DNSハンズオン
フルサービスリゾルバ

NTTコミュニケーションズ株式会社
技術開発部
高田 美紀

Internet Week 2016
2016/11/30

2016/12/1 15:30 更新
更新分は赤字で表示

Unbound設定の設計(1)

- 基本的には標準設定を使用: 最小限の設定
- DNSSEC検証を設定する
  - auto-trust-anchor-file 指定
- unbound-control を有効にする
  - remote-control:<改行>
  - <tab>control-enable: yes
- 使用するインタフェースの設定
  - <tab>interface: 127.0.0.1
- interface に loopback 以外を指定する場合
  - デフォルトでは全て拒否。必要なアドレスだけアクセス許可
  - 例: 192.0.2.0/24 からのアクセスを許可する場合
  - <tab>access-control: 192.0.2.0/24 allow

Unbound設定の設計(2)

- ラウンドロビンDNSを有効にする
  - <tab>rrset-roundrobin: yes
- DNSSEC検証失敗の詳細をログに出力する
  - 今回は /var/log/messages
  - <tab>val-log-level: 2
- キャッシュ容量の制限緩和。サーバのメモリ量に応じて設定
  - <tab>rrset-cache-size: 400m
  - <tab>msg-cache-size: 200m
- その他チューニングパラメータ等の解説はしません
  - 日本語マニュアル
    - ✓ http://unbound.jp/unbound/unbound-conf/
  - DNS Summer Day 2016 IIJ 島村さん資料
    - ✓ BIND9 との違い、BIND9 からの移行で注意すべき点など豊富
    - ✓ http://dnsops.jp/event/20160624/unbound.pdf

Unboundのインストール

- ソースコードのダウンロード
  - http://www.unbound.net/download.html
  - Current version (1.5.10)
  - wget http://www.unbound.net/downloads/unbound-1.5.10.tar.gz
- 今回は src/ 配下に取得してあります

- tar xzvf src/unbound-1.5.10.tar.gz
- cd unbound-1.5.10
- ./configure
- make
- sudo make install
- cd ..
- 確認: ls -al /usr/local/sbin/unbound
  - -rwxr-xr-x 1 root root 3106061 11月 30 14:35 2016 /usr/local/sbin/unbound

Unboundの設定(1)

- ここからは root で作業してください
  - sudo -s -H
- “unbound” group/user 作成
  - groupadd --system unbound
  - useradd --system -g unbound -s /sbin/nologin unbound
  - 確認: id unbound
- DNSSEC 鍵ディレクトリ作成
  - cd /usr/local/etc/unbound/
  - mkdir key
  - chown unbound:unbound key
  - chmod 755 key
    - ✓ unbound ユーザが書き込むため、標準から変更
  - 確認: ls -al key
    - ✓ drwxr-xr-x 2 unbound unbound 4096 11月 30 14:52 2016 key

Unboundの設定(2)

- DNSSEC Trust anchor の取得 → root.key 生成
  - cd /usr/local/
  - sudo -u unbound sbin/unbound-anchor -a etc/unbound/key/root.key
  - 確認: ls –al etc/unbound/key/root.key
    - ✓ -rw-r--r-- 1 unbound unbound 759 11月 30 14:52 2016 etc/unbound/key/root.key

- unbound-control コマンドのための鍵ファイル生成
  - sbin/unbound-control-setup
  - 確認: ls –al /usr/local/etc/unbound/unbound_*
    - ✓ 4ファイルできているはず
    - ✓ -rw-r----- 1 root root 2459 11月 30 14:48 2016 /usr/local/etc/unbound/unbound_control.key
    - ✓ -rw-r----- 1 root root 1330 11月 30 14:48 2016 /usr/local/etc/unbound/unbound_control.pem
    - ✓ -rw-r----- 1 root root 2459 11月 30 14:48 2016 /usr/local/etc/unbound/unbound_server.key
    - ✓ -rw-r----- 1 root root 1318 11月 30 14:48 2016 /usr/local/etc/unbound/unbound_server.pem

unbound.conf の作成

- cd /usr/local/etc/unbound
- mv unbound.conf unbound.conf.orig
- cat >unbound.conf
- server:
- <tab>interface: 127.0.0.1
- <tab>auto-trust-anchor-file: "/usr/local/etc/unbound/key/root.key"
- <tab>rrset-roundrobin: yes
- <tab>val-log-level: 2
- <空行>
- remote-control:
- <tab>control-enable: yes
- <control-d>
- 確認: cat unbound.conf

Unboundの起動

- unbound.conf のシンタックスチェック
  - /usr/local/sbin/unbound-checkconf
  - 確認:
    - ✓ unbound-checkconf: no errors in /usr/local/.../unbound.conf
- 起動
  - /usr/local/sbin/unbound
- 起動確認
  - tail /var/log/messages
  - unbound: [PID:0] info: start of service (unbound 1.5.10).

unboundの動作確認

- drill での確認。-D は enable DNSSEC
  - drill -D @127.0.0.1 internetweek.jp A
  - drill -D @127.0.0.1 www.nic.ad.jp A
  - drill -D @127.0.0.1 www.asahi.com A
  - drill -D @127.0.0.1 nasa.gov A
- dig での確認
  - dig +dnssec @127.0.0.1 internetweek.jp A
- 結果が返ってくること
  - ad フラグ: DNSSEC 検証成功

unbound-control

- unbound 動作を制御したり、統計情報を表示したりするツール
  - /usr/local/sbin/unbound-control
- コマンド例
  - start　起動
  - stop　終了
  - reload　設定ファイル再読み込み
  - flush *name*　キャッシュから *name* の A,AAAA,MX,
  - PTR,NS,SOA などを削除
  - flush_zone *name*　*name* 以下の名前を削除
  - status　ステータス表示
  - stats　統計情報表示