ISC BIND Update

DENOG 3
Frankfurt, 2011-10-20

Shane Kerr

<shane@isc.org>

Introduction

- ## Who is ISC?

    - ## We make open source software

        - BIND
        - ISC DHCP

    - ## We host and provide Internet services

        - F root
        - SNS
        - SIE

- ## Who am I?

    - ## BIND 10 Engineering Manager

BIND 9 and BIND 10

- BIND 9 – the most used DNS server
- BIND 10 – new vision for BIND
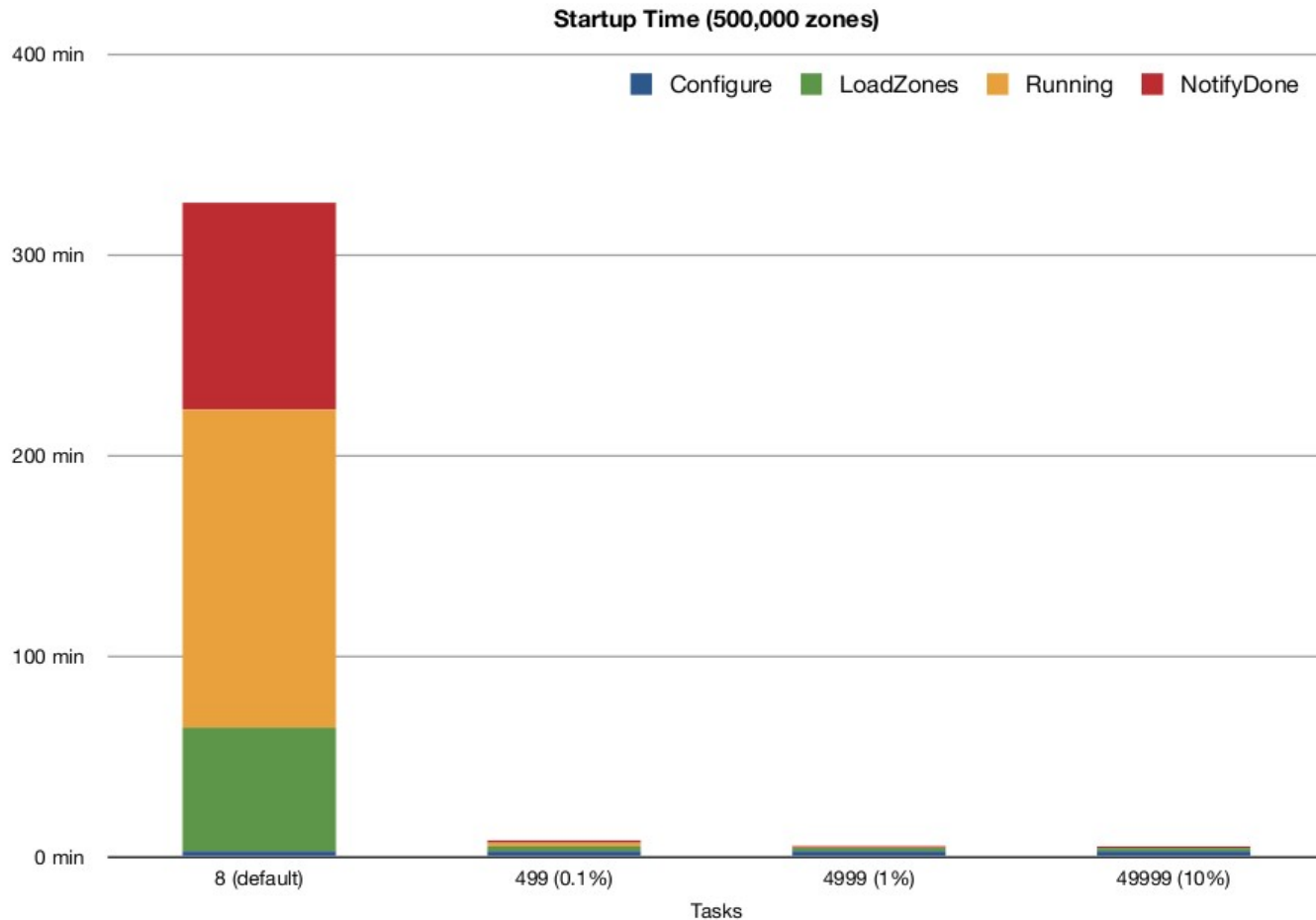
ISC and BIND 9: How Do We Pay for It?

- ISC provides support
  http://www.isc.org/support

- ISC offers custom development
  http://www.isc.org/support/software-development

- ISC gives training
  http://www.isc.org/support/training

  - Just had IPv6 training in Frankfurt

  - 3-day DNSSEC course in Rome in November

- ISC runs the BIND Forum
  http://www.isc.org/software/guild/bf

ISC

ISC and BIND 9:
How Do We Do It?

- Team of 5 developers

- Started using Scrum about a year ago

  - An "Agile" methodology

  - Slightly modified for our environment

- Push to improve testing of code

  - New code via test-driven development (TDD)

  - Also testing older code, finding ancient bugs

BIND 9:
Startup Time Improvements

http://www.isc.org/community/blog/201107/major-improvement-bind-9-startup-performance

Startup Time (500,000 zones)

BIND 9: DNSSEC Improvements

- 'auto-dnssec' can now use NSEC3

- New dnssec-signzone options:

  - -D puts DNSSEC data in a separate file, so you can "$INCLUDE example.com.signed", and not have to modify the original zone file

  - -X allows different expieration time for DNSKEY, useful if KSK on a separate system

- Option to set default TTL for DNSKEY record

- dnssec-dsfromkey can now read from stdin:
```
dig dnskey isc.org | dnssec-dsfromkey -f - isc.org
```

BIND 9: DNSSEC In-Line Signing

- Acts as a slave getting unsigned data

- Acts as a master sending signed data

- Separates the signing function from the Master DNS server

- Also known as "signer in the middle" or "bump in the wire"

BIND 9:
More Goodies!

