BIND 9.9から9.11へ移行のポイント（権威DNSサーバー編）

2018年6月27日

DNS Summer Day 2018

（株）日本レジストリサービス

本資料の内容

- BIND 9.9.xをお使いの方に向けた、変更点の紹介
  - 権威DNSサーバー機能関連
  - ログ関連
  - その他
- DNS Cookie （RFC 7873）の概要と運用へのインパクト

BIND 9.11とは

- 長期間のサポートを受けられる、BIND 9のメジャーバージョン（Extended Support Version: ESV）
- BIND 9.11.3（2018年3月リリース）からESVに指定された
- 2021年12月末までサポートされる予定
- 1つ前のESVはBIND 9.9で、2018年6月末でサポート期間終了（**あと3日です！**）

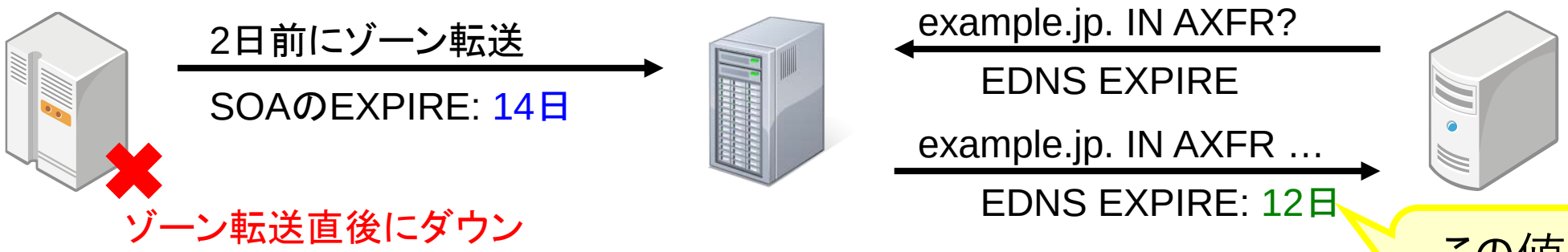
JPRSの藤原和典が著者に加わっているRFC 8198（NSEC/NSEC3 RRを利用して、反復検索せずにドメイン名の不存在を確認する）は、BIND 9.12以降でサポートされています（BIND 9.12ではNSECのみサポート）

権威DNSサーバー機能関連（1/4）

- `update-policy: local;`の挙動変更
  - 「localhostから」かつ「自動生成された専用のTSIG鍵を使った」場合のみ受け入れるよう意味を変えた
  - 自動生成されたTSIG鍵を他のホストにコピーして使っている場合に注意
  - JPRSも注意喚起を実施 <https://jprs.jp/tech/notice/2018-03-22-bind9-dynamicupdate.html>
- パイプライン化されたTCP問い合わせへの応答
  - RFC 7766に準拠し、1本のTCPセッションで並行して複数の問い合わせ・応答を処理できるようになった
  - クライアントとの互換性に問題がある場合、`keep-response-order`でホワイトリスト

権威DNSサーバー機能関連（2/4）

- `request-expire`の追加
  - RFC 7314のEDNS EXPIREオプションを付けるか指定する（デフォルトはyes）
  - オリジナルのexpire時間の代わりに、ゾーン転送元がデータを受け取ってからの時間を知ることができる: 多段でゾーン転送を行っているときに便利



- `max-records`の追加
  - ゾーン内のレコード数に上限を設ける（デフォルトは0: 上限なし）
  - ゾーン転送を受ける際に、大量のレコードを転送されるのを防げる

権威DNSサーバー機能関連（3/4）

（項目だけ紹介）

- DNS RRLが標準で有効化
  - configure時に`--enable-rrl`を指定しなくてもよくなった
- ゾーンのデータベースバックエンドとしてDynDBに対応
- ゾーン設定の動的管理バックエンドとしてLMDBに対応
- ゾーン設定をゾーン情報の形で配布できるCatalog Zonesに対応

権威DNSサーバー機能関連（4/4）

（項目だけ紹介）

- `in-view`: viewをまたいだゾーンの共有
- `masterfile-format`（変更）
  - ゾーンファイルのフォーマットとして`map`が増えた
- `masterfile-style`（追加）
  - デフォルトは`relative`: 以前と同じ形式
- `serial-update-method`（変更）
  - Dynamic DNSのシリアル番号の形式として`date`（YYYYMMDDnn）が増えた

ログ関連（1/3）

- クエリログフォーマットの変更
  - 接続元IPアドレス（2001:db8::c:53#23456）の前に、named内部のクライアントオブジェクトID（@0x????????????????）が追加された
  - EDNSバージョン番号（E(n)）が追加された
  - DNS Cookieの検証結果（正しい: V、正しくない: K）が追加された

クエリログの例

queries: info: client @0x7f8db039d7a0 192.0.2.254#6278 (example.jp): query: example.jp IN A -E(0)DCV (203.119.40.1)

