code diversityの概況

Nov/21/2012　DNSDAY

伊藤 高一

Abstract

- ネームサーバのcode diversityについて、簡単に振り返る。
- 現時点で利用可能な実装について、話者の情報収集の及んだ範囲で紹介する。
- 取り上げなかった実装については、単に情報収集が及ばなかっただけであり、他意はない。

これまでを振り返って

太古の昔

- 1983～1984年
  - 最初のネームサーバの実装、Jeevesが開発された。
  - プラットフォームはTOPS-20/DECsystem20
- soon
  - BINDが開発された。
- 1987年
  - RFC 1033～1035発行
- 1995年ごろ
  - WindowsやMacで動作するネームサーバも見かけた。
- 1997年
  - BIND8リリース

2000年

- データセンタを作った。
- Layer 2、Layer 3の機器は、当時のマーケットでの代表的な機種群でdiversityをほぼ達成した。
- ネームサーバも、当然diversityを確保したかった。
- プラットフォームは、まだSPARCも現役だったのでdiversityを確保できた。
- 肝心のネームサーバソフトウェアは、BIND8一択。
  - 今回、振り返ってみたら、djbdnsが既に登場していたらしい。
  - BIND9は、この年にリリースされた。

200x年代前半

- 2001年
  - djbdns 1.0.5(最後の公式リリース: Wikipediaより)
- 2002年
  - NSD(4月のプレゼンで1.0.0-β is available)
  - MaraDNS 1.0.01
    - authoritative/recursive兼用
  - Nominum ANS/CNSも2002年リリースらしい
- PowerDNSについては情報得られず
  - pdns-announce MLのアーカイブの最初のポストが
    - Mar 20 2003, PowerDNS 2.9.7 released!
  - PowerDNS Recursorは2006年にリリース
    - 最初のバージョンが3.0

2006年ごろ

- このころの仕事場の自家用ネットワーク
- 小さな会社なのに、やたら趣味に走った構成。
- authoritativeサーバ
  - primary: BIND
  - secondary: NSD
- recursiveサーバ
  - BIND
  - unbound
  - quaggaでIGP anycast
- NSDでAS112相当(IGPで実装)

やってみて思ったこと

- 「重複をお許しください。」
- うん、許す許す :-)
- 以下、プロトコルの脆弱性じゃなくって実装の脆弱性という前提で…
- 毒入れ系はヤバいけど
  - 影響を受けるヤツを止めても機能維持できる。
- 止まっちゃう系は余裕
  - キャパシティの問題はあるが…

やってみて思ったこと

- まぁもちろん対策はするんですが
  - 全滅はしないので、緊急度合が下がる。
  - 対象が全台じゃないので、工数/重複が少なくて済む。
    - でも頻度は上がる。
    - どうも「総和は一定」ではない気がするのはなぜ…?
- n(≧2)種類の実装を
  - 触れてうれしい

    v.s.
  - 触らなきゃいけなくて大変

2007年～

- 「それは何故か7月にやってくる」
  - by みんみんさん@dnsops.jp BoF(2009年9月4日)
- 2007年
  - (query) IDが予測できちゃう
- 2008年
  - Kaminsky氏による毒入れ手法の発見
  - BINDは軽減策としてport randomizationを導入した
- 2009年
  - type ANYでdynamic update
- 2010年、2011年、2012年
  - 律儀にやってきた (^^;

2007年

- BIND8 end of life
- BIND9はconfigの後方互換には注意が払われていたが、コードはスクラッチ。
- BIND8とBIND9でもdiversityだった。

200x年代後半～今年

- 2008年
  - unbound Release 1.0.0
- 2010年
  - MaraDNS 2.0.01
    - authoritativeサーバとrecursiveサーバを分離
- 2011年
  - PrimDNS
- 2012年
  - Knot DNS v1.0.0
- 2012年
  - YADIFA Release 1.0.0

利用できる実装

BIND9

- リリース元
  - Internet Systems Consortium
- authoritativeサーバ/recursiveサーバを1プロセスで兼用できる。
  - ISC自身も分離することを勧めている。
- view{}によるsplit DNSなど豊富な機能
- dig、DNSSEC関係などのユーティリティもバンドルされている。

BIND10

- リリース元
  - Internet Systems Consortium
- 機能毎にモジュールが分割されている。
  - authoritativeサーバのモジュール、recursiveサーバのモジュールは、両方とも提供されている。
- まだDevelopment release

NSD

- リリース元
  - NLnet Labs
- authoritativeサーバ専用
- root/TLDをターゲットに開発
- {H,K,L}.root-servers.netで稼働中
  - 2012年10月、某ASからversion.bindにより観測
- zone compilerにより中間形式に変換してからサーバにロードする。
  - ロード前に書式チェックが強制される。
  - 中間形式は全ゾーンで1ファイル。
  - ゾーンの追加/削除にはプロセスの再起動が必要。

