DNSOPS.jp
DNS Operators Group, Japan

DNSソフトウェア最新動向

Internet Week 2021 - DNS DAY

DNSOPS.jp 幹事 / NTTコミュニケーションズ(株)
髙田 美紀 (たかた みき)

お品書き

- DNSサーバソフトウェア実装の最新動向
  - 権威DNS: JPRS 阿波連さん
  - フルリゾルバ: DNSOPS.jp 髙田

- こんにち広く利用されているOSS実装について紹介します
- 脆弱性情報については取り扱いません
- DoT, DoH についても同様

DNSOPS.jp
DNS Operators Group, Japan

権威DNSサーバ編 (阿波連さん)

DNSOPS.jp
DNS Operators Group, Japan

フルリゾルバ編 (髙田)

DNSOPS.jp
DNS Operators Group, Japan

自己紹介

- 名前: 髙田 美紀 (たかた みき)
- dnsops.jp 幹事 (2011～)
- InternetWeek 2021 プログラム委員

- 本業
  - NTTコミュニケーションズ株式会社 デジタル改革推進部
  - 社内向けデータ分析基盤 (Hadoop, Kafka, k8s, etc.)

DNSOPS.jp
DNS Operators Group, Japan

Unboundの概要

- https://nlnetlabs.nl/projects/unbound/about/
- オランダ NLnet Labs 製
  - 2007年～
- 特徴
  - BINDよりも高速・軽量
  - DNSSEC 対応
  - DoT, DoH 対応
  - フルリゾルバ実装だが、任意のゾーンを権威DNSとして動作させることもできる

Unbound 有償サポート

- https://nlnetlabs.nl/services/contracts/
- NSD, Unbound, etc.

	Gold	Silver	Bronze
Support & Contact Hours	Business Hours*	Business Hours*	Business Hours*
Security Alerts & Patches	Highest Priority	High Priority	Best Effort
Response Time	4 hours	12 hours	24 hours
Consultancy	32 hours	12 hours	No
Dedicated Chat Channel	Yes	Yes	No
Email Support	Yes	Yes	Yes

* Business Hours are 09.00 - 18.00 hrs Central European Time (Amsterdam, the Netherlands)

Unbound 最近の変更点

- DoH Support (1.12.0)
- TCPストリームの再利用 (1.13.0)
- NSID (RFC 5001) Support (1.13.1)
- 設定パラメータ関係
  - infra-keep-probing: yes / no (default: no) (1.13.0)
    - ダウンしているホストをプローブするかどうか
    - 応答がなければ infra-host-ttl秒 (default:300) 待って再度プローブする
  - udp-connect: yes / no (default: yes) (1.13.0)
    - SAD DNS 対策。ソケットconnect() を使う
  - tcp-auth-query-timeout: msec (default: 3000) 追加 (1.13.2)
    - 権威DNS への接続タイムアウト
  - val-nsec3-keysize-iterations: (default: “1024 150 2048 150 4096 150”) (1.13.2)
    - NSEC3 反復回数を BIND, Knot, PowerDNS に合わせた

DNSOPS.jp
DNS Operators Group, Japan

Knot Resolver の概要

- https://www.knot-resolver.cz/
- CZ(チェコ共和国) NIC製
  - 2014年～
- シンプルな core と拡張モジュールでの実装
  - 拡張モジュール開発はユーザも任意に行える (C, Lua, Go)
  - 設定自体も Lua で書く
- スレッドを使わず、複数インスタンスで冗長化
  - Zero downtime restart
  - キャッシュのバックエンドを永続化、インスタンス間で共有できる
- Prometheus メトリクスのエンドポイントを内蔵
- めっちゃモダン
- 利用実績: Cloudflare

Knot Resolver 最近の変更点

- DNSSEC validationがデフォルトで有効に (4.0.0)
  - root の Trust anchor も内包
- DoH Support (4.0.0)
- DNS64 まわりの改善 (5.4.3)
- ログ形式を見やすくするなど、運用改善コードもある
- メモリリークの修正など、怖い修正も見られる
- 設定項目名の変更がカジュアルに行われている模様
  - Changelog をちゃんと読みましょう

- Ubuntu の公式 apt パッケージは古い場合があります
  - Ubuntu 22.04 では 5.4.2 (最新版) が入りますが、Ubuntu 20.04 では 3.2.1。
  - Knot のインストールドキュメントを参照しましょう
    - https://knot-resolver.readthedocs.io/en/stable/quickstart-install.html
  - (Knot の公式レポジトリから入れる方法が書いてあります)

DNSOPS.jp
DNS Operators Group, Japan

プロトコルの話

EDNS バッファサイズ

- Unbound
  - デフォルトは 1232 (1.12.0)
  - edns-buffer-size で変更できる
- Knot Resolver
  - デフォルトは 1232 (5.2.0)
  - net.bufsize() で変更できる
  - https://knot-resolver.readthedocs.io/en/stable/daemon-bindings-net_dns_tweaks.html

IP_PMTUDISC_OMIT

- Unbound
  - IPv6 での実装を修正 (1.13.2)
- Knot Resolver
  - 明示的にオフにしている (5.2.0)

DNSOPS.jp
DNS Operators Group, Japan

HTTPS RR

- HTTPS RR の登場により、HTTPS サービスを DNS に登録する方法が変わっていきます
  - 参考:
    - IW2021 HTTPSリソースレコードへの期待
    - JANOG48 WebサーバのDNSへの登録方法が変わるよ
      - https://www.janog.gr.jp/meeting/janog48/wp-content/uploads/2021/07/janog48-lt5-yamaguchi.pdf
- フルリゾルバでは大きな対応は必要ではない
  - ログ、キャッシュ内容の表示部分
  - drill, kdig などクライアントツール

DNSOPS.jp
DNS Operators Group, Japan

EDNS tcp-keepailve

- Unbound
  - 1.8.0 でサポート
  - edns-tcp-keepalive: yes / no (default: no)
    - yes の場合、 EDNS TCP Keepalive を enable する
  - edns-tcp-keepalive-timeout: msec (default: 120,000)
    - クライアントが EDNS tcp keepalive に対応している場合、この設定をクライアントに送信します。
    - 受信TCPバッファ等の空き状況によって、設定値が変化します
- Knot Resolver
  - サポートなし

ZONEMD

- Unbound
  - 1.13.2 にてサポート
  - zonemd-check: yes / no (default: no)
    - yes の場合、ZONEMD レコードでの検証を行う
  - zonemd-reject-absence: yes / no (default: no)
    - yes の場合、ZONEMD レコードのないゾーンを拒否する
  - zonemd-permissive-mode: yes / no (default: no)
    - yes の場合、検証失敗してもログに出力するだけになる
- Knot Resolver
  - 非対応

ANYクエリへの応答を小さくする

- Unbound
  - 1.8.3 にてサポート、1.9.2 にて返答が NOTIMPL に
  - deny-any: yes / no (default: no)
    - yes の場合、ANY クエリに対して NOTIMPL を返す

- Knot Resolver
  - document には明記されていない
  - ANY のクエリには SERVFAIL を返すもよう (5.4.2)