BIND 9.11から9.16への移行のポイント（権威DNSサーバー編）

2021年6月25日

DNS Summer Day 2021

（株）日本レジストリサービス

阿波連　良尚（あはれん　よしたか）

本資料の内容

- BIND 9.11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 9.16とは
  - 最近の更新リリース状況
  - 大きな変更: netmgr
  - 機能分類ごとの変更点の説明
  - 9.17以降に予定されている変更

参考情報として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 9.16とは

- 長期間のサポートを受けられるExtended Support Version（ESV）になる**予定**のメジャーバージョン
- 2024年第一四半期までサポートされる予定
- 現在のESVはBIND 9.11で、2021年末でサポート期間終了
  - 致命的な脆弱性の修正は2022年第一四半期までは提供される見込み
- 現在の開発版（奇数メジャーリリース）はBIND 9.17
  - 開発版リリースは全て昔のalpha・beta・rcバージョンに相当
  - 新機能を試してISCにフィードバックしたい人々向け

そろそろ9.16の評価に向けた準備が必要な時期

最近の更新リリース状況

- 毎月のリリースでバグ修正がなされている
  - BIND 9.11でもセキュリティ以外の修正が含まれる
- マルチスレッド関連のバグを精力的に修正している
  - ThreadSanitizer（スレッド間のデータ競合やデッドロックを検出する仕組み）を使ったテストを開発過程で定期実行し、コードの問題を検出
  - ISC GitLabのIssueを「ThreadSanitizer」「TSAN」で検索すると雰囲気が分かる
  - netmgrの導入（後述）にあたっても威力を発揮
  - 今まで運よく？誰にも踏まれなかった古からのバグも……

大きな変更: netmgr （9.16～）

- 非同期I/Oライブラリであるlibuvを用いるようにする改修
  - DNS-over-HTTPS（DoH）など新しいトランスポートへの対応など拡張性や保守性を見据えて選択したもの
  - ネットワーク処理やタスク処理を書き直す大改修になる
  - namedだけでなく、dig・delv・nsupdateなどにも利用される
- 導入まで（導入した後も）の長い道のり
  - BIND 9.15・9.17（開発版）に導入され、安定させながらBIND 9.16に数年がかりでバックポート
  - バグやパフォーマンスの問題をBIND 9.16でも修正中

ゾーン関連

- max-ixfr-ratioオプションの追加
  - **プライマリー側で**ゾーン転送にIXFR応答を使うサイズの上限
  - セカンダリー側でIXFRでゾーン更新を受け取る間、転送に含まれる更新量が多いとクエリの処理に影響が出ていた
  - このオプションを指定すると、ある程度大きな更新についてはプライマリー側でAXFRに切り替えて応答することができる
  - ゾーンの大きさの相対値で指定: デフォルトはunlimited
- mirror zone（実験的機能）
  - type secondaryと似ているが、ゾーン全体をDNSSEC検証してから使う
  - ルートゾーンについてはルートヒント情報からprimaryを自動的に選択
  - RFC 7706のローカルにルートゾーンを持たせる際に便利

DNSSEC関連

- ビルド時のDNSSECサポートが必須に（9.13～）
  - コンパイル時にDNSSECサポートを無効化できなくなった
  - BIND 9のビルドには、OpenSSLが必須に
- Key and Signing Policy（KASP）
  - namedがプライマリーとしてゾーンを管理しているとき、DNSSEC署名を自動化するためのポリシーを定義する仕組み
  - auto-dnssecオプションやinline-signingオプションなどに代わり、dnssec-policyオプションが追加された
  - dnssec-keymgrコマンドでDNSSEC鍵ロールオーバーを行う

ログ関連

- タイムスタンプ形式を選べるようになった（9.12～）
  - print-timeオプションの引数として、下記を指定できる
    local: 従来の形式（25-Jun-2021 13:00:00.000）
    iso8601: ISO 8601形式（2021-06-25T13:00:00.000）
    iso8601-utc: ISO 8601（UTC）形式（2021-06-25T04:00:00.000Z）
  - 互換性のため、yesを指定するとlocalと見なされる
- ゾーン転送関連のログ出力項目の追加・変更（9.15～）
  - 転送完了時にシリアル番号がプライマリー側で出力されるようになった
  - generalに出ていた一部のメッセージをxfr-in（セカンダリー側）に変更
  - ゾーンサイズ・レコード数・メッセージ数についてセカンダリー側（受信する側）でも出力されるようになった

EDNS関連

- DNS Flag Day 2020対応（9.11にもバックポート済）
  - EDNSバッファサイズのデフォルト値が1232に変更された
- EDNS TCP Keepalive（RFC 7828）対応（9.12～）
  - TCP接続のタイムアウト値を伝えるためのEDNS拡張
  - TCP pipelining（RFC 7766など）でTCP接続を使いまわすようになったので、サーバーとクライアントとの間でタイムアウト値をネゴシエーションできるように導入された
  - TCP timeout関連のオプションも併せて追加

