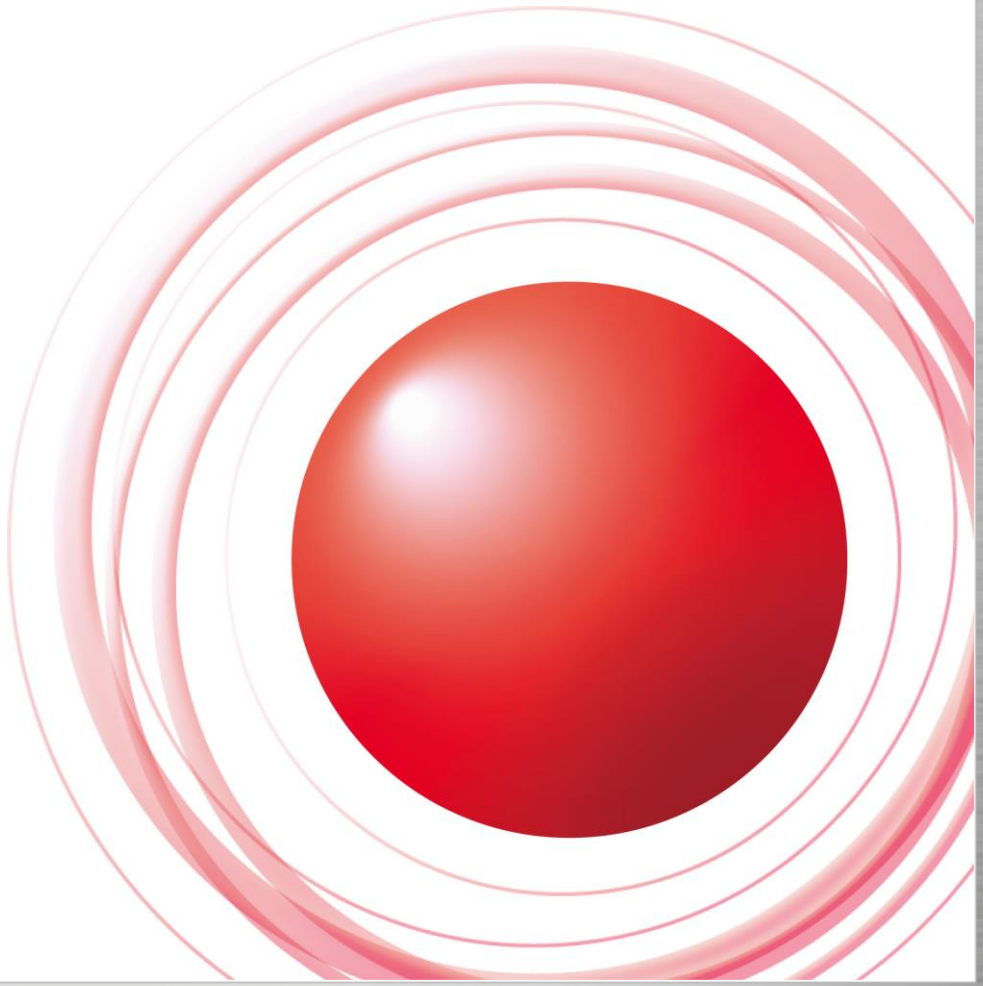
Unboundの紹介とその運用

IIJ
Internet Initiative Japan



株式会社インターネットイニシアティブ
島村 充 <simamura@iij.ad.jp>

Ongoing Innovation

Unboundとは

- オランダ NLnet Labs製キャッシュDNSサーバーソフトウェア(フルサービスリゾルバ)
- 2007/02 初版リリース
- 2008/05 1.0リリース
- 最新版は1.5.9 (2016/06/09リリース)
- そこそこ性能がいい (BIND9比 3倍強)
  - 今日日性能が問題になることなんてよっぽど大規模なISP以外ないですが
- DNSSEC Validation対応
  - FreeBSD10のローカルの名前解決用

