FreeBSD 10でunboundを使ってみる

力武 健次 （りきたけ けんじ）/ @jj1bdx

2013年11月28日 DNSOPS.JP BoF

そもそもなんでUnbound を使うことになったのか

- BINDのサポートが大変
  - リリーススケジュールとの調整が難しい
- DNSSEC validationの効率的実装をしたい
  - libcを書き換えたくない
  - local caching resolverが欲しい
- さらに詳しい事情はこちらを
  - http://blog.des.no/2013/09/dns-in-freebsd-10/

PortsからUnboundもBINDも なくなるということはありません

- FreeBSD 10のbaseに組み込む実装は全部/usr/sbinの下に入るが，Portsは/usr/localの下なので関係ない
- baseのライブラリは/usr/lib/private (!)というなかなか変な名前のディレクトリに入る（ここのライブラリの中身をbase以外で触ったらどうなるのかは予想がつかない）
- BINDを使いたければPortのdns/bind99あたりが良
- baseのUnboundはlibeventをリンクしてないので，大規模なcache resolverならPortのdns/unboundがおすすめ

実際の設定は?

- /etc/rc.confにこの1行だけ

  local_unbound_enable=“YES"

- **service local_unbound start** で起動します
- 実際には /usr/sbin/local-unbound-setup が動いてセットアップをしてくれます

/etc/resolv.confが消えてなくなるわけではありません

- resolvconf(8) というコマンドで自動設定
- こんな感じです

```
search priv.example.com
options no_tld_query
# nameserver 172.xx.yyy.1
# nameserver 172.xx.yyy.2
nameserver 127.0.0.1
options edns0
```

- 127.0.0.1に他のcache resolverを動かしている場合は設定変更が当然ですが必要です

Unboundのデフォルト設定で困ること

- man 5 unbound.conf を良く読む必要あり
- プライベートアドレスの逆引きはデフォルトではnxdomainを返すようになっている
- ローカルゾーンを定義してやる必要あり

ローカルゾーン用設定例(1)

```
# /var/unbound/private.conf
server:
        # these local-zones are
        # to unblock private address reverse lookups
        local-zone: “priv.example.com." nodefault
        local-zone: "xx.172.in-addr.arpa." nodefault
        local-zone: "d.f.ip6.arpa." nodefault

        # insecure domains for DNSSEC
        domain-insecure: "priv.k2r.org"
        domain-insecure: "xx.172.in-addr.arpa"
        domain-insecure: "d.f.ip6.arpa"
```

ローカルゾーン用設定例(2)

```
# /var/unbound/forward.conf
forward-zone:
        name: .
        forward-addr: 172.xx.yyy.1
        forward-addr: 172.xx.yyy.2
        forward-addr: fdxx:yyy:zzz:qqq::ww:1
        forward-addr: fdxx:yyy:zzz:qqq::ww:2
```

ローカルゾーン用設定例(3)

```
# /var/unbound/unbound.conf
# Generated by local-unbound-setup
server:
        username: unbound
        directory: /var/unbound
        chroot: /var/unbound
        pidfile: /var/run/local_unbound.pid
        auto-trust-anchor-file: /var/unbound/root.key
# ここからは手動で追加
include: /var/unbound/private.conf
include: /var/unbound/forward.conf
```

Unbound+ldns他の変化によるメリット

- OpenSSHでSSHFP RRのvalidationができるようになった
- local_unboundをenableすることで,
  resolv.confのresolver数制限(3)を気にせずに,
  好きなだけforwarderの相手が増やせる
- DHCPなどの動的設定にも自動で対応できる

余談: FreeBSD 10の開発状況

- 現在テスト中 (10.0-RC1) (2013-12-09現在)，2014年初めにリリースの予定
- 基本的には磐石かつ安定している
- libiconvがCitrusベースとなりlibcに組み込まれたことによる問題が10.0-BETA3まではあったが，現在は解消している．この問題に関する共有ライブラリのoverloadingによる対策はこちら: https://github.com/jj1bdx/freebsd-gnu-libiconv-hack
- 9.2-RELEASEを使っていれば移行は苦労しないはず

要約

- FreeBSD 10からはUnbound+Idnsが標準装備
- 今までのPortsとは一切干渉しない
- とはいえUnboundなのでプライベートアドレスだとそれなりの設定は必要
- FreeBSDの中では/usr/lib/privateとか作って結構ややこしいことになっているが，今後のことを考えて今回の実装変更を行った