    tcp-initial-timeout: TCP接続を受け付けてから、クライアントが最初のメッセージを送るまでの待ち時間

    tcp-idle-timeout: EDNS TCP Keepaliveが無効なクライアント向けタイムアウト

    tcp-keepalive-timeout: EDNS TCP Keepaliveが有効なクライアント向けタイムアウト

チューニング関連

- --with-tuning=large がデフォルトに
  - configureオプションで指定できるチューニング設定のデフォルトがsmallからlargeに変わった
  - ソケットバッファサイズや一度のシステムコールで処理するイベント数やタスク数などが増え、メモリ使用量が増える
- CPUコア数が多いとメモリ使用量が劇的に増える
  - https://gitlab.isc.org/isc-projects/bind9/-/issues/2398
  - AArch64でCPUコア数が256個ある環境で、BIND 9.11と比べてメモリ使用量（RSS）が184MBから17.8GBまで増えたというバグ報告
  - amd64でCPUコア数が32個、レコード数10個程度のゾーン1個で試すと手元の実験環境では47MB（9.11.31）→225MB（9.16.18）に増えた

digコマンド

- YAMLサポート（9.15～）
  - 出力形式をYAMLにできる: プログラムで読み取りたい時に便利
  - 内容はdnstap-readコマンドと共通
- Extended DNS Errors（EDE）サポート（9.11にもバックポート済）
  - RFC 8914で定められた、エラーコードのためのEDNS拡張
  - ServFailの場合でも、「権威DNSサーバーが応答しない」「DNSSEC署名がおかしい」などといった詳細な情報を得られる
  - namedがEDEでエラー情報を返す機能は未実装
    https://gitlab.isc.org/isc-projects/bind9/-/issues/1836

その他細かい変更

- primary/secondaryという言葉を使うようにする
  - RFC 8499（DNS Terminology: DNS用語集、JPRSの藤原和典も著者の1人）に合わせる形で修正
  - 設定ファイルやコマンド出力などでmaster/slaveの代わりに使われる
  - 設定ファイルでの記載についてはmaster/slaveも利用可能
- ソースtarballの圧縮方式がgzipからxzに（9.15～）
  - BIND 9.16.18で試すと6.5MB（gzip -9）→4.8MB（xz）に削減
  - モダンなGNU tarやBSD tarなら -J （大文字）で展開できる

機能や設定項目の削除（1）

- cleaning-intervalオプションの廃止（9.15～）
  - もともとはキャッシュメモリを定期的に掃除する間隔を制御するもの
  - BIND 9.11でも既に効果がないオプションになっていた
  - BIND 9.16では設定ファイルから削除するようメッセージがログに記録される
- dnssec-enableオプションの廃止（9.13～）
  - DNSSEC検証のオプション……ではなく、問い合わせに対してDNSSEC関連のレコードを返すか否か（デフォルトはyes）
  - 廃止により、ゾーンにDNSSEC関連のデータが含まれていれば常にDNSSEC関連のレコードを返すようにした

機能や設定項目の削除（2）

- digコマンドのIDNA 2003フォールバックの削除（9.13～）
  - ほとんどの場合影響を受けないはず
- digコマンドの+sigchase/+topdown/+trusted-keysの削除（9.12～）
  - DNSSEC検証しながら問い合わせるにはdelvコマンドをご利用ください
- digコマンドの逆引き用ip6.int（-i）オプション削除（9.13～）
  - ip6.intは10年以上前に廃止、現在はip6.arpaを使う
  - -xオプションでIPv4・IPv6ともに使えます
- dnssec-keygenコマンドでHMAC鍵を作る機能を削除（9.12～）
  - HMAC鍵の生成にはtsig-keygenコマンドをご利用ください

機能や設定項目の削除（3）

- lwresd関連のコードを削除（9.12～）
  - 使っている人はほぼいないはず
- 権威側EDNS Client-Subnet（ECS）サポートを削除（9.13～）
  - クエリに含まれるECS情報に基づいてACLを定義する機能が削除された
- GeoIPサポートを削除（9.15～）
  - GeoIP2（libmaxminddb）に置き換え
- DNSSEC Lookaside Validation（DLV）サポートを削除（9.15～）
  - DLVは、ルートゾーンが署名されていなかった時代に、特定のドメイン名配下でDNSSEC検証をできるようにする仕組み
  - 現在では使われることはない

9.17以降に予定されている変更（1）

- Windowsサポート終了
  - 9.18でWindowsサポートは廃止される予定
  - Windowsバイナリパッケージが提供されなくなるが、digコマンドについては非公式だが提供継続される可能性も
- digの出力にトランスポートを追加 [ISC GitLab #1816]
  - どのトランスポートを使ったか: UDP・TCP（・TLS）を表示する
  - 特定のqtypeは必ずTCPになったり、TC bitがオンの場合に自動的にTCPフォールバックするので、地味だがうれしい機能追加
  - 9.16にバックポートされる予定とチケットに記載されていたが外れた

9.17以降に予定されている変更（2）

- 反復検索でAA bitがオフの応答を破棄 [ISC GitLab #2485]
  - プロトコルに準拠しない挙動への対応をやめてコードをシンプルに
  - 影響調査含めて実装内容を検討中

情報ソース

- ISC Webサイト（ドキュメントやブログ記事）
  - https://www.isc.org/bind/
  - https://www.isc.org/blogs/
- ソースパッケージに含まれるCHANGESやリリースノート
- ISC GitLabのIssueやマージリクエスト
  - https://gitlab.isc.org/isc-projects/bind9
- bind-usersメーリングリストの投稿
  - https://lists.isc.org/pipermail/bind-users/

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