ISC & BIND Update

ICANN 51, October 2014

Vicky Risk, Product Manager
Agenda

1. Current offering for TLD operators
   - 2014 Development Initiatives
   - Missing features & Roadmap
   - Software support strategies
   - Development and support team
   - Security vulnerability process

2. Performance vs. Functionality

3. New feature decisions

4. TLD User base
2014 Development Initiatives

- Refocusing on BIND9
  - Released BIND 9.10.0, 9.10.1
  - DDOS support, simulation test bed
  - Fuzz testing (Codenomicon CROSS)
    - Improving automated test coverage
    - Creating new DNSSEC documentation

- Open source contributors, OS packagers
  source.isc.org

- Re-hosted DLV site, upgrading bug db
“Missing” Features & RFCs

- **DNSSEC Key policy manager**
  - We have key generation, and in-line signing, this would automate rolling keys, manage overlap and housekeeping (deleting old files)

- **DNS Parent updating**
  - Child DNS, Child DNS KEY records

- **Negative trust anchor**
  - Available today to subscribers, will be in 9.11
BIND 9.10 - April 2014

- **MAP zone file format**
  - speed start-up

- **Native PKCS#11**
  - simplify HSM integration
    - RRL on by default
    - New statistics
    - Zones sharing between views
    - DNSSEC troubleshooting “Delv”
    - DNS Pre-fetch
    - DNS Cookies (first DNS server to implement)
    - CAA records support (9.10.1)
    - Linux SECCOMP (9.10.1)
BIND 9.11 planned features

- One-touch zone addition
- DNSSEC Key policy manager
- Wire-speed logging with DNStap
- Parent updating (CDNS, CDNSKEY rr)
- DNSSEC Negative Trust Anchor
- DDOS mitigations (resolver features)

In Planning & Design phase
Targeted – mid 2015
Agenda

1. Current offering for TLD operators
   - Development Initiatives
   - Missing features & Roadmap
   - Software support strategies
   - Development and support team
   - Security vulnerability process

2. Performance vs. Functionality

3. New feature decisions

4. TLD User base
Open Source – funded by subscriptions

- In 2013 we introduced support subscriptions, replacing the BIND Forum Membership as our primary funding mechanism
- SW maintenance and incremental feature development is entirely funded by support subscriptions
## Multiple Support Levels

<table>
<thead>
<tr>
<th>Benefits &amp; Levels</th>
<th>Gold</th>
<th>Silver</th>
<th>Bronze</th>
<th>Basic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product Support</strong></td>
<td><strong>Critical Response</strong>&lt;br&gt;30 minutes&lt;br&gt;24 x 7&lt;br&gt;<strong>Standard Response</strong>&lt;br&gt;4 business hours 9am - 5pm EST Monday - Friday&lt;br&gt;Phone &amp; Email</td>
<td><strong>Critical Response</strong>&lt;br&gt;1 hour&lt;br&gt;24 x 7&lt;br&gt;<strong>Standard Response</strong>&lt;br&gt;8 business hours 9am - 5pm EST Monday - Friday&lt;br&gt;Phone &amp; Email</td>
<td><strong>Critical Response</strong>&lt;br&gt;2 hours&lt;br&gt;Business hours only&lt;br&gt;<strong>Standard Response</strong>&lt;br&gt;8 business hours 9am - 5pm EST Monday - Friday&lt;br&gt;Email</td>
<td>Not included</td>
</tr>
<tr>
<td><strong>Advance Security Incident Notifications</strong></td>
<td><strong>When first patch is available for security issue</strong></td>
<td><strong>5 business days before public disclosure</strong></td>
<td><strong>5 business days before public disclosure</strong></td>
<td><strong>3 business days before public disclosure</strong></td>
</tr>
</tbody>
</table>

© 2014 ISC
Basic Subscription

- $10k USD annual subscription
- Good for people who don’t need technical support
- >3 days advance notice of a security vulnerability
- Software fix for the problem
- Security for your network

the BASELINE for everyone
Support customers

- Search engine
- Privacy for your support issues (no need to post on open lists)
- Priority in getting bugs fixed and feature requirements addressed
- Annual configuration review
- Up to 7x24 support with 30 minute response time for critical issues
Multiple release train options

- Published EOL dates
- ESV versions

- **9.6.0**
  - 2008
  - 9.6-ESV-R10
  - EOL

- **9.6.0**
  - 2008
  - 9.6-ESV-R10
  - EOL

- **9.8.0**
  - 2011
  - Easier DNSSEC deployment (9.7)
  - Built-in trust anchor for root DNS64