脆弱性

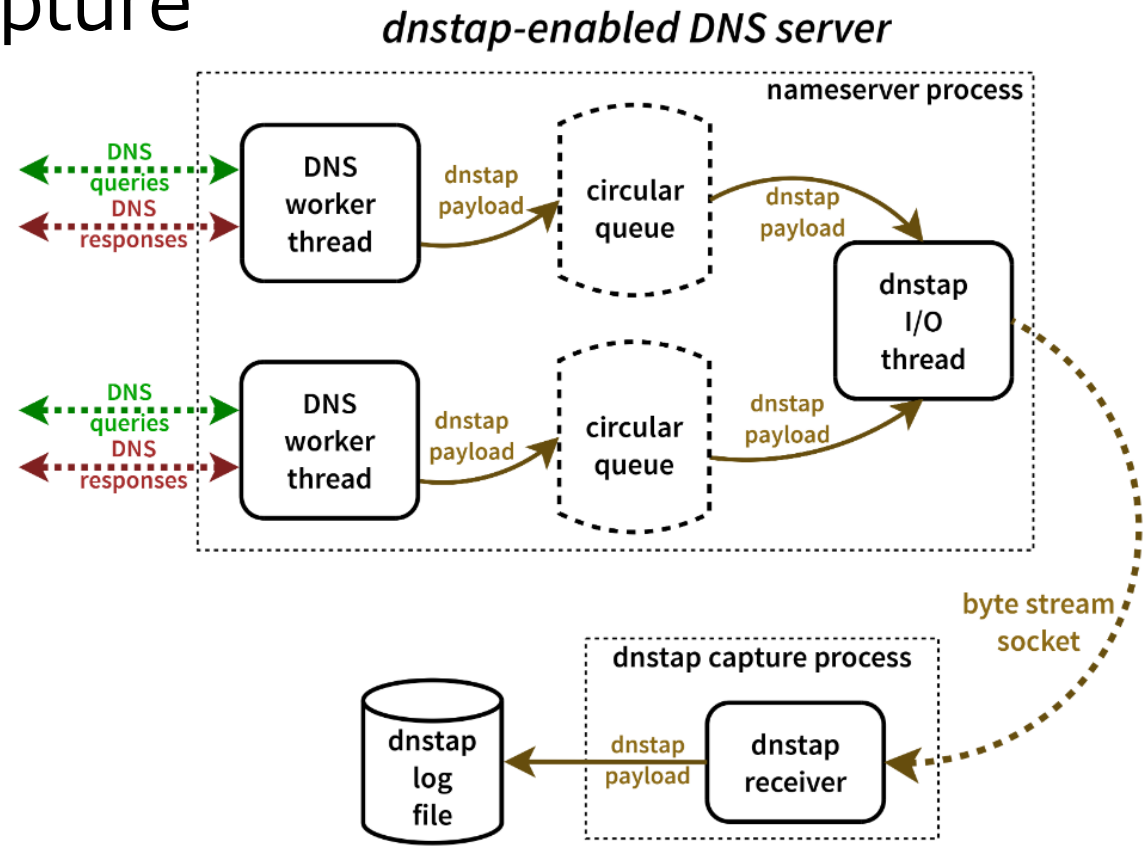
- 脆弱性は過去4件(3回)
  - CVE-2012-1192 (2011/05/27)
    - --enable-chcking OR --enable-debugでbuildし、”interface-automatic: yes”の時に細工されたDNSパケットを受け取るとcrash
      - つまりデフォルトでは影響なし
  - CVE-2011-4528 CVE-2011-4869 (2011/12/20)
    - 細工されたレコードの応答を処理するとcrash
  - CVE-2014-8602 (2014/12/08)
    - delegation chainの段数制限がなく、リソースを浪費
      - 他のDNSサーバーソフトウェアも影響

BIND9になく、Unboundにある機能

- Negative Trust Anchor
  - DNSSEC検証に失敗した特定のドメインだけ検証しない
  - BIND9も9.11で実装
    - ただし永続化はできない (最長1週間)
- DNSSEC署名のexpireを一定期間許す機能
- use-caps-for-id (0x20)
  - クエリのエントロピーを上げる
- キャッシュポイズニング攻撃の部分的検知
  - TXIDの不一致をカウント
- Query Name Minimisation (RFC7816)

BIND9になく、Unboundにある機能

- DNS over TLS
- DNStap
  - “high speed DNS logging without packet capture”



BIND9になく、Unboundにある機能

- prefetch
  - もともとはGoogle Public DNSの機能
  - BINDも9.10で実装→速攻でcrash bug!
    - 2014/04/29 9.10.0リリース
    - 2014/05/09 9.10.0-P1リリース
- (query) ratelimit
  - 1.5.4(2015/07/09)で実装
  - cache側でratelimitが実装されることはないと思っていたが…。
  - ゾーン(NS)毎、cacheされてない場合に所定のQPSを超えるとSERVFAILを返す(らしい)