- RFC 1918 reverse zones in empty-zones table
  - Like 10.IN-ADDR.ARPA, 168.192.IN-ADDR.ARPA
  - As per RFC 6303
- Dynamic DNS (DDNS) improvements:
  - Can now set SOA to current UNIX time (seconds since 1970)
  - 'rndc sync' can write the zone without a freeze/thaw cycle
- 'also-notify' can now use named lists and TSIG keys
- 'rndc flushtree' clears cache under a name:
  - 'rndc flushtree example.de' also clears www.example.de
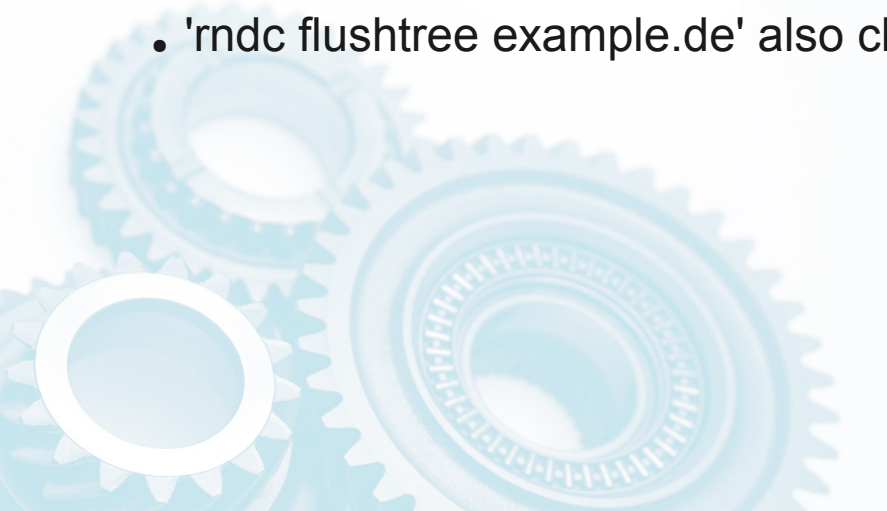
BIND 9:
NXDOMAIN Redirection

BIND 9 Plans

- 9.10 expected 2012 quarter 1
    - DNSSEC Improvements 2: Key Management
    - SERVFAIL caching
    - Health & internal state monitoring
    - "Large Server" performance settings
- Possible futures (maybe 2012 quarter 3)
    - Multi-master
    - BIND 9 script integration mapping
    - Whole answer caching

Why BIND 10?

- BIND 9 is more than 10 years old
- The computing world has changed
  - Multi-core machines, massive RAM, …
- The networking world has changed
  - Fiber everywhere, mobile devices, …
- DNS software "marketplace" has evolved
  - Special-purpose servers, new ideas
- An architecture for the next 10+ years

What is BIND 10?

- Authoritative DNS server
  - DNSSEC-enabled
  - SQL or in-memory data sources
  - Master and/or slave mode
- Recursive DNS server
  - No DNSSEC yet (but coming)
- DNS libraries

BIND 10 History

- Original idea from Paul Vixie
- *Motivation for BIND 10* written by Paul Vixie & João Damas
- 10 TLDs agreed to be initial sponsors
    https://www.isc.org/bind10/sponsors
- 2009-04-01 (April 1st, really!) start

What is Special about BIND 10?

- Customizable
  - Both "out of the box" and bespoke
  - Full run-time control (no restarts)
- Scalable
- Reliable
  - Well-tested
  - Resilient to failures and software errors
- Re-usable
  - Well-defined APIs and libraries

Cool BIND 10 Technologies?

- Cooperating processes
    - Helps customization, scaling, …
- Generic data sources
    - SQLite and in-memory now, more later
- Full run-time configuration
    - New modules can use easily
    - RESTful HTTP/SSL interface
- Best logging system around

Putting the *Open* Back in *Open Source*

- BIND 10 development is *public*
- https://bind10.isc.org
  - Plans, designs, meeting minutes, …
  - Build reports, bug tickets, …
  - Public Git repository
- Working with other open source
  - Giving back to upstream
- Today!
- Goal: a product *and* a community

5 Year Plan

- ✔ Year 1: Authoritative-only server
- ✔ Year 2: Recursive server
- • Year 3: Production-ready
- • Year 4: BIND 9 transition, user joy
- • Year 5: Really fun stuff
  - – Cluster support
  - – Embedded support
  - – Smart, adaptive DNS behavior

BIND 10 Releases

- 2010-03-19 1st prototype release
  - Following releases about every 6 weeks
- 2011-02-24 recursive resolver release
- 2011-05-19 TSIG arrives
- 2011-07-05 ACLs arrive
- 2011-08-19 More TSIG, more ACLs, more RR types
- 2011-10-14 IXFR (inbound)

Current Status

- Working DNS server
  - Some developers use it, site uses it
- Currently expanding feature set

http://bind10.isc.org/wiki/Year3Plan

Thank You to our Generous Sponsors