BIND 9.16から9.18への移行のポイント

2023年11月21日

Internet Week 2023 DNSOPS.JP BoF

（株）日本レジストリサービス

礒浪　直生（いそなみ　なおき）

自己紹介

- 礒浪 直生（いそなみ なおき）
  - 2022年：JPRSに新卒入社 技術研修センターに配属
  - 2023年：システム部に配属（至現在）

    データセンターネットワークの構築・運用、JP DNSサーバーの構築・運用などに従事

    BIND 9.18の技術評価も行ってます！

本日の内容

- BIND 9.16をお使いの方に向けた、変更点と移行のポイントのご紹介
  - BIND 9.18とは
  - BIND 9.16からの変更点

本資料の内容は参考情報であり、個人的な見解を含んでいます
所属組織や開発元の意見を代表するものではありません

BIND 9.18とは

- 長期間のサポートを受けられるExtended Support Version（ESV）になった最新のメジャーバージョン
- 2026年第1四半期までサポートされる予定
- 現在のESVはBIND 9.16で、2024年第1四半期でサポート期間終了
- 現在の開発版（奇数メジャーバージョン）はBIND 9.19
  - 新機能を試してISCにフィードバックしたい人々向け

BIND 9.16からの変更点

リファクタリング

- ネットワークインタフェース
  - BINDネイティブから非同期I/Oライブラリであるlibuvライブラリに完全に置き換わった
  - DNS over TLS, DNS over HTTPSに対応した
    - DNS over HTTPSではTLS暗号化接続と非暗号化接続の両方がサポート
- メモリ割り当てスキーム
  - BIND内部メモリアロケータから汎用メモリアロケータを使うように変わった
  - パフォーマンス向上のため、jemallocライブラリの使用が強く推奨されている
- これらの変更は、部分的に9.16にバックポートされている

ゾーン管理関連

- Zone Transfer over TLS（XFR over TLS, XoT）
  - 送受信双方の暗号化ゾーン転送をサポート
  - TLSハンドシェイク時にDoT-ALPNというALPNトークンの選択が必要
    - RFC9103非準拠のXoTサーバーで問題が発生する可能性がある

- MAP形式のゾーンファイルは廃止された
  - MAP形式は、BIND 9のインメモリゾーンデータベースのイメージ
  - named-compilezoneでRAWフォーマットに変換し、設定を適切に変更することが推奨されている

DNSSEC関連

- Aggressive Use of DNSSEC-Validated Cache (RFC 8198)がデフォルトで有効(synth-from-dnssec)
  - Aggressive Use of DNSSEC-Validated Cache (RFC 8198)の機能
    - 以前にキャッシュされたNSEC/NSEC3リソースレコードで表現される範囲内に問い合わされた名前があれば、署名を検証するリゾルバーは直ちにネガティブ応答を返す
    - ワイルドカードの存在を利用して肯定応答を合成する
  - パフォーマンス低下を引き起こす場合があったため、BIND 9.14.8でいったん無効にされたが、不具合が修正されBIND 9.18でデフォルトで有効になった
    - 否定応答合成は現在、NSECを使用するゾーンでのみサポート

Extended DNS Errors (EDE)(RFC 8914)

- EDEの一部が実装された
  - 25個あるうちの3つがBIND 9.18で実装されている（BIND9.19では7つ）
    - 3 – Stale Answer
      - リゾルバが制限時間内に名前解決の結果を得ることが出来ず、エラーを返す代わりに以前にキャッシュしたデータで応答した
    - 18 – Prohibited
      - 未承認のクライアントからクエリを受け取った権威サーバー、リゾルバは、REFUSEDメッセージにこのコードを注釈として付与することができる
    - 19 – Stale NXDOMAIN Answer
      - リゾルバが制限時間内に名前解決の結果を得ることが出来ず、エラーを返す代わりに以前にキャッシュしたNXDOMAINを応答した
    - 3, 19は機能としては、RFC 8767に書いてある（BIND9 serve-staleオプション）

digコマンド

- オプションの追加
  - DoTクエリを送信できるようになった（+tls）
  - DoHクエリを送信できるようになった（+https）
    - DoT/DoHによるDNSクエリーの転送はサポートされていない
  - IPV4ONLY.ARPA　AAAAを検索し、見つかったDNS64プレフィックスを表示（+dns64prefix）

- オプションの廃止
  - +[no]mappedオプションの廃止
    - このオプションはマップされたIPv4 over IPv6アドレスの使用の許可するものだった
    - IPv6ソケットは、IPv6パケットの送受信のみに明示的に制限されるようになったため廃止

BIND ディストリビューションのコマンド

- rndc
  - libuvに置き換えたことにより、UNIXドメインのソケット通信が出来なくなった
  - localhost:953等を使用して接続する必要がある
- デーモンでも管理プログラムでもないバイナリは$bindirに移された
  - $sbindirは、ddns-confgen, named, rndc, rndc-confgen, tsig-confgenのみ
- Pythonユーティリティのサポートの廃止
  - 依存しているdnssec-checkds, dnssec-coverage, dnssec-keymgrも削除
  - これらで提供されていた機能はnamedに統合（ dnssec-policy ）

情報ソース

- Release Notes — BIND 9 9.18.19 documentation
- BIND 9 Significant Features Matrix (isc.org)
- Changes to be aware of when moving from BIND 9.16 to 9.18 (isc.org)

執筆時点の情報が含まれています
公式の最新情報をご確認ください