内部のクライアントオブジェクトID

EDNSバージョン

DNS Cookie

ログ関連（2/3）

- namedのオプションによるログ出力先ファイル指定
  - ログ設定がない場合のデフォルトでは、起動直後のログはsyslogに出力していた
  - namedの起動オプションに「`-L (filename)`」が追加され、デフォルトのログ出力先としてファイルを指定できるようになった
- ログファイル出力のバッファリング
  - ログのchannel設定に`buffered`オプションが追加され、バッファリングを有効にする（ログ出力時に毎回flushしないようにする）ことができるようになった
  - 異常終了時にログの一部が失われることと引き換えに、性能の向上が期待できる
  - デフォルトではバッファリングしない

ログ関連（3/3）

- ログカテゴリの追加
  - `dnstap`: dnstap関連のログ
  - `trust-anchor-telemetry`: トラストアンカー情報を通知するクエリを受けたときのログ（ルート以外では通常来ないはず）
- dnstap
  - DNSトラフィックをサーバー側で記録する仕組み
  - 詳しくは <http://dnstap.info/>

その他（1/4）

- `tcp-clients`のデフォルト値変更
  - DNSサーバーとして、同時に受け付けるTCPクライアント接続数の制限
  - 100から150に増えた
- `minimal-any`の追加
  - デフォルトはno
  - yesに設定すると、UDPでANYクエリを受け取ったときにすべてのレコードを応答する代わりに、レコード1つとそれに対応するRRSIG（もしあれば）だけ応答する
  - ANYクエリによるDDoS増幅器になるのを避けるのが目的

その他（2/4）

- read-only rndcの追加
  - named.confに書くrndcのアクセス制御として、read-onlyが指定できるようになった
  - 特定のrndcクライアントに、サーバーに変更を加えないコマンドだけ許可することができる
- rndcコマンド
  - -r: サーバーからのコマンド結果コードを表示
  - modzone/showzoneコマンド: addzoneで追加したゾーンの表示と編集
  - managed-keysコマンド: トラストアンカーの表示や更新
  - zonestatusコマンド: 読み込み日時、シリアル番号などゾーンステータスの表示

その他（3/4）

（項目だけ紹介）

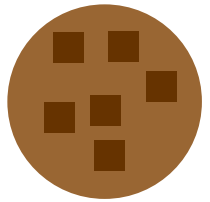
- GeoIPデータベースを用いたACLのサポート
- EDNS Client Subnetサポート（実験的）
- CDSレコード・CDSKEYレコードの自動生成
- 統計情報関連（出力形式の変更・追加、項目追加）
- configureオプション `--with-tuning=large`
  - ソースコード内の定数を高性能サーバー向けに変更
  - 詳しくは <https://kb.isc.org/article/AA-01314>

その他（4/4）

（項目だけ紹介）

- ネットワークインタフェースの追加・削除の自動スキャン
- HSM対応: PKCS#11のネイティブ対応
- `lock-file`（追加）
  - ロックファイルによる二重起動防止; 起動時オプション`-X` *`(lockfile)`*でも指定可
- `message-compression`（追加）
  - CPU使用率を減らすためにDNS名前圧縮をオフにできる; デフォルトはオン

DNS Cookie （RFC 7873）とは



- DNSメッセージの偽装を検知する仕組み
  - EDNS拡張として小さなデータ（Cookie）を埋め込み、相手からのメッセージに同じものが含まれているか否かで偽装を検知する
- クライアントとサーバー両方で相互に確認する
  - クライアント: 問い合わせメッセージにクライアントクッキーを含めて送り、返ってきた応答メッセージに同じクライアントクッキーが含まれているか確認する
  - サーバー: 問い合わせメッセージに含まれるサーバークッキーに関して、クライアントのIPアドレス等から妥当性を検証する

クッキー対応の問い合わせと応答の例

権威DNSサーバー運用へのインパクト

- メッセージサイズの増大
  - 問い合わせや応答にクッキーが含まれるようになる
  - 仮にすべてのクライアントがDNS Cookieに対応した場合には、帯域幅が5％程度増加する見込み
- サーバーインスタンス間でのserver secretの共有
  - サーバークッキーは、クライアントの情報（IPアドレス・クライアントクッキー）とserver secret（サーバーだけが知っている秘密情報）から計算される
  - ロードバランサー配下にいたり、anycastを構成しているサーバーは、同じserver secretを共有している必要がある
  - RFC 7873ではサーバークッキーの生成に同じserver secretを36日以上使いまわしてはならない（MUST NOT）とされており、頭が痛い

BIND 9.11.3での対応状況

- デフォルト設定では、サーバークッキーが不正でも通常通り扱う
- サーバー側でCookieの扱いをオフにする機能がない
  - ロードバランサーなどで、DNS Cookie未対応のサーバーと混在させるときに困る
- ロールオーバー機能がない
  - 複数のserver secretを指定することができない
  - ロールオーバー時に、古いserver secretを元にしたサーバークッキーが不正なものとみなされる
- BIND 9.11.4で上記の機能不足は解決される見込み
  - 6月14日に最初のリリース候補版（9.11.4rc1）が公開された