フルリゾルバ編

BIND9.11からBIND9.16移行のポイント

2021年6月25日

DNS Summer DAY 2021

株式会社QTnet
技術本部　通信サービス設備部

末松慶文 (yo_suematsu at qtnet.co.jp)

自己紹介

末松慶文 - DNSを含むサーバ関連の構築と運用・保守などを十数年

所属

株式会社QTnet （旧 九州通信ネットワーク株式会社）

日本DNSオペレータズグループ 幹事

・DNSの耐障害性強化に向けてJPRSと共同研究を開始 (2015年7月13日)

JPRS: JPRSが新gTLD「.jprs」でDNSの耐障害性強化に向けてISPとの共同研究を開始　http://jprs.co.jp/press/2015/150713.html

QTNet: JPRSとの共同研究について　https://www.qtnet.co.jp/info/2016/20160118.html

・APRICOT 2017 TLD Anycast DNS servers to ISPs (JPRS, QTnet)

https://2017.apricot.net/program/schedule/#/day/9/network-operations-2

・JPRSおよび電力系通信事業者8社が共同研究の成果を公開

https://www.qtnet.co.jp/info/2017/20171031_1.html

https://tldlabs.jprs/acts/s001/

個人の見解であり、所属する組織の見解を示すものではありません。

さまざまなBIND

・オープンソース版　　例：BIND 9.11.33
　サポート: コミュニティサポート(ML: bind-users)、有償のサポート
　今回はこちらを対象にお話しします。

・Subscription版　　例：BIND 9.11.33-S1
　サポート: 有償のサポート

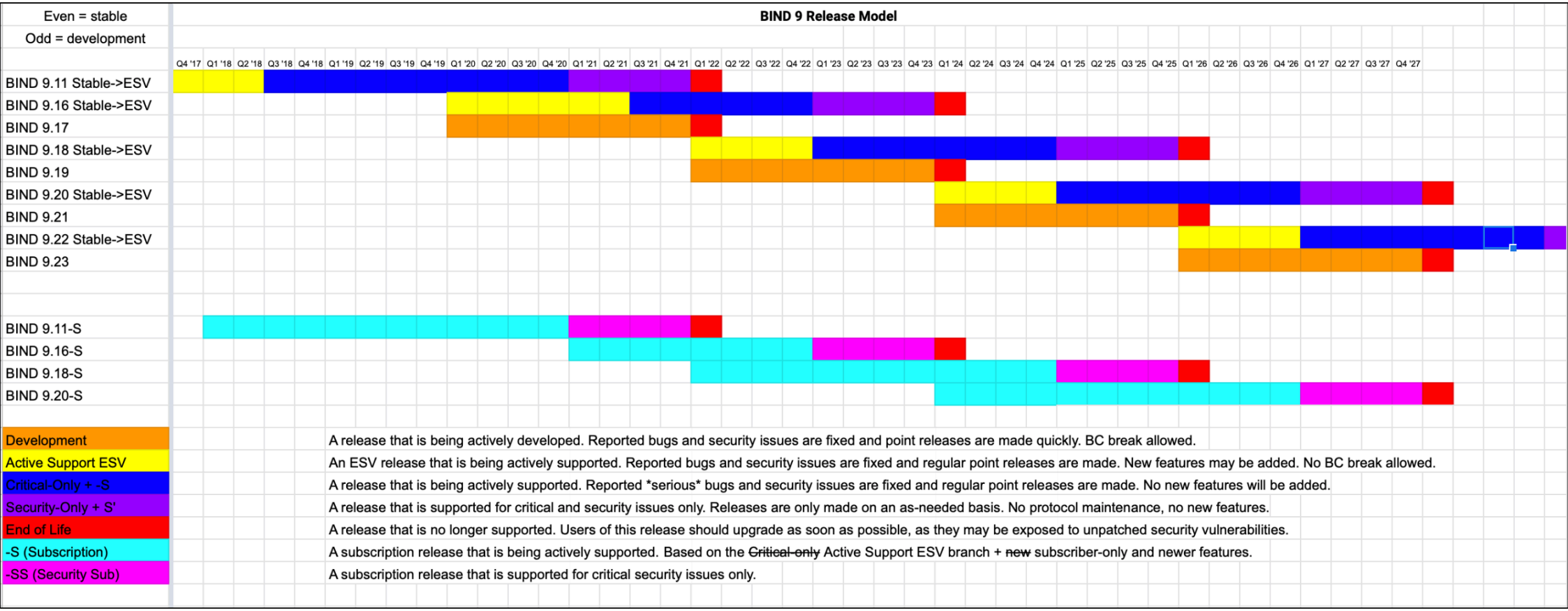
・OSに付属するBIND　例：BIND 9.9.4-RedHat-9.9.4-50.el7
　サポート: 各ディストリビューションのポリシーに準じる。

