BINDO What's old, what's new, what's borrowed and what's blue? Ondřej Surý, ISC



Release Schedule

- •We are moving from annual stable branches to bi-annual
 - Every stable release will be supported for four years
- Longer development branches accommodate more ambitious refactoring



BIND 9.11 ESV — something old

Only critical and security fixes



info@isc.org

BIND 9.16 — something new

- New asynchronous multi-threaded networking framework
- •New KASP-based dnssec-policy
- Serve Stale improvements
- Numerous other bugfixes and refactorings



BIND 9.16 Network Manager

- Based on excellent libuv library (see, something borrowed)
- Improved authoritative performance
 - Still working on the recursive performance
- Needed for all other transport protocols



BIND 9.16 dnssec-policy

- •Key and Signing Policy (KASP) based
- Generates new keys as needed
- Automatically roll ZSK and KSK
 - •Needs manual trigger for DS check with *rndc*
- Automatic algorithm roll
- Supports NSEC3 (since 9.16.10)
- Obsoletes dnssec-keymgr



BIND 9.16 Serve-Stale Improvements

- Changed defaults per RFC 8767 recommendations:
 - max-stale-ttl changed from 1 week to 1 day to declutter the cache.
 - *stale-answer-ttl* changed from 1 second to 30 seconds.
- •New configuration options:
 - *stale-cache-enable* has been introduced to enable or disable keeping stale answers in cache.
 - *stale-refresh-time* has been introduced to allow serving stale RRset before refreshing it.
 - *stale-answer-client-timeout* that controls the time that `named` waits for remote server to answer before serving answer to the client.



info@isc.org

BIND 9.16 — other notable changes

- DNS Flag Day 2020: Default EDNS0 buffer size changed from 4096 to 1232
- SipHash 2-4 based DNS Cookies (now RFC 9018)
- DNSSEC now mandatory and DLV is now obsolete
- PKCS#11 ECDSA and EdDSA fixes (OpenSSL engine_pkcs11 now preferred)
- Cleaned up all ThreadSanitizer warnings
- Participating in the OSS-Fuzz program



BIND 9.17 — new development

- •New autotools build system easier to maintain and faster
- Documentation changed from DocBook to sphinx-build (backported to 9.16)
- DNS Flag Day 2020: additionally, named sets IP_DONTFRAG socket option to disable fragmentation (under investigation after report from Anand)
- Support for DNS over TLS (since 9.17.7)
- Support for DNS over HTTPS (since 9.17.10)
- Support for XFR over TLS (since 9.17.10)



DNS over TLS (DoT)

- Encrypted transports on port 853 based on the new network manager infrastructure in BIND
- Currently only in the development branch, but it will be backported to 9.16 when dust settles



Why did we do DoH?



Photo by <u>Ian</u> on <u>Unsplash</u>



DNS over HTTPs (DoH)

- Default settings for listen-on port 443 for DoH
- Unencrypted HTTP/2 queries for situations when TLS offloading to another server is required
- Followed Unbound's lead re: status codes



dig for DoH - 9.17.11

\$ dig +https @doh.example.com isc.org A

;; SERVER: 1.2.3.4#443(doh.example.com) (HTTPS)

;; WHEN: Thu Mar 11 15:50:58 EET 2021

; <<>> DiG 9.17.10 <<>> +https @doh.example.com isc.org A ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56070 ;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 ;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 1232 ; COOKIE: e40f41fc38f3768e0100000604a20425472ceb9ec62ced0 (good) ;; QUESTION SECTION: ;isc.org. IN A ;; ANSWER SECTION: isc.org. 60 IN A 149.20.1.66 Big



;; Query time: 306 msec

;; MSG SIZE rcvd: 80

info@isc.org

Test improvements

- More realistic simulation of real Internet
 traffic
- Profile DoH and DoT
- Load test TCP traffic
- Based on DNS Shotgun
- Need traffic samples!



What awaits in the near future?

- Network Manager improvements
 - Reduce the number of competing threads by moving tasks and all old socket code to Network Manager (WIP)
 - Recursive performance improvements
- Backport DoT, DoH and NetMgr improvements to 9.16
- That should conclude stabilizing 9.16 branch



Help we could use from you

- Do you use serve-stale? If so, have you found it useful in bridging an outage?
- Can you provide an anonymized PCAP dump?
- Test feedback on development branch
- Thank you for helping others on bind-users!



On-going webinar series on managing BIND

- <u>https://www.isc.org/blogs/bind-management-</u> webinar-series-2021/ (register, recordings, slides)
- •Next session April 21, using DNSdist with BIND
- Includes a half-hour hands-on lab
- •whole thing is taught by Carsten Strotmann

ISC

W UNIVERSITY OF CALIFORNIA, BERKELEY

From Wikipedia, the free encyclopedia

The University of California, Berkeley (UC Berkeley, Berkeley, Cal, or California) is a public research university in Berkeley, California. Established in 1868 as the state's first land-grant university, it was the first campus of the University of California system and a founding member of the Association of American Universities. Its 14 colleges and schools offer over 350 degree programs and enroll 31,000 undergraduate and 12,000 graduate students. Berkeley is ranked among the world's top universities by major educational publications.

BIND PROJECT BEGINS

The Berkeley Internet Name Domain (BIND) package was originally written at the University of California at Berkeley as a graduate-student project, under a grant from the US Defense Advanced Research Projects Administration (DARPA). Versions of BIND through 4.8.3 were maintained by the Computer Systems Research Group (CSRG) at UC Berkeley. Douglas Terry, Mark Painter, David Riggle, and Songnian Zhou made up the initial BIND project team.

INN NTERNETNEWS) DFTWARE FIRST RELEASED

Wikipedia





Internet Systems Consortium

- 3rd level Technical Support
- Advance Security
 Notifications
- BIND 9 DNS, Kea DHCP open source
- contact us at isc.org





Photo by Sharon McCutcheon on Unsplash

