DNS実装ダイバーシティの話 Unbound

InternetWeek2012

(株)NTTPCコミュニケーションズ
高田 美紀

自己紹介とお詫び

- WebARENAホスティングサービス
  - 1999年～
  - 共用レンタルサーバ、VPSなど
- DNSOPS.JP 幹事
- お詫び
  - 資料の公開が遅れて申し訳ありません
  - 実環境では「まだ」使っていません
  - 検討段階

Unboundとは

- キャッシュDNSサーバソフトウェア
  - 権威DNSサーバの機能もある
- オランダNLnet Labs他4組織で開発
  - http://unbound.net/
  - BINDの代替、DNSサーバの多様性
  - 現在はNLnet Labsにて開発、保守
- 日本Unboundユーザ会
    - http://unbound.jp/
    - 和訳マニュアル、アップデートのアナウンスなど

なぜUnbound?

- 不定期的にやってくるBIND脆弱性発見
  - クリティカル、workaroundなし
- アップデートにはコストがかかる
  - 検証、各所への連絡、実際の作業、重点監視
- アップデートまでに攻撃されるリスク
  - 1パケットでnamedが死んだり
  - DNSサービスの断=>サービス全断
- 高パフォーマンス
  - (参考資料を参照)

BIND(キャッシュ)との違い

- 挙動の違い
  - DNSラウンドロビン
  - 多段CNAME
  - cache snooping
- ない機能
  - View
  - AAAA filter
  - ResponsePolicyZone
  - DNS64
- 各種コマンド
  - rndc
    - unbound-control
  - dig
    - drill
- ログ形式

挙動の違い(1)

- DNSラウンドロビン
  - unbound 1.4.17にて実装
  - デフォルトではオフ
    - rrset-roundrobin: yes
- 多段CNAME
  - 9段以上の多段になるとSERVFAIL
  - RFCには特に規定がない部分

挙動の違い(2)

- cache snooping
  - キャッシュDNSサーバへの非再帰検索
  - unboundは返答しないのがデフォルト
    - キャッシュには再帰検索しかこない筈だから?
  - NW単位で許可設定
    - allow-control: 192.168.0.0/24 allow_snoop
  - BINDからの置き換えと考えると必要かと

導入シナリオ

- bindをunboundに置き換え
  - 置き換え時の一時的なコストのみ
  - 可能ならおすすめ
- hot standby
  - LBの後ろにBINDとunbound両方用意
- cold standby
  - 通常はBINDを使用
  - namedが死んだらunbound登場
  - BIND特有の機能を使っているなどの場合
- 置き換え以外は両方のサーバを管理することになる
  - おすすめではないが、背に腹はかえられない
  - unboundにも脆弱性発見の可能性がある

cold standbyの一手法

- bind付属のプロセス監視ツール
  - contrib/nanny/nanny.pl
  - psとdigで監視、異常があったら再起動
- 改造
  - 異常検知時にunboundを起動する
  - unbound稼働中の異常検知
    - namedは起動しない

参考資料

- UnboundキャッシュDNSサーバ 大規模用と向け機能の実装
  - 東 大亮さん
  - http://dnsops.jp/event/20120901/Unbound-higashi-dnsops-2012summerday2-final.pdf
  - DNS Summer Days 2012での発表資料