BIND9にあって、Unboundにない機能

- 権威DNSサーバー
  - 権威・キャッシュの混在は不可
  - local-zone, local-dataで上書き可能
    - additionalは上書きしない (後述)
- みんな大好きview
  - キャッシュDNSサーバーに要るの…?
    - 実は昔IIJで使ってたんです…
- RPZ (Response Policy Zone)
  - 児ポブロックで使っているISPがあると聞いたことがあります
  - ブロック自体はlocal-dataで可能

BIND9にあって、Unboundにない機能

- みんな大好きAAAA filter
  - 止めたい。でも(だれも太鼓判を押してくれなくて)止められない！
    - “`private-address: ::/0`” とunbound.confに書くとすべてのAAAAを落とす
    - contrib/aaaa-filter-iterator.patch

      by Stephane Lapieさん(朝日ネット)
      - Aがあるときだけ落とす(BIND9と同じ)

昔なかった機能

- みんな大好きquerylog
  - 1.4.11(2011/06/30)で実装
  - `unbound-control set_option log-queries: yes`

```
Jun 15 09:50:03 host unbound: [751:0] info: 127.0.0.1 github.com. AAAA IN
```

```
Jun 15 09:58:24 host named[31170]: queries: info: client 127.0.0.1#60141
  (github.com): view external: query: github.com IN AAAA + (127.0.0.1)
```

情報はちょっと少なめ

- みんな大好きRound Robin
  - 1.4.17(2012/05/24)で実装 (by 東さん)
  - デフォルトでは無効
  - `rrset-roundrobin: yes`
    - RFC3484あるし、必要ですかね…?

昔なかった機能

- minimal-responses
  - AUTHORITY, ADDITIONALセクションを省略して良い場合に削って応答を返す
    - 応答パケットサイズを小さくして帯域節約・TCP fallbackを抑制
  - 1.4.17(2012/05/24)で実装 (by 東さん)
  - デフォルトでは無効
  - `minimal-responses: yes`

Unbound運用の実際

- IIJでのUnbound利用状況
  - 法人向け 回線サービスのキャッシュDNSサーバー
    - 2013/4頭～ 一部サービス用
    - 2014/6末～ 全サービス
  - 個人向けは…? BIND9です…
    - 昔viewを使っていた
    - AAAA filter (もう止めようよ…)
    - そのうちUnboundに (年内にできたらいいな)
- 脆弱性対応
  - 1回 (CVE-2014-8602)
  - crashしたことなどなし

ちょっとしたハマりどころ

- DSR構成のLBを使っていたり、anycastをしている場合、サービス用のIPアドレスとInterfaceのIPアドレスが異なる
  - その場合に、なにもケアしないと、応答をInterfaceのIPアドレスから返そうとする
  - “interface-automatic: yes” とすると、クエリを受けたIPアドレスから返す

```
interface-automatic: <yes or no>
  Detect source interface on UDP queries and copy them to replies.
  This  feature  is experimental, and needs support in your OS for
  particular socket options.  Default value is no.
```

Unbound移行時(後)のトラブル

- TCP無応答問題
  - 移行直後から、たまにTCPクエリをこぼす
  - `incoming-num-tcp` のデフォルト値(10)が小さすぎて詰まっていた
    - 当時open resolverだったり、網内にopen forwarderが大量にいた所為もあると思われる
  - `incoming-num-tcp: 1000` にして解消

Unbound移行時(後)のトラブル

- 応答UDPパケットサイズ制限無し問題
  - まだopen resolverだった頃、ANY応答が61.5KBの名前をひたすら引かれ、1Gbpsのuplinkが埋まって死亡
    - 1.4.21で`max-udp-size`オプション導入(by 東さん)。デフォルト4KB
- BIND9との応答内容の微妙な変化
  - 応答の細かいところが微妙に違う
    - 当時詳細は調べたけど忘れてしまいました…
  - 多少心配していたけど、問い合わせが来たことはない

パラメーターチューニング

- Unbound: Howto optimise (unbound.net)
  - 基本はこれを熟読
  - 日本Unboundユーザー会 による和訳

- DNSキャッシュサーバ 設計と運用のノウハウ (東 大亮)
- DNSキャッシュサーバ チューニングの勘所 (東 大亮)
  - unboundだけではなく、BIND9も解説