・アプライアンス　　例：Infoblox
　サポート: 各製品のポリシーに準じる。

BIND Release Model

- BIND 9.11
  - 長期間サポートバージョン Extended Support Version(ESV)
  - 2021年12月末にサポート終了
  - 2022年3月末まで致命的な脆弱性の修正はベストエフォートで提供

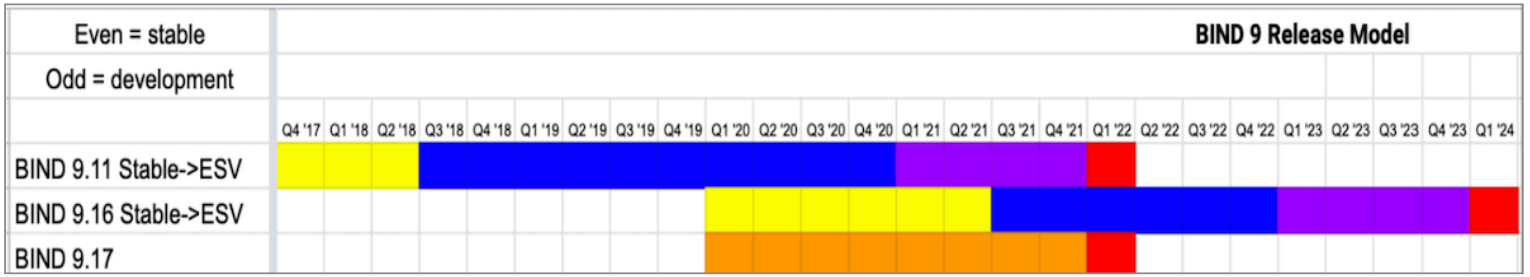
参考：https://kb.isc.org/docs/aa-00896



BINDバージョンアップに向けて

・バージョンの選定
- BIND 9.11　Status: ESV
- BIND 9.16　Status: Current-Stable
- BIND 9.17　Status: Development

recommended for production use. by ISC



引用: https://www.isc.org/blogs/2021-bind-release-model/

・バージョンアップの際のポイント
- BIND9.11と9.16の機能差分の確認
- 機能試験
- 性能試験(応答性能)
- 応答差異の確認

今回はこちらの話を

ISCよりスライドを
提供いただきました

9.16

- New asynchronous, multi-threaded networking framework
- New KASP-based dnssec-policy
- Serve Stale improvements
- 9.16 will be declared ESV with the July release:
  - no more refactoring
  - no performance regression from 9.11

BIND9.16で追加された機能の一覧

Feature	Full resolver	Authoritative DNS
DDOS Mitigation: Serve Stale	✓	
DNSSEC: Key and Signing Policy		✓
DNSSEC: "validate-except" Permanent Negative trust anchors	✓	
EDNS Padding (RFC 7830)	✓	✓
Management: automatic DNSTAP file rolling	✓	✓
Management: timestamp suffix option for rolled log files and DNSTAP files	✓	✓
Mirror Zones		✓
Module - plug-in support for query processing	✓	✓
Performance: EDNS TCP keepalive support (RFC 7828)	✓	✓
Performance: glue cache	✓	✓
Performance: minimal responses	✓	✓
Performance: answer synthesis from cached NSEC	✓	
Performance: Pipelined TCP queries (server side)	✓	✓
QNAME Minimization	✓	
RPZ: refactored RPZ	✓	
RPZ: Response Policy Service API	✓	

filter-aaaa.so でのみ使用

BIND9.16で削除された機能一覧

Feature	Full resolver	Authoritative DNS	備考
EDNS Client-Subnet (ECS) option support for authoritative servers		✓	
DLV (DNSSEC Look-Aside Validator)	✓		
Windows 32-bit support	✓	✓	deprecated

