  - multiple configurations
  - monitoring
  - automation!
- More paperwork (SLAs etc...)

CZ.NIC | CZ DOMAIN REGISTRY
Multiple vendors: traps

- Beware of OEMs
  - Ask what's inside your DNS "appliance"!
- Often customized versions of open-source SW
  - Same "packet-of-death"
  - Changes over time, ask your OEM!
Recommendations

- Use **at least two** DNS vendors
  - **at very least** at the edge
- Beware of OEMs
Discussion: Common config interface

• Deleting a zone is always the same, right?
• RESTCONF example

```bash
```

• What else do you need?
Discussion: Common config interface

• What do you configure most frequently?
  • Add/delete zone?
  • Configure parameters for zone slaving?
    – TSIG keys?
    – ACL?
  • How does it look like?
• Zone content?
• ...??????
Recommendations

• Thank you for discussion!

• Use **at least two** DNS vendors
  - **at very least** at the edge

• Beware of OEMs