これだけは変更しておけパラメータ (全員)

- rrset-cache-size/msg-cache-size
  (デフォルト4MB(小さすぎでしょ!))
  - rrset-cache-sizeはmsg-cache-sizeの2倍
  - サーバーのメモリに応じて。
    - “mallocのオーバーヘッドにより、総メモリ使用量は設定ファイルに記入した総キャッシュメモリの2倍（あるいは2.5倍）まで増える可能性があります。“ らしい

これだけは変更しておけパラメータ (ISP)

- libeventの利用(compile時)
  - fd 1024個制限の突破
- num-threads (デフォルト1)
  - CPU個数と同じに (自動検出してよ…)
- incoming-num-tcp (デフォルト10(低すぎ…))
  - TCPクエリ数に応じて。1000くらい?
- outgoing-num-tcp (デフォルト10(低すぎ…))
  - 水責め攻撃に加担しているclient数に応じて
  - 権威DNSサーバー(UDP)が詰まる→TCPで聞く→TCPも詰まる→こっちも詰まる
  - 1000くらい?

これだけは変更しておけパラメータ (ISP)

- num-queries-per-threads (デフォルト1024)
  - QPSに応じて
- outgoing-range (デフォルト4096)
  - num-queries-per-threadsの2倍にする

- net.core.rmem_max, rmem_default
  - カーネルパラメータ
  - 適当に、4 or 8MBくらいらしい

Unboundの悩ましいところ

- unbound_control reloadするとキャッシュが揮発する
  - ACLの変更適用などでreloadする場合。
    - 大抵のパラメータはunbound_control set_optionでreloadなしに変更可能なのですが…
      - 設定ファイルとの整合性に気を配る必要あり
  - キャッシュ揮発→若干レスポンスが悪化する
    - 大抵の場合はそんなに影響ない(即座に回復する)
  - 高アクセス時間帯にはやらない方がよいかも
  - LB配下に複数台いる場合、時間をずらすなど
    - もっと丁寧にやるなら、サービスから抜いて、dump_cacheして、reloadして、dumpを基に暖めてから戻す とか…

Unboundの悩ましいところ?

- RD bitの立っていないクエリに応えない
  - dig +trace … するときに困る
    - ユーザが普通に使う分には全く困らない
  - はじめのクエリ(“.”のNSの検索)をresolv.confのIPアドレスにRD bit無しで投げるため
  - access-controlの第二パラメータにallowの代わりにallow_snoopと書くと応答する

```
access-control: 192.0.2.0/24 allow
                    ↓
access-control: 192.0.2.0/24 allow_snoop
```

  - dig @a.root-servers.net +trace ... する
  - drill –T ... する (root-serversに直接聞く)

Unboundの悩ましいところ?

- local-dataがAdditionalを上書きしない
  - ユースケース: 特定のMTAに対するメールの迂回配送をしたいような場合、local-dataでMTAのIPアドレスを乗っ取る
  - `minimal-responses: yes`にしていない場合、MXレコードを問い合わせるとAdditionalにMTAの元々のAレコードが入っている。
  - MTAが乗っ取ったIPアドレスではなく、元々のIPアドレスに配送してしまう(← ホント??)

postfix/sendmailとも乗っ取ったIPアドレスに配送をし、元々のIPアドレスには配送しない。

Package

- RHEL(CentOS)7にてbase入り (パチパチパチ～)
- これで「BIND9以外はベンダー保守がないから…」っていう言い訳ができなくなりますね!

・・・・・・

- と こ ろ が…　versionが **1.4.20**

  RHEL 7.0 Beta　2013/12/11

  Unbound 1.4.21　2013/09/10

  - `max-udp-size`オプションなし
  - Negative Trust Anchorなし
  - `cache-max-negative-ttl`オプションなし
  - CVE-2014-8602 patch適用済み

参考文献

- Unbound: Howto optimise (unbound.net)
- DNSキャッシュサーバ 設計と運用のノウハウ (東 大亮)
- UnboundとNSDの紹介　BIND9との比較編 (東 大亮)
- Unbound キャッシュDNSサーバ大規模用途向け機能の実装 (東 大亮)

IIJ Internet Initiative Japan

Any Questions?

Ongoing Innovation