We will try to create a separate dig.exe and post that as a separate download, so people can still use dig on Windows. If we are able to do this, it will not be an officially maintained product.
https://www.isc.org/blogs/bind-update-summer2021/

フルリゾルバ追加機能 (1/2)

・DDOS Mitigation: Serve Stale

- 権威DNSが応答を返せない状態となった際に、フルリゾルバが期限切れのキャッシュを利用することで名前解決を継続可能にする機能

参考：https://kb.isc.org/docs/serve-stale-implementation-details

- デフォルト無効
- Serve StaleとFetch-limitsを同時に有効にした際にServeFail応答を返す問題があったが、BIND9.16.13にて修正

他にも・・
安定化のための変更を
BIND9.16.17にて実施

ISCよりスライドを
提供いただきました

BIND 9.16 Serve Stale improvements

Changed defaults per RFC 8767 recommendations:

- *max-stale-ttl* changed from 1 week to 1 day to declutter the cache.
- *stale-answer-ttl* changed from 1 second to 30 seconds.

New configuration options:

- *stale-cache-enable* has been introduced to enable or disable keeping stale answers in cache.
- *stale-refresh-time* has been introduced to allow serving stale RRset before refreshing it.
- *stale-answer-client-timeout* that controls the time that `named` waits for remote server to answer before serving answer to the client.

Several of these changes were based on research from JPRS and the ISP group, including QTNET - we appreciate the testing!

- https://indico.dns-oarc.net/event/38/contributions/846/attachments/804/1424/evaluation%20of%20anti-DDoS%20features%201.pdf

.

フルリゾルバ追加機能 (2/2)

- Performance: minimal responses
  - Authority , Additionalセクションを削って応答を返す
  - 応答サイズ削減によるレスポンスの向上
  - デフォルトはno-auth-recursive

> no-auth-recursive: the same as no-auth when recursion is requested in the query (RD=1), or the same as no if recursion is not requested.

- QNAME Minimization

参考：https://www.isc.org/blogs/qname-minimization-and-privacy/

  - 名前解決に必要な最低限の情報のみを権威DNSに問い合わせするようにする技術
  - デフォルトはrelaxed 、将来のリリースではstrictに(RFC 7816に忠実に従う)

予期しない応答があった場合、通常の問い合わせにフォールバックする

確認すべき資料

- BIND 9 Significant Features Matrix
  - https://kb.isc.org/article/AA-01310/0/BIND9-Significant-Features-Matrix.html
- BIND Updates
  - https://www.isc.org/blogs/bind-update-summer2021/
- BIND 9.16 Administrator Reference Manual (ARM)
  - https://kb.isc.org/docs/bind-916-administrator-reference-manual
- Release Notes
  - https://www.isc.org/download/

正確な情報と詳細については公式のドキュメントをご確認ください。

ISCよりスライドを
提供いただきました

BIND 9.18

- Planned for January, 2022
- Includes DNS over TLS (DoT) & DNS over HTTPS (DoH)
- Encrypted transports based on the new network manager infrastructure
- Includes XFR over TLS
- DoT and DoH are currently available in 9.17 for testing

ここ九州の地で、わたしたちは地域のみなさまの暮らしが豊かに、光り輝くよう
さまざまな情報通信サービスの提供に取り組んでおります。

日々変化する情報通信のフィールドで、**「安心」**、**「わかりやすい」**サービスを
「九州」からお客さまに提供し続けたい。
コア事業である『QT PRO』『BBIQ』『QTmobile』とともに未来へ挑戦します。