- **9.8.6**
  - 2013 - Sept
  - Basic RRL

- **9.9.0**
  - 2012
  - NXDOMAIN redirect
  - In-line signing

- **9.9.4**
  - 2012
  - In-line signing
  - Basic RRL

- **ESV**
  - 2013 - Sept
  - Multiple DLZ (per zone)
  - GeoIP ACL, DNS Cookies

- **9.9.5**
  - 2013 - Jan
  - Response Policy Zones (RPZ)
  - Writable DLZ zones, static stub zones
  - Configurable resolver timeouts

- **9.9.6**
  - 2013 - Jan
  - 21 featurettes
  - 37 bug fixes

- **9.10**
  - 2014 - Jan
  - Prefetch, Map zone, zone sharing between views
  - Statistics: JSON, udp/tcp

- **9.10.1**
  - 2014 - Jan
  - Multiple DLZ (per zone)
  - GeoIP ACL, DNS Cookies

- **EOL**
  - 2014 - Jan
  - DELV, PKCS #11

- **9.11**
  - 2015 - July
  - EOL
Operating Systems

- redhat
- CentOS
- ubuntu
- SUSE
- debian
- fedora
- Microsoft Windows®
- Oracle Solaris
- HP-UX
- OpenBSD
- FreeBSD

© 2014 ISC
Staff supporting BIND

7 x 24 On-call rota includes both support & development (escalation)

**BIND9 Development**
- Dedicated BIND Software Engineering (3 + 1 p/t)
- Build/test/security engineer (1)
- Engineering Director (1)

**BIND9 Support**
- Tech support staff (4)
- Consulting and training (2)
- Customer service (1)
- Project manager (1)
Security Vulnerability Process

- Published security vulnerability handling policy
- Conduct analysis and communications confidentially and securely
- Leverage Industry best-practices

www.first.org/cvss
Risk assessment

http://cve.mitre.org/
Unique identifier
Phased Disclosure Process

- Enables operators to upgrade critical systems before the vulnerability is published
- We provide advance notification to:
  - Root operators (free, 5-day)
  - Operating system packagers (free, 24 hour)
  - Subscribers
  - OEMs
Agenda

1. Current offering for TLD operators
2. **Performance vs. Functionality**
3. New feature decisions
4. TLD User base
Performance vs. Functionality

- BIND is intended as a complete, reference implementation
- A comprehensive feature set and faithful adherence to standards is higher priority than performance leadership
Features vs. Performance

Adding features

Periodically, optimize
Features vs. Performance

- In general, adding features reduces performance
- Ideally, you periodically schedule in optimization work or new methods – e.g. Map-zone file format, DNS pre-fetch
- We look for unexpected changes in performance
TLD Requirements

Manageability, stability & performance
- Efficient, automate-able process for adding zones, updating a large network of slaves frequently
- DNSSEC operational support – In-line signing
- HSM support

Performance - incremental signing for large zones
- Time to transfer large, signed zones
- Fast reload/restart
Independent Benchmarking

What would make this most useful?

- Active participation from users in creating realistic test scenarios
- Ability to compare configuration options (which may be product-specific)
- Comparisons between successive versions of the same product
- Comparisons between h/w or OS platform choices per product
Agenda

1. Current offering for TLD operators
2. Performance vs. Functionality
3. New feature decisions
4. TLD User base
New Feature Considerations

- Do no harm
- Long-standing commitment to open standards
- Scalability, efficiency and security of the DNS & Internet
- Is requestor contributing somehow?
- Balance the needs of different types of users
BIND installed base?

**BIND** – 266,277 servers

**Microsoft**

**Nominum**

**NSD**

Figure 1: Distribution of name server software versions — Dataset I.

From The Measurement Factory, 2010
http://dns.measurement-factory.com/surveys/201010/
Since 1994, ~55 nodes
First to sign mutual responsibilities agreement with ICANN
TLDs using and supporting BIND

* multi-vendor

Permission received to list
User Base

A very small proportion of users actually support the open source they use.

CCTLD and GTLDs supporting BIND make up 10% of our support base.

Annualized BIND subscription revenue as of August 29, 2014 by industry grouping

- carrier 31%
- OEM 15%
- gTLD 6%
- isp 6%
- tech 20%
- root operator 0%
- ccTLD 7%
- govt 3%
- edu 3%
- fin 3%
- defense 5%

© 2014 ISC
References

- 2013 Annual Report
- Sign up to receive Bind Announcements
  - https://lists.isc.org/mailman/listinfo/bind-announce
- Software support policy
- Security vulnerability reporting
- Security vulnerability disclosure
  - https://kb.isc.org/article/AA-00861/0
- ISC Open Source license