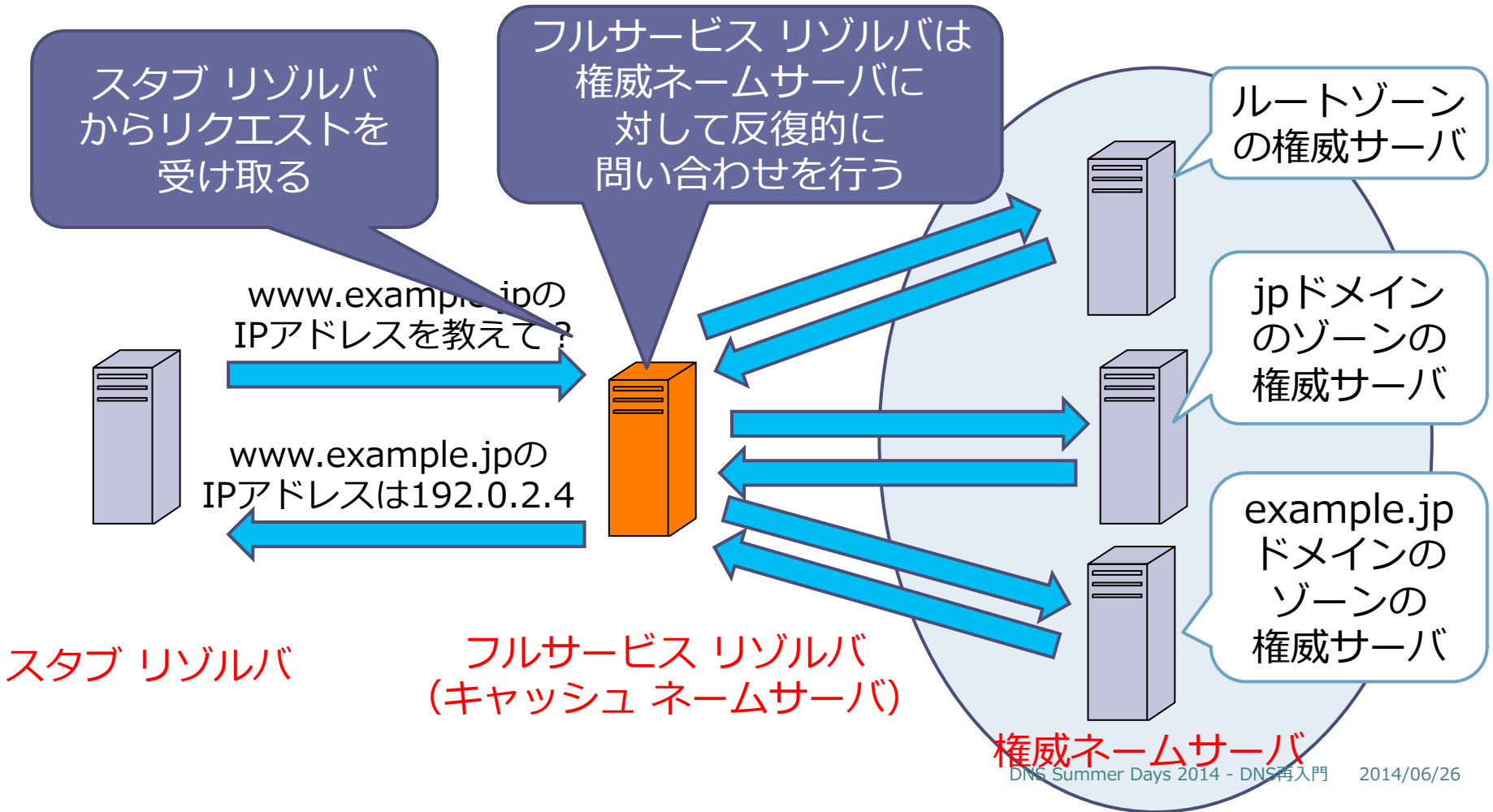
夏のDNS祭り 2014　2014-07-05

ハンズオン - Unbound編

株式会社ハートビーツ 滝澤 隆史

フルサービス リゾルバ


スタブ リゾルバからリクエストを受け取る
フルサービス リゾルバは権威ネームサーバに対して反復的に問い合わせを行う
www.example.jpのIPアドレスを教えて？
www.example.jpのIPアドレスは192.0.2.4
ルートゾーンの権威サーバ
jpドメインのゾーンの権威サーバ
example.jpドメインのゾーンの権威サーバ
スタブ リゾルバ
フルサービス リゾルバ（キャッシュ ネームサーバ）
権威ネームサーバ

Unboundのインストール

Unboundのインストール

- Fedora EPELで提供されているRPMパッケージをインストールする。
  - ConoHaのVPSでは標準でEPELのリポジトリが登録されている。
  - EPELリポジトリが入っていない場合は次のページを参照
    - https://fedoraproject.org/wiki/EPEL
- yumコマンドでインストールを行う。

```
$ sudo yum --enablerepo=epel install unbound
```

unbound-controlの準備

- 下記作業はrcスクリプト内で実行されるため不要
- unbound-control用の公開鍵証明書とプライベート鍵のペアの作成

```
$ cd /etc/unbound
$ sudo unbound-control-setup
$ sudo chgrp unbound unbound_*.{key,pem}
$ ls -l unbound_*.{key,pem}
-rw-r----- 1 root unbound 1277  7月 3 17:36 2014 unbound_control.key
-rw-r----- 1 root unbound  802  7月 3 17:36 2014 unbound_control.pem
-rw-r----- 1 root unbound 1281  7月 3 17:36 2014 unbound_server.key
-rw-r----- 1 root unbound  790  7月 3 17:36 2014 unbound_server.pem
```