Knot DNS

- リリース元
  - CZ.NIC
- authoritativeサーバ専用
- TLDをターゲットに開発
- zone compilerで中間形式に変換してからサーバにロードする。
  - 中間形式は1ゾーンで3ファイル。
  - 全ゾーンが同じディレクトリ直下にフラットに生成される(1.1.0時点)。
  - ゾーンの追加/削除はknotc reload。

YADIFA

- リリース元
  - EURid
    - .euのレジストラ
- Release 1.0.0の時点ではauthoritativeサーバ専用
- RIPE64ではBeyond BIND and NSDというタイトルでプレゼンしている。
- でもdynamic updateに対応していたり、recursiveサービスやRDBバックエンドを検討していたり、NSDやKnot DNSとは違った方向を目指している。
- DNSSECの署名もサーバ自身がやるらしい?

PowerDNS

- リリース元
  - PowerDNS.COM.BV
    - Open Source
    - 商業サポートあり
- authoritativeサーバとrecursiveサーバ両方(独立)
- authoritativeサーバはRDBバックエンドとパイプバックエンド

PrimDNS

- リリース元
  - GREE Labs
- authoritativeサーバ専用
- ゾーンデータはテキスト/RDB/外部プロセスからの応答
- GREEのプロダクションで内部向けとして実運用。
- DNSSEC非対応(2012年4月時点)

MaraDNS

- リリース元
  - Sam Trenholme氏
- 1.xはauthoritativeサーバ/recursiveサーバが1プロセスで兼用できた。
- 2.xから独立した。
- small, lightweight, easy to setup
- DNSSEC非対応

Unbound

- リリース元
  - NLnet Labs
- recursiveサーバ専用
- 絞り込まれた機能

Nominum

- 発売元
  - Nominum, Inc.
    - 商用ソフトウェア製品
- authoritativeサーバ(ANS)
- recursiveサーバ(VANTIO)

Trinzic DDI

- 発売元
  - Infoblox, Inc.
- IPアドレスのリソース管理統合アプライアンス
  - ハードウェア製品の他、virtualアプライアンスもあり。
- authoritativeサーバ、recursiveサーバ、DHCP

トレンド

トレンド

- authoritativeサーバとrecursiveサーバの分離
- root/TLDグレード(の|を目指す)ヨーロッパ勢
  - NSD
  - Knot DNS
- シンプルなrecursive専用サーバ
  - Unbound
- 多機能派
  - BIND
  - PowerDNS
  - PrimDNS
  - YADIFAもこっちを目指している?

参考URL

参考URL

- 全般
  - http://jprs.jp/tech/
  - http://en.wikipedia.org/wiki/Comparison_of_DNS_server_software
- BIND
  - http://www.isc.org/software/bind
  - http://bind10.isc.org/wiki

参考URL

- NSD
  - http://www.nlnetlabs.nl/projects/nsd/
  - http://meetings.ripe.net/ripe-42/presentations/ripe42-dns-aons/index.html
  - http://www.nlnetlabs.nl/downloads/NSD_DenicTechnical.pdf
  - http://ccnso.icann.org/node/32377
  - http://ripe62.ripe.net/presentations/146-NSD4-RIPE62-03.pdf
  - http://unbound.jp/nsd/

参考URL

- Knot DNS
  - http://www.knot-dns.cz/
  - http://ripe63.ripe.net/presentations/145-KNOT-20111103-LS-RIPE63.pdf
  - https://ripe64.ripe.net/presentations/125-KNOT-20120418-OS-RIPE64.pdf
  - https://ripe65.ripe.net/presentations/183-knotdns-ripe65.pdf
  - http://xkcd.com/844/

参考URL

- YADIFA
  - http://www.yadifa.eu/
  - http://ripe63.ripe.net/presentations/154-RIPE63-DNSWG-BeyondBindAndNSD-PeterJanssenEURID.pdf
  - https://ripe64.ripe.net/presentations/132-RIPE64-YADIFA.pdf

参考URL

- PowerDNS
  - http://www.powerdns.com/content/home-powerdns.html
- PrimDNS
  - http://labs.gree.jp/Top/OpenSource/PrimDNS.html
  - http://labs.gree.jp/blog/2011/04/3299/
  - http://www.dnsops.jp/bof/20120425/DNSOPS_BoF_2012Spring.txt
- MaraDNS
  - http://www.maradns.org/

参考URL

- Unbound
  - http://www.unbound.net/
  - http://www.unbound.net/documentation/ietf67-design-02.pdf
  - http://www.unbound.net/documentation/ripe56_unbound_02.pdf
  - http://www.unbound.jp/unbound/
- Nominum
  - http://www.nominum.com/
- Trinzic DDI
  - http://www.infoblox.com/en/products/nios.html