Unboundの設定

- 設定ファイルのディレクトリに移動
  ```
  $ cd /etc/unbound
  ```
- インストール時の設定をバックアップ
  ```
  $ sudo cp -p unbound.conf{,.orig}
  ```
- 設定の確認
  ```
  $ sed '/^.*#/ d;/^$/ d' unbound.conf
  ```
- デフォルトのままで利用可能
  - 必要に応じて、interface, access-controlを設定
  - デフォルト値は小規模向けなので大規模向け用途の場合にはチューニングも行う。

Unboundの設定

- EPELのunboundパッケージでは余計な設定が入っているので無効化
  - prefetchの記述をコメントアウト

    ```
    #prefetch: yes
    ```
  - dlv-anchor-fileの記述をコメントアウト

    ```
    #dlv-anchor-file: ～
    ```

Unboundの設定

```
server:
    verbosity: 1
    interface: 0.0.0.0
    interface: ::0
    access-control: 192.0.2.1/24 allow
    access-control: 2001:db8:dead:beef::1 allow
    rrset-roundrobin: yes
    minimal-responses: yes
    edns-buffer-size: 1280
remote-control:
    control-enable: yes
```

デフォルトはローカルホストにバインド。ホスト自身のリゾルバとして使用する場合はデフォルトのままにする。

デフォルトはローカルホストのみ許可。他のホストにサービスを提供する倍は許可するネットワークを指定する。

unbound-controlを使うため有効にする。

RFC 6891 Extension Mechanisms for DNS (EDNS(0)))
"Choosing between 1280 and 1410 bytes for IP (v4 or v6) over Ethernet would be reasonable. "

Unboundの設定（チューニング）

- 『Unbound: Howto Optimise』W.C.A. Wijngaards
  - http://www.unbound.net/documentation/howto_optimise.html
  - http://unbound.jp/unbound/howto_optimise/
- 『DNSキャッシュサーバ チューニングの勘所』東 大亮さん
  - http://www.slideshare.net/hdais/dns-32071366
- 項目
  - num-threads
  - msg-cache-slabs, rrset-cache-slabs, infra-cache-slabs, key-cache-slabs
  - rrset-cache-size, msg-cache-size
  - outgoing-range, num-queries-per-thread
  - so-rcvbuf

Unboundの起動

```
$ sudo service unbound start
Starting unbound: Jul 03 17:49:46 unbound[3491:0]
warning: increased limit(open files) from 1024 to
8290
                                                    [  OK  ]
```

動作確認

```
$ dig @127.0.0.1 . SOA +multi
中略
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8283
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.                      IN SOA

;; ANSWER SECTION:
.                       86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. (
                                2014070300 ; serial
                                1800       ; refresh (30 minutes)
                                900        ; retry (15 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )

;; Query time: 517 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jul  3 18:50:35 2014
;; MSG SIZE  rcvd: 92
```

動作確認（DNSSECの検証もできる）

```
$ dig @127.0.0.1 . SOA +multi +dnssec
中略
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24503
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
中略
;; ANSWER SECTION:
.                       86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. (
                                2014070300 ; serial
                                1800       ; refresh (30 minutes)
                                900        ; retry (15 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )
.                       86400 IN RRSIG SOA 8 0 86400 20140710000000 (
                                20140702230000 8230 .
                                cb+Fahc6QqFbLwe2kse8uQJJlmJHQvJdl9Zl+P1H5umf
                                rtnWqrW2S/OHG/tYYrgl47QV3AAMmC3DRqX/IpxmEgpg
                                rGsE2lpeLyhq3bbBG5/svghJIjj8fIp44tcyx5g0ixys
                                /xKA2W1J85PCojN5He6YkOF8F44EZqK3HocaQNQ= )
```

以下略

resolv.confの修正

- /etc/resolv.conf
  - 以下の内容を記述

```
nameserver 127.0.0.1
```

- ConoHa VPSはDHCPを使用している再起動時にも反映させるために以下の作業も行う。
- /etc/sysconfig/network-scripts/ifcfg-eth0
  - 以下の内容を追加

```
PEERDNS=yes
DNS1=127.0.0.1
DNS2=127.0.0.1
```

動作確認

```
$ dig . SOA +multi
中略
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14900
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.                      IN SOA

;; ANSWER SECTION:
.                       86400 IN SOA a.root-servers.net. nstld.verisign-grs.com. (
                                2014070300 ; serial
                                1800       ; refresh (30 minutes)
                                900        ; retry (15 minutes)
                                604800     ; expire (1 week)
                                86400      ; minimum (1 day)
                                )

;; Query time: 398 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jul  3 18:52:58 2014
;; MSG SIZE  rcvd: 92
```

OS起動時にunbound起動

```
$ sudo chkconfig unbound on
$ sudo chkconfig --list unbound
unbound  0:off  1:off  2:on  3:on  4:on  5:on  6:off
```

unbound-control

基本操作

- 停止

```
$ sudo unbound-control stop
ok
```

- 起動

```
$ sudo unbound-control start
Jul 03 19:45:04 unbound[6797:0] warning:
increased limit(open files) from 1024 to
8290
```

- リロード

```
$ sudo unbound-control reload
ok
```

キャッシュの操作

- キャッシュのダンプ

```
$ sudo unbound-control dump_cache
```

- 指定したゾーンのキャッシュのクリア

```
$ sudo unbound-control flush_zone ゾーン
```

- 全ゾーンのキャッシュのクリア

```
$ sudo unbound-control flush_zone